UDC 681.3.06 **doi: 10.20998/2522-9052.2018.4.06**

O. Tsyhanenko[1], Kh. Rzayev[2], T. Mammadova[2]

[1]Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine
[2] Azerbaijan State University of Oil and Industry, Baku, Azerbaijan

MATHEMATICAL MODEL OF THE MODIFIED NIEDERREITER CRYPTO-CODE STRUCTURES

Subject of research is the modification of the Niederreiter crypto-code construction on non-binary codes. **The purpose** of this work is to develop a mathematical model of a modified Niederreiter crypto-code structure using algebrogeometric block codes with a shortening of the information parcel. **The tasks to be solved are:** to formalize the procedures for the formation of codograms and their further decoding; develop a mathematical model of the Niederreiter crypto-code structure modified by shortening the information parcel and fixing the admissible positional vectors of the plaintext transformation based on equilibrium coding. The following **results** were obtained. Studies of the Niederreiter crypto-code structures in MES revealed the main reason for the impossibility of the practical implementation of decoding algorithms when using non-binary codes in the classical scheme. It has been established that it is necessary to fix a subset of plaintext for which the error localization procedure, with the X, P and D (private key) masking matrices selected by the sender, cannot be performed. With its help, we need to “weed out” the error vector sets that do not allow using the classical version of decoding information on the receiving side when using the classical Niederreiter scheme on m-th codes. When constructing a mathematical model, the identified feature was considered. As a result, a mathematical model of the Niederreiter crypto-code structure modified by shortening the information package and fixing admissible positional vectors of the plaintext transformation based on equilibrium coding is obtained. **Conclusion.** The scientific novelty of the obtained results is as follows: the proposed modified mathematical model of the Niederreiter crypto-code structure ensures its practical implementation. Reducing the field power when building a classic Niederreiter scheme reduces the amount of data transferred by shortening the error vector before generating the syndrome on the sender side and, accordingly, the energy costs of its implementation; The use of the quantum-stable and promising Niederreiter crypto-code construction has been further developed, the identified feature and the proposed modification ensure its competitiveness.

Keywords: modified Niederreiter crypto-code structure; modified shortened elliptic-curve codes; equilibrium coding; information secrecy.

Introduction

Modern requirements for ensuring the quality of service for users of global computer networks put forward new challenges for the integrated solution of the main criteria for the quality of service - reliability and security of service. Integrated mechanisms to ensure increased requirements are unsymmetrical crypto-code information security tools based on McEliece and Niederreiter theoretic code schemes (TKS), built on non-binary error-tolerant codes and allowing operation in various data exchange modes [1 - 5]. The asymmetric cryptosystems proposed in [1, 2] provide the required performance indicators, cryptographic strength and reliability of the transmitted data, and most importantly, the use of a single software / hardware (hardware) mechanism in ensuring the required performance of the main criteria for quality of service.

At the same time, the analysis of the software implementation of an asymmetric crypto-code system on the Niederreiter TCS carried out in [4, 5] showed significant implementation difficulties, which makes it difficult to use code-theoretic schemes to build crypto-resistant asymmetric systems. Development of modified crypto-code systems using modified algebrogeometric codes is a promising direction in solving this technical problem.

During a pilot study of Niederreiter’s CCS on the MES, it was determined that the use of non-binary codes with the Niederreiter's classical ACCS requires modifications, namely, fixing a subset of open texts for which the error localization procedure, with selected X, P and D, cannot be performed. The aim of the article is to develop a formal mathematical description of modified crypto-code information security tools based on the Niederreiter TCS using algebrageometric block codes based on the shortening of information symbols and fixing a subset of open texts, allowing for a reduction in the volume of key data while maintaining the level of crypto resistance, crypto resistance and energy costs on their implementation.

The potential strength of theoretical-code schemes is determined by the complexity of decoding a random (n, k, d) block code. Consequently, to build potentially persistent theoretical code schemes, it is necessary to use modification methods that do not allow the minimum code distance to be reduced. By masking the code with a fast decoding algorithm (of polynomial complexity) under an arbitrary (random) block code, one can present the decoding task for an adversary as a computationally complex problem (exponential complexity). For an authorized user of the system (having a secret key) decoding is a polynomially solvable problem. In the work of Sidelnikov [1], an effective method was proposed for breaking into asymmetric McEliece and Niederreiter schemes built on generalized Reed-Solomon codes. It is noted that one of the promising directions in the development of potentially stable theoretical code schemes are schemes constructed using algebraic geometry codes. Algebraic block codes constructed from algebraic curves (algebraic codes) have good asymptotic characteristics. Their use in discrete symmetric channels allows you to get the greatest energy gain from coding (among algebraic block codes) and effectively deal with the resulting error packets. Ways to shorten linear block codes, without changing the minimum distance, allow you to build hack-resistant asymmetric crypto-code systems with a smaller volume of cryptograms and key data. In accordance with the formal mathematical description of asymmetric crypto-code systems based on the Niederreiter TCS in the direct error correction mode and automatic questioning proposed in [2], mathematical models of modified asymmetric cryptosystems based on the Niederreiter TCS are proposed that reduce the energy costs of their implementation.

Research results

Mathematical model of a modified asymmetric crypto-code system of information protection using algebra-geometric block codes based on Niederreiter's code-theoretic scheme based on shortening (shortening of information symbols). Formally given by the combination of the following elements [2]:

– set of open texts $M_i = \left\{ M_1, M_2, ..., M_{q^k} \right\},$,

where $M_i = \left\{ e_0, e_{h_1}, ...e_{h_k}, e_{e-1} \right\}$, $\forall e_e \in GF(q)$, h_e – error vector symbols are zero, $|h| = e/2$, or e_i*=0,* $\forall e_i \in h$;

– the set of fixed open texts then the set of usable open texts $M = M_C - M_F$;

– set of closed texts $S = \left\{ S_0, S_1, ...S_{q^r} \right\}$, where $S_i = \left\{ S^*_{X_0}, S^*_{h_1}, ...S^*_{h_j}, S^*_{X_r} \right\}$, $\forall S_{X_r} \in GF(q)$;

– a set of direct reflections (based on the use of a public key - an elliptic-curve code check matrix (*EC*): $\varphi = \{ \varphi_1, \varphi_2, ..., \varphi_r \}$, where a set of back reflections (based on the use of a private (private) key - masking matrices), $\varphi^{-1} = \left\{ \varphi_1^{-1}, \varphi_2^{-1}, ..., \varphi_r^{-1} \right\}$, where $\varphi_i^{-1} : S_{r-h_e} \to M, i = 1, 2, ..., e$.

– the set of keys that parameterize direct mappings (public key of an authorized user):

$$KU_{a_i} = \left\{ KU_{1_{a_i}}, KU_{2_{a_i}}, ..., KU_{r_{a_i}} \right\} = \\ = \left\{ H^{EC_1}_{X_{a_i}}, H^{EC2}_{X_{a_i}}, ..., H^{ECr}_{X_{a_i}} \right\},$$

where $H^{EC_i}_{X_{a_i}}$ – check r×n matrix disguised as a random algebrogeometric block code (n, k, d) with elements $GF(q)$, i.e

$$\varphi_i : M \xrightarrow{KU_{i_{a_i}}} {S^*}_{r-h_e},$$

$i = 1, 2, ..., e,$, a_i – set of coefficients of a polynomial curve $a_1 ... a_6$, $\forall a_i \in GF(q)$, uniquely defines a specific set of curve points from space P^2;

– a set of keys that parameterize reverse mappings (personal (private) key of an authorized user):

$$KR = \{ KR_1, KR_2, ..., KR_r \} = \\ \left\{ \{X, P, D\}_1, \{X, P, D\}_2, ..., \{X, P, D\}_r \right\},$$

$\{X, P, D\}_i = \left\{ X^i, P^i, D^i \right\}$, where X^i – masking nondegenerate randomly equiprobably formed by key source $k \times k$ matrix with elements from GF(q); P – permutable randomly equally formed key source $n \times n$ matrix with elements from GF(q); D – a diagonal matrix formed with a key source with elements from GF(q) i.e

$$\varphi_i^{-1} : {S^*}_{r-h_e} \xrightarrow{KR_i} M, \; i = 1, 2, ..., s.$$

The complexity of performing reverse mapping φ_i^{-1} without knowing the key $K_i^* \in K^*$ connected with the solution of the theoretical complex problem of decoding a random code (code of general position). The initial data when describing the considered asymmetric crypto-code information security system are:

– nonbinary equilibrium code over *GF(q)*, i.e., multiple sequences of length n and weight $w(\varepsilon_i)$;

– algebrogeometric block (*n, k, d*) code *C* over *GF(q)*, that is, so many code words $C_i \in C$, when equality holds $C_i H^T = 0$, where *H* – algebraic block code check matrix;

– *IV* – initialization vector, *IV*= |*h*| =½ where – reduction elements (*h*$_e$ – error vector symbols are zero, */h/=1/2e*, i.e e_i *= 0,* $\forall e_i \in h$);

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

– *r* –parameter $r \in_R Z_{q^m}$, $Z_{q^m} = \left\{ 0, 1, ...2^n - 1 \right\}$,

– *n* – some parameter $n \in_R Z_{q^n}, Z_{q^n} = \left\{ 1, ...2^n \right\}$;

Let $M_C = \left\{ M_1, M_{2,} ...M_{q^k} \right\}$, set of all open texts (*n, k, d*) of block code. Define a subset of committed open texts $M_F = \left\{ M_1, M_{2,} ...M_n \right\}$, where

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

When coding, the elements of the set of fixed open texts do not participate, the set of suitable open texts will be $M = M_C - M_F$.

Based on the equilibrium coding, the closed text is formed by the entered plaintext $M_i \in M$ with a given key H_X^{ECu}, $u \in \{1, 2, ..., s\}$.

This is done by forming a syndromic (in terms of noise-resistant coding) sequence, which corresponds to an equilibrium sequence:

$$M_i = e = \{ e_0, e_1, ..., e_{n\text{-}1} \},$$

$$S_{X_j} = \phi_u\left(M_i, H_X^{ECu}\right) = M_i \times \left(H_X^{ECu}\right)^T,$$

moreover, the Hamming weight (the number of nonzero elements) of the vector is not greater than the corrective power of used algebraic block (n,k,d) code:

$$\forall i : 0 \le w(M_i) \le t = \lfloor (d-1)/2 \rfloor .$$

The power of sets M and C is determined by the allowable range of weights that is, in the general case (for all valid values $w(M_i)$) we have:

$$m = \sum_{i=0}^{t} (q-1)^i \times C_n^i,$$

where C_n^i – binomial coefficient, $C_n^i = \frac{n!}{i!\cdot(n-1)!}$.

The most appropriate value $w(M_i)$ choose according to the required value of the security of information transfer. Then for $w(M_i) = const = w(e)$ we have: $m = (q-1)^{w(e)} \times C_n^{w(e)}$, and the sequence $M_i = \{e_0, e_1, ..., e_{n-1}\}$ from the set $M = \{M_1, M_2, ..., M_m\}$ formed as a result of some mapping ψ, implemented by redundant coding by non-binary equilibrium codes of non-redundant information sequences.

Formed closed text $C_j \in C$ uniquely corresponds to the vector $M_i = \{e_0, e_1, ..., e_{n\text{-}1}\}$.

Form the initialization vector *IV=EC–h*$_j$, where h_j – information symbols are zero, $|h| = k/2$, i.e, $I_i = 0,\ \forall I_i \in h$.

Formation of a shortened error vector e_x*=e(A) – IV.*

The public key is generated by multiplying the check matrix of the algebraic code by the masking matrix:

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

where H_X^{ECu} – check $n \times (n-k)$ matrix of algebrogeometric block code (n,k,d) with elements from $GF(q)$. Syndrome sequence enters the communication channel:

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

On the receiving side, an authorized user who knows the masking (matrix set $\{X,P,D\}_u = \{X^u, P^u, D^u\}$) and the initialization vectors (the number and places of the zero symbols of the error vector) form a code sequence as one (any) of the possible solutions to the equation: $S^*_{r-h_e} = c^*_{X_i} \cdot H^T_{X_j}$,

that is, finds such a vector $c^*_{X_i}$, which decomposes into an amount: $c^*_{X_i} = c_{X_i} + M_i$, where c_{X_i} – one (any) of the possible code words of a masked code with a check matrix $H^T_{X_j}$, i.e $c_{X_i} \times H^T_{X_j} = 0$.

Then an authorized user using the matrix set $\{X,P,D\}_u = \{X^u, P^u, D^u\}$, form a vector: $\bar{c}^* = c^*_X \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1}$, that is, unmasks the code sequence $c^*_{X_i}$. After the substitution we get the equality:

$$\bar{c}^* = c^*_X \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1} = \left(c_{X_i} + M_i\right) \cdot \left(D^u\right)^{-1} \times$$
$$\times \left(P^u\right)^{-1} = c_{X_i} \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1} + M_i \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1}.$$

The authorized user who formed the vector has the ability to apply a fast (polynomial complexity) noise-resistant decoding algorithm and thus form a vector $\bar{c}^* = c^*_X \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1}$ and vector

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

To restore the information equilibrium sequence M_i enough to multiply the vector again M_i^u and the masking matrix D^u and P^u, but in a different order:

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

Forming the desired error vector e: $M = M_i + IV$

When deciphering a cryptogram (after receiving the error vector, before using the equilibrium coding algorithm), “zero” shortening symbols are introduced based on the initialization vector for information.

Evaluation of energy costs for software implementation and the complexity of code transformations in the proposed MACCS of Niederreiter. For the evaluation of time and speed indicators it is customary to use the unit cpb, where cpb (cycles per byte) – the number of processor cycles that must be spent to process 1 byte of incoming information. The complexity of the algorithm is calculated by the expression

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

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

In tablt 1 shows the results of studies of the dependence of the length of the code sequence of an algebraic code in the Niederreiter crypto-code system on the number of processor cycles to perform elementary operations in the software implementation of the crypto-code systems.

Analysis table 1, 2 shows that the use of modified (shortened) elliptic codes allows you to save the volume of transmitted data in the Niederreiter asymmetric crypto-code system, but at the same time to ensure the required level of cryptographic resistance when implemented over a smaller field *GF(*2^6 *–* 2^8*)* due to the use of the entropy of the initialization vector h_r.

Table 1. **The results of studies of the dependence of the length of the code sequence in the ACCS Niederreiter on the number of processor cycles**

The length of the code sequence		Niedereiter			Niedereiter on shortened codes			Niedereiter with fixed vectors		
		10	100	1000	10	100	1000	10	100	1000
Number of function calls implementing elementary operations	Character reading	11 018 042	30 800 328	80 859 933	10 294 397	28 750 457	76 759 874	11 431 2131	33 460 317	82 473 442
	String comparison	3 663 356	10 199 898	26 364 634	3 406 921	9 246 748	25 478 498	3 673 756	12 119 867	29 469 389
	String concatenation	1 834 983	5 125 564	13 415 329	1 705 544	5 045 748	12 379 422	1 947 681	6 114 478	14 456 729
Sum		16 516 381	46 125 790	120 639 896	15 406 862	43 042 953	114 617 794	17 053 568	51 694 662	12 639 9 560
The duration of the functions* in processor cycles	Character reading	297 487	831 609	2 183 218	295 374	810 478	2 001 167	300 479	843 705	2 745 148
	String comparison	197 821	550 794	1 423 690	178 814	531 379	1 248 684	213 478	561 754	1 739 170
	String concatenation	544 990	1 522 293	3 984 353	544 990	1 328 114	3 586 486	578 174	1 647 638	4 007 883
Sum		1 040 298	2 904 696	7 591 261	1 006 781	2 749 548	7 247 488	1 092 131	3 053 097	8 492 201
Duration of execution** in ms		0,55	1,53	4	0,52	1,37	3,4	0,56	1,55	4,1

*Note: * 1000 operations per processor clock cycles: character reading - 27 clock cycles, string comparison - 54 clock cycles, string concatenation - 297 clock cycles.*

*** for the calculation, a processor with a clock frequency of 2 GHz, considering the load by the operating system of 5%, was taken.*

In table 2 the results of studies assessing the temporal and velocity indicators of the procedures for the formation and decoding of information in crypto-code systems based on the ACCS and the MCCS Niederreiter. We will conduct a comparative assessment of the developed mathematical model and practical algorithms for the implementation of the Niederiterter's MACCS at MES.

Let's introduce the following notation.: lI – the length of the information sequence (block), which is fed to the input of the CCS scheme(in bits): lK – the length of the public key (in bits); lK+ – private key length (in bits); codogram length (lS – codogram length (in bits); OK – the complexity of the formation of codograms (the number of group operations); OSK – the complexity of solving the problem of analysis (the number of group operations); OK+ – the complexity of solving the problem of analysis (the number of group operations); L0 – source text length R – relative coding rate; old – the classical McEliece-Niederreiter ACCS proposed in [16]. In table 3 and Fig. 1 shows the results of studies of the complexity of cryptogram formation in various GF(2m). Analysis of the results in Fig. 1 indicates an increase in the rate of cryptogram formation when using shortened MES. The length of the codogram (in bits) is determined by the expression:

$$l_S = \left(2\sqrt{q} + q + 1 - 1/2k\right) \times m .$$

In tabl. 4 and fig. 2 shows the results of studies of the complexity of decrypting a cryptogram in various GF(2^m).

Table 2. **The results of studies assessing the time and speed indicators of the procedures for the formation and decoding of information**

Crypto-code systems	The length of the code sequence	Algorithm Throughput Rate (bytes / sec)	CPU core utilization (%)	Algorithm complexity, Per (cpb)
Niederreiter's ACCS	100	46 125 790	56	61,5
	1000	120 639 896	56	62,0
Niederreiter's MCCS with fixed vectors	100	51 694 662	56	61,7
	1000	126 399 560	56	62,2
Niederreiter's MCCS on shortened elliptic codes	100	52 721 778	56	61,5
	1000	127 389 928	56	62,1

Table 3. **Dependence of the cryptogram formation complexity in different *GF(2^m)***

GF(2^m)			3	4	5	6	7	8	9	10
R	1	0.5 (*old*)	817	2140	8706	10722	83000	207422	710920	**52704**
	2	0.75 (*old*)	968	6282	11461	60760	210170	605005	1018079	**103822**
	3	0.5	817	2140	8706	**10722**	83000	207422	710920	4572881
	4	0.75	968	6282	11461	**60760**	210170	605005	1018079	5561379

Table 4. **The results of studies of the complexity of decoding cryptograms in various *GF(2^m^)***

GF(2*^m^*)			3	4	5	6	7	8	9	10
R	1	0.5 (*old*)	120	680	2092	12397	127523	1203984	10637991	**175645127**
	2	0.75 (*old*)	640	2378	7512	61246	136495	1494284	12768954	**193648924**
	3	0.5	1280	11028	78634	**760553**	4566721	12948312	92516734	1.00E+09
	4	0.75	5127	23674	277830	**5220573**	19768512	52694229	10637991	175645127

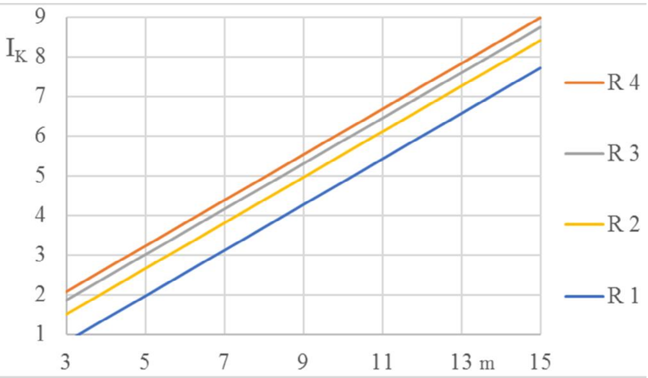

Fig. 1. The dependence of the cryptogram formation complexity in different *GF(2^m^)*

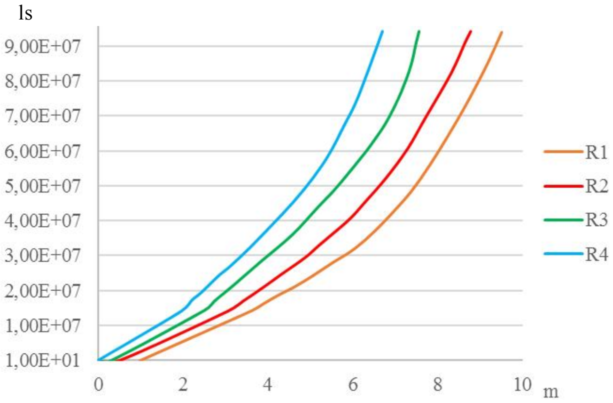

Fig. 2. The dependence of the cryptogram decoding complexity in various *GF(2^m^)*

Analysis table 3, 4 and Fig. 1, 2 showed that further reduction of the Galois field power leads to a significant decrease in the complexity of formation (≈ 3 times) and decoding (≈ 5 times) of the cryptogram.

In tablt 5 and Fig. 3 shows the results of studies of the complexity of hacking by the method of decoding decoding in various *GF*(2*^m^*).

The complexity of forming a codogram is determined by the expressions:

- for shortened MES (when implementing systematic coding, the following expression is defined):

$$O_K = (r+1)\times\left(2\sqrt{q}+q+1-1/2k\right)+O\left(\frac{1-K_C^u}{K_f}\times L\right);$$

for non-systematic coding:

$$O_K = O_K = (k+1)\times(k+1)\times\left(2\sqrt{q}+q+1-1/2k\right)+$$
$$+O\left(\frac{1-K_C^u}{K_f}\times L\right).$$

Table 5. **The dependence of the complexity of hacking over GF(2^m^)**

GF(2*^m^*)			3	4	5	6	7	8	9	10
R	1	0.5(*old*)	2.868	4.843	6.22	7.891	8.995	10.37	11.74	**13.19**
	2	0.75(*old*)	4.867	6.613	8.03	12.245	13.13	15.16	17.18	**19.23**
	3	0.5	8.234	12.647	14.742	**18.767**	21.102	24.05	27.002	29.95
	4	0.75	9.764	13.32	16.892	**19.76**	22.93	26.11	29.302	32.484

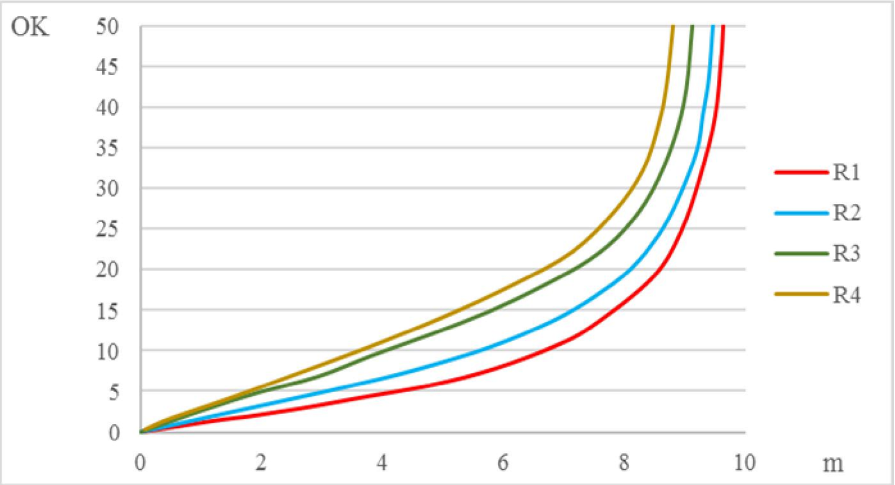

Fig. 3. The dependence of the complexity of hacking over *GF(2^m^)* (peer decoding)

Analysis of fig. 3 showed that reducing the power of the field to 26 did not lead to a significant reduction in the complexity of cracking a cryptogram using the method of decoding decoding.

The complexity of forming a codogram is determined by the expressions:

– shortened MES: for systematic and non-systematic coding, respectively, is determined by the expressions:

$$O_K = (r+1)\times\left(2\sqrt{q}+q+1-1/2k\right)+O\left(\frac{1-K_C^u}{K_f}\times L\right);$$

$$O_K = (k+1)\times(k+1)\times\left(2\sqrt{q}+q+1-1/2k\right)+$$
$$+O\left(\frac{1-K_C^u}{K_f}\times L\right).$$

The complexity of solving the problem of analysis (decoding) we define the expression:

$$O_{K+} = N_{покр}\times\left(2\sqrt{q}+q+1-1/2k\right)\times r+N_F \ \vee\ (N_K)$$

The complexity of decoding codogram is determined by the following expressions:

$$O_{SK} = 2\times\left(2\sqrt{q}+q+1-1/2k\right)^2+1/2k^2+4t^2+$$
$$+\frac{(t^2+t-2)^2}{4}+O\left((\alpha-z\times\log k)\Big/\left|K_z^c\times L\right|\right).$$

In tablt 6 and Fig. 4 shows the results of studies of the complexity of hacking and the complexity of coding for different speeds R in different GF (2m).

In tablt 7 and Fig. 5 shows the dependence of the volume of open key data for various indicators of sustainability.

Analysis of the results of the table 6, 7 and Fig. 4, 5 clearly demonstrates why an increase in the relative data transfer rate was obtained: the amount of key data in the proposed Niederreiter crypto-code structure on modified (shortened) elliptic codes is half as much as on binary codes in the classic Niederreiter's ACCS.

In table 8 shows the results of studies of the capacitance characteristics in the software implementation of the power field.

The resulting table 8 shows the number of group operations of the Niederreiter's ACCS software implementation when building on elliptic and modified (shortened) elliptic codes depending on the field strength.

Table 6. **Hacking complexity and coding complexity for different speeds R**

lg(ls)			3	4	5	6	7	8	9	10
R	1	0.5 (*old*)	18.22	21.42	38.77	54.13	82.14	165.84	358.33	**672.37**
	2	0.75 (*old*)	33.17	51.75	61.09	78.37	83.72	179.13	371.09	**684.94**
	3	0.5	56.88	78.92	94.91	**120.83**	182.39	276.27	459.81	783.46
	4	0.75	58.03	80.52	104.56	**128.79**	189.74	287.33	476.52	794.28

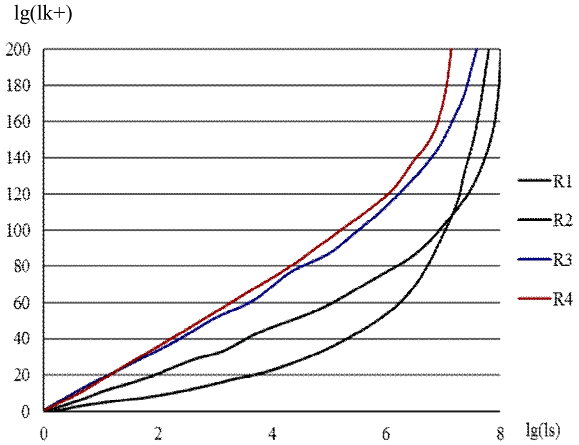

Fig. 4. Summary of hacking complexity and coding complexity

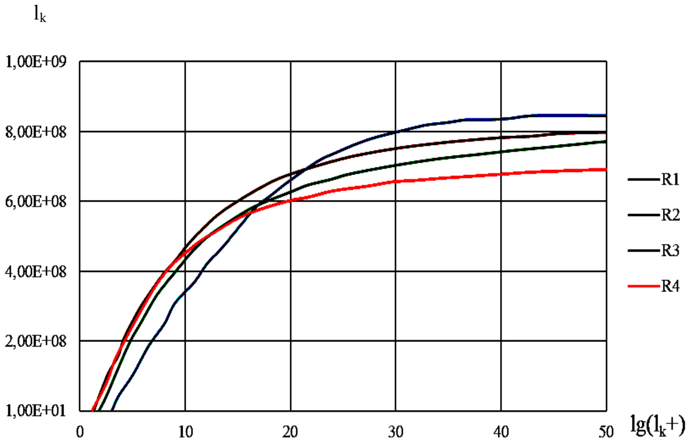

Fig. 5. Volume dependence of open key data for various sustainability indicators

Table 7. **Volume Dependencies of Open Key Data**

lg(l_k+)			5	20	35	50
R	1	0.5(old)	30	2278137	**12329538**	22541273
	2	0.75(old)	87	4351076	**14097276**	77520337
	3	0.5	968	1034682	**6126273**	8602376
	4	0.75	799	1897092	**6832018**	7027160

Table 8. **The dependence of the speed of the software implementation on the power of the field (the number of group operations)**

Cryptosystems	2^5	2^6	2^7	2^8	2^9	2^{10}
Niederreiter's ACCS on *ES*	1×10^7	$1,8\times10^7$	$3,2\times10^7$	$4,7\times10^7$	$6,3\times10^7$	$\mathbf{8,2\times10^7}$
Niederreiter's MACCS on shortened *MES*	1×10^7	$\mathbf{1,7\times10^7}$	$2,9\times10^7$	$4,4\times10^7$	$6,2\times10^7$	8×10^7

Analysis table 6, showed that when implementing the Niederreiter's ACCS over GF (210), 82.5×10^6 group operations are necessary, then the implementation of MACCS on shortened MES over GF (2^6) requires $17.7 – 18.6 \times 10^6$ group operations, which is 4.5 times less than when implemented in ES.

As can be seen from the dependencies shown in Fig. 6, the proposed modified crypto-code systems based on the Niederreiter TCS provide high rates of robustness and reliability of the processed and transmitted information. Their use will allow the use of open channels of IP networks for the transmission of confidential (commercial) information in real time, providing the required indicators of security and reliability.

Conclusion

Thus, a formal mathematical description of modified crypto-code information security tools based on Niederreiter's TCS using algebrageometric block codes based on shortening information symbols is proposed, which allows developing practical algorithms and conducting a study of the energy costs of their implementation.

Transferring the key sequence using the Niederreiter modified ACCS based on shortened codes allows using open communication channels of communication systems and significantly reducing the volumes of key sequences stored by users of this system.

The assessment of the complexity of the software implementation of crypto-code information security tools based on the Niederreiter TCS confirms the assumption that the computational cost of calculating a cryptogram / codogram is reduced, that key data (public key) need to be stored by an authorized user. The use of shortened elliptic codes allows you to increase the amount of data transmitted by hr characters, while ensuring the resistance of the cryptosystem when it is formed in the GF field (26-28), which significantly reduces the energy costs of its implementation, and allows its use in mobile applications.

Conducted research on the use of the fraction of the weight of the error vector allows, based on the main indicators of the communication channels of the communication system, to strengthen one of the indicators of the integrated mechanism - reliability or security.

References

1. Grischuk, R.V. & Danik, Y.G. (2016), *Basics of Cyber-security*, ZhNAEU, Zhitomir, 636 p.
2. Korolev, A. (2016), *Cyberspace and Information Terrorism*, URL: http://vpoanalytics.com/2016/02/15/kiberprostranstvo-i-informacionnyj-terrorizm (accessed on September 1, 2018).
3. Donald L. Evans (2001), *Security requirements for cryptographic modules*, URL: https://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf (accessed on September 1, 2018).
4. Yevseiev, S. & Tsyhanenko, O. (2018), "Development of asymmetrical crypto-coded construction of Niderraiter on modified codes, *Sistemi obrobki informacii*, No. 2 (153), pp. 127-135.
5. Lily, Chen, Stephen, Jordan, Yi-Kai, Liu, Dustin, Moody, Ray, Perlner and Daniel, Smith-Tone (2016), *Report on Post-Quantum Cryptography*, URL: http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf (accessed on September 1, 2018).
6. Hang, Dinh, Cristopher, Moore and Alexander Russell (2011), *McEliece and Niederreiter Cryptosystems that Resist Quantum Fourier Sampling Attacks*, URL: https://dl.acm.org/citation.cfm?id=2033093 (accessed on September 1, 2018).
7. Joo, Yeon Cho, Helmut, Griesser and Danish Rafique, (2017), "A McEliece-Based Key Exchange Protocol for Optical Communication Systems", *Proceedings of the 2nd Workshop on Communication Security*, pp 109-123. URL: https://link.springer.com/chapter/10.1007%2F978-3-319-59265-7_8 (accessed on September 1, 2018).
8. Evseev, S., Korol, O., Rzaev, H., & Imanova, Z. (2016), "Development of a modified asymmetric McElice crypto-code system with truncated elliptic codes", *Eastern European Journal of Advanced Technologies*, Vol. 4, 9 (82), pp. 18-26.
9. Yevseiev, S., & Korol, O. (2018). "Teoretiko-methodological ambushes of the hybrids of crypto-coded constructions on excess codes", *Information economy: stages of development, management methods, models*, KhNEU. Kharkiv, pp. 233-280.
10. Sidelnikov, V.M., (2002), "Cryptography and coding theory", Proceedings of the conference "M*oscow University and the Development of Cryptography in Russia*", Moscow State University, pp. 1-22.
11. Dudikevich, V.B., Kuznetsov, O.O. and Tomashevsky, B.P. (2010), "Crypto-code protection of information with non-binary equilibrium encoding", *The hour zahist of information*, No. 2, pp. 14-23.
12. Dudikevich, V.B., Kuznetsov, O.O. and Tomashevsky B.P. (2010), "Non-dual equilibrium coding method", *Modern information protection*, No. 3, pp. 57-68.
13. Kirill Morozov, Partha Sarathi Roy, Kouichi Sakurai (2017), "On unconditionally binding code-based commitment schemes", *Proceedings of the 11th International Conference on Ubiquitous Information Management and Communication*, ACM New York, NY, USA, DOI: https://doi.org/10.1145/3022227.3022327.

14. Biswas, Bhaskar & Sendrier, Nicolas (2008), “McEliece Cryptosystem Implementation. Theory and Practice”, *International Conference on Post-Quantum Cryptography*, pp. 47-62.
15. Evseev, S.P., Rzaev, Kh.N. and Tsyganenko, A.S. (2016). “Analysis of the software implementation of direct and inverse transformation using the method of non-binary equilibrium coding”, *Bezpeka Informatsii*, 2016, Vol. 22 # 2, Nash Format, Kyiv, pp. 196-203.
16. Niederreiter, H. (1986), “Knapsack-Type Cryptosystems and Algebraic Coding Theory”, *Probl. Control and Inform. Theory*, Vol. 15, pp. 19-34.
17. Rukhin, A., Soto, J., (2000), “A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications”, *NIST Special Publication*, 800-22.

Надійшла (received) 11.09.2018
Прийнята до друку (accepted for publication) 17.10.2018

Математична модель модифікованої крипто-кодової конструкції Нідеррайтера

О. С. Циганенко, Х. Н. Рзаєв, Т. А. Мамедова

Предметом вивчення в статті є модифікація крипто-кодової конструкції Нідеррайтера на недвійковий кодах. **Метою** є розробка математичної моделі модифікованої крипто-кодової конструкції Нідеррайтера з використанням алгеброгеометричних блокових кодів з укороченням інформаційної посилки. **Завдання**: формалізувати процедури формування кодограм і їх подальшого розкодування; розробити математичну модель крипто-кодової конструкції Нідеррайтера, модифікованої за допомогою укорочення інформаційної посилки і фіксації допустимих позиційних векторів перетворення відкритого тексту на основі рівноважного кодування. Отримані наступні **результати**. Дослідження крипто-кодової конструкції Нідеррайтера на МЕС дозволили виявити основну причину неможливості практичної реалізації алгоритмів розкодування при використанні недвійковий кодів в класичній схемі. Встановлено, що потрібно фіксування підмножини відкритих текстів, для яких процедура локалізації помилки, при обраних відправником матрицях маскування X, P і D (особистий ключ) не може бути виконана. З його допомогою потрібно "відсіяти" набори вектора помилки, які не дозволяють використовувати класичний варіант розкодування інформації на приймальному боці при використанні класичної схеми Нідеррайтера на m-них кодах. При побудові математичної моделі врахована виявлена особливість. В результаті отримана математична модель крипто-кодової конструкції Нідеррайтера, модифікована за допомогою укорочення інформаційної посилки і фіксації допустимих позиційних векторів перетворення відкритого тексту на основі рівноважного кодування. Висновки. Наукова новизна отриманих результатів полягає в наступному: запропонована модифікована математична модель крипто-кодової конструкції Нідеррайтера забезпечує її практичну реалізацію. Зменшення потужності поля при побудові класичної схеми Нідеррайтера дозволяє знизити обсяг переданих даних шляхом укорочення вектора помилки перед формуванням синдрому під час пересилання і відповідно енергетичні витрати на її реалізацію; отримали подальший розвиток використання квантово-стійкою і перспективною в використанні крипто-кодової конструкції Нідеррайтера, виявлена особливість і запропонована модифікація забезпечує її конкурентоспроможність.

Ключові слова: модифікована крипто-кодова конструкція Нідеррайтера; модифіковані укорочені еліптичні коди; рівноважне кодування; інформаційна скритність.

Математическая модель модифицированной крипто-кодовой конструкции Нидеррайтера

А. С. Цыганенко, Х. Н. Рзаєв, Т. А. Мамедова

Предметом изучения в статье является модификация крипто-кодовой конструкции Нидеррайтера на недвоичных кодах. **Целью** является разработка математической модели модифицированной крипто-кодовой конструкции Нидеррайтера с использованием алгеброгеометрических блоковых кодов с укорочением информационной посылки. **Задачи**: формализовать процедуры формирования кодограмм и их дальнейшего раскодирования; разработать математическую модель крипто-кодовой конструкции Нидеррайтера, модифицированную с помощью укорочения информационной посылки и фиксации допустимых позиционных векторов преобразования открытого текста на основе равновесного кодирования. Получены следующие **результаты**. Исследования крипто-кодовой конструкции Нидеррайтера на МЕС позволили выявить основную причину невозможности практической реализации алгоритмов раскодирования при использовании недвоичных кодов в классической схеме. Установлено, что требуется фиксирование подмножества открытых текстов, для которых процедура локализации ошибки, при выбранных отправителем матрицах маскировки X, P и D (личный ключ) не может быть выполнена. С его помощью нужно “отсеять” наборы вектора ошибки, которые не позволяют использовать классический вариант раскодирования информации на приемной стороне при использовании классической схемы Нидеррайтера на m-ных кодах. При построении математической модели учтена выявленная особенность. В результате получена математическая модель крипто-кодовой конструкции Нидеррайтера, модифицированная с помощью укорочения информационной посылки и фиксации допустимых позиционных векторов преобразования открытого текста на основе равновесного кодирования. **Выводы**. Научная новизна полученных результатов состоит в следующем: предложенная модифицированная математическая модель крипто-кодовой конструкции Нидеррайтера обеспечивает ее практическую реализацию. Уменьшение мощности поля при построении классической схемы Нидеррайтера позволяет снизить объем переданных данных путем укорочения вектора ошибки перед формированием синдрома на стороне отправителя и соответственно энергетические затраты на ее реализацию; получили дальнейшее развитие использование квантово-устойчивой и перспективной в использовании крипто-кодовой конструкции Нидеррайтера, выявленная особенность и предложенная модификация обеспечивает ее конкурентоспособность.

Ключевые слова: модифицированная крипто-кодовая конструкция Нидеррайтера; модифицированные укороченные эллиптические коды; равновесное кодирование; информационная скрытность.