Використання модифікованої крипто-кодової конструкції (МККК) Нідеррайтера з додатковими векторами ініціалізації (з множиною неприпустимих позиційних векторів вектора помилок і множиною позицій укорочення вектора помилки) вимагає збільшення швидкодії криптоперетворень системи вцілому. 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. Такий підхід дозволяє будувати гібридні крипто-кодові конструкції на основі синтезу модифікованих криптокодових конструкцій Нідеррайтера на модифікованих (укорочених або подовжених) кодах на елиптичних кривих з процедурами нанесення збитку. Суттєвою відмінністю від класичних гібридних (комплексних) криптосистем є використання несиметричної криптосистеми для забезпечення безпеки даних з швідкими процедурами криптоперетворень (формування та розкодування кодограми). В роботі розглядаються способи побудови збиткових кодів і підходи використання в гібридної крипто-кодової конструкції Нідеррайтера на модифікованих еліптичних кодах. Пропонуються практичні алгоритми використання механізму нанесення збитку MV2 в крипто-кодової конструкції Нідеррайтера на модифікованих еліптичних кодах, що дозволяє реалізувати гібридну крипто-кодову конструкцію. Наведені результати порівняльної оцінки енерговитрат на формування інформаційної посилки при різних способах нанесення збитку, що визначило вибір способу нанесення збитку в практичних алгоритмах. Проведені дослідження підтверджують конкуренту спроможність запропонованої криптосистеми в Інтернет-технологіях та мобільних мережах, забезпечення практичної реалізації на сучасних платформах та необхідної криптостійкості в умовах постквантової криптографії

Ключові слова: збиткові коди, гібридна крипто-кодова конструкція Нідеррайтера, модифіковані еліптичні коди, багатоканальна криптографія

UDC 621.391
DOI: 10.15587/1729-4061.2019.156620

DEVELOPMENT OF NIEDERREITER HYBRID CRYPTO-CODE STRUCTURE ON FLAWED CODES

S. Yevseiev
Doctor of Technical Sciences, Senior Researcher*
E-mail: serhii.yevseiev@hneu.net
O. Tsyhanenko
Postgraduate student*
A. Gavrilova
Senior Lecturer*
V. Guzhva
PhD, Associate Professor, Professor**
O. Milov
PhD, Associate Professor*
V. Moskalenko
PhD, Associate Professor**
I. Opirskyy
Doctor of Technical Sciences
Department of Information Security
Lviv Polytechnic National University
S. Bandery str., 12, Lviv, Ukraine, 79013
O. Roma
Doctor of Technical Sciences, Senior Researcher
Department No. 1
Institute of Special Communication and Information Security
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute"
Verhniokluchova str., 4, Kyiv, Ukraine, 03056
B. Tomashevsky
PhD, Senior Researcher
Department of Cyber Security
Ternopil Ivan Puluj National Technical University
Ruska str., 56, Ternopil, Ukraine, 46001
O. Shmatko
PhD, Associate Professor**
*Department of Cyber Security and Information Technology
Simon Kuznets Kharkiv National University of Economics
Nauky ave., 9-A, Kharkiv, Ukraine, 61166
**Department of Software Engineering and
Information Technology Management
National Technical University "Kharkiv Polytechnic Institute"
Kyrpychova str., 2, Kharkiv, Ukraine, 61002

1. Introduction

Today, cybersecurity can be fully considered an important aspect of the activity of any society. With the rapid development of the information environment of the Internet, the complexity and laboriousness of the formation of information protection from unauthorized access, the growth of vulnerabilities of critical systems to hybrid cyberattacks is

a significant problem for different users [1–3]. In addition, despite the fact that most organizations are improving information protection systems, cybercriminals continue to find ways to circumvent them, carrying out destructive activities. Information protection involves achieving and maintaining security properties in user resources that are aimed at preventing relevant cyber threats [4–7]. As a result, the development of high-quality software products and digital equipment of national production will increase the level of cyber security of the state.

In [8], an approach to using flawed codes in crypto-code systems was proposed. This approach allows building complex cryptosystems based on the synthesis of crypto-code structures (CCS) (a model of provable stability) and cryptosystems on flawed codes (multichannel cryptography). This approach allows reducing energy costs in the practical implementation of the Niederreiter CCS on the modified (MCCS) (shortened/elongated) elliptic codes (*MEC*) while maintaining the cryptographic resistance of the whole system.

2. Literature review and problem statement

In [8–11], approaches to ensuring security and speed of data processing were proposed, but special attention should be paid to crypto-code systems based on the McEliece and Niederreiter schemes, which are quantum-stable [12, 13].

In [13], the McEliece-Niederreiter combined scheme was proposed; however, like the traditional Niederreiter scheme, the authors consider equilibrium coding in the Niederreiter scheme on binary codes, which does not allow building cryptosystems with the required level of cryptographic resistance. This is confirmed by the results of studies in [14]. An additional complication in the form of using two schemes is a forced step towards the performance of the described construction, which resulted in a decrease in performance and an increase in energy intensity.

In [14], an attack on the McEliece and Niederreiter schemes based on linear-fractional transformations is shown, which allow us to find the generating (check) matrix and crack the cryptosystem. Therefore, a promising direction is the development of McEliece and Niederreiter schemes on algebraic geometric codes (codes based on elliptic curve parameters) or cascade codes.

In [15], the possibility of practical implementation of the Niederreiter asymmetric crypto-code system on elliptic codes was touched upon, but it requires an increase in the speed of crypto-transformations.

In [16, 17], approaches to the implementation of McEliece CCS under post-quantum cryptography are proposed.

In [18], an approach to the implementation of the Niederreiter MCCS on *MEC* is proposed. However, the disadvantage is a slight reduction in energy consumption.

In [19, 20], an equilibrium coding method based on *m*-th codes (Reed-Solomon codes) was proposed; however, the disadvantage is the lack of a practical algorithm for decoding the syndrome on the receiving side and the possibility of hacking based on an adjustable decoder.

In [21], the authors confirm the complexity of the practical implementation of the Niederreiter scheme and consider the possibility of using cryptosystems in *VPN* channels.

In [22], the authors propose to use Reed-Solomon (*RS*) codes when constructing an asymmetric crypto-code system based on the McEliece scheme. However, the authors do not take into account the possibility of hacking a cryptosystem based on linear fractional transformations.

In [23], the authors proposed to use the Niederreiter asymmetric crypto-code system on elliptic codes [23]. This approach provides protection against possible attacks, and the required level of cryptographic strength. However, an unresolved issue is the difficulty of practical implementation with the required power of the $GF(2^{10}–2^{13})$ field to ensure a guaranteed level of cryptographic strength.

The analysis [13–23] showed a significant interest in the practical implementation and use of McEliece and Niederreiter CCS in the context of post-quantum cryptography. However, the proposed versions of the Niederreiter cryptosystem on binary and non-binary block codes do not take into account the possibility of an attack based on fractional-linear transformations, which does not allow for the required level of stability of the proposed solutions. The proposed approach to reducing energy consumption during the implementation of McEliece CCS on flawed codes in [8] allows for the reduction of energy consumption and the required level of durability. Therefore, it is advisable to develop a Niederreiter CCS using flawed codes, which will reduce the power of the $GF(2^4)$ field with a guaranteed level of strength and form the Niederreiter hybrid crypto-code structure (HCCS) on *MEC*.

3. The aim and objectives of the study

The aim of the study is to develop the Niederreiter hybrid crypto-code structure based on the analysis of methods of using flawed codes, practical encryption algorithms (codogram generation) and decryption (decoding codogram) on modified (shortened) elliptic codes.

To achieve this aim, the following objectives were considered:

– to analyze the principles of formation of the Niederreiter MCCS on flawed codes, taking into account the regularity of the necessary fixation of positional vectors of the plaintext to form the error vector during equilibrium coding of non-binary codes;

– to develop practical transformation algorithms in the Niederreiter CCS on modified (shortened) elliptic codes with flawed codes;

– to analyze the costs of software implementation of the hybrid cryptosystem on the crypto-code structure with flawed codes, to assess the strength of the proposed cryptosystem.

4. Analysis of construction principles of Niederreiter MCCS on flawed codes

In [24], a code cryptosystem was proposed based on masking a check matrix of an algebraic block code. The main advantage of Niederreiter ACCS is the high speed of information conversion (the relative coding speed is close to 1). In [19, 20], an algorithm for equilibrium coding on non-binary codes and an algorithm for generating cryptograms in the Niederreiter crypto-code system on Reed-Solomon codes are proposed.

To reduce energy costs with a guaranteed level of security, the Niederreiter MCCS on *MEC* was proposed in the work [8, 15].

This approach provides a reduction in the field power and allows you to implement the classic version of the Niederreiter scheme with a guaranteed level of cryptographic strength.

Consider the overall Niederreiter MCCS on *MEC*: let the set

$$M_C = \left\{M_1, M_{2,} ... M_{q^k}\right\},$$

of all open texts (n, k, d) of the block code. We define the set of fixed open texts $M_F = \left\{M_1, M_{2,} ... M_n\right\}$, where

$$M_i^u \cdot P^u \cdot D^u ! = M_i \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1} \cdot P^u \cdot D^u,$$

which are not suitable for further cryptogram generation. This set is proposed to be used as an initialization vector (IV_1). The second vector of initialization forms the vector of positions for shortening the error vector:

$$IV_2 = |h| = ½,$$

where IV_2 is the abbreviation element (h_e is the error vector symbols, equal to zero, $|h|=1/2e$, that is, $e_i=0$, $e_i \in$h).

In the classical Niederreiter scheme at the first stage of cryptogram generation, plaintext characters are converted into error vector symbols based on an equilibrium coding algorithm. The resulting error vector at the second stage of cryptogram generation is "shortened" based on the code shortening algorithm and multiplied by the check matrix of the algebraic (elliptical) code:

$$S^*_{r-h_e} = \left(e_n - h_e\right) \times H_X^{EC^T},$$

where H_X^{ECu} is the check $n \times (n-k)$ matrix of an algebra-geometric block (n, k, d) code with elements from $GF(q)$,

$$H_X^{ECu} = X^u \cdot H \cdot P^u \cdot D^u, \quad u \in \{1, 2, ..., s\},$$

masking matrix mappings defined by the set of matrices $\{X, P, D\}_i$, where X is a non-degenerate $k \times k$ matrix over $GF(q)$, P is a permutational $n \times n$ matrix over $GF(q)$ with one nonzero element in each row and each column of the matrix, D is a diagonal $n \times n$ matrix over $GF(q)$ with nonzero elements on the main diagonal.

After the formation of the key matrices of the private key, the authorized user needs to form elements of the set of fixed open texts that are not suitable for the subsequent formation of a cryptogram (syndrome from the error vector).

Let us consider the basic principles of constructing cryptosystems on flawed codes: in [25, 26], the theoretical and practical bases of the construction of flawed codes are considered. The flawed text refers to the text obtained by further deformation of the non-redundant character codes. Thus, a necessary and sufficient condition for the text flaw with a loss of meaning is the reduction of the lengths of the text character codes beyond their redundancy. As a result, the flawed text has a length shorter than the length of the source text, and does not make sense of the source text [25].

The theoretical basis for the construction of flawed texts is the removal of the ordering of the source text characters and, as a consequence, the reduction of the redundancy of the language characters in the flawed text [25].

At the same time, the amount of information expressing this ordering will be equal to the decrease in the text entropy compared to the maximum possible entropy value, i.e., the equiprobable appearance of any letter after any previous letter [25].

The methods of information calculation proposed in [26] make it possible to identify the ratio of the amount of predictable (i. e. generated by certain rules) information and the amount of unexpected information that cannot be predicted in advance.

Text redundancy is calculated by the formula:

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

where M is the source text; B is language redundancy ($B=R-r$, R is the absolute entropy of the language ($R=\log N$, N is the power of the alphabet, r is the entropy of the language per character, $r=H(M)/L$, L is the message length M in language characters); $H(M)$ – message entropy (uncertainty); L_0 is the message length M in language symbols with meaning; B_A is language redundancy.

To obtain a flawed text (*FTC*) and damage (*DCH*), the method of "perfect" compression after performing m cycles of the damage mechanism C_m is used [25, 26].

The number of cycles required to reduce the length of the source text is:

$$m \rangle \frac{\log n - B_A}{\log \eta},$$

where n is the power of the source symbol representation; B_A is language redundancy; η is the number of times the length of the source text in MV2 is reduced at each step (some constant factor).

A quantitative measure of damage effectiveness is the degree of meaning destruction, equal to the difference between the entropies of the flawed text and the source text on different segments of the flawed text:

$$d = H(FTC) - \sum_{i=1}^{s} H(M_i) p_i,$$

$$\sum_{i=1}^{s} p_i = 1, \quad s = \left[\frac{L_0 - L_{FTC}}{L_{FTC}}\right],$$

where M_i is the part of the source text corresponding to the i-th segment, p_i is its probability, L_0 is the length of Mi and is equal to the length L_{FTC} – flawed text, s is the number of segments.

For an ergodic source of the source text characters:

$$d_{\max} = \log L_{FTC} - H(M_i).$$

Fig. 1 shows a block diagram of one step of the universal mechanism of damage.

The informational core of some text is understood as the flawed text *CFT*, obtained by cyclic transformation of the universal mechanism of damage C_m.

The universal mechanism of damage C_m can be described [30, 31]:

$$CFT/CH_{FT} = E_1(M, KU^{EC}),\ CHD/CH_D = E_2(M, KU^{EC}),$$

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

where $CFT/CH_{FT} = CFT/CH_{FT}^i, ...,\ CFT/CH_{FT}^m$, $KU^{EC} = (K_D^i, ..., K_D^m, KU_1^{EC}, ..., KU_m^{EC})$, $CHD/CH_D = CHD/CH_D^i, ..., CHD/CH_D^m$.

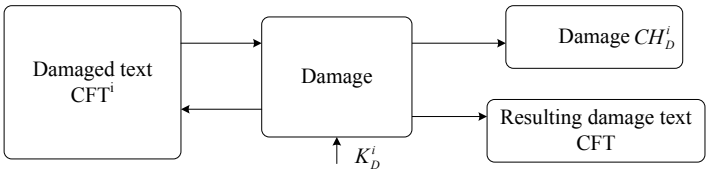

Fig. 1. Block diagram of one step of the mechanism of damage

Thus, we have two ciphertexts: (damage (CH_D) and flawed text (*FTC*)). The resulting texts are meaningless either in the alphabet of the source text, or in the alphabet of the ciphertext. In fact, the ciphertext of the original message (*M*) is represented as a combination of two flawed ciphertexts, each of which separately cannot restore the original text.

To restore the original sequence, there is no need to know intermediate flawed sequences. It is necessary to know only the last flawed sequence (the last flawed text after performing all the cycles) and all the damages with the rules of their application.

Cryptographic flawed texts are texts obtained in the following ways [26]:

– *Approach 1*: damage to the source text with subsequent encryption of the flawed text and/or its damage (Fig. 2);

– *Approach 2*: damage to the ciphertext (Fig. 3);

– *Approach 3*: damage to the source text and the ciphertext of the flawed text (Fig. 4).

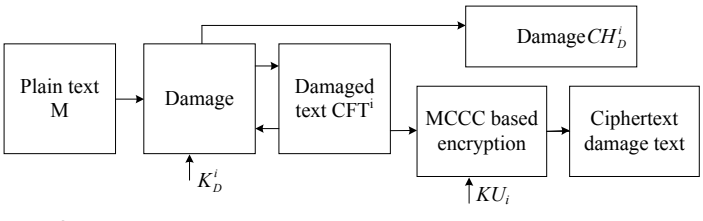

Fig. 2. Block diagram of the hybrid cryptosystem based on damage to the source text (Approach 1)

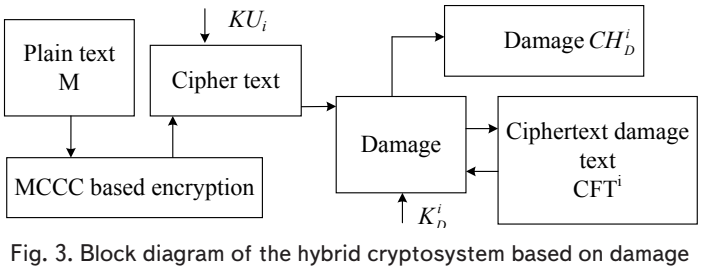

Fig. 3. Block diagram of the hybrid cryptosystem based on damage to the ciphertext (Approach 2)

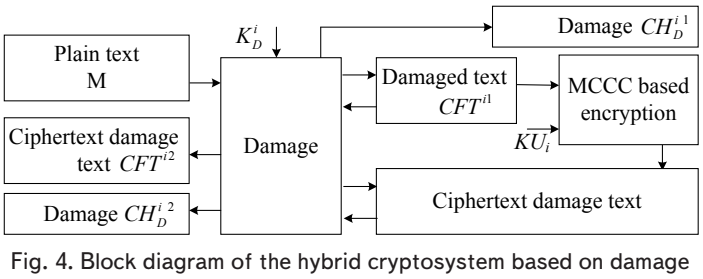

Fig. 4. Block diagram of the hybrid cryptosystem based on damage to the source text and ciphertext (Approach 3)

To determine the optimal method, we analyze the ratio of the number of required additional operations to implement the approach to the size of the resulting outgoing data. The dependence of group operations of ACCS implementation field power is given in Table 1.

Table 1

Dependence of software implementation on field power (number of thousands of additional operations before encryption/after/total)

Approach	2^5	2^7	2^9	2^{11}
1	1002/–/1002	3285/–/3285	6322/–/6322	11078/–/8247
2	–/1501/1501	–/4289/4289	–/9296/9296	–/15908/15908
3	992/1487/2479	2952/4428/7380	5793/8690/14483	10086/15130/25216

Table 2 shows the length of transmitted data.

Table 2

Length of transmitted data in bytes

Approach	2^5	2^7	2^9	2^{11}
1	500902	902403	1642357	2374489
2	375298	667029	1072313	1652979
3	627533	1044069	1868102	2716713

The ratio of these values shows the bit rate of throughput for each additional operation (Table 3).

Table 3

Number of bits per additional operation

Approach	2^5	2^7	2^9	2^{11}
1	2,5E-04	4,55E-04	4,812E-04	4,341E-04
2	4,999E-04	8,038E-04	**10,836E-04**	**12,03E-04**
3	4,938E-04	8,836E-04	9,691E-04	11,602E-04

Thus, using the approach to damage the ciphertext with the Niederreiter MCCS on *MEC*, presented in Fig. 4 (third approach) increases throughput starting from the *GF* field (2^9). This method is the best approach for building the Niederreiter hybrid CCS on *MEC*. The synthesis of the Niederreiter *MEC* crypto-code structure with a cryptosystem on flawed codes proposed by the authors allows building complex (hybrid) crypto-code structures whose stability is determined by the strength of two cryptosystems to ensure the implementation of fast crypto-transformations by reducing the field power.

Consider the algorithms for the practical implementation of the cryptogram formation and decoding based on the Niederreiter crypto-code structure on *MEC* using flawed texts and damaging the ciphertext.

5. Practical algorithms for generating and decrypting cryptograms

The algorithm for generating a cryptogram in the Niederreiter hybrid CCS on *MEC* using flawed texts will be represented as a sequence of steps (Fig. 5):

Step 1. Entering the information to be encoded, one of the elements of the set of suitable open texts. Introduction of 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 non-binary equilibrium coding algorithm.

Step 3. Formation of the initialization vector IV_1.

Step 4. Formation of a shortened error vector: $e_x=e(A)-IV_2$.

Step 5. Formation of the codogram:

$$S^*_{r-h_e}=(e_n-h_e)\times H_X^{EC^T}.$$

Step 6. Formation of the flawed text *CFT* and damage CHD.

The algorithm for decoding a codogram in the Niederreiter hybrid CCS on *MEC* using flawed texts is presented as a sequence of steps (Fig. 6):

Step 1. Entering the flawed text *CFT*, which is decoded. Introduction of the private key *–X, P, D* matrices. Introduction of damage *CHD*.

Step 2. Getting the length of the remnants and splitting the flawed text.

Step 3. Obtaining the S_{Xi} characters of the codogram and forming the complete codogram $S_X==S_{Xi}\,||S_{Xi}||...||S_{Xn}$.

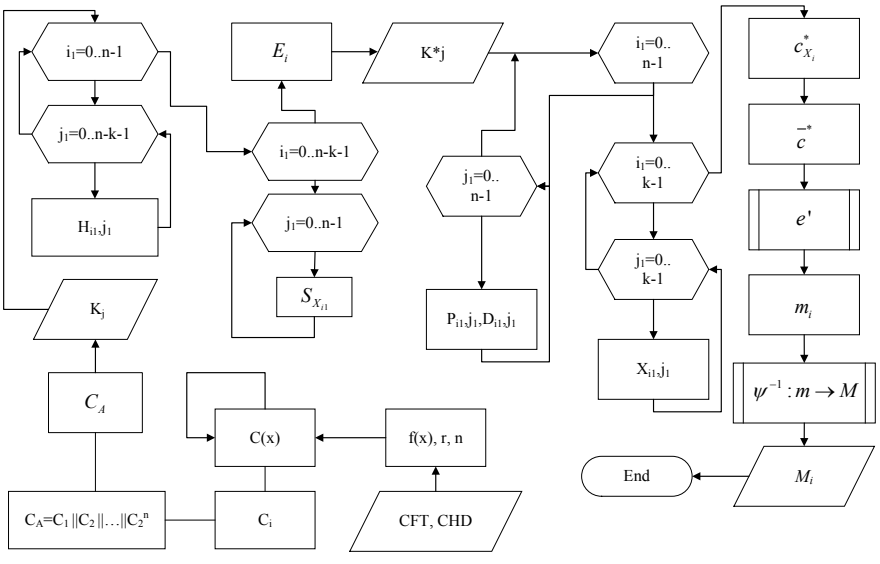

Fig. 6. Algorithm for decoding codograms in the Niederreiter hybrid CCS on *MEC*

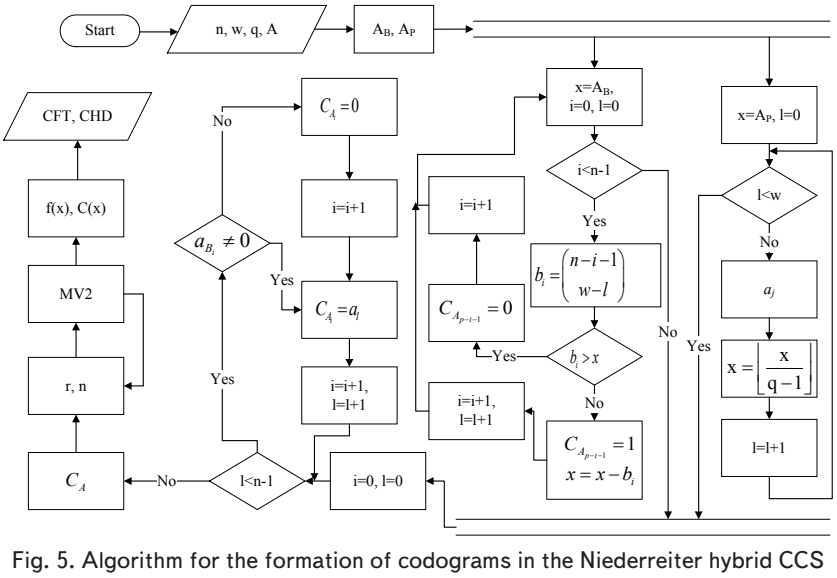

Fig. 5. Algorithm for the formation of codograms in the Niederreiter hybrid CCS on *MEC*

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

$$S^*_{r-h_e}=\vec{c}^{\,*}\times\left(H_X^{EC}\right)^T.$$

Step 5. Removing the action of the diagonal and permutation matrices:

$$\vec{c}^{\,*}=c_X^*\cdot D^{-1}\cdot P^{-1}.$$

Step 6. Decoding the vector $\vec{c}^{\,*}$. Formation of the vector e_x'.

Step 7. Converting the vector e_x'.

$e_x=e_x'\times P\times D$.

Step 8. Formation of the desired error vector e: $e=e_x+IV_2$.

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

Thus, the proposed algorithms make it possible to practically implement the Niederreiter hybrid CCS on *MEC* using flawed texts. This approach allows the use of the proposed Niederreiter HCCS in Internet protocols and provides a guaranteed level of cryptographic security.

We will conduct a study on the evaluation of the energy costs of the software implementation of the proposed Niederreiter hybrid crypto-code structure *MEC* with flawed codes, investigating their cryptographic strength based on the NIST STS 822 statistical package.

6. Evaluation of energy costs for software implementation of the proposed hybrid cryptosystem

To estimate the time and speed indicators, it is common to use the unit of measurement *cpb*, where *cpb* (*cycles per byte*) is the number of processor cycles that need to be spent to process 1 byte of incoming information.

The complexity of the algorithm is calculated by the expression

$$Per = Utl * CPU\_clock / Rate,$$

where *Utl* is the utilization of the processor core (%); *Rate* is the algorithm bandwidth (byte/s).

Table 4 shows the results of studies of the dependence of the input sequence length on the *MV2* algorithm on the number of processor cycles.

Table 4

Results of studies of the dependence of the input sequence length on the MV2 algorithm on the number of processor cycles

Length of the code sequence		*MV*2		
		10	100	1000
Number of function calls implementing elementary operations	Summation	3942	28673	275499
	Difference	1794	3810	23881
	Division	3274	4804	20104
	Multiplication	19	109	1009
	Comparison	8939	60963	578784
Summ		17968	98359	899277
Duration of the functions * in processor cycles	Summation	19,53	93,58	2297,36
	Difference	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	4826,43
Summ		89	321	7499
Duration of execution ** in ms		89	321	7499

*Note: * – the duration of 1,000 operations in processor cycles: reading a character – 27 cycles, string comparison – 54 cycles, string concatenation – 297 cycles; ** – for the calculation, a processor with a clock frequency of 2 GHz was used, taking into account the load by the operating system of 5 %*

Table 5 shows the results of studies assessing the time and speed indicators of the procedures for applying and removing damage.

Table 5

Results of studies assessing the time and speed indicators of the procedures for applying and removing damage

Indicators	Length of the code sequence	Algorithm throughput rate (bytes/s)	CPU core utilization (%)	Algorithm complexity, Per (cpb)	Indicators
The number of function calls that implement elementary operations	10	0,089	112,3596	90	0,801
	100	0,321	311,5265	322	1,034
	1,000	7,499	133,3511	7500	66,166

Table 6 shows the results of studies of the dependence of the length of the code sequence of the Niederreiter hybrid CCS on the number of processor cycles for performing elementary operations in the software implementation of crypto-code systems.

Analysis of the results of Table 6 showed that the energy intensity of the practical implementation of the Niederreiter HCCS will decrease by 7 %, while implementation is possible on the main software and hardware platforms that are widely used:

– 8/16 bit microcontrollers and smart cards;

– 32-bit microprocessors and microcontrollers (ARM, IA 32);

– 64-bit general-purpose processors (AMD64, Intel 64).

Table 7 shows the results of studies assessing the time and speed indicators of the procedures for applying and removing damage.

Table 7

Results of studies assessing the time and speed indicators of the procedures for applying and removing damage

Indicators	Length of the code sequence	Work time (s)	Algorithm throughput rate (bytes/s)	CPU core utilization (ticks)	Algorithm complexity, Per (cpb)
The number of function calls that implement elementary operations	10	0,089	112,3596	90	0,801
	100	0,321	311,5265	322	1,034
	1000	7,499	133,3511	7500	66,166

Thus, the conducted analysis of the basic principles of constructing Niederreiter modified crypto-code structures and multi-channel cryptography systems on flawed codes allows us to develop hybrid cryptosystems. The main difference from the "classical" approach to the formation of a hybrid cryptosystem is the use of asymmetric crypto-code structures with fast crypto-transformation algorithms (the speed of transformations is comparable to the speed of crypto-transformation in the BSC). The Niederreiter CCS is the main mechanism for ensuring the stability (security) of information with the subsequent use of the *MV2* algorithm (a system on flawed codes). This approach reduces energy costs (the power of the Niederreiter MCCS alphabet) and then transfers it in one or more channels.

Table 6

Results of studies of the dependence of the length of the code sequence on the number of processor cycles

Length of the code sequence		Niederreiter HCCS on *MEC*			Niederreiter CCS on *MEC*		
		10	100	1000	10	100	1000
Number of function calls implementing elementary operations	Character reading	10 294 397	28 750 457	76 759 874	11 018 042	30 800 328	80 859 933
	String comparison	3 406 921	9 246 748	25 478 498	3 663 356	10 199 898	26 364 634
	String concatenation	1 705 544	5 045 748	12 379 422	1 834 983	5 125 564	13 415 329
Summ		15 406 862	43 042 953	114 617 794	16 516 381	46 125 790	120 639 896
Duration of the functions * in processor cycles	Character reading	295374	810478	2 001 167	297 487	831 609	2 183 218
	String comparison	178 814	531 379	1 248 684	197 821	550 794	1 423 690
	String concatenation	544 990	1 328 114	3 586 486	544 990	1 522 293	3 984 353
Summ		1 006 781	2 749 548	7 247 488	1 040 298	2 904 696	7 591 261
Duration of execution ** in ms		0,52	1,37	3,4	0,55	1,53	4

*Note: ** – for the calculation, a processor with a clock frequency of 2 GHz was taken, taking into account the load by the operating system of 5 %*

7. Evaluation of the cryptographic strength of the proposed hybrid cryptosystem

To assess the cryptographic strength of the proposed cryptosystem, we consider separately each of the components of the hybrid (integrated) cryptosystem.

The McEliece and Niederreiter crypto-code structures belong to the secret models of provable resistance [14] based on the theoretical complexity problem – decoding of a random code. Thus, for an authorized user, the encoding and decoding procedures are polynomially complex tasks, and for an attacker, an NP-complete problem, with an increase in (n, k, d) parameters, the complexity increases exponentially.

Suppose a code cryptosystem is used that is constructed by masking an algebraic block (n, k, d) code over $GF(q)$. Cryptanalysis of such a system consists in solving the problem of decoding a masked (n, k, d) code over $GF(q)$ without using a fast (polynomial complexity) rule that defines a secret key.

The volume of the secret key (the dimension of the X, P, D matrices) is

$$l_{\text{c.d.}} = \left(k^2 + n^2\right) \cdot \log_2 q \text{ bit},$$

$k \times k$ elements from $GF(q)$ of the X matrix and $n \times n$ elements from $GF(q)$ of the $\Lambda = P \cdot D$ matrix.

Consequently, the complexity of the implementation of the most simple attack, aimed at a total bust of secret key data, is

$$S_{\text{p.d.}} = 2^{l_{\text{c.d.}}}.$$

At the same time, cryptanalysis can be performed by one of the currently known non-algebraic decoding algorithms, which allow a universal way to solve the decoding problem (n, k, d) of a code over $GF(q)$ by the brute force methods. Let us analyze the most computationally efficient non-algebraic coding methods, investigate their capabilities in solving the cryptanalysis problem of the developed crypto-code information protection tools.

The simplest and most effective method for decoding redundant block codes of small length is the correlation method, which is based on comparing the received code word with errors with all code words and choosing the nearest code word (in the Hamming metric) [28–31]. This method allows decoding according to the maximum likelihood criterion (the maximum similarity criterion of the received word with errors and the code word identified by it) and is optimal from the point of view of minimizing the error of decoding the code word [28–31]. The complexity of the implementation of correlation decoding (n, k, d) of the code over $GF(q)$ is estimated as

$$S_{c.d.} = q^k.$$

The tabular (syndromic) decoding method is somewhat simpler than the correlation one, but it assumes the linearity of the code word being used [28–31]. The codes used in the developed cryptosystems are linear, therefore, an attacker can use syndromic decoding to solve the cryptanalysis problem.

The basis of tabular (syndromic) decoding is the comparison of the syndrome sequence to possible error vectors. To implement non-algebraic decoding of a linear block code with an arbitrary structure, it is sufficient to keep the correspondence of all syndrome sequences and error vectors, for example, in the form of a 2×N table, where N is the power of the set of error vectors that can potentially be corrected by the used (n, k, d) code over $GF(q)$.

Suppose that (n, k, d) code over $GF(q)$ can potentially correct all errors, up to $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ and cannot fix other errors. Then

$$N = \sum_{i=1}^{\left\lfloor \frac{d-1}{2} \right\rfloor} (q-1)^i \cdot \frac{n!}{i! \cdot (n-i)!},$$

and the complexity of the implementation of syndromic decoding is estimated by the expression:

$$S_{\text{s.d.}} = 2N.$$

Another, the most effective method of non-algebraic decoding is a permutation decoder. This method allows decoding a linear block code with an arbitrary structure in a finite number of steps.

In essence, it consists of a sequential transformation of a codeword and a permutation of characters that are invariant with respect to the code. In the monographs [28–31], an estimate of the complexity of the implementation of the permutation decoder is obtained as an expression:

$$S_{\text{p.d.}} \geq \left\lceil \frac{n}{n-k} \left\lceil \frac{n-1}{n-k-1} \ldots \left\lceil \frac{n-t-1}{n-k-t-1} \right\rceil \right\rceil \right\rceil, \quad t = \left\lfloor \frac{d-1}{2} \right\rfloor.$$

Fig. 7–9 show the dependences of the complexity of various cryptanalysis methods based on non-algebraic decoding of redundant block codes (on the correlation, syndrome, and permutation decoder). The score is given on a logarithmic scale.

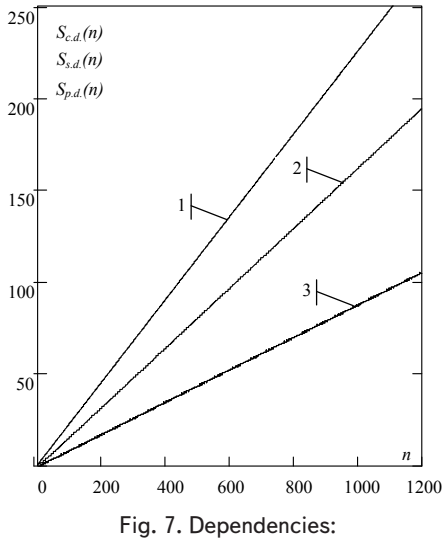

Fig. 7. Dependencies:
$1 - S_{\text{c.d.}}(\text{n})$, $2 - S_{\text{s.d.}}(\text{n})$, $3 - S_{p.d.}(\text{n})$ for $q = 2$, $k = 0{,}75 \cdot n$

As follows from the above dependencies, already with the code length, the correlation and syndromic decoding methods become computationally inefficient, their application for cryptanalysis becomes impractical. In the case of a permu-

tation decoder (for this, the attacker must have a generator and/or a check matrix of the code used, which is the public key in the proposed cryptosystems), the cryptanalysis complexity is significantly lower. However, even if the attacker has a public key and uses a permutation decoder, cryptanalysis becomes computationally inefficient.

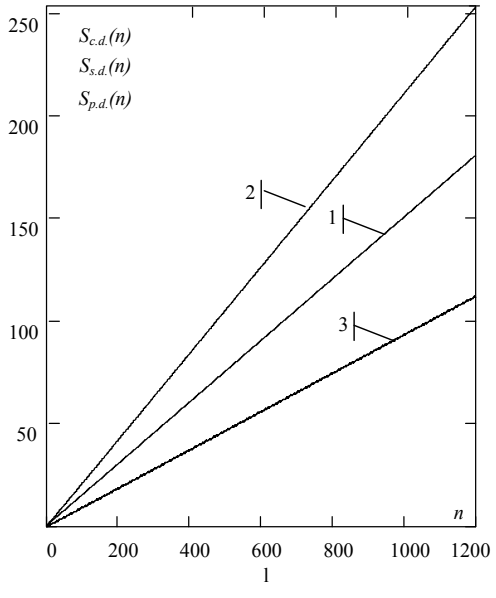

Fig. 8. Dependencies:
$1-S_{\text{c.d.}}(n)$, $2-S_{\text{s.d.}}(n)$, $3-S_{p.d.}(n)$ for $q=2$, $k=0{,}5\cdot n$

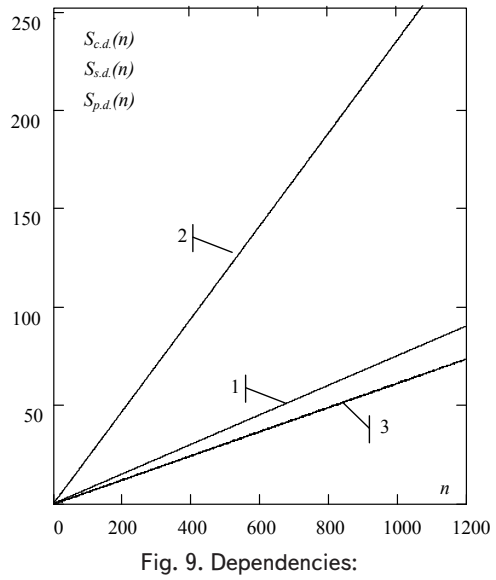

Fig. 9. Dependencies:
$1-S_{c.d.}(n)$, $2-S_{s.d.}(n)$, $3-S_{\text{p.d.}}(n)$ for $q=2$, $k=0{,}25\cdot n$

It should be noted that for high-speed redundant codes, the correlation decoder is less effective than the syndromic one. With a decrease in the relative coding rate, the computational efficiency of syndromic decoding decreases, and with $R=k/n<0{,}5$ the correlation decoder is more preferable for the attacker to use it as a method of cryptanalysis.

Fig. 10 shows the dependencies $S_{\text{c.d.}}(R)$, $S_{\text{s.d.}}(R)$ and $S_{\text{p.d.}}(R)$ for $q=2$ and fixed length of the code used. The score is given on a logarithmic scale. The analysis of these dependences confirms the conclusion that the computational efficiency of syndrome decoding and the increase in computational efficiency of correlation decoding are reduced while the relative speed of the code used decreases. The computational efficiency of the syndrome and correlation decoders is equivalent with $R\approx 0{,}65$.

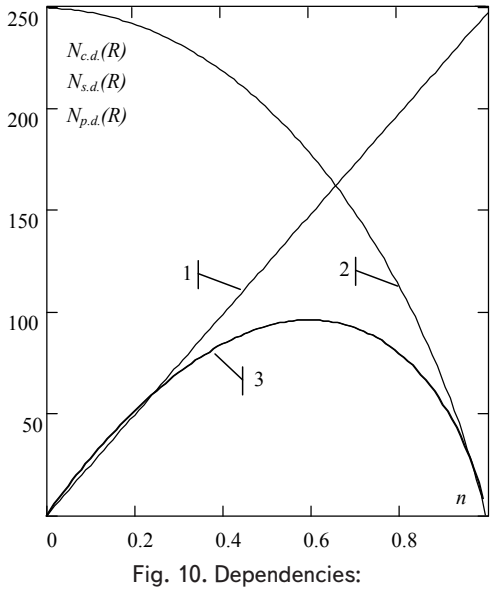

Fig. 10. Dependencies:
$1-N_{\text{c.d.}}(R)$, $2-N_{\text{s.d.}}(R)$, $3-N_{\text{p.d.}}(R)$ for $q=2$

The analysis of the dependences in Fig. 10 shows that the use of a permutation decoder with a public key known to the attacker with the length of the code n=1,000 used for cryptanalysis is computationally inexpedient, the crypto-code information protection system effectively ensures the security of data transmission in computer systems and networks.

Thus, the conducted studies have shown that with a proper choice of parameters of the masked code, the developed cryptosystems on algebraic block codes provide the required resistance to the cryptanalytic attacks of the attacker, based on nonalgebraic decoding methods of the random block code.

The evaluation of the cryptographic strength of multichannel cryptography on flawed codes is given in [25, 26]. In [32], issues of the cryptographic strength of hybrid crypto-code structures on *EC* (*MEC*) with multichannel cryptography based on the McEliece scheme are considered. In [14], an attack on crypto-code structures (theoretic-code schemes) with the possibility of finding the elements of the generating matrix and masking matrices was justified. Due to the fact that the G (generating matrix) and H (check matrix) matrices of an error-resistant code are orthogonal, the author in [14] assumes that the proposed method based on linear fractional transformations can calculate the elements of the G and H matrices. This assumption allows approximating the results of the evaluation of the cryptographic strength of the hybrid crypto-code structure based on the McEliece scheme for the evaluation of the cryptographic stability of the proposed integrated cryptosystem.

However, the proposed solution of the integrated system consists of two cryptosystems and, accordingly, joint cryptographic resistance will be higher each separately. Moreover, additional session keys (IV_1, IV_2 initialization vectors) provide additional cryptographic strength.

8. Discussion of the main indicators of Niederreiter hybrid crypto-code structures

The theoretical basis for building flawed texts is to remove the ordering of the source text characters and, as a result, reduce the redundancy of language characters in the flawed text. At the same time, the amount of information expressing this ordering will be equal to the decrease in the entropy of the text compared to the maximum possible entropy value corresponding to the absence of orderliness in the text in general, that is, the equiprobable appearance of any letter after any previous letter. The methods of information calculation proposed by C. Shannon make it possible to identify the ratio of the amount of predictable (i.e. generated by certain rules) information and the amount of unexpected information that cannot be predicted in advance.

To restore the original sequence, there is no need to know intermediate flawed sequences. It is necessary to know only the last flawed sequence (the last flawed text after performing all the cycles) and all the damages with the rules of their application.

Cryptographic flawed texts are texts obtained in the following ways [25, 26]: damage to the source text, followed by encryption of the flawed text and/or its damage, damage to the ciphertext, damage to the ciphertext of the flawed text and/or ciphertext.

The main difference of the proposed complex system from the "classical" concept is the use of the whole system at BSC to ensure the cryptographic strength of the system as a whole, and the crypto-code structures based on the McEliece or Niederreiter schemes, which provide stability in post-quantum cryptography.

The paper [32] presents the results of studies of the main criteria for cryptosystems based on the McEliece crypto-code scheme, as well as the theoretical foundations of the cryptographic strength of the proposed McEliece modified crypto-code structures (MCCS) with *EC* and hybrid MCCS with flawed codes by reducing the power of the Galois field without reducing the level of cryptographic strength of the hybrid cryptosystem as a whole with their software implementation. Taking into account that the McEliece and Niederreiter schemes use one approach to the formation of a private key (masking matrices are similar) and the encoding and decoding algorithms use classical algorithms of the noise-resistant coding theory, it is proposed to use the method for estimating the strength of the HCCS proposed in [32]. The overall strength of the proposed approach to the formation of a hybrid cryptosystem consists of the strength of the Niederreiter modified crypto-code structure and the strength of the multi-channel cryptosystem on flawed codes.

Assessment of the implementation complexity of the intruders' attacks. Suppose that a crypto-code cryptosystem, constructed by masking an algebraic block (n, k, d) code over $GF(q)$ is used. Cryptanalysis of such a system consists in solving the problem of decoding a masked (n, k, d) code over $GF(q)$ without using a fast (polynomial complexity) rule that defines a secret key. The volume of the secret key (the dimension of the X, P, D masking matrices) is

$$l_{\text{с.к.}} = \left(k^2 + n^2\right)\cdot \log_2 q \text{ bit},$$

($k\times k$ elements from $GF(q)$ of the X matrix and $n\times n$ elements from $GF(q)$ of the $\Lambda=P\cdot D$ matrix) [8, 14, 15, 24] for the classical Niederreiter ACCS. For the Niederreiter MCCS on *MEC*, the volume of the secret key is

$$l_{\text{с.к.MCCC}} = \left(k^2 + n^2 + n\right)\cdot \log_2 q \text{ bit},$$

where n is the elements of the initialization vector IV_2, and for the Niederreiter MCCS on *MEC*, the volume of the secret key is (Table 8):

$$l_{\text{с.к.HCCC}} = \left(k^2 + n^2 + n\right)\cdot \log_2 q + \frac{n!}{t!(n-t)!} \text{ bit},$$

where $\frac{n!}{t!(n-t)!}$ – elements of the initialization vector IV_1 $\left(t = \frac{d-k-1}{2}\right)$.

Table 8

Volume of the secret key, bits

	2^3	2^4	2^5	2^6	2^7	2^8	2^9
$l_{\text{с.д.}}$	150	1000	5525	26988	138103	645200	2921625
$l_{\text{с.д.MCCS}}$	171	1060	5680	27366	138992	647240	2926224
$l_{\text{с.д.HCCS}}$	191	1165	10175	67077	472367	679625	24991204

Consequently, the complexity of the implementation of the most simple attack, aimed at a total bust of secret key data, is:

$$S_{\text{р.д}} = 2^{l_{\text{с.д.}}},\ S_{\text{р.д. MCCS}} = 2^{l_{\text{с.д.MCCS}}},\ S_{\text{р.д.HCCC}} = 2^{l_{\text{с.д.HCCC}}}.$$

One of the main components of the evaluation of the strength of cryptographic algorithms is the assessment of its statistical security. An algorithm is considered to be statistically safe if the sequence it generates is not inferior in its properties to a random sequence – such sequences are called "pseudo-random".

For an experimental assessment of how closely cryptoalgorithms approximate the generators of "random" sequences, statistical tests are used. The proposed NIST (American National Standards Institute) NIST STS 822 test suite for testing random or pseudo-random number generators is one approach to implementing the task of evaluating the statistical security of cryptographic primitives and may provide a preliminary assessment of the cryptographic strength of the complex system as a whole. Using this package allows, with a high degree of probability, drawing conclusions as to how far the sequence that is generated by the primitive under study is statistically safe.

The NIST STS test suite was proposed during the competition for a new US national standard of block encryption. This set was used to study the statistical properties of candidates for a new block cipher. Today, the testing methodology proposed by NIST is the most common among developers of cryptographic information security tools [27].

The research results are summarized in Table 9.

The results presented in Table 9 show that despite the reduction in the field power to $GF(2^6)$ for MCCS and $GF(2^4)$ for HCCS, the statistical characteristics of such crypto-code structures turned out to be at least as good as the traditional Niederreiter CCS on $GF(2^{10})$. All cryptosystems passed 100 % of the tests, and the best result was shown by the HCCS on shortened *MEC*: 155 out of 189 tests were passed at the level of 0,99, which is 82 % of the total number of tests. At the same time, the traditional CCS on $GF(2^{10})$ showed 149 tests at the level of 0,99.

Table 9

Results of statistical security studies

Cryptosystems	Number of tests in which more than 99 % of sequences passed the test, (%)	Number of tests in which more than 96 % of sequences passed the test, (%)	Number of tests in which less than 96 % of sequences passed the test, (%)
Niederreiter CCS on *MEC*	149 (78,83)	189 (100)	0 (0)
Niederreiter CCS on shortened *MEC*	151 (79,89)	189 (100)	0 (0)
Niederreiter CCS on extended *MEC*	152 (80,42)	189 (100)	0 (0)
Niederreiter HCCS on extended *MEC*	**153** (80,95)	189 (100)	0 (0)
Niederreiter HCCS on shortened *MEC*	**155** (82)	189 (100)	0 (0)

Thus, the proposed methods for providing basic security services of information resources allow integrated (by one mechanism) provision of the necessary level of stability and reliability of data.

Let us examine the speed of the proposed *CCS*. To do this, we estimate the complexity of cryptographic transformation: the complexity of generating a cryptogram (encryption) S_e and the complexity of an inverse cryptographic transformation (decryption) S_d in group operations in the final field $GF(q)$.

The formation of a cryptogram corresponds to the calculation of a codeword of a masked (n, k, d) code over $GF(q)$. If the masked code is specified by the generator matrix G, in the general case in a non-systematic form, then to form a code word, it is enough to multiply the information vector of length n characters by the H_X matrix. This procedure corresponds to an unsystematic coding rule, the complexity of its implementation will be $2t\times n$ operations of addition and multiplication over a finite field. The complexity of the operation of adding a random error vector to the code word will be n addition operations. Therefore, for the non-systematic coding method:

$$S_e=2\times t\times n.$$

For the MCCC, no additional operations are required – only selective reading is required according to the *IV*2 initialization vector. But for HCCC complication of the damage algorithm. In general terms (Fig. 11):

$$S_{e(HCCS)}=2\times t\times n+n\times m.$$

However, when $L>1$, then

$$S_{e(HCCS)}=2\times t\times n+n\times m\times L.$$

If the masked code is specified by the check matrix H, in the general case in a non-systematic form, then to form a code word, it is necessary to calculate the check characters and place them in the appropriate place in the code word.

The complexity of decryption is determined by the complexity of the algebraic algorithm for decoding an algebraic block code. For BSC codes, RS codes and their generalizations, alternant codes and their subclasses, error localization is reduced to solving a system of linear equations. The decoding complexity is:

$$S_d=n^{5/2}+(2\times n^3)+t^{5/2},$$

$$S_{d(HCCS)}=n\times m\cdot L+n^{5/2}+(2\times n^3)+t^{5/2}.$$

The dependence of the operations of addition and multiplication over a finite field in various cryptosystems is presented in Table 10.

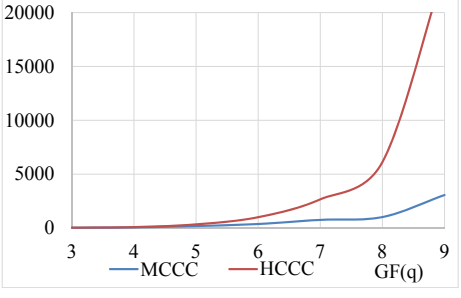

Fig. 11. Dependencies of cryptogram formation complexity, using the (n, k, d) code over $GF(q)$

Table 10

Dependence of the operations of addition and multiplication over a finite field in various cryptosystems

Cryptosystem	$GF(q)$						
	3	4	5	6	7	8	9
Niederreiter MCCS on *MEC*	821	7627	64948	531613	4278546	34201122	272768399
Niederreiter HCCS on *MEC*	828	7657	65103	532243	4280451	34206222	272789350

The results in Table 10 confirm a 7-fold decrease in the number of operations of addition and multiplication over a finite field in the proposed Niederreiter hybrid crypto-code structures on flawed codes over $GF(2^4)$ compared to the modified Niederreiter crypto-code structure on *MEC* over $GF(2^6)$. The result obtained confirms the competitiveness of the Niederreiter HCCS for post-quantum cryptography.

The use of *EC* (*MEC*) ensures protection against the attack proposed in [14], which provides additional security of the system as a whole.

9. Conclusions

1. The analysis of the principles of the formation of the Niederreiter MCCS on flawed codes, taking into account the regularity of the necessary fixation of the positional vectors of the plaintext to form the error vector in the equilibrium coding of non-binary codes, allows the *MV2* algorithm to be used to damage the cryptogram, which allows practical implementation of the Niederreiter hybrid crypto-code structure. In contrast to the classical representation of hybrid (complex) cryptosystems, the Niederreiter CCS on *MEC* with a fast crypto-transformation algorithm (a cryptosystem

of provable durability) is used to ensure cryptographic resistance. This approach can significantly reduce the energy costs of practical implementation, and the possibility of using the proposed structure in the protocols of the transport level of Internet systems.

2. The proposed algorithms of cryptogram formation, taking into account the mechanism of damage *MV2* to the hybrid Niederreiter crypto-code structure, ensure its practical implementation. The presented research results of the energy intensity of the practical implementation of the Niederreiter HCCS confirm the 7 % cost reduction, while implementation is possible on the main software and hardware platforms that are widely used.

3. As a result of the research, it was shown that the use of the developed hybrid cryptosystems with the appropriate code parameters allows ensuring the security and reliability of data transmission in case an attacker uses non-algebraic decoding methods. In addition, the practical use of crypto-code structures of information protection allows you to comprehensively solve the problem of ensuring the security and reliability of data transmission. Statistical analysis of the cryptographic strength of the output sequences of the Niederreiter HCCS based on flawed codes using NIST STS 822 confirms their cryptographic strength, which proves the possibility of their use as an alternative replacement for RSA-like algorithms in Internet applications.

References

1. Androshchuk H. O. Kiberbezpeka: tendentsiyi v sviti ta Ukraini // Kiberbezpeka ta intelektualna vlasnist: problemy pravovoho zabezpechennia: materialy Mizhnarodnoi naukovo-praktychnoi konferentsiyi. Kyiv: Vyd-vo «Politekhnika», 2017. P. 30–36.
2. Grishchuk R. V., Danik Yu. G. Osnovy kiberbezopasnosti: monografiya / Yu. G. Danik (Ed.). Zhitomir: ZHNAEU, 2016. 636 p.
3. Zabezpechennia informatsiynoi bekhpeky derzhavy: nav. pos. / Ivanchenko I. S., Khoroshko V. O., Khokhlachova Yu. Ye., Chyrkov D. V.; V. O. Khoroshko (Ed.). Kyiv: PVP "Zadruha", 2013. 170 p.
4. Baranov O. A. Pro tlumachennia ta vyznachennia poniattia «kiberbezpeka» // Pravova informatyka. 2014. Issue 2. P. 54–62.
5. Babych Ye. Yu. Zabezpechennia kiberbezpeky v Ukraini // Aktualni zadachi ta dosiahnennia u haluzi kiberbezpeky: materialy Vseukrainskoi naukovo-praktychnoi konferentsiyi. Kropyvnytskyi: KNTU, 2016. P. 77–78.
6. Leonenko G. P., Yudin A. Yu. Problemy obespecheniya informacionnoy bezopasnosti sistem kriticheski vazhnoy informacionnoy infrastruktury Ukrainy // Information Technology and Security. 2013. Issue 1 (3). P. 44–48.
7. Yevseiev S., Koc G. P., Korol' O. G. Analysis of the legal framework for the information security management system of the NSMEP // Eastern-European Journal of Enterprise Technologies. 2015. Vol. 5, Issue 3 (77). P. 48–59. doi: https://doi.org/10.15587/1729-4061.2015.51468
8. Yevseiev S. Ispol'zovanie ushcherbnyh kodov v kripto-kodovyh sistemah // Systemy obrobky informatsiyi. 2017. Issue 5 (151). P. 109–121. doi: https://doi.org/10.30748/soi.2017.151.15
9. Method for calculating of R-learning traffic peakedness / Kuchuk N., Mozhaiev O., Mozhaiev M., Kuchuk H. // 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T). 2017. doi: https://doi.org/10.1109/infocommst.2017.8246416
10. Approaches to selection of combinatorial algorithm for optimization in network traffic control of safety-critical systems / Kuchuk G., Kharchenko V., Kovalenko A., Ruchkov E. // 2016 IEEE East-West Design & Test Symposium (EWDTS). 2016. doi: https://doi.org/10.1109/ewdts.2016.7807655
11. Multiservice network security metric / Mozhaev O., Kuchuk H., Kuchuk N., Mozhaev M., Lohvynenko M. // 2017 2nd International Conference on Advanced Information and Communication Technologies (AICT). 2017. doi: https://doi.org/10.1109/aiact.2017.8020083
12. Report on Post-Quantum Cryptography / Chen L., Jordan S., Liu Y.-K., Moody D., Peralta R., Perlner R., Smith-Tone D. // NIST. 2016. doi: https://doi.org/10.6028/nist.ir.8105
13. Dinh H., Moore C., Russell A. McEliece and Niederreiter Cryptosystems that Resist Quantum Fourier Sampling Attacks // Lecture Notes in Computer Science. 2011. P. 761–779. doi: https://doi.org/10.1007/978-3-642-22792-9_43
14. Sidel'nikov V. M. Teoriya kodirovaniya. Moscow: FIZMATLIT, 2008. 324 p.
15. Practical implementation of the Niederreiter modified cryptocode system on truncated elliptic codes / Yevseiev S., Tsyhanenko O., Ivanchenko S., Aleksiyev V., Verheles D., Volkov S. et. al. // Eastern-European Journal of Enterprise Technologies. 2018. Vol. 6, Issue 4 (96). P. 24–31. doi: https://doi.org/10.15587/1729-4061.2018.150903
16. Cho J. Y., Griesser H., Rafique D. A McEliece-Based Key Exchange Protocol for Optical Communication Systems // Lecture Notes in Electrical Engineering. 2017. P. 109–123. doi: https://doi.org/10.1007/978-3-319-59265-7_8
17. Development of mceliece modified asymmetric crypto-code system on elliptic truncated codes / Yevseiev S., Rzayev K., Korol O., Imanova Z. // Eastern-European Journal of Enterprise Technologies. 2016. Vol. 4, Issue 9 (82). P. 18–26. doi: https://doi.org/10.15587/1729-4061.2016.75250
18. Yevseiev S., Tsyhanenko O. Development of asymmetrical crypto-coded construction of niderraiter on modified codes // Systemy obrobky informatsiyi. 2018. Issue 2 (153). P. 127–135. doi: https://doi.org/10.30748/soi.2018.153.16
19. Dudykevych V. B., Kuznetsov O. O., Tomashevskyi B. P. Krypto-kodovyi zakhyst informatsiyi z nedviykovym rivno vahovym koduvanniam // Suchasnyi zakhyst informatsiyi. 2010. Issue 2. P. 14–23.
20. Dudykevych V. B., Kuznietsov O. O., Tomashevskyi B. P. Metod nedviykovoho rivnovahovoho koduvannia // Suchasnyi zakhyst informatsiyi. 2010. Issue 3. P. 57–68.
21. De Vries S. Achieving 128-bit Security against Quantum Attacks in OpenVPN. URL: https://internetscriptieprijs.nl/wp-content/uploads/2017/04/1-Simon-de-Vries-UT.pdf

22. Enhanced public key security for the McEliece cryptosystem / Baldi M., Bianchi M., Chiaraluce F., Rosenthal J., Schipani D. // arXiv.org. URL: https://arxiv.org/abs/1108.2462
23. Yevseiev S., Rzayev Kh., Tsyhanenko A. Analysis of the software implementation of the direct and inverse transform in non-binary equilibrium coding method // Journal of Information Security. 2016. Vol. 22, Issue 2. P. 196–203.
24. Niederreiter H. Knapsack-type cryptosystems and algebraic coding theory // Problems of Control and Information Theory. 1986. Vol. 15, Issue 2. P. 159–166.
25. Mishchenko V. A., Vilanskiy Yu. V. Ushcherbnye teksty i mnogokanal'naya kriptografiya. Minsk: Enciklopediks, 2007. 292 p.
26. Mishchenko V. A., Vilanskiy Yu. V., Lepin V. V. Kriptograficheskiy algoritm MV 2. Minsk, 2006. 177 p.
27. A statistical test suite for random and pseudorandom number generators for cryptographic applications / Rukhin A., Sota J., Nechvatal J., Smid M., Barker E., Leigh S. et. al. // NIST. 2000. doi: https://doi.org/10.6028/nist.sp.800-22
28. Berlekemp E. R. Algebraicheskaya teoriya kodirovaniya. Moscow: Mir, 1971. 480 p.
29. Teoriya kodirovaniya / Kasami T., Tokura N., Ivadari E., Inagaki Ya. Moscow: Mir, 1978. 576 p.
30. Kuznecov A. A., Korolev R. V., Tomashevskiy B. P. Ocenka stoykosti kripto–kodovyh sredstv zashchity informacii k atakam zloumyshlennika // Systemy upravlinnia, navihatsii ta zviazku. 2010. Issue 2 (14). P. 114–117.
31. Naumenko N. I., Stasev Yu. V., Kuznetsov O. O. Teoretychni osnovy ta metody pobudovy alhebraichnykh blokovykh kodiv. Kharkiv: KhUPS, 2005. 267 p.
32. Yevseiev S. P., Ostapov S., Bilodid I. Research of the properties of hybrid crypto-code constructions // Ukrainian Information Security Research Journal. 2017. Vol. 19, Issue 4. P. 278–290. doi: https://doi.org/10.18372/2410-7840.19.12206

На основі аналізу систем технічної діагностики проведено дослідження силових впливів, що виникають в технологічних комплексах. У зв'язку з поділом силових впливів на детерміновані та випадкові, запропоновано різні способи виділення вібрації інформаційних діагностичних характеристик для забезпечення оперативного і достовірного виявлення дефектів, які швидко розвиваються. Достовірна діагностика дозволить перейти з системи планово-попереджувальних ремонтів на організацію ремонтів по поточному стану і зниженню витрат на ремонт і відновлення вузлів технологічних комплексів шляхом раннього виявлення дефектів, що зароджуються у вузлах.

Проаналізувавши процес поширення віброакустичних хвиль, зумовлених силовим впливом, створено математичну модель виникнення та поширення пружних хвиль в складних технологічних комплексах від місць їх виникнення до точки спостереження. Наведено кінематичні схеми розповсюдження низькочастотних вібрацій, вібросигналів від щітково-колекторного вузла, а також хвилі від внутрішнього кільця підшипника. Це дало змогу обґрунтувати математичну модель виникнення та поширення віброакустичних хвиль в деталях і вузлах складних технологічних комплексів від різних джерел вібрації.

За результатами порівняльного аналізу результатів дослідження реальних вібраційних полів та результатів чисельного моделювання підтверджено адекватність моделі і реального процесу. Наведено графіки часової реалізації сигналів у моделі, спектри реалізованих сигналів, а також їх автокореляційні функції, що відображають основні характеристики сигналів в точці вимірювання. Отримані результати можуть бути використані для технічної діагностики та щодо зниження витрат на ремонт і відновлення вузлів складних технологічних комплексів шляхом раннього виявлення дефектів, що зароджуються у вузлах

Ключові слова: вібросигнал, стохастичний, підшипники кочення, поля вібрації, віброакустичні хвилі, ударні імпульси

UDC 004.94:681.2:621.3
DOI: 10.15587/1729-4061.2019.155839

THE DEVELOPMENT OF METHODS FOR DETERMINING VIBRATION STOCHASTIC FIELDS OF TECHNOLOGICAL COMPLEXES

N. Marchenko
PhD, Associate Professor
Department of
Computerized Control Systems*
O. Monchenko
PhD, Associate Professor
Department of
Biocibernetics and Aerospace Medicine*
E-mail: monchenko_olena@ukr.net
G. Martyniuk
PhD
Department of
Information-Measurement Systems*
*National Aviation University
Kosmonavta Komarova ave., 1, Kyiv,
Ukraine, 03058

1. Introduction

Nowadays, in general, more and more attention is paid to the technical diagnostics of sophisticated technological complexes (TCs) in operation and to the prognoses of their further performance. To a large extent, this is due to the role of technical diagnostics in reducing the cost of repair and restoration of TC units by early detection of defects that originate in the assembly parts. Only reliable diagnostics can allow the transition from the system of planned