Caspian Journal of Applied Mathematics, Ecology and Economics
V. 5, No 2, 2017, December
ISSN 1560-4055

Development of a Modified Asymmetric McEliece Crypto-code System Elongated on Elliptic Truncated Codes

Kh. Rzayev

Abstract. Offers mathematical model of asymmetric crypto-code system based on McEliece theoretical-code scheme, practical algorithms of cryptogram/codegram encryption/encoding and decryption/decoding, analyze the expenses on software implementation of the information protection crypto-code means based on McEliece TCS.

Key Words and Phrases: asymmetric crypto-code system, theoretical-code system, modified error-correcting codes.

1. Introduction and analysis of the literature

Development of telecommunication systems and technologies, the rapid growth of computer technology put forward new requirements for the basic quality of customer service criteria (authorized users). The main indicators for the results of the analysis of standards in this area are ensuring authenticity of (reliability) transmitting data and ensuring the security of the entire processing cycle and data storage [1, 2, 3]. To provide the authenticity are used mechanisms of error-correcting coding, and to provide security - cryptographic mechanisms based on the methods of symmetrical and asymmetrical cryptography. Perspective direction, in our opinion, is the use of asymmetric cryptosystems based on McEliece theoretical - code schemes, which provide integrated (one mechanism) authenticity of indicators at the level of 2^9– 2^{12} and cryptographic strength - 2^{30} – $2^{35}$of group operations while it build over GF(2^{10}). Given cryptosystem has been widely used with the development of computing capabilities and communication devices and their software. In [4], the authors propose to use a cryptosystem McEliece Sequitur software, which allows integrated to solve performance problems and security in the transmission of confidential information. In [5, 6, 7] McEliece cryptosystem is offered to use for provide basic security services: confidentiality and integrity in stegasystem based on MPEG Layer-III or MP3 audio files, to ensure accessibility and digital signature while transferring confidential medical information. At the same time, carried out in [8] analysis of program realization of asymmetric crypto-code system on the Niederreiter TCS showed significant implementation complexity that makes it difficult to use theoretical coding schemes for

the construction of asymmetric cryptographic systems. In [9] are considered the new approaches to breaking the McEliece cryptosystem based on randomized concatenated codes.

To provide the required indicators of cryptographic strength and increase volume of transmitted data by the authors is proposed McEliece modified asymmetric crypto-code system (MACCS) on the elongated elliptical codes, which is a promising direction in solving this scientific and technical problems.

2. The aims and tasks of the research

The purpose of work is to consider the mathematical model of McEliece MACCS, algorithms, encryption / decryption information MACCS, study their implementation complexity, analysis of program realization costs of MACCS on modified (elongated) elliptic codes.

To achieve this goal the following tasks were set:

– develop a method for masking McEliece MACCS on the elongated elliptical codes;

– consider the mathematical model and basic algorithms to transform information McEliece MACCS on the elongated codes;

– carry out a study of tasks complexity encoding/decoding and encryption/ decryption codegram/cryptogram when implemented in different levels of cryptographic resistance;

– analyze the costs of software implementation of the crypto-code means of information security based on McEliece TCS.

3. Developing a method of masking McEliece elliptic codes MACCS using curve parameters as secret data

Known methods for the modification of linear block codes more fully discussed in [10 – 14]. Fig. 1 shows the most common modification methods.

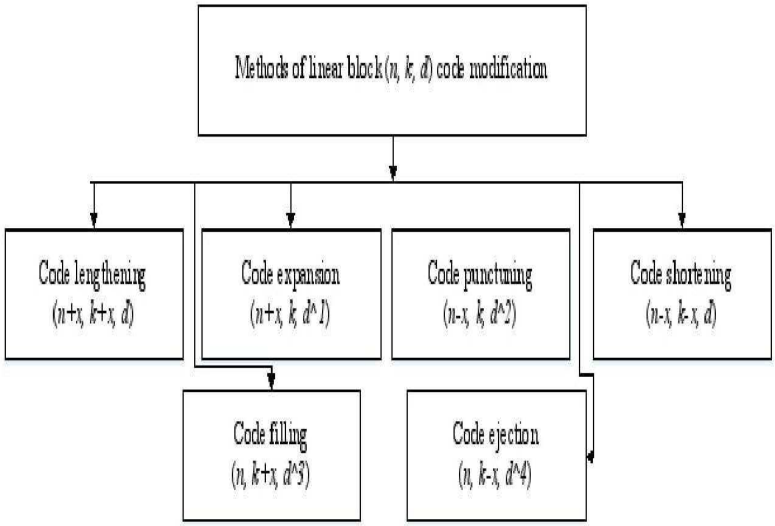

Fig. 1. Means of linear block codes modification

Lengthening of (n, k, d) linear block code is to increase the length of the $n + x$ by adding new information symbols $k + x$. *Expansion* of $(n,\ k,\ d)$ linear block code is to increase the length of the $n + x$ by adding new check symbols $r + x$. *Punctuning* $(n,\ k,\ d)$ of linear block code is to reduce the length of the n - x by decreasing of check symbols r - x. *Shortening (n, k, d)* of linear block code is to reduce the length of the n - x by decreasing of check symbols k – x. *Filling* (n, k, d) of linear block code is to increase the length of the $k + x$ information symbols without increasing the code length. *Ejection* (n, k, d) of linear block code is to reduce the k – x information symbols without code length increasing.

Potential resistance of theoretical code schemes defined by the complexity of decoding the random (n, k, d) block code. Hence, for the construction of a potentially persistent theoretical code schemes should be used modification techniques that do not allow reducing the minimum code distance. Methods of lengthening and shortening of the linear block codes do not change the minimum distance and, therefore, allow us to construct asymmetric crypto-code systems resistant to breaking [15].

Using the definition of elliptic codes [15, 16], we have the following properties:

Property 1. Elliptic (n, k, d) code over $GF(q)$, built through projection $\varphi : EC \to P^{k-1}$, connected with characteristics $k + d \geq n$, where: $n \leq 2\sqrt{q}+q+1$, $k \geq \alpha$, $d \geq n - \alpha$, $\alpha = 3\ .\ degF$.

Property 2. Elliptic (n, k, d) code over $GF(q)$, built through projection $\varphi : EC \to P^{r-1}$, connected with characteristics $k + d \geq n$, where $n \leq 2\sqrt{q} + q + 1$, $k \geq n - \alpha$, $d \geq \alpha$, $\alpha = 3\ .\ degF$.

Suppose A - generating matrix of elliptic $(n,\ k,\ d)$ code over $GF(q)$ dimension of $M \times n$, $M = \alpha$, α=3. $degF$.

$$A = \begin{pmatrix} F_0(P_0) & F_0(P_1) & ... & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & ... & F_1(P_{n-1}) \\ ... & ... & ... & ... \\ F_{M-1}(P_0) & F_{M-1}(P_1) & ... & F_{M-1}(P_{n-1}) \end{pmatrix} = \|F_j\,(P_i)\|_{n,M}\,.$$

To reduce the amount of key data in code-theoretic scheme on elliptic codes use the following features of the matrix A construction.

The generating matrix A is formed as a result of displaying elliptic curve points by basis of generating functions. The generating matrix of the elliptic code is built on curve

$$y^2z + a_1xy + a_3yz^2 = x^3 + a_2x^2z + a_4xz + a_6z^3,$$

$a_i \in GF(q)$, with the polynomial coefficients, which uniquely define the form of the curve and, accordingly, multiplicity of projective points which construct elliptic code (its generating matrix). Following statement is true.

Statement 1. [15] Elliptic $(n,\ k,\ d)$ code over $GF(q)$ is uniquely defined by multiplicity $a_1 \ldots\ a_6, \forall a_i \in GF(q)$.

Proof. Consider an elliptic generating matrix of elliptic $(n,\ k,\ d)$ code over $GF(q)$:

$$A = \begin{pmatrix} F_0(P_0) & F_0(P_1) & ... & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & ... & F_1(P_{n-1}) \\ ... & ... & ... & ... \\ F_{M-1}(P_0) & F_{M-1}(P_1) & ... & F_{M-1}(P_{n-1}) \end{pmatrix}.$$

Each character of generating matrix is formed by calculating the value of the generating function Fj in the point Pi of elliptic curve. The number M of generating functions is determined by the design characteristics of an elliptic $(n,\ k,\ d)$ code. Kind of functions Fj is determined by degree a of curve points projection and, therefore, defined by code design parameters.

Thus, if design $(n,\ k,\ d)$ elliptic code characteristics is given, the uniqueness of the generator matrix defines a multiplicity of points $P1,\ P2,\ \ldots,\ Pn$, which are computed generator functions values. A specific multiplicity of points from space P^2 is uniquely determined by polynomial curve view i.e. multiplicity of coefficients $a_1 \ldots\ a_6, \forall a_i \in GF(q)$.

Corollary 1. The volume of private key (in bits) in motivated crypto-code system based on the theoretical - code McEliece scheme built on elliptical $(n,\ k,\ d)$ code over $GF(2^m)$ is determined by the sum of matrix elements $X,\ P,\ D$ (in bits), and is given by

$$l_{K_+} = 5 \times n^2 \times k^2 \times m. \tag{1}$$

Proof. Indeed, secret key in McEliece scheme - generating matrix A (generating code matrix) and masking matrix $X,\ P,\ D$. In order to determine private key (in bits) of an elliptic $(n,\ k,\ d)$ code over $GF(2^m)$, according to 1, it is sufficient to define multiplicity

of coefficients $a_1 \ldots a_6$, $\forall a_i \in GF(2^m)$, and elements of masking matrixes. Total must be stored $l_{K+} = 5 \times n^2 \times k^2 \times m$ bits of secret key information.

Expression (1) enables to evaluate the amount of secret key data in motivated crypto-code system based on McEliece theoretical-code scheme with elliptical codes. Fig. 2 shows the dependence of the volume of key data on the dimension of $GF(q^m)$ field for a different $q = 2, 4, 16, 32$. The figure also shows the time required for exhaustive search of key data while performing of 10^{15} searches in second.

Thus, the proposed method of masking based on construction of the modified theoretical-code schemes on elliptic codes, in which use the parameters of the elliptic curve as secret data, can significantly reduce the amount of key data in compare to the classical McEliece scheme. At the same time as a potentially resistant, are considered scheme with $l_{K+} > 80$ bits. As follows from the above in Fig. 2 dependencies for building a theoretical code - scheme should be used elliptical codes with code word length$>$ 220 bits.

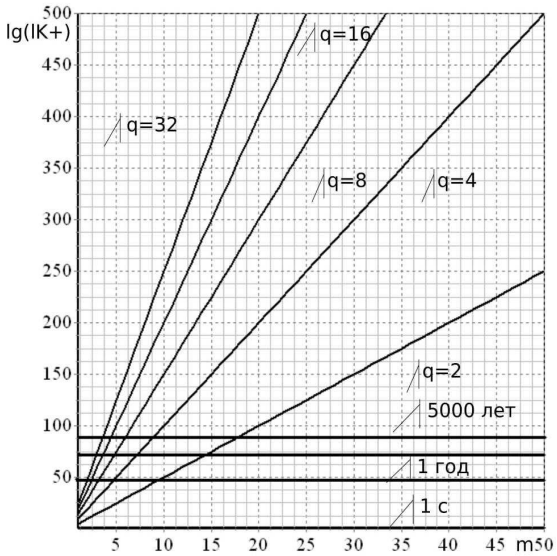

Fig. 2. The dependencies of the volume of secret key data in McEliece MACCS

The most simple and convenient method for modifying a linear block code, which stores the minimum code distance and increases the amount of data transmitted is the elongation of its length after forming initialization vector, by reducing the information symbols. Let $I = (I_1, I_2, \ldots, I_k)$ - information vector of (n, k, d) block code. Choose a subset h of the information symbols, $|h| = x$, $x \leq \frac{1}{2} k$ and form *initialization vector*.

We place an information vector I in a subset of zeros h, i.e. $I_i = 0, \forall I_i \in h$. On the other positions of the vector I put the information symbols. After in position of initialization vector add information symbols. For the modification (lengthening) elliptic codes will use reduction of the curve points multiplicity. The following statement is true.

Statement 2. Let EC - elliptic curve over $GF(q)$, $g = g(EC)$ - curve genus, $EC(GF(q))$ - multiplicity of its points over a finite field, $N = EC(GF(q))$ - their number.

Fix a subset $h_1 \subseteq h$, $|h_1| = x_1$. Let an elliptic *(n, k, d)* code over *GF(q)* built through a mapping in the form φ*:* $X \to P^{k-1}$ is given. Then the parameters of the elongate on x_1 symbols from *GF(q)* elliptic code built through mapping φ*:(*$X \cup h_1$*)* $\to P^{k-1}$, are related as follows : $k \geq \alpha - x + x_1$, $d \geq n - \alpha$, $\alpha = 3$ *. degF.*

Proof. If $x_1 < x$, then the lengthening code on x_1 is equivalent to shortening the source code on the x - x_1. Having substituted these parameters in the expression (1), we obtain the result of corollary 1.

Corollary 2. If you know the type of elliptic curve (multiplicity $a_1 \ldots a_6, \forall a_i \in GF(q)$), the subset of h and *h1* are completely determine the modified elliptical (n, k, d) codes over *GF(q)*, built through the mapping of the form:φ*:*$X \to P^{k-1}$ and φ*:(*$X \cup h_1$*)* $\to P^{k-1}$.

Proof. Multiplicity of coefficients $a_1 \ldots a_6, \forall a_i \in GF(q)$ is uniquely defined form of the elliptic curve, and, accordingly, multiplicity of its points *EC(GF(q))*. Using a mapping in the form of φ*:* $EC \to P^M$ and the results of statements 1-2, construct the elliptical (n, k, d) code over *GF(q)*. If you know the elongating symbols, then we construct the elongated codes.

According to the statement 3, it are symbols from multiplicity *h1*, which completely determine the modified elliptical *(n, k, d)* code over *GF(q)*.

Statement 3. Fix a subset $h_1 \subseteq h$, $|h_1| = x_1$. Let an elliptic (n, k, d) code over *GF(q)*, built through a mapping of the form φ*:* $X \to P^{r-1}$ is given. Then the elliptic code parameters of the elongated on x_1 characters from *GF(q)*, built by mapping of the form φ*:(*$X \cup h_1$*)* $\to P^{r-1}$, will be connected by the relations: $n = 2\sqrt{q} + q + 1 - x + x_1$, $k \geq n - \alpha$, $d \geq \alpha$, $\alpha = 3$ *. degF.*

Corollary 3. If you know the form of an elliptic curve (multiplicity $a_1 \ldots a_6$, $\forall a_i \in GF(q)$), the subset of h and *h1* completely determine the modified elliptical (n, k, d) codes over *GF(q)*, built through the mapping of the form: φ*:*$X \to P^{r-1}$ and φ*:(*$X \cup h_1$*)* $\to P^{r-1}$.

Proof. The multiplicity of coefficients $a_1 \ldots a_6$, $\forall a_i \in GF(q)$ uniquely defines form of an elliptic curve, and, accordingly, multiplicity of its points *EC(GF(q))*. Using a mapping of the form φ*:* $EC \to P^?$ and results of statements 1 - 2, construct an elliptic (n, k, d) code over *GF(q)*. If you know the lengthening symbols, then we construct the elongated codes. According to the statement 3, the symbols of the multiplicities h and *h1*, which completely determine the modified elliptical (n, k, d) code over *GF(q)*.

Results of statements 2, 3, and their corollaries allow us to construct modified (elongated) elliptical (n, k, d) codes over *GF(q)*. Define the following algorithm for constructing modified elliptic codes.

Algorithm for constructing elongated elliptic codes.

Step 1. Fix an elliptic curve over *GF(q)*. Find a lot of simple points of the curve *EC(GF(q))*: $(P_1, P_2, \ldots, P_N)$. Construct a shortened (n, k, d) code over *GF(q)* as a result of mapping φ*:* $X \to P^M$.

Step 2. Fix a subset of points of the curve h_1*(GF(q))*: $(P_{x1}, P_{x2}, \ldots, P_{xx1})$, $h_1 \subseteq h$, $|h_1| = x_1$.

Step 3. Construct a mapping φ*:* $(X \cup h_1) \to P^M$. If $M = k$, we obtain an elongated elliptical (n, k, d) code over *GF(q)* with the parameters, $n = 2\sqrt{q} + q + 1 - x + x_1$, $k \geq \alpha - x + x_1$, $d \geq n - \alpha$, $\alpha = 3$ *. degF.* (see Corollary of Statement 4). If $M = r$, we

obtain an elongated elliptical (n, k, d) code over $GF(q)$ with the following parameters: $n = 2\sqrt{q} + q + 1 - x + x_1$, $k \geq n - \alpha$, $d \geq \alpha$, $\alpha = 3 \,.\, degF$ (see Corollary of Statement 3).

Using the result of Statement 2 and its corollaries, define a theoretical-code scheme on the modified elliptic codes built by mapping of the form $\varphi: X \to P^{k-1}$ and $\varphi: (X \cup h_1) \to P^{k-1}$. The following statement is true.

Statement 4. The elongated elliptical (n, k, d) code over $GF(2^m)$, built through the mapping of the form $\varphi: (X \cup h_1) \to P^{k-1}$, determines the modified theoretic-code scheme with parameters:

- the dimension of secret key (in bits):

$$l_{K+} = (x - x_1) \cdot |\log_2 (2\sqrt{q} + q + 1)|; \tag{2}$$

- the dimension of information vector (in bits):

$$l_I = (\alpha - x + x_1) \cdot m; \tag{3}$$

- the dimension of cryptogram (in bits):

$$l_S = (2\sqrt{q} + q + 1 - x + x_1) \cdot m; \tag{4}$$

- relative transmission rate:

$$R = (\alpha - x + x_1) / (2\sqrt{q} + q + 1 - x + x_1)\,. \tag{5}$$

Proof. According to the result of Statement 1, a modified crypto-code system based on McEliece theoretical-code scheme built using the generating matrix of algebraic (n, k, d) block of code over $GF(2^m)$, has the following parameters: the size of the secret key $k \times n$ symbols from $GF(2^m)$; a vector of length k of information symbols from $GF(2^m)$; length of codegram - n symbols from $GF(2^m)$; relative transmission rate - R = k / n.

Enumerate all the points of the curve. Number of them $N \leq 2\sqrt{q} + q + 1$. Consequently, to enumerate the curve points it is necessary $|\log_2 (2\sqrt{q} + q + 1)|$ bits. If the subset power of shortening symbols is $|h| = x$, then to denote all shortening symbols is needed $x \cdot \log_2 (2\sqrt{q} + q + 1)$ bit. These symbols are held in secret and set the amount of key data - the expression (2). If the subset power of lengthening symbols is $|h_1| = x_1$, then to denote all modifications symbols is required $(x - x_1) \cdot |\log_2 (2\sqrt{q} + q + 1)|$ bit. These symbols are held in secret and set the amount of key data - the expression (2).

Using the result of Statement 3 and its corollaries, define theoretical – code scheme on the modified elliptic codes built by mapping in the form $\varphi: X \to P^{r-1}$ and $\varphi: (X \cup h_1) \to P^{r-1}$. The following statement is true

Statement 5. The elongated elliptical (n, k, d) code over $GF(2^m)$, built through the mapping of the form: $\varphi: (X \cup h_1) \to P^{r-1}$ specifies the modified theoretic - code scheme with parameters:

- the dimension of the secret key is defined by expression (2);
- the dimension of information vector (in bits):

$$l_I = (2\sqrt{q} + q + 1 - \alpha) \cdot m; \tag{6}$$

- the dimension of codegram is defined by expression (3);
- the relative transmission rate:

$$R = (2\sqrt{q} + q + 1 - \alpha) / (2\sqrt{q} + q + 1 - x + x_1). \quad (7)$$

Proof. According to the result of Statement 1, theoretical - code scheme is constructed using the check matrix of algebraic block (*n, k, d*) code over *GF(2^m)*, has the following parameters: an information vector of length *k* characters from *GF(2^m)*; codegram length - n symbols from *GF(2^m)*; relative transmission rate - $R = k / n$. Substitute the parameters of modified (shortened and elongated) elliptic (*n, k, d*) codes over *GF(q)*, built through the mapping of the form $\varphi: X \to P^{r-1}$ and $\varphi: (X \cup h_1) \to P^{r-1}$(see statement 3) obtain, accordingly, the expression (6), (7).

Thus, the results of statements 2, 3 and their corollaries allow to build a modified elongated elliptical (*n, k, d*) codes over *GF(q)*. Statements 4 and 5 allow you to specify a modified asymmetric crypto-code system on McEliece TCS on modified elliptic codes, thereby providing the required cryptographic resistance.

Consider the formal description of a modified asymmetric crypto-code system of information protection based on the use of modification methods.

4. Mathematical model and basic algorithms of information converting in the proposed McEliece system on elongated codes

Mathematical model of modified asymmetric crypto-code information protection system using algebraic block codes based on McEliece theoretic -code scheme based on elongation (information symbols increassng) is formally defined by combination of the following elements:

- multiplicity of plaintexts

$M = \{M_1, M_2, ..., M_{q^k}\}$, where $M_i = \{I_0, I_{h_{r_1}}, .. I_{h_{r_j}}, I_{k-1}\}$, $\forall I_j \in GF(q)$, h_j–information symbols equal to zero, $|h| = \frac{1}{2}k$, i.e. $I_i = 0, \forall I_i \in h$; h_r–information symbols of lengthening *k*, $|h| = \frac{1}{2}k$;

- multiplicity of closed texts *(codegrams)*

$C = \{C_1, C_2, ..., C_{q^k}\}$, where $C_i = (c^*_{X_0}, c^*_{h_{r_1}}, ..., c^*_{h_{r_j}}, c^*_{X_{n-1}})$, $\forall c^*_{X_j} \in GF(q)$;

- multiplicity of straight mappings (based on the use of generating matrix public key)

$\varphi = \{\varphi_1, \varphi_2, ..., \varphi_s\}$, where $\varphi_i : M \to C_{h_r}$, $i = 1, 2, ..., s$;

- multiplicity of reverse mappings (based on the use of masking matrix private key)

$\varphi^{-1} = \{\varphi_1^{-1}, \varphi_2^{-1}, ..., \varphi_s^{-1}\}$, where $\varphi_i^{-1} : C_{h_r} \to M$, $i = 1, 2, ..., s$;

- multiplicity of keys, parametrizing straight mapping (the public key of an authorized user)

$$K_{a_1} = \{K_{1_{a_1}}, K_{2_{a_1}}, ..., K_{1_{s_1}}\} = \{G_X{}^{EC_1}_{a_1}, G_X{}^{EC_2}_{a_1}, ..., G_X{}^{EC_s}_{a_1}\},$$

where $G_X{}^{EC_i}_{a_1}$-generating $n \times k$ matrix masked as a random albebra-geometric block (n, k, d) code with elrments from $GF(q)$, i.e. $\varphi_i : M \xrightarrow{K_{ia_1}} C_{h_r}, i = 1, 2, ..., s$.

a_i – multiplicity of coefficients of the polynomial curve $a_1 \ldots\ a_6$, $\forall a_i \in GF(q)$, uniquely defining a specific set of curve points from the space P^2.

- multiplicity of keys, parameterizing reverse mappings (personal (private) key of authorized user)

$$K^* = \{K_1^*, K_2^*, ..., K_s^*\} = \{\{X, P, D\}_1, \{X, P, D\}_2, ..., \{X, P, D\}_s\},$$

$$\{X, P, D\}_i = \{X^i, P^i, D^i\},$$

where X^i – masking nondegenerate randomly equiprobably formed by source of keys matrix $k \times k$ with elements from $GF(q)$; P^i – permutational randomly equiprobably formed by source of keys matrix $n \times n$ with elements from $GF(q)$; D^i – diagonal formed by source of keys matrix $n \times n$ with elements from $GF(q)$, i.e.

$$\varphi_i^{-1} : C \xrightarrow{K_i^*} M, i = 1, 2, ..., s.$$

Complexity of performing reverse mapping φ_i^{-1} without knowledge a key $K_i^* \in K^*$ associated with solution of theoretic complexity problems in random code decoding (generic position code).

Initial data in the description of the considered asymmetric crypto-code information protection systems are the parameters described in the previous model.

In asymmetric crypto-code system based on McEliece TCS modified (elongated) algebrogeometric *(n, k, d)* code C_{h_r} with rapid decoding algorithm is masking random *(n, k, d)* code $C_{h_r}{}^*$ by multiplying generating matrix G^{EC} of C_{k-h_j} code on the secret masking matrices X^u, P^u and D^u, what provide formation of open key for authorized user:

$$G_X^{ECu} = X^u \cdot G^{EC} \cdot P^u \cdot D^u, u \in \{1, 2, ..., s\},$$

where G^{EC} – generating $n \times k$ matrix of algebrogeometric (n, k, d) code with elements from $GF(q)$, built on the basis of using the polynomial curve coefficients $a_1 \ldots\ a_6$, $\forall a_i \in GF(q)$, chose by user, uniquely defining a specific set of curve points from the space P^2.

Forming secret text $C_j \in C_{h_r}$ by the entered plaintext $M_i \in M$ and given public key $G_{X\,a_1}^{ECu}$, $u \in \{1, 2, ..., s\}$ is performed by forming of shortened code word and then elongation of masked code with adding to its randomly formed vector $e = (e_0, e_1, ..., e_{n-1})$:

$$C_j = \varphi_u\left(M_i, G_X^u\right) = M_i \cdot \left(G_X^u\right)^T + e.$$

For each formed secret text $C_j \in C_{h_r}$ the appropriate vector $e = (e_0, e_1, ..., e_{n-1})$ acts as a single session key, i.e. for specific E_j, vector e is formed randomly, equiprobably and independently of the other secret texts.

The channel receives $C_j^* = C_j - C_{k-h_j} + C_{h_r}$.

On the receiving side, an authorized user who knows the rule of masking, the number and location of zero information symbols can take advantage of a fast decoding algorithm of algebrogeometric code (with polynomial complexity) to recover the plaintext:

$$M_i = \varphi_u^{-1}\left(C_j^*, \{X, P, D\}_u\right).$$

To recover the plaintext an authorized user replaces lengthening symbols on non-zero information symbols

$$C_j^* = C_{h_r} \to C_{k-h_j},$$

from recovered secret text C_j reduces the effect of the secret of permutational and diagonal matrices P^u and D^u:

$$\begin{aligned} C &= C_j^* \cdot (D^u)^{-1} \cdot (P^u)^{-1} = \left(M_i \cdot (G_X^u)^T + e\right) \cdot (D^u)^{-1} \cdot (P^u)^{-1} = \\ &= \left(M_i \cdot (X^u \cdot G \cdot P^u \cdot D^u)^T + e\right) \cdot (D^u)^{-1} \cdot (P^u)^{-1} = \\ &= M_i \cdot (X^u)^T \cdot (G)^T \cdot (P^u)^T \cdot (D^u)^T \cdot (D^u)^{-1} \cdot (P^u)^{-1} + e \cdot (D^u)^{-1} \cdot (P^u)^{-1} = \\ &= M_i \cdot (X^u)^T \cdot (G)^T + e \cdot (D^u)^{-1} \cdot (P^u)^{-1}, \end{aligned}$$

decodes received vector with Berlekamp-Massey algorithm [10 – 14]:

$$C = M_i \cdot (X^u)^T \cdot \left(G^{EC}\right)^T + e \cdot (D^u)^{-1} \cdot (P^u)^{-1},$$

i.e. get rid of the second term and from the multiplier $\left(G^{EC}\right)^T$ in the first term at right side of equation, and then reduces the effect of masking matrix X^u.

Received result of decoding M_i^* is need to be multiplied by $(X^u)^{-1}$:

$$M_i^* \cdot (X^u)^{-1} = M_i.$$

Received solution is plaintext M_i, to which are added lengthening symbols: $M_j = M_i + h_r$ – the essence of sent message.

Consider the practical algorithms of codegram forming and decoding, and a block diagram of communication protocol in a real time at developed McEliece ACCS.

The algorithm of codegram formation in modified McEliece asymmetric crypto-code system with shortened modified code define by sequence of the following steps:

Step 1. Fix a definite field *GF(q)*. Fix an elliptic curve $y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz + a_6z^3$ and set of it points $EC(GF(q)):(P_1, P_2, \ldots, P_N)$ over *GF(q)*. Fix subset of points $h(GF(q))$: $(P_{x1}, P_{x2}, \ldots, P_{xx})$, $h \subseteq EC(GF(q))$, $|h|=x$ and keep it in secret.

Step 2. Form initialization vector $IV=EC–h_j$, h_j–information symbols equal to zero, $|h| = \frac{1}{2}k$, i.e. $I_i = 0, \forall\ I_i \in h$;

Step 3. By entering information vector I form the code word c. If *(n, k, d)* code over *GF(q)* is given by its generating matrix in such case $c = IG$.

Step 4. Form the random vector of error e such, as $w(e) \le t$, $t = \lfloor (d-1)/2 \rfloor$. Add formed vector to code word, receive the code word: $c^*=c+e$.

Step 5. Form the codegram by initialization vector symbols deleting (shortening): $c_X^* = c^* - IV$.

Fig. 3 shows algorithm of encoding in McEliece MACCS.

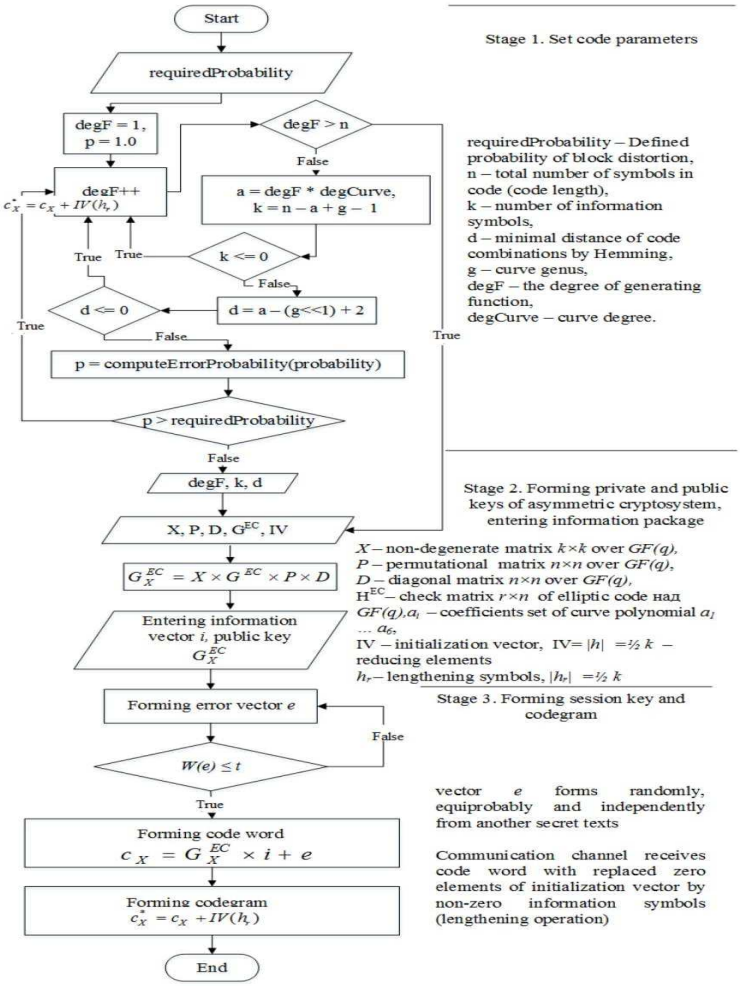

Fig. 3. Algorithm of codegram formation in McEliece MACCS

Algorithm of codegram decoding in modified theoretical-code schemas on elliptic codes define by sequence of the following steps:

Step 1. Entering codegram to be decoding. Entering the private key - generating and / or the elliptic code check matrix.

Step 2. Codegram - a code word with elliptic code errors. Error vector weight $w(e) \leq t$. Decoding codegram – find error vector.

Step 3. Form needed information vector.

Step 4. Add to information vector symbols of information packages from initialization vector position.

Offered decoding algorithm on McEliece MACCS is shown on fig.4.

$c_X^* = c^* + IV\,(h_r)$.

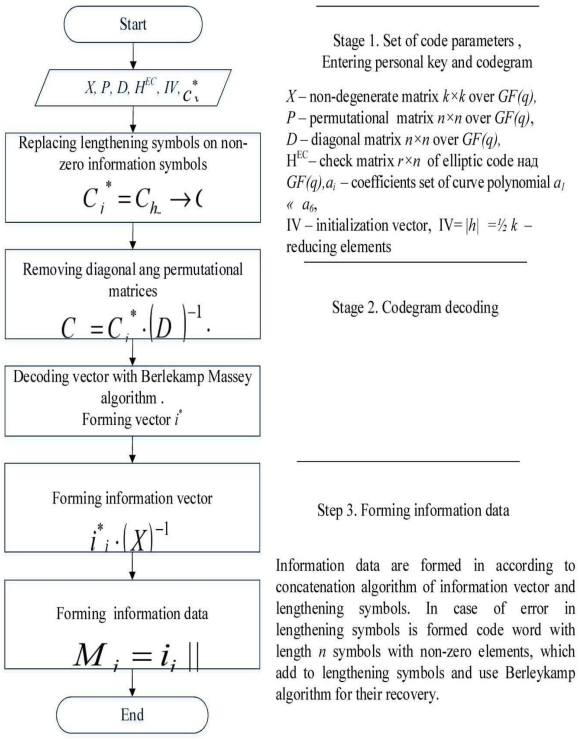

Fig. 4. Algorithm of codegram decoding in McEliece MACCS

Block diagram of information exchange protocol in a real time mode with the use of asymmetric cryptosystems based on a modified McEliece TCS with modified (elongated) elliptical codes is shown in Fig. 5.

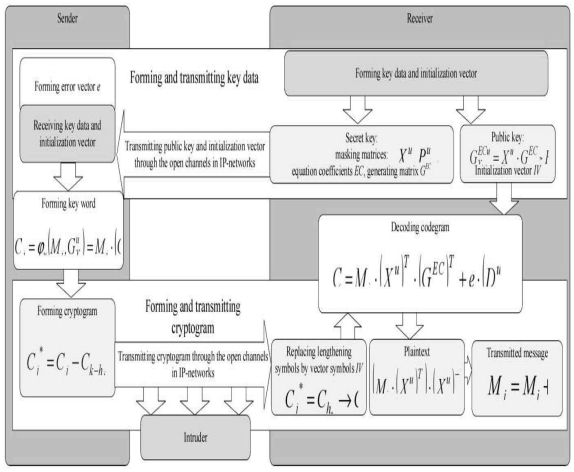

Fig. 5. Protocol of information exchange in a real time mode with use of modified McEliece TCS with elongated EC

5. Evaluation of energy costs for program implementation and the complexity of the proposed McEliece MACCS code transformation

To estimate time and speed parameters is common to use the unit of measurement *cpb* where cpb (*cycles per byte*) - the number of processor cycles, which should be spent to process 1 byte of incoming information. Algorithm complexity calculates from expression:

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

where Utl– utilization of the CPU core (%);

$Rate$ – algorithm bandwidth (bytes/sec).

In table. 1 are shown dependency research results of code length sequence of algebro-geometric code in McEliece and Niederraiter TCS from number of processor cycles due to executing elementary operations in program realization of crypto-code systems.

Table 1

Research results according to the length of the code sequence in McEliece ACCS in dependency of CPU cycles number

Code sequence length		McEliece on elongated codes			McEliece		
		10	100	1000	10	100	1000
The number of function calls realizing elementary operations	Symbol reading	11 432 131	33 460 317	82 473 442	11 018 042	30 800 328	80 859 933
	String comparing	3 673 756	12 119 867	29 469 389	3 663 356	10 199 898	26 364 634
	String concatenation	1 947 681	6 114 478	14 456 729	1 834 983	5 125 564	13 415 329
Sum		17 053 568	51 694 662	126 399 560	16 516 381	46 125 790	120 639 896
Duration of executing functions in processor cycles*	Symbol reading	300 479	843 705	2 745 148	297 487	831 609	2 183 218
	String comparing	213 478	561 754	1 739 170	197 821	550 794	1 423 690
	String concatenation	578 174	1 647 638	4 007 883	544 990	1 522 293	3 984 353
Sum		109 157	1 092 131	3 053 097	1 040 298	2 904 696	7 591 261
Executing duration** in msec		0,56	1,55	4,1	0,55	1,53	4

Note:

** duration of 1000 operations in processor cycles: symbol reading – 27 cycles, string comparing – 54 cycles, string concatenation – 297 cycles;*

*** for calculating is taken processor with a clock speed 2 GHz taking into account operating system loading 5 %*

Table 2 shows the investigation results for evaluating time and speed parameters of procedures of forming and decoding information in the non-symmetric crypto-code systems based on McEliece ACCS and MCCS.

Table 2

Investigation results for evaluating time and speed parameters of procedures of forming and decoding information

Crypto-code systems	Code sequence length	Algorithm bandwidth, Rate (bytes / sec)	CPU utilization (%)	Algorithm complexity, Per (cpb)
McEliece ACCS	100	46 125 790	56	61,5
	1000	120 639 896	56	62,0
McEliece MCCS	100	51 694 662	56	61,7
	1000	126 399 560	56	62,2

Analysis of table 1.2 shows that the use of modified (elongated) elliptic codes allows to save the volume of transmitted in McEliece a crypto-code system data, but at the same time provide the required level of cryptographic resistance during the implementation over smaller field $GF(2^6 - 2^8)$ through the use of entropy of initialization vector h_r.

Research information reliability and secrecy, which can be provided by modified crypto-code systems on elliptic curves. Fix $(n,\ k,\ d)$ elliptic code over $GF(q)$. Define modified crypto-code scheme on the basis of McEliece TCS on modified (elongated) codes. Define the session key e – error vector, which adds to code word during codegram formation. Let $w(e) \le t$, $t = \lfloor (d-1)/2 \rfloor$. Denote share of error vector weight e by symbol $\rho = w(e) \ / \ t$. Then potential resistance of theoretical-code scheme with elliptic codes, will be determined by $\rho \times t$, interference resistance of transmitted codegrams by $(1 - \rho) \times t$. The complexity of hacking the proposed modified system define by the expression of the random code decoding analysis complexity with commutation decoder:

$$I_{K+} = N_{nokp} nr, \text{where } N_{nokp} \ge \frac{C_n^t}{C_{n-k}^t} = \frac{n\,(n-1)\,...\,(n-t-1)}{(n-k)\,(n-k-1)\,...\,(n-k-t-1)}$$

Interference resistance is defined by minimal ratio signal/noise, needed for providing the required reliability. Fix the ratio signal/noise and modulation type. Suppose that digital message transmission is carried out through discrete channel without memory, i.e. errors in sequently transmitted code symbols happen independently with probability P_o. Then the probability of the error multiplicity i on the block length is equal [10 – 14]:

$$P_i = C_n^i P_o^i \,(1 - P_o)^{n-i}\,.$$

If the decoding procedure allows correcting $t = \lfloor (d-1)/2 \rfloor$ errors, the probability of an incorrect decoding is:

$$P_{ou} = \sum_{i=t+1}^{n} P_i = \sum_{i=t+1}^{n} C_n^i P_o^i \,(1 - P_o)^{n-i}\,.$$

At the integrated solution of problems of reliability and information secrecy of data transmitting, modified crypto-code system will be correct $(1 - \rho) \times t$ happened errors, hence:

$$P_{ou} = \sum_{i=(1-\rho)t+1}^{n} P_i = \sum_{i=(1-\rho)t+1}^{n} C_n^i P_o^i (1 - P_o)^{n-i}.$$

Fix $GF(2^{10})$ and $P_o = 10^{-3}$.

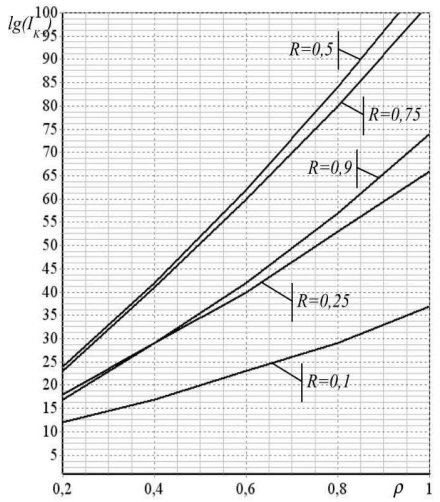

Fig. 6. Dependency of hacking complexity $I_{K+}(\rho)$ over $GF(2^{10})$

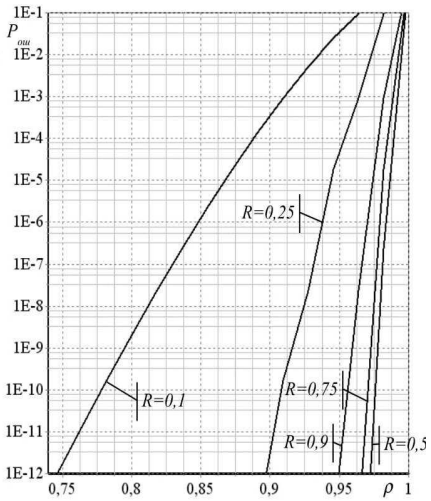

Fig. 7. Dependency of error decoding probability $P_{ou}(\rho)$ over $GF(2^{10})$

Fig. 6 shows dependencies of theoretical-code scheme hacking complexity with permutational decoder $I_{K+}(\rho)$ while use of elliptic codes with relative speed R. Fig. 7 shows dependencies of error decoding probability $P_{ou}(\rho)$ with an integrated solution of problems of reliability and information secrecy.

As it is seen from the dependences shown in Fig. 6, 7, modified crypto-code system based on McEliece TCS have high indexes of reliability and information secrecy. Increasing index ρ leads on the one hand to increasing of circuit resistance and on the other side reduce its noise resistance. Research integrated increasing of reliability and information secrecy of data transmission with use of offered systems.

Fig. 8 summarizes dependencies of error decoding probabilities and complexity of hacking theoretical-code scheme with elliptic codes under different R and $\rho = 0,9$.

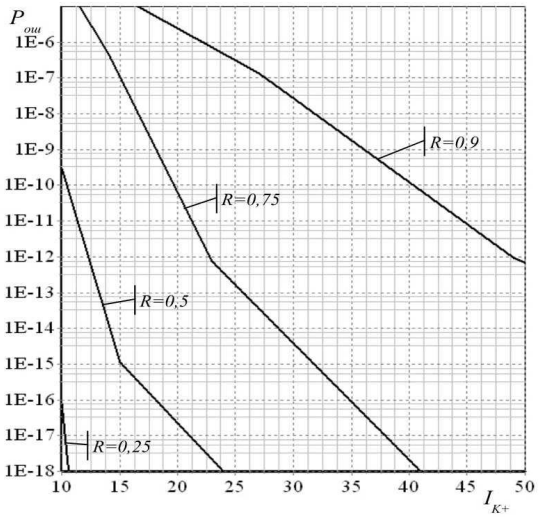

Fig. 8. Summarized dependencies of error decoding probability and hacking complexity $P_{ош}(I_{K+})$ for $\rho = 0,9$

As it is seen from the dependences shown in Fig. 8 proposed modified crypto-code systems based on McEliece TCS provide high resistance and reliability indicators of the processed and transmitted information. Their use will enable use open channels of IP-networks for transmitting confidential (commercial) information in the real-time mode thus providing required indexes of reliability and safety.

6. Conclusions

In a result of conducted researches:

1. Analyzed overall structure of the asymmetrical crypto-code systems construction based on McEliece TCS enabling to provide integrated (with single device) the required indicators for reliability, efficiency and data security. A major shortcoming of ACCS based on McEliece TCS is big volume of key data, that constricts their use in different communication system areas (today cryptographic resistance on the level of provable resistance model is provided while building ACCS in Galua field $GF(2^{13})$). Using modified elongated elliptic codes allows reducing the volume of key data while keeping the cryptographic resistance requirements and transmission of big volume of information.

2. Offered mathematical model, practical algorithms of codegram encoding/decoding in developed McEliece MACCS enable to implement high-speed information processing at the real-time mode. The complexity of codegram formation and decoding is defined by encoding/decoding complexity of modified (elongated) elliptic codes and a polynomially depends on the code length and it correcting dependence.

3. Transferring the key sequence using a modified McEliece ACCS based on the shortened codes allows using open communication channels of communication systems and significantly reducing the volume of the key sequences that are stored by users of the

system. Evaluation software implementation complexity of information protection crypto-code means based on McEliece TCS confirms the assumption if reducing the computing costs to calculate cryptogram/codegram, necessity to store key data (public key) by authorized user.

Performed researches of error vector ρ usage enable on the basis of the main indexes of telecommunication system channels to enhance one of the integrated mechanisms indicator – reliability or safety.

References

[1] S.Q. Semenov, *Models and methods of managing network resources in information and telecommunication systems* , monograph / S.G. Semenov, A.A. Smirnov, E.V. Meleshko - Kharkov: NTU "KhPI", 2011, 212 p.

[2] Kh.N. Rzaev, *Analysis of the state and ways of improving the safety protocols of modern telecommunication networks*, monograph / under. Ed. V.S. Ponomarenko. / Kh. N. Rzaev, O.G. Korol // Information technologies in management, education, science and industry: monograph / - H.: Publisher Rozhko SG 2016. - P. 217 - 234

[3] Telecommunication services in the world economy [Electronic resource]: Access mode: http://www.gumer.info/bibliotek_Buks/Econom/world_econom/30.php

[4] Transmission of Picturesque content with Code Base Cryptosystem [Electronic resource]: - Access mode: https://doaj.org/article/6714b60516cc4aa79e56d0c421febaf3

[5] Steganography application program using the ID3v2 in the MP3 audio file on mobile phone [Electronic resource]: - Access mode: https://doaj.org/article/707a6506be9e49698fd75323fcc1302c

[6] Space-Age Approach To Transmit Medical Image With Codebase Cryptosystem Over Noisy Channel [Electronic resource]: - Access mode: https://doaj.org/article/5c7da3a1e3ec4f83b552199034bd3241

[7] An Authenticated Transmission of Medical Image with Codebase Cryptosystem over Noisy Channel [Electronic resource]: - Access mode: https://doaj.org/article/39a3ac65d5b24b348f069dfc82eb6248

[8] Kh.N. Rzayev, *Analysis of the software implementation of the non-binary equilibrium coding method*, Kh. N. Rzaev, A.S. Tsyganenko // Azerbaijan Technical University, Scientific Works Volume1, 1, 2016, 1, p.107- 112, ISNN 1815-1779. - P. 107-113.

[9] On the Usage of Chained Codes in Cryptography [Electronic resource]: - Access mode: https://doaj.org/article/c0f40bdb1f6149f4ac107d44a95c9531

[10] R. Bleikhut, *Theory and practice of codes that control errors*, Per. with English. - M.: The World, 1986, 576 p.

[11] J. Clark, *Coding with error correction in digital communication systems*, trans. with English. / Ed. B. S. Tsybakova. M.: Radio and Communication, 1987, 392 p.

[12] F.J. McWilliams, *Theory of Error Correcting Codes*, FJ McWilliams, N. JA A. Sloan-M.: Communications, 1979, 744 p.

[13] V.M. Muter, *Fundamentals of noise-immune telecasting of information*, VM Muter-L.: Energoatomizdat. Leningr. Otd-tion, 1990, 288 p.

[14] Theory of coding, Per. with japan. / T. Kasami, N. Tokura, E. Iwadari, J. Inagaki / ed. B. S. Tsybakov and S. I. Gelfand. - M.: The World, 1978, 576 p.

[15] S.P. Evseev, *An investigation of asymmetric and symmetriction theoretic coding schemes with elliptical codes*, Naukov prats of NAU. Series: Electronics that system management - Kiev: the NAU. - 2006 - Vip, **2(8)**, 9-16.

[16] A.A. Bolotov, *Algorithmic foundations of elliptical cryptography*, Moscow: MEI, 2000, 100 p.

Khazail Rzayev
Azerbaijan State University of Oil and Industry, Azadlyg av., 20, AZ10109, Baku, Azerbaijan
E-mail:xazail49@mail.ru

Received 22 March 2017
Accepted 15 September 2017