Serhii Yevseiev (Ukraine), **Alla Gavrilova** (Ukraine),
Bogdan Tomashevsky (Ukraine), **Firuz Samadov** (Azerbaijan)

RESEARCH OF CRYPTO-CODE DESIGNS CONSTRUCTION FOR USING IN POST QUANTUM CRYPTOGRAPHY

Abstract

The article analyzes construction of crypto-code designs (CCDs) on the basis of asymmetric Mac-Alice and Niederreiter crypto-code systems on elliptical (EC) and modified elliptic codes (MEC), which, in the conditions of post-quantum cryptography, allow to provide a guaranteed level of crypto stability, to counteract the modern Attacks and attack by V. Sidelnikov on the theoretical code schemes of McEliece and Niederreiter.

Schemes of hybrid crypto-code designs constraction the lossy codes are addressed. Methods of constructing mechanisms of confidentiality and integrity of banking information resources under hybrid threats to security components (information security, cybersecurity, information security) are proposed.

Using of a lossy code is suggested to this end. Lossy Code allow you to increase the speed of code changes by reducing the power of the field when causing damage to open text and reducing the amount of data transferred by causing harm to the cipher text. The methods of constructing unprofitable codes and approaches for use in hybrid KKK of McEliece and Niederreiter on modified elliptic codes are considered. Practical algorithms for the use of the MV2 mechanism in McEliece's CCD and Niederreiter's modified elliptic codes are proposed, which allows the implementation of the CCD hybrid scheme. The comparative results of the study of stability and power capacity with respect to their practical use in automated banking systems are presented.

Keywords McEliece' crypto-code designs, Niederreiter's crypto-code designs, elliptic codes, modified elliptical codes, hybrid crypto-code designs

JEL Classification H56

С. Євсеєв (Україна), **А. Гаврилова** (Україна), **Б. Томашевський** (Україна),
Ф. Самадов (Азербайджан)

ДОСЛІДЖЕННЯ КРИПТО-КОДОВИХ КОНСТРУКЦІЙ ДЛЯ ВИКОРИСТАННЯ В ПОСТ КВАНТОВІЙ КРИПТОГРАФІЇ

Анотація

У статті проводиться аналіз побудови крипто-кодових конструкцій (ККК) на основі несиметричних крипто-кодових систем Мак-Еліса і Нідеррайтера на еліптичних (*EC*) та модифікованих еліптичних кодах (*MEC*), які в умовах постквантової криптографії дозволяють забезпечити гарантований рівень криптостійкості, протидіяти сучасним атакам і атаці В. Сідельникова на теоретико-кодові схеми Мак-Еліса і Нідеррайтера.

Розглянуті схеми побудови гібридних крипто-кодових конструкцій на збиткових кодах. Запропоновані методи побудови механізмів конфіденційності і цілісності банківських інформаційних ресурсів в умовах дії гібридних загроз на складові безпеки (інформаційній безпеці, кібербезпеці, безпеці інформації).

Для цього пропонується використовувати збиткові коди. Збиткові коди дозволяють збільшити швидкість кодових перетворень за рахунок зменшення потужності поля при нанесенні збитку відкритого тексту і зменшити обсяг переданих даних за рахунок нанесення шкоди шифртексту. Розглядаються способи побудови збиткових кодів і підходи використання в гібридних ККК Мак-Еліса і Нідеррайтера на модифікованих еліптичних кодах. Пропонуються практичні алгоритми використання механізму MV2 в ККК Мак-Еліса і Нідеррайтера на модифікованих еліптичних кодах, що дозволяє реалізувати гібридну схему ККК. Наведені порівняльні результати дослідження стійкості та енергетичній ємності щодо їх практичного використання в автоматизованих банківських системах.

S. KUZNETS KHNUE

Founder:

Simon Kuznets Kharkiv National University of Economics, Nauky avenue, 9-A, Kharkiv, 61166, Ukraine
http://www.hneu.edu.ua/

Received on: 12th of November, 2018
Accepted on: 14th of December, 2018

Serhii Yevseiev, Chief of Department of Cyber Security and Information Technology Simon Kuznets Kharkiv National University of Economics, Ukraine.

Alla Gavrilova, Senior Lecturer Department of Cyber Security and Information Technology Simon Kuznets Kharkiv National University of Economics, Ukraine.

Bogdan Tomashevsky, Associate Professor of Department of Cyber Security Ternopil Ivan Puluj National Technical University, Ukraine.

Firuz Samadov, PhD in Technical Sciences, Associate Professor, Department of Computer Systems and networks, Azerbaijan Technical University, Azerbaijan.

http://dx.doi.org/10.21511/dm.4(4).2018.03

Ключові слова крипто-кодова конструкція Мак-Еліса, крипто-кодова конструкція Нідеррайтера, еліптичні коді, модифіковані еліптичні коди, гібридні крипто-кодові конструкції

Класифікація JEL H 56

INTRODUCTION

The age of high technology is characterized by the sharp increase in the volume of processed data, quantum technologies and artificial intelligence development in all spheres of human activity, the emergence of hybrid threats in cyberspace and the reduction of the stability of classical algorithms of traditional and asymmetric cryptography. Research in the field of quantum computing impact, using the phenomena of quantum superposition and quantum confusion for the transmission and data processing, has shown that quantum computers that use special algorithms (for example, Shore's algorithm) will be able to factorize numbers at polynomial time (Androshchuk, 2017; Babych, 2016; Baldi et al., 2016; Chen, 2016; Grischuk & Danik, 2016; Leonenko & Yudin, 2013). Therefore, cryptographic systems on asymmetric cryptography algorithms (RSA, ECC, DSA) will be vulnerable to brute force attacks using a full-scale quantum computer. So that, the main research and development of cryptographic information security (KPI) is aimed at finding solutions that would not be vulnerable to quantum computing and would be simultaneously resistant to attacks using conventional computers. Such algorithms refer to the section of quantum-safe cryptography (or quantum-resistant cryptography) (De Vries, 2016; Hryshchuk & Molodetska-Hrynhchuk, 2018; Hryshchuk & Molodetska, 2016; Kuchuk et al., 2016; Kuchuk et al., 2017; Mozhaev et al., 2017), among which NIST specialists distinguish cipher-code systems of Mac-Alice and Niederreiter. The main disadvantage is the computational complexity of their implementation. To insure guaranteed stability, the power of the GF (210–213) field is required. In addition, the possibility of implementing Sidelnikov's attack when using blocking codes BCH, Hopp's, Reed-Solomon's codes, alternative Hopp's codes (De Vries, 2016; Dinh et al., 2011; Sidelnikov, 2008). In the view of V. Sidelnikov, the perspective direction is the use of algebra-geometric (built using curves, for example, elliptic, Fermat, Suzuki, Hermite, etc.) or cascading codes (Baldi et al., 2016; Cho et al., 2017; Dudikevich et al., 2010; Morozov et al., 2017; Sidelnikov, 2008).

1. LITERATURE REVIEW

The main advantage of the symmetric (Rao-Nama scheme) and non-symmetric McEliece and Niederreiter crypto-code systems is the high speed of cryptographic transmissions and the simultaneous securing of the confidentiality of data transmitted by open communication channels (Baldi et al., 2016; Morozov et al., 2017; Niederreiter, 1986). The general classification of crypto-code systems and security services that provide their use are shown in Figure 1.

In the paper (Evseev et al., 2016), it is proposed to use modified NKSKS (IKSS) for modified EC (MEC) to reduce the power consumption of cryptanalons in the Nuclear Physics and Mathematics Laboratory of McEliece.

2. AIMS

The purpose of the article is a research of the crypto-code designs construction on the basis of elliptic codes modification with further lossy based on multichannel cryptography, analysis of the properties of safety and energy of modified Mak-Alice constructions in the conditions of post-quantum cryptography.

3. METHODS

To modify the linear block code, which does not reduce the minimum code distance, remains shortening its length by reducing the information symbols (Evseev et al., 2016; Yevseiev, et al., 2016). In works (Evseev et al., 2016; Yevseiev, 2017; Yevseiev & Korol, 2018; Yevseiev & Tsyhanenko, 2018; Evseev et al., 2017) the mathematical apparatus for constructing modified elliptic codes is given.

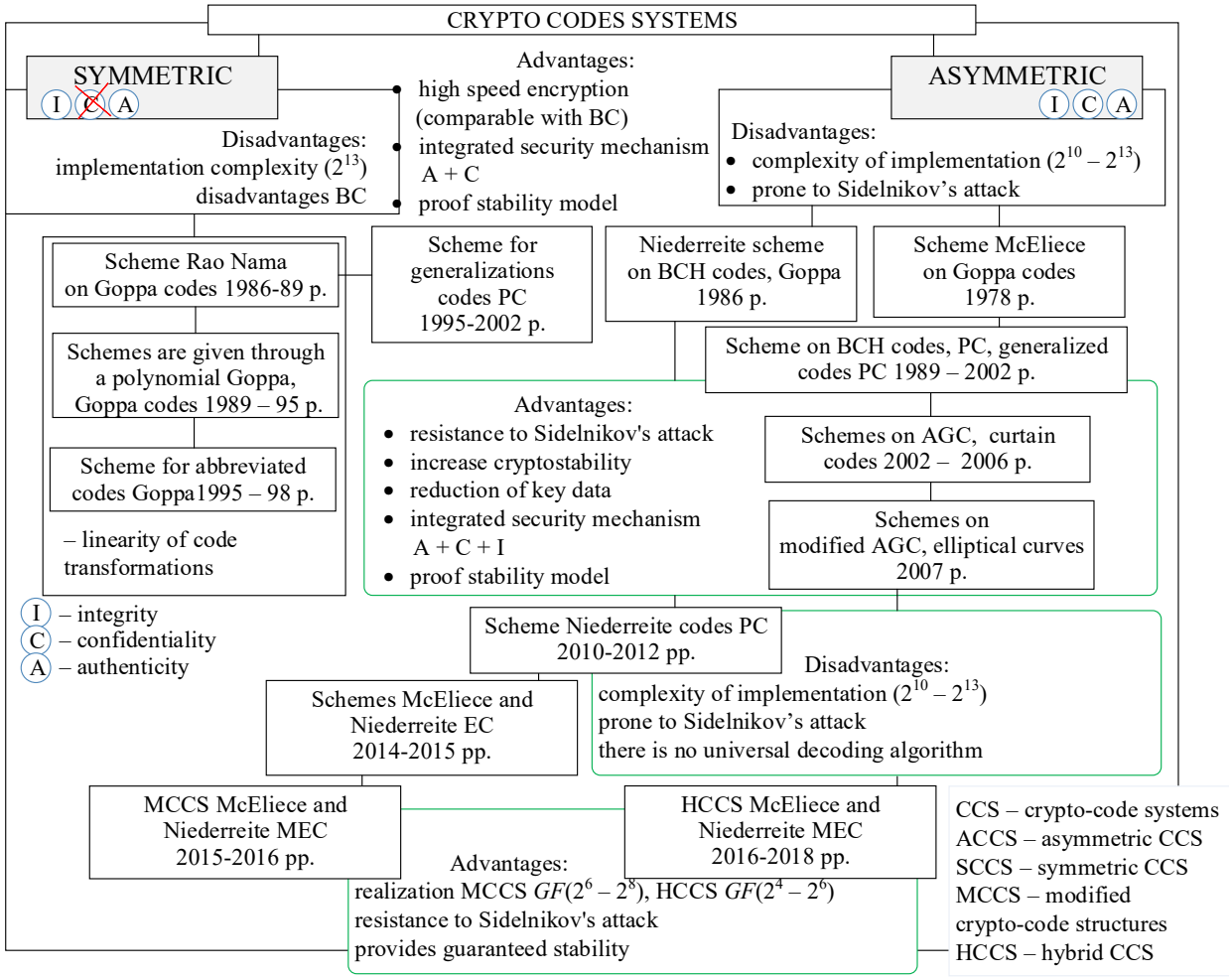

Figure 1. Classification of cryptosystems based on CCS

To modify (shorten) elliptic codes, we will use a decrease in the set of points of the curve. The following statements are true (Babych, 2016; Baranov, 2014).

Statement 1 (Evseev et al., 2016; Yevseiev & Korol, 2018). Let *EC* – elliptic curve over *GF(q)*, *g=g(EC)* – the curve type, *EC*(*GF*(*q*)) – the set of its points over the finite field, *N=EC*(*GF*(*q*)) – their number. Let *X* and *h* – non-disjoint subsets of the points, $X \cup h = EC\left(GF\left(q\right)\right)$, $\left|h\right| = x$, $x \le 1/2k$. When encoding an information vector, the characters of the set of h do not participate (they are zero) and they can be discarded, and the resulting codeword will be shorter on *x* code symbols. Then the shortened elliptic (*n*, *k*, *d*) code over *GF*(*q*), is constructed by displaying the form $\varphi : X \to P^{k-1}$, which is related to the characteristics $k + d \ge n$, moreover: $n = 2\sqrt{q} + q + 1 - x$, $k \ge \alpha - x, d \ge n - \alpha, \alpha = 3 \cdot degF$.

Statement 2 (Evseev et al., 2016; Yevseiev & Korol, 2018). *The shortened* elliptic-curve (*n*, *k*, *d*) code over *GF*(*q*), is constructed by displaying the form $\varphi : X \to P^{r-1}$, which is related to the characteristics $k + d \ge n$, moreover:

$$n = 2\sqrt{q} + q + 1 - x,\ k \ge n - \alpha, d \ge \alpha, \alpha = 3 \cdot degF. \quad (1)$$

Using the result of the assertions 1, 2 specify McEliece's MACCS on MEC, constructed by displaying the form $\varphi : X \to P^{k-1}$, та $\varphi : X \to P^{r-1}$. The following statements are true.

Statement 3 (Evseev et al., 2016; Yevseiev & Korol, 2018). *The shortened* elliptic-curve (*n*, *k*, *d*) code over $GF(2^m)$, is constructed by displaying the form $\varphi : X \to P^{k-1}$, defines the MCCS on MEC with the parameters:

http://dx.doi.org/10.21511/dm.4(4).2018.03

- the dimension of the secret key: $l_{K+} = \left(x - x_1\right) \cdot \left[\log_2 \left(2\sqrt{q} + q + 1\right)\right];$ (2)
- the dimension of the information vector (in bits): $l_I = \left(\acute{a} - x + x_1\right) \cdot m;$ (3)
- the codec dimension: $l_S = \left(2\sqrt{q} + q + 1 - x\right) \cdot m;$ (4)
- relative encoding speed: $R = \dfrac{\left(\acute{a} - x\right)}{\left(2\sqrt{q} + q + 1 - x\right)}.$ (5)

Statement 4 (Evseev et al., 2016; Yevseiev & Korol, 2018). *The shortened* elliptic-curve (*n*, *k*, *d*) code over *GF*(2^m), constructed by displaying the form $\varphi : X \to P^{r-1}$, constructed by displaying the form:

- the dimension of the secret key is determined by the expression (3);
- the dimension of the information vector (in bits): $l_I = \left(2\sqrt{q} + q + 1 - x\right) \cdot m;$ (6)
- the codec dimension is determined by the expression (3.16);
- relative transmission rate: $R = \dfrac{\left(2\sqrt{\acute{q}} + q + 1 - \right)}{\left(2\sqrt{q} + q + 1 - x\right)}.$ (7)

The second way of modifying a linear block code that retains the minimum code distance and increases the amount of data transmitted is to extend its length after the formation of the initialization vector, by reducing the information symbols. The mathematical apparatus of a modified crypto-code construction based on the McEliece scheme is given in (Evseev et al., 2016; Yevseiev, 2017; Yevseiev & Korol, 2018; Yevseiev et al., 2017).

Statement 5 (Evseev et al., 2016; Yevseiev & Korol, 2018). Extended elliptic-curve (*n*, *k*, *d*) code over *GF*(2^m), constructed by displaying the form $\ddot{o} : (X \cup h_1) \to P^{k-1}$, defines the MCCS with the parameters:

- the dimension of the secret key (in bits): $l_{K+} = \left(x - x_1\right) \cdot \left[log_2 \left(2\sqrt{q} + q + 1\right)\right];$ (8)
- the dimension of the information vector (in bits): $l_I = \left(\acute{a} - x + x_1\right) \cdot m;;$ (9)
- the size of the cryptogram (in bits): $l_S = \left(2\sqrt{q} + q + 1 - x + x_1\right) \cdot m;$ (10)
- relative transmission speed: $R = \dfrac{\left(\acute{a} - x + x_1\right)}{\left(2\sqrt{q} + q + 1 - x + x_1\right)}.$ (11)

The analysis carried out in (Evseev et al., 2016; Yevseiev, 2017; Yevseiev & Korol, 2018; Yevseiev et al., 2017)shows that the use of modified (shortened / extended) MECs can reduce the power capacity of the software implementation of the McEliece's MCCS almost in 2 times, but at the same time provide the required level of crypto stability while implementing a smaller field GF(26 – 28).

Investigation of the properties of construction of cryptosystems on the loss codes. In order to provide basic information security services, in the conditions of growing information security threats (IS), cyber security (CB), information security (IS) in works (Yevseiev, 2017; Yevseiev & Korol, 2018; Yevseiev et al., 2017), it is proposed to use hybrid crypto-code designs based on the synthesis of McEliece and Niederreiter MCCS on MEC and the unprofitable codes of multichannel cryptography.

In the works (Yevseiev, 2017; Yevseiev & Korol, 2018) the theoretical and practical bases of the construction of loss codes are considered. Lucrative text is understood the text obtained because of further deformation of non-redundant codes of letters (Mishchenko & Vilansky, 2007; Mishchenko et al., 2006).

The theoretical basis for constructing unprofitable texts is the disturbance of the ordering of the characters of the source text and because of the reduction of redundancy of the symbols of the language in the redundancy text. At the same time, the amount of information that expresses this ordering will be equal to the decrease in the entropy of the text as compared with the maximum possible amount of entropy, that is, the equally probable appearance of any letter after any previous letter. Methods of calculating the information proposed in (Mishchenko & Vilansky, 2007) allow us to find out the ratio of the amount of predicted (that is, formed according to certain rules) information and the amount of unexpected information that cannot be foreseen in advance. The redundancy of the text is determined by the expression (Yevseiev, 2017; Yevseiev & Korol, 2018):

$$B(M) = B_A L_0 = \left(log\, N - \frac{H(M)}{L_0} \right) \cdot L_0, \qquad (12)$$

where M – is the original text, B – redundancy of the language ($B = R - r,$, R – redundancy of the language $(R = log\, N)$, N – capacity of the alphabet, r – entropy of the language for one character, $r = H(M)/L$, L – the length of the message M in the characters of the language), $H(M)$ – entropy (uncertainty) of the message,

L0 – the length of the message M of the characters of the language with the contents, BA – redundancy of the language.

To obtain redundancy text (FTC) and redundancy (DCH) the "ideal" compression method is used after executing m cycles of the Cm (Yevseiev & Tsyhanenko, 2018; Yevseiev et al., 2016).

A quantitative measure of the effectiveness of causing damage is the degree of change in meaning, equal to the difference in entropy of the lossy text and source text at different segments of the length of the redundancy text:

$$d = H(FTC) - \sum_{i=1}^{s} H(M_i) p_i, \ \sum_{i=1}^{s} p_i = 1, \ s = \left[\frac{L_0 - L_{FTC}}{L_{FTC}} \right], \qquad (13)$$

where Mi – is the part of the source text corresponding to the i - th segment, pi – it's probability, L0 – the length Mi, equal to the length of the LFTC – redundancy text, s – the number of segments.

In Figure 2 shows the structural scheme of one step of the universal mechanism of causing damage.

Under the information core of some text is understood the laconic text of the *CFT*, obtained as a result of the cyclic transformation of the universal mechanism of causing damage to C_m.

The universal mechanism for causing damage to Cm can be described (Sidelnikov, 2008; Yevseiev, 2017):

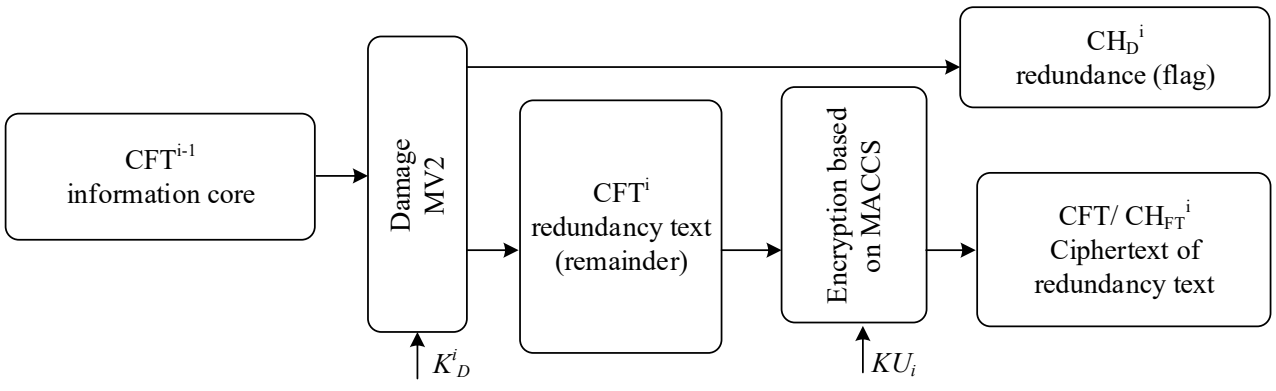

Figure 2. The block diagram of one step of the universal mechanism of causing damage

http://dx.doi.org/10.21511/dm.4(4).2018.03

$$CFT / CH_{FT} = E_1\left(M\ , KU^{EC}\right),$$
$$CHD/CH_D = E_2\left(M\ , KU^{EC}\right),$$
$$M = E_{1.2}^{-1}(CFT / CH_{FT}, CHD/CH_D, KU^{EC}),$$

where

$$CFT / CH_{FT} = CFT / CH_{FT}^{i},\ldots,CFT / CH_{FT}^{m},$$
$$KU^{EC} = ö\left(K_D^{i},\ldots,K_D^{m}, KU_l^{EC},\ldots,KU_m^{EC}\right),$$
$$CHD / CH_D = CHD / CH_D^{i},\ldots,CHD / CH_D^{m}.$$

The main methods of causing damage are shown in Figure 3, 4 shows the basic protocols of security services based on the use of loss-making codes.

The unity distance for a random cipher model for which there is a probability of obtaining meaningful text in random and equally probable choices of the key K and an attempt to decrypt the encrypt text $N_s = H(K)\frac{2^{HL}}{|I|^L} = 1$ is equal to:

$$L = U_0 = \frac{H(K)}{log|I| - H} = \frac{H(K)}{B \cdot l\,og|I|}, \qquad (14)$$

where B – redundancy of the source text, H – entropy on the letter of meaningful text in the input alphabet I, $|I| > 2$, 2^{HL} – he approximate value of the number of meaningful texts.

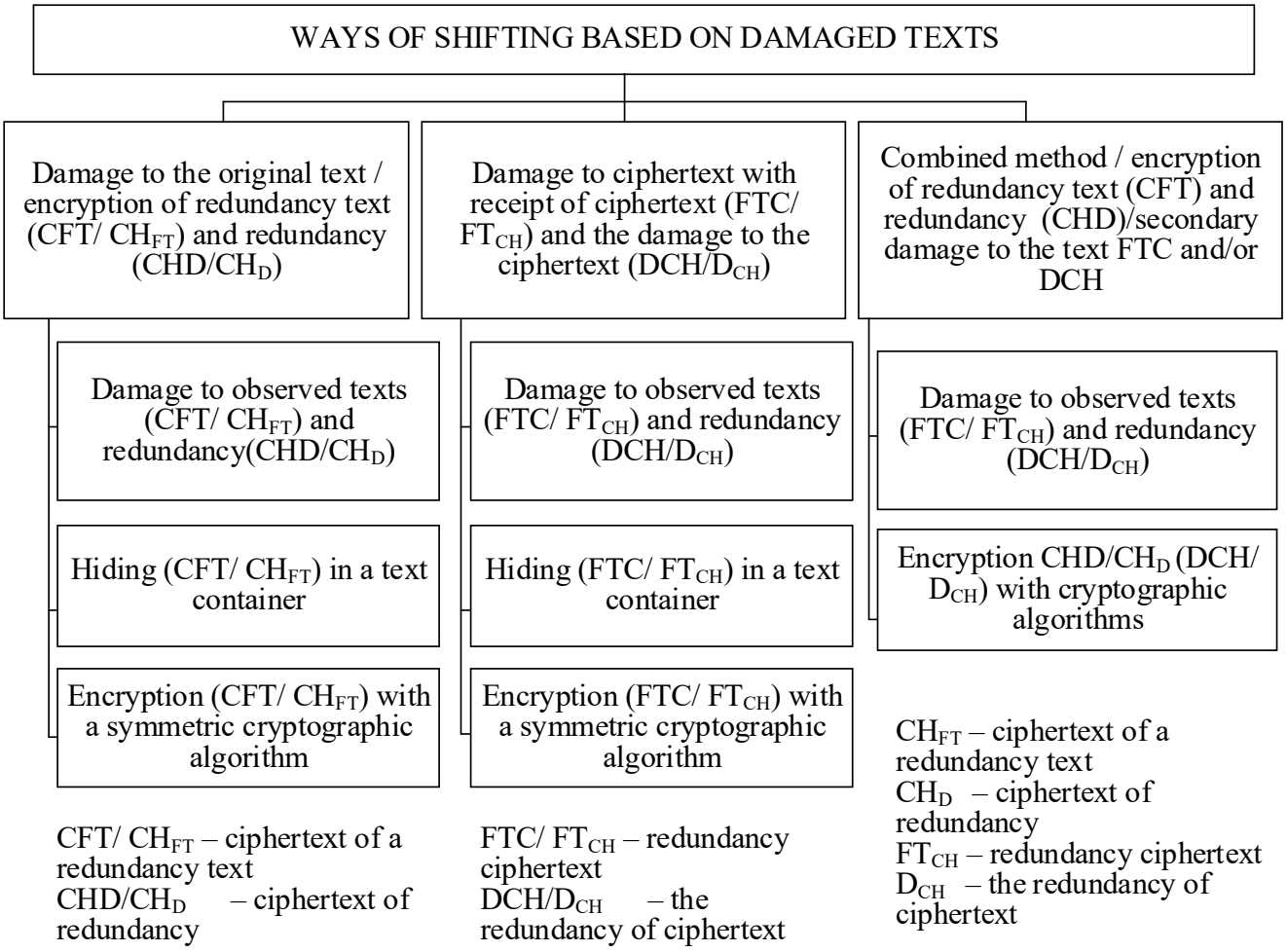

Figure 3. The main ways of causing damage

The conducted analysis in the works (Mishchenko & Vilansky, 2007; Mishchenko et al., 2006; Yevseiev, 2017; Yevseiev & Korol, 2018; Yevseiev, & Tsyhanenko, 2018) showed that hybrid cryptographic code structures provide the possibility of their practical implementation, with a significant reduction of field strength. In this way, it ensures its competitiveness and the possibility of considering as an alternative to classical algorithms of asymmetric cryptography.

An analysis of methods for causing damage in works (Mishchenko & Vilansky, 2007; Mishchenko et al., 2006; Yevseiev, 2017; Yevseiev & Korol, 2018; Yevseiev, & Tsyhanenko, 2018) showed that the first and second methods of causing damage with subsequent cryptographic transformations are the most suitable for use in Internet protocols, which reduces the power of the alphabet in the formation of cryptograms in the McEliece and Niederreiter MCCS, structural schemes are shown in Figure 5, 6 respectively. The unity distance for the first method (Expression 15) will be transformed:

$$U_0 = \frac{\sum_{i=1}^{m}\left(H\left(CHD^{(i)}\right)\right) + H\left(KU_i^{EC}\right)}{B \cdot log|I|}. \quad (15)$$

Such system is based on the incorrect distortion of the damage and stability through the use of subsequent encryption on the basis of MCCS. This leads to the inability to find out the encryption text of the redundancy text. The unity distance for the second method (Expression 16) will be transformed:

$$U_0 = \frac{H\left(KU_i^{EC} + H\left(FTC/FT_{CH}\right) + H\left(DCH/D_{CH}\right) + \sum_{i=1}^{m}\left(H\left(CHD^{(i)}\right)\right) + H\left(KU_i^{EC}\right)\right)}{B \cdot log|I|}. \quad (16)$$

The second option allows you to increase the distance of unity compared to the first way.

To estimate the reduction of energy costs for the practical implementation of crypto-code designs in (Yevseiev & Tsyhanenko, 2018) the results of the evaluation of the complexity of the formation of cryptograms and its decoding with the use of the Niederreiter's CCS, the evaluation of the hurdle's complexity by the most effective method of decoding (permutations by a decoder) are given.

Further reduction of the Galois field power leads to a significant reduction in the complexity of the formation (≈ in 3 times) and decoding (≈ in 5 times) of cryptograms and provides a guaranteed level of crypto stability (Yevseiev & Korol, 2018; Yevseiev, & Tsyhanenko, 2018).

To estimate time and speed indicators, it is accepted to use a unit of measurement cpb, where cpb (cycles per byte) - the number of processor counts that need to be spent to handle 1 byte of input information. The complexity of the algorithm is determined by the formula:

$$Per = Utl \cdot CPU\_clock/Rate, \quad (17)$$

where Utl – utilization of the core of the processor (%), $Rate$ – bandwidth of the algorithm (bytes/s).

4. RESULTS

In Table 1 the results of studies of the dependence of the length of the input sequence on the *MV*2 algorithm from the number of processor cycles to perform elementary operations in the program implementation are presented.

http://dx.doi.org/10.21511/dm.4(4).2018.03

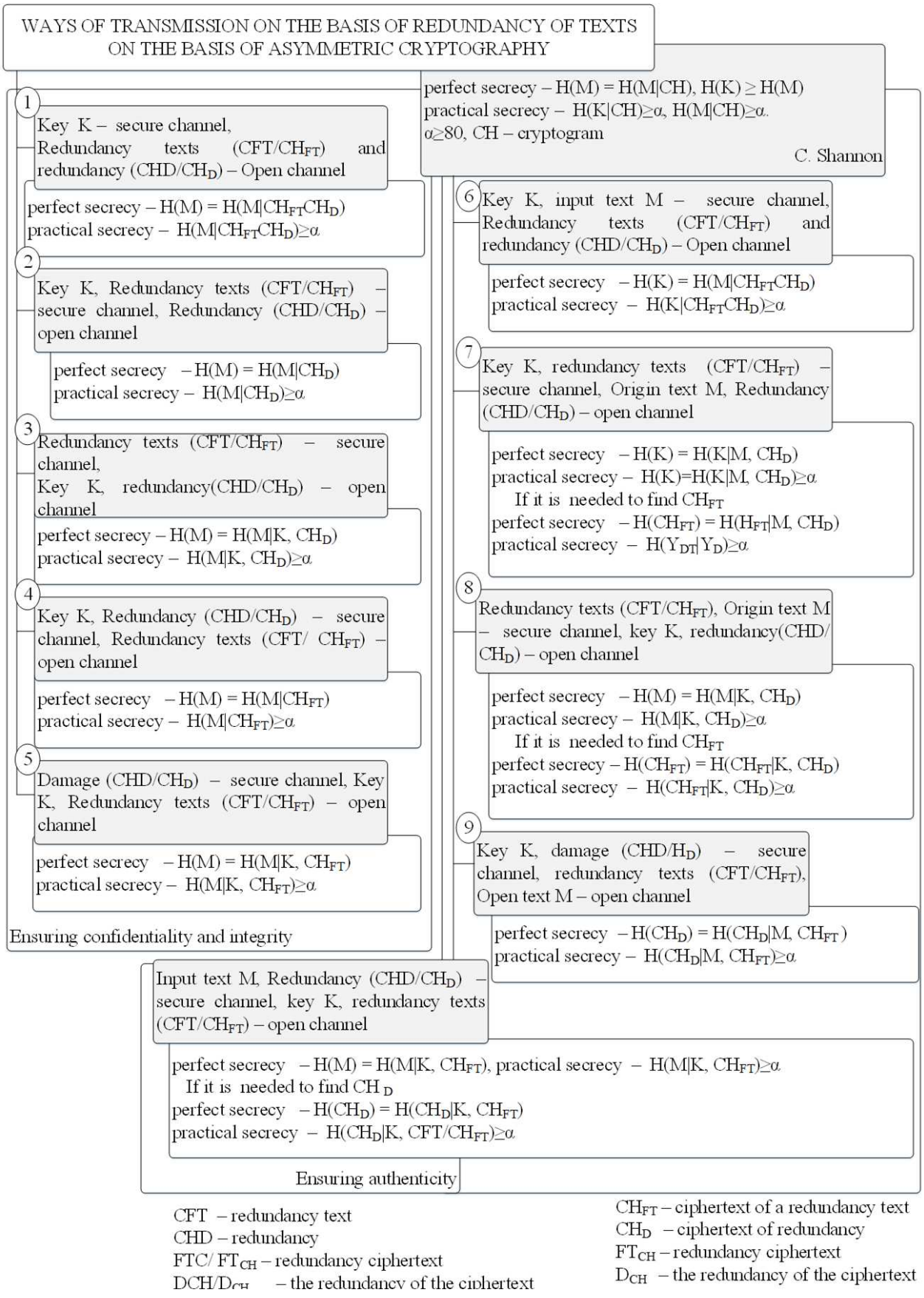

Figure 4. Basic protocols for providing security services

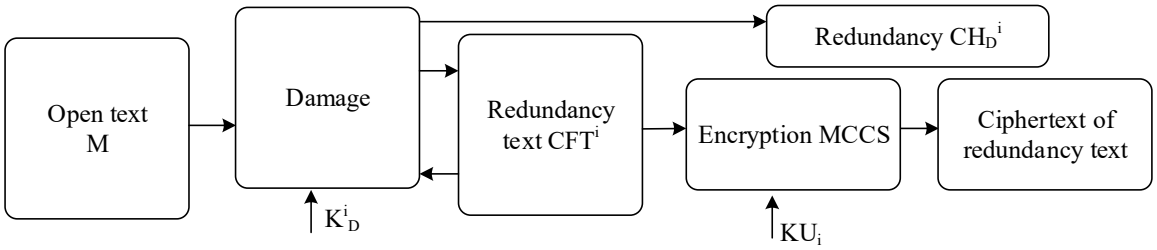

Figure 5. Structural diagram of construction of a hybrid crypto-code system on the basis of causing damage to open text

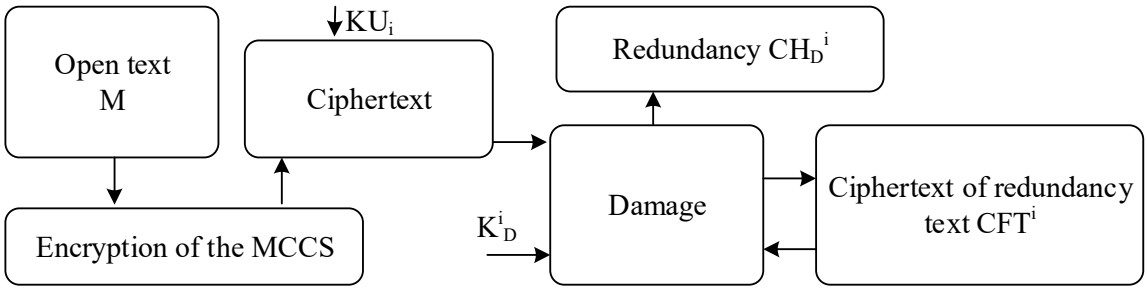

Figure 6. The block diagram of construction of a hybrid cryptosystem on the basis of damage to cipher text

Table 1. The results of studies on the dependence of the length of the input sequence on the MV2 algorithm from the number of processor counts

Code sequence length		MV2		
		10	100	1,000
The number of calls of functions that implement elementary operations	addition	3,942	28,673	275,499
	subtraction	1,794	3,810	23,881
	division	3,274	4,804	20,104
	multiplication	19	109	1,009
	comparison	8,939	60,963	578,784
Sum		17,968	98,359	899,277
Runtime * in milliseconds	addition	19.53	93.58	2,297.36
	subtraction	8.89	12.43	199.14
	division	16.22	15.68	167.65
	multiplication	0.09	0.36	8.41
	comparison	44.28	198.96	4,826.43
Sum		89	321	7,499
Runtime * in milliseconds		89	321	7,499

In Table 2 the results of researches of the estimation of time and speed indicators of procedures of drawing and removal of damage are resulted.

Table 2. Results of research of time кand speed indicators of procedures of drawing and removal of damage

Indexes	Code sequence length	Work time (sec)	Bandwidth of the algorithm, Rate (byte /sec)	Recycle the core of the processor (ticks)	complexity of the algorithm, Per (cpb)
The number of calls of functions that implement elementary operations	10	0.089	112.3596	90	0.801
	100	0.321	311.5265	322	1.034

http://dx.doi.org/10.21511/dm.4(4).2018.03

Thus, an analysis of the basic principles of the McEliece (Niederreiter) MCCS and multichannel cryptography systems on redundancy codes allows the formation of hybrid cryptosystems.

The difference between the HCCS in the McEliece or Niederreiter schemas of the "classic" approach to the formation of a hybrid (integrated) cryptosystem is the use of asymmetric crypto-code structures with fast algorithms of cryptographic transformations as the main mechanism for ensuring the stability (security) of information followed by the use of MV2 algorithm (multichannel system on loss codes), which reduces energy costs (the capacity of the MCCS alphabet on the *MEC*).

In the works (Yevseiev, 2017; Yevseiev & Korol, 2018; Yevseiev, & Tsyhanenko, 2018) algorithms of the hybrid crypto-code system of McEliece on MEC are proposed which allow in case of concealing of loss-making ciphertext CFT/CH_{FT} all its possible values are determined by an additional key field:

$$U_0 = \frac{H\left(CFT/CH_{FT}\right) + \sum_{i=1}^{m}\left(H\left(CHD^{(i)}\right)\right) + H\left(KU_i^{EC}\right)}{B \cdot log|I|}. \quad (18)$$

In the case of additional concealment of the last encryption text, the damage to the CHD/CH_D due to its smallness and the admissibility with the ciphertext of the redundancy text CFT/CH_{FT} the distance of unity can be further increased:

$$U_0 = \frac{H\left(CHD/CH_D\right) + H\left(CFT/CH_{FT}\right) + \sum_{i=1}^{m}\left(H\left(CHD^{(i)}\right)\right) + H\left(KU_i^{EC}\right)}{B \cdot log|I|}. \quad (19)$$

Thus, multichannel cryptography on the basis of the loss-making codes allows for the integration of cryptographic systems, combining crypto-code designs with the same concept (McEliece and Niederreiter MCCS on MEC) and the systems on the loss-making codes that complement each other providing the necessary security measures and reliability, and enrich the total system with its properties. In addition, such an approach provides for counteracting V. Sidelnikov's attack on the basis of fine-linear transformations (Sidelnikov, 2008).

In works (Evseev et al., 2016; Yevseiev, 2017; Yevseiev, & Korol, 2018; Yevseiev et al., 2017) a formal description of the McEliece's MCCS mathematical model on modified elliptic codes is considered, (Mishchenko et al., 2006) considered the universal mechanism of causing losses and methods of transmission in systems on redundancy codes. The main difference between mathematical models is the formation of a codogram based on shortening or lengthening, as well as the method of causing damage. The main difference between elongated codes is the use of the abbreviation symbols in the McEliece's MCCS, with the subsequent replacement of the information symbols of the open information.

In Figures 7, 8 the structural protocols based on the McEliece's HCCS with modified (shortened / extended) elliptic-curve codes according to the second method of causing damage are given.

In (Yevseiev & Tsyhanenko, 2018) a formal description of the mathematical model of the hybrid Niederreiter's HCCS is presented. An analysis of the practical implementation of the encryption/decryption algorithms in the HCCS of the Niederreiter shows that when forming a cryptogram (syndrome) after the formation of an error vector by an algorithm of equilibrium coding, the initialization vector that defines the reduction of symbols to the error vector – he (error vector symbols equal to zero), |h|=1/2e, that is $e_i = 0, \forall e_i \in h,$ encrypted by the MV2 algorithm and transmitted by two independent open channels. When encrypting cryptograms (after receiving the error vector, before using the equilibrium coding algorithm), for the information to be entered, the "zero" characters are shortened.

The algorithm for forming a cryptogram in a modified HCCS of Niederreiter is presented in the form of a sequence of steps:

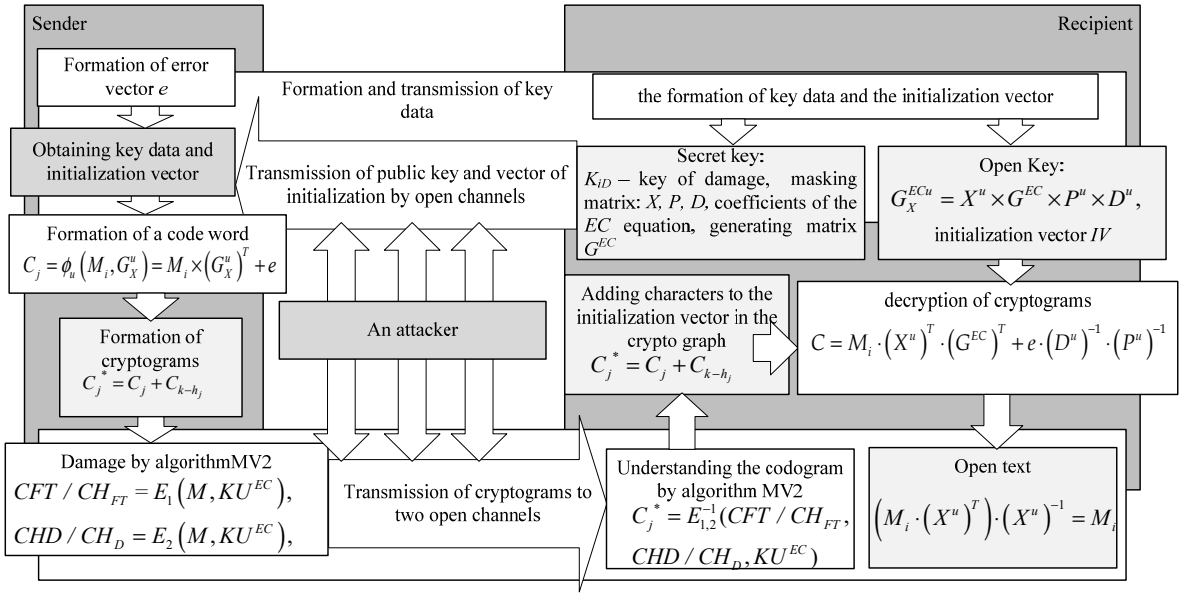

Figure 7. The protocol of exchange with the help of the McEliece's HCCS on shortened MES

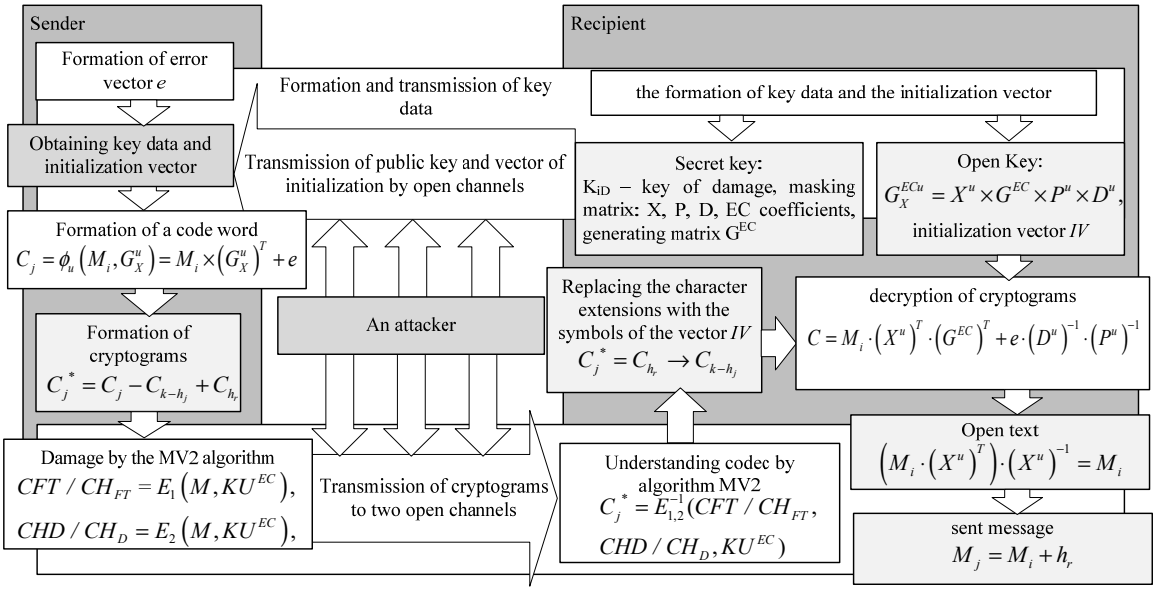

Figure 8 Protocol for the exchange with McEliece's HCCS on extended MES

Step 1. Entering information that is subject to coding.

Entering the public key H_X^{EC}.

Step 2. Formation of the error vector *e*, the weight of which does not exceed ≤ t – corrects the ability of the elliptic code based on the algorithm of non-dual equilibrium coding.

Step 3. Formation of the initialization vector IV_1, IV_1 – where the set of fixed open texts, which are not suitable for the further formation of cryptograms.

Step 4. Formation of the truncated error vector: e_x=*e*(*A*) – IV_2, where IV_2 – is the elements of the reduction (h_e –

http://dx.doi.org/10.21511/dm.4(4).2018.03

the symbols of the vector of the error vector that are equal to zero, $|h|=1/2e$, i.e. $\mathring{a}_i = 0, \forall \mathring{a}_i \in h$).

Step 5. Formation of the codec:

$$S^*_{r-h_e} = \left(e_n - h_e\right) \cdot H_x^{EC^T}. \qquad (20)$$

Step 6. Formation of the redundancy text of the CFT and the damage to the CHD.

The algorithm for decoding the codec in the modified of Niederreiter's CCS is presented in the form of a sequence of steps:

Step 1. Entering the redundancy text of the CFT, that is decomposable. The introduction of a private key - the matrices X, P, D. The introduction of the redundancy of CHD.

Step 2. Getting the length of the remainder and splitting the redundancy text.

Step 3. Get the S_{Xi} character of the codec and create a complete codec

$$S_X = S_{Xi} \| S_{Xi} \| \ldots \| S_{Xn..} \qquad (21)$$

Step 4. Finding one of the possible solutions of the equation

$$S^*_{r-h_e} = \bar{c}^* \left(H_x^{EC}\right)^T. \qquad (22)$$

Step 5. Removal of diagonal and residual matrices:

$$\bar{c}^* = c_x^* \cdot D^{-1} \cdot P^{-1} \cdot \qquad (23)$$

Step 6. Decoding the vector $\bar{c}^*$. Formation of the vector $\mathring{a}_{\tilde{o}}'$.

Step 7. Converting the vector $\mathring{a}_{\tilde{o}}'$:

$$\mathring{a}_{\tilde{o}} = \mathring{a}_{\tilde{o}}' \cdot P \cdot D. \quad (24)$$

Step 8. Formation of the desired error vector $\mathring{a}: \mathring{a} = \mathring{a}_{\tilde{o}} + IV_2$.

Step 9. Transforming the vector *e* based on the use of non-binary equilibrium code into the information sequence.

5. DISCUSSION

In the works (Evseev et al., 2016; Yevseiev, 2017; Yevseiev, & Korol, 2018; Yevseiev et al., 2017), comparisons were made between the McEliece's MCCS on MEC and HCCS with the use of modified elliptic codes. Results of researches of practical realization MCCS on MEC confirm that the number of group operations has been reduced by 4.5 times due to the construction of the GF (26-24).

In Table 3 shows the results of investigations of capacitive characteristics in the program realization of the field power of the HCCS scheme of McEliece on the MEC. In addition, the use of EU (MES) constructed on flat curves of the third kind provides formation of generating or verification matrices by finding the value of generator functions at the points of the curve. This allows to synthesize methods of constructing corresponding matrices with elements of geometric curves, which cannot be achieved by V. Sidelnikov's attack.

Table 3. The dependence of the software implementation speed on the power of the field (number of group operations)

Cryptographic algorithms	power GF(2m)						
	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}
McEliece on shortened MEC	8,293,075	10,007,947	17,787,431	28,595,014	44,079,433	61,974,253	79,554,764
McEliece on extended MEC	8,506,422	11,156,138	18,561,228	33,210,708	48,297,112	65,171,690	84,051,337
HCCS on MCCS McEliece on extended MEC	5,612,316	7,900,315	14,892,945	25,565,274	42,279,183	58,963,778	76,564,173
HCCS on MCCS McEliece on shortened MEC	5,942,627	7,905,257	14,682,411	25,595,014	42,116,327	58,468,143	75,474,764

For statistic studies of the stability of the investigated cryptosystems we will use the package NIST STS 822 (Yevseiev et al., 2017). The results of the studies are shown in Table 4.

Table 4. Results of research on statistical safety

Cryptosystems	The number of tests in which the testing passed more than 99% of the sequences	The number of tests in which tests were over 96% of the sequences	The number of tests in which testing was less than 96% of the sequences
CCS McEliece	149 (78.83%)	189 (100%)	0 (0%)
MCCS McEliece on shortened MEC	151 (79.89%)	189 (100%)	0 (0%)
MCCS McEliece on extended MEC	152 (80.42%)	189 (100%)	0 (0%)
HCCSRC on extended MEC	153 (80.95%)	189 (100%)	0 (0%)
HCCSRC on shortened MEC	155 (82 %)	189 (100%)	0 (0%)

Listed in Table 4 indicators showed that despite the decrease of the Galois field power to $GF(2^6)$ for MCCS and $GF(2^4)$ for HCCS respectively, the statistical characteristics of such cryptographic code designs were at least not worse than the traditional McEliece's CCS on $GF(2^{10})$. All cryptosystems passed 100% tests, with the best result revealed by the HCCSRC on shortened MEC: 155 out of 189 tests passed at the level of 0.99, which is 82% of the total number of tests. At the same time, the traditional McEliece's CCS on $GF(2^{10})$ showed 149 tests at 0.99.

CONCLUSIONS

The analysis of the crypto-code designs construction on modified elliptic codes and synthesis with multi-channel cryptography lossy procedures allow to build complex (hybrid) cryptosystems that provide the basic data security services in the conditions of hybrid threats of post-quantum cryptography. The proposed CCS provide the security of information resources (the safe time – $\grave{O}_{\acute{A}} > 200$ p., resistance to cryptanalysis of $Ð_{\hat{E}} < 10^{25} - 10^{35}$ of group operations), authenticity of data transmission ($P_{пом} < 10^{-9}$) and reduction of energy costs for their practical realization in 10^{-12} times (encryption, decryption) by reducing the order $GF(q)$.

Using of algebra-geometric codes (codes on elliptic curves) and their modifications eliminates the possibility of implementing V. Sidelnikov's attack (finding an impedance-proof verification matrix), which greatly enhances the crypto stability of the system under post-quantum cryptography. The implementation of the proposed cryptosystems allows to increase the level of protection of information resources of Internet protocols and to create competitive conditions for alternative use in post-quantum cryptography.

REFERENCES

1. Androshchuk, G. O. (2017). Cybersecurity: Trends in the World and Ukraine (pp. 30-36). *Cyber security and intellectual property: problems of legal provision.* Kyiv: Vyd-vo "Politekhnika".
2. Babych, E. U. (2016). Забезпечення кібербезпеки в Україні [Zabezpechennya kiberbezpeky v Ukrayini] (pp. 77-78). *Aktualni zadachi ta dosyahnennya u haluzi kiberbezpeky.* Kropivnitsky: KNTU.
3. Baldi, M., Bianchi, M., Chiaraluce, F., Rosenthal, J., & Schipani, D. (2016). Enhanced public key security for the McEliece cryptosystem.

http://dx.doi.org/10.21511/dm.4(4).2018.03

Journal of Cryptology, 29(1), 1-27. Retrieved from https://link.springer.com/article/10.1007/s00145-014-9187-8
4. Baranov, O. A. (2014). Про тлумачення та визначення поняття «кібербезпека» [Pro tlumachennya ta vyznachennya ponyattya «kiberbezpeka»]. *Pravova informatyka, 2,* 54-62.
5. Bassham, L. E., Rukhin, A. L., Soto, J., Nechvatal, J. R., Smid, M. E., Leigh, S. D., Levenson, M., Vangel, M., & Heckert, N. A. (2010). A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. *Special Publication (NIST SP).* Retrieved from http://www.nist.gov/manuscript-publication-search.cfm?pub_id=151222
6. Chen, L., Jordan, S., Liu, Y-K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). *Report on Post-Quantum Cryptography.* http://dx.doi.org/10.6028/NIST.IR.8105
7. Cho, J. Y., Griesser, H., & Rafique, D. (2017). A McEliece-based key exchange protocol for optical communication systems. *Proceedings of the 2nd Workshop on Communication Security* (pp. 109-123). Retrieved from https://link.springer.com/chapter/10.1007%2F978-3-319-59265-7_8
8. De Vries, S. (2016). *Achieving 128-bit security against Quantum Attacks in OpenVPN* (Master Thesis). University of Twente. Retrieved from https://internetscriptieprijs.nl/wp-content/uploads/2017/04/1-Simon-de-Vries-UT.pdf
9. Dinh, H., Moore, C., & Russell, A. (2011). *McEliece and niederreiter cryptosystems that resist quantum fourier sampling attacks.* Proceeding Crypto 11 Proceedings of the 31st annual conference on advances in cryptology (pp. 761-779). Retrieved from https://dl.acm.org/citation.cfm?id=2033093
10. Dudikevich, V. B., Kuznetsov, O. O., & Tomashevsky, B. P. (2010). Крипто-кодовий захист інформації з недвійковим рівно ваговим кодуванням [Krypto-kodovyy zakhyst informatsiyi z nedviykovym rivnovahovym koduvannyam]. *Suchasnyi zakhyst informatsii, 2,* 14-23.
11. Dudikevich, V. B., Kuznetsov, O. O., & Tomashevsky, B. P. (2010). Метод недвійкового рівноважого кодування [Metod nedviykovoho rivnovahovoho koduvannya]. *Suchasnyi zakhyst informatsii, 3,* 57-68.
12. Evseev, S., Rzaev, H., Korol, O., & Imanova, Z. (2016). Разработка модифицированной несимметричной крипто-кодовой системы мак-элиса на укороченных эллиптических кодах [Razrabotka modifitsirovannoy nesimmetrichnoy kripto-kodovoy sistemy Mak-Elisa na ukorochennykh ellipticheskikh kodakh]. *Eastern-European Journal of Enterprise Technologies*, *4/9*(82), 18-26. Retrieved from http://journals.uran.ua/eejet/article/viewFile/75250/80864
13. Grischuk, R. V., & Danik, Y. G. (2016). *Основи кібербезпеки [Osnovy kiberbezpeky]* (636 p.). Zhitomir: ZhNAEU.
14. Hryshchuk, R. & Molodetska-Hrynhchuk, K. (2018). Foundation of State's Information Security in Social Networking Services in Conditions of Hybrid War. *Information & Security: An International Journal, 41*, 55-73.
15. Hryshchuk, R., & Molodetska, K. (2016). Synergetic Control of Social Networking Services Actors' Interactions. *Recent Advances in Systems, Control and Information Technology, 543*, 34-42. http://dx.doi.org/10.1007/978-3-319-48923-0_5
16. Kuchuk, G., Kharchenko, V., Kovalenko, A., & Ruchkov, E. (2016). Approaches to Selection of Combinatorial Algorithm for Optimization in Network Traffic Control of Safety-Critical Systems. *IEEE East-West Design & Test Symposium (EWDTS),* 384-389. http://dx.doi.org/10.1109/EWDTS.2016.7807655
17. Kuchuk, N., Mozhaiev, O., Mozhaiev, M., & Kuchuk, H. (2017). Method for calculating of R-learning traffic peakedness. *4th International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T)* (pp. 359-362). http://dx.doi.org/10.1109/INFOCOMMST.2017.8246416
18. Leonenko, G. P., & Yudin, A. Y. (2013). Проблемы обеспечения информационной безопасности систем критически важной информационной инфраструктуры Украины [Problemy obespecheniya informatsionnoy bezopasnosti sistem kriticheski vazhnoy informatsionnoy infrastruktury Ukrainy]. *Information Technology and Security, 1*(3), 44-48.
19. Mishchenko, V. A., & Vilansky, Yu. V. (2007). *Damage texts and multichannel cryptography* (292 p.). Minsk: Encyclopedic.
20. Mishchenko, V. A., Vilansky, Yu. V., & Lepin V. V. (2006). *The cryptographic algorithm MV 2.* Minsk.
21. Morozov, K., Roy, P. S., & Sakurai, K. (2017). On unconditionally binding code-based commitment schemes. *Proceeding IMCOM 17 Proceedings of the 11th International Conference on Ubiquitous Information Management and Communication.* USA: NY, New York. http://dx.doi.org/10.1145/3022227.3022327
22. Mozhaev, O., Kuchuk, H., Kuchuk, N., Mykhailo, M., & Lohvynenko, M. (2017). Multiservice network security metric. *2nd International Conference on Advanced Information and Communication Technologies (AICT)* (pp. 133-136). http://dx.doi.org/10.1109/AIACT.2017.8020083
23. Niederreiter, H. (1986). Knapsack type cryptosystems and algebraic coding theory. *Probl. Control and Inform. Theory, 15,* 19-34.
24. Sidelnikov, V. M., (2008). *Теория кодирования [Teoriya kodirovaniya]* (324 p). M.: Fyzmatlyt.
25. Yevseiev, S. (2017). The Use of Damage Codes in Crypto-Code Systems. *Information Processing Systems, 5*(151), 109-121. Retrieved from http://www.hups.mil.gov.ua/periodic-app/article/18004/eng
26. Yevseiev, S., & Korol, O. (2018). Theoretical and methodological principles of construction of hybrid crypto-code structures on the loss codes. *Information economy: stages of development, management methods, models.* Kharkiv: VSEM, KhNEU.
27. Yevseiev, S., & Tsyhanenko, O. (2018). Розробка несиметричної крипто-кодової конструкції Нідеррайтера на модифікованих еліптичних кодах [Rozrobka nesimetrichnoї kripto-kodovoї konstrukcії Niderrajtera na modifikovanih eliptichnih kodah]. *Information Processing Systems, 2*(153), 127-135. Retrieved from http://www.hups.mil.gov.ua/periodic-app/article/18788
28. Yevseiev, S., Kots, H., & Liekariev, Y. (2016). Developing of multi-factor authentication method based on Niederreiter-McEliece modified crypto-code system. *Eastern-European Journal of Enterprise Technologies, 6/4*(84), 11-23. https://doi.org/10.15587/1729-4061.2016.86175
29. Yevseiev, S., Kots, H., Minukhin, S., Korol, O., & Kholodkova, A. (2017). The development of the method of multifactor authentication based on hybrid crypto-code constructions on defective codes. *Eastern-European Journal of Enterprise Technologies, 5/9*(89), 19-35. https://doi.org/10.15587/1729-4061.2017.109879