Methods of information systems protection

UDC 004. 75 doi: https://doi.org/10.20998/2522-9052.2022.3.10

Bogdan Tomashevsky[1], Serhii Yevseiev[2], Serhii Pohasii[2], Stanislav Milevskyi[2]

[1] Ternopil Ivan Puluj National Technical University, Ternopil, Ukraine
[2] National Technical University “Kharkiv Polytechnic Institute”, Kharkiv, Ukraine

MECHANISMS FOR ENSURING THE SECURITY OF CHANNELS OF A PROSPECTIVE MANAGEMENT SYSTEM

Abstract. The development of military (state) control systems in modern conditions of hybrid warfare requires the possibility of rapid expansion of both functionality and scaling of the physical and logical basis of management, increasing the range of digitization and use of both military and civilian communication channels to manage troops and weapons. Not only the computing power of the enemy, the means of suppressing and / or blocking the communication channels of the control system, but also the development of quantum technologies that place new and more stringent requirements on security mechanisms based on symmetric and asymmetric cryptography algorithms. According to NIST, a full-scale quantum computer breaks both symmetric and asymmetric cryptosystems in polynomial time, significantly reducing their resilience. The paper proposes mechanisms of post-quantum cryptography, which allow to ensure the stability of not only communication channels, but also elements of the structure of the control system. The basis of post-quantum encryption algorithms is the combination of algorithms (schemes) of crypto-code structures with cryptosystems on unprofitable codes (multi-channel cryptography), as well as the possibility of combining them with digital steganography methods. This approach provides the ability to hide elements of management commands, and the use of different channels provides the ability to hide individual elements of cryptograms.

Keywords: crypto-code constructions; algebraic geometric codes4 LDPC-codes; troop control system; quantum period.

Introduction

The control system of troops and weapons is one of the main elements of the infrastructure of the Armed Forces, which allows to perform a variety of functions, from timely delivery of combat signals in the vertical subordination of combat units, to logistics and technical functions. The share of cyber threats is growing and this trend will intensify with the development of information technologies and their convergence with artificial intelligence technologies in the next decade. The growth of such influence on the functioning of both national and transnational governance structures creates a new security situation. There is a division of spheres of influence in cyberspace between the world's centers of power, and their desire to ensure the realization of their own geopolitical interests is growing [1]. In the conditions of hybrid war, stricter requirements are set for the functionality of a promising system of joint leadership and military management based on [2]:

– digitalization of activities and introduction of modern information technologies, including electronic communications, in the field of defense;

– digital transformation of the activity of the Ministry of Defense of Ukraine, the General Staff of the Armed Forces of Ukraine, other bodies of military management of the Armed Forces of Ukraine and governing bodies of other components of the Defense Forces;

– construction of the Joint Defense Network, which will be based on the electronic communication network and information systems of the Ministry of Defense of Ukraine and the Armed Forces of Ukraine;

– creation and development of operations networks based on modern digital means, by which field communication system of the Armed Forces of Ukraine will be re-equipped, development of new (improvement of existing) combat control systems. The formation of a promising system of joint leadership and military management requires the use of fundamentally new approaches to structural elements, security protocols not only in terms of hybrid warfare, but also possible cyber-attacks by cybercriminals, their integration with social engineering, synergies and hybridity.

Analysis of recent research and publications [1–7] identifies the need to create an automated system of defense components, which should comply with NATO standards, doctrines and recommendations at all levels of control (tactical, operational and strategic) with certain specifics of basic capabilities [7]. In addition, the NIST of the United States has conducted research [3, 8-10], which calls into question the stability of modern symmetric and asymmetric cryptosystems with the advent of a full-scale quantum computer. In addition, the Shore algorithm allows to factorize the number N over time O ($\lg^3 N$), using O (lg N) bit register, which is significantly faster than any classical method of factorization. The advantages of using quantum registers are significant memory savings (N quantum bits can contain 2^N bits of information), the interaction between qubits allows for one operation to affect the entire register (quantum parallelism) [3, 8-11]. Table 1 shows the results of a comparative analysis of the complexity of factorization for classical and quantum algorithms, table 2 – the complexity of the implementation of the Shore method of discrete logarithm of a group of points *EC* [3, 8-11]. These results indicate a significant reduction in computing resources when using a full-scale computer, which significantly reduces the efficiency of modern algorithms for symmetric and asymmetric cryptography to provide security services.

Table 2 shows the results of the analysis of the complexity of the implementation of the Shore method of discrete logarithm of a group of *EC* points [3, 8–11].

Table 1 – **Comparative analysis of the complexity of factorization for classical and quantum algorithms**

Module size N, bit	**The number of required qubits 2*n***	**The complexity of the quantum algorithm 4*n*³**	**The complexity of the classical algorithm**
512	1024	$0.54 \cdot 10^9$	$1.6 \cdot 10^{19}$
3072	6144	$12 \cdot 10^{10}$	$5 \cdot 10^{41}$
15360	30720	$1.5 \cdot 10^{13}$	$9.2 \cdot 10^{80}$

Table 2 – **The complexity of the implementation of the Shore method of discrete logarithm of a group of EC points**

Algorithm for calculating a discrete logarithmic equation			
The size of the order of the base point, bits	**The number of required qubits *f(n)=7n+ +4log₂n+10***	**The complexity of the quantum algorithm 360*n*³**	**The complexity of the classical algorithm**
163	1210	$1.6 \cdot 10^9$	$3.4 \cdot 10^{24}$
256	1834	$6 \cdot 10^9$	$3.4 \cdot 10^{38}$
571	4016	$6.7 \cdot 10^{10}$	$8.8 \cdot 10^{85}$
1024	7218	$3.8 \cdot 10^{11}$	$1.3 \cdot 10^{154}$

In the conditions of post-quantum cryptography, NIST experts suggest considering special attacks (SIDE-CHANEL ATTACKS). The implementation of these attacks is aimed at finding vulnerabilities in the practical implementation of the cryptosystem, primarily in the means of cryptographic protection [3, 8–11].

The possibility of using quantum technology by the enemy and/or cybercriminals to hack the command and control system of troops and weapons is questionable to ensure cryptographic stability of cryptograms, which are based on modern algorithms of symmetric and asymmetric cryptography. This requires in the post-quantum period to significantly increase the length of key messages [8], as well as to use post-quantum cryptographic algorithms, among which one of the most promising are algorithms of crypto-code constructs McEliece, based on algebraic geometry or LDPC codes (Low Density Parity Code).

The aim and objectives of the study. The aim of the work is to study the mechanisms of ensuring the security of the channels of a promising system of joint leadership and military management based on post-quantum algorithms. To achieve the aim of the work it is necessary to solve the following tasks:

– analysis of construction of McEliece crypto-code constructions on algebraic geometric codes and/or unprofitable codes;

– construction of Niederreiter crypto-code constructions on LDPC and/or unprofitable codes;

– assessment of the stability of the proposed crypto-code structures.

Analysis of McEliece crypto-code constructions on algebraic geometric codes and/or loss-making codes

The main advantage of crypto-code constructions is the integrated combination of symmetric encryption – speed of crypto-transformations, and asymmetric encryption – providing cryptographic stability based on a theoretically complex problem – decoding random code, as well as building crypto-code constructions (CCC) based on interference methods. coding provides the ability to correct errors, which, in turn, allows you to use a data transfer approach with direct error correction. However, a significant drawback is the complexity of their practical implementation in the GF alphabet (2^{10}-2^{13}), as well as significant energy costs. In addition, [12] proposed a practical algorithm for breaking these structures using cyclic noise-tolerant codes, the essence of which is to find the elements of the generating matrix and remove the effect of masking matrices. The orthogonality of the matrices – generating and testing – allows to consider the effectiveness of the attack on the Niederreiter scheme. Promising direction of elimination of the revealed regularities in [12] suggests to use cascade or algebrogeometric codes – codes constructed on the basis of algebra of the theory of noise-tolerant coding and geometrical parameters of a curve, in particular elliptic curves.

The formation of the crypto-code structure of McEliece is shown in fig. 1. Let G be a generating matrix of linear (n, k, d) code over $GF(q)$ with polynomial decoding complexity, X be a nondegenerate k ´ k-matrix over $GF(q)$, D be a diagonal matrix with non-zero diagonal elements, P is an adjustable matrix of size n´ n. The permutable matrix implements the permutation of the coordinates of the vector in the form of matrix multiplication, namely, the element p_{ij} of the matrix P is equal to 1 if and only if the coordinate with the number i passes by permutation into the coordinate with the number j. In other cases $p_{ij} = 0$. Thus, the matrix P contains only one unit in each column and in each row. The product of the matrices $L = P \times D$ specifies the permutable matrix L with nonzero elements of the field $GF(q)$. The permutable matrix L (unipotent matrix) when rearranging the coordinates of the vector preserves the Heming distance, i.e. $d\,(a, b) = d\,(a \times L, b \times L)$, where $d(x, y)$ is the Heming distance between the vectors x and y [11–14].

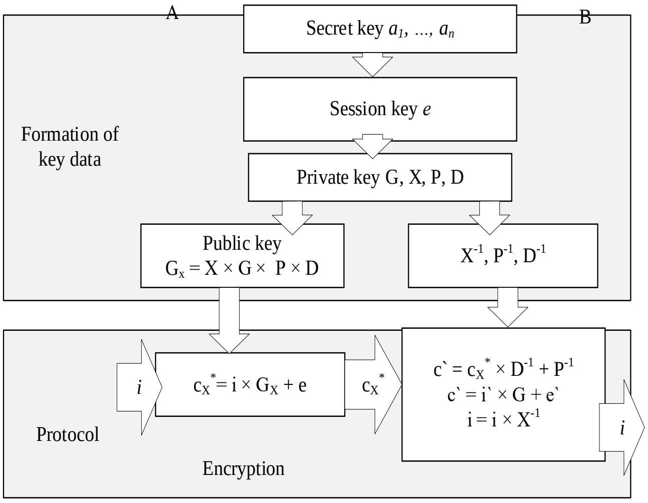


Fig. 1. Data exchange protocol using the McEliece CCC on the *EC*

The public key in an asymmetric cryptosystem based on McEliece CCC is the generating matrix G_X*=X×G×P×D,* obtained by multiplying the linear generation matrix *(n, k, d)* code on *GF(q)* on the masking matrix (*X*, *P*, *D*), personal (private) key are matrices *X, P, D*. Closed information (codogram) is a vector of length *n* and is calculated as a rule

$$c_X^* = i \times G_X + e, \qquad (1)$$

where vector $c_X = i \times G_X$ belongs to *(n, k, d)* code with a generating matrix G_X; *i* – *k*-bit information vector; vector e – secret weight error vector *£ t (session secret key).*

The general scheme of algebraic geometric coding was first proposed in [12]. Let *C* – class divisors on *X* degree α . Then *C* sets the display $\phi : X \to P^m$, set of generator functions $y_i = \phi(x_i)$ specifies the algebraic geometry code of length $n \le N$.

Code characteristics (n,k,d) related by ratio $k + d \ge n - g + 1$. If $2g - 2 < \alpha \le n$, then the code is related to the characteristics $(n, \alpha - g + 1, d), d \ge n - \alpha$.

The code dual to it is also algebraic with characteristics $(n, n - \alpha + g - 1, d_\perp)$, $d_\perp \ge \alpha - 2g + 2$. Set the McEliece CCC based on elliptical codes as follows [11]. Let G^{EC}– generating matrix for elliptical *(n, k, d)* code on *GF(q)* of view:

$$G^{EC} =$$

$$= \begin{pmatrix} F_0(P_0) & F_0(P_1) & \ldots & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & \ldots & F_1(P_{n-1}) \\ \ldots & \ldots & \ldots & \ldots \\ F_{k-1}(P_0) & F_{k-1}(P_1) & \ldots & F_{k-1}(P_{n-1}) \end{pmatrix} = \qquad (2)$$

$$= \left\| F_j \left(P_i \right) \right\|_{n,k}$$

and dimension *k´n, k = a, a=3×degF*.

Let *X* – nondegenerate *k ´ k*-matrix on *GF(q), D* – diagonal matrix with non-zero diagonal elements, *P* – permutable matrix size *n ´ n*. Define an asymmetric *McEliece CCC with an elliptical code:* public key matrix $G_X^{EC} = X \times G^{EC} \times P \times D$, personal (private) key - matrices *X, P, D.*

Closed information (codegram) is a vector of length *n* and is calculated according to the rule: $c_X^* = i \times G_X^{EC} + e$, where the vector belongs to the elliptical *(n, k, d)* code with a generating matrix G_X^{EC}, *i – k-* bit information vector, vector *e* – secret weight error vector *£ t*. The formation of the Niederreiter crypto-code construction is shown in Fig. 2.

Let *H* – test matrix of linear *(n, k, d)* code on *GF(q)* with polynomial decoding complexity. Let *X* – nondegenerate *r ´ r*-matrix on *GF(q), D* – діагональна матриця з ненульовими елементами на діагоналі, *P* – permutation matrix of size *n ´ n*. The public key in the Niederreiter scheme is the matrix H_X *=X×H×P×D*, the personal (private) key is the masking matrices – *X, P, D.* Closed information (codegram) S_X is a syndrome-vector of length *r = n – k* and is calculated according to the rule:

$$S_X = e \times H_X^T, \qquad (3)$$

where vector *e* – vector of length *n* and weight *£ t*, carrying confidential information (information message to be closed).

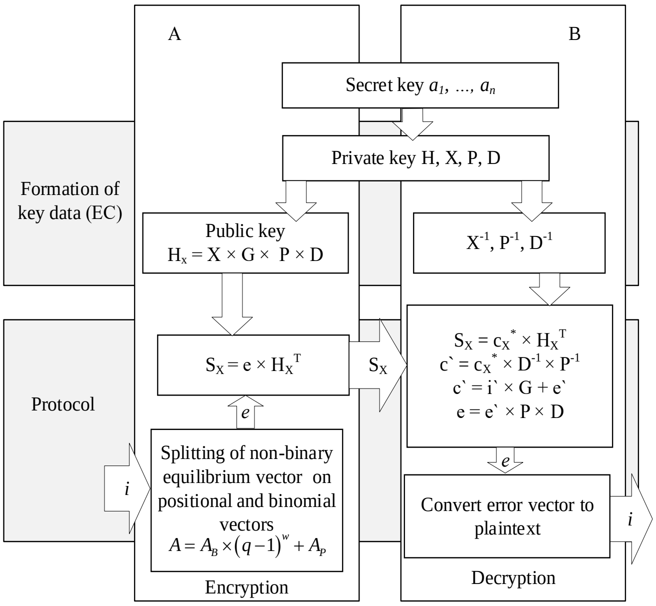

A
B
Secret key $a_1, \ldots, a_n$
Private key H, X, P, D
Formation of key data (EC)
Public key
$H_x = X \times G \times P \times D$
X^{-1}, P^{-1}, D^{-1}
Protocol
$S_X = e \times H_X^T$
S_X
$S_X = c_X^* \times H_X^T$
$c` = c_X^* \times D^{-1} \times P^{-1}$
$c` = i` \times G + e`$
$e = e` \times P \times D$
e
i
Splitting of non-binary equilibrium vector on positional and binomial vectors
$A = A_B \times (q-1)^w + A_P$
e
Convert error vector to plaintext
i
Encryption
Decryption

Fig. 2. Protocol of data exchange using Niederreiter CCC on the EC

To transmit non-binary symbols in [11], an algorithm for forming a non-binary equilibrium code sequence is proposed, which is schematically shown in Fig. 3.

The method of non-binary equilibrium coding on the basis of generalized binomial-positional representation allows to implement an asymmetric cryptosystem with Niederreiter CCC on the basis of algebraic geometric codes (AGC), which significantly enhances its statistical cryptographic stability and provide the necessary data reliability and efficiency.

In order to reduce the energy consumption of CCC, it is proposed to use modified elliptical codes - shortened and/or extended, which reduce the field strength to GF(2^6-2^8), as well as maintain the required level of stability through the use of additional initialization vectors. To modify the elliptical code that does not reduce the minimum code distance, it is proposed to reduce the number of information symbols.

Let $I=(I_1, I_2, \ldots, I_k)$ – information vector *(n, k, d)* of block code. Determine the subset *h* of information symbols, */h/=x, x*≤1/2*k*. Place in the information vector *I* in the subset *h* zeros, ie $I_i=0$, $\forall I_i \in h$. At other positions of vector *I* we will place information symbols.

When encoding the information vector, the characters of the set *h* are not used (they are zero) and can be discarded, and the resulting code word will be shorter by *x* code characters. To modify (shorten) elliptical codes, it is proposed to use reducing the set of curve points. Then *shortened* elliptical *(n, k, d)* code on *GF(q)*, built through the reflection of the view $\varphi: X \to P^{k-1}$, connected by characteristics *k+d≥n,* moreover: $n = 2\sqrt{q} + q + 1 - x$, $k \ge \alpha - x$, $d \ge n - \alpha$, $\alpha = 3 \times degF$.

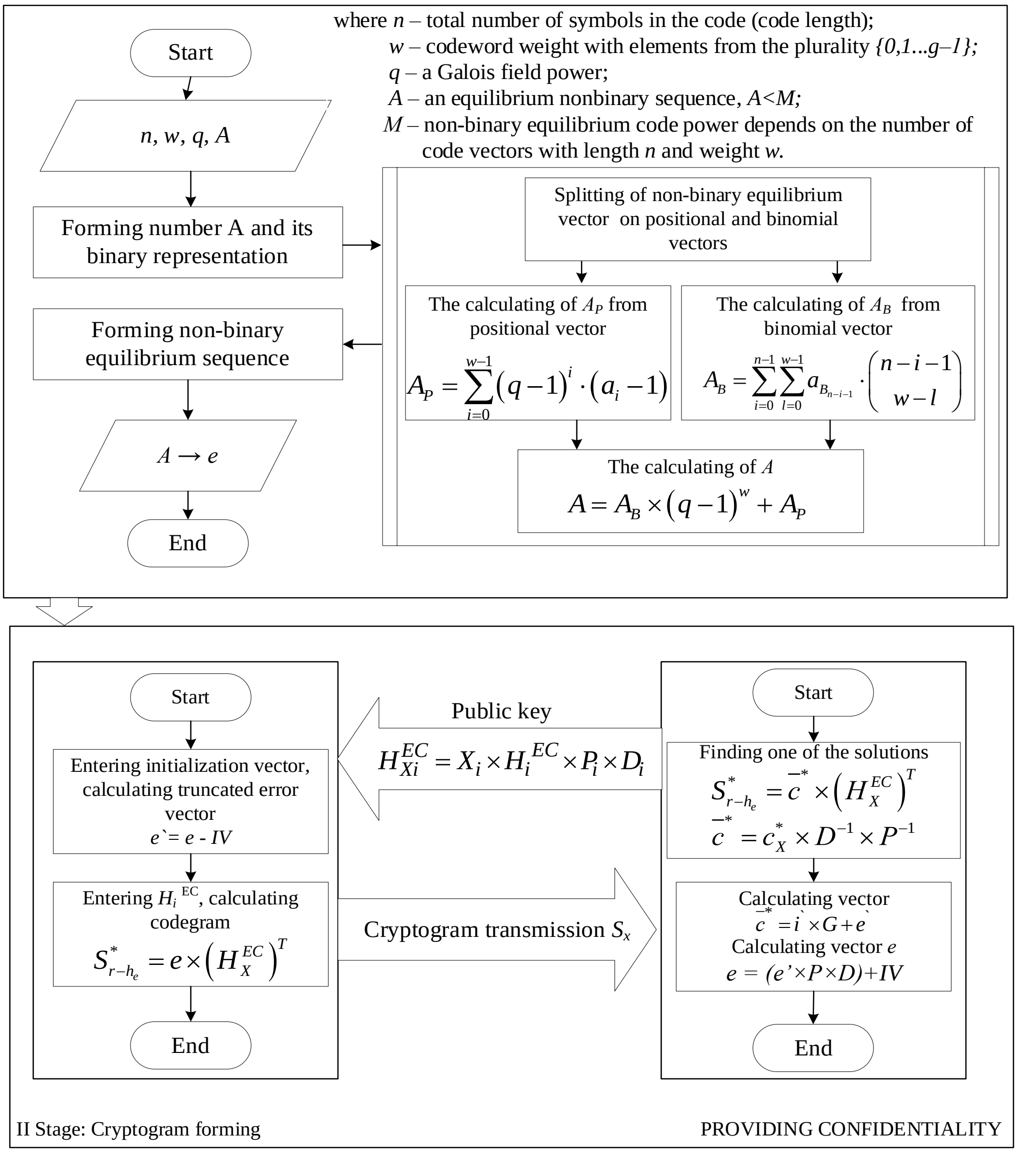

where n – total number of symbols in the code (code length);
w – codeword weight with elements from the plurality $\{0,1...g-1\}$;
q – a Galois field power;
A – an equilibrium nonbinary sequence, $A<M$;
M – non-binary equilibrium code power depends on the number of code vectors with length n and weight w.
Start
n, w, q, A
Forming number A and its binary representation
Forming non-binary equilibrium sequence
$A \to e$
End
Splitting of non-binary equilibrium vector on positional and binomial vectors
The calculating of A_P from positional vector
$A_P = \sum_{i=0}^{w-1}(q-1)^i\cdot(a_i-1)$
The calculating of A_B from binomial vector
$A_B = \sum_{i=0}^{n-1}\sum_{l=0}^{w-1} a_{B_{n-i-1}}\cdot\binom{n-i-1}{w-l}$
The calculating of A
$A = A_B\times(q-1)^w + A_P$
Start
Entering initialization vector, calculating truncated error vector
$e` = e - IV$
Entering H_i^{EC}, calculating codegram
$S^*_{r-h_e} = e\times\left(H_X^{EC}\right)^T$
End
Public key
$H_{Xi}^{EC} = X_i\times H_i^{EC}\times P_i\times D_i$
Cryptogram transmission S_x
Start
Finding one of the solutions
$S^*_{r-h_e} = \bar{c}^*\times\left(H_X^{EC}\right)^T$
$\bar{c}^* = c_X^*\times D^{-1}\times P^{-1}$
Calculating vector
$\bar{c}^* = i`\times G + e`$
Calculating vector e
$e = (e'\times P\times D)+IV$
End
II Stage: Cryptogram forming
PROVIDING CONFIDENTIALITY

Fig. 3. Scheme of formation of code words of non-binary equilibrium code

Shortened elliptical *(n, k, d)* code on $GF(2^m)$, built through the reflection of the view $\varphi: X\to P^{k-1}$, determines the modified CCC (MCCC) on the modified elliptical codes (MEC) with parameters:

– secret key dimension:

$$l_{K+} = x\cdot\left\lceil \log_2\left(2\sqrt{q}+q+1\right)\right\rceil;\ l_I=(\alpha-x)\cdot m; \qquad (4)$$

– dimension of information vector (in bits):

$$l_I=(\alpha-x)\times m; \qquad (5)$$

– dimension of the codegram:

$$l_S = \left(2\sqrt{q}+q+1-x\right)\cdot m; \qquad (6)$$

– relative encoding rate:

$$R = (\alpha - x)/\left(2\sqrt{q}+q+1-x\right). \qquad (7)$$

Fig. 4 shows the algorithm for forming a cryptogram/codogram. The decoding algorithm in the McEliece MCCC with shortened MES is shown in Fig. 5.

The second way to modify the linear block code, which maintains a minimum code distance and increases the amount of transmitted data, is to lengthen its length after the formation of the initialization vector, by reducing the information symbols. Let $I = (I_1, I_2, ..., I_k)$ – information vector *(n, k, d)* block code. Choose a subset h of information symbols, $/h/ = x$, $x \le 1/2\, k$ and *form the initialization vector*. Place in the information vector I in the subset h zeros, ie $I_i = 0,\ \forall I_i \in h$. At other positions of vector I we will place information symbols. After that, we add information symbols in the position of the initialization vector. To modify (lengthen) the elliptical codes, we will use decreasing the set of curve points.

Parameters of *extended* by x_1 characters from $GF(q)$ elliptical code constructed through the mapping of the view $\varphi:(X\cup h_1)\to P^{k-1}$, $n = 2\sqrt{q}+q+1-x+x_1$ will be connected by such relationships:

$$n = 2\sqrt{q}+q+1-x+x_1,$$

$$k \ge \alpha - x + x_1,\ d \ge n - \alpha,\ \alpha = 3\times deg\ F.$$

Elongated elliptical *(n, k, d)* code on $GF(2^m)$, built through the reflection of the view $\varphi:(X\cup h_1)\to P^{k-1}$, determines the MCCC with parameters:

– secret key dimension (in bits):

$$l_{K+} = (x - x_1)\cdot\left\lceil \log_2\left(2\sqrt{q}+q+1\right)\right\rceil; \qquad (8)$$

– dimension of information vector (in bits):

$$l_I = (\alpha - x + x_1)\cdot m; \qquad (9)$$

– cryptogram dimension (in bits):

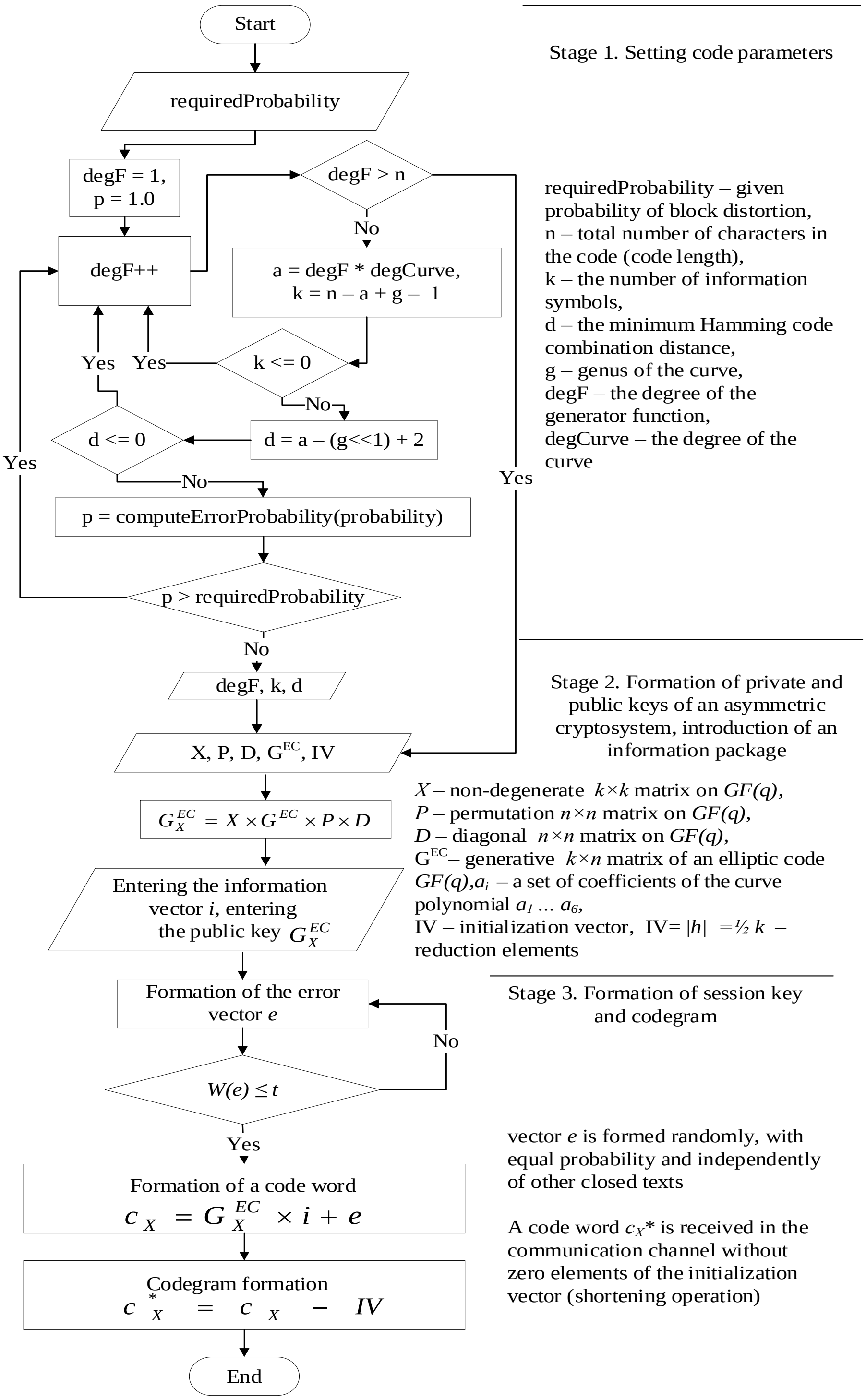
$$l_S = \left(2\sqrt{q}+q+1-x+x_1\right)\cdot m\,; \qquad (10)$$

– relative baud rate:

$$R = (\alpha - x + x_1)/\left(2\sqrt{q}+q+1-x+x_1\right). \qquad (11)$$

For Niederreiter CCC, an additional initialization vector is used to define codewords that satisfy the decoding algorithm. Fig. 6 and 7 show the protocol of exchange in an asymmetric cryptosystem based on Niederreiter CCC on extended and shortened *MEC*. The algorithm for forming a cryptogram in the modified Niederreiter CCC at *MEC*, taking into account the identified pattern, will be presented in the form of a sequence of steps [11, 16, 17]:

Step 1. Entering the information to be encoded, one of the elements of a set of suitable plaintexts. Public key input H_X^{EC}.


Start
requiredProbability
degF = 1, p = 1.0
degF > n
No
degF++
a = degF * degCurve, k = n – a + g – 1
Yes
Yes
k <= 0
No
d <= 0
d = a – (g<<1) + 2
Yes
No
Yes
p = computeErrorProbability(probability)
p > requiredProbability
No
degF, k, d
X, P, D, G^EC, IV
$G_X^{EC} = X \times G^{EC} \times P \times D$
Entering the information vector *i*, entering the public key G_X^{EC}
Formation of the error vector *e*
No
$W(e) \le t$
Yes
Formation of a code word $c_X = G_X^{EC} \times i + e$
Codegram formation $c_X^* = c_X - IV$
End

Stage 1. Setting code parameters

requiredProbability – given probability of block distortion,
n – total number of characters in the code (code length),
k – the number of information symbols,
d – the minimum Hamming code combination distance,
g – genus of the curve,
degF – the degree of the generator function,
degCurve – the degree of the curve

Stage 2. Formation of private and public keys of an asymmetric cryptosystem, introduction of an information package

X – non-degenerate $k\times k$ matrix on *GF(q)*,
P – permutation $n\times n$ matrix on *GF(q)*,
D – diagonal $n\times n$ matrix on *GF(q)*,
G^{EC}– generative $k\times n$ matrix of an elliptic code *GF(q)*,a_i – a set of coefficients of the curve polynomial $a_1 \dots a_6$,
IV – initialization vector, IV= |*h*| =½ *k* – reduction elements

Stage 3. Formation of session key and codegram

vector *e* is formed randomly, with equal probability and independently of other closed texts

A code word c_X* is received in the communication channel without zero elements of the initialization vector (shortening operation)

Fig. 4. Algorithm for forming a codogram in the McEliece MCCC with shortened MEC

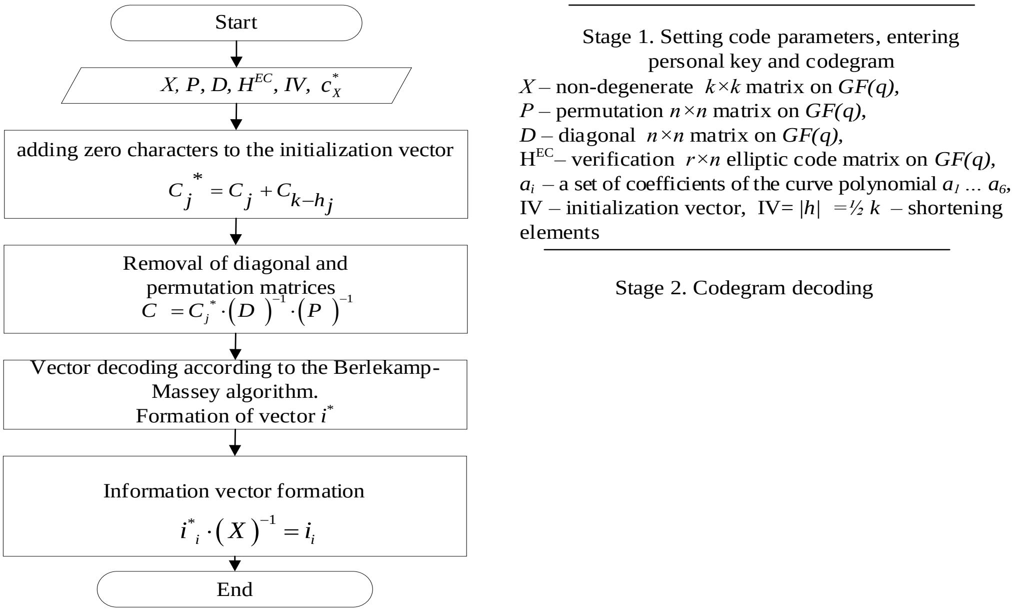

Start
$X, P, D, H^{EC}, IV, c_X^*$
adding zero characters to the initialization vector
$C_j^* = C_j + C_{k-h_j}$
Removal of diagonal and permutation matrices
$C = C_j^* \cdot (D)^{-1} \cdot (P)^{-1}$
Vector decoding according to the Berlekamp-Massey algorithm.
Formation of vector i^*
Information vector formation
$i^*_i \cdot (X)^{-1} = i_i$
End
Stage 1. Setting code parameters, entering personal key and codegram
X – non-degenerate $k\times k$ matrix on $GF(q)$,
P – permutation $n\times n$ matrix on $GF(q)$,
D – diagonal $n\times n$ matrix on $GF(q)$,
H^{EC}– verification $r\times n$ elliptic code matrix on $GF(q)$,
a_i – a set of coefficients of the curve polynomial $a_1 \dots a_6$,
IV – initialization vector, IV= $|h|$ =½ k – shortening elements
Stage 2. Codegram decoding

Fig. 5. Decoding algorithm in the McEliece MCCC with shortened MES

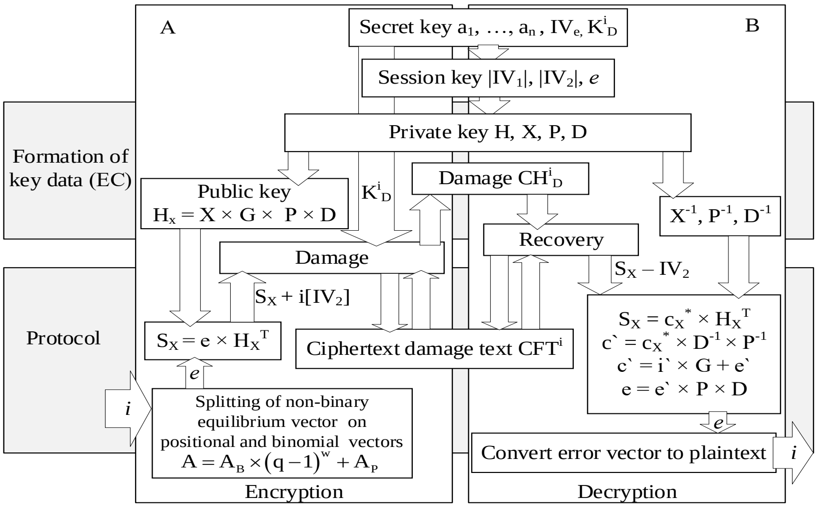

A
B
Secret key $a_1, \dots, a_n$, IV_e, K^i_D
Session key $|IV_1|$, $|IV_2|$, e
Private key H, X, P, D
Formation of key data (EC)
Public key
$H_x = X \times G \times P \times D$
K^i_D
Damage CH^i_D
X^{-1}, P^{-1}, D^{-1}
Recovery
Damage
$S_X - IV_2$
$S_X + i[IV_2]$
Protocol
$S_X = e \times H_X^T$
Ciphertext damage text CFT^i
$S_X = c_X^* \times H_X^T$
$c` = c_X^* \times D^{-1} \times P^{-1}$
$c` = i` \times G + e`$
$e = e` \times P \times D$
e
i
Splitting of non-binary equilibrium vector on positional and binomial vectors
$A = A_B \times (q-1)^w + A_P$
e
Convert error vector to plaintext
i
Encryption
Decryption

Fig. 6. Exchange protocol in an asymmetric cryptosystem based on Niederreiter CCC on extended MEC

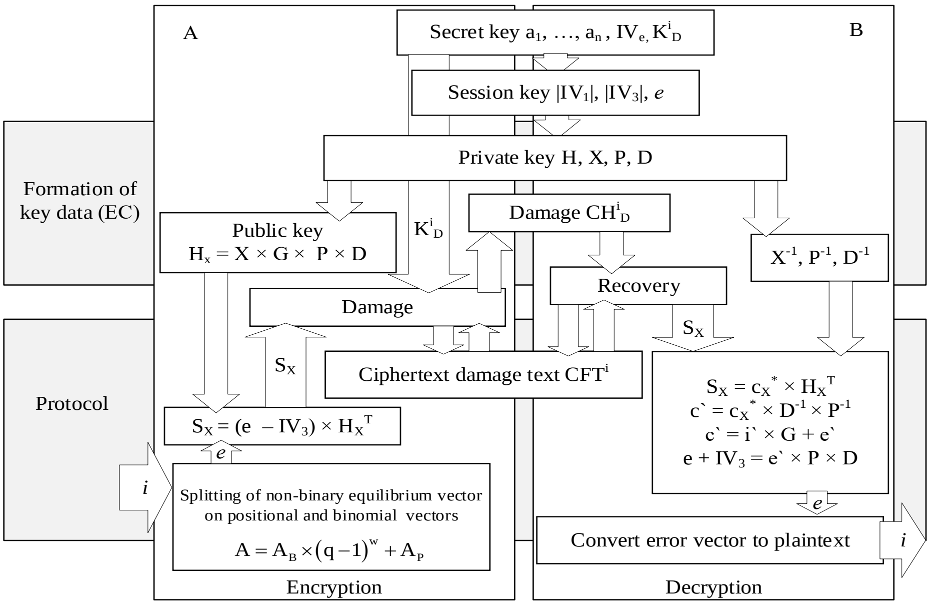

A
B
Secret key $a_1, \dots, a_n$, IV_e, K^i_D
Session key $|IV_1|$, $|IV_3|$, e
Private key H, X, P, D
Formation of key data (EC)
Damage CH^i_D
Public key
$H_x = X \times G \times P \times D$
K^i_D
X^{-1}, P^{-1}, D^{-1}
Recovery
Damage
S_X
S_X
Ciphertext damage text CFT^i
Protocol
$S_X = c_X^* \times H_X^T$
$c` = c_X^* \times D^{-1} \times P^{-1}$
$c` = i` \times G + e`$
$e + IV_3 = e` \times P \times D$
$S_X = (e - IV_3) \times H_X^T$
e
i
Splitting of non-binary equilibrium vector on positional and binomial vectors
$A = A_B \times (q-1)^w + A_P$
e
Convert error vector to plaintext
i
Encryption
Decryption

Fig. 7. Exchange protocol in an asymmetric cryptosystem based on Niederreiter CCC on shortened MEC

Step 2. Formation of an error vector *e*, the weight of which does not exceed £ *t* (corrective ability of the elliptical code based on the algorithm of non-binary equilibrium coding).

Step 3. Formation of the initialization vector *IV₁*.

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

Step 5. Codogram formation:

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

The algorithm for decoding the codogram in the modified Niederreiter CCC on *MEC* will be written as a sequence of steps [11, 16, 17]:

Step 1. Input of the codogram S_X, which is decoding. Private key input – matrices *X, P, D*.

Step 2. Finding one of the possible solutions of the equation: $S^{*}_{r-h_e}=\bar{c}^{*}\times\left(H_X^{EC}\right)^T$.

Step 3. Removal of diagonal and permutable matrices influence: $\bar{c}^{*}=c_X^{*}\cdot D^{-1}\cdot P^{-1}$.

Step 4. Decoding of the vector $\bar{c}^{*}$. Formation of the vector e_x'.

Step 5. Transformation of the vector e_x': $e_x=e_x'\times P\times D$.

Step 6. Formation of the desired vector of error *e*: $e=e_x+IV_2$.

Step 7. Transformation of the vector *e* based on the use of non-binary equilibrium code into an information sequence.

To further reduce energy costs while maintaining the level of sustainability, it is proposed to create a hybrid McEliece, Niederreiter CCC (HCCC) with MEC based on the use of unprofitable codes. The theoretical basis for the construction of unprofitable texts is to remove the order of the symbols of the source text and, as a consequence, reduce the redundancy of language symbols in the unprofitable text. The amount of information expressing this order will be equal to the decrease in the entropy of the text compared to the maximum possible value of entropy, the corresponding lack of order in the text in general, i.e., equally likely to appear any letter after any previous letter [18, 19]. Cryptographic unprofitable texts are texts obtained in the following ways [18, 19]: damage to the original text with subsequent encryption of unprofitable text and/or its losses, damage to ciphertext, damage to ciphertext of unprofitable text and/or ciphertext of losses.

Taking to account that the McEliece and Niederreiter CCC use the same approach to the formation of the private key (masking matrices are similar), and coding and decoding algorithms use the classical algorithms of noise-tolerant coding theory, it is proposed to use the approach to assessing the stability of HCCC, proposed in [11]. The overall stability of the proposed approach to the formation of HCCC consists of the stability of the modified crypto-code structure of Niederreiter and the stability of the multichannel cryptosystem on unprofitable codes. Universal mechanism of damage C_m can be described as:

$$\begin{gathered}
CFT/CH_{FT}=E_1\left(M,KU^{EC}\right),\\
CHD/CH_D=E_2\left(M,KU^{EC}\right), \qquad (12)\\
M=E_{1,2}^{-1}\left(CFT/CH_{FT},CHD/CH_D,KU^{EC}\right),\\
CFT/CH_{FT}=CFT/CH_{FT}^{i},...,CFT/CH_{FT}^{m},\\
KU^{EC}=\varphi(K_D^{i},...,K_D^{m},KU_1^{EC},...,KU_m^{EC},\\
CHD/CH_D=CHD/CH_D^{i},...,CHD/CH_D^{m}
\end{gathered}$$

Thus, as a result we have two ciphertexts (loss (CH_D) and unprofitable text (*FTC*)), each of which does not make sense either in the alphabet of the original text or in the alphabet of ciphertext. In fact, the ciphertext of the original message (*M*) is presented as a set of two unprofitable ciphertexts, each of which separately cannot recover the original text.

The main methods of damage are shown in Fig. 8 and Fig. 9. They reflect the basic protocols for providing security services based on the use of lossy codes.

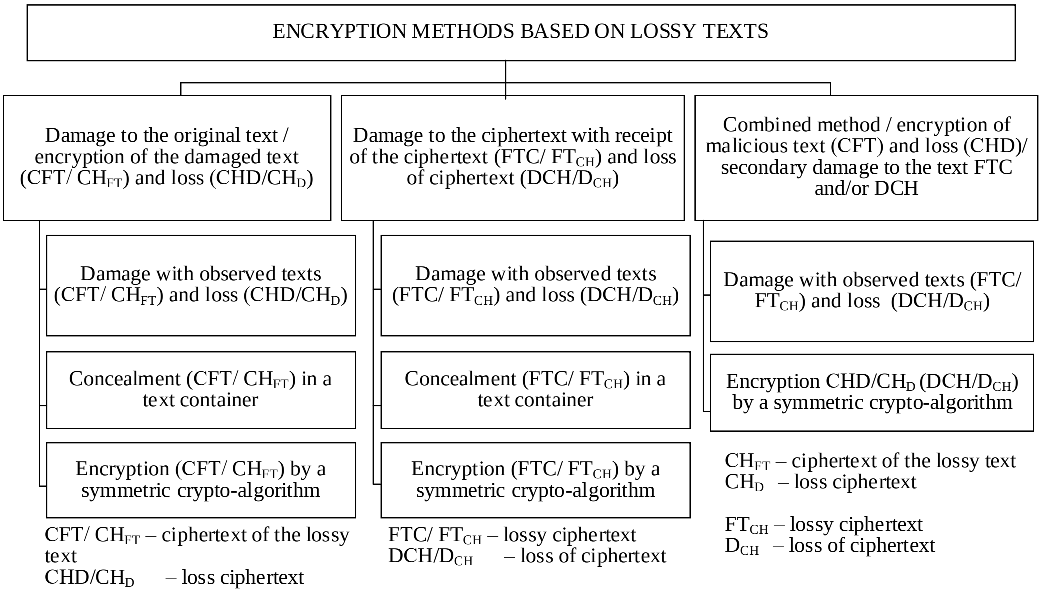

ENCRYPTION METHODS BASED ON LOSSY TEXTS
Damage to the original text / encryption of the damaged text (CFT/ CH_FT) and loss (CHD/CH_D)
Damage to the ciphertext with receipt of the ciphertext (FTC/ FT_CH) and loss of ciphertext (DCH/D_CH)
Combined method / encryption of malicious text (CFT) and loss (CHD)/ secondary damage to the text FTC and/or DCH
Damage with observed texts (CFT/ CH_FT) and loss (CHD/CH_D)
Damage with observed texts (FTC/ FT_CH) and loss (DCH/D_CH)
Damage with observed texts (FTC/ FT_CH) and loss (DCH/D_CH)
Concealment (CFT/ CH_FT) in a text container
Concealment (FTC/ FT_CH) in a text container
Encryption CHD/CH_D (DCH/D_CH) by a symmetric crypto-algorithm
Encryption (CFT/ CH_FT) by a symmetric crypto-algorithm
Encryption (FTC/ FT_CH) by a symmetric crypto-algorithm
CH_FT – ciphertext of the lossy text
CH_D – loss ciphertext
FT_CH – lossy ciphertext
D_CH – loss of ciphertext
CFT/ CH_FT – ciphertext of the lossy text
CHD/CH_D – loss ciphertext
FTC/ FT_CH – lossy ciphertext
DCH/D_CH – loss of ciphertext

Fig. 8. The main methods of damage

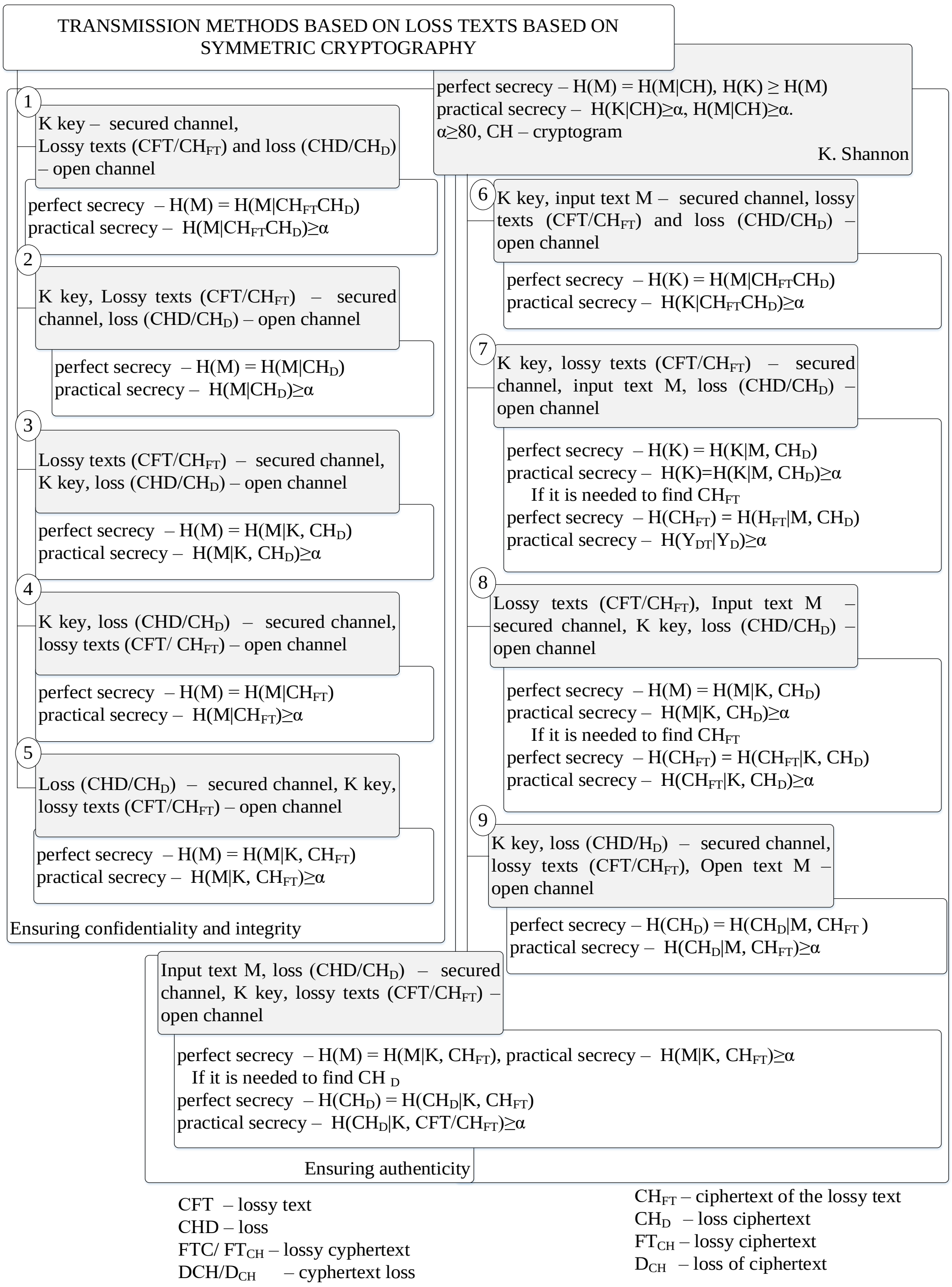

TRANSMISSION METHODS BASED ON LOSS TEXTS BASED ON SYMMETRIC CRYPTOGRAPHY
perfect secrecy – H(M) = H(M|CH), H(K) ≥ H(M)
practical secrecy – H(K|CH)≥α, H(M|CH)≥α.
α≥80, CH – cryptogram
K. Shannon
1
K key – secured channel, Lossy texts (CFT/CH$_{FT}$) and loss (CHD/CH$_D$) – open channel
perfect secrecy – H(M) = H(M|CH$_{FT}$CH$_D$)
practical secrecy – H(M|CH$_{FT}$CH$_D$)≥α
2
K key, Lossy texts (CFT/CH$_{FT}$) – secured channel, loss (CHD/CH$_D$) – open channel
perfect secrecy – H(M) = H(M|CH$_D$)
practical secrecy – H(M|CH$_D$)≥α
3
Lossy texts (CFT/CH$_{FT}$) – secured channel, K key, loss (CHD/CH$_D$) – open channel
perfect secrecy – H(M) = H(M|K, CH$_D$)
practical secrecy – H(M|K, CH$_D$)≥α
4
K key, loss (CHD/CH$_D$) – secured channel, lossy texts (CFT/ CH$_{FT}$) – open channel
perfect secrecy – H(M) = H(M|CH$_{FT}$)
practical secrecy – H(M|CH$_{FT}$)≥α
5
Loss (CHD/CH$_D$) – secured channel, K key, lossy texts (CFT/CH$_{FT}$) – open channel
perfect secrecy – H(M) = H(M|K, CH$_{FT}$)
practical secrecy – H(M|K, CH$_{FT}$)≥α
Ensuring confidentiality and integrity
6
K key, input text M – secured channel, lossy texts (CFT/CH$_{FT}$) and loss (CHD/CH$_D$) – open channel
perfect secrecy – H(K) = H(M|CH$_{FT}$CH$_D$)
practical secrecy – H(K|CH$_{FT}$CH$_D$)≥α
7
K key, lossy texts (CFT/CH$_{FT}$) – secured channel, input text M, loss (CHD/CH$_D$) – open channel
perfect secrecy – H(K) = H(K|M, CH$_D$)
practical secrecy – H(K)=H(K|M, CH$_D$)≥α
If it is needed to find CH$_{FT}$
perfect secrecy – H(CH$_{FT}$) = H(H$_{FT}$|M, CH$_D$)
practical secrecy – H(Y$_{DT}$|Y$_D$)≥α
8
Lossy texts (CFT/CH$_{FT}$), Input text M – secured channel, K key, loss (CHD/CH$_D$) – open channel
perfect secrecy – H(M) = H(M|K, CH$_D$)
practical secrecy – H(M|K, CH$_D$)≥α
If it is needed to find CH$_{FT}$
perfect secrecy – H(CH$_{FT}$) = H(CH$_{FT}$|K, CH$_D$)
practical secrecy – H(CH$_{FT}$|K, CH$_D$)≥α
9
K key, loss (CHD/H$_D$) – secured channel, lossy texts (CFT/CH$_{FT}$), Open text M – open channel
perfect secrecy – H(CH$_D$) = H(CH$_D$|M, CH$_{FT}$)
practical secrecy – H(CH$_D$|M, CH$_{FT}$)≥α
Input text M, loss (CHD/CH$_D$) – secured channel, K key, lossy texts (CFT/CH$_{FT}$) – open channel
perfect secrecy – H(M) = H(M|K, CH$_{FT}$), practical secrecy – H(M|K, CH$_{FT}$)≥α
If it is needed to find CH $_D$
perfect secrecy – H(CH$_D$) = H(CH$_D$|K, CH$_{FT}$)
practical secrecy – H(CH$_D$|K, CFT/CH$_{FT}$)≥α
Ensuring authenticity
CFT – lossy text
CHD – loss
FTC/ FT$_{CH}$ – lossy cyphertext
DCH/D$_{CH}$ – cyphertext loss
CH$_{FT}$ – ciphertext of the lossy text
CH$_D$ – loss ciphertext
FT$_{CH}$ – lossy ciphertext
D$_{CH}$ – loss of ciphertext

Fig. 9. Basic protocols for providing security services

The main advantage of the proposed methods and protocols for providing security services based on the use of lossy codes is the use not, and McEliece and Niederreiter MCCC on modified shortened or extended EC to ensure cryptocurrency and / or lossy text.

The unity distance for a random cipher model for which there is a probability to obtain meaningful text by randomly and equally probable selection of the key K and an attempt to decrypt the ciphertext when $N_S = H(K)\dfrac{2^{HL}}{|I|^L} = 1$ is equal to:

$$L = U_0 = \frac{H(K)}{\log|I| - H} = \frac{H(K)}{B\log|I|}, \qquad (13)$$

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

Thus, a necessary and sufficient condition for the loss of meaningless text is to reduce the code lengths of text characters beyond their redundancy. As a result, the unprofitable text has a length less than the length of the source text, and does not make sense of the source text [18, 19].

A quantitative measure of the effectiveness of the damage is the degree of destruction of the value equal to the difference between the entropy of the unprofitable text and the source text at different segments of the length of the unprofitable text:

$$d = H(FTC) - \sum_{i=1}^{s} H(M_i)\, p_i , \qquad (14)$$

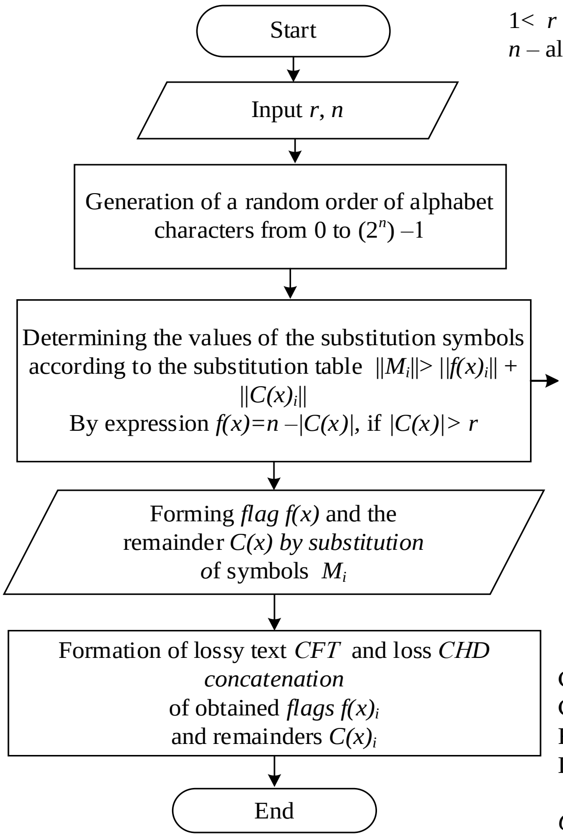
$$\sum_{i=1}^{s} p_i = 1,\ s = \left[\left(L_0 - L_{FTC} \right) / L_{FTC} \right] \qquad (15)$$

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

Fig. 10 shows a universal mechanism of damage (algorithm *MV2* (lossy text formation)).

The transformation definition set in the MV2 algorithm is a set $\{0, 1\}^n$ – consider as the power of the alphabet of a family of source texts, which is associated with some probability distribution of the letters of this alphabet, and the symbols of the source text – the value of a discrete random element [18].

The main methods of damage are shown in Fig. 11–13. 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 source data. The dependence of group operations of HCCC implementation on field strength is given in table 3. Table 4 shows the length of the transmitted data. The ratio of these values shows the bit rate of the bandwidth for each additional operation (Table 5).


Start
Input r, n
Generation of a random order of alphabet characters from 0 to (2^n) –1
Determining the values of the substitution symbols according to the substitution table ||M_i||> ||f(x)_i|| + ||C(x)_i||
By expression f(x)=n –|C(x)|, if |C(x)|> r
Forming flag f(x) and the remainder C(x) by substitution of symbols M_i
Formation of lossy text CFT and loss CHD concatenation of obtained flags f(x)_i and remainders C(x)_i
End

$1< r < n$ – a positive integer
n – alphabet power

Symbol	Remainder length	Remainder $C(x)$	Flag $f(x)$
S_1	r	0^r	$0^{n-r-1}1$
S_2	r	$0^{r-1}1$	$0^{n-r-1}1$
…	…	…	…
S_{2^r+1}	$r+1$	0^{r+1}	$0^{n-r-2}1$
…	…	…	…
$S_{2^{n-1}-2^r}$	$n-2$	1^{n-2}	01
$S_{2^{n-1}-2^r+1}$	$n-1$	0^{n-1}	1
…	…	…	…
$S_{2^n-2^r}$	$n-1$	1^{n-1}	1
$S_{2^n-2^r+1}$	r	0^r	0^{n-r}
…	…	…	…
S_{2^n}	r	1^r	0^{n-r}

CFT/ CH_{FT} – ciphertext of the lossy text
CHD/CH_D – loss ciphertext
FTC/ FT_{CH} – lossy ciphertext
DCH/D_{CH} – loss of ciphertext
$f(x)$ – flag (loss)
$C(x)$ – remainder (loss code)

Fig. 10. Universal mechanism of damage - algorithm MV2

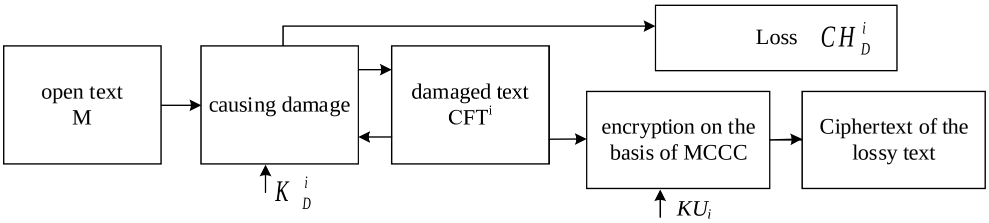


Fig. 11. Block diagram of a hybrid cryptosystem based on damage to the original text (approach 1)

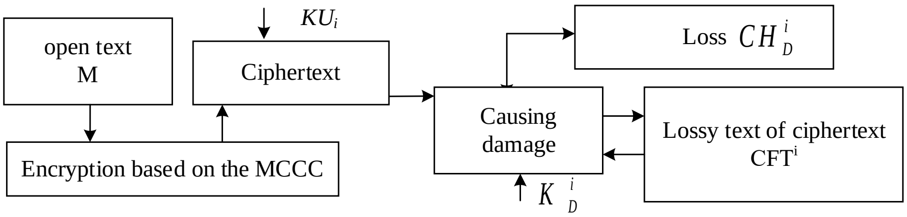


Fig. 12. Block diagram of a hybrid cryptosystem based on damage to ciphertext (approach 2)

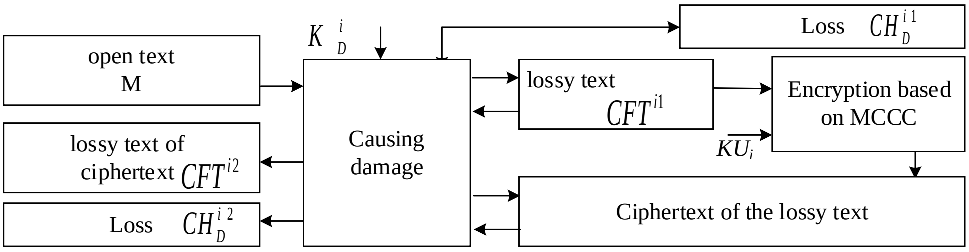


Fig. 13. Block diagram of a hybrid cryptosystem based on damage to the original text and ciphertext (approach 3)

Table 3 – **Dependence of software implementation on field strength (number of thousands of additional operations before encryption / after / amount)**

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 4 – **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

Table 5 – **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, the use of approach 3 in inflicting damage to ciphertext from the Niederreiter on MEC is shown in Fig. 7 increases the bandwidth in the field *GF* (2^9). This method is the optimal approach for building a hybrid CCC.

The algorithm for forming a cryptogram in Niederreiter HCCC is shown in Fig. 14, 15:

Step 1. Entering information to be encoded. Entering a 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 *MEC* based on the algorithm of non-binary equilibrium coding [11].

Step 3. Formation of a shortened error vector: $e_x=e(A) – IV$

Step 4. Codogram formation:

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

Step 5. Formation of unprofitable text (balance) and flag (loss):

$$E_{K_{MV2}} : S^*_{r-h_e} \to \left\| f(x)_i \right\| + \left\| C(x)_i \right\|. \qquad (16)$$

The codegram decoding algorithm in Niederreiter HCCC is shown in Fig. 16, 17*:*

Step 1. Obtaining meaningful text of the codegram based on the *MV2* algorithm:

$$E^{-1}_{K_{MV2}} : \left\| f(x)_i \right\| + \left\| C(x)_i \right\| \to S^*_{r-h_e}. \qquad (17)$$

Step 2. Input of the S_X codegram to be decoded. Entering a private key – matrices *X, P, D.*

Step 3. Finding one of the possible solutions to the equation

$$S^*_{r-h_e} = \bar{c}^* \times \left(H_X^{MEC}\right)^T. \qquad (18)$$

Step 4. Removing the effect of diagonal and permutation matrices:

$$\bar{c}^* = c_X^* \cdot D^{-1} \cdot P^{-1}. \qquad (19)$$

Step 5. Decoding of the vector $\bar{c}^*$. The formation of the vector e_x*'*.

Step 6. Transformation of the vector e_x*'*:

$$e_x = e_x' \times P \times D. \qquad (20)$$

Step 7. Formation of the desired error vector *e*:

$$e = e_x + IV \qquad (21)$$

Step 8. Transformation of the vector *e* based on the use of a non-binary equilibrium code into an information sequence.

Construction of Niederreiter's crypto-code constructions on LDPC and/or lossy codes

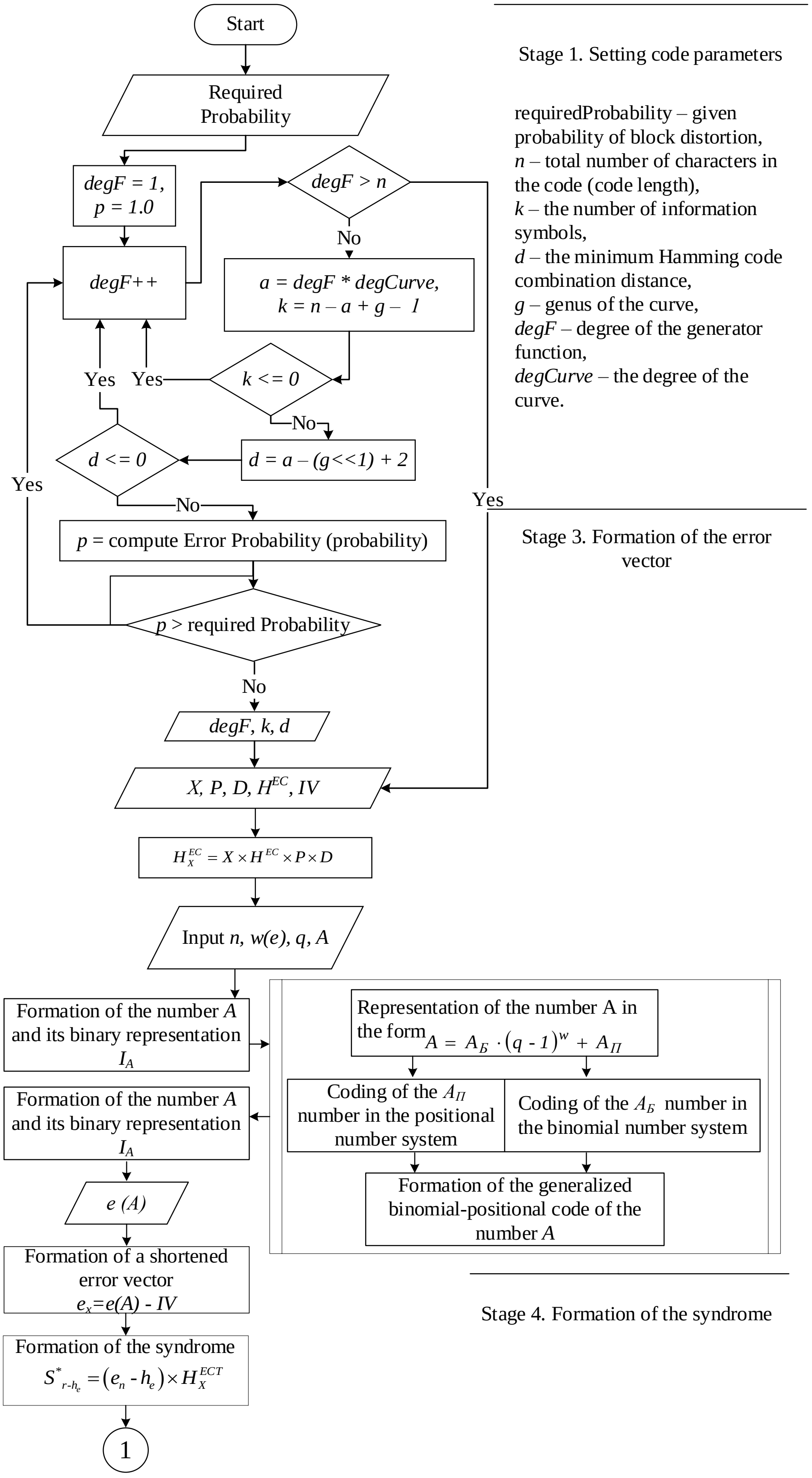
Low Density Parity Check (LDPC) codes are linear block codes whose check matrices in each column and each row have a small number of ones compared to the number of zeros in them [20–25].

To form the CCC on LDPC codes and/or lossy codes, we will use the approach of forming the *H* matrix, which is proposed in works [20–22].

A regular LDPC code with block length *n* is formed on the basis of the check matrix *H,* which is characterized by a constant number of ones in a row W_r and a constant number of ones in the column W_c.

The verification matrix H has a low density of ones (the density of ones is considered low if the specific part of ones is less than 50% of all elements of the verification matrix).

Based on the given parameters n, Wr, Wc the corrective properties of the code t, bits are changed. At the same time, the position of the ones in the verification matrix H is formed on the basis of random permutations of the columns of the base submatrix, which contains only one one in each column.


Start
Required Probability
degF = 1, p = 1.0
degF > n
No
degF++
a = degF * degCurve, k = n – a + g – 1
Yes
Yes
k <= 0
No
d <= 0
d = a – (g<<1) + 2
Yes
Yes
No
p = compute Error Probability (probability)
p > required Probability
No
degF, k, d
X, P, D, H^EC, IV
$H_X^{EC} = X \times H^{EC} \times P \times D$
Input n, w(e), q, A
Formation of the number A and its binary representation I_A
Representation of the number A in the form $A = A_Б \cdot (q-1)^w + A_П$
Coding of the $A_П$ number in the positional number system
Coding of the $A_Б$ number in the binomial number system
Formation of the number A and its binary representation I_A
Formation of the generalized binomial-positional code of the number A
e (A)
Formation of a shortened error vector $e_x=e(A) - IV$
Formation of the syndrome $S^*_{r-h_e} = (e_n - h_e) \times H_X^{ECT}$
1

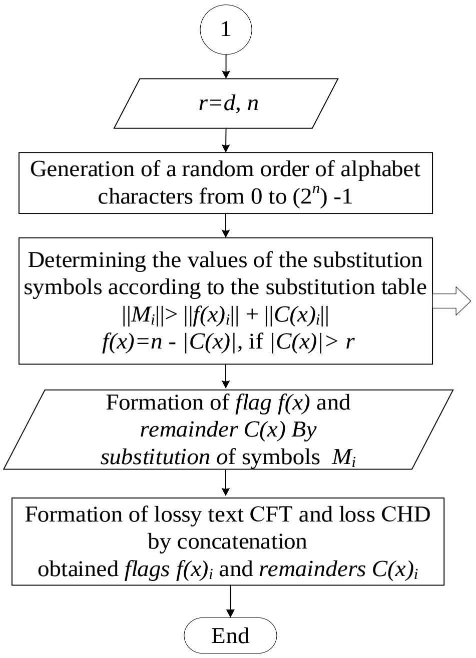
Stage 1. Setting code parameters

requiredProbability – given probability of block distortion,
n – total number of characters in the code (code length),
k – the number of information symbols,
d – the minimum Hamming code combination distance,
g – genus of the curve,
degF – degree of the generator function,
degCurve – the degree of the curve.

Stage 3. Formation of the error vector

Stage 4. Formation of the syndrome

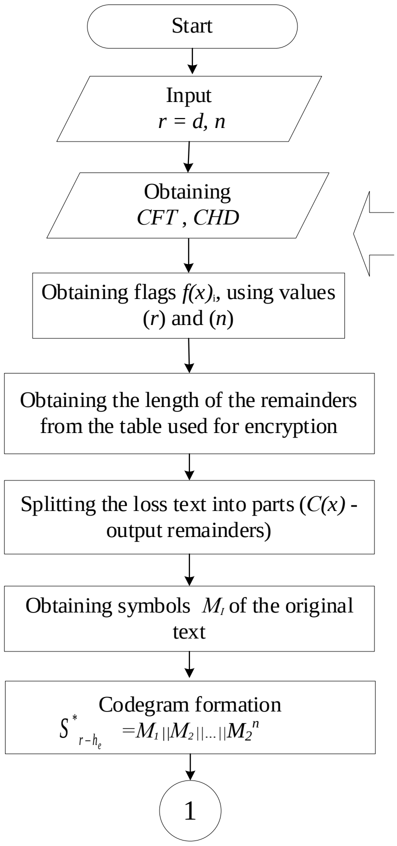
Fig. 14. Codegram formation in Niederreiter HCCC on MEC


1
r=d, n
Generation of a random order of alphabet characters from 0 to (2^n) -1
Determining the values of the substitution symbols according to the substitution table
||M_i||> ||f(x)_i|| + ||C(x)_i||
f(x)=n - |C(x)|, if |C(x)|> r
Formation of flag f(x) and remainder C(x) By substitution of symbols M_i
Formation of lossy text CFT and loss CHD by concatenation obtained flags f(x)_i and remainders C(x)_i
End

Stage 5. Causing damages

Symbol	remainder length	remainder $C(x)$	Flag $f(x)$
S_1	r	0^r	$0^{n-r-1}1$
S_2	r	$0^{r-1}1$	$0^{n-r-1}1$
…	…	…	…
S_{2^r+1}	$r+1$	0^{r+1}	$0^{n-r-2}1$
…	…	…	…
$S_{2^{n-1}-2^r}$	$n-2$	1^{n-2}	01
$S_{2^{n-1}-2^r+1}$	$n-1$	0^{n-1}	1
…	…	…	…
$S_{2^n-2^r}$	$n-1$	1^{n-1}	1
$S_{2^n-2^r+1}$	r	0^r	0^{n-r}
…	…	…	…
S_{2^n}	r	1^r	0^{n-r}

Fig. 15. Codegram formation in Niederreiter HCCC on MEC


Start
Input
r = d, n
Obtaining
CFT , CHD
Obtaining flags f(x)_i, using values (r) and (n)
Obtaining the length of the remainders from the table used for encryption
Splitting the loss text into parts (C(x) - output remainders)
Obtaining symbols M_I of the original text
Codegram formation
S*_{r-h_e} =M_1||M_2||...||M_2^n
1

Stage 1. Formation of a meaningful

Symbol	Remainder length	Remainder $C(x)$	Flag $f(x)$
M_1	r	0^r	$0^{n-r-1}1$
M_2	r	$0^{r-1}1$	$0^{n-r-1}1$
…	…	…	…
M_{2^r+1}	$r+1$	0^{r+1}	$0^{n-r-2}1$
…	…	…	…
$M_{2^{n-1}-2^r}$	$n-2$	1^{n-2}	01
$M_{2^{n-1}-2^r+1}$	$n-1$	0^{n-1}	1
…	…	…	…
$M_{2^n-2^r}$	$n-1$	1^{n-1}	1
$M_{2^n-2^r+1}$	r	0^r	0^{n-r}
…	…	…	…
M_{2^n}	r	1^r	0^{n-r}

$f(x)$ – flag,
$C(x)$ – remainder

Fig. 16. Codegram decoding in Niederreiter HCCC on MEC

At the same time, the speed of the regular LDPC code, depending on the parameters of the check matrix, is determined by the formula:

$$r_k = \frac{n - \left(\begin{array}{c} n\cdot W_c/W_r - \\ -(W_c-1) \end{array} \right)}{n} = 1-\frac{W_c}{W_r}+\frac{W_c-1}{n}. \tag{22}$$

At the same time, LDPC code H matrices of the same size and with the same parameters can generate codes with different code distance d and correction ability t. From this follows the task of finding the best verification matrix of the LDPC code with the given parameters n, W_r, W_c by the criterion of the maximum corrective capacity

$$t_{\max} \le (d_{\max}-2)/2.$$

The verification matrix of the LDPC code can be represented as:

$$H = \left[\begin{array}{c} H_1/\pi_1(H_1) \\ \vdots/\pi_{Wc-1}(H_1) \end{array} \right], \tag{23}$$

where H_1 – base submatrix, $\pi_1(H_1)$ – submatrices obtained by randomly permuting the columns of the base submatrix H_1, $i = 1, 2, \ldots, W_c - 1$.

The verification matrix H can be reduced to the form:

$$H = \left[A \middle| I_{n-k} \right], \tag{24}$$

where A – some fixed $((n-k)\times k)$ – matrix with 0 and 1 (no longer sparse with ones), and I_{n-k} – a ones matrix of size $((n-k)\times(n-k))$.

The code word generation matrix G has the form:

$$G = \left[I_k \middle| -A^T \right]. \tag{25}$$

If the matrix H is presented in the form (24), then the matrix G (25) is easily obtained from the matrix H by transformations using the Gaussian method [26, 27]. The code distance d for a regular LDPC code is defined as follows: d is equal to the smallest number of columns of the H matrix, which in sum give 0; d is equal to the smallest weight of a row (the number of ones in a row) of the matrix G.

Use of these codes ensures compliance with the IEEE 802.16 standard. LDPC codes in the IEEE 802.16e standard are all represented by independent check matrices. For these verification matrices, there are a total of six basic matrices that's why 802.16e LDPC codes have strict structures and dimensions. Suppose the verification matrix H has size $m \times n$, where m is the number of parity checks and n – is the number of codeword coordinates. Thus, the code size (number of source symbols) $k = n - m$.

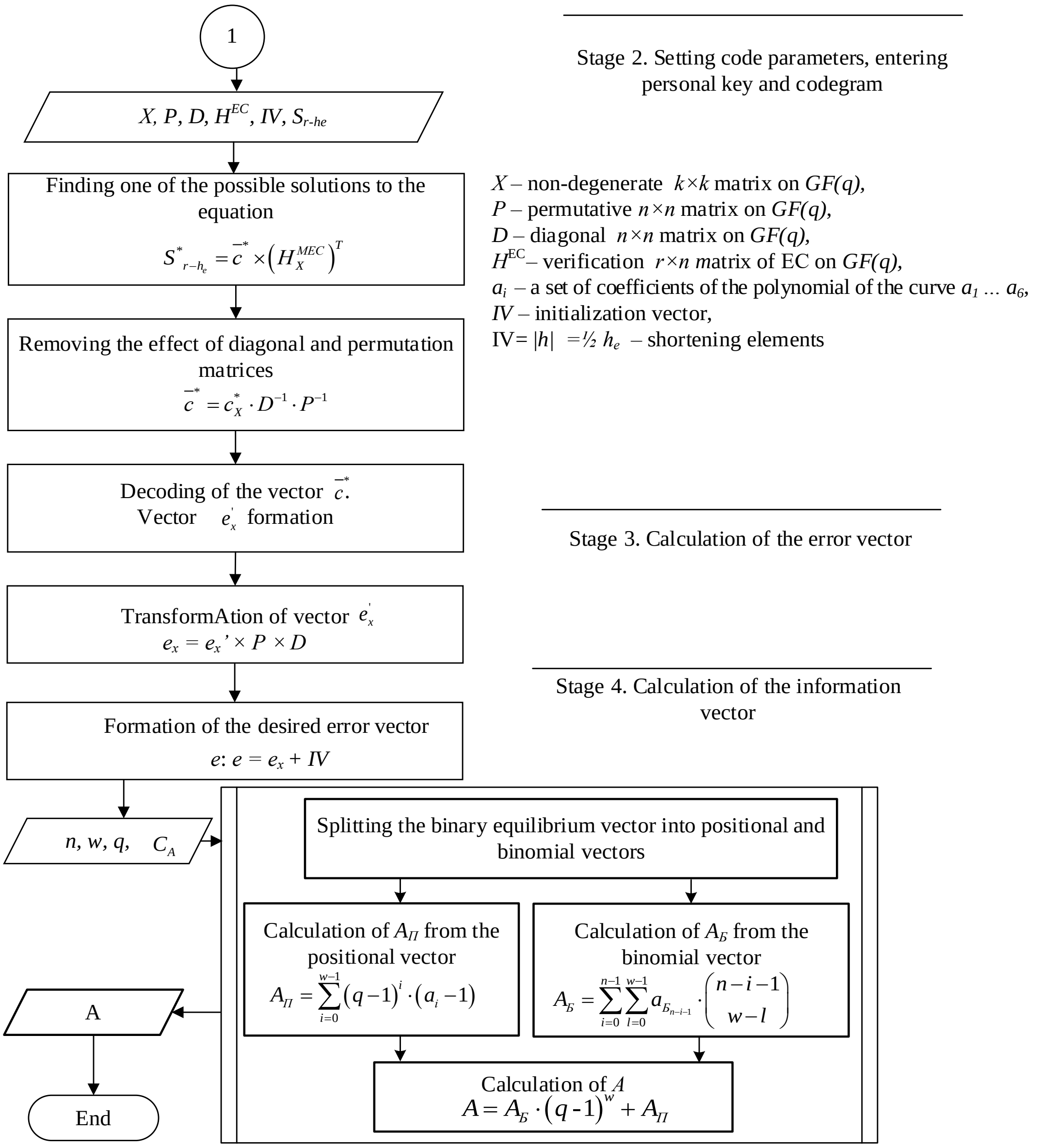

1
Stage 2. Setting code parameters, entering personal key and codegram
$X, P, D, H^{EC}, IV, S_{r-he}$
Finding one of the possible solutions to the equation
$S^*_{r-h_e} = \bar{c}^* \times (H_X^{MEC})^T$
X – non-degenerate $k\times k$ matrix on GF(q),
P – permutative $n\times n$ matrix on GF(q),
D – diagonal $n\times n$ matrix on GF(q),
H^{EC}– verification $r\times n$ matrix of EC on GF(q),
a_i – a set of coefficients of the polynomial of the curve $a_1 \dots a_6$,
IV – initialization vector,
IV= |h| =½ h_e – shortening elements
Removing the effect of diagonal and permutation matrices
$\bar{c}^* = c_X^* \cdot D^{-1} \cdot P^{-1}$
Decoding of the vector $\bar{c}^*$.
Vector e_x' formation
Stage 3. Calculation of the error vector
TransformAtion of vector e_x'
$e_x = e_x' \times P \times D$
Stage 4. Calculation of the information vector
Formation of the desired error vector
e: $e = e_x + IV$
n, w, q, C_A
Splitting the binary equilibrium vector into positional and binomial vectors
Calculation of $A_П$ from the positional vector
$A_П = \sum_{i=0}^{w-1} (q-1)^i \cdot (a_i - 1)$
Calculation of $A_Б$ from the binomial vector
$A_Б = \sum_{i=0}^{n-1} \sum_{l=0}^{w-1} a_{Б_{n-i-1}} \cdot \binom{n-i-1}{w-l}$
A
Calculation of A
$A = A_Б \cdot (q-1)^w + A_П$
End

Fig. 17. Codegram decoding in Niederreiter HCCC on MEC

The check matrix is a combination of several $z \times z$ submatrices. Each submatrix or permutation is either a ones matrix or a zero matrix, so the base matrix simply needs to be a set of numbers that define the individual right-cycle shifts for the permutations. The size of the base matrix $m_b \times n_b$, where $m = zm_b$ and $n = zn_b$ (so we can determine $k = zk_b$). The input data of the base matrix are real numbers not less than -1. The verification matrix is constructed by replacing each entry of the base matrix with $z \times z$ submatrix: every –1 is exchanged with a zero matrix and every non-negative number with a ones matrix with a cyclic right shift. Therefore, given the code dimension k (or block length n) and the basis matrix, the LDPC code is defined.

Apparently, any LDPC code check matrix in the IEEE 802.16e standard is represented in an approximate lower-triangular form without any row or column operations, so fast coding can be incorporated directly. For any matrix H in 802.16e, it always has $N = n$ and $g = z$. This approach allows using these channels for the transmission of both control and combat commands/signals.

Assessment of the stability of the proposed crypto-code constructions

To estimate time and speed indicators, it is customary to use a unit of measurement *cpb*, where *cpb* (*cycles per byte*) – the number of processor cycles required to process 1 byte of input information.

The complexity of the algorithm can be calculated using the expression

$$Per = Utl * CPU\_clock / Rate, \qquad (26)$$

where *Utl* – processor core utilization (%); *Rate* – Algorithm bandwidth (byte/s).

Table 6 shows the results of studies of the dependence of the length of the input sequence on the *MV2* algorithm on the number of processor cycles.

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

Table 8 shows the results of research on the dependence of the length of the code sequence of

Niederreiter HCCC on the number of processor cycles for performing elementary operations in the software implementation of CCC.

Analysis of the results of the table 8 showed that the energy consumption of the practical implementation of Niederreiter HCCC will decrease by 7%, while the implementation is possible on the main hardware and software platforms that have become widespread:

– 8/16-bit microcontrollers and smart cards;

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

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

Table 9 presents the results of studies of the assessment of time and speed indicators of procedures for applying and removing damages.

Table 6 – **Results of research on the dependence of the length of the input sequence on the MV2 algorithm on the number of processor cycles**

The length of the code sequence		***MV*2**		
		10	**100**	**1000**
The number of function calls that implement elementary operations	addition	3942	28673	275499
	subtraction	1794	3810	23881
	division	3274	4804	20104
	multiplication	19	109	1009
	comparison	8939	60963	578784
Sum		17968	98359	899277
Duration of execution of functions* in processor clocks	addition	19.53	93.58	2297.36
	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	4826.43
Sum		89	321	7499
Duration of execution** in msec		89	321	7499

*Note: * – duration of 1000 operations in processor clocks: character reading – 27 clocks, line comparison – 54 clocks, line concatenation – 297 clocks; ** – for the calculation, a processor with a clock frequency of 2 GHz is taken, taking into account the loading of the operating system at 5%*

Table 7 – **Research results of evaluation of time and speed indicators of procedures for applying and removing damage**

Indicators	**The length of the code sequence**	**Bandwidth of the algorithm, Rate (bytes/sec)**	**Processor core utilisation (%)**	**Algorithm complexity, Per (cpb)**	**Indicators**
The number of calls to functions 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

Table 8 – **Results of research on the dependence of the length of the code sequence on the number of processor cycles**

The length of the code sequence		**Niederreiter HCCC on *MEC***			**Niederreiter CCC on *MEC***		
		10	**100**	**1000**	**10**	**100**	**1000**
The number of function calls that implement elementary operations	Reading the symbol	10294 397	28750 457	76759 874	11018 042	30800 328	80 859 933
	String comparison	3 406 921	9 246 748	25478 498	3 663 356	10199 898	26 364 634
	String concatenation	1 705 544	5 045 748	12379 422	1834 983	5125 564	13 415 329
Sum		15406 862	43042 953	114617 794	16516 381	46125 790	120639 896
Duration of execution of functions* in processor clocks	Reading the symbol	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
Sum		1 006 781	2 749 548	7 247 488	1 040 298	2 904 696	7 591 261
Duration of execution** in msec		0,52	1,37	3,4	0,55	1,53	4

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

Table 9 – **Results of studies of the assessment of time and speed indicators of procedures for applying and removing damage**

Indicators	The length of the code sequence	Working time (s)	Bandwidth of the algorithm, Rate (bytes/sec)	Processor core utilisation (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 analysis of the basic principles of the construction of Niederreiter MCCC and systems of multi-channel cryptography on lossy codes allows for the development of hybrid cryptosystems.

The main difference from the "classical" approach of forming a hybrid cryptosystem is the use of CCC with fast algorithms of crypto-transformations (the speed of transformations can be compared with the speed of crypto-transformations in BSC). Niederreiter CCC acts as the main mechanism for ensuring the stability (security) of information with the subsequent use of the *MV2* algorithm (systems based on lossy codes).

This approach provides a reduction in energy costs (the power of the Niederreiter MCCC alphabet) with further transmission through one or more channels, which allows the use of almost every type of cyberspace channel in a prospective system of joint leadership and military control.

Statistical tests are used to experimentally assess how closely crypto-algorithms approximate generators of "random" sequences [11].

The NIST STS test suite was proposed as part of a competition for a new US national block cipher standard. This set was used to investigate the statistical properties of candidates for a new block cipher.

Today, the testing method proposed by NIST is the most common among developers of cryptographic means of information protection [11].

The results of the research are given in table 10.

Table 10 – **Results of statistical security studies**

Cryptosystems	Number of tests in which > 99% of sequences passed tests, (%)	Number of tests in which > 96% of sequences passed tests	Number of tests in which < 96% of sequences passed tests
CCC on *MEC*	149 (78,83)	189	0
CCC on shortened *MEC*	151 (79,89)	189	0
CCC on lengthened *MEC*	152 (80,42)	189	0
HCCC on shortened *MEC*	**153** (80,95)	189	0
HCCC on lengthened *MEC*	**155** (82)	189	0

The results in the table 10, show that despite the reduction of the field strength to $GF(2^6)$ for MCCC and $GF(2^4)$ for HCCC, the statistical characteristics of such crypto-code constructions turned out to be, at least, no worse than the traditional Niederreiter CCC on $GF(2^{10})$. All cryptosystems passed 100% of tests, and the best result was shown by HCCC 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, Niederreiter traditional CCC on $GF(2^{10})$ showed 149 tests at the level of 0.99. The results of the speed of transformations are shown in Fig. 18.

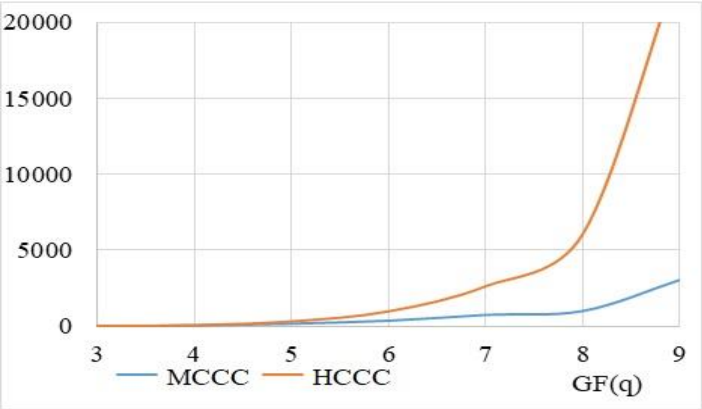


Fig. 18. Dependencies of the complexity of cryptogram formation, when using (n, *k*, *d*) code on GF(*q*)

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

The complexity of decoding is determined by the complexity of the algebraic algorithm for decoding the algebraic block code.

For BCH codes, RS codes and their generalizations, alternative codes and their subclasses, error localization is reduced to solving a system of linear equations.

The complexity of decoding is:

$$S_{рш}=n^{5/2}+(2\times n^3)+t^{5/2}, \qquad (27)$$

$$S_{рш(HCCC)}=n\times m\times L+n^{5/2}+(2\times n^3)+t^{5/2}. \qquad (28)$$

The dependence of addition and multiplication operations on the finite field in various cryptosystems is presented in the table 11. The results in the table 10 confirm a reduction of ≈ 7 times the number of addition and multiplication operations over the finite field in the proposed HCCC on lossy codes over $GF(2^4)$ in comparison with MCCC on *MEC* over the field $GF(2^6)$.

The obtained result confirms the competitiveness of HCCC in post-quantum cryptography.

Table 11 – **Dependence of addition and multiplication operations on the final field in different cryptosystems**

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

Conclusions

1. In the conditions of a hybrid war, the use of means of information suppression/blocking significantly reduces the possibility of using control system means and communication channels based on outdated hardware communication tools and a cipher body. The use of civilian channels of cyberspace (a set of Internet, computer and mobile technology channels) requires the use of cryptographic systems. However, in the conditions of the rapid growth of computing capabilities of quantum computers (the emergence of full-scale quantum computers), ensuring the stability of classical symmetric and asymmetric cryptosystems (including asymmetric cryptosystems based on elliptic curves) is called into question. Which in turn requires the use of post-quantum cryptography algorithms. Among the contenders are the crypto-code constructions of McEliece and Niederreiter, which provide stability requirements and integrated (additionally) ensure the reliability and efficiency of providing information.

2. The presented algorithms of crypto-code constructions provide the necessary level of stability, efficiency and reliability when using various communication channels, which allows their use in a prospective system of joint leadership and military management in the conditions of conducting hybrid warfare.

3. The combination of crypto-code constructions with damage mechanisms (lossy codes) provides an additional increase (maintenance) of the stability level and the practical implementation of HCCC on various algebraic geometric codes and/or LDPC codes. This approach provides a ≈ 7-fold reduction in the number of addition and multiplication operations over the final field in the proposed HCCC on lossy codes over $GF(2^4)$ in comparison with MCCC on MEC over the field $GF(2^6)$ and the possibility of timely change of constructions and/or code constructions, which will allow to ensure the use of cyberspace channels in the prospective system of joint management and military control.

References

1. (2021), *Cybersecurity Strategy of Ukraine safe cyberspace is the key to successful development of the country*, Decree of the President of Ukraine dated August 26, 2021 No. 447/2021, URL: https://www.president.gov.ua/documents/4472021-40013.
2. (2021), *Про Стратегічний оборонний бюлетень України*, Decree of the President of Ukraine dated August 20, 2021 No. 473/2021, URL: https://www.president.gov.ua/documents/4732021-40121.
3. (2016), *Report on Post-Quantum Cryptography*, URL: http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf
4. Hryshchuk, R.V. and Danik, Yu.G. (2016), *Fundamentals of cyber security*, Monograph, Zhnaeu, Zhytomyr, 2016, 636 p.
5. Ralph D., Thiele (2013),"Building C4ISR Capabilities in and for the Gulf", *ISPSW Strategy Series*, Issue No. 227, available at: https://www.files.ethz.ch/isn/164095/227_Thiele.pdf
6. National Research Council (2006), *C4ISR for Future Naval Strike Groups*, 300 p., available at: http://nap.edu/11605.
7. Yevseev, S.P., Tomashevskyi, B.P., Ivanchenko, S.O., Zinchenko, Y.V. and Havrylenko O.V. (2021), "Structural model of a modified special purpose system", *Special Telecommunications Systems and Information Protection*, Issue 1 (35), pp. 25–39.
8. Bartock, M., Cichonski, J., Souppaya, M., Smith, M., Witte, G. and Scarfone, K. (2016), *Guide for Cybersecurity Event Recovery*, NIST, DOI: https://doi.org/10.6028/NIST.SP.800-184
9. NIST (2020), *Security requirements for cryptographic modules*, URL: https://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
10. NIST (2017), Guide to LTE Security, URL: https://csrc.nist.gov/publications/drafts/800-187/sp800_187_draft.pdf
11. Yevseiev, S., Ponomarenko, V., Laptiev, O. and Milov, O. (2021), *Synergy of building cybersecurity systems*, monograph, PC TECHNOLOGY CENTER, Kharkiv, 188 p.
12. Sidelnikov, V. M. (2002), "Cryptography and Coding Theory", *Moscow University and the Development of Cryptography in Russia*, MSU, Moscow, pp. 1-22.
13. Kuznetsov, O.O., Yevseev, S.P. and Watermelon S.V. (2008), *Information protection and economic security of the enterprise*, Monograph, KhNEU, Kharkiv, 360 p.

14. Kuznetsov, O. O., Evseyev, S. P., Kavun, S. V. and Korol, O. G. (2009), *Signals and codes. Algebraic Methods for Synthesis*, Monograph, KhNEU, Kharkiv, Ukraine, 384 p.
15. Hoppa, V. D. (1984), "Codes and information", *Uspekhi matematicheskih nauk*, Vol. 30, no. 1(235), pp. 77–120.
16. Yevseyev, S.P. and Tsyhanenko, O.S. (2018), “Development of Niederreiter's asymmetric crypto-code construction on modified elliptic codes”, *Information Processing Systems*, Issue 2(153), pp. 127-135.
17. Rzayev, Kh. and Mammadova T. (2018), “Mathematical model of the modified Niederreiter crypto-code structures”, Advanced Information Systems, Vol. 2, No. 4, pp. 37-44, DOI: https://doi.org/10.20998/2522-9052.2018.4.06
18. Michtchenko, V., and Vilanski, Y. (2007), *Damaged texts and multichannel cryptography*, Encyclopedics, Minsk, 292 p.
19. .Michtchenko, V., Vilanski, Y., and Lepin, V. (2007), *MV 2 cryptographic algorithm*, Minsk, 2007, 147 p.
20. Rafael, Misoczki, Jean-Pierre, Tillich, Nicolas, Sendrier and Paulo S. L. M., Barreto (2013), *MDPC-McEliece: New McEliece Variants from Moderate Density Parity-Check Codes*, 21 p., available at: https://eprint.iacr.org/2012/409.pdf.
21. Kozlov, A. V., Krouk, E. A., and Ovchinnikov, A. A. (2013), ”An approach to development of block-commutative codes with low density of parity check”, *Journal of instrument engineering*, Vol. 56, No. 8, pp. 9-14.
22. Akulinin, S.A. and Sviridova, I.V. (2015), “Setting ldpc codes for channels with additive white gaussian noise“, *Bulletin of VSTU*, Vol. 11, No. 6, pp. 117-120.
23. Novikov, R.S. and Astrakhantsev, A.A. (2013), “Analysis of characteristics of error-correcting codes”, *Information processing systems*, issue 9 (116), pp. 164–167.
24. Bashkirov, A.V. (2015), Implementation of the LDPC-decoder on the massively parallel computing devices, VSTU, Voronezh.
25. Huang, J., Zhou, S. and Willett, P. (2008), “Nonbinary LDPC coding for multicarrier underwater acoustic communication”, *IEEE J. Sel. Areas Commun.*, pp. 1684-1696, DOI: https://doi.org/10.1109/JSAC.2008.081208
26. Berlekamp, E.R. (2015), *Algebraic Coding Theory: Revised Edition,* Revised ed. Edition, WSPC, 502 p.
27. Blahut, R. (1983), *Theory and Practice of Error Control Codes Reprint. with corr Edition,* Addison-Wesley, 500 p.

Received (Надійшла) 21.03.2022
Accepted for publication (Прийнята до друку) 15.06.2022

ВІДОМОСТІ ПРО АВТОРІВ / ABOUT THE AUTHORS

Томашевський Богдан Паїсійович – кандидат технічних наук, старший науковий співробітник, кафедра кібербезпеки, Тернопільський національний технічний університет ім. І. Пулюя, Тернопіль, Україна;
Bogdan Tomashevsky – Candidate of Engineering Sciences, Senior researcher, Department of Cyber Security, Ternopil Ivan Puluj National Technical University, Ternopil, Ukraine;
e-mail: bogdan_tomashevsky@tntu.edu.ua; ORCID ID: https://orcid.org/0000-0002-1934-4773.

Євсєєв Сергій Петрович – доктор технічних наук, професор, професор кафедри кібербезпеки, Національний технічний університет “Харківський політехнічний інститут”, Харків, Україна;
Serhii Yevseiev – Doctor of Technical Sciences, Professor, Department of Cyber Security, National Technical University “Kharkiv Polytechnic Institute”, Kharkiv, Ukraine;
e-mail: Serhii.Yevseiev@gmail.com; ORCID ID: https://orcid.org/0000-0003-1647-6444.

Погасій Сергій Сергійович – кандидат економічних наук, доцент, доцент кафедри кібербезпеки, Національний технічний університет “Харківський політехнічний інститут”, Харків, Україна;
Serhii Pohasii – Candidate of Economic Sciences, Associate Professor, Department of Cyber Security, National Technical University “Kharkiv Polytechnic Institute”, Kharkiv, Ukraine;
e-mail: spogasiy1978@gmail.com; ORCID ID: https://orcid.org/0000-0002-4340-3693.

Мілевський Станіслав Валерійович – кандидат економічних наук, доцент кафедри кібербезпеки, Національний технічний університет “Харківський політехнічний інститут”, Харків, Україна;
Stanislav Milevskyi – Candidate of Economic Sciences, Associate Professor, Department of Cyber Security, National Technical University “Kharkiv Polytechnic Institute”, Kharkiv, Ukraine;
e-mail: milevskiysv@gmail.com; ORCID ID: https://orcid.org/0000-0001-5087-7036.

Механізми забезпечення безпеки каналів перспективної системи управління

Б. П. Томашевський, С. П. Євсеєв, С. С. Погасій, С. В. Мілевський

Анотація. Розвиток систем військового (державного) управління в сучасних умовах гібридної війни вимагає можливості стрімкого розширювання як функціональності, так і масштабування фізичної та логічної основи управління, нарощування спектра цифровізації та використання як військових, так і цивільних каналів зв’язку щодо управління військами та зброєю. При цьому необхідно враховувати не тільки обчислювальні можливості противника, засоби придушення та/або блокування каналів зв’язку системи управління, а також розвиток квантових технологій, які висувають нові більш жорсткі вимоги до механізмів забезпечення безпеки на основі алгоритмів симетричної та несиметричної криптографії. За рахунками спеціалістів НІСТ США повномасштабний квантовий комп’ютер забезпечує злам, як симетричних, так й несиметричних криптосистем за поліноміальний час, що суттєво зменшує їх стійкість. В роботі пропонуються механізми постквантової криптографії, які дозволяють забезпечити стійкість не тільки каналів зв’язку, та й елементів структури системи управління. Основою постквантових алгоритмів шифрування поєднання алгоритмів (схем) крипто-кодових конструкцій з криптосистемами на збиткових кодах (багатоканальної криптографії),а також можливість їх поєднання з методами цифровій стеганографії. Такий підхід забезпечує можливість приховування елементів управлінських команд, а використання різних каналів забезпечує можливість приховування окремих елементів криптограм.

Ключові слова: крипто-кодові конструкції; алгеброгеометричні коди; LDPC-коди; система управління військами; квантовий період.