МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ УКРАИНЫ
ХАРЬКОВСКИЙ НАЦИОНАЛЬНЫЙ
УНИВЕРСИТЕТ РАДИОЭЛЕКТРОНИКИ

РАДИОТЕХНИКА

Всеукраинский межведомственный научно-технический сборник

ТЕМАТИЧЕСКИЙ ВЫПУСК «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Основан в 1965 г.

В Ы П У С К 1 9 5

Харків
Харківський національний
університет радіоелектроніки
2018

УДК 621.3

Сборник включен в список специальных изданий ВАК Украины по физико-математическим и техническим наукам.
Регистрационное свидетельство КВ № 12098-969 ПР от 14. 12. 2006.
Ответственность за содержание статей несут авторы.

Ответственный за выпуск: А.И. Лучанинов, д-р физ.-мат. наук, проф.
Технический секретарь Е.С. Полякова

Рекомендовано Ученым советом Харьковского национального университета радиоэлектроники, протокол № 74 от 28.12.2018.

Адрес редакционной коллегии: Харьковский национальный университет радиоэлектроники (ХНУРЭ), просп. Науки, 14, Харьков, 61166, тел. (0572) 7021-397.

Сборник «Радиотехника» включен в Каталог подписных изданий Украины, подписной индекс ***08391***

СОДЕРЖАНИЕ

ПЕРСПЕКТИВНЫЕ КРИПТОГРАФИЧЕСКИЕ СИСТЕМЫ И ПРОТОКОЛЫ
ПЕРСПЕКТИВНІ КРИПТОГРАФІЧНІ СИСТЕМИ ТА ПРОТОКОЛИ

И.Д. Горбенко, Е.Г. Качко, Ю.И. Горбенко, И.В. Стельник, С.А. Кандий, М.В. Есина Методы построения общесистемных параметров и ключей для NTRU PRIME UKRAINE 5 - 7 уровней стойкости. Product form 5

И.Д. Горбенко, А.Н. Алексейчук, О.Г. Качко, М.В. Есина, В.А. Бобух, С.О. Кандий, *В.А. Пономарь* Вычисление общих параметров для NTRU PRIME UKRAINE 6-7 уровней стойкости 17

Е.Г. Качко, Д.К. Телевный Криптоанализ хеш-функции Купина при использовании в схемах подписи Меркла 27

О.О. Кузнецов, Ю.І. Горбенко, М.С. Луценко, Д.І. Прокопович-Ткаченко, М.В. Пастухов NIST PQC: Кодові криптосистеми 32

О.А. Мельникова, О.В. Джурик, А.О. Маслєннікова Еліптичні криві Едвардса. Порівняння криптографічних бібліотек 41

І.Д. Горбенко, І.С. Кудряшов, В.В. Онопрієнко Порівняльний аналіз постквантових стандартів електронного підпису на основі мультиваріативних квадратичних перетворень 46

О.О. Кузнецов, Ю.І. Горбенко, А.С. Кіян, А.О. Уварова, Т.Ю. Кузнецова Порівняльні дослідження та аналіз ефективності гібридної кодової криптосистеми 61

А.А. Кузнецов, Е.П. Колованова, Д.И. Прокопович-Ткаченко, Т.Ю. Кузнецова Анализ и исследование свойств алгеброгеометрических кодов 70

Ю.І. Горбенко, Є.Ю. Каптьол Сутність та особливості реалізації методу Гровера на класичному комп'ютері для симетричного крипто аналізу 89

А.А. Кузнецов, А.В. Потий, Н.А. Полуяненко, С.Г. Вдовенко Комбинирующие и фильтрующие функции на основе регистров сдвига с нелинейными обратными связями 101

М.Ю. Родінко Оцінка стійкості симетричного блокового шифру «Кипарис» до диференційного криптоаналізу 113

А.А. Кузнецов, А.В. Потий, Н.А. Полуяненко, И.В. Стельник Нелинейные функции усложнения для потоковых симметричных шифров 125

МЕТОДЫ И АЛГОРИТМЫ ЗАЩИТЫ И СОКРЫТИЯ ИНФОРМАЦИИ
МЕТОДИ ТА АЛГОРИТМИ ЗАХИСТУ ТА ПРИХОВУВАННЯ ІНФОРМАЦІЇ

І.Ф. Аулов, К.Є. Лисицький Засоби моделювання та аналізу ризиків в середовищі хмарних обчислень 138

С.М. Конюшок Дослідження *k*-вимірності булевої функції шифру LILI-128 144

А.А. Кузнецов, И.В. Московченко, Д.И. Прокопович-Ткаченко, Т.Ю. Кузнецова Эвристические методы градиентного поиска криптографических булевых функцій 150

Г.В. Ахмаметьєва, Мпуту Крістофер Бвабва Стеганоаналіз цифрових зображень в умовах різного ступеню наповненості контентів 165

Д.Г. Биличенко, Е.Ю. Витюк, Р.В. Олейников Сравнительный анализ алгоритмов консенсуса для технологии распределенных реестров 174

В.І. Єсін, В.В. Вілігура Метод розробки баз даних, що легко адаптуються до змін в предметній області 184

О.О. Кузнецов, О.О.Стефанович, Д.И. Прокопович-Ткаченко, К.О.Кузнецова 3D стеганографічне приховування інформації 193

Е.В. Исирова, А.В. Потий Децентрализованные протоколы консенсуса: возможности и рекомендации по применению 203

МЕТОДЫ ВЫЯВЛЕНИЯ, РАСПОЗНАВАНИЯ И УПРАВЛЕНИЯ ЛЕТАТЕЛЬНЫМИ АППАРАТАМИ
МЕТОДИ ВИЯВЛЕННЯ, РОЗПІЗНАВАННЯ ТА УПРАВЛІННЯ ЛІТАЛЬНИМИ АПАРАТАМИ

В.Н. Олейников, О.В. Зубков, В.М. Карташов, И.В. Корытцев, С.И. Бабкин, С.А. Шейко Исследование эффективности обнаружения и распознавания малоразмерных беспилотных летательных аппаратов по их акустическому излучению 209

І.Д. Горбенко, О.А. Замула, С.Г. Вдовенко, В.І Черниш Метод оцінки зрілості системи управління безпекою при організації повітряного руху 218

А.А. Кузнецов, Р.В. Сергиенко, А.А. Уварова Нечеткий экстрактор на помехоустойчивых кодах для биометрической криптографии 224

В.М. Карташов, В.Н. Олейников., С.А. Шейко, С.И. Бабкин, И.В. Корытцев., О.В. Зубков Особенности обнаружения и распознавания малых беспилотных летательных аппаратов 235

РЕФЕРАТЫ 244

CONTENT

PERSPECTIVE CRYPTOGRAPHIC SYSTEMS AND PROTOCOLS

I.D. Gorbenko, O.G. Kachko, Yu. I. Gorbenko, I.V. Stelnik, S.O. Kandy, M.V. Yesina Methods for constructing system-wide parameters and keys for NTRU PRIME UKRAINE 5 – 7 stabvility levels. Product form 5

I.D. Gorbenko, A.N. Alekseychuk, O.G. Kachko, M.V. Yesina, V.A. Bobukh, S.O. Kandy, V.A. Ponomar General parameters for NTRU PRIME UKRAINE 6 – 7 stability levels calculation 17

O. Kachko, D. Televnyi The Kupyna hash function cryptanalysis with Merkle Trees Signature schemes 27

A.A. Kuznetsov, Yu.I. Gorbenko, M.S. Lutsenko, D.I. Prokopovych-Tkachenko, M.V. Pastukhov NIST PQC: Code-Based Cryptosystems 32

O. Melnykova, O. Dzhuryk, A. Masliennikova Edwards elliptic curves. Comparison of cryptographic libraries 41

I.D. Gorbenko, I.S. Kudryashov, V.V. Onoprienko Comparative analysis of post quantum standards for electronic signature based on multivariate quadratic transformations 46

A.A. Kuznetsov, Y.I. Gorbenko, A.S. Kiian, A.A. Uvarova, T.Y. Kuznetsova Comparative studies and analysis of efficiency code-based hybrid cryptosystem 61

A.A. Kuznetsov, I.P. Kolovanova, D.I. Prokopovych-Tkachenko, T.Y. Kuznetsova Analysis and investigation of algebraic geometric codes properties 70

Yu.I. Gorbenko, Ye.Yu Kaptyol Essence and features of Grover's method implementation on a classical computer for symmetric cryptanalysis 89

A.A. Kuznetsov, A.V. Potii, N.A. Poluyanenko, S.G. Vdovenko Combining and filtering functions in the framework of nonlinear-feedback shift register 101

M.Yu. Rodinko Evaluation of block cipher "Cypress" strength against differential cryptanalysis 113

A.A. Kuznetsov, A.V. Potii, N.A. Poluyanenko, I.V. Stelnik Combining and filtering functions in the framework of nonlinear-feedback shift register 125

METHODS AND ALGORITHMS FOR PROTECTION AND CONCEALING INFORMATION

I.F. Aulov, K.E. Lisickiy Tools for modeling and analysis of risks in the cloud computing environment 138

S.M. Koniushok Investigation of the k-dimensionality of the LILI-128 cipher Boolean function 144

A.A. Kuznetsov, I.V. Moskovchenko, D.I. Prokopovych-Tkachenko, T.Y. Kuznetsova Heuristic methods for gradient search of cryptographic Boolean functions 150

A. V. Akhmametieva, Mputu Chrisopher Bwabwa Steganananalysis of digital images in conditions of varying degrees of contents fullness 165

D. Bilichenko, K. Vitiuk, R. Oliynykov Comparative analysis of consensus algorithms for distributed ledger technologies 174

V.I. Yesin, V.V. Vilihura Method for developing databases being easily adaptable to changes in the subject domain 184

A.A. Kuznetsov, O.O. Stefanovych, D.I. Prokopovych-Tkachenko, K.O. Kuznetsova 3D steganography hiding of information 193

K.V. Isirova, O.V. Potii Decentralized consensus protocols: possibilities and recommendations for use 203

METHODS FOR AIRCRAFT DETECTION, RECOGNITION AND CONTROL

V.N. Oleynikov, O.V. Zubkov, V.M. Kartashov, I.V. Korytsev, S.I. Babkin, S.A. Sheiko Investigation of the efficiency of detection and recognition of small-sized unmanned aerial vehicles by their acoustic radiation 209

I.D. Gorbenko,O.A. Zamula, S.G. Vdovenko, V.I. Chernysh Method of Maturity Assessment of Air Traffic Management Security System 218

A.A. Kuznetsov, R.V. Serhiienko, A.A. Uvarova Code based fuzzy extractor for biometric cryptography 224

V.M. Kartashov, V.N. Oleynikov, S.A. Sheyko, S.I. Babkin, I.V. Koryttsev, O.V. Zubkov Peculiarities of small unmanned aerial vehicles detection and recognition 235

ABSTRACTS 244

ПЕРСПЕКТИВНЫЕ КРИПТОГРАФИЧЕСКИЕ СИСТЕМЫ И ПРОТОКОЛЫ

UDC 519.2:519.7

I.D. GORBENKO, Dr. Sc.,(Tecnology), O.G. KACHKO, Cand. Sc. (Tecnology), Yu.I. GORBENKO, Cand. Sc. (Tecnology), I.V. STELNIK, S.O. KANDYI, M.V. ESINA, Cand. Sc. (*Tecnology*)

METHODS OF BUILDING GENERAL PARAMETERS AND KEYS FOR NTRU Prime Ukraine OF 5^{th} – 7^{th} LEVELS OF STABILITY. PRODUCT FORM

Introduction

There is now a reasonable suspicion that in the post-quantum period, existing standards for asymmetric cryptographic transformations are likely to be broken up by a third-level crypt analyst with polynomial or sub-exponential complexity using quantum cryptanalysis systems [1 – 5]. An important feature of the post-quantum period is the significant uncertainty regarding the source data for cryptanalysis and counteraction – basically, in our opinion, in terms of the capabilities of quantum computers, their mathematical and software resources, as well as applications for cryptanalysis and the implementation of potentially possible attacks [1, 4 – 5]. Therefore, in the future, in the post-quantum period, cryptographic transformations and cryptographic protocols that will be stable both against classical and possible quantum crypto analytic systems should be applied. The indicated problem of creating and standardizing asymmetric cryptographic transformations that will be stable, both against classical and against quantum attacks, is extremely important and should be solved before the post-quantum period. Previous studies have shown that significant prospects for constructing asymmetric cryptographic transforms such as asymmetric cipher (ASC), key encapsulation protocol (KEP), and digital signature (DS) have cryptographic transformations based on the use of quantum polynomials over finite fields [6 – 8]. Due to the fact that algebraic lattices are among the effective attacks on the indicated transformations, the asymmetric transformations of the ASC, KEP and DS are also called as those ones based on “algebraic lattices”

The following cryptographic transformations: NTRUEncrypt ANSI X9.9 8 [9, 14]; NTRU prime [6, 16] and NTRU Prime Ukraine [10] are historically important achievements in the application of the “algebraic lattices”. The construction of the ASC and KEP projects with cryptographic stability of 1^{st} -5^{th} levels of stability is the maximum achievement in the first two directions. At the same time they require ASC, KEP and DS of the 6^{th} – 7^{th} levels, rather, for the post-quantum period, taking into account possible new achievements in the construction of quantum computers and their mathematical support and software. Moreover, under the 6th level of security, we will understand the resistance against 384 bits of classical cryptographic stability and 192 bits of quantum cryptographic stability, respectively, and under the 7th level of security we will understand the resistance against 512 bits of classical cryptographic stability and 256 bits of quantum cryptographic stability, respectively. The need for such levels of stability can also be explained by the standards of symmetric crypt-transforms [17], which provide 256 bits of quantum stability and a consistent application of both symmetric and asymmetric cryptographic transformations.

The results of the analysis showed that when constructing the ASC and KEP of the 6th – 7th levels it is necessary to solve the following problematic tasks:

- justification of methods for investigation and construction with their use of general parameters of cryptographic transformations;
- justification of methods and generation of asymmetric key pairs;
- justification of the method and implementation of direct and inverse cryptographic transformations of encryption and decryption;
- comparative analysis and decision-making on the choice of mechanisms of the ASC of the 6^{th}-7^{th} levels of cryptographic stability.

The purpose of this paper is to propose solutions to the first and second tasks, that is, methodological considerations and construction with their use of general-system parameters and keys of crypto-transformations of the ASC and the KEP of the 6^{th} – 7^{th} levels of stability, as well as experimental confirmation by means of software modeling in the case of using PRODUCT FORM [14] for private keys and blinding polynomial.

1. List and essence of general-system parameters and keys

Below is the essence and list of general-system parameters of the cryptographic transformations of the ASC and KEP of the 6^{th} – to 7^{th} levels of stability in the ring of polynomials over the finite field. When considering, we will focus on standard references and consider, respectively: NTRUEncrypt ANSI X9.98 [9, 14], NTRU Prime [6, 16] and NTRU Prime Ukraine [10].

The NTRU Prime Ukraine NSRU mechanism is a NTRU-like cryptosystem that is promising for use in the post-quantum period. The NTRU cryptosystem was chosen for several reasons. It is fully compliant with IEEE P1363 standards according to lattice-based public key cryptography specifications (IEEE P1363.1). The NTRUEncrypt cryptosystem provides high-speed and low-resource memory usage, and can be used in applications such as mobile devices and start-up cards. In April 2011, NTRUEncrypt was accepted as the ANSI X9.98 standard for use in financial services, currently it's tested by time. Taking into account known possible attacks, NTRU Prime Ukraine uses new parameters, such as those proposed in [6,16]. In addition, some reduction in the computational complexity of the ASC has been achieved. Algorithmic optimization and capabilities of modern computer systems (AVX-operations, parallelization, etc.) were used for optimization.

General-system parameters and keys, destination and formulas for their calculations are given in Tables 1, 2 [6 – 10].

Table 1

General-system parameters of ASC NTRU Prime

Notation	Use	Formula
$(Z/q)[x]$	Ring of polynomials Each element Z/q is usually encoded in $\lceil \log_2 q \rceil$ bit. Reduction is allowed due to the packaging of several elements in one	
n (N)	Polynomial order. Determines the number of its coefficients. A prime number for which the polynomial $x^n - x - 1$ is irreversible	$n \geq \max\{3, 2t\}$
P	Monic polynomial of n degree, irreducible over the field $(Z/q)[x]$, by which polynomials are reduced – elements of R/q field	$x^n - x - 1$
R	Ring of polynomials $Z[x]$ over a finite field with a module $x^n - x - 1$	$Z[x]/(x^n - x - 1)$
$R/3$	Ring of polynomials $(Z/3)[x]$ over a finite field with a module $x^n - x - 1$	$(Z/3)[x]/(x^n - x - 1)$
R/q	Ring of polynomials $(Z/q)[x]$ over a finite field with a module $x^n - x - 1$	$(Z/q)[x]/(x^n - x - 1)$
p	Smaller module, which reduces all the coefficients of the R / 3 polynomial	$p = 3$
t	The natural number, the number of nonzero elements of T polynomial depends on this parameter.	$t \geq 1$, T = 2t
q	Larger module, the prime number, by which all the coefficients of the polynomial R/q are reduced	$q \geq 48t + 3$
k	Level of cryptostability	256, 384, 512

It should be noted that $R/3 \subset R/q \subset R$ as plurals.

A small element is also *t*-small if it has exactly 2*t* nonzero coefficients.

The number of non-zero elements in the private key and in the blinding polynomial is determined by *n* and the cryptostability *k*, which must be ensured. For all parameters they are identical and equal to T.

Table 2

Parameters and keys required for generating keys

Notation	Use	Formula
G	Random small polynomial, reversible in $R/3$. The number 1 and -1 is not necessarily equal. The secret parameter used to calculate the public key.	G ∈ R/3 T=2n/3+1
F	Random t-small polynomial that defines a private key	$F \in R/3$ $T=2t$
f	A small polynomial, irreducible in R/q, is a private (personal) key.	$f=(1+3F) \bmod q \ \ f \in R/q$
h	The sender's public key.	$h=3g/f \in R/q$
$\underline{h}$	h encoded in a row	The length $\underline{h}$ is equal to $n\lceil \log_2 q \rceil$

2. Presentation of elements of polynomials ring over a finite field

For any odd number l we denote the ring Z_l of classes of residues by the module l. Further, the elements of this ring are identified with the integers belonging to the segment $[-1/2(l-1), 1/2(l-1)]$. In particular, for any $a \in Z$ the record $a \bmod l$ denotes a single integer $a' \in [-1/2(l-1), 1/2(l-1)]$ such that $a \equiv a' \bmod l$.

Let us fix a natural number t and different prime numbers n, q such that $n \geq \max\{3, 2t\}$, $q \geq 48t+3$ and the polynomial $x^n - x - 1$ is irreducible over the field Z_q. Let's also mark

$$R = Z[x]/(x^n - x - 1),\ R/q = Z_q[x]/(x^n - x - 1),\ R/3 = Z_3[x]/(x^n - x - 1).$$

Let's consider that $R/3 \subset R/q \subset R$ as plurals.

From the above conditions, it follows that the ring R/q is a ring of polynomials over a finite field, which consists of q^n polynomials of the form $u = u_0 + u_1 x + \cdots + u_{p-1} x^{n-1}$, where u_i there are integers of the interval $[-1/2(q-1), 1/2(q-1)]$, $i \in \overline{0, n-1}$ which are added and multiplied by the modulum q. In this case, the addition and multiplication of the polynomials themselves (elements of the field R/q) takes place by the modulus of the polynomial $x^n - x - 1$.

For any polynomial $u = u_0 + u_1 x + \cdots + u_{n-1} x^{n-1} \in R$ denote $u \bmod q$ by the polynomial $(u_0 \bmod q) + (u_1 \bmod q)x + \cdots + (u_{n-1} \bmod q)x^{n-1} \in R/q$. $u \bmod 3$ notation has also a similar meaning.

Let us assume that $u \in R$ is called *small* if $u \in R/3$. A small polynomial will be called t*-small* one if it has exactly $2t$ nonzero coefficients.

Also, for any polynomial $u = u_0 + u_1 x + \cdots + u_{n-1} x^{n-1} \in R$ we denote in the form

$$\| u \|_\infty = \max_{0 \leq i \leq p-1} |u_i|, \qquad \| u \|_1 = \sum_{i=0}^{n-1} |u_i|,\ \| u \|_2 = \left(\sum_{i=0}^{n-1} |u_i|^2 \right)^{1/2}. \tag{1}$$

In the future, we will use similar notation for an arbitrary vector $u = (u_0, u_1, ..., u_{n-1}) \in R^n$.

In this work, as is customary in similar works, the notations are used:

$$\binom{a}{b} = \frac{a!}{b! * (a-b)!};\ \binom{a}{b\ \ c} = \binom{a}{b} * \binom{a-b}{c} \tag{2}$$

3. Method for calculation of general-system parameters and keys OF 6^{th} AND 7^{th} stability levels in F1 * F2 + F3 form (product form)

The performed analysis showed that, when using the special form of the task of the secret (private) key [11, 14], there is a possibility to reduce significantly the complexity (time) of such a key generation and the main operations associated with the generation of the public key, and performance of asymmetric encryption and decryption with stability of 128, 192 and 256 bits versus quantum attacks (256, 384, and 512 bits of classical attacks, respectively).

3.1. General statements

An algorithm for generating parameters is proposed in [11]. It is proposed for generating parameters with a maximum cryptostability of 256 bits for classical attacks (128 against quantum attacks) for a classical NTRU algorithm with a polynomial X^n-1 and a value $q = 2^m$, where the product form is used for the private key F and the polynomial r. The algorithm for formation of parameters for a polynomial x^n-x-1 is given in [6, 16]. It uses the standard polynomial format as an array of 1, -1, 0 with a limitation of cryptostability to K = 300 for classical attacks. In addition, the algorithms NTRUPrime [6, 16] and NTRUPrime Ukraine, considered in this work, use different algorithms for the formation of keys and cryptographic transformations, therefore there is a need for studying algorithms for generating parameters. In [15] the algorithm is presented and parameters for the 5^{th} – 7^{th} levels of stability for the usual polynomial problem are calculated. This paper is devoted to the algorithmic analysis of parameters generation for the 5^{th} – 7^{th} levels of stability in the case of using the product form that meets the requirements for a post-quantum ASC to provide 384 and 512 bits of cryptostability with respect to classical attacks and, respectively, 192 and 256 for quantum attacks.

The generation parameters, to provide 384 (192) and 512 (256) bits for the specified data, can be given in the following sequence [11 – 16]:

- choice of a prime number of n – degree polynomial;
- formation of key space for private keys;
- calculation of the maximum number of non-zero elements in the message;
- computing the security parameter based on the key space and the meet-in-the-middle attack (upper security boundary);
- calculation of the larger module *q;*
- calculation of the complexity (time) of a hybrid attack.

3.2. Choice of the degree of the polynomial *N*

A prime number is used as a polynomial degree. To select a minimum number, let us consider the attacks associated with the use of the sieve. According to [12], the minimum prime number must satisfy inequality:

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

For stability against classical attacks, k = 384, we obtain a prime number N = 659, and for a critical stability 512 we obtain a prime – N = 877. But, in accordance with [11], the minimum value of n for reciving cryptostability, which is not less than 256, is 743, exactly this value will be used as the minimum N.

3.3. Formation of key space for private keys

The transition to the cryptostability of the 6^{th} and 7^{th} levels requires an increase in the order of the polynomials N. This, in turn, leads to an increase in the computational complexity of the multiplication operations for these polynomials. In order to reduce this effect, for the representation of small polynomials, instead of the usual one, a special form of the polynomial (product) [11] is used: $F=F_1*F_2+F_3$, for specification of which 3 polynomials are used: F_1, F_2, F_3. Each of them is a small polynomial, with an equal number of units and minus units, this number is, respectively, equal to d_1, d_2, d_3. By analogy with t-small ones, these are d_1, d_2, d_3 small polynomials. But the

number of units and minus units in them are the same. To obtain a polynomial F, we perform the multiplication operation of the polynomials F_1, F_2 followed by the modulation of the X^n-X-1 and the addition of the polynomial F_3.

The maximum number of nonzero elements for polynomial F: $2d_1 * 2d_2 + 2d_3$. The value of nonzero coefficients of a polynomial F may differ from the values of nonzero coefficients of the t-small polynomial, which extends the key space of the polynomial F with the appropriate choice of d_1, d_2, d_3.

To select d_1, d_2, d_3 authors [11] recommend the use of the following algorithm:

Let the values d_1, d_2, d_3 be respectively chosen for the polynomials F_1, F_2, F_3.

In order the search for keys, using the polynomials F_1, F_2, F, was approximately of the same complexity, we choose $d_1 \approx d_2 \approx d_3$.

To balance the number of zeros and nonzero elements d_1, d_2 and d_3, the condition $2d_1*d_2+d_3 \approx N/3$ must be satisfied, i.e., the value d_i is the positive root of the equation: $2d^2+d-N/3=0$, whose solution for a positive value d:

$$d_1 = \left\lceil \frac{-1+\sqrt{1+\frac{8N}{3}}}{4} \right\rceil;$$

$$d_2 = \left\lceil \frac{\frac{N}{3}-d_1}{2d_1} \right\rceil \qquad (4)$$

$$d_3 = \max \left\lceil \frac{\frac{d_1+1}{2}}{\frac{N}{3}-2d_1d_2} \right\rceil$$

But for practical purposes, the authors [11] used formulas (4) to find d_1, d_2. And values of d_3 were chosen more than d_1, d_2. Thus, for N = 743 from formulas 4 we get d_1, d_2=11, d_3=6, and according to Table 3 [11] for N = 743 the values d_1, d_2 = 11, d_3 = 15. This is probably due to the need to increase the key space to provide the required cryptostability against the MITM attack.

In the future, we use the following formula for calculation:

$$d_1 = d_2 = \left\lceil \frac{-1+\sqrt{1+\frac{8N}{3}}}{4} \right\rceil; \qquad (5)$$

The value of d_3 is determined so that at N close to N, obtained for the usual form of setting keys, to provide the necessary cryptostability, when using the Product Form [15].

For N = 743 the values of d_1, d_2 =11, d_3 = 15 [11].

Regarding the key G, the usual method of setting 1 and -1 elements is used for its setting. To provide the maximum key space for this key, the number of units is N/3 +1, the number of minus items is N/3. When calculating N/3, it may be a rejection of a fractional part or a rounding. For example, rounding is used in [11], while the fractional part is thrown away in EESS # 1 [14].

In the course of the research, both methods were considered and it was discovered experimentally that the choice of the method did not actually affect other parameters.

3.4. Calculation of the maximum number of nonzero elements in the message

When encrypting the data the disguised message, converted into a small polynomial, should contain a sufficient number of non-zero elements, defined by d_m parameter to protect against attacks. On the other hand, if the number of non-zero elements is large, then the probability of re-selecting a mask and multiplying by a blinding polynomial will be high. This factor greatly affects the computational complexity of encryption.

To select the maximum possible value of d_m, where the probability of repeated execution of the multiplication operation does not exceed 2^{-10}, the formula [11] is used:

$$2^{-10} \geq 1 - \frac{\sum_{i=d_m}^{N-2d_m-1}\left(\sum_{j=d_m}^{N-d_m-i}\left(\binom{N}{i}\binom{N-i}{j}\right)\right)}{3^N} \quad (6)$$

For N=739, we get d_m=205, which coincides with [11].

3.5. Calculation of the security parameter based on the key space and the meet-in-the middle attack (upper security boundary)

To calculate the security parameter, taking into account the key space and meet-in- the middle attack, the number of keys, taking into account their form of representation and the meet-in-the middle attack, is determined.

For this purpose, the square root of this quantity is calculated, that is, [11]

$$O\left(\sqrt{\frac{\binom{N}{d_1}\binom{N}{d_2}\binom{N}{d_3}}{N}}\right); \quad (7)$$

where $\binom{N}{d}$ – is the number of keys, taking into account the number of (1) and (-1), that is

$$\binom{N}{d} = \binom{N}{d} * \binom{N-d}{d} \quad (8)$$

In (7) the division into N takes into account the possibility of cyclic transformation (automorphism) of the key.

Inequality [11] is used to determine the minimum prime number that provides the required cryopresistance *k*.

$$2^k \leq \sqrt{\frac{\binom{N}{d_1} * \binom{N}{d_2} * \binom{N}{d_3}}{N}} \quad (9)$$

This formula is used to calculate d_3 for N. If $d_3 > 3d_1$, then the next N is chosen. The latter condition is related to the efficiency of multiplying the polynomials given in the product form..

As the calculations show the condition (9) is much stronger than the condition (3), which we used previously to determine the minimum prime number. The results of the determination of N and the values of d_1, d_2, d_3 for cryptostabilities 256, 384 and 512 are given in Table 3 after the definition of q.

3.6. Ensuring no errors in decoding. Formation of q

In [11], the mechanism of the ASC of the transformation is determined, which basically coincides with the ASC transformation for NTRUPrime Ukraine, with the exception of using the algorithm of the field $R/q = Z_q[x]/(x^n - x - 1)$ in the last instead of the ring (Z / qZ) [X] (XN-1) and simple q instead of $q = 2^m$.

When encrypting/decrypting, the following operations are performed:

$$E_h(m,r) = c = (m + rh) \bmod q,\ m, r \in R/3,\ \text{h} \in \text{R/q} \quad (10)$$

$$D_f(c) = (cf(\bmod q) \bmod 3,\ c \in R/q \quad (11)$$

Sufficient conditions for error-free decryption are also defined, which set restrictions for the module q

$$\| mf + 3rg \|_\infty < q/2 \quad (12)$$

Consider the condition (7) for the case of using the product form for the keys F and *r*.

Let $r = r_1 * r_2 + r_3$, $F = F_1 * F_2 + F_3$ where $r_1, r_2, r_3, F_1, F_2, F_3$ d – are small polynomials. In this case $\|r\|_1 \leq \|r_1\| * \|r_2\| + \|r_3\| = 4d_1 * d_2 + 2d_3$; $\|F\|_1 \leq \|F_1\| * \|F_2\| + \|F_3\| = 4d_1 * d_2 + 2d_3$, where d_1, d_2, d_3 – are the number of 1 (-1) in the polynomials. Then the condition (7) $\| mf + 3rg \|_\infty < q/2$ taking into accounta $\| m \|_\infty = \| g \|_\infty = 1$, f = 3F + 1, and values $\|r\|_1, \|F\|_1$, can be presented in the form of:

$3(8d_1d_2+4d_3) < q/2 - 1$. From here

$$q \geq 24(2d_1d_2+d_3) + 3. \quad (13)$$

Thus, if a product form is used, the value q is determined by the values d_1, d_2, d_3. The minimum value of q is determined from the inequality (8). In addition, the value q must be prime and such that the polynomial $x^n - x - 1$ is irreducible over the field $\mathbf{Z}_q$.

Table 3 lists the parameters that provide the required cryptographic stability and the absence of decryption errors without taking into account the combined attack.

Table 3

Values of parameters that provide
the required cryptostability and lack of decryption errors

K	N	d_1	d_2	d_3	d_m	q
256	743	11	11	15	205	6263
384	1019	13	13	31	290	8867
512	1409	16	16	43	411	13327

3.7. Calculation of complexity (time) of hybrid attack execution

The calculation of complexity (time) is performed in the following way. Matrix-base is divided into 2 parts. One part of the length of the r lines is used to search the key part with the help of "meet-in-the middle" attack, the other, using the length 2N-r, is processed as part of the lattice. Finding the optimal r, in which the "meet- in-the middle" attack and attack on the lattice gives roughly the same time, that exceeds the needed one, taking into account the required cryptosecurity.

3.7.1. Meet- in-the middle attack

As a search object, you can select F key, for which the product form is used and G key, for setting of which the regular polynomial F/3 is used with a number of N/3 + 1 units and -1 N/3. Next $d_G = \frac{N}{3}$. If key G is found, then it is easy to find G^{-1}, and then F.

Next, let's consider the use of G key for search. The number of rows of the base, for which *r* search is performed, and the number of -1 in key G (d_G) are used as search parameters. The method from [11] is used to determine the time complexity of a hybrid attack.

To prevent the message from being reproduced, a combined attack is also considered with respect to a polynomial having d_m units (minus units).

The method of using a combined attack for key G and message M is the same, so it is further described for key G. The minimum time, required for both attacks, is taken as the final result.

First, the key space is defined, that is, the total number of keys G

$$Total = \binom{N}{d_G + 1 \quad d_G}$$

To determine the probability of the presence of *a* units and b -1 in the selected base area, the following formula is used:

$$P(v(a,b)) = \frac{\binom{N-r}{d_G+1-a \quad d_G-b}}{Total}$$

The probability $P(v(a,b))$ is used to calculate the number of H (p) versions, that should be considered:

$$H(P) = -\sum_{\substack{0\le a\le d_G+1,\\ 0\le b\le d_G}} \binom{r}{a \quad b} P(v(a,b)) log_2 P(v(a,b))$$

Taking into account the specifics of the "meeting-in-the middle" attack and the possibility of cyclic keys permutations, the general formula for calculating the time for the "meeting-in-the middle" attack is:

$$T_{MITM}(N,r,\ d_G) \ge 0.5(H(P) - log_2 N); \quad (14)$$

$T_{MITM}(N,r,\ d_m)$ is determined similarly.

Table 4 shows the calculation results of $T_{MITM}(N,r,\ d_G)$ for cryptostability of the 6th and 7th levels for d_G and d_m

Table 4

Combined attack. MITM (6th and 7th levels of cryptostability)

K	N	d_G	$T_{MITM}(N,r,d_G)$	r(d_G)	d_m	$T_{MITM}(N,r,d_m)$	r(d_m)
256	743	247	256	329	205	256	338
384	1019	339	384	491	290	384	501
512	1409	469	512	653	411	512	661

The value r (d_m) is used for the next attack, it exceeds r (d_G) for all K values..

3.7.2. Attack on the lattice

Let the size of the lattice, for which the attack is performed, be S = 2N – r.

1. First, the Hermite constant is determined using the formula:

$$h = e^{\frac{\ln\sqrt{\pi eq/2}}{S}} \quad (15)$$

2. The size of the block β and the iteration number m are sought for the lattice, for which the Hermite constant value is selected. The initial size of the block is 60, the final size is S. The BKZ-2 emulator [18] is used for searching.

3. The value of the attack on the lattice is determined, that is, the number of operations for the construction of Korkin-Zolotarev-reduced basis of a complete lattice of dimension S:

$$T_{Lattice} = 2^{E(\beta,m,S)}, \quad (16)$$

where $E(\beta,m,S) = 0{,}000784314\beta^2 + 0{,}366098\beta + \log_2(Sm) + 0{,}875$

This time should not be less than the value that corresponds to the cryptostability K.

Table 5 shows the experimental results of calculation of $T_{Lattice}$, agreed with T_{MITM} for cryptostability of the 6th and 7th levels for $r = \max(\mathrm{r}(d_G),\ \mathrm{r}(d_m))$.

Table 5

Combined attack. Attack on the lattice
(Cryptostability of the 6th and 7th levels)

K	N	r	T_{MITM}	β	m	$T_{Lattice}$
256	743	338	256	342	18	232
384	1019	501	384	499	16	393
512	1409	661	512	758	17	744

As can be seen from Table 5 for K = 256 $T_{Lattice} < 256$, i.e., to achieve the cryptostability of 256 it is necessary to increase the value of N. For K = 384 and 512 values of $T_{Lattice} > K$, to determine the most effective attacks, it is necessary to agree the value of *r*.

According to the calculations, to ensure the cryptostability of K = 256 in case of using not only the MITM and attack on the lattice, it is necessary to choose the parameters

N= 787, d_1 =12, d_2 =12, d_3 =15, d_m =219, d_G =262

The first row of Table 5 shows these parameters:

K	N	r	T_{MITM}	β	m	$T_{Lattice}$
256	787	337	256	374	17	262

These are parameters used later for K = 256.

3.7.3. Calculation of time for hybrid attack

You can choose different ways to calculate the time for a hybrid attack.

1. By formula 12, find the minimum value of *r*, at which $T_{MITM}(N,r,\ d_G) \geq K$, $T_{MITM}(N,r,\ d_m) \geq K$. For *r*, determine the size of the lattice (S = 2N – r). Determine the time required for cryptanalysis in accordance with 3.7.2 for a lattice of a given size. If for the given S the $T_{Lattice} \geq K$ parameters are found, matching parameters for finding r is being performed, in which both times exceed K, and the difference between $T_{Lattice}$ and T_{MITM} is minimal.

2. Start calculations to determine the minimum size of the lattice S for which $T_{Lattice} \geq K$. For r = 2N-S determine $T_{MITM}(N,r,\ d_G)$, $T_{MITM}(N,r,\ d_m)$ for the MITM attack. If the parameters $T_{MITM}(N,r,\ d_G) \geq K$, $T_{MITM}(N,r,\ d_m) \geq K$ are found. matching of the parameters is carried out as in the previous case.

3. Use an iterative algorithm, in which simultaneously execute the values $T_{MITM}(N,r,\ d_G)$, $T_{MITM}(N,r,\ d_m)$, for the selected *r*. In this case, r is determined, in which all three values satisfy the condition of the cryptostability K and are the closest to each other. Such a method is used in [11, 6].

In the case of solution of the problem for cryptostability more than 256, the time for the solution of each task is essentially significant. We use the first way, as the most effective on the part of computational complexity.

The results for the hybrid attack after matching are given in Table 6.

Table 6

Hybrid attack

K	N	r	T_{MITM}	β	m	$T_{Lattice}$
256	787	343	260.69	371	18	259
384	1019	508	390.16	496	15	390
512	1409	817	633.39	684	16	633

4. Algorithm of calculation of general system parameters

The above justification allowed us to construct a set of general-system parameters for the post-quantum asymmetric cryptographic transformations of the ASC and KEP type experimentally by means of software simulation. The algorithm given below is intended for generating general-system parameters and a suite of parameters for the ASC on an algebraic lattice with resistance 2^{512} to classical attacks and 2^{256} against attacks based on a quantum attack. The algorithm is implemented taking into account the data given in [9]. Thus, the generation of parameters is proposed to be performed in such a sequence.

Input data: K Security Level

Output data: **N, $\mathbf{d_1}, \mathbf{d_2}, \mathbf{d_3}$, $\mathbf{d_G}$, $\mathbf{d_m}$, q**

1. Choose a prime number N (n) (Formula 3)
2. Calculate values d_1, d_2, d_3 (Formula 5)
3. Calculate a value $d_G = \frac{N}{3}$
4. Determine the cryptostability k (Formula 9), which is provided by the selected N, d_1, d_2, d_3. If k <K, then choose the next prime number N and proceed to step 2 of the algorithm
5. Calculate the value of d_m (Formula 6)
6. Calculate the value of q, which must satisfy the condition (Formula 8), be prime and such that the polynomial $x^n - x - 1$ is irreducible over the field $\mathbf{Z}_q$
7. Calculate the minimum value 0 <r ≤ N, at which $T_{MITM}(N, r, d_G) > K$, $T_{MITM}(N, r, d_m) > K$ are simultaneously executed (Formula 14). If there is no such value, then choose the next prime number and go to step 2
8. Calculate the size of the lattice S = 2N – r
9. Calculate $T_{Lattice}$ (Formula 16)
10. If $T_{Lattice} < K$, choose the next prime number and go to step 2
11. If $T_{Lattice} < K$, choose the next prime number and go to step 2 2
12. While $T_{Lattice} > T_{MITM}$
    a. r:=r + 1;
    b. Calculate $T_{MITM}(N, r, d_m)$ (Formula 12)
    c. Calculate $T_{Lattice}$ (Formula 14)

Table 7 provides a complete set of parameters for PRODUCT FORM representing the private key F and dazzling polynomial r (Cryptostability of the 6th and 7th levels).

Table 7

Parameters for NTRUPrime Ukraine
(Cryptostability of 6th and 7th levels).
PRODUCT FORM

K	N	d_1	d_2	d_3	dm	q
256	787	12	12	15	219	7307
384	1019	13	13	31	290	8867
512	1409	16	16	43	411	13327

Conclusion

1. In the future, in the post-quantum period, cryptographic transformations and cryptographic protocols that will be resistant to classical and possible quantum cryptographic analytical systems should be applied. The problem of creating and standardizing asymmetric cryptographic transformations that will be stable, both against classical and against quantum attacks, is pointed out, and it is extremely important and should be solved before the post-quantum period.

2. Previous studies have shown significant prospects for constructing asymmetrical cryptographic transforms such as asymmetric code (ASC), key encapsulated protocol (KEP) and digital signature (DS) have cryptographic transformations based on the use of rings of polynomials over finite fields.

3. Historically important advances in the application of "algebraic lattices" are the following cryptographic transformations as: NTRUEncrypt ANSI X9.9 8; NTRU prime and NTRU Prime Ukraine.

4. When using the special form F1 * F2 + F3 the private (personal key) task the possibility appears to reduce significantly the complexity (time) of generating such a key and the basic operations related to generating a public key, as well as performing asymmetric encryption and decryption with a resistance of 128, 192 and 256 bits against quantum attacks (256, 384 and 512 bits of classical attacks, respectively).

5. The substantiated and implemented algorithm for generating general-system parameters has allowed to construct a suite of parameters for the ASC on the algebraic lattice with a resistance of 2^{384},.. 2^{512} against classical attacks and 2^{192}, 2^{256} against attacks based on a quantum attack.

6. The performed simulation has allowed to obtain experimentally a set of general-system parameters for k = 384 and $k = 512$ for the post-quantum ASC.

References:

1. Neal Koblitz and Alfred J. Menezes A Riddle wrapped in an Enigma. Department of Mathematics, Box 353.350, University of Washington, Seattle, WA 98195 U.S.A. – Access mode: https://eprint.iacr.org/2015/1018.pdf.

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

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

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

5. Gorbenko Yu. I. Methods of construction and analysis, standardization and application of cryptographic systems: monograph / Yuri I. Gorbenko. – Kharkov : Fort, 2016. – 959 p. (In Ukr.)

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

7. NTRU Open Source Project [Electronic resource]. – Access mode: https://github.com/NTRU OpenSource Project/ntru-crypto.

8. I. Gorbenko, O. Kachko, K. Pogrebnyak. Features of parameters calculation for NTRU algorithm // Прикладная радиоэлектроника. – 2015. – Т. 14. – № 3. – С. 272-277.

9. American National Standard X 9.98-2010. Lattice-Based Polynomial Public Key Encryption Algorithm Part 1: Key Establishment: Part 2: Data Encryption, 2010.

10. Gorbenko I.D. General Provisions and Analysis of NTRU Prime IIT Ukraine Directional Encryption Algorithm / I.D Gorbenko, O.G. Kachko MV Yesina // Radiotechnika. – 2018. – № 193. – P. 5-16. (In Russ.)

11. Horstein J. Choosing Parameters for NTRUEncrypt / J.Horstein, J.Pipher, J.Schanck, J.Silverman, W. Whyte, Z. Zhang [Electronic resource]. – Access mode: https://eprint.iacr.org/2015/708.pdf.

12. Laarhoven Th. Sieving voe closest lattice vectors (with preprocessing). [Electronic resource]. – Access mode: https://arxiv.org/pdf/1607.04789.pdf.

13. Nick Howgrave Graham NTRU Cryptosystems Technical Report. Report #4, Version 2. A Meet-In-The-Middle Attack on an NTRU Private key / Nick Howgrave Graham, Joseph H. Silverman, William Whyte [Electronic resource]. – Access mode.

14. Efficient Embedded Security Standards (EESS) [Electronic resource]. – Access mode: https://github.com /NTRUOpenSourceProject/ntru-crypto/blob/e5655c2a10b74b5a0256ca849dbe85e4860f2eb5/doc/EESS1-2015v3.0.pdf.

15. Gorbenko I.D. Improved method for generating system-wide parameters for NTRU Prime Ukraine / I.D. Gorbenko, O.G. Kachko, Yu.I. Gorbenko, M.V. Yesina // Radiotechnika. – 2018. – № 195. – P. 5 – 16.

16. Daniel J. Bernstein. Chitchanok Chuengsatiansup, Tanja Lange, Christine van Vredendaal NTRU Prime: reducing attack surface at low cost. [Electronic resource]. – Access mode: https://eprint.iacr.org/2016/461.pdf

17. Gorbenko I., Kuznetsov A., Lutsenko M. and Ivanenko D. The research of modern stream ciphers // 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T). – Kharkov, 2017. – P. 207-210.

18 Yuanmi Chen and Phong Q. Nguyen. BKZ 2.0: Better Lattice Security Estimates. [Electronic resource]. – Access mode https://www.iacr.org/archive/asiacrypt2011/70730001/70730001.pdf

JSC «Institute of Information Technologies»;
Kharkiv National V.N. Karazin University;
Kharkiv NationalUniversity of Radio Electronics *Received 06.11.2018*

UDC 004.056.55

I.D. GORBENKO, Dr. Sc. (Technology), A.N. ALEKSEYCHUK, Dr. Sc. (Technology),
O.H. KACHKO, Cand. Sc. (Technology), M.V. YESINA, Cand. Sc. (Technology),
V.A. BOBUKH, Cand. Sc. (Technology), S.O. KANDYI, V.A. PONOMAR Cand. Sc. (Technology)

CALCULATION OF GENERAL PARAMETERS FOR NTRU PRIME UKRAINE OF 6-7 LEVELS OF STABILITY

Introduction

Investigations of perspective (including post-quantum) asymmetric cryptanalytic transforms such as asymmetric code (ASC), key encapsulation protocol (KEP) and digital signature (DS) confirm the promising use for constructing post-quantum transformation standards in polynomial rings over finite fields [1 – 4]. The main candidates for constructing the asymmetric cryptographic transforms are NTRUEncrypt ANSI X9.98 [1], NTRU Prime [2] and NTRU Prime Ukraine [3]. Special attention was paid to the ASC and KEP construction in [1], since they provide cryptographic stability up to 256 bits of classical stability and up to 128 bits of quantum stability.

At the same time, the standards of symmetric cryptographic transformations have been constructed and used, which provide cryptographic stability of 512 bits of classical and 256 bits of quantum stability [5, 6]. Therefore, in our opinion, in the long run, the ASC, KEP and DS of 6-7 levels of stability are needed. Moreover, under the 6th level of security it is proposed to understand resistance against 384 bits of classical cryptographic stability and 192 bits of quantum cryptographic stability, respectively, and under the 7th level of security it is proposed to understand resistance against 512 bits of classical cryptographic stability and 256 bits of quantum cryptographic stability, respectively. The implementation of 6-7 levels of stability is associated with the complex problematic task of constructing common parameters and keys for cryptographic transformations in a ring of polynomials over finite fields for recognized and accepted security models [4, 9].

The purpose of this paper is to carry out research and develop an effective practical algorithm for construction and experimental confirmation of the built-in system-wide parameters and keys of cryptographic transformations of the ASC and KEP of 6-7 levels of stability based on transformations in a ring of polynomials over finite fields.

1. Method for calculating general parameters for the algorithm (NTRU Prime Ukraine)

1.1. Basic concepts and notation

Let us consider the general provisions regarding the algorithm of the ASC in the ring of polynomials over a finite field called NTRUPrime [2, 4]. The generation of system-wide parameters is one of the important stages of the ASC mechanism in this algorithm. Let's consider its general provisions regarding the general parameters of NTRUPrime.

Let us denote the ring of residue classes Z_l modulo l for any odd number l. Elements of such a ring are identified with integers belonging to the segment $\left[-1/2\,(l-1), 1/2\,(l-1)\right]$. For any $a \in Z$ the record $a \bmod l$, means the unique integer $a' \in \left[-1/2\,(l-1), 1/2\,(l-1)\right]$ such that $a \equiv a' \bmod l$. Let us fix the general parameters of the algorithm NTRUPrime: a natural number t and different prime numbers n, q such that

$$n \geq \max\{3, 2t\},\ q \geq 48t + 3 \text{ and polynomial } x^n - x - 1, \tag{1}$$

which is irreducible over the field $\mathbf{Z}_q$ [2,4]. Let us also denote the ring of polynomials

$$R = Z[x]/(x^n - x - 1),\ R/q = Z_q[x]/(x^n - x - 1),\ R/3 = Z_3[x]/(x^n - x - 1), \tag{2}$$

where $R/3 \subset R/q \subset R$ as sets.

From the above it follows that in the NTRUPrime the ring of polynomials R/q is a field that consists of q^n polynomials of the form $u = u_0 + u_1 x + \cdots + u_{n-1} x^{n-1}$, where u_i are integers from the segment

$$\left[-1/2\,(q-1), 1/2\,(q-1)\right],\ i \in \overline{0, n-1}, \tag{3}$$

which are added and multiplied modulo q. At the same time, the multiplication of the polynomials themselves (elements of the field) takes place by the modulus of the polynomial $x^n - x - 1$. Also, for any $u = u_0 + u_1 x + \cdots + u_{n-1} x^{n-1} \in R$ let us denote polynomial $u \bmod q$

$$(u_0 \bmod q) + (u_1 \bmod q)x + \cdots + (u_{n-1} \bmod q)x^{n-1} \in R/q. \tag{4}$$

A similar meaning has a notation $u \bmod 3$, i.e.

$$(u_0 \bmod 3) + (u_1 \bmod 3)x + \cdots + (u_{n-1} \bmod 3)x^{n-1} \in R/3. \tag{5}$$

Polynomial $u \in R$ of the (2) type is called *small* polynomial, if $u \in R/3$, that is, the coefficients of the polynomial take values (-1, 0, 1). Also, we will call such a polynomial *t*-ternary (*small*) if it has exactly 2*t* nonzero coefficients (-1, 1).

For any $u = u_0 + u_1 x + \cdots + u_{n-1} x^{n-1} \in R$ we will use such notation

$$\| u \|_\infty = \max_{0 \le i \le n-1} | u_i |,\ \| u \|_1 = \sum_{i=0}^{n-1} | u_i |,\ \| u \|_2 = \left(\sum_{i=0}^{n-1} | u_i |^2 \right)^{1/2}. \tag{6}$$

Next, consider the requirement for *q* defined for $q \ge 48t + 3$. In essence, this condition defines the requirement for an admissible *q* value, which ensures the uniqueness of the encryption and decryption algorithms. Moreover, as shown by the preliminary analysis, there is a need for a reasonable reduction of the value of *q*, first of all for the ASC of 6 and 7 levels of cryptographic stability.

2. Determination of the ASC transformation mechanism

After the construction of system-wide parameters, the next step is the formation (generation) of an asymmetric key pair. Let us consider the problem of forming an asymmetric key pair for an algorithm in the NTRUPrimeUkraine.

2.1. Analysis of algorithm for key generation

To generate the keys, we chose the standard generation scheme, which was proposed in [1].

1. A small polynomial $G \in R/3$ is formed, for which there exists $G^{-1} \bmod q$.
2. A *t*-small polynomial $F \in R/3$ is formed.
3. The polynomial value $f = 3F + 1$ is calculated.
4. The polynomial $h = 3g / f \in R/q$ is calculated.

Polynomials *f* and *h* are the secret and public keys, respectively.

Note that the value h is calculated in the field R/q by multiplying the polynomial $3g$ by the polynomial, which is inverse to f in R/q. This is always possible, since the reverse f^{-1} polynomial exists, because $\| f \|_1 = 2t > 0$.

In [7] the scheme of keys formation is offered, in which the public key is calculated by the formula $h=G/(3F)$ and polynomials F, $G^{-1} \bmod 3$ are stored as the private key. However, such a scheme requires additional multiplication by G^{-1} in the process of decoding. This process also contains two multiplications, substantially different in time from the direct transformation, which requires only one multiplication, the additional multiplication will further increase the asymmetry.

As arguments, the authors suggest the following: a reduction in the length of keys and insignificant increase in time for decryption in the case of using hardware for the implementation of transformations. Indeed, as shown below, the value of *q,* compared with the version applied to NTRUPrime, is increased by 1.5 times. A twofold increase reduces the length of each coefficient by only one bit. An increase by 1.5 times, as a rule, practically does not increase the length of the polynomial element. Indeed, parameters for n=761, t=143, q≥32*143+1=4591 (simple irreducible). In the case of packing 3 numbers, as recommended by authors [7], it requires 37 bits, that is, 5 bytes. When using q≥48*143+1=6869 (simple irreducible). Packing of 3 numbers requires 39 bits, that is, 5 bytes too. At the same time, for the private key you need to store an additional component G^{-1}, which significantly increases the secret key. Below we will show you how to define a limit on q value in the conditions of key generation according to the proposed scheme to provide guaranteed decryption for 6 and 7 levels of stability.

2.2. Pseudo-trapdoor one-way function

Let us consider the requirements and the possibility of reducing q based on the analysis of a pseudo-trapdoor function using cryptographic transformations of the ASC and KEP type in the ring of polynomials over a finite field.

It is known [1 - 3], that for any private key f and the corresponding public key h in the ring of polynomials over a finite field, there are functions of encryption E_h and decryption D_f

$$E_h(m,r) = c = (m + rh) \bmod q\ ,\ m,r \in R/3\ ,\ \| r \|_1 = 2t\ , \tag{7}$$

$$D_f(c) = (cf(\bmod q) \bmod 3\ ,\ c \in R/q\ . \tag{8}$$

Let us determine the conditions under which the uniqueness of encryption (7) and decryption (8) are ensured.

Statement 1 [1, 2]. Encryption (7) and decryption (8) uniqueness is provided for any of the above key data f, g, h, r and message m, that is

$$D_f(E_h(m,r)) = m\ . \tag{9}$$

Proof of property (9) is given in [1], but a polynomial x^n-1 and q=2048 is considered there. Let us consider it, but at the same time let us define the conditions of reduction and the admissible limit of the value of the module q.

Let the cryptogram $c = E_h(m,r)$ be received as a result of encryption, and when decrypting the message $m' = D_f(c)$. Let us prove that $m = m'$ and define the condition of uniqueness. In the proof, we will substitute the value from (7) in (8). As a result, we get

$$(cf) \bmod q = (mf + rhf) \bmod q\ . \tag{10}$$

Next we substitute the value of h in (10), as a result we have

$$(mf + 3rgf\ /\ f) \bmod q = (mf + 3gr) \bmod q\ . \tag{11}$$

Analysis (11) shows that if the moduli of the coefficients of the polynomials mf and $3rg$ of the polynomial $mf + 3rg \in R$ are smaller than $q/2$ and, in general, the condition

$$\| mf + 3rg \|_\infty < q/2\ , \tag{12}$$

is fulfilled, then (10), taking into account (12), can be presented in the following form

$$(cf) \bmod q = (mf + 3rg) \bmod q = mf + 3rg. \tag{13}$$

Taking into account (10) and (12), when decoding *R/3* in the polynomial ring, we have

$$m' = (cf(\bmod q)) \bmod 3 = (mf) \bmod 3 + (3rg) \bmod 3 = (mf) \bmod 3 + 0\ . \tag{14}$$

Finally, we will substitute (7) in (14) and have

$$m' = (m(1+3F) \bmod 3 = m + 0 = m. \quad (15)$$

Thus, to ensure the uniqueness of encryption (7) and decryption (8), that is, $D_f(E_h(m,r)) = m' = m$ it is enough to make sure that inequality (12) is fair. In essence, (12) is necessary, but with certain constraints even sufficient condition.

Next, let us consider the possibility of reducing the value of q and determine to what extent this can be done to ensure unambiguity and no error in decoding. For this we use the lemma from [7].

Lemma. For any $u, v \in R$ following inequalities are fair

$$\| uv \|_\infty \le 2 \| u \|_\infty \| v \|_1, \ \| uv \|_\infty \le 2 \| u \|_2 \| v \|_2.$$

First, let us use the lemma to clarify its proof and the conditions for uniqueness of decryption, and then consider the essence of its proof.

Using formulas (14) and taking into account that in the NTRU Prime Ukraine messages are the polynomial m and key data are the polynomials g and F belong to $R/3$, that is, the polynomial coefficients take values (-1, 0, 1) and taking into account that $\| m \|_\infty = \| g \|_\infty = 1$, $\| F \|_1 = \| r \|_1 = 2t$ we have that the maximum coefficient of polynomial (15) can be determined in this way

$$\begin{aligned} &\| mf + 3rg \|_\infty = \| m(1+3F) + 3rg \|_\infty \le \| m \|_\infty + 3 \| mF + rg \|_\infty \le \\ &\le 1 + 3(2 \| m \|_\infty \| F \|_1 + 2 \| g \|_\infty \| r \|_1) = 1 + 6(\| m \|_\infty \| F \|_1 + \| g \|_\infty \| r \|_1) \le 1 + 24t < q/2. \end{aligned} \quad (16)$$

The last inequality follows from the fact that for our case $q \ge 48t + 3$ .Thus, statement 1 is proved.

Note that if we use the polynomial F instead of the polynomial 1 + 3F in formula (16) we obtain $16t<q/2$, which is equivalent to the requirement $q \ge 32t+1$. It is precisely this expression used to calculate q in [6].

Now let's show that the lemma also holds, that is, that it is true and its use is correct.

It should be noted that in fact the lemma argues that the maximum value of the coefficient [7] is limited

$$\| uv \|_\infty \le 3 \| u \|_\infty \| v \|_1, \ u, v \in R. \quad (17)$$

That is, we can conclude that the decryption of messages in the cryptosystem of the NTRU Prime Ukraine is correct, but subject to condition $q \ge 48t + 3$ [2]. Detailed proof of the lemma. Let $u = \sum_{i=0}^{n-1} u_i x^i$, $v = \sum_{i=0}^{n-1} v_i x^i$; then the product of the polynomials u and v in the ring $Z[x]$ equals $\sum_{i=0}^{2n-2} w_i x^i$, where $w_i = \sum_{j=0}^{i} u_j v_{i-j}$, $i \in \overline{0, 2n-2}$. Consequently, the product of these polynomials in a ring R equals

$$uv = (w_0 + w_n)x^0 + \sum_{i=1}^{n-2} (w_i + w_{i+n} + w_{i+n-1})x^i + (w_{n-1} + w_{2n-2})x^{n-1}.$$

Further, for any $i \in \overline{1, n-2}$ such equalities are fair:

$$w_i + w_{i+n} + w_{i+n-1} = \sum_{j=0}^{i} u_j v_{i-j} + \sum_{j=0}^{i+n} u_j v_{i-j} + \sum_{j=0}^{i+n-1} u_j v_{i-j} =$$

$$= \sum_{j=0}^{i-1} u_j v_{i-j} + u_i (v_0 + v_{n-1}) + \sum_{j=i+1}^{n-1} u_j (v_{i+n-j} + v_{i+n-1-j}) = \quad (18)$$

$$= (u_0 v_i + u_1 v_{i-1} + \cdots + u_i v_0 + u_{i+1} v_{n-1} + u_{i+2} v_{n-2} + \cdots + u_{n-1} v_{i+1}) +$$

$$+ (u_i v_{n-1} + u_{i+1} v_{n-2} + \cdots + u_{n-1} v_i).$$

Hence,

$$| w_i + w_{i+n} + w_{i+n-1} | \le$$

$$\le \max_{0 \le l \le n-1} | u_l | (| v_i | + | v_{i-1} | + \cdots + | v_0 | + | v_{n-1} | + | v_{n-2} | + \cdots + | v_{i+1} |) +$$

$$+ \max_{0 \le l \le n-1} | u_l | (| v_{n-1} | + | v_{n-2} | + \cdots + | v_i |)$$

$$\le 2 \max_{0 \le l \le n-1} | u_l | \sum_{j=0}^{n-1} | v_j | = 2 \| u \|_\infty \| v \|_1 .$$

Similarly, we obtain that

$$| w_0 + w_n | \le 2 \| u \|_\infty \| v \|_1 , \; | w_{n-1} + w_{2n-2} | \le 2 \| u \|_\infty \| v \|_1 ,$$

wherefrom the validity of the formula (14) follows.

Further, based on the formula (18) and Cauchy-Bunyakovskii inequality we find that $| w_i + w_{i+n} + w_{i+n-1} | \le 2 \| u \|_2 \| v \|_2$, $i \in \overline{1, n-2}$; furthermore,

$$| w_0 + w_n | \le 2 \| u \|_2 \| v \|_2 , \; | w_{n-1} + w_{2n-2} | \le 2 \| u \|_2 \| v \|_2 ,$$

Where from the validity of formula (17) follows.

3. Analysis of encryption and decryption algorithms

The padding scheme [NAEP] [10] is used to ensure the stability of the cryptosystem against attacks based on the adaptively selected encrypted messages (IND-CCA2 security). Note that the very padding scheme is used in [1].

Three functions are used in the encryption and decryption algorithms shown below:

$$F : Message \times Random\ bits \to R / 3 ,$$

$$G : Message \times Random\ bits \times Public\ key \to \{ r \in R / 3 : \| r \|_\infty = 2t \} ,$$

$$H : R / q \to R / 3 ,$$

The first function is a reversible mapping, that is, so that each of the functions F and F^{-1} has a fast computation algorithm, and the last two are constructed on the basis of keyless, but stable, hash functions.

Encryption algorithm [1].

Input: natural numbers l_1, l_2; public key h, message $M \in \{0,1\}^{l_1}$.

1: **repeat**

2: generate a random equiprobable vector $b \in \{0,1\}^{l_2}$.

3: calculate $r = G(M, b, h)$, $m = (F(M, b) + H(rh (\mathrm{mod}\, q))) \bmod 3$.

4: **until** each of the number of coefficients of the polynomial m equal to 1, −1 and 0, respectively, is at least t.

5: calculate $E_h(m, r) = (m + rh) \bmod q$.

Output: encrypted message $c = E_h(m, r)$.

Decryption algorithm.

Input: private key (f, g), public key h; encrypted message $c \in R / q$.

1: put $m' = D_f(c) = (cf(\bmod q)) \bmod 3$, $\tilde{r} = (c - m') \bmod q$;

2: calculate $(M', b') = F^{-1}\left((m' - H(\tilde{r})) \bmod 3\right)$, $r' = G(M', b', h)$;

3: **if** $\tilde{r} = (r'h) \bmod q$ and each of the numbers of the polynomial m' coefficients equal to 1, -1 and 0, respectively, are at least no less than t, then $M = M'$;

4: **else** $M = \perp$

5: **end if**

Output: M.

Based on the results of 2.2, the presented encryption scheme ensures that there are no errors in messages decoding.

4. Selection (generation) of parameters

Algorithms for generating parameters for classical NTRU and NTRUPrime are given in [1, 2, 4, 7, 11] and others. In all the papers devoted to the generation of parameters, the parameters are formed for cryptographic stability up to 256 bits inclusive. The feature of this subsection is that it considers the construction of general parameters of the ASC and KEP for cryptographic resistance 2^{512} against classical attacks and 2^{256} against quantum attacks, using the techniques outlined in other works.

According to the cryptographic transformation scheme given in subsections 1 and 2, the following parameters should be selected:

- a prime number *n*, which defines the order of a polynomial;
- parameter *t*, which determines the number of non-zero elements in a small polynomial;
- parameter *q*, which defines a module for polynomial coefficients that specifies an public key. The same module is used for cryptographic transformations of encryption and decryption.

4.1. Selection of a minimum prime *n*

To select a minimum prime number, let us consider the attacks associated with using the sieve. According to [14, 15], the minimum prime number must satisfy inequalities

$$2^k \le (3/2)^n \tag{19}$$

For resistance against classical attacks, *k*=512 we obtain a minimum of *n*=877.

4.2. Selection of the parameter *t*

The task of restoring a private key $(f = (1 + 3F) \bmod q, g)$ under the public key h of a cryptosystem is reduced to solving an equation $(h' + 3Fh') = G$ for unknowns $F, G \in \frac{R}{3}$, where $\| F \| = 2t$ and $h' = (3^{-1} h) \bmod q$. This problem can be formulated as follows.

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

$$\| (h' + 3Fh') \bmod q \|_\infty = 1 \tag{20}$$

The complexity of solving a given task by a complete overview of all polynomials $F \in \Phi$ requires $| \Phi | = 4^t \binom{n}{2t}$ operations.

The given function increases monotonically with the increase in *n*. The value $\log_2|\Phi|=1088$ corresponds to the minimum *n*=883 and *t*=145 (choice of *t* is discussed below), which almost 2 times exceeds the required complexity.

To reduce the complexity you can apply attacks under the general name “meet-in-the-middle attacks”.

Depending on the cryptosystem, there are various estimates of the complexity of this attack. To ensure the stability of the cryptosystem under consideration, with respect to the meet-in-the-middle attacks, the values of n and t are selected for a given security parameter k based on the condition

$$2^k \le 2^{t+1}\binom{n}{2t}^{1/2}. \tag{21}$$

The value t, obtained by formula (21), limits the cryptostability value k above, that is, to provide a guaranteed possibility to achieve a predetermined value of k, taking into account other attacks, it is necessary to set the value k with the stock to calculate the value of t in formula (21). That is, the value $k + \Delta k$ should be used instead of $k = 512$ in formula (21). The value of the parameter $\Delta k = k / 2$ has been experimentally found in the calculation of parameters.

4.3. Selection of *q* parameter

To exclude the decryption error, you must choose a prime number for the given n and t

$$q \ge 48t + 3 \tag{22}$$

such that the polynomial $x^n - x - 1$ is irreducible over the field Z_q.

One set of values (n, t) corresponds to many q values. The performed analysis showed that q value choice may affect the length of the message being encrypted, because the increase in q value increases the number of bits for its internal appearance. As our calculations have shown, it is enough to choose the smallest q, which satisfies formula (22).

4.4. Attack on the lattice

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

$$\begin{pmatrix} 1 & 0_{1\times n} & h' \\ 0_{n\times 1} & I_n & H \\ 0_{n\times 1} & 0_{n\times 1} & qI_n \end{pmatrix}. \tag{23}$$

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

To assess the attack on the lattice (construction of the reduced base B of the lattice the traditional approach is use [8]. It is believed that the base B is constructed using the block algorithm of Korkin-Zolotarev: BKZ 2.0 [13]. The BKZ 2.0 algorithm depends on the natural parameters β and m, which denote the so-called *block length* and the *number of iterations*, respectively, and allows us to construct a base of the complete N-dimensional lattice for $C = 2^{E(\beta, m, N)}$ operations reduced according to Korkin-Zolotarev, where

$$E(\beta, m, N) = 0,000784314\ \beta^2 + 0,366078\ \beta + \log(nm) + 0,875. \tag{24}$$

The values of β, m are found using the BKZ 2.0 emulator [13].

4.5. Essence and vulnerability of a combined attack

Previous studies have shown that among the potential analytical attacks the combined (hybrid) attack is the most vulnerable one [9].

The essence of the attack is as follows. First, the base of the lattice (24), which corresponds to the algorithm, is divided into 2 parts. The first part is used to attack the lattice, the "meet-in-the-middle" attack is applied to the second part. To determine the parameters there is such a division option, for which:

- cryptostability for each type of attacks provides the necessary value;
- attacks require about the same time, this time is defined as the cryptostability of the system against a combined attack.

In [9] a formula was got for evaluating the complexity of the "meet-in-the-middle" attack depending on the number of base rows used for this attack. A similar attack is considered in [7], where another formula is provided. Different formulas relate to the fact that methods of analytical calculation of this complexity are not known. We used both methods in our implementation. With regard to the method for determining the complexity for the lattice, in these works and others, the BKZ 2.0 emulator is used.

Table 1 demonstrates the results of determining the parameters for the cryptosecurity of 512 bits.

Table 1

Parameters for cryptosecurity of 512 bits

n	t	q	r	T'_{MITM}	T''_{MITM}	$T_{Lattice}$
1259	210	10103	752	512	469	513
1283	214	10289	797	541	494	513
1289	215	10331	808	548	501	513
1291	215	10331	812	549	503	513
1297	216	10453	823	556	510	512
1301	217	10427	830	562	514	514
1303	217	10429	835	564	517	513
1307	218	10499	842	570	522	513
1319	220	10567	866	584	537	512
1321	220	10597	867	585	537	514
1327	221	10613	881	592	546	512
1361	227	10957	943	630	585	512
1373	229	11057	965	644	599	513
1381	230	11059	981	653	608	513
1399	233	11213	1014	674	629	514
1409	235	11299	1035	689	642	512
1423	237	11383	1059	704	657	514
1427	238	11437	1068	711	663	512
1429	238	11443	1072	712	665	512

Notations in the Table:

n – degree of the polynomial;

t – determines the number of non-zero elements in the secret key (dazzling polynomial);

r – the number of rows of the base for which the "meet-in-the-middle" attack is performed;

T'_{MITM} – the complexity of the attack, according to [9] (Bit);

T''_{MITM} – the complexity of the attack, according to [7] (Bit);

$T_{Lattice}$ – the complexity of the attack on the lattice (Bit).

Gray colors highlighted the values of the parameters for which both methods gave a positive result.

The results of the detailed analysis of the combined (hybrid) attack are given in [9]; it is assumed that, when implemented with protection from it, IND-CCA2 semantic resistance to quantum attack is provided.

Conclusions

1 In the future the cryptographic transformations of the ASC, KEP of 6-7 levels of stability type will be demanded. Under 6 security level, it is suggested to understand resistance against 384 bits of classical cryptographic stability and 192 bits of quantum cryptographic stability, respectively, and under 7 security level l, it is suggested to understand resistance against 512 bits of classical cryptographic stability and 256 bits of quantum cryptographic stability, respectively.

2. The implementation of 6-7 levels of stability is associated with the complex problem task of generating common parameters and keys for cryptographic transformations in the ring of polynomials over the finite fields for recognized and accepted security models.

3. There is a need for a reasonable decrease in the value of q, first of all for ASC 6 and 7 levels of cryptographic stability.

4. Unambiguous encoding (7) and decoding (8) is ensured for any of the above key data f, g, h, r and message m.

5. Following inequalities are fair for any $u, v \in R$

$$\| uv \|_\infty \le 2 \| u \|_\infty \| v \|_1 , \quad \| uv \|_\infty \le 2 \| u \|_2 \| v \|_2 .$$

6. According to the proposed scheme of cryptographic transformations, it is necessary to choose the following parameters:

- prime number n, which determines the order of the polynomial;
- parameter t, which determines the number of non-zero elements in a small polynomial;
- parameter q, which defines a module for polynomial coefficients that specifies a public key.

7. The results of determining the parameters for the cryptosecurity of 512 bits are shown in Table. 1 of this paper. It is believed that a combined attack is the most vulnerable to the ASC, IND-CCA2 semantic resistance to quantum attack is provided, while protecting against it.

References:

1. American National Standard X 9.98-2010. Lattice-Based Polynomial Public Key Encryption Algorithm Part 1: Key Establishment: Part 2: Data Encryption, 2010.

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

3. I. Gorbenko, O. Kachko, K. Pogrebnyak. Features of parameters calculation for NTRU algorithm // Прикладная радиоэлектроника. – 2015. – V. 14. – № 3. – P. 272-277.

4. Gorbenko I.D. General Provisions and Analysis of NTRU Prime IIT Ukraine Directional Encryption Algorithm / I.D. Gorbenko, E.G. Kachko, M.V. Yesina // Radiotekhnika: All-Ukr. Sci. Interdep. Mag. – Kharkiv : KNURE. – 2018. – № 193. – P. 5-16.

5. DSTU 7624: 2014. Information Technology. Cryptographic protection of information. The algorithm of symmetric block transformation. [On-line]. Internet: http://shop.uas.org.ua/ua/informacijni-tehnologii-kriptografichnij-zahist-informacii-algoritm-simetrichnogo-blokovogo-peretvorennja.html.

6. Gorbenko I., Kuznetsov A., Lutsenko M. and Ivanenko D. The research of modern stream ciphers // 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T). – Kharkov, 2017. – P. 207-210.

7. Bernstein D.J. NTRU Prime / Bernstein D.J., Chuengsatiansup Ch., Lange T., van Vredendaal Ch. // [Electronic resource]. – Access mode: http://eprint.iacr.org/2016/461.

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

9. Wunderer Th. Revising the hibrid attack: improved analysis and refined security estimates // http://eprint.iacr.org/2016/733.

10. Howgrave-Graham N. NAEP: provable security in the presence of decryption failures / Howgrave-Graham N., Silverman J.H., Singer A., Whyte W. // [Electronic resource]. – Access mode: http://eprint.iacr.org/2003/172.

11. Choosing Parameters for NTRUEncrypt Jeff Hoffstein, Jill Pipher, John M. Schanck, Joseph H. Silverman , William Whyte, and Zhenfei Zhang// [Electronic resource]. – Access mode: https://eprint.iacr.org/2015/708.pdf.

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

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

14. Becker A., Ducas L., Gama N., Laarhoven Th. New directions in nearest neighbor searching with application to lattice sieving // SODA 2016. – Proccedings. SIAM, 2016. – P. 10 – 24.

15. Laarhoven Th. Sieving voe closest lattice vectors (with preprocessing). [Electronic resource]. – Access mode: https://arxiv.org/pdf/1607.04789.pdf.

JSC "Institute of Information Technologies", Kharkiv;
Institute for Special Communications and Information Protection
of the National Technical University of Ukraine "Igor Sikorsky
Kyiv Polytechnic Institute";
V.N. Karazin Kharkiv National University;
Kharkiv National University of Radio Electronics

Received 02.10.2018

UDC 004 056 55

O. KACHKO, Ph.D., D. TELEVNYI

THE KUPYNA HASH FUNCTION CRYPTANALYSIS WITH MERKLE TRESS SIGNATURE SCHEMES

Introduction

In the modern world, digital signatures (DSAs) have become a crucial element in any cryptographic system. Their usage is not limited only by enterprise or banking systems. The application happens to be huger than thought. The «MUST HAVE» feature of every modern CRM or ERP system. The most widely used systems are based on the asymmetric pair cryptography.

With the development of quantum computing a new problem appears for existing signatures. Some are based on the asymmetric transformation, mostly in GF or EC. Thus, quantum algorithms can solve Discrete logarithm tasks or factorization in seemingly short time and memory which makes existing schemes vulnerable. To gain enough strength either a key size must be increased, or a signature run timing, that would result to insufficiency of the signatures.

Since late 70's other schemes were developed. One of them is hash-based signatures. But the machine capabilities did not allow to use them rather than RSA or DSAs.

Modern hardware lacks such problems, as well as new algorithms were developed. The signature schemes can be divided into OTS (Lamport, Winternitz, etc.) and FTS (Merkle trees, etc.).

Since the large scaling of systems, the later are more preferred. The main goal of this paper is to analyze the security of Merkle Tree Signature Schemes and the national standard application to it.

The Kupyna hash function

Ukraine had used the GOST 34.311-95 [1] has function before it was replaced in 2015 by DSTU 7564:2014 [2]. According to authors, the new hash function is based on common, well-known and reliable constructs. [3].

The construction concept features the Even-Mansour scheme with Davies-Mayer compress function and inner permutation block from Kalyna (DSTU 7664:2014) [2].

The hash function supports several modes, defined as Kupyna-n and the set of

$$n \in \{8s \mid s = 1,2,..64\}. \tag{1}$$

The recommended modes are Kupyna-256, 384, 512.

The hash function pads the input message into $m_1, \ldots, m_n$ parts of l bits (512, 1024). The computation consists of the compression function, which iteratively updates the previous block-hash, and the reduction function to form the output.

$$\begin{gathered} h_0 = IV \\ h_i = f\left(h_{i-1}, m_i\right), i = 1,..t \\ h = \Omega\left(h_t\right) \end{gathered} \tag{2}$$

The compression function is the part which can be attacked. The standard [dstu] defines it as

$$f\left(h_{i-1}, m_i\right) = T^{xor}\left(h_{i-1} xor m_i\right) xor T^{+}\left(m_i\right) xor h_{i-1} \tag{3}$$

The reduction function takes the n most significant bits from the sum by modulo 2 of the permuted last block hashes with non-processed one.

$$\Omega\left(h_t\right) = trunc_n\left(T^{xor}\left(h_t\right) xor h_t\right) \tag{4}$$

The latest step may be attacked by the collision search of a pair:

$$h = \Omega\left(h'_t\right)$$
$$h = \Omega\left(h_t\right) \quad (5)$$

Where both n-most significant bits of the value are the same despite the hash values being different.

It the current section we focus on the permutation steps security analysis. The construction of both T-permutations is similar with Grostl hash.

In the «Analysis of the Kupyna-256 Hash Function» [4] paper authors performed cryptanalysis on the Kupyna-256 permutation function.

They describe collision attacks on the round-reduced hash up to 5 rounds and collisions to the compression function up to 7 rounds.

The compression function attack included semi-free-start collisions and based on the rebound attack on Grøstl using SuperBox matching. [5,6]

Considering T^+ permutation has round constant adding with modulo 2^{64}, the paper provides modified attack rather than on Grostl.

The attack presumes finding the pairs of input value for T^+ and T^{xor}.

The results of rebound attacks are listed in table 1.

Table 1

Overview of collision attack on the compression function

rounds	Time complexity	Memory complexity
6	2^{70}	2^{70}
7	2^{125}	2^{70}

The collision attacks were performed on the Kupyna-256.

The attack on the reduced hash is a straight-forward rebound attack on the reduced Grostl-256. The idea of attack is representation of the hash function with permutations without the left-multiplication with 8X8 MDS matrix over GF 2^8 (so-called MixBytes step) and defining the MixBytes^{-1} inverse transformation. The hash function now has the following look (6).

$$\hat{h}_0 = MB^{-1}\left(IV\right)$$
$$\hat{h}_i = \hat{T}^{xor}\left(MB\left(\hat{h}_{i-1}\right) xor m_i\right) xor\, \hat{T}^{+}\left(m_i\right) xor\, \hat{h}_{i-1},$$
$$i = 1,..,t \quad (6)$$
$$h = \Omega\left(MB\left(\hat{h}_t\right)\right)$$

The results for collision attacks on the reduced Kupina-256 listed in table 2.

Table 2

Overview of collision attack on the reduced hash function

rounds	Time complexity	Memory complexity
4	2^{67}	2^{59}
5	2^{120}	2^{59}

Merkle Signature Scheme

One of the most notable cons of OTS (one-time signatures) is the key management. The cryptsystem must guarantee the identity of the used key and its consistency. Few public keys are to be used and their length should be rather short. To make such schemes feasible, an efficient key management system must be used to reduce the number of keys and their size.

Ralph Merkle introduced in his research paper a new signature scheme for signing many messages with one key. [7] The following scheme is based on the tree structure where all steps of signature process can be observed as a tree traverse. In fig. 1 a such tree is listed.

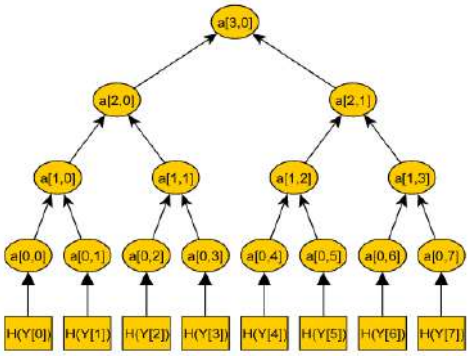


Figure 1. Merkle tree scheme

The big advantage of Merkle Signature Scheme is the fact that many messages are signed with a short number of keys. But the cost of such efficiency is inadequate. To generate a public key *pub*, 2^n OTS must be generated. If tree contains 2^{n+1} -1 nodes, the same number of hash function applying must be performed to get a public key. It's obvious that the size of the tree is limited with available memory and runtime complexity.

The signature generation requires *auth* nodes to be computed. To reduce of such inter-state nodes, some cache techniques must be applied. This increases the storage requirements.

Nevertheless, the verification time is quite fast comparing to the other steps.

The last researches were headed to build an algorithm to reduce the storage size and compute in efficient time. This strategy was called Merkel Tree traversal.

The signature of the Merkle Signature Scheme consists of the ots sig' and n nodes $auth_0$, ..., $auth_{n-1}$. If a 256-bit hash function is used, the signature size would be $|sig|=|sig'|+n*256$ bits.

To efficiently compute a node in tree a tree-hash algorithm is required. The main idea of it is calculating the needed sub-tree from left to right only saving the needed nodes.

The classic traversal computes at O(*2(H-1)*) complexity and O(H*(H+1)) memory. But in [8] a logarithm time and space algorithm was introduced by M.Szydlo. The main idea is reducing the active tree-hash instances. The presented algorithm stores *3log(N)* and computed in *2log(N)*, where N – number of available signatures.

The further development brought the idea of storing such trees and computing them in hypertrees – trees with sub-tree nodes of the same height. This approach is a fractal presentation of traversal.

A good value for h, in which the space requirements are minimal, would be $h = logH = loglogN$. Using this parameter would result in a time and space bound of $sig_{time} = 2logN/loglogN$ and $sig_{space} = 5/2log2N/loglogN$.

In [9] improvements were proposed: using PRNG with seeds for private keys generation. This idea supposes storing only seeds, relatively smaller to the private keys themselves.

The other idea is using many Merkle trees rather than a big one. The [9] lists the results of such approach to sign a message on Pentium dual core 1.8GHz. The following result is shown in table 3 below.

Table 3

Timing and memory results

signatures	Mem_{upd}	mem_{out}	mem_{sign}	t_{kgen}	t_{sign}	t_{verify}
2^{40}	3160 bytes	1640, bytes	1860 bytes	723 m	26.1 ms	19.6 ms
2^{40}	3200 bytes	1680, bytes	2340 bytes	390 m	10.7 ms	10.6 ms
2^{80}	7320 bytes	4320 bytes	3620 bytes	1063 m	26.0 ms	18.1 ms
2^{80}	7500 bytes	4500 bytes	4240 bytes	592 m	10.1 ms	10.1 ms

Merkle signature scheme cryptanalysis

The given section describes the security of the Merkle Signature Scheme. If an attacker has message *m* and *sig* and wants to counterfeit a signature of the *m`*, he has two cases.

The first presumes that attacker finds a valid sig'_a with a public key $Y_i`$ and $H(Y_i`) = H(Y_i) = A_0$. The attacker can achieve this by finding a valid OTS of the message *m`* with equal public keys, i.e $Y_i` = Y_i$. When found, this would mean that OTS is broken. Therefore, breaking OTS means the Merkle Signature Scheme also breaks. If this cannot be achieved, then the attack of a second preimage can be performed, i.e. finding sig'_a $H(Y_i`) = H(Y_i)$, $Y_i` \neq Y_i$.

Thus, the Merkle Signature Scheme is secure if the hash function in OTS is second preimage resistant. As mentioned in section 1, the Kupyna hash has such characteristics. The possible attack may occur only in case of a weak public key.

The other option is generation a valid sig'_a with a public key $Y_i`$ and $A`_i = H(Y_i`) \neq H(Y_i) = A_0$. In this case an auth path must be changed $A'n=An=pub$ with $A'i=H(a'i-1||auth'i-1)$ $i=1, ..., n$ to make a valid signature. If the attacker finds a single $auth'_i$ so that $H(A'_i||auth'_i) = A_{i+1}=A_{i+1}$, then a valid auth. path is found.

Hence to counterfeit an attack $auth'_i$ must be found, so that $H(A'_i||auth'_i) = H(A_i||auth_i)$. If the hash function in OTS is not second image resistant, then the attack is possible.

So, the Merkle Tree is secure when OTS is secure and the hash function is second image resistant.

The cryptographic hash function is secure when is second preimage and collision resistant. But the Merkle Tree Scheme does not require it to be collision resistant. Thus, we can reduce the bit level of security of second preimage resistant hash function in this scheme. Thus, more lightweight hash functions can be used.

Conslusions

The modern national standard defines the modes of Kupyna-n hash function. Kupyna-256, 384, 512 modes have second preimage attack resistance and collisions resistance. Due to having the structure like Grøstl, the round attack to reduced hash can be performed. The listed above modes are strong after the 7 rounds.

The Merkle trees were known since 80s, but improvements were published past few years.

Thus, making Merkle Signature Schemes an alternative to conventional existing schemes. The message can be signed with reasonable time and one public key can be used for 2^{80} signatures.

These schemes may utilize hash functions lighter than the existing standards with lesser bit-security level.

Since Kupyna-n has varying security levels, the lesser level function can be used in OTS in Merkle Signature Schemes due to the property of Merkle trees to be collision resistant.

References

1. Metrology and Certification of the Commonwealth of Independence States. GOST 34.311-95. Information technology. Cryptographic Data Security. Hash function. Metrology and Certification of the Commonwealth of Independence States. Minsk, 1995. (In Rus).

2. Roman Oliynykov, Ivan Gorbenko, Oleksandr Kazymyrov, Victor Ruzhentsev, Oleksandr Kuznetsov, Yurii Gorbenko, Oleksandr Dyrda, Viktor Dolgov, Andrii Pushkaryov, Ruslan Mordvinov, Dmytro Kaidalov. A new encryption standard of Ukraine: The Kalyna block cipher. Cryptology ePrint Archive. Report 2015/650, 2015. http://eprint.iacr.org/2015/650.pdf

3. Roman Oliynykov, Ivan Gorbenko, Oleksandr Kazymyrov, Victor Ruzhentsev, Oleksandr Kuznetsov, Yurii Gorbenko, Artem Boiko, Oleksandr Dyrda, Viktor Dolgov, Andrii Pushkaryov. A New Standard of Ukraine: The Kupyna Hash Function. Cryptology ePrint Archive. Report 2015/885, 2015. https://eprint.iacr.org/2015/885.pdf

4. Christoph Dobraunig, Maria Eichlseder, and Florian Mendel. Analysis of the Kupyna-256 Hash Function, Graz University of Technology, Austria, Cryptology ePrint Archive. Report 2015/956, 2015. https://eprint.iacr.org/2015/956.pdf

5. Mendel F., Rechberger C., Schl affer M., Thomsen S.S.: Rebound attacks on the reduced Grøstl hash function. In: Pieprzyk, J. (ed.) Topics in Cryptology – CT-RSA 2010. LNCS. – Vol. 5985. – P. 350–365. Springer (2010)

6. Jean J., Naya-Plasencia M., Peyrin T. Improved rebound attack on the finalist Grøstl. In: Canteaut, A. (ed.) Fast Software Encryption – FSE 2012. LNCS. – Vol. 7549. – P. 110–126. Springer (2012)

7. Ralph Merkle. Secrecy, authentication and public key systems // A certified digital signature.Ph.D. dissertation, Dept. of Electrical Engineering, Stanford University, 1979.

8. Michael Szydlo. Merkle tree traversal in log space and time. Eurocrypt, 2004.

9. Klintsevich K., Okeya, Vuillaume C., Buchmann J., Dahmen E. Merkle signatures with virtually unlimited signature capacity. 5th International Conference on Applied Cryptography and Network Security. – ACNS07, 2007.

V.N. Karazin Kharkiv National University *Received 05.09.2018*

УДК 004.056.5

A.A. KUZNETSOV, Doctor of Sciences, Yu.I. GORBENKO, Ph.D.,
M.S. LUTSENKO, D.I. PROKOPOVYCH-TKACHENKO, Ph.D., M.V. PASTUKHOV, Ph.D.

NIST PQC: CODE-BASED CRYPTOSYSTEMS

1. Introduction

The National Institute of Standards and Technology (NIST) addressed to the public and announced the launch of a Post-Quantum Cryptography (PQC) bidder competition, which is scheduled for adoption in 2020–2022 [1, 2], In particular, on post-quantum electronic digital signature schemes (EDS), public key encryption schemes and key encapsulation mechanisms. Among the promising areas of research, code-based public-key cryptosystems (Code-Based Public-Key Cryptosystems) occupy a special place, allowing to effectively implement all three groups of algorithms.

The feature of the contest announced by NIST is that algorithms based on mathematical methods that are not sufficiently tested can be submitted. Therefore, study of such algorithms regarding their resistance to quantum cryptographic analysis requires significant time expenses. The aforementioned fact determines relevance of the comprehensive study of the submitted projects, their comparative analysis, as well as the assessment of their security [1, 2]. Within this work, we limit ourselves to research of algorithms of code-based cryptosystems, we will conduct their primary analysis and systematization.

For the primary evaluation of cryptographic properties, an analysis was made of the correspondence of the presented algorithms to modern requirements for public-key cryptosystems, namely, ensuring the properties of indistinguishability [3]. The property of indistinguishability of ciphertext determines the cryptostability of the algorithm to chosen plaintext attack. Providing such an indistinguishability under chosen plaintext attack (IND-CPA) is considered a basic requirement for most provably protected public-key cryptosystems [3], although some schemes also provide cryptographic resistance against chosen ciphertext attacks and adaptive chosen ciphertext attacks. Such indistinguishability properties are designated as IND-CCA1 and IND-CCA2, respectively [3].

2. Characteristics of EDS algorithms

Authors presented 3 different code-based schemes for EDS generation and verification: pqsigRM, RaCoSS, RankSign.

2.1. pqsigRM scheme

The pqsigRM was developed by a group of researchers from Korea [4]. It is based on the Reed-Mueller code (RM), improving the scheme based on Goppa codes, developed by Courtois, Finiasz and Sendrier (CFS). The benefit of this algorithm is controlled time of signing. Compared to CFS, signature time does not depend on the ability to fix t errors. Also, signature time and security level is controlled by changing parameters.

2.2. RacoSS scheme

Name of this algorithm stands for a Random Code-based Signature Scheme. RaCoSS is proved to be strong existentially unforgeable under chosen message attack (SEUF-CMA). The signature size is small in respect of other code-based signature schemes apart from CFS signature scheme with 81 bits security. However, the key sizes of CFS signature scheme are much higher than RaCoss. The key generation, signature generation and signature verification processes can easily be speeded up by parallel computation.

2.3. RankSign scheme

RankSign cryptosystem was introduced in 2014 [5]. This signature scheme is based on a code in the rank metric. The general idea is to use the LRPC code (which is equivalent to the MDPC in the Hamming metric or NTRU in the Euclidean metric) as a loophole for calculating the error asso-

ciated with the message. The signature scheme has small parameters and is relatively fast. Since we need to pick a large value for *q*, all known combinatorial attacks are ineffective to violate the RankSign's security. Thus, the best attacks against it are based on the calculations of Griubner.

3. Comparative analysis of the EDS

A comparative analysis of the presented algorithms of EDS will be useful in terms of their performance and length parameters. Fig. 1 shows the values of the length of signatures for different versions of algorithms with different security levels. In order to demonstrate the values more clearly the length is given in bytes, on a logarithmic scale.

Analyzing the obtained data, it can be noted that for versions of RacoSS algorithm, the length of the public and private keys is the smallest, while the length of the ciphertext for this scheme also takes one of the smallest values. It was not possible to investigate length of a private key of the RankSign scheme because it does not require the use of a private key. The largest length of the ciphertext corresponds to the RankSign and in case the provided security level is increased, length of ciphertext increases as well as the length of the public key.

Fig. 2 shows the parameters of the speed of the key generation, the generation and verification of the signature, as well as indicates computing platform, which was used in the testing. Speed, given in milliseconds, is converted to the number of cycles, taking into account the specifications of a particular computing platform.

In terms of performance it is obvious that the most efficient algorithm will be the one with higher indicators. Analyzing the histograms, it's obvious that the Optimized RacoSS is faster than all the presented algorithms. While the signature scheme pqsigRM for its various versions showed comparable performance, which is an order of magnitude less than the speed of RankSign and RacoSS.

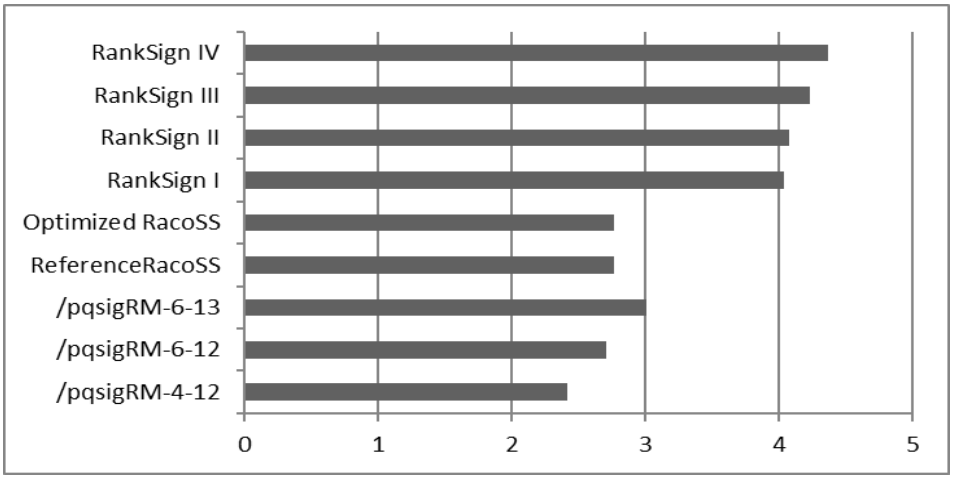


Fig. 1. Comparison of generated signatures (in bytes, logarithmic scale) of different EDS schemes

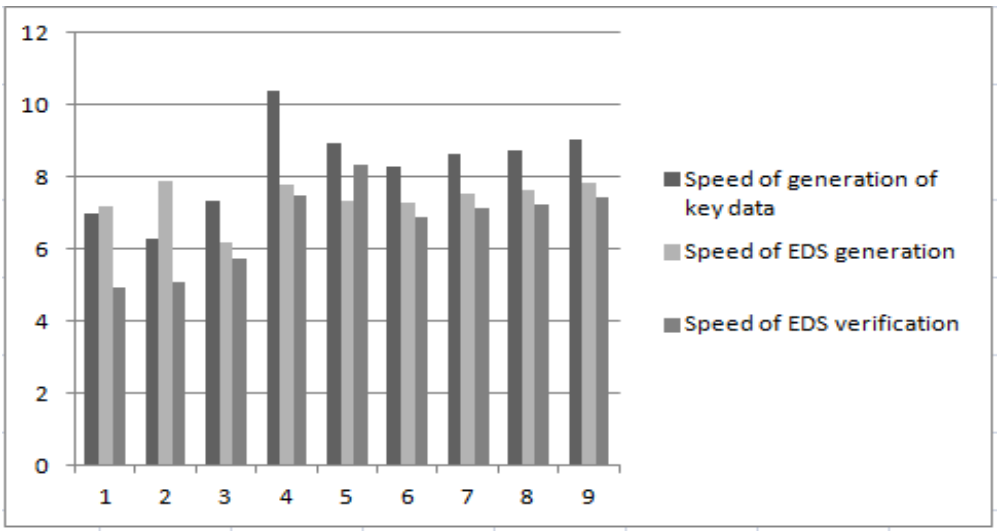


Fig. 2. Speed parameters at all stages of the algorithms

4. Characteristics of public-key cryptosystems

After analyzing the projects submitted to the contest, five code-based public-key cryptosystems were allocated: BIG QUAKE [6], HQC [7], LEDApkc [8], LOCKER [5] та McNie [5].

4.1. BIG QUAKE scheme

Within the framework of the project, an public-key cryptosystems is proposed, which turns into a key encapsulation mechanism. The authors of the project assume the use of Goppa binary codes in this scheme. BIQ QUAKE is built like the Niderraiter scheme. Compared to the original Niederreiter scheme, proposal avoids the computation of a bijection between words of fixed length and constant weight words. This provides a light scheme more suitable for embedded system with restricted computing resources.

4.2.HQC scheme

The HQC name is the abbreviation Hamming Quasi-cyclic, which implies the use of the quasi-cyclic Hamming code HQC is a code-based public key cryptosystem with several desirable properties. It is proved IND-CPA assuming the hardness of (a decisional version of) the Syndrome Decoding on structured codes. By design, HQC perfectly fits the recent KEMDEM transformation, and allows to get a hybrid encryption scheme with strong security guarantees (IND-CCA2).

4.3. LEDApkc scheme

This project was presented by a group of Italian researchers. LEDApkc is a public-key cryptosystem built from the McEliece cryptosystem based on linear error-correcting codes. In particular, LEDApkc exploits the advantages of relying on quasicyclic low-density parity-check (QC-LDPC) codes providing high decoding speeds and compact keypairs. Among the advantages of the LEDApkc scheme are the following. Built on an NP-complete problem under reasonable assumptions. Exploits improved BF decoders which are faster than classical BF decoders.

4.4. LOCKER scheme

The proposal is based on variations of the LRPC approach. The scheme is effective in terms of the size of the parameters and the computational complexity, which uses the properties of the rank metric. The LOCKER has the probability of failure, but this probability is justified and can be very low from 2^{-64} to 2^{-128}. Also, the positive point is that the choice of parameters is universal.

4.5. McNie scheme.

The authors of the hybrid scheme that unites elements of the McElice and Niderreiter cryptosystems are Korean scientists. McNie provides smaller key sizes employing quasi-cyclicity of matrices for 128-bit, 192-bit and 256-bit securities compared to those of RSA.

McNie can use various kinds of known block codes as inputs even though McEliece cryptosystem based on those codes were broken. The reason is that a random code is used in the encryption so that McNie is secure against structural and information set decoding attacks.

5. Comparative analysis of public-key cryptosystems

Fig. 3 shows the lengths of the ciphertext for different versions of encryption schemes which provide different levels of security. Analyzing the obtained results, it should be noted that the length of the public key and ciphertext for the Big Quake algorithm are the largest. McNie, on the other hand, shows the lowest values of all parameters, while it is able to provide fifth security level as well as other schemes.

The obtained comparison results for speed indicators are shown in Fig. 4. The data given in milliseconds was reduced to the number of cycles that require the execution of the algorithm, taking into account the features of the used computing platform.

The analysis shows that the Big Quake algorithm provides the greatest speed of key generation. The McNie and LEDApkc algorithms are relatively comparable, while the versions of HQC algorithm provide the lowest performance of all the schemes.

Analyzing data, it's obvious that the encryption speed is fairly high in all encryption schemes, but LEDApkc - 5.3 provides the best performance. The decryption rate is comparable to the McNie, Big Quake and HQC algorithms, while LEDApkc performance is the best.

So, in terms of performance, the most effective of the schemes presented is the LEDApkc scheme in all its variants, and HQC, in turn, showed the worst results.

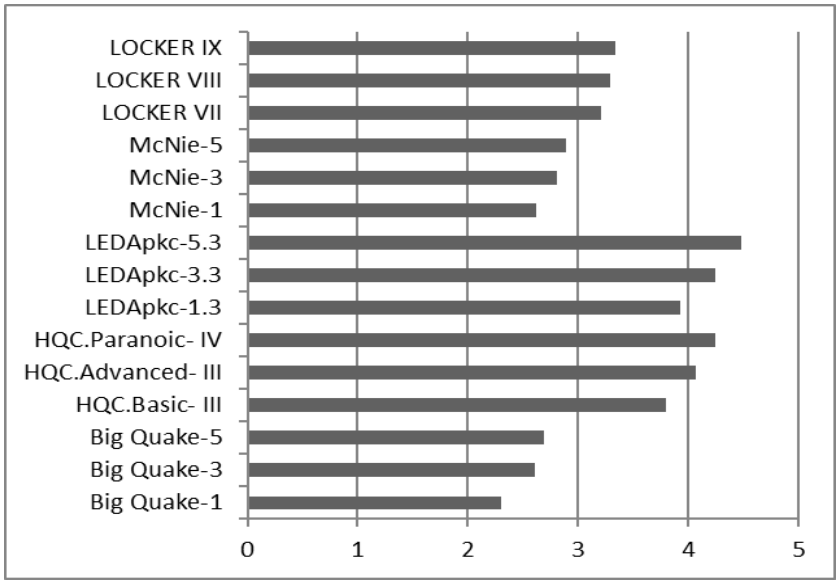


Fig. 3. Comparison of ciphertext lengths (in bytes, logarithmic scale) of different encryption schemes

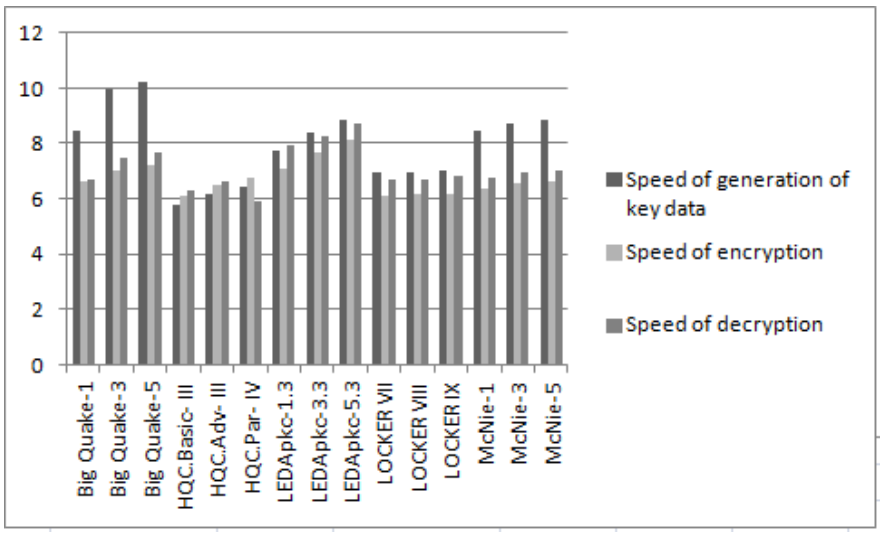


Fig. 4. Histogram of values of the speed of encryption schemes (logarithmic scale)

6. Characteristics of key encapsulation mechanisms

All 12 key encapsulation algorithms presented for the contest are analyzed: BIKE [9], Classic McElice [10], DAGS [11], Edon-K [12], LAKE [13], LedaKem [14], Lepton [15], NTS-KEM [16], Ouroboros-R [17], QC–MDPC KEM [18], RLCE-KEM [19], RQC [20].

6.1. BIKE

In BIKE (BIt Flipping Key Encapsulation is used Quasi-cyclic codes with parity check (QC-MDPC) with moderate density, that can be decoded using the technique of bit flipping. The algorithm has an IND-CPA cryptographic stability, due to the use of the technique of bit flipping is expected and the provision of IND-CCA resistance. The BIKE-1 scheme is based on the variation of the McElice algorithm. In BIKE-1, accelerated key generation is provided. The public key has a double length, compared to BIKE-2. The basis of the BIKE-2 algorithm is the Niederreiter cryptosystem with the parity check matrix.

6.2. Classic McElice

Classic McElice is a scheme proposed by a group of researchers from the USA, Japan, the Netherlands, Germany, France. There is variation of the McElice algorithm, based on the binary Goppa code. This key encapsulation algorithm is designed to ensure the security of IND-CCA2 at a very high level of cryptographic stability. The authors suggest that the algorithm can find an effective application even in systems with limited computing capabilities and resources, while maintaining effective cryptographic stability.

6.3. DAGS

DAGS (Key Encapsulation from DyAdic GS Codes) is an algorithm for key encapsulation submitted by researchers from the universities of the Netherlands, United States, Senegal, France, Brazil. The DAGSa Key Encapsulation Mechanism based on Quasi-Dyadic (QD) Generalized Srivastava codes. The authors claim that this is the first algorithm based on structured algebraic codes that provide not only IND-CPA cryptostability, but also IND-CCA. Presumably the algorithm can find application in applications for the Internet of things.

6.4. Edon-K

Edon-K presented by Norwegian scientists. This algorithm is based on the McElice scheme, but uses a different family of codes. These codes are defined over another field and are not based on the Hamming metric. This approach allows to significantly reduce the length of public keys. In the

construction of EDON-K authors use one related class of matrices that they call quasi-binary quasi-orthogonal matrices. EDON-K is designed to offer CCA2 security without a need of some extra CPA-to-CCA transformation.

6.5. LAKE

LAKE (Low rAnk parity check codes Key Exchange) is another algorithm presented by a group of scientists from France. The algorithm is based on the Ideal-LRPC parity codes and the IND-CPA key encapsulation mechanism (KEM). The scheme has some probability of error during decapsulation. The proposed scheme is very effective, both from the point of view of the chosen sizes of basic parameters (keys and ciphertext) and computational complexity.

6.6. LedaKem

LedaKem (Low dEnsity coDe-bAsed key encapsulation mechanism) is based on the Niederreiter cryptosystem with linear error correction. LEDAkem takes advantage of the use of low-density quasi-cyclic codes (QC-LDPC) that provide high decoding rates and small key lengths. It should be noted the extremely short length of the obtained ciphertext – 64 bytes, even at a category 5 of cryptographic stability. The scheme possesses IND-CCA cryptostability.

6.7. Lepton

Lepton (LEarning PariTy with Noise) is Chinese encapsulation algorithm. This algorithm is based on the variation of Learning Parity with Noise (LPN). The Lepton.CPA is aimed at achieving CPA-security, and is based on Ring-CLPN (Compact Learning Parity with Noise). The Lepton.CCA is a KEM scheme for achieving CCA security, which is obtained by applying the Fujisaki-Okamoto transformation over Lepton.CPA.

6.8. NTS-KEM

NTS-KEM scheme submitted by researchers from the United Kingdom. NTS-KEM can be considered as a variant of the McElice public-key cryptography scheme. In this mechanism, binary linear Goppa codes are used in the Niederreiter cryptosystem. NTS-KEM provides the security of IND-CCA (like as KEM) in a Random Oracle model using a transformation similar to the Fujisaki-Okamoto or Dent transformations.

6.9. Ouroboros-R

Ouroboros-R presented by the researchers from France. The quasi-cyclic code used allows the decoding process to be accelerated. The algorithm has some similarities with NTRU-like circuits. Ouroboros-R also has the probability of failure, due to the decoding algorithm used. Ouroboros-R possesses the crypto-resistance of IND-CPA in accordance with the assumptions of 2-QCRSD and 3-QCRSD.

6.10. QC-MDPC KEM

QC-MDPC KEM was developed by researchers from Canada. The algorithm is based on the McElice cryptosystem. QC-MDPC KEM uses a quasi-cyclic parity check with a moderate density. The authors state that the algorithm may not be fast enough compared to other algorithms. The algorithm provides IND-CPA cryptographic stability.

6.11. RLCE-KEM

RLCE-KEM is a scheme for key encapsulating of researcher from the United States. The algorithm uses the McElice cipher scheme based on a random linear code. The advantage of the RLCE scheme is that its security does not depend on any particular structure of underlying linear codes. It is believed that the security in RLCE depends on the NP-hardness of decoding random linear codes.

6.12. RQC

RQC (Rank Quasi-Cyclic) is formed by a group of French scientists. The RQC scheme is based on a quasi-cyclic code. The approach used to key encapsulating the makes it possible to guarantee IND-CCA2 cryptographic stability and provides high performance indicators. The authors indicate that the algorithm has a zero probability of decoding failure.

7. Comparative analysis of key encapsulation mechanisms

According to the data submitted by authors, the smallest length of a private key is in scheme Edon-K, for both variations. The largest private keys of the algorithms DAGS-5 and RLCE-KEM, It should be noted that for all algorithms the length of ciphertext is relatively small and ranges from 32 to 9032.75 bytes. The smallest length – variations of the LedaKem and RLCE-KEM ID = 6 scheme. Some authors intentionally tried to minimize the length of the ciphertext as shown on Fig. 5.

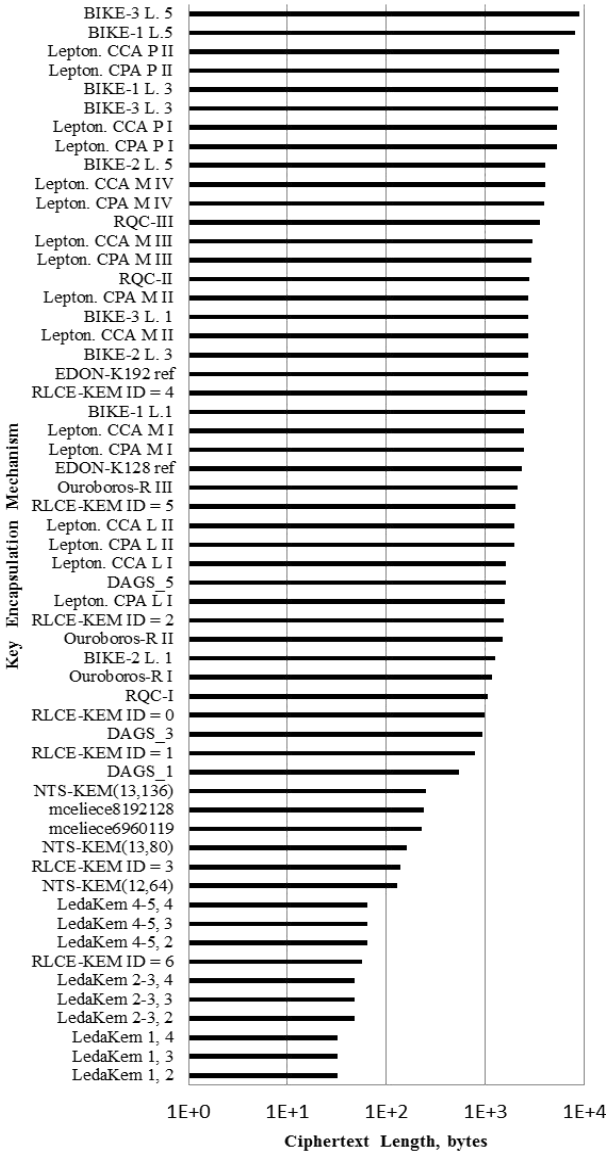


Fig. 5. Ciphertext lengths (in bytes, logarithmic scale) of key encapsulation algorithms

Evaluation of the performance in the format of the number of processor cycles spent on the execution of the main operation is shown in Fig. 6. In Fig. 6 shown the data for various variants of algorithms providing the highest level of cryptographic stability.

Analysis of the results of the comparison shows that the comparable speed of all operations have algorithms Lepton.CCA and Lepton.CPA, Ouroboros-R, LAKE, LedaKem. The EDON-K, Classic McElic, RLCE-KEM, DAGS_5 schemes have a fairly large performance gap between key generation and encapsulation.

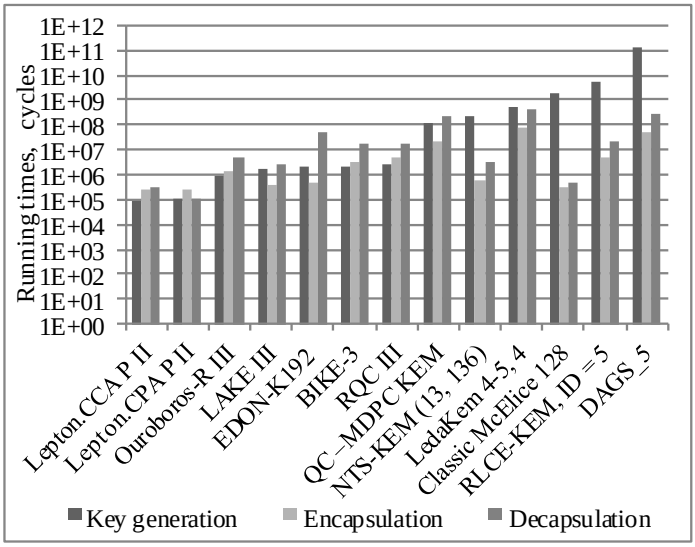


Fig. 6. Performance (in cycles, logarithmic scale) of key encapsulation algorithms

The Lepton algorithm has rather small lengths of both public and private keys, and due to the algorithm used, public and private keys, and due to the algorithm used, the speed of generating key data for this scheme is greatest. The lowest speed of key generation in DAGS_5. The Lepton algorithm also has the fastest rate of key encapsulation, the slowest rate is LedaKem scheme.

Conclusions

The National Institute of Standards and Technology of the United States announced the launch of a contest for the selection of applicants for the standards of post-quantum algorithms, which decisions are scheduled for adoption in 2020–2022. Since NIST intends to standardize post-quantum alternatives to its existing standards for key establishment (SP 800-56A, SP 800-56B). And these standards are used in a wide variety of Internet protocols, such as TLS (Transport Layer Security), SSH (Secure Shell), IKE (Internet Key Exchange), IPsec (IP Security), and DNSSEC (Domain Name System Security Extensions). So, presented schemes will be evaluated by the security they provide in these applications.

Code-based cryptography is now considered one of the most promising areas [21 – 24]. This is confirmed by the fact that out of the 82 projects submitted for the contest, 20 are based on codes. Among them there are 3 electronic digital signature generation and verification schemes, 5 encryption schemes and 12 mechanisms of key encapsulation. Having examined their general characteristics and having conducted a preliminary comparative analysis of their effectiveness, we can conclude that the best indicators, in terms of performance, and the length of signatures, secret and public keys have been demonstrated by the RacoSЬIб LEDApkc scheme and Lepton.

References:

1. D. Bernstein, J. Buchmann and E. Dahmen. Post-Quantum Cryptography. Springer-Verlag, Berlin-Heidleberg, 2009. – 245 p.

2. D. Moody. Post-Quntum Cryptography: NIST's Plan for the Future" The Seventh International Conference on Post-Quntum Cryptography, Japan, 2016. Internet: https://pqcrypto2016.jp/data/pqc2016_nist_announcement.pdf [March 8, 2016].

3. J. Katz, Y. Lindell. Introduction to Modern Cryptography: Principles and Protocols. Chapman & Hall / CRC Press, 2007. 553 p.

4. Lee, Young-Sik Kim, Yong-Woo Lee, Jong-Seon No. A modified RM code-based post-quantum digital signature algorithm [On-line]. Internet: https://sites.google.com/view/pqsigrm/home

5. Post-Quantum Cryptography, Round 1 Submissions, 2017. [On-line]. Internet: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.

6. Alain Couvreur, Magali Bardet, Elise Barelli, Olivier Blazy, Rodolfo Canto-Torres, Philippe Gaborit, Ayoub Otmani, Nicolas Sendrier, Jean-Pierre Tillich. Binary Goppa QUAsi-cyclic Key Encsapulation [On-line] Internet: https://bigquake.inria.fr/

7. Carlos Aguilar Melchor, Nicolas Aragon, Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Edoardo Persichetti, Gilles Zémor. Hamming Quasi-Cyclic [On-line]. Interner: http://pqc-hqc.org/

8. Marco Baldi, Alessandro Barenghi, Franco Chiaraluce, Gerardo Pelosi, Paolo Santini. LEDApkc Public Key Cryptosystem [On-line]. Internet: https://www.ledacrypt.org/LEDApkc/

9. Nicolas Aragon, Paulo Barreto, Slim Bettaieb, Loic Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Phillipe Gaborit, Shay Gueron, Tim Guneysu, Carlos Aguilar Melchor, Rafael Misoczki, Edoardo Persichetti, Nicolas Sendrier, Jean-Pierre Tillich, Gilles Zemor. BIKE – Bit Flipping Key Encapsulation. NIST Submission, 2017. [On-line]. Internet: http://bikesuite.org/#spec.

10. Daniel J. Bernstein, Tung Chou, Tanja Lange, Ingo von Maurich, Rafael Misoczki, Ruben Niederhagen, Edoardo Persichetti, Christiane Peters, Peter Schwabe, Nicolas Sendrier, Jakub Szefer. Classic McEliece. NIST Submission, 2017. [On-line]. Internet: https://classic.mceliece.org/index.html.

11. Gustavo Banegas, Paolo S.L M. Barreto, Brice Odilon Boidje, Pierre-Louis Cayrel, Gilbert Ndollane Dione, Kris Gaj, Cheikh Thiecoumba Gueye, Richard Haeussler, Jean Belo Klamti, Ousmane N'diaye, Duc Tri Nguyen. DAGS: Key Encapsulation using Dyadic GS Codes. NIST Submission, 2017. [On-line]. Internet: https://www.dags-project.org/#files.

12. Danilo Gligoroski, Kristian Gjøsteen. Post-quantum Key Encapsulation Mechanism EDON-K. NIST Submission, 2017. [On-line]. Internet: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.

13. Nicolas Aragon, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Adrien Hauteville, Olivier Ruatta, Jean-Pierre Tillich, Gilles Zémor. LAKE – Low rAnk parity check codes Key Exchange. NIST Submission, 2017. Internet: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.

14. Marco Baldi, Alessandro Barenghi, Franco Chiaraluce, Gerardo Pelosi, Paolo Santini. LEDAkem (Low dEnsity coDe-bAsed key encapsulation mechanism). NIST Submission, 2017. [On-line]. Internet: https://www.ledacrypt.org/LEDAkem/

15. Y. Yu, J. Zhang. Lepton: Key Encapsulation Mechanisms from a variant of Learning Parity with Noise. NIST Submission, 2017. [On-line]. Internet: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.

16. M. Albrecht, C. Cid, K. G. Paterson, C. J. Tjhai, M. Tomlinson. NTS-KEM. NIST Submission, 2017. [On-line]. Internet: https://nts-kem.io/.

17. C. A. Melchor, J.-C. Deneuville, N. Aragon, P. Gaborit, S. Bettaieb, A. Hauteville, L. Bidoux, G. Zémor. Ouroboros-R. NIST Submission, 2017. [On-line]. Internet: http://pqc-ouroborosr.org/.

18. A. Yamada, E. Eaton, K. Kalach, P. Lafrance, A. Parent. QC-MDPC KEM: A Key Encapsulation Mechanism Based on the QC-MDPC McEliece Encryption Scheme, NIST Submission, 2017. [On-line]. Internet: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.

19. Y. Wang. RLCEKeyEncapsulation Mechanism (RLCE-KEM) Specifcation. NIST Submission, 2017. [On-line]. Internet: http://quantumca.org/.

20. C. A. Melchor, N. Aragon, S. Bettaieb, L. Bidoux, O. Blazy, J.-C. Deneuville, P. Gaborit, G. Zemor. Rank Quasi-Cyclic (RQC). NIST Submission, 2017. [On-line]. Internet: http://pqc-rqc.org/.

21. Yu.V.Stasev, A.A.Kuznetsov. Asymmetric Code-Theoretical Schemes Constructed with the Use of Algebraic Geometric Codes // Cybernetics and Systems Analysis. – Vol. 41, Issue 3. – P. 354-363, May 2005.

22. A. Kuznetsov, I. Svatovskij, N. Kiyan and A. Pushkar'ov. Code-based public-key cryptosystems for the post-quantum period // 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kharkov, 2017. – P. 125-130.

23. A. Kuznetsov, R. Serhiienko and D. Prokopovych-Tkachenko.Construction of cascade codes in the frequency domain // 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kharkov, 2017. – P. 131-136.

24. Yu.V. Stasev, A.A. Kuznetsov. Asymmetric code-theoretical schemes constructed with the use of algebraic geometric codes // *Kibernetika i Sistemnyi Analiz*/. – No. 3. – P. 47-57, May-June 2005.

V.N. Karazin Kharkiv National University;
JSC "Institute of Information Technologies", Kharkiv;
University of Customs and Finance, Dnipro

Received 02.11.2018

УДК 004.428.4

О.А. МЕЛЬНИКОВА, канд. техн. наук, О.В. ДЖУРИК, А.О. МАСЛЄННІКОВА

ЕЛІПТИЧНІ КРИВІ ЕДВАРДСА. ПОРІВНЯННЯ КРИПТОГРАФІЧНИХ БІБЛІОТЕК

Вступ

У 2007 році Едвардс [1] виявив цікаву нормальну форму для еліптичних кривих (ЕК), яка була введена Бернштейном і Ланге [2] та нині відома як модель Едвардса. Криві Едвардса – це сімейство еліптичних кривих, яке широко використовується у криптографічних перетвореннях і є найбільш цікавим з точки зору практичних застосувань. Зручність програмування і висока швидкість виконання операцій – головні переваги кривих даного класу у порівнянні з іншими відомими формами представлення еліптичних кривих (Вейерштраса, Монтгомері і т.і.). Окремим випадком цієї моделі кривої є скручена крива Едвардса, яка дозволяє зменшити обчислювальну складність операцій подвоєння та додавання точок ЕК. Такі криві також мають інші привабливі властивості, а саме: підтримка повного закону додавання та сумісність з моделлю Монтгомері, що у свою чергу відкриває можливість для використання так званої “ступінчатої схеми Монтгомері” – швидкого алгоритму визначення кратних точок.

Симетрія точок кривих Едвардса щодо обох координатних осей тягне за собою цікаві та зручні властивості цих кривих. Для кривих Едвардса досить використовувати один параметр d замість звичайних двох параметрів a і b класичної кривої в канонічній формі.

У 2017 році було оголошено, що визначені в RFC 7748 еліптичні криві Curve25519 та Curve448 будуть додані до списку ЕК, схвалених до використання в розробках для державних проектів, які надаються документом NIST SP 800-186. Інтерес до їх використання суттєво зріс внаслідок виникнення припущення, що рекомендовані NSA у стандарті електронного цифрового підпису (ЕЦП) FIPS 186-4 константи еліптичних кривих над GF(P) можуть надавати їм переваги при веденні криптоаналізу. Curve25519 та Curve448 є позначеннями для кривих Монтгомері, яким відповідають еквівалентні скручена крива Едвардса Ed25519 та крива Едвардса Ed448.

Крива Едвардса Ed25519 знайшла своє практичне застосування в ряді протоколів, бібліотек і програмних продуктів. Зокрема, вона використовується для автентифікації та обміну ключами в таких системах, як OpenSSH, I2p, Tor, Tox. Ця крива запропонована IETF для використання в алгоритмі TLS.

Криптографічна бібліотека Libsodium

Еліптична крива Бернштейна та підтримка її математичного апарату реалізовані в Libsodium [3] – криптографічній бібліотеці, що призначена для створення програмного інструментарію зашифрування / розшифрування контенту, ґешування паролів, формування та перевірки електронних цифрових підписів інформації.

Проект Libsodium анонсувала компанія OpenDNS у вигляді аналога створеної раніше криптографічної бібліотеки NaCl (Networking and Cryptography library), архітектура якої так само побудована на еліптичній кривій Ed25519. NaCl не отримала широкого поширення в зв'язку з проблемами перенесення на інші платформи.

Libsodium представлена як універсальна бібліотека, що забезпечує сумісність з NaCl на рівні API та підтримку ряду платформ. Бібліотека включається в пакети для багатьох операційних систем, її функції доступні користувачам через API. Серед платформ, які підтримують Libsodium, найбільш відомі: Bitrig, OpenBSD, Dragonfly BSD, NetBSD, FreeBSD, SmartOS, OSX, Linux, Windows, iOS і Android.

Libsodium надає спрощений API з набором безпечних криптографічних опцій і методів. За рахунок цього використання Libsodium вимагає менше спеціальних знань, у порівнянні з аналогами. Так, наприклад, OpenSSL має надлишкову функціональність, зокрема містить

безліч криптографічних примітивів і режимів, що ускладнює вибір користувачем безпечного набору. Наявність великої кількості параметрів команд призводить до складностей при роботі, а також до періодичного виявлення вразливостей.

Libsodium вирішує проблему оптимального вибору, надаючи користувачеві готовий до використання компактний і простий набір функцій, що містить тільки безпечні методи. Libsodium підтримується різними компіляторами й операційними системами, включаючи Windows (з MinGW або Visual Studio, x86 і x86-64), iOS і Android.

Функції Libsodium, які надаються за допомогою API:

1) зашифрування з використанням автентифікації з відкритими (public-key) і загальними (shared-key) ключами, які забезпечують надійність передачі зашифрованого повідомлення і гарантують його цілісність;

2) створення та перевірка електронних цифрових підписів з використанням кривої Ed25519 за відкритим і особистим ключами дозволяє одержувачеві перевірити, що повідомлення надіслано саме тим, від кого його очікували отримати, і що воно не було змінено третьою особою;

3) операції ґешування, які дозволяють сформувати так званий "зліпок" від повідомлення, який має фіксовану довжину і надає можливість перевірити відповідність ґеш-значення та початкового повідомлення, але не дозволяє відновити елементи повідомлень з ґеш-значення;

4) формування ключів з коротких повідомлень для ґеш-таблиць, що дозволяють виключити проведення DoS-атак через колізії ґеш-значень;

5) безпечний генератор псевдовипадкових чисел для використання в криптографічних перетвореннях.

У бібліотеці реалізовано цифровий підпис з використанням кривої Бернштейна та алгоритму ґешування SHA-512. Команда Бернштейна оптимізувала Ed25519 для сімейства процесорів Nehalem / Westmere x86-64. Верифікація може виконуватися порціями по 64 підписи для підвищення пропускної спроможності. Ed25519 призначена для забезпечення стійкості до атак, порівняної з якістю 128-бітових симетричних шифрів. Відкритий ключ має довжину 256 біт, а підпис – 512. Серед програмного забезпечення для DNS користується популярністю ЕЦП з відкритим ключем довжиною 32 байт та підписом 64 байт, які мають таку саму стійкість, як і 256-байтовий RSA-2048 підпис.

Приблизно з квітня 2016 року в багатьох відомих месенджерах, таких як Facebook Messanger, Viber, WhatsApp, з'явилася функція секретного обміну повідомленнями. Повідомлення, які надсилаються та отримуються, доступні лише для читання на пристрої, який використовується для створення або відкриття бесіди. Це означає, наприклад, що користувач не може переглядати попередню розмову на своєму ноутбуці, якщо спочатку створив або відкрив її на своєму смартфоні. Крім того, секретні бесіди створюють ефемерний характер процесу секретного обміну повідомленнями, надаючи користувачу можливість контролювати, як довго одержувач може бачити повідомлення. Описаний функціонал було реалізовано за допомогою end-to-end шифрування, яке використовує відкриті реалізації протоколу Signal.

.Net Core бібліотека NSec

На базі Libsodium була розроблена криптографічна бібліотека для .Net Core – NSec [4], що також реалізує алгоритм електронного цифрового підпису Ed25519 та інші сучасні криптографічні примітиви, такі як X25519 (протокол обміну ключами Діфі-Гелмена, який базується на еліптичній кривій) та ChaCha20-Poly1305 (симетричний шифр та формування коду автентифікації повідомлень). Перевагами цієї бібліотеки є легкість у використанні, швидке виконання операцій та потокобезпечність. Також слід зазначити, що NSec є бібліотекою з відкритим програмним кодом. Крім послуг безпеки, що надаються самими криптографічними примітивами, NSec намагається зробити навіть саме використання цих примітивів максимально безпечним за замовчуванням. Це стосується, наприклад, особливостей організації зберігання та вилучення конфіденційних даних, таких як ключі.

Crypto++

Серед існуючих бібліотек слід відмітити також бібліотеку Crypto++ [5], реалізації якої надають захист від атак зі сторонніх каналів. Це атаки, засновані на припущенні, що деяка інформація зі сторонніх каналів (наприклад, час обчислень) залежить від команд, що виконуються, або від вхідних даних. Для забезпечення такого захисту використовуються, за можливістю, апаратні інструкції. Також, для мінімізації витоків у бібліотеці використовуються алгоритми та шаблони доступу до кеш-пам'яті.

Бібліотека підтримує цифровий підпис з використанням кривої Едвардса з наступними параметрами: розмірність поля – 2^{255}- 19, параметр кривої d – 121665 / 121666, SHA-512 в якості функції ґешування, базова точка $B(x, y)$, де x – парне число, порядок кривої – просте 253-бітове число.

Серед недоліків можна відмітити невелику популярність у використанні бібліотеки програмним забезпеченням: лише i2pd (некомерційна реалізація i2p клієнта).

Bouncy Castle

Bouncy Castle – це програмна бібліотека [6], у якій представлена велика кількість криптографічних примітивів. Існують реалізації Bouncy Castle мовами програмування Java та C#. Бібліотека підтримує як стандартні високорівневі криптографічні API відповідних платформ, так і низькорівневі API для більш гнучкого й ефективного доступу до функціоналу. Відповідно до RFC 8032 у Bouncy Castle було введено низькорівневі реалізації кривих Ed25519 та Ed448.

Існує також версія Bouncy Castle, яка була розроблена для операційної системи Android. Ця бібліотека одержала назву Spongy Castle. На жаль, платформа Android супроводжується скороченою версією Bouncy Castle.

Крім того, слід зазначити, що у листопаді 2016 року вийшли перші релізи Bouncy Castle, сертифіковані FIPS. На відміну від попередніх розробок, у сертифікованих версіях бібліотеки контролюється виконання вимог FIPS щодо алгоритмів, які підтримують низькорівневі API.

OpenSSL

OpenSSL – відкритий програмний продукт, розроблений як універсальна бібліотека для криптографії, що використовує протоколи Secure Sockets Layer і Transport Layer Security. Використовується, зокрема, в бібліотеці cUrl для реалізації роботи за протоколом https. Доступна для більшості UNIX-подібних операційних систем (включаючи Solaris / OpenSolaris, Linux, Mac OS X, QNX4, QNX6 і чотирьох операційних систем BSD з відкритим програмним кодом), а також для OpenVMS і Microsoft Windows. Існують реалізації мовами програмування C, assembly, Perl. OpenSSL заснований на SSLeay, розробка якого була неофіційно призупинена в 1998 році.

OpenSSL не було сертифіковано, але для забезпечення багатьох його можливостей був створений криптографічний модуль OpenSSL FIPS Object Module, який отримав сертифікат відповідності стандарту безпеки FIPS 140-2, що визначає вимоги до криптографічних модулів, необхідні для їх використання в державних установах США. Сертифікат виданий Американським інститутом стандартів і технологій (NIST) після проведення відповідного аудиту коду проекту. Причому сертифікат було видано на програмний код продукту, а не конкретну бінарну збірку, що розширює область використання OpenSSL в державних проектах.

Серед несиметричних криптографічних алгоритмів OpenSSL підтримує також X25519 та X448 (протокол узгодження ключів Діфі-Гелмена, заснований на використанні ЕК Curve25519 та Curve448, або еквівалентних Ed25519 та Ed448 із оцінками рівнів безпеки у 128 та 224 біт, відповідно), ЕЦП PureEdDSA та EdDSA згідно RFC8032 (використовує Curve448 у формі кривої Едвардса Ed448 та Curve25519 у формі скрученої кривої Едвардса Ed25519 із ґешуванням SHA-512).

Порівняння криптографічних бібліотек за сумісністю з операційними системами та за станом реалізації перетворень на кривих Едвардса

Табл. 1 і 2 відображають основні криптографічні бібліотеки, їх сумісність з різноманітними ОС та стан реалізації цифрового підпису на кривій Едвардса, окремих базових операцій над точками ЕК Едвардса та базових операцій над точками ЕК інших типів (Вейерштраса, Монтгомері).

Таблиця 1

Бібліотека	ЕК Едвардса	Інші типи ЕК	ЕЦП EdDSA
Botan	+	+	+
CryptoComply	+	+	+
Libgcrypt	+	+	+
Libsodium	+	+	+
Nsec	+	+	+
OpenSSL	+	+	+
wolfCrypt	+	+	+
Bouncy Castle	+	+	+
Crypto++	+	+	+
ACE	-	+	-
Nettle	-	+	-

Таблиця 2

Бібліотека	ОС	Потоко-безпечність
cryptlib	AMX, ARINC 653, BeOS, ChorusOS, CMSIS-RTOS/mbed-rtos, DOS, DOS32, eCOS, embOS, FreeRTOS/OpenRTOS, uItron, MQX, MVS, Nucleus, OS/2, Palm OS, QNX Neutrino, RTEMS, SMX, Tandem NonStop, Telit, ThreadX, uC/OS II, Unix (AIX, FreeBSD, HP-UX, Linux, macOS, Solaris, etc.), VDK, VM/CMS, VxWorks, Win16, Win32, Win64, WinCE/PocketPC/etc, XMK	+
wolfCrypt	Win32/64, Linux, macOS, Solaris, ThreadX, VxWorks, FreeBSD, NetBSD, OpenBSD, embedded Linux, WinCE, Haiku, OpenWRT, iPhone (iOS), Android, Nintendo Wii and Gamecube through DevKitPro, QNX, MontaVista, NonStop, TRON/ITRON/µITRON, Micrium's µC/OS, FreeRTOS, SafeRTOS, Freescale MQX, Nucleus, TinyOS, HP-UX	+
OpenSSL	Solaris, IRIX, HP-UX, MPE/iX, Tru64, Linux, Android, BSD (OpenBSD, NetBSD, FreeBSD, DragonflyBSD), NextSTEP, QNX, UnixWare, SCO, AIX, 32 and 64-bit Windows (Visual Studio, MinGW, UWIN, CygWin), UEFI, macOS (Darwin), iOS, HURD, VxWorks, uClinux, VMS, DJGPP (DOS), Haiku	+
Libsodium	macOS, Linux, OpenBSD, NetBSD, FreeBSD, DragonflyBSD, Android, iOS, 32 and 64-bit Windows (Visual Studio, MinGW, C++ Builder), NativeClient, QNX, JavaScript, AIX, MINIX, Solaris	+
CryptoComply	Linux (RHEL, CentOS, Debian, Ubuntu, etc.), Windows, iOS, Android, FreeBSD, macOS, Solaris, Java Runtime Environment	+
Crypto++	Unix (AIX, OpenBSD, Linux, MacOS, Solaris, etc.), Win32, Win64, Android, iOS, ARM	+
ACE	Unix, Windows, and more	+
Botan	Linux, Windows, macOS, Android, iOS, FreeBSD, NetBSD, OpenBSD, DragonflyBSD, AIX, QNX, Haiku, IncludeOS	+
NSec	Windows 10, macOS, CentOS, Debian, Fedora, OpenSUSE, Ubuntu	+
Libgcrypt	All 32 and 64 bit Unix Systems (GNU/Linux, FreeBSD, NetBSD, macOS etc.), Win32, Win64, WinCE and more	+
Bouncy Castle	General Java API: J2ME, Java Runtime Environment 1.1+, Android. Java FIPS API: Java Runtime 1.5+, Android. C# API (General & FIPS): CLR 4.	-

Порівняння обчислюваних характеристик криптографічних бібліотек

Було проведено експериментальні дослідження з метою порівняння швидкодії розглянутих бібліотек, а саме Libsodium v4.0 та NSec v 18.6, скомпільованих з використанням мови програмування C# та компілятора Roslyn. Експеримент проводився із

використанням програмного забезпечення Microsoft Visual Studio 2017 Community з проектним рішенням, яке застосовує бібліотеки, збудовані для 64-розрядних процесорів. Вимірювався час виконання операцій формування та перевірки ЕЦП із використанням перетворень на еліптичній кривій Едвардса Ed25519 при застосуванні ґеш-функції SHA-512 для текстів довжини 10000 символів (бібліотеки підтримують двобайтове кодування символів). Оскільки інтерфейс функцій цих бібліотек не дозволяє виклик ґешування окремо від функцій формування / перевірки підпису, для виключення з результатів аналізу часу виконання ґеш-функції такі самі експерименти було проведено для мінімальної довжини тексту (1 символ). Результати вимірювань та їх порівняльні оцінки відображені у табл. 3. Таким чином, із розглянутих варіантів бібліотек NSec має кращі оцінки за рядом показників. Експерименти проводилися на комп'ютері з такими характеристиками: процесор – Intel® Core™ I 5-3210M (x64) CPU @ 2.50 GHz, ОЗП – 6,00Гб, HDD – 1000 Гб, ОС – MS Windows 10.

Таблиця 3

Розмір тексту, символів		10 000		1		(1)/(2)	(3)/(4)
Напрям перетворення		формування ЕЦП, такти / нс	перевірка ЕЦП, такти / нс	формування ЕЦП, такти / нс	перевірка ЕЦП, такти / нс		
		1	2	3	4		
I	NSec	1794 / 717,6	2175 / 870,0	652 / 260,8	1572 / 628,8	0,83	0,42
II	Libsodium	1810 / 724,0	2085 / 834,0	858 / 343,2	1576 / 630,4	0,87	0,54
(II) / (I)		1,01	0,96	1,32	1,00		

Висновки

Криві Едвардса набули великої популярності у криптографічному суспільстві та серед програмістів. Бібліотеки з використанням криптографії на ЕК Едвардса можна знайти на багатьох відомих мовах програмування, а спектр їх застосування доволі великий: криптовалюти (Nano, Monero), підписуюче програмне забезпечення (signify, asignify), DNS Пз (dnscrypt-proxy, DNSCryptClient), SSH Пз (OpenSSH, PuTTY), ОС (OpenBSD, OpenWrt), мережі (Tor, I2P), протоколи (TLS 1.3, Signal Protocol, SSH). Еліптичні криві Едвардса та алгоритми з їх використання реалізовані у таких бібліотеках, як Libsodium, OpenSSL, NSec, Botan, CryptoComply, Libgcrypt, wolfCrypt, Bouncy Castle, Crypto++. Найбільшого поширення набула бібліотека Libsodium, що має також .Net Core аналог – NSec, перевагами якого є легкість у використанні та швидке виконання операцій. При цьому Crypto++ пропонує більш розширені можливості: не тільки застосування електронного цифрового підпису, але й використання базових операцій на кривій, таких як подвоєння та складання точок, що може бути корисним при проведенні власних досліджень, удосконалень та додаткових розробок.

Список літератури:

1. *Edwards H.M.* A normal form for elliptic curves // Bulletin of the American Mathematical Society. 2007. P. 393 – 422.

2. *D.J. Bernstein, T. Lange*. Faster addition and doubling on elliptic curves // In K. Kurosawa, editor, ASIACRYPT, volume 4833 of LNCS. 2007. P. 29-50.

3. Libsodium for .NET – A secure cryptographic library: [Електронний ресурс]. Режим доступу: https://github.com/adamcaudill/libsodium-net.

4. A modern and easy-to-use cryptographic library for .NET Core based on Libsodium: [Електронний ресурс]. Режим доступу: https://github.com/ektrah/nsec.

5. Crypto++ Library: [Електронний ресурс]. Режим доступу: https://www.cryptopp.com.

6. The Bouncy Castle Crypto APIs: [Електронний ресурс]. Режим доступу: https://www.bouncycastle.org.

7. OpenSSL. Cryptography and SSL / TLS Toolkit: [Електронний ресурс]. Режим доступу: https://www.openssl.org/.

Харківський національний
університет радіоелектроніки

Надійшла до редколегії 08.10.2018

УДК 004.056.55

І.Д. ГОРБЕНКО, д-р техн. наук, І.С. КУДРЯШОВ, В.В. ОНОПРІЄНКО

ПОРІВНЯЛЬНИЙ АНАЛІЗ ПОСТКВАНТОВИХ СТАНДАРТІВ ЕЛЕКТРОННОГО ПІДПИСУ НА ОСНОВІ МУЛЬТИВАРІАТИВНИХ КВАДРАТИЧНИХ ПЕРЕТВОРЕНЬ

Вступ

Наприкінці 2016 року NIST (Національний інститут стандартів та технології) США оголосив конкурс на нові стандарти постквантової асиметричної криптографії [1]. До таких систем належать, зокрема, механізми електронного підпису(ЕП), направленого шифрування(НШ) та протоколи інкапсуляції ключів(ПІК). Значне число кандидатів на ЕП розроблено на основі застосування мультиваріативних квадратичних перетворень (Multivariate Quadratic Transformations, MQ-transformations) [3 – 10]. Механізми MQ-перетворень дозволяють забезпечити необхідні рівні стійкості, швидкодію та застосування в малоресурсних системах. Такі властивості MQ-перетворень мають суттєве значення для практичних додатків, тому їх аналіз та порівняння є важливою проблемною задачею, тим більше, що вона вирішується NIST США на міжнародному рівні.

Метою статі є розгляд та аналіз механізмів електронного підпису, які були запропоновані на конкурс NIST PQC, а також порівняння їх властивостей згідно з вимогами NISN щодо технічних, техніко-економічних та техніко-експлуатаційних.

У роботі розглянуті 8 з 9 MQ-схем, а саме: LUOV [3], Gui [4], Rainbow [5], MQDSS [6], TPSig [7], DualModeMS [8], HiMQ-3 [9] та GeMSS [10]. Для первинної оцінки криптографічної стійкості було проведено аналіз відповідності алгоритмів ЕП вимогам до криптосистем з відкритим ключем, а саме – до забезпечення захищеності від підробки [11, 12]. Сутність такої захищеності зведена до оцінки захищеності до атак на основі адаптивного підбору повідомлень (UF-CMA)[12] та стійкості від екзестенційної підробки з адаптивним підбором повідомлень (EUF-CMA).

При описі вимог до алгоритмів-кандидатів конкурсу були визначені такі рівні криптографічної стійкості, що визначені в [1, 2]:

Рівень 1: коли атака, яка зламує EUF-CMA-стійкий алгоритм, повинна вимагати для своєї реалізації пошуку ключа аналогічно AES-128; рівень 2 – потребує пошуку колізії для 256-бітної геш-функції аналогічно SHA256/SHA3-256; рівень 3 – аналогічний пошук ключа AES-192; рівень 4 – пошук колізії для 256-бітної геш-функції, наприклад SHA384/SHA3-384; рівень 5: коли атака на EUF-CMA-стійкий алгоритм ЕП вимагає обчислювальних ресурсів, аналогічних пошуку ключа AES-256.

Ми висуваєм також перспективні вимоги забезпечення 6 та 7 рівнів безпеки, маючи на увазі забезпечення 364 та 512 біт класичної та відповідно 192 та 256 біт квантової безпеки.

Проведений аналіз показників має початковий характер. Усі результати показників були отримані експериментальним шляхом засобом программного моделювання. Але уже на початковому етапі досліджень визначені основні проблеми, що повязані зі складністю та вартістю у широкому змісті – як вартості застосування, так і вартості криптоаналізу, так як ці характеристики є антагоністичними. Зменшення розмірів параметрів та ключів дозволяє зменшити складність криптографічних перетворень, але при цьому, як правило, зменшується складність криптоаналізу. Тому, уже на цьому етапі досліджень проекту NIST постала проблема мінімізації вартості асиметричних криптоперетворень типу АСШ, ЕП та ПІК. Тому будемо розглядати і цю проблему, по аналогії, як безумовну при дослідженні.

1. Сутність та загальна характеристика MQ-механізмів

Серед кандидатів на асиметричні перетворення типу АСШ, ЕП та ПІК 10 пропозицій грунтуються на механізмах багатовимірних MQ-перетворень. Аналіз показує, що

багатовимірна MQ криптографія ґрунтується на складності вирішення задач, що пов'язані з багатовимірними поліномами над кінцевими полями та вирішенням систем багатовимірних поліноміальних рівнянь. Основними особливостями MQ-перетворень є невеликі, у порівнянні з іншими, ключі, складність асиметричних перетворень та невеликі обчислювальні ресурси здійснення перетворень. Як наслідок, вказане дозволяє реалізувати MQ-перетворення у відносно простих засобах ЕП.

Розглянемо сутність MQ-перетворенння. Нехай F_q є скінченне поле з q елементами. Також, нехай система мультиваріативних квадратичних поліномів $P=(P^{(1)},...,P^{(m)})$, з m рівняннями та n змінними визначена як:

$$P^{(k)}(x_1,...,x_n)=\sum_{i=1}^{n}\sum_{j=1}^{n}\gamma_{ij}^{(k)}x_i x_j+\sum_{i=1}^{n}\beta_i^{(k)}x_i+\alpha_0^{(k)},$$
$$k=1...m,\gamma_{ij}^{(k)},\beta_i^{(k)},\alpha_0^{(k)}\in \mathrm{F}_q \qquad (1)$$

Основна ідея для конструкції MQ-схем полягає у тому, що необхідно обрати **секретну** систему $F=(F^{(1)},...,F^{(m)}):\mathrm{F}_q^n\to\mathrm{F}_q^m$ (так зване центральне відображення), яка складається з m мультиваріативних квадратичних поліномів, n змінних, яка може бути інвертована з поліноміальною складністю.

Для того щоб сховати структуру центрального відображення F у публічному ключі, необхідно обрати два афінних лінійних відображення $S:\mathrm{F}_q^m\to\mathrm{F}_q^m$ та $T:\mathrm{F}_q^n\to\mathrm{F}_q^n$. В якості публічного ключа використовується композиція квадратичних відображень $P=S\circ F\circ T$, яку важко відрізнити від випадкової системи і, тому складно інвертувати. В якості приватного ключа використовується сукупність відображень (S,F,T), при знанні яких можна інвертувати публічний ключ P.

Послідовність (схема) генерації та перевірки ЕП [9], що базується на MQ-перетвореннях, наведено на рис. 1.

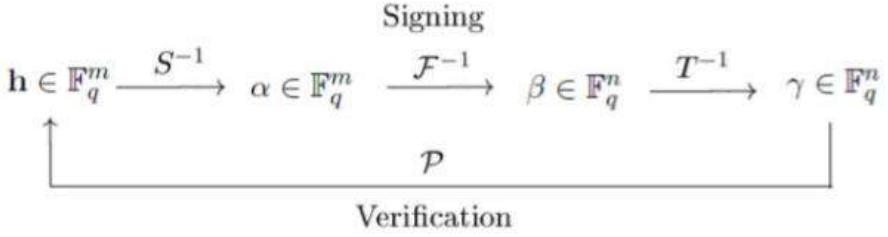


Рис. 1. Схеми вироблення та перевірки ЕП на основі MQ-схеми

2. Характеристика та властивості відомих механізмів ЕП

На конкурс NIST було подано вісім кандидатів, що грунтуються на MQ-перетвореннях – **LUOV** [3], **Gui** [4] , **Rainbow** [5], **MQDSS** [6], **TPSig** [7], **DualModeMS** [8] , **HIMQ-3** [9] та **GeMSS** [10] . Розглянемо їх та виберемо параметри, що необхідні для порівняння.

Механізм (схема) LUOV [3] (автор Ward Beullens) – Lifted Unbalanced Oil and Vinegar – є простим удосконаленням схеми UOV, у якому значно зменшено розмір відкритих ключів. Схема ЕП Unbalanced Oil and Vinegar (UOV) є однією з найстаріших і найкраще вивчених криптосистем. Схема UOV дуже проста. Має невеликі розміри ЕП та є достатньо швидкою. Основним недоліком UOV є те, що в ній відкриті ключі досить великі. В ній використовується операція піднесення публічного ключа (lifted – означає піднесений) до розширення поля таким чином, щоб зменшити розмір ключа. Схема LUOV може бути використана в двох режимах. Звичайний режим ЕП, в якому повідомлення аутентифікуються шляхом безпосередньо додавання ЕП. Іншим є режим відновлення повідомлень, який

дозволяє зменшити розміри ЕП та повідомлення. Причому, у режимі відновлення повідомлення частина повідомлення не передається, вона може бути відновлена безпосередньо на основі ЕП. Автори представили шість різних модифікацій схем ЕП, які, використовуючи відповідні параметри, реалізують 2, 4, та 5 рівні захисту. До особливостей запропонованих модифікації необхідно віднести можливості зменшення розміру ЕП та публічного ключа. Це досягається за рахунок зміни степеня розширення поля, коли чим менший степінь, тим більше розмір публічного ключа, а ЕП менші. Причому розмір секретного ключа залишається незмінним. Модель EUF-CMA безпеки в схемі LUOV гарантується за рахунок використання для реалізації механізму ЕП схеми UOV.

Механізм (схема) Gui [4] (автори – Ming-Shing Chen, Albrecht Petzoldt, Dieter Schmidt, Bo-Yin Yang) базується на HFEv-схемі ЕП, яку вперше запропонували Патарін, Куртуіз та Губін. В модифікованій схемі QUARTZ, як і в Gui, використовується спеціально розроблений процес вироблення ЕП, що дозволяє зменшити порівняно з оригінальним дизайном HFEv розміри ЕП. В Gui застосовується інший підхід. Він зводиться до зниження степені поліномів HFE та одночасно зменшенні числа рівнянь та змінних vigenar. Вказане дозволяє різко прискорити процес розробки (створення) схеми ЕП без послаблення його безпеки. Але стандартна схема Gui гарантує лише універсальну непідробність. Для того щоб отримати EUF-CMA захист, необхідно ввести деякі додаткові перетворення. При цьому основна різниця полягає у тому, що необхідно використовувати випадковий бінарний вектор r, або так звану сіль. Крім того, замість генерації ЕП для ґеш-значення $h = H(d)$, ЕП виробляється для $H(H(d) \| r)$. Результатом ЕП є значення, $\sigma^* = (\sigma, r)$, де σ – це стандартний підпис Gui. Щодо нього гарантується, що зловмисник не може підробити пару ґеш-підписів [4]. У цілому на конкурс було представлено три модифікації Gui-184, Gui-312, та Gui-448, з відповідними параметрами, які забезпечують 1, 3, та 5 рівні захисту, як і у HFEv.

Механізм ЕП Rainbow [5] (автори – Ming-Shing Chen, Albrecht Petzoldt, Dieter Schmidt, Bo-Yin Yang) базується на добре відомій UOV схемі, яка була запропонована ще у 1999 році. Безпосередньо ЕП Rainbow було створено у 2005 році та дороблено для захисту від знайденої атаки у 2008 році засобом зміни параметрів. Стандартна схема Rainbow надає лише універсальну непідробність. Для того, щоб отримати EUF-CMA захист, необхідно ввести параметри, що схожі з Gui перетворення. В Rainbow запропоновано найбільшу кількість модифікацій алгоритму – всього 9. Показано, що запропоновані варіанти параметрів відповідають, вірніше забезпечують 1, 3, 4 та 5 рівні захисту.

Механізм MQDSS [6] (автори – Ming-Shing Chen, Andreas Husing, Joost Rijneveld, Simona Samardjiska, Peter Schwabe) є механізмом ЕП, що грунтується на мультваріативних квадратичних перетвореннях. Механізм розроблений шляхом застосування до 5-крокової схеми ідентифікації перетворення Фіата-Шаміра (Fiat-Shamir transformation, FST). Якщо застосувати щодо схеми ідентифікації з $2q+1$ кроками схему FST, то отримаємо схему ЕП MQDSS. Вона адаптована до вирішення MQ-проблеми. Алгоритм генерації ключа MQDSS-q-n формально відповідає MQ. Доказ EUF-CMA безпеки ґрунтується на доказі безпеки будь-якої схеми, до якої було застосовано у FST (детальніше у [6]). Всього було запропоновано 15 варіацій схеми, але експериментальні дослідження показників виконані лише для двох схем: MQDSS-31-48 та MQDSS-31-64. Вони забезпечують тільки 2 та 4 рівні захисту відповідно. Необхідно відмітити, що ця схема має найменшу обчислювальну складність генерації ключової пари.

Механізм TPSig [7] (автори – Yossi (Joseph) Peretz, Nerya Granot) – є схемою ЕП, що базується на рішенні MQ-проблеми та проблеми NSARE(Асиметричні Алгебраїчні Рівняння Рікатті). Ця схема вже відхилена на конкурсі через те, що складність встановлення секретного ключа з підпису була лінійною. Схема **TPSig** має 2 модифікації для 1 та 5 рівнів захисту відповідно.

Механізм DualModeMS [8] (автори – J.-C. Faug`ere, L. Perret, J. Ryckeghem) – A Dual Mode for Multivariate-based Signature – є ЕП на основі мультиваріативних перетворень з

доволі нестандартною властивістю. Властивість ця полягає у тому, що публічний ключ має дуже маленький розмір, у той час коли сам підпис є великим. Цей підпис базується на HFEv схемі, яка модифікується за допомогою методу SBP, що дозволяє перетворити будь-який мультиваріативний підпис на основі MI на новий підпис, але з меншим публічним ключем, та більшим підписом. Таким чином, цей механізм поділяється на дві модифікації. На першому рівні (внутрішньому) – Inner.DualModeMs – рівні здійснюється ЕП, який базується на HFEv схемі, а на другому(зовнішньому) виконуються операції методу SBP. Цей підпис свого роду є підписом GeMSS з перетворенням SBP [11]. При використанні механізму забезпечується модель EUF-CMA захисту. Він грунтується на HFEv схемі, як на внутрішньому рівні так і на зовнішньому. Всього запропоновано три модифікації алгоритму: DualModeMS128, DualModeMS192, DualModeMS256, які повинні забезпечувати 1, 3, та 5 рівні безпеки відповідно. Для кожної з цих модифікацій наведено вхідні параметри системи, але показники щодо розміру ключів, ЕП та обчислювальної ефективності наведені лише для варіанту DualModeMS128.

Механізм HIMQ-3 [9] (автор – Kyung-Ah Shim) – A High Speed Signature Scheme based on Multivariate Quadratic Equations – є ЕП, що базується на модифікації стандартної MQ-схеми ЕП з парадигмою MQ+IP. Її сутність полягає у тому, що складність базується не тільки на вирішенні MQ-проблеми, а також на проблемі невизначеності ізоморфізму поліномів (IP-problem). В механізмі при виробленні ЕП, спочатку необхідно ввести деякі модифікації центрального відображення. Математичний доказ EUF-CMA було представлено у поданій на конкурс документації. Існують дві модифікації ЕП HiMQ-3 та HiMQ-3F, обидві забезпечують перший рівень захисту, і, мабуть, їх можна використовувати у смарт-картках.

Механізм GeMSS [10] (автори – J.-C. Faug`ere, L. Perret, J. Ryckeghem, A. Casanova, G. Macario-Rat, J. Patarin) – Great Multivariate Signature Scheme – що має схожість з DualModeMS. Відмінність полягає в тому, що ЕП при використанні має малий розмір, в той час, коли публічний ключ має великий розмір, а процес верифікації ЕП доволі швидкий. Цей ЕП базується на HFEv-схемі, оскільки HFE схема є доволі дослідженою в мультиваріативній криптографії. По суті GeMSS походить від QUARTZ, але має більш швидкі алгоритми, разом з тим ЕП є більш захищеним. Ця схема має три модифікації – GeMSS128, GeMSS192, GeMSS256 алгоритми. Для кожної модифікації визначені відповідні параметри, при застосуванні яких забезпечують 1, 3, 5 рівні захисту відповідно. Відмінність м**еханізму GeMSS** від ЕПА DualModeMS в тому, що він має відносно малі розміри відкритого ключа, але великі розміри ЕП. В той же час в механізмі модель EUF-CMA забезпечується за рахунок використаної схеми HFEv.

3. Порівняльний аналіз розміру ключів та підпису

Проведений аналіз дозволив визначити розміри публічного та секретного ключів та ЕП відповідно до вказаних авторами даних. В табл. 1 наведені модифікації різних алгоритмів, їх відповідний рівень безпеки, розміри ключів та ЕП. Для зручності порівнювальні характеристики були нормовані в вигляді байтів.

Так як значення параметрів відрізняються на декілька порядків, для більшої зручності на рис. 1 – 4 довжини ключових даних та ЕП наведені у логарифмічному масштабі. Сутність такого методу полягає в перетворенні величин даних наступним чином: $n = \log_{10} N$, де N – початкове значення, тобто довжини публічного та секретного ключів, а також ЕП, які підлягають масштабуванню, причому n є результатом обчислення десяткового логарифму над значенням, яке підлягає масштабуванню.

Слід зазначити, що дані наведені у гістограмах, відповідають усім вказаним вище варіаціям, та вони є впорядковані за зменшенням довжини. Відповідно до вимог системи, яка буде використовувати механізми ЕП, якщо зафіксувати рівень захисту, будуть змінюватися переваги на користь використання меншого публічного ключа, або секретного ключа. Так,

наприклад, у малоресурсних системах переважними будуть алгоритми, які використовують менші розміри ключових даних.

Таблиця 1

Характеристика основних криптографічних параметрів (у байтах)

№	Схема	Модифікація	Рівень захисту	Розмір публічного ключа	Розмір секретного ключа	Розмір підпису
1	LUOV	LUOV-8-63-256	2	15,872	32	319
		LUOV-8-90-351	4	46,080	32	441
		LUOV-8-117-404	5	100,967	32	521
		LUOV-48-49-242	2	7,476	32	1,741
		LUOV-64-68-330	4	19,968	32	3,175
		LUOV-80-86-399	5	40,244	32	4,813
2	GUI	Gui-184	1	426,292	19,559	45
		Gui-312	3	2,002,023	60,724	63
		Gui-448	5	5,928,141	159,642	83
3	Rainbow	Ia	1	152,064	100,250	64
		Ib	1	151,860	106,189	78
		Ic	1	192,205	143,360	104
		IIIb	3	524,391	380,314	112
		IIIc	3	720,794	538,112	156
		IVa	4	565,453	376,116	92
		Vc	5	1,723,700	1,274,266	204
		VIa	5	1,351,373	892,109	118
		VIb	5	1,352,704	944,538	147
4	MQDSS	MQDSS-31-48	2	62	32	32,882
		MQDSS-31-64	4	88	48	67,800
5	TPSig	TPSig-1	1	86,324	973	84,224
		TPSig-2	5	266,240	1,690	512
6	DualMo-deMS	DualModeMS128	1	528	18,038,184	32,640
7	HiMQ-3	HiMQ-3	1	128,744	12,074	75
		HiMQ-3F	1	100,878	14,878	67
8	GeMSS	GeMSS128	1	417,408	14,208	48
		GeMSS192	3	1,304,192	39,440	88
		GeMSS256	5	3,603,792	82,056	104

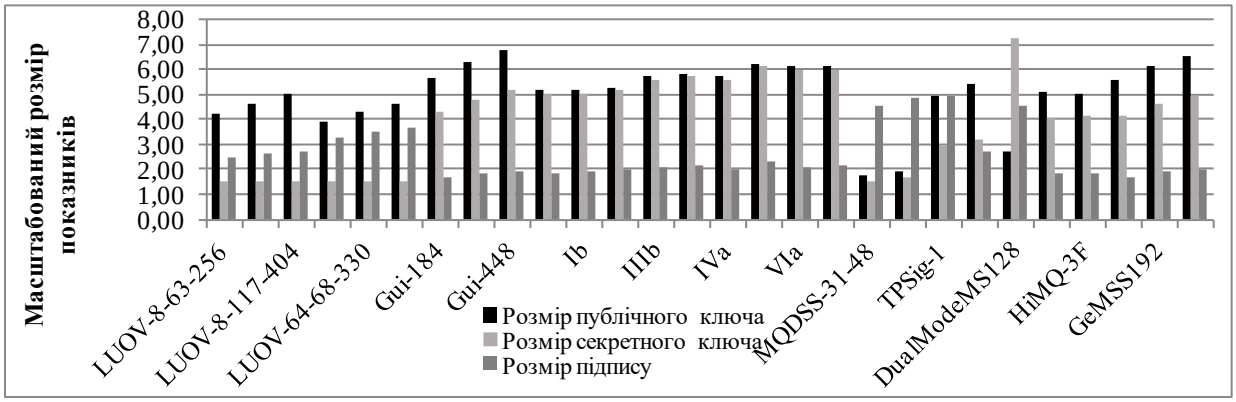


Рис. 2. Зведена гістограма показників розмірів ключових даних та ЕП
(байтів у логарифмічному масштабі)

Рис. 3. Гістограма порівнювального аналізу показників розміру публічного ключа
(байтів у логарифмічному масштабі) для ЕП

Рис. 4. Гістограма порівнювального аналізу показників розміру секретного ключа
(байтів у логарифмічному масштабі) для ЕП

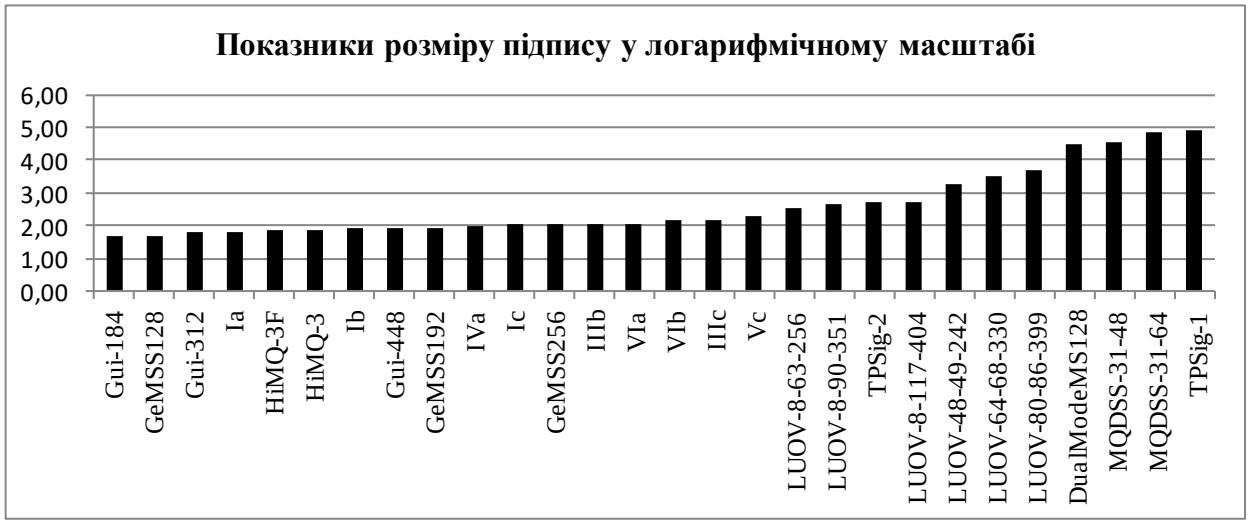


Рис. 5. Гістограма порівнювального аналізу показників розміру підпису (байтів у логарифмічному масштабі) для ЕП

Відповідно до даних, які показані на рис. 2, можна зробити висновок, що найменші довжини публічного ключа має MQDSS. В одній модифікації алгоритму – 62 байти (для рівня захисту 2), у другій – 88 (рівень захисту 4). Найбільші довжини публічного ключа мають Gui та GeMSS для рівня захисту 5 (для Gui також рівень захисту 3) – 5,928,141 байтів для Gui-448, 3,603,792 байтів для GeMSS256, та 2,002,023 для Gui-312. Також відносно малі довжини публічного ключа мають модифікації алгоритму LUOV для усіх представлених рівнів захисту. Усі інші представники мають приблизно рівні показники відповідно до забезпечених рівнів захисту.

Порівняльний аналіз для секретних (або приватних) ключів (рис. 3) показав, що серед представлених кандидатів найменші показники характерні для схеми підпису LUOV та MQDSS – в обох випадках по 32 байти. Однак слід зазначити, що LUOV реалізує 2, 4 та 5 рівні захисту, у той час, коли MQDSS має такий розмір лише для захисту рівня 1. Найбільші розміри секретних ключів мають DualModeMS та Rainbow схеми 18,038,184 та 1,274,266 байтів відповідно. Інші алгоритми мають приблизно однакові показники відповідно до реалізованих рівнів захисту.

Варто зауважити, що для усіх алгоритмів розміри підпису не перебільшують 100,000 байтів. Найменші показники відповідно до рівнів захисту мають Gui, GeMSS, та Rainbow, 45-83, 48-104, та 64-204 байти відповідно. При цьому вони можуть реалізовувати найвищий ступінь захисту. Найбільші розміри ЕП мають TpSig, DualModeMS та MQDSS, хоча ці показники відповідають рівням захисту 1 та 2. Відносно малі показники розміру підпису має також HiMQ-3, а LUOV розташувався посередині, хоча розмір підписів цього алгоритму значно перевищує лідерів у цьому показнику.

4. Порівняльний аналіз показників швидкодії

Оцінка показників швидкодії алгоритмів ЕП проведена авторами на різних обчислювальних платформах та представлена у табл. 2. Така оцінка наведена у циклах процесору, які необхідні для виконання операцій генерації ключової пари, створення ЕП, та його верифікації. Варто зазначити, що показники були отримані в процесі виконання алгоритмів без використання технологій оптимізації продуктивності. Деякі показники були вказані у мілісекундах та секундах, витрачених на виконання тієї чи іншої операції на зазначених обчислювальних платформах. Для того щоб проаналізувати обчислювальну ефективність алгоритмів, такі результати були переведені у кількість затрачених циклів процесору, визначену виходячи з характеристик обчислювальної платформи.

Така оцінка може дозволити провести порівняльний аналіз, не беручи до уваги обчислювальне середовище, з іншого боку вона носить лише первинний ознайомчий характер обчислювальної ефективності наведених вище алгоритмів.

Таблиця 2

Показники обчислювальної ефективності алгоритмів електронного підпису
(данні таблиці наведені у циклах процесору, які необхідно виконати для проведення кожної операції)

№	Схема	Модифікація	Генерація ключової пари	Вироблення ЕП	Перевірка ЕП
1	LUOV	LUOV-8-63-256	39,421,493	26,714,796	15,123,202
		LUOV-8-90-351	154,498,995	81,889,845	49,173,941
		LUOV-8-117-404	276,912,036	144,203,736	84,564,465
		LUOV-48-49-242	27,419,223	88,046,948	50,301,626
		LUOV-64-68-330	90,548,276	259,662,473	125,317,813
		LUOV-80-86-399	192,475,607	595,199,427	273,408,571
2	GUI	Gui-184	2,408,000,000	1,910,000,000	252,517
		Gui-312	43,817,000,000	25,436,000,000	724,044
		Gui-448	239,502,000,000	872,949,000,000	2,004,155
3	Rainbow	Ia	1,302,000,000	601,000	350,000
		Ib	4,578,000,000	2,044,000	1,944,000
		Ic	4,089,000,000	1,521,000	939,000
		IIIb	26,172,000,000	5,471,000	4,908,000
		IIIc	31,612,000,000	4,047,000	2,974,000
		IVa	11,176,000,000	1,823,000	1,241,000
		Vc	116,046,000,000	8,688,000	6,174,000
		VIa	45,064,000,000	3,916,000	2,897,000
		VIb	164,689,000,000	16,755,000	11,224,000
4	MQDSS	MQDSS-31-48	2,957,276	266,840,340	191,666,288
		MQDSS-31-64	6,680,606	776,183,461	571,665,382
5	TPSig	TPSig-1	212,676,920	864,000	1,387,800
		TPSig-2	302,400,000	1,228,500	2,160,000
6	DualMo-deMS	DualModeMS128	2,072,200,000,000	6,006,000,000	6,994,000
№	Схема	Модифікація	Генерація ключової пари	Створення підпису	Перевірка підпису
7	HiMQ-3	HiMQ-3	157,899,562	321,443	614,735
		HiMQ-3F	232,452,977	162,823	527,330
8	GeMSS	GeMSS128	1,398,800,000	3,172,000,000	19,656,000
		GeMSS192	6,422,000,000	7,904,000,000	65,494,000
		GeMSS256	18,174,000,000	12,740,000,000	160,420,000

На рис. 5 – 8 наведені гістограми швидкодії для усіх модифікацій алгоритмів. Найменша кількість циклів, затрачених на виконання операцій, є більш кращим показником. Якщо кількість циклів має більше значення – це означає, що виконання операції займає багато часу і потребує більш потужної обчислювальної платформи.

На рис. 5 наведено зведену гістограму усіх показників швидкодії, яка показує загальне співвідношення ефективності обчислення кожної з трьох операцій (формування ключових даних, вироблення та перевірка ЕП) для кожної з наведених варіацій. Усі дані наведено у кількості циклів процесору, які необхідно використати при виконанні тієї чи іншої операції.

Майже однакову швидкість виконання всіх операцій має алгоритм LUOV. Невелика різниця між трьома операціями також є у GeMSS, MQDSS, та TPSig які мають невеликі аномалії у процесі перевірки підпису для першого кандидату, та генерації ключової пари для двох останніх. Суттєво більше часу на генерацію ключової пари вимагає Rainbow, хоча він

виконує операції з ЕП значно швидше більшості алгоритмів. Gui вимагає малих затрат на перевірку підпису, проте для створення підпису і ключової пари навпаки – великих.

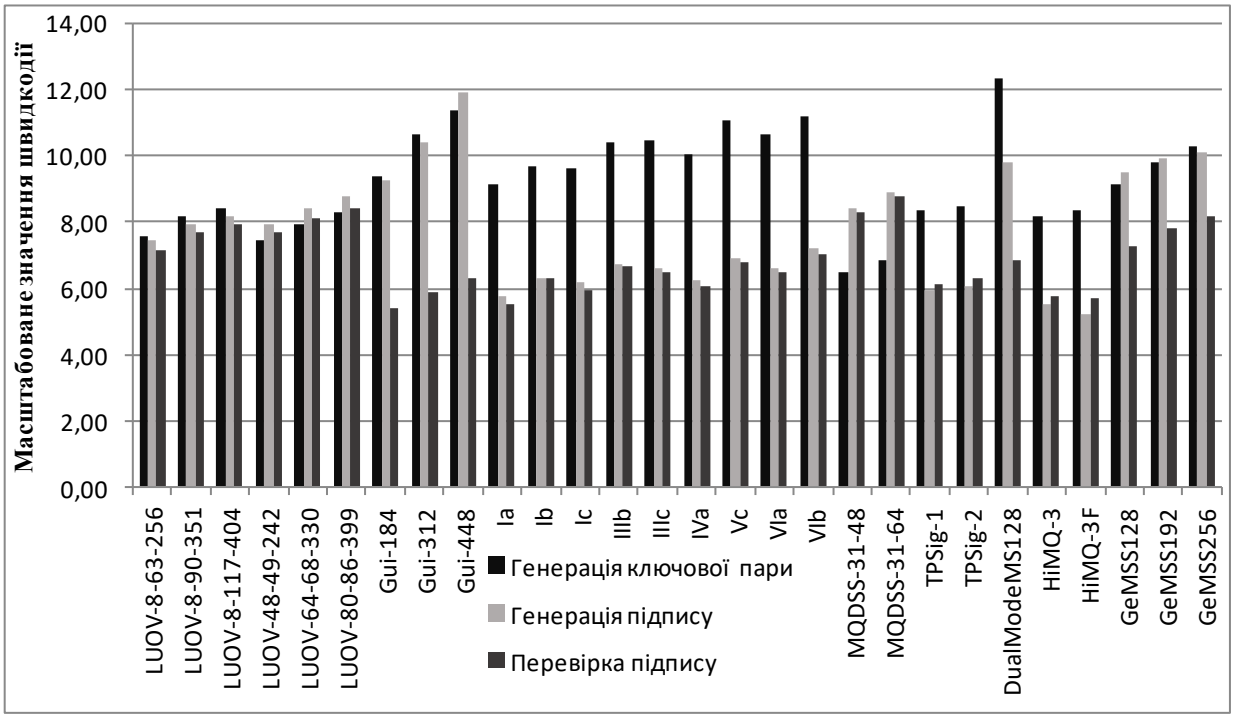


Рис. 6. Зведена гістограма показників швидкодії (циклів у логарифмічному масштабі)

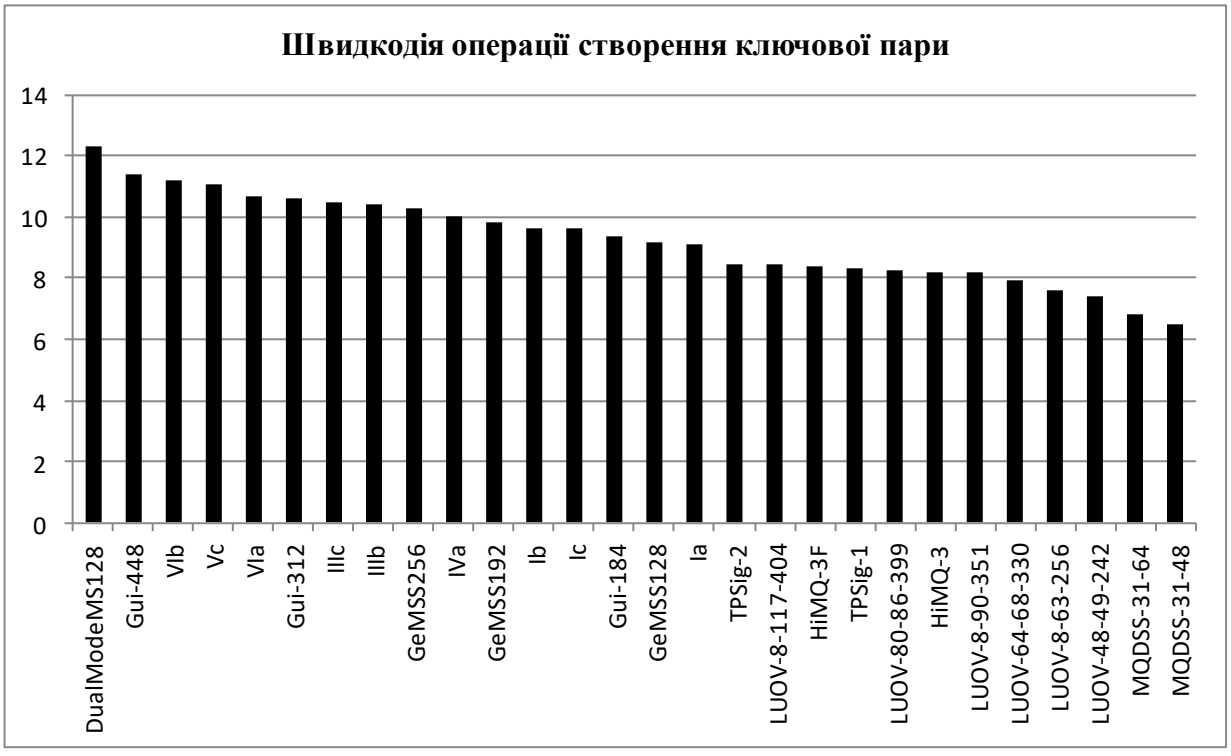


Рис. 7. Гістограма порівнювального аналізу показників швидкодії операції створення ключової пари (циклів у логарифмічному масштабі) для алгоритмів електронного підпису

Рис. 8. Гістограма порівнювального аналізу показників швидкодії операції генерації підпису (циклів у логарифмічному масштабі) для алгоритмів електронного підпису

Рис. 9. Гістограма порівнювального аналізу показників швидкодії операції перевірки підпису (циклів у логарифмічному масштабі) для алгоритмів електронного підпису

Оцінка швидкості операції створення ключової пари (рис. 6) показала, що найшвидшими схемами є MQDSS та LUOV, у той час, коли DualModeMS демонструє найгірші показники через додаткове SBP перетворення. Варто зазначити, що MQDSS та LUOV мають також і малі розміри ключових даних, а DualModeMS навпаки має великий розмір секретного ключа, який отримується шляхом «перенесення» ключових даних з публічного ключа до секретного.

Гістограма аналізу швидкодії операції вироблення ЕП вказує на те, що найшвидшим є HiMQ-3, але він реалізує лише 1 рівень захисту. Середні показники демонструє LUOV, а найгіршими за показником швидкодії створення ЕП є Gui та GeMSS.

Показники швидкодії операції перевірки ЕП демонструють такі результати: швидкими є Gui, Rainbow, та HiMQ-3 (що характерно, тому що HiMQ-3, як вже зазначалось, реалізує лише 1 рівень захисту), повільними є MQDSS, LUOV та GeMSS.

5. Обгрунтування вибору перспективних алгоритмів

Усі отримані результати узагальнені для кожного показника та наведені в табл. 3.

Таблиця 3

Показники зайнятих місць, відповідно до зазначених показників, модифікацій схем ЕП на основі MQ-перетворень

Модифікація	Розмір публічного ключа	Розмір секретного ключа	Розмір підпису	Створення ключової пари	Створення підпису	Перевірка підпису	Сума
HiMQ-3	12	11	6	7	2	4	42
HiMQ-3F	11	13	5	10	1	3	43
Ia	13	18	4	13	3	2	53
LUOV-8-63-256	5	1	18	4	14	18	60
TPSig-1	9	9	28	9	4	8	67
LUOV-8-90-351	8	2	19	6	15	20	70
LUOV-48-49-242	4	4	22	3	16	21	70
Gui-184	18	14	1	15	22	1	71
Ib	14	19	7	17	8	9	74
TPSig-2	16	10	20	12	5	11	74
Ic	15	20	11	16	6	6	74
LUOV-64-68-330	6	5	23	5	18	24	81
MQDSS-31-48	2	7	26	1	19	26	81
LUOV-8-117-404	10	3	21	11	17	23	85
IVa	20	23	10	19	7	7	86
MQDSS-31-64	1	8	27	2	21	28	87
GeMSS128	17	12	2	14	23	19	87
LUOV-80-86-399	7	6	24	8	20	27	92
Gui-312	26	16	3	23	27	5	100
IIIb	19	22	13	21	11	14	100
IIIc	21	24	16	22	10	13	106
VIa	23	25	14	24	9	12	107
GeMSS192	22	15	9	18	25	22	111
Vc	25	27	17	25	12	15	121
VIb	24	26	15	26	13	17	121
Gui-448	28	21	8	27	28	10	122
DualModeMS128	3	28	25	28	24	16	124
GeMSS256	27	17	12	20	26	25	127

Наведені в таблиці дані дозволяють зробити висновок, що сумарними оцінками показників швидкодії та розмірів ключів і підпису, перспективними кандидатами на пост-квантовий стандарт електронного підпису можуть бути HiMQ-3, Rainbow та LUOV. Перевага належить схемам Rainbow та LUOV тому, що вони можуть реалізувати декілька рівнів захисту, тим самим підлаштовуючись під потреби. Також ці механізми мають різні перспективи використання. Так, наприклад, LUOV має малі розміри ключів, що дозволить

використовувати цей алгоритм у криптографії для пристроїв з обмеженими ресурсами. У той самий час, Rainbow має одні з найменших показників розміру підпису.

6. Схема підпису RAINBOW

Пропонується розглянути схему Rainbow[5] як приклад реалізації схеми підпису на базі мультиваріативних багатовимірних перетворень. Цей механізм базується на схемі UOV [13]. Сутність таких схем полягає у тому, що існують два типи змінних – vinegar (змінні O) та oil (змінні M). Перші при обчисленні центрального відображення (1) обираються випадковим чином, а інші – використовуються як значення геш-функції від повідомлення. Особливістю схеми UOV є те, що зазвичай кількість v змінних O має складати $v = 2o...3o$ від кількості o змінних M.

Для схеми підпису Rainbow існують такі загальносистемні параметри [5]: (q, v_1, o_1, o_2), де q – порядок поля (зазвичай береться розширення поля ступеню 2, у поданих специфікаціях – 16 для модифікацій «a», 31 для модифікацій «b», 256 для модифікацій «c»); v_1 – кількість змінних O на першому рівні; o_1, o_2 – таке, що $o_1 + o_2 = m$, розміри рівнів Rainbow (кількість рівнянь на кожному рівні); U – кількість рівнів; $m = n - v_1$ – кількість рівнянь, де n – кількість змінних.

Для модифікації Ib маємо такі параметри (31, 36, 28, 28). Можна визначити, що $m = 28 + 28 = 56$ – кількість рівнянь для цієї модифікації. $n = v1 + m = 36 + 56 = 92$ – кількість змінних.

Генерація ключової пари

Для створення центрального відображення будується система індексів: нехай $V = \{1, 2, 3, \ldots, n\}$ – множина індексів. Також нехай існує $v_1, ..., v_{u+1}$ – $u+1$змінних, таких, що задовольняють вимозі $0 < v_1 < v_2 \ldots < v_{u+1} = n$. Також для кожного $\ell = 1, \ldots, u+1$ існує множина індексів $V_\ell = \{1, 2, \ldots, v_\ell\}$. Таким чином, кількість елементів множини V_i, або її потужність, складає $|V_i| = v_i$.

Нехай $o_i = v_{i+1} - v_i$ для $i = 1, \ldots, u$

Також визначимо множини індексів змінних Oil O_i такі, що $O_i = V_{i+1} - V_i$ для кожного $i = 1, \ldots, u$.

Далі будуються поліноми центрального відображення (1):

$$f^{(k)}(x_1, ..., x_n) = \sum_{i, j \in V_\ell, i \le j} \alpha_{ij}^{(k)} x_i x_j + \sum_{i \in V_\ell, j \in O_\ell} \beta_{ij}^{(k)} x_i x_j + \sum_{i \in V_\ell \cup O_\ell} \gamma_i^{(k)} x_i + \delta^{(k)},$$

Відповідно можна визначити, що для кожного $k \in \{v_1 + 1, ..., n\}$ існує лише одне $\ell \in \{1, ..., u\}$ таке, що $k \in O_\ell$. Кожний з рівнів $\ell = 1, \ldots, u$ можна описати райдугою (rainbow) змінних [14]:

$[x_1, \ldots, x_{v1}]$, $\{x_{v1+1}, \ldots, x_{v2}\}$

$[x_1, \ldots, x_{v2}], \{x_{v2+1}, \ldots, x_{v3}\}$

……

$[x_1, \ldots, x_{v_{u-1}}] \{x_{v_{u-1}} + 1, \ldots, x_n\}$

Для кожного рівня l змінні у квадратних дужках «[]» є змінними Vinegar, а у фігурних дужках «{}» – змінними Oil.

Таким чином, для модифікації (31, 36, 28, 28) можна визначити, що:

$v_1 = 36, v_2 = 64, v_3 = 92$ – кількість змінних Vinegar на різних рівнях;

$o_1 = 28, o_2 = 28$ – кількість змінних Oil на різних рівнях;

$V_1 = \{1,...,36\}, V_2 = \{1,...,64\}, V_3 = \{1,\ldots,92\}$ – індекси змінних Vinegar;

$O_1 = \{37,...,64\}, O_2 = \{65,\ldots,92\}$ – індекси змінних Oil.

Оскільки подані специфікації мають лише 2 рівня, відповідно для них можна легко описати таку райдугу. Для модифікації Ib:

$[x_1,...,x_{36}]\{x_{37},\ldots,x_{64}\}$

$[x_1,\ldots,x_{64}]\{x_{65},\ldots,x_{92}\}$

Легко бачити, що кількість поліномів $f^{(k)}$ буде дорівнювати $n-(v_1+1)+1=n-v_1=m$. Коефіцієнти $\alpha_{ij}^{(k)}, \beta_{ij}^{(k)}, \gamma_i^{(k)}$ та $\delta^{(k)}$ є випадково вибраними елементами поля F_q.

Далі випадковим чином з елементів поля генерується F_q матриця M_S розміром $m \times m$ таким чином, що в полі F_q існує матриця $InvS$ така, що $M_S * InvS = E$, де E – одинична матриця.

Випадковим чином генерується вектор-стовпець c_S із елементів поля F_q розміром *m*.

Можна стверджувати, що $S = M_S x + c_S$ є афінним відображенням.

Далі випадковим чином генерується з елементів поля F_q матриця M_T розміром $n \times n$ таким чином, що в полі F_q існує матриця $InvT$ така, що $M_T * InvT = E$, де E – одинична матриця.

Випадковим чином генерується вектор-стовпець c_T із елементів поля F_q розміром *n*.

Тому можна стверджувати, що $T = M_T x + c_T$ є афінним відображенням.

Приватний ключ складається з ($InvS, c_S, F, InvT, c_T$).

Публічним ключом є композиція відображень $P = S \circ F \circ T$. Для того щоб забезпечити захист EUF-CMA, необхідно до секретного та публічного ключа додати розмір ℓ випадкової послідовності [5]. Отже, ключевою парою є $(sk, pk) = ((InvS, c_S, F, InvT, c_T, \ell), (S \circ F \circ T, \ell))$

Вироблення ЕП

Нехай для підпису поданий документ d. Для цього документу обчислюється геш-значення $h = H(d)$. Легко можна обчислити $x = S^{-1}(h)$. Сутність вироблення ЕП полягає у тому, що необхідно знайти прообраз y центрального відображення F для значення x, тобто $F(y) = x$.

Підпис створюється наступним чином. Маємо особистий ключ ($InvS, c_S, F, InvT, c_T$), та повідомлення d:

1. Заповнюються перші v_1 значень вектору y як змінні Оцту (тобто їх заповнення дозволить знайти однозначне рішення системи):

   a) випадковим чином генеруються v_1 елементів поля F_q $y_1,...,y_{v_1}$ і підставляються замість змінних Оцту у рівняння $f^{(k)}$. Таким чином отримуємо нову систему рівнянь:

   $$\hat{f}^{(k)} = f^{(k)}(y_1,...,y_{v_1}), k = v_1+1,...,n;$$

   b) для відображення $\hat{f}^{(k)}$, яке є афінним, знаходимо такі $\hat{F}$ та c_F що $\hat{F}^{(k)} = \hat{F}x + c_F$;

   c) якщо матриця $\hat{F}$ не є зворотною, перейти до кроку 1, *a*.
2. Нехай є повідомлення d. Обчислюється значення $h = H(d)$.
3. Необхідно значення $h = H(d)$ перетворити на *m* елементів поля F_q.
4. Обчислюється $x = InvS(d - c_S)$.

5. Обчислимо $y_{v_1+1},\ldots,y_{v_2}$ що $y_{v_1+1},\ldots,y_{v_2} = InvF((x_{v_1+1},\ldots,x_{v_2}) - c_F)$.
6. Підставимо ці значення у систему рівнянь $\widehat{f}^{(v_2+1)},...,\widehat{f}^{(n)}$, отримаємо нову систему:

$$\widehat{f}^{(v_2+1)},...,\widehat{f}^{(n)} = \widehat{f}^{(v_2+1)}(y_{v_1+1},\ldots,y_{v_2}),...,\widehat{f}^{(n)}(y_{v_1+1},\ldots,y_{v_2})$$

7. Знайдемо останні $y_{v_2+1},\ldots,y_n$ як рішення системи рівнянь

$$y_{v_2+1},\ldots,y_n = (\widehat{f}^{(v_2+1)} = x_{v_2+1},\ldots,\widehat{f}^{(n)} = x_n)$$

8. Якщо не існує таких рішень або рішення не є випадковим, повернутись до кроку 2.
9. Обчислити $z = InvT(y - c_T)$.
10. Підписом є документ d є z.

Перевірка підпису

Перевірка підпису здійснюється наступним чином. Маємо публічний ключ $P = S \circ F \circ T$, повідомлення d та підпис $\sigma = z$:

1. Обчислимо $h = H(d)$.
2. Знайдемо рішення $h' = P(z)$.
3. Якщо h та h` співпадають $h = h'$, підпис є коректним.

Для досягнення захисту EUF-CMA підпис та перевірка підпису здійснюються для $h = H(H(d) \| r)$, де r – випадково генерована послідовність довжиною ℓ біт. Підписом у цьому випадку є $\sigma = (z, r)$ [5].

Висновки

1. Як показав аналіз, 8 із 9 MQ- схем ЕП, а саме: LUOV [3], Gui [4], Rainbow [5], MQDSS [6], TPSig [7], DualModeMS [8], HiMQ-3 [9] та GeMSS [10] заслуговують уваги з точки зору можливого застосування в якості схеми ЕП.

2. В процесі первинної оцінки криптографічної стійкості було проведено аналіз відповідності алгоритмів ЕП вимогам до криптосистем з відкритим ключем, а саме – до забезпечення захищеності від підробки [11, 12]. Сутність такої захищеності зведена до оцінки захищеності до атак на основі адаптивного підбору повідомлень (UF-CMA)[12] та стійкості від екзестенційної підробки з адаптивним підбором повідомлень (EUF-CMA).

3. Серед кандидатів на асиметричні перетворення типу 10 пропозицій грунтуються на механізмах багатовимірних MQ-перетворень. Аналіз показує, що багатовимірна MQ криптографія ґрунтується на складності вирішення задач, що пов'язані з багатовимірними поліномами над кінцевими полями та вирішенням систем багатовимірних поліноміальних рівнянь. Основними особливостями MQ-перетворень є невеликі, у порівнянні з іншими, ключі, складність асиметричних перетворень та невеликі обчислювальні ресурси здійснення перетворень.

4. Порівняльний аналіз для секретних (або приватних) ключів (рис. 3) показав, що серед представлених кандидатів найменші показники характерні для схеми підпису LUOV та MQDSS – в обох випадках по 32 байти. Однак слід зазначити, що LUOV реалізує 2, 4 та 5 рівні захисту, у той час, коли MQDSS має такий розмір лише для 1 рівня

5 Найбільші розміри ЕП мають TpSig, DualModeMS та MQDSS, хоча ці показники відповідають рівням захисту 1 та 2. Відносно малі показники розміру ЕП має також HiMQ-3, а LUOV розташувався посередині, хоча розмір ЕП цього алгоритму значно перевищує лідерів у цьому показнику.

6. Майже однакову швидкість виконання всіх операцій має алгоритм LUOV. Невелика різниця між трьома операціями також є у GeMSS, MQDSS, та TPSig які мають невеликі аномалії у процесі перевірки підпису для першого кандидату, та генерації ключової пари для

двох останніх. Суттєво більше часу на генерацію ключової пари вимагає Rainbow, хоча він виконує операції з ЕП значно швидше більшості алгоритмів.

7. Механізм Rainbow базується на схемі UOV [13]. Сутність таких схем полягає у тому, що існують два типи змінних – vinegar (змінні O) та oil (змінні M). Перші при обчисленні центрального відображення (1) обираються випадковим чином, а інші – використовуються як значення геш-функції від повідомлення.

8. В ході досліджень було встановлено, що практично всі схеми відповідають формальним вимогам до кандидатів на постквантові схеми електронного підпису, тобто мають різні модифікації алгоритмів, які забезпечують різні рівні захисту (від одного рівня до чотирьох).

9. Попередні дослідження дозволили визначити в якості перспективних ЕП схеми Rainbow, LUOV та HiMQ-3, але слід зазначити, що вимірювання цих показників проводилися з використанням неоптимізованих алгоритмів у операційних системах. Подальші дослідження оптимізованих реалізацій є перспективним напрямом.

Список літератури:

1. Post-Quantum Cryptography, Round 1 Submissions, 2017. [On-line]. Internet: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.

2. Post-Quantum Cryptography, Call for Proposals, 2016. [On-line]. Internet: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization/Call-for-Proposals

3. Ward Beullens, Bart Preneel, Alan Szepieniec, Frederik Vercauteren. LUOV: Lifted Unbalanced Oil and Vinegar, NIST Submission, 2017. [On-line]. Internet: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.

4. Jintai Ding, Ming-Shen Chen, Albrecht Petzoldt, Dieter Schmidt, Bo-Yin Yang. Gui, NIST Submission, 2017. [On-line]. Internet: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.

5. Jintai Ding, Ming-Shen Chen, Albrecht Petzoldt, Dieter Schmidt, Bo-Yin Yang. Rainbow. NIST Submission, 2017. [On-line]. Internet: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.

6. Simona Samardjiska, Ming-Shing Chen, Andreas Hulsing, Joost Rijneveld, Peter Schwabe. MQDSS, NIST Submission, 2017. [On-line]. Internet: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.

7. Joseph Peretz, Nerya Granot. TPSig, NIST Submission, 2017. [On-line]. Internet: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.

8. J.-C. Faugère, L Perret, J Ryckeghem. DualModeMS: A Dual Mode for Multivariate-based Signature, NIST Submission, 2017. [On-line]. Internet: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.

9. Kyuang-Ah Shim, Cheol-Min Park, Aeyoung Kim. HiMQ-3: A High Speed Signature Scheme based on Multivariate Quadratic Equations, NIST Submission, 2017. [On-line]. Internet: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.

10. A. Casanova, J.-C. Faugère, G. Macario-Rat, J Patarin, L Perret, J Ryckeghem. GeMSS: A Great Multivariate Short Signature, NIST Submission, 2017. [On-line]. Internet: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.

11. Katz, Jonathan; Lindell, Yehuda. Introduction to Modern Cryptography: Principles and Protocols. Chapman & Hall / CRC Press, 2007. 404 p.

12. Bellare, Mihir; Rogaway, Phillip. Introduction to Modern Cryptography. [On-line]. Internet: http://web.cs.ucdavis.edu/~rogaway/classes/227/spring05/book/main.pdf, September 21, 2005.

13. Kipnis, Aviad. Unbalanced Oil and Vinegar Signature Schemes – extended version. EURO-CRYPT, 1999.

14. Jintai Ding, Dieter Schmidt. Rainbow, a New Multivariable Polynomial Signature Scheme. Springer-Verlag Berlin Heidelberg, 2005.

Харківський національний
університет імені В.Н. Каразіна;
АТ «Інститут інформаційних технологій», Харків

Надійшла до редколегії 03.11.2018

УДК 004.056.5

О.О. КУЗНЕЦОВ, д-р техн. наук, Ю.І. ГОРБЕНКО, канд. техн. наук,
А.С. КІЯН, А.О. УВАРОВА, Т.Ю. КУЗНЕЦОВА

ПОРІВНЯЛЬНІ ДОСЛІДЖЕННЯ ТА АНАЛІЗ ЕФЕКТИВНОСТІ ГІБРИДНОЇ КОДОВОЇ КРИПТОСИСТЕМИ

1. Вступ

Переважна більшість сучасних криптографічних систем побудована на механізмах, які забезпечують захист завдяки складності вирішення певної математичної задачі такої, як дискретне логарифмування, факторизація тощо [1, 2]. На противагу, криптосистеми, що засновані на кодуванні, нині не застосовуються широким загалом, але у найближчий час все може докорінно змінитися. Ця зміна обумовлена прагненням світової спільності створити повномасштабний квантовий комп'ютер, який буде здатен прискорити виконання операцій звичайного комп'ютера в десятки чи навіть сотні разів [3]. З огляду на це актуальними стали дослідження у лоні постквантової криптографії, тобто криптографії, що представляє алгоритми, які є стійкими до квантового та класичного криптоаналізу. Існує чотири основних напрямків досліджень: криптографія, заснована на геш-функціях; криптографія, заснована на алгебраїчних решітках; криптографія, заснована на факторизації поліномів та криптографія, заснована на завадостійких кодах [4]. У дослідженні ми зосереджуємо увагу саме на останньому напрямку, зважаючи на декілька факторів. По-перше, системи, засновані на кодах, здатні надавати такі переваги, як контроль помилок у каналі. По-друге, висока швидкість криптоперетворення та доведена стійкість до класичного і квантового криптоаналізу відрізняють кодові системи від їх конкурентів [5]. Найпопулярнішими криптосистемами, що базуються на використанні кодування, є схеми Мак-Еліса та Нідеррайтера.

Проаналізувавши їх структуру, переваги та недоліки, ми пропонуємо нову, так звану, гібридну криптосистему, що поєднує принципи зашифрування двох вищезгаданих систем та надає додаткові суттєві переваги, що будуть розглянуті надалі.

2. Дослідження принципів побудови кодових схем

2.1. Криптосистема Мак-Еліса

Криптосистема Мак-Еліса є так званою класичною криптосистемою, що базується на використанні кодів. Вона була запропонована більше 30 років тому і досі вважається стійкою не тільки до класичного, а й до квантового криптоаналізу. Сутність даної схеми можна визначити як маскування швидкого правила декодування за допомогою матричного множення породжуючої матриці алгебраїчного блокового коду на випадкові матриці (що є секретними ключами) [6]. Зловмисник, тобто той, хто має тільки відкритий ключ, повинен використати складний алгоритм неалгебраїчного декодування. Цей алгоритм визначається як NP-повна задача. Уповноважений користувач, який має секретний ключ, знімає дію маскуючих матриць і застосовує швидкий алгебраїчний алгоритм декодування. Далі визначимо алгоритм шифрування за допомогою схеми Мак-Еліса:

1). Зафіксуємо скінчене поле $GF(q)$. G – породжуюча матриця (n,k,d) кода над $GF(q)$, X – невироджена $k\times k$ матриця з елементами з $GF(q)$, P та D – перестановочна та діагональна $n\times n$ матриці відповідно (для двійкових кодів матриця D не використовується).

2). Сформуємо матрицю $G_X = X\cdot G\cdot P\cdot D$. Вона є відкритим ключем схеми Мак-Еліса. При цьому матриці X, P та D є секретним ключем.

3). Криптограма формується згідно з наступним правилом:

$$c_X^* = I\cdot G_X + e, \tag{1}$$

де e – це вектор помилок, вага Хемінга якого відповідає вимозі:

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

I – k-розрядний інформаційний вектор над полем $GF(q)$.

Виконавши згадані кроки, отримаємо кодове слово $c_X = I \cdot G_X$, що викривлене вектором помилок. У цьому випадку вектор e слід розглядати як одноразовий секретний ключ. Його вага визначає складність декодування спотвореного кодового слова (криптограми) [7].

Алгоритм розшифрування можна описати такими кроками:

1) Побудування вектору $\overline{c}^{*} = c_X^{*} \cdot D^{-1} \cdot P^{-1}$. Матриця $\Lambda = D^{-1} \cdot P^{-1}$ зберігає відстань і вагу за Хемінгом. Це означає, що побудований вектор є спотвореним не більше, ніж у $w_h(e)$ розрядів. Для двійкових кодів цей крок трохи відрізняється, оскільки у такому випадку ми не використовуємо матрицю D і побудова вектора зводиться до множення $\overline{c}^{*} = c_X^{*} \cdot P^{-1}$.

2) При використанні алгоритму поліноміальної складності декодування вектору $\overline{c}^{*} = I' \cdot G + e'$, тобто знаходження I'.

3) Обчислення початкового k-розрядного інформаційного вектора $I = I' X^{-1}$ [6-7].

Отже, розшифрування за схемою Мак-Еліса виконується завдяки зняттю дії маскуючих матриць та використанню алгоритму декодування, що має поліноміальну складність [8].

2.2. Криптосистема Нідеррайтера

Наступним кроком розглянемо особливості функціонування теоретико-кодової схеми Нідеррайтера (Niederreiter). Вона заснована також на перевагах використання маскуючих матриць, як у схемі Мак-Еліса [7 – 9]. Визначимо алгоритм шифрування, що виконується у даній схемі:

1) Зафіксування скінченого поля $GF(q)$. Нехай H – перевірочна матриця алгебраїчного (n,k,d) коду над $GF(q)$ (в оригінальній статті було запропоновано використовувати узагальнені коди Ріда – Соломона).

2) Формування секретного ключа, що містить такі складові: X – невироджена $(n-k)\times(n-k)$ матриця з елементами з $GF(q)$, P – перестановочна $n \times n$ матриця, D – діагональна $n \times n$ матриця (для двійкових кодів ця матриця не використовується).

3) Обчислення відкритиого ключа схеми згідно з правилом

$$H_X = X \cdot H \cdot P \cdot D.$$

4) Формування криптограми здійснюється за рахунок множення вектора e на транспонований відкритий ключ:

$$s_X = e \cdot H_X^T.$$

Криптограма складається з $(n\text{-}k)$ елементів [10] . Вектор e зберігає у собі інформацію, що прагнемо зашифрувати, тобто є інформаційним вектором. Інформаційний вектор додатково перетворюється за допомогою рівноважного кодування. Отримавши повідомлення, легітимний користувач, аналогічно з випадком криптосистеми Мак-Еліса, знімає дію маскуючих матриць і, використовуючи алгоритм швидкого декодування, отримує вектор e, що після рівноважного декодування представляє собою початково передану інформацію [11].

2.3. Нова гібридна криптосистема

Зважаючи на доведену стійкість розглянутих криптосистем (докладніше вона розглянута у наступному розділі), ми пропонуємо нову гібридну криптосистему, яка має ті ж переваги, що і її попередники, та навіть покращує їх показники. В основі пропонованої системи лежить поєднання принципів кодування інформації згідно із схемою Мак-Еліса та Нідеррайтера.

Секретними ключами гібридної схеми аналогічно першим двум схемам є матриця X (розмір $k \times k$ елементів), матриця P (розмір $n \times n$ елементів) та, у випадку недвійкового кодування, матриця D (розмір $n \times n$) [7, 11].

Відкритий ключ схеми – матриця $G_X = X \cdot G \cdot P \cdot D$, де G – породжуюча $k \times n$ матриця. З метою зашифрування інформаційний вектор розбивається на дві складові (I_1 та I_2). Після цього здійснюється формування криптограми:

$$c_X^* = I_1 \cdot G_X + e .$$

При цьому перша складова інформації множиться на відкритий ключ $c_X = I_1 \cdot G_X$, як і у перетворенні згідно із схемою Мак-Еліса. Друга інформаційна складова I_2 перетворюється відповідно до схеми Нідеррайтера, а саме I_2 довжини m трансформується у закодований інформаційний вектор e довжиною n елементів (наприклад, за допомогою рівноважного кодування). Для утвореного вектору повинні виконуватися умови [7]:

$$w_h(e) \le t = \left\lfloor \frac{d-1}{2} \right\rfloor m = \left\lfloor \log_q \left(\sum_{i=0}^{t} (q-1)^i \frac{n!}{i!(n-i)!} \right) \right\rfloor$$

З метою забезпечення найбільшої стійкості рекомендується максимізувати вагу Хеммінга вектора e, оскільки тоді перебор всіх можливих значень цього вектору значно ускладнюється. Розшифрування у гібридній схемі відбувається, як і у схемі Мак-Еліса, що було описано у попередньому підрозділі, але з тією відмінністю, що інформація вилучається не тільки з вектору I, а ще й з вектору помилок e [12]. Цей факт дозволяє значно підвищити відносну швидкість передачі інформації, що докладішне буде розглянуто надалі .

3. Порівняльний аналіз криптосистем

Порівнюючи ефективність криптосистем, скористаємося такими чинниками, як відносна швидкість передачі інформаціїї, стійкість до класичного та квантового криптоаналізу, об'єм ключових даних, що потребує криптосистема, та довжина шифртексту відповідно до кожного варіанту.

3.1. Відносна швидкість передачі інформації

Спочатку розглянемо відносну швидкість передачі інформації. Вона характеризує ступінь використання в коді з виправленням помилок інформаційних можливостей двійкових послідовностей довжини n.

Оцінка відносної швидкості для схеми Мак-Еліса є найпростішою, оскільки відомо, що сформована за цим алгоритмом криптограма має довжину n, тоді як початковий інформаційний вектор має довжину k біт. Отже, відносна швидкість передачі у цьому випадку [13, 14] :

$$R = \frac{\log_2 2^k}{n} = \frac{k}{n}.$$

Відносна швидкість передачі інформації для схеми Нідеррайтера докладно розглянута у [7]. Згідно з цими даними вона становить

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

З використанням гібридної криптосистеми шифртекст, що формується, має довжину n, тоді як інформація кодується з поєднанням принципів Мак-Еліса та Нідеррайтера, розбиваю-

чи на дві складові I_1 та I_2, причому I_1 має довжину k біт, а I_2 перетворюється завдяки рівноважному кодуванню, тому максимально можлива прихована кількість біт визначається, як у схемі Нідеррайтера $\log_q\left(\sum_{i=0}^{t}(q-1)^i\frac{n!}{i!(n-i)!}\right)=n-k$. Тобто оцінку відносної швидкості передачі для гібридної криптосистеми можна зазначити як

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

З наведених даних одразу можна зробити висновок, що з точки зору величини відносної швидкості гібридна система значно випереджає своїх попередників, за рахунок використання у кодуванні двох складових [7].

3.2. Стійкість до класичного криптоаналізу

Варто зазначити, що дослідниками було доведено, що стійкості криптосистем Мак-Еліса та Нідеррайтера еквівалентні. Продемонструємо це. Нехай відомо: синдром $c=e\cdot H_x$, тоді можна обчислити вектор $b=a\cdot E+e$, причому $c=b\cdot H_x$. У такому випадку b розглядають як шифртекст у системі Мак-Еліса. За умови, що знайдена атака зі складністю W для системи Мак-Еліса та відомо алгоритм для обчислення вектору a, який є секретною інформацією в схемі Мак-Еліса, вектор e, який містить секретну інформацію, у системі Нідеррайтера можна представити у вигляді $e=a\cdot E+b$, тобто складність визначення вектору e збігається зі складністю визначення вектора a. У протилежному випадку, коли існує ефективна атака на схемі Нідеррайтера, можливо, використовуючи у якості шифртексту вектор $(a\cdot E+e)\cdot \mathrm{D}^T=e\cdot \mathrm{D}^T$, обчислити вектори e та a. Варто зауважити, що з описаної вище точки зору слідує еквівалентність оцінок стійкості криптосистем Мак-Еліса та Нідеррайтера і гібридної криптосистеми [15].

Безпечність усіх трьох криптосистем заснована на нездатності вирішити такі фундаментальні проблеми теорії кодування, як загальна проблема декодування лінійних кодів та проблема знаходження кодового слова с заданною вагою.

Якщо розглядати можливість реалізації атак, варто згадати, що, незважаючи на те, що криптосистема Мак-Еліса, заснована на кодах Гоппа, досі вважається стійкою, як зазначав Роберт Мак-Еліс в своїй оригінальній статті, існує два основних шляхи, якими зловмисник може атакувати криптосистему [6]:

1. Зловмисник може спробувати відновити секретний ключ з відкритого ключа, а потім розшифрувати повідомлення.

2. Зловмисник може безпосередньо декодувати повідомлення, не вивчаючи структуру коду Гоппа.

Реалізацією подібного типу атак займається велика кількість дослідників, але досі не винайдено оптимальний ефективний варіант.

Також оцінку стійкості кожної з криптосистем до атак можна здійснити за допомогою визначення мінімальної кількості множин, що покривають усі помилки (кровельні множини). Їх кількість обчислюється згідно з формулою

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

Причому $C_n^t = \frac{n!}{t!(n-t)!}$ представляє загальну кількість комбінацій помилок, а $C_{n-k}^t = \frac{(n-k)!}{t!(n-k-t)!}$ – максимальна кількість комбінацій помилок, які можуть бути покриті даною множиною [7]. Оцінка з цієї точки зору є певним чином заниженою, оскільки не враховується обчислювальна складність формування слів-кандидатів, що обчислюється відповідно до обраної множини.

3.3. Стійкість до квантового криптоаналізу

Нині існують різноманітні квантові алгоритми, серед яких найпопулярнішими є квантовий алгоритм Шора, квантовий алгоритм Гровера пошуку елемента в несортованій базі, квантові алгоритми криптоаналізу для перетворень в фактор-кільці та інші [16].

У ряді джерел зазначається, що квантовий алгоритм Шора не є ефективним для зламу безпеки криптосистеми Мак-Еліса. Найефективнішим квантовим алгоритмом по відношенню до кодової схеми Мак-Еліса є алгоритм Гровера. Він правильно розглядається не як через «базу даних», а як пошук коренів функції. З цієї точки зору варто розглянути застосування алгоритму Гровера в межах атаки декодування множини [17].

Алгоритм Гровера є загальним конструктивним перетворенням з умовних ланцюгів у квантові ланцюги знаходження коренів. Докладна реалізація квантової атаки декодування множини даних продемонстрована у [18, 19].

Варто відзначити, що базова атака декодування множини даних виконує пошук кореня функції випадковим чином. Пошук використовує приблизно в середньому $\frac{C_n^k}{0,29C_{n-t}^k} \approx c^{n/\lg n}$ проходів функції. Із застосуванням алгоритму Гровера ця оцінка трансформується у

$$\sqrt{\frac{C_n^k}{0,29C_{n-t}^k}} \approx c^{(1/2)n/\lg n}.$$

Кожна ітерація є квантовою функцією, що виконується за $O(n^3)$ кубітових операцій. Кожна ітерація також потребує часу $n^{O(1)}$ на квантовому комп'ютері розміру $n^{O(1)}$. Загальний час для знаходження S дорівнює $c^{(1/2+O(1))n/\lg n}$ на квантовому комп'ютері розміру $n^{O(1)}$. Знайшовши S, можна обчислити *m* та *e*, застосовуючи незначні додаткові зусилля [20].

Продемонструємо розглянуту інформацію щодо відносної швидкості передачі інформації та стійкості до обох видів криптоаналізу на прикладах, що наведені у табл. 1.

Таблиця 1

Залежність стійкості та відносної швидкості від виправляючої здатності коду

Параметри коду	Відносна швидкість передачі			Стійкість до класичного криптоаналізу, біт			Стійкість до квантового криптоаналізу, біт		
	М.	Н.	Г.	М.	Н.	Г.	М.	Н.	Г.
(2048,1828,41)	0,89	0,71	0,96	65,5			32	47,9	14,2
(2048, 1608,81)	0,78	0,63	0,92	90			44	49	26,7
(2048,1388, 121)	0,67	0,58	0,86	100			49	49	36
(2048,1168, 161)	0,57	0,54	0,8	100			48,7	48,1	42
(2048,948, 201)	0,46	0,51	0,74	92			44	47	46
(2048,728, 241)	0,35	0,49	0,67	78,9			38	46	49

Слід зауважити, що у таблиці використані такі позначення: М-криптосистема Мак-Еліса; Н-криптосистема Нідеррайтера; Г-гібридна криптосистема. Дані, що представлені у таблиці, крім стійкості до класичного криптоаналізу, оскільки для усіх трьох схем вона еквівалентна, задля кращого візуального сприйняття можна представити за допомогою графічного зображення (рис. 1, 2).

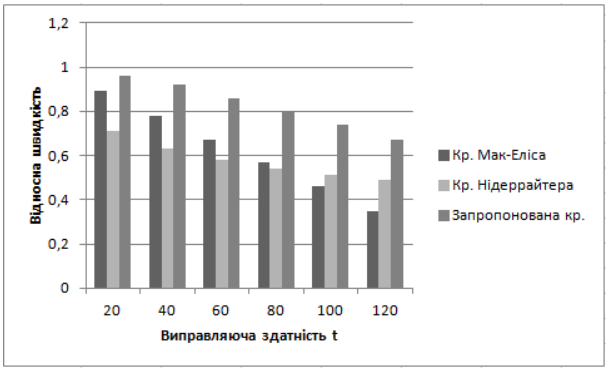


Рис. 1. Порівняння відносної швидкості передачі криптосистем

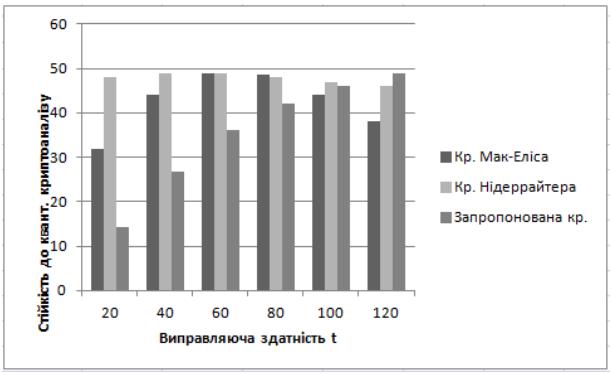


Рис. 2. Порівняння стійкості криптосистем до квантового криптоаналізу

Аналізуючи розглянуті дані, можна зробити висновок, що при однакових параметрах коду усі три криптосистеми забезпечують один і той же рівень стійкості до класичного криптоаналізу. Однак результати стійкості щодо квантового криптоаналізу різняться: стійкість до квантового криптоаналізу криптосистеми Мак-Еліса починає спадати після зниження відносної швидкості коду за межі 0,66. Очевидно, що збільшення виправляючої здатності гібридної криптосистеми і в той же час зі зменшенням відносної швидкості передачі, стійкість до квантвого криптоаналізу також зростає, але подальші дослідження продемонстрували, що ця тенденція зміниться за тієї ж умови, що впливає на стійкість схеми Мак-Еліса, а саме зниження відносної швидкості передачі інформації за межі 0,66.

3.4. Порівняння обсягу ключових даних та довжин шифртексту

Наступним кроком порівняємо об’єм ключових даних та довжини шифртексту, що формується відповідно до кожної з трьох криптосистем.

Оскільки у роботі розглядається двійковий випадок використання криптосистем, тому при оцінці обсягу ключових параметрів не буде враховано матрицю D, а також розгляд ведеться без врахування секретного поліному коду Гоппа.

Ключові параметри та спосіб формування шифртексту збігаються у випадку гібридної схеми та схеми Мак-Еліса, тому їх оцінки можна вважати еквівалентними. Секретний ключ цих схем складається з матриць X та P. Матриця X має розміри $k \times k$ елементів, а обсяг, який займає матриця P, визначається вектором перестановки з n елементів. Розмір відкритого ключа обох схем визначається матрицею $G_X = X \cdot G \cdot P$, розміром $k \times n$ елементів. Довжина сформованого шифртексту визначається згідно з довжиною криптограми $c_X^* = I_1 \cdot G_X + e$, що складається з n елементів. Отже, для криптосистеми Мак-Еліса та

гібридної криптосистеми довжина секретного ключа $l_{с.к.} = k \cdot k + n$, відкритого ключа $l_{в.к.} = k \cdot n$, а сформованого шифртексту $l_{ш.т} = n$. Звідси можна зазначити недолік криптосистем, що полягає у збільшеній довжині шифртексту відносно початкового інформаційного вектора. Відомо, що для криптосистеми Нідеррайтера секретним ключем є також матриці X та P. Розмір матриці P визначається, як і у попередньому випадку, але матриця X відрізняється і має розміри $(n-k)\times(n-k)$ елементів. Відкритим ключем цієї схеми є матриця $H_X = X \cdot H \cdot P$, що складається з $n\times(n-k)$ елементів. Довжина синдрому $s_X = e \cdot H_X^T$ при цьому дорівнює $(n-k)$.

Отже, для криптосистеми Нідеррайтера справедливі такі оцінки: обсяги секретного ключа $l_{с.к.} = (n-k)\cdot(n-k)+n$, обсяги відкритого ключа $l_{в.к.} = n\cdot(n-k)$, довжина шифр тексту $l_{ш.т} = n-k$.

Проаналізувавши наведену інформацію, можна зробити висновок, що обсяги секретного ключа у схемі Мак-Еліса та гібридній різняться з обсягами секретного ключа у схемі Нідеррайтера на $n^2 - 2\cdot n\cdot k$, різниця між сформованим шифртекстом дорівнює *k* елементів, але в той же час розміри відкритого ключа у схемі Нідеррайтера більші на n^2 елементів

Продемонструємо цей факт на прикладах, що відображено у табл. 2. Для розгляду різних рівнів безпеки було обрано параметри коду, що найчастіше зустрічаються у науковій літературі. Для більш наглядного розуміння представимо наведені у таблиці дані за допомогою гістограм (рис. 3 – 4).

Таблиця 2

Порівняння показників ефективності криптосистем

Криптосистема Мак-Еліса					
Параметри коду	Довжина ключів,біт	Довжина шифр тексту, біт	Відносна швидкість передачі	Стійкість до класичного криптоаналізу, біт	Стійкість до квантового криптоаналізу, біт
(1024,524,101)	812176	1024	0,51	54	25,8
(2048,1751,55)	6654097	2048	0,85	77	37,6
(4096,2584,253)	27754896	4096	0,88	128	62,6
(8192,6957,191)	105399785	8192	0,85	263	130
(16384,10322,867)	275675716	16384	0,63	636	310
Криптосистема Нідеррайтера					
Параметри коду	Довжина ключів, біт	Довжина шифр тексту, біт	Відносна швидкість передачі	Стійкість до класичного криптоаналізу, біт	Стійкість до квантового криптоаналізу, біт
(1024,524,101)	763024	500	0,57	54	26,7
(2048,1751,55)	698513	297	0,68	77	49
(4096,3604,83)	2261392	492	0,87	128	90,2
(8192,6957,191)	11650537	1235	0,84	263	166
(16384,10322,867)	136084036	6062	0,47	636	286
Гібридна криптосистема					
Параметри коду	Довжина ключів, біт	Довжина шифр тексту, біт	Відносна швидкість передачі	Стійкість до класичного криптоаналізу, біт	Стійкість до квантового криптоаналізу, біт
(1024,524,101)	812176	1024	0,79	54	24,2
(2048,1751,55)	6654097	1945	0,95	77	18,9
(4096,3604,83)	27754896	3892	0,95	128	31,8
(8192,6957,191)	105399785	7618	0,93	263	77
(16384,10322,867)	275675716	13107	0,8	636	267

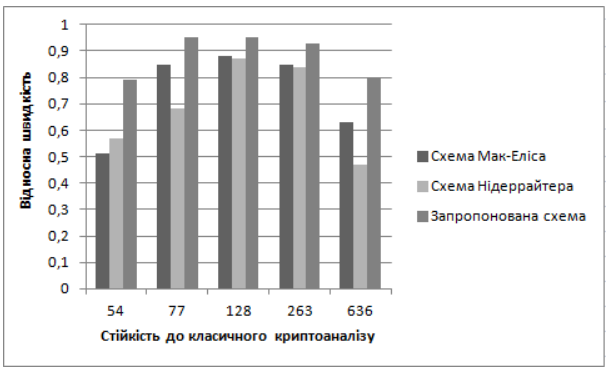


Рис. 3. Залежність між відносною швидкістю та стійкістю криптосистем

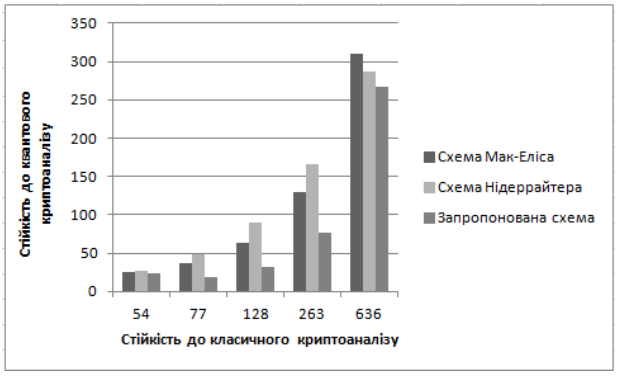


Рис. 4. Залежність між величиною стійкості до класичного та квантового криптоаналізу

Проаналізувавши наведені дані, можна зробити висновок, що для забезпечення аналогічного рівня стійкості до квантового криптоаналізу, порівняно зі звичайним криптоаналізом (наприклад, порівнюючи показники для параметру коду n=16384 n=8192), необхідно збільшити обсяги ключових даних більше, ніж у три рази. Також варто відзначити, що стійкість криптосистем до квантового криптоаналізу безпосередньо залежить від показників їх відносної швидкості.

Через перевагу в останньому показнику гібридна криптосистема показала продемонстрували результати у стійкості до квантового криптоаналізу, але зменшення стійкості не є критичним, порівняно з іншими схемами. На жаль, однозначно визначити, яка з трьох криптосистем забезпечує найкращий захист, неможливо, оскільки дані для різних наборів параметрів кодів будуть різнитися.

Однак, очевидною перевагою гібридної криптосистеми, про яку варто нагади, в контексті розгляду ефективності криптосистем, є те, що вона дозволяє шифрувати більший об'єм інформації з використанням того ж об'єму ключів, при цьому забезпечуючи належний рівень захисту.

Висновки

Проаналізувавши весь спектр інформації, що стосується кодових криптосистем, можна зробити ряд висновків.

По-перше, дослідження виявили, що використання алгебраїчних кодів у контексті постквантової криптографії є дуже перспективним напрямком, оскільки вони дозволяють забезпечити високу швидкість криптоперетворення, контроль помилок, що можуть відбутися у каналі зв'язку, а також стійкість до класичного та квантового криптоаналізу. У зв'язку з наявністю згаданих переваг у використанні кодів з метою побудування алгоритмів постквантової криптографії було запровоновано новий, так званий гібридний алгоритм, що поєднує принципи зашифрування згідно з криптосистемами Мак-Еліса та Нідеррайтера.

У свою чергу, подальший порівняльний аналіз всіх трьох криптосистем виявив, що використовуючи запропоновану схему, ключові дані займають ті ж обсяги, що і ключові дані

криптосистеми Мак-Еліса, і формуються за аналогічний час, при цьому дозволяючи забезпечити більшу відносну швидкість передачі і аналогічну стійкість до криптоаналізу. Единим недоліком є збільшений час розшифрування за рахунок додання вилучення інформації, як у схемі Нідеррайтера, але збільшення цього показника не є критичним.

Незважаючи на продемонстровані переваги для усіх криптосистем залишається відкритим питання зменшення обсяги використовуваних ключових даних, які, в умовах використання квантових комп'ютерів для забезпечення стійкості, ще потрібно буде збільшити в рази. Даний напрямок залишається актуальним вектором дослідження в лоні сучасної криптографії.

Список літератури:

1. Menezes A.J., P.C. van Oorschot, Vanstone S.A. // Handbook of Applied Cryptography. CRC Press, 1997. – 794 p.

2. Ferguson N. and Schneier B. Practical Cryptography. – John Wiley & Sons, 2003. – 432 p.

3. Moody D. Post-Quntum Cryptography: NIST's Plan for the Future // The Seventh International Conference on Post-Quntum Cryptography, Japan, 2016. [On-line]. Available: https://pqcrypto2016.jp

4. Koblitz N. and Menezes A.J. A Riddle Wrapped in an Enigma. [On-line] Available: https://eprint.iacr.org/2015/1018.pdf

5. MacWilliams F. J. and Sloane N. J. A. The theory of error-correcting codes. North-Holland, Amsterdam, New York, Oxford, 1977. – 762 p.

6. McEliece R. J. A public-key cryptosystem based on algebraic coding theory // DSN Progress Report 42-44, Jet Propulsion Lab., January-February, 1978. – P. 114-116.

7. Kuznetsov A., Svatovskij I., Kiyan N. and Pushkar'ov A. Code-based public-key cryptosystems for the post-quantum period. 2017 // 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T). – Kharkov, 2017. – P. 125-130.

8. Finiasz M. and Sendrier N. Security bounds for the design of codebased cryptosystems // M. Matsui, ed., Advances in Cryptology, ASIACRYPT. – 2009. – Vol. 5912 of Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2009. – P. 88 -105.

9. Courtois N., Finiasz M. and Sendrier N. How to achieve a McEliece-based digital signature scheme // Advances in Cryptology – ASIACRYPT. – 2001. – Vol. 2248. – P. 157–174.

10. Niederreiter H. Knapsack-type cryptosystems and algebraic coding theory // Problem Control and Inform Theory. – 1986. – Vol. 15. – P. 19-34.

11. Kuznetsov A., Pushkar'ov A., Kiyan N. and Kuznetsova T. Code-based electronic digital signature // IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, 2018. – P. 331-336.

12. Kuznetsov A., Lutsenko M., Kiian N., Makushenko T. and Kuznetsova T. Code-based key encapsulation mechanisms for post-quantum standardization // IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT). – Kyiv, Ukraine, 2018. – P. 276-281.

13. Kuznetsov A., Kiian A., Lutsenko M., Chepurko I. and Kavun S. Code-based cryptosystems from NIST PQC // IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT). – Kyiv, Ukraine, 2018. – P. 282-287.

14. Sidelnikov V. M. and Shestakov S. O. On insecurity of cryptosystems based on generalized Reed-Solomon codes // Discrete Mathematics and Applications. – 1992. – p. 439-444.

15. Yuan Xing Li, R. H. Deng and Xin Mei Wang. On the equivalence of McEliece's and Niederreiter's public-key cryptosystems // IEEE Transactions on Information Theory. – Jan. 1994. – Vol. 40, no. 1. – P. 271-273.

16. Bernstein D., Buchmann J. and Dahmen E. Post-Quantum Cryptography. – Springer-Verlag, Berlin-Heidleberg, 2009. – 245 p.

17. Proos J. and Zalka C. 2003. Shor's discrete logarithm quantum algorithm for elliptic curves // Quantum Info. Comput. – 3, 4 (July 2003). – P. 317-344.

18. Bernstein D.J., Lange T., Peters C. Attacking and Defending the McEliece Cryptosystem // Buchmann J., Ding J. (eds) Post-Quantum Cryptography. PQCrypto 2008. Lecture Notes in Computer Science. – Vol. 5299. Springer, Berlin, Heidelberg. – pp 31-46.

19. 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.

20. Sendrier N. Decoding one out of many // Yang, B.Y., ed.: PQCrypto 2011. – Vol. 7071 of LNCS. Springer, 2011. – P. 51-67.

Харківський національний
університет імені В.Н.Каразіна;
АТ «Інститут інформаційних технологій», Харків

Надійшла до редколегії 05.11.2018

УДК 621.394.147

А.А. КУЗНЕЦОВ, д-р техн. наук, Е.П. КОЛОВАНОВА, канд. техн. наук,
Д.И. ПРОКОПОВИЧ-ТКАЧЕНКО, канд. техн. наук, Т.Ю. КУЗНЕЦОВА

АНАЛИЗ И ИССЛЕДОВАНИЕ СВОЙСТВ АЛГЕБРОГЕОМЕТРИЧЕСКИХ КОДОВ

Введение

Алгеброгеометричекие коды как линейные системы на алгебраических кривых впервые были предложены В.Д. Гоппой [1, 2]. Асимптотические свойства таких кодов исследованы в [3]. Коды, построенные по кривым с большим числом точек по сравнению с родом, лежат выше границы Варшамова – Гилберта. Интерес представляют схемы практического применения этих кодов для помехоустойчивой передачи дискретных сообщений, алгоритмы их построения и декодирования, получаемый энергетический выигрыш от кодирования.

Цель данной работы – исследование алгоритмов построения и декодирования алгеброгеометрических кодов, оценка достигаемой энергетической эффективности.

1. Определение и конструктивные свойства алгеброгеометрических кодов

Зафиксируем конечное поле $GF(q)$. Пусть X – гладкая проективная алгебраическая кривая в проективном пространстве P^n, т.е. совокупность решений $p_1(x_0, x_1, ..., x_n)$, $p_2(x_0, x_1, ..., x_n)$, …, $p_N(x_0, x_1, ..., x_n)$, $\forall\ p \in P^n$ системы однородных неприводимых алгебраических уравнений степени d с коэффициентами из $GF(q)$.

Пусть $g = g(X)$ – род кривой, причем, согласно [4]:

– если $d < n$, то X – вырожденная кривая;
– если $d = n$, то X – рациональная нормальная кривая рода 0;
– если $n < d < 2n$, то $g \le d - n$;
– если $d = 2n$, то $g \le n + 1$;
– если $d \ge 2n$, то $g \le \frac{m(m-1)}{2}(n-1) + m\varepsilon$, где $m = \left[\frac{d-1}{n-1}\right]$, $\varepsilon = d - 1 - m(n-1)$.

В табл. 1 приведена верхняя оценки рода g кривой X.

Таблица 1

Верхняя оценка рода g кривой X в P^n

d	$g(P^2)$	$g(P^3)$	$g(P^4)$	$g(P^5)$	$g(P^6)$
2	0	-	-	-	-
3	1	0	-	-	-
4	3	1	0	-	-
5	6	2	1	0	-
6	10	4	2	1	0
7	15	6	3	2	1
8	21	9	5	3	2
9	28	12	7	4	3
10	36	16	9	6	4

Пусть $X(GF(q))$ – множество точек кривой X над конечным полем $GF(q)$, $N = \left|X(GF(q))\right|$ – их число. Число N точек кривой X над $GF(q)$ ограничено сверху выражением Хассе – Вейля [1 – 3]:

$$N \le 2\sqrt{q} \cdot g + q + 1.$$

В табл. 2 приведена верхняя оценка числа точек кривой над конечным полем.

Таблица 2

Оценка верхней границы числа точек гладкой проективной кривой

g	d	$N = \lvert X(GF(q)) \rvert$				
		$GF(4)$	$GF(8)$	$GF(16)$	$GF(32)$	$GF(64)$
0	2	5	9	17	33	65
1	3	9	14	25	44	81
2	4	10	18	33	53	97
3	4	17	24	41	66	113
4	5	21	29	49	77	129
5	5		34	57	88	145
6	5		39	65	99	164
7	6		44	73	110	180
8	6		49	81	121	196
9	6		54	89	132	212
10	6		59	97	143	228
11	7		64	105	154	244
12	7		69	113	165	260
13	7			121	176	276
14	7			129	187	292
15	7			137	198	308

Предельные значения числа точек гладких кривых сведены в табл. 3.

Таблица 3

Максимальные значения точек X кривой в P^2 над $GF(q)$

d	$N = \lvert X(GF(q)) \rvert$				
	$GF(4)$	$GF(8)$	$GF(16)$	$GF(32)$	$GF(64)$
3	9	14	25	44	81
4	14	24	34	63	113
5	17	28	65	99	164

Пусть C – класс дивизоров на X степени α. Тогда C задает отображение $\phi: X \to P^m$, набор генераторных функций $y_i = \phi(x_i)$ задает алгеброгеометрический код длины $n \le N$. Кодовые характеристики (n, k, d) связаны соотношением $k + d \ge n - g + 1$ [1, 2]. Если $2g - 2 < \alpha \le n$, код связан характеристиками $(n, \alpha - g + 1, d), d \ge n - \alpha$. Дуальный к нему код также является алгеброгеометрическим с характеристиками $(n, n - \alpha + g - 1, d_\perp), d_\perp \ge \alpha - 2g + 2$.

Для оценки потенциальных возможностей блоковых кодов проводят их сравнение с кодовыми границами. Кодовые границы указывают на наилучшие теоретически возможные линейные блоковые коды и подробно описаны в [5 – 8].

Граница Синлгтона указывает на максимально достижимое кодовое расстояние при заданных параметрах (n, k, d) кода и записывается в виде

$$d \le n - k + 1.$$

Коды, лежащие на границе Синлгтона, называют кодами с максимально достижимым кодовым расстоянием (МДР коды).

Граница Варшамова – Гилберта является нижней кодовой границей, т.е. она гарантирует существование кодов с параметрами (n, k, d), лежащими на этой границе. Обобщение границы Варшамова – Гилберта на недвоичные коды имеет вид

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

или

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

Для (n, k, d) кода рассмотрим параметры: $R = k/n$ – относительная скорость кода как доля информационных символов в передаваемых данных; $\delta = d/n$ – относительное минимальное расстояние кода как доля ошибок в принятом слове, которые может обнаружить код. Устремим $n \to \infty$.

Асимптотическая форма границы Синлгтона примет вид

$$R \leq 1 - \delta.$$

Асимптотическая граница Варшамова – Гилберта примет вид

$$R \leq 1 - H_q(\delta).$$

В [3] приведена асимптотическая граница алгеброгеометрических кодов

$$R \leq 1 - \delta - \left(\sqrt{q} - 1\right)^{-1}.$$

На рис. 1 представлены асимптотические границы: 1 – граница Синлгтона; 2 – граница Варшамова – Гилберта; 3 – граница алгеброгеометрических кодов.

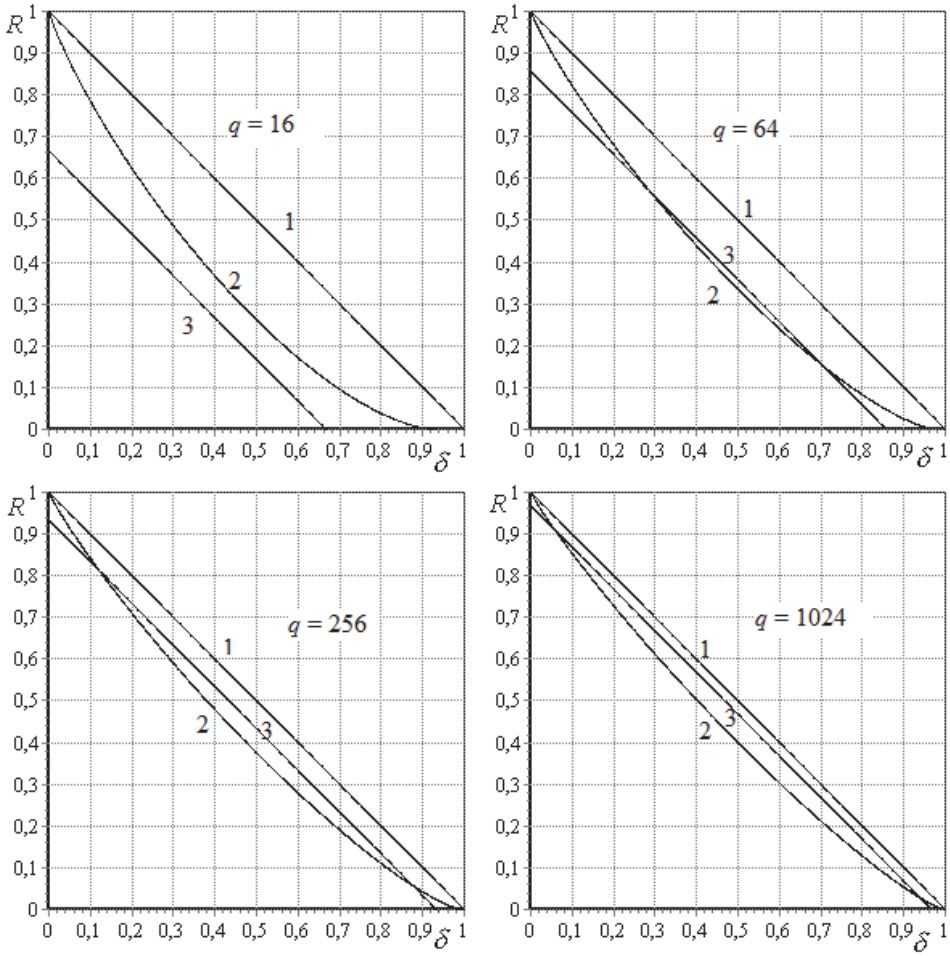


Рис. 1. Асимптотические свойства алгеброгеометрических кодов

Приведенные зависимости свидетельствуют о том, что при возрастании мощности q алфавита кодовых символов асимптотические свойства алгеброгеометрических кодов улучшаются. Очевидно, что при большом q эти коды лежат выше границы Варшамова – Гилберта, что свидетельствует о высоких потенциальных характеристиках.

Конструктивные кодовые характеристики алгеброгеометрических кодов по кривым рода $g=0$, $g=1$, $g=3$, $g=6$ над $GF(4)$ сведены в табл. 4. Соответствующие конструктивные оценки кодовых параметров по кривым различного рода $g=0$, $g=1$, $g=3$, $g=6$ над $GF(8)$, $GF(16)$, $GF(32)$, $GF(64)$ сведены в табл. 5 – 8.

2. Кодирование и декодирование алгеброгеометрическими кодами

Рассмотрим операции кодирования алгеброгеометрическими кодами для общего случая – для кривых, заданных в проективном пространстве P^u совокупностью решений *u – 1* однородных неприводимых алгебраических уравнений от *n* неизвестных, исследуем алгоритмы формирования кодовых слов в систематическом и несистематическом виде.

2.1. Кодирование в несистематическом виде через порождающую матрицу

Зафиксируем гладкую проективную алгебраическую кривую *X* в проективном пространстве P^u над полем $GF(q)$ как это совокупность решений *u – 1* однородных неприводимых алгебраических уравнений от n переменных с коэффициентами из $GF(q)$:

$$\begin{cases} f_1\left(x_0, x_1, ..., x_{u-1}\right) = 0 \\ f_2\left(x_0, x_1, ..., x_{u-1}\right) = 0 \\ ... \\ f_{u-1}\left(x_0, x_1, ..., x_{u-1}\right) = 0 \end{cases}. \tag{1}$$

Пусть $p_0\left(x_0, x_1, ..., x_{u-1}\right)$, $p_1\left(x_0, x_1, ..., x_{u-1}\right)$, …, $p_{N-1}\left(x_0, x_1, ..., x_{u-1}\right) - N$ совместных решений системы уравнений (1) – точек кривой *X*.

Зафиксируем дивизор D кривой X и множество рациональных функций, ассоциированных с дивизором D, т.е. множество, состоящее из нуля и функций $F \neq 0$, для которых $(F) + D \geq 0$. Это эквивалентно набору генераторных функций

$$F_0\left(x_0, x_1, ..., x_{u-1}\right),\ F_1\left(x_0, x_1, ..., x_{u-1}\right),\ F_2\left(x_0, x_1, ..., x_{u-1}\right),\ \ldots,\ F_{w-1}\left(x_0, x_1, ..., x_{u-1}\right),$$

где $F_0, F_1, ..., F_w$ – формы одинаковой степени и $F_0(x_0, x_1, ..., x_{u-1}) \neq 0$.

Иначе говоря,

$$\phi(x) = \left(F_0(x), F_1(x), ..., F_{w-1}(x)\right),$$

как точка в P^w.

Пусть α – степень класса дивизоров, $\alpha > g - 1$, тогда отображение $\phi: X \to P^w$ задает порождающую матрицу

$$G = \begin{pmatrix} F_0\left(p_0\left(x_0, x_1, ..., x_{u-1}\right)\right) & F_0\left(p_1\left(x_0, x_1, ..., x_{u-1}\right)\right) & ... & F_0\left(p_{n-1}\left(x_0, x_1, ..., x_{u-1}\right)\right) \\ F_1\left(p_0\left(x_0, x_1, ..., x_{u-1}\right)\right) & F_1\left(p_1\left(x_0, x_1, ..., x_{u-1}\right)\right) & ... & F_1\left(p_{n-1}\left(x_0, x_1, ..., x_{u-1}\right)\right) \\ ... & ... & ... & ... \\ F_{k-1}\left(p_0\left(x_0, x_1, ..., x_{u-1}\right)\right) & F_{k-1}\left(p_1\left(x_0, x_1, ..., x_{u-1}\right)\right) & ... & F_{k-1}\left(p_{n-1}\left(x_0, x_1, ..., x_{u-1}\right)\right) \end{pmatrix} \tag{2}$$

алгеброгеометрического кода, с конструктивными характеристиками $(n \leq N, k \geq \alpha - g + 1,\ d \geq n - \alpha)$.

Таблица 4

Конструктивные кодовые характеристики алгеброгеометрических кодов над $GF(4)$

$\deg f$	$\deg X = 2,\ g = 0$			$\deg X = 3,\ g = 1$			$\deg X = 4,\ g = 3$			$\deg X = 5,\ g = 6$		
	a	n,k,d	n,k,d	a	n,k,d	n,k,d	a	n,k,d	n,k,d	a	n,k,d	n,k,d
1	2	**5, 3, 3**	5, 2, 4	3	9, 3, 6	9, 6, 3	4	14, 2, 10	–	5	–	–
2	4			6	**9, 6, 3**	9, 3, 6	8	14, 6, 6	14, 8, 4	10	17, 5, 7	–
3	6			9			12	14, 10, 2	14, 4, 8	15	17, 10, 2	17, 7, 5

Таблица 5

Конструктивные кодовые характеристики алгеброгеометрических кодов над $GF(8)$

$\deg f$	$\deg X = 2,\ g = 0$			$\deg X = 3,\ g = 1$			$\deg X = 4,\ g = 3$			$\deg X = 5,\ g = 6$		
	a	n,k,d	n,k,d	a	n,k,d	n,k,d	a	n,k,d	n,k,d	a	n,k,d	n,k,d
1	2	9, 3, 7	9, 6, 4	3	14, 3, 11	14, 11, 3	4	24, 2, 20	–	5	–	–
2	4	9, 5, 5	9, 4, 6	6	14, 6, 8	14, 8, 6	8	24, 6, 16	24, 18, 4	10	28, 5, 18	–
3	6	**9, 7, 3**	9, 2, 8	9	**14, 9, 5**	14, 5, 9	12	24, 10, 12	**24, 14, 8**	15	28, 10, 13	28, 18, 5
4	8			12	14, 12, 2	14, 2, 12	16	24, 14, 8	24, 10, 12	20	28, 15, 8	28, 13, 10
5	10			15			20	24, 18, 4	24, 6, 16	25	28, 20, 3	28, 8, 15

Таблица 6

Конструктивные кодовые характеристики алгеброгеометрических кодов над $GF(16)$

$\deg f$	$\deg X = 2,\ g = 0$			$\deg X = 3,\ g = 1$			$\deg X = 4,\ g = 3$			$\deg X = 5,\ g = 6$		
	a	n,k,d	n,k,d	a	n,k,d	n,k,d	a	n,k,d	n,k,d	a	n,k,d	n,k,d
1	2	17, 3, 15	17, 14, 4	3	25, 3, 22	25, 22, 3	4	34, 2, 30	–	5	–	–
2	4	17, 5, 13	17, 12, 6	6	25, 6, 19	25, 19, 6	8	34, 6, 26	34, 28, 4	10	65, 5, 55	–
3	6	17, 7, 11	17, 10, 8	9	25, 9, 16	**25, 16, 9**	12	34, 10, 22	34, 24, 8	15	65, 10, 50	65, 55, 5
4	8	17, 9, 9	17, 8, 10	12	25, 12, 13	25, 13, 12	16	34, 14, 18	**34, 20, 12**	20	65, 15, 45	65, 50, 10
5	10	**17, 11, 7**	17, 6, 12	15	25, 15, 10	25, 10, 15	20	34, 18, 14	34, 16, 16	25	65, 20, 40	**65, 45, 15**
6	12	17, 13, 5	17, 4, 14	18	25, 18, 7	25, 7, 18	24	34, 22, 10	34, 12, 20	30	65, 25, 35	65, 40, 20
7	14	17, 15, 3	17, 2, 16	21	25, 21, 4	25, 4, 21	28	34, 26, 6	34, 8, 24	35	65, 30, 30	65, 35, 25
8	16			24			32	34, 30, 2	34, 4, 28	40	65, 35, 25	65, 30, 30
9	18			27			36			45	65, 40, 20	65, 25, 35
10	20			30			40			50	65, 45, 15	65, 20, 40
11	22			33			44			55	65, 50, 10	65, 15, 45

Таблица 7

Конструктивные кодовые характеристики алгеброгеометрических кодов над $GF(32)$

deg$f$	$\deg X = 2,\ g = 0$			$\deg X = 3,\ g = 1$			$\deg X = 4,\ g = 3$			$\deg X = 5,\ g = 6$		
	a	n,k,d	n,k,d	a	n,k,d	n,k,d	a	n,k,d	n,k,d	a	n,k,d	n,k,d
1	2	33, 3, 31	33, 30, 4	3	44, 3, 41	44, 41, 3	4	63, 2, 59	–	5	–	–
2	4	33, 5, 29	33, 28, 6	6	44, 6, 38	44, 38, 6	8	63, 6, 55	63, 57, 4	10	99, 5, 89	–
3	6	33, 7, 27	33, 26, 8	9	44, 9, 35	44, 35, 9	12	63, 10, 51	63, 53, 8	15	99, 10, 84	99, 89, 5
4	8	33, 9, 25	33, 24, 10	12	44, 12, 32	44, 32, 12	16	63, 14, 47	63, 49, 12	20	99, 15, 79	99, 84, 10
5	10	33, 11, 23	33, 22, 12	15	44, 15, 29	**44, 29, 15**	20	63, 18, 43	63, 45, 16	25	99, 20, 74	99, 79, 15
6	12	33, 13, 21	33, 20, 14	18	44, 18, 26	44, 26, 18	24	63, 22, 39	63, 41, 20	30	99, 25, 69	99, 74, 20
7	14	33, 15, 19	33, 18, 16	21	44, 21, 23	44, 23, 21	28	63, 26, 35	63, 37, 24	35	99, 30, 64	99, 69, 25
8	16	33, 17, 17	33, 16, 18	24	44, 24, 20	44, 20, 24	32	63, 30, 31	63, 33, 28	40	99, 35, 59	99, 64, 30
9	18	33, 19, 15	33, 14, 20	27	44, 27, 17	44, 17, 27	36	63, 34, 27	63, 29, 32	45	99, 40, 54	99, 59, 35
10	20	33, 21, 13	33, 12, 22	30	44, 30, 14	44, 14, 30	40	63, 38, 23	63, 25, 36	50	99, 45, 49	99, 54, 40
11	22	**33, 23, 11**	33, 10, 24	33	44, 33, 11	44, 11, 33	44	**63, 42, 19**	63, 21, 40	55	99, 50, 44	99, 49, 45
12	24	33, 25, 9	33, 8, 26	36	44, 36, 8	44, 8, 36	48	63, 46, 15	63, 17, 44	60	99, 55, 39	99, 44, 50
13	26	33, 27, 7	33, 6, 28	39	44, 39, 5	44, 5, 39	52	63, 50, 11	63, 13, 48	65	99, 60, 34	99, 39, 55
14	28	33, 29, 5	33, 4, 30	42	44, 42, 2	44, 2, 42	56	63, 54, 7	63, 9, 52	70	**99, 65, 29**	99, 34, 60
15	30	33, 31, 3	33, 2, 32	45			60	63, 58, 3	63, 5, 56	75	99, 70, 24	99, 29, 65
16	32			48			64		63, 1, 60	80	99, 75, 19	99, 24, 70
17	34			51			68			85	99, 80, 14	99, 19, 75
18	36			54			72			90	99, 85, 9	99, 14, 80
19	38			57			76			95	99, 90, 4	99, 9, 85
20	40			60			80			100		99, 4, 90

Таблица 8

Конструктивные кодовые характеристики алгеброгеометрических кодов над $GF(64)$

deg$f$	$\deg X = 2,\ g = 0$			$\deg X = 3,\ g = 1$			$\deg X = 4,\ g = 3$			$\deg X = 5,\ g = 6$		
	a	n,k,d	n,k,d	a	n,k,d	n,k,d	a	n,k,d	n,k,d	a	n,k,d	n,k,d
1	2	65, 3, 63	65, 62, 4	3	81, 3, 78	81, 78, 3	4	113, 2, 109	–	5	–	–
2	4	65, 5, 61	65, 60, 6	6	81, 6, 75	81, 75, 6	8	113, 6, 105	113, 107, 4	10	164, 5, 154	–
3	6	65, 7, 59	65, 58, 8	9	81, 9, 72	81, 72, 9	12	113, 10, 101	113, 103, 8	15	164, 10, 149	164, 154, 5
4	8	65, 9, 57	65, 56, 10	12	81, 12, 69	81, 69, 12	16	113, 14, 97	113, 99, 12	20	164, 15, 144	164, 149, 10
5	10	65, 11, 55	65, 54, 12	15	81, 15, 66	81, 66, 15	20	113, 18, 93	113, 95, 16	25	164, 20, 139	164, 144, 15

6	12	65, 13, 53	65, 52, 14	18	81, 18, 63	81, 63, 18	24	113, 22, 89	113, 91, 20	30	164, 25, 134	164, 139, 20
7	14	65, 15, 51	65, 50, 16	21	81, 21, 60	81, 60, 21	28	113, 26, 85	113, 87, 24	35	164, 30, 129	164, 134, 25
8	16	65, 17, 49	65, 48, 18	24	81, 24, 57	81, 57, 24	32	113, 30, 81	113, 83, 28	40	164, 35, 124	164, 129, 30
9	18	65, 19, 47	65, 46, 20	27	81, 27, 54	**81, 54, 27**	36	113, 34, 77	113, 79, 32	45	164, 40, 119	164, 124, 35
10	20	65, 21, 45	65, 44, 22	30	81, 30, 51	81, 51, 30	40	113, 38, 73	113, 75, 36	50	164, 45, 114	164, 119, 40
11	22	65, 23, 43	65, 42, 24	33	81, 33, 48	81, 48, 33	44	113, 42, 69	113, 71, 40	55	164, 50, 109	164, 114, 45
12	24	65, 25, 41	65, 40, 26	36	81, 36, 45	81, 45, 36	48	113, 46, 65	113, 67, 44	60	164, 55, 104	164, 109, 50
13	26	65, 27, 39	65, 38, 28	39	81, 39, 42	81, 42, 39	52	113, 50, 61	113, 63, 48	65	164, 60, 99	164, 104, 55
14	28	65, 29, 37	65, 36, 30	42	81, 42, 39	81, 39, 42	56	113, 54, 57	113, 59, 52	70	164, 65, 94	164, 99, 60
15	30	65, 31, 35	65, 34, 32	45	81, 45, 36	81, 36, 45	60	113, 58, 53	113, 55, 56	75	164, 70, 89	164, 94, 65
16	32	65, 33, 33	65, 32, 34	48	81, 48, 33	81, 33, 48	64	113, 62, 49	113, 51, 60	80	164, 75, 84	164, 89, 70
17	34	65, 35, 31	65, 30, 36	51	81, 51, 30	81, 30, 51	68	113, 66, 45	113, 47, 64	85	164, 80, 79	164, 84, 75
18	36	65, 37, 29	65, 28, 38	54	81, 54, 27	81, 27, 54	72	113, 70, 41	113, 43, 68	90	164, 85, 74	164, 79, 80
19	38	65, 39, 27	65, 26, 40	57	81, 57, 24	81, 24, 57	76	**113, 74, 37**	113, 39, 72	95	164, 90, 69	164, 74, 85
20	40	65, 41, 25	65, 24, 42	60	81, 60, 21	81, 21, 60	80	113, 78, 33	113, 35, 76	100	164, 95, 64	164, 69, 90
21	42	**65, 43, 23**	65, 22, 44	63	81, 63, 18	81, 18, 63	84	113, 82, 29	113, 31, 80	105	164, 100, 59	164, 64, 95
22	44	65, 45, 21	65, 20, 46	66	81, 66, 15	81, 15, 66	88	113, 86, 25	113, 27, 84	110	164, 105, 54	164, 59, 100
23	46	65, 47, 19	65, 18, 48	69	81, 69, 12	81, 12, 69	92	113, 90, 21	113, 23, 88	115	**164, 110, 49**	164, 54, 105
24	48	65, 49, 17	65, 16, 50	72	81, 72, 9	81, 9, 72	96	113, 94, 17	113, 19, 92	120	164, 115, 44	164, 49, 110
25	50	65, 51, 15	65, 14, 52	75	81, 75, 6	81, 6, 75	100	113, 98, 13	113, 15, 96	125	164, 120, 39	164, 44, 115
26	52	65, 53, 13	65, 12, 54	78	81, 78, 3	81, 3, 78	104	113, 102, 9	113, 11, 100	130	164, 125, 34	164, 39, 120
27	54	65, 55, 11	65, 10, 56	81			108	113, 106, 5	113, 7, 104	135	164, 130, 29	164, 34, 125
28	56	65, 57, 9	65, 8, 58	84			112	113, 110, 1	113, 3, 108	140	164, 135, 24	164, 29, 130
29	58	65, 59, 7	65, 6, 60	87			116			145	164, 140, 19	164, 24, 135
30	60	65, 61, 5	65, 4, 62	90			120			150	164, 145, 14	164, 19, 140
31	62	65, 63, 3	65, 2, 64	93			123			155	164, 150, 9	164, 14, 145
32										160	164, 155, 4	164, 9, 150

Алгеброгеометрический код на кривой X над $GF(q)$, построенный через порождающую матрицу G, – это линейный код, все кодовые слова ($c_0, c_1, ..., c_{n-1}$) которого задаются равенством

$$\sum_{i=0}^{k-1} I_i F_i\left(p_j\left(x_0, x_1, ..., x_{u-1}\right)\right) = c_j\ ,\ \ j = 0, ..., n-1\,.$$

Для формирования кодового слова $\left(c_0, c_1, ...c_{n-1}\right)$ алгеброгеометрического кода, заданного через порождающую матрицу, достаточно умножить информационный вектор $\left(I_0, I_1, ...I_{k-1}\right)$ на матрицу (2), т.е. для всех $j = 0, ..., n-1$ выполнить следующее преобразование:

$$c_j = \sum_{i=0}^{k-1} I_i F_i\left(p_j\left(x_0, x_1, ..., x_{u-1}\right)\right). \tag{3}$$

Очевидно, что формирование кодового слова осуществляется итеративной процедурой, позволяющей на каждом шаге работы алгоритма формировать соответствующий кодовый символ.

2.2. Кодирование в систематическом виде через проверочную матрицу

Пусть $\alpha > 2g - 2$, тогда отображение $\phi : X \to P^w$ задает проверочную матрицу

$$H = \begin{pmatrix} F_0\left(p_0\left(x_0, x_1, ..., x_{u-1}\right)\right) & F_0\left(p_1\left(x_0, x_1, ..., x_{u-1}\right)\right) & ... & F_0\left(p_{n-1}\left(x_0, x_1, ..., x_{u-1}\right)\right) \\ F_1\left(p_0\left(x_0, x_1, ..., x_{u-1}\right)\right) & F_1\left(p_1\left(x_0, x_1, ..., x_{u-1}\right)\right) & ... & F_1\left(p_{n-1}\left(x_0, x_1, ..., x_{u-1}\right)\right) \\ ... & ... & ... & ... \\ F_{n-k-1}\left(p_0\left(x_0, x_1, ..., x_{u-1}\right)\right) & F_{n-k-1}\left(p_1\left(x_0, x_1, ..., x_{u-1}\right)\right) & ... & F_{n-k-1}\left(p_{n-1}\left(x_0, x_1, ..., x_{u-1}\right)\right) \end{pmatrix} \tag{4}$$

алгеброгеометрического кода, с конструктивными характеристиками

$$\left(n \le N, k \ge n - \alpha + g - 1,\ d \ge \alpha - 2g + 2\right).$$

Алгеброгеометрический код по кривой X над $GF(q)$, построенный через проверочную матрицу H, – это линейный код, состоящий из всех слов $(c_0, c_1, ..., c_{n-1})$ длины $n \le N$, для которых выполняется равенство $d + g - 1$ уравнений

$$\sum_{i=0}^{n-1} c_i F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right) = 0\ ,\ \ j = 0, ..., w\,. \tag{5}$$

Для формирования кодовых слов заданного таким образом алгеброгеометрического кода на пространственных кривых воспользуемся приемами обращения матриц.

Разобьем кодовое слово $\left(c_0, c_1, ...c_{n-1}\right)$ на множества информационных и проверочных позиций (см. рис. 2).

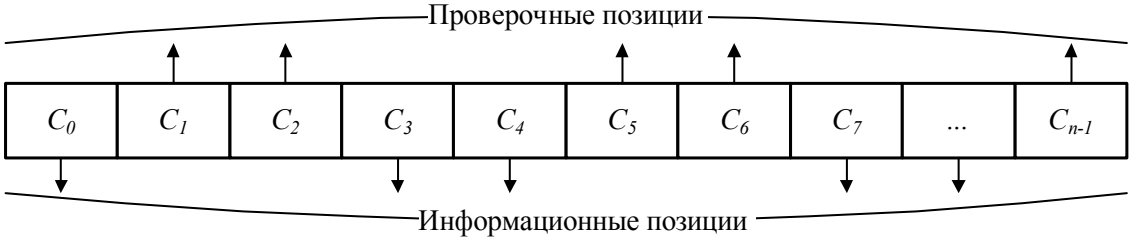


Рис. 2. Разбиение кодового слова на информационные и проверочные позиции

Пусть U – множество k информационных позиций кодового слова (т.е. множество номеров позиций, входящих в заданный информационный набор кода) и W – множество $r = n - k$ проверочных позиций. Объединение множеств $U \cup W$ содержит все целые числа (номера) от 0 до $n - 1$.

На k информационных позициях кодового слова, т.е. на позициях множества U, разместим k символов сообщения $\left(I_0, I_1, ...I_{k-1}\right)$, а на проверочных позициях множества W разместим r нулевых символов.

Вычислим суммы

$$S_j = \sum_{i=0}^{n-1} c_i F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right),\ j = \overline{0, r-1},$$

или в матричной форме

$$\left\|S_j\right\|_r = \left\|F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right)\right\|_{k,r} \left\|c_i\right\|_k^T. \tag{6}$$

Задача формирования кодового слова состоит в том, чтобы вычислить и записать на r проверочных позициях такие символы c_i, $i \in W$, которые удовлетворяют уравнениям (5).

Из определения алгеброгеометрического кода следует, что значения $r=n-k$ проверочных символов могут быть найдены из системы линейных уравнений

$$\sum_{i \in W} c_i F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right) = -S_j,\ j = \overline{0, r-1}.$$

В матричном представлении последняя запись эквивалентна выражению

$$\left\|F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right)\right\|_{r,r} \left\|c_i\right\|_r^T = \left\|-S_j\right\|_r.$$

Для нахождения значений $r = n - k$ проверочных символов, используя методы обращения матриц, запишем

$$\left\|c_i\right\|_r = \left\|F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right)\right\|_{r,r}^{-1} \left\|-S_j\right\|_r^T, \tag{7}$$

где $\left\|F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right)\right\|_{r,r}^{-1}$ – матрица, обратная матрице $\left\|F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right)\right\|_{r,r}$, т.е.

$$\left\|\left\|F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right)\right\|_{r,r}\right\|_{r,r}^{-1} = \left\|\frac{A\left[\left\|F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right)\right\|_{r,r}\right]}{\Delta_{\left\|F_j\right\|_{r,r}}}\right\|_{r,r},$$

где $A\left[\left\|F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right)\right\|_{r,r}\right]$ – алгебраическое дополнение элемента $\left\|F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right)\right\|_{r,r}$; $\Delta_{\left\|F_j\right\|_{r,r}}$ – определитель матрицы $\left\|F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right)\right\|_{r,r}$.

Поскольку размещение проверочных позиций обычно известно и фиксировано, то заранее можно найти обратную матрицу для системы уравнений (5) и получить все проверочные символы умножением вектора $\left(S_0, S_1, ...S_{r-1}\right)$ на матрицу $\left\|F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right)\right\|_{r,r}^{-1}$.

В качестве информационных могут быть выбраны любые k позиций кодового слова. Следовательно, всегда можно выбрать такое множество проверочных (и информационных) позиций, для которого матрица $\left\|F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right)\right\|_{r,r}^{-1}$ наиболее удобна для вычислений.

Таким образом, для формирования кодового слова алгеброгеометрического кода, заданного через проверочную матрицу, достаточно хранить элементы матриц $\left\|F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right)\right\|_{k,r}$ и $\left\|F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right)\right\|_{r,r}^{-1}$ либо поочередно вычислять $\left\|F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right)\right\|_{k,r}$ как значения генераторных функций в точках пространственной кривой.

2.3. Декодирование алгеброгеометрических кодов

Рассмотрим кодовое слово алгеброгеометрического *(n, k, d)* кода над *GF(q)*, построенного по алгебраическим кривым в P^u. Предположим, что алгеброгеометрический код задан через проверочную матрицу:

$$H = \begin{pmatrix} F_{0,0,\ldots,0}\left(p_j\left(x_0, x_1, \ldots, x_{u-1}\right)\right) \\ F_{1,0,\ldots,0}\left(p_j\left(x_0, x_1, \ldots, x_{u-1}\right)\right) \\ \\ F_{0,0,\ldots,\deg F}\left(p_j\left(x_0, x_1, \ldots, x_{u-1}\right)\right) \end{pmatrix},$$

где $F_{i_0,i_1,\ldots,i_{u-1}}$ – одночлен степени $i_0 + i_1 + \ldots + i_{u-1} \le \deg F$, т.е.

$$F_{i_0,i_1,\ldots,i_{u-1}} = x_0^{i_0} \cdot x_1^{i_1} \cdot \ldots \cdot x_{u-1}^{i_{u-1}},\ i = 0, \ldots, M-1; \quad M = C_{u+\deg F}^{u} - 1.$$

Справедливо равенство $C \cdot H^T = 0$, откуда следует

$$\sum_{j=0}^{n-1} C_j \cdot F_{i_0,i_1,\ldots,i_{u-1}}\left(p_j\left(x_0, x_1, \ldots, x_{u-1}\right)\right) = 0,$$

для всех $i = 0, \ldots, M-1$.

Предположим, что при передаче по каналу с ошибками кодовое слово исказилось, вектор ошибок обозначим в виде

$$e = (e_0, e_1, \ldots, e_{n-1}),$$

а принятое с ошибками слово в виде

$$C^* = (C^*_0, C^*_1, \ldots, C^*_{n-1}) = C + e = (C_0 + e_0, C_1 + e_1, \ldots, C_{n-1} + e_{n-1}).$$

Определим синдромную последовательность как вектор

$$s = \left(s_{0,0,\ldots,0}, s_{1,0,\ldots,0}, \ldots, s_{0,0,\ldots,\deg F}\right),$$

вычисленный по правилу

$$s_{i_0,i_1,\ldots,i_{u-1}} = \sum_{j=0}^{n-1} e_j \cdot F_{i_0,i_1,\ldots,i_{u-1}}\left(p_j\left(x_0, x_1, \ldots, x_{u-1}\right)\right),\ i = 0, \ldots, M-1.$$

По определению значение синдромной последовательности *s* зависит только от вектора ошибок *e* и не зависит от кодового слова *C*. Действительно, вычислим произведение

$$C^* \cdot H^T = 0,$$

получим

$$(C + e) \cdot H^T = C \cdot H^T + e \cdot H^T = e \cdot H^T,$$

откуда следует справедливость $i = 0, \ldots, M-1$ равенств:

$$\sum_{j=0}^{n-1} (c_j + e_j) \cdot F_{i_0,i_1,\ldots,i_{u-1}}\left(p_j\left(x_0, x_1, \ldots, x_{u-1}\right)\right) = \sum_{j=0}^{n-1} e_j \cdot F_{i_0,i_1,\ldots,i_{u-1}}\left(p_j\left(x_0, x_1, \ldots, x_{u-1}\right)\right) = s_{i_0,i_1,\ldots,i_{u-1}}. \quad (8)$$

Задача алгебраического декодирования состоит в нахождении вектора

$$e = (e_0, e_1, \ldots, e_{n-1})$$

по известной синдромной последовательности

$$s = \left(s_{0,0,\ldots,0}, s_{1,0,\ldots,0}, \ldots, s_{0,0,\ldots,\deg F}\right).$$

Нахождение вектора *e* позволяет, в свою очередь, восстановить кодовое слово *C* по известной последовательности C^*:

$$C = C^* - e = (C_0^* - e_0, C_1^* - e_1, ..., C_{n-1}^* - e_{n-1}).$$

Решение поставленной задачи сопряжено с нахождением *n* неизвестных в системе из M линейных уравнений, причем $M < n$. Строго говоря, при решении поставленной задачи методами линейной алгебры в общем случае существует множество решений обозначенной системы уравнений. В то же время следует отметить, что только

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

значений последовательности

$$(e_0, e_1, \ldots, e_{n-1})$$

не равны нулю, т.е. почти все $e_j = 0$, за исключением некоторого (конечного) их числа (*v*). С учетом этого ограничения существует одно (единственное) решение совокупности уравнений (8).

Обозначим множество $e_j \neq 0$ символом *E*. Для однозначного нахождения вектора ошибок воспользуемся искусственным приемом, состоящем во введении многочлена локаторов ошибок:

$$\begin{aligned}\Lambda(x_0, x_1, ..., x_{u-1}) = x_0^{v-u+1} + a_{v-u,1,...,0} \cdot x_0^{v-u} \cdot x_1 + ... + \\ + a_{1,0,...,0} \cdot x_0 + a_{0,1,...,0} \cdot x_1 + ... + a_{0,0,...,1} \cdot x_{u-1} + a_{0,0,...,0},\end{aligned} \tag{9}$$

решениями которого являются локаторы – такие наборы $(X_{0_j}, X_{1_j}, ..., X_{u-1_j})$, которые обращают в нуль многочлен (9), причем соответствующие элементы вектора ошибок $e_\xi \in E$.

Многочлен (9) однозначно задает расположение ошибок в векторе

$$e = (e_0, e_1, \ldots, e_{n-1}),$$

так как однозначно указывает на его ненулевые компоненты. Другими словами, нахождение коэффициентов $a_{i_0, i_1, ..., i_{u-1}}$ многочлена локаторов ошибок $\Lambda(x_0, x_1, ..., x_{u-1})$ позволяет однозначно указать расположение возникших при передаче кодового слова ошибок (но не их значения – истинные значения ненулевых величин e_j), например путем поочередной подстановки всех наборов $p_j(x_0, x_1, ..., x_{u-1}) = (X_{0_j}, X_{1_j}, ..., X_{u-1_j})$ в многочлен $\Lambda(x_0, x_1, ..., x_{u-1})$ и проверке на его равенство нулю.

Умножим многочлен (9) на e_j и вычислим в точке $(X_{0_j}, X_{1_j}, ..., X_{u-1_j})$, получим:

$$\begin{aligned}e_j \cdot X_{0_j}^{v-u+1} + a_{v-u,1,...,0} \cdot e_j \cdot X_{0_j}^{v-u} \cdot X_{1_j} + ... + \\ + a_{1,0,...,0} \cdot e_j \cdot X_{0_j} + a_{0,1,...,0} \cdot e_j \cdot X_{1_j} + ... + a_{0,0,...,1} \cdot e_j \cdot X_{u-1_j} + a_{0,0,...,0} \cdot e_j.\end{aligned} \tag{10}$$

Проанализируем полученное выражение.

Если $e_j \notin E$, т.е. $e_j = 0$, тогда все слагаемые полученного многочлена равны нулю, т.е. имеем равенство нулю всего выражения (10).

Если $e_j \in E$, т.е. $e_j \neq 0$, тогда соответствующие наборы $(X_{0_j}, X_{1_j}, ..., X_{u-1_j})$ обращают в нуль многочлен (9) и, соответственно, многочлен (10).

Таким образом, при любом значении e_j имеем равенство нулю выражения (10).

Просуммируем по всем *j = 0,...,n-1*, получим:

$$\sum_{j=0}^{n-1} e_j \cdot X_{0_j}^{v-u+1} + \sum_{j=0}^{n-1} a_{v-u,1,\ldots,0} \cdot e_j \cdot X_{0_j}^{v-u} \cdot X_{1_j} + \ldots +$$
$$+ \sum_{j=0}^{n-1} a_{1,0,\ldots,0} \cdot e_j \cdot X_{0_j} + \sum_{j=0}^{n-1} a_{0,1,\ldots,0} \cdot e_j \cdot X_{1_j} + \ldots + \quad (11)$$
$$+ \sum_{j=0}^{n-1} a_{0,0,\ldots,1} \cdot e_j \cdot X_{u-1_j} + \sum_{j=0}^{n-1} a_{0,0,\ldots,0} \cdot e_j .$$

Проанализируем полученное выражение. Значения $a_{i_0,i_1,\ldots,i_{u-1}}$ не зависят от j, вынесем их за знак суммирования. С учетом введенных выше обозначений, значение одночлена

$$F_{i_0,i_1,\ldots,i_{u-1}} = x_0^{i_0} \cdot x_1^{i_1} \cdot \ldots \cdot x_{u-1}^{i_{u-1}}$$

в точке $(X_{0_j}, X_{1_j}, \ldots, X_{u-1_j})$ примет вид

$$F_{i_0,i_1,\ldots,i_{u-1}}(X_{0_j}, X_{1_j}, \ldots, X_{u-1_j}) = X_{0_j}^{i_0} \cdot X_{1_j}^{i_1} \cdot \ldots \cdot X_{u-1_j}^{i_{u-1}} .$$

С учетом последнего выражение (11) перепишется в виде:

$$\sum_{j=0}^{n-1} e_j \cdot F_{v-u+1,0,\ldots,0}(X_{0_j}, X_{1_j}, \ldots, X_{u-1_j}) + a_{v-u,1,\ldots,0} \sum_{j=0}^{n-1} \cdot e_j \cdot F_{v-u,1,\ldots,0}(X_{0_j}, X_{1_j}, \ldots, X_{u-1_j}) + \ldots +$$
$$+ a_{1,0,\ldots,0} \sum_{j=0}^{n-1} \cdot e_j \cdot F_{1,0,\ldots,0}(X_{0_j}, X_{1_j}, \ldots, X_{u-1_j}) + a_{0,1,\ldots,0} \sum_{j=0}^{n-1} \cdot e_j \cdot F_{0,1,\ldots,0}(X_{0_j}, X_{1_j}, \ldots, X_{u-1_j}) + \ldots +$$
$$+ a_{0,0,\ldots,1} \sum_{j=0}^{n-1} \cdot e_j \cdot F_{0,0,\ldots,1}(X_{0_j}, X_{1_j}, \ldots, X_{u-1_j}) + a_{1,0,\ldots,0} \sum_{j=0}^{n-1} \cdot e_j = 0.$$

Но по введенному выше определению

$$s_{i_0,i_1,\ldots,i_{u-1}} = \sum_{j=0}^{n-1} e_j \cdot F_{i_0,i_1,\ldots,i_{u-1}} \left(p_j \left(x_0, x_1, \ldots, x_{u-1} \right) \right).$$

Следовательно, имеем:

$$s_{v-u+1,0,\ldots,0} + a_{v-u,1,\ldots,0} \cdot s_{v-u,1,\ldots,0} + \ldots +$$
$$+ a_{1,0,\ldots,0} \cdot s_{1,0,\ldots,0} + a_{0,1,\ldots,0} \cdot s_{0,1,\ldots,0} + \ldots +$$
$$+ a_{0,0,\ldots,1} \cdot s_{0,0,\ldots,1} + a_{0,0,\ldots,0} \cdot s_{0,0,\ldots,0} = 0.$$

Вернемся теперь к рассмотрению многочлена (9). Умножим его на произвольный одночлен $x_0^{i_0} \cdot x_1^{i_1} \cdot \ldots \cdot x_{u-1}^{i_{u-1}}$ и проведем аналогичные рассуждения. По аналогии с (10) сохранится равенство нулю при любом значении e_j. После суммирования по всем $j = 0,\ldots,n-1$ и выполнения очевидных подстановок получим рекуррентную формулу:

$$s_{i_0+v-u+1,i_1,\ldots,i_{u-1}} + a_{v-u,1,\ldots,0} \cdot s_{i_0+v-u,i_1+1,\ldots,i_{u-1}} + \ldots +$$
$$+ a_{1,0,\ldots,0} \cdot s_{i_0+1,i_1,\ldots,i_{u-1}} + a_{0,1,\ldots,0} \cdot s_{i_0,i_1+1,\ldots,i_{u-1}} + \ldots +$$
$$+ a_{0,0,\ldots,1} \cdot s_{i_0,i_1,\ldots,i_{u-1}+1} + a_{0,0,\ldots,0} \cdot s_{i_0,i_1,\ldots,i_{u-1}} = 0.$$

Выполнив соответствующие преобразования для всех $i = 0,\ldots,M-1$ получим систему линейных уравнений:

$$\begin{cases} s_{v-u+1,0,\ldots,0} + a_{v-u,1,\ldots,0} \cdot s_{v-u,1,\ldots,0} + \ldots + \\ + a_{1,0,\ldots,0} \cdot s_{1,0,\ldots,0} + a_{0,1,\ldots,0} \cdot s_{0,1,\ldots,0} + \ldots + \\ + a_{0,0,\ldots,1} \cdot s_{0,0,\ldots,1} + a_{0,0,\ldots,0} \cdot s_{0,0,\ldots,0} = 0; \\ \\ s_{v-u+2,0,\ldots,0} + a_{v-u,1,\ldots,0} \cdot s_{v-u+1,1,\ldots,0} + \ldots + \\ + a_{1,0,\ldots,0} \cdot s_{2,0,\ldots,0} + a_{0,1,\ldots,0} \cdot s_{1,1,\ldots,0} + \ldots + \\ + a_{0,0,\ldots,1} \cdot s_{1,0,\ldots,1} + a_{0,0,\ldots,0} \cdot s_{1,0,\ldots,0} = 0; \\ \ldots \\ s_{2v-2u+2,0,\ldots,0} + a_{v-u,1,\ldots,0} \cdot s_{2v-2u+1,1,\ldots,0} + \ldots + \\ + a_{1,0,\ldots,0} \cdot s_{v-u+2,0,\ldots,0} + a_{0,1,\ldots,0} \cdot s_{v-u+1,1,\ldots,0} + \ldots + \\ + a_{0,0,\ldots,1} \cdot s_{v-u+1,0,\ldots,1} + a_{0,0,\ldots,0} \cdot s_{v-u+1,0,\ldots,0} = 0. \end{cases} \quad (12)$$

При числе неизвестных z в многочлене локаторов ошибок, меньшем числа элементов синдромной последовательности, система линейных уравнений (12) разрешима. Сложность ее решения, например методом Гаусса, составит z^2.

Решения системы (12) дают значения неизвестных коэффициентов многочлена локаторов ошибок $\Lambda(x_0, x_1, ..., x_{u-1})$ (9), который, в свою очередь, однозначно задает значения локаторов – таких наборов $(X_{0_j}, X_{1_j}, ..., X_{u-1_j})$, которые обращают в нуль многочлен (9), причем соответствующие элементы $e_i \in E$.

Поиск искомых $(X_{0_j}, X_{1_j}, ..., X_{u-1_j})$ может быть выполнен, например, поочередной подстановкой всех $(X_{0_j}, X_{1_j}, ..., X_{u-1_j})$, $j = 0,...,n-1$ в многочлен $\Lambda(x_0, x_1, ..., x_{u-1})$ и проверкой на равенство нулю.

Найденные $(X_{0_j}, X_{1_j}, ..., X_{u-1_j})$ локализуют ошибку в кодовом слове, т.е. приравняют нулю $n - v$ неизвестных в системе (8). Так как число оставшихся неизвестных $v < M$, система (8) разрешима. Сложность ее решения, например методом Гаусса, не превосходит v^2. Решение системы (8) дает искомые (ненулевые) значения вектора ошибок $e = (e_0, e_1, ..., e_{n-1})$, т.е. задача декодирования решена.

3. Энергетическая эффективность алгеброгеометрического кодирования

Для оценки энергетической эффективности алгеброгеометрического кодирования рассмотрим вариант передачи дискретных сообщений М-ми ортогональными сигналами.

При некодированной передаче сообщений вероятность ошибочного приема М-х символов при когерентном приеме ортогональных сигналов определяется выражением [5]:

$$P_c = 1 - \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} e^{-\frac{u^2}{2}} \left[\frac{1}{\sqrt{2\pi}} \int_{-\infty}^{u+\sqrt{2\gamma}} e^{-\frac{z^2}{2}} dz \right]^{M-1} du, \quad (13)$$

где γ – отношение сигнал/шум для М-го символа, $M = 2^m$; γ_2 – нормированное отношение сигнал/шум на двоичную единицу, $\gamma_2 = \gamma / m$.

На рис. 3 представлены зависимости вероятности ошибочного приема М-го символа при когерентном приеме ортогональных сигналов.

Передача М-х ортогональных сигналов позволяет получить значительный выигрыш помехоустойчивости при фиксированном соотношении сигнал/шум, или существенный энергетический выигрыш при фиксированной вероятности ошибки символа. При увеличении мощности ансамбля сигналов этот выигрыш возрастает.

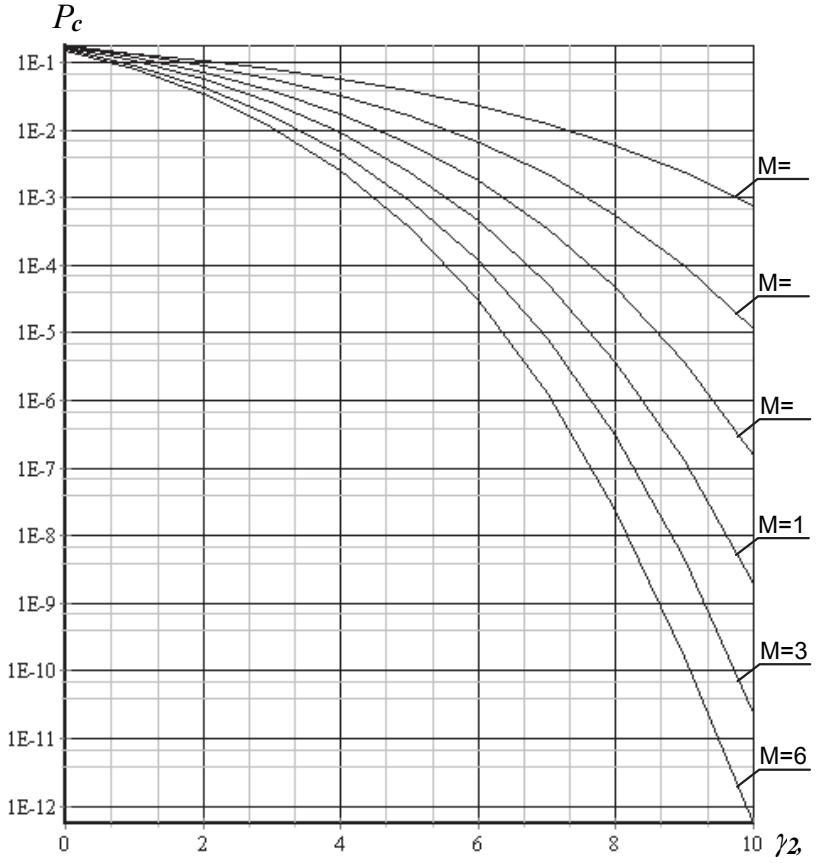


Рис. 3. Зависимости вероятности ошибочного приема М-х символов
от нормированного энергетического отношения сигнал/шум, приходящегося на один бит

Пусть задан код (n,k,d). Полагаем, что ошибки в последовательно передаваемых кодовых символах происходят независимо с вероятностью P_o. Тогда вероятность ошибки кратности i на длине блока n будет

$$P_i = C_n^i P_o^i \left(1-P_o\right)^{n-i}. \tag{14}$$

Если декодер исправляет $t=(d-1)/2$ ошибок, то вероятность ошибочного декодирования блока

$$P_{бл} = \sum_{i=t+1}^{n} P_i = \sum_{i=t+1}^{n} C_n^i P_o^i \left(1-P_o\right)^{n-i}. \tag{15}$$

Если принять предположение о случайном возникновении $2t+1$ и более ошибок в результате ошибочного декодирования кодового слова, то математическое ожидание ошибочных информационных символов на выходе декодера определяется выражением [6]

$$m_{ош} = \sum_{i=t+1}^{n-t} \frac{(i+t)k}{n} P_i + k \sum_{i=n-t+1}^{n} P_i, \tag{16}$$

а вероятность ошибочного декодирования информационного символа

$$P_{од} = m_{ош} P_{бл}. \tag{17}$$

Применение кодов, обнаруживающих и исправляющих ошибки, приводит к увеличению избыточности передаваемых данных. Если зафиксировать энергию сообщения, передаваемо-

го в канал, то энергия, приходящаяся на один символ, уменьшится пропорционально внесенной избыточности. Для расчета зависимостей вероятности ошибки на символ на выходе декодера (14) – (17) с учетом внесенной избыточности отношение сигнал/шум γ в выражении (13) уменьшим в $R = k/n$ раз.

Рассмотрим вариант передачи дискретных сообщений 4-ми ортогональными сигналами. Передаваемые сообщения закодируем алгеброгеометрическим кодом, построенным над полем $GF(4)$ (выбранные параметры кода выделены в табл. 4). На рис. 4 представлены зависимости вероятности ошибки 4-го символа от нормированного соотношения сигнал/шум при когерентном приеме 4-х ортогональных сигналов с использованием помехоустойчивых алгеброгеометрических кодов. Зависимость, отмеченная как «M=4», соответствует некодированной передачи. Зависимость, отмеченная как (5, 3, 3), соответствует алгеброгеометрическому коду по кривой рода $g = 0$, кодовые характеристики которого лежат на границе Синлгтона. Это код с максимально достижимым кодовым расстоянием (МДР код) – расширенный код Рида – Соломона. Наибольший энергетический выигрыш алгеброгеометрические коды (в том числе МДР коды) дают при скоростях $R \approx 2/3$.

Зависимости, представленные на рис. 4, свидетельствуют о преимуществах использования алгеброгеометрических кодов для помехоустойчивой передачи сообщений. Так, при значении вероятности ошибки на символ $P_c = 10^{-5}$ применение кода (9,6,3) дает энергетический выигрыш ≈0,6dB по сравнению с некодированной передачей сообщений и ≈0,2dB по сравнению с МДР кодом.

Рассмотрим вариант передачи дискретных сообщений 8-ми ортогональными сигналами. Передаваемые сообщения закодируем алгеброгеометрическим кодом, построенным над полем $GF(8)$. Конструктивные кодовые характеристики выбранных кодов выделены в табл. 5. На рис. 5 представлены зависимости вероятности ошибки 8-го символа от нормированного соотношения сигнал/шум при когерентном приеме 8-х ортогональных сигналов с использованием помехоустойчивых алгеброгеометрических кодов. Зависимость, отмеченная как «M=8», соответствует некодированной передаче. При значении вероятности ошибки на символ $P_c = 10^{-6}$ применение кода (23,14,7) дает энергетический выигрыш ≈2dB по сравнению с некодированной передачей сообщений и ≈0,8dB по сравнению с МДР кодом.

Рассмотрим вариант передачи дискретных сообщений 16-ми ортогональными сигналами. Передаваемые сообщения закодируем алгеброгеометрическим кодом, построенным над полем $GF(16)$. Конструктивные кодовые характеристики выбранных для оценки кодов выделены в табл. 6. На рис. 6 представлены зависимости вероятности ошибки 16-го символа от нормированного соотношения сигнал/шум при когерентном приеме 16-х ортогональных сигналов с использованием помехоустойчивых алгеброгеометрических кодов. Зависимость, отмеченная как «M=16», соответствует некодированной передаче. При значении вероятности ошибки на символ $P_c = 10^{-6}$ применение кода (65,45,15) дает энергетический выигрыш ≈3dB по сравнению с некодированной передачей сообщений и ≈1dB по сравнению с МДР кодом.

Рассмотрим вариант передачи дискретных сообщений 32-ми ортогональными сигналами. Передаваемые сообщения закодируем алгеброгеометрическим кодом, построенным над полем $GF(32)$. Выбранные кодовые характеристики выделены в табл. 7. На рис. 7 представлены зависимости вероятности ошибки 32-го символа от нормированного соотношения сигнал/шум при когерентном приеме 32-х ортогональных сигналов с использованием помехоустойчивых алгеброгеометрических кодов. Зависимость, отмеченная как «M=32», соответствует некодированной передаче. При значении вероятности ошибки на символ $P_c = 10^{-9}$ применение кода (99,65,29) дает энергетический выигрыш ≈4,5dB по сравнению с некодированной передачей сообщений и ≈1dB по сравнению с МДР кодом.

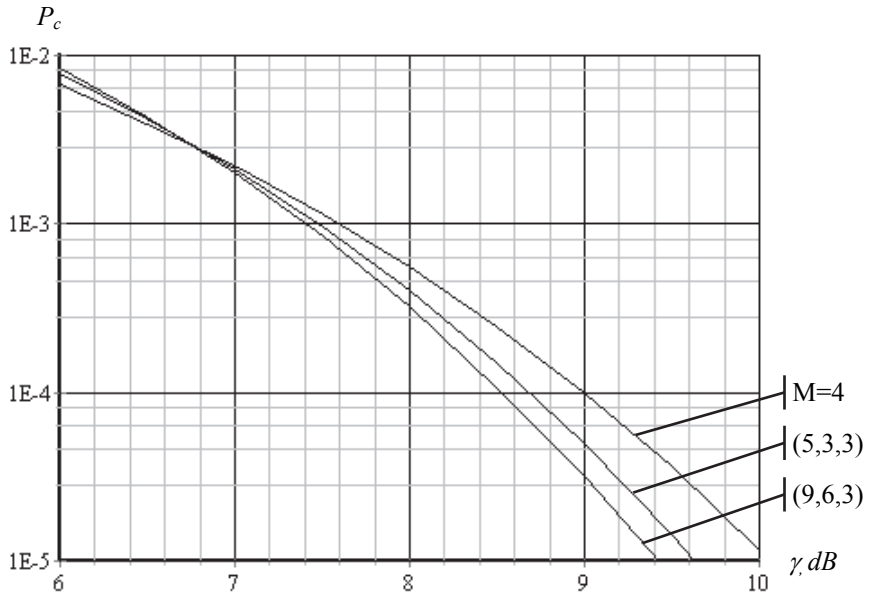


Рис. 4. Энергетическая эффективность алгеброгеометрических кодов при когерентном приеме 4-х ортогональных сигналов

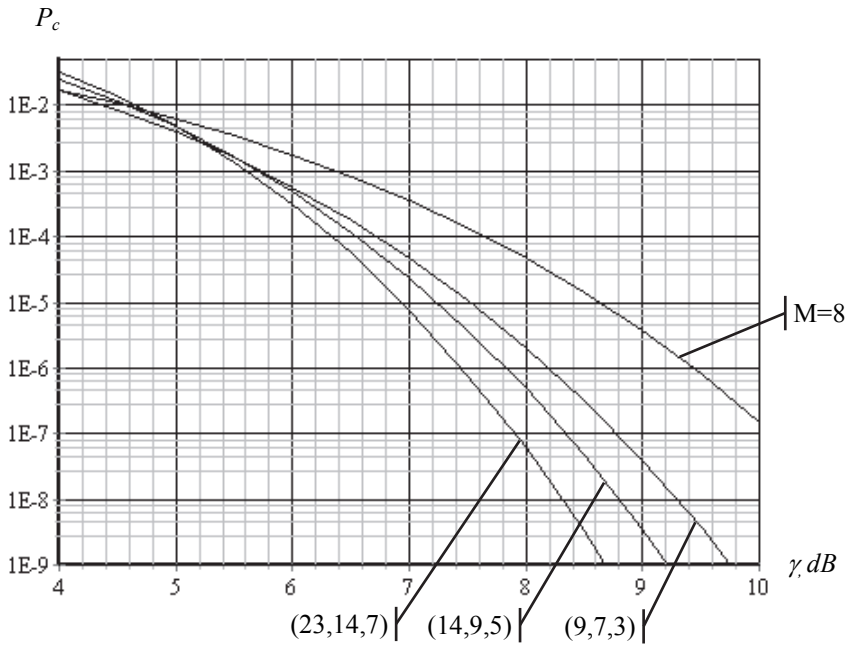


Рис. 5. Энергетическая эффективность алгеброгеометрических кодов при когерентном приеме 8-х ортогональных сигналов

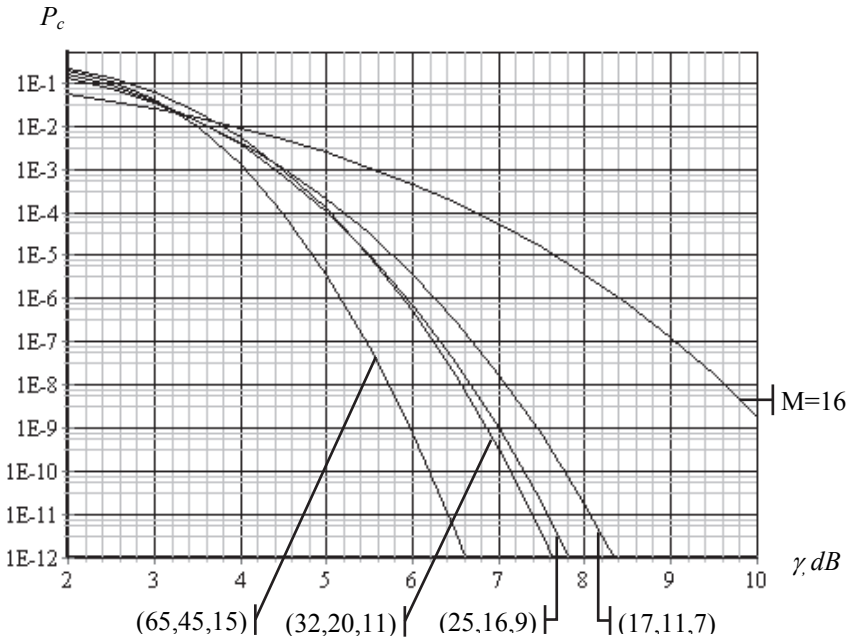


Рис. 6. Энергетическая эффективность алгеброгеометрических кодов при когерентном приеме 16-х ортогональных сигналов

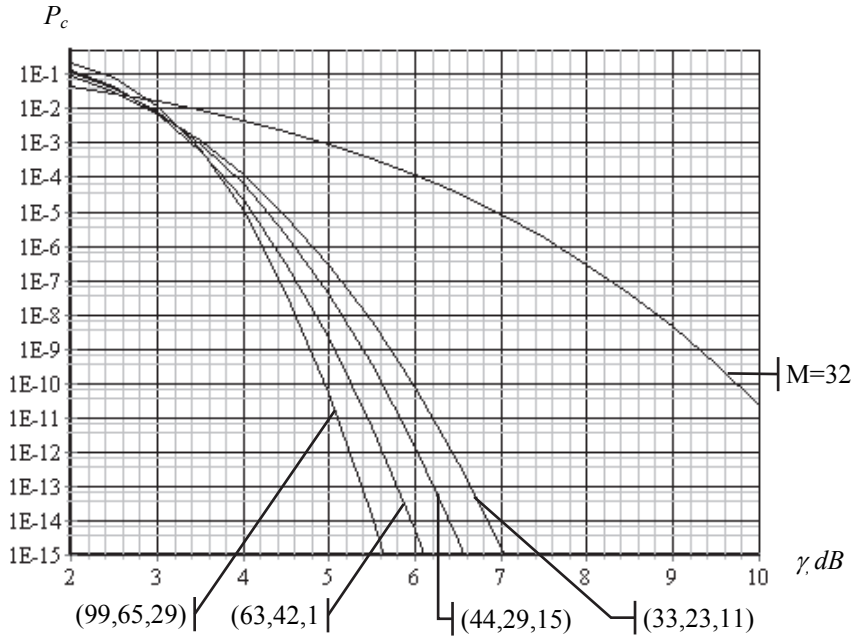


Рис. 7. Энергетическая эффективность алгеброгеометрических кодов при когерентном приеме 32-х ортогональных сигналов

Рассмотрим вариант передачи дискретных сообщений 64-ми ортогональными сигналами. Передаваемые сообщения закодируем алгеброгеометрическим кодом, построенным над полем $GF(64)$ с параметрами, выделенными в табл. 8. На рис. 8 представлены зависимости вероятности ошибки 64-го символа от нормированного соотношения сигнал/шум при когерентном приеме 64-х ортогональных сигналов с использованием помехоустойчивых алгеброгеометрических кодов. Зависимость, отмеченная как «M=64», соответствует некодированной передаче. При значении вероятности ошибки на символ $P_c = 10^{-12}$ применение кода (164,110,49) дает энергетический выигрыш ≈6dB по сравнению с некодированной передачей сообщений и ≈0,8dB по сравнению с МДР кодом.

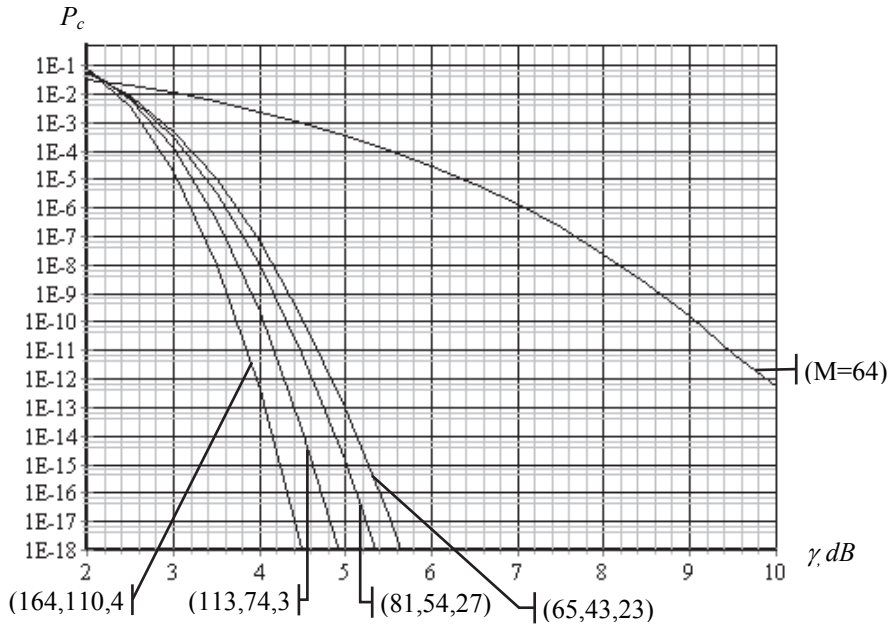


Рис. 8. Энергетическая эффективность алгеброгеометрических кодов при когерентном приеме 64-х ортогональных сигналов

Как следует из представленных на рис. 4 – 8 зависимостей, применение алгеброгеометрических кодов для повышения помехоустойчивости передачи сообщений в дискретных каналах без памяти приводит к значительному энергетическому выигрышу. Их использование позволяет существенно снизить вероятность ошибки на символ при фиксированном соотношении сигнал/шум, приходящемся на один передаваемый бит. Энергетический выигрыш возрастает при переходе к кодам, построенным по кривым с большим числом точек по отношению к роду кривой.

Сравним сложность реализации процедур кодирования-декодирования для рассмотренных кодов с известными схемами. Оценку сложности процедур кодирования-декодирования (так же, как и оценку энергетического выигрыша алгеброгеометрического кодирования) проведем в сравнении с кодами Рида – Соломона.

Если код задан порождающей матрицей G, то процедура систематического кодирования эквивалентна умножению информационного слова i на эту матрицу: $c = iG$, где c – кодовое слово. Сложность алгоритмов систематического кодирования алгеброгеометрических кодов и кодов Рида – Соломона в этом смысле практически равноценна.

Коды Рида – Соломона – подкласс кодов БЧХ, к их декодированию применимы те же методы, что и для кодов БЧХ. Одним из наиболее эффективных алгоритмов алгебраического декодирования кодов БЧХ является алгоритм Берлекэмпа – Месси и его модификации (улучшения). Известно [7], что алгоритм Берлекэмпа – Месси содержит число умножений, порядка t^2, или, формально, сложность алгоритма $O(t^2)$. Для большого t используют ускоренный алгоритм Берлекэмпа – Месси, позволяющий уменьшить вычислительную сложность алгоритма. Еще более эффективным, с точки зрения вычислительной сложности, является рекуррентный алгоритм Берлекэмпа – Месси. Асимптотическая сложность декодирования кодов Рида – Соломона в этом случае не превосходит величины $O(n\log^2 n)$, причем очень близка к величине $O(n\log n)$.

Алгоритмы декодирования алгеброгеометрических кодов получили развитие в работах [9 – 11]. Так, в работе [9] предложен алгоритм декодирования, сложность которого определяется величиной $O(n^3)$. Дальнейшее развитие процедуры декодирования в работе [10] позволило снизить сложность вычислений (показано на примере кодов по кривым Эрмита) до величины $O(n^{7/3})$. В работе [11] рассматривается алгоритм декодирования, сложности $O(n^2)$, допускающий распараллеливание вычислений (на n процессорах). Очевидно, существующие алгоритмы декодирования алгеброгеометрических кодов сопоставимы по вычислительной сложности с алгоритмами декодирования кодов БЧХ.

Выводы

Исследования показали, что алгеброгеметрические коды обладают высокими конструктивными характеристиками. В частности, приведенные на рис. 1 зависимости свидетельствуют о том, при возрастании мощности алфавита кодовые соотношения улучшаются. При большой длине алгеброгеметрические коды лежат выше границы Варшамова – Гилберта, что свидетельствует о высоких потенциальных характеристиках. Нами были получены кодовые характеристики для различных кривых над конечными полями $GF(2^m), m = 2,..,6$ (см. табл. 4 – 8).

Как показывают результаты исследований, практическая реализация алгоритмов кодирования и декодирования алгеброгеметрических кодов сводится к простым и вычислительно эффективным операциям над конечными полями. Нами были представлены несколько вариантов построения кодов (в систематическом и несистематическом виде), а также простой алгоритм декодирования. Реализация этих алгоритмов не требует существенных вычислительных затрат. Как показывает анализ, сложность кодирования и декодирования сопоставима с другими известными классами кодов.

Для оценки энергетической эффективности алгеброгеометрического кодирования мы рассмотрели вариант передачи дискретных сообщений М-ми ортогональными сигналами. Как следует из представленных на рис. 4 – 8 зависимостей, применение алгеброгеометрических кодов в дискретных каналах без памяти приводит к значительному энергетическому выигрышу. Энергетический выигрыш возрастает при переходе к длинным кодам, построенным по кривым с большим числом точек по отношению к роду кривой.

Высокая энергетическая эффективность алгеброгеометрического кодирования в сочетании с приемлемой сложностью практической реализации позволяют говорить о возможности построения эффективных помехоустойчивых систем, основанных на использовании таких кодов. Разработка и реализация практических рекомендаций по непосредственному использованию алгеброгеометрических кодов в современных телекоммуникационных системах и сетях является перспективным направлением дальнейшей работы.

Список литературы:

1. Гоппа В.Д. Коды на алгебраических кривых // Докл. АН СССР. – 1981. – Т.259. № 6. – С. 1289-1290.
2. Гоппа В.Д. Коды и информация // Успехи математических наук. – 1984. –Т.30, вып. 1(235). – С. 77-120.
3. Цфасман М.А. Коды Гоппы, лежащие выше границы Варшамова – Гилберта // Проблемы передачи информации. – 1982. – Т.18, №3. – С. 3-6.
4. Шафаревич И.Р. Основы алгебраической геометрии. – Москва : Наука, 1972. – 568с.
5. Стейн С., Джонс Дж. Принципы современной теории связи и их применение к передаче дискретных сообщений. – Москва : Связь, 1971. – 376с.
6. Касами Т., Токура Н., Ивадари Е., Инагаки Я. Теория кодирования. – Москва : Мир, 1978. – 576с.
7. Блейхут Р. Теория и практика кодов, контролирующих ошибки : пер. с англ. – Москва : Мир, 1986. – 576 с.
8. Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки. – Москва : Связь, 1979. – 744 с.
9. Feng G.L., Rao T.R.N. Decoding algebraic geometric codes up to the designed minimum distance // IEEE Trans. Inform. Theory. – 1993. – Vol. 39, N 1 – P. 37-46.
10. Sakata S., Justesen J., Madelung Y., Jensen H.E., Hoholdt T. Fast Decoding of Algebraic-Geometric Codes up to the Designed Minimum Distance // IEEE Trans. Inform. Theory. – 1995. – Vol. 41, N 5 – P. 1672-1677.
11. Olshevksy V., Shokrollahi A. A displacement structure approach to decoding algebraic geometric codes // Proceedings of the 31st annual ACM Symposium on Theory of Computing (STOC). – 1999. – P. 235-244.

Харьковский национальный
университет имени В.Н.Каразина;
АО «Институт информационных технологий», Харьков;
Университет таможенного дела и финансов, Днепр

Поступила в редколлегию 05.11.2018

УДК 519.2:519.7: 003.026

Ю.І. ГОРБЕНКО, канд. техн. наук, Є.Ю. КАПТЬОЛ

СУТНІСТЬ ТА ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ МЕТОДУ ГРОВЕРА НА КЛАСИЧНОМУ КОМП'ЮТЕРІ ДЛЯ СИМЕТРИЧНОГО КРИПТОАНАЛІЗУ

Вступ

Нині в криптографічному загалі широко обговорюється та досліджуються проблема створення та стандартизації перспективних криптографічних перетворень, в першу чергу для постквантового періоду [1, 2]. Суттєві результати досягнуто в частині розроблення, стандартизації та застосування симетричного криптоперетворення [3]. Разом з тим, продовжується розвиток та здійснюються спроби розробити більш ефективні методи криптоаналізу симетричних криптосистем – симетричних блокових перетворень (СБП), симетричних потокових перетворень (СПП) та функцій гешування(ФГ). Підтвердженням цьому є прийняття та застосування міжнародних ДСТУ ISO/IEC 18033-3, 18034-4, ДСТУ 7624:2014, ДСТУ 7564:2014, FIPS – 197, FIPS – 202 тощо. При цьому, великий інтерес до задач криптоаналізу проявляють як безпосередньо криптоаналітики так і розробники стандартизованих симетричних та асиметричних криптосистем.

Зрозуміло, що криптоаналітики направляють свої зусилля на безпосередній злам відповідних криптосистем, а розробники та ті, що застосовують криптографічні перетворення, – на перевірку їх криптографічних властивостей. Якщо раніше для спроб вирішення задач криптоаналізу застосовувались класичні спеціалізовані комп'ютерні системи, засоби та класична математика, то нині розробляються квантові комп'ютери та практично розроблені відповідні квантові математичні методи [1 – 3]. Але освоєння та застосування квантових систем та квантових математичних методів, а також програмування носить як методологічний аспект, так і психологічний – складність сприйняття.

Дослідження, що проведені, дозволяють прогнозувати використання для симетричного криптоаналізу квантового методу, що отримав назву методу Гровера [3, 4].

Метою цієї статі є деталізація, освоєння для застосування, перевірка криптоаналітичних властивостей та демонстрація застосування методу Гровера при криптоаналізі СБП, в тому числі і з методичними цілями освоєння методу при навчанні з використанням прикладів, але поки що на класичному комп'ютері.

Сутність особливості методу гровера

У загальній постановці сутність метода Гровера полягає в проведенні вичерпного пошуку специфічного (унікального) елементу у несортованій базі даних, що складається з $N = 2^n$ елементів, де n – довжина квантового регістру (кількість кубітів) [4]. Для криптоаналізу СБП специфічність елементу може зводитись до сеансового чи довгострокового ключа, сінхропослідовності тощо. Особливістю, наприклад, ключа є те, що при його застосуванні зашифровані дані можуть бути розшифрованими за поліноміальний час.

У порівнянні з найкращими класичними методами метод Гровера передбачає проведення пошуку з квадратичним прискоренням, замість $O(N)$ всього за $O(\sqrt{N})$ групових операцій. Для отримання такого прискорення використовується квантова суперпозиція станів. Причому, як показує аналіз, основним застосуванням методу Гровера є реалізований на його основі алгоритм криптоаналізу СБП Гровера. Зрозуміло, чому метод носить узагальнений зміст, так метод може бути реалізований у вигляді алгоритму криптоаналізу СП, ФГ, асиметричного шифру в кільці поліномів тощо [3, 4].

Наше обґрунтування методу Гровера ґрунтуються на його потенційних можливостях. Так, в табл. 1 наведено результати розрахунку стійкості СБП проти квантового криптоаналізу [4]. Наведені в табл. 1 дані дозволяють зробити висновок, що при розробленні

та введенні в експлуатацію хоча б одного квантового комп'ютера, значне число симетричних криптоперетворень буде зламаними, а деякі будуть під суттєвою підозрою.

Таблиця 1

Стійкість симетричних криптосистем проти квантового криптоаналізу на основі методу Гровера [3, 4]

№ п/п	Шифр	Параметри		Стійкість при атаці на	
		Розмір блока, біт	Розмір ключа, біт	блок повідомлення	ключ
1	AES-128	128	128	2^{64} ($10^{19,2}$)	2^{64} ($10^{19,2}$)
2	AES-256	128	256	2^{64} ($10^{19,2}$)	2^{128} ($10^{38,4}$)
3	DES	64	56	2^{32} ($10^{9,6}$)	2^{28} ($10^{8,4}$)
4	TDES	64	168	2^{32} ($10^{9,6}$)	2^{134} ($10^{40,2}$)
5	ГОСТ-28147	64	256	2^{32} ($10^{9,6}$)	2^{128} ($10^{38,4}$)
6	Калина-128	128	128	2^{64} ($10^{19,2}$)	2^{64} ($10^{19,2}$)
7	Blowfish	64	448	2^{32} ($10^{9,6}$)	2^{224} ($10^{67,2}$)

Спочатку розглянемо сутність та зробимо відповідний аналіз методу Гровера та етапів його виконання.

1. На першому кроці квантовий регістр з n кубітів, необхідних для представлення пошукового простору розміру $N = 2^n$, встановлюється у стан $|0\rangle$ у вигляді

$$|0\rangle^{\otimes n} = |0\rangle \tag{1}$$

Після цього квантова система встановлюється в стан рівної суперпозиції станів. Для цього над квантовим регістром з n кубітами виконується перетворення Адамара $H^{\otimes n}$, що складається з використання n звичайних гейтів (вентилів) Адамара 3]:

$$|\psi\rangle = H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle \tag{2}$$

2. На другому кроці $\frac{\pi}{4}\sqrt{2^n}$ разів застосовуються ітерації Гровера. Така кількість застосування ітерації Гровера зумовлюється необхідністю отримання реальної оптимальної ймовірності того, що отриманий стан системи буде саме тим, який шукається, а також необхідністю того, що необхідний стан матиме загальне зміщення фази не більше $\frac{\pi}{4}$ радіани [4]. Причому, кожна ітерація Гровера проводить амплітудне підсилення ймовірності знаходження елементу бази, що шукається. Кожна ітерація Гровера складається із застосування квантового оракула O та застосування оператора дифузії.

Спочатку йде виклик квантового оракула O, що модифікує систему в залежності від того, чи знаходиться система в необхідному стані. Оракул характеризується тим, що може аналізувати та модифікувати систему без зведення її до класичного стану, тобто продовжує знаходиться в квантовому стані. Конкретна реалізація квантового оракула залежить від кожного окремого випадку та задачі. Наприклад , у випадку криптоаналізу СБП оракул виконує розшифрування на ключі та повертає результат – успіх чи ні. Спільним для кожного оракула є те, що він розпізнає, чи знаходиться система в правильному стані та, якщо система знаходиться в правильному стані, оракул повертає фазу на π радіани, в іншому ж випадку він не робитиме нічого, позначивши правильний стан для подальших модифікацій наступними операціями. Причому, через зсув фаз можлива ситуація, коли правильний стан залишається тим самим, хоча його амплітуда матиме протилежний знак.

Ефект реакції оракула на систему (x) можна відобразити як

$$|x\rangle \xrightarrow{\text{O}} (-1)^{f(x)}|x\rangle, \tag{3}$$

де $f(x)=1$, якщо система знаходиться в правильному стані (успішному) та $f(x)=0$ – в іншому випадку. Точна реалізація оракула залежить від $f(x)$, а $f(x)$ залежить від задачі пошуку. Як уже зазначалось, у випадку криптоаналізу СБП, $f(x)=1$, якщо розшифрування на даному ключі оракулом є успішним.

Наступна частина ітерації Гровера називається оператором дифузії. Оператор дифузії проводить інверсію щодо середнього. Амплітуда кожного стану перетворюється так, щоб вона була набагато вищою за середнє настільки, наскільки вона була нижчою за середнє значення, та навпаки.

Оператор дифузії складається з трьох послідовних операцій: застосування перетворення Адамара $H^{\otimes n}$, умовного фазового зсуву, котрий зсуває кожен стан, окрім $|0\rangle$, на -1, та ще одного застосування перетворення Адамара $H^{\otimes n}$. Умовний фазовий зсув відображається унітарним оператором $2|0\rangle\langle 0|-I$ [5]:

$$\begin{aligned}\left[2|0\rangle\langle 0|-I\right]|0\rangle &= 2|0\rangle\langle 0|0\rangle - I = |0\rangle \\ \left[2|0\rangle\langle 0|-I\right]|x\rangle &= 2|0\rangle\langle 0|x\rangle - I = -|x\rangle\end{aligned} \tag{4}$$

Згідно з нотацією (2) стосовно $|\psi\rangle$ та за врахування (4) отримуємо оператор дифузії як

$$H^{\otimes n}\left[2|0\rangle\langle 0|-I\right]H^{\otimes n} = 2H^{\otimes n}|0\rangle\langle 0|H^{\otimes n} - I = 2|\psi\rangle\langle\psi| - I \tag{5}$$

З урахуванням оракула O (3) та оператора дифузії (5), повну ітерацію Гровера можна подати у вигляді

$$\left[2|\psi\rangle\langle\psi|-I\right]\text{O}\,. \tag{6}$$

Аналіз показує, що основною вимогою до ітерації Гровера є вимога мінімізації її складності (часу виконання). Слід відмітити, що складність і відповідно точний час виконання оракула залежить від конкретних задач і реалізацій. Тому виклик оракула звичайно розглядається як одна елементарна операція.

Загальна складність (час виконання) однієї ітерації Гровера становить $O(2n)$, що пояснюється необхідністю виконання двох перетворень Адамара, а також складності застосування $O(n)$ вентилів при виконанні умовного фазового зсуву зі складністю $O(n)$. У цілому складність виконання всього алгоритму Гровера можна оцінити як $O(\sqrt{N}) = O(\sqrt{2^n}) = O(2^{\frac{n}{2}})$ ітерацій, кожна зі складністю $O(n)$.

Схематичне зображення алгоритму Гровера з додатковим кубітом для оракула згідно з [3] наведено на рис. 1.

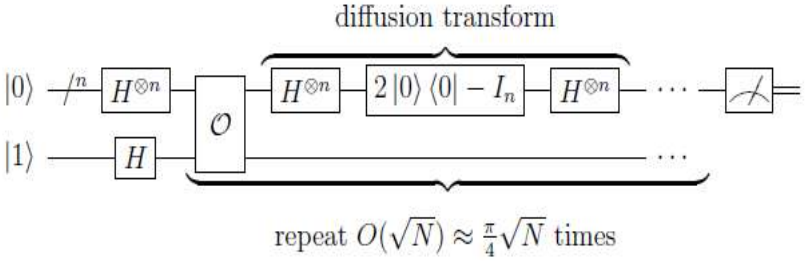


Рис.1. Алгоритм Гровера з додатковим кубітом для оракула

Для визначення результату виконання ітерації Гровера виконуються класичні вимірювання, причому результат буде правильним з достатньо високою ймовірністю. На цьому виконання алгоритму Гровера завершується, його складність становить $O(1)$ [4, 5].

Необхідно відмітити, що алгоритм Гровера є квантовим алгоритмом і вимагає застосування квантового комп'ютера та квантової математики. По суті квантова математика методу Гровера наведена вище, формули (1) – (6) та на рис. 1. Квантовий комп'ютер ще недоступний. Проте його можна реалізувати на класичному комп'ютері. Але слід зауважити, що реалізація його на класичному комп'ютері, що не підтримує квантові властивості, не є прийнятною передусім з точки зору складності (часу) виконання. Так, на квантовому комп'ютері, завдяки квантовим властивостям, наприклад можливість обстежувати весь регістр одразу без розгляду кожного окремого елемента, оракул розглядається як одна елементарна операція, а її виконання займає набагато менше потужності (часу), ніж це потребує на класичному комп'ютері. Тобто, виконання алгоритму Гровера на класичному комп'ютері є суттєво складнішим. Так, по суті лише реалізація оракула замість $\sqrt{N}$ звертань потребуватиме $N\sqrt{N}$ звертань. Відповідно час застосування алгоритму зростає настільки, що використання методу Гровера буде повільнішим, навіть у порівнянні зі складністю пошуку ключа СБП методом «грубої сили» тощо.

З метою демонстрації практичної реалізації методу Гровера розглянемо його на прикладі алгоритму пошуку унікального елементу при симетричному перетворенні.

Приклад 1. Припустимо, що система складається з $N = 16 = 2^4$ станів, і стан, який ми шукаємо, x_0, має індекс 7 та представлений бітовою строчкою $|7\rangle = |0111\rangle$. Розглянемо алгоритм Гровера пошуку данного «унікального» елемента по кроках.

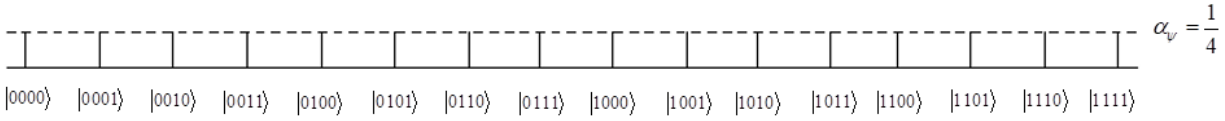
1. Для того щоб описати цю систему, потрібно $n = 4$ кубіти. У відповідності до алгоритму Гровера зробимо ініціалізацію квантового регістру з $n = 4$ кубітів, що необхідне для представлення пошукового простору розміру $N = 2^4$, встановивши регістр у початковий стан:

$$|\psi_0\rangle = |0000\rangle$$

2. Проведемо перетворення Адамара, що дозволяє отримати значення амплітуди, що пов'язана з кожним станом з рівною ймовірністю перебування в кожному з 16 можливих станів:

$$|\psi\rangle = H^{\otimes 4}|0000\rangle = (H|0\rangle)^{\otimes 4} = \frac{1}{4}\sum_{i=0}^{15}|i\rangle$$

Геометрично це можна зобразити як



3. За вказаних даних оптимальним для отримання рішення є виконання ітерацій Гровера, кількість яких визначається таким чином:

$$\frac{\pi}{4}\sqrt{2^n} = \frac{\pi}{4}\sqrt{16} = \frac{4\pi}{4} = \pi \approx 3.14$$

В подальшому для використання округлимо число ітерацій до трьох. В кожній ітерації першим кроком є виклик квантового оракула O, потім проводиться інверсія середнього, або ж оператор дифузії.

4. При пошуку елементу з індексом 7 оракул дає такі значення [3, 4]:

$$U_f(|0111\rangle|-\rangle) = -|0111\rangle|-\rangle; \qquad U_f(|i\rangle|-\rangle) = |i\rangle|-\rangle, \text{ if } i \neq 7;$$

5. Далі визначимо $|u\rangle$ використовуючи (2), в результаті маємо

$$|u\rangle = \frac{1}{\sqrt{15}}\sum_{\substack{i=0\\ i\neq 7}}^{15}|i\rangle = \frac{\begin{array}{c}|0000\rangle+|0001\rangle+|0010\rangle+|0011\rangle+|0100\rangle+|0101\rangle+|0110\rangle+|1000\rangle+|1001\rangle+|1010\rangle\\ +|1011\rangle+|1100\rangle+|1101\rangle+|1110\rangle+|1111\rangle\end{array}}{\sqrt{15}}$$

Також аналогічно (2) маємо, що $|\psi\rangle = \frac{\sqrt{15}}{4}|u\rangle + \frac{1}{4}|0111\rangle$

6. Наступним кроком знайдемо

$$|\psi_1\rangle|-\rangle = U_f(|\psi\rangle|-\rangle) = \left(\frac{\begin{array}{c}|0000\rangle+|0001\rangle+|0010\rangle+|0011\rangle+|0100\rangle+|0101\rangle+|0110\rangle-|0111\rangle+|1000\rangle+\\ |1001\rangle+|1010\rangle+|1011\rangle+|1100\rangle+|1101\rangle+|1110\rangle+|1111\rangle\end{array}}{4}\right)|-\rangle$$

Зазначимо, що $|0111\rangle$ є єдиним елементом, що має стан зі знаком "$-$".

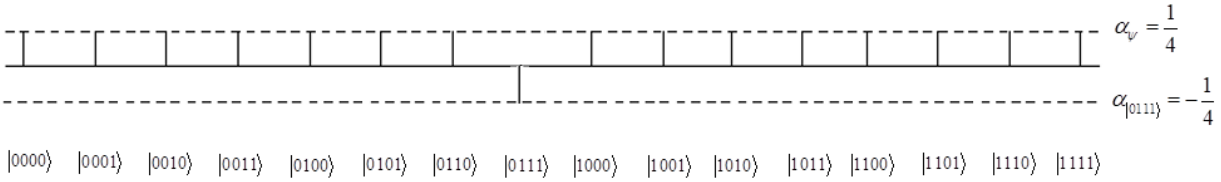
Запишемо $|\psi_1\rangle$ у вигляді

$$|\psi_1\rangle = |\psi\rangle - \frac{1}{2}|0111\rangle \ ,$$

або у вигляді

$$|\psi_1\rangle = \frac{\sqrt{15}}{4}|u\rangle - \frac{1}{4}|0111\rangle$$

Геометрично подамо отримані значення у вигляді позитивних та негативних:



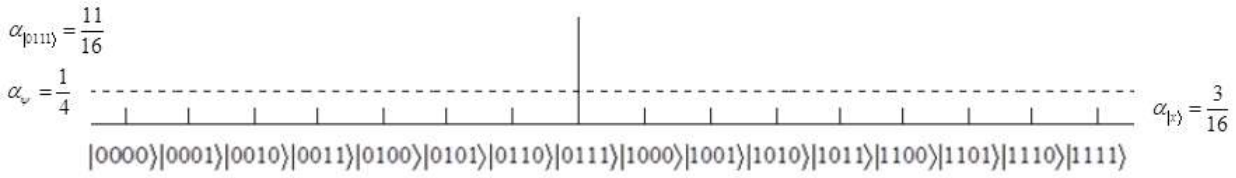
7. Далі ми обчислюємо

$$|\psi_2\rangle = (2|\psi\rangle\langle\psi| - I)|\psi_1\rangle; \qquad |\psi_2\rangle = \frac{3}{4}|\psi\rangle + \frac{1}{2}|0111\rangle;$$

$$|\psi_2\rangle = \frac{3\sqrt{15}}{16}|u\rangle + \frac{4}{16}|0111\rangle = \frac{3\sqrt{15}}{16}|u\rangle + \frac{1}{4}|0111\rangle$$

Слід відмітити, що $\langle\psi|\psi\rangle = 16\frac{1}{4}\left[\frac{1}{4}\right] = 1$. На додаток до цього, так як $|0111\rangle$ є одним з базисних векторів, можемо використати відповідність $\langle\psi|0111\rangle = \langle 0111|\psi\rangle = \frac{1}{4}$.

В результаті геометрично можна подати як

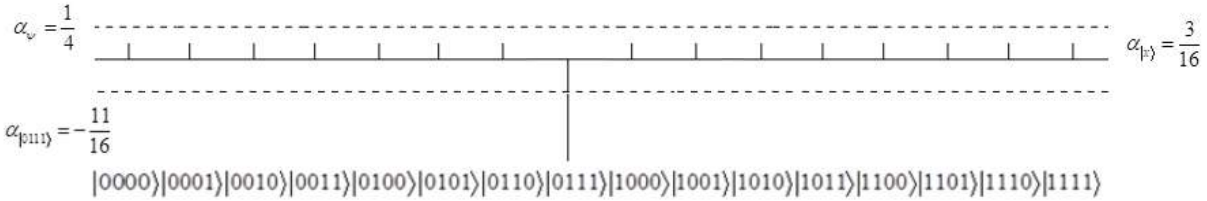


Наведеним результатом завершується перша ітерація G, залишилося ще дві.
Далі отримуємо, що

$$|\psi_3\rangle=\frac{3}{4}|\psi\rangle-\frac{7}{8}|0111\rangle$$

$$|\psi_3\rangle=\frac{3\sqrt{15}}{16}|u\rangle-\frac{11}{16}|0111\rangle$$

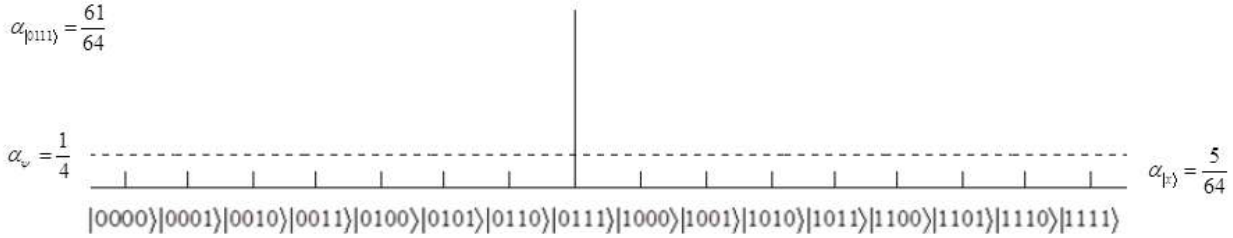
Геометрично результат подаємо як



$$|\psi_4\rangle=(2|\psi\rangle\langle\psi|-I)|\psi_3\rangle=\frac{5}{16}|\psi\rangle+\frac{7}{8}|0111\rangle$$

$$|\psi_4\rangle=\frac{5\sqrt{15}}{64}|u\rangle+\frac{61}{64}|0111\rangle$$

Геометрично результат другої ітерації подаємо як

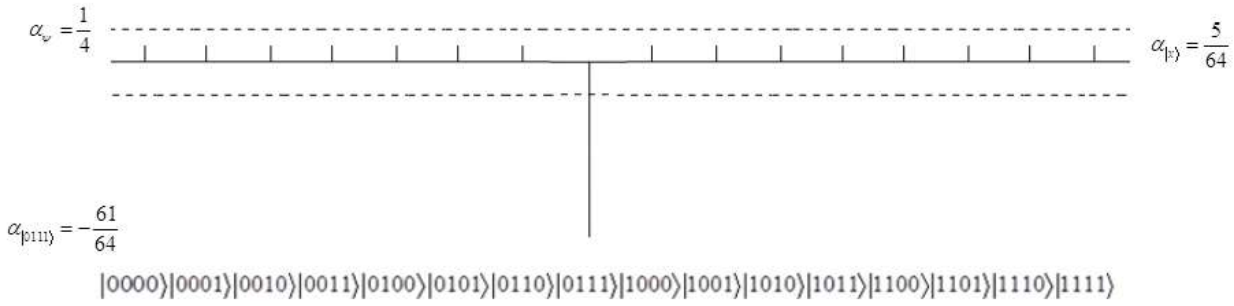


Отриманим значенням завершується друга ітерація, залишається ще одна G ітерація. При її виконанні маємо:

$$|\psi_5\rangle=\frac{5}{16}|\psi\rangle-\frac{33}{32}|0111\rangle$$

$$|\psi_5\rangle=\frac{5\sqrt{15}}{64}|u\rangle-\frac{61}{64}|0111\rangle$$

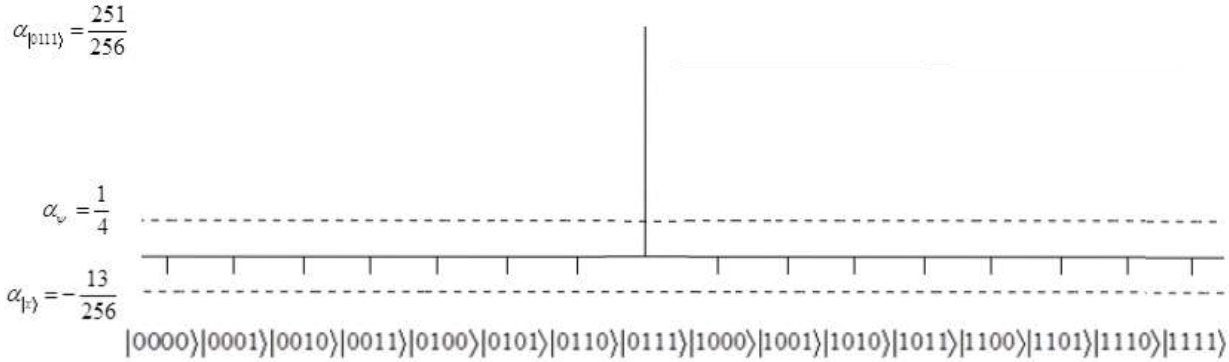
Геометрично результат третьої ітерації подаємо як



$$|\psi_6\rangle = (2|\psi\rangle\langle\psi| - I)|\psi_5\rangle = -\frac{13}{64}|\psi\rangle + \frac{33}{32}|0111\rangle$$

$$|\psi_6\rangle = -\frac{13\sqrt{15}}{256}|u\rangle + \frac{251}{256}|0111\rangle$$

На завершення третьої ітерації маємо



Наведеним завершується виконання третьої ітерації G.

Вимірювання стану $|\psi_6\rangle$ дасть результат у вигляді стану $|0111\rangle$ з ймовірністю, що становить:

$$P = \left|\frac{251}{256}\right|^2 \approx 0{,}961$$

Таким чином, шанс отримання результату $|0111\rangle$, який має індекс 7, близько 96,1 %. Ймовірність отримання невірного стану становить близько 3,9 %. Хоча метод Гровера є ймовірнісним, зі зростанням N похибка стає незначною.

Приклад 2. Припустимо, що система складається з $N = 256 = 2^8$ станів, і стан, який ми шукаємо, x_0, має індекс 15 та представлений бітовою строчкою

$$|x\rangle = |15\rangle = |0000000000001111\rangle$$

1. Розглянемо алгоритм Гровера пошуку данного «унікального» елемента.

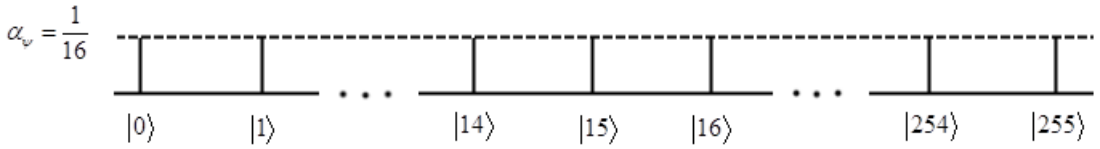
Для того щоб описати цю систему, потрібно $n = 8$ кубіти. У відповідності до алгоритму Гровера зробимо ініціалізацію квантового регістру з $n = 8$ кубітів, що необхідне для представлення пошукового простору розміру $N = 2^8$, встановивши регістр у початковий стан:

$$|\psi_0\rangle = |00000000\rangle$$

2. Проведемо перетворення Адамара, що дозволяє отримати значення амплітуди, що пов'язана з кожним станом з рівною ймовірністю перебування в кожному з 16 можливих станів:

$$|\psi\rangle = \frac{1}{16}\sum_{i=0}^{255}|i\rangle$$

Геометрично отримаємо результат



3. По аналогії з прикладом 1 маємо

$$\frac{\pi}{4}\sqrt{256} = \frac{16\pi}{4} = 4\pi \approx 12,56 \approx 13$$

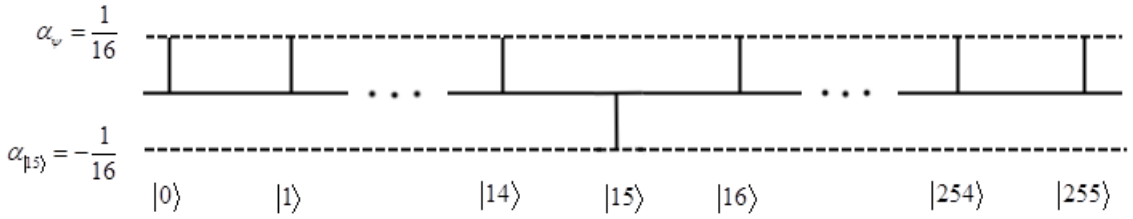
$$|u\rangle = \frac{1}{\sqrt{255}}\sum_{\substack{i=0\\ i\neq 15}}^{255}|i\rangle$$

$$|\psi\rangle = \frac{\sqrt{255}}{16}|u\rangle + \frac{1}{16}|x\rangle$$

4. Для першої ітерації маємо

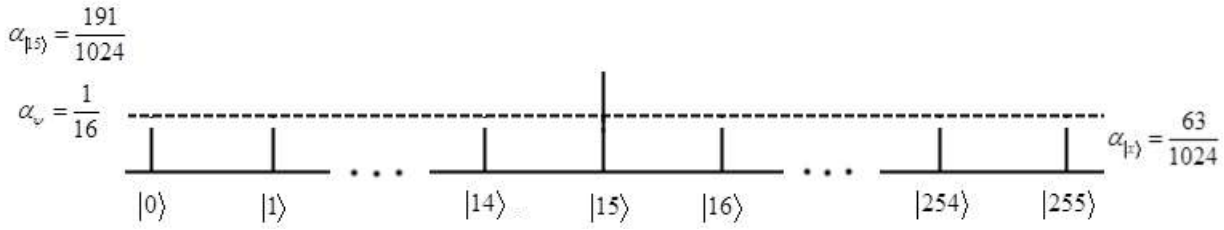
$$|\psi_1\rangle = |\psi\rangle - \frac{1}{8}|x\rangle$$

$$P = 0.00390625$$



$$|\psi_2\rangle = \left(2|\psi\rangle\langle\psi| - I\right)|\psi_1\rangle = \frac{63}{64}|\psi\rangle + \frac{1}{8}|x\rangle$$

$$P = 0.03479099$$

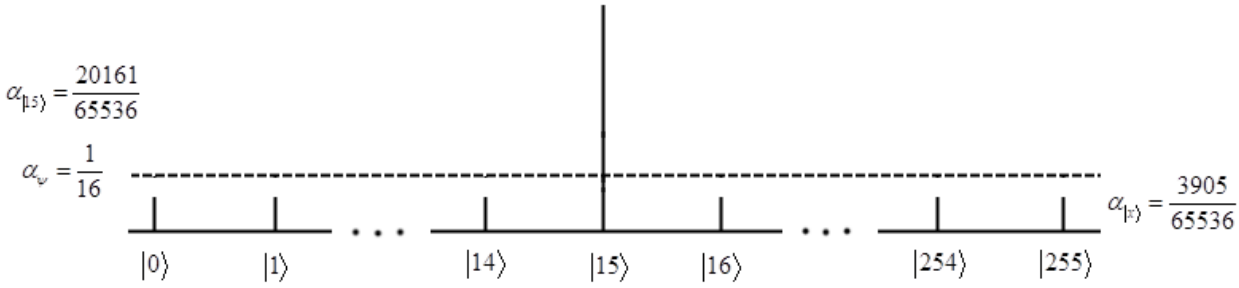


5. Друга ітерація

$$|\psi_3\rangle = \frac{63}{64}\left(|\psi\rangle - \frac{1}{8}|x\rangle\right) - \frac{1}{8}|x\rangle = \frac{63}{64}|\psi\rangle - \frac{127}{512}|x\rangle$$

$$|\psi_4\rangle = \left(2|\psi\rangle\langle\psi| - I\right)|\psi_3\rangle = \frac{3905}{4096}|\psi\rangle + \frac{127}{512}|x\rangle$$

$$P = 0.094637722$$



6. Третя ітерація

$$|\psi_5\rangle = \frac{3905}{4096}\left(|\psi\rangle - \frac{1}{8}|x\rangle\right) - \frac{127}{512}|x\rangle = \frac{3905}{4096}|\psi\rangle - \frac{12033}{32768}|x\rangle$$

$$|\psi_6\rangle = \left(2|\psi\rangle\langle\psi| - I\right)|\psi_5\rangle = \frac{237887}{262144}|\psi\rangle + \frac{12033}{32768}|x\rangle$$

$$P = 0.17972063$$

7. Четверта ітерація

$$|\psi_7\rangle = \frac{237887}{262144}\left(|\psi\rangle - \frac{1}{8}|x\rangle\right) - \frac{12033}{32768}|x\rangle = \frac{237887}{262144}|\psi\rangle - \frac{1007999}{2097152}|x\rangle$$

$$|\psi_8\rangle = \left(2|\psi\rangle\langle\psi| - I\right)|\psi_7\rangle = \frac{14216769}{16777216}|\psi\rangle + \frac{1007999}{2097152}|x\rangle$$

8. П’ята ітерації

$$|\psi_9\rangle = \frac{14216769}{16777216}\left(|\psi\rangle - \frac{1}{8}|x\rangle\right) - \frac{1007999}{2097152}|x\rangle = \frac{14216769}{16777216}|\psi\rangle - \frac{78728705}{134217728}|x\rangle$$

$$|\psi_{10}\rangle = \left(2|\psi\rangle\langle\psi| - I\right)|\psi_9\rangle = \frac{831144511}{1073741824}|\psi\rangle + \frac{78728305}{134217728}|x\rangle$$

9. Шоста ітерація

$$|\psi_{11}\rangle = \frac{831144511}{1073741824}\left(|\psi\rangle - \frac{1}{8}|x\rangle\right) - \frac{78728305}{134217728}|x\rangle = \frac{831144511}{1073741824}|\psi\rangle - \frac{5869756031}{8589934592}|x\rangle$$

$$|\psi_{12}\rangle = \left(2|\psi\rangle\langle\psi| - I\right)|\psi_{11}\rangle = \frac{47323492673}{68719476736}|\psi\rangle + \frac{5869756031}{8589934592}|x\rangle$$

10. Сьома ітерація

$$|\psi_{13}\rangle = \frac{47323492673}{68719476736}\left(|\psi\rangle - \frac{1}{8}|x\rangle\right) - \frac{5869756031}{8589934592}|x\rangle = \frac{47323492673}{68719476736}|\psi\rangle - \frac{422987878657}{549755813888}|x\rangle$$

$$|\psi_{14}\rangle = \left(2|\psi\rangle\langle\psi| - I\right)|\psi_{13}\rangle = \frac{2605715652415}{4398046511104}|\psi\rangle + \frac{422987878657}{549755813888}|x\rangle$$

11. Восьма ітерація

$$|\psi_{15}\rangle = \frac{2605715652415}{4398046511104}\left(|\psi\rangle - \frac{1}{8}|x\rangle\right) - \frac{422987878657}{549755813888}|x\rangle = \frac{2605715652415}{4398046511104}|\psi\rangle - \frac{29676939886463}{35184372088832}|x\rangle$$

$$|\psi_{16}\rangle = \left(2|\psi\rangle\langle\psi| - I\right)|\psi_{15}\rangle = \frac{137088861868097}{281474976710656}|\psi\rangle - \frac{29676939886463}{35184372088832}|x\rangle$$

12. Дев’ята ітерація

$$|\psi_{17}\rangle = \frac{137088861868097}{281474976710656}\left(|\psi\rangle - \frac{1}{8}|x\rangle\right) - \frac{29676939886463}{35184372088832}|x\rangle =$$

$$= \frac{137088861868097}{281474976710656}|\psi\rangle - \frac{2036413014601729}{2251799813685248}|x\rangle$$

$$|\psi_{18}\rangle = \left(2|\psi\rangle\langle\psi| - I\right)|\psi_{17}\rangle =$$

$$= \frac{6737274144956479}{18014398509481984}|\psi\rangle + \frac{2036413014601729}{2251799813685248}|x\rangle$$

13. Десята ітерація

$$|\psi_{19}\rangle = \frac{6737274144956479}{18014398509481984}\left(|\psi\rangle - \frac{1}{8}|x\rangle\right) - \frac{2036413014601729}{2251799813685248}|x\rangle =$$

$$= \frac{6737274144956479}{18014398509481984}|\psi\rangle - \frac{137067707079467135}{144115188075855872}|x\rangle$$

$$|\psi_{20}\rangle = \left(2|\psi\rangle\langle\psi| - I\right)|\psi_{19}\rangle =$$

$$= \frac{294117838197747521}{1152921504606846976}|\psi\rangle + \frac{137067707079467135}{144115188075855872}|x\rangle$$

14. Одинадцята ітерація

$$|\psi_{21}\rangle = \frac{294117838197747521}{1152921504606846976}\left(|\psi\rangle - \frac{1}{8}|x\rangle\right) - \frac{137067707079467135}{144115188075855872}|x\rangle =$$

$$= \frac{294117838197747521}{1152921504606846976}|\psi\rangle - \frac{9066451091283644161}{9223372036854775808}|x\rangle$$

$$|\psi_{22}\rangle = \left(2|\psi\rangle\langle\psi| - I\right)|\psi_{21}\rangle =$$

$$= \frac{9757090553372197183}{73786976294838206464}|\psi\rangle + \frac{9066451091283644161}{9223372036854775808}|x\rangle$$

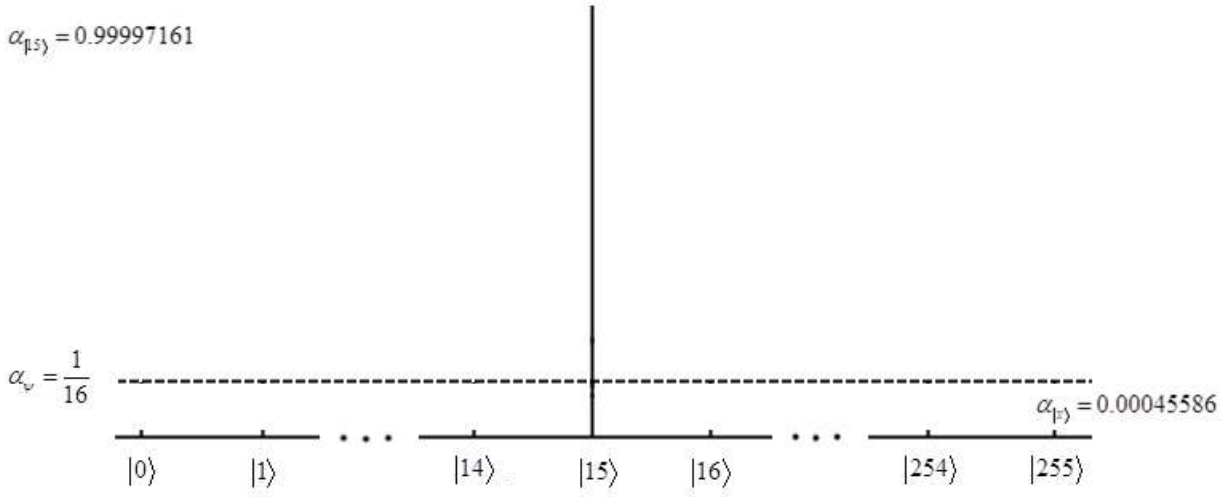
15. Дванадцята ітерація

$$|\psi_{23}\rangle = \frac{9757090553372197183}{73786976294838206464}\left(|\psi\rangle - \frac{1}{8}|x\rangle\right) - \frac{9066451091283644161}{9223372036854775808}|x\rangle =$$

$$= \frac{9757090553372197183}{73786976294838206464}|\psi\rangle - \frac{590009960395525423487}{590295810358705651712}|x\rangle$$

$$|\psi_{24}\rangle = \left(2|\psi\rangle\langle\psi| - I\right)|\psi_{23}\rangle =$$

$$= \frac{34443835020295196225}{472236648286964521 3696}|\psi\rangle + \frac{590009960395525423487}{590295810358705651712}|x\rangle$$



$$P = \left|0.99997161\right|^2 \approx 0.99994322 \approx 99.994322\%$$

16. Тринадцята ітерація

$$\left|\psi_{25}\right\rangle = \frac{34443835020295196225}{4722366482869645213696}\left(\left|\psi\right\rangle - \frac{1}{8}\left|x\right\rangle\right) - \frac{590009960395525423487}{590295810358705651712}\left|x\right\rangle =$$

$$= \frac{34443835020295196225}{4722366482869645213696}\left|\psi\right\rangle - \frac{37795081300333922299393}{377789318629571617095 68}\left|x\right\rangle$$

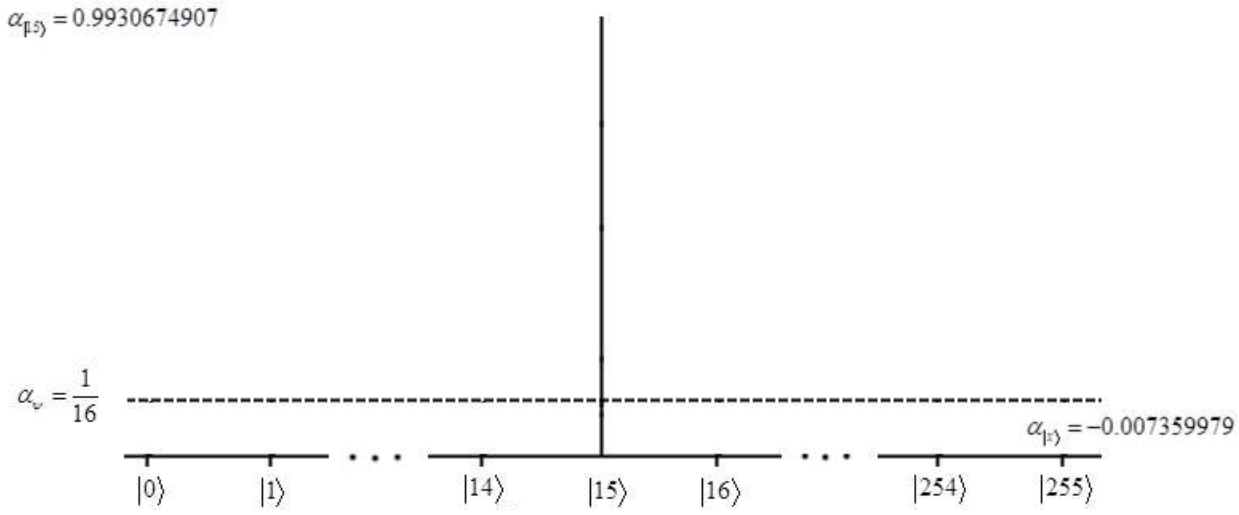
$$\left|\psi_{26}\right\rangle = \left(2\left|\psi\right\rangle\left\langle\psi\right| - I\right)\left|\psi_{25}\right\rangle =$$

$$= -\frac{35590675859035029740993}{3022314549036572936765 44}\left|\psi\right\rangle + \frac{37795081300333922299393}{377789318629571617095 68}\left|x\right\rangle$$

$$\left|\psi\right\rangle = \frac{\sqrt{255}}{16}\left|u\right\rangle + \frac{1}{16}\left|x\right\rangle$$

$$\left|\psi_{26}\right\rangle = -\frac{35590675859035029740993\sqrt{255}}{48357032784585166988247 04}\left|u\right\rangle + \frac{48021797305837070245813 11}{48357032784585166988247 04}\left|x\right\rangle$$

Наприкінці отримуємо значення ймовірності правильного визначення елемента 15.



$$P = \left| \frac{48021797305837070245813 11}{48357032784585166988247 04} \right|^2 \approx 0,98618305$$

З прикладу 2 можна зробити висновок, що для досягнення найкращого результату кількість ітерацій Гровера потрібно округляти до меншого.

Висновки

1. Суттєві результати досягнуто в частині розроблення, стандартизації та застосування симетричного криптоперетворення. Разом з тим, продовжується розвиток та здійснюються спроби розробити більш ефективні методи криптоаналізу симетричних криптосистем – симетричних блокових перетворень (СБП), симетричних потокових перетворень (СПП) та функцій гешування(ФГ). Одним із основних є метод Гровера.

2. Освоєння та застосування квантових систем та квантових математичних методів, а також відповідне їх програмування має як методологічний, так і психологічний аспект – складність сприйняття.

3. Метод Гровера полягає в проведенні вичерпного пошуку специфічного (унікального) елементу у несортованій базі даних, що складається з $N = 2^n$ елементів, де n довжина квантового регістру (кількість кубітів).

4. Для криптоаналізу СБП специфічність елементу може зводитись до сеансового чи довгострокового ключа, сінхропослідовності тощо. Особливістю ключа є те, що при його застосуванні зашифровані дані можуть бути розшифрованими за поліноміальний час.

5. У порівнянні з найкращими класичними методамии метод Гровера передбачає проведення пошуку з квадратичним прискоренням. Для отримання такого прискорення використовується квантова суперпозиція станів.

6. Конкретна реалізація квантового оракула залежить від кожного окремого випадку та задачі. Наприклад, у випадку криптоаналізу СБП, оракул виконує розшифрування на ключі та вертає результат – успіх чи ні.

Метод Гровера може бути застосований як на класичному, так і квантовому комп'ютері, хоча реалізація на класичному комп'ютері не є рентабельною.

7. Наведені 1 та 2 приклади підтвердили ефективність методу Гровера стосовно пошуку в несортованій базі: для: 4-бітного числа з ймовірністю близько 96,1 % зі складністю в три раунди; для 8-бітного числа з ймовірністю близько 99 % зі складністю в 13 раундів (силова атака вимагає 256 раундів).

8. Таким чином, застосування методу Гровера для пошуку специфічного елементу в несортованій базі дійсно дозволяє досягти квадратичне прискорення пошуку, вимагає $\sqrt{N}$ раундів у порівнянні з N «грубої сили».

Список літератури:

1. Neal Koblitz and Alfred J. Menezes A Riddle wrapped in an Enigma. Department of Mathematics, Box 353.350, University of Washington, Seattle, WA 98195 U.S.A. – Access mode: https://eprint.iacr.org/2015/1018.pdf.

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

3. Горбенко Ю. І. Методи побудування та аналізу, стандартизація та застосування криптографічних систем : монографія. – Харків : Форт, 2016. – 959 с.

4. Lov K. Grover. A fast quantum mechanical algorithm for database search. 3C-404A, Bell Labs 600 Mountain Avenue Murray Hill NJ 07974. https://arxiv.org/pdf/quant-ph/9605043.pdf.

5. Emma Strubell. An Introduction to Quantum Algorithms. COS498 – Chawathe. https://people.cs.umass.edu/~strubell/doc/quantum_tutorial.pdf.

АТ «Інститут інформаційних технологій», Харків;
Харківський національний
університет імені В.Н. Каразіна

Надійшла до редколегії 06.11.2018

УДК 004.056.5

А.А. КУЗНЕЦОВ, д-р техн. наук, А.В. ПОТИЙ, д-р техн. наук,
Н.А. ПОЛУЯНЕНКО, канд. техн. наук, С.Г. ВДОВЕНКО

КОМБИНИРУЮЩИЕ И ФИЛЬТРУЮЩИЕ ФУНКЦИИ НА ОСНОВЕ РЕГИСТРОВ СДВИГА С НЕЛИНЕЙНЫМИ ОБРАТНЫМИ СВЯЗЯМИ

1. Введение

1.1. Исследуемая модель

Рассмотрим общую структурную схему комбинирующего генератора (рис. 1) и фильтрующего генератора (рис. 2) псевдослучайной последовательности (ПСП) с применением нескольких регистров сдвига с линейными обратными связями (LFSR) или регистров сдвига с нелинейными обратными связями (NLFSR) – $SR_i\,(i=1,\ldots,L)$. Функция f рассматривается как комбинирующая или фильтрующая функция от L переменных.

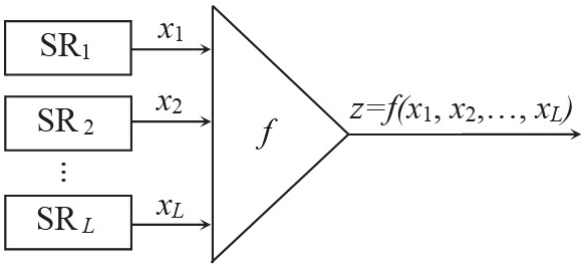


Рис. 1. Структурная схема комбинирующего генератора ПВП

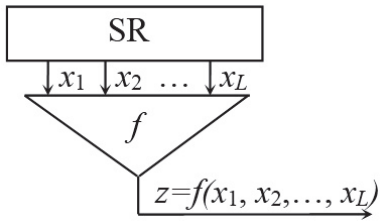


Рис. 2. Структурная схема фильтрующего генератора ПВП

Булевой функцией, которая соответствует NLFSR, в общем виде называется булево отображение вида $f: GF_2^L \to GF_2$. Булевые функции будем представлять в виде многочленов (поленом Жегалкина или алгебраическая нормальная форма – АНФ) над полем F_2:

$$f(x_1,\ldots x_L) = \bigoplus_{N\in P\{1,2,\ldots,L\}} a_N \prod_{i\in N} x_i\,, \tag{1}$$

где $P\{1,2,\ldots,L\}$ – множество всех подмножеств $\{1,2,\ldots,L\}$ (булеан), $a_N \in F_2$.

Будем исследовать только те NLFSR, которые формируют модифицированную последовательность де Брейна (которая является последовательностью максимального периода, то есть М-последовательностью). Обозначим такие нелинейные регистры как M-NLFSR.

1.2. Изучаемые криптографические свойства M-NLFSR

Рассмотрим некоторые из основных, в данном случае, показателей оценки криптографической стойкости:

– *Сбалансированность.*

Булева функция f от L переменных называется сбалансированной, если функция принимает значение 0 и 1 одинаково часто. Это одно из наиболее естественных необходимых

свойств, накладываемых на булевы функции, которые используются в текущих шифрах [1].

Если булева функция сбалансирована, то вероятность того, что она примет значение 0 или 1, одинакова и равна 1/2. Это позволяет ослабить статистические зависимости между входом функции и ее выходом. В противном случае у криптоаналитика есть возможность, используя распределение всех соотношений, провести криптоанализ шифра.

– *Наличие запретов*.

В случае анализа ПСП, который генерируется с помощью фильтрующего генератора, возникает еще одно понятие – запрет булевой функции, то есть наличие комбинаций выходной последовательности, которая не может иметь место ни при каких комбинациях входной последовательности.

Интуитивно понятно, что наличие запрета в фильтрующей функции генератора делает ее «слабее», этот запрет никогда не появится в выходной последовательности генератора, которая ухудшает его статистические свойства.

– *Корреляционная иммунность*.

Требование корреляционной иммунной функции связано с противостоянием корреляционной атаке, идея которой заключается в следующем [2]. Рассмотрим комбинирующий генератор ПВП (рис. 1). Ключом генератора являются начальные состояния всех регистров. Объем ключа равен $2^{l_1+\ldots+l_L}$, где l_i – длина SR_i для $i=1,\ldots,L$.

Каждый из SR_i генерирует последовательность $x_i = x_i^1 x_i^2 \ldots$, как правило, близкую по своим свойствам случайно. В частности, при достаточно большой длине последовательности для случайно выбранного ее бита x_i^j имеет место вероятность случайного события $x_i^j = 0$: $\mathrm{P}[x_i^j = 0] \approx 1/2$. Итак, если $y = y^1 y^2 \ldots$ – произвольная последовательность, которая не зависит от x_i, то

$$\mathrm{P}[x_i^j = y^j] = \mathrm{P}[x_i^j = 0]\cdot\mathrm{P}[y^j = 0] + \mathrm{P}[x_i^j = 1]\cdot\mathrm{P}[y^j = 1] \approx \frac{1}{2}\left(\mathrm{P}[y^j = 0] + \mathrm{P}[y^j = 1]\right) = \frac{1}{2} \qquad (2)$$

Предположим, что $\mathrm{P}[f = x_1] \neq 1/2$ (в этом случае говорят, что функция f коррелирует с переменной x_1). С помощью корреляционной атаки найдем исходное состояние s_1 SR_1. Для этого будем перебирать все возможные 2^{l_1} состояний SR_1, для каждого из них строим последовательность $z' = z'_1 z'_2 \ldots$ и подсчитываем количество совпадений с ПВП $z'_i = z_i$. Для всех последовательностей, кроме одной (генерируемой s_1), доля совпадений будет $\approx 1/2$. Тем самым, определим, что часть ключа – состояние s_1. Если функция f имеет корреляцию со всеми своими переменными (или со всеми, кроме одной – тогда состояние регистра, соответствующего этой переменной, найдем последним, зная состояние всех остальных регистров), то найдем ключ генератора с $2^{l_1} + \ldots + 2^{l_L}$ испытаниями, что гораздо меньше сложности атаки грубой силы.

– *Нелинейность*.

Практика показывает [3], что криптографические преобразования, которые обладают свойствами, близкими к свойствам линейных функций, во многих случаях приводят к существенному снижению устойчивости шифров. По этой причине в криптографии важное значение имеют функции, свойства которых исключают слабости, присущие функциям, близким к линейным. Таким образом, желаемым качеством функции является ее нелинейность, что понимается в широком смысле как отрицание линейности. В блочных и поточных шифрах применения функции с высокой нелинейностью способствуют повышению устойчивости шифров к линейному и дифференциальному методам криптоанализа.

1.3. Постановка задачи

В литературе мало описывается связь между различными криптографическими свойствами. Практика показывает [1], что в качестве компонент шифра необходимо выбирать «хорошие со всех сторон» функции, что есть на самом деле очень непростой задачей, поскольку многие свойства противоречат друг другу. Хотя теоретические результаты показывают, что в случайной функции много криптографических параметров, близких к оптимальным. Вопрос в том, как ее выбрать?

Кроме оптимизации показателей криптографической стойкости, при практической реализации необходимо учитывать простоту реализации (как программной, так и аппаратной). Чем меньше ресурсов (памяти, количество элементарных операций – при программной реализации; логических элементов и возможность их распараллеливания – при аппаратной) затрачивается алгоритмом на формирование очередного бита, тем легче получить более быстродействующий, дешёвый в изготовлении и менее энергозатратный при использовании конечный продукт.

Работа является расширением материалов, полученных авторами и изложенных в [4] для случая использования АНФ с нелинейностью произвольного порядка. Для полноты изложения материала в данной работе приводятся результаты, изложенные в [4].

В статье анализируется возможность использования M-NLFSR в качестве комбинирующей или фильтрующей функции. Изучается вопрос оптимизации выбора M-NLFSR по критериям максимальной корреляционной иммунности и нелинейности при различной алгебраической степени и возможности минимизации количества используемых мономов.

1.4. Используемые определения

F_2 – конечное поле из двух элементов, 0 и 1;

V_L – L-мерное векторное пространство над полем F_2, $V_L = (F_2)^L$. Сложение в пространстве V_L побитовое по модулю 2.

Пусть $A = a_1, a_2, \ldots, a_{2^L-1}, a_{2^L}$ последовательность длины 2^L из элементов алфавита $\{0,1\}$.

A называется последовательностью де Брейна порядка L, если среди всех кортежей длины L: $(a_1, a_2, \ldots, a_L)$, $(a_2, a_3, \ldots, a_{L+1})$, …, $(a_{2^L+L+1}, a_{2^L+L+2}, \ldots, a_{2^L})$, каждый из возможных кортежей присутствует и встречается ровно один раз, т.е. встречаются все возможные 2^L комбинации над алфавитом $\{0,1\}$ [5, 6].

Аналогичные последовательности $2^L - 1$ без кортежей из одних нулей называется *модифицированными последовательностями де Брейна*.

Степень монома (булевый одночлен) $x^N = \prod_{i \in N} x_i$ определяется как $|N|$ (число элементов подмножества N).

Алгебраической степенью $\deg(f)$ или *порядком нелинейности* булевой функции f называется число переменных в самом длинном слагаемом (мономе) ее АНФ. Булева функция степени 1 называется аффинной. Ее АНФ имеет вид

$$f(x) = a_1 x_1 \oplus a_2 x_2 \oplus \ldots \oplus a_L x_L \oplus b, \tag{3}$$

где $b \in F_2, a \in V_L$. Если $b = 0$, то функция называется линейной, а соответствующий ей регистр сдвига LFSR. Функция называется квадратичной, кубической и т.д., если ее алгебраическая степень соответственно 2, 3 и т.д. Функция с $\deg(f) = 1$ является аффинной. Случай, когда в аффинной функции $a_0 = 0$, соответствует линейной функции. Множество аффинных булевых функций от L переменных обозначается как A_L.

Весом Хэмминга или просто *весом* двоичного вектора называется число единиц среди его компонент. Вес Хэмминга булевой функции есть вес вектора ее значений. Вес вектора или функции обозначается как $wt(x)$ и $wt(f)$.

Расстояние Хэмминга $dist(f,g)$ между двумя функциями f и g есть вес функции $f \oplus g$. Другими словами, это число тех $x \in V_L$, на которых $f(x) \neq g(x)$.

Нелинейностью N_f булевой функции f называется расстояние Хэмминга между f и множеством аффинных функций.

Максимально нелинейной называется булева функция от L переменных (L любое) такая, что расстояние Хэмминга от данной функции до множества всех аффинных функций является максимально возможным. В случае четного L максимально возможное значение нелинейности равно $2^{L-1} - 2^{(L/2)-1}$. В случае нечетного L точное значение максимального расстояния неизвестно. Термин «максимально нелинейная функция» принят в отечественной литературе, тогда как в англоязычной широкое распространение получил термин «бент-функция». Аналогия между терминами неполная. При четном числе переменных L бент-функции и максимально нелинейные функции совпадают, а при нечетном L бент-функции (в отличие от максимально нелинейных) не существуют. Кроме того, все бент-функции не сбалансированы (в отличие от функций соответствующих M-NLFSR, как будет показано ниже), что делает их уязвимыми к статистическому анализу.

2. Полученные результаты

2.1. Сбалансированность

M-NLFSR, как и M-LFSR, генерируют модифицированную последовательность де Брейна, и если добавить к рассмотрению состояние заполнения всех ячеек нулевым значением, то полученная функция будет сбалансированной. При равновероятном и независимом выборе аргументов булевой функции f, которая образует M-NLFSR, вероятности ее значений, соответственно $P(1) = wt(f)/2^L$ $P(0) = 1 - wt(f)/2^L$.

2.2. Наличие запретов

M-NLFSR являются функциями, которые не имеют запретов. Это следует из того, что NLFSR формируют последовательность де Брейна, которая по определению имеет все возможные комбинации последовательности.

Однако следует быть осторожными, поскольку вполне сбалансированная фильтрующая функция в том или ином виде переносит свойства входной последовательности свойству последовательности, которая генерируется [7]. Например, в работе [8] установлен новый критерий, который идейно говорит следующее: «фильтрующая функция сохраняет запреты (в соответствующем смысле) тогда и только тогда, когда она полностью сбалансирована». Соответственно, если на вход функции поступает «далекая» от случайной последовательности, то и на выходе ее статистические свойства будут плохие.

2.3. Корреляционная иммунность

Приведенные в данном и следующем разделе утверждение и теоремы даны без доказательства с целью сокращения объема работы. Доказательства являются общедоступными и приведены, например, в [1 – 3, 9 – 12].

Наличие корреляционно иммунной функции степени m означает, что значения функции $Z = f(X)$ статистически независимы от любого набора с не более чем m компонентов произвольного вектора аргументов $X = (F_2)^L$. Это равнозначно условию, что на выход преобразования не «просачивается» информация о векторах, поступающих на вход преобразования и имеющих вес Хэмминга не более m.

Булева функция f называется корреляционно иммунного порядка m, $1 \le m \le L$, если для любой совокупности номеров m переменных $1 \le i_1 < i_2 < \ldots < i_m \le L$ случайные величины $X = \left(x_{i_1}, x_{i_2}, \ldots, x_{i_m}\right)$ и $Y = f\left(x_1, x_2, \ldots, x_L\right)$ являются независимыми.

Можно показать, что корреляционно иммунная порядка m функция от L переменных является корреляционно иммунной произвольного меньшего порядка. Таким образом, булевой функции f соответствует какой-либо максимальный порядок ее корреляционной иммунности $m_{\max}$, который обозначается $cor(f)$.

Случай, когда $m = L$ имеет место только когда $f = const$. Максимального корреляционного иммунитета степени $m = L - 1$ достигают только аффинные функции, то есть криптографически слабые. Кроме того, если f сбалансированная и $cor(f) = L - 2$, то функция f также аффинная. Таким образом, имеет смысл рассматривать порядок корреляционной иммунности m только в диапазоне $1 \le m \le L - 3$.

Сбалансированная корреляционно-иммунная функция порядка называется -стойку функцией. Формально, любую сбалансированную булеву функцию можно рассматривать как 0-стойку и произвольную булеву функцию как (-1) стойку. По аналогии с вводимым обозначения для максимального порядка устойчивости:

$$sut(f) = \begin{cases} -1, & \text{если } f \text{ не збалансированная,} \\ cor(f), & \text{если } f \text{ збалансированная.} \end{cases}$$

Неравенство Зигенталера. Если f – корреляционно-иммунная порядка m функция на $(F_2)^L$, то:

$deg(f) \le L - m$;

если f – сбалансированная и $sut(f) = m \le L - 2$, то $deg(f) + sut(f) \le L - 1$.

Неравенство Зигенталера является одним из многих противоречий криптографических свойств функций друг другу: высокий порядок корреляционной иммунной функции влечет ее низкую алгебраическую степень, и наоборот.

Если функция сбалансированная, $sut(f) = m \le L - 2$ и $\deg(f) = L - m - 1$, то f называется *m-оптимальной*. Откуда имеем m-оптимальные f для LFSR $m = L - 1 - \deg(f) = L - 2$ и для NLFSR второго порядка $m = L - 1 - \deg(f) = L - 3$ и т.д. Значение максимального порядка устойчивости для m-оптимальных функций, в зависимости от длины регистра и алгебраической степени, приведены в табл. 1.

Таблица 1

Значение максимального порядка устойчивости для m-оптимальных функций

	L						
	3	4	5	6	7	8	9
M-LFSR	1	2	3	4	5	6	7
M-NLFSR 2-го порядка	0	1	2	3	4	5	6
M-NLFSR 3-го порядка	–	0	1	2	3	4	5
M-NLFSR 4-го порядка	–	–	0	1	2	3	4

Таблица 2

Распределение количества регистров в зависимости от максимальной устойчивости для M-NLFSR

$sut(f)$	Количество M-LFSR	Количество M-NLFSR 2-го порядка	Количество M-NLFSR 3-го порядка	Количество M-NLFSR 4-го порядка
$L=2$				
m=0	0	–	–	–
m=1	1	–	–	–
$L=3$				
m=0	0	–	–	–
m=1	^{m}2	–	–	–
$L=4$				
m=0	0	4	–	–
m=1	2	^{m}10	–	–
m=2	0	–	–	–
$L=5$				
m=0	0	64	1024	–
m=1	2	52	^{m}896	–
m=2	0	^{m}6	–	–
m=3	^{m}4	–	–	–
$L=6$				
m=0	0	788	1434988	44586880
m=1	2	1044	640762	^{m}20424832
m=2	0	76	^{m}19450	–
m=3	4	^{m}38	–	–
m=4	0	–	–	–

Таблица 3

Распределение количества регистров в зависимости от максимальной устойчивости для M-PCHOC с $deg(f)\le 2$

$sut(f)$	Количество M-NLFSR	Количество M-LFSR	Количество M-NLFSR 2-го порядка
$L=7$			
m=0	33 988	0	33 988
m=1	25 582	4	25 578
m=2	4 090	0	4 090
m=3	388	10	378
m=4	4	0	^{m}4
m=5	4	^{m}4	–
$L=8$			
m=0	1 686 218	0	1 686 218
m=1	2 120 124	0	2 120 124
m=2	194 798	0	194 798
m=3	16 624	12	16 612
m=4	188	0	188
m=5	46	4	^{m}42
m=6	0	0	–
$L=9$			
m=0	284 956 836	0	284 956 836
m=1	208 843 950	2	208 843 948
m=2	24 325 344	0	24 325 344
m=3	1 091 584	16	1 091 568
m=4	21 192	0	21 192
m=5	876	28	848
m=6	10	0	^{m}10
m=7	2	^{m}2	

Таким образом, мы определили верхнюю границу значений для m-стойких функций. В работе исследованы корреляционная иммунность всего множества M-NLFSR размерностью $2 \le L \le 6$ (результаты представлены в табл. 2), а также M-LFSR и M-NLFSR 2-го порядка для $L \le 9$ (табл. 3). Как видно из табл. 2, 3, M-NLFSR достигают значения для m-оптимальных функций (в таблице обозначены как «^{m}») при всех изученных L. Однако есть очень большая доля (примерно половина всего множества M-NLFSR 2-го порядка при $7 \le L \le 9$ и 2/3 при $L = 6$), которая не имеет корреляционной иммунности.

2.4. Нелинейность

Нелинейностью функции f, как уже было сказано, называется расстояние от f к классу аффинных функций A_L:

$$N_f = dist(f, A_L) = \min_{g \in A_L} dist(f, g). \quad (4)$$

Следующие утверждения показывают, что чем выше порядок корреляционной иммунной функции, тем ниже верхний предел ее нелинейности.

Если f сбалансированная и m-стойкая, $m \le L-2$. Тогда $N_f \le 2^{L-1} - 2^{m+1}$.

По аналогии с понятием m-оптимальной функции вводится специальное название для m-устойчивой функции максимально возможной нелинейности.

Если функция f из $(F_2)^L$ сбалансированная, $sut(f) = m \le L-2$ и $N_f = 2^{L-1} - 2^{m+1}$, то f называется *m-насыщенной*.

В табл. 4 приведены рассчитанные значения максимально возможной нелинейности сбалансированной функции в зависимости от ее устойчивости.

Таблица 4

Значения нелинейности m-насыщенных функций в зависимости от их максимальной устойчивости

	$sut(f)$						
	0	**1**	**2**	**3**	**4**	**5**	**6**
$L=3$	2	0	–	–	–	–	–
$L=4$	6	4	0	–	–	–	–
$L=5$	14	12	8	0	–	–	–
$L=6$	30	28	24	16	0	–	–
$L=7$	62	60	56	48	32	0	–
$L=8$	126	124	120	112	96	64	0
$L=9$	254	252	248	240	224	192	128

Однако значения нелинейности, приведенные в табл. 4, не обязательно достижимы. Обозначим через $N_{f\max}(L,m)$ *максимально возможную нелинейность* m-стойкой булевой функции, заданной на $(F_2)^L$ и приведем верхнюю оценку для нелинейности m-стойких функций.

Из приведенного следует, что $N_{f\max}(L,-1) = 2^{L-1} - 2^{L/2-1}$ – это значение может достигаться только для четных L. Если f является сбалансированной функцией и L – четное значение, справедливо $N_{f\max}(L,m) = 2^{L-1} - 2^{L/2-1} - 2^{m+1}$ [2].

В [13] указывается, что для нечетных L и $L \le 7$, $N_{f\max}(L,-1) = 2^{L-1} - 2^{(L-1)/2}$, но для нечетных L и $L \ge 15$, справедливо неравенство $N_{f\max}(L,-1) > 2^{L-1} - 2^{(L-1)/2}$.

При $m \ge L-2$, согласно неравенству Зигенталера $\deg(f) \le 1$, откуда $N_{f\max}(L,m) = 0$. Также в [13] ссылаются на доказанное неравенство $N_{f\max}(L, L-3) = 2^{L-2}$ и

гипотезу, что $N_{f\max}(L, L-4) = 2^{L-1} - 2^{L-3}$. Кроме того, приведены некоторые точные значения $N_{f\max}(L,m)$ для малых L и m:

$N_{f\max}(4,0) = 4$;

$N_{f\max}(5,-1) = N_{f\max}(5,0) = N_{f\max}(5,1) = 12$;

$N_{f\max}(6,0) = 26$; $N_{f\max}(6,1) = N_{f\max}(6,2) = 24$;

$N_{f\max}(7,-1) = N_{f\max}(7,0) = N_{f\max}(7,1) = 56$.

Указанные результаты не противоречат результатам, полученным в данной работе и приведенным ниже.

Полученные нами результаты распределения по нелинейности всего множества M-РСНОС размерностью до $L \le 6$ сведены в табл. 5.

Таблица 5

Распределение количества регистров в зависимости от нелинейности

N_f	Количество M-LFSR	Количество M-NLFSR 2-го порядка	Количество M-NLFSR 3-го порядка	Количество M-NLFSR 4-го порядка
$L = 2$				
0	1			
$L = 3$				
0	2			
$L = 4$				
0	2			
4		14		
$L = 5$				
0	6			
4			296	
8		66	1624	
12		56		
$L = 6$				
0	6			
4				1 424
8			2 892	80 004
12			57 688	1 844 824
16		350	615 116	19 851 036
20			988 840	42 826 836
24		1 596	430 664	407 588

В табл. 6, 7 сведены результаты распределения для $L \le 6$ в зависимости от нелинейности и максимального порядка устойчивости, а в табл. 8, 9 – результаты для M- NLFSR 2-го порядка при $7 \le L \le 9$.

Таблица 6

Распределение количества регистров в зависимости
от нелинейности и максимальной устойчивости для M-NLFSR (при $L \le 6$ $\deg(f) = 1,2$)

N_f	Количество M-LFSR				Количество M-NLFSR 2-го порядка			
	$sut(f)$, при $m =$				$sut(f)$, при $m =$			
	0	1	2	3	0	1	2	3
$L = 2$								
0		1	–	–	–	–	–	–
$L = 3$								
0		m 2	–	–		–	–	–
$L = 4$								
0		2		–			–	–
4			–	–	41)	m 10	–	–
$L = 5$								
0		2		m 4				–
4				–				–
8				–	8	52	m 6	–
12			–	–	561)		–	–
$L = 6$								
0		2		4				
4								
8								
12								
16					48	188	76	m 38
20				–				–
24				–	740	8561)		–

Таблица 7

Распределение количества регистров в зависимости
от нелинейности и максимальной устойчивости для M-NLFSR (при $L \le 6$ $\deg(f) = 3,4$)

N_f	Количество M-NLFSR 3-го порядка			Количество M-NLFSR 4-го порядка	
	$sut(f)$, при $m =$			$sut(f)$, при $m =$	
	0	1	2	0	1
$L = 2$					
0	–	–	–	–	–
$L = 3$					
0	–	–	–	–	–
$L = 4$					
0	–	–	–	–	–
4	–	–	–	–	–
$L = 5$					
0			–	–	–
4	128	168	–	–	–
8	896	728	–	–	–
12			–	–	–
$L = 6$					
0					
4				652	772
8	516	2 030	346	46 484	33 520
12	57 688			1 132 844	711 980
16	201 388	397 360	16 368	13 341 932	6 509 104
20	988 840			29 715 620	13 111 216
24	186 556	241 372[1)]	m 2 736	349 348	58 240[1)]

Таблица 8

Распределение количества регистров в зависимости
от нелинейности и максимальной устойчивости для M-NLFSR (при $7 \le L \le 9$ $\deg(f) = 2$)

N_f	$sut(f)$, при $m =$		
	0	1	2
$L = 7$			
0	0	0	0
32	40	716	494
48	7 624	24 862	3 596
56	26 324[1)]	0	0
$L = 8$			
0	0	0	0
64	148	1 578	2 226
96	65 078	380 856	192 572
112	1 620 992	1 737 690	0
$L = 9$			
0	0	0	0
128	200	4398	6 608
192	498 196	4 872 526	4 953 980
224	67 714 544	203 967 024	19 364 756
240	216 743 896	0	0

Таблица 9

Распределение количества регистров в зависимости
от нелинейности и максимальной устойчивости для M-NLFSR (при $7 \le L \le 9$ $\deg(f) = 2$)

N_f	$sut(f)$, при $m =$			
	3	4	5	6
0	0	0	0	–
32	378	***m*** 4	–	–
48	0	–	–	–
56	–	–	–	–
0	0	0	0	0
64	2 342	188	***m*** 42	–
96	14 270	0	–	–
112	0	–	–	–
0	0	0	0	0
128	12 198	2 550	848	***m*** 10
192	1 079 370	18 642	0	–
224	0	0	–	–
240	0	–	–	–

Как видно из приведенных результатов, M-NLFSR одновременно достигают максимально возможную устойчивость и максимальную нелинейность. Причем, все *m*-оптимальные функции также являются и *m*-насыщенными (в табл. 6 – 9 отмечены значком «***m***»). Кроме того, многие M-NLFSR которые не являются ***m***-насыщенными функциями по определению, достигают максимально возможного результата для $N_{f\max}(L,m)$, приведенных выше (в табл. 6 – 9 отмечены значком «**1)**»).

Приведем некоторые из полученных нелинейных рекуррентных соотношений одновременно *m*-оптимальных и *m*-насыщенных функций соответствующих M-NLFSR:

для M-NLFSR второго порядка размерности $L=5$ (с нелинейностью N_f=8 и максимальной устойчивостью $sut(f)$=2, количество мономов – 6):

$$f=x_2+x_3+x_4+x_5+x_2\cdot x_3+x_1\cdot x_3$$
$$f=x_1+x_3+x_4+x_5+x_1\cdot x_4+x_1\cdot x_2$$
$$f=x_1+x_2+x_4+x_5+x_1\cdot x_4+x_3\cdot x_4$$
$$f=x_1+x_2+x_4+x_5+x_1\cdot x_4+x_1\cdot x_3$$
$$f=x_1+x_2+x_3+x_5+x_1\cdot x_4+x_1\cdot x_3$$
$$f=x_1+x_3+x_4+x_5+x_1\cdot x_4+x_2\cdot x_4$$

для M-NLFSR третьего порядка размерности $L=6$ (с нелинейностью N_f=24 и максимальной устойчивостью $sut(f)$=2, 70 функций по 10 мономов, 346 по 12 мономов, 1124 – 14 мономов, 924 – 16 мономов, 252 – 18 мономов, 20 – 20 мономов):

$$f=x_4+x_5+x_6+x_1\cdot x_2+x_1\cdot x_3+x_2\cdot x_3+$$
$$+x_3\cdot x_4+x_1\cdot x_2\cdot x_3+x_1\cdot x_3\cdot x_4+x_1\cdot x_3\cdot x_5$$
$$f=x_3+x_4+x_5+x_6+x_1\cdot x_2+x_1\cdot x_4+x_2\cdot x_5+$$
$$+x_1\cdot x_2\cdot x_3+x_1\cdot x_2\cdot x_4+x_1\cdot x_2\cdot x_5$$

для M-NLFSR второго порядка размерности $L=9$ (с нелинейностью N_f=128 и максимальной устойчивостью $sut(f)$=6, количество мономов – 10):

$$f=x_1+x_2+x_3+x_4+x_5+x_6+x_7+x_9+x_2\cdot x_5+x_2\cdot x_8$$
$$f=x_2+x_3+x_4+x_5+x_6+x_7+x_8+x_9+x_1\cdot x_7+x_4\cdot x_7$$
$$f=x_1+x_2+x_3+x_4+x_5+x_7+x_8+x_9+x_4\cdot x_6+x_4\cdot x_8$$
$$f=x_1+x_2+x_4+x_5+x_6+x_7+x_8+x_9+x_1\cdot x_5+x_3\cdot x_5$$
$$f=x_1+x_2+x_3+x_4+x_6+x_7+x_8+x_9+x_3\cdot x_5+x_3\cdot x_6$$
$$f=x_1+x_2+x_3+x_5+x_6+x_7+x_8+x_9+x_3\cdot x_6+x_4\cdot x_6$$
$$f=x_1+x_2+x_3+x_4+x_6+x_7+x_8+x_9+x_1\cdot x_6+x_5\cdot x_6$$
$$f=x_1+x_2+x_3+x_5+x_6+x_7+x_8+x_9+x_3\cdot x_4+x_3\cdot x_8$$
$$f=x_1+x_2+x_3+x_4+x_6+x_7+x_8+x_9+x_2\cdot x_7+x_5\cdot x_7$$
$$f=x_1+x_2+x_3+x_5+x_6+x_7+x_8+x_9+x_2\cdot x_4+x_2\cdot x_7$$

Анализируя полученные результаты, видим, что симметричные M-NLFSR имеют одинаковые показатели $sut(f)$ и N_f. Все изученные M-NLFSR с $\deg(f)\geq 2$ имеют $N_f\geq 2^{L-\deg(f)}$.

Выводы

Получено и исследовано полное множество M-NLFSR $2\leq L\leq 6$, а также с $7\leq L\leq 9$, имеющих алгебраическую степень формирующей АНФ не выше $\deg(f)\leq 2$.

Функции, соответствующие M-NLFSR, являются сбалансированными функциями и не имеют запретов.

Протестирована и определена их корреляционная иммунность и нелинейность. Приведено распределение количества M-NLFSR для разных значений корреляционной иммунности, нелинейности, алгебраической степени и числа мономов в АНФ.

Показано, что M-NLFSR достигают значений корреляционной иммунности, соответствующих m-оптимальным функциям при всех изученных L. Однако есть большая доля функций, которые не имеют корреляционной иммунности. Кроме того, функции могут быть одновременно m-оптимальными и m-насыщенными.

Приведен ряд m-оптимальных и одновременно m-насыщенных функций, соответствующих M-NLFSR, при этом обладающих минимальным количеством мономов АНФ, что позволяет на их основе (при заданных размерах) минимизировать затраты (временные и аппаратные) для генерации ПВП.

Список литературы:

1. Городилова А.А. От криптоанализа шифра к криптографическому свойству булевой функции // Прикладная дискретная математика. – 2016. – № 3(33). – С.16–44

2. Панкратова И.А. Булевы функции в криптографии : учеб. пособие. – Томск : Изд. Дом Томск. гос. ун-та, 2014. – 88 с.

3. Мухачев В.А., Хорошко В.А. Методы практической криптографии. – К. : ООО «Полиграф-Консалтинг», 2005. – 215 с

4. Потий А.В., Полуяненко Н.А. Расчет числа образующих полиномов для регистров сдвига с нелинейной обратной связью с нелинейностью произвольного порядка // Міжнар. наук. конф. питання оптимізації обчислень (ПОО-XLIV) Інституту кібернетики імені В.М. Глушкова НАН України, 26–29 вересня 2017 року. Хмельницька область, м. Кам'янець-Подільський.

5. Хачатрян Л.Г. Методы построения последовательностей де Брейна // Дискретна математика. – 1991. – Т. 3, вып. 4. – С. 62–78

6. Knuth D. The Art of Computer Programming. Vol. II. Seminumerical Algorithms. — USA, Commonwealth of Massachusetts: Addison-Wesley, 1969. – P.634.

7. Логачев О.А., Сальников А.А., Смышляев С.В., Ященко В.В. Булевы функции в теории кодирования и криптологии ; 2-е изд. – Москва : МЦНМО, 2012. – 584с.

8. Смышляев С.В. О криптографических слабостях некоторых классов преобразований двоичных последовательностей // Прикладная дискретная математика. – 2010. – № 1. – С. 5–15.

9. Токарева Н. Н. Обобщения бент-функций. Обзор работ // Дискретный анализ и исследование операций. – 2010. – Т. 17, №1. – С.33-62

10. Токарева Н.Н. Нелинейные булевы функции : бент-функции и их обобщения. Издательство LAP LAMBERT Academic Publishing (Saarbrucken, Germany), 2011. – 180 с. ISBN: 978-3-8433-0904-2.

11. Агафонова И.В. Криптографические свойства нелинейных булевых функций. Семинар по дискрет. гармон. анализу и геометр. моделированию. – СПб. : DHA & CAGD, 2007. – С. 1–24.

12. Шевелев Ю.П. Дискретная математика. Ч. 1: Теория множеств. Булева алгебра (Автоматизированная технология обучения «Символ») : учеб. пособие. – Томск. гос. ун-т систем управления и радиоэлектроники, 2003. –118 с. ; Молдовян А.А. Криптография. Скоростные шифры. – БХВ-Петербург, 2002. – 496 с.

13. Таранников Ю.В. О корреляционно-иммунных и устойчивых булевых функциях. Математические вопросы кибернетики. – Москва : Физматлит, 2002. – Вып. 11. – С. 91–148.

Харьковский национальный
университет имени В.Н. Каразина;
АО «Институт информационных технологий», Харьков;
Национальный университет обороны Украины
имени Ивана Черняховского, Киев

Поступила в редколлегию 28.10.2018

УДК 621.3.06

М.Ю. РОДІНКО

ОЦІНКА СТІЙКОСТІ СИМЕТРИЧНОГО БЛОКОВОГО ШИФРУ «КИПАРИС» ДО ДИФЕРЕНЦІЙНОГО КРИПТОАНАЛІЗУ

Вступ

В останні роки все більшого розвитку набуває малоресурсна криптографія, метою якої є створення симетричних примітивів (блокових та потокових шифрів, функцій гешування) для застосування у нересурсоємних пристроях. Висока зацікавленість у розробці таких примітивів спостерігається і з боку Національного Інституту Стандартів і Технологій США, який у 2018 році оголосив про конкурс з розробки малоресурсних алгоритмів для застосування у простих електронних пристроях [1].

Відповідно до світових тенденцій в Україні розроблений перспективний малоресурсний симетричний блоковий шифр «Кипарис» [2]. Метою розробки малоресурсного алгоритму було забезпечення високої швидкодії перетворень зі збереженням високого рівня криптографічної стійкості, прийнятної для застосування шифру у постквантовий період. Блоковий шифр «Кипарис» оперує 256- та 512-бітовими блоками даних із використанням ключа шифрування аналогічної довжини.

У попередніх роботах [2, 3] були представлені результати досліджень лавинних та статистичних показників блокового шифру «Кипарис», його швидкісних характеристик, а також результати щодо оцінки диференційних властивостей алгоритму. Оскільки, диференційний криптоаналіз (ДК) [4] є найбільш розповсюдженим серед відомих методів криптоаналізу симетричних блокових шифрів, обґрунтування стійкості до ДК є невід'ємною частиною оцінки будь-якого блокового шифру.

В основі блокового шифру «Кипарис» лежить ARX-перетворення (складається з операцій додавання за модулем, циклічного зсуву та побітового додавання), яке знайшло широке застосування у малоресурсних алгоритмах (ChaCha [5], SPECK [6], TEA [7] і т.д.). Однак, не дивлячись на простоту застосовуваних операцій, розробники ARX-шифрів стикаються з проблемами при оцінці верхньої границі диференційної ймовірності шифру через відсутність загального теоретичного підходу до оцінки стійкості ARX-шифрів до ДК. У роботі [3] запропоновані евристичні методи пошуку найбільш ймовірних одноциклових диференційних характеристик блокового шифру «Кипарис», за допомогою яких знайдено одноциклові характеристики з ймовірністю 1/4 та 1/8.

Метою роботи є оцінка практичної стійкості блокового шифру «Кипарис» до диференційного криптоаналізу, що визначається ймовірністю кращої знайденої диференційної характеристики. Для досягнення цієї мети у роботі пропонуються методи пошуку багатоциклових диференційних характеристик для блокового шифру «Кипарис».

1. Диференційний криптоаналіз блокових шифрів

В основі диференційного криптоаналізу [4] блокових шифрів лежить аналіз проходження різниці між двома відкритими текстами крізь цикли шифрування та оцінка ймовірності перетворення вхідної різниці a у вихідну різницю b. Максимальне значення диференційної ймовірності визначається як [8, 9]

$$\mathrm{MEDP}(a,b) = \max_{a\neq 0,b} \mathrm{EDP}(a,b), \tag{1}$$

де $\mathrm{EDP}(a,b)$ – середня за ключами ймовірність диференціалу.

Значення MEDP(a,b) називається теоретичною стійкістю блокового шифру до диференційного криптоаналізу [10]. Однак, як правило, при аналізі блокових шифрів, користуються

оцінкою практичної стійкості [10], яка визначається верхньою границею ймовірності диференційної характеристики, або

$$\mathrm{MEDP}(\Omega) = \max_{\Omega \in (a,b)} \mathrm{EDP}(\Omega(a,b)). \tag{2}$$

де $\mathrm{EDP}(\Omega(a,b))$ – середня за ключами ймовірність диференційної характеристики.

Як правило, сучасні ітеративні блокові шифри є марковськими. Для марковського шифру ймовірність багатоциклової характеристики може бути апроксимована добутком ймовірностей одноциклових характеристик [8].

Нехай задано ітеративний блоковий шифр $E_k^{(r)}(x)$ з розміром ключа κ, що складається з r ітерацій циклової функції $f(x)$. Для успішної атаки на блоковий шифр необхідно знайти $(r-1)$ -циклову диференційну характеристику з ймовірністю [8]

$$P(E_k^{(r-1)}(x) + E_k^{(r-1)}(x+a) = b) = p >> 2^{-n}. \tag{3}$$

Для традиційних блокових шифрів, що базуються на S-блоках, максимальна ймовірність ДХ для одного циклу перетворення визначається максимумом таблиці розподілу різниць S-блока та мінімальною кількістю гілок активізації лінійного перетворення [9]. Подібний підхід є застосовуваним до шифрів, побудованих згідно зі стратегією широкого сліду, таких як AES, Калина, Camellia та ін., завдяки тому, що нелінійна та лінійна складові цих алгоритмів побудовані із застосуванням прозорого математичного апарату, а значить мають теоретично обґрунтовані криптографічні властивості [11].

2. Оцінка стійкості ARX-шифрів до диференційного криптоаналізу

У якості нелінійної операції в ARX-шифрах виступає додавання n-бітових слів за модулем 2^n, а циклові ключі, як правило, вводяться за допомогою операції XOR, тому, диференційна ймовірність шифру визначається ймовірностями перетворення різниць (обчислених за допомогою операції XOR) на модульних суматорах [12]. Розмір модуля є достатньо великим у порівнянні з розмірністю S-блоків (як правило, 32-64 біти), що з точки зору обчислювальної складності унеможливлює побудування повної таблиці розподілу різниць.

Визначення мінімальної кількості гілок активізації також є складною задачею, оскільки перемежування простих (нелінійних та лінійних) операцій, що не підпорядковується чіткому математичному обґрунтуванню, є складним з точки зору аналізу його криптографічних властивостей.

Часто один цикл перетворення ARX-шифру містить декілька нелінійних та лінійних операцій, що чергуються між собою, при цьому ключове забілювання застосовується лише на початку кожного циклу. Згідно з класичною теорією [8] такий шифр не є марковським, оскільки вхідні значення нелінійних операцій, починаючи з другої, не рандомізуються ключем. Тим не менше, в сучасних роботах з диференційного криптоаналізу ARX-шифрів робиться припущення, що шифр є марковським, і ймовірність ДХ для одного циклу перетворення обчислюється як добуток ймовірностей перетворення різниць при проходженні крізь нелінійні операції [12]. Таке припущення не матиме суттєвого впливу на результат оцінки, проте значно спростить процес оцінювання (хоча, поодинокі приклади випадків, коли шифр поводить себе як немарковський, також наведені в літературі [13]). В будь-якому разі, на поточний момент невідомо, як розраховувати диференційну ймовірність у разі припущення про «немарковість» шифру. Викладені у цій статті результати також базуються на припущенні, що «Кипарис» є марковським шифром.

Вперше підхід до проектування ARX-шифрів, які є доказово стійкими до для диференційного (лінійного) криптоаналізу, представлений в [14]. Якщо для блокових шифрів, побудованих на основі S-блоків, застосовується стратегія широкого сліду, то для ARX-шифрів

пропонується так звана стратегія довгого сліду (англ. long trail strategy). Нова стратегія пропонує використовувати S-блоки разом з простими лінійними операціями [14]. Застосування запропонованого підходу при розробці шифру SPARX дозволило отримати оцінку верхньої границі диференційної ймовірності для цього шифру.

Що стосується оцінки стійкості існуючих ARX-шифрів, на сьогоднішній день не існує універсального теоретичного методу оцінки верхньої границі ймовірності ДХ для ARX-шифрів. Існуючі методи оцінки, як правило, базуються на результатах застосування евристичних алгоритмів пошуку кращих диференційних характеристик [12, 13]. До найбільш відомих таких методів можна віднести наступні:

- модифікований алгоритм Мацуї із застосуванням часткових таблиць розподілу різниць [12], найбільш розвинутий з існуючих методів;
- метод, заснований на пошуку ймовірносних нейтральних бітів (англ. probabilistic neutral bits) [15], наразі застосований до потокових шифрів Salsa та ChaCha;
- метод, заснований на задачі здійснимості булевих формул (англ. SAT solvers) [13], який також запропонований для криптоаналізу шифру Salsa.

Найбільшого застосування набув метод пошуку на основі часткових таблиць розподілу різниць, запропонований А. Бірюковим та В. Вєлічковим [12].

Таблиця розподілу різниць (TPP) для додавання n-бітових слів за модулем 2^n містить ймовірності перетворення двох вхідних різниць у вихідну після проходження крізь операцію модульного додавання.

Означення 1 [12, 16]. Нехай α, β та γ – фіксовані n-бітні різниці (за операцію XOR). Диференційна ймовірність додавання за модулем 2^n (xdp^+) – це ймовірність, з якою вхідні різниці α та β переходять у вихідну різницю γ після проходження через операцію додавання, обчислена для всіх пар n-бітових вхідних текстів (x, y):

$$\mathrm{xdp}^+(\alpha,\beta\to\gamma)=2^{-2n}\cdot\#\{(x,y):((x\oplus\alpha)+(y\oplus\beta))\oplus(x+y)\}=\gamma. \quad (4)$$

Як можна помітити з формули (4), розрахунок значення ймовірності прямим шляхом перебирання усіх вхідних пар навіть для одного переходу є обчислювально складною задачею. Ефективний алгоритм для практичного обчислення значення xdp^+ представлений в [17].

У зв'язку з великим розміром модуля n, навіть із застосуванням ефективного алгоритму, побудування повної таблиці розподілу різниць є нездійсненною на практиці задачею. У свою чергу в [12] пропонується будувати так звану часткову TPP, що містить диференціали $(\alpha,\beta\to\gamma)$ з ймовірністю, що дорівнює або перевищує заданий поріг p_{thres} [12]:

$$(\alpha,\beta,\gamma)\in D\Leftrightarrow(\alpha,\beta\to\gamma)\geq p_{thres}. \quad (5)$$

Далі пропонується побудувати таку часткову таблицю для усієї циклової функції та, використовуючи модифікований алгоритм Мацуї, здійснити пошук диференційних характеристик. Цей метод був успішно застосований до блокових шифрів заснованих на мережі Фейстеля з ARX-подібною цикловою функцією, а саме таких як SPECK, TEA, XTEA та ін.

Можна відмітити, що описаний метод найбільше підходить до шифрів з достатньо простою цикловою функцією, в якій не передбачається поділу вхідного значення на слова. Це пояснюється тим, що коли операції додавання та зсуву застосовуються до цілого вхідного значення, побудувати часткову TPP для такої циклової функції достатньо просто.

3. Функція шифрування блокового шифру «Кипарис»

Блоковий шифр «Кипарис» оперує блоками даних розміром l біт, із використанням ключа шифрування довжиною k біт, $l,k\in\{256,512\}$, $l = k$. Операції циклової функції виконуються над s-бітними словами, $s\in\{32,64\}$. Загальні параметри шифру наведені в табл. 1 [2].

Таблиця 1

Загальні параметри блокового шифру «Кипарис»

Параметр	Кипарис-256	Кипарис-512
Розмір блока (l), біт	256	512
Довжина ключа (k), біт	256	512
Довжина слова (s), біт	32	64
Кількість циклів (t)	10	14

Схематичне зображення функції зашифрування наведено на рис. 1. Як видно з рисунку, шифр «Кипарис» представляє собою мережу Фейстеля з ARX-перетворенням у якості циклової функції, що містить 8 додавань за модулем 2^s, 8 додавань за модулем 2 та 8 циклічних зсувів.

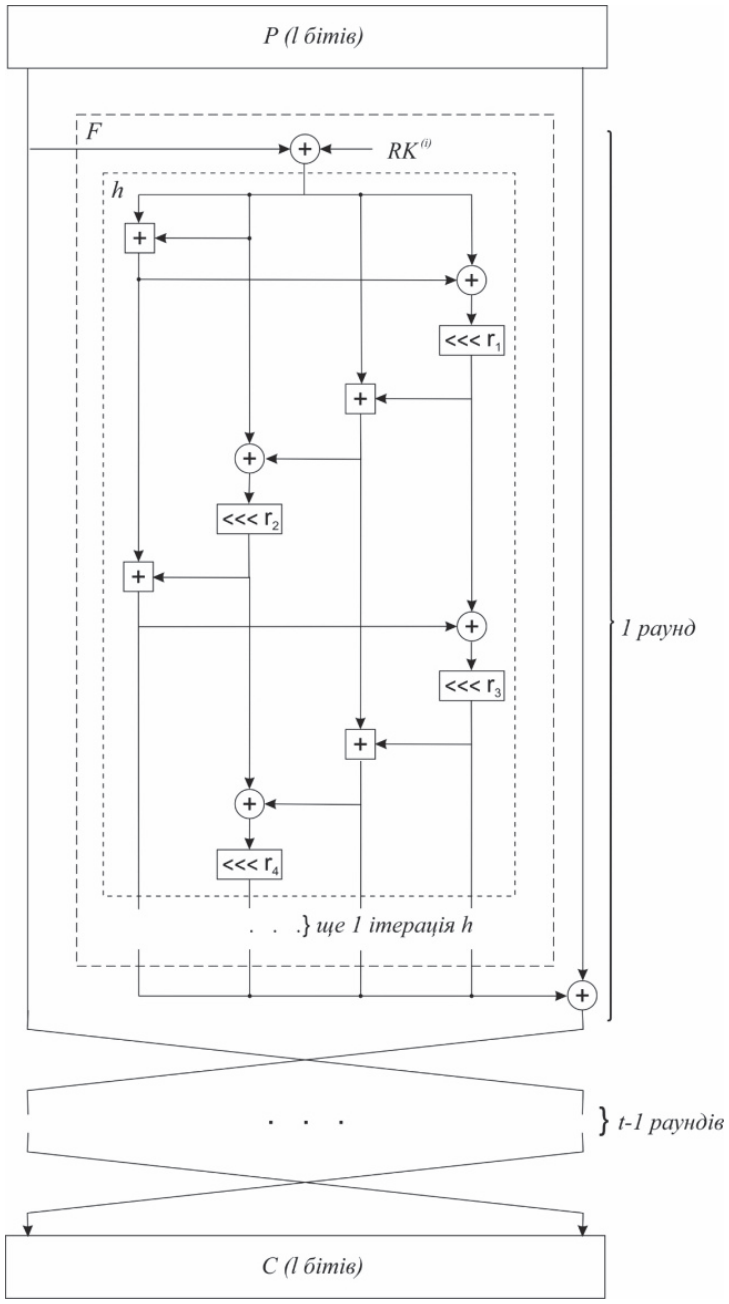


Рис. 1. Функція зашифрування шифру «Кипарис»

4. Математична модель оцінки стійкості блокового шифру «Кипарис» до диференційного криптоаналізу

Нехай $\oplus$ (XOR) є операцією, що визначає різницю між парою текстів, а $\boxplus$ є операцією додавання за модулем 2^s, для якої диференційна ймовірність $\mathrm{xdp}^+ \le 1$. Введемо наступні припущення.

Припущення 1. Блоковий шифр «Кипарис» є марковським шифром, тому:

1) Середня за ключами ймовірність одноциклової ДХ $\mathrm{EDP}^{(1)}(\Omega)$ дорівнює добутку ймовірностей перетворення вхідних різниць на восьми модульних суматорах:

$$\mathrm{EDP}^{(1)}(\Omega) = \prod_{i=1}^{8} \mathrm{xdp}^+(\alpha_i, \beta_i \to \gamma_i), \tag{6}$$

де (α_i, β_i) – різниці на вході *i*-го суматора, γ_i – різниця на виході *i*-го суматора.

2) Середня за ключами ймовірність *r*-циклової ДХ визначається добутком ймовірностей одноциклових ДХ [8].

Нехай $(\Omega_1, \Omega_2, ..., \Omega_r)$ – множина одноциклових ДХ таких, що $\Omega_1 = (\alpha, \beta_1), \Omega_2 = (\beta_1, \beta_2), ..., \Omega_r = (\beta_{r-1}, \beta_r)$ та $\Omega = (\alpha, \beta_1, ..., \beta_r)$. Тоді ймовірність $\mathrm{EDP}^{(r)}(\Omega)$ може бути апроксимована як

$$\mathrm{EDP}^{(r)}(\Omega) = \prod_{i=1}^{r} \mathrm{EDP}^{(1)}(\Omega_i). \tag{7}$$

Припущення 1 витікає із загальноприйнятих припущень, що робляться з метою спрощення отримання оцінок для ARX-шифрів [12, 13].

Припущення 2. При обчисленні вихідної різниці γ, в яку перетворюються вхідні різниці α та β після проходження крізь операцію модульного додавання, обирається вихідна різниця, що має максимальну ймовірність:

$$\gamma = \boxplus(\alpha, \beta), \mathrm{xdp}^+(\alpha, \beta \to \gamma) = \max \Gamma, \tag{8}$$

де Γ – множина усіх можливих вихідних різниць для (α, β).

У багатьох випадках для пари вхідних різниць (α, β) існує декілька вихідних різниць з максимальною ймовірністю. Якщо таких різниць небагато (≈5-10), тоді обчислюються диференційні шляхи для усіх можливих варіантів. У разі, коли значення $\max \Gamma$ є достатньо малим, кількість вихідних різниць з максимальною ймовірністю може бути дуже великою (тисячі та десятки тисяч). Тоді робиться випадкова вибірка (random sampling) з множини різниць, що мають максимальну імовірність, та будуються диференційні шляхи лише для них.

Припущення 3. У високоймовірнісних одноциклових ДХ шифру «Кипарис» вхідні різниці мають малу вагу Хемінга, а саме 3-7 активних бітів (при цьому, активні біти рознесені по різним словам). Таке припущення пояснюється тим, що вхідні різниці найбільш ймовірних переходів в таблиці розподілу різниць для модульного додавання мають малу кількість активних бітів. Обґрунтуємо припущення 3 більш детально.

Означення 2. Кількістю активних біт *b* у різниці (α, β), яка поступає на вхід суматора, називається число одиниць, що міститься у доданку $\alpha \oplus \beta$.

Розглянемо часткову ТРР для додавання за модулем 2^{32}, що містить переходи з ймовірністю $\mathrm{xdp}^+(\alpha, \beta \to \gamma) \ge 1/2$. Для переходів з ймовірністю $\mathrm{xdp}^+(\alpha, \beta \to \gamma) = 1$, яких у ТРР

всього чотири, кількість активних біт у вхідній різниці дорівнює $b \le 1$. Зазначимо, що це справедливо для будь-якого значення n (табл. 2).

Для переходів з ймовірністю $\mathrm{xdp}^+\left(\alpha, \beta \to \gamma\right) = 1/2$ (для $n = 32$ таких всього 744), кількість активних біт у вхідній різниці обмежується двома, $b \le 2$.

У [16] наводиться вираз, що описує зв'язок між позиціями бітів вхідної та вихідної різниць й імовірністю, а саме верхня границя диференційної ймовірності операції модульного додавання визначається як $\Pr\left[\alpha, \beta \to \gamma\right] \le 2^{-k}$, де $k = \#\left\{i : \neg\left(\alpha[i] = \beta[i] = \gamma[i]\right), 0 \le i \le n-2\right\}$, тобто кількість бітових позицій, за виключенням найбільш значущого біта, на яких біти різниць α, β, γ не є рівними.

Таблиця 2

Переходи в TPP для додавання за модулем 2^n з ймовірністю $\mathrm{xdp}^+\left(\alpha, \beta \to \gamma\right) = 1$

№	α	β	γ
1	0	0	0
2	$1\underbrace{0\ldots0}_{n-1}$	0	$1\underbrace{0\ldots0}_{n-1}$
3	0	$1\underbrace{0\ldots0}_{n-1}$	$1\underbrace{0\ldots0}_{n-1}$
4	$1\underbrace{0\ldots0}_{n-1}$	$1\underbrace{0\ldots0}_{n-1}$	0

Таблиця 3

Результати щодо розповсюдження активних бітів для циклової функції блокового шифру «Кипарис»

128-бітова вхідна різниця (1 позначає слово, в якому є активні біти)	Кількість активних бітів на виході циклової функції	
	Нижня границя	Верхня границя
1000	14	14
0100	19	19
0010	7	7
0001	10	10
1100	5	33
0110	12	26
0011	3	17
0101	9	29
1010	7	21
1001	4	24
1110	2	40
1101	5	43
1011	3	21
0111	2	36

Таким чином, мінімізація кількості активних бітів у різниці на вході модульних суматорів підвищує загальну ймовірність ДХ. У шифрі «Кипарис» перші три слова різниці, що подається на вхід циклової функції, попадають на вхід модульного суматора одразу, а четверте – після застосування операцій побітового додавання та циклічного зсуву, тому припущення про малу кількість активних біт на вході циклової функції є цілком обґрунтованим. Враховуючи вплив лінійних операцій на процес розповсюдження активних бітів, припускається, що 1-2 активних біти на вході циклової функції добре розповсюдяться по різним словам на виході. Експерименти показали, що 1 активний біт на вході циклової функції переходить щонайменше у 7 активних бітів на виході (див. табл. 3). У свою чергу, декілька активних бі-

тів у різних словах можуть знищитись за рахунок застосування лінійних операцій. Таким чином, приблизно 3-7 активних бітів на вході циклової функції, які розподілені між різними словами, дозволять отримати високоймовірну ДХ, оскільки забезпечать оптимальне розповсюдження активних бітів для максимізації ймовірності перетворення різниць на суматорах.

5. Методи пошуку багато циклових диференційних характеристик блокового шифру «Кипарис»

Як зазначалось вище, найбільш відомим методом пошуку диференційних характеристик є модифікований метод Мацуї із застосуванням часткових ТРР [12], який добре підходить до шифрів з простими цикловими функціями з невеликим розміром входу, що послідовно обробляється декількома операціями додавання та зсуву. У випадку шифру «Кипарис», де 128/256-бітове вхідне значення циклової функції ділиться на 32/64-бітові слова, які проходять крізь велику кількість операцій додавання, часткова ТРР повинна містити диференціали з достатньо низькою ймовірністю. Крім того, кількість диференційних шляхів зростає з кожним суматором. Все це призводить до того, що обсяг часткової ТРР стає значно великим для обчислення за прийнятний час. Тому вважатимемо, що при побудуванні диференційних характеристик для шифру «Кипарис» краще обчислювати значення ймовірностей на суматорах на льоту, користуючись швидким алгоритмом, запропонованим Ліпмою та Моріарі [17].

У [3] представлено три методи пошуку кращих диференційних характеристик для одного циклу перетворень шифру «Кипарис». Оптимізований метод дозволив знайти одноциклову характеристику, що має ймовірність ¼. У цьому розділі пропонуються методи пошуку багатоциклових диференційних характеристик та результати їх застосування.

5.1. Метод пошуку багатоциклових ДХ, заснований на побудуванні множини високоймовірнісних одноциклових ДХ

Нагадаємо, що пошук диференційних характеристик проводиться з метою знаходження високоймовірнісних диференційних шляхів та підтвердження, що ймовірність найкращої знайденої (r-1)-циклової ДХ $\mathrm{EDP}^{(r-1)}(\Omega) < 2^k$, де k – довжина ключа шифрування. Для виконання цієї задачі, по-перше, пропонується побудувати достатньо велику множину одноциклових ДХ та виконати пошук можливих комбінацій одноциклових ДХ у двоциклові (багатоциклові) ДХ. В загальному вигляді ***метод*** складається з наступних кроків.

1) Згідно з Припущенням 3, сформувати множину вхідних різниць Ξ, для яких буде побудовано одноциклові ДХ. До множини Ξ включити усі можливі комбінації $l/2$ – бітових рядків з вагою Хемінга 1-7 бітів ($l/2$ – довжина напівблока, що подається на вхід циклової функції). Оскільки нас цікавитимуть не лише найбільш ймовірні ДХ, до множини включено й різниці з вагою Хемінга 1-3 бітів.

2) Побудувати одноциклові ДХ для вхідних різниць з множини Ξ. Вихідні різниці після проходження крізь операцію модульного додавання обчислювати згідно з Припущенням 2, а ймовірність одноциклової ДХ $\mathrm{EDP}^{(1)}(\Omega)$ згідно з пунктом 1 Припущення 1. Зазначимо, що для однієї вхідної різниці, як правило, буде існувати декілька ДХ.

3) Враховуючи, що довжина ключа дорівнює k, а кількість циклів шифрування дорівнює t, з усіх обчислених ДХ до множини Ψ включити ДХ, що мають ймовірність $\mathrm{EDP}^{(1)}_{thres}(\Omega) \geq 2^{-k/t}$.

4) Якщо для вхідних різниць з деякою вагою Хемінга обчислення всіх ДХ потребує значних обчислювальних ресурсів, зменшити значення $\mathrm{EDP}^{(1)}_{thres}(\Omega)$ для ДХ, побудованих для вхідних різниць з цією вагою Хемінга.

5) Здійснити пошук комбінацій одноциклових ДХ з множині Ψ у двоциклові (багатоциклові) ДХ.

Запропонований метод був застосований до шифру «Кипарис-256». У зв'язку з обмеженням обчислювальних ресурсів, до множини Ψ були додані ДХ:

- з ймовірністю $\mathrm{EDP}^{(1)}_{thres}(\Omega) \geq 2^{-26}$ для вхідних різниць з вагою Хемінга 1-4 бітів;
- з ймовірністю $\mathrm{EDP}^{(1)}_{thres}(\Omega) \geq 2^{-18}$ для вхідних різниць з вагою Хемінга 5 бітів;
- з ймовірністю $\mathrm{EDP}^{(1)}_{thres}(\Omega) \geq 2^{-10}$ для вхідних різниць з вагою Хемінга 6 бітів.

Результати побудування множини високоймовірнісних одноциклових ДХ наведені в табл. 4.

Таблиця 4

Характеристики множини високоймовірнісних одноциклових ДХ

Вага Хемінга вхідної різниці	$\mathrm{EDP}^{(1)}_{thres}(\Omega), \log_2 n$	$\mathrm{MEDP}^{(1)}(\Omega), \log_2 n$	$\lvert\Psi\rvert$
1	-26	> -26	0
2	-26	-14	2986
3	-26	-12	10357
4	-26	-6	28392
5	-18	-2	1446
6	-10	-3	343

Як і було припущено у математичній моделі (див. Припущення 3), ДХ, побудовані для вхідних різниць з вагою Хемінга 4-6 бітів, мають високу ймовірність. Деякі з отриманих ДХ представлені у табл. 5.

Таблиця 5

Найбільш ймовірні одноциклові диференційні характеристики блокового шифру «Кипарис»

Вхідна різниця у 32-бітових словах, hex	Вихідна різниця у 32-бітових словах, hex	$\mathrm{EDP}^{(1)}(\Omega), \log_2 n$
0 80000000 800000 80008080	80000000 4000 80 80	-2
80000 80080000 80000000 80000000	800 4040040 80080000 80000	-3
0 80000000 1800000 80008080	80000000 4000 80 80	-3
180000 80080000 80000000 80000000	800 4040040 80080000 80000	-4
80000 80000 80800000 8080	80000800 4044040 80080080 80080	-5
80000000 0 80000000 80008000	88000000 40404404 808088 800088	-6
80000000 80000000 80800000 80	8000000 40400404 808008 800008	-6
80 80 80000080 8000	8 40040440 80800800 80000800	-7
8000 8000 8080 800000	800 4044040 80080080 80080	-7
80000000 80000800 800 800	800000 40040040 80000800 80000000	-7
0 80 80000000 808080	80 400000 8000 8000	-7
0 800000 8000 80800080	800000 40 80000000 80000000	-7
80000000 80000000 81800000 80	8000000 40400404 808008 800008	-7
0 100 1 1010100	100 800000 10000 10000	-8
0 200 2 2020200	200 1000000 20000 20000	-8
0 800 8 8080800	800 4000000 80000 80000	-8
0 1000 10 10101000	1000 8000000 100000 100000	-8
0 2000 20 20202000	2000 10000000 200000 200000	-8
0 4000 40 40404000	4000 20000000 400000 400000	-8
0 8000 80 80808000	8000 40000000 800000 800000	-8
180 80 80000080 8000	8 40040440 80800800 80000800	-8
80 80 80000180 8000	8 40040440 80800800 80000800	-8
100 80 80000000 808080	80 400000 8000 8000	-8
80001000 80000800 800 800	800000 40040040 80000800 80000000	-8
8000 8000 8180 800000	800 4044040 80080080 80080	-8
80000000 40000000 400000 40004040	40000000 2000 40 40	-8
0 40 c0000000 404040	40 200000 4000 4000	-8
0 800000 18000 80800080	800000 40 80000000 80000000	-8
0 40000000 80400000 40004040	40000000 2000 40 40	-8

Не дивлячись на те, що деякі ДХ мають вихідну різницю, яка співпадає з вхідною різницею інших ДХ, жодних комбінацій одноциклових ДХ у двоциклові виявлено не було (див. пункт 5 запропонованого методу). Це означає, що отримані ДХ, вихідні різниці яких мають малу вагу Хемінга, не можуть бути продовжені для побудування багатоциклових ДХ з високою ймовірністю.

5.2. Пошук існуючих найбільш ймовірних багатоциклових ДХ та оцінка стійкості блокового шифру «Кипарис-256»

Наступний крок на шляху пошуку багатоциклових ДХ полягає у продовженні одноциклових ДХ з множини Ψ на декілька циклів. Відмітимо, що особливість архітектури мережі Фейстеля дозволяє підбирати вхідну різницю таким чином, щоб «пропустити» один цикл шифрування, тобто створити таку ситуацію, коли на певному циклі на вхід циклової функції подається значення $\Delta X = 0$, ймовірність перетворення якого дорівнює 1. З метою максимізації ймовірності ДХ для перших трьох циклів шифрування, в якості лівої половини різниці пропонується подати значення ΔX, а в якості правої – $\Delta Y = F(\Delta X)$. Завдяки цьому ймовірність ДХ для 1-го та 3-го циклів буде однаковою, а для 2-го – дорівнюватиме 1. Шлях проходження вхідної різниці для чотирьох циклів шифрування зображено на рис. 2.

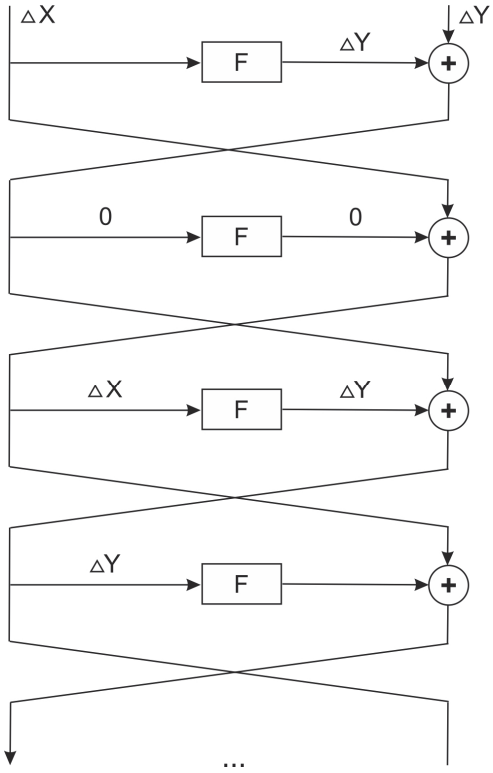


Рис. 2. Шлях проходження вхідної різниці для 4-х циклів шифрування

Пошук найбільш ймовірних багатоциклових ДХ складається з наступних кроків.

1) Визначити l-бітову вхідну різницю як таку, що складається з двох $l/2$ – бітових половин ΔX та ΔY.

2) Сформувати множину Z l-бітових вхідних різниць для пошуку багатоциклових ДХ наступним чином. Визначити вхідну різницю ζ_i з множини Z як $\zeta_i = (\Delta X_i \,|\, \Delta Y_i)$, де ΔX_i та ΔY_i – значення вхідної та вихідної різниць i-ї ДХ з множини Ψ відповідно.

3) Для кожної вхідної різниці ζ_i з множини Z побудувати ДХ для j циклів за умови, що $\mathrm{EDP}^{(j)}(\Omega) > 2^{-256}$. ДХ для кожного циклу будувати згідно пунктів (2) – (4) методу, представленого у розд. 5.1.

У табл. 6 представлені параметри однієї з найбільш ймовірних ДХ, знайденої за допомогою описаного вище методу. Зазначимо, що за рахунок застосування механізму випадкової вибірки 1) при обчисленні значень вихідних різниць для операції модульного додавання та 2) при обранні виходу з циклової функції між циклами шифрування, значення $\mathrm{EDP}^{(j)}(\Omega)$ є апроксимованим (обчислення всіх існуючих диференційних шляхів навіть для одного значення вхідної різниці є обчислювально складною задачею).

Таблиця 6

Параметри однієї з найбільш ймовірних знайдених багатоциклових ДХ для блокового шифру «Кипарис»

Номер циклу, j	ДХ $\Omega(a,b)$ для j-го циклу, hex	$\mathrm{EDP}^{(1)}(\Omega), \log_2 n$	$\mathrm{EDP}^{(j)}(\Omega), \log_2 n$
1	a = (00000000 80008000 00800080 00800080 80008000 40004000 00800080 00800080), b = (00000000 80008000 00800080 00800080 00000000 00000000 00000000 00000000)	-10	-10
2	a = (00000000 00000000 00000000 00000000 00000000 80008000 00800080 00800080), b = (00000000 00000000 00000000 00000000 00000000 80008000 00800080 00800080)	0	-10
3	a = (00000000 80008000 00800080 00800080 00000000 00000000 00000000 00000000), b = (00000000 80008000 00800080 00800080 80008000 40004000 00800080 00800080)	-10	-20
4	a = (80008000 40004000 00800080 00800080 00000000 80008000 00800080 00800080), b = (80008000 40004000 00800080 00800080 c0204020 90009000 00a000a0 00800080)	-27	-47
5	a = (c0204020 90009000 00a000a0 00800080 80008000 40004000 00800080 00800080), b = (c0204020 90009000 00a000a0 00800080 5208d204 40444044 08820882 0a800a80)	-74	-121
6	a = (5208d204 40444044 08820882 0a800a80 c0204020 90009000 00a000a0 00800080), b = (5208d204 40444044 08820882 0a800a80 266e7071 a74313f2 0088e7e0 10fa6fd2)	-102	-223

Таким чином, знайдена найбільш ймовірна ДХ для шести циклів шифрування має ймовірність

$$\mathrm{MEDP}^{(6)}(\Omega) \approx 2^{-223}.$$

Отримане значення $\mathrm{MEDP}^{(6)}(\Omega)$ будемо називати практичною стійкістю блокового шифру «Кипарис» до диференційного криптоаналізу. Через застосування механізму випадкової вибірки, значення $\mathrm{MEDP}^{(6)}(\Omega)$ може дещо відрізнятися у різних експериментах, проте це суттєво не впливає на загальний результат оцінки, оскільки

$$\mathrm{MEDP}^{(7)}(\Omega) << 2^{-256}, 7 < (r-1).$$

Таким чином, блоковий шифр «Кипарис-256» є практично стійким до диференційного криптоаналізу.

Висновки

1. Найбільшу ймовірність мають одноциклові диференційні характеристики блокового шифру «Кипарис», вхідна різниця яких містить приблизно 3 – 7 активних бітів, які розподілені між різними словами. Це пояснюється оптимальним розповсюдження активних бітів, що призводить до максимізації ймовірності перетворення різниць на суматорах.

2. Застосування запропонованого методу пошуку багатоциклових диференційних характеристик, заснованого на побудуванні множини високоймовірнісних одноциклових диференційних характеристик, до блокового шифру «Кипарис-256» показало, що побудовані одноциклові ДХ, вихідні різниці яких мають малу вагу Хемінга (а значить і достатньо високу ймовірність), не можуть бути продовжені для побудування багатоциклових ДХ з високою ймовірністю.

3. Одна зі знайдених найбільш ймовірних багатоциклових диференційних характеристик для блокового шифру «Кипарис-256» може бути побудована лише для шести циклів шифрування з ймовірністю $\mathrm{MEDP}^{(6)}(\Omega) \approx 2^{-223}$, що дає підстави стверджувати, що блоковий шифр «Кипарис-256» є практично стійким до диференційного криптоаналізу.

Список літератури:

1. Lightweight Cryptography. Project Overview. URL: https://csrc.nist.gov/projects/lightweight-cryptography.

2. Родінко М.Ю., Олійников Р.В. Постквантовий малоресурсний симетричний блоковий шифр «Кипарис» // Радіотехніка. – 2017. – Вип. 189. – С. 100-107.

3. Родінко М.Ю., Олійников Р.В. Методи пошуку диференційних характеристик циклової функції симетричного блокового шифру «Кипарис» // Радіотехніка. – 2017. – Вип. 191. – С. 47-51.

4. Biham, E. Differential Cryptanalysis of DES-like Cryptosystem / E. Biham, A. Shamir // Journal of Cryptology. – 1991. – Vol. 4. – P. 3-72.

5. Bernstein D. J. ChaCha, a Variant of Salsa // Workshop Record of SASC: The State of the Art of Stream Ciphers.

6. Beaulieu R. et al. The SIMON and SPECK lightweight block ciphers // Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE. – IEEE, 2015. – С. 1-6.

7. Wheeler D. J. and Needham R. M. TEA, a Tiny Encryption Algorithm // International Workshop on Fast Software Encryption, Springer, Heidelberg, 1995. – P. 363–366.

8. Lai X., Massey J. L. and Murphy S. Markov ciphers and differential cryptanalysis // Workshop on the Theory and Application of of Cryptographic Techniques, Springer, Berlin, Heidelberg, 1991. – P. 17-38.

9. Canteaut, Anne, and Joëlle Roué. Differential Attacks Against SPN: A Thorough Analysis // International Conference on Codes, Cryptology, and Information Security. Springer, Cham, 2015.

10. Kanda M., Takashima Y., Matsumoto T., Aoki K., Otha K. A strategy for constructing fast round functions with practical security against differential differential and linear cryptanalysis // Selected Areas in Cryptography. – SAC 1998, Proceedings. – Springer Verlag, 1999. – P. 264 – 279.

11. Daemen, Joan, and Vincent Rijmen. The wide trail design strategy // IMA International Conference on Cryptography and Coding. Springer, Berlin, Heidelberg, 2001.

12. Biryukov A., Velichkov V. Automatic Search for Differential Trails in ARX Ciphers // CT-RSA. – 2014. – Т. 8366. – С. 227-250.

13. Mouha, Nicky and Bart Preneel. Towards finding optimal differential characteristics for ARX: Application to Salsa20. Cryptology ePrint Archive, Report 2013/328, 2013.

14. Dinu D. et al. SPARX: A Family of ARX-based Lightweight Block Ciphers Provably Secure Against Linear and Differential Attacks // Proceedings of ASIACRYPT'16. – P. 1-21, 2016.

15. Aumasson J. P. et al. New features of Latin dances: analysis of Salsa ChaCha and Rumba // Lecture Notes in Computer Science. – 2008. – Vol. 5086. – P. 470-488.

16. Lipmaa, Helger, Johan Wallén, and Philippe Dumas. On the additive differential probability of exclusive-or. // International Workshop on Fast Software Encryption. Springer, Berlin, Heidelberg, 2004.

17. Lipmaa H. and Moriai S. Efficient algorithms for computing differential properties of addition // International Workshop on Fast Software Encryption, Springer, Berlin, Heidelberg, 2001. – P. 336-350.

Харківський національний
університет імені В.Н. Каразіна

Надійшла до редколегії 25.10.2018

УДК 004.056.5

А.А. КУЗНЕЦОВ, д-р техн. наук, А.В. ПОТИЙ, д-р техн. наук,
Н.А. ПОЛУЯНЕНКО, канд. техн. наук, И.В. СТЕЛЬНИК

НЕЛИНЕЙНЫЕ ФУНКЦИИ УСЛОЖНЕНИЯ ДЛЯ ПОТОКОВЫХ СИММЕТРИЧНЫХ ШИФРОВ

Введение

Анализ современных схем потокового шифрования, таких как SNOW 2.0 0, Decim 0 KCipher-2 0, Sosemanuk 0, Grain 0, MICKEY 2.0 0, Trivium 0 показывает, что основными компонентами являются итеративные генераторы битового потока и функция усложнения, формирующая из некоторых комбинаций битов внутреннего состояния выходной блок.

Итеративные генераторы битового потока, как правило, строятся на основе регистров сдвига с линейными обратными связями (РСЛОС), основная задача которых гарантировать неповторимость внутреннего состояния генератора достаточно большой промежуток времени его работы и гарантировать, что обеспечены хорошие локальные статистические свойства. Данным требованиям отвечают регистры, формирующие последовательность де Брейна. Однако данную последовательность можно генерировать также и регистрами сдвига с нелинейными обратными связями (РСНОС). Применение в качестве итеративных генераторов РСНОС позволяют сохранить все достоинства использования РСЛОС, но при этом генераторы лишены главного недостатка РСЛОС – линейности.

Вместе с тем, при проектировании криптографических систем с применением РСНОС появляются новые проблемные вопросы, связанные с выбором нелинейного регистра. Теория РСЛОС достаточно хорошо изучена 0, РСНОС изучены намного меньше, чем РСЛОС 0. Первый алгоритм для построения наименьшего РСНОС заданной, двоичной последовательностью был представлен Янсеном (Jansen) в 1991 году 0, 0. Альтернативные алгоритмы были даны 0].

Известно, как построить РСЛОС с максимальным периодом, их функции обратной связи соответствуют примитивному многочлену над F_2. В общем случае неизвестно, как построить все РСНОС с максимальным периодом. Основной метод заключается в поиске таких регистров с соответствующими свойствами. Как правило, все приведенные в литературе регистры с нелинейной обратной связью имеют достаточно сложную структуру и состоят не из одного структурного элемента. Если же РСНОС имеет простую структуру, то он является регистром малого размера.

Отсутствуют какие-либо общие методы проектирования РСНОС максимального периода [8, 15]. Построение специального класса РСНОС с максимальным периодом было дано Миккелвайтом (Mykkeltveit) и др. [16]. В работе Е. Дубровой (E. Dubrova) [15] приведен пример сдвига регистра Галуа размером $L = 100$ ячеек, который генерирует последовательность с максимальным периодом, но эта последовательность не обладает свойством последовательности де Брейна, то есть некоторые кортежи битов появляются более одного раза в последовательности.

При этом с увеличением размера используемого регистра, возрастает его конструктивная сложность. Если удается сформировать РСНОС формирующий последовательность де Брейна необходимого размера, то его структура будет настолько сложной, что его реализация в системах шифрования, в качестве итеративного генератора, будет недопустимо ресурсоемкой.

Сложность конструкции напрямую связана с размерами и стоимостью аппаратной реализации шифра, который ее использует, а также в большинстве случаев влияет на его быстродействие. Чем меньше конструктивная сложность функции, тем проще ее схемная реализация. Особенно это актуально для так называемой легковесной (или малоресурсной) криптографии.

С другой стороны, если изначально производить поиск РСНОС с заданными конструктивными особенностями, в частности – простота реализации, то найденный регистр может иметь уязвимости к определенным типам атак, для нейтрализации которых необходимо вводить в алгоритм дополнительные узлы и, как следствие, увеличивать общую ресурсоемкость всей схемы.

Возникает вопрос о возможности оптимизации структуры РСНОС между простотой аппаратной/программной реализации и соответствием некоторым заданным свойствам формируемой последовательности. Под простотой реализации будем понимать число операций, необходимое и достаточное для вычисления следующего состояния итеративного генератора.

Приведенные в работе результаты отражают взаимосвязь конструктивных характеристик РСНОС (таких как максимальная алгебраическая степень, количество мономов) и некоторых необходимых криптографических свойств формируемой им последовательности (автокорреляции и линейной сложности).

1. Полученные результаты

1.1. Булевы функции

Для дальнейшего изложения приведем некоторые определения, которыми будем пользоваться в работе:

F_2 – конечное поле из двух элементов, 0 и 1. Операции в F_2 – умножение и сложение по модулю 2;

V_L L – мерное векторное пространство над полем F_2, $V_L = (F_2)^L$. Сложение в пространстве V_L побитовое по модулю 2.

Булева функция от L переменных есть отображение из V_L в F_2. Расширенные булевы функции – отображения из V_L в Z (множество целых чисел). Еще более общие псевдобулевы функции – отображения из V_L в R (множество действительных чисел).

Число векторов пространства V_L равно 2^L как число всевозможных комбинаций L базисных векторов с коэффициентами 0 и 1.

Пусть $Z_2 = \{0,1\}$. Через $Z_2^{\,L}$ будем обозначать множество всех двоичных векторов $x = (x_1, \ldots, x_L)$ длины L. Будем считать, что все векторы лексикографически упорядочены.

Произвольная функция отображения из множества $Z_2^{\,L}$ в множество Z_2 называется *булевой функцией от L переменных*.

Каждую булеву функцию от L переменных можно однозначно определить вектором ее значений длины 2^L. Например, функциям f и g соответствуют векторы (1001) и (00010110). Пусть далее f обозначает вектор значений длины 2^L функции f. Будем считать, что аргументы функции (т.е. векторы длины L) перебираются в лексикографическом порядке.

Пусть $\oplus$ обозначает сложение по модулю 2 (операцию XOR). Известно, что каждая булева функция однозначно может быть задана своей *алгебраической нормальной формой* (АНФ), в отечественной литературе АНФ также называют полиномом Жегалкина.

АНФ есть выражение булевой функции в виде

$$f(x_1, \ldots x_L) = \bigoplus_{N \in P\{1,2,\ldots,L\}} a_N \prod_{i \in N} x_i \ , \qquad (1)$$

где $P\{1,2,\ldots L\}$ – множество всех подмножеств $\{1,2,\ldots L\}$ (булеан), $a_N \in F_2$.

Для вычисления АНФ заданной функции имеются несложные алгоритмы (см., например, 0).

Степень монома (булевый одночлен) $x^N = \prod_{i \in N} x_i$ определяется как $|N|$ (число элементов подмножества N).

Алгебраической степенью $\deg(f)$ или *порядком нелинейности* булевой функции f называется число переменных в самом длинном слагаемом (мономе) ее АНФ. Булева функция степени 1 называется *аффинной*. Ее АНФ имеет вид $f(x) = a_1 x_1 \oplus a_2 x_2 \oplus \cdots \oplus a_L x_L \oplus b =$

$= \langle a, x \rangle \oplus b$, где $b \in F_2, a \in V_L$. Функция называется квадратичной, кубической и т.д., если ее алгебраическая степень равна соответственно 2, 3 и т.д.

1.2. Последовательность де Брейна

Пусть $A = a_1, a_2, \ldots, a_{2^L-1}, a_{2^L}$ последовательность длины 2^L из элементов алфавита $\{0,1\}$.

A называется *последовательностью де Брейна* порядка L, если среди всех кортежей длины L: $L\,(a_1, a_2, \ldots, a_L)$, $(a_2, a_3, \ldots, a_{L+1})$, …, $(a_{2^L-L+1}, a_{2^L-L+2}, \ldots, a_{2^L})$, каждый из возможных кортежей присутствует и встречается ровно один раз, т.е. встречаются всевозможные 2^L комбинации над алфавитом $\{0,1\}$ 0.

Аналогичные последовательности длины $2^L - 1$ без кортежа из одних нулей называются *модифицированными последовательностями де Брейна*.

Легко заметить, что из последовательности де Брейна можно получить модифицированную последовательность де Брейна вычеркиванием одного нуля, а из модифицированной последовательности де Брейна – последовательность де Брейна добавлением одного нуля.

Аналогичные последовательности можно построить для алфавита из k элементов. Например, 0011 и 002212011 являются последовательностями де Брейна порядка $L = 2$ над алфавитами $\{0,1\}$ и $\{0,1,2\}$ соответственно. Последовательности де Брейна используются в криптографии в силу своих хороших статистических свойств – не отличимых, в статистическом смысле, от истинно случайных последовательностей.

В 1894 г. С. Флай Санте Марие 0 и в 1946 г. де Брейн 0 доказали существование таких последовательностей для любого натурального числа L, над любым алфавитом из k-элементов и показали, что число различных последовательностей (B_n)

$$B_n = \left[(k-1)!\right]^{k^{L-1}} k^{k^{L-1}-L} \tag{2}$$

(две последовательности считаются различными, если любую из них невозможно получить циклическим сдвигом другой). Для случая булевых функций, т.е. $k = 2$, выражение (2) примет вид

$$B_n = 2^{2^{L-1}-L} \tag{3}$$

Для оценки полученных результатов в табл. 1 приведены количественные значения числа различных последовательностей де Брейна полученных в соответствии с выражением (2).

$$B_n = \left[(k-1)!\right]^{k^{L-1}} k^{k^{L-1}-L}.$$

Как видим, уже при $L = 7$ и $k = 2$ количество различных последовательностей де Брейна приобретает размер затрудняющий обработку (поиск, хранение, анализ) всего множества.

Добавим, что число примитивных полиномов степени L равно

$$\frac{\varphi\left(2^L - 1\right)}{L}, \tag{4}$$

где φ – функция Эйлера.

Таблица 1

Число различных последовательностей де Брейна при заданных L и k

L	k		
	2	3	4
2	1	24	20 736
3	2	373 248	$\approx 1.8 \cdot 10^{20}$
4	16	$\approx 1.2 \cdot 10^{19}$	$\approx 8.4 \cdot 10^{85}$
5	2 048	$\approx 4.4 \cdot 10^{60}$	$\approx 2.1 \cdot 10^{350}$
6	67 108 864	$\approx 1.7 \cdot 10^{186}$	$\approx 5.3 \cdot 10^{1409}$
7	2^{57}	$\approx 1 \cdot 10^{1698}$	$\approx 1.4 \cdot 10^{5649}$
8	2^{120}	$\approx 1 \cdot 10^{1698}$	$6^{16384} \cdot 4^{16376}$
9	2^{247}	$\approx 1.4 \cdot 10^{5101}$	$6^{65536} \cdot 4^{65527}$

Обзор 0 дает наиболее полный экскурс в теорию последовательностей де Брейна и историю их использования для решения различных задач.

М-РСНОС будем называть те РСНОС, которые реализуют булевы функции, формирующие модифицированные последовательности де Брейна. Если же эти функции являются линейными – то соответствующие регистры будем назвать М-РСЛОС. В общем случае М-РСЛОС являются частным случаем М-РСНОС.

Период последовательности де Брейна $(T_{ПБ})$ определяется размером алфавита или, как его еще называют, основанием последовательности де Брейна k, а также разрядностью состояний (числом ячеек памяти итеративного генератора) – L:

$$T_{ПБ} = k^L. \tag{5}$$

И, соответственно, период модифицированной последовательности де Брейна (T) будет определен как

$$T = k^L - 1. \tag{6}$$

1.3. Максимальная алгебраическая степень АНФ последовательностей де Брейна

Максимальная алгебраическая степень АНФ для М-РСНОС при $k = 2$ определяется как

$$\deg(f) \le L - 2 \text{ (для } L > 2). \tag{7}$$

Данное утверждение было описано еще Голомбом в работе 0.

Нами были получено распределение числа модифицированных последовательностей де Брейна в зависимости от порядка нелинейности формирующего данную последовательность М-РСНОС или, что равносильно, от максимальной алгебраической степени АНФ формирующего полинома. Полученное распределение для $k = 2$ приведено в табл. 2.

Таблица 2

Распределения числа М-РСНОС в зависимости от порядка нелинейности $\deg(f)$ для $k = 2$.

	Количество М-РСЛОС	Количество М-РСНОС 2-го порядка	Количество М-РСНОС 3-го порядка	Количество М-РСНОС 4-го порядка
2	1	–	–	–
3	2	–	–	–
4	2	14	–	–
5	6	122	1 920	–
6	6	1 946	2 095 200	65 011 712
7	18	64 038	*неизвестно*	*неизвестно*
8	16	4 017 982	*неизвестно*	*неизвестно*
9	48	519 239 746	*неизвестно*	*неизвестно*

Отметим, что с увеличением алгебраической степени АНФ экспоненциально увеличивается число полиномов, формирующих модифицированные последовательности де Брейна, а следовательно, и вероятность того, что произвольным образом выбранный М-РСНОС будет иметь более алгебраическую степень.

1.4 Количество мономов АНФ М-РСНОС

Пусть τ – число мономов в рекуррентном соотношении определяющая обратную связь в РСНОС. Для всех М-РСНОС τ – четное число. Распределение общего количества мономов в зависимости от τ для $4 \le L \le 6$ опубликовано в 0. Также в 0 доказано, что минимальное количество мономов в полиноме соответствует 2 (достигается только для М-РСЛОС), а максимальное вычисляется соотношением $2^{L-1}-2$ (кроме $L=2$). Распределение имеет гауссовский характер.

Нами получено и приведено в табл. 3 аналогичное распределение, учитывающее $\deg(f)$.

Таблица 3

Распределение количества мономов АНФ М-РСНОС
в зависимости от порядка нелинейности для $k=2$

τ	Количество о М-РСЛОС	Количество М-РСНОС 2-го порядка	Количество о М-РСНОС 3-го порядка	Количество М-РСНОС 4-го порядка
$L=2$				
1	1	–	–	–
$L=3$				
2	2	–	–	–
$L=4$				
2	2	–	–	–
4	–	10	–	–
6	–	4	–	–
$L=5$				
2	2	–	–	–
4	4	26	66	–
6	–	66	426	–
8	–	26	858	–
10	–	4	490	–
12	–	–	76	–
14	–	–	4	–
$L=6$				
2	2	–	–	–
4	4	42	94	106
6	–	312	4 414	6 512
8	–	782	50 380	147 042
10	–	596	239 916	1 322 050
12	–	192	553 804	5 890 004
14	–	22	658 398	14 115 280
16	–	–	420 692	19 139 124
18	–	–	141 894	15 146 272
20	–	–	23 808	7 057 286
22	–	–	1 742	1 892 112
24	–	–	58	274 994
26	–	–	–	20 294
28	–	–	–	628
30	–	–	–	8

Исходя из принципов комбинаторики можно показать, что количество возможных обратных связей для РСНОС размерностью в L ячеек и порядком нелинейности $\deg(f)$ определяется соотношением

$$n_L^{\deg(f)} = L \cdot \left(1 + \sum_{i=1}^{\deg(f)-1} \frac{\prod_{j=1}^{i} (L-j)}{(1+i)!} \right). \quad (8)$$

Как видим из табл. 4, количество мономов для изученных М-РСНОС лежит в диапазоне $2 \le \tau \le \frac{2}{3} n_L^{\deg(f)}$, а пик распределения приблизительно соответствует $\frac{1}{3} n_L^{\deg(f)}$.

1.5. Автокорреляционная функция

Пусть $S = (s(1), s(1), s(3), \ldots)$– периодическая последовательность с периодом T. *Автокорреляционная функция* (АКФ) S является целочисленной функцией:

$$AC(t) = \frac{1}{T} \sum_{t=1}^{T} (2s(i)-1)(2s(i+t)-1), \quad (9)$$

для $0 \le t \le T-1$

Для примера на рис. 1 показана АКФ М-РСЛОС при $L=4$ и $T=15$, определяемая рекуррентным соотношением $s_{(5+t)} = s_{(4+t)} + s_{(1+t)}$, а на рис. 2 – АКФ М-РСНОС при $L=4$, определяемая рекуррентным соотношением $s_{(5+t)} = s_{(4+t)} + s_{(3+t)} + s_{(2+t)} +$

$+ s_{(1+t)} + s_{(4+t)} \cdot s_{(2+t)} + s_{(3+t)} \cdot s_{(2+t)}$.

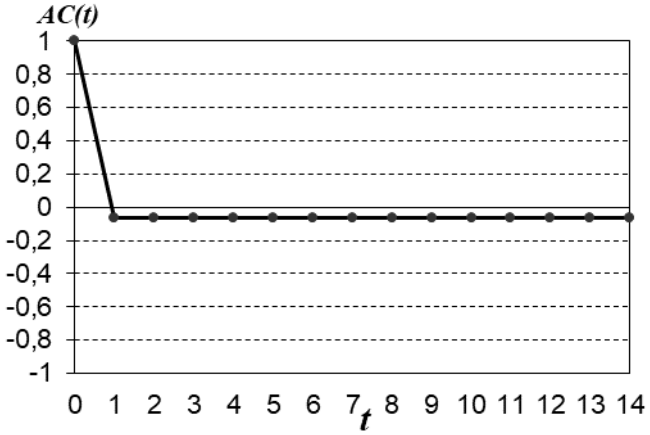


Рис. 1. АКФ для М-РСЛОС при $L=4$

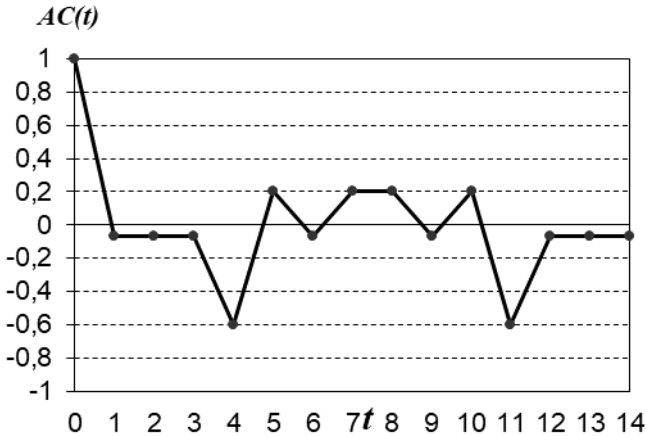


Рис. 2. АКФ для М-РСНОС при $L=4$

Анализируя полученные результаты, можно утверждать, что все АКФ имеют симметричный вид относительно середины графика (не включая нулевое значение, соответствующее отсутствию сдвижки); только М-РСЛОС имеют постоянную и минимальную корреляцию со своими сдвинутыми копиями последовательности.

Кроме того, значение АКФ значительно меняется в зависимости от выбранного М-РСНОС при формировании результирующей последовательности. С практической точки зрения понятно, что чем меньше коррелирует последовательность со своей же сдвинутой копией, тем менее она подвержена атакам, использующим данную уязвимость. Причем важно, чтобы не было корреляции при любой сдвижке.

Введем значение АКФ, которое будет характеризовать ее максимальное значение (взятое по модулю) для всех $1 \le t \le T-1$, обозначим как $AC_{\max}$. Значение $AC_{\max}$ ограничено снизу выражением $AC_{\max} \ge 1/T$, достигаемое только при использовании в качестве функций обратных связей М-РСЛОС.

Обобщенные результаты для значения $AC_{\max}$ приведены в табл. 4 – 7.

Таблица 4

Распределение максимального значения АКФ для $L = 3 (T = 7)$

$AC_{\max}$	Количество М-РСНОС	Количество М-РСЛОС
$1/T = 0.14286$	**2**	2

Таблица 5

Распределение максимального значения АКФ для $L = 4 (T = 15)$

$AC_{\max}$	Кол-во М-РСНОС	Кол-во М-РСЛОС	Кол-во М-РСНОС 2-го порядка
$1/T = 0.06667$	**2**	2	–
$5/T = 0.33333$	**10**	–	10
$9/T = 0.60000$	**4**	–	4

Таблица 6

Распределение максимального значения АКФ для $L = 5 (T = 31)$

$AC_{\max}$	Кол-во М-РСНОС	Кол-во М-РСНОС 2-го порядка	Кол-во М-РСНОС 3-го порядка
$1/T = 0.03226$	**6**	–	–
$5/T = 0.16129$		–	56
$7/T = 0.22581$	**154**	8	146
$9/T = 0.29032$	**1156**	78	1078
$11/T = 0.35484$	**170**	12	158
$13/T = 0.41935$	**382**	14	368
$15/T = 0.48387$	**8**	–	8
$17/T = 0.54839$	**110**	10	100
$21/T = 0.67742$	**6**	–	6

Таблица 7

Распределение максимального значения АКФ для $L = 6 (T = 63)$

$AC_{\max}$	Кол-во М-РСНОС 2-го порядка	Кол-во М-РСНОС 3-го порядка	Кол-во М-РСНОС 4-го порядка
$5/T = 0.07937$	–	–	12
$7/T = 0.11111$	–	10	468
$9/T = 0.14286$	10	12 772	391 484
$11/T = 0.17460$	44	49 556	1 534 900
$13/T = 0.20635$	212	351 690	10 906 882
$15/T = 0.23810$	222	274 756	8 522 742
$17/T = 0.26984$	920	766 838	23 851 328
$19/T = 0.30159$	128	167 810	5 202 124
$21/T = 0.33333$	242	269 832	8 344 838
$23/T = 0.36508$	32	30 922	955 434
$25/T = 0.39683$	70	143 930	4 450 510
$27/T = 0.42857$	4	3 336	100 228
$29/T = 0.46032$	12	10 684	346 834
$31/T = 0.49206$	–	174	5 480
$33/T = 0.52381$	50	12 216	377 528
$35/T = 0.55556$	–	8	116
$37/T = 0.58730$	–	140	4 656
$41/T = 0.65079$	–	526	16 146
$45/T = 0.71429$	–	–	2

Как видим, изученные последовательности, сформированные нелинейными регистрами, уступают по характеристикам АКФ последовательностям, сформированным линейными регистрами. Лучшее значение для изученных М-РСНОС соответствует $AC_{\max} = 5/T$ и достигается при наличии максимального порядка нелинейности.

Характер распределения примерно одинаков для любого порядка нелинейности.

1.6. Линейная сложность

Линейная сложность (Li) псевдослучайной последовательности – самый короткий регистр сдвига, с помощью которого формируется данная периодическая последовательность, при условии, что первые Li значений последовательности являются начальными заполнениями регистра.

Оценка линейной сложности является одним из основных параметров системы. Любая последовательность, которую можно сгенерировать автоматом (линейным или нелинейным) над конечным полем, имеет конечную линейную сложность. Таким образом, можно построить алгоритм, с помощью которого определяется линейная сложность любой последовательности, независимо от способа ее генерации, при этом знание структуры схемы, формирующей исходную последовательность, является лишним.

Для вычисления линейной сложности наиболее распространенным является алгоритм Берлекэмпа – Месси, суть которого изложена в 0, 0.Таким образом, большая линейная сложность формируемой последовательности является необходимым (но недостаточным) условием практической стойкости генераторов псевдослучайных последовательностей.

В идеале линейная сложность должна быть близкой или равной периоду последовательности. Линейная сложность была получена еще Golomb в работе 0.

М-РСНОС имеют в большинстве случаев максимальную линейную сложность $Li_{\max} = 2^L - 2$ или близкую к ней. Нами получены и приведены результаты распределения линейной сложности с учетом порядка нелинейности.

В табл. 8 – 10 приведено распределение линейной сложности для всего множества полиномов, формирующих последовательность де Брейна размерностью $L = 2,\ldots,6$, а также дано распределение в зависимости от порядка нелинейности формирующего последовательность регистра. В табл. 11 – 13 приведено распределение линейной сложности для М-РСЛОС и М-РСНОС 2-го порядка при $7 \le L \le 9$.

Таблица 8

Распределение линейной сложности последовательностей де Брейна для $L = 4$

Li	Кол-во М-РСНОС	Кол-во М-РСЛОС	Кол-во М-РСНОС 2-го порядка
4	**2**	6	–
12	**4**	–	4
14	**10**	–	10

Таблица 9

Распределение линейной сложности последовательностей де Брейна для $L = 5$

Li	Кол-во М-РСНОС	Кол-во М-РСЛОС	Кол-во М-РСНОС 2-го порядка	Кол-во М-РСНОС 3-го порядка
5	**6**	6	–	–
15	**10**	–	–	10
20	**4**	–	–	4
25	**306**	–	20	286
30	**1 722**		102	1620

Таблица 10

Распределение линейной сложности последовательностей де Брейна для $L = 6$

Li	Кол-во М-РСНОС	Кол-во М-РСНОС 2-го порядка	Кол-во М-РСНОС 3-го порядка	Кол-во М-РСНОС 4-го порядка
6	**6**	–	–	–
27	**10**	–	–	10
30	**8**	–	–	8
32	**12**	–	–	12
33	**8**	–	–	8
35	**62**	–	–	62
36	**152**	–	10	142
38	**478**	–	14	464
39	**1 036**	–	48	988
41	**3 572**	–	106	3 466
42	**6 100**	–	200	5 900
44	**17 240**	–	536	16 704
45	**28 702**	4	936	27 762
47	**86 056**	–	2 650	83 406
48	**134 290**	4	4 184	130 102
50	**401 102**	8	12 692	388 402

51	**453 734**	20	14 184	439 530
53	**1 364 978**	48	43 184	1 321 746
54	**1 819 148**	68	56 930	1 762 150
56	**5 453 680**	158	171 298	5 282 224
57	**3 190 982**	126	100 724	3 090 132
59	**9 557 084**	256	297 988	9 258 840
60	**11 148 860**	338	347 518	10 801 004
62	**33 441 564**	916	1 041 998	32 398 650

Таблица 11

Распределение линейной сложности последовательностей де Брейна для М-РСНОС с $\deg(f) \le 2$ при $L = 7$

Li	Количество М-РСЛОС	Количество М-РСНОС 2-го порядка
7	18	–
105	–	22
112	–	594
119	–	8 044
126	–	55 378

Таблица 12

Распределение линейной сложности последовательностей де Брейна для М-РСНОС с $\deg(f \le 2)$ при $L = 8$

Li	Количество М-РСЛОС	Количество М-РСНОС 2-го порядка
8	16	–
208	–	2
214	–	2
218	–	2
220	–	6
222	–	18
224	–	26
226	–	96
228	–	204
230	–	726
232	–	1 020
234	–	2 914
236	–	5 954
238	–	18 168
240	–	17 578
242	–	52 538
244	–	96 554
246	–	289 222
248	–	147 584
250	–	440 762
252	–	738 236
254	–	2 206 370

Таблица 13

Распределение линейной сложности последовательностей де Брейна для М-РСНОС с $\deg(f) \le 2$ при $L = 9$

Li	Количество М-РСЛОС	Количество М-РСНОС 2-го порядка
9	48	
456	–	2
459	–	2
462	–	6
465	–	34
468	–	30
471	–	504
474	–	1 866
477	–	1 386
480	–	21 112
483	–	74 458
486	–	42 542
489	–	599 644
492	–	2 097 832
495	–	795 706
498	–	11 163 082
501	–	39 051 092
504	–	7 268 192
507	–	101 824 464
510	–	356 297 792

Как видим из полученных результатов, подавляющая часть М-РСНОС имеет максимальную или отличающуюся на несколько единиц от максимальной линейной сложности. Характер распределения сохраняется для любого значения $\deg(f)$.

Профиль линейной сложности изученных последовательностей близок к математическому ожиданию линейной сложности, как и для истинно случайной последовательности.

Выводы

Булевы функции, формирующие последовательность де Брейна, привлекательны в качестве итеративных генераторов в потоковых шифрах в силу своих хороших локальных статистических характеристик, максимального периода формируемой последовательности и простоты реализации.

Использование нелинейности в булевых функциях влечет увеличение конструктивных характеристик.

Так, большинство М-РСНОС имеет в своей структуре количество мономов равное 1/3 от максимального значения. К примеру, для $L = 32$ большинство М-РСНОС будет иметь порядка 10^9 слагаемых, а каждое слагаемое будет содержать произведение до 30 различных значений, что, с точки зрения практической реализации, для систем потокового шифрования неприемлемо. Однако, как показано в работе, имеются М-РСНОС с минимальным количеством коэффициентов обратной связи.

Изученные последовательности, сформированные нелинейными регистрами, уступают по характеристикам АКФ последовательностям, сформированными линейными регистрами.

Лучшее значение для изученных М-РСНОС соответствует $AC_{\max} = 5/T$ (для М-РСЛОС все $AC_{\max} = 1/T$) и достигается при наличии максимального порядка нелинейности. Характер распределения примерно одинаков для любого порядка нелинейности. Однако, учитывая относительно равномерное распределение $AC_{\max}$, можно предположить, что произвольно

взятая булева функция, формирующая последовательность де Брейна, будет иметь невысокий показатель $AC_{\max}$.

В отличие от М-РСЛОС подавляющая часть М-РСНОС с $\deg(f) \geq 2$ имеет максимальную или отличающуюся на несколько единиц от максимальной линейную сложность $Li_{\max} = 2^L - 2$. Характер распределения сохраняется для любого значения $\deg(f) \leq 2$. При этом профиль линейной сложности близок к математически ожидаемому, как и для истинно случайных последовательностей.

Таким образом, поиск конструктивно простых РСНОС, формирующих последовательность де Брейна, а также оптимизация структуры для соответствия необходимым криптографическим свойствам, является сложной задачей, требующей дальнейшего изучения.

Список литературы:

1. Marcus Schafheutle. A First Report on the Stream Cipher SNOW. http://www.cryptonessie.org

2. C. Berbain, O. Billet, A. Canteaut, N. Courtois, B. Debraize, H. Gilbert, L. Goubin, A. Gouget, L. Granboulan, C. Lauradoux, M. Minier, T. Pornin, and H. Sibert. Decim – A new Stream Cipher for Hardware applications. In ECRYPT Stream Cipher Project Report 2005/004. Available at http://www.ecrypt.eu.org/stream/

3. S. Kiyomoto, T. Tanaka, and K. Sakurai, "A word-oriented stream cipher using clock control," Workshop Recod of SASC 2007, pp.260–274, January 2007 [Електронний ресурс]. – Режим доступу: https://www.cosic.esat.kuleuven.be/ecrypt/stream/papersdir/2007/029.pdf

4. The eSTREAM Project – eSTREAM Phase 3. SOSEMANUK (Portfolio Profile 1). [Електронний ресурс]. – Режим доступу: http://www.ecrypt.eu.org/ stream /sosemanukpf.html

5. The eSTREAM Project – eSTREAM Phase 3. Grain (Portfolio Profile 2). [Електронний ресурс]. – Режим доступу: http://www.ecrypt.eu.org/stream/ grainpf.html

6. The eSTREAM Project – eSTREAM Phase 3. MICKEY (Portfolio Profile 2). [Електронний ресурс]. – Режим доступу: http://www.ecrypt.eu.org/stream/ mickeypf.html

7. The eSTREAM Project – eSTREAM Phase 3. Trivium (Portfolio Profile 2). [Електронний ресурс]. – Режим доступу: http://www.ecrypt.eu.org/stream/triviumpf.html

8. Dabrowski P., Łabuzek G., Rachwalik T., Szmidt J. Searching for Nonlinear Feedback Shift Registers with Parallel Computing. [Електронний ресурс]. 2013 URL: https://eprint.iacr.org/2013/542.pdf (дата звернення: 07.10.2016).

9. Fredricksen H. A survey of full length nonlinear shift register cycle algorithms," SIAM Review. 1982, vol. 24, № 2. P. 195–221.

10. Jansen C.J. Investigations On Nonlinear Streamcipher Systems: Construction and Evaluation Methods. Ph.D. Thesis, Technical University of Delft. 1989.

11. Jansen C.J. The maximum order complexity of sequence ensembles. Lecture Notes in Computer Science, Adv. Cryptology-Eupocrypt'1991, Berlin, Germany. 1991, vol. 547, P. 153–159.

12. Linardatos D., Kalouptsidis N. Synthesis of minimal cost nonlinear feedback shift registers // Signal Process. – 2002. – Vol. 82, № 2. – P. 157–176.

13. Rizomiliotis P., Kalouptsidis N. Results on the nonlinear span of binary sequences // IEEE Transactions on Information Theory. – 2005. – Vol. 51, № 4. – P. 1555–5634.

14. Limniotis K., Kolokotronis N., Kalouptsidis N. On the nonlinear complexity and Lempel-Ziv complexity of finite length sequences // IEEE Transactions on Information Theory. – 2007. – vol. 53, № 11. – P. 4293–4302.

15. E. Dubrova, A scalable method for constructing Galois NLFSRs with period 2n-1 using cross-join pairs // IEEE Transactions on Information Theory. – 2013. – vol. 59(1). – P. 703-709.

16. Mykkeltveit J., Siu M-K., Tong P. On the cyclic structure of some nonlinear shift register sequences // Inform. and Control. – 1979. – vol. 43. – P. 202-215.

17. Carlet C. Boolean functions for cryptography and error correcting codes // In: Crama Y., Hammer P. L. (Eds.), Boolean Methods and Models, Cambridge University Press, http://www-rocq.inria.fr/secret/Claude.Carlet/ chap-fcts-Bool.pdf

18. Knuth, D. The Art of Computer Programming. Vol. II. Seminumerical Algorithms. – USA, Commonwealth of Massachusetts: Addison-Wesley, 1969. – P.634.

19. Flye-Sainte Marie C. Solution to question number 48 // l'Intermediaire des Mathematiciens. –1894. – V. 1. – P. 107-110.

20. de Bruijn N.G. A combitorial problem // Nederl. Akad. Wetensch. Proc. –1946. – V. 49. – P. 758-764.

21. H. Fredricksen. A survey of full length nonlinear shift register cycle algorithm // SIAM Review, 24(2):195–221, 1982.

22. Mayhew G.L., Golomb S.W. Characterizations of generators for modified de Bruijn sequences. Advances in applied mathematics 13(4), 454-461 (1992) https://www.sciencedirect.com/ science/article/pii/019688589290021N

23. Berlekamp E. R. Algebraic Coding Theory. McGraw-Hill, NY, 1968. – P.474.

24. McWilliams F.J. Sloane N.J. The Theory of Error-Correcting Codes // North-Holland, 1978. – P. 762.

25. Mayhew G.L., Golomb S.W. Linear spans of modified de Bruijn sequences // IEEE Trans. Inform. Theory. – 1990. – № 36(5). – P. 1166–1167.

Харьковский национальный
университет имени В.Н. Каразина;
АО «Институт информационных технологий», Харьков;
Государственная служба специальной связи и защиты
информации Украины, Киев

Поступила в редколлегию 22.10.2018

МЕТОДЫ И АЛГОРИТМЫ ЗАЩИТЫ И СОКРЫТИЯ ИНФОРМАЦИИ

УДК 004.056.5

І.Ф. АУЛОВ, канд. техн. наук, К.Е. ЛИСИЦЬКИЙ

ЗАСОБИ МОДЕЛЮВАННЯ ТА АНАЛІЗУ РИЗИКІВ В СЕРЕДОВИЩІ ХМАРНИХ ОБЧИСЛЕНЬ

Вступ

Хмарні рішення представляють собою складні системи з дуже розгалуженою архітектурою, яка складається з великої кількості компонентів та зв'язків між ними, що в залежності від питомих вимог замовника можуть мати різні конфігурації. При побудові таких систем особливу увагу необхідно приділяти моделюванню та аналізу ризиків. Як показує практика, найбільшу ефективність від моделювання та аналізу загроз в системах, в тому числі системах хмарних обчислень, можливо досягти лише при застосуванні методів з моделювання та аналізу загроз на всіх етапах створення та життєвого циклу системи, починаючи з проектування архітектури майбутньої системи. Такий підхід дозволяє реалізувати забезпечення глибокого та послідовного захисту в системі. Для моделювання та аналізу ризиків може бути використане програмне забезпечення як з відкритим похідним кодом, так і з закритим, а також безкоштовне та те, що потребує придбання ліцензії.

1. Засоби моделювання та аналізу ризиків з відкритим кодом

Для аналізу можливості застосування в задачах моделювання загроз та оцінки ризиків в середовищі хмарних обчислень було обрано наступні програмні продукти з відкритим кодом:

- OWASP Threat Dragon;
- CAIRIS;
- Mozilla Seasponge.

1.1. OWASP Threat Dragon

OWASP Threat Dragon – це програма для моделювання загроз у веб-середовищі, що дозволяє створювати графічні моделі систем, та на їх основі виконувати автоматичну генерацію та аналіз загроз і їх наслідків. Розробники програми ставили перед собою мету з реалізації простого та зручного інтерфейсу користувача для створення моделей систем та потужного автоматизованого алгоритму з генерації та аналізу загроз за набором правил для використання програми на різних етапах розробки системи [1].

Програма розробляється в рамках проекту Open Web Application Security Project (OWASP) та поширюється як вільний продукт за ліцензією Apache 2.0. Поточною версією є версія 0.1.26, опублікована 17 травня 2017 року [2]. Проект OWASP з'явився 1 грудня 2001 року і був створений в якості неприбуткової благодійної організації в Сполучених Штатах 21 квітня 2004 року з метою забезпечення безпеки веб-застосунків в мережі Інтернет. До складу спільноти OWASP входять корпорації, освітні організації, а також приватні особи зі всього світу. Спільнота працює над створенням наукових статей, навчальних підручників, документації інструментів та технологій, присвячених безпеці веб-застосунків в мережі Інтернет, що публікуються відкрито [3].

Програма поставляється у вигляді електронного додатка для встановлення на ПК для OS X та Windows або веб-додатку для роботи через браузер. Як метод визначення та аналізу загроз використовується метод STRIDE.

Основними перевагами інструмента є:

- простий та зручний інтерфейс користувача;
- потужний автоматизований алгоритм з обробки та оцінці загроз за правилами, який

дозволяє залучати звичайних користувачів, що не є експертами до роботи;

– інтеграція з іншими інструментами життєвого циклу розробки;
– використання підходу STRIDE для класифікації загроз;
– відкритість вихідного коду;
– безкоштовність.

Головним недоліком проекту є те, що він знаходиться на етапі розробки, та деякий функціонал ще не реалізовано. Також проект може застосовуватися для моделювання загроз в хмарному середовищі, але не є спеціально розробленим для цього.

1.2. CAIRIS

CAIRIS представляє собою платформу для виявлення, визначення та перевірки безпеки систем на основі аналізу ризиків. CAIRIS був розроблений в рамках докторських досліджень Shamal Faily з реалізації програмних засобів для моделювання та аналізу безпеки програмного забезпечення на етапі розробки [4]. Утиліта знайшла своє широке застосування в різних сферах з аналізу безпеки та ризиків, в тому числі і критичних системах. Інтерфейс програми та закладений підхід також дозволяє використовувати її і для систем хмарних обчислень. Утиліта CAIRIS має відкритий вихідний код [5] та поширюється під ліцензією Apache Software.

CAIRIS є клієнт-серверним рішенням. Використання на сервері в якості мови програмування Python дозволяє підтримувати ОС на базі Linux, Windows, macOS. [5]. Доступ до клієнта надається через браузер. Останньою версією CAIRIS є версія 1.5.3 випущена 11 лютого 2018 року.

Переваги CAIRIS на відміну від інших утиліт:

– простий та доступний інтерфейс, що дозволяє визначити вимоги до системи та її архітектуру, і на базі цього виконати моделювання та аналіз;
– проведення моделювання та аналізу ризиків з врахуванням особливості та впливу середовища моделювання на систему, компонентів та зв’язків між ними, а також значення ризиків;
– підтримка автоматичного масштабування в процесі роботи над моделлю та її доопрацювання на основі аналізу попередньо створених зв’язків та елементів системи;
– візуалізація результатів у вигляді звітів та діаграм;
– підтримка інтеграції з іншими інструментами за рахунок надання стандартного інтерфейсу для взаємодії та форматів даних;
– підтримка розширення функціоналу;
– простота встановлення, підтримка різних ОС, наявність прикладів;
– безкоштовність.

Недоліки програми полягають у відсутності шаблонів та наборів елементів, загроз для моделювання в системах хмарних обчислень.

1.3. Mozilla Seasponge

Mozilla Seasponge – це безкоштовний онлайн інструмент для моделювання загроз, який створений фондом Firefox за підтримки наукового товариства в рамках ініціативи Mozilla Winter of Security у 2014 році для допомоги системним адміністраторам визначити та оцінити ризики, з якими стикаються їх мережі. Інструмент базується на основі сучасних веб-технологій та є проектом з відкритим кодом, останнє оновлення якого було 7 січня 2016 року. Використання сучасних веб-технологій дозволяє працювати з інструментом за допомогою веб-браузера в різних операційних системах. Метою створення розробники SeaSponge вважають те, що моделювання загроз часто ігнорується в життєвому циклі розробки програмного забезпечення, незважаючи на те, що це дуже важливий аспект архітектури безпеки системи, тому необхідне рішення, що відповідає вимогам відкритості, безкоштовності та доступності всім розробникам, наприклад на відміну від закритого рішення, як інстру-

мент моделювання загроз від компанії Microsoft [6].

SeaSponge дозволяє моделювати систему, за допомогою якої можна визначити потенційні загрози та ризики, та підтримує кілька видів діаграм для моделювання логічних розділів вашої системи в окремих місцях. Кожна діаграма містить потоки даних, апаратні та логічні компоненти.

Переваги утиліти SeaSponge:

– відкритість вихідного коду;
– створення моделей систем за допомогою графічного інтерфейсу;
– можливість роботи на різних платформах за допомогою веб-браузера;
– безкоштовність.

До недоліків утиліти SeaSponge можна віднести:

– відсутність визначених шаблонів загроз та необхідність їх самостійної реалізації;
– відсутність стандартних компонентів для моделювання загроз в хмарі;
– розробка знаходиться на ранньому етапі, відсутня реалізація багатьох заявлених функцій.

2. Засоби моделювання та аналізу ризиків з закритим кодом

В якості засобів для вирішення задач моделювання загроз та оцінки ризиків в середовищі хмарних обчислень було розглянуто наступні програмні продукти закритим кодом:

– Microsoft Threat Modeling Tool;
– RiskWatch;
– vsRisk.

2.1. Microsoft Threat Modeling Tool

Програма Threat Modeling Tool розроблена компанією Microsoft для моделювання та аналізу загроз на етапі розробки та узгодження архітектури програмного забезпечення та представляє собою основний елемент в концепції життєвого циклу безпечної розробки програмного забезпечення (SDL) Microsoft [7]. Головним призначенням програми є мінімізація витрат на етапі проектування архітектури, впровадження та використання системи за рахунок використання адекватних мір з захисту, що відповідають загрозам.

Перша версія цього програмного забезпечення з’явилася в 2011 році під назвою Threat Analysis & Modeling Tool. На той час програмне забезпечення дозволяло експертам, не пов'язаним з безпекою, створювати та аналізувати моделі загроз для різних систем. В 2016 році вийшла оновлена версія програмного забезпечення, яка змінила назву на Microsoft Threat Modeling Tool та отримала розширену функціональність з моделювання та аналізу загроз в хмарному середовищі на основі технології Azure. Для вирішення цієї задачі програмне забезпечення в своєму складі має готовий набір стандартних компонентів хмари Azure та набір з загроз, які можуть бути реалізовані для компонентів та зв’язків між ними. Поточна версія поширюється вільно та доступна для завантаження на офіційному сайті Microsoft; працює в середовищі операційних систем Windows 7 та вище [8].

Визначення загроз та вразливостей системи в програмі базується на методах STRIDE та DREAD [8].

Основними перевагами програмного забезпечення є:

– моделювання, аналіз загроз та вразливостей безпеки на етапі проектування архітектури системи;
– автоматизація процесу моделювання та аналізу загроз, наявність зворотного зв’язку при моделюванні;
– візуалізація моделей та можливість отримання формалізованих звітів з аналізу моделі;
– наявність набору стандартних компонентів та загроз для моделювання та аналізу в середовищі хмарних обчислень;
– можливість додавати нові та редагувати чинні компоненти та загрози;

– використання методів STRIDE для класифікації загроз за типом та методу DREAD за наслідками;

– безкоштовність.

До недоліків можна віднести:

– закритість вихідного коду, що не дозволяє за необхідності розширити функціонал та перевірити коректність реалізації методів аналізу;

– підтримка ОС Windows;

– наявність компонентів та набору загроз тільки для моделювання та аналізу в середовищі хмари на базі технології Azure.

2.2. RiskWatch

З 1993 року компанія RiskWatch є світовим лідером у наданні рішення щодо оцінки ризиків. Підхід RiskWatch базується на тому, що ефективність керування ризиками безпеки та відповідності залежить від їх кількісної оцінки [9]. Утиліта була розроблена у 1988 році за участі Національного Інституту Стандартів та Технологій США, Міністерства Оборони США та Міністерства Оборони Канади. RiskWatch є комерційним та не надає відкритий код проекту.

RiskWatch працює на усіх пристроях, які мають доступ до інтернету, а також в офлайн режимі. Мінімальні системні вимоги, встановлені виробником: Windows Server 2008, JRE1.6, ApacheTomcat7.0, MySQL, MySQLDriver3.5, IE8Version 8.0.7600.16385, Firefox, Chrome [10].

RiskWatch підхід забезпечує попередню оцінку ризику та захисту від динамічних загроз, що можуть змінюватися.

RiskWatch зосереджений на забезпеченні:

– комплексного підходу, що ґрунтується на доказах та відповідає моделям ризику стандартів ISO 32001, Sandia Lab і FEMA;

– системи, яку клієнт може легко налаштувати для виконання будь-якого типу оцінок ризику, яка має відношення до своєї галузі;

– моделі підприємства, яке надає клієнтам єдиний вид ризиків у розподіленому підприємстві;

– захисту на основі оцінки ризику в режимі реального часу для зосередження зусиль та максимізації результатів;

– технологічного агностичного рішення, призначеного для підтримки різних екосистем;

– оновлення інформації про загрози та засобів протидії їм;

– актуального набору американських та міжнародних правил, найкращих практик і тематичних досліджень [9].

До переваг RiskWatch окрім відносної простоти використання можна віднести:

– глибоко відпрацьована та добре зарекомендована методологія аналізу ризиків;

– поєднання кількісної та якісної оцінки ризиків;

– велика база загроз, вразливостей та контрзаходів – база знань;

– можливість редагування та удосконалення бази знань;

– формування звітів.

Головним недоліком утиліти є закритість вихідного коду та необхідність купувати ліцензію для її використання.

2.3. vsRisk

Інструмент аналізу ризиків vsRisk був розроблений британською компанією IT Governance разом з Vigilant Software, це сучасний продукт аналізу ризиків, який базується на міжнародному стандарті ISO 27001. vsRisk є комерційним та не надає відкритий код проекту. vsRisk підтримує ОС Windows 7 та вище [11].

Цей програмний продукт надає простий та зрозумілий інтерфейс та має такі переваги:

– дозволяє оцінювати ризики порушення конфіденційності, цілісності та доступності

інформації для бізнесу, а також, з точки зору законодавства та контрактних обов'язків, перебуває в чіткій відповідності до стандарту ISO 27001;

– підтримує наступні стандарти (ISO/IEC 27002, BS7799-3:2006, ISO/IEC TR 13335-8:1998, NIST SP 800-30);

– містить інтегровану базу знань (загроз та вразливостей), яка регулярно оновлюється.

Окрім закритості вихідного коду та необхідності придбання ліцензії до недоліків vsRisk відноситься те, що він не надає кількісну оцінку ризиків, обмежуючись тільки якісною оцінкою ризиків.

Крім зазначеного недоліку, на поточний момент в базі знань vsRisk відсутні загрози та вразливості для моделювання систем хмарних обчислень.

3. Порівняння програмного забезпечення

Для порівняння програмного забезпечення для моделювання та аналізу загроз пропонується використовувати вимоги, що визначені в табл. 1.

Таблиця 1

Порівняння засобів моделювання та аналізу ризиків

ВИМОГИ	Microsoft Threat odeling Tool	OWASP Threat Dragon	CAIRIS	Mozilla Seasponge	RiskWatch	vsRisk
Підтримка моделювання та аналізу загроз в хмарному середовищі	+/-	+/-	+/-	-	+/-	-
Можливість застосування на різних етапах розробки системи	+	+	+	-	+	-
Автоматизований аналіз та формування звітів	+	+	+	-	+	-
Отримання якісної оцінки ризиків	+	+	+	+	+	+
Отримання кількісної оцінки ризиків	+	-	+	-	+	-
Простота застосування (можливість працювати без залучення експерту)	+	+	+	+	+/-	+
Інтеграція з іншими засобами	+/-	+	+	+	-	-
Можливість розширення функціональності	-	+	+	+	-	-
Кросплатформеність	-	+/-	+/-	+	+	-
Безкоштовність	+	+	+	+	-	-
Відкритість вихідного коду	-	+	+	+	-	-
Функціональність продукту, відповідає заявленому (розробка завершена)	+	-	+	-	+	+

За результатами порівняння можна зробити наступні висновки:

– жодна з програм в повній мірі не відповідає висунутим вимогам;

– програми OWASP Threat Dragon, Mozilla Seasponge – знаходяться на етапі розробки, та не можуть на поточний момент застосовуватися без суттєвої доробки;

– внаслідок відкритості коду та умов ліцензування програмне забезпечення OWASP Threat Dragon, CAIRIS та Mozilla Seasponge може бути доопрацьоване під потреби середовища хмарних обчислень;

– для застосування програмного забезпечення Microsoft Threat Modeling Tool необхідним є створення бази об'єктів, загроз та вразливостей для хмарного середовища, що побудоване не тільки на технологіях Windows Azure.

Висновки

Моделювання та аналіз ризиків для інформаційних систем є складною задачею та вимагає високого рівня кваліфікації від співробітника, який її проводить. Хоча моделювання ризиків в хмарному середовищі використовує аналогічні підходи тим, що застосовуються в інформаційно-телекомунікаційних системах внаслідок суттєвих відмінностей, пов`язаних з властивостями обробки інформації в хмарі та особливістю побудови хмари, вони мають суттєві відмінності, які необхідно враховувати. Для спрощення цього процесу та зменшення кількості помилок впроваджуються програмні продукти, які автоматизують дії та дозволяють перевіряти коректність розроблених моделей. В результаті дослідження були розглянуті програмні продукти моделювання та оцінки ризиків з відкритим та закритим вихідним кодом, а також комерційні продукти.

За результатами порівняння зроблені такі висновки: висунутим вимогам для моделювання та оцінки ризиків безпеки в хмарному середовищі повністю не відповідає жодний продукт; програмні продукти OWASP Threat Dragon, CAIRIS, Mozilla Seasponge не можуть бути застосовані та потребують доробок, але завдяки відкритості коду та умовам ліцензування це програмне забезпечення може бути доопрацьоване під потреби середовища хмарних обчислень та може бути розширені їх функціональні можливості. Застосування комерційних продуктів RiskWatch та vsRisk можливе лише при реалізації необхідного функціоналу їх розробниками. Закритість вихідних кодів продуктів та відсутність можливості розширення функціоналу сторонніми розробниками призводить до ризику неможливості їх застосування в майбутньому.

На сьогодні за сукупністю вимог та реалізованим функціональним можливостям найбільш перспективним є використання утиліти Microsoft Threat Modeling Tool. При цьому актуальними залишаються питання створення та підтримки бази загроз, елементів та зв’язків між ними в актуальному стані. Використання методологій STRIDE та DREAD, які використовуються в програмному продукті Microsoft Threat Modeling Tool дозволяє отримати попередні результати з аналізу ризиків системи на різних етапах її життєвого циклу, які надалі можуть бути основою більш детальних досліджень.

Список літератури:

1. OWASP Threat Dragon [Електронний ресурс]. Режим доступу: https://www.owasp.org/index.php/About_The_Open_Web_Application_Security_Project.

2. OWASP Threat Dragon on Github [Електронний ресурс]. Режим доступу: https://github.com/mike-goodwin/owasp-threat-dragon-desktop.

3. The Open Web Application Security Project (OWASP) Електронний ресурс]. Режим доступу: https://www.owasp.org.

4. CAIRIS [Електронний ресурс]. Режим доступу: https://cairis.org/.

5. CAIRIS [Електронний ресурс]. https://github.com/failys/cairis.

6. Mozilla launches free, online threat modelling tool [Електронний ресурс]. Режим доступу: https://siliconangle.com/blog/2015/04/01/mozilla-launches-free-online-threat-modelling-tool/.

7. Microsoft Threat Modeling Tool [Електронний ресурс]. Режим доступу: https://docs.microsoft.com/en-us/azure/security/azure-security-threat-modeling-tool.

8. Threat Modeling [Електронний ресурс]. Режим доступу: https://msdn.microsoft.com/en-us/library/ff648644.aspx.

9. RiskWatch technical specifications [Електронний ресурс]. Режим доступу: http://www.riskwatch.com/wp-content/uploads/2014/05/SWDataSheet.pdf.

10. RiskWatch [Електронний ресурс]. Режим доступу: http://www.riskwatch.com/.

11. vsRisk [Електронний ресурс]. Режим доступу: https://www.vigilantsoftware.co.uk/product/vsrisk-standalone.

Акціонерне товариство
«Інститут інформаційних технологій», Харків;
Харківський національний
університет імені В.Н. Каразіна

Надійшла до редколегії 05.10.2018

УДК 621.391:519.2

С.М. КОНЮШОК, канд. техн. наук

ДОСЛІДЖЕННЯ k-ВИМІРНОСТІ БУЛЕВОЇ ФУНКЦІЇ ШИФРУ LILI-128

Вступ

Атаки на основі відібраних векторів ініціалізації відносять до найбільш потужних атак на синхронні потокові шифри (СПШ). Зокрема, кубічна атака [1], статистична атака FKM [2], а також їх різноманітні модифікації та вдосконалення [3 – 8]. До будь-якого криптографічного алгоритму, який можливо описати за допомогою булевої функції $F:\{0,1\}^{l_0}\times\{0,1\}^{l_1}\to\{0,1\}$ (один з аргументів якої є секретним, а другий – загальнодоступним параметром), застосовуються подібні атаки. Для СПШ, в якості F (наприклад, функція ключа $k\in\{0,1\}^{l_0}$ та вектора ініціалізації $c\in\{0,1\}^{l_1}$) можливо обрати знак вихідної послідовності генератора гами шифру в певному такті. Слід зауважити, що функція F вважається доступною зловмиснику в вигляді оракула ("чорної скрині"), зокрема, може бути невідомим алгоритм, який реалізує цю функцію.

На етапі попередніх обчислень зловмисник може подавати на вхід оракула будь-які пари векторів $(x,y)\in\{0,1\}^{l_0}\times\{0,1\}^{l_1}$, обчислюючи значення $F(x,y)$, щоб зібрати потрібну інформацію про властивості функції F. Потім зловмисник отримує доступ до оракулу $F_k(c)=F(k,c)$, $c\in\{0,1\}^{l_1}$, де значення ключа $k\in\{0,1\}^{l_0}$ невідоме. Зловмисник може обирати будь-які вектори $c\in\{0,1\}^{l_1}$ та обчислювати значення $F_k(c)$ при фіксованому ключі k, спрямовуючи зусилля на відновлення цього ключа (або отримати про нього деяку інформацію). Іншою можливою стратегією зловмисника є побудова розрізняючої атаки, спрямованої на те, щоб статистично відрізнити (за прийнятний час з достатньо високою надійністю) відображення F_k від випадкового рівноімовірного відображення $\Phi:\{0,1\}^{l_1}\to\{0,1\}$ [3, 4].

Атака FKM [2] базується на основі статистичного наближення функції F булевою функцією g, що залежить лише від деяких розрядів ключа. Це дозволяє спочатку відновити вказані розряди методом максимуму правдоподібності, а потім знайти решту ключа шляхом повного перебору. В [2] вказані способи вибору функцій F і g для побудови атаки, але не дано теоретичного обґрунтування ефективності таких способів. Крім того, залишається відкритим питання про можливість підвищити ефективність атаки, описаної в [2], шляхом вибору наближення функції F з більш широкого класу булевих функцій.

В статтях [9, 10] описана статистична атака на СПШ, що узагальнює атаку FKM, а також кубічну атаку. Вказана атака базується на наближенні булевих функцій алгебраїчно виродженими функціями [11], застосовуючи поліноміальний ймовірнісний алгоритм побудови (в певному сенсі як завгодно близьких до найкращих з можливих) наближень функції F за відомим допустимим для F підпростором.

Побудова наближень булевих функцій алгебраїчно виродженими функціями потребує ефективних алгоритмів побудови k-вимірних наближень булевих функцій [12] та алгоритмів перевірки k-вимірності булевих функцій [13].

У даній статті викладено результати дослідження k-вимірності булевої функції шифру LILI-128 з застосуванням вдосконаленого тесту розпізнавання k-вимірності булевих функцій, заданих за допомогою оракулів.

Основні означення та допоміжні результати

Наукові основи тесту викладені в [13]. Наведемо основні означення та допоміжні результати, що потрібні для викладення матеріалу даної роботи.

Нехай $f: V_n = \{0,1\}^n \to \{0,1\}$ – булева функція від n змінних, $\hat{f}(\alpha) = 2^{-n} \sum\limits_{x \in V_n} (-1)^{f(x) \oplus \alpha x}$, $\alpha \in V_n$ – її нормовані коефіцієнти Уолша-Адамара.

Функція $f: V_n = \{0,1\}^n \to \{0,1\}$ називається алгебраїчно виродженою, якщо вона є k-вимірною для деякого $k < n$ та невиродженою – в протилежному випадку [14 – 16].

Функція f називається k-вимірною, $k \in \overline{0, n-1}$, якщо множина $Sp(f) = \{\alpha \in V_n : \hat{f}(\alpha) \neq 0\}$ породжує підпростір вимірності не більше за k векторного простору V_n або, що рівносильно, якщо існує не менше за $n-k$ лінійно незалежних несуттєвих векторів функції f, тобто векторів, що належать множині $I_f = \{\alpha \in V_n : f(x \oplus \alpha) \equiv f(x), x \in V_n\}$ [17].

Відомо, що для помірних значень k функції, близькі до k-вимірних, володіють криптографічними слабкостями, що дозволяє здійснювати певні атаки на генератори гами, побудовані на основі зазначених функцій [18 – 20]. У зв'язку з цим практично важливою є розробка ефективних алгоритмів перевірки властивості k-вимірності булевих функцій.

Слід зауважити, якщо булева функція від n змінних f задана за допомогою вектора значень (таблиці істинності), то для перевірки умови приналежності булевої функції f до множини всіх k-вимірних булевих функцій n змінних можливо застосувати природній детермінований алгоритм, трудомісткість якого складає $O(n^2 2^n)$ двійкових операцій. Цей алгоритм полягає в обчисленні всіх значень $\hat{f}(\alpha)$ за допомогою швидкого перетворення Адамара [21, с. 217], побудові множини $Sp(f)$ та знаходженні базису векторного простору I_f методом Гауса. Функція f є k-вимірною в тому і тільки в тому випадку, коли отриманий базис містить не менше $n-k$ векторів. Цей алгоритм не застосовується на практиці, якщо n є достатньо великим числом (наприклад, $n \geq 64$), а функція f задається за допомогою оракула (певного алгоритму, що дозволяє обчислювати значення $f(x)$ за довільними вхідними аргументами $x \in V_n$).

В [17] запропоновано ймовірнісний алгоритм або тест k-вимірності, який для довільної функції $f: V_n \to \{0,1\}$, заданої за допомогою оракула, та чисел $k \in \overline{0, n-1}$, $\varepsilon \in (0,1)$ перевіряє основну гіпотезу H_0 про те, що f є k-вимірною функцією, проти альтернативи H_1: f знаходиться на відстані (Гемінга) не менше за $2^n \varepsilon$ від множини k-вимірних функцій n змінних. Зазначений алгоритм полягає в генерації незалежних випадкових рівноймовірних векторів $h_1, ..., h_l \in V_n$ та перевірці рівностей

$$f(h_j \oplus Z_{ij}) = f(Z_{ij}),\ i \in \overline{1,m} \tag{1}$$

для кожного $j \in \overline{1,l}$, де Z_{ij} – незалежні в сукупності випадкові рівноймовірні вектори з V_n, що не залежать від $h_1, ..., h_l$. Позначимо ν_l число значень $j \in \overline{1,l}$, для яких виконуються рівності (1). Тоді гіпотеза H_0 приймається, якщо $\frac{\nu_l}{l} \geq 0{,}9 \cdot 2^{-k}$ та відхиляється у протилежному випадку. В [17] пропонується вибрати $l = 2^k C$, $m = 2^k k \varepsilon^{-1} C'$, де $C, C' = const$, що приводить до оцінки трудомісткості алгоритму $O(2^{2k} k \varepsilon^{-1})$ запитів до оракула f (або $O(n 2^{2k} k \varepsilon^{-1})$ двійкових операцій).

Для оцінювання ймовірності помилки першого роду (тобто ймовірності того, що тест "не визнає" такою k-вимірну функцію) в [17] використовується нерівність Чернова:

$$\mathrm{P}\left(\frac{\nu_l}{l} < 0{,}9\cdot 2^{-k} \mid H_0\right) \le \mathrm{P}\left(\frac{\nu_l}{l} - \mathrm{E}\frac{\nu_l}{l} < -0{,}1\cdot 2^{-k} \mid H_0\right) \le \exp\left\{-0{,}02\cdot\frac{C}{2^k}\right\}. \qquad (2)$$

Зауважимо, що вираз у правій частині (2) залежить від k та не прямує до нуля, якщо k є (як завгодно повільно) зростаючою функцією від n, наприклад, $k = \lceil \log n \rceil$, $n \to \infty$.

Вдосконалений тест k-вимірності булевих функцій

В роботі [13] запропонований більш ефективний імовірнісний тест k-вимірності, трудомісткість якого складає $O(2^k k^2\, \varepsilon^{-1})$ запитів до оракула (або $O(n\, 2^k k^2\, \varepsilon^{-1})$ двійкових операцій). При цьому верхня межа ймовірності помилки першого роду запропонованого тесту не залежить від k, а верхня межа ймовірності помилки другого роду є по суті така ж сама, що й для тесту з [17].

Алгоритм перевірки k-вимірності булевих функцій, що запропонований в роботі [13], має такий вигляд.

Вхідні дані: $f : V_n \to \{0,1\}$, $k \in \overline{0, n-1}$, $\varepsilon \in (0,1)$.

Параметри: $t = k + c$, $m = 2^{t+4} t\, \varepsilon^{-1}\delta^{-1}$, де $c \in \mathrm{N}$, $\delta \in (0, 1/2)$, $c, \delta = const$).

1. Згенерувати випадкову рівноймовірну $t \times n$-матрицю X, побудувати множину $Sp(f_X)$, за якою знайти базис $a_1, ..., a_l$ векторного простору I_{f_X} (дуального до підпростору, що породжується множиною $Sp(f_X)$). Перевірити умову $l \ge t - k$, за виконанням якої перейти до кроку 2. У протилежному випадку – прийняти гіпотезу H_1 (f знаходиться на відстані не менше $2^n \varepsilon$ від множини k-вимірних функцій).

2. Для кожного $j \in \overline{1, l}$ покласти $h_j = a_j X$, згенерувати незалежні випадкові рівноймовірні вектори $Z_{1j}, ..., Z_{mj}$ та перевірити рівності (1). За виконанням зазначених рівностей для всіх $j \in \overline{1, l}$ прийняти гіпотезу H_0 (f – k-вимірна функція), у протилежному випадку – прийняти гіпотезу H_1.

Ймовірність помилки першого роду (відхилити вірну гіпотезу H_0) тесту, який реалізований описаним алгоритмом, не перевищує 2^{-c}, а ймовірність помилки другого роду (відхилити вірну гіпотезу H_1) не перевищує $\max\{5\cdot 2^{-c-1}, \delta + \exp\{-7c2^c\}\}$.

Потоковий шифр LILI-128

LILI-128 [22] – це синхронний потоковий шифр, що був учасником конкурсу NESSIE [23] та базується на регістрах зсуву з лінійним зворотнім зв'язком, з довжиною ключа, яка дорівнює 128 бітів. Генератор псевдовипадкових послідовностей LILI-128 використовує два регістри зсуву з лінійним зворотнім зв'язком та дві функції для генерації двійкової послідовності. Структура генератора представлена на рис. 1.

Як видно з рис. 1, в структурі генератору псевдовипадкових послідовностей шифру LILI-128 можливо виділити блок управління рухом та блок генерації даних. Вихідна послідовність $c(t)$ блоку управління рухом визначає закон руху блоку генерації даних.

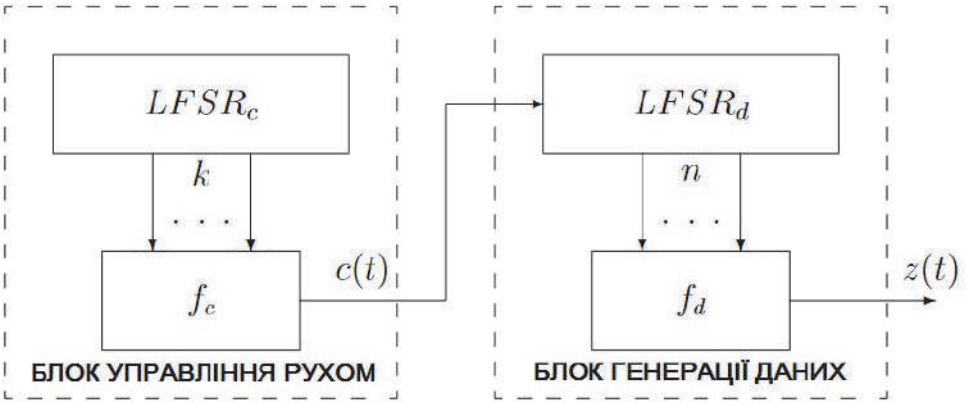


Рис. 1. Генератор LILI-128

Стан LILI-128 визначається як зміст двох регістрів зсуву з лінійним зворотнім зв'язком: $LFSR_c$ та $LFSR_d$, довжиною 39 та 89 біт відповідно. За поточним станом генератору обчислюються значення функцій f_c та f_d, а також функцій зворотного зв'язку. В якості оракулу була обрана булева функція від 89 змінних f_d.

Дослідження k-вимірності булевої функції шифру LILI-128

Обчислювальні експерименти проведені з використанням пакету прикладних програм Maple на ПЕОМ типу Intel(R) Core(TM) i7-3770K 3,5 GHz, 8 Gb RAM в середовищі операційної системи Windows 7 та були організовані наступним чином.

Фіксувалися значення вхідних даних k, ε та δ (від якого безпосередньо залежить ймовірність помилки другого роду та значення p_0 ймовірності помилки першого роду тесту, яке дозволяє обчислити значення параметрів $c = -\log_2(p_0)$ та $t = k + c$), що дозволяє обчислити значення $m = 2^{t+4} t\, \varepsilon^{-1}\delta^{-1}$. Під час проведення обчислювального експерименту значення ε, δ та p_0 були обрані рівними 0,125. Для кожного набору параметрів здійснювалося по 25 запусків тесту для кожного значення k від 1 до 10.

Таблиця 1

k	m	Кількість прийнятих гіпотез		Середній час перевірки гіпотези, сек.		$2^k k^2 \varepsilon^{-1}$
		H_0	H_1	H_0	H_1	
1	4	0	25	–	0,034	16
2	5	0	25	–	0,063	128
3	6	0	25	–	0,115	576
4	7	0	25	–	0,189	2048
5	8	0	25	–	0,301	6400
6	9	0	25	–	1,086	18432
7	10	0	25	–	2,116	50176
8	11	0	25	–	3,599	131072
9	12	3	22	70916,094	8,165	331776
10	13	25	0	152103,787	–	819200

Як видно з табл. 1, середній час перевірки гіпотези H_0 значно перевищує відповідний показник для H_1, що пов'язано з необхідністю виконання кроку 2 вдосконаленого тесту k-вимірності в повному обсязі для кожного $j \in \overline{1,l}$. Відзначимо також, що середній час пере-

вірки гіпотези залежить від k та зростає повільніше ніж аналітична оцінка трудомісткості алгоритму (кількість запитів до оракулу).

Висновки

В результаті виконання вдосконаленого тесту k-вимірності до функції f_d від 89 змінних шифру LILI-128 встановлено, що $k = 10$. Таким чином, $k < n$, що свідчить про потенційну можливість реалізації статистичної атаки, яка базується на наближенні булевих функцій алгебраїчно виродженими функціями.

Вдосконалений тест може бути застосований до аналізу відповідних властивостей булевих функцій (зокрема, від десятків чи сотен змінних), які використовуються в сучасних симетричних криптосистемах.

Список літератури:

1. Dinur I. Cube attacks on tweakable black box polynomials / I. Dinur, A. Shamir // Advances in Cryptology. – EUROCRYPT'09. Proceedings. Springer-Verlag, 2009. – P. 278–299.

2. Fischer S. Chosen IV statistical analysis for key recovery attacks on stream ciphers / S. Fischer, S. Khazaei, W. Meier // AFRICACRYPT 2008. Proceedings. Springer-Verlag, 2008. – P. 236–245.

3. Aumasson J.-Ph. Efficient FPGA implementations of high-dimensional cube testers on the stream cipher Grain-128 / J.-Ph. Aumasson, I. Dinur, L. Hensen, W. Meier, A. Shamir // Cryptology ePrint Archive. – URL: http://eprint.iacr.org/2009/218 (last access: 29.10.18).

4. Aumasson J.-Ph. Cube testers and key recovery attacks on reduced-raund MD6 and Trivium / J.-Ph. Aumasson, I. Dinur, W. Meier, A. Shamir // Fast Software Encryption – FSE'09. Proceedings. Springer-Verlag. 2009. – P. 1–22.

5. Aumasson J.-Ph. New features of latin dances: analysis of Salsa, ChaCha, and Rumba / J.-Ph. Aumasson, S. Fischer, S. Khazaei, W. Meier, C. Rechberger // Fast Softvare Encryption – FSE 2008, Proceedings. Springer-Verlag. 2008. – P. 470–488.

6. Dinur I. An experimentally verified attack on full Grain-128 using dedicated reconfigurable hardware / I. Dinur, T. Gueysu, C. Paar, A. Shamir, R. Zimmermann // Cryptology ePrint Archive. – URL: http://eprint.iacr.org/2011/282 (last access: 29.10.18).

7. Dinur I. Breaking Grain-128 with dynamic cube attacks / I. Dinur, A. Shamir // Fast Software Encryption – FSE'11. Proceedings. Springer-Verlag. 2011. – P. 167–187.

8. Faisal Sh. Extended cubes: enhancing cube attacks by low-degree non-linear equations / Sh. Faisal, M. Resa, W. Susilo, J. Seberry // Proc. of the 6-th ACM Symp. on Information, Comput. and Communication Security (AIACCS'11). 2011. – P. 296 – 305.

9. Алексейчук А.Н. Обобщенная статистическая атака на синхронные поточные шифры / А.Н. Алексейчук, С.Н. Конюшок, А.Ю. Сторожук // Захист інформації. – 2015. – Т. 17. – № 3. – С. 54 – 65.

10. Алексейчук А.Н. Статистическая атака на генератор гаммы с линейным законом реинициализации начального состояния и функцией усложнения, близкой к алгебраически вырожденной / А.Н. Алексейчук, С.Н. Конюшок, А.Ю. Сторожук // Радиотехника. – 2014. – Вып. 176. – С. 13–21.

11. Алексейчук А.Н. Алгебраически вырожденные приближения булевых функций / А.Н. Алексейчук, С.Н. Конюшок // Кибернетика и системный анализ. – 2014. – Т. 50. – № 6. – С. 3–14.

12. Олексійчук А.М. Швидкі алгоритми побудови k-вимірних наближень наближень булевих функцій / А.М. Олексійчук, С.М. Конюшок, А.Ю. Сторожук // Захист інформації. – 2015. – Т. 17. – № 1. – С. 43–52.

13. Алексейчук А.Н. Усовершенствованный тест k-мерности для булевых функций / А.Н. Алексейчук, С.Н. Конюшок // Кибернетика и системный анализ. – 2013. – Т. 49. – № 2. – С. 27 – 35.

14. Lechner, R. L. Harmonic analysis of switching functions / R.L. Lechner // Recent Developments in Switching Theory. – New-York. Academic Press, 1971. – P. 122–228.

15. Dawson E. Construction of correlation immune Boolean functions / E. Dawson, C.K. Wu // Information and Communication Security, Proceedings. Berlin. Springer-Verlag, 1997. – P. 170–180.

16. Алексеев, Е.К. О некоторых мерах нелинейности булевых функций // Прикладная дискретная математика. – 2011. – № 2(12). – С. 5–16.

17. Gopalan P. Testing Fourier dimensionality and sparsity / P. Gopalan, R. O'Donnell, A. Servedio, A. Shpilka, K. Wimmer // SIAM J. on Computing. – 2011. – Vol. 40(4). – P. 1075 – 1100.

18. Golic J., Morgari G. On the resynchronization attack // Fast Software Encryption. – FSE'03, Proceedings. – Springer-Verlag, 2003. – P. 100 – 110.

19. Алексеев Е.К. О некоторых мерах нелинейности булевых функций // Прикладная дискретная математика. – 2011. – № 2(12). – С. 5 – 16.

20. Алексеев Е.К. Об атаке на фильтрующий генератор с функцией усложнения, близкой к алгебраически вырожденной // Материалы Шестой междунар. науч. конф. по проблемам безопасности и противодействия терроризму, 11 – 12 ноября 2010 г., Том 2. – Москва : МЦНМО, 2011. – С. 114 – 122.

21. Логачев О.А. Булевы функции в теории кодирования и криптологии / О.А. Логачев, А.А. Сальников, В.В. Ященко. – Москва : МЦНМО, 2004. – 470 с.

22. Simpson L.R. LILI Keystream Generator / L.R. Simpson, E. Dawson, J.D. Golić, W.L. Millan // Selected Areas in Cryptography. – SAC 2000. Lecture Notes in Computer Science, vol 2012. – Springer, Berlin, Heidelberg. – P. 248 – 261.

23. NESSIE New European Schemes for Signatures, Integrity, and Encryption // URL: https://www.cosic.esat.kuleuven.be/nessie/ (last access: 29.10.18).

Інститут спеціального зв'язку та захисту інформації
національного технічного університету України
«Київський політехнічний інститут» імені Ігоря Сікорського

Надійшла до редколегії 01.11.2018

УДК 004.056.5

А.А. КУЗНЕЦОВ, д-р техн. наук, И.В. МОСКОВЧЕНКО, канд. техн. наук,
Д.И. ПРОКОПОВИЧ-ТКАЧЕНКО, канд. техн. наук, Т.Ю. КУЗНЕЦОВА

ЭВРИСТИЧЕСКИЕ МЕТОДЫ ГРАДИЕНТНОГО ПОИСКА КРИПТОГРАФИЧЕСКИХ БУЛЕВЫХ ФУНКЦИЙ

Введение

Важным элементом большинства современных симметричных шифров являются нелинейные блоки замен (S-блоков) [1 – 4], которые описываются с помощью булевых или, в общем случае, векторных криптографических функций [5 – 29]. Показатели стойкости таких функций (сбалансированность, нелинейность, автокорреляция и пр.) непосредственно влияют на эффективность симметричных шифров, их устойчивость к большинству современных криптоаналитических атак [5 – 17]. В частности, в работах [5 – 7] исследованы алгебраические свойства S-блоков современных блочных шифров, показано их влияние на устойчивость к алгебраическому криптоанализу. В [8 – 11] исследованы комбинаторные свойства нелинейных узлов применительно к безопасности различных режимов шифрования и ключевого расписания. В работах [12, 13] исследуется влияние S-блоков на лавинные эффекты, дифференциальные и линейные свойства блочных шифров. Работы [14 – 16] посвящены исследованию свойств нелинейных узлов замены в современных поточных шифрах в сравнении с алгоритмом «Strumok», предлагаемым в качестве нового стандарта поточного шифрования Украины [17]. Методы построения S-блоков исследуются многими авторами, например [18 – 20]. Однако наиболее распространенным и развитым остается математический аппарат криптографических булевых функций [21 – 28]. В частности, в [21] представлено новое рекурсивное построение булевой функции с максимальным алгебраическим иммунитетом; в [22, 23] рассмотрены генетические алгоритмы построения булевых функций с требуемыми криптографическими свойствами; в [24] исследуется метод имитации отжига; в [25, 26] исследуются эволюционные методы; работы [27, 28] посвящены эвристическим методам градиентного поиска.

Цель данной работы – продолжение исследований метода градиентного спуска, впервые предложенного в [28], оценка его вычислительной сложности в сравнении с наиболее близким аналогом из [27]. Для этого в разд. 1 вводятся необходимые термины и определения; в разд. 2 кратко излагаются исследуемые эвристические методы [27, 28] и приводятся расчетные данные необходимого числа операций для реализации градиентного спуска (табл. 1). В разд. 3 оцениваются свойства метода градиентного подъема по формированию высоко нелинейных корреляционно-иммунных криптографических булевых функций. В разд. 4 предлагается методика оценки эффективности эвристических методов и приводятся результаты сравнительных исследований. В частности, показано, что метод градиентного спуска из [28] за значительно меньшее число итераций (в десятки раз) позволяет формировать криптографические булевы функции с требуемыми показателями нелинейности и автокорреляции. В разд. 5 приводятся результаты исследований криптографических свойств формируемых булевых функций, проводится сравнение с наилучшими известными оценками. В заключение полученные результаты обобщаются, кратко формулируются направления дальнейших исследований.

1. Показатели стойкости криптографических булевых функций

Введем основные понятия и определения математического аппарата булевой алгебры, используемые при оценке эффективности нелинейных узлов замен симметричных шифров [1 – 17].

Булевой функцией f от n переменных является функция [1 – 17], осуществляющая отображение из поля $GF(2^n)$ всех двоичных векторов $x = (x_1, \ldots, x_n)$ длины n в поле $GF(2)$. Обыч-

но булевы функции представляются в алгебраической нормальной форме (АНФ) и рассматриваются как сумма произведений составляющих координат.

Алгебраическая степень deg(f) является степенью самого длинного слагаемого функции, представленной в алгебраической нормальной форме. Алгебраическая степень отражает стойкость к аналитическим атакам, призванным свести данную функцию к криптографически слабой (линейной).

Последовательностью функции f называется (1,-1)-последовательность, определенная как $((-1)^{f(\alpha_0)}, (-1)^{f(\alpha_1)}, \ldots, (-1)^{f(\alpha_{2^n-1})})$ [1 – 17].

Таблицей истинности функции f называется (0,1)-последовательность, определенная как $(f(\alpha_0), f(\alpha_1), f(\alpha_{2^n-1}))$ [1-17].

Последовательность функции *f* является *сбалансированной*, если ее (0,1)-последовательность ((1,-1)-последовательность) содержит одинаковое количество нулей и единиц (единиц и минус единиц). Функция *f* является сбалансированной, если сбалансирована ее последовательность [1 – 17].

Эквивалентное определение сбалансированности [1 – 17]: функция *f* над $GF(2^n)$ является сбалансированной, если ее выходные значения являются равновероятными:

$$| \{x \mid f(x) = 0 \} | = | \{x \mid f(x) = 1 \}| = 2^{n-1}.$$

Сбалансированность функции является показателем стойкости, отражающим слабость выходной последовательности к статистическим атакам.

Аффинной функцией f называется функция вида $f = a_1x_1 \oplus \ldots \oplus a_nx_n \oplus c$, где $a_j, c \in GF(2), j = 1, 2,..., n$. Функция *f* называется *линейной*, если $c = 0$ [1 – 17].

Весом Хэмминга вектора α ((0,1)-последовательности α), обозначаемым как $W(\alpha)$, является количество единиц в векторе (последовательности) [1 – 17].

Расстоянием Хэмминга d(f,g) между последовательностями двух функций *f* и *g* является количество позиций, в которых различны последовательности этих функций [1 – 17].

Нелинейность N_S преобразования – минимальное расстояние Хэмминга между выходной последовательностью *S* и всеми выходными последовательностями аффинных функций над некоторым полем [1 – 17]: $N_S = min\ \{d(S,\varphi)\}$, где φ – множество аффинных функций.

Нелинейность функции N_f – минимальное расстояние Хэмминга N_f между функцией *f* и всеми аффинными функциями над $GF(2^n)$ [1 – 17], где φ – множество аффинных функций.

Для произвольной функции *f* нелинейность N_f над $GF(2^n)$ может достигать [1 – 17]: $N_f \le 2^{n-1} - 2^{n/2-1}$.

Для сбалансированной функции *f* над $GF(2^n)$ ($n \ge 3$) нелинейность N_f может достигать [1 – 17]:

$$N_f \le \begin{cases} 2^{n-1} - 2^{n/2-1} - 2, n = 2k, \\ \left\lfloor\left\lfloor 2^{n-1} - 2^{n/2-1} \right\rfloor\right\rfloor, n = 2k+1, \end{cases}$$

где $\lfloor\lfloor x \rfloor\rfloor$ – максимальное четное целое, меньшее либо равное *x*.

Нелинейность функции является показателем, отражающим стойкость функций к корреляционным (линейным) атакам.

Функция *f* обладает *корреляционным иммунитетом* порядка *k*, если выходная последовательность функции $y \in Y$ статистически не зависит от любого подмножества из *k* входных координат [1 – 17]:

$$\forall \{x_1, \ldots, x_k\} \quad P(y \in Y / \{x_1, \ldots, x_k\} \in X) = P(y \in Y).$$

Эквивалентное определение корреляционного иммунитета в терминах преобразования Уолша [1 – 17]: функция *f* над полем $GF(2^n)$ имеет корреляционный иммунитет порядка *k*, *КИ*(*k*), если ее преобразование Уолша удовлетворяет равенству $F(\omega) = 0$ для всех $\omega \in V_n$ таких, что $1 \le W(\omega) \le k$: $\forall \omega \in V_n, F(\omega) = 0$, *КИ*(*f*) = *k*.

Преобразование Уолша $F(\omega)$ функции f над полем $GF(2^n)$ определяется как принимающая действительные значения функция [1 – 17]:

$$F(\omega) = 2^{-n} \sum_x (-1)^{f(x) \oplus \langle \omega, x \rangle},$$

где $\omega \in V_n$, $f(x)$, $\langle \omega, x \rangle \in N$ ($\langle \omega, x \rangle$ – скалярное произведение $w_1 x_1 \oplus \ldots \oplus w_n x_n$) .

Корреляционно-иммунная функция k-го порядка – функция, обладающая корреляционным иммунитетом порядка k. Сбалансированные корреляционно-иммунные функции называются *эластичными функциями*.

Функция f над полем $GF(2^n)$ удовлетворяет [1 – 17]:

- критерию распространения относительно вектора α, $KP(\alpha)$, если функция $f(\mathrm{x}) \oplus f(\mathrm{x} \oplus \alpha)$ является сбалансированной, $x \in V_n$, где $x = (x_1, x_2, \ldots, x_n)$:

$$P(f(\mathrm{x}) = f(\mathrm{x} \oplus \alpha)) = \frac{1}{2};$$

- критерию распространения степени k, $KP(k)$, если удовлетворяется критерий распространения относительно всех векторов $\alpha \in V_n$ при $1 \le W(\alpha) \le k$:

$$P(f(\mathrm{x}) = f(x \oplus \alpha)) = \frac{1}{2} \qquad , \forall \alpha : 1 \le W(\alpha) \le k;$$

- строгому лавинному критерию, *СЛК*, если f удовлетворяет критерию распространения степени 1:

$$P(f(\mathrm{x}) = f(\mathrm{x} \oplus \alpha)) = \frac{1}{2}, \ \forall \alpha : W(\alpha) = 1.$$

Степень корреляционного иммунитета/критерия распространения отражает стойкость функций к корреляционным атакам, призванным найти линейные свойства данной функции.

Функция f над $GF(2^n)$ называется бент-функцией [1 – 17], если

$$2^{-n/2} \sum_{x \in V_n} (-1)^{f(x) \oplus \langle \beta, x \rangle} = \pm 1.$$

для всех $\beta \in V_n$.

Последовательность бент-функции называется бент-последовательностью. Для бент-функций справедливы следующие утверждения [1 – 17]:

$\langle \xi, \ell \rangle = \pm 2^{n/2}$ для любой аффинной последовательности ℓ длины 2^n;

$f(x) \oplus f(x \oplus \alpha)$ сбалансирована $\forall \alpha \in V_n$, $W(\alpha) \ne 0$;

$f(x) \oplus \langle \alpha, x \rangle$ принимает значение единица $2^{n-1} \pm 2^{n/2-1}$ раз $\forall \alpha \in V_n$;

$f(x) \oplus h(x)$, где $h(x)$ – аффинная функция, также является бент-функцией.

Автокорреляционная функция $\hat{r}(s)$ для $s \in 0 \ldots 2^n - 1$ определена как

$$\hat{r}(s) = \sum_{x=0}^{2^n-1} \hat{f}(x) \hat{f}(x \oplus s).$$

Значение автокорреляции отражает стойкость функций к классу аналитических атак, призванным найти корреляцию между фрагментами функции.

Говорят, что функция f удовлетворяет характеристике распространения m, если

$$\left(1 \le |s| \le m\right) \Rightarrow |\hat{r}(s)| = 0.$$

Аналогично, автокорреляция $AC(f)$ функции f определяется как модуль наибольшего значения $\hat{r}(s)$:

$$AC(f) = \max_{s \ne 0} \left| \sum_{ч} \hat{f}(x) \hat{f}(x \oplus s) \right| = \max_{s \ne 0} |\hat{r}(s)|.$$

Автокорреляция $\hat{r}(s)$ обеспечивает утечку информационного потока со входа на выход функции.

2. Эвристические методы градиентного поиска

В данной работе исследуются эвристические методы градиентного поиска. В частности, метод градиентного подъема В. Миллана, Э. Кларка, Э. Доусона, 1997 г. [16] и разработанный на его основе метод градиентного спуска [17].

2.1. Эвристический метод градиентного подъема

Суть метода состоит в повышении нелинейности произвольной булевой функции путем комплементации некоторой позиции в таблице истинности исходной функции. Каждая позиция таблицы истинности соответствует уникальным входным данным. Метод позволяет создать полный список/перечень таких входных данных функции, что комплементация любой соответствующей данному входу выходной позиции в таблице истинности будет увеличивать нелинейность данной функции. Список/перечень таких позиций в таблице истинности обозначается как 1 – *Improvement Set* функции $f(x)$, или 1 – IS_f [16].

Определение 1 [16]. Пусть $g(x) = f(x) \oplus 1$ для $x = x_a$ и $g(x) = f(x)$ для всех остальных x. Если $N_g > N_f$, то $x_a \in 1 - IS_f$.

В [16] представлен быстрый систематический метод определения множества 1 – IS_f заданной булевой функции путем использования ее таблицы истинности и преобразований Уолша – Адамара. Для нахождения множества 1 – IS_f заданной булевой функции необходимо сначала определить значения коэффициентов преобразования Уолша – Адамара, которые соответствовали бы величинам, близким к абсолютному значению максимального коэффициента, WH_{max}.

Определение 2. Пусть $f(x)$ является булевой функцией с преобразованием Уолша – Адамара $F(w)$, где WH_{max} обозначает максимальное абсолютное значение $F(w)$. Тогда будут существовать одна или более линейных функций $L_w(x)$, имеющих минимальное расстояние до функции $f(x)$, и для данных w будет справедливо равенство $|F(w)| = WH_{max}$.

Определяется следующее множество:

$$W_1^+ = \{ w: F(w) = WH_{max} \} \text{ и}$$

$$W_1^- = \{ w: F(w) = - WH_{max} \}.$$

Также определяются множества w, для которых значения *WHT* приближены к максимуму:

$$W_2^+ = \{ w: F(w) = WH_{max} - 2\},$$

$$W_2^- = \{ w: F(w) = - (WH_{max} - 2)\},$$

$$W_3^+ = \{ w: F(w) = WH_{max} - 4\} \text{ и}$$

$$W_3^- = \{ w: F(w) = - (WH_{max} -4)\}.$$

Когда таблица истинности изменяется ровно в одном месте, все *WHT* значения изменяются на +2 или -2. Из этого следует, что для увеличения нелинейности все *WHT* значения в множестве W_1^+ должны быть изменены на -2, все *WHT* значения в множестве W_1^- должны быть изменены на 2, а также все *WHT* значения в множестве W_2^+ должны быть изменены на -2, все *WHT* значения в множестве W_2^- должны быть изменены на 2. Если первые два условия являются очевидными, то следующие два условия требуются для того, чтобы все другие значения $|F(w)|$ оставались меньшими, чем WH_{max}. Данные условия могут быть представлены в виде простых тестов.

Теорема 1 [16]. Пусть дана некоторая булева функция $f(x)$ с *WHT* $F(w)$ и определены множества $W^+ = W_1^+ \cup W_2^+$ и $W^- = W_1^- \cup W_2^-$. Тогда для некоторого входа x существует элемент из *Improvement Set* и выполняются следующие два условия:

$$f(x) = L_w(x) \text{ для всех } w \in W^+,$$

и $f(x) \neq L_w(x)$ для всех $w \in W$.

Если функция $f(x)$ не сбалансирована, понижение несбалансированности может быть достигнуто использованием дополнительного ограничения:

если $F(0) > 0$, $f(x) = 0$, иначе $f(x) = 0$.

Критерием градиентного поиска является максимизация расстояния по Хеммингу между формируемой последовательностью и последовательностями линейных функций. После обновления алгебраической формы булевой функции производятся аналогичные операции: выполняется преобразование Уолша – Адамара *WHT* и находится максимальные значения коэффициентов преобразования; формируется множество *Improvement Set*; находятся элементы последовательности функции, совпадающие с элементами последовательности ближайшей линейной формы; инвертирование совпавших элементов и повышение нелинейности функции, посредством «отдаления» от ближайшей линейной функции. Далее выполняются очередные итерации, аналогичные рассмотренным выше.

Проведенные исследования показали, что рассмотренный метод градиентного подъема вычислительно затратен и, при большом числе аргументов булевой функции, требует выполнения значительного числа повторяющихся итераций. Для снижения вычислительной сложности в [17] предложен метод градиентного спуска с бент-последовательностями в качестве входных данных.

2.2. Эвристический метод градиентного спуска

Данный метод основан на комплементации позиций бент-последовательностей для градиентного поиска сбалансированных булевых функций по критерию максимизации расстояния Хемминга между формируемыми последовательностями и последовательностями всех линейных функций. Это позволяет снизить вычислительные затраты на поиск булевых функций с требуемыми криптографическими свойствами.

Основной идеей метода градиентного спуска является эффективное понижение нелинейности заданных бент-последовательностей при каждой из 2n/2–1 обязательных комплементаций. В табл. 1 представлены расчетные данные для векторных пространств V4 – V12. В столбце 2 указана нелинейность (значение преобразования Уолша) бент-последовательностей, рассматриваемых как входные данные, в столбце 3 указана максимально достижимая нелинейность функций (максимальное значение преобразования Уолша), которые мы хотели бы получить в качестве выходных данных, и в столбце 4 указано количество бит, которое необходимо изменить в бент-последовательностях для получения желаемого результата.

Таблица 1

Расчетные значения для векторных пространств $V_4 – V_{12}$

	Максимально достижимые показатели для бент-функций		Максимально достижимые показатели для сбалансированных функций / Наилучший известный результат		Необходимо изменить позиций в бент-последовательности
	N_f	$F(w)$	N_f	$F(w)$	
V_4	6	4	4/4	8/8	2 позиции
V_6	28	8	26/26	12/12	4 позиции
V_8	120	16	118/116	20/24	8 позиции
V_{10}	496	32	494/492	36/40	16 позиции
V_{12}	2016	64	2014/2010	68/76	32 позиции

На рис. 1 представлены возможные потери нелинейности при комплементации необходимого числа позиций бент-последовательности.

Для достижения заданной верхней границы нелинейности необходимо из общего числа позиций x таблицы истинности, подлежащих комплементации, определить то число позиций y, изменение которых повлечет изменение WH на +2, и то число позиций z, изменение которых повлечет изменение WH на -2, $x = y + z$. В табл. 1 представлены расчетные данные, отображающие необходимое число требуемых комплементаций бент-последовательности для заданного векторного пространства в соответствии с теоремой 2.1 из [17].

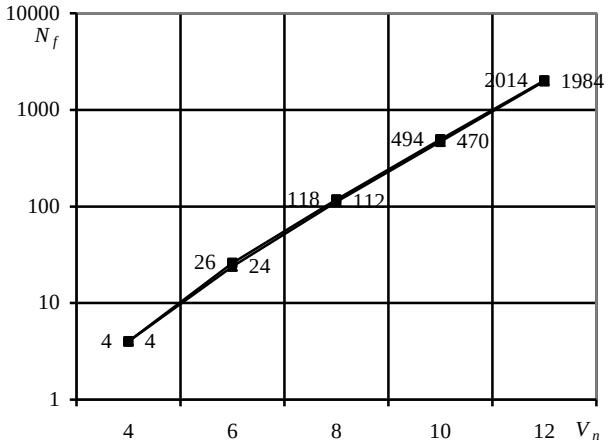


Рис. 1. Возможные потери нелинейности при комплементации

Таблица 2

Расчетные данные необходимого числа комплементаций бент-последовательности

	Необходимо изменить позиций в бент-последовательности, *NeedSteps*	Необходимо изменить значение нелинейности		Требуется для этого изменений, n^- и n^+
		N_f, с _ на _	$F(w)$, с _ на _	
V_4	2	6→4	4→8	$n^- = 2$ (изменения с $F(w) = +2$)
V_6	4	28→26	8→12	$n^- = 3$ (изменения с $F(w) = +2$) $n^+ = 1$ (изменения с $F(w) = -2$)
V_8	8	120→116	16→24	$n^- = 6$ (изменения с $F(w)$=+2) $n^+ = 2$ (изм-я с $F(w)$=-2)
V_{10}	16	496→492	32→40	$n^- = 10$ (изменения с $F(w)$=+2) $n^+ = 6$ (изменения с $F(w)$=-2)
V_{12}	32	2016→2010	64→76	$n^- = 19$ (изменения с $F(w)$=+2) $n^+ = 13$ (изменения с $F(w)$=-2)

После расчета необходимого числа комплементаций бент-последовательности на первом шаге эвристического поиска выполняется преобразование Уолша – Адамара WH и определяется максимальное расстояние по Хеммингу к одной или нескольким последовательностям линейных функций $L_i(x)$. Эта операция соответствует выбору нулевого значения коэффициентов преобразования Уолша – Адамара WH, после чего формируется множество линейных функций, составляющих *Improvement Set*. Далее производится инвертирование элементов последовательности бент-функции, совпадающих с элементами последовательностей линейных функций из множества *Improvement Set*. В результате несбалансированность функции снижается, но снижается также и нелинейность, т.е. последовательность функции не является уже максимально отдаленной от последовательностей линейных функций $L_i(x)$. На следующей итерации все операции повторяются. Таким образом, в качестве критерия градиентного поиска криптографических функций предлагаемым методом является макимизация минимального расстояния по Хеммингу формируемой последовательности и последовательностей линейных функций.

В целом предлагаемый метод структурно состоит из трех основных этапов.

На первом этапе используются процедуры градиентного спуска, позволяющие получить высоко нелинейную последовательность.

На втором этапе используется процедуры восстановления алгебраической нормальной формы функции по выходной последовательности.

На третьем этапе, в зависимости от среды практического приложения, используется процедура модификации алгебраической нормальной формы функции *f(x)*. Это позволяет при сохранении основных показателей стойкости (сбалансированности и нелинейности) путем применения аффинных преобразований улучшить либо динамические свойства нелинейного преобразования, либо корреляционные характеристики.

Таким образом, разработанный метод позволяет формировать сбалансированные криптографические функции с высокими показателями нелинейности. При этом, как показано на рис. 1, значения нелинейности лежат в узком диапазоне значений, который зависит от размерности векторного пространства.

Следует отметить, что для современных поточных шифров важным показателем эффективности является также корреляционная иммунность, характеризующая устойчивость схемы шифрования к корреляционным атакам. Проведем оценку нелинейности и корреляционного иммунитета булевых функций, которые могут быть синтезированы разработанным методом.

3. Оценка нелинейности и корреляционного иммунитета формируемых функций

Для криптографических булевых функций известна взаимосвязь между достижимой степенью корреляционного иммунитета m и ее нелинейностью N_f [30]:

$$N_f = 2^{n-1} - 2^{m+1}, \quad (1)$$

справедливая для

$$m \geq n/2 - 2. \quad (2)$$

Как видно из (1), повышение степени корреляционного иммунитета m ведет к понижению нелинейности, и наоборот. Поэтому разработчикам средств криптографической защиты в зависимости от условий практического использования приходится находить компромисс между требуемой нелинейностью и желаемой степенью корреляционного иммунитета. Достоинство разработанного метода состоит в возможности строить функции с различными значениями криптографических показателей.

Так, например, в табл. 3 на основе (1) и (2) представлена достижимая степень корреляционного иммунитета $CI_{\max}(k)$ с указанием соответствующей нелинейности $N_{f\,\min}$. Фактически приведенные в таблице данные соответствуют нижней границе нелинейности, гарантированно получаемой при использовании разработанного метода. В табл. 4 приведена достижимая степень корреляционного иммунитета $CI_{\max}(k)$ с указанием максимально возможной нелинейности для сбалансированных функций $N_{f\,\max}$, т.е. здесь приведена верхняя граница нелинейности функций при использовании разработанного метода. На рис. 2 для наглядности табличные данные изображены в виде диаграммы.

Таблица 3

Нижняя граница нелинейности
при заданном корреляционном иммунитете

	V_4	V_6	V_8	V_{10}	V_{12}
$CI_{\max}(k)$	1	2	3	4	5
$N_{f\,\min}$	4	24	112	480	1984

Таблица 4

Верхняя граница нелинейности при заданном корреляционном иммунитете

	V_4	V_6	V_8	V_{10}	V_{12}
$CI_{\max}(k)$	1	1	2	3	4
$N_{f\max}$	4	26	116	492	2010

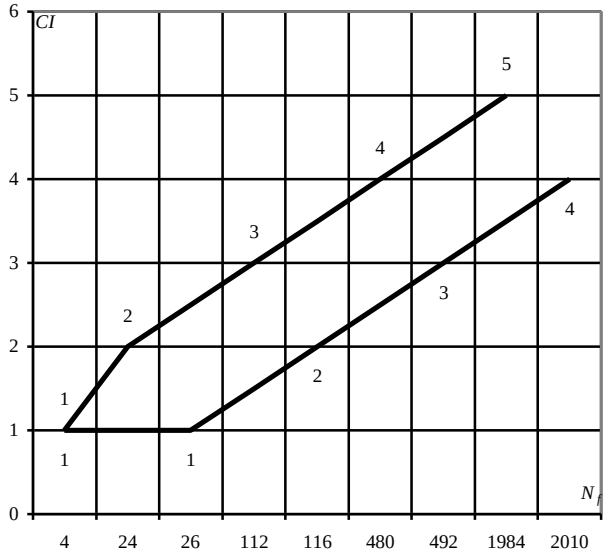


Рис. 2. Граничные показатели корреляционного иммунитета

Как показывает анализ приведенных данных, применение разработанного метода позволяет формировать булевы функции, которые, помимо высоких значений нелинейности, потенциально могут быть корреляционно-иммунными функциями. При их применении в поточных шифрах будет обеспечена высокая устойчивость к различным криптографическим атакам. Так, например, применение разработанного метода над пространством V_8 позволяет формировать функции с показателем нелинейности $N_{f\min} = 112$ и степенью корреляционного иммунитета $CI_{\max}(3)$, что является лучшим известным на сегодняшний день результатом.

Следует отметить, что вероятностный поиск эвристическими методами описывается некоторым случайным процессом, конкретная реализация которого суть случайные величины – значения показателей стойкости найденной функции (см. п. 1). Соответствующие вероятности наступления искомых случайных событий указывают на среднее число попыток до успеха – построения криптографической булевой функции с требуемыми свойствами. Таким образом, для оценки вычислительной эффективности эвристических методов, т.е. оценки соответствия полученного результата требуемому, необходимо провести оценку распределения вероятностей формирования булевых функций с различными криптографическими показателями.

4. Методика оценки эффективности эвристических методов и результаты исследований

Предлагаемая методика использует в качестве показателя вычислительной эффективности среднее число попыток, которое потребуется выполнить с использованием эвристического метода, для формирования криптографической функции с требуемыми показателями стойкости.

В соответствии с основными положениями теории вероятности и математической статистики неизвестную функцию распределения рассматриваемой случайной величины определяют по результатам наблюдений, по выборке [18]. Выборкой объема L для случайной величины A называется последовательность $X_1, X_2, \ldots, X_L$ из L независимых наблюдений этой

величины, т.е. совокупность значений, принятых L независимыми случайными величинами $A_1, A_2, \ldots, A_L$, имеющими тот же закон распределения $F_A(x)$, что и рассматриваемая величина A. В этом случае говорят, что выборка $X_1, X_2, \ldots, X_L$ взята из генеральной совокупности величины A, а под законом распределения генеральной совокупности понимают закон распределения случайной величины A. Значения $X_1, X_2, \ldots, X_L$ называют выборочными значениями [18].

Введем следующие обозначения: SI_i – случайная величина, значения которой представляют собой исходы эвристического поиска – численное выражение i-го показателя стойкости криптографической булевой функции; $X_1, X_2, \ldots, X_L$ – выборка объема L случайной величины SI_i; $F_{SI_i}(x)$ – функция распределения случайной величины SI_i.

Оценим значения теоретических функций распределения $F_{SI_i}(x)$, являющихся вероятностями событий $\{SI_i < x\}$, с помощью частот этих событий по выборке объема L. Обозначим через v_x количество выборочных значений, меньших x. Тогда $\frac{v_x}{L}$ частоты попадания выборочных значений левее точки x в данной выборке, т.е. частоты событий $\{SI_i < x\}$. Эти частоты являются функциями от x и являются, соответственно, эмпирическими функциями распределения $F^*_{SI_i}(x)$ случайных величин SI_i, полученными по данной выборке: $F^*_{SI_i}(x) = \frac{v_x}{L}$. Частота события в L независимых опытах является оценкой для вероятности этого события, т.е.

$$F_{SI_i}(x) \approx F^*_{SI_i}(x) = \frac{v_x}{L}.$$

Используя функцию распределения $F_{SI_i}(x)$, введем показатель вычислительной эффективности эвристических методов как среднее число K_{cp} попыток вероятностного формирования булевой функции с требуемыми свойствами:

$$K_{cp} = \frac{1}{F_{SI_i}(x)} \approx \frac{1}{F^*_{SI_i}(x)}.$$

Если принять предположение о статистической независимости m случайных величин SI_i, $i = 1,..,m$, тогда вероятность формирования криптографической функции с показателями $SI_i < x, i = 1,..,m$ будет определяться вероятностью совместного события, записанной через произведение вероятностей независимых событий: $\prod_{i=1}^{m} F_{SI_i}(x)$.

Среднее число попыток вероятностного формирования криптографической функции с $SI_i < x, i = 1,..,m$ вычислим по выражению

$$K_{cp} = \frac{1}{\prod_{i=1}^{m} F_{SI_i}(x)} \approx \frac{1}{\prod_{i=1}^{m} F^*_{SI_i}(x)}.$$

Наибольший интерес в криптографических целях представляют два основных показателя: нелинейность N_f и автокорреляция AC [1 – 17], причем необходимо максимизировать нелинейность и минимизировать автокорреляцию. Для оценки вычислительной эффективности по этим двум показателям стойкости последнее выражение перепишем в виде

$$K_{cp} = \frac{1}{\left(1 - F_{N_f}(x)\right) \cdot F_{AC}(x)} \approx \frac{1}{\left(1 - F^*_{N_f}(x)\right) \cdot F^*_{AC}(x)},$$

где $F_{N_f}(x)$ и $F^*_{N_f}(x)$ – теоретическое и эмпирическое значение вероятностей наступления события $\{N_f \le x\}$; $F_{AC}(x)$ и $F^*_{AC}(x)$ – теоретическое и эмпирическое значение вероятностей наступления события $\{AC \le x\}$;

Используя показатель K_{cp}, проведем сравнительные исследования вычислительной эффективности эвристических методов вероятностного формирования криптографических

булевых функций. В качестве объекта исследования будут выступать метод случайной генерации [1 – 17], метод градиентного подъема и предложенный в [16] эвристический метод градиентного спуска [17].

На рис. 3 представлены гистограммы частот событий $\{N_f = x\}$ для сбалансированных булевых функций, построенных над V_8, объем выборки L =10000. Как видно из приведенных данных, эвристический метод градиентного спуска (IKK) позволяет формировать булевы функции с показателями нелинейности $N_f \geq 114$ с вероятностью 1, $N_f \geq 116$ с вероятностью 0.5. Следующий за ним по вычислительной эффективности метод градиентного подъема (MSD) позволяет формировать криптографические функции с показателями нелинейности $N_f \geq 112$ с вероятностью 1, $N_f \geq 114$ с вероятностью 0.5 и $N_f \geq 116$ с вероятностью 0.1. Метод же случайной генерации (RG) является вообще малоэффективным, наиболее вероятное значение нелинейности находится в диапазоне 80 – 104.

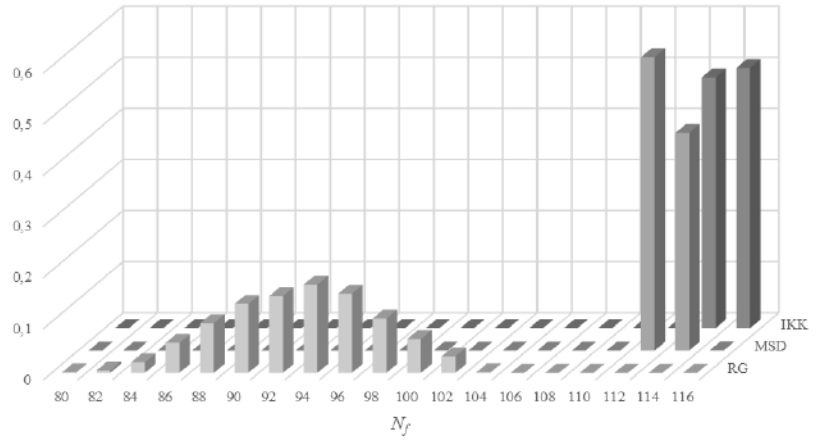


Рис. 3. Гистограммы частот событий $\{N_f = x\}$, объем выборки L = 10000

На рис. 4 представлены гистограммы частот событий $\{AC = x\}$ для сбалансированных булевых функций, построенных над V_8, объем выборки L =10000.

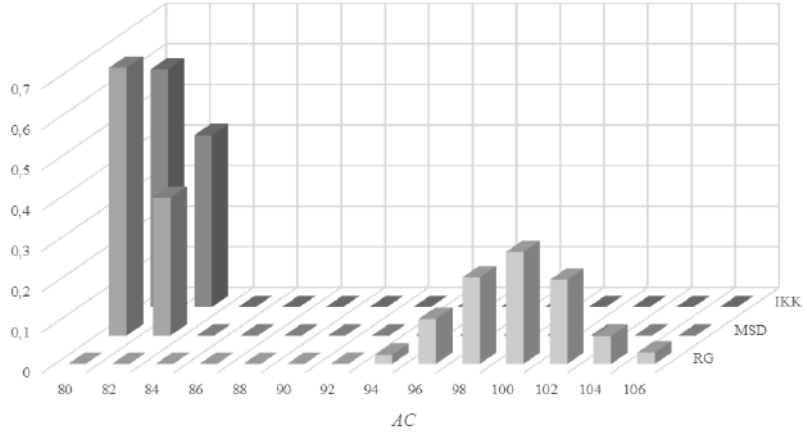


Рис. 4. Гистограммы частот событий $\{AC = x\}$, объем выборки L = 10000

Как показывает анализ, эвристический метод градиентного спуска не уступает ближайшему аналогу – методу градиентного поиска. Он позволяет формировать булевы функции с низким показателем автокорреляции.

На рис. 5 представлены зависимости K_{cp} для: метода случайной генерации с AC = 80 (RG, AC=80); метода случайной генерации с AC = 120 (RG, AC=120); метода градиентного подъема с AC = 24 (MCD, AC=24); метода градиентного подъема с AC = 32 (MCD, AC=32); метода градиентного спуска с AC = 24 (IKK, AC=24); метода градиентного спуска с AC = 32 (IKK, AC=24).

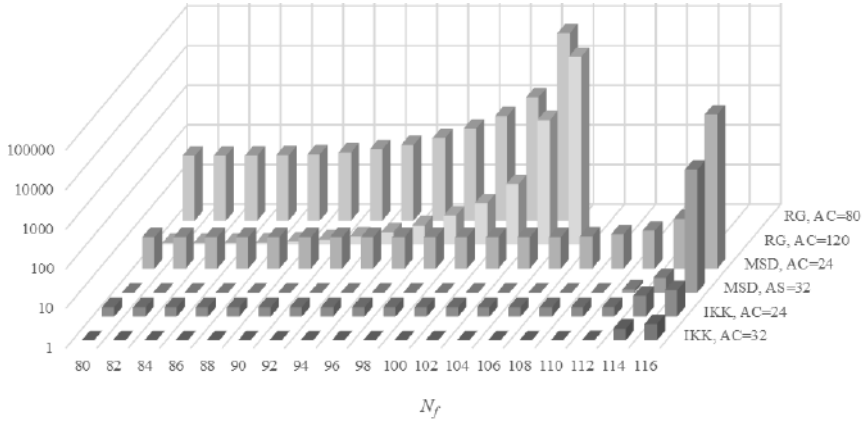


Рис. 5. Зависимости среднего числа K_{cp}

Анализ зависимостей, приведенных на рис. 4, показывает, что метод градиентного спуска позволяет формировать булевы функции с высокими криптографическими показателями (нелинейностью и автокорреляцией) за меньшее число попыток (в среднем). Так, например, формирование криптографической функции с AC = 24 и N=116 для метода случайной генерации вычислительно недостижимо по причине чрезвычайно высокого среднего числа попыток. Для тех же параметров метод градиентного подъема потребует в среднем около 8000 попыток. Метод градиентного спуска при тех же показателях потребует в среднем четыре попытки, т.е. среднее число попыток снизилось в 2000 раз. При требованиях к криптографическим свойствам AC = 24 и N=114 метод градиентного подъема потребует в среднем около 15 попыток, а метод градиентного спуска – около 3.

5. Криптографические свойства формируемых булевых функций

Проведем сравнительные исследования свойств криптографических булевых функций с наилучшими известными аналогами: генетическим алгоритмом [31], алгоритмами NLT и ACT [32], которые относятся к классу эвристических методов.

В табл. 5 представлены результаты сравнительной оценки нелинейности функций, полученные при использовании разработанного метода градиентного спуска, метода-прототипа (эвристического метода градиентного подъема) и наилучших известных эвристических методов (все данные, за исключением последней строки, взяты из [31]).

Приведенные данные свидетельствуют, что среди эвристических методов разработанный метод позволяет достигать наивысшей нелинейности. Высокая нелинейность свидетельствует о высокой степени замешивания данных, что определяет стойкость криптопреобразований. Нам впервые удалось построить функции с наивысшей известной нелинейностью среди эвристических методов: $N_f = 488$ для V_{10} и $N_f = 2002$ для V_{12}.

Таблица 5

Сравнительная оценка нелинейности функций

	V_6	V_8	V_{10}	V_{12}
Теоретически достижимая нелинейность	26	118	494	2014
Метод случайной генерации [31]	-	112	472	1954
Hill Climbing Method [27]	-	114	476	1960
Genetic Algorithm [31]	26	116	484	1976
NLT [32]	26	116	486	1992
ACT [32]	26	116	484	1986
Разработанный метод [28]	26	116	488	2002

В табл. 6 приведены сравнительные характеристики наилучших известных методов, позволяющих строить функции с низкими значениями автокорреляции [31]. Как видно из приведенной таблицы, разработанный метод позволяет строить функции с низкими значе-

ниями автокорреляции. Над V_8 методы *NLT* и *ACT* позволяют строить функции с AC=16, однако при этом нелинейность равна 112. Разработанный метод позволяет строить функции с нелинейностью 116. Над всеми остальными векторными пространствами полученные значения сопоставимы с результатами для других методов.

Таблица 6

Сравнительная оценка автокорреляции функций

	V_6	V_8	V_{10}	V_{12}
Zhang Zheng [33, 34]	16	24	48	96
Maitra [35, 36]	16	24	40	80
NLT [32]	16	16	64	144
ACT [32]	16	16	56	128
Разработанный метод [28]	16	24	40	72

На рис. 6 – 10 представлены спектральные свойства булевых функций, построенных различными способами. В скобках приведены показатели: (n, $deg(f)$, N_f, AC).

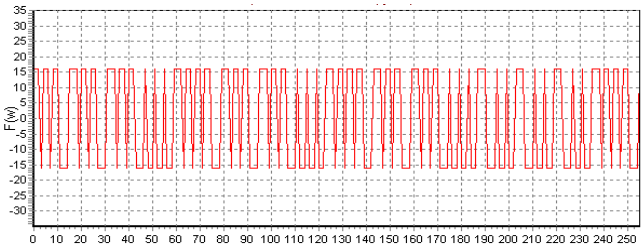


Рис. 6. Бент-функция [31 – 40]: (8, 4, 120, 0)

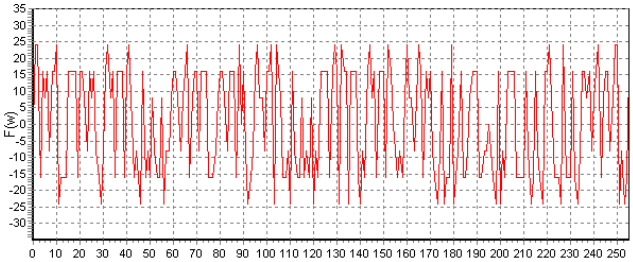


Рис. 7. Разработанный метод [28]: (8, 7, 116, 24)

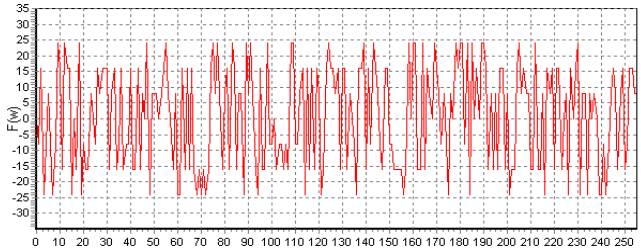


Рис. 8. Hill Climbing Method [28]: (8, 6, 116, 24)

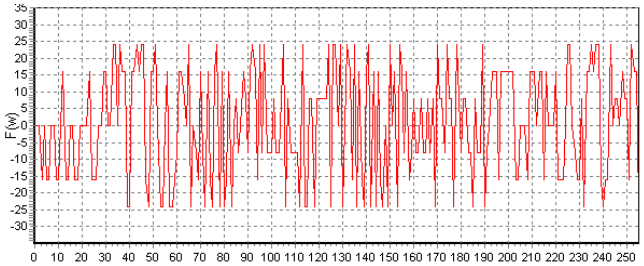


Рис. 9. Метод Maitra – Pasalic [37]: (8, 6, 116, 80)

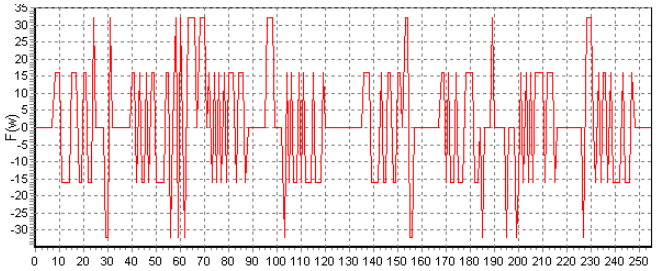


Рис. 10. Метод Seberry-Zhang [38 – 40]: (8, 4, 112, 128)

Приведенные данные показывают, что криптографические булевы функции, построенные в соответствии с разработанным методом [28], имеют максимально достижимую алгебраическую степень, высокую нелинейность низкую автокорреляцию. По большинству показателей стойкости сформированные функции не уступают известным методам.

Выводы

Проведенные исследования вычислительной эффективности эвристических методов показали, что методы градиентного поиска позволяют за приемлемое число итераций формировать криптографические булевы функции с высокими показателями нелинейности и низкой автокорреляцией. Метод градиентного спуска, предложенный в [17], оказался эффективнее Hill Climbing Method из [16]. В частности, результаты экспериментальных исследований показывают, что метод градиентного спуска из [28] требует в десятки раз меньшее число итераций, т.е. он значительно эффективнее в вычислительном аспекте. Предложенная методика оценки вычислительной эффективности эвристических методов может быть использована и для других методов, в том числе использующих расширенный набор показателей стойкости.

Сравнительные исследования криптографических свойств булевых функций показали, что формируемые предложенным вычислительным методом функции обладают высокими показателями: показатель нелинейности приближается к верхней теоретической границе; показатель автокорреляции является одним из самых низких по сравнению с другими методами синтеза; при равных показателях нелинейности формируемые функции имеют максимально достижимую алгебраическую степень; все известные методы синтеза уступают по спектральным характеристикам функций. Таким образом, на основе проведенных исследований можно сделать вывод о том, что функции, построенные в соответствии с разработанным методом [28], имеют высокие показатели стойкости и превосходят по данным показателям известные функции.

Перспективным направлением дальнейших исследований является разработка вероятностной модели синтеза нелинейных узлов замен с высокими криптографическими свойствами, проведение экспериментальных исследований и обоснование практических рекомендаций по внедрению полученных результатов.

Список литературы:

1. Information technology. Security techniques. Encryption algorithms. Part 3: Block ciphers. ISO/IEC 18033-3: 2010, 2010.

2. Advanced Encryption Standard. Federal Information Processing Standards Publications FIPS-197, 2001.

Information technologies. Cryptographic Data Security. Symmetric block transformation algorithm. National Standard of Ukraine DSTU 7624:2014, 2015 (in Ukr.).

3. Information technology. Cryptography protection of information. Block ciphers. National Standard of Russian Federation GOST R 34.12-2015, 2015 (in Rus.).

4. Information technology and security. Information security. Cryptography encryption and integrity control algorithms. State Standard of the Republic of Belarus STB 34.101.31-2011, 2011.

5. O.O. Kuznetsov, Yu.I. Gorbenko, I.M. Bilozertsev, A.V. Andrushkevych, O.P. Narizhnyi. Algebraic Immunity of Non-linear Blocks of Symmetric Ciphers // Telecommunications and Radio Engineering. – 2018. – Vol. 77, Issue 4. – P. 309-325.

6. B. N. Tran, T. D. Nguyen and T. D. Tran. A New S-Box Structure to Increase Complexity of Algebraic Expression for Block Cipher Cryptosystems // International Conference on Computer Technology and Development, Kota Kinabalu, 2009. – P. 212-216.

7. A. Kuznetsov, R. Serhiienko, D. Prokopovych-Tkachenko and Y. Tarasenko. Evaluation of Algebraic Immunity of modern block ciphers // IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, 2018. – P. 288-293.

8. M. McLoone and J. V. McCanny. High-performance FPGA implementation of DES using a novel method for implementing the key schedule // IEE Proceedings – Circuits, Devices and Systems, vol. 150, no. 5, pp. 373, 6 Oct. 2003.

9. A. Kuznetsov, I. Kolovanova and T. Kuznetsova. Periodic characteristics of output feedback encryption mode // 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kharkov, 2017. – P. 193-198.

10. S. Sulaiman, Z. Muda and J. Juremi. The new approach of Rijndael key schedule // Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), Kuala Lumpur, 2012, pp. 23-27.

11. O. Kuznetsov, Y. Gorbenko and I. Kolovanova. Combinatorial properties of block symmetric ciphers key schedule // Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T), Kharkiv, 2016, pp. 55-58.

12. F. H. Nejad, S. Sabah and A. J. Jam. Analysis of avalanche effect on advance encryption standard by using dynamic S-Box depends on rounds keys // International Conference on Computational Science and Technology (ICCST), Kota Kinabalu, 2014, pp. 1-5.

13. H. Liu and C. Jin. Lower Bounds of Differential and Linear Active S-boxes for 3D-like Structure // The Computer Journal, vol. 58, no. 4, pp. 904-921, April 2015.

14. A. Kuznetsov, Y. Gorbenko, A. Andrushkevych and I. Belozersev. Analysis of block symmetric algorithms from international standard of lightweight cryptography ISO/IEC 29192-2 // 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kharkov, 2017, pp. 203-206.

15. I. Gorbenko, A. Kuznetsov, M. Lutsenko and D. Ivanenko. The research of modern stream ciphers // 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kharkov, 2017, pp. 207-210.

16. A. Kuznetsov, V. Frolenko, E. Eremin and O. Zavgorodnia. Research of cross-platform stream symmetric ciphers implementation // IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, 2018, pp. 300-305.

17. I. Gorbenko, O. Kuznetsov, Y. Gorbenko, A. Alekseychuk and V. Tymchenko, "Strumok keystream generator," 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, 2018, pp. 294-299.

18. V. Gopi and E. Logashanmugam. Design and analysis of nonlinear AES S-box and mix-column transformation with the pipelined architecture // International Conference on Current Trends in Engineering and Technology (ICCTET), Coimbatore, 2013, pp. 235-238.

19. H. Wang, H. Zheng, B. Hu and H. Tang. Improved Lightweight Encryption Algorithm Based on Optimized S-Box // International Conference on Computational and Information Sciences, Shiyang, 2013, pp. 734-737.

20. I. Das, S. Nath, S. Roy and S. Mondal. Random S-Box generation in AES by changing irreducible polynomial // International Conference on Communications, Devices and Intelligent Systems (CODIS), Kolkata, 2012, pp. 556-559.

21. Y. Chen, W. Tian and Y. Zhang. Construction for Balanced Boolean Function with Maximum Algebraic Immunity // 7th International Conference on Advanced Software Engineering and Its Applications, Haikou, 2014, pp. 32-34.

22. C. E, S. Liang and T. Zhang. Construction Method of Boolean Functions Based on Genetic Algorithm // 7th International Conference on Wireless Communications, Networking and Mobile Computing, Wuhan, 2011, pp. 1-4.

23. R. Asthana, N. Verma and R. Ratan. Generation of Boolean functions using Genetic Algorithm for cryptographic applications // IEEE International Advance Computing Conference (IACC), Gurgaon, 2014, pp. 1361-1366.

24. Bharti and D. K. Sharma. Searching boolean function using simulated annealing and hill climbing optimization techniques // International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), Ramanathapuram, 2016, pp. 62-64.

25. W. Millan, J. Fuller and E. Dawson. New concepts in evolutionary search for Boolean functions in cryptology // Evolutionary Computation, 2003. CEC '03. The 2003 Congress on, 2003, pp. 2157-2164 Vol.3.

26. S. Picek, C. Carlet, S. Guilley, J. F. Miller and D. Jakobovic. Evolutionary Algorithms for Boolean Functions in Diverse Domains of Cryptography // Evolutionary Computation, vol. 24, no. 4, pp. 667-694, Dec. 2016.

27. W. Millan, A. Clark, E. Dawson. Smart Hill Climbing Finds Better Boolean Functions // Proceedings of the Workshop on Selected Areas on Cryptography SAC 97, Springer-Verlag, pp. 50-63, 1997.

28. Y. Izbenko, V. Kovtun and A. Kuznetsov. The Design of Boolean Functions by Modified Hill Climbing Method // Sixth International Conference on Information Technology: New Generations, Las Vegas, NV, 2009, pp. 356-361.

29. A statistical test suite for random and pseudorandom number generators for cryptographic applications. NIST Special Publication 800-22, 2001.

30. E. Pasalic and T. Johansson. Further results on the relation between nonlinearity and resiliency of Boolean functions // Proc. IMA Conf. Cryptography and Coding (Lecture Notes in Computer Science). New York: Springer-Verlag, 1999, vol. 1746, pp. 35–45.

31. Clark J., Jacob S., Stepney S., Maitra, Millan W. Evolving Boolean Functions Satisfying Multiple Criteria // Proceedings of INDOCRYPT'02. LNCS Vol. 2551, Springer (2002) 246-259.

32. Millan W., Clark A., Dawson E. An Effective Genetic Algorithm for Finding Highly Non-linear Boolean Functions // Proceedings of the First International Conference on Information and Communications Security. LNCS Vol. 1334. Springer-Verlag, Berlin Heidelberg New York (1997) 149-158.

33. Y. Zheng and X. M. Zhang. Improved upper bound on the nonlinearity of high order correlation immune functions // Selected Areas in Cryptography-SAC 2000, Lecture Notes in Computer Science, Volume 2012, pages 264–274. Springer Verlag, 2000.

34. X-M. Zhang and Y. Zheng. GAC-the criterion for global avalanche characteristics of cryptographic functions // Journal of Universal Computer Science, 1(5):316–333, 1995.

35. S. Maitra. Highly nonlinear balanced Boolean functions with very good autocorrelation property // Workshop on Coding and Cryptography-WCC 2001, Paris, January 8–12, 2001. Electronic Notes in Discrete Mathematics, Volume 6, Elsevier Science, 2001.

36. S. Maitra. Autocorrelation properties of correlation immune Boolean functions // INDOCRYPT 2001, Lecture Notes in Computer Science Volume 2247, pages 242–253. Springer Verlag, December 2001.

37. S. Maitra and E. Pasalic. Further constructions of resilient Boolean functions with very high nonlinearity // IEEE Transactions on Information Theory, 48(7): 1825–1834, July 2002.

38. J. Seberry, X.-M. Zhang and Y.Zheng. Nonlinearity and Propagation Characteristics of Balanced Boolean Functions // Information and Computation, Vol. 119, No 1, pp. 1 – 13, 1995.

39. J.Seberry, X.M.Zhang, Y.Zheng. On Constractions and Nonlinearity of Correlation Immune Functions // Advances in Cryptology – EUROCRYPT'93, vol.765, Lecture Notes in Computer Science, Springer-Verlag, pp.181-199,1994.

40. J. Seberry and X. Zhang. Hadamar Matrices, Bent Functions and Cryptography // J.H.Dinitz and D.R. Stinson, editors, Contemporary Design Theory: A Collection of Surveys,chapter 11, pages 431-559, John Wiley and Sons, Inc, 1995.

Харьковский национальный
университет имени В.Н.Каразина;
Харьковский национальный университет
Воздушных Сил имени Ивана Кожедуба;
Университет таможенного дела и финансов, Днепр

Поступила в редколлегию 04.11.2018

УДК 004.056.5

А.В. АХМАМЕТЬЕВА, канд.техн.наук, Мпуту Кристофер БВАБВА

СТЕГАНОАНАЛИЗ ЦИФРОВЫХ ИЗОБРАЖЕНИЙ В УСЛОВИЯХ РАЗЛИЧНОЙ СТЕПЕНИ НАПОЛНЕННОСТИ КОНТЕНТОВ

Введение

Широкое использование цифровых технологий и компьютерной техники в любой сфере деятельности человека приводит к необходимости защиты информации от утечки или несанкционированного использования и копирования. Ввиду ограничений на применение криптографических средств получили распространение разработки в области стеганографии, позволяющей организовать скрытый канал передачи конфиденциальных данных, который может быть использован злоумышленниками для кражи ценной информации. Поэтому важной задачей является развитие стеганоанализа, направленного на выявление какой-либо дополнительной информации (ДИ) в анализируемом цифровом контенте [1, 2]. Наиболее удобным контейнером в стеганографии является цифровое изображение (ЦИ) благодаря наличию в нем избыточной информации и возможности сокрытия значительного объема данных.

В большинстве современных исследований, посвященных стеганоанализу ЦИ [3 – 5], вычислительные эксперименты проводятся на основе изображений в градациях серого, что не совсем отражает текущее состояние современных медиаконтентов – ведь в качестве контейнеров выбирают цветные изображения, которые легко получить с помощью любых устройств (цифровых фотоаппаратов, смартфонов, планшетов и др.) или из базы изображений [6 – 9]. ЦИ в градациях серого в современном мире достаточно редкое явление, как правило, это профессиональные художественные фото, которых нет (или очень мало) в открытом доступе. С одной стороны, стеганоанализ ЦИ в градациях серого нетрудно применить и для цветных изображений, анализируя каждую цветовую составляющую в отдельности, а с другой стороны, остаются неучтенными особенности цветов изображения – триплетов значений яркости красной, зеленой и синей цветовых составляющих. Именно на основе учета этих особенностей в работах [10, 11] разработан наиболее эффективный в условиях малых значений пропускной способности скрытого канала связи (СПС) стеганоаналитический метод для ЦИ и видео.

Однако при вычислительных экспериментах в [10] рассматриваются только случаи погружения ДИ в одну произвольную цветовую составляющую цветных изображений, что несколько сужает его область применения.

Цель и задачи исследования

Цель работы – усовершенствование стеганоаналитического метода, основанного на анализе последовательных триад цветовых триплетов в матрице уникальных цветов, позволяющего выявлять наличие вложений ДИ в условиях разной степени наполненности цветных ЦИ.

Под разной степенью наполненности ЦИ будем понимать погружение ДИ в одну, две или три цветовые составляющие цветных изображений.

Для достижения поставленной цели необходимо решить следующие задачи:

- проанализировать влияние погружения ДИ в пространственную область ЦИ при условии заполнения двух и трех цветовых составляющих;
- провести уточнение параметров оригинального стеганоаналитического метода с учетом анализа последовательных триад цветовых триплетов в матрице уникальных цветов при условии разной степени наполненности ЦИ;
- выявить отличия в количестве последовательных триад цветовых триплетов в матрице уникальных цветов стеганосообщений (СС), полученных на основе контейнеров в формате с потерями, и оригинальных контейнеров в формате без потерь;

– разработать основные шаги стеганоаналитического метода, способного выявлять вложения ДИ в условиях разной степени наполненности ЦИ.

Основные результаты исследований

В качестве контейнеров для стеганопреобразования будем рассматривать цветные ЦИ в формате с потерями, представленные в соответствии с цветовой схемой RGB, где каждый пиксель изображения описывается как триплет значений (r_{mn}, g_{mn}, b_{mn}), r_{mn}, g_{mn}, b_{mn} – значения яркости (m,n)-го пикселя красной, зеленой и синей цветовых матриц соответственно. Уникальные триплеты ЦИ будем называть уникальными цветами, их количество обозначим U.

Стеганоаналитический метод [10] основан на подсчете количества последовательных Red-, Green- и Blue-триад в матрице уникальных цветов UCT, содержащей U упорядоченных уникальных триплетов (r_k, g_k, b_k), $k = \overline{1,U}$. Под последовательными Red-, Green- и Blue-триадами будем понимать:

$$(r_k, g_k, b_k) \in UCT \; AND (r_k - 1, g_k, b_k) \in UCT \; AND (r_k + 1, g_k, b_k) \in UCT, k = \overline{1,U}; \quad (1)$$

$$(r_k, g_k, b_k) \in UCT \; AND (r_k, g_k - 1, b_k) \in UCT \; AND (r_k, g_k + 1, b_k) \in UCT, k = \overline{1,U}; \quad (2)$$

$$(r_k, g_k, b_k) \in UCT \; AND (r_k, g_k, b_k - 1) \in UCT \; AND (r_k, g_k, b_k + 1) \in UCT, k = \overline{1,U} \quad (3)$$

соответственно. При подсчете количества последовательных триад триплетов в матрице уникальных цветов будем использовать понятие среднего триплета $(r_k, g_k, b_k) \in UCT$, для которого выполняются условия (1), (2) или (3) в зависимости от вида триады.

Пустой контейнер в формате с потерями содержит не более 2,5 % средних триплетов, соответствующих Red-, Green- и Blue-триадам [10], при погружении ДИ их количество значительно возрастает и в случае одной заполненной цветовой составляющей указывает на цветовую матрицу изображения, используемую в процессе стеганопреобразования. С целью выявления характера изменений количества Red-, Green- и Blue-триад при погружении ДИ в две и три цветовые составляющие был проведен вычислительный эксперимент на основе 300 ЦИ в формате с потерями, где ДИ погружалась:

– в красную и синюю матрицы;
– в зеленую и синюю матрицы;
– в красную и зеленую матрицы;
– во все три цветовые составляющие изображения.

При погружении ДИ значения СПС составляли 0,2 бит/пиксель, 0,1 бит/пиксель.

В ходе вычислительного эксперимента установлено, что возмущения в количестве последовательных триад при погружении ДИ в две и три цветовые составляющие ЦИ несколько отличаются от возмущений при вложении ДИ в одну произвольную матрицу: значения количества Red-, Green- и Blue-триад одного изображения между собой находятся в соотношении менее чем в 1,5 раза. Однако в зависимости от СПС и того, какая цветовая составляющая использовалась при стеганопреобразовании, возникает высокая вероятность некорректного выявления СС. В табл. 1 приведены ошибки, возникающие при определении стеганоаналитическим методом [10] СС, сформированного погружением ДИ в две и три цветовые составляющие, как СС только с одной заполненной цветовой составляющей.

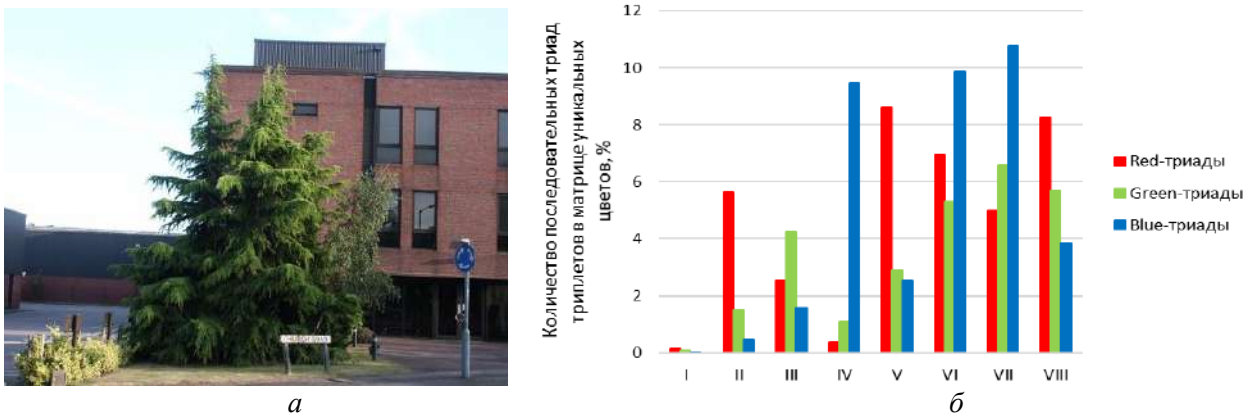
Таблица 1

Ошибки при определении степени наполнения СС, %

Степень наполнения	СПС 0.2 бит/пиксель			СПС 0.1 бит/пиксель		
	Красная	Зеленая	Синяя	Красная	Зеленая	Синяя
Красная и зеленая	0	0.33	0.33	0.67	0	23.67
Красная и синяя	0	0	0.33	0	1.33	1.33
Зеленая и синяя	8	0	0.67	24	0	10.33
Красная, зеленая, синяя	1.33	2.67	9.33	18	12.33	26.33

Как видно из табл. 1, количество ошибок возрастает с уменьшением значения СПС. При этом мы наблюдаем ситуацию, когда выявленная цветовая составляющая как заполненная на самом деле таковой не является: в 23.67 % СС выявлена синяя цветовая составляющая (СС сформированы погружением ДИ в красную и зеленую матрицы при СПС 0,1 бит/пиксель), в 8 и 24 % СС выявлена красная цветовая составляющая (СС сформированы погружением ДИ в зеленую и синюю матрицы при СПС 0,2 и 0,1 бит/пиксель соответственно). В случае же трех заполненных матриц количество Red-, Green- и Blue-триад неравномерно, в 13,33 и 56,67 % СС (при СПС 0,2 и 0,1 бит/пиксель соответственно) определяется только одна матрица, что неверно.

На рис. 1 приведен пример содержания последовательных триад триплетов в ЦИ при условии разной степени наполненности цветовых составляющих.



а *б*

Рис.1. Количество последовательных цветовых триад в изображении: а) ЦИ; б) количество триад в ЦИ и СС, сформированных погружением ДИ при СПС 0.1 бит/пиксель с разной степенью наполненности: I – оригинальный контейнер; II – заполнена красная цветовая составляющая; III – заполнена зеленая цветовая составляющая; IV – заполнена синняя цветовая составляющая; V – заполнены все цветовые составляющие; VI – заполнены красная и синяя цветовые составляющие; VII – заполнены зеленая и синяя цветовые составляющие; VIII – заполнены красная и зеленая цветовые составляющие

Как видно из рис. 1, в случае I однозначно определяется пустой контейнер; в случаях II, III и IV возмущения Red-, Green- и Blue-триад указывают на заполненные красную, зеленую и синюю цветовые составляющие соответственно; в случае V можно заподозрить наличие ДИ в красной матрице, хотя на самом деле заполнены все; в случае VI предполагаются две или три заполненные матрицы; в случае VII может быть выявлена только синяя цветовая составляющая, а зеленая пропущена; в случае VIII количество Red-триад указывает на красную матрицу, хотя заполненной была и зеленая.

С учетом полученных в ходе эксперимента результатов проведем уточнение параметров стеганоаналитического метода [10], а именно величины $V = 1.5$, определяющей величину разрыва между триадами разного вида ЦИ в условиях:

$$pR = \max(pR, pG, pB) \;\&\; pR > V \cdot pG \;\&\; pR > V \cdot pB; \quad (4)$$

$$pG = \max(pR, pG, pB) \;\&\; pG > V \cdot pR \;\&\; pG > V \cdot pB; \quad (5)$$

$$pB = \max(pR, pG, pB) \;\&\; pB > V \cdot pR \;\&\; pB > V \cdot pG; \quad (6)$$

указывающих на красную, зеленую или синюю цветовую составляющую соответственно.

В ходе вычислительного эксперимента при проведении стеганоанализа СС в условиях (4) – (6) значения $V \in [1.25, 2]$ с шагом 0,05, после чего определяются ошибки 1-го (FN) и 2-го рода (FP), где ошибки 1-го рода – пропуск СС, ошибки 2-го рода – определение пустого контейнера как СС. В результате эксперимента на основе 2400 ЦИ (300 контейнеров, 900 СС с одной заполненной матрицей, 900 СС с двумя заполненными матрицами, 300 СС с тремя заполненными матрицами) установлено, что с уменьшением параметра V уменьшаются ошибки 1-го рода, но при этом увеличиваются ошибки 2-го рода: для СПС 0.2 бит/пиксель при $V = 1.25$ $FN = 0.1111\%, FP = 0.1852\%$, а при $V = 2$ $FN = 1\%, FP = 0\%$; для СПС 0,1 бит/пиксель при $V = 1.25$ $FN = 1.1111\%, FP = 0.1852\%$, а при $V = 2$ $FN = 5\%, FP = 0\%$ (табл. 2). Таким образом, в стеганоаналитическом методе [10] допустимо принять $V = 1.5$, т.к. дальнейшее увеличение V приводит к резкому скачку ошибок 1-го рода. При этом уменьшение параметра V также нецелесообразно, поскольку это приведет к увеличению ошибок при детектировании СС, сформированных погружением ДИ в одну цветовую составляющую.

Таблица 2

Ошибки 1-го и 2-го рода при изменении параметра V стеганоаналитического метода [10], %

	СПС 0,1 бит/пиксель							
V	1,25	1,3	1,35	1,4	1,45	1,5	1,55	1,6
FN	1,1111	1,1111	1,2222	1,2222	1,2222	1,2222	1,4444	1,5556
FP	0,1852	0,1852	0,1852	0,1852	0,1481	0,0741	0,037	0,037
V	1,65	1,7	1,75	1,8	1,85	1,9	1,95	2
FN	1,7778	2,1111	2,4444	2,7778	3,3333	3,6667	4,2222	5
FP	0,037	0,037	0,037	0	0	0	0	0
	СПС 0,2 бит/пиксель							
V	1,25	1,3	1,35	1,4	1,45	1,5	1,55	1,6
FN	0,1111	0,2222	0,2222	0,3333	0,3333	0,3333	0,5556	0,5556
FP	0,1852	0,1852	0,1852	0,1852	0,1481	0,0741	0,037	0,037
V	1,65	1,7	1,75	1,8	1,85	1,9	1,95	2
FN	0,5556	0,5556	0,5556	0,5556	0,7778	0,8889	1	1
FP	0,037	0,037	0,037	0	0	0	0	0

Поскольку в результате стеганопреобразования пространственной области все СС сохраняются в формате без потерь, при анализе имеющегося ЦИ неизвестно, какой контейнер был использован: в формате с потерями, или в формате без потерь. Если формат с потерями – можно по крайней мере установить факт наличия или отсутствия в анализируемом контенте ДИ, в случае формата без потерь оригинального контейнера – количество Red-, Green- и Blue-триад в таких ЦИ изначально очень высокое, что не позволит выявить СС [12]. Таким образом, задача определения степени наполненности СС неразрывно связана с определением формата оригинального контейнера. Кроме того, при погружении ДИ в ЦИ в формате без потерь количество последовательных триад триплетов практически не меняется – эту особенность мы будем использовать при усовершенствовании стеганоаналитического метода.

В работе [12] предложен метод выявления факта сжатия ЦИ, также основанный на анализе количества последовательных триад триплетов в матрице уникальных цветов, однако при вычислительных экспериментах рассматриваются только оригинальные контейнеры, и пороговое значение $T_{\lim} = 7.5$ [12] может применяться только для отделения пустых цифровых контентов. Если же необходимо выявить исходный формат СС, необходимо изменить подход к выявлению факта сжатия. Поскольку в условиях СС количество средних триплетов разного вида превышает пороговое значение $T_{\lim}$, а в основе обоих методов [10] и [12] лежит подсчет количества Red-, Green- и Blue-триад в матрице уникальных цветов изображения, поэтому выявление факта сжатия анализируемого ЦИ и его стеганоанализ будут проводиться параллельно.

Выполним интеграцию базового стеганоаналитического метода [10] и метода выявления факта сжатия цифровых контентов [12] с целью обеспечения возможности определять СС, сформированные с разной степенью заполнения цветовых составляющих. По результатам стеганоанализа изображения должна быть получена следующая информация: формат оригинального контейнера *format*, степень наполненности СС *degree*, цветовая составляющая *component*, используемая в стеганопреобразовании (при условии одной заполненной цветовой матрицы). Основный шаги усовершенствованного стеганоаналитического метода следующие.

Шаг 1. Формирование матрицы UCT размером $U \times 3$ уникальных триплетов цветов $(r_k, g_k, b_k), k = \overline{1,U}$ для ЦИ I.

Шаг 2. Подсчет количества последовательных триад для каждой цветовой составляющей.

2.1 *Если* для текущего триплета $(r_k, g_k, b_k), k = \overline{1,U}$ в UCT одновременно существуют триплеты $(r_k + 1, g_k, b_k)$ и $(r_k - 1, g_k, b_k)$, *то* $countR = countR + 1$, $countR$ – количество Red-триад в UCT;

2.2 *Если* для текущего триплета $(r_k, g_k, b_k), k = \overline{1,U}$ в UCT одновременно существуют триплеты $(r_k, g_k + 1, b_k)$ и $(r_k, g_k - 1, b_k)$, *то* $countG = countG + 1$, $countG$ – количество Green-триад в UCT;

2.3 *Если* для текущего триплета $(r_k, g_k, b_k), k = \overline{1,U}$ в UCT одновременно существуют триплеты $(r_k, g_k, b_k + 1)$ и $(r_k, g_k, b_k - 1)$, *то* $countB = countB + 1$, $countB$ – количество Blue-триад в UCT.

Шаг 3. Вычислить:

$$pR = \frac{countR}{U} \cdot 100, \; pG = \frac{countG}{U} \cdot 100, \; pB = \frac{countB}{U} \cdot 100.$$

Шаг 4. Детектирование наличия/отсутствия ДИ.

4.1 *Если* $pR < T_{low}$ & $pG < T_{low}$ & $pB < T_{low}$,
то $format = $"*с потерями*",
$degree = $"*пустой контейнер*",
$component = $"*нет заполненных цветовых составляющих*";

4.2 *иначе если* $pR = \max(pR, pG, pB)$ & $pR > V \cdot pG$ & $pR > V \cdot pB$,
то $format = $"*с потерями*",
$degree = $"*одна цветовая составляющая*",
$component = $"*красная цветовая составляющая*";

4.3 *иначе если* $pG = \max(pR, pG, pB)$ & $pG > V \cdot pR$ & $pG > V \cdot pB$,

то $format = "$*с потерями*$"$,
$degree = "$*одна цветовая составляющая*$"$,
$component = "$*зелёная цветовая составляющая*$"$;

4.4 *иначе если* $pB = \max(pR, pG, pB)\ \&\ pB > V \cdot pR\ \&\ pB > V \cdot pG;$,
то $format = "$*с потерями*$"$,
$degree = "$*одна цветовая составляющая*$"$,
$component = "$*синяя цветовая составляющая*$"$;

4.5 *иначе если* $pR < T_{low}'\ \&\ pG < T_{low}'\ \&\ pB < T_{low}'$,
то $format = "$*с потерями*$"$,
$degree = "$*пустой контейнер*$"$,
$component = "$*нет заполненных цветовых составляющих*$"$;

4.6 *иначе*

4.6.1 Погрузить произвольную бинарную последовательность во все цветовые составляющие ЦИ I с СПС 0.25 бит/пиксель, результат I'.

4.6.2 Сформировать матрицу UCT' размером $U' \times 3$ уникальных триплетов цветов $\left(r_k', g_k', b_k'\right), k = \overline{1, U'}$ для ЦИ I'.

4.6.3 Определить количество последовательных триад изображения I' для каждой цветовой составляющей, результат – $countR'$, $countG'$, $countB'$;

4.6.4 Вычислить:

$$pR' = \frac{countR'}{U'} \cdot 100,\ pG' = \frac{countG'}{U'} \cdot 100,\ pB' = \frac{countB'}{U'} \cdot 100.$$

4.6.5 Определить:

$$aR = \left|pR - pR'\right|,\ aG = \left|pG - pG'\right|,\ aB = \left|pB - pB'\right|.$$

4.6.6 *Если* $aR < T_{abs}\ \&\ aG < T_{abs}\ \&\ aB < T_{abs}$,
то $format = "$*без потерь*$"$,
$degree = "$*не определена*$"$,
$component = "$*не определена*$"$;

4.6.7 *иначе* $format = "$*с потерями*$"$,
$degree = "$*две или три цветовые составляющие*$"$,
$component = "$*не определена*$"$.

На первом этапе предлагаемого метода (шаги 1 – 3) определяется процентное содержание Red-, Green- и Blue-триад pR, pG, pB относительно общего количества уникальных цветов, используемые как для стеганоанализа, так и для выявления факта сжатия ЦИ. Далее полученные значения pR, pG, pB сравниваются с пороговым значением T_{low}, определенным в работе [10] как $T_{low} = 2.5$ (шаг 4.1): непревышение данного порога свидетельствует о пустом контейнере, а также о формате оригинального контейнера с потерями. В том случае, если наблюдается превышение максимального значения из pR, pG, pB над двумя другими в 1,5 раза (параметр V), однозначно определяется заполненная цветовая составляющая (шаги 4,2 – 4,4), и соответственно в процессе стеганопреобразования использовались ЦИ в формате с потерями.

В шаге 4.5 осуществляется сравнение значений pR, pG, pB с порогом T_{low}', что связано с тем, что некоторые оригинальные контейнеры как в формате с потерями, так и в формате без потерь содержат количество триад в диапазоне от 2,5 % до 4 – 5 %, при этом ЦИ в формате без потерь в таком случае реагируют на возмущения в результате стеганопреобразова-

ния также, как и ЦИ в формате с потерями. В качестве примера таких ЦИ в формате *.tif можно привести изображения из базы McGill [8]. Примем $T_{low}' = 4.5$. Если $pR < T_{low}'$, $pG < T_{low}'$, $pB < T_{low}'$, то такое изображение определяется как незаполненное, его формат – с потерями (в этом случае ошибки определения формата не являются существенными, т.к. возможно выявить наличие ДИ в таких контентах).

Далее для разделения СС от ЦИ в формате без потерь поверх анализируемого изображения во все три цветовые составляющие погружаем некоторую ДИ – произвольную бинарную последовательность, в результате получаем СС I', для которого определяем процент Red-, Green- и Blue-триад pR', pG', pB' и находим абсолютную разность между содержанием средних триплетов анализируемого изображения I и СС I'. Эти значения разности aR, aG, aB сравниваются с пороговым значением T_{abs}, указывающего на величину изменений в количестве последовательных триад триплетов. Использование порога T_{abs} связано с характерной особенностью ЦИ в формате без потерь, содержащих изначально большое количество средних триплетов, при возмущениях цветовых матриц сохранять практически неизменным количество Red-, Green- и Blue-триад. Таким образом, выполнение условия $aR < T_{abs}$ & $aG < T_{abs}$ & $aB < T_{abs}$ указывает на формат без потерь оригинального контейнера и, соответственно, невозможность выявить наличие ДИ в анализируемом изображении. Иначе мы имеем СС с двумя или тремя заполненными цветовыми составляющими. Примем $T_{abs} = 2$.

Для оценки эффективности предложенного стеганоаналитического метода с возможностью выявления факта сжатия оригинального контейнера проведем вычислительный эксперимент, по результатам которого определим ошибки первого и второго рода по следующим критериям:

- Критерий 1 – выявление СС и незаполненных контейнеров среди всех анализируемых ЦИ, включающих 718 контейнеров и 2218 СС с разной степенью наполненности;
- Критерий 2 – выявление цветовой составляющей среди ЦИ, включающих 718 контейнеров и 1318 СС с одной заполненной цветовой составляющей;
- Критерий 3 – определение формата оригинального контейнера среди 2936 ЦИ, изначально хранившихся в формате с потерями, и 355 ЦИ, изначально хранившихся в формате без потерь.

В случае критериев 1 и 2 под ошибками первого рода будем понимать пропуск СС, под ошибками второго рода – определение незаполненного контейнера как СС. В случае критерия 3 под ошибками первого рода будем понимать пропуск факта сжатия при его наличии, под ошибками второго рода – определение несжатого цифрового контента как подвергшегося сжатию. Результаты вычислительного эксперимента приведены в табл. 3.

Таблица 3

Эффективность выявления СС и определения формата оригинальных контейнеров для ЦИ, %

	Критерий 1	Критерий 2	Критерий 3
СПС 0.2 бит/пиксель			
Ошибки 1-го рода	1.8485	0.3035	0.1022
Ошибки 2-го рода	2.3677	0.3549	16.9184
СПС 0.1 бит/пиксель			
Ошибки 1-го рода	9.2425	0.8346	0.0341
Ошибки 2-го рода	2.3677	0.3549	16.9184

Как видно из табл. 3, разработанный стеганоаналитический метод показал высокую эффективность выявления СС, сформированных погружением ДИ в контейнеры, изначально хранимые в формате с потерями, при этом в случае одной заполненной цветовой составляю-

щей (критерий 2) ошибки минимальны. В основном ошибки возникают при выявлении СС с двумя и тремя заполненными цветовыми матрицами с уменьшением значений СПС (1,8485 % ошибок 1-го рода при СПС 0,2 бит/пиксель против 9,2425% ошибок 1-го рода при СПС 0,1 бит/пиксель). Более того, формат СС, сформированных на основе контейнеров в формате с потерями, в большинстве случаев определен верно (ошибки 1-го рода, т.е. пропуск факта сжатия, составляют всего 0,1022 %), однако 16,9184 % из ЦИ, изначально хранимых в формате без потерь, определены как подвергавшиеся сжатию и содержащие ДИ в двух и трех цветовых составляющих, что требует дополнительных исследований для более точного выявления факта сжатия анализируемых ЦИ.

Выводы

Предложено усовершенствование стеганоаналитического метода выявления вложений ДИ, основанного на учете количества последовательных триад триплетов в матрице уникальных цветов ЦИ, путем расширения его области применения, а именно возможности выявлять СС, сформированные с разной степенью наполненности цифровых контентов.

По результатам исследований проанализирован характер изменения последовательных Red-, Green- и Blue-триад в матрице уникальных цветов ЦИ в результате погружения ДИ в две и три цветовые составляющие контейнера, с учетом которого осуществлено уточнение параметров базового стеганоаналитического метода [10]. Результаты экспериментов показали, что для обеспечения корректного выявления СС, сформированных на основе погружения ДИ в две и три цветовые составляющие цветных ЦИ, изначально хранящихся в формате с потерями, необходимо установить, подвергался ли анализируемый контент сжатию, т.к. характер возмущений в результате стеганопреобразования ЦИ в формате с потерями и ЦИ в формате без потерь различный, что позволило интегрировать стеганоаналитический метод [10] и метод выявления факта сжатия [12].

Результаты экспериментов, направленных на оценку эффективности усовершенствованного стеганоаналитического метода, показали, что предложенные изменения не снижают высокой эффективности при определении заполненной цветовой составляющей изображения при условии заполнения только одной цветовой матрицы ЦИ (ошибки 1-го рода не превышают 1 %), при этом обеспечивая корректное выявление СС, сформированных при погружении ДИ в две или три цветовые составляющие (при СПС 0,2 бит/пиксель ошибки 1-го рода составляют 1,85%, ошибки 2-го рода – 2,37%). Однако при анализе ЦИ, изначально хранящихся в формате без потерь, возникают ошибки 2-го рода, что требует дополнительных исследований для более точного выявления факта сжатия анализируемых ЦИ.

При необходимости точного определения заполненных цветовых составляющих СС разработанный метод можно скомбинировать с существующими стеганоаналитическими методами, анализирующими отдельные цветовые матрицы ЦИ.

Список литературы:

1. Стеганография, цифровые водяные знаки и стеганоанализ / А.В. Аграновский, А.В. Балакин, В.Г. Грибунин, С.А. Сапожников. – Москва : Вузовская книга, 2009. – 220 с.

2. Bohme R. Advanced statistical steganalysis. – Springer, 2010. – 302 p.

3. Jean-Francois Couchot. Improving Blind Steganalysis in Spatial Domain using a Criterion to Choose the Appropriate Steganalyzer between CNN and SRM+EC / Jean-Francois Couchot, Raphael Couturier, Michel Salomon // ICT Systems Security and Privacy Protection. 32nd IFIP TC 11 International Conference, SEC 2017, Rome, Italy, May 29-31, 2017. – Pp. 327-340. DOI: https://doi.org/10.1007/978-3-319-58469-0_22

4. Wei Huang. Novel cover selection criterion for spatial steganography using linear pixel prediction error / Wei Huang, Xianfeng Zhao // Science China. Information Sciences. – 2016. – Vol. 59. – Pp. 059103:1–059103:3. DOI: 10.1007/s11432-016-5530-z

5. Tomáš Denemark. Improving Selection-Channel-Aware Steganalysis Features / Tomáš Denemark, Jessica Fridrich, Pedro Comesaña-Alfaro // IS&T International Symposium on Electronic Imaging 2016. – Pp. MWSF-080.1-MWSF-080.8.

6. NRCS Photo Gallery: [Электронный ресурс] // United States Department of Agriculture. Washington, USA. Режим доступа: http://photogallery.nrcs.usda.gov

7. Uncompressed Color Image Database (UCID) [Электронный ресурс]: Multimedia Phylogeny Datasets. Режим доступа: http://www.recod.ic.unicamp.br/~oikawa/datasets.html

8. McGill Calibrated Colour Image Database [Электронный ресурс]: Fred Kingdom's Laboratory at McGill Vision Research. Режим доступа: http://tabby.vision.mcgill.ca/html/welcome.html

9. Never-compressed image database [Электронный ресурс]: Sam Houston State University. Режим доступа: http://www.shsu.edu/qxl005/New/Downloads/

10. Ахмаметьева А.В. Стеганоанализ цифровых изображений, хранящихся в формате с потерями // Захист інформації. – 2016. – Вип. 23. – С.135-145.

11. Akhmametieva A. Steganalysis of digital contents, based on the analysis of unique color triplets // Annales Mathematicae et Informaticae. – 2017. – No.47. – Pp. 3-18.

12 Akhmametieva A. Method of detection the fact of compression in digital images as an integral part of steganalysis // Інформатика та математичні методи в моделюванні. – 2016. – Т.6. – №4. – С. 357-364.

Одесский национальный
политехнический университет

Поступила в редколлегию 12.11.2018

УДК 004.043

Д.Г. БІЛІЧЕНКО, К.Ю. ВІТЮК, Р.В. ОЛІЙНИКОВ, д-р техн. наук

ПОРІВНЯЛЬНИЙ АНАЛІЗ АЛГОРИТМІВ КОНСЕНСУСУ ДЛЯ ТЕХНОЛОГІЇ РОЗПОДІЛЕНИХ РЕЄСТРІВ

Вступ

В сучасному світі технологій, що розвиваються, людям доводиться довіряти третій стороні для обміну даними. Але вона не завжди може забезпечити виконання відповідних послуг безпеки, необхідних користувачеві. Найпростішим прикладом є DDoS атака на сервер, після якої користувач на невизначений час не матиме доступу до своїх даних. Більш того, існує ряд атак, які можуть порушити цілісність даних користувача. На сьогодні вже існують технологічні рішення цієї проблеми. Одним з таких рішень є розподілений реєстр.

Метою роботи є визначення основних параметрів систем на базі технології розподілених реєстрів та вибір найбільш оптимальної галузі застосування цих систем за допомогою визначених параметрів.

Для проведення порівняльного аналізу було обрано три різні системи на основі технології розподілених реєстрів: Ethereum [1], IOTA [2] и Hedera Hashgraph [3].

В процесі аналізу були розглянуті структури реєстрів та механізми консенсусу. Порівняльний аналіз основних параметрів та їх показників, якими можна охарактеризувати обрані системи, такі як пропускна здатність і масштабованість, дав змогу визначити набір умов, необхідних для найпродуктивнішого використання тієї чи іншої системи. Також порівняльний аналіз включає в себе розгляд ряду існуючих атак на дані системи.

1. Структури розподілених реєстрів

У цій частині статті будуть розглянуті дві технології розподілених реєстрів: блокчейн [4] і спрямований ациклічний граф (DAG – Directed acyclic graph) [5]. Відкриті реєстри забезпечують зберігання транзакцій в обох технологіях. Транзакції служать вхідними даними, які змінюють стан реєстру. Однак для ведення реєстру ці два підходи використовують різні структури даних. Блокчейн зберігає транзакції в блоках, в той час як в DAG вони зберігаються у вузлах. Ці дві структури даних будуть описані і проаналізовані в наступному підрозділі.

1.1. Блокчейн

Блокчейн складається з упорядкованих елементів, які називаються блоками. Кожен блок складається з заголовка і списку транзакцій. У заголовок блоку включається: геш списку транзакцій, геш попереднього блоку і службова інформація. Перший блок в ланцюжку блокчейна називається генезис-блоком. Генезис-блок відрізняється від інших блоків тільки тим, що не має попередників [4]. Структура блокчейна зображена на рис. 1.

Рис. 1. Блокчейн як структура даних

1.2. Спрямований ациклічний граф

У порівнянні з блокчейном, структура DAG зберігає по одній транзакції в кожному вузлі. Загальна структура DAG показана на рис. 2.

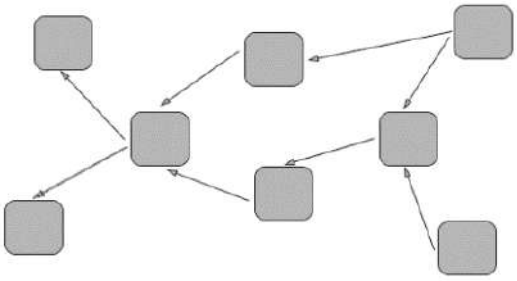


Рис. 2. Структура DAG

Існує кілька проектів на базі DAG, вони значно відрізняються один від одного, але мають деякі загальні властивості:

• ациклічність. Час йде в одному напрямку. Більш нові транзакції посилаються на більш старі, але не навпаки. В DAG кожен вузол залежить від попередніх вузлів, які посилаються на нього. Це дозволяє виконувати транзакції локально або навіть оффлайн, обробляти, підтверджувати і завершувати пізніше.

• затримка. Швидкість виконання і час підтвердження, обмежені не розміром блоку, а пропускною спроможністю між сполученими вузлами.

• без комісії. Робота мережі здійснюється без задіяння майнінгу. Кожен емітент транзакції одночасно є валідатором, або делегатом або свідком, задіяним у випадках конфліктів і суперечок.

• транзакції з нульовим значенням. Це повідомлення або не цінні транзакції, незалежно від того, чи потрібен цифровий підпис чи ні в UDP-пакеті.

• обрізка бази даних. Називається "snapshotting" в IOTA. Це дозволяє вузлам зберігати тільки ту історію, в якій вони зацікавлені або мають відношення до неї [5].

2. Консенсус

У відкритому і загальнодоступному середовищі, де кожен вузол може подивитися і доповнити реєстр, блоки та вузли можуть бути зловмисними, і їм не можна беззастережно довіряти. У таких середовищах повинен бути реалізований механізм консенсусу для чесного і безпечного функціонування системи. Існує так звана проблема Візантійських Генералів (Byzantine Fault Tolerance, BFT) [6], ця проблема полягає в тому, що система повинна забезпечувати надійність роботи при таких умовах: асинхронність, зловмисний вузол, підробка повідомлень, спам повідомлення, повідомлення можуть не доходити взагалі.

2.1. Блокчейн

Алгоритми досягнення консенсусу в блокчейн орієнтованих системах зазвичай вимагають певної форми голосування серед відомого набору учасників. Один метод, який часто називають консенсусом Накамото, обирає лідера за допомогою певної форми лотереї. Лідер потім пропонує блок, який може бути доданий до реєстру. Цей блок містить список раніше зафіксованих записів. Записи перевіряються на достовірність усіма іншими вузлами і їх послідовність підтверджується. І Bitcoin, і Ethereum засновані на функції лотереї, яка називається доказом виконання роботи (proof-of-work, PoW) [7], також Ethereum анонсував підтримку доказу володіння частки (proof-of-stake) [8] в найближчому майбутньому. Обраний лідер розсилає новий запис іншим учасникам, які неявно голосують за прийняття запису, додаючи його в свою локальну копію реєстру.

Доказ виконання роботи (proof-of-work). Цей алгоритм досягнення консенсусу призначений для підтвердження транзакцій і створення нових блоків. За допомогою PoW майнери конкурують між собою за завершення транзакцій в мережі і винагородження. Користувачі мережі надсилають один одному цифрові токени, після чого всі транзакції збираються в блоки і записуються в блокчейн. Робота мережі заснована на вирішенні складних математичних задач і можливості легко довести, що рішення отримано. Наприклад, в Bitcoin і Ethereum використовується гешування як криптографічна задача. Ця задача вимагає того, щоб геш-блоку транзакцій разом з nonce (вільна змінна в функції) відповідав певному шаблону. Шаблон по-

чинається з визначеного числа нульових біт. Вузли, які генерують блоки в PoW системах, називаються майнерами, а процес називається майнінгом. Учасник мережі, який першим вирішив задачу і знайшов потрібний геш, отримує винагороду, а транзакції в блоці вважаються підтвердженими [7].

Доказ володіння частки (proof-of-stake, PoS). У той час як в PoW системах майнери використовують свої обчислювальні ресурси, щоб бути обраними для створення блоку, proof-of-stake вимагає від учасників частки монет, які вони зберігають в мережі. Proof-of-stake вирішує проблему великих витрат на електроенергію, яка існує в PoW. Валідатори ставлять свої монети на транзакції шляхом блокування монет. Чим більше валідатор ставить, тим вище шанс, що він буде обраний для створення наступного блоку. Якщо некоректний блок був прийнятий, наприклад містив подвійну витрату, ставка валідатора згорає, тим самим забезпечуючи його покарання. PoS має деякі переваги над PoW. По-перше, кількість енергії, що витрачається в PoW, набагато більше. По-друге, покарання за проведення атаки набагато легше реалізовується в PoS. Так, наприклад, після проведення атаки в мережі на базі PoW, зловмисник все ще володіє своїм апаратним забезпеченням. У той час як в PoS ставка згорає, тим самим позбавляючи зловмисника засобів [8].

2.2. Спрямований ациклічний граф

Для досягнення консенсусу в Hashgraph використовується протокол "gossip" (плітки). Його роботу можна описати так: якийсь учасник мережі випадково вибирає іншого і передає йому інформацію, яку він знає. У свою чергу цей учасник знову передає цю інформацію вже іншому випадковому учаснику. Таким чином, якщо один учасник був обізнаний про якусь інформацію, це поширюється з експоненційною швидкістю, поки кожний учасник не знатиме цю інформацію [3].

В системі IOTA кожна наступна транзакція посилається на дві попередні, в результаті чого утворюється складний ланцюжок транзакцій, який підвищує ступінь їх підтвердженості. Цей механізм зв'язку називається Tangle [2]. Учасники мережі самі підтверджують транзакції один одного, тому немає потреби в майнерах. Щоб провести свою транзакцію потрібно вибрати дві мало підтверджені транзакції і перевірити на суперечливість спочатку їх, а потім і всі транзакції на які посилаються обрані дві. Рівень підтвердженості транзакції рахується як сума проведеної роботи самої транзакції і всіх, які прямо або побічно посилаються на неї до останніх відомих в мережі. За допомогою даного механізму в мережі досягається консенсус [9].

3. Механізми консенсусу

В даному розділі будуть порівняні механізми досягнення консенсусу в криптовалютах Ethereum, IOTA, Hedera Hashgraph.

3.1. Ethereum

На даний момент Ethereum використовує урізану версію протоколу GHOST. У ньому використовується класичний PoW. Майнеру необхідно раніше інших "знайти" правильний блок і відправити його іншим учасникам для підтвердження та внесення в локальні сховища кожного. Перевагами даного підходу є:

- на можливість видобутку криптовалюти не впливає її кількість у майнера;
- захист від DoS-атак;
- атаки вимагають великих обчислювальних потужностей і витрат, тому не вигідні.

З недоліків можна виділити наступні:

- більша частина обчислювальних потужностей витрачається на забезпечення безпеки, але результат обчислень марний;
- погана масштабованість;
- атака 51 % можлива [7].

3.2. IOTA

Однією з перших криптовалют, які використовують ациклічний граф стала IOTA. У IOTA використовується PoW тільки не в класичному варіанті, а в такому, щоб його можна було застосовувати для ациклічного графа. Розробники назвали його Tangle. Цей варіант має ряд переваг, порівняно зі стандартним PoW:

• хороша масштабованість;

• висока швидкість обробки транзакції;

• відсутність необхідності зберігати всі попередні транзакції в пам'яті;

• відсутність комісії;

• легкість проведення мікротранзакцій;

• пропускна здатність мережі не обмежена і залежить від кількості пристроїв.

Але присутні і деякі недоліки:

• поки мережа недостатньо велика, є так званий координатор, який потужніший будь-якого вузла і є головним валідатором, що робить мережу не в повному обсязі децентралізованою;

• геш-функція Kerl, яка розроблена авторами IOTA, не в повному обсязі досліджена, хоч і є реалізацією SHA-3 тільки для трійкового коду з невеликими змінами [8].

3.3. Hedera Hashgraph

Криптовалюта на основі Hashgraph – запатентованої технології, що базується на спрямованому ациклічному графі. Hashgraph є aBFT протоколом, який вирішує завдання знаходження консенсусу, навіть якщо зловмисні учасники можуть контролювати мережу і видаляти або сповільнювати повідомлення за їх вибором.

До переваг Hashgraph можна віднести такі:

• хороша масштабованість;

• пропускна здатність обмежена параметрами мережі;

• менший обсяг даних, які необхідно зберігати на кожному пристрої;

• можливість роботи зі смарт-контрактами.

З недоліків можна виділити:

• проект запатентований і не знаходиться в відкритому доступі;

• розробники використовують власні розробки криптоалгоритмів, такі як геш-функція і цифровий підпис, які погано вивчені [3].

4. Вид розподіленого реєстру

Блокчейн є розподіленим реєстром, але не будь-який розподілений реєстр це блокчейн.

4.1. Ethereum

В основі криптовалюти Ethereum лежить блокчейн-технологія. Особливість протоколу GHOST полягає в тому, що, по суті, він є політикою вибору головного ланцюжка в дереві блоків. Основною модифікацією протоколу є те, що блоки, які виходять за межі основного ланцюга, можуть сприяти його вазі. Суть протоколу полягає в тому, що головним ланцюжком вибирається не найдовший, як у Bitcoin, а "найважчий". Приклад на рис. 3 показує, що навіть якщо зловмисникові вдається побудувати найдовший ланцюжок (1A, 2A, 3A, 4A, 5A, 6A), він все одно не буде обраний як головний, тому що дерево, в якому знаходиться ланцюжок 1B, 2C, 3D, 4B, має більшу вагу. Але ланцюжки 2D, 3F, 4C, 5B і 2B, 3B будуть також відкинуті, що не усуває проблему витрати зайвих обчислювальних ресурсів на обробку блоків [1].

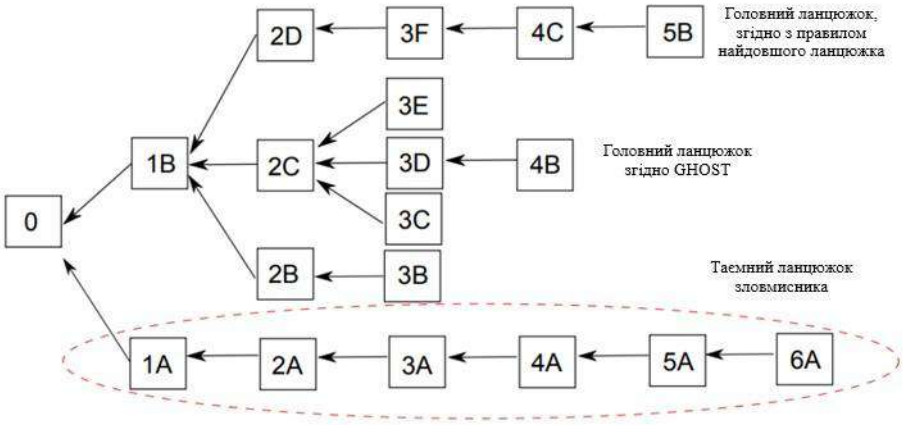


Рис. 3. Дерево блоків для прикладу роботи GHOST

4.2. IOTA

Головною особливістю цієї криптовалюти є спосіб зберігання транзакцій, так званий "клубок" (tangle), спрямований ациклічний граф. Транзакції, що випускаються вузлами, складають tangle-граф, який і є реєстром для зберігання транзакцій. Структура мережі формується таким чином: коли транзакція надходить, вона повинна підтвердити дві попередні транзакції, це підтвердження представлено у вигляді стрілок на рис. 4. Якщо стрілки між транзакціями A і B немає, але є спрямований шлях довжиною як мінімум 2 від A до B, можна сказати, що A побічно підтверджує B. Також існує перша транзакція, яка прямо або побічно підтверджена всіма іншими транзакціями. Спочатку в мережі була адреса, на балансі якої були всі токени. Перша транзакція відправляла ці токени на кілька інших адрес, так званих засновників. Всі токени в мережі були створені в першій транзакції і в майбутньому більше створюватися не будуть, і майнінгу не буде, тобто нагорода майнерам не буде "з'являтися з повітря". Головна ідея tangle полягає в наступному: щоб учасник міг провести транзакцію, він повинен "працювати", щоб підтвердити інші транзакції. Більш того, учасник, який ініціює транзакцію, сприяє безпеці мережі, це означає, що вузол перевіряє, чи немає в підтверджених транзакціях конфліктів. Якщо вузол з'ясував, що в транзакції є конфлікт з історією мережі, він не підтвердить конфліктну транзакцію, в будь-якому випадку, прямому чи непрямому [2].

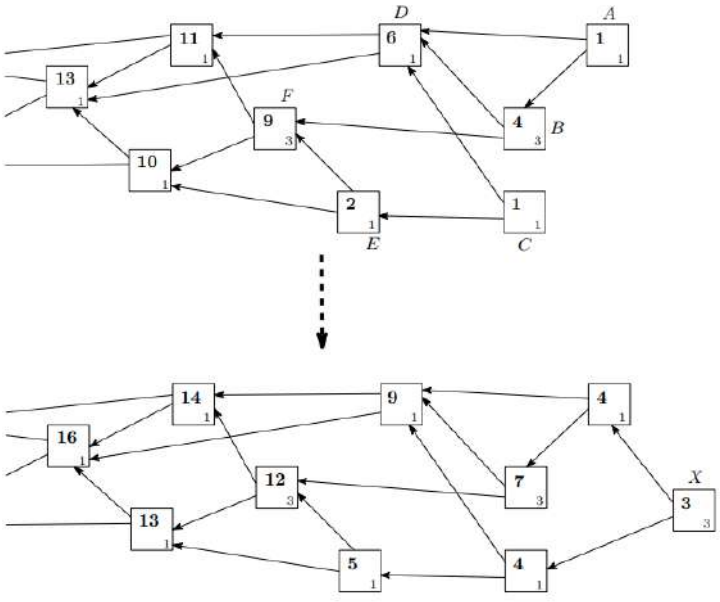


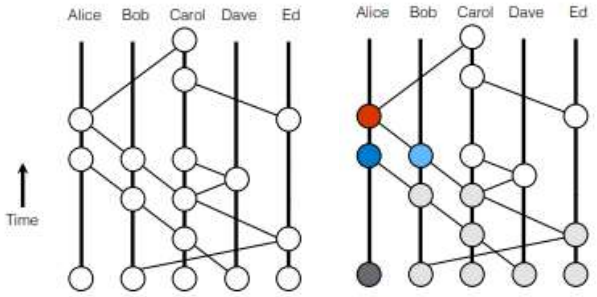
Рис. 4. Формування структури мережі IOTA

4.3. Hedera Hashgraph

Так як консенсус в Hashgraph заснований на протоколі Gossip, то його структуру можна відобразити в такому вигляді, як на рис. 5, *а*. Історія будь-якого протоколу "пліток" може бути представлена графом, де кожен учасник – це колонка вершин. Коли Аліса отримує "плітку" від Боба, в якій він розповідає все, що знає, ця плітка відображається вершиною в колонці Аліси. Від цієї вершини розходяться два зв'язки до безпосередньо попередніх пліток Аліси і Боба.

У консенсусі Hashgraph, граф є структурою даних. Рис. 5, *б* ілюструє цю структуру. Кожна подія (вершина) зберігається в пам'яті як послідовність біт, підписана автором. Наприклад, одна подія у Аліси (чорна вершина) означає той факт, що Боб виконав синхронізацію, в якій переслав Алісі все, що знав. Ця подія створена Алісою, нею ж підписана і містить геші двох інших подій: її останньої події, і події Боба, що передує події після синхронізації.

Hashgraph записує історію того, як учасники спілкуються між собою. По суті, через "плітки" поширюється сам hashgraph. Якщо нова транзакція поміщається в корисне навантаження події, вона буде швидко поширюватися серед всіх учасників, поки кожен не буде її знати. Аліса дізнається про транзакції, і вона буде точно знати, коли Боб дізнався про транзакції. Також буде знати, коли Керол дізналася про факт, що Боб дізнався про транзакції [10].



а *б*

Рис. 5. Структура консенсусу Hashgraph (*а*), структура даних Hashgraph (*б*)

5. Пропускна здатність

Одним з важливих показників розподіленого реєстру є його пропускна здатність. Оскільки від цього параметра безпосередньо залежить швидкість обробки транзакцій. І у випадку з криптовалютами є одним з найголовніших показників.

Пропускна здатність Ethereum згідно з [11] дорівнює приблизно п’ять транзакцій в секунду. За заявою розробника максимально досяжний показник дорівнює 15.15 TPS (transactions per second) [1].

Через будову ациклічного графа і самої концепції IOTA, пропускна здатність мережі залежить лише від кількості активних учасників. З ростом кількості учасників зростає і пропускна здатність мережі.

Однією з переваг технології DAG є висока пропускна здатність, яка залежить від кількості учасників. Розробники Hashgraph стверджують, що ця цифра може бути порядку 500 000 TPS [3].

6. Масштабованість

За останній рік популярність криптовалюти різко зросла. Тому деякі розробники зіткнулися з проблемою масштабованості. Це досить важливий параметр, оскільки з ростом популярності криптовалюти, все більше людей хочуть стати її власниками.

Ethereum володіє не дуже хорошою масштабністю, як і всі системи, засновані на блокчейн технології. Проблема полягає в тому, що складно зберігати точні записи того, хто чим володіє при зростаючому числі користувачів, особливо, якщо звичайні люди зможуть розра-

ховуватися за свої дрібні покупки. Тому Ethereum залежить від мережі вузлів, кожен з яких зберігає всю історію транзакцій і поточний стан балансів, контрактів і сховищ. Це, безумовно, громіздка задача, тим більше, що загальна кількість транзакцій зростає приблизно кожні 10 – 12 секунд з кожним новим блоком. Занепокоєння полягає в тому, що, якщо розробники збільшать розмір кожного блоку, щоб він вміщав більше транзакцій, обсяг збережених вузлами даних збільшиться, тим самим ефективно викидаючи людей з мережі. Якщо кожен вузол досить збільшиться, то тільки кілька великих компаній зможуть мати ресурси для їх забезпечення [12].

Технологія Tangle відмінно справляється з проблемою масштабованості. Кожен новий учасник підвищує продуктивність, стабільність і безпеку мережі, що, безсумнівно, йде їй на користь.

У Hashgraph, також немає проблем з масштабністю. DAG добре справляється з цим завданням, роблячи мережу безпечніше і стабільніше з кожним новим учасником.

7. HASH-функція

У всіх з перерахованих розподілених реєстрів використовуються геш-функції. Вони необхідні для забезпечення цілісності, а в PoW для забезпечення безпеки і підтвердженням виконаної роботи.

У GHOST використовується SHA-256 [1].

Автори IOTA розробили власну геш-функцію Kerl і позиціонують її як стійку до колізій.

Спочатку в IOTA використовувалася функція гешування Curl, але вона виявилася нестійка до диференціального криптоаналізу і в результаті на зміну їй прийшла функція гешування Kerl, яка, по суті, є трійковою версією відомої SHA-3 [13].

У Hashgraph також розробники вказали стійку до колізій геш-функцію. Про неї мало що відомо.

8. Атаки

Важливим критерієм вибору криптовалюти є її надійність і захищеність. І необхідно знати до яких атак вразлива та чи інша криптовалюта. У цій частині будуть розглянуті види атак, що реалізуються на обрані системи.

8.1. Ethereum

На Ethereum можлива реалізація ряду атак, до яких схильні блокчейн системи.

• Атака 51 %. Атака полягає в тому, що зловмисник може мати більш ніж 50 % обчислювальних потужностей всієї системи. Це призведе до того, що шанс знаходження наступного блоку у нього буде вище, ніж у всій мережі, і він зможе контролювати які транзакції підтверджувати, а які ні, і будувати свій ланцюжок.

• Double-spending. Атака подвійної витрати полягає в тому, що зловмисник може створити кілька транзакцій, в яких витрачає одні і ті ж монети. При нормальній роботі мережі така атака неможлива, оскільки інші учасники просто проігнорують блок з "некоректними" транзакціями. Але при атаці 51 %, коли порушується нормальна робота мережі, провести атаку подвійної витрати стає реально, оскільки зловмисник сам вирішує які транзакції включати в блок.

• Атака Сивіли. Суть цієї атаки полягає в тому, що мережа не може точно розрізняти фізичні машини. Тобто зловмисник може заповнити мережу підконтрольними йому клієнтами, що дозволить йому "відключати" деяких користувачів, не беручи від них і не відправляючи їм зміни в мережі. Також виникає небезпека атаки 51 % з усіма наслідками.

• DDoS атаки. Можливо переповнити мережу великою кількістю запитів. У результаті чого вона стане повільніше працювати. Також можливо відключати деякі вузли, але, щоб дійсно вплинути на роботу мережі, потрібно мати дуже великі потужності [14].

8.2. IOTA

В [2] згадується сценарій атаки, в якому зловмисник намагається "випередити" мережу самостійно:

1. Зловмисник посилає платіж продавцеві і отримує товар після того, як продавець вирішує, що транзакція має досить велику сукупну вагу.

2. Зловмисник випускає транзакцію з подвійною тратою.

3. Зловмисник використовує свої обчислювальні ресурси, щоб випустити багато маленьких транзакцій, які підтвердять транзакцію подвійної витрати, але не будуть підтверджувати вихідну транзакцію, яку він відправив продавцеві, прямо або побічно.

4. Зловмисник може мати безліч особистостей Сивіл.

5. Альтернативним методом до п. 3 буде такий, коли зловмисник випускає велику транзакцію подвійної витрати, використовуючи свої обчислювальні ресурси. Ця транзакція буде мати дуже велику власну вагу і буде підтверджувати транзакції раніше, ніж законна транзакція, відправлена продавцю.

6. Зловмисник сподівається, що його "нечесний subtangle" випередить чесний. Якщо це відбувається, головний tangle продовжує зростати від транзакції подвійної витрати [2].

Більш того, в IOTA можливе проведення аналога "атаки 51 %", але її можна здійснити, контролюючи вже 34 % обчислювальних потужностей. На даний момент в IOTA використовується централізований "координатор" як тимчасовий контрзахід, який буде відключений, коли мережа стане досить великою [13].

8.3. Hedera Hashgraph

Hashgraph розроблявся як наступне покоління розподіленого реєстру, тому розробники врахували недоліки блокчейна. У Hashgraph присутній захист від DDoS атак і атаки Сивіли. На даний момент відомі дві потенційні атаки:

• Атака ⅓. Дана атака – це атака 51 %, тільки для ациклічного графа. Для досягнення консенсусу необхідне число чесних учасників має становити більш ⅔. Тому якщо їх число буде менше ⅔, то мережа стане працювати некоректно.

• Атаки на криптографію. Розробники Hashgraph придумали власну геш-функцію. Але вона добре не вивчена, можливо в майбутньому будуть знайдені вразливості [10].

9. Порівняльна харатеристика

Результатом проведеної роботи стала порівняльна таблиця трьох алгоритмів консенсусу, використовуваних в криптовалютах.

Критерій порівняння	GHOST (Ethereum)	Tangle (IOTA)	Hashgraph (Hedera Hashgraph)
Вид	PoW	PoW	ABFT
Технологія	Блокчейн	Спрямований ациклічний граф	Спрямований ациклічний граф
Пропускна здатність	15.15 TPS	повний об'єм, який надається зовнішньою мережею	повний об'єм, який надається зовнішньою мережею
Масштабованість	погана	хороша	хороша
Надійність роботи	50 %+ чесних учасників	2/3+ чесних учасників	2/3+ чесних учасників
Геш-функція	SHA-256	Kerl	Стійка до колізій геш-функція
Атаки	Атака подвійної витрати, DoS, атаки на геш-функцію, атака 51%, атака Сивіли	1/3 + зловмисників, атаки на криптографію	1/3 + зловмисників, атаки на криптографію

Висновки

Технологія розподілених реєстрів (DLT) дозволяє обслуговувати глобальну структуру даних в розподіленому середовищі, з учасниками, які не довіряють один одному. Було визначено, що головними відмінними рисами розподілених реєстрів є незмінність, стійкість до цензури, децентралізоване обслуговування і усунення необхідності довіри третій стороні.

Дані в таблиці відображають ті основні показники, якими варто керуватись при виборі системи на основі технології розподілених реєстрів

За результатами порівняльного аналізу алгоритмів консенсусу можна зробити наступні висновки. Найбільше блокчейн підходить для зберігання даних в системах, які не мають потреби у великій пропускній спроможності, близько 10 транзакцій в секунду. Наприклад, блокчейн може застосовуватись для зберігання, підтвердження і передачі авторського права. Також блокчейн можна використати для системи електронного голосування, оскільки в такій системі немає постійного потоку транзакцій, а використовується тільки коли необхідно провести голосування і зберегти цілісність результатів. Ще одним вдалим застосуванням блокчейна буде створення інфраструктури відкритих ключів на його основі.

Ациклічний граф краще підійде в системах, де необхідна хороша масштабованість і велика пропускна здатність, наприклад в криптовалюті. Також ця технологія може стати хорошим рішенням в додатках для швидкого обміну інформацією, де не потрібна комісія. Існує велика ймовірність того, що незабаром ці технології повністю замінять розподілені реєстри на основі блокчейна.

Список літератури:

1. Yonatan Sompolinsky, Aviv Zohar Secure High-Rate Transaction Processing in Bitcoin (full version), 2013. 31 p.

2. Popov Serguei The Tangle, 2018. 28 p.

3. Hedera Hashgraph Whitepaper [Electronic resource] Mode of access: www. URL: https://www.hedera.com/whitepaper.

4. Что такое блокчейн простыми словами [Electronic resource] Mode of access: www. URL: https://prostocoin.com/blog/blockchain-guide

5. Everything You Need to Know About Directed Acyclic Graphs (DAGS) [Electronic resource] Mode of access: www. URL: https://www.coinbureau.com/education/directed-acyclic-graphs-dags/.

6. Что такое Byzantine Fault Tolerance (BFT) и какие есть решения? [Electronic resource] Mode of access: www. URL: https://golos.io/ru--kriptovalyuta/@encryptmymoney/chto-takoe-byzantine-fault-tolerance-bft-i-kakie-est-resheniya.
7. Proof-of-Work: Как это работает [Electronic resource] Mode of access: www. URL: https://ru.ihodl.com/tutorials/2018-01-23/proof-work-kak-eto-rabotaet/.
8. Обзор: алгоритмы консенсуса в блокчейне [Electronic resource] Mode of access: www. URL: https://decenter.org/ru/obzor-algoritmy-konsensusa-v-blokcheyne.
9. Скрябин Б. Основные принципы работы IOTA [Electronic resource] Mode of access: www. URL: https://distributedlab.com/blog/ru/main-principles-of-iota
10. Leemon Baird The Swirlds hashgraph consensus algorithm: fair, fast, byzantine fault tolerance. SWIRLDS TECH REPORT SWIRLDS-TR-2016-01, 2016. – 28 p.
11. Etherscan The Ethereum Block Explorer [Electronic resource] Mode of access: www. URL: https://etherscan.io/
12. How Will Ethereum Scale? [Electronic resource] Mode of access: www. URL: https://www.coindesk.com/information/will-ethereum-scale/.
13. Берлизева Александра Обзор криптовалюты IOTA [Electronic resource] Mode of access: www. URL: https://cryptofeed.ru/knowledge/obzor-kriptovalyuty-iota/.
14. Что угрожает блокчейн-сетям: рассматриваем атаки и способы защиты [Electronic resource] Mode of access: www. URL: https://habr.com/company/bitfury/blog/346656/.

Харківський національний
університет радіоелектроніки

Надійшла до редколегії 09.11.2018

УДК 004.652: 004.658.3

В.И. ЕСИН, д-р техн. наук, В.В. ВИЛИГУРА

МЕТОД РАЗРАБОТКИ БАЗ ДАННЫХ, ЛЕГКО АДАПТИРУЕМЫХ К ИЗМЕНЕНИЯМ В ПРЕДМЕТНОЙ ОБЛАСТИ

Введение

Исследования актуального состояния информатизации в компаниях, организациях, учреждениях свидетельствуют о том, что во многих из них эксплуатируются разноплановые информационные системы организационного управления (ИСОУ). При этом для решения новых задач, связанных с расширением сферы деятельности и, соответственно, предметных областей (ПрО), возникает потребность в более функциональных, с улучшенными характеристиками качества информационных систем (ИС), которые требуют меньших затрат на сопровождение. То есть существующие информационные системы и их основной функциональный компонент база данных (БД) требуют реализации процедур реинжиниринга («систематической трансформации существующей системы с целью улучшения ее характеристик качества, поддерживаемой ею функциональности, понижения стоимости ее сопровождения, вероятности возникновения значимых для заказчика рисков, уменьшения сроков работ по сопровождению системы» [1]). При этом одним из важных требований, предъявляемых к процессу реинжиниринга БД ИСОУ, является своевременность завершения соответствующих проектов в рамках запланированного бюджета с заданными характеристиками качества. Однако, как свидетельствуют результаты анализа IT-проектов [2 – 4], многие проекты были провалены или завершены с опозданием, причем с гораздо большими затратами, чем планировалось. Это, как правило, связано с ограниченностью функциональности соответствующих методов проектирования. В контексте БД указанная ограниченность обусловлена ориентацией традиционной методологии их проектирования на итерационную, довольно сложную и трудоемкую процедуру. В результате обостряется противоречие между необходимостью адаптации структуры БД ИСОУ к условиям динамичных изменений предметных областей и требованием стабильности структуры создаваемой БД при обеспечении заданных значений ее показателей качества при ограниченности выделяемых временных и финансовых ресурсов. Разрешение данного проблемного противоречия вызывает объективную необходимость пересмотра существующих подходов, методологий и технологий реинжиниринга баз данных.

Основные отличительные особенности информационной технологии, обеспечивающей механизм адаптируемости БД ИСОУ к изменениям условий функционирования

Опираясь на результаты проведенного анализа: различных информационных технологий (ИТ) управления данными, интеграции данных, реинжиниринга информационных систем, а также тенденций их развития [5 – 20]; классических методов проектирования баз данных и, в первую очередь, реляционных [4, 21 – 23]; различных моделей данных, используемых при моделировании предметных областей [22, 24 – 39], учитывая требования, предъявляемые к корпоративным БД рассматриваемого класса ИС, на основании созданных моделей [40 – 45] и схемы БД, инвариантной к предметным областям [46], была разработана информационная технология (частично представленная в [47]), обеспечивающая механизм адаптируемости БД ИСОУ к изменениям условий функционирования. Она, как совокупность методов, в основу которых были положены разработанные и обоснованные модели данных [40 – 45] и схема БД с универсальным базисом отношений [46], а также специально созданного программного обеспечения, не привязана к конкретным аппаратным платформам, хотя некоторые ее реализации связаны с определенными программными системами.

Некоторые принципиальные отличительные особенности предлагаемой ИТ от традиционной технологии разработки реляционных баз данных (РБД) с целью их интеграции с суще-

ствующими или замены существующих БД показаны на рис. 1, 2 с помощью графического представления основных фаз проектирования РБД ИСОУ в виде взаимосвязанных функциональных блоков методологии моделирования IDEF0.

Рис. 1. Представление основных фаз традиционной технологии проектирования реляционных баз данных в нотации IDEF0

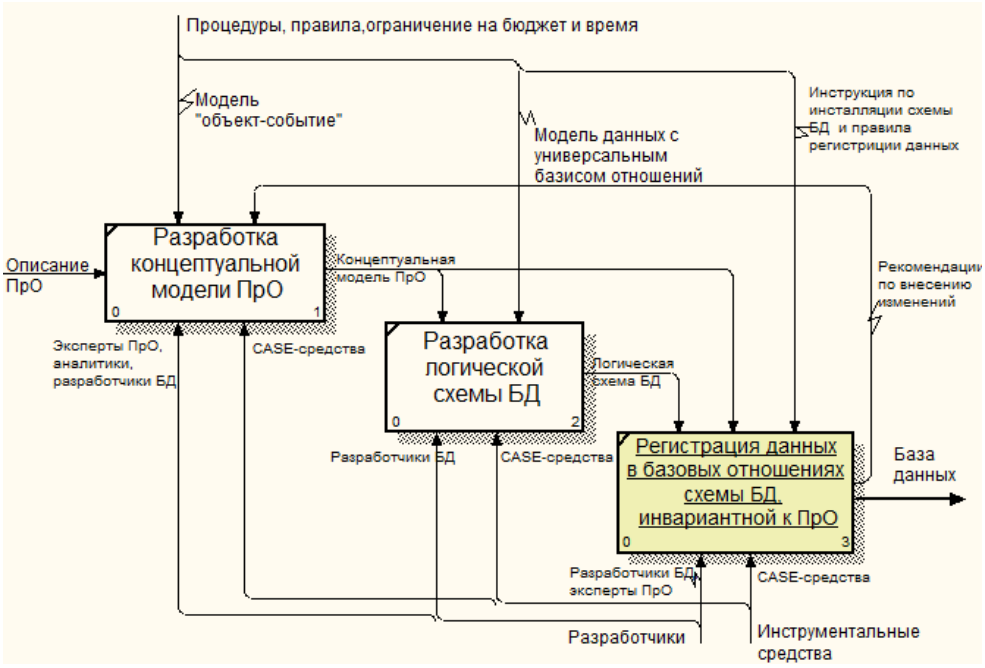


Рис. 2. Представление основных фаз предлагаемой технологии проектирования баз данных в нотации IDEF0

На рис. 1 приведены основные фазы методологии проектирования традиционной реляционной БД с применением средств существующих моделей: одной из так называемых «расширенных» моделей [48] и реляционной. Данный подход, как известно, приводит к затратному характеру процесса проектирования РБД ИСОУ в условиях динамичных изменений ПрО. Обоснованность этого утверждения объясняется тем, что при традиционном подходе к проектированию РБД осуществляемая последовательная трансформация описания моделируемой ПрО, выполненного, в частности, с помощью одной из распространенных

«расширенных» моделей – модели «сущность-связь», сначала в отношения (с соответствующими атрибутами) реляционной модели данных, которые затем отображаются в таблицы (с их именами и заголовками столбцов) схемы БД реляционной СУБД, приводит к жесткой взаимосвязанности структуры таблиц физической схемы БД с сущностями моделируемой ПрО, их связями и свойствами, затрудняющей процесс адаптации к изменениям условий функционирования. Динамичные изменения ПрО вызывают необходимость корректирования не только концептуальной модели ПрО, но и модификации, во многих случаях значительной, логической и физической схем БД ИСОУ.

Разработанные с целью решения научной проблемы, заключающейся в разрешении сформулированного выше проблемного противоречия, модель «объект-событие» [40 – 43], модель данных с универсальным базисом отношений [44, 45], инвариантная к предметным областям схема БД [46], синтаксическая и семантическая модели языка модели данных (ЯМД) [49, 50] позволили, не изменяя последовательности классического процесса проектирования РБД (при замене соответствующих средств разработки на новые), для различных ПрО создавать БД ИСОУ, отвечающие требованиям потребителей информационного продукта. При этом благодаря разработанным выразительным средствам модели «объект-событие» обеспечивается комплексное представление данных моделируемой ПрО, их структуры и ограничений целостности. Модель данных с универсальным базисом отношений, являющаяся отображением модели «объект-событие», позволила в условиях динамичных изменений предметных областей, на этапе логического проектирования РБД ИСОУ упростить создание схем БД, за счет введенного универсального базиса отношений, используя его для описания структур и представления данных (статических и временны*х* свойств объектов) различных моделируемых ПрО. Набор предопределенных отношений инвариантной к ПрО схемы БД, полученных в результате отображения универсального базиса отношений, и имеющих принципиальные отличия в назначении и структуре относительно проектируемых базовых отношений при традиционной технологии, позволил создавать РБД ИСОУ, способные к адаптации в условиях динамичных изменений предметных областей при стабильности схемы БД и одновременному хранению данных различных ПрО.

В результате, процесс проектирования РБД ИСОУ для различных ПрО превращается в процесс регистрации данных моделируемой ПрО (рис. 2), описанных средствами модели «объект-событие» и модели данных с универсальным базисом отношений, в базовых отношениях заранее инсталлированной схемы БД, инвариантной к предметным областям, в соответствии с рассматриваемым ниже одним из основных методов предлагаемой технологии – методом разработки БД ИСОУ.

Метод разработки БД ИСОУ с инвариантной к предметным областям схемой

Предлагаемый метод как совокупность операций, ориентированных на практическое решение задачи создания отвечающего требованиям потребителей информационного продукта, способного к адаптации в условиях динамичных изменений предметных областей при стабильности схемы реляционных БД ИСОУ, основывается на разработанных: модели «объект-событие», модели данных с универсальным базисом отношений, схеме БД, инвариантной к предметным областям, языке модели данных, специальном программном инструментарии разработчика БД. Основные технологические операции данного метода, связываемые с соответствующими этапами создания РБД ИСОУ, представлены на рис. 3 в виде функциональных блоков методологии моделирования IDEF0. Рассмотрим их для каждого этапа более подробно.

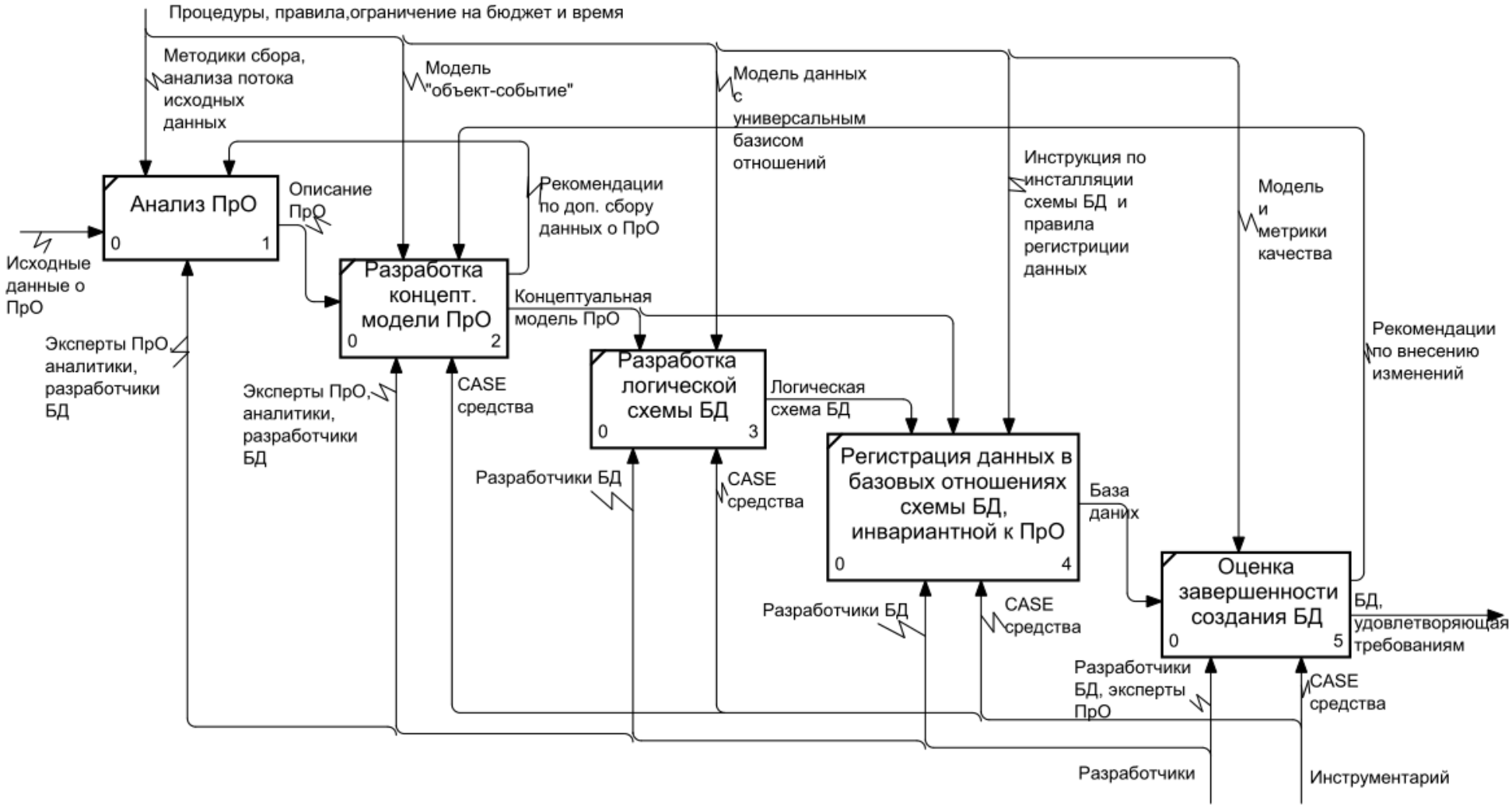


Рис. 3. Представление основных технологических операций метода разработки базы данных в нотации IDEF0

Этап 1. Анализ предметной области.

Данный этап является важным этапом в процессе проектирования БД ИСОУ, поскольку именно на нем формируется большинство проектных решений. Анализ ПрО состоит из анализа данных и анализа задач, сведения о которых могут быть получены путем изучения документации, проведения собеседований, наблюдения за работой предприятия, проведения исследований, проведения анкетирования и другими способами. Собранные сведения фиксируются (формулируются) в виде описания ПрО и определенных ограничений, отражающих основные требования пользователей, на естественном языке. К ключевым результатам данного этапа также относятся: описание правил организации контроля и защиты данных, их резервного копирования и восстановления, первичный вариант стратегии внедрения, предварительная оценка объема создаваемой БД и некоторые другие.

Этап 2. Разработка концептуальной модели ПрО.

Как известно [22, 23, 48, 51, 52], этап разработки концептуальной модели ПрО заключается в построении описания предметной области в терминах языка концептуального моделирования. В предлагаемом методе – это представление данных моделируемой ПрО, полученных на предыдущем этапе, в соответствии с нотациями средств концептуального моделирования, изложенными в [41, 43, 49, 50].

Для проверки корректности концептуальной модели рассматриваемой ПрО на данном этапе можно воспользоваться формальными методами анализа, изложенными в [53, 54].

Результатом этого этапа есть концептуальная модель (схема) ПрО, представленная выразительными средствами модели «объект-событие», в том числе в виде формализованного описания на ЯМД. При этом строки метаописания, составленные в соответствии с синтаксисом ЯМД, представляют собой также определенного рода документацию, облегчающую совместную и индивидуальную работу аналитиков, экспертов ПрО, разработчиков БД, прикладных программистов и конечных пользователей.

Этап 3. Разработка логической схемы БД.

За этапом концептуального моделирования следует этап преобразования (трансформации) описания ПрО в описание базы данных – этап логического проектирования – разработки логической схемы БД. В соответствии с разработанной концептуальной моделью ПрО, и механизмом ее преобразования, изложенным в [55], создается логическая схема РБД. По сути, разработка логической схемы РБД ИСОУ есть последовательное отображение элементов множеств формальных объектов, соотносимых с базовыми понятиями модели «объект-событие», в значения соответствующих им атрибутов отношений модели данных с универсальным базисом отношений и формирование ограничений целостности. Создаваемое таким образом представление данных ПрО в модели данных с универсальным базисом отношений оказывается полезным и в дальнейшем – при эксплуатации, сопровождении и развитии уже сформированной БД ИСОУ, являясь важной документацией.

Этап 4. Регистрация данных в базовых отношениях схемы БД, инвариантной к ПрО.

Данный этап соответствует этапу разработки физической схемы БД ИСОУ в традиционной технологии создания РБД. Однако, в отличие от традиционной технологии, в предлагаемом методе не предполагается создание новых объектов схемы БД ИСОУ или их модернизация при динамичных изменениях предметных областей. Процесс разработки заключается в инсталляции (одноразово, в соответствии с подготовленной инструкцией – шаблоном команд) инвариантной к предметным областям схемы БД [46] с последующей процедурой непосредственной регистрации в ее соответствующих базовых отношениях сначала метаданных, а затем данных из разработанных на предыдущих этапах концептуальной модели и логической схемы ПрО. При расширении набора объектов, событий, характеристик объектов,

событий, параметров объектов моделируемой ПрО в БД не создаются новые базовые отношения, атрибуты, ключи или иные объекты схемы, а просто добавляется новая запись в одно из существующих базовых отношений инсталлированной схемы БД. Это дает возможность при реинжиниринге БД ИСОУ, построенных на основе такой схемы, упростить процесс их адаптации к динамичным изменениям предметных областей.

Процедура регистрации метаданных и данных моделируемой ПрО может осуществляться как с помощью разработанного программного инструментария проектировщика БД, так и с помощью программных приложений, созданных специально для потребителя информационного продукта. При этом следует отметить, что и в одном, и в другом программном инструментарии для обращения к БД, построенной на основе схемы, инвариантной к ПрО, при занесении, модификации метаданных и данных ПрО можно применять не только операторы языка SQL, но и строки метаописания ЯМД.

В состав подготовленного на сегодняшний день программного инструментария разработчика БД, построенной на основе схемы, инвариантной к ПрО, входят программы: оперативного удаления данных; регистрации данных; просмотра соответствия занесенных в БД данных создаваемой концептуальной схеме ПрО (с возможностью автоматического сохранения во внешней памяти в виде специальной нотации графа модели «объект-событие» интенсионала и экстенсионала моделируемой ПрО); определения (задания) прав доступа к данным вплоть до конкретного элемента и некоторые другие.

Этап 5. Оценка завершенности создания БД.

Решение о завершении процесса создания РБД принимается на основе сравнительного анализа значений атрибутов качества базы данных, полученных с использованием метрик модели качества:

$$Q_{DB} = \{H_i^{DB}, S_{ij}^{DB}, M_{jk}^{DB(i)}, At_{jl}^{DB(i)}\}, \quad (1)$$

где H_i^{DB} – i-я характеристика качества БД (i=1,…,I); S_{ij}^{DB} – j-я подхарактеристика (j=1,…,J) i-й характеристики качества; $M_{jk}^{DB(i)}$ – k-я метрика (k=1,…,K) j-й подхарактеристики i-й характеристики качества; $At_{jl}^{DB(i)}$ – l-й атрибут (l=1,…,L;) j-й подхарактеристики i-й характеристики качества – переменная, которой присваивается значение в результате измерения (применения метрики), $At_{jl}^{DB(i)} \in Z$; $Z = (z_1,\ldots,z_\Theta)$, например для соответствующих H_i^{DB}, S_{ij}^{DB} атрибутами качества являются: оперативность устранения некорректных данных в БД, адаптация объектов схемы БД, непрерывность использования данных БД, среднее время отклика на запрос, среднее время, затрачиваемое на модификацию, и другие [56], и требования, предъявляемые к этим атрибутам со стороны потребителя информационного продукта. В случае неудовлетворительных значений атрибутов качества БД формулируется набор рекомендаций по внесению соответствующих изменений, и этапы 2 – 5 повторяются. При этом следует отметить, что итерационный характер носит не разработка схем (логической и физической) базы данных, как соответствующих процессов в традиционной технологии проектирования РБД с надлежащей оценкой достижимости значений атрибутов качества БД модели (1) требованиям потребителя информационного продукта, а обычный процесс записи данных в предопределенный набор базовых отношений схемы БД с универсальным базисом отношений с последующим визуальным контролем модифицированных данных, реализованным с помощью специального разработанного программного инструментария.

Это позволяет существенно экономить временной и финансовый ресурсы, выделяемые на реинжиниринг БД ИСОУ.

Данный метод был апробирован на нескольких РБД ИСОУ для различных ПрО.

Выводы

1) Показана актуальность проблемы, заключающейся в разрешении противоречия между необходимостью адаптации структуры БД ИСОУ к условиям динамичных изменений предметных областей и требованием стабильности структуры создаваемой БД при обеспечении заданных значений ее показателей качества при ограниченности выделяемых временных и финансовых ресурсов.

2) Приведены принципиальные отличительные особенности предлагаемой ИТ, обеспечивающей механизм адаптируемости БД ИСОУ к изменениям условий функционирования, от традиционной технологии проектирования реляционных баз данных.

3) Разработан один из основных методов предлагаемой информационной технологии, позволяющий:

- создавать в процессе реинжиниринга отвечающие требованиям потребителей информационного продукта базы данных ИСОУ для различных моделируемых ПрО при меньших (в сравнении с традиционным подходом) временных и финансовых ресурсах;
- адаптировать РБД ИСОУ, построенные на основе схемы БД с универсальным базисом отношений, к динамичным изменениям предметных областей, без изменения схемы БД, за счет использования созданной предопределенной структуры базовых отношений;
- автоматически в процессе моделирования ПрО создавать достаточно подробную и понятную специалистам различного профиля и квалификации документацию о различных уровнях представления данных разрабатываемой БД, которая будет полезна не только при проектировании конкретной БД, но и в дальнейшем, при ее эксплуатации, сопровождении и модернизации.

Список литературы:

1. Bergey J. A reengineering process framework / John Bergey, William Hefley, Walter Lamia, Dennis Smith // Software Engineering Institute, Carnegie Mellon University, Pittsburgh, 1999. – 12 p.
2. Chaos Manifesto 2013: Think Big, Act Small online version. The Standish Group [Electronic resource]. – Access mode : https://www.immagic.com/eLibrary/ARCHIVES/GENERAL/GENREF/S130301C.pdf, last accessed 2018/07/28.
3. Standish Group 2015 Chaos Report – Q&A with Jennifer Lynch [Electronic resource]. – Access mode : https://www.infoq.com/articles/standish-chaos-2015, last accessed 2018/07/28.
4. Connolly T. M. Database systems: a practical approach to design, implementation, and management. Sixth edition / Thomas M. Connolly, Carolyn E. Begg. – Harlow, Essex, England : Pearson Education Limited, 2015. – 1329 p.
5. Варламов О. О. Эволюционные базы данных и знаний для адаптивного синтеза интеллектуальных систем. Миварное информационное пространство. – Москва : Радио и связь, 2002. – 282 с.
6. Гринев М. Н. Управление данными: достижения и проблемы / М. Н. Гринев, С. Д. Кузнецов // Всероссийский конкурсный отбор обзорно-аналитических статей по приоритетному направлению "Информационно-телекоммуникационные системы", 2008. – 48 с.
7. Костенко Б. Б. История и актуальные проблемы темпоральных баз данных / Б. Б. Костенко, С. Д. Кузнецов // Труды Института системного программирования РАН. – Москва : ИСП РАН, 2007. – Т. 13, № 2. – С. 77-114.
8. Филатов В. А. Методы и средства проектирования информационных систем и распределенных баз данных / В. А. Филатов, Р. В. Семенец // Вестник Херсонского нац. техн. ун-та – 2007. – № 4(27). – С. 203-207.
9. Глобальні інформаційні системи та технології (моделі ефективного аналізу, опрацювання та захисту даних) / [Пасічник В. В., Жежнич П. І., Кравець Р. Б., Пелещишин А. М. та інш.]. – Львів : Вид-во Нац. ун-ту «Львівська політехніка», 2006. – 350 с.
10. Шаховська Н. Б. Сховища та простори даних / Н. Б. Шаховська, В. В. Пасічник. – Львів: Вид-во Нац. ун-ту «Львівська політехніка», 2009. – 244 с.
11. Bergey J. A reengineering process framework / John Bergey, William Hefley, Walter Lamia, Dennis Smith // Software Engineering Institute, Carnegie Mellon University, Pittsburgh, 1999. – 12 p.
12. Brodie M. L. Legacy information systems migration: gateways, interfaces, and the incremental approach / M. L. Brodie, M. Stonebraker. – Morgan Kaufmann Publishers Inc., 1995. – 210 p.

13. Comella-Dorda S. A survey of legacy system modernization approaches / S. Comella-Dorda, K. Wallnau, R. C. Seacord, J. Robert // Software Engineering Institute (Technical Note CMU/SEI-200-TN-003), Pittsburgh, 2000. – 30 p.

14. Database Research: Achievements and Opportunities into the 21st Century / [A. Silberschatz, M. R. Stonebraker, J. Ullman and other] // SIGMOD Record. – 1996. – № 25(1). – P. 52-63.

15. Lenzerini M. Data integration: A theoretical perspective // Proceedings of the ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems (PODS 2002). – 2002. – P. 233-246.

16. Lehman M. M. Laws of software evolution revisited // Proc. of European Workshop on Software Process Technology, 1996. – P. 108–124.

17. The Asilomar Report on Database Research / [P. A. Bernstein, M. L. Brodie, S. Ceri and other] // ACM SIGMOD Record. – 1998. – № 27(4). – P. 74-80.

18. The Claremont Report on Database Research [Electronic resource] / [R. Agrawal, A. Ailamaki, P. A. Bernstein and other]. – Access mode : http://db.cs.berkeley.edu/claremont/claremontreport08.pdf, last accessed 2018/07/28.

19. The Global Information Technology Report 2014. Rewards and Risks of Big Data // Insight Report World Economic Forum, 2014. – 369 p.

20. The Global Information Technology Report 2015. ICTs for Inclusive Growth // Insight Report World Economic Forum, 2015. – 381 p.

21. Зиндер Е. З. Проектирование баз данных: новые требования, новые подходы // СУБД. – 1996. – № 3. – С. 10-22.

22. Цикритзис Д. Модели данных / Д. Цикритзис, Ф. Лоховски ; пер. с англ. – Москва : Финансы и статистика, 1985. – 344 с.

23. Пасічник В. В. Організація баз даних та знань / В. В. Пасічник, В. А. Резніченко. – К. : Вид. група BHV, 2006. – 384 с.

24. Abrial J. R. Data semantics // Data Base Management, Klimbie J. W. and Koffeman K. L., eds., North-Holland, Amsterdam. – 1974. – P. 1-59.

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

26. Langefors B. Infological model and information user views // Information Systems. – 1980. – № 5. – P.17-32.

27. Roussopoulos N. Using semantic networks for data base management / N. Roussopoulos, J. Mylopoulos // Proceedings of the 1st International Conference on Very Large Data Bases. – ACM. – 1975. – P. 144-172.

28. Thalheim B. Entity-relationship modeling: foundations of database technology // Springer-Verlag Berlin Heidelberg. – 2000. – 639 p.

29. Кодд Е. Ф. Расширение реляционной модели для лучшего отражения семантики. Пер. с англ. М. Р. Когаловский // СУБД. – 1996. – № 5.

30. Модель "сущность-связь" в задачах представления объектно-реляционных свойств предметной области / [В. А. Филатов, Е. Б. Чапланова, С. С. Танянский, А. И. Сизов] // Управляющие системы и машины: информационные технологии. – 2011. – № 3. – С. 73-78.

31. Gruber T. R. Toward principles for the design of ontologies used for know ledge sharing // International journal of human-computer studies. – 1995. – Vol. 43. – № 5. – P. 907-928.

32. Guarino N. Formal Ontology and Information Systems // Formal Ontology in Information Systems. Proceedings of FOIS'98, 6–8 June 1998, Trento, Italy: – IOS Press, Amsterdam, 1998. – P. 3–15.

33. Палагин А. В. Онтологические методы и средства обработки предметных знаний: монография / А. В. Палагин, С. Л. Крывый, Н. Г. Петренко. – Луганск : изд-во ВНУ им. В. Даля, 2012. – 323 с.

34. Halpin T. Conceptual schema and relational database design (2nd edition). – Sydney, Australia: Prentice-Hall of Australia Pty., Ltd. – 1995. – 500 p.

35. Halpin T. Entity Relationship modeling from an ORM perspective. Part 1. // Journal of Conceptual Modeling – 1999. – Minneapolis USA. – P. 1-10.

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

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

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

39. The object data standard: ODMG 3.0. Edited by R.G.G. Cattel, Douglas K. Barry. Morgan Kauffmann Publishers, 2000. – 280 p.

40. Есин В. И. Семантическая модель данных «объект-событие» // Вісник Харк. нац. ун-ту імені В. Н. Каразіна. Сер.: Математичне моделювання. Інформаційні технології. Автоматизовані системи управління. – 2010. – № 925. – С. 65-73.

41. Security and noise immunity of telecommunication systems: new solutions to the codes and signals design problem. Collective monograph. – Minden, Nevada, USA : ASC Academic Publishing. – 2017. – 198 p. (Yesin V. I., Yesina M. V. Chapter 8, Means for conceptual modeling of information system databases, P. 160-196).

42. Есин В. И. Модель данных «объект-событие»: требования и синтез модели // Computer science and cyber security – International electronic scientific journal. – 2017. – Issue. 3 (7). – P. 33-44, https://periodicals.karazin.ua/cscs/article/view/10003, last accessed 2018/07/28.

43. Есин В. И. Выразительные средства модели данных «объект-событие» // Радиотехника. – 2017. – Вып. 191. – С. 99-112.

44. Есин В. И. Универсальная модель данных и ее математические основы // Системи обробки інформації. – 2011. – № 2(92). – С.21-24.

45. Есин В. И. Модель данных с универсальной фиксированной структурой // Теоретичні та прикладні аспекти побудови програмних систем : матеріали міжнар. наук. конф., м. Київ, 15-17 грудня 2014 р. – Кіровоград : ФО-П Александрова М. В., 2014. – С. 112-116.

46. Есин В. И. Инвариантная к предметным областям схема базы данных и ее отличительные особенности // Радиотехника. – 2018. –Вып. 193. – С. 133-142.

47. Technology for Developing Databases of Information Systems / [V. M. Grachev, V. I. Esin, N. G. Polukhina, S. G. Rassomahin] // Bulletin of the Lebedev Physics Institute. – New York, USA : Allerton Press, Inc. – 2014. – Vol. 41. – № 5. – P. 119-122.

48. Date C. J. An Introduction to Database Systems, 8th Edition. – Pearson. Addison-Wesley, 2004. – XXVII, 983, I-22 p.

49. Есин В. И. Язык для универсальной модели данных / В. И. Есин, М. В. Есина // Системи обробки інформації. – 2011. – № 5(95). – С. 193-197.

50. Есин В. И. Язык описания и манипулирования данными, хранящимися в БД с УМД / В. И. Есин, М. В. Есина // Компьютерное моделирование в наукоемких технологиях (КМНТ-2010) : междунар. науч.-техн. конф., 18-21 мая 2010 г. : тезисы докл. – Харьков : Харьк. нац. ун-т им. В. Н. Каразина, 2010. – Ч. 2. – С. 104-108.

51. Когаловский М. Р. Концептуальное моделирование в технологиях баз данных и онтологические модели / М. Р. Когаловский, Л. А. Калиниченко // Труды Симпозиума «Онтологическое моделирование». – Москва : ИПИ РАН, 2008, С. 114-148.

52. Цаленко М. Ш. Моделирование семантики в базах данных. – Москва : Наука. Гл. ред.физ-мат.лит., 1989. – 288 с.

53. Жолткевич Г. Н. К проблеме формализации концептуального моделирования информационных систем / Г. Н. Жолткевич, Т. В. Семенова // Вісник Харк. нац. ун-ту імені В. Н. Каразіна. Сер.: Математичне моделювання. Інформаційні технології. Автоматизовані системи управління. – 2003. – № 605. – С. 33-42.

54. Жолткевич Г. Н. Представление полусхем предметных областей информационных систем средствами реляционных баз данных / Г. Н. Жолткевич, Т. В. Семёнова, К. А. Федорченко // Вісник Харк. нац. ун-ту імені В. Н. Каразіна. Сер.: Математичне моделювання. Інформаційні технології. Автоматизовані системи управління. – 2004. – № 629, вип. 3. – С. 11-24.

55. Есин В. И. Метод моделирования предметной области с помощью универсальной модели данных // Системи озброєння і військова техніка. – 2011. – № 2(26). – С. 128-131.

56. Yesin V. I. A cybernetic approach to solving the problem of database reengineering // Telecommunications and Radio Engineering. – 2018. Volume 77, Issue 5. – P. 399-409. doi: 10.1615/TelecomRadEng.v77.i5.40.

Харьковский национальный
университет имени В.Н. Каразина

Поступила в редколлегию 11.10.2018

УДК 004.056.5

О.О. КУЗНЕЦОВ, д-р техн. наук, О.О. СТЕФАНОВИЧ,
Д.І. ПРОКОПОВИЧ-ТКАЧЕНКО, канд. техн. наук, К.О. КУЗНЕЦОВА

3D СТЕГАНОГРАФІЧНЕ ПРИХОВУВАННЯ ІНФОРМАЦІЇ

Вступ

Стеганографія, у широкому сенсі, це такий спосіб передачі закодованого інформаційного повідомлення, при якому приховується сам факт його існування [1, 2]. На відміну від криптографії, методи стеганографії дають можливість замінити несуттєві частки даних на конфіденційну інформацію так, щоб неможливо було запідозрити існування вбудованого таємного послання [1].

На сьогодні у зв'язку з розвитком обчислювальної техніки і нових каналів передачі інформації з'являються нові стеганографічні методи, в основі яких лежить приховування інформації в комп'ютерних файлах – контейнерах, які володіють високим рівнем природньої надмірності (фото- та відеозображення, аудіо-файли, текстові документи, тощо). Сутність приховування полягає в скритній заміні надмірних даних інформаційними повідомленнями, вилучити або навіть встановити факт наявності яких може тільки вповноважена особа, що має секретний стеганографічний ключ [1, 2].

Останніми роками з'явився та отримав розвиток новий напрям комп'ютерної стеганографії, який пов'язаний із приховуванням інформаційних повідомлень в штучно створених контейнерах, надмірність в який породжена технічними особливостями зберігання, обробки та/або передачі даних [3 – 14]. Такі методи «технічної» стеганографії набули поширення при приховуванні інформаційних повідомлень в різних за своєю природою штучних контейнерах. Зокрема, методи мережевої стеганографії у якості носія (контейнеру) використовують переданий по мережі пакет або сукупність пакетів даних, процедури приховування та вилучення інформаційних даних засновані на використанні особливостей функціонування мережевого стеку протоколів передачі даних [3 – 6]. Побудову прихованих кластерних каналів засновано на використанні особливостей зберігання даних у сучасних файлових системах [7 – 9]. Існують і інші напрямки розвитку технічної стеганографії, зокрема, які засновані на використанні штучної надмірності тривимірних (3D) моделей об'єктів [10 – 14]. Останніми роками тривимірні моделі набули значного поширення та розповсюдження в різних застосуваннях, зокрема при обробці медичних даних, музейних експонатів та зразків культурної спадщини, імітаційних моделей промислових зразків та виробничих процесів, комп'ютерних ігор, тощо. При цьому стеганографічні методи застосовують для захисту авторського права тривимірних моделей, скритого приховування певної інформації, захисту від випадкових викривлень або певних похибок, тощо. Отже дослідження нових методів приховування даних із використанням 3D-технологій є перспективним напрямком сучасних досліджень.

В цій роботі розвивається новий підхід, запропонований в [15 – 17], щодо стеганографічного приховування даних в твердотільних об'єктах за допомогою технології 3D-друку. Сутність цього підходу полягає в перетворенні інформаційного повідомлення на 3D-модель, яку розміщують всередині 3D-моделі контейнеру із подальшим роздрукуванням (створенням, вирощуванням). Зовнішній вигляд отриманого твердотільного об'єкту, його експлуатаційні та естетичні властивості не змінюються в процесі вбудовування інформаційного повідомлення. Крім того, видалити або спотворити приховане повідомлення без руйнування або значного пошкодження виробу неможливо, отже маємо нову технологію стеганографічного захисту інформації як для скритної її передачі, так і для забезпечення авторського права, тощо.

1. Приховування інформаційних даних

В роботах [15 – 17] було запропоновано прототип комплексу стеганографічного захисту, в якому інформаційні дані приховуються в процесі пошарового створення (вирощування)

твердотільного об'єкта при використанні різних технологій 3D-друку. Основна ідея полягає у вбудовуванні (стеганографічному кодуванні) інформаційних даних в цифрову 3D-модель, за якої в подальшому пошарово створюється (роздруковується) твердий об'єкт (готовий виріб або прототип для подальшого доведення). Процес вбудовування реалізується з використанням секретних ключових даних, що виключає несанкціонований доступ до інформації, що захищається, порушення її цілісності, автентичності та конфіденційності. Крім того, застосовані методи стеганографічного захисту не повинні знижувати експлуатаційних, естетичних та будь-яких інших властивостей готового виробу, оскільки технології, що застосовуються для нанесення шарів, не модифікуються. Отже, пропонований комплекс інваріантний способу пошарового вирощування, тобто може комплектуватися довільними периферійними пристроями 3D-друку різних фірм виробників з будь-якими матеріалами і принципами пошарового створення [15 – 17].

Головна ідея приховування даних полягає в розміщенні інформаційного повідомлення у середині довільної комп'ютерної моделі фізичного об'єкту, яку можна роздрукувати на 3D принтері – іграшці, статуетці, сувенірі тощо. Інформаційне повідомлення подається у двійковому вигляді і кожен біт перетворюється на певний фрагмент фізичної моделі. Як приклад (рис. 1), кожен біт може кодуватися тривимірним кубом встановленого розміру, причому наповненість куба відповідає вмісту відповідного біту: «0» відповідає пустому (не заповненому) кубу, «1» – заповненому. Інформативний признак може бути і іншим, наприклад заповнення різними матеріалами, або одним матеріалом але із різною щільністю, орієнтованістю, формою елементарних «бітових» фізичних моделей, тощо.

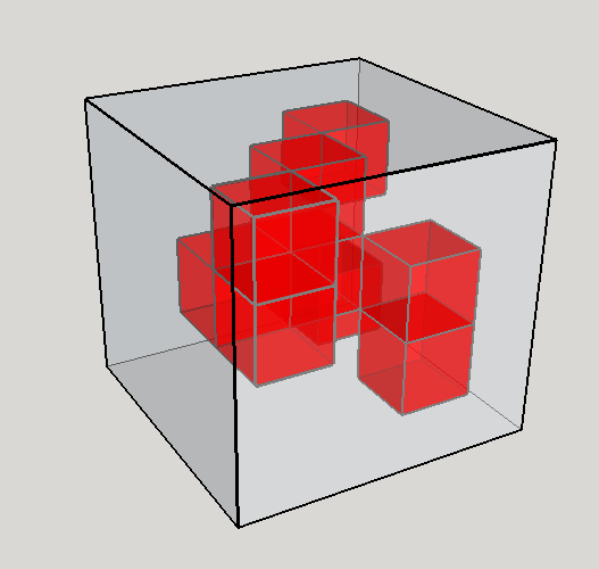


Рис. 1. Схематичне подання стеганографічного кодування – перетворення інформаційного повідомлення на фрагмент комп'ютерної моделі фізичного об'єкту

Для автоматизованого кодування було застосовано спеціалізоване програмне забезпечення OpenSCAD, яке призначене для створення твердотільних тривимірних САПР-об'єктів. Воно є вільним і доступним під операційними системами Linux / UNIX, Microsoft Windows і Apple Mac OS X.

На рис. 2 продемонстровано кодування інформаційного повідомлення «Tomorrow never comes until it's too late». Кожен символ повідомлення подається у бінарному вигляді за допомогою коду ASCII. Далі, для обраної кубічної форми «бітових» моделей та розміру 3x3x3 міліметри виконується кодування кожного інформаційного біту. Для цього було розроблено програмне забезпечення, яке формує відповідний вихідний код, що розміщується у робочому

полі програми OpenSCAD. На рис. 2 всі елементарні фізичні моделі згруповано у контейнер розміром 11x3x10 відповідних кубів (ці налаштування додатково встановлюються у розробленому програмному забезпеченні).

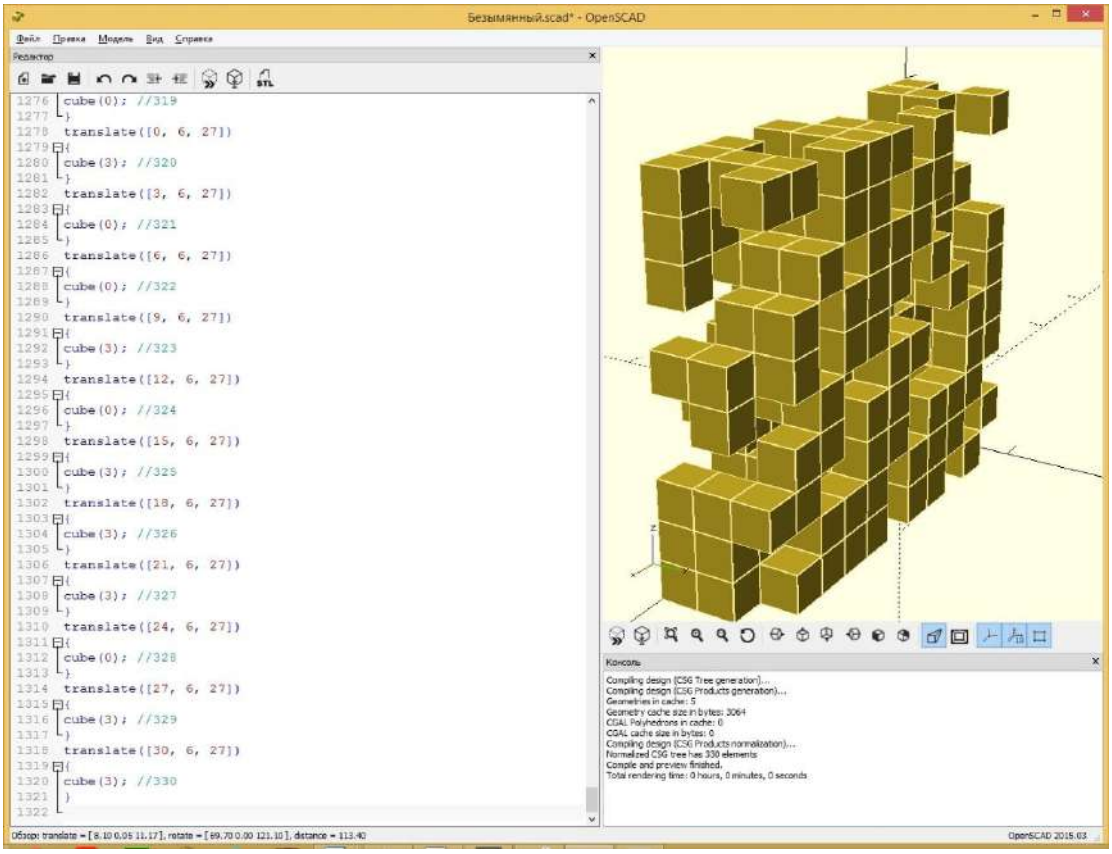


Рис. 2. Приклад стеганографічного кодування за допомогою програми OpenSCAD

На рис. 2 зліва можна побачити вихідний код, в якому задаються координати та розмір тривимірних кубів – носіїв інформаційних бітів. Праворуч наведено створену тривимірну модель інформаційного повідомлення, яка відповідає всім заданим вхідним параметрам.

Таким чином, в результаті стеганографічного кодування інформаційне повідомлення спочатку перетворюється у трьохвимірну булеву матрицю, яка, в свою чергу, перетворюється в комп'ютерну модель фізичного об'єкту. Сформована комп'ютерна модель булевої матриці розміщується у середині основної моделі контейнеру так, щоб її краї не виходили за межі зовнішнього тіла, як це схематично наведено на рис. 3. При цьому застосовувалося спеціалізоване програмне забезпечення MakerBot Desktop з технологій 3D-друку.

Розмістити таку матрицю в середині іншої моделі можна різними способами, наприклад:

- всі заповнені куби під час друку на 3D принтері заповнювати іншим кольором;
- всі заповнені куби під час друку на 3D принтері залишати порожніми.

Недоліком другого способу є зменшення кінцевої ваги тіла, що при детальному аналізі може видати факт наявності таємного повідомлення. Заповнення бітів іншим кольором (або, наприклад, іншим матеріалом) зменшує ймовірність виявлення прихованого повідомлення, але збільшує складність його зчитування.

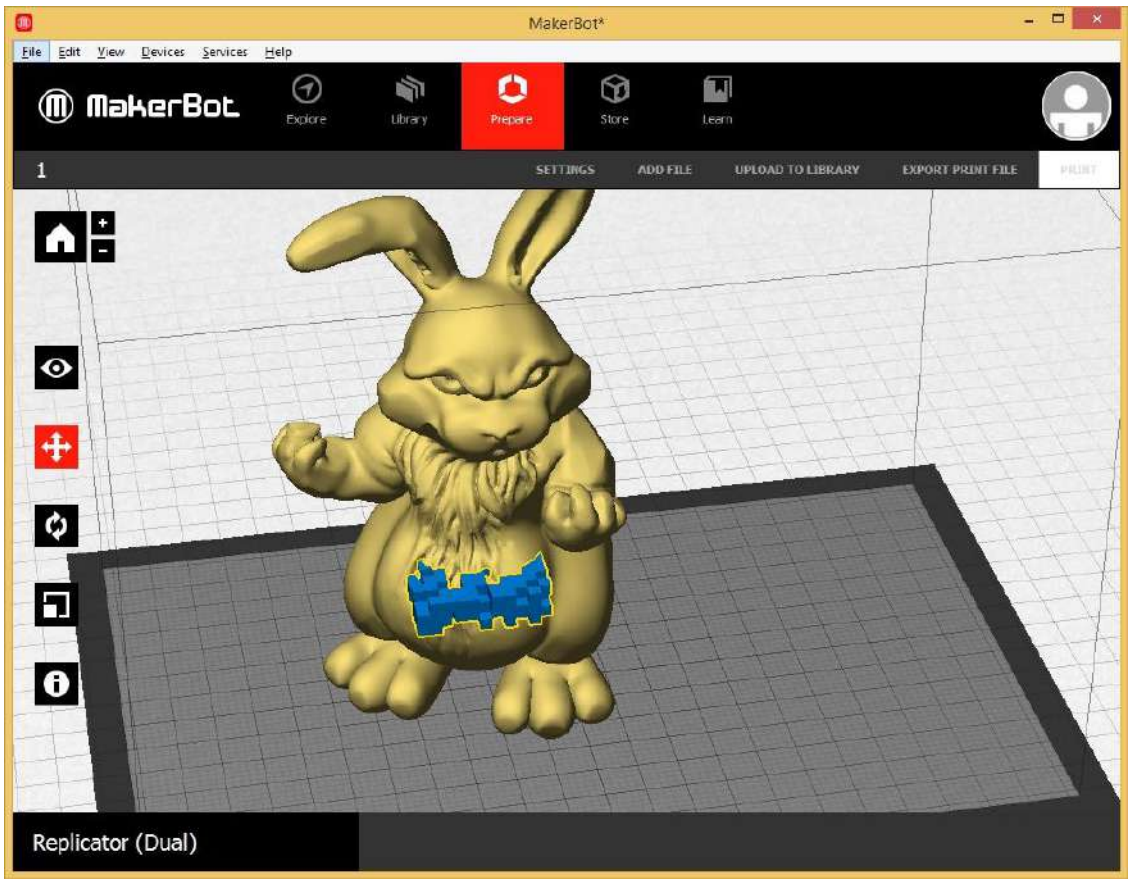


Рис. 3. Розміщення тривимірної моделі інформаційного повідомлення
у середині основної моделі контейнеру

На рис. 4 показаний процес пошарового створення твердотільного об’єкту-контейнеру із вбудованим інформаційним повідомленням. Ліворуч на рисунку показана схематична візуалізація процесу друку, праворуч – фотографія реального процесу на 68 шарі 3D-друку, який було виконано із застосуванням 3D принтеру «Flashforge Creator Dual». На рис. 5 показано завершення друку 3D-моделі та готовий виріб із вбудованим повідомленням.

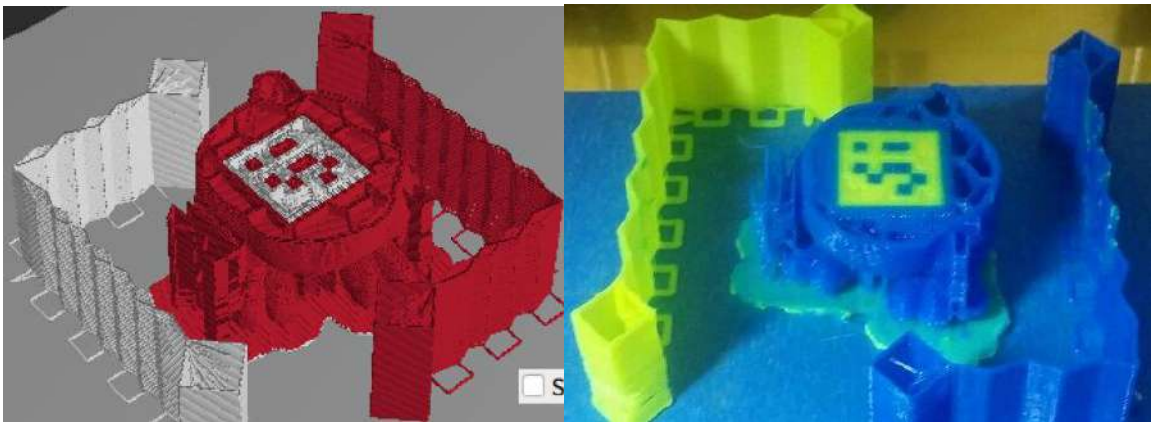


Рис. 4. Пошарове створення твердотільного об’єкту-контейнеру
із вбудованим інформаційним повідомленням

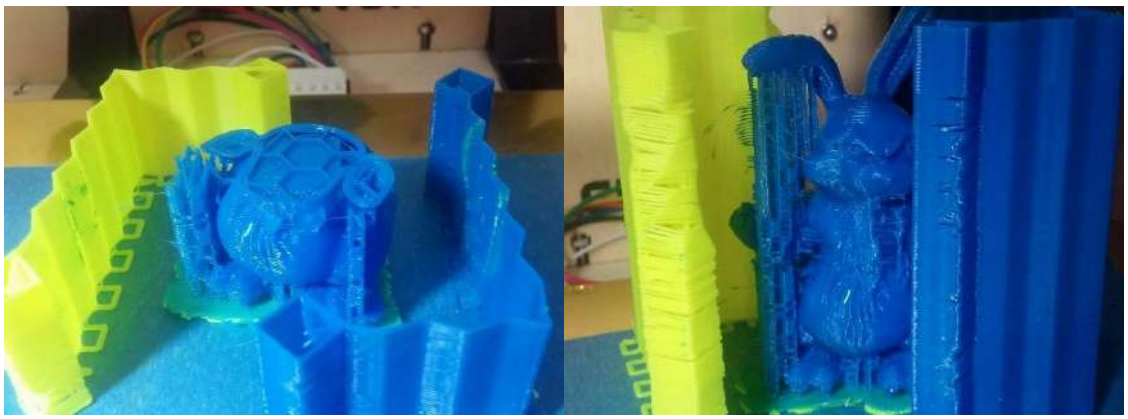


Рис. 5. Завершення друку та готовий виріб із вбудованим повідомленням

2. Вилучення інформаційних даних

Процес вилучення вбудованих даних здійснюється за допомогою сканування отриманого твердотільного об'єкту. Витягнуті сканером дані піддаються стеганографічному декодуванню з використанням секретних ключових даних. На цьому етапі забезпечуються різні послуги безпеки, наприклад, цілісність, автентичність, причетність, конфіденційність, тощо. Для підвищення достовірності (завадостійкості) вбудовані дані додатково піддаються надмірному кодуванню, яке дозволяє з заданою вірогідністю виявляти і/або виправляти помилки, що виникли в процесі пошарового друку/сканування. Пропонований комплекс може використовувати в різних областях: для прихованої передачі інформаційних повідомлень із забезпеченням різних послуг безпеки (цілісності, автентичності, причетності, конфіденційності та ін.). Видалення, спотворення або модифікація вбудованих даних неможливі без фізичного руйнування готового виробу, тобто пропонований комплекс ідеально підходить для забезпечення достовірності пошарово вирощених виробів, захисту їх від несанкціонованого копіювання та недобросовісних підробок, забезпечення авторського права, тощо [1, 2].

Слід відмітити, що на сьогодні день ще не розроблено надійних засобів вилучення інформаційних даних [15 – 17]. Саме невизначеність конкретної процедури вилучення вбудованих даних за допомогою сканування отриманого твердого тіла є головним невирішеним питанням з приводу практичного застосування запропонованого комплексу 3D-стеганографії. Зокрема, система може комплектуватися різними периферійними пристроями 3D-друку, які застосовують різні технології пошарового вирощування та різний за своїми фізичними властивостями вихідній матеріал. Відповідні процедури сканування отриманого твердого тіла повинні враховувати ці особливості і, по можливісті, забезпечувати надійне та безпомилкове вилучення прихованих даних.

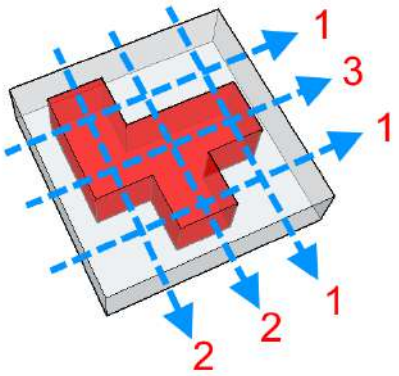
Одним із можливих напрямків у вирішенні зазначених проблем є застосування лазерних сканерів, в яких потік когерентного, монохроматичного, поляризованого і вузьконаправленого потоку випромінювання, що утворює паралельний пучок, зменшується в результаті поглинання в середовищі в деяку заздалегідь обумовлену кількість разів. Для встановлення принципової можливості зчитування прихованого повідомлення з 3D-моделі, що пошарово створена (надрукована) на 3D-принтері без пошкодження самої моделі або повідомлення, було проведено наступні експериментальні дослідження.

2.1. Опис лабораторної установки та умов проведення експериментальних досліджень

Головна ідея проведення експерименту полягає в вузьконаправленому опромінюванні готового виробу (із вбудованим повідомленням) за різними кутами та напрямками, достатніми для однозначного визначення внутрішньої структури виробу. При цьому як вихідні дані

враховуються значення інтенсивності випромінювання, що зменшуються в результаті поглинання.

При кодуванні інформаційних бітів пустими та заповненими кубами схема опромінення готового виробу може бути подана у спрощеному вигляді як на рис. 6 (ліворуч). В кінці стрілок вказане умовне значення результату вимірювання зменшення інтенсивності випромінювання (пропорційно до товщини заповненого матеріалом об'єкту). Праворуч на цьому ж рисунку подано значення інформаційних бітів, які, як очікується, буде вилучено із твердотільного об'єкту.



1	0	0
1	1	1
0	1	0

Рис. 6. Спрощена схема опромінення готового виробу (ліворуч)
та очікуваний результат вилучення даних (праворуч)

Оскільки ніяких інших відомостей щодо внутрішньої структури виробу немає, розміщення заповнених фрагментів (і відповідних бітів) повинне враховувати однозначність вилучення тільки за результатами вимірювання (зображені на рисунку ліворуч результати вимірювання мають два можливі рішення, одне з яких не співпадає із наведеним праворуч). Таке розміщення, фактично, є номограмою, яку застосовують при формуванні японських кросвордів.

Для спрощення умов проведення експерименту було виготовлено просту фізичну модель у формі сходинок із ABS-пластика жовтого та синього кольорів. Така форма дозволяє швидко змінювати товщину заповненого матеріалом об'єкту (рис. 7). Фактично, маємо шість різних значень, які умовно відповідають наступним інформаційним бітовим послідовностям:

- без заповнення – бітова послідовність (00000);
- одне заповнення (перша сходинка) – бітова послідовність (10000);
- два заповнення (друга сходинка) – бітова послідовність (11000);
- три заповнення (третя сходинка) – бітова послідовність (11100);
- чотири заповнення (четверта сходинка) – бітова послідовність (11110);
- п'ять заповнень (п'ята сходинка) – бітова послідовність (11111).

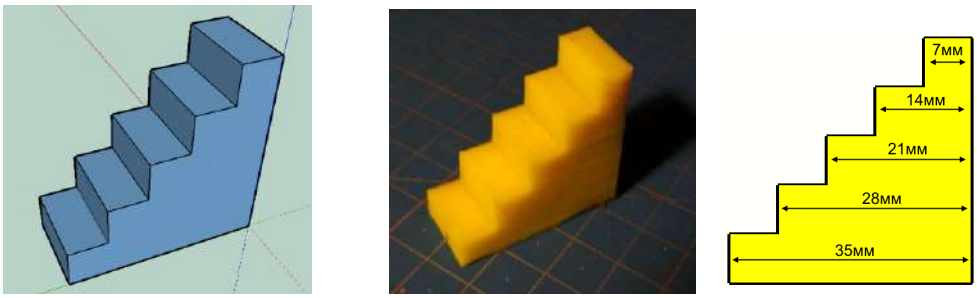


Рис. 7. Спрощена фізична модель інформаційних даних

Для проведення досліджень було застосовано оптичні прилади з лабораторії кафедри фізичної оптики фізичного факультету. Відомо, що кожен матеріал має свій показник

поглинання – величина, зворотня відстані, на якому потік монохроматичного випромінювання, що утворює паралельний пучок, зменшується в результаті поглинання в середовищі в деяку заздалегідь обумовлену кількість разів. Показник поглинання визначається властивостями речовини і в загальному випадку залежить від довжини хвилі λ світла, що поглинається. Ця залежність є спектром поглинання речовини.

В якості монохроматичного випромінювання використовувалися наявні у лабораторії лазери видимого спектру, що відрізнялися довжиною хвилі та потужністю випромінювання. Пучок лазерного світла проходив через досліджуване тіло. Випромінювання, що не поглиналося пластиком, потрапляло на закріплений з іншої сторони фоторезистор – фотоелектричний напівпровідниковий приймач випромінювання, принцип дії якого ґрунтується на ефекті фотопровідності (явищі зменшення опору напівпровідника у разі збудження носіїв заряду світлом). Для зчитування і подальшої обробки даних був використаний мікроконтролер «Arduino UNO». На фоторезистор подавалася напруга 5 В. В залежності від степені збудження фотоелементу змінювався його опір. Мікроконтролер робив заміри зміни напруги кожні 40 мс, оцифровував їх та відправляв на персональний комп’ютер.

Схематично лабораторну установку зображено на рис. 8. Вона включає досліджуване тіло із пластику у вигляді сходинок (рис. 7), лазер як джерело вузьконаправленого опромінювання готового виробу, фоторезистор та мікроконтролер, для зчитування розсіяного випромінювання. На рис. 9 наведено фотографію зібраної лабораторної установки та збільшену фотографію процесу оптичного опромінювання.

Для прийому та відображення поточного значення фоторезистора, а також розрахунку середнього арифметичного із виконаних замірів застосовувалося розроблене програмне забезпечення. Оскільки спектр поглинання речовини був невідомий для виготовленого зразка, у досліді використовувалися всі наявні в лабораторії лазери із різними характеристиками (див. табл. 1).

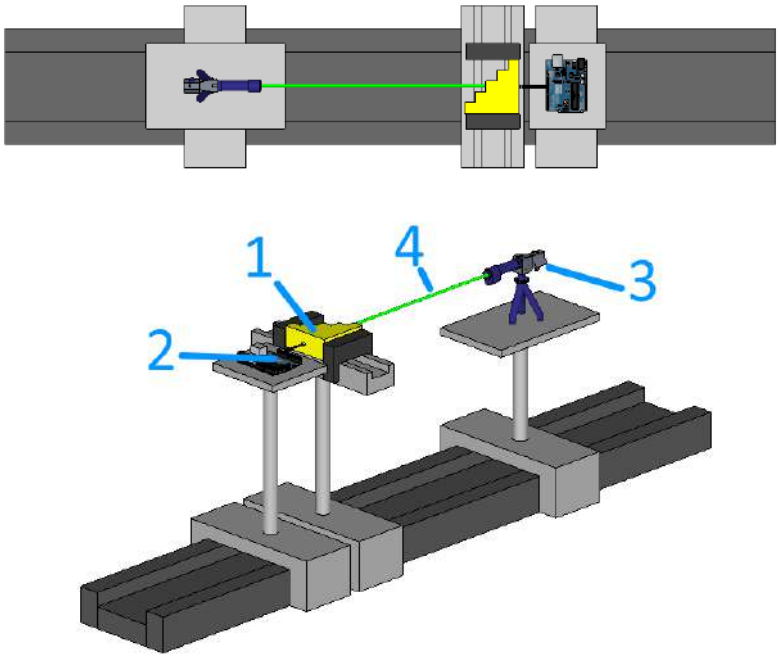


Рис. 8. Схема лабораторної установка: 1 – досліджуване тіло із пластику у вигляді сходинок; 2 – фоторезистор та мікроконтролер, що зчитує дані; 3 – лазер; 4 – лазерне випромінювання

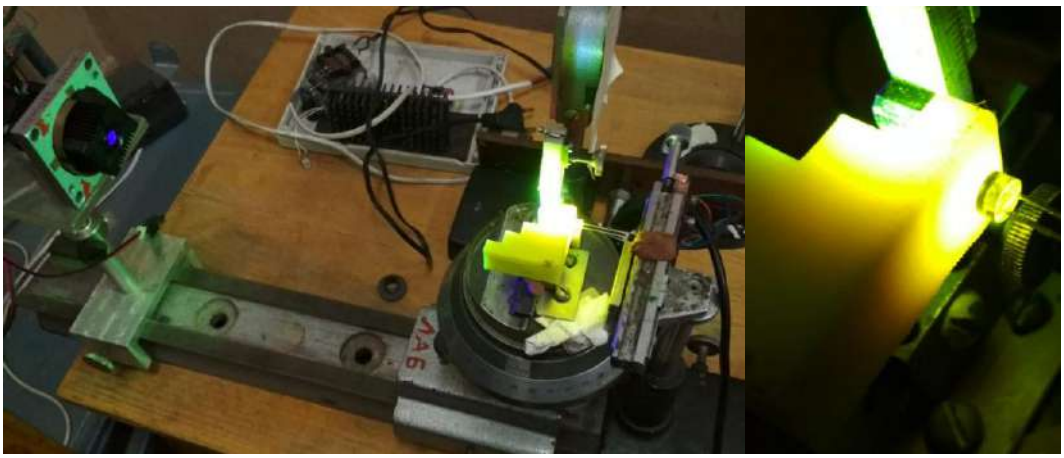


Рис. 9. Фотографія зібраної лабораторної установки (ліворуч)
та збільшена фотографія процесу опромінювання (праворуч)

Таблиця 1

Характеристики лазерів, які застосовувалися в експерименті

Номер	Довжина хвилі, нм	Потужність, мВт	Видимий колір
1	532	100	Зелений
2	650	25	Червоний
3	405	90	Фіолетовий
4	445	160	Синій
5	650	25	Червоний

Кожним лазером просвічувалися різні товщини досліджуваного тіла та робились заміри відсотку світла, що пройшов крізь дану ділянку тіла. Експеримент проводився за відсутності будь-яких інших ввімкнених джерел світла, тобто у темряві. Крок зміни товщини досліджуваного тіла 7 мм був обраний враховуючи товщину лазерного пучка, товщина якого знаходиться у межах 5-6 мм. Для коректності досліду, пучок лазерного випромінювання повинен повністю потрапляти на ділянку із однією товщиною. Мікроконтролер має вольтметр, що виявляє зміну напруги з кроком 5/1024 вольта, тому під час оцифровки аналогового значення отримуємо число від 0 (світло не потрапляє взагалі) до 1024 (максимальна кількість світла, яку може розпізнати фоторезистор).

2.2. Результати експерименту та їх інтерпретація

Отримані результати експериментальних досліджень (усереднені за виконаними вимірюваннями) зведено у табл. 2.

За наведеними у таблиці даними можна зробити висновок, що зразок із жовтого пластику найменше поглинає зелене лазерне випромінювання із довжиною хвилі λ=532 нм. Хоч обидва зразки виготовлені з однакового виду пластику, із-за різниці кольору вони мають зовсім різні показники поглинання. Тіло, що виготовлено з синього пластику, має значно більший показник поглинання. Навіть на мінімальній товщині тіло з синього пластику поглинуло світло з кожного лазера, якого б вистачило для визначення найменшої товщини.

Таблиця 2

Результати вимірювань

Зразок жовтого кольору						
Номер лазера	Товщина ділянки, мм					
	0	7	14	21	28	35
1	1024	1001	775	162	33	4
2	1024	995	426	65	6	0
3	1024	995	97	5	1	0
4	1024	998	500	59	5	0
5	1024	995	336	57	4	0
Зразок синього кольору						
Номер лазера	Товщина ділянки, мм					
	0	7	14	21	28	35
1	1024	0	0	0	0	0
2	1024	0	0	0	0	0
3	1024	0	0	0	0	0
4	1024	0	0	0	0	0
5	1024	0	0	0	0	0

Отримані результати для зразка матеріалу жовтого кольору свідчать, що для різної товщини матеріалу маємо різні значення інтенсивності випромінюванні і ці різниці досить суттєві. Отже, за результатами вимірювань принципово можливо встановити товщину матеріалу, та, відповідно, визначити вміст прихованих інформаційних бітів.

Висновки

В роботі досліджено новий напрямок технічної стеганографії, який пов'язаний із приховуванням інформаційних даних в процесі пошарового створення (вирощування) твердотільного об'єкта при використанні різних технологій 3D-друку. Інформаційні дані перетворюються в цифрову 3D-модель елементарних фізичних об’єктів, які розміщуються всередині 3D-моделі виробу-контейнеру. Після роздрукування твердий об'єкт фізично містить приховану інформацію, яку неможливо видалити або спотворити без пошкодження контейнеру. Крім того, застосовані методи не знижують експлуатаційних, естетичних та будь-яких інших властивостей готового виробу, оскільки технології, що застосовуються для нанесення шарів, не модифікуються, приховування є інваріантним способу пошарового вирощування, тобто можуть застосовуватися різні пристрої 3D-друку з будь-якими матеріалами і принципами пошарового створення.

Процес вилучення вбудованих даних здійснюється за допомогою сканування отриманого твердотільного об’єкту. Саме невизначеність конкретної процедури сканування отриманого твердого тіла є головним невирішеним питанням з приводу практичного застосування запропонованого комплексу 3D-стеганографії.

За результатами експериментальних досліджень встановлено принципову можливість зчитування прихованого повідомлення з 3D-моделі із застосуванням лазерних сканерів, в яких потік когерентного, монохроматичного, поляризованого і вузьконаправленого потоку випромінювання, що утворює паралельний пучок, зменшується в результаті поглинання в середовищі в деяку заздалегідь обумовлену кількість разів. Отримані результати для зразка матеріалу жовтого кольору свідчать, що для різної товщини маємо різні значення інтенсивності випромінюванні і ці різниці досить суттєві. Отже, за результатами вимірювань принципово можливо встановити товщину матеріалу, та, відповідно, визначити вміст прихованих інформаційних бітів.

Наведені результати експериментальних досліджень не є остаточними та потребують подальшого уточнення та відтворення. Зокрема, невирішеними є питання обрання типу і характеристик лазеру, погодженість цих характеристик із властивостями матеріалів

твердотільного об’єкту, налаштування фоторезисторів, тощо. Крім того, перспективним, на нашу думку, є проведення експериментальних досліджень із іншими видами випромінювання, видами та кольорами пластику.

Список літератури:

1. Katzenbeisser S., Petitcolas F. A. Information Hiding Techniques for Steganography and Digital Watermarking. – Norwood, MA, USA: Artech House, 2000. – 220 p.

2. Petitcolas F. A. P., Anderson R. J. and Kuhn M. G. Information hiding-a survey // Proceedings of the IEEE. – vol. 87, no. 7. – pp. 1062-1078. – Jul 1999.

3. Mazurczyk W., Smolarczyk M., Szczypiorski K. Retransmission steganography and its detection // Soft Computing, vol. 15, no. 3, pp. 505-515, 2011.

4. Nair A. S., Kumar A., Sur A. and Nandi S. Length based network steganography using UDP protocol // IEEE 3rd International Conference on Communication Software and Networks, Xi'an, 2011, pp. 726-730.

5. Ahsan K. and Kundur D. Practical data hiding in TCP Lip // ACM Workshop on Multimedia and Security, 2002, [On-line]. Internet: http://ee.tamu.edu/deepalpdf/ acm02.pdf.

6. S. H. Sellke, C. Wang, S. Bagchi and N. B. Shroff, "TCP/IP Timing Channels: Theory to Implementation", pp. 2204-2212, 2009.

7. Khan H., Javed M., Khayam S.A., Mirza F. Designing a cluster-based covert channel to evade disk investigation and forensics // Computers & Security. – Volume 30, Issue 1. – January 2011. [On-line]. Internet: https://www.sciencedirect.com/science/article/pii/ S016740481000088X

8. Khan H., Javed M., Khayam S.A., Mirza F. Evading Disk Investigation and Forensics using a Cluster-Based Covert Channel / National University of Science & Technology (NUST). – Islamabad 44000, Pakistan. [On-line]. Internet: https://www.sigsac.org/ccs/CCS2009/pd/abstract_17.pdf

9. Morkevičius N., Petraitis G., Venčkauskas A., Čeponis J. Covert Channel for Cluster-based File Systems Using Multiple Cover Files // Information Technology and Control, 2013, Vol.42, No.3. pp. 32. [On-line]. Internet: http://itc.ktu.lt/index.php/ITC/article/ view/3328

10. Rani R. and Deep G. Digital 3D barcode image as a container for data hiding using steganography // 4th International Conference on Signal Processing, Computing and Control (ISPCC), Solan, 2017. – P. 325-330.

11. Sun Z. , Z. m. Lu and Z. Li. Reversible Data Hiding for 3D Meshes in the PVQ-Compressed Domain // International Conference on Intelligent Information Hiding and Multimedia, Pasadena, CA, USA, 2006, pp. 593-596.

12. Wang K., Lavoué G., Denis F., Baskurt A. and He X. A Benchmark for 3D Mesh Watermarking // Shape Modeling International Conference, Aix-en-Provence, 2010. – P. 231-235.

13. Motwani M. C., Bryant B. D., Dascalu S. M. and F. C. Harris Jr. 3D Multimedia Protection Using Artificial Neural Network // 7th IEEE Consumer Communications and Networking Conference, Las Vegas, NV, 2010. – P. 1-5.

14. Vasić B. Annotation of cultural heritage 3-D models by robust data embedding in the object mesh // 22nd Telecommunications Forum Telfor (TELFOR), Belgrade, 2014. – P. 842-849.

15. Кузнецов А.А., Коваленко О.Ю. Стеганографическая защита информации с использованием 3D-печати // Інформаційна безпека держави, суспільства та особистості : зб. тез доповідей Всеукр. наук.-практ. конф., 16 квітня 2015 р. – Кіровоград : КНТУ, 2015. – С. 91-92.

16. Кузнецов О.О. Лекція 12: Технічна стеганографія. Приховування даних в твердотільних об'єктах за допомогою 3D-друку : Електронний конспект лекцій за дисципліною «Стеганографія». – Харків : Харк. нац. ун-т ім. Каразіна, 2016. – 14 с.

17. Коваленко О.Ю. Розробка лабораторного комплексу технічної стеганографії з використанням тривимірного друку : Пояснювальна записка до дипломної роботи бакалавра (Керівник О.О. Кузнецов). – Харків : Харк. нац. ун-т ім. Каразіна, 2015. – 47 с.

Харківський національний
університет імені В.Н. Каразіна;
АТ «Інститут інформаційних технологій», Харків

Надійшла до редколегії 09.11.2018

УДК 004.056

К.В. ІСІРОВА, О.В. ПОТІЙ, д-р техн. наук,

ДЕЦЕНТРАЛІЗОВАНІ ПРОТОКОЛИ КОНСЕНСУСУ: МОЖЛИВОСТІ ТА РЕКОМЕНДАЦІЇ ЩОДО ВИКОРИСТАННЯ

Вступ

Побудова систем для надійного надання користувачам послуг, пов’язаних із використанням інформаційних технологій, стає все більш актуальною задачею. Виникає необхідність побудови систем керування, в тому числі критичними інфраструктурами. Такі задачі традиційно вирішувалися за допомогою побудови централізованих систем з центральним "керуючим" або "хабом", на який покладалися обов’язки керування та контролю за системою. Проте, із різким збільшенням спектру електронних систем та кількості користувачів побудова централізованих систем стає менш ефективним рішенням. Будь-яка централізована система має своє максимально допустиме навантаження при перевищенні якого її функціонування стає неефективним. Більше того, необхідно брати до уваги зростаючі ризики з боку кібернетичних атак, які змушують шукати нові стратегії забезпечення безпеки систем. Особливо це стосується систем, які обробляють критичну інформацію. Традиційно "слабким місцем" будь-якої централізованої структури є її вершина (тобто центральний орган управління), вихід із ладу його внаслідок спрямованої атаки фактично означає зупинку функціонування всієї системи. Виходом вбачається перехід на децентралізовані системи. В яких кожен із учасників виконує частину обов’язків керуючого.

На сьогодні найпоширенішим прикладом успішного впровадження децентралізованих систем безумовно слугують криптовалюти. Необхідно зазначити, що такий принцип побудови може бути успішно впроваджений також в інших сферах, в тому числі у сфері електронних довірчих послуг [3].

Особливо важливим питанням при цьому є формулювання політик та вимог, за якими функціонує децентралізована система. Необхідно забезпечити всім користувачам єдине бачення стану системи в кожен конкретний момент часу. Це можливо із використанням технології blockchain. По суті, blockchain – це журнал з фактами (реєстр фактів), який реплікується на кілька комп'ютерів, об'єднаних в мережу рівноправних вузлів (P2P). Фактами може бути що завгодно, від фінансових операцій та до підписання контенту. Члени мережі – анонімні особи, звані вузлами. Всі комунікації всередині мережі використовують криптографію, щоб надійно ідентифікувати відправника і одержувача. Коли вузол хоче додати факт в журнал, в мережі формується консенсус, щоб визначити, де цей факт повинен з'явитися в журналі; цей консенсус називається блоком.

Надійне забезпечення доступності інформації щодо стану системи досягається за допомогою децентралізованих протоколів консенсусу.

Децентралізовані протоколи консенсусу можуть мати досить широкий спектр застосування:

- формування журналу транзакцій цифрових валют;
- кластери;
- контролери баз даних;
- високонадійні обчислювальні системи;
- критичні технічні системи;
- авіоніка (система управління авіаційним обладнанням);
- космічні системи;
- управління ядерними реакторами, тощо.

Мета статті – формулювання вимог до децентралізованих протоколів консенсусу, проведення порівняльного аналізу існуючих за обраними критеріями, а також надання рекомендацій щодо можливості застосування в залежності від вхідних параметрів.

Призначення протоколів консенсусу

Блоки в децентралізованій мережі одночасно формуються безліччю «учасників». Такі блоки, що задовольняють критеріям, відправляються в мережу та включаються в розподілену базу блоків. Виникають ситуації, коли кілька нових блоків в різних частинах розподіленої мережі посилаються на один і той же блок, тобто ланцюжок блоків може ділитися. Спеціально чи випадково можна обмежити ретрансляцію інформації про нові блоки (наприклад, один із ланцюжків може розвиватися в рамках локальної мережі). У цьому випадку можливо паралельне нарощування різних ланцюжків. У кожному з нових блоків можуть зустрічатися як однакові транзакції, так і різні, що увійшли тільки в один ланцюжок. Коли ретрансляція блоків відновлюється, учасники мають дійти згоди (консенсусу) щодо того, який ланцюжок вважати вірним. Це можливо з використанням децентралізованих протоколів консенсусу.

Консенсус – це спосіб, завдяки якому різні вузли мережі досягають згоди про набір даних, який представляє з себе стан цієї мережі. Наприклад, транзакції, баланси на різних рахунках, результати виконання смарт-контрактів. Система на базі технології blockchain може бути представлена у вигляді машини станів. Протокол консенсусу має забезпечувати послідовність дій, які забезпечують кожному вузлу доступ до актуального поточного стану мережі.

Основними вимогами до таких протоколів є [1, 2]:

– Відсутність центральної довіреної сторони (функціонування в середовищі взаємної недовіри: жоден з учасників не довіряє іншому).

– Рівноправність вузлів (мережа складається з рівноправних вузлів. Якщо зовнішня сторона або зловмисник намагається вивести з дії певну кількість вузлів, мережа продовжує нормально функціонувати до тих пір, поки чесні учасники складають необхідну більшість серед працюючих).

– Більшість вузлів є «чесними».

– «Чесні» учасники не знають, які вузли контролюються зловмисниками (список збійних («атакованих») вузлів невідомий чесним учасникам та може динамічно оновлюватися).

– у кожного вузла або їх деякої множини можливі збої, повне відключення, довільна поведінка (в тому числі і скоординована зловмисником для проведення атаки мережі)

– Мережа не є надійною (можливі довільні затримки і втрати (пропуски) повідомлень)

Перші дві вимоги формулюються виходячи із принципу децентралізації системи. Необхідна кількість чесних вузлів залежить від типу протоколу консенсусу (можливі варіанти: >1/2 чесних учасників, >2/3 чесних учасників). При цьому кожний чесний вузол приходить в один і той же стан в умовах збоїв частини вузлів (або скоординованої роботи злочинних вузлів) та працює за наперед відомим формалізованим протоколом (без участі людини або будь-якої додаткової інформації)

Виділяються такі припущення, за яких протоколи мають продовжувати функціонувати [12]:

– чесні функціонуючі вузли складають більшість (понад 1/2 або більше 1/3 учасників);

– час прийняття рішення не є фіксованим;

– використовується значна надмірність (можна виконувати ідентичні завдання).

Порівняльний аналіз протоколів консенсусу

В залежності від того, які правила використовуються для досягнення згоди між учасниками, можна виділити такі групи протоколів консенсусу.

Proof of Work протоколи [4, 5]

Основні характеристики:

– кількість вузлів-учасників є необмеженою;

– вузли анонімними;

– репутація вузлів невідома;

– необхідна кількість «чесних вузлів» 51 % для надійного функціонування протоколу;

– існує можливість централізації;

– вразливість до атаки 51 %;

– простота масштабування. Додавання нового вузла проходить без змін правил функціонування системи;

– низька пропускна здатність (швидкість формування блоку досягає в деяких випадках 10 хвилин);

– високі енергетичні витрати.

Учасники починають вважати головним ланцюжок з урахуванням рівня складності геш-значення і довжини ланцюжка (правило найдовшого ланцюжка). У разі рівного розподілу складності і довжини перевага віддається тому ланцюжку, кінцевий блок якого з'явився раніше. Найяскравішим прикладом є протокол консенсусу Bitcoin.

Існують також інші правила вибору головного ланцюжку, наприклад кількість блоків у дереві, що утворює певний ланцюжок (як у алгоритмі GHOST) [4] (рис.1).

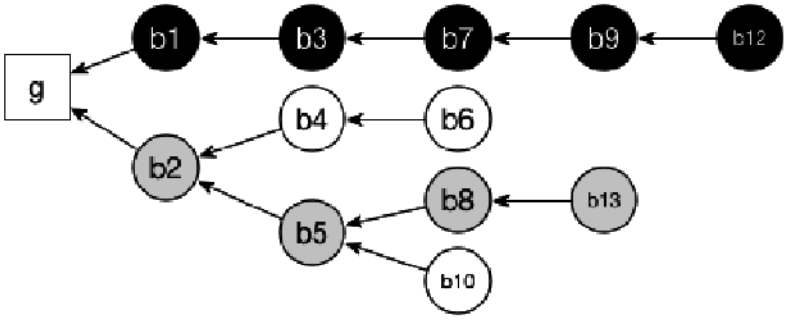


Рис. 1. Протокол консенсусу GHOST [4]

Транзакції, що увійшли тільки в відхилений ланцюжок, втрачають статус підтверджених. У 2017 – 2018 рр. були запропоновані нові алгоритми PoW консенсусу SPECTRE та PHANTOM [5], в яких використовується структура циклічного направленого графу (рис. 2) завдяки чому відсутня втрата блоків. Недоліком протоколів SPECTRE та PHANTOM слід зазначити необхідність зберігання великої кількості інформації.

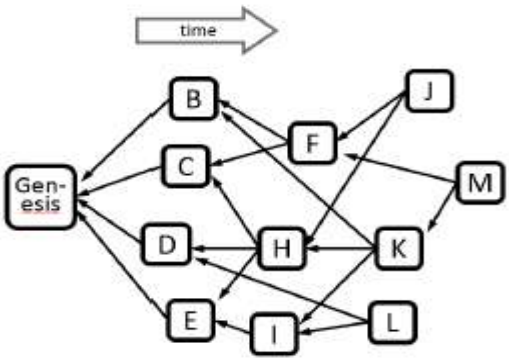


Рис. 2. Протокол консенсусу PHANTOM [5]

Proof of Stake протоколи [6, 7].

Основні характеристики:

– вузли-учасники не анонімні;

– вузли-учасники мають репутацію;

– монетарна мотивація учасників чесно слідувати протоколу. При спробі атаки "ставка" учасника-порушника згорає.

По суті відбувається голосування (рис. 3). Новий блок формує учасник, який зробив найбільшу «ставку». Логіка протоколів такого типу полягає в тому, що учасникам із великою кількістю монет, невигідно робити спроби атак, оскільки успішна атака призведе до знецінення криптовалюти. Таким чином, для учасника немає більш вигідної стратегії, ніж чесно слідувати протоколу.

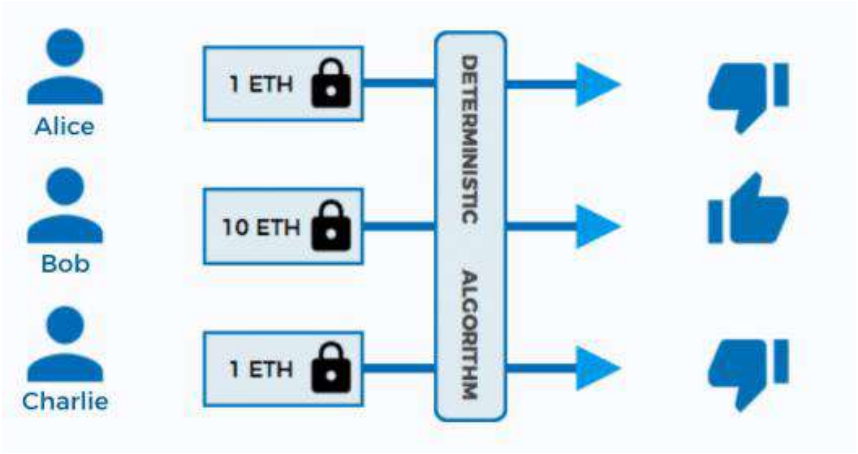


Рис. 3. PoS протокол консенсусу

При цьому вузли можуть передавати свої голоси іншим, які будуть голосувати від їх імені, таким чином утворюючи колегію виборців (Delegated PoS) [7].

BFT протоколи.

Основні характеристики:

– базуються на задачі Візантійських генералів;

– вузли-учасники не є анонімними;

– для надійного функціонування чесних учасників має бути >2/3;

– ймовірність відміни рішення є експоненційно спадною;

– для прийняття рішення необхідна кінцева кількість кроків;

– висока пропускна здатність;

– можливі елементи централізації.

Протоколи BFT історично з'явилися першими. Practical BFT [8, 9] протокол являв собою по суті варіант клієнт-серверної архітектури, коли тільки після звернення клієнта до серверу, транзакція могла бути передана іншим учасникам для підтвердження. Нові протоколи Algorand [10] та Hashgraph [11], наприклад позбавлені цього недоліку. Згідно з протоколом Algorand серед учасників випадковим чином обирається деякий підкомітет, який приймає рішення про підтвердження транзакції. Підтвердження відбувається у декілька етапів, на кожному з яких обирається окремий підкомітет. Протокол має високу пропускну здатність, добре масштабується. Проте, недоліком є погане функціонування у нестабільних мережах з великими затримками.

Табл. 1 містить зведені дані порівняння основних груп протоколів консенсусу.

Таблиця 1

Зведена таблиця порівняння протоколів консенсусу

Протоколи		Анонімність/ відкритість вузлів-учасників	Наявність репутації вузлів-учасників	Мотивація вузлів-учасників	Математична задача	Кількість «чесних вузлів»	Простота масштабування
PoW	GHOST	Вузли є анонімні	Репутація вузлів невідома	Винагородження за вирішення блоку	Пошук прообразу геш-функції	>1/2	Легко масштабувати
	SPECTRE						
	PHANTOM						
PoS	DelPoS DPoS	Вузли не анонімні	Вузли мають репутацію	Мотивація учасників чесно слідувати протоколу полягає в тому, що немає більш вигідної стратегії	Система "голосування"	>1/2	Труднощі у масштабуванні
BFT	Practical BFT	Вузли не анонімні	Вузли мають репутацію	Мотивація учасників чесно слідувати протоколу лежить за межами протоколу	«Проблема Візантійських генералів»	>2/3	Важко масштабувати
	Honey Badger BFT						
	ALGORAND						Легко масштабувати
	HSHGRAPH						

Таким чином, можна зробити висновки, що кожна з груп має свої переваги та недоліки. Табл. 2 наводить їх у зведеній формі.

Таблиця 2

Переваги та недоліки основних груп протоколів консенсусу

Протоколи	Переваги	Недоліки
PoW	Доказова стійкість Легка масштабованість	Високі енергетичні затрати Втрата частини інформації Необхідність зберігати великий об'єм інформації Низька пропускна спроможність
PoS	Відсутність математичного доведення стійкості	Висока пропускна спроможність Мотивація учасників чесно слідувати протоколу
BFT	Висока пропускна здатність Рішення, яке отримане не може бути відмінено з часом Для отримання рішення необхідна кінцева кількість кроків	Необхідність 2/3 чесних вузлів Відсутність мотивації учасників чесно слідувати протоколу

Можливо виділити наступні рекомендації:

1. Вибір протоколу консенсусу має базуватися насамперед на умовах, в яких передбачається функціонування системи.

2. Можливе поєднання декількох протоколів в один (так звані гібридні протоколи).

3. Якщо система має функціонувати в умовах взаємної недовіри без додаткових інструментів контролю за користувачами, доцільне використання PoW протоколів, не дивлячись на низьку пропускну здатність таких протоколів.

4. Для систем закритого типу із наперед прогнозованою кількістю вузлів і без перспектив швидкого розширення використання BFT протоколів є вигідним. При цьому необхідно

додатково забезпечувати мотивацію вузлів-учасників чесно слідувати протоколу. Необхідною є первинна ідентифікація учасників.

5. Для не анонімних систем відкритого типу доцільним є використання PoS протоколів.

6. Якщо система має специфічну архітектуру та особливі умови функціонування, можливе використання гібридних багатошарових протоколів консенсусу, розроблених відповідно до особливостей даної системи. Одним із прикладів може бути поєднання PoW та PoS протоколу, в якому нові користувачі, які ще не мають попередньої історії транзакцій та, відповідно, особистої репутації, користуються PoW протоколом, який в даному випадку забезпечуватиме їх накопиченням репутації. Після проходження "порогу довіри" користувач переходить на використання PoS протоколу.

Висновки

1. Децентралізовані системи здатні краще забезпечити функціонування електронних систем в умовах збільшення спектру електронних послуг та зростання кількості користувачів.

2. Для надійного функціонування децентралізованих систем (в тому числі у критичних інфраструктурах) можливе використання технології blockchain із децентралізованими протоколами консенсусу.

3. Вибір протоколу консенсусу має базуватися за умов, в яких передбачається функціонування системи. Для систем закритого типу із заздалегідь прогнозованою кількістю учасників доцільним вбачається використання BFT протоколу із додатковим забезпеченням контролю за чесністю учасників. Для анонімних систем із відсутністю можливості контролю передбачається використання доопрацьованих PoW протоколів PoS.

Список літератури:

1. L. Aniello, R. Baldoni, E. Gaetani, F. Lombardi, A. Margheri, and V. Sassone. A prototype eval-uation of a tamper-resistant high performance blockchain-based transaction log for a distributed database // EDCC. IEEE, 2017.

2. C. Cachin, R. Guerraoui, and L. Rodrigues. Introduction to reliable and secure distributed programming // Springer, 2011.

3. K. Isirova and O. Potii. Decentralized public key infrastructure development principles // IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT). – Kiev, 2018. – P. 305-310.

4. J. A. Garay, A. Kiayias, and N. Leonardos. The Bitcoin Backbone Protocol // Analysis and Applications, volume 9057 of LNCS, pages 281{310. Springer, 2015.

5. Aggelos Kiayias1 and Giorgos Panagiotakos. On Trees, Chains and Fast Transactions in the Blockchain Yonatan Sompolinsky and Aviv Zohar. PHANTOM: A Scalable BlockDAG protocol

6. Bernardo Machado David, Peter Gazi, Aggelos Kiayias, and Alexander Russell. Ouroboros praos: An adaptively-secure, semi-synchronous proof-of-stake protocol. IACR Cryptology ePrint Archive, 2017:573, 2017.

7. George Danezis and Sarah Meiklejohn. Centrally banked cryptocurrencies // 23nd Annual Network and Distributed System Security Symposium, NDSS 2016, San Diego, California, USA, February 21-24, 2016. The Internet Society, 2016.

8. Stefano De Angelis; Leonardo Aniello1; Roberto Baldoni1,Federico Lombardi;Andrea Margheri and Vladimiro Sassone. PBFT vs Proof-of-Authority: Applying the CAP Theorem to Permissioned Blockchain

9. M. Castro and B. Liskov. Practical byzantine fault tolerance and proactive recovery // ACM Trans. Comput. Syst., 20(4):398{461, 2002.

10. Algorand Whitepaper: https://www.algorand.com/docs/whitepapers/

11. LEEMON BAIRD. THE SWIRLDS HASHGRAPH CONSENSUS ALGORITHM: FAIR, FAST, BYZANTINE FAULT TOLERANCE

12. D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun. A review on consensus algorithm of blockchain.

Харківський національний
університет імені В.Н. Каразіна;
АТ «Інститут інформаційних технологій», Харків

Надійшла до редколегії 29.10.2018

МЕТОДЫ ВЫЯВЛЕНИЯ, РАСПОЗНАВАНИЯ И УПРАВЛЕНИЯ ЛЕТАТЕЛЬНЫМИ АППАРАТАМИ

УДК 629.7.022

В.Н. ОЛЕЙНИКОВ, канд. техн. наук, О.В. ЗУБКОВ, канд. техн. наук,
В.М. КАРТАШОВ, д-р техн. наук, И.В. КОРЫТЦЕВ, канд. техн. наук,
С.И. БАБКИН, канд. техн .наук, С.А. ШЕЙКО, канд. техн. наук

ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ ОБНАРУЖЕНИЯ И РАСПОЗНАВАНИЯ МАЛОРАЗМЕРНЫХ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ ПО ИХ АКУСТИЧЕСКОМУ ИЗЛУЧЕНИЮ

Введение

Одной из актуальных задач является защита гражданских и военных объектов от беспилотных летательных аппаратов (БПЛА), несущих потенциальную угрозу. Для решения этой задачи требуется обнаружить БПЛА в зоне охраняемого объекта, определить пеленг на БПЛА и задействовать защитные системы. При обнаружении БПЛА в системах военного назначения приоритет отдается пассивным методам, в частности методам пассивной акустической и оптической локации. БПЛА, как правило, представляют собой аэродинамические объекты типа моноплан или мультикоптер, являющиеся локализованными источниками акустического излучения (АИ). В работе рассматриваются вопросы обнаружения и распознавания БПЛА на основе обработки собственного АИ, создаваемого БПЛА в полете.

Важно отметить – несмотря на то, что задачи обнаружения и распознавания направлены на достижение общей цели, математически и алгоритмически они решаются по-разному. Для реализации распознавания БПЛА создается база данных, в которой хранятся векторы признаков АИ, соответствующие различным моделям БПЛА и режимам полета. Однако на рынке постоянно появляются новые модификации летательных аппаратов, поэтому практически все базы данных будут очень ограниченными и задача распознавания может быть реализована только по отношению к имеющимся в базе векторам признаков АИ. В то же время для повышения надежности первичного обнаружения БПЛА необходим универсальный метод, учитывающий общие признаки АИ, характерные для любых моделей БПЛА.

1. Особенности АИ БПЛА, помех и шумов

Для выявления характерных особенностей информационных акустических сигналов и создания их адекватной математической модели, необходимой на этапе разработки алгоритмов обнаружения и распознавания, были проведены эксперименты по измерению спектральной плотности мощности (СПМ) АИ БПЛА. Типовая реализация СПМ АИ квадрокоптера содержит узкополосные спектральные составляющие основного тона, его гармоник и широкополосную шумовую составляющую, обусловленную срывом турбулентного воздушного потока винтов (рис. 1).

Анализ СПМ различных моделей малоразмерных БПЛА [1 – 4], способных нести полезную нагрузку, например в виде профессиональной видеокамеры, показал, что частота основного тона АИ БПЛА находится в пределах от 90 до 240 Гц. Количество гармоник основного тона АИ БПЛА – от 10 до 40, но с увеличением расстояния до БПЛА, вследствие поглощения звука в атмосфере, высокочастотные гармоники существенно ослабляются до уровня фоновых шумов и поэтому их нецелесообразно включать в процесс обработки. В дальнейшем в процессе обработки используются от двух до восьми гармоник основного тона АИ БПЛА.

Важную роль в процессе синтеза алгоритмов обнаружения и распознавания сигналов, как известно, играют характеристики помех и шумов. На рис. 2 показан пример сглаженной реализации СПМ природных атмосферных шумов, которая зависит от ряда параметров, отражающих состояние приземного слоя атмосферы в момент проведения измерений. Значения

СПМ природных атмосферных шумов хорошо аппроксимируются функцией логарифмически-нормального закона распределения

$$S(f) = \frac{1}{\sigma\sqrt{2\pi}f} e^{-\frac{(\ln(x)-\ln a)^2}{2\sigma^2}}. \quad (1)$$

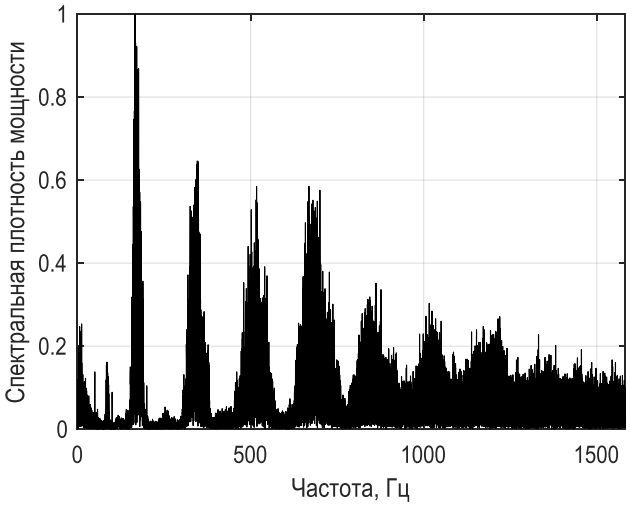


Рис. 1. Реализация СПМ АИ квадрокоптера DJI Phantom 3

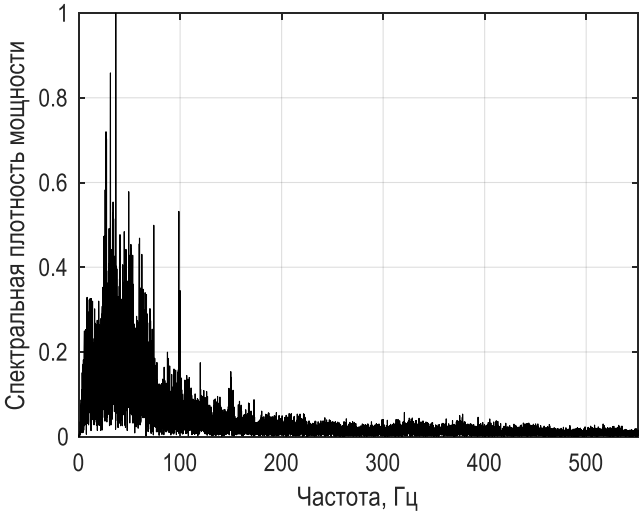


Рис. 2. Сглаженная реализация СПМ природных атмосферных шумов

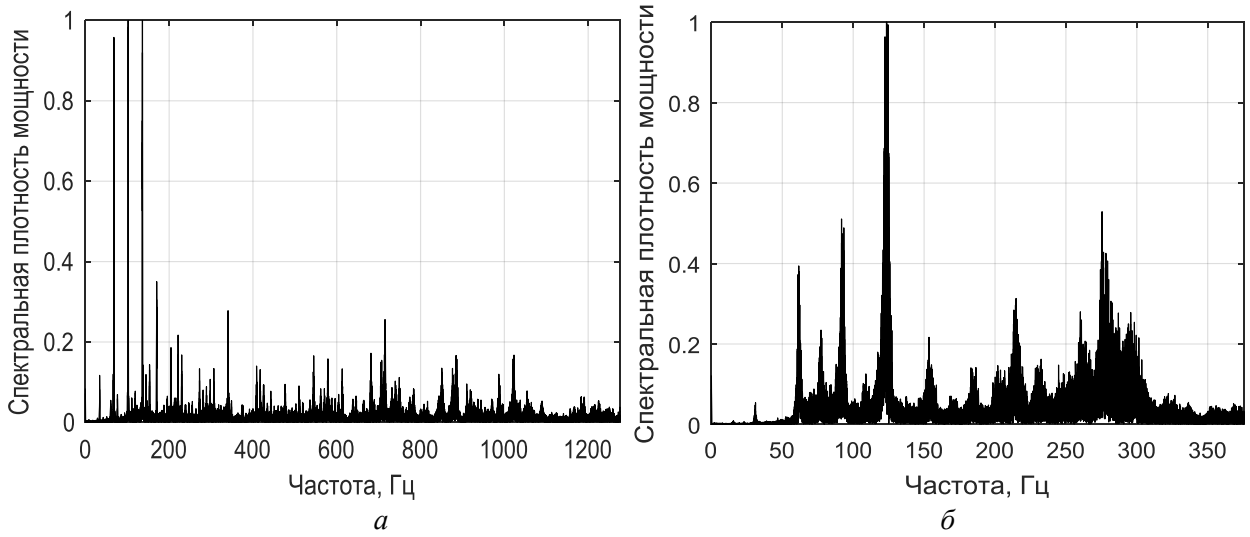
Огибающая СПМ АИ БПЛА (рис. 1) может быть описана полиномами высоких степеней. Сопоставление маски шаблона природных атмосферных шумов с полиномиальной моделью СПМ АИ БПЛА позволяет произвести их классификацию.

Серьезную проблему при обнаружении и распознавании АИ БПЛА оказывают шумы бензиновых и дизельных автомобильных двигателей, трамваев, железнодорожного транспорта, голоса людей и животных. Типовые реализации СПМ шумов автомобильного дизельного и бензинового двигателей представлены на рис. 3, *а*,*б*.

СПМ шумов автомобильных двигателей имеют характер схожий с СПМ БПЛА. Частота основного тона АИ автомобильных двигателей существенно меньше частоты вращения авиационных двигателей и находится в пределах от 40 до 80 Гц, поэтому отличить их от АИ БПЛА можно по более низкой частоте основного тона. Это различие является характерным отличительным признаком.

Анализ аудиозаписей речи человека показал, что СПМ многих речевых сигналов имеют сходный характер с СПМ БПЛА, при этом частота основного тона, как правило, находится в диапазоне свыше 200 Гц с вероятностью 98 % [5], что может служить дополнительным признаком отличия речевого сигнала от сигнала АИ БПЛА.

Важным параметром сигнала АИ БПЛА является время квазистационарности: этот параметр определяет возможную максимальную протяженность сегмента при реализации алгоритмов обнаружения и распознавания. Сигнал АИ БПЛА разбивается на сегменты фиксированной длины, не превышающей длительности интервала стационарности, в пределах которого предполагается постоянство среднего значения, дисперсии, и частотной структуры сигнала. На больших интервалах времени АИ БПЛА является нестационарным, однако из-за инерционности механических узлов винтомоторной группы БПЛА в пределах определенного промежутка времени его акустические характеристики практически не изменяются.



а *б*

Рис. 3. Типовые реализации СПМ шумов автомобильного дизельного (*а*) и бензинового двигателей (*б*)

На рис. 4. приведена сонограмма акустического сигнала, полученная во время пилотажа БПЛА DJI Phantom 3, из которой следует, что стационарность сигнала сохраняется на интервалах протяженностью более 1 секунды.

Дополнительным критерием отличия речевых сигналов и сигналов АИ БПЛА является различное время стационарности. В [5] показано, что максимальная длительность фонем речевых сигналов не превышает 345 мс. Со сменой фонемы изменяются и ее спектральные характеристики.

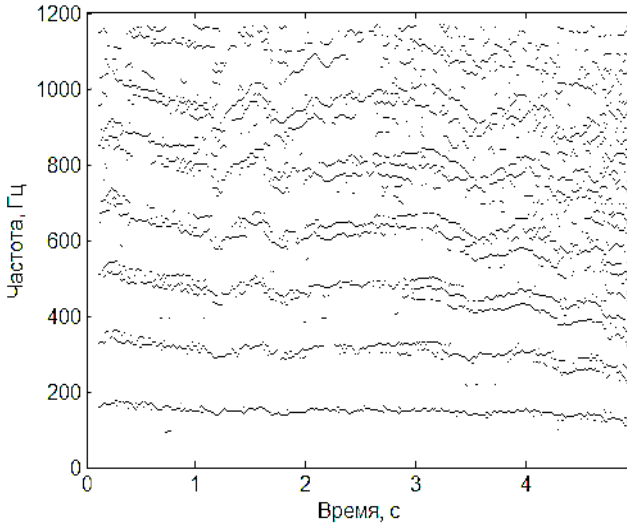


Рис. 4. Сонограмма акустического сигнала, полученная во время пилотажа БПЛА DJI Phantom 3

2. Алгоритм обнаружения АИ БПЛА

При обнаружении АИ БПЛА необходимо решать следующие задачи:

—осуществлять различение природных шумов окружающей среды и АИ БПЛА;

—обеспечивать эффективную борьбу с внешними источниками акустических помех, имеющими спектральные характеристики схожие с БПЛА;

—обеспечивать независимость принятия решения от модели БПЛА и режима его полета.

С учетом анализа АИ БПЛА, шумов городского транспорта, речевых сигналов, шумов природной окружающей среды разработан алгоритм обнаружения АИ БПЛА, включающий несколько этапов.

На первом этапе обработки осуществляется фильтрация акустического сигнала с выхода микрофона фильтром верхних частот для устранения влияния низкочастотных помех.

На втором этапе выполняется дискретизация сигнала с частотой $F_д$ и сегментация последовательности отсчетов с длиной сегмента N отсчетов: X_i, i=0…N-1.

На третьем этапе вычисляется автокорреляционная функции (АКФ) в пределах дискретизированного сегмента:

$$B(j) = \sum_{i=0}^{j} X_i \cdot X_{N-i-1}, j = 0 \dots 2N-1 . \quad . \quad (2)$$

На четвертом этапе вычисляется БПФ от АКФ каждого сегмента. Как показано в [2], вычисление БПФ от первой, второй и т.д. АКФ позволяет повысить отношение сигнал/шум при выделении гармонического сигнала на фоне шумов. Дополнительно выполняется сглаживание СПМ S(f) фильтром скользящего среднего с длиной окна τ = 15-20 отсчетов:

$$\overline{S(F)} = \frac{1}{\tau}\sum_{f=F}^{F+\tau-1} S(f),\ F = 0 \dots 2N. \quad (3)$$

Сглаживание позволяет упростить дальнейший поиск максимумов СПМ.

На пятом этапе осуществляется поиск всех локальных максимумов спектра в пределах 80 Гц – 3 кГц и вычисление глобальных максимумов и минимумов СПМ.

На шестом этапе вычисляются частоты основного тона, проверяется наличие не менее двух гармоник основного тона с предельным отклонением частот не более 6 % от частот, кратных основному тону. При этом гармоники основного тона проверяются на соответствие глобальным максимумам СПМ. В случае соблюдения этих условий проводятся дополнительные проверки на идентичность СПМ природным шумам и речевым звукам. При анализе идентичности СПМ природным шумам полученная СПМ аппроксимируется в соответствии с (1). Далее вычисляются отклонения абсолютных значений локальных максимумов и минимумов СПМ от аппроксимирующей кривой. При относительной погрешности аппроксимации свыше 10 % шумы следует относить к природным.

Для анализа идентичности СПМ речевым сигналам используется объединение текущего обрабатываемого сегмента с последующим в единый сегмент длиной 2N отсчетов. Полученный массив разбивается на три новых субсегмента и для пар 1-2, 2-3, 3-4 вычисляются взаимно корреляционные функции. Для каждой из них повторяются этапы 4-6 данного алгоритма. Вычисление СПМ по взаимно корреляционной функции позволяет выявлять в спектре периодические составляющие сигнала согласно [6]. БПЛА считается обнаруженным, если частоты основного тона и гармоник основного тона первичного обрабатываемого сегмента звукового сигнала совпадают с полученными на основании анализа СПМ взаимно корреляционных функций пар субсегментов.

3. Алгоритм распознавания АИ БПЛА

В системах автоматического распознавания АИ технических средств выделяют три основных этапа: выделение информационных признаков, обучение и распознавание. На первом этапе из исходного акустического сигнала выделяют вектор признаков, который является компактным описанием акустических характеристик сигнала, достаточных для распознавания. Обучение предполагает получение набора эталонных векторов признаков АИ для ряда моделей БПЛА при типичных режимах работы винтомоторной группы, условиях полета, и характера местности. С целью распознавания проводится сравнение текущего вектора признаков с хранимыми в системе эталонными векторами признаков по одному из правил принятия решения.

3.1. Выделение информационных признаков методом мел-кепстральных коэффициентов

Для распознавания АИ БПЛА предлагается использовать метод мел-кепстральных коэффициентов (Mel-Frequency Cepstral Coefficients – MFCC), который получил широкое распространение в системах распознавания речи [7] и в области диагностики технических систем [8]. Преимущество метода объясняется независимостью получаемого вектора признаков АИ БПЛА от длины исходного фрагмента обрабатываемого сигнала, его относительно малым размером и учетом разброса характеристик АИ исследуемого объекта.

Для снижения влияния внешних антропогенных шумов сигнал обрабатывается цифровым фильтром верхних частот. Далее последовательность отсчетов сигнала разбивается на сегменты, протяженность которых меньше времени стационарности АИ БПЛА.

В пределах сегмента предлагается производить нормализацию записанного сигнала, поскольку на уровень записываемого акустического сигнала, излученного БПЛА, влияет ряд факторов: режим работы двигателей, их число, удаленность от микрофона, ракурс летательного аппарата, погодные условия. Применение нормализации позволяет уменьшить разброс уровней записанного акустического сигнала для различных условий полета и наблюдения БПЛА.

После выполнения нормализации исходный сегмент разбивается на субсегменты, идущие с перекрытием 75 % в пределах сегмента. Для снижения искажений при спектральном анализе, обусловленных конечным размером выборки, к каждому субсегменту применяется весовая обработка. В качестве весовой функции выбрано окно Хэмминга. Далее выполняется дискретное преобразование Фурье:

$$X[k] = \sum_{n=0}^{N-1} x[n] e^{\frac{-2\pi i}{N} kn}, \ k \in 0,1..N-1 \quad (4)$$

Значения индексов *k* соответствует частоте $f = \frac{F_s}{N}$, где F_s – частота дискретизации сигнала. Для повышения отношения сигнал/шум осуществляется накопление спектров в пределах сегмента.

Сигнал, представленный в частотной области, далее обрабатывается набором полосно-пропускающих фильтров с треугольной аппроксимацией частотных характеристик. Границы частотной характеристики фильтров вычисляются в шкале мел.

Оконная функция для реализации полосно-пропускающих фильтров описывается выражением

$$H_m[k] = \begin{cases} 0 & k < f[m-1] \\ \frac{(k - f[m-1])}{(f[m] - f[m-1])} & f[m-1] \le k < f[m] \\ \frac{(f[m+1] - k)}{(f[m+1] - f[m])} & f[m] \le k \le f[m+1] \\ 0 & k > f[m+1] \end{cases}, \quad (5)$$

где *m* – номер фильтра, $m \in 1..N_F$, N_F – количество полосно-пропускающих фильтров.

Энергия сигнала для каждой полосы треугольного окна в логарифмическом представлении

$$S[m] = ln(\sum_{k=0}^{N-1} |X[k]|^2 H_m[k]), \ m \in 1..N_F, \quad (6)$$

где k – номер отсчета спектра.

Для уменьшения количества выходных параметров и декорреляции компонентов применяется дискретное косинусное преобразование, в результате которого получаем вектор *C* (вектор признаков), содержащий набор мел-частотных кепстральных коэффициентов

$$C[n] = \sum_{m=0}^{N_F - 1} S[m] cos\left(\frac{\pi n\left(m + \frac{1}{2}\right)}{N_F}\right), n \in 1..N_{kk}, \quad (7)$$

где N_{kk} – количество рассчитываемых мел-частотных кепстральных коэффициентов.

В результате обработки сигнала в соответствии с предложенным алгоритмом значительное количество отсчетов АИ заменяется на компактный набор мел-частотных кепстральных коэффициентов.

3.2. Правило принятия решений

При распознавании АИ БПЛА производится сравнение его вектора признаков с эталонным вектором признаков, полученным на этапе обучения. Для принятия решений о принад-

лежности входного звукового образа, представленного вектором признаков, применено решающее правило, базирующееся на методах корреляционного анализа. В этом случае мерой степени близости (коэффициента подобия) между векторами признаков акустических параметров исходного сигнала *C* и эталонным вектором признаков *CE* используется коэффициент корреляции между координатами точек пространства параметров акустических характеристик:

$$R_{C,CE} = \frac{cov(C,CE)}{\sqrt{s_C^2 s_{CE}^2}}, \quad (8)$$

где $cov(C, CE)$ – ковариация случайных величин *C* и *CE*, s_C^2, s_{CE}^2 – выборочные дисперсии случайных величин *C* и *CE*.

4. Результаты эксперимента

Для исследования эффективности рассмотренных алгоритмов обнаружения и распознавания была сформирована фонотека тестовых акустических сигналов, соответствующих различным моделям БПЛА и режимам их полета. Записи полетов БПЛА получены в условиях города и загородной местности, а также в студии звукозаписи. Длительность каждого из тестовых сигналов составляет около 600 с.

Звукозапись АИ БПЛА осуществлялась с использованием измерительного конденсаторного микрофона Superlux ECM-999, имеющего круговую диаграмму направленности. Выход микрофона подключался посредством симметричного аудиоинтерфейса XLR ко входу внешней звуковой карты Behringer U-Phoria UM2. Звуковой сигнал оцифровывался с частотой дискретизации F_s= 48 кГц и разрядностью 24 бита.

Тестовые сигналы ТС1 – ТС3 представляют собой АИ квадрокоптеров DJI Phantom 3 и Syma X5SW**.** Тестовый сигнал ТС1 записан в условиях города. Начальный участок протяженностью 200 с содержит звуки окружающей городской среды и фрагменты речи, последующие 400 с соответствуют зависанию квадрокоптера DJI Phantom 3 на высоте 2 м на дистанциях от 5 до 80 м с шагом 5 м. Сигнал ТС2 записан при вертикальном взлете квадрокоптера DJI Phantom 3 от поверхности земли до высоты 110 м. Запись ТС3 соответствует пилотажу квадрокоптера Syma X5SW на высоте 2-10 м с максимальным удалением от микрофона на расстояние 40 м.

В ряд тестовых сигналов включены типичные мешающие сопутствующие акустические сигналы (ТС4 – ТС8), присутствующие при проведении обнаружения и распознавания АИ БПЛА: ТС4 – шум ветра, ТС5 – разговорная речь,ТС6 – шум автомобильной магистрали, ТС7 – шум рельсового электротранспорта (трамвай, железнодорожный состав), ТС8 – шумы мотокосы.

При реализации алгоритма обнаружения осуществляется фильтрация звукового сигнала с выхода микрофона фильтром верхних частот с частотой среза 80 Гц далее производится сегментация последовательности отсчетов временной реализации звукового сигнала с длиной сегмента N=16384 отсчетов. Для указанной выше частоты дискретизации сегменты соответствуют интервалу времени 0,34 с.

При реализации алгоритма мел-кепстральных коэффициентов используется участок спектра АИ БПЛА в полосе 80 – 2600 Гц. Размер сегмента выбран равным 1 с, применено дискретное преобразование Фурье с числом отсчетов N=16384. Число коэффициентов для формирования вектора признаков выбрано равным 16 (количество полосно-пропускающих фильтров с треугольной аппроксимацией частотных характеристик – 32), их увеличение не обеспечивает повышения точности распознавания, поскольку с повышением номера коэффициента его значимость уменьшается.

Для распознавания АИ БПЛА методом мел-кепстральных коэффициентов выполняется сравнение текущего вектора признаков с эталонными векторами признаков АИ БПЛА, хранимыми в системе, в соответствии с выражением (8). Сигнал, из которого извлекается

эталонный вектор признаков, должен обладать некими усредненными параметрами, характерными для большинства условий наблюдения. По этой причине эталонный вектор признаков, извлеченный из сигнала АИ БПЛА, записанного в студии звукозаписи, проявил себя недостаточно эффективно, он оказался слишком «стерильным», лишенным особенностей окружающей среды. На практике целесообразно иметь несколько эталонных векторов признаков АИ для БПЛА одного типа, полученных для различных условий его полета, наблюдения и характера местности.

На рис. 5, *а* представлено изменение коэффициента подобия для векторов признаков тестового сигнала ТС1 и эталоного вектора признаков АИ квадрокоптера DJI Phantom 3. Эталонный вектор признаков АИ извлекается из сигнала, записанного на удалении 10 м от БПЛА. Точками в правой верхней части рисунка нанесена шкала расстояния до квадрокоптера.

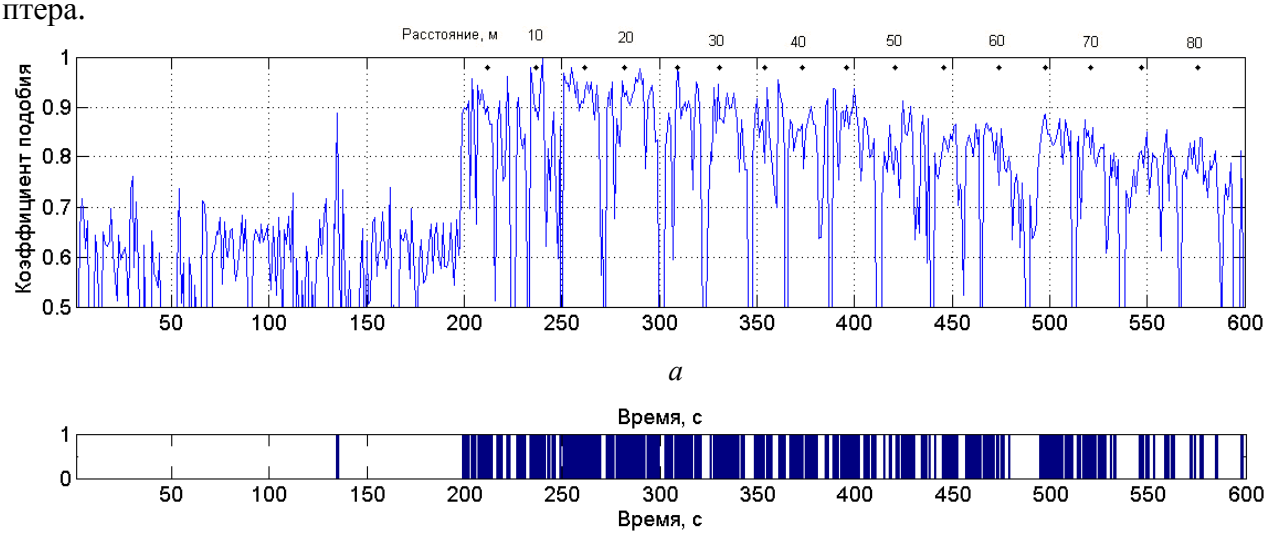


Рис. 5. Изменение коэффициента подобия для векторов признаков тестового сигнала ТС1 и эталонного вектора признаков АИ квадрокоптера DJI Phantom 3 (*а*);
результат работы алгоритма принятия решения о распознавании АИ БПЛА (*б*)

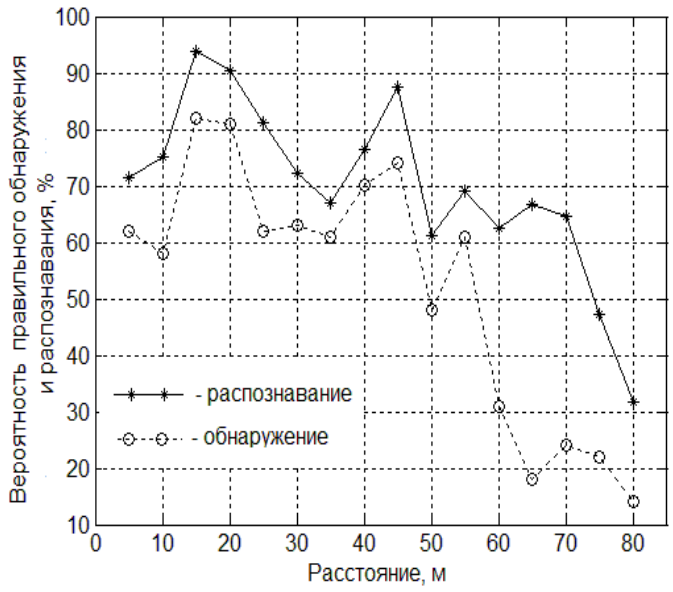


Рис. 6. Зависимости вероятности правильного обнаружения и распознавания от расстояния до квадрокоптера DJI Phantom 3

Результат работы алгоритма принятия решения о распознавании АИ БПЛА представлен на рис. 5, *б* в виде диаграммы, у которой при превышении порога отображается вертикальный столбик. На начальном участке записи тестового сигнала (0 – 200 с) присутствуют только звуки окружающей городской среды и фрагменты речи. Это позволяет при выбранном пороге принятия решения о распознавании (0,80) определить вероятность ложного распознавания ($P_{лр}$ < 0,5%). Участок записи тестового сигнала ТС1 (201 – 600 с) использовался для построения зависимости вероятности правильного распознавания $P_{пр}$ от расстояния до БПЛА в условиях города

(рис. 6). На этом же рисунке представлена аналогичная зависимость для алгоритма обнаружения в виде зависимости верятности правильного обнаружения $P_{по}$ от расстояния до источника АИ.

Характер поведения графиков обеих зависимостей, полученных независимыми методами, очень схож, совпадает даже в деталях.

Оценки результатов обработки для тестовых сигналов ТС1-ТС3 АИ квадрокоптеров с использованием алгоритма обнаружения и распознавания методом мел-кепстральных коэффициентов приведены в таблице:

Тестовый сигнал	Алгоритм обнаружения		Метод мел-кепстральных коэффициентов	
	$P_{по}$, %	$P_{ло}$, %	$P_{пр}$, %	$P_{лр}$, %
АИ квадрокоптера DJI Phantom 3 при горизонтальном полете на дистанции 80 м (ТС1).	45,5	1,0	69,2	0,5
АИ квадрокоптера DJI Phantom 3 при вертикальном взлете от поверхности земли до высоты 110 м (ТС2).	25,6	1,0	32,5	0,5
АИ квадрокоптера Syma X5SW при пилотаже квадрокоптера на высоте 2-10 м с максимальным удалением от микрофона на 40 м (ТС3).	60,8	-	78,4	-
Шум ветра (ТС4).	-	0	-	0
Разговорная речь (ТС5).	-	1,3	-	0,2
Шум автомобильной магистрали (ТС6).	-	2,6	-	0,15
Шум рельсового электротранспорта (ТС7).	-	1,5	-	0
Шум мотокосы (ТС8).	-	1,1	-	0

Большие различия оценок верятности правильного обнаружения и распознавания объясняются различными условиями полета БПЛА, режимом работы винтомоторной группы, затуханием сигнала АИ при удалении от микрофона, наличием переотражений от зданий.

Результаты устойчивости алгоритмов обнаружения и распознавания к шумам окружающей среды исследовались с использованием тестовых сигналов ТС4 – ТС8 и представлены в таблице. Алгоритм обнаружения оказался наиболее чувствительным к шумам автомобильной магистрали и рельсового электротранспорта. Метод распознавания на основе мел-кепстральных коэффициентов оказался менее чувствительным к шумам окружающей среды .

Выводы

Результаты обработки аудиозаписей БПЛА, полученных с использованием ненаправленного микрофона, показали, что алгоритм обнаружения достаточно эффективно работает при удалении объекта до 80 м: он обеспечивает вероятность правильного обнаружения порядка 50 % на расстояниях до 50 м и порядка 15 % на удалении 80 м. Вероятность ложного обнаружения в условиях города – до 1 %. Работа алгоритма одинаково эффективна для любой из рассмотренных моделей БПЛА.

Использование метода мел-кепстральных коэффициентов позволяет обеспечивать вероятность правильного распознавания до 60 % на дистанции 50 м, 30 % на расстояниях до 80 м. Вероятность ложного распознавания в условиях города – до 0,5 %. Такие результаты обеспечиваются только для конкретного типа БЛЛА, при наличии его векторов признаков для разных режимов полета.

Полученные результаты исследований позволяют говорить о возможности использовать рассмотренные алгоритмы обнаружения и распознавания акустических сигналов БПЛА для задач оперативного контроля воздушного пространства.

Список литературы:

1. Олейников В.Н., Шейко С.А., Бабкин С.И. Исследование характеристик акустического излучения малых беспилотных летательных аппаратов // Сб. науч. тр. VI Междунар. радиоэлектронного форума “Прикладная радиоэлектроника. Состояние и перспективы развития (МРФ-2017)”. Международная научная конференция “Радиолокация. Спутниковая навигация. Радиомониторинг”. 24-26 октября 2017 г., Харьков, Украина : Точка, 2017. – С.107-11.

2. Kartashov,V.,Oleynikov,V.,Koryttsev,I.,Zubkov,O.,Babkin,S.,Sheiko,S. Processing and recognition of small unmanned vehicles’ sound signals // International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T). – Kharkiv, 2018. – P. 1-5.

3. Карташов В.М., Олейников В.Н., Шейко С.А., Бабкин С.И., Корытцев И.В., Зубков О.В., Анохин М.А. Информационные характеристики звуковых сигналов малых беспилотных летательных аппаратов // Радиотехника. – 2017. – Вып 191. – С. 181-187.

4. Kartashov V.M., Oleynikov V.N, Sheyko S.A., Babkin S.I., Koryttsev I.V., Zubkov O.V., Anokhin M.A. Information characteristics of sound radiation of small unmanned aerial vehicles // Telecommunications and Radio Engineering (English translation of Elektrosvyaz and Radiotekhika). – 2018. – **V**.77(10). – P. 915-924.

5. Журавлев В. Анализ информационных параметров и характеристик сигналов маскирования речи на объектах информационной деятельности // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2007. – Вип. 1 (14). – С. 170-176.

6. Останин С.А. Увеличение отношения сигнал шум методом последовательного вычисления автокорреляционной функции // Журнал радиоэлектроники. – 2011. – № 12. – С.17-26.

7. Заковряшин А.С., П.В. Малинин, Лепендин А.А. Применение распределений мел-частотных кепстральных коэффициентов для голосовой идентификации личности // Управление, вычислительная техника и информатика. – 2007. – №5. – С. 156-160.

8. A. Bernardini, F. Mangiatordi, E. Pallotti, L. Capodiferro; F. Ugo Bordoni. Drone detection by acoustic signature identification // Electronic Imaging, Imaging and Multimedia Analytics in a Web and Mobile World. – 2017. – P. 60-64.

Харьковский национальный
университет радиоэлектроники

Поступила в редколлегию 11.10.2018

.

УДК 004.413.7

І.Д. ГОРБЕНКО, д-р техн. наук, О.А. ЗАМУЛА, д-р техн. наук,
С.Г. ВДОВЕНКО, В.І. ЧЕРНИШ

МЕТОД ОЦІНКИ ЗРІЛОСТІ СИСТЕМИ УПРАВЛІННЯ БЕЗПЕКОЮ ПРИ ОРГАНІЗАЦІЇ ПОВІТРЯНОГО РУХУ

Вступ та постановка проблеми дослідження

Безпека на повітряному транспорті – це комплексна властивість авіаційної транспортної системи виконувати свої функції без нанесення шкоди самій системі або населенню. Питання забезпечення захисту інфраструктури системи організації повітряного руху (ОрПР) провайдера аеронавігаційного обслуговування (АНО) здійснюється шляхом забезпечення безпеки інформаційно-телекомунікаційних систем (ІТС), фізичної безпеки, кадрової безпеки та забезпечення безперервності надання послуг з АНО. Аеронавігаційне обслуговування – це обслуговування, яке здійснюється провайдерами АНО на всіх етапах польоту повітряних суден, що включає організацію повітряного руху, зв'язок, навігацію, спостереження (радіотехнічне забезпечення), пошук і рятування, метеорологічне обслуговування та надання аеронавігаційної інформації [1]. Провайдер АНО – це суб'єкт авіаційної діяльності, який надає послуги з елементів (напрямів) аеронавігаційного обслуговування повітряних суден [1]. Система організації повітряного руху (ОрПР) – це частина аеронавігаційної системи, яка складається з наземних та повітряних компонентів організації повітряного руху [1]. Система ОрПР включає також людські ресурси, процедури та обладнання (технічні засоби та програмне забезпечення), що використовуються для реалізації завдань з ОрПР, а також передбачає наявність систем зв’язку, навігації та спостереження (ЗНС).

Забезпечення інформаційної безпеки (ІБ) при ОрПР являє собою комплексну проблему, яка включає:

- правове регулювання застосування інформаційних технологій (ІТ);
- вдосконалення технологій розробки ІТ і захисту інформації в інформаційно-телекомунікаційних системах (ІТС);
- розвиток системи сертифікації; забезпечення відповідних організаційно-технічних умов експлуатації ІТС.

Недопущення авіаційних подій та інцидентів, пов'язаних з операційними діями при наданні послуг з аеронавігаційного обслуговування є бажаним результатом діяльності галузі та провайдерів АНО. Захист інфраструктури в частині, що стосується забезпечення ІБ провайдера АНО, необхідно для того, щоб в умовах виникнення загроз в розумній мірі забезпечувалась безпека при ОрПР. Забезпечення безпеки системи організації повітряного руху являє собою захист системи ОрПР провайдера АНО від загроз безпеки, захист вразливих місць, а також внесок системи ОрПР в забезпечення безпеки цивільної авіації, національної безпеки і оборони та охорони правопорядку [2].

1. Аналіз процесу забезпечення безпеки системи організації повітряного руху провайдера аеронавігаційного обслуговування

Інфраструктура системи ОрПР охоплює персонал, процедури, інформацію, ресурси, засоби і служби, у тому числі центри управління, аеропорти і обладнання, включаючи системи ЗНС та інформаційно-телекомунікаційні системи (ІТС). Захист інфраструктури системи ОрПР реалізується за допомогою забезпечення безпеки інформаційно-телекомунікаційних систем $InfSEC$, фізичної безпеки $PhSEC$ і безпеки персоналу $HrSEC$.

Забезпечення безпеки ІТС провайдера АНО передбачає застосування заходів захисту інформації та даних, які обробляються, зберігаються або передаються в ІТС, від випадкової або навмисної втрати цілісності, конфіденційності та доступності, а також захисту самих систем від

втрати цілісності або доступності. Заходи щодо забезпечення безпеки ІТС включають в себе захист:

- робочих місць персоналу провайдера АНО;
- автоматизованих систем керування повітряним рухом (АС КПР);
- систем передачі інформації і даних.

Відповідні заходи також передбачають ідентифікацію загроз інформаційної безпеки (ІБ) інфраструктури провайдера АНО, складання документальної бази стосовно протидії загрозам ІБ.

При розробці програми забезпечення безпеки ІТС провайдера АНО повинні застосовувати підхід до управління ризиком.

Фізична безпека $PhSEC$ – складовачастина діяльності з забезпечення безпеки системи ОрПР, що передбачає прийняття фізичних заходів для захисту персоналу, запобігання несанкціонованого доступу до обладнання, засобів, матеріалів і документів та забезпечення гарантій того, що система захисту не буде зруйнована. Фізична безпека передбачає вжиття заходів, покликаних виключити можливість доступу до будівель, ресурсів або інформації, що зберігається, з боку персоналу, який не має на те відповідного дозволу. Фізична безпека може забезпечуватися простим замиканням дверей або застосуванням складного багаторівневого підходу з використанням заходів стримування, виявлення і захисту. Заходи безпеки повинні застосовуватися таким чином, щоб при цьому забезпечувалася ефективність використання наявних ресурсів. Іншими словами, по відношенню до передбачуваних загроз заходи безпеки повинні бути економічно ефективними і відповідати ступеню критичності об'єктів.

Безпека персоналу $HrSEC$ є складовою частиною діяльності по забезпеченню безпеки системи ОрПР провайдера АНО, що передбачає використання процедур, які дозволяють оцінити можливість надання будь-якій особі, враховуючи при цьому його лояльність, ступінь довіри до нього і надійність, початкового та постійного доступу до конфіденційної інформації і доступу в контрольовані зони об’єктів провайдера АНО без створення неприйнятного ризику безпеки системи ОрПР.

2. Загальна модель управління ризиками безпеки інфраструктури системи організації повітряного руху

Повністю виключити ризик неможливо, тому управління ризиком безпеки при ОрПР провайдер АНО повинен здійснювати на основі підходу, що передбачає використання наявної інформації стосовно потенційного ризику .

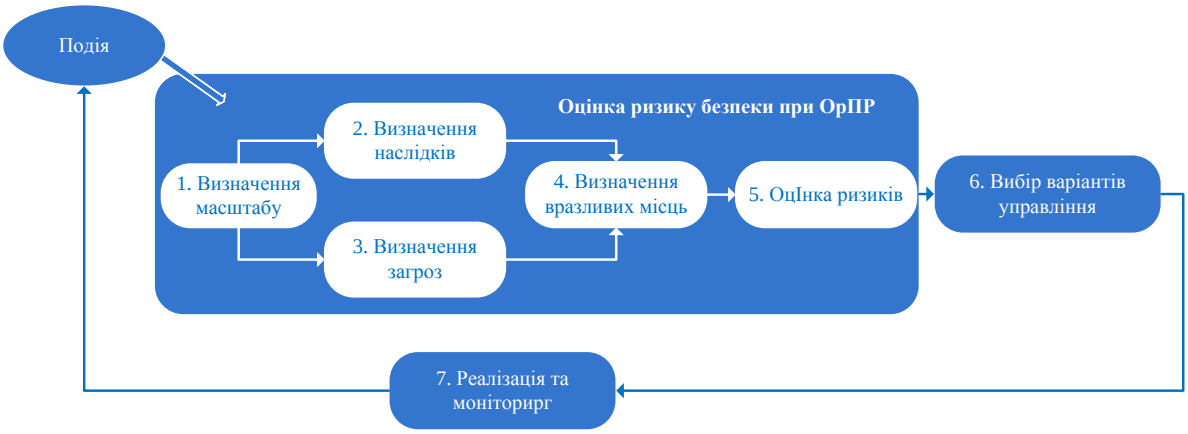
Процес управління ризиками $R(ATM)$ забезпечує можливість використання провайдером АНО структурованого підходу до прийняття обґрунтованих рішень щодо ризику безпеки персоналу $HrSEC$, фізичної безпеки $(PhSEC)$ та інформаційної безпеки (безпеки ІТС – $InfSEC$) і визначається правилом [2]:

$$R(ATM) = R\ (HrSEC), R\ (PhSEC), R\ (InfSEC). \quad (1)$$

Процес управління ризиком безпеки охоплює ряд взаємопов'язаних елементів і являє собою безперервно здійснювану діяльність циклічного характеру. Рисунок ілюструє цей процес, який може використовуватися провайдером АНО для систематичного виявлення ризику безпеки і визначення варіантів попередження наслідків [2].

Модель управління ризиком безпеки при ОрПР, що представлена в [2], має ряд недоліків, а саме:

- не враховує процеси управління фактором ризику для безпеки польотів;
- відсутність деталізації процедури управління ризиками, пов’язаними з безпекою персоналу $HrSEC$, інформаційною $InfSEC$ і фізичною безпекою $PhSEC$ відповідно;
- відсутність кількісної шкали оцінки визначення наслідків від реалізації загрози $T(ATM)$;
- відсутність кількісної шкали оцінки критичності активів провайдера АНО.



Процес управління ризиком безпеки при ОрПР

Одним із проблемних місць при розробці системи управління безпекою при ОрПР провайдером АНО є відсутність єдиного підходу до класифікації процесів управління безпекою ІТС. Для ефективного управління ризиком провайдер АНО визначає ініційовану подію, що забезпечить можливість постійного корегування процесу управління безпекою системи ОрПР (HrSEC, InfSEC, PhSEC). Оцінку ризику безпеки провайдер АНО може проводити на регулярній основі або у зв'язку зі зміною основних факторів, які здійснюють вплив на ступінь загрози системи ОрПР, при цьому характерними ініціюючими подіями є:

- зміна характеру загрози (типів загроз або частоти їх виникнення);
- інцидент, що пов'язаний з порушенням безпеки;
- зміна політики в сфері безпеки, яка може привести до зміни пріоритетів в сфері ризику або параметрів прийнятного ризику;
- впровадження змін у систему ОрПР.

3. Оцінка зрілості системи управління безпекою при ОрПР

Безпека в системі організації повітряного руху характеризується комплексом заходів протидії загрозам (у тому числі, загрозам інформаційної безпеки), які направлені на систему організації повітряного руху провайдера аеронавігаційного обслуговування. Такими загрозами можуть бути спроби атаки на активи провайдера АНО (органи обслуговування повітряного руху (ОПР), об’єкти радіотехнічного забезпечення (зв’язку, навігації, спостереження), персонал, тощо).

Основним напрямом забезпечення безпеки при ОрПР є захист інфраструктури провайдера АНО. Одним з найактуальніших на сьогодні питань в рамках забезпечення безпеки при ОрПР є оцінка ефективності системи управління безпекою при ОрПР, що розроблюється провайдером АНО. Управління безпекою при ОрПР, що включає захист інфраструктури системи ОрПР, спрямовано на підвищення якості управління провайдера АНО взагалі, тому показники ефективності їх формування та використання мають бути інтегрованими в систему управління провайдера АНО на всіх рівнях прийняття рішень, що викликає необхідність розробки методів оцінки ефективності [2].

На теперішній час відсутність кількісної оцінки щодо зрілості процесів забезпечення безпеки інфраструктури ускладнює створення відповідної системи управління провайдерами АНО.

Рівні зрілості бізнес-процесу –це розвиток провайдера АНО відповідно до стандартизованих моделей оцінки рівня зрілості управління, що визначаються різними характеристиками, такими як місія, стратегія, організаційна структура, безпека польотів, безпека при ОрПР та ін. Переходи з рівня на рівень роблять провайдера АНО більш конкурентоспроможним, підвищують рівень безпеки польотів та експлуатаційну ефективність системи ОрПР.

Більшість підприємств застосовують універсальну модель оцінки рівня зрілості управління – Capability Maturity Model Integration (CMMI) [3]. Набір моделей (методологій) дозволяє вдосконалити бізнес-процеси в організаціях різних розмірів і видів діяльності та може використову-

ватись для покращення процесу як на рівні проекту чи відділу, так і на рівні цілої організації. CMMI дозволяє інтегрувати традиційно відокремлені організаційні функції, ставити цілі та пріоритети покращення процесів, забезпечує інструкцією по створенню якісних процесів і дає контрольну точку для оцінки поточних процесів [CMMI]. Відповідно до [3 – 5] існує 5 рівнів зрілості, кожен з яких вказує на зрілість (з точки зору управління процесами безпеки) організації.

У сфері інформаційних технологій рівень зрілості визначається за допомогою моделі зрілості можливостей (модель повноти потенціалу) створення програмного забезпечення (ПЗ) – Capability Maturity Model (CMM) та ДСТУ ISO / IEC 15504 [4].

Вищезазначені методології не описують процедуру оцінки зрілості безпеки при ОрПР. Для визначення кількісного показника рівня розвитку системи управління безпекою при ОрПР провайдера АНО авторами розроблена та запропонована шкала еволюції, що заснована на п'яти загальних рівнях зрілості від A до E:

Ідентифікатор рівня	Якісний показник	Кількісний показник	Відповідність встановленим вимогам, %
A	Відсутній	0	(0 – 20]
B	Початковий	1	(20 – 40]
C	Середній	2	(40 – 60]
D	Високий	3	(60 – 80]
E	Оптимізований	4	(80 – 100]

Показником, що характеризує організаційну ефективність процесу забезпечення безпеки при ОрПР, формування і використання заходів з безпеки інфраструктури системи ОрПРв умовах стратегічного управління, є загальний рівень зрілості системи управління безпекою при ОрПР, який визначається на основі часткових рівнів зрілості для напрямків:

- безпека персоналу $HrSEC$;
- безпеку інформаційно-телекомунікаційних систем $InfSEC$;
- фізичної безпеки $PhSEC$;
- підтримки національних інтересів S, з ваговим коефіцієнтом часткового рівня 0,25 (або 25 %) та визначається виразом

$$M(SAS) = \left((M(HrSEC) \cdot 0{,}25) + (M(InfSEC) \cdot 0{,}25) + (M(PhSEC) \cdot 0{,}25) + (M(S) \cdot 0{,}25)\right) \cdot 100\%. \quad (2)$$

Відповідний підхід дозволяє охарактеризувати основні процеси забезпечення безпеки об'єктів АНО, зв'язку, навігації, спостереження (ЗНС) та інших структурних підрозділів провайдера АНО. Оцінка зрілості безпеки при ОрПР є основною складовою такого бізнес-процесу підприємства як якість надання послуг з АНО користувачам повітряного простору.

Авторами запропоновано при визначенні часткових рівнів зрілості системи безпеки при ОрПР використовувати опитувальник, у якому аудитор визначає відповідність провайдера АНО встановленим вимогам за напрямками $HrSEC, InfSEC, PhSEC, S$.

Частковий показник рівня зрілості за кожним запитанням відповідного напрямку опитувальника може бути обчислено відповідно до виразу

$$R\ (Q_i) = A_i\ \cdot W_i, \quad (3)$$

де: Q_i – і – та вимога відповідного напрямку; A_i – виконання Q_i-ї вимоги відповідного напрямку (кількісний показник знаходиться у діапазоні $0 < A_i \leq 2$), де 0 – вимога не виконується; 1 – вимога виконується частково; 2 – вимога виконується у повному обсязі; W_i – ваговий коефіцієнт Q_i-ї вимоги (встановлюється аудитором при розробленні листу відповідності, кількісний показник знаходиться у діапазоні $0 < Q_i \leq 4$).

Часткові показники для напрямків можуть бути розраховані відповідно до виразів:

$$RM(InfSEC) = \frac{R_{cur}(Q_1(InfSEC)) + R_{cur}(Q_i(InfSEC))}{R_{max}(Q_1(InfSEC)) + R_{max}(Q_i(InfSEC))} \cdot 100\%, \quad (4)$$

де $R_{cur}(Q_1(InfSEC)) + R_{cur}(Q_i(InfSEC))$ – підсумкова сума відповідей з урахуванням вагового коефіцієнту W_i для напрямку «безпека ІТС» (інформаційна безпека); $R_{max}(Q_1(InfSEC)) + R_{max}(Q_i(InfSEC))$ – підсумкова сума максимального значення відповідей (виконання вимог) з урахуванням вагового коефіцієнту W_i для напрямку «безпека ІТС» (інформаційна безпека);

$$RM(HrSEC) = \frac{R_{cur}(Q_1(HrSEC)) + R_{cur}(Q_i(HrSEC))}{R_{max}(Q_1(HrSEC)) + R_{max}(Q_i(HrSEC))} \cdot 100\% \quad , \quad (5)$$

де $R_{cur}(Q_1(HrSEC)) + R_{cur}(Q_i(HrSEC))$ – підсумкова сума відповідей з урахуванням вагового коефіцієнту W_i для напрямку безпека персоналу; $R_{max}(Q_1(HrSEC)) + R_{max}(Q_i(HrSEC))$ – підсумкова сума максимального значення відповідей (виконання вимог) з урахуванням вагового коефіцієнту W_i для напрямку безпека персоналу;

$$RM(PhSEC) = \frac{R_{cur}(Q_1(PhSEC)) + R_{cur}(Q_i(PhSEC))}{R_{max}(Q_1(PhSEC)) + R_{max}(Q_i(PhSEC))} \cdot 100\% \quad , \quad (6)$$

де $R_{cur}(Q_1(PhSEC)) + R_{cur}(Q_i(PhSEC))$ – підсумкова сума відповідей з урахуванням вагового коефіцієнту W_i для напрямку фізична безпека; $R_{max}(Q_1(PhSEC)) + R_{max}(Q_i(PhSEC))$ – підсумкова сума максимального значення відповідей (виконання вимог) з урахуванням вагового коефіцієнту W_i для напрямку фізична безпека;

$$RM(S) = \frac{R_{cur}(Q_1(S)) + R_{cur}(Q_i(S))}{R_{max}(Q_1(S)) + R_{max}(Q_i(S))} \cdot 100\% \quad , \quad (7)$$

де $R_{cur}(Q_1(S)) + R_{cur}(Q_i(S))$ – підсумкова сума відповідей з урахуванням вагового коефіцієнту W_i для напрямку підтримка національних інтересів; $R_{max}(Q_1(S)) + R_{max}(Q_i(S))$ – підсумкова сума максимального значення відповідей (виконання вимог) з урахуванням вагового коефіцієнту W_i для напрямку підтримка національних інтересів.

Висновки

Провайдери АНО повинні забезпечити облік заходів безпеки при проектуванні, впровадженні та експлуатації нових ІТС. Крім того, провайдери АНО повинні визначити програмні і апаратні засоби ІТС як елементи інфраструктури системи ОрПР які, зокрема, можуть включати в себе:

- ресурси і компоненти системи ОрПР;
- контролюючі системи диспетчеризації, які мають відношення до забезпечення безпеки;
- системи контролю доступу та охоронної сигналізації органів обслуговування повітряного руху;
- системи спостереження;
- електронні пристрої, що використовуються для обробки, зберігання і передачі критично важливої інформації провайдера АНО.

Захист критичних ІТС провайдера АНО повинен передбачати процедури оцінки ризику. Це може досягатися шляхом охоплення критичних елементів інфраструктури системи ОрПР, оцінками ймовірності загроз (атак), вразливостей і впливу або наслідків відмови ІТС.

Провайдери АНО повинні розробляти заходи зниження ризику потенційних атак на інфраструктури системи ОрПР і перевіряти реалізацію цих заходів, використовуючи механізм регулярного контролю за виконанням вимог, наприклад шляхом проведення аудитів та інспекторських перевірок.

Авторами вперше запропоновано метод оцінки зрілості системи управління безпекою при організації повітряного руху провайдера аеронавігаційного обслуговування. Зазначений метод дозволяє визначити фактичний та прогнозований рівні відповідності системи управління безпекою при організації повітряного руху чинним вимогам нормативно-правових актів, міжнародних стандартів та з урахуванням вагових коефіцієнтів.

Список літератури:

1.Повітряний кодекс України від 19.05. 2011. – № 3393-VI.

2. Керівництво з безпеки системи організації повітряного руху, DOC ICAO 9985.

3. Денис М. Ахен, Арон Клауз, Ричард Тернер CMMI: Комплексный подход к совершенствованию процессов. Практическое введение в модель. – Москва : МФК, 2005. – 300 с.

4. ДСТУ ISO/IEC TR 15504-4:2002 Інформаційні технології. Оцінювання процесів життєвого циклу програмних засобів. Ч. 4. Настанови з виконання оцінювання (ISO/IEC TR 15504-4:1998, IDT).

5. Проверка и оценка деятельности по управлению информационной безопасностью : учеб. пособие для вузов / П.Г. Милославская, М.Ю. Сенаторов, А Н. Толстой. – Москва : Горячая Линия-Телеком, 2014. – 166 с.

Харківський національний
університет імені В.Н. Каразіна

Надійшла до редколегії 05.10.2018

УДК 004.056.5

А.А. КУЗНЕЦОВ, д-р техн. наук, Р.В. СЕРГИЕНКО, канд. техн. наук, А.А. УВАРОВА

НЕЧЕТКИЙ ЭКСТРАКТОР НА ПОМЕХОУСТОЙЧИВЫХ КОДАХ ДЛЯ БИОМЕТРИЧЕСКОЙ КРИПТОГРАФИИ

Введение

Важным направлением современных исследований в области киберзащиты являются биометрические методы аутентификации личности [1 – 12]. Они широко используются в различных приложениях: криминалистике, электронной коммерции, защите авторского права, электронном документообороте и пр.

В последние годы интерес к биометрическим методам значительно расширился. От традиционных биометрических систем, основанных на сравнении полученных биометрических образов с хранимыми эталонными копиями, современные технологии перешли к формированию криптографических ключей «на лету». В этом случае биометрические данные уже не нуждаются в хранении, передаче, сложных и дорогостоящих средствах защиты и т.д., исключается возможность их преднамеренной и/или случайной компрометации. Все процедуры верификации, идентификации и аутентификации выполняются по деперсонализированным криптографическим ключам (паролям, кодам доступа, пин-кодам), а уникальные биометрические персональные данные личности остаются в безопасности. Формируемые деперсонализированные ключевые последовательности будем называть в дальнейшем биометрическими ключами.

Следующим этапом в развитии подобных технологий будет построение полноценных биометрических криптографических систем, в которых биометрические данные личности должны использоваться как источник уникальных секретных параметров. При этом пользователю не нужно будет запоминать криптографические ключи (пароли) и/или использовать дополнительные устройства их хранения, передачи и пр. Биометрическая криптосистема в любое время и в любом месте инициализируется посредством извлечения «на лету» нужных параметров из предоставленных биометрических образов (с возможными ошибками, стираниями и пр.) без компрометации этих образов. При этом необходимо обеспечить максимальный набор услуг и гарантий безопасности, учитывающих особенности построения биометрических криптосистем.

В данной работе рассматриваются методы формирования криптографических ключей из биометрических образов[1] с использованием нечетких экстракторов [3, 4].

Традиционно нечеткие экстракторы, как и предшествовавшие им нечеткие контейнеры [2], строятся с использованием методов помехоустойчивого кодирования. На начальном этапе биометрические данные в некотором смысле «объединяются» с элементами помехоустойчивых кодов (например, с кодовыми словами или синдромными последовательностями). Для нечетких экстракторов дополнительно формируется открытая вспомогательная строка (helper string), которая «помогает» в извлечении секретного параметра по нечетко заданной биометрии. На этапе непосредственного использования применяется помехоустойчивое декодирование, которое устраняет возможную неопределенность (вызванную искажениями, стираниями и пр.) в предоставленных пользователем биометрических образах. Если различия в наборах характеристик невелики (не превышают исправляющей способности кодов), тогда нечеткие экстракторы (хранилища) позволяют однозначно восстановить секретный параметр (биометрический ключ).

[1] Под биометрическими образами (данными) здесь и далее понимаются наборы биометрических характеристик, представимых в виде бинарных векторов, которые можно сравнивать в метрике Хемминга. Предполагается, что различные наборы характеристик одного и того же пользователя отличаются друг от друга не более, чем на 25 % (этот порог соответствует предельным корректирующим возможностям помехоустойчивых кодов).

В данной работе предлагается новая схема нечеткого экстрактора, в основе которой лежит кодовая криптосистема Мак-Элиса [13]. Показано, что новая конструкция позволяет формировать криптографические пароли из биометрических образов даже без использования несекретных helper string. При использовании helper string значительно возрастает доля корректируемых искажений биометрических образов. Кроме того, предлагаемая конструкция относится к классу постквантовых методов защиты информации, т.е. ожидается ее безопасное использование даже в условиях применения универсальных квантовых компьютеров для решения задач криптографического анализа.

Нечеткие хранилища и нечеткие экстракторы

В [1] рассмотрено формирование секретного ключа с использованием биометрии, упрощенная схема которого приведена на рис. 1.

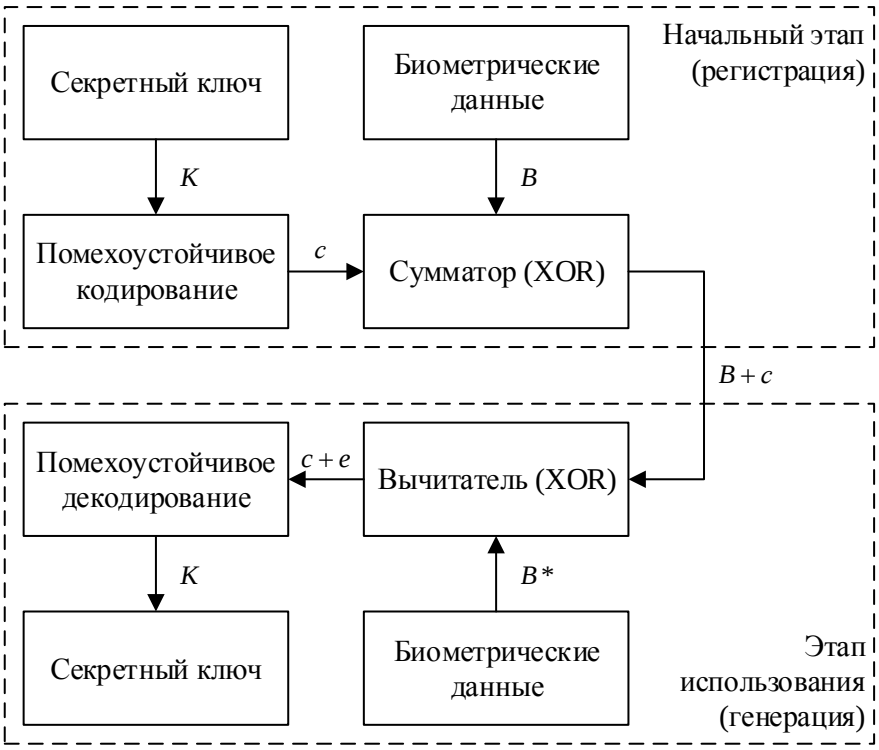


Рис. 1. Схема формирования биометрического ключа

На начальном этапе формируется секретный параметр (ключ) K, который кодируется помехоустойчивым кодом. К полученному кодовому слову c прибавляются биометрические данные пользователя B. Полученный «носитель» $B+c$ фактически является зашумленным биометрией секретным ключом. Если на этапе использования будут предоставлены биометрические данные B^*, близкие к исходным $B^* \approx B$, тогда, после их вычитания, декодирование позволит восстановить секретный ключ. Действительно, после вычитания получим:

$$(B+c)-B^*=c+e,$$

где $e=B-B^*$ интерпретируется как вектор ошибок.

Если вес Хемминга вектора e (число ненулевых его компонент) не превышает исправляющей способности помехоустойчивого кода t, тогда декодирование вектора $(B+c)-B^*$ позволит найти вектор c, вектор e и, как следствие, ключевой параметр K.

Очевидно, что криптографические свойства схемы [1] зависят как от выбранного помехоустойчивого кода, так и от способа формирования биометрических данных. Секретный параметр K в закодированном виде содержится в «носителе» $B+c$ и, очевидно, возможны статистические атаки, восстанавливающие кодовое слово c и секретный ключ K.

Схема нечеткого хранилища впервые предложена в работе [2]. В ее основе также лежит использование помехоустойчивых кодов. Секретный параметр «прячется» в закодированном наборе данных, предоставленных пользователем. Любой пользователь сможет извлечь секретный параметр только если его набор будет близок к исходному набору, а небольшие различия будут исправлены в процессе помехоустойчивого декодирования. Статистический анализ нечеткого хранилища вероятно может привести к возможной атаке на хранящийся секретный ключ.

Дальнейшее развитие технологии биометрических ключей получило в работах [3 – 12] и др. В частности, в основополагающих работах [3, 4] предложены так называемые нечеткие экстракторы, конструкции которых очень близки к схемам формирования ключей из [1]. Основными являются две конструкции [3, 4]:

- на основе кодовых слов (рис. 2);
- на основе синдромов (рис. 3).

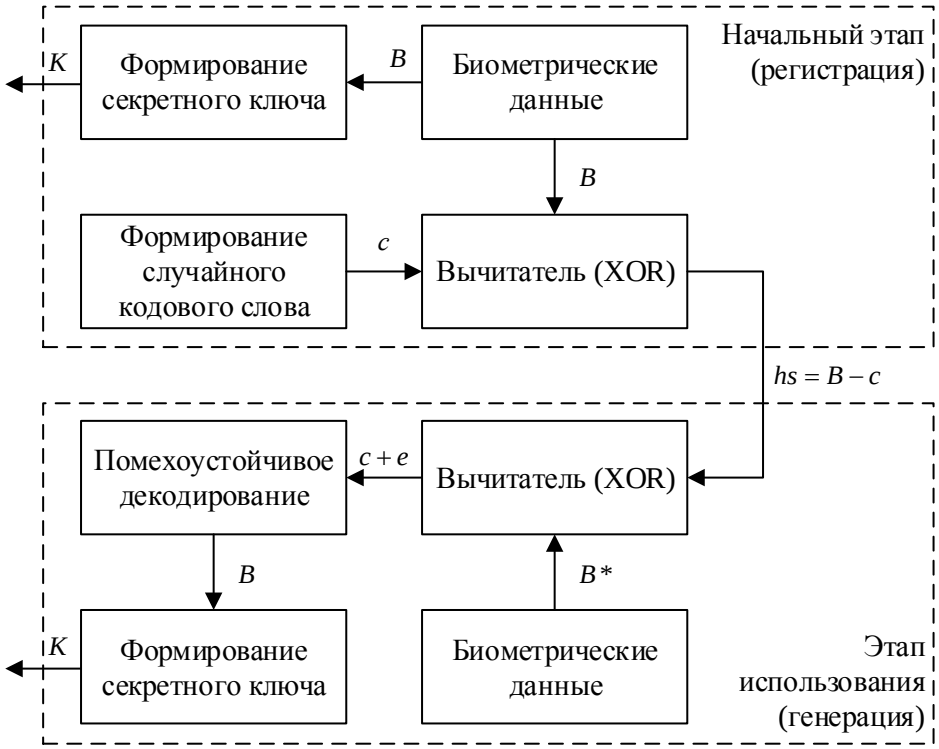


Рис. 2. Схема нечеткого экстрактора на основе кодовоых слов

Пусть задан помехоустойчивых блоковый $(n, k, d = 2t+1)$ код с исправляющей способностью t ошибок. Предполагается, что наличие биометрических данных B позволяет сформировать секретный ключ K и некоторую helper string hs (для этого используются различные приемы и техники, например Secure Sketches [3, 4]).

В первой конструкции (на основе кодовых слов, см. рис. 2) на начальном этапе (регистрации биометрического ключа) формируется случайное кодовое слово c. Открытая вспомогательная строка hs формируется посредством вычитания из биометрических данных B слова c:

$$hs = B - c,$$

причем по этой открытой строке в последствии можно восстановить секретный ключ K.

Действительно, на этапе использования пользователь предоставляет биометрические данные B^*, из которых отнимается подсказка hs. Если $B^* \approx B$ тогда имеем

$$B^* - hs = B^* - (B - c) = c + e,$$

где $e = B^* - B$, и если вес Хемминга вектора e не превышает t, тогда декодирование вектора $B^* - hs$ позволит найти вектор c, вектор e и, как следствие, биометрические данные B:

$$B = c + hs.$$

Правильное восстановление биометрических данных B позволяет сформировать секретный ключ K (как и на этапе регистрации).

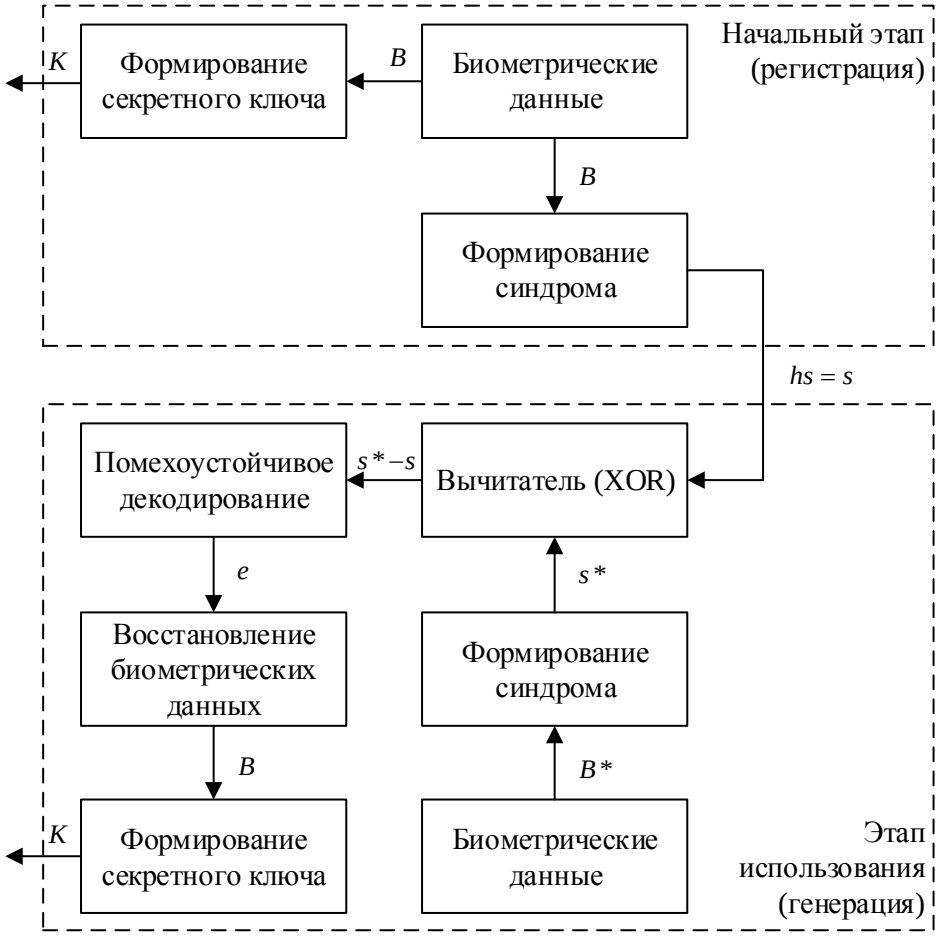


Рис. 3. Схема нечеткого экстрактора на основе синдромов

Вторая схема (см. рис. 3) оперирует синдромными последовательностями s, которые зависят исключительно от вектора ошибок e. Например, для линейных блоковых кодов, заданных проверочной матрицей H, для любого кодового слова c справедливы равенства [14, 15]:

$$c \cdot H^T = 0,\ s = (c + e) \cdot H^T = e \cdot H^T.$$

На начальном этапе с использованием B формируется синдромная последовательность s, которая выступает в качестве открытых вспомогательных данных. На этапе использования пользователь предъявляет биометрические данные B^*, по которым вычисляется синдромная последовательность s^*. Если $B^* \approx B$, тогда наличие подсказки $hs = s$ и синдрома s^* позволяет восстановить B и сформировать секретный ключ K.

Действительно, если, например, $s = B \cdot H^T$ и $s^* = B^* \cdot H^T$, тогда

$$s^* - s = e \cdot H^T,$$

где $e = B^* - B$, и если вес Хемминга вектора e не превышает t, тогда синдромное декодирование вектора $s^* - s$ позволит найти вектор e.

Правильное восстановление биометрических данных $B = B^* - e$ позволяет сформировать секретный ключ K (как и на этапе регистрации).

Очевидно, что схемы на рис. 1 и 2 для двоичного случая (сложение и вычитание реализуются операцией XOR) практически совпадают. Основное отличие состоит в том, что на рис. 1 секретный ключ формируется случайным образом, а затем кодируется помехоустойчивым кодом. На рис. 2 секретный ключ формируется из биометрических данных B, которые однозначно должны быть восстановлены в случае представления пользователем данных $B^* \approx B$. Однако в обеих схемах используется общий подход, состоящий в «подмешивании» биометрических данных B к кодовому слову c (случайно сформированному или как закодированному ключу K). Это, на наш взгляд, несет основную угрозу использования подобных биометрических ключей. Если в открытом виде передаются, хранятся и/или обрабатываются биометрические данные (даже с подмешанными к ним кодовыми словами, синдромами и пр.), следует ожидать статистических атак, направленных на восстановление кодовых слов c, биометрических данных B и ключей K.

В данной работе предлагается новая схема нечеткого экстрактора, в которой биометрические данные не хранятся и не передаются ни в каком виде. Наша схема использует кодовую криптосистему Мак-Элиса в интерпретации Code-Based Electronic Digital Signature из работы [16].

Предлагаемая схема нечеткого экстрактора

В основе нашего предложения лежит использование кодовой криптосистемы Мак-Элиса [13].

А. Кодовая криптосистема Мак-Элиса

Кодовая криптосистема Мак-Элиса предложена в 1978 году [13] и за 40 лет существования не обнаружила существенных уязвимостей. В случае использования кодов Гоппы [17] с достаточной длиной и кодовым расстоянием считается надежным кандидатом на постквантовое применение, т.е. предполагается ее безопасное использование даже при использовании полномасштабных универсальных квантовых компьютеров для решения задач криптографического анализа [18, 19].

Открытым ключом в схеме Мак-Элиса является матрица

$$G_X = X \cdot G \cdot P \cdot D, \tag{1}$$

где G – порождающая матрица алгебраического $(n, k, d = 2t+1)$ кода над $GF(q)$ (в оригинальной статье [13] предлагалось использовать двоичный код Гоппы [17]), 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 в (1) 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

$$c_X^* = I \cdot G_X + e, \tag{2}$$

где вектор

$$c_X = I \cdot G_X$$

является кодовым словом замаскированного кода, т.е. c_X принадлежит $(n,k,d=2t+1)$ коду с порождающей матрицей G_X, I – k-разрядный информационный вектор над $GF(q)$, вектор e – секретный вектор ошибок веса t.

Злоумышленнику необходимо декодировать c_X^*, используя известную ему порождающую матрицу G_X. Однако декодирование случайного кода (при соответствующих параметрах n,k,q и $d=2t+1$) вычислительно недостижимо. Не зная матрицы X, P и D злоумышленник не может восстановить матрицу G и воспользоваться алгоритмом декодирования полиномиальной сложности. Для уполномоченного пользователя (знающего секретный ключ) декодирование – полиномиально разрешимая задача. Действительно, легитимный пользователь, получив вектор c_X^*, строит вектор

$$\bar{c}^* = c_X^* \cdot D^{-1} \cdot P^{-1}. \quad (3)$$

Далее, используя алгоритм полиномиальной сложности, он декодирует вектор $\bar{c}^* = I' \cdot G + e'$, т.е. находит I'. Затем вычисляет k-разрядный информационный вектор

$$I = I' X^{-1}. \quad (4)$$

Дополнительным секретным параметром, который можно использовать в случае применения кодов Гоппы, является многочлен Гоппы $G(x)$ [13].

В. Новая схема нечеткого экстрактора на помехоустойчивых кодах

Предлагаемая схема нечеткого экстрактора позволяет формировать криптографические ключи даже без использования несекретных helper string. При использовании helper string значительно возрастает доля корректируемых искажений биометрических образов.

Упрощенная схема предлагаемого нечеткого экстрактора приведена на рис. 4.

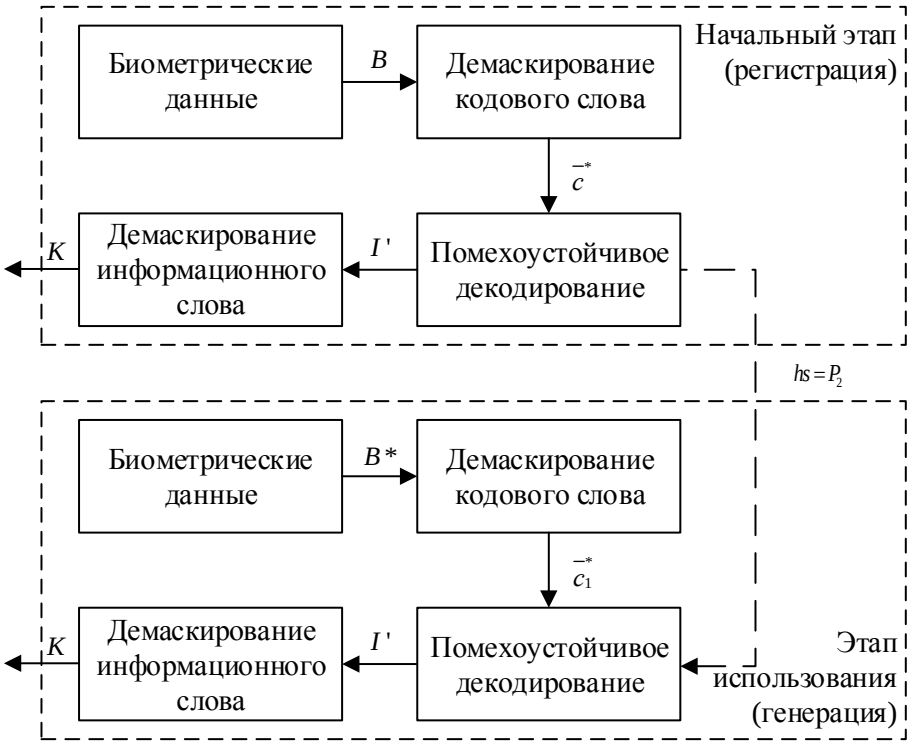


Рис. 4. Предлагаемая схема нечеткого экстрактора (прерывистая линия соответствует возможному использованию helper string)

На начальном этапе биометрические данные[2] B интерпретируются как кодовое слово (2) замаскированного кода в криптосистеме Мак-Элиса. В соответствии с (3) производится его демаскирование, полученный вектор $\overline{c}^*$ декодируется. Из декодированного кодового слова извлекается вектор I', который также демаскируется в соответствии с (4). Полученная информационная последовательность I интерпретируется как секретный биометрический ключ K. В простейшем случае $K = I$, хотя возможна и более сложная конструкция генерации K из I, например посредством однонаправленного хеширования: $K = h(I \| i)$, где $x \| y$ – операция конкатенации (присоединения) строк x и y; i – дополнительные (служебные) данные, которые используются для вычисления секретного ключа.

На этапе использования пользователь предъявляет биометрические данные B^*, которые, как и на этапе регистрации, интерпретируются как кодовое слово (2) замаскированного кода в криптосистеме Мак-Элиса. В соответствии с (3) производится его демаскирование, полученный вектор (обозначим его $\overline{c}_1^*$) декодируется. Если $B^* \approx B$ и, в нашей интерпретации,

$$B = I \cdot G_X + e \quad \text{и} \quad B^* = I \cdot G_X + e^*, \tag{5}$$

где e и e^* – два различных вектора с весом Хемминга меньше t, тогда декодирование векторов

$$\overline{c}^* = (I \cdot G_X + e) \cdot D^{-1} \cdot P^{-1} = I' \cdot G + e \cdot D^{-1} \cdot P^{-1}$$

и

$$\overline{c}_1^* = (I \cdot G_X + e^*) \cdot D^{-1} \cdot P^{-1} = I' \cdot G + e^* \cdot D^{-1} \cdot P^{-1}$$

позволит восстановить один и тот же вектор I'.

После демаскировании вектора I' по правилу (4) формируется секретный ключ K (как и на этапе регистрации).

В основе нашего метода лежит предположение (5), которое по сути сводится к наличию у всех биометрических характеристик, принадлежащих одному и тому же пользователю, некоторой общей информации (энтропии), которую условно можно задать вектором I. Эта информация в закодированном виде искажается в процессе обработки биометрических образов (использование различных биометрических датчиков, влияние помех, стираний и пр.). Если предположить, что биометрические образы искажаются ошибками, вес Хемминга которых не превосходит исправляющей способности t, тогда во всех случаях использования секретный ключ будет восстановлен верно. Для снижения влияния случайных ошибок на этапе регистрации следует сформировать наиболее достоверный набор биометрических характеристик, например посредством многократного формирования с усреднением полученного результата.

Эффективность использования предлагаемого нечеткого экстрактора, как и других рассмотренных выше методов, зависит от характеристик используемого помехоустойчивого кода. Фактически False Rejection Rate (FRR) определяется вероятностью ошибочного декодирования (для случая $B^* \approx B$). Однако наше предположение (5) выглядит более естественным, в предлагаемом экстракторе исправляются различные искажения одного и того же кодового слова, содержащего биометрическую энтропию. В схемах [1, 3, 4] исправляются различия биометрических образов одного и того же пользователя, т.е. основное предположение, лежащее в основе этих конструкций, имеет вид $|B - B^*| = e$, где вес Хемминга вектора e

[2] Предполагается, что на этапе регистрации формируется наиболее достоверный набор биометрических характеристик, представленных в виде бинарных векторов

должен быть меньше t. Если учесть возможность разнонаправленного искажения биометрических образов $B-B^*$, тогда наш экстрактор интуитивно представляется более надежным.

Следует отметить, что в схеме на рис. 4 может вовсе не использоваться helper string, т.е. наш экстрактор может работать «вслепую». Из каждого предоставленного биометрического образа будут извлечены ключевые данные и, при выполнении (5), восстановленные ключи будут совпадать.

Тем не менее дополнительное использование helper string существенно снижает FRR.

Запишем матрицу G в виде «объединения» двух подматриц – квадратной матрицы G_1 размерности $k \times k$ и прямоугольной матрицы G_2 размерности $k \times (n-k)$:

$$G = G_1 \| G_2 . \tag{6}$$

Тогда слово $\bar{c} = I' \cdot G$ можем записать в виде

$$\bar{c} = P_1 \| P_2 , \text{ где } P_1 = I' \cdot G_1 , \; P_2 = I' \cdot G_2 .$$

Используя последние тождества найдем:

$$P_2 = P_1 \cdot G_1^{-1} \cdot G_2 , \tag{7}$$

где матрица G_1^{-1} является обратной[3] к матрице G_1.

На рис. 4 прерывистая линия соответствует возможному использованию P_2 в качестве helper string (на этапе использования при декодировании $\bar{c}_1^*$). Это позволяет значительно снизить действие ошибок и повысить, таким образом, вероятность правильного восстановления вектора I' и секретного ключа K (т.е. снизить FRR). Действительно, если ошибки (ненулевые элементы вектора e) распределены равномерно по всему слову $\bar{c}^* = I' \cdot G + e'$, тогда, имея неискаженную часть P_2 кодового слова $I' \cdot G$, можно «проигнорировать» все ошибки, приходящиеся на «вторую» часть слова. Это эквивалентно повышению исправляющей способности кода соответственно длине вектора P_2. Поясним это следующими рассуждениями.

Пусть ошибки (ненулевые элементы вектора e) происходят случайно, равновероятно и независимо друг от друга. Обозначим символом p – вероятность искажения одного символа кодового слова. Тогда вероятность искажения m символов кодового слова длины n:

$$P(m) = C_n^m p^m (1-p)^{n-m},$$

где $C_n^m = \dfrac{n!}{m!(n-m)!}$ – биномиальный коэффициент.

Вероятность ошибки декодирования (соответствует FRR в нашей модели без применения helper string) при использовании $(n, k, d = 2t+1)$ кода запишется в виде

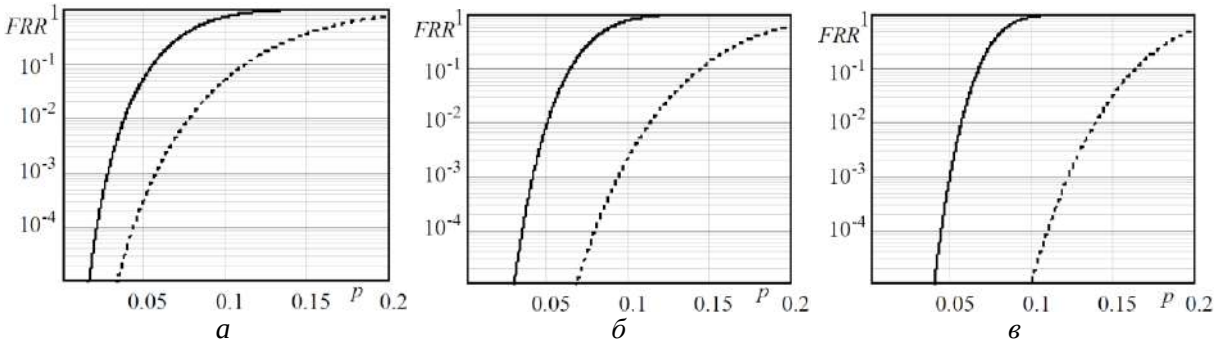
$$FRR = 1 - \sum_{i=0}^{t} P(i) = 1 - \sum_{i=0}^{t} C_n^i p^i (1-p)^{n-i} . \tag{8}$$

При использовании helper string ошибки нужно исправить только на позициях вектора P_1, и вероятность ошибки декодирования (при аналогичных рассуждениях) примет вид

[3] Для обратимости матрицы G_1 необходимо правильно реализовать представление (6): это не «объединение» первых (любых) k столбцов матрицы G, а псевдослучайный выбор таких k столбцов из G, которые образуют невырожденную квадратную матрицу G_1.

$$FRR^* = 1 - \sum_{i=0}^{t} C_k^i p^i (1-p)^{k-i} . \quad (9)$$

На рис. 5 приведены расчетные зависимости FRR для некоторых (*n, k, d*) параметров двоичных кодов БЧХ: *а* – (127, 64, 21); *б* – (255, 115, 43); *в* – (512, 211, 83).



а *б* *в*

Рис. 5. Расчетные зависимости FRR (сплошная линия – без helper string; прерывистая линия – с helper string)

Как следует из приведенных зависимостей, при выборе соответствующих (*n, k, d*) параметров FRR может быть очень низкой. Например, при формировании 64-битного ключа с использованием двоичного (127, 64, 21)-кода и $p = 0,05$ значение FRR для экстрактора без helper string не превосходит 10^{-1}. Использование helper string снижает FRR на два порядка. Увеличение длины и исправляющей способности кода приводит к снижению FRR. Например, для (512, 211, 83)-кода с даже для $p = 0,15$ использование helper string позволяет сформировать 211 битный ключ с FAR не более 10^{-1}.

Следует отметить, что другая важная характеристика биометрических паролей False Acceptance Rate (FAR), характеризующая вероятность ошибочного формирования секретного ключа неуполномоченным пользователем, возрастает при увеличении исправляющей способности t кода. При значительном увеличении t (за счет увеличения избыточности P_2) экстрактор сможет извлекать один и тот же ключ для любых предоставленных биометрических данных, т.е. для $B^* \neq B$. Например, если использовать двоичный код с параметрами (511, 112, 239) с 399-битной подсказкой $hs = P_2$, тогда даже при искажении всех 112 бит вектора P_1, экстрактор их исправит ($t = 119$) и однозначно восстановит вектор I и секретный ключ K. Другими словами, любой пользователь, предоставивший произвольный набор B^*, сможет правильно восстановить ключ K. С этой точки зрения при выборе (*n, k, d*) параметров кода следует выбирать компромиссное решение между ожидаемыми значениями FRR и FAR. Если предположить, что $k < \frac{n}{2}$ и все пользователи обладают равноудаленными друг от друга биометрическими данными, тогда FAR (при использовании helper string) можно условно оценить следующим выражением:

$$FAR^* = \begin{cases} q^{-k+t}, & k > t; \\ 1, & k \le t, \end{cases} \quad (10)$$

где q – мощность алфавита символов, над которым построен помехоустойчивых код (для двоичного кода $q = 2$).

Действительно, в предложенном экстракторе в качестве секретного ключа K используется вектор I (или функция от этого вектора) длины k кодовых символов. При равноудаленных кодовых словах (биометрических образах) и равновероятном их выборе вероятность

совпадения ключей для разных пользователей равна q^{-k}. Нечеткий экстрактор основан на помехоустойчивом декодировании и, в случае использования helper string, все t ошибок могут быть исправлены на блоке P_1 длиной k кодовых символов, т.е., если $k > t$ вероятность совпадения секретных ключей для различных равновероятно выбранных биометрических образов будет равна q^{-k+t}. Для $k \le t$ исправляющая способность кода позволяет полностью подобрать нужный вектор для любого биометрического набора, т.е. «пропуск цели» является достоверным событием. Если helper string не используется, тогда на каждые k кодовых символов приходится в среднем $\frac{t}{n}$ исправляемых ошибок и FAR можно оценить как $q^{-k+\frac{t}{n}k}$.

В заключение отметим, что все приведенные рассуждения, соотношения и расчетные значения приведены для «идеальных» условий, когда наборы биометрических характеристик формируются в виде бинарных векторов со случайными, равновероятными (при $p < 0,5$) и независимыми ошибками. В реальных условиях характер ошибок может значительно отличаться. Необходимо проводить дальнейшие исследования, в том числе экспериментального характера для обоснования практических рекомендаций по непосредственному использованию предложенного нечеткого экстрактора.

Выводы

Предложен нечеткий экстрактор, основанный на кодовой криптосистеме Мак-Элиса. Наше предложение, с одной стороны, использует сильные стороны кодовой криптосистемы: криптографическую стойкость, основанную на проблеме синдромного декодирования; устойчивость к квантовым методам криптоанализа; относительно высокую скорость преобразования (по сравнению с другими криптосистемами с открытым ключом). С другой стороны, наш экстрактор посредством подбора нужных (*n, k, d*) параметров помехоустойчивого кода позволяет обеспечить сколь угодно малые FRR (при условии выполнения ряда предположений о характере ошибок). Использование подсказок (helper string) значительно снижает FRR, однако с увеличением исправляющей способности кода это может увеличить FAR за счет неправильного «исправления» биометрических признаков. Выбор компромиссного решения по параметрам кода с учетом характеристики возникающих ошибок, экспериментальные исследования FRR и FAR являются перспективными направлениями дальнейшей работы.

Список литературы:

1. Hao F., Anderson R., Daugman J. Combining cryptography with biometrics effectively: Technical Report UCAM-CL-TR-640. – Cambridge: University of Cambridge Computer Laboratory, 2005. – 17 p.
2. A. Juels, M. Sudan. A fuzzy vault scheme // Des. Codes Cryptography. – 2006. – Vol. 38, no. 2. – P. 237-257..
3. Y. Dodis, R. Ostrovsky, L. Reyzin, A. D. Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data // SIAM J. Comput. – 2008. – Vol. 38, no. 1. – P. 97-139,
4. Yevgeniy Dodis, Leonid Reyzin, Adam Smith. Fuzzy Extractors. A Brief Survey of Results from 2004 to 2006. [On-line]. Internet: http://www.cs.bu.edu/~reyzin/papers/fuzzysurvey.pdf
5. H. Kang, Y. Hori, T. Katashita, M. Hagiwara and K. Iwamura. Cryptographie key generation from PUF data using efficient fuzzy extractors // 16th International Conference on Advanced Communication Technology, Pyeongchang, 2014. – P. 23-26.
6. N. Li, F. Guo, Y. Mu, W. Susilo and S. Nepal. Fuzzy Extractors for Biometric Identification // IEEE 37th International Conference on Distributed Computing Systems (ICDCS), Atlanta, GA, 2017. – P. 667-677.
7. Y. Wen and Y. Lao. Efficient fuzzy extractor implementations for PUF based authentication // 12th International Conference on Malicious and Unwanted Software (MALWARE), Fajardo, 2017. – P. 119-125.
8. T. Kaur and M. Kaur. Cryptographic key generation from multimodal template using fuzzy extractor // Tenth International Conference on Contemporary Computing (IC3), Noida, 2017. – P. 1-6.
9. N. K. Gupta and M. Kaur. A robust and secure multitrait based fuzzy extractor // 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Delhi, 2017 – P. 1-6.
10. C. Huth, D. Becker, J. Guajardo, P. Duplys and T. Güneysu. LWE-based lossless computational fuzzy extractor for the Internet of Things // IEEE International Symposium on Hardware Oriented Security and Trust (HOST), McLean, VA, 2017. – P. 154-154.
11. C. Huth, D. Becker, J. G. Merchan, P. Duplys and T. Güneysu. Securing Systems With Indispensable Entropy: LWE-Based Lossless Computational Fuzzy Extractor for the Internet of Things // IEEE Access. – 2017. – Vol. 5, P. 11909-11926, 2017.
12. A. Schaller, T. Stanko, B. Škorić and S. Katzenbeisser. Eliminating Leakage in Reverse Fuzzy Extractors // IEEE Transactions on Information Forensics and Security. – 2018. – Vol. 13, no. 4. – P. 954-964

13. 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.

14. Clark G.C., Cain J.B. Error-Correction Coding for Digital Communications // Springer, 1981. – 432 p.

15. Blahut R. E. Theory and Practice of Error Control Codes. – Addison Wesley Publishing Company, Inc., Reading, Massachusetts, 1983, 1983 – 500 p.

16. A. Kuznetsov, A. Pushkar'ov, N. Kiyan and T. Kuznetsova. Code-based electronic digital signature // IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, 2018. – P. 331-336.

17. V.D. Goppa. A New Class of Linear Correcting Codes // Problems Inform. Transmission, 6: 3 (1970), 207-212.

18. D. Bernstein, J. Buchmann and E.Dahmen. Post-Quantum Cryptography. – Springer-Verlag, Berlin-Heidleberg, 2009. – 245 p.

Харьковский национальный
университет имени В.Н. Каразина;
Академия национальной армии
имени гетмана Петра Сагайдачного;
Государственное конструкторское
бюро «Южное», Днепр

Поступила в редколлегию 07.11.2018

УДК 629.7.022

В.М. КАРТАШОВ, д-р техн. наук, В.Н. ОЛЕЙНИКОВ, канд. техн. наук,
С.А. ШЕЙКО, канд. техн. наук, С.И. БАБКИН, канд. техн. наук,
И.В. КОРЫТЦЕВ, канд .техн. наук, О.В. ЗУБКОВ, канд. техн. наук

ОСОБЕННОСТИ ОБНАРУЖЕНИЯ И РАСПОЗНАВАНИЯ МАЛЫХ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

Введение

В настоящее время количество сфер применения малых беспилотных летательных аппаратов (БПЛА) стремительно растет. Среди сравнительно новых потребительских рынков БПЛА можно отметить лесное, сельское и дорожное хозяйство, энергетику и связь, добычу и транспортировку нефти и газа, безопасность и охрану окружающей среды и т.д. Многие малые БПЛА стали доступными для обычных пользователей, причем их оснащение достаточно сложное и включает фото- и видеокамеры, систему автопилота и навигации, что делает управление такими БПЛА достаточно простым. Решая эти задачи, они позволяют экономить большие материальные, энергетические и людские ресурсы. БПЛА существенно сокращают время решения таких задач, в ряде случаев позволяют сохранить человеческие жизни, уменьшить ущерб от стихийных бедствий и чрезвычайных ситуаций, которых в последнее время становится все больше [1, 2].

Повсеместное использование малых БПЛА помимо, несомненно, позитивных сторон породило ряд проблем, связанных с неадекватным поведением некоторых владельцев БПЛА, несанкционированным мониторингом объектов и территорий государственной важности, участившимися случаями вторжения в личную жизнь и т.д. В ряде перечисленных случаев актуальной становится задача обнаружения БПЛА в воздухе [2].

Настоящий краткий обзор посвящен беспилотным летательным аппаратам – их классификации, видам использования таких аппаратов, обнаружению и распознаванию малых БПЛА.

1. Использование беспилотных летательных аппаратов

Работы, направленные на создание беспилотных летательных аппаратов, начались давно [2], еще в годы первой мировой войны. В 1930-е годы появились первые дистанционно-пилотируемые воздушные мишени. А во время второй мировой войны появляется первый ударный беспилотный самолет – немецкий самолет-снаряд Фау-1. Впоследствии ударные самолеты-снаряды большой дальности относили к крылатым ракетам и не называли беспилотными самолетами. В конце 1950-х годов появляются беспилотные разведчики. 70-ми годами XX века датируются научно-исследовательские разработки и в области боевых (ударных) БПЛА, а также беспилотных самолетов с большой высотой и продолжительностью полета, предназначенных для длительного наблюдения и использования в составе разведывательно-ударных комплексов. В 1970-х – 1980-х годах этой тематикой занимались конструкторские бюро П.О. Сухого, А.Н. Туполева, В.М. Мясищева, А.С. Яковлева, Н.И. Камова. В КБ им. А.Н. Туполева созданы беспилотные разведчики «Ястреб», «Стриж», «Рейс» , а также ударный «Коршун», созданный совместно с НИИ «Кулон». В КБ им. А.С. Яковлева спроектирован комплекс «Пчела».

БПЛА все больше находят широкое применение и в других видах деятельности человечества. К примеру, в сельском хозяйстве БПЛА с GPS- навигацией используются для опыления растений на полях. При этом достигается значительная экономия химикатов и более тщательная обработка посевов по сравнению с пилотируемой авиацией. Они используются для доставки медикаментов и гуманитарных грузов в труднодоступные районы, могут применяться для проверки линий электропередачи трубопроводов. Дроны, другое название БПЛА, могут использоваться и государственной службой по чрезвычайным ситуациям для

мониторинга и прогнозирования, а также при контроле опасных объектов (безопасность и охрана окружающей среды) и многие другие. В частности, в качестве несущей платформы метеорологических измерительных комплексов для исследования атмосферного пограничного слоя (АПС) [3, 4] могут использоваться БПЛА мультикоптерного типа [5]. Они имеют преимущества по отношению к БПЛА самолетного типа, которые, в силу высокой скорости перемещения в атмосфере, не обеспечивают достаточного пространственного и временного разрешения измерений, обладают низкой чувствительностью, не позволяют исследовать турбулентные процессы. В настоящее время доступные и относительно недорогие мультикоптеры обеспечивают подъем с полезной нагрузкой 3 – 5 кг на высоту 2 – 4 км при длительности полета 30 – 40 мин. В современных БПЛА бортовая система навигации и управления может обеспечивать:

- полет по заданному маршруту (задание маршрута производится с указанием координат и высоты поворотных пунктов маршрута);
- изменение маршрутного задания или возврат в точку старта по команде с наземного пункта управления;
- облет указанной точки;
- стабилизацию углов ориентации БПЛА, – поддержание заданных высот и скорости полета (путевой либо воздушной),
- сбор и передачу телеметрической информации и параметрах полета и работе целевого оборудования, – программное управление устройствами целевого оборудования.

Все это позволяет обеспечить большую мобильность и оперативность измерений при невысокой стоимости эксплуатации БПЛА. Основные преимущества технологии измерений параметров атмосферного пограничного слоя с помощью БПЛА мультикоптерного типа:

- прямые контактные измерения метеорологических и турбулентных характеристик АПС;
- возможность оперативных кратковременных измерений характеристик АПС в заданных точках атмосферы (на высотах от 0 до 4000 м);
- высокое пространственное и временное разрешение;
- хорошая помехозащищенность;
- возможность измерения вертикальных профилей метеорологических, турбулентных и экологических характеристик АПС посредством контролируемого подъема (спуска) БПЛА по заданной программе;
- небольшие вес и габаритные размеры устройства;
- относительно невысокая цена.

Основные недостатки технологии измерений параметров АПС с помощью БПЛА мультикоптерного типа:

- небольшая длительность измерений (20 – 40 мин);
- относительно низкая грузоподъемность несущей платформы (требуется создание специализированных измерительных комплексов, имеющих малый вес, небольшие габаритные размеры и низкое энергопотребление).

Независимо от области применения, полномасштабное выполнение миссий БПЛА может включать такие подзадачи как обнаружение, локализация и идентификация целей, сопровождение и целеуказание [6, 7]. Как свидетельствуют различные источники информации, в настоящее время в нашей стране и за рубежом по результатам оценки вклада различных технических средств в эффективность боевых действий группировок вооруженных сил приоритеты отданы средствам получения разведывательной информации. Воздушная разведка по справедливости считается одной из самых опасных боевых задач. Подлежащие разведке цели противная сторона стремится скрыть и защищает их мощной объектовой и войсковой ПВО. Особенно опасна воздушная разведка в начальный период боевых действий, когда ПВО противника еще не подавлена, а также при отсутствии господства в воздухе. Поэтому особую

актуальность приобретает использование комплексов на основе беспилотных летательных аппаратов для воздушной разведки [7].

В большинстве перечисленных случаев актуальной становится задача обнаружения БПЛА в воздухе.

2. Типы БПЛА

Проанализировав существующие БПЛА, можно классифицировать их по особенностям их конструктивного исполнения [2].

Микро-БПЛА выполнены в своем большинстве по классической аэродинамической схеме, реже встречается схема «летающее крыло». По расположению крыла – высокопланы. Встречаются самолеты, имеющие поперечное V крыла. Двигатели электрические, в основном тянущие. Горизонтальное оперение – прямоугольное, расположенное низко относительно вертикального. Данные БПЛА осуществляют взлет с руки, а посадку – на парашюте. Мини-БПЛА выполнены по классической аэродинамической схеме. Крыло расположено высоко. Фюзеляжи представлены в виде как гондолы, так и однофюзеляжных схем. Вертикальное оперение представлено однокилевым, двухкилевым разнесенным, реже встречается V-образное. Двигатели в основном поршневые, толкающие или тянущие. Взлет осуществляют с пусковых установок, а посадку – на парашюте или по-самолетному. Миди-БПЛА отличаются от мини-БПЛА только тем, что осуществляют взлет и посадку по-самолетному, имеют неубирающееся трехопорное шасси с носовой опорой и поршневые двигатели. Макси-БПЛА выполнены по классической аэродинамической схеме. Крыло расположено низко. Оперение V-образное. Двигатели толкающие и представлены как ТРД, ТВД, так и ПД. Шасси убирающееся. Взлет и посадку выполняют по-самолетному.

«Беспилотники» различаются по массе (от аппаратов массой в полкилограмма, сравнимых с авиамоделью, до 10-15-тонных гигантов), высоте и продолжительности полета. Беспилотные летательные аппараты массой до 5 кг (класс «микро») могут взлетать с любой самой маленькой площадки и даже с руки, поднимаются на высоту 1 – 2 км и находятся в воздухе не более часа. Как самолеты-разведчики их используют, например, для обнаружения в лесу или в горах военной техники и террористов. «Беспилотники» класса «микро» массой всего 300 – 500 г, образно говоря, могут заглянуть в окно, поэтому их удобно использовать и в городских условиях. Следом за «микро» идут беспилотные летательные аппараты класса «мини» массой до 150 кг. Они работают на высоте до 3 – 5 км, продолжительность полета составляет 3 – 5 ч. Следующий класс – «миди». Это более тяжелые многоцелевые аппараты массой от 200 до 1000 кг. Высота полета достигает 5 – 6 км, продолжительность – 10 – 20 ч. И, наконец, «макси» – аппараты массой от 1000 кг до 8 – 10 т. Их потолок – 20 км, продолжительность полета – более 24 ч. Вероятно, вскоре появятся машины класса «супермакси». Можно предположить, что их масса превысит 15 т. Такие «тяжеловозы» будут нести на борту огромное количество аппаратуры различного назначения и смогут выполнять самый широкий круг задач.

3. Каналы обнаружения БПЛА

Информация для выявления и последующей пеленгации БПЛА может быть получена путем приема специальными средствами отраженной и излучаемой энергии во всех диапазонах спектра электромагнитных и акустических волн.

Любому материальному объекту, в том числе и БПЛА, присущи демаскирующие признаки, которые выделяют его в окружающей среде, делая его заметным для наблюдения. В настоящее время степень заметности определяют значением его сигнатур в радиочастотном, инфракрасном (ИК) и видимом диапазонах спектра, а также акустической сигнатурой. Современные легкие БПЛА имеют сигнатуры небольшого значения: их изготовляют с использованием композитных материалов и пластика со специальной окраской и особенной комбинацией слоев; небольшие бензиновые или электрические двигатели излучают мало тепла и работают почти бесшумно [8].

Значительное разнообразие возможных вариантов построения и использования средств наблюдения в каждом из указанных диапазонов обусловливает трудности оценивания их эффективности.

Акустический канал. Суммарный спектр акустического излучения тактического БПЛА обусловлен гармоническими и широкополосными составляющими. Он включает в себя гармонические оставляющие излучения двигателя, шума оборотов винта, излучение механической природы, а также высокочастотную и низкочастотную составляющие шума двигателя с непрерывными по частоте спектрами. В шуме силовой установки БПЛА, имеющей поршневой двигатель воздушного охлаждения, при отсутствии в его выхлопном тракте глушителя определяющим источником внешнего шума является поршневой двигатель [8 – 13].

Оптический канал. Оптическое обнаружение БПЛА очень зависит от факторов окружающей среды. Увеличение дальности обнаружения достигается за счет сужения поля зрения, уменьшения зоны обзора и увеличения времени поиска. Поэтому визуальные сенсоры являются неэффективными устройствами для проведения поиска. При поступлении внешних целеуказаний от более эффективного поискового средства оптические сенсоры могут быть эффективно использованы для сопровождения БПЛА [8, 14]. Поскольку беспилотники являются значительно меньшими по размерам по сравнению с пилотируемыми средствами, то это усложняет их обнаружение с помощью оптических средств. Сравнительно с самолетом контрастность БПЛА относительно фона является меньшей через отсутствие световых маяков, уменьшенный факел малого двигателя и меньшую поверхность отражения [14].

ИК канал. Тепло от БПЛА выделяется, в основном, силовой установкой и, в меньшей мере, электронными компонентами, а также точками торможения на несущих краях крыльев, пропеллеров и винтов. Разработчики беспилотников стараются предупредить излучение в ИК диапазоне в направлении размещенных на земле приемников и направить это излучение в сторону неба [8, 14 – 15]. Кроме того, используют материалы с малой излучательной способностью, такие как серебро и алюминий [16]. В данном случае возможность БПЛА быть обнаруженным определяется его излучательной способностью, контрастом и площадью излучения.

Радиоканал. Поиск БПЛА с помощью активных радиолокационных станций достаточно продуктивный, так как они имеют относительно большой импульсный объем поиска и значительную дальность обнаружения [17]. Однако РЛС могут быть определены противником по собственному излучению. Радиолокационное обнаружение БПЛА может быть приемлемым только тогда, когда не ставятся требования к скрытности работы или высокой мобильности [15]. Как уже отмечалось, большинство БПЛА изготавливают из композитных материалов, которые достаточно плохо отражают электромагнитные волны. Радиоволны проникают через поверхность беспилотника и только частично отражаются от нее [15].

Канал радиоразведки. БПЛА могут быть обнаруженными и средствами радиотехнической разведки путем приема и анализа радиосигналов линий связи и управления, радиолокационных высотомеров, постановщиков активных помех и радиолокационных станций. Однако этим методом можно установить лишь направление на БПЛА, причем точность определения повышается при увеличении времени наблюдения. Некоторые низкочастотные линии связи могут быть обнаружены на значительных дальностях. Излучение бортовых РЛС и постановка активных помех БПЛА могут быть обнаружены на еще больших дальностях. Этот метод требует минимального оборудования и позволяет быстро определить пеленг цели при дальнейшей выдаче целеуказаний на средства оптического или ИК наблюдения.

Перспективным направлением надежного обнаружения БПЛА является комплексирование информации, которая поступает по каналам разной физической природы.

В работе [18] описана комплексная сенсорная сеть обнаружения БПЛА, содержащая радиолокационный, акустический и телевизионный каналы. Однако предложенный алгоритм работы системы не учитывает эффективности каналов обнаружения с учетом разных физических признаков беспилотников. Результаты исследования по разработке метода обнаруже-

ния БПЛА на основе анализа их сигнатур в акустическом и радиолокационном диапазонах волн представлены в работе [19]. Другие виды и сети обнаружения описаны в работах [20 – 24].

Оценивая преимущества и недостатки рассмотренных физических каналов обнаружения БПЛА, можно сделать вывод, что для обнаружения малоразмерных и малоскоростных беспилотников (микро-БПЛА), так называемых БПЛА широкого применения, являющихся наиболее востребованными в решении гражданских и военных задач, оптимальным является акустический канал.

4. Обнаружение и распознавание БПЛА широкого применения

4.1. Источники акустических сигналов БПЛА

Основными источниками шума микро-БПЛА являются двигатель, воздушный винт и планер. Поскольку скорости полета таких БПЛА дозвуковые, то аэродинамическим шумом планера можно пренебречь из-за его небольшой значимости. Источниками шума в поршневом двигателе являются процессы впуска свежего заряда (шум впускания), горения, выпуска отработанных газов (шум выпуска); механическое перемещение деталей, которое сопровождается ударами и трением в сочленениях и стыках. Последние совместно с процессом горения являются источниками корпусного шума. Акустический шум обычно увеличивается по мере увеличения мощности двигателя [2 – 25].

Электрические двигатели имеют более низкие шумовые характеристики, однако их использование ограничивается БПЛА малым радиусом действия.

Двигатели большинства не реактивных БПЛА являются достаточно небольшими для использования глушителей и снижению таким образом акустической заметности. Кроме того, природный и антропогенный шум окружающей среды усложняет обнаружение БПЛА по их акустическому портрету. Но поскольку беспилотники этого класса имеют малые ИК и радиолокационные сигнатуры, по сравнению с пилотируемой авиацией, то использование акустических каналов для их обнаружения становится весьма актуальным. Акустические сенсоры позволяют наземным средствам производить поиск и обнаружение БПЛА в пассивном режиме, снижая таким образом вероятность определения противником собственных позиций. Поэтому модификация существующих акустических систем поиска или создание новых может обеспечить надежный метод обнаружения БПЛА [16].

Для детального анализа акустических сигналов используют решетки микрофонов, поскольку использование отдельного микрофона даст лишь грубую оценку акустического сигнала [10]. Акустические антенные решетки могут эффективно использоваться для обнаружения и сопровождения низко летающих БПЛА на тактических расстояниях. В то же время акустическая решетка, кроме пространственного накопления сигналов, позволяет оценивать время прихода фронта акустической волны в разные точки пространства, что, в свою очередь, содействует оценке угла распространения волны относительно решетки, т.е. можно вычислить пеленг на источник излучения. Для БПЛА среднего размера с двигателем внутреннего сгорания дальность обнаружения в пять раз превышает этот же показатель для беспилотника с электрическим двигателем [1, 2, 11, 12].

Характеристики направленности – одна из важнейших характеристик источников шума в авиации. Факторы направленности излучения различных источников используются в классических подходах авиационной акустики для расчета ожидаемых уровней шума самолетов на местности. Эти методы расчета также входят в методику прогноза границ слышимости и заметности малоразмерных беспилотных летательных аппаратов с винтомоторной установкой. В работе [26] приведены результаты акустических испытаний малоразмерного БПЛА с поршневым двигателем в заглушенной камере АК-2 ЦАГИ. Показано, что при работе силовой установки на взлетном режиме в задней полусфере в направлениях $105 – 120^0$ в суммарном шуме силовой установки доминирует излучение на частоте первой гармоники шума вращения винта. На оси коленчатого вала доминирующим является акустическое излучение

от поршневого двигателя. Здесь же описаны факторы направленности суммарного акустического излучения силовой установки и отдельных его частей.

4.2. Информационные характеристики акустических сигналов БПЛА

При гармоническом обнаружении анализируются узкие полосы частот на коротких временных интервалах. Сигнал подают в виде суммы гармоник с неизвестными частотами и фазами. Если сигналы слабые, то гармонический детектор работает более надежно чем энергетический [13, 14, 24].

Суммарный спектр акустического излучения тактического БПЛА обусловлен гармоническими и широкополосными составляющими. Он включает в себя гармонические составляющие излучения от двигателя, шума вращения винта, излучение механического происхождения, а также высокочастотную и низкочастотную составляющие шума двигателя с непрерывными по частоте спектрами. В шуме силовой установки БПЛА, включающего поршневой двигатель воздушного охлаждения, при отсутствии в его выхлопном тракте глушителя определяющим источником внешнего шума является поршневой двигатель.

Дискретные составляющие следуют с частотами $f_i = f_0 \times i$, которые кратны частоте зажигания f_0, где $i = 1, 2, 3\ldots$ – номер соответствующей гармоничной составляющей. На высоких частотах значимость периодических процессов в формировании спектра акустического излучения двигателя заметно ослабляется, поскольку более важную роль в суммарном акустическом излучении начинают играть процессы случайного происхождения. В частности, для шума выхлопа может быть существенной вихревая составляющая. На самом же деле выхлопной тракт двигателя формирует в атмосфере последовательность импульсов давления, частотный спектр которого представлен на рис. 1 [5, 27].

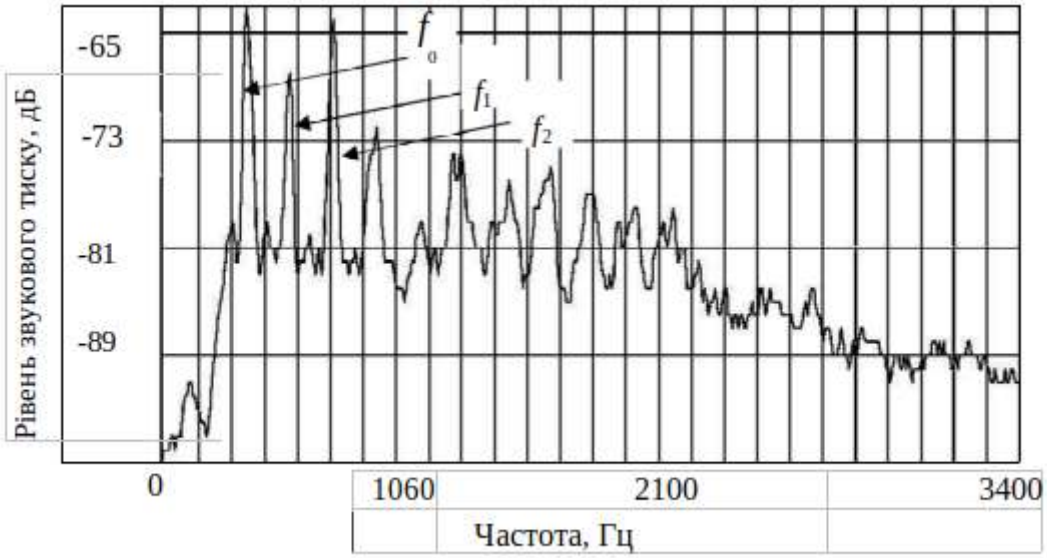


Рис. 1. Типовый спектр акустистического излучения работы силовой установки БПЛА

Другой информационной характеристикой акустических сигналов БПЛА, используемый для их распознавания, является фазовый портрет этих сигналов [28].

Геометрическую дальность обнаружения акустических сигналов определяют зоной акустической освещенности, полученной в результате построения лучевой картины, которая зависит от стратификации атмосферы, рельефа подстилающей поверхности, высоты источника звука и характеристик его направленности.

4.3. Обнаружение и распознавание малозаметных БПЛА

Более тщательное исследование различных информационных характеристик акустических сигналов, малозаметных БПЛА двух видов проведено в работах [29 – 32]. Экспериментальная установка для исследований состояла из измерительного конденсаторного микрофона Superlux ECM-999, установленного в фокусе параболического отражателя диаметром 0,6 м. Выход микрофона подключался по симметричному аудиоинтерфейсу XLR ко входу внешней звуковой карты Behringer U-Phoria UM2. Звуковой сигнал оцифровывался с частотой дискретизации 48 кГц и разрядностью 24 бита. Эксперименты проводились в условиях города, во внутреннем дворе университета. Отношение сигнал/шум в обрабатываемых записях составило около 20 дБ. Исследованы акустические излучения квадрокоптера DJI Phantom 2 и моноплана Skywalker Falcon 1340 mm EPO Flying Wing. По результатам обработки записей получены спектры используемых БПЛА, их спектрограммы и нормированные автокорреляционные функции, а также фазовые портреты. Анализ полученных информационных характеристик позволил сделать такие выводы:

- экспериментальное исследование звуковых сигналов квадрокоптера и моноплана показало, что их спектры имеют ярко выраженные гармонические составляющие с частотами, кратными частоте вращения винта;
- гармонические составляющие звукового сигнала квадрокоптера шире, чем у моноплана, что объясняется некоторым различием режимов работы двигателей в процессе полета или при работе системы компенсации ветровых возмущений;
- при большом различии режимов двигателей квадрокоптера спектральные максимумы разделяются на несколько, что может являться одним из признаков для классификации БПЛА;
- в звуковых сигналах исследованных БПЛА, при наличии накопления спектров, уверенно наблюдаются гармоники с частотами до 8 – 10 кГц;
- при акустическом наблюдении БПЛА самолетного типа под малыми углами к направлению движения структура спектра изменяется незначительно, что дает возможность применять временное накопление на длительных интервалах.

Для построения первичных признаков звукового образа БПЛА принимаемые пассивным содаром звуковые колебания БПЛА преобразуются в электрический сигнал, представляющий собой реализацию широкополосного случайного процесса, описание которого может быть дано энергетическим спектром. Поэтому информационными признаками звукового образа БПЛА могут служить оценки спектральных коэффициентов, определяемые по дискретной реализации, содержащей заданное количество отсчетов. Переход ко вторичным информационным признакам осуществляется путем построения ковариационной матрицы спектральных коэффициентов и ее диагонализации. После проведенных расчетов набор признаков, поступивший на вход системы, соответствует некоторому классу, если среднее значение коэффициента подобия по всем парам сличаемых векторов больше определенной пороговой величины. Проведенные теоретические исследования позволяют разработать модуль формирования коллекции звуковых образов БПЛА и модуль, реализующий правило принятия решений.

Выводы

1. Создание и широкое применение, часто несанкционированное, БПЛА различного конструктивного исполнения и веса поставили насущную проблему разработки эффективных технических средств их оперативного обнаружения и распознавания.

2. Информация для выявления и последующей пеленгации БПЛА может быть получена путем приема специальными средствами отраженной и излучаемой энергии во всех диапазонах спектра электромагнитных и акустических волн. Для решения проблемы обнаружения

БПЛА в настоящее время используются каналы: акустический, оптический, инфракрасный и радиоканал, а также канал радиоразведки. Для обнаружении малозаметных и малоскоростных БПЛА из известных наиболее эффективным является акустический канал.

3. Суммарный спектр акустического излучения тактического БПЛА обусловлен гармоническими и широкополосными составляющими. При применении акустических систем для обнаружения и распознавания БПЛА в настоящее время используются частотные спектры, спектрограммы, нормированные автокорреляционные функции и фазовые портреты принятых сигналов.

4. Актуальной задачей является задача разработка эффективных методов пеленгации БПЛА. Классические методы пеленгации не позволяют решать задачу в условиях быстро меняющейся динамической обстановки, которая характерна для БПЛА. Они не удовлетворяют запросам практики по точности измерений и, особенно, по угловой разрешающей способности. Удовлетворение требований может быть достигнуто использованием пространственных решеток и современных методов пространственной обработки

5. Информационными признаками звукового образа БПЛА могут служить оценки спектральных коэффициентов, а также параметры моделей авторегрессии.

Список литературы:

1. Кошкин Р.П. Беспилотные авиационные системы. – Москва : Стратегические приоритеты, 2016. – 676 с.

2. Цепляева Т.П., Поздышева Е. М., Поштаренко А. Г. Анализ применения беспилотных комплексов / Нац. аэрокосм. ун-т им. Н.Е. Жуковского «ХАИ». – https:www.khai.edu/csp/portal//Archiv/OIKIT39/p_149-154. pdf. Дата обращения 16.09.2017 г.

3. Kartashov V.M., Babkin S.I., Tolstykh E.G. Methodical errors in meteorological measurements during correlation processing of signals from radio acoustic sounding system // Telecommunications and Radio Engineering. – 2017. – **V**.76(20). – P. 1861-1867.

4. Semenets V.V., Kartashov V.M., Leonidov V.I. Registration of refraction phenomenon in the problem of acoustic sounding of atmosphere in airports zone // Telecommunications and Radio Engineering. -2018. – **V**.77(5). – P. 461-468.

5. Корольков В.А. Автоматизированные акустические и оптоэлектронные комплексы и системы для экологического и метеорологического мониторинга атмосферы : дис. … дра техн. наук ; специальность 05.11.13 – Приборы и методы контроля природной среды, веществ, материалов и изделий. – Томск, 2017. – 471 с.

6. Теодорович Н.Н., Строганова С.М., Абрамов П.С. Способы обнаружения и борьбы с малогабаритными беспилотными летательными аппаратами // Интернет-журнал “НАУКОВЕДЕНИЕ”. – 2017. – Т.9, №1. http://naukovedenie.ru/PDF/13TVN117.pdf (доступ свободный).

7. Амелин К.С., Миллер А.Б.. Алгоритм уточнения местонахождения легкого БПЛА на основе калмановской фильтрации измерений пеленгационного типа / Санкт-Петербург. гос. ун-т // Анализ и синтез систем управления. Информационные процессы. – 2013. – Т. 13, № 4. – С. 338–352.

8. Даник Ю.В, Бугайов М.В. Аналіз ефективності виявлення тактичних безпілотних літальних апаратів пасивними та активними засобами спостереження // Зб. наук. праць ЖВІ ДУТ. Інформаційні системи’15. – 2015. – Вип.10. – С.5-20.

9. Горбунов В. А. Эффективность обнаружения целей. – Москва : Воениздат, 1979. – С. 16.

10. Sadasivan S. Acoustis siqnature of an unmanned air vehicle – exploitation for aircraft localisation and parameter estimation / S. Sadasivan, M. Gurubasavaraj, S.R. Sekar // Eronautical DEF SCI J. – 2001. – Vol. 51, № 3. – P. 279–283.

11. Massey K. Noise Measurements of Tactical UAVs / K. Massey, R. Gaeta // Georgia Inst. of Technology / GTRI / ATAS, Atlanta. 16th AIAA / CEAS Aeroacoustics Conference. American Institute of Aeronautics and Astronautics, 2010. – P. 1-16.

12. Marino L. Experimental analysis of UAV-propellers noise // 16th AIAA/CEAS Aeroacoustics Conference. University «La Sapienza», Rome, Italy. – American Institute of Aeronautics and Astronautics, 2010. – P. 1-14.

13. Pham T. TTCP AG-6: Acousting detection and tracking of UAVs / T.Pham, N.Srour // U.S. Army Research Laboratory. Proc. of SPIE. – 2004. – Vol. 54. – P. 24–29.

14. Zelnio A.M. Detection of small aircraft using an acoustic array. Thesis. B.S. – Electrical Engineering, Wright State University, 2007. – 55 p.

15. Соловьев В. А. Проблемы обнаружения беспилотных летательных аппаратов оптико-электронными устройствами // Электронный математический и медико-биологический журнал. – 2011. – Т. 10. – Вып. 3. – С. 1–13.

16. Beel J. J. Anti-UAV Defense For Ground Forces and Hypervelocity Rocket Lethality Models. – Monterey, California : Naval Postgr aduate School, 1992. – P. 36–46.

17. Moses A. Radar-based detection and identification for minia ture air vehicles / A. Moses, M. J. Rutherford, K. P. Valavanis // IEEE International Conference on Control Applications.

18. Detecting, Tracking and Identifying Airborne Threats with Netted Sensor Fence / W. Shi, G. Arabadjis, B. Bishop, P. Hill // Sensor Fusion – Foundation and Applications. – Rijeka, Croatia : InTech Europe, 2001. – P. 139–158.

19. Даник Ю.Г., Пулеко І.В., Бугайов М.В. Виявлення безпілотник літальних апаратів на основі аналізу акустичних та радіолокаційних сигналів // Вісник ЖДТУ. – 2014. – № 4 (71). – С.71- 80.

20. Weiqun Shi, Ronald Fante, John Joder, and Gregory Crowford. Multi-Modal Netted Sensor Fence for Homeland Security. Approved for Public Release; Distribution Unlimited Case, #05-0354. – P. 1-12.

21. Nanjaport Intrater, W. Nathan Alexander, William J. Davenport, Sheril M. Grace, and Amanda Dropkin. Experimental Study of Quadcopter Acoustic and Performance at static Thrust Condidtions. Aeroacoustics Conferences. 30 May-1 June. 2016, Lyon, France. 22Nd AIAA/CEAS Aeroacoustics Conference. American Institute of Aeronautics and Astronautics. – P. 1-14.

22. Kartashov V.M., Tikhonov V.F., Voronin V.V. Fuatures of construction and application of complex system for the atmosphere remote sounding // Telecommunications and Radio Engineering. – 2016. – **V**.76(8). – P. 743-749.

23. Saravanakumar A. Exploitation of Acoustic signature of low flying Aircraft using Acoustic Vector sensor / A. Saravanakumar, K. Senthilkumar // Defence Science Journal. – March 2014. – Vol. 64, No. 2. – P. 95–98.

24. Самохин В. Ф. Экспериментальное исследование источников шумности беспилотного летательного аппарата с винто-кольцевым движителем в толкающей компоновке / В.Ф. Самохин, С.П. Остроухов, П.А. Мошков // Электронный журнал «Труды МАИ». – 2012. – Вып. № 70. – С.1–24.

25. Мошков П.А. Прогнозирование и снижение шума на местности легких винтовых самолетов : дис. … канд. техн. наук. – Москва : МАИ (НИУ), 2015. – 143 с.

26. Мошков П.А., Беляев И.В., Остриков Н.Н. Экспериментальное исследование акустических характеристик беспилотного летательного аппарата в заглушенной камере АК-2 // XI Междунар. науч. конф. по амфибийной и безаэродромной авиации “Гидроавиасалон-2016”, г. Геленджик, 23-24 сентября 2016. Тез. докл. – Москва : ЦАГИ, 2016. – С. 45.

27. Гордієнко Ю.О., Бугайов М.В., Солонець О.І., Солопій О.А. Особливості акустичних сигналів безпілотних літальних апаратів // Наука і техніка Повітряних Сил Збройних Сил України. – 2016. – № 1 (22). – С.32-35.

28. Пащенко Р.Э., Коршунов В.В., Цюпак Д.О., Богданова О.А. Распознавание БПЛА мультироторного типа с использованием фазовых портретов // Наука і техніка Повітряних Сил Збройних Сил України. – 2013. – № 4 (13). – С. 68-72.

29. Олейников В.Н., Шейко С.А., Бабкин С.И. Исследование характеристик акустического излучения малых беспилотных летательных аппаратов // Сб. науч. тр. VI Междунар. радиоэлектрон. форума “Прикладная радиоэлектроника. Состояние и перспективы развития (МРФ-2017)”. Междунар. науч. конф. “Радиолокация. Спутниковая навигация. Радиомониторинг”. 24-26 октября 2017 г. Харьков, Украина. – Харьков : Точка, 2017. – С.107 – 110.

30. Карташов В.М., Корытцев И.В., Зубков О.В., Анохин М.А. Обнаружение БПЛА на фоне акустических шумов и помех // Там же. – С. 68-70.

31. Карташов В.М., Олейников В.Н., Шейко С.А., Бабкин С.И., Корытцев И.В., Зубков О.В., Анохин М.А. Информационные характеристики звуковых сигналов малых беспилотных летательных аппаратов // Радиотехника. – 2017. – Вып 191. – С. 181-187.

32. Kartashov V.M., Oleynikov V.N, Sheyko S.A., Babkin S.I., Koryttsev I.V., Zubkov O.V., Anokhin M.A. Information characteristics of sound radiation of small unmanned aerial vehicles // Telecommunications and Radio Engineering. – 2018. – **V**.77(10). – P. 915-924.

Харьковский национальный
университет радиоэлектроники

Поступила в редколлегию 05.11.2018

РЕФЕРАТЫ РЕФЕРАТИ ABSTRACTS

ПЕРСПЕКТИВНЫЕ КРИПТОГРАФИЧЕСКИЕ СИСТЕМЫ И ПРОТОКОЛЫ
ПЕРСПЕКТИВНІ КРИПТОГРАФІЧНІ СИСТЕМИ ТА ПРОТОКОЛИ
PERSPECTIVE CRYPTOGRAPHIC SYSTEMS AND PROTOCOLS

УДК 004.056.55

Методы построения общесистемных параметров и ключей для NTRU PRIME UKRAINE 5 – 7 уровней стойкости. Product form / *И.Д. Горбенко, Е.Г. Качко, Ю.И. Горбенко, И.В. Стельник, С.А. Кандий, М.В. Есина* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2018. – Вып. 195. – С. 5 – 16.

Проведено исследование и выполнена разработка эффективного практического алгоритма построения общесистемных параметров и ключей криптопреобразования типа несиммметричный шифр для специальной формы задания полиномов Product Form. Приведен экспериментально определенный набор параметров для алгоритма **NTRU PRIME UKRAINE** для 5 – 7 уровней стойкости с учетом комбинированной атаки.

Ключевые слова: несиммметричный шифр, общесистемные параметры, квантовая стойкость, уровень стойкости, конечные поля, Product Form

Табл. 7. Библиогр.: 18 назв.

УДК 004.056.55

Методи побудування загальних параметрів та ключів для NTRU PRIME UKRAINE 5 – 7 рівнів стійкості. Product form / *І.Д. Горбенко, О.Г. Качко, Ю.І. Горбенко, І.В. Стельнік, С.О. Кандій, М.В. Єсіна* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. – Вип. 195. – С. 5 – 16.

Проведено дослідження та виконано розробку ефективного практичного алгоритму побудування загальносистемних параметрів та ключів криптоперетворень типу асиметричний шифр для спеціальної форми завдання поліномів Product Form. Наводиться експериментально визначений набір параметрів для алгоритму **NTRU PRIME UKRAINE** для 5 – 7 рівнів стійкості з урахуванням комбінованої атаки.

Ключові слова: асиметричний шифр, загальні параметри, квантова стійкість, рівень стійкості, скінчені поля, Product Form.

Табл. 7. Бібліогр.: 18 назв.

UDC 004.056.55

Methods for constructing system-wide parameters and keys for NTRU PRIME UKRAINE 5 – 7 stabvility levels. Product form / *I.D. Gorbenko, O.G. Kachko, Yu. I. Gorbenko, I.V. Stelnik, S.O. Kandy, M.V. Yesina* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2018. – №195. – P. 5 – 16.

The research was carried out and the development of an effective practical algorithm for the construction of system-wide parameters and keys of cryptographic transformations such as asymmetric ciphers for a special form of setting the Product Form polynomial was performed. The experimental confirmation of the built-in system-wide parameters for 5 – 7 stability levels **NTRU PRIME UKRAINE,** taking into account a combined attack. is given.

Key words: asymmetric cipher, general parameters, quantum stability, stability level, finite fields, Product Form.

7 tab. Ref.: 18 items.

УДК 004.056.55

Вычисление общих параметров для NTRU PRIME UKRAINE 6-7 уровней стойкости / *И.Д. Горбенко, А.Н. Алексейчук, О.Г. Качко, М.В. Есина, В.А. Бобух, С.О. Кандий, В.А. Пономарь* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2018. – Вып. 195. – С. 17 – 26.

Проведено исследование и выполнена разработка эффективного практического алгоритма построения общесистемных параметров и ключей криптопреобразований типа асимметричный шифр и протокол инкапсуляции ключей. Приводится экспериментальное подтверждение построенных общесистемных параметров и ключей криптопреобразования типа асимметричный шифр и протокол инкапсуляции ключей 6-7 уровней стойкости на основе преобразований в кольце полиномов над конечным полями. Приводятся виды атак, которые являются возможными касательно указанных криптопреобразований.

Ключевые слова: общие параметры, квантовая стойкость, кольцо полиномов, уровень стойкости, конечные поля.

Табл. 1. Библиогр.: 15 назв.

УДК 004.056.55

Обчислення загальних параметрів для NTRU PRIME UKRAINE 6 – 7 рівнів стійкості / *І.Д. Горбенко, А.М. Олексійчук, О.Г. Качко, М.В. Єсіна, В.А. Бобух, С.О. Кандій, В.А. Пономар* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. – Вип. 195. – С. 17 – 26.

Проведено дослідження та виконано розробку ефективного практичного алгоритму побудування загальносистемних параметрів та ключів криптоперетворень типу асиметричний шифр та протокол інкапсуляції ключів. Наводиться експериментальне підтвердження побудованих загальносистемних параметрів та ключів криптоперетворень типу асиметричний шифр та протокол інкапсуляції ключів 6 – 7 рівнів стійкості на основі перетворень в кільці поліномів над скінченими полями. Наводяться види атак, які є можливими щодо зазначених криптоперетворень.

Ключові слова: загальні параметри, квантова стійкість, кільце поліномів, рівень стійкості, скінчені поля.

Табл. 1. Бібліогр.: 15 назв.

UDC 004.056.55

General parameters for NTRU PRIME UKRAINE 6 – 7 stability levels calculation / *I.D. Gorbenko, A.N. Alekseychuk, O.G. Kachko, M.V. Yesina, V.A. Bobukh, S.O. Kandy, V.A. Ponomar* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2018. – №195. – P. 17 – 26.

The research was carried out and the development of an effective practical algorithm for the construction of system-wide parameters and keys for cryptographic transformations such as asymmetric ciphers and the key encapsulation protocol was performed. The experimental confirmation of the built-in system-wide parameters and keys of cryptographic transformations such as asymmetric cipher and the key encapsulation protocol of 6 – 7 stability levels based on transformations in the ring of polynomials over the finite fields is presented. The types of attacks that are possible with respect to the specified cryptographic transformations are also presented in this work.

Key words: general parameters, quantum stability, ring of polynomials, stability level, finite fields.

1 tab. Ref.: 15 items

УДК 004.056.55

Криптоанализ хеш-функции Купина при использовании в схемах подписи Меркла / *Е.Г. Качко, Д.К. Телевный* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2018. – Вып. 195. – С. 27 – 31.

Статья посвящена анализу уровня безопасностиб хеш-функции Купина ДСТУ 7564:2014 при использовании в схемах подписи Меркла. Робота описывает возможные атаки на хеш, и их последствия для схемы подписи. Результати покзывают целесообразность использования хеша в схеме, основанные на результатах производительности, уровня безопасности и стойкости.

Ключевые слова: проблема обхода дерева, схемы деревьев меркла, купина, криптоанализ, схемы подписей, эцп.

Табл. 3. Ил. 1. Библиогр.: 9 назв.

УДК 004.056.55

Криптоаналіз геш-функції Купина при використанні у схемах підпису Меркла / *О.Г. Качко, Д.К. Телевний* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. – Вип. 195. – С. 27 – 31.

Стаття присвячена аналізу рівня безпеки хеш-функції Купина ДСТУ 7564:2014 при використанні у схемах підпису Меркла. Робота описує можливі аттаки на геш, та їх наслідки у схемі підпису. Результати показують доцільність використання гешу у схемі, що базубться на результатах потужності, рівня безпеки та стійкості.

Ключові слова: проблема обходу дерева, схеми дерев меркла, купина, криптоаналіз, схемі підпису, ецп.

Табл. 3. Іл. 1. Бібліогр.: 9 назв.

UDC 004.056.55

The Kupyna hash function cryptanalysis with Merkle Trees Signature schemes / *O. Kachko, D. Televnyi* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2018. – №195. – P. 27 – 31.

The paper is devoted to the security analysis of the Kupyna (DSTU 7564:2014) hash function applied to Merkle tree signature schemes. The paper lists possible attacks on the hash, and their application for signature schemes. The results show expediency of using the Kypuna hash in Merkel schemes based on the performance, security levels and strength against known cryptanalytic attacks.

Key words: tree traversal problem, merkle tree schemes, kupyna, cryptanalisys, dsa. mss.

3 tab. 1 fig. Ref.: 9 items.

УДК 004.056.5

NIST PQC: Кодовые криптосистемы / *А.А. Кузнецов, Ю.И. Горбенко, М.С. Луценко, Д.И. Прокопович-Ткаченко, Н.В. Пастухов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2018. – Вып. 195. – С. 32 – 40.

Исследуются кодовые схемы, которые были представлены на конкурс постквантовых криптографических алгоритмов NIST PQC. Рассмотрены общие характеристики алгоритмов, их основные свойства и параметры. Проведен сравнительный анализ схем электронной цифровой подписи, направленного шифрования и схем инкапсуляции ключей по критериям скорости и длины основных криптографических параметров.

Ключевые слова: постквантовая криптография; подписи в кодах; криптосистемы с открытым ключом; механизмы инкапсуляции ключей; криптографические параметры.

Ил. 6. Библиогр.: 24 назв.

УДК 004.056.5

NIST PQC: Кодові криптосистеми / *О.О. Кузнецов, Ю.І. Горбенко, М.С. Луценко, Д.І. Прокопович-Ткаченко, М.В. Пастухов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. – Вип. 195. – С. 32 – 40.

Досліджуються кодові схеми, які були представлені на конкурс постквантових криптографічних алгоритмів NIST PQC. Розглянуто загальні характеристики алгоритмів, їх основні властивості і параметри. Проведено порівняльний аналіз схем електронного цифрового підпису, направленого шифрування і схем інкапсуляції ключів за критеріями швидкості і довжини основних криптографічних параметрів.

Ключові слова: постквантова криптографія; підписи на кодах; криптосистеми з відкритим ключем; механізми інкапсуляції ключів; криптографічні параметри.

Іл. 6. Бібліогр.: 24 назв.

UDC 004.056.5

NIST PQC: Code-Based Cryptosystems / *A.A. Kuznetsov, Yu.I. Gorbenko, M.S. Lutsenko, D.I. Prokopovych-Tkachenko, M.V. Pastukhov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2018. – №195. – P. 32 – 40.

The code-based schemes, which were submitted to the contest of post-quantum crypto algorithms NIST PQC, are studied in this work. The general characteristics of the algorithms are explored and basic properties and parameters are estimated. A comparative analysis of the electronic digital signature schemes, public-key cryptosystems and key encapsulation schemes are carried out according to the criteria of speed and length of the main cryptographic parameters.

Keywords: Post-Quantum Cryptography; Code-Based Signatures; Public-Key Cryptosystems; Key Encapsulation Mechanisms; Cryptographic Parameters

6 fig. Ref.: 24 items.

УДК 004.428.4

Эллиптические кривые Эдвардса. Сравнение криптографических библиотек / *О.А. Мельникова, О.В. Джурик, А.О. Масленникова* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2018. – Вып. 195. – С. 41 – 45.

Кривые Эдвардса – это форма представления эллиптических кривых, которая поддерживает быстрый, унифицированный и полный закон сложения точек. Кривые Эдвардса приобрели большую популярность благодаря эффективным формулам сложения и удвоения точек. Рассматриваются и сравниваются программные библиотеки, которые поддерживают кривые Эдвардса и цифровую подпись EdDSA.

Ключевые слова: эллиптические кривые Эдвардса, электронная цифровая подпись, криптографические библиотеки, несимметричная криптография.

Табл. 3. Библиогр.: 7 назв.

УДК 004.428.4

Еліптичні криві Едвардса. Порівняння криптографічних бібліотек / *О.А. Мельникова, О.В. Джурик, А.О. Маслєннікова* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. – Вип. 195. – С. 41 – 45.

Криві Едвардса – це форма представлення еліптичних кривих, яка підтримує швидкий, уніфікований та повний закон додавання точок. Криві Едвардса набули великої популярності завдяки

ефективним формулам додавання та подвоєння точок. Розглядаються та порівнюються програмні бібліотеки, які підтримують криві Едвардса та цифровий підпис EdDSA.

Ключові слова: еліптичні криві Едвардса, електронний цифровий підпис, криптографічні бібліотеки, несиметрична криптографія

Табл. 3. Бібліогр.: 7 назв.

UDC 004.428.4

Edwards elliptic curves. Comparison of cryptographic libraries / *O. Melnykova, O. Dzhuryk, A. Masliennikova* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2018. – №195. – P. 41 – 45.

Edwards Curves is a form of representing elliptic curves that supports fast, unified, and complete law of addition of points. Edwards curves have attracted great interest for their efficient addition and doubling formulas. In this paper, we described and compared programming libraries, which implemented Edwards curves and EdDSA signature.

Key words: Edwards elliptic curves, digital signature, cryptographic programming libraries, public-key cryptography

3 tab. Ref.: 7 items.

УДК 004.056.55

Сравнительный анализ пост квантовых стандартов электронной подписи на основе мультивариативних квадратичных преобразований / *И.Д. Горбенко, И.С. Кудряшов, В.В. Оноприенко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2018. – Вып. 195. – С. 46 – 60.

Приводятся результаты анализа и сравнения механизмов электронной подписи с использованием многомерных преобразований в квадратичных конечных полях. В качестве основных критериев использованы длины ключей и электронной подписи, а также вычислительная эффективность подписи и проверки подписи. Сравнение сделано по электронным подписям LUOV, Gui, Rainbow, MQDSS, TPSig, DualModeMS, HiMQ-3 и GeMSS. Указанные кандидаты выбраны по безусловным частным и интегральному безусловному критерию криптографической устойчивости к атаке на основе адаптивного подбора сообщений.

Ключевые слова: асимметричный ключ, асимметричные криптопреобразования, многомерные преобразования, электронная подпись, квадратичные поля, постквантовые электронные подписи.

Табл. 3. Ил. 9. Библиогр.: 14 назв.

УДК 004.056.55

Порівняльний аналіз пост квантових стандартів електронного підпису на основі мультиваріативних квадратичних перетворень / *І.Д. Горбенко, І.С. Кудряшов, В.В. Онопрієнко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. – Вип. 195. – С. 46 – 60.

Наведено результати аналізу та порівняння механізмів електронного підпису з використанням баготовимірних перетворень в квадратичних скінченних полях. В якості основних критеріїв використані довжини ключів та електронного підпису, обчислювальна ефективність підпису та перевірки підпису. Порівняння зроблено щодо електронних підписів LUOV, Gui, Rainbow, MQDSS, TPSig, DualModeMS, HiMQ-3 та GeMSS. Кандидати вибрані по безумовних часткових та інтегральному безумовному критерію криптографічної стійкостіі до атаки на основі адаптивного підбору повідомлень.

Ключові слова: асиметричний ключ, асиметричні криптоперетворення, багатовимірні перетворення, електронний підпис, квадратичні поля, постквантові електронні підписи.

Табл. 3. Іл. 9. Бібліогр.:14 назв.

UDC 004.056.55

Comparative analysis of post quantum standards for electronic signature based on multivariate quadratic transformations / *I.D. Gorbenko, I.S. Kudryashov, V.V. Onoprienko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2018. – №195. – P. 46 – 60.

The results of the analysis and comparison of electronic signature mechanisms using multidimensional transformations in quadratic finite fields are presented. The key and electronic signature lengths, as well as the computational efficiency of the signature and signature verification are used as the main criteria. Comparison made by electronic signatures LUOV, Gui, Rainbow, MQDSS, TPSig, DualModeMS, HiMQ-3 and GeMSS. These candidates are selected by unconditional private and integral unconditional criterion for cryptographic resistance to attack based on adaptive selection of messages.

Key words: asymmetric key, asymmetric crypto-transformations, multidimensional transformations, electronic signature, quadratic fields, post-quantum electronic signatures.

3 tab. 9 fig. Ref.: 14 items.

УДК 004.056.55

Сравнительные исследования и анализ эффективности гибридной кодовой криптосистемы / *А.А. Кузнецов, Ю.И. Горбенко, А.С. Киян, А.А. Уварова, Т.Ю. Кузнецова* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2018. – Вып. 195. – С. 61 – 69.

Рассмотрены основные принципы построения и функционирования криптосистем Мак-Элиса и Нидеррайтера, в основе которых лежит использование кодов. Предложена новая гибридная криптосистема, которая объединяет принципы шифрования согласно упомянутым схемам. Также осуществлено анализ и сравнительные исследования с точки зрения стойкости, объема ключевых данных и относительной скорости передачи информации новой схемы и криптосистем Мак-Элиса и Нидеррайтера, который представлен как в аналитическом виде, так и с помощью графического изображения. В ходе сравнительных исследований выявлено, что гибридная криптосистема сохраняет позитивные аспекты своих предшественников, а также позволяет увеличить относительную скорость передачи с одновременным сохранением показателей стойкости к классическому и квантовому криптоанализу, однако, к сожалению, до сих пор сохраняется одно важное ограничение- большие объемы необходимых ключевых данных.

Ключевые слова: алгебраические коды; криптография на основе кодов; криптосистема Мак-Элиса; криптосистема Нидеррайтера; криптосистема с открытым ключом; пост-квантовая криптосистема.

Табл. 2. Іл. 4. Бібліогр.: 20 назв.

УДК 004.056.55

Порівняльні дослідження та аналіз ефективності гібридної кодової криптосистеми / *О.О. Кузнецов, Ю.І. Горбенко, А.С. Кіян, А.О. Уварова, Т.Ю. Кузнецова* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. – Вип. 195. – С. 61 – 69.

Розглянуто основні принципи побудови та функціонування криптосистем Мак-Еліса і Нідеррайтера, в основі яких лежить використання кодів. Запропоновано нову гібридну криптосистему, що поєднує принципи зашифрування згідно зі згаданими схемами. Здійснено аналіз та порівняльні дослідження з точки зору стійкості, обсягу ключових параметрів, довжини шифртексту і відносної швидкості передачі інформації нової схеми і криптосистем Мак-Еліса та Нідеррайтера, що представлено в аналітичному вигляді та за допомогою графічного зображення. У ході порівняльних досліджень виявлено, що гібридна криптосистема зберігає позитивні аспекти своїх попередників, а також дозволяє збільшити відносну швидкість передачі зі збереженням показника стійкості до класичного та квантового криптоаналізу, однак, на жаль, досі зберігається важливе обмеження - великі розміри необхідних ключових даних.

Ключові слова: алгебраїчні коди; криптографія на основі кодів; криптосистема Мак-Еліса; криптосистема Нідеррайтера; асиметрична криптосистема; постквантова криптосистема.

Табл. 2. Іл. 4. Бібліогр.: 20 назв.

UDC 004.056.55

Comparative studies and analysis of efficiency code-based hybrid cryptosystem / *A.A. Kuznetsov, Y.I. Gorbenko, A.S. Kiian, A.A. Uvarova, T.Y. Kuznetsova* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2018. – №195. – P. 61 – 69.

The basic principles of construction and operation of McEliece and Niederreiter cryptosystems based on the use of error-correcting codes are considered. A new hybrid cryptosystem, that combines rules of encryption according to the above-mentioned schemes, is proposed. Also, an analysis and comparative studies are carried out in terms of stability, volume of public and private keys, length of ciphertext and relative speed of information transmission of the new proposed scheme and McEliece and Niederreiter cryptosystems presented both in an analytical form and by means of a graphic. Comparative studies revealed that the hybrid cryptosystem retains the positive aspects of its predecessors, as well as allows increase in the relative transmission rate with the preservation of the stability indicator to the classical and quantum cryptanalysis, but, unfortunately, one important limitation is still preserved - a large size of the required key data.

Key words: Algebraic codes; Code-based cryptography; McEliece cryptosystem; Niederreiter cryptosystem; Public-key cryptosystem; Post-quantum cryptosystem.

2 tab. 4 fig. Ref.: 20 items.

УДК 621.394.147

Анализ и исследование свойств алгеброгеометрических кодов / *А.А. Кузнецов, Е.П. Колованова, Д.И. Прокопович-Ткаченко, Т.Ю. Кузнецова* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2018. – Вып. 195. – С. 70 – 88.

Рассматриваются линейные блоковые помехоустойчивые коды, построенные по алгебраическим кривым (алгеброгеометрические коды), оцениваются их конструктивные свойства, изучаются алгоритмы построения и декодирования. Исследуется энергетическая эффективность передачи дискретных сообщений М-ми ортогональными сигналами при применении алгеброгеометрических кодов, оценивается достигаемый энергетический выигрыш от использования помехоустойчивого кодирования. Показано, что в дискретных каналах без памяти удается получить значительный энергетический выигрыш, который возрастает при переходе к длинным алгеброгеометрическим кодам, построенным по кривым с большим числом точек по отношению к роду кривой. Установлено, что вычислительная сложность реализации алгеброгеометрических кодов сопоставима с другими известными помехоустойчивыми кодами, например кодами Рида – Соломона, и др. Таким образом, высокая энергетическая эффективность в сочетании с приемлемой вычислительной сложностью реализации подтверждают перспективность использования алгеброгеометрических кодов в современных телекоммуникационных системах и сетях для повышения помехоустойчивости каналов передачи данных.

Ключевые слова: алгеброгеометрический код, энергетический выигрыш, ортогональный сигнал, помехоустойчивое кодирование.

Табл. 8. Ил. 8. Библиогр.: 11 назв.

УДК 621.394.147

Аналіз і дослідження властивостей алгеброгеометричних кодів / *О.О. Кузнецов, Є.П. Колованова, Д.І. Прокопович-Ткаченко, Т.Ю. Кузнецова* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. – Вип. 195. – С. 70 – 88.

Розглядаються лінійні блокові завадостійкі коди, побудовані по алгебраїчним кривим (алгеброгеометричні коди), оцінюються їх конструктивні властивості, вивчаються алгоритми побудови та декодування. Досліджується енергетична ефективність передачі дискретних повідомлень М-ми ортогональними сигналами при застосуванні алгеброгеометричних кодів, оцінюється енергетичний виграш від використання завадостійкого кодування. Показано, що в дискретних каналах без пам'яті вдається отримати значний енергетичний виграш, який зростає при переході до довгих алгеброгеометричних кодів, побудованих за кривими з великим числом точок по відношенню до роду кривої. Встановлено, що обчислювальна складність реалізації алгеброгеометричних кодів порівнянна з іншими відомими завадостійкими кодами, наприклад кодами Ріда – Соломона, та ін. Таким чином, висока енергетична ефективність в поєднанні з прийнятною обчислювальною складністю реалізації підтверджують перспективність використання алгеброгеометричних кодів в сучасних телекомунікаційних системах і мережах для підвищення завадостійкості каналів передачі даних.

Ключові слова: алгеброгеометричний код, енергетичний виграш, ортогональний сигнал, завадостійке кодування.

Табл. 8. Іл. 8. Бібліогр.: 11 назв.

UDC 621.394.147

Analysis and investigation of algebraic geometric codes properties / *A.A. Kuznetsov, I.P. Kolovanova, D.I. Prokopovych-Tkachenko, T.Y. Kuznetsova* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2018. – №195. – P. 70 – 88.

Linear block noise-proof codes constructed according to algebraic curves (algebraic geometric codes) are considered, their design properties are evaluated, algorithms of construction and decoding are studied. The energy efficiency of the transmission of discrete messages by M-ary orthogonal signals in the application of algebraic geometric codes is studied; the achievable energy gain from the use of noise-immune coding is estimated. It is shown that in discrete channels without memory it is possible to obtain a significant energy gain, which increases with the transition to long algebraic geometric codes constructed by curves with a large number of points with respect to the genus of the curve. It is established that the computational complexity of implementing algebraic geometric codes is comparable to other known noise-resistant codes, for example, Reed-Solomon codes and others. Thus, high energy efficiency in combination with acceptable computational complexity of implementation confirm the prospects of algebraic geometric codes using in modern telecommunication systems and networks to improve the noise immunity of data transmission channels.

Keywords: algebraic geometric code, energy gain, orthogonal signal, noise-immune coding

8 tab. 8 fig. Ref.: 11 items.

УДК 519.2: 519.7: 003.026

Сущность и особенности реализации метода Гровера на классическом компьютере для симметричного криптоанализа / *Ю.И. Горбенко, Е.Ю Каптьол* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2018. – Вып. 195. – С. 89 – 100.

Статья посвящена детализации, освоению для применения, проверке криптоаналитических свойств и демонстрации применения метода Гровера при криптоанализе симметричных криптографических преобразований. Приводится суть метода и его детализация с целью реализации квантового алгоритма Гровера на классическом компьютере.

Ключевые слова: метод Гровера, сложность поиска в несортированной базе, примеры поиска на классическом компьютере

Табл. 1. Ил. 1. Библиогр.: 5 назв.

УДК 519.2:519.7 : 003.026

Сутність та особливості реалізації методу Гровера на класичному комп'ютері для симетричного криптоаналізу / *Ю.І. Горбенко, Є.Ю. Каптьол* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. – Вип. 195. – С. 89 – 100.

Стаття присвячена деталізації, засвоєнню для застосування, перевірці криптоаналітичних властивостей та демонстрації застосування методу Гровера при криптоаналізі симетричних криптографічних перетворень. Наводиться сутність методу та його деталізація з метою реалізації квантового алгоритму Гровера на класичному комп'ютері.

Ключові слова: метод Гровера, складність пошуку в несортованій базі, приклади пошуку на класичному комп**'**ютері.

Табл. 1. Іл. 1. Бібліогр.: 5 назв.

UDC 519.2: 519.7: 003.026

Essence and features of Grover's method implementation on a classical computer for symmetric cryptanalysis / *Yu.I. Gorbenko, Ye.Yu Kaptyol* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2018. – №195. – P. 89 – 100.

This paper is devoted to detailing, mastering for use, checking cryptanalytic properties and demonstrating the use of Grover's method for cryptanalysis of symmetric cryptographic transformations. The essence of the method and its refinement are presented in order to implement Grover's quantum algorithm on a classical computer.

Key words: Grover method, search complexity in the unsorted database, examples of search on a classical computer.

1 tab. 1 fig. Ref.: 5 items.

УДК 004.056.5

Комбинирующие и фильтрующие функции на основе регистров сдвига с нелинейными обратными связями / *А.А. Кузнецов, А.В. Потий, Н.А. Полуяненко, С.Г. Вдовенко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2018. – Вып. 195. – С. 101 – 112.

Рассмотрены возможности применения регистров сдвига с нелинейными обратными связями, формирующих последовательность максимального периода, в качестве комбинирующей или фильтрующей функции. Исследованы основные показатели криптографической стойкости таких функций, такие как сбалансированность, наличие запретов, корреляционная иммунность и нелинейность. Проанализированы и приведены экспериментальные значения корреляционной иммунности и нелинейности для всех регистров сдвига с нелинейными обратными связями, формирующие последовательность максимального периода, для размера регистра до шести ячеек включительно, а также регистры с размерностью до девяти ячеек включительно с алгебраической степенью образующего многочлена не выше 2. Изучена возможность оптимизации выбора булевых функций по критериям максимальной корреляционной иммунности и нелинейности при различной алгебраической степени и минимизации количества мономов в образующем полиноме.

Ключевые слова: генераторы псевдослучайных последовательностей; фильтрующие функции; комбинирующие функции; криптографический анализ; нелинейные полиномы.

Табл. 9. Ил. 2. Библиогр.: 13 назв.

УДК 004.056.5

Комбінуючі та фільтруючі функції на основі регістрів зсуву з нелінійними зворотними зв'язками / *О.О. Кузнецов, О.В. Потій, М.О. Полуяненко, С.Г. Вдовенко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. – Вип. 195. – С. 101 – 112.

Розглянуто можливості застосування регістрів зсуву з нелінійними зворотними зв'язками, які формують послідовність максимального періоду, в якості комбінучої або фільтрувальної функції. Досліджено основні показники криптографічного стійкості таких функцій, такі як збалансованість, наявність заборон, кореляційний імунітет і нелінійність. Проаналізовано та наведено експериментальні значення кореляційної імунності та нелінійності для всіх регістрів зсуву з нелінійними зворотними зв'язками, що формують послідовність максимального періоду, для розміру регістра до шести осередків включно, а також регістри з розмірністю до дев’яти осередків включно з алгебраїчним ступенем утворюючого многочлена не вище 2. Вивчено можливість оптимізації вибору булевих функцій за критеріями максимальної кореляційної імунності та нелінійності при різному алгебраїчному ступеню та мінімізації кількості одночленів в утворюючому поліномі.

Ключові слова: генератори псевдовипадкових послідовностей; фільтруючі функції; комбінуючі функції; криптографічний аналіз; нелінійні поліноми.

Табл. 9. Іл. 2. Бібліогр.: 13 назв.

UDC 004.056.5

Combining and filtering functions in the framework of nonlinear-feedback shift register / *A.A. Kuznetsov, A.V. Potii, N.A. Poluyanenko, S.G. Vdovenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2018. – №195. – P. 101 – 112.

Strong cryptography of stream ciphers is determined, among other things, by the ability of a generated pseudorandom sequence to resist analytical attacks. One of the main components of the pseudorandom stream cipher sequence generating algorithm are Boolean functions for combining and filtering. The paper considers the possibility of applying nonlinear-feedback shift registers that generate a maximum length sequence as a combining or filtering function. This work examines the main indicators of cryptographic strength of such functions, as: balance, the prohibitions presence, correlation immunity and nonlinearity. The study analyzes and demonstrates correlation immunity’s and nonlinearity’s experimental values for all nonlinear feedback shift registers, that generate a maximum length sequence, for register sizes up to 6 cells inclusively, and registers sizes up to 9 cells inclusively with algebraic degree of the polynomial under 2. The possibility of optimizing the process of selecting Boolean functions according to the criteria of maximum correlation immunity and nonlinearity with various algebraic degree and minimization of the number of monomials in the polynomial are studied.

Key words: generators of the pseudorandom sequence; filtering function; combining function; cryptanalysis; nonlinear polynomials

9 tab. 2 fig. Ref.: 13 items.

УДК 621.3.06

Оценка стойкости симметричного блочного шифра «Кипарис» к дифференциальному криптоанализу / *М.Ю. Родинко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2018. – Вып. 195. – С. 113 – 124.

Представлена оценка практической стойкости малоресурсного блочного шифра «Кипарис» к дифференциальному криптоанализу, которая определяется вероятностью лучшей найденной дифференциальной характеристики. Предложена математическая модель оценки стойкости блочного шифра «Кипарис» к дифференциальному криптоанализу и методы поиска многоцикловых дифференциальных характеристик. В основе первого метода лежит комбинирование высоковероятностных одноциклових дифференциальных характеристик в многоцикловые, в основе второго - продолжение одноциклових характеристик на несколько циклов. В результате применения второго метода поиска к блочному шифру «Кипарис-256» найдена дифференциальная характеристика для шести циклов шифрования. Поскольку больше, чем для шести циклов шифрования дифференциальных характеристик с вероятностью выше вероятности атаки полного перебора, не найдено, блочный шифр «Кипарис-256» является практически стойким к дифференциальному криптоанализу.

Ключевые слова: дифференциальный криптоанализ, дифференциальная характеристика, симметричный блочный шифр, малоресурсная криптография.

Табл. 6. Ил. 2. Библиогр: 17 назв.

УДК 621.3.06

Оцінка стійкості симетричного блокового шифру «Кипарис» до диференційного криптоаналізу / *М.Ю. Родінко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. – Вип. 195. – С. 113 – 124.

Представлено оцінку практичної стійкості малоресурсного блокового шифру «Кипарис» до диференційного криптоаналізу, що визначається ймовірністю кращої знайденої диференційної характеристики. Запропоновано математичну модель оцінки стійкості блокового шифру «Кипарис» до диференційного криптоаналізу та методи пошуку багатоциклових диференційних характеристик. В основі першого методу лежить комбінування високоймовірнісних одноциклових диференційних характеристик у багатоциклові, в основі другого – продовження одноциклових характеристик на декілька циклів. В результаті застосування другого методу пошуку до блокового шифру «Кипарис-256» знайдено диференційну характеристику для шести циклів шифрування. Оскільки більше, ніж для шести циклів шифрування не знайдено диференційних характеристик з ймовірністю вищою за ймовірність атаки повного перебирання, блоковий шифр «Кипарис-256» є практично стійким до диференційного криптоаналізу.

*Ключові слова:*диференційний криптоаналіз, диференційна характеристика, симетричний блоковий шифр, малоресурсна криптографія.

Табл. 6. Іл. 2. Бібліогр: 17 назв.

UDC 621.3.06

Evaluation of block cipher “Cypress” strength against differential cryptanalysis / *M.Yu. Rodinko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2018. – №195. – P. 113 – 124.

This paper presents an evaluation of the practical strength of the lightweight block cipher “Cypress” to the differential cryptanalysis, which is determined by the probability of the best found differential characteristic. The paper proposes a mathematical model for evaluating the block cipher “Cypress” to differential cryptanalysis and methods for searching for multi-round differential characteristics. The first method is based on the combination of highly probable one-round differential characteristics into multi-round ones, while the second method is based on the extension of one-round characteristics for several rounds. As a result of the application of the second search method to the block cipher Cypress-256, a 6-round differential characteristic was found. Since it was not found a differential characteristics for more than six rounds with a probability which is higher than the probability of a brute-force attack, the block cipher Cypress-256 is practically resistant to differential cryptanalysis.

Key words: differential cryptanalysis, differential characteristic, block cipher, lightweight cryptography.

6 tab. 2 fig. Ref.: 17 items.

УДК 004.056.5

Нелинейные функции усложнения для потоковых симметричных шифров / *А.А. Кузнецов, А.В. Потий, Н.А. Полуяненко, И.В. Стельник* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2018. – Вып. 195. – С. 125 – 137.

Нелинейные булевы функции исследуются по всему миру очень активно. Тем не менее, в этой области остается множество открытых вопросов. Теория нелинейных булевых функций, пригодных для использования в криптографических стойких алгоритмах, в значительной степени неполна. Несмотря на наличие многочисленных публикаций на эти темы, многие вопросы, связанные с взаимосвязью конструктивных характеристик, влияющей на производительность генератора и его криптографические характеристики, пока ещё остаются открытыми. Генерация особого типа последовательностей, называемых последовательностями де Брейна, с минимальными аппаратно-программными затратами, обоснование возможности их применения в качестве нелинейных функций усложнения системах поточного шифрования, является главной темой работы. Приведены оценки криптографических показателей нелинейных функций усложнения итеративных генераторов битовых последовательностей при различных характеристиках формируемой последовательности, таких как линейная сложность и автокорреляция.

Ключевые слова: генераторы псевдослучайных последовательностей; последовательность де Брейна; криптографический анализ; булевы функции; нелинейные функции усложнения.

Табл. 13. Ил. 2. Библиогр.: 25 назв.

УДК 004.056.5

Комбінуючі та фільтруючі функції на основі регістрів зсуву з нелінійними зворотними зв’язками / *О.О. Кузнецов, О.В. Потій, М.О. Полуяненко, І.В. Стєльнік* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. – Вип. 195. – С. 125 – 137.

Нелінійні булеві функції досліджуються по всьому світу дуже активно. Проте, в цій області залишається безліч відкритих питань. Теорія нелінійних булевих функцій, придатних для використання в криптографічно стійких алгоритмах, в значній мірі неповна. Незважаючи на наявність численних

публікацій на ці теми, багато питань, пов'язаних з взаємозв'язком конструктивних характеристик, що впливає на продуктивність генератора і його криптографічних характеристик, поки ще залишаються відкритими. Генерація особливого типу послідовностей, званих послідовностями де Брейна, з мінімальними апаратно-програмними витратами, обґрунтування можливості їх застосування в якості нелінійних функцій ускладнення системах потокового шифрування, є головною темою роботи. В роботі наведено оцінки криптографічних показників нелінійних функцій ускладнення ітеративних генераторів бітових послідовностей при різних характеристиках формованої послідовності, таких як лінійна складність і автокореляція.

Ключові слова: генератори псевдовипадкових послідовностей; послідовність де Брейна; криптографічний аналіз; булеві функції; нелінійні функції ускладнення.

Табл. 13. Іл. 2. Бібліогр.:25 назв.

UDC 004.056.5

Combining and filtering functions in the framework of nonlinear-feedback shift register / *A.A. Kuznetsov, A.V. Potii, N.A. Poluyanenko, I.V. Stelnik* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2018. – №195. – P. 125 – 137.

Currently, nonlinear Boolean functions are being investigated very actively around the world. However, many open questions remain in this area. The theory of nonlinear Boolean functions suitable for use in robust cryptographic algorithms is largely incomplete. Despite the presence of numerous publications on these topics, many issues related to the interrelation of design characteristics affecting the performance of the generator and its cryptographic characteristics are still open. The generation of a special type of sequences, called de Brain sequences, with minimal hardware and software costs, the rationale for their use as non-linear functions of the complexity of stream encryption systems, is the main theme of this work. The paper presents estimates of cryptographic indicators of nonlinear complexity functions of iterative bit sequence generators with various characteristics of the generated sequence, such as linear complexity and autocorrelation.

Keywords: pseudo-random sequence generators; de Brain sequence; cryptographic analysis; Boolean functions; nonlinear complication functions

13 tab. 2 fig. Ref.: 25 items.

МЕТОДЫ И АЛГОРИТМЫ ЗАЩИТЫ И СОКРЫТИЯ ИНФОРМАЦИИ
МЕТОДИ ТА АЛГОРИТМИ ЗАХИСТУ ТА ПРИХОВУВАННЯ ІНФОРМАЦІЇ
METHODS AND ALGORITHMS FOR PROTECTION AND CONCEALING INFORMATION

УДК 004.056.5

Средства моделирования и анализа рисков в среде облачных вычислений / *И.Ф. Аулов, К.Е. Лисицкий* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2018. – Вып. 195. – С. 138 – 143.

Статья посвящена средствам, которые могут применяться для моделирования и анализа рисков в среде облачных вычислений. Рассматривается бесплатное программное обеспечение с открытым кодом: OWASP Threat Dragon, CAIRIS, Mozilla Seasponge и коммерческое с закрытым кодом: Microsoft Threat Modeling Tool, RiskWatch, vsRisk, а также анализируются его преимущества и недостатки. Предложены требования к программам моделирования и анализа рисков в среде облачных вычислений. На основе оценки соответствия предъявляемым требованиям было выполнено сравнение существующего программного обеспечения в результате которого было определено, что хотя Microsoft Threat Modeling Tool не в полной мере им соответствует, но в данный момент является лучшей для моделирования и анализа рисков в облаках.

Ключевые слова: моделирование угроз, облачные вычисления, анализ рисков.

Табл. 1. Библиогр.: 10 назв.

УДК 004.056.5

Засоби моделювання та аналізу ризиків в середовищі хмарних обчислень / *І.Ф. Аулов, К.Є. Лисицкий* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. – Вип. 195. – С. 138 – 143.

Стаття присвячена засобам, що можуть застосовуватися для моделювання та аналізу ризиків в середовищі хмарних обчислень. Розглядається безкоштовне програмне забезпечення з відкритим кодом: OWASP Threat Dragon, CAIRIS, Mozilla Seasponge та комерційне з закритим програмним кодом: Microsoft Threat Modeling Tool, RiskWatch, vsRisk, а також аналізуються його перевагм та недоліки. Запропоновано вимоги до програм моделювання та аналізу ризиків в середовищі хмарних обчислень. На основі оцінки відповідності висунутим вимогам було виконано порівняння існуючого програмного забезпечення в результаті якого було визначено, що хоча Microsoft Threat Modeling Tool не в повній мірі їм відповідає, але наразі є найкращою для моделювання та аналізу ризиків в хмарах.

Ключові слова: моделювання загроз, хмарні обчислення, аналіз ризиків.

Табл. 1. Бібліогр.: 10 назв.

UDC 004.056.5

Tools for modeling and analysis of risks in the cloud computing environment / *I.F. Aulov, K.E. Lisickiy* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2018. – №195. – P. 138 – 143.

This article focuses on tools that can be used to model and analyze risks in a cloud computing environment. The article discusses free open source software: OWASP Threat Dragon, CAIRIS, Mozilla Seasponge and commercial with closed code: Microsoft Threat Modeling Tool, RiskWatch, vsRisk, as well as an analysis of its advantages and disadvantages. The article proposes requirements for modeling programs and risk analysis in the cloud computing environment. Based on the compliance assessment, a comparison was made of existing software, which resulted in the determination that although the Microsoft Threat Modeling Tool does not fully comply with them, it is currently the best for modeling and analyzing risks in the clouds.

Key words: threat modeling, cloud computing, risk analysis.

1 table. Ref.: 10 items.

УДК 621.391:519.2

Исследование *k*-мерности булевой функции шифра LILI-128 / *С.Н. Конюшок* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2018. – Вып. 195. – С. 144 – 149.

Представлены результаты экспериментального исследования *k*-мерности булевой функции шифра LILI-128, которые продемонстрировали потенциальную возможность реализации статистической атаки, основанной на приближении булевых функций алгебраически вырожденными функциями.

Ключевые слова: криптографические свойства булевых функций, k-мерная функция, вероятностный алгоритм, усовершенствованный тест k-мерности, шифр LILI-128.

Табл. 1. Ил. 1. Библиогр.: 23 назв.

УДК 621.391:519.2

Дослідження *k*-вимірності булевої функції шифру LILI-128 / *С.М. Конюшок* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. – Вип. 195. – С. 144 – 149.

Представлено результати експериментального дослідження *k*-вимірності булевої функції шифру LILI-128, що продемонстрували потенційну можливість реалізації статистичної атаки, яка базується на наближенні булевих функцій алгебраїчно виродженими функціями.

Ключові слова: криптографічні властивості булевих функцій, k-вимірна функція, імовірнісний алгоритм, вдосконалений тест k-вимірності, шифр LILI-128.

Табл. 1. Іл. 1. Бібліогр.: 23 назви.

UDC 621.391:519.2

Investigation of the k-dimensionality of the LILI-128 cipher Boolean function / *S.M. Koniushok* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2018. – №195. – P. 144 – 149.

The paper presents results of the experimental study of the k-dimensionality of the LILI-128 cipher Boolean function, which demonstrated the potential for the realization of a statistical attack based on near-proximity of Boolean functions with algebraically degenerate functions.

Keywords: cryptographic properties of boolean functions, k-dimensional function, probabilistic algorithm, improved k-dimensional test, LILI-128 cipher.

1 tab. 1 fig. Ref.: 23 items.

УДК 004.056.5

Эвристические методы градиентного поиска криптографических булевых функций / *А.А. Кузнецов, И.В. Московченко, Д.И. Прокопович-Ткаченко, Т.Ю. Кузнецова* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2018. – Вып. 195. – С. 150 – 164.

Рассматриваются эвристические методы градиентного поиска криптографических булевых функций, удовлетворяющих требуемым свойствам сбалансированности, нелинейности, автокорреляции и др. показателям стойкости. Исследуется предложенный метод градиентного спуска, в частности приводятся оценки нелинейности и корреляционной иммунности синтезируемых булевых функций. Предлагается методика оценки вычислительной эффективности методов градиентного поиска, основанная на построении выборочных (эмпирических) функций распределения, характеризующих вероятность формирования булевых функций с показателями стойкости не ниже требуемых. В качестве показателя вычислительной эффективности предлагается среднее число попыток, которое по-

требуется выполнить с использованием эвристического метода, для формирования криптографической булевой функции с требуемыми свойствами. Приводятся сравнительные оценки эффективности рассмотренных эвристических методов. Показано, что предложенный метод градиентного спуска позволяет формировать криптографические функции с требуемыми показателями стойкости за меньшее число шагов. Приводятся результаты исследований криптографических свойств формируемых булевых функций в сравнении с наилучшими известными оценками.

Ключевые слова: симметричная криптография; нелинейные блоки замен; булевы функции; сбалансированность, нелинейность, автокорреляция.

Табл. 6. Ил. 10. Библиогр.: 40 назв.

УДК 004.056.5

Евристичні методи градієнтного пошуку криптографічних булевих функцій / *О.О. Кузнецов, І.В. Московченко, Д.І. Прокопович-Ткаченко, Т.Ю. Кузнецова* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. – Вип. 195. – С. 150 – 164.

Розглядаються евристичні методи градієнтного пошуку криптографічних булевих функцій, що задовольняють необхідним властивостям збалансованості, нелінійності, автокореляції та ін. показникам стійкості. Досліджується запропонований метод градієнтного спуску, зокрема наводяться оцінки нелінійності і кореляційної імунності синтезованих булевих функцій. Пропонується методика оцінки обчислювальної ефективності методів градієнтного пошуку, заснована на побудові вибіркових (емпіричних) функцій розподілу, що характеризують ймовірність формування булевих функцій з показниками стійкості не нижче необхідних. Як показник обчислювальної ефективності пропонується середнє число спроб, яке буде потрібно виконати з використанням евристичного методу, для формування криптографічної булевої функції з необхідними властивостями. Наводяться порівняльні оцінки ефективності розглянутих евристичних методів. Показано, що запропонований метод градієнтного спуску дозволяє формувати криптографічні функції з необхідними показниками стійкості за менше число кроків. Наводяться результати досліджень криптографічних властивостей формованих булевих функцій в порівнянні з найкращими відомими оцінками.

Ключові слова: симетрична криптографія; нелінійні блоки замін; булеві функції; збалансованість, нелінійність, автокореляція.

Табл. 6. Іл. 10. Бібліогр.:40 назв.

UDC 004.056.5

Heuristic methods for gradient search of cryptographic Boolean functions / *A.A. Kuznetsov, I.V. Moskovchenko, D.I. Prokopovych-Tkachenko, T.Y. Kuznetsova* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2018. – №195. – P. 150 – 164.

Heuristic methods of gradient search of cryptographic Boolean functions that satisfy the required properties of balance, nonlinearity, autocorrelation, and other stability indicators are considered. The proposed method of gradient descent is investigated, in particular, estimates of nonlinearity and correlation immunity of the synthesized Boolean functions are given. A method for evaluating the computational efficiency of gradient search methods is proposed, based on the construction of sample (empirical) distribution functions, which characterize the probability of the formation of Boolean functions with persistence indicators not lower than those required. As an indicator of computational efficiency, we propose the average number of attempts that need to be performed using the heuristic method to form a cryptographic Boolean function with the required properties. It is shown that the proposed gradient descent method allows the formation of cryptographic functions with the required durability indicators in fewer steps. The results of investigations of the cryptographic properties of the formed Boolean functions in comparison with the best known assessments are given.

Keywords: heuristic methods, cryptographic Boolean functions, symmetric cryptography, nonlinear substitute blocks

6 tab. 10 fig. Ref.: 40 items.

УДК 004.056.5

Стеганоанализ цифровых изображений в условиях различной степени наполненности контентов / *А.В. Ахмаметьева, Мпуту Кристофер Бвабва* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2018. – Вып. 195. – С. 165 – 173.

Предложено усовершенствование стеганоаналитического метода выявления вложений дополнительной информации в цветные цифровые изображения, основанного на учёте последовательных триад триплетов в матрице уникальных цветов и показавшего высокую эффективность выявления стеганосообщений, сформированных при условии заполнения только одной цветовой составляющей контейнера. Однако в процессе стеганопреобразования возможны случаи погружения конфиденци-

альных данных в две и три цветовые составляющие изображений, что обеспечивает сокрытие большего объёма информации и требует доработки существующего метода стеганоанализа. В ходе проведенных исследований проанализирован характер возмущений количества средних триплетов в матрице уникальных цветов в результате погружения дополнительной информации в две и три цветовые составляющие изображений, изначально хранимых в формате с потерями, а также с учётом полученных результатов уточнены параметры оригинального метода выявления стеганосообщений. Установлено, что характер изменений количества последовательных триад триплетов в результате стеганопреобразования отличается в случаях использования контейнеров в формате с потерями и контейнеров в формате без потерь. На основании полученных данных проведено усовершенствование стеганоаналитического метода путём интеграции его с методом выявления факта сжатия цифровых контентов, разработанного ранее. По результатам вычислительных экспериментов разработанный метод обеспечивает высокую эффективность при выявлении стеганосообщений, сформированных с разной степенью наполненности контейнеров, не снижая при этом правильность выявления заполненных цветовых составляющих, если дополнительная информации погружалась только в одну цветовую составляющую цифровых изображений. Разработанный метод может использоваться как основа для комплексного стеганоанализа цифровых контентов с применением существующих методов, анализирующих отдельные цветовые матрицы изображений.

Ключевые слова: стеганоанализ, цифровое изображение, последовательные триады триплетов, пространственная область, формат с потерями, формат без потерь.

Табл. 3. Ил. 1. Библиогр. 12 назв.

УДК 004.056.5

Стеганоаналіз цифрових зображень в умовах різного ступеню наповненості контентів / *Г.В. Ахмаметьєва, Мпуту Крістофер Бвабва //* Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. – Вип. 195. – С. 165 – 173.

Запропоновано удосконалення стеганоаналітичного методу виявлення вкладень додаткової інформації в кольорові цифрові зображення, заснованого на врахуванні послідовних тріад триплетів в матриці унікальних кольорів, який показав високу ефективність виявлення стеганоповідомлень, сформованих за умови заповнення тільки однієї колірної складової контейнера. Однак в процесі стеганоперетворення можливі випадки вбудови конфіденційних даних в дві або три колірні складові зображень, що забезпечує приховування більшого обсягу інформації і вимагає доопрацювання існуючого методу стеганоаналізу. В ході проведених досліджень проаналізовано характер збурень кількості середніх триплетів в матриці унікальних кольорів в результаті вбудови додаткової інформації в дві і три колірні складові зображень, спочатку збережених в форматі з втратами, а також з урахуванням отриманих результатів уточнені параметри оригінального методу виявлення стеганоповідомлень. Встановлено, що характер змін кількості послідовних тріад триплетів в результаті стеганоперетворення відрізняється у випадках використання контейнерів в форматі з втратами і контейнерів в форматі без втрат. На підставі отриманих даних проведено удосконалення стеганоаналітичного методу шляхом інтеграції його з методом виявлення факту стиску цифрових контентів, розробленого раніше. За результатами обчислювальних експериментів розроблений метод забезпечує високу ефективність при виявленні стеганоповідомлень, сформованих з різним ступенем наповненості контейнерів, не знижуючи при цьому правильність виявлення заповнених колірних складових, якщо додаткова інформації була вбудована тільки в одну колірну складову цифрових зображень. Розроблений метод може використовуватися як основа для комплексного стеганоаналізу цифрових контентів із застосуванням існуючих методів, які аналізують окремі колірні матриці зображень.

Ключові слова: стеганоаналіз, цифрове зображення, послідовні тріади триплетів, просторова область, формат з втратами, формат без втрат

Табл. 3. Іл. 1. Бібліогр. 12 назв.

UDC 004.056.5

Steganalysis of digital images in conditions of varying degrees of contents fullness / *Anna V. Akhmametieva, Mputu Chrisopher Bwabwa //* Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2018. – №195. – P. 165 – 173.

An improvement of the steganalytic method for detection of the presence of additional information in color digital images which showed high efficiency in identifying stego formed by embedding of secret data only into one color component of the container is presented. The proposed method analyses digital image in the spatial domain and is based on the accounting of sequential color triads in the matrix of unique colors of the digital content. However, in the process of steganographic transformation cases of embedding of confidential data into two and three color components of images are possible that ensures the concealment of a

larger amount of information and requires the improvement of the existing method of steganalysis. In the course of the conducted research the character of perturbations in the quantity of sequential triads of triplets in a matrix of unique colors as a result of embedding of additional information into two and three color components of images originally stored in a losses format was analyzed. Considering obtained results the parameters of the original method for detecting of stego was refined. It has been established that the character of changes in the quantity of sequential triads of triplets as a result of steganographic transformation is different in cases of using containers in a losses format and containers in a lossless format. Based on the obtained data the steganalytic method has been improved by integrating it with the method of detection the fact of compression of digital content developed earlier. The developed method provides high efficiency in detecting stego formed with different degree of container fullness without reducing the accuracy of identifying the filled color components if the additional information was embedded into only one color component of the digital images. This method can be used as a basis for complex steganalysis of digital contents by using existing methods that analyzes color matrixes of images separately.

Keywords: steganalysis, digital image, sequential triads of triplets, spatial domain, losses format, lossless format

3 tab. 1 fig. Ref.: 12 items.

УДК 004.043

Сравнительный анализ алгоритмов консенсуса для технологии распределенных реестров / *Д.Г. Биличенко, Е.Ю. Витюк, Р.В. Олейников* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2018. – Вып. 195. – С. 174 – 183.

Приведена сравнительная характеристика алгоритмов достижения консенсуса в распределенных реестрах, основанных на разных технологиях, таких как блокчейн и направленный ациклический граф. Приведены преимущества и недостатки алгоритмов консенсуса GHOST, Tangle и Hashgraph, а также рекомендации по выбору оптимального варианта.

Ключевые слова: блокчейн, алгоритм консенсуса, GHOST, Tangle, Hashgraph.

Табл. 1. Ил. 5. Библиогр.: 14 назв.

УДК 004.043

Порівняльний аналіз алгоритмів консенсусу для технології розподілених реєстрів / *Д.Г. Біліченко, К.Ю. Вітюк, Р.В. Олійников* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. – Вип. 195. – С. 174 – 183.

Наведено порівняльну характеристику алгоритмів досягнення консенсусу в розподілених реєстрах, які засновані на різних технологіях, таких як блокчейн та направлений ациклічний граф. Наведені переваги та недоліки алгоритмів коненсусу GHOST, Tangle и Hashgraph, а також рекомедації щодо вибору оптимального варіанту.

Ключові слова: блокчейн, алгоритм консенсусу, GHOST, Tangle и Hashgraph.

Табл. 1. Іл. 5. Бібліогр.: 14 назв.

UDC 004.043

Comparative analysis of consensus algorithms for distributed ledger technologies / *D. Bilichenko, K. Vitiuk, R. Oliynykov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2018. – №195. – P. 174 – 183.

The comparative characteristic of consensus algorithms in distributed ledgers based on different technologies such as blockchain and directed acyclic graph is given in the article. Advantages and disadvantages of GHOST, Tangle and Hashgraph consensus algorithms are given, as well as recommendations of optimal variant selection.

Keywords: blockchain, consensus algorithm, GHOST, Tangle, Hashgraph.

1 Tab. 5. Fig. Ref.: 14 items.

УДК 004.652: 004.658.3

Метод разработки баз данных, легко адаптируемых к изменениям в предметной области / *В.И. Есин, В.В. Вилигура* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2018. – Вып. 195. – С. 184 – 192.

Предлагается метод разработки реляционных баз данных с инвариантной к предметным областям схемой, применение которого в отличие от традиционной технологии проектирования позволяет: создавать в процессе реинжиниринга отвечающие требованиям потребителей информационного продукта базы данных для различных моделируемых предметных областей при меньших временных и

финансовых затратах; адаптировать реляционные БД, построенные на основе схемы с универсальным базисом отношений, к динамичным изменениям предметных областей, без изменения схемы БД, за счет использования созданной предопределенной структуры базовых отношений.

Ключевые слова: база данных, реляционная база данных, схема базы данных, модель данных, модель данных с универсальным базисом отношений, модель данных «объект-событие».

Ил. 3. Библиогр.: 56 назв.

УДК 004.652: 004.658.3

Метод розробки баз даних, що легко адаптуються до змін в предметній області / *В.І. Єсін, В.В. Вілігура* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. – Вип. 195. – С. 184 – 192.

Пропонується метод розробки реляційних баз даних з інваріантної до предметних областей схемою, застосування якого на відміну від традиційної технології проектування дозволяє: створювати в процесі реінжинірингу бази даних для різних модельованих предметних областей, що відповідають вимогам споживачів інформаційного продукту, при менших часових і фінансових витратах; адаптувати реляційні БД, побудовані на основі схеми з універсальним базисом відношень, до динамічних змін предметних областей, без зміни схеми БД, за рахунок використання створеної зумовленої структури базових відношень.

Ключові слова: база даних, реляційна база даних, схема бази даних, модель даних, модель даних з універсальним базисом відношень, модель даних «об'єкт-подія».

Іл. 3. Бібліогр.: 56 назв.

UDC 004.652: 004.658.3

Method for developing databases being easily adaptable to changes in the subject domain / *V.I. Yesin, V.V. Vilihura* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2018. – №195. – P. 184 – 192.

A method for developing relational databases with the schema invariant to subject domains is proposed. The use of this method unlike the traditional technology of designing relational databases allows: creating databases for various simulated subject domains that meet the requirements of consumers of the information product in the process of reengineering, with less time and financial costs; adapting relational databases built on the basis of a scheme with a universal basis of relations to dynamic changes in subject domains, without changing the database schema, due to the use of the created predetermined structure of basic relations.

Key words: database, relational database, database schema, data model, data model with an universal basis of relations, "object-event" data model.

3 fig. Ref.: 56 items.

УДК 004.056.5

3D стеганографическое сокрытие информации / *А.А. Кузнецов, О.О. Стефанович, Д.И. Прокопович-Ткаченко, Е.А. Кузнецова* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2018. – Вып. 195. – С. 193 – 202.

Исследовано новое направление технической стеганографии, связанное с сокрытием информационных данных в процессе послойного создания (выращивания) твердотельного объекта при использовании различных технологий 3D-печати. Информационные данные преобразуются в цифровую 3D-модель элементарных физических объектов, которые размещаются внутри 3D-модели изделия-контейнера. После распечатки твердый объект физически содержит скрытую информацию, которую невозможно удалить или исказить без повреждения контейнера. Кроме того, применяемые методы не снижают эксплуатационных, эстетических и любых других свойств готового изделия, поскольку технологии, применяемые для нанесения слоев, не модифицируются, сокрытие является инвариантным к способу послойного выращивания, то есть могут применяться различные устройства 3D-печати с любыми материалами и принципами послойного создания.

Ключевые слова: стеганография; 3D-принтер; сокрытие информационных данных; 3D-модель; лазерные сканеры.

Табл. 2. Ил. 9. Библиогр.: 17 назв.

УДК 004.056.5

3D стеганографічне приховування інформації / *О.О. Кузнецов, О.О. Стефанович, Д.И. Прокопович-Ткаченко, К.О. Кузнецова* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. – Вип. 195. – С. 193 – 202.

Досліджено новий напрямок технічної стеганографії, який пов'язаний із приховуванням інформаційних даних в процесі пошарового створення (вирощування) твердотільного об'єкта при використанні різних технологій 3D-друку. Інформаційні дані перетворюються в цифрову 3D-модель елемен-

тарних фізичних об’єктів, які розміщуються всередині 3D-моделі виробу-контейнеру. Після роздрукування твердий об'єкт фізично містить приховану інформацію, яку неможливо видалити або спотворити без пошкодження контейнеру. Крім того, застосовані методи не знижують експлуатаційних, естетичних та будь яких інших властивостей готового виробу, оскільки технології, що застосовуються для нанесення шарів, не модифікуються, приховування є інваріантним способу пошарового вирощування, тобто можуть застосовуватися різні пристрої 3D-друку з будь-якими матеріалами і принципами пошарового створення.

Ключові слова: стеганографія; 3D-друк; приховування інформаційних даних; 3D-модель; лазерні сканери.

Табл. 2. Іл. 9. Бібліогр.:17 назв.

UDC 004.056.5

3D steganography hiding of information / *A.A. Kuznetsov, O.O. Stefanovych, D.I. Prokopovych-Tkachenko, K.O. Kuznetsova* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2018. – №195. – P. 193 – 202.

A new direction of technical steganography related to the concealment of information in the process of layer-by-layer creation (cultivation) of a solid-state object using various 3D-printing technologies is investigated. Information data are converted into a digital 3D-model of elementary physical objects that are placed inside this 3D-model of the container product. After printing, a solid object physically contains the hidden information that cannot be deleted or distorted without damaging the container product. In addition, the applied methods do not reduce the operational, aesthetic and any other properties of the finished product. The proposed complex is invariant to the method of layer-by-layer growing, that is, it can be equipped with any peripheral devices of 3D-printing of various manufacturers with any materials and principles of layer-by-layer creation.

Keywords: steganography; 3D-printing; hiding information data; 3D-model; laser scanners

2 tab. 9 fig. Ref.: 17 items.

УДК 004.056

Децентрализованные протоколы консенсуса: возможности и рекомендации по применению / *Е.В. Исирова, А.В. Потий* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2018. – Вып. 195. – С. 203 – 208.

Освещены проблемные вопросы построения централизованных систем. Предложено проектирование децентрализованных систем, в том числе для критических инфраструктур. Проведен сравнительный анализ существующих децентрализованных протоколов консенсуса и даны рекомендации по их применению.

Ключевые слова: децентрализованные системы, технология blockchain, протоколы консенсуса, PoW протоколы, PoS протоколы, BFT протоколы.

Табл. 2. Ил. 3. Библиогр.: 12 назв.

УДК 004.056

Децентралізовані протоколи консенсусу: можливості та рекомендації щодо використання / *К.В. Ісірова, О.В. Потій* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. – Вип. 195. – С. 203 – 208.

Висвітлено проблемні питання побудови централізованих систем. Запропоноване проектування децентралізованих систем в тому числі для критичної інфраструктури. Проведений аналіз існуючих децентралізованих протоколів консенсусу та надані рекомендації щодо їх застосування.

Ключові слова: децентралізовані системи, технологія blockchain, протоколи консенсусу, PoW протоколи, PoS протоколи, BFT протоколи.

Табл. 2. Іл. 3. Бібліогр .: 12 назв.

UDK 004.056

Decentralized consensus protocols: possibilities and recommendations for use / *K.V. Isirova, O.V. Potii* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2018. – №195. – P. 203 – 208.

Centralised systems development problematic issues are described. Decentralized systems development including for critical infrastructures is proposed. Existing decentralized consensus protocols comparative analysis is carried out and recommendations for their use are proposed.

Key words: decentralized systems, blockchain technology, consensus protocols, PoW protocols, PoS protocols, BFT protocols.

2 tab. 3 fig. Ref.: 12 items.

МЕТОДЫ ВЫЯВЛЕНИЯ, РАСПОЗНАВАНИЯ И УПРАВЛЕНИЯ ЛЕТАТЕЛЬНЫМИ АППАРАТАМИ
МЕТОДИ ВИЯВЛЕННЯ, РОЗПІЗНАВАННЯ ТА УПРАВЛІННЯ ЛІТАЛЬНИМИ АПАРАТАМИ
METHODS FOR AIRCRAFT DETECTION, RECOGNITION AND CONTROL

УДК 629.7.022

Исследование эффективности обнаружения и распознавания малоразмерных беспилотных летательных аппаратов по их акустическому излучению / *В.Н. Олейников, О.В. Зубков, В.М. Карташов, И.В. Корытцев, С.И. Бабкин, С.А. Шейко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2018. – Вып. 195. – С. 209 – 217.

Рассмотрены особенности спектрального состава акустических излучений беспилотных летательных аппаратов, природных шумов, индустриальных излучений автомобильного и рельсового транспорта, речевых звуков человека. Для распознавания акустических излучений беспилотного летательного аппарата предложен метод на основании коэффициентов мел-кепстарльного анализа. Также предложен универсальный метод обнаружения акустических излучений беспилотного летательного аппарата по характерным особенностям спектра. Оба метода апробированы с использованием экспериментальных записей акустических излучений и дают идентичные качественные результаты. Получены зависимости эффективности распознавания от расстояния для предложенных методов. Универсальный метод уступает методу распознавания по надежности распознавания и вероятности ложного обнаружения, но не требует создания базы образов акустических излучений.

Ключевые слова: беспилотный летательный аппарат, акустическое излучение, обнаружение, распознавание.

Табл. 1. Ил. 6. Библиогр.: 8 назв.

УДК 629.7.022

Дослідження ефективності виявлення і розпізнавання малорозмірних безпілотних літальних апаратів по їх акустичному випромінюванню / *В.М. Олейников, О.В. Зубков, В.М. Карташов, І.В. Корытцев, С.І. Бабкин, С.О. Шейко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. – Вип. 195. – С. 209 – 217.

Розглянуто особливості спектрального складу акустичних випромінювань безпілотних літальних апаратів, природних шумів, індустріальних випромінювань автомобільного та рейкового транспорту, мовних звуків людини. Для розпізнавання акустичних випромінювань безпілотного літального апарату запропонований метод на підставі коефіцієнтів мел-кепстарльного аналізу. Також запропонований універсальний метод виявлення акустичних випромінювань безпілотного літального апарату за характерними особливостями спектру. Обидва методи апробовані з використанням експериментальних записів акустичних випромінювань і дають ідентичні якісні результати. Отримано залежності ефективності розпізнавання від відстані для запропонованих методів. Універсальний метод поступається методу розпізнавання по надійності розпізнавання і ймовірності помилкового виявлення, але не вимагає створення бази образів акустичних випромінювань.

Ключові слова: безпілотний літальний апарат, акустичне випромінювання, виявлення, розпізнавання.

Табл. 1. Іл. 6. Бібліограф.: 8 назв.

UDC 629.7.022

Investigation of the efficiency of detection and recognition of small-sized unmanned aerial vehicles by their acoustic radiation / *V.N. Oleynikov, O.V. Zubkov, V.M. Kartashov, I.V. Korytsev, S.I. Babkin, S.A. Sheiko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2018. – №195. – P. 209 – 217.

The features of acoustic spectrum of UAVs, spectrum of natural and industrial acoustic noise, noise spectrum of automobile and rail transport, and human speech spectrum were investigated. The method for recognition of UAV sound based on the Mel-frequency cepstral coefficients was proposed. The universal method for detecting UAV based on characteristic features of acoustic spectrum was proposed as well. Both methods were tested using experimental recordings of UAVs and noise sounds and got close well results. The universal recognition method has some worse recognition reliability and false alarm probability, but does not need creation of sound and noise images base.

Key words: unmanned aerial vehicle, acoustic radiation, detection, recognition

1 tab. 6 fig. Ref. 8 items.

УДК 004.413.7

Метод оценки зрелости системы управления безопасностью при организации воздушного движения / *И.Д. Горбенко, А.А. Замула, С.Г. Вдовенко, В.И Черныш* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2018. – Вып. 195. – С. 218 – 223.

Защита инфраструктуры системы организации воздушного движения провайдера аэронавигационного обслуживания осуществляется путем обеспечения безопасности информационно-телекоммуникационных систем, физической безопасности, кадровой безопасности и обеспечения непрерывности предоставления услуг по аэронавигационному обслуживанию. Впервые предложен метод оценки зрелости системы управления безопасностью при организации воздушного движения провайдера аэронавигационного обслуживания, который позволяет определить фактический и прогнозируемый уровни соответствия системы управления безопасностью при организации воздушного движения действующим требованиям нормативно-правовых актов, международных стандартов с учетом весовых коэффициентов.

Ключевые слова: риск, управление безопасностью, провайдер, информационная безопасность, зрелость системы.

Табл. 1. Ил. 1. Библиогр.: 5 назв.

УДК 004.413.7

Метод оцінки зрілості системи управління безпекою при організації повітряного руху / *І.Д. Горбенко, О.А. Замула, С.Г. Вдовенко, В.І Черниш* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. – Вип. 195. – С. 218 – 223.

Питання забезпечення захисту інфраструктури системи організації повітряного руху провайдера аеронавігаційного обслуговування здійснюється шляхом забезпечення безпеки інформаційно-телекомунікаційних систем, фізичної безпеки, кадрової безпеки та забезпечення безперервності надання послуг з аеронавігаційного обслуговування. Вперше запропоновано метод оцінки зрілості системи управління безпекою при організації повітряного руху провайдера аеронавігаційного обслуговування. Зазначений метод дозволяє визначити фактичний та прогнозований рівні відповідності системи управління безпекою при організації повітряного руху чинним вимогам нормативно-правових актів, міжнародних стандартів та з урахуванням вагових коефіцієнтів.

Ключові слова: ризик, управління безпекою, провайдер, інформаційна безпека, зрілість системи.

Табл. 1. Іл. 1. Бібліогр.: 5 назв.

UDC 004.413.7

Method of Maturity Assessment of Air Traffic Management Security System / *I.D. Gorbenko, O.A. Zamula, S.G. Vdovenko, V.I. Chernysh* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2018. – №195. – P. 218 – 223.

The protection of the air traffic management system infrastructure of the air navigation services provider is carried out by ensuring the security of information and telecommunications systems, physical security, personnel security and ensuring the continuity of air navigation services provision. Here the authors first proposed a method for assessing the maturity of a security management system in the air traffic management system of air navigation service provider. The proposed method allows determining the actual and predicted levels of compliance of the security management system in the air traffic management system to the current requirements of regulatory legal acts, international standards, taking into account the weight coefficients.

Keywords: risk, management security, provider, information security, system maturity.

1 tab. 1 fig. Ref.: 5 items.

УДК 004.056.5

Нечеткий экстрактор на помехоустойчивых кодах для биометрической криптографии / *А.А. Кузнецов, Р.В. Сергиенко, А.А. Уварова* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2018. – Вып. 195. – С. 224 – 234.

Рассмотрены методы формирования криптографических ключей из биометрических образов с использованием нечетких экстракторов. Предложена схема нечеткого экстрактора, в основе которой лежит кодовая криптосистема Мак-Элиса. Показано, что новая конструкция нечеткого экстрактора позволяет формировать криптографические пароли из биометрических образов даже без использования несекретных подсказок (helper string). При использовании helper string значительно возрастает доля корректируемых искажений биометрических образов. Предлагаемая конструкция относится к классу постквантовых методов защиты информации, т.е. ожидается ее безопасное использование в условиях применения универсальных квантовых компьютеров для решения задач криптоанализа.

Ключевые слова: криптосистема на основе кода; нечеткий экстрактор; биометрическая криптография; криптографические ключи.

Ил. 5. Библиогр.: 18 назв.

УДК 004.056.5

Нечіткий екстрактор на перешкодостійких кодах для біометричної криптографії / *О.О. Кузнецов, Р.В. Сергиенко, А.О. Уварова* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. – Вип. 195. – С. 224 – 234.

Розглянуто методи формування криптографічних ключів з біометричних образів з використанням нечітких екстракторів. Запропоновано нову схему нечіткого екстрактора, в основі якої лежить кодова криптосистема Мак-Еліса. Показано, що нова конструкція нечіткого екстрактора дозволяє формувати криптографічні паролі з біометричних образів навіть без використання несекретних підказок (helper string). При використанні helper string значно зростає частка коректованих спотворень біометричних образів. Крім того, пропонована конструкція відноситься до класу постквантових методів захисту інформації, тобто очікується її безпечне використання навіть в умовах застосування універсальних квантових комп'ютерів для вирішення завдань криптоаналізу.

Ключові слова: криптосистема на основі коду; нечіткий екстрактор; біометрична криптографія; криптографічні ключі.

Іл. 5. Бібліогр.:18 назв.

UDC 004.056.5

Code based fuzzy extractor for biometric cryptography / *A.A. Kuznetsov, R.V. Serhiienko, A.A. Uvarova* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2018. – №195. – P. 224 – 234.

Methods of forming cryptographic keys of biometric images using fuzzy extractors are considered. A new scheme of a fuzzy extractor based on the McEliece cryptosystem is proposed. It is shown that the new design of the fuzzy extractor allows forming cryptographic passwords from biometric images even without the use of non-secret helper string. When using helper string, the proportion of corrected distortions of biometric images increases significantly. In addition, the proposed design relates to a class of post-quantum information security methods, i.e. it is expected to be safely used even for solving cryptanalysis problems with universal quantum computers.

Keywords: code based cryptosystem; fuzzy extractor; biometric cryptography; cryptographic keys

5 fig. Ref.: 18 items.

УДК 629.7.022

Особенности обнаружения и распознавания малых беспилотных летательных аппаратов / *В.М. Карташов, В.Н. Олейников., С.А. Шейко, С.И. Бабкин, И.В. Корытцев., О.В. Зубков* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2018. – Вып. 195. – С. 235 – 243.

Проведен обзор и анализ методов обнаружения и распознавания беспилотных летательных аппаратов (БПЛА). Рассмотрены каналы для обнаружения БПЛА – акустический, оптический, радиолокационный, инфракрасный, канал радиоразведки. Сравнены и оценены преимущества и недостатки используемых каналов. В случае малых БПЛА имеется ряд существенных сложностей и ограничений. Одним из направлений в обнаружении БПЛА являются акустические наблюдения. Шум, создаваемый силовой установкой БПЛА и воздушным винтом, является существенным демаскирующим признаком. Создание и совершенствование методов обнаружения, пеленгации и распознавания малых БПЛА путем приёма и обработки их звуковых сигналов является актуальной задачей. При применении такого метода обнаружения БПЛА используются частотные спектры, спектрограммы, нормированные автокорреляционные функции и фазовые портреты акустических сигналов. Информационными признаками звукового образа БПЛА могут служить оценки спектральных коэффициентов, определяемые по дискретной реализации, содержащей заданное количество отсчетов, а также параметры моделей авторегрессии.

*Ключевые слова:*обнаружение, распознавание. беспилотный летательный аппарат, акустический шум.

Ил. 1. Библиогр.: 32 назв.

УДК 629.7.022

Особливості виявлення та розпізнавання малих безпілотних літальних апаратів / *В.М. Карташов, В.М. Олейніков, С.О. Шейко, С.І. Бабкін, І.В. Коритцев., О.В. Зубков* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. – Вип. 195. – С. 235 – 243.

Проведено огляд та аналіз методів виявлення та розпізнавання безпілотних літальних апаратів (БПЛА).Розглянуті канали для виявлення БПЛА – акустичний, оптичний, інфрачервоний, радіолокаційний, канал радіорозвідки. Порівняні та оцінені переваги і недоліки каналів, які використовуються. У випадку малих БПЛА є ряд суттєвих складнощів та обмежень. Одним з напрямків у виявленні БПЛА є акустичні спостереження. Шум, що створюється силовою установкою БПЛА та повітряним гвинтом, є суттєвим демаскуючою ознакою. Створення та удосконалення методів виявлення , пеленгації і розпізнавання малих БПЛА шляхом прийому та обробки їх акустичних сигналів є актуальне завдання. При застосуванні такого методу виявлення БПЛА використовуються частотні спектри, спектрограми, нормовані автокореляційні функції і фазові портрети. Інформаційними ознаками звукового обліку БПЛА можуть слугувати оцінки спектральних коефіцієнтів, які визначаються за дискретною реалізацією, що містить задану кількість відліків, а також параметри моделей авторегресії.

Ключові слова: виявлення, розпізнавання, безпілотний літальний апарат, акустичний шум.

Іл. 1. Бібліогр.: 32 назв.

UDC 629.7.02

Peculiarities of small unmanned aerial vehicles detection and recognition / *V.M. Kartashov, V.N. Oleynikov, S.A. Sheyko, S.I. Babkin, I.V. Koryttsev, O.V. Zubkov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2018. – №195. – P. 235 – 243.

Review and analysis of methods for detection and recognition of unmanned aerial vehicles (UAVs) are conducted. The channels for the detection of UAVs - acoustic, optical, radar, infrared, radio channel are considered. The advantages and disadvantages of the channels used are compared and appreciated. In the case of small UAVs, there are a number of significant difficulties and limitations. One of the directions in the UAVs detection is acoustic observation. The noise generated by the UAV propulsion system and the air propeller is a significant demasking feature. Creating and improving methods for detecting, guiding and recognizing small UAVs by the reception and processing their sound signals is an urgent task. When using such a method of detecting UAVs, frequency spectra, spectrograms, normalized autocorrelation functions, and phase portraits of acoustic signals are used. Estimates of spectral coefficients, determined by a discrete realization containing a predetermined number of samples, as well as parameters of autoregression models can serve as information signs of the UAVs sound image.

Keywords: detection, recognition, unmanned aerial vehicles, acoustic noise.

1 fig. Ref.: 32 items.

ЗБІРНИК НАУКОВИХ ПРАЦЬ
РАДІОТЕХНІКА
Випуск 195
Російською, українською та англійською мовами

СБОРНИК НАУЧНЫХ ТРУДОВ
РАДИОТЕХНИКА
Выпуск 195
На русском, украинском и английском языках

Коректор Л.І. Сащенко

Підп. до друку 28.12.2018. Формат 60x90/8. Папір офсет. Гарнітура Таймс. Друк. ризограф.
Ум. друк. арк**.** 13,2. Обл.-вид. арк. 12,77. Тираж 300 прим. Зам. № 282. Ціна договір.

Харківський національний університет радіоелектроніки (ХНУРЕ)
Просп. Науки, 14, Харків, 61166.

Оригінал-макет підготовлено і збірник надруковано у ПФ „Колегіум”, тел. (057) 703-53-74.
Свідоцтво про внесення суб’єкта видавничої діяльності до Державного реєстру видавців.
Сер. ДК №1722 від 23.03.2004.