Розвиток радіотехнічного забезпечення, АСУ та зв'язку Повітряних Сил

UDC 004.942 DOI: 10.30748/nitps.2019.37.12

S. Yevseiev

S. Kuznets Kharkiv National University of Economics, Kharkiv

RESEARCH OF CRITERIA OF MODIFIED NON-SYMMETRIC CRYPTO-CODE CONSTRUCTION OF MCELIECE ON EXTENDED ELLIPTIC CODES

The computing development in the post-quantum cryptography era puts forward new requirements for cryptographic mechanisms for providing basic security services. The advent of a full-scale quantum computer casts doubt on the cryptographic strength of cryptosystems based on symmetric cryptography and public-key cryptography. One of the promising areas in the opinion of US NIST experts is the use of crypto-code constructions (crypto-code schemes or code-theoretic schemes) by McEliece or Niederreiter. The construction allows one integrated mechanism to provide the basic requirements for cryptosystems – cryptographic stability, speed of crypto conversion and in addition – reliability based on the use of noise-resistant coding. However, their use is difficult due to the large volume of power of the alphabet, and the possibility of hacking based on Sidelnikov's attack. The paper proposes to use non-cyclic noise-resistant codes on elliptic curves in a modified McEliece cryptosystem that are not susceptible to Sidelnikov's attack. The main criteria for constructing a modified crypto-code based on the McEliece scheme on elongated elliptic codes are investigated. It is proposed to reduce the energy intensity in the proposed crypto code design by reducing the power of the Galois field while ensuring the level of cryptographic stability of the modified cryptosystem as a whole with its software implementation. To reduce the field power, it is proposed to use modified elliptical codes, which allows to reduce the field power by 2 times. A comparative assessment of the performance of cryptocurrencies in the proposed design of the cryptosystem is carried out. The results of statistical stability studies based on the NIST STS 822 package confirm the cryptographic strength of the proposed cryptosystem on modified elongated elliptical codes.

Keywords: *Asymmetric McEliece crypto-code system, Crypto-code construction on algebro-geometric codes, Modified (extended) elliptic codes, Confidentiality, Integrity.*

Introduction

The rapid growth of the volume of data being processed and the development of computing technology has put forward new requirements for reliability and data security. Studies on the influence of quantum computing using quantum superposition and quantum entanglement to transmit and process data have shown that quantum computers that use special algorithms (for example, Shor's algorithm) will be able to factorize numbers in polynomial time [1–2]. Thus, RSA, ECC, DSA cryptographic systems will be vulnerable to brute force attacks using a full-scale quantum computer. Therefore, the main research and development of cryptographic information security tools (CIST) are currently aimed at finding solutions that confront quantum computing and at the same time must be resistant to attacks using ordinary computers. Such algorithms are related to the section of quantum-resistant cryptography (quantum secure cryptography or quantum resistant cryptography) [3–4]. Through the imminent emergence of new schemes, sufficient attention has not been paid to the well-known, asymmetric crypto-code systems (ACCS) based on McEliece theoretical code schemes (TCS), which are also quantum-stable.

The advent of a full-scale quantum computer casts doubt on the cryptographic strength of cryptosystems based on symmetric cryptography and public-key cryptography. One of the promising areas in the opinion of US NIST experts is the use of crypto-code constructions (crypto-code schemes or code-theoretic schemes) by McEliece or Niederreiter. Such crypto-code constructions, as estimated by the US NIST experts, can provide cryptographic stability in post-quantum cryptography provided that they are constructed in the Galois field GF (2^{10}–2^{13}). This provides an additional approach to data transmission based on direct error correction (based on the use of error-correcting codes in designs), the speed of cryptographic conversions is comparable to the encryption speed of block-symmetric cipher algorithms. In turn, this approach provides the required level of quick-action and reliability of data transmission.

The construction allows one integrated mechanism to provide the basic requirements for cryptosystems – cryptographic stability, speed of crypto conversion and in addition – reliability based on the use of noise-resistant coding. However, their use is difficult due to the large volume of power of the alphabet, and the possibility of hacking based on Sidelnikov's attack. The paper proposes to use non-cyclic noise-resistant codes on elliptic curves in a modified McEliece cryptosystem that are not susceptible to Sidelnikov's attack. The main criteria for constructing a modified crypto code based on the McEliece scheme on elongated elliptic codes are investigated. It is proposed to reduce the energy intensity in the proposed crypto-code design by reducing the power of the Galois field while ensuring the level of cryptographic stability of the modified cryptosystem as a whole with its software implementation. To reduce the field power, it is proposed to use modified elliptical codes, which allows to reduce the field power by 2 times. A comparative assessment of the performance of cryptocurrencies in the proposed design of the cryptosystem is carried out. The results of statistical stability studies based on the NIST STS 822 package confirm the cryptographic strength of the proposed cryptosystem on modified elongated elliptical codes.

Analysis of recent studies and publications. The main advantage of symmetric and asymmetric CCS is the high speed of information conversion and the integrated provision of reliability and information concealment (confidentiality) that satisfies the basic security requirements.

For security reasons, the perspective direction is the use of asymmetric cryptosystems based on CCS McEliece integrated (with one mechanism) providing reliability values at the level of $2^9 – 2^{12}$ and crypto stability of $2^{30} – 2^{35}$ group operations when constructed over the field GF(2^{10}).

Fig. 1 shows the results of studies of the speed of cryptographic transformations with modern symmetric and asymmetric cryptosystems.

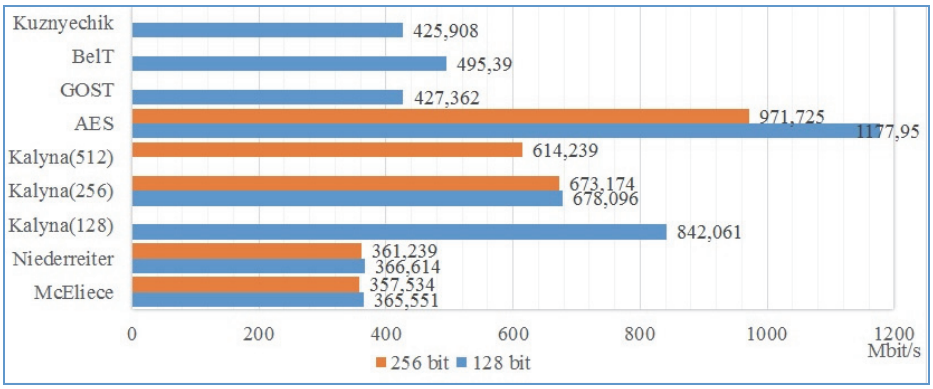

Fig. 1. Results of the analysis of the speed of information conversion

Tabl. 1 shows the results of comparative studies of the effectiveness of cryptographic information security methods at a fixed level of stability and there are presented: average (the complexity of cryptanalysis is the best-known algorithm of at least 2^{128} operations); high (the complexity of cryptanalysis is the best-known algorithm of at least 2256 operations); super-high (the complexity of cryptanalysis is the best-known algorithm of at least 2^{512} operations) [4].

Hence, as it follows from the above results of the comparative analysis (Fig. 1 and Tabl. 1), asymmetric cryptographic algorithms using TCS allow the cryptographic protection of information to be realized on the technology of public keys. And thus they provide the speed of crypto-code transformation of information with the speed of encryption of block-symmetric ciphers (BSC).

In addition, the practical use of ACCS information security allows to ensure the security and reliability of data, based on the integration of channel coding and encryption mechanisms in a comprehensive manner.

Table 1

Results of comparative researches of efficiency of cryptographic methods of information security at the fixed stability level

Methods of cryptographic transformation	Security model	Length of key data, [bits]	Speed of cryptographic transitions, [bits / sec]	Additional features
Block symmetric ciphers	Practical security	128, 256, 512	$10^6 – 10^9$	None
Stream symmetric ciphers	Practical security	128, 256, 512	$10^7 – 10^{10}$	None
Asymmetric PCAs are similar cryptographic algorithms	Proof Security	3248 (128), 15424 (256)	$10^2 – 10^3$	None
Asymmetric CCS using code structures	Proof Security	$0{,}5 \cdot 10^6$ (128), $2 \cdot 10^6$ (256)	$10^6 – 10^8$	Error monitoring, increasing reliability

In [5–8], the authors propose McEliece crypto-code systems based on various codes.

In [9–11], an equilibrium coding method based on m-th codes (Reed-Solomon codes) was proposed; however, the disadvantage is the lack of a practical algorithm fordecoding the syndrome on the receiving side and the possibility of hacking based on a rearranged decoder. In [13] proposes a modification of the Reed-Solomon codes, which exceeds the Guruswami-Sudan decoding radius $1 - \sqrt{R}$ of the Reed-Solomon codes at low speeds R. The idea is to select the Reed-Solomon codes U and V with the corresponding speeds in (U | U + V) and decode them using the soft information decoder Koetter-Vardy.

In [5; 12], the use of alternating Goppa codes in the McEliece cryptosystem and the classical Goppa codes in the Niederreiter cryptosystem are proposed. In [14], the authors confirm the complexity of the practical implementation of the Niederreiter scheme and consider the possibility of using cryptosystems in VPN channels. In [15] article proposes a new class of convolutional codes, which allows an effective algorithm for algebraic decoding, the use of the McEliece cryptosystem in a variant. Unlike the classic McEliece cryptosystems, which use block codes, the authors propose the use of a convolutional encoder as part of the public key.

In [16] the authors propose a new Niederreiter cryptosystem based on quasi-cyclic codes $m - 1$ m, which is quantum-secure. This new cryptosystem has a good transfer rate compared to the one that uses the Hopp binary codes and uses smaller keys.

In [6–7; 12], the authors use low density quasi-cyclic parity codes (QC-LDPC) [8] and on codes with the maximum rank distance [6–7] to build McEliece and Niederreiter cryptosystems, respectively. In [12], the construction of the McEliece and Niederreiter schemes based on the alternating Goppa codes is considered.

In computer networks with decisive feedback, the authors ensure the use of the McEliece crypto-code design in the G.709 optical transport network (OTN) infrastructure infrastructure to provide integrated requirements for both reliability and [17]. In [18], the authors proposed to use the Niederreiter asymmetric crypto-code system on elliptic codes. This approach provides protection against possible attacks described in [19] and the required level of cryptographic strength. But there remained unresolved questions of practical implementation with the necessary power of the GF(2^{10}–2^{13}) field to ensure a guaranteed level of cryptographic strength.

Thus, the analysis showed that crypto-code constructions belong to the section of quantum-resistant cryptography and can be used instead of asymmetric cryptosystems in the near future. In this regard, their improvement is of wide interest among the scientific community.

However, all the codes proposed by the authors are cyclical and prone to Sidelnikov's attacks [19]. The essence of Sidelnikov's attack comes down to finding the elements of the generating matrix and removing the action of masking matrices based on linear fractional transformations and the property of triply transitivity of the automorphism group of the generalized Reed-Solomon code. As a solution Sidelnikov proposes the use of non-cyclic codes based on cascade or algebraic-geometric codes (codes on elliptic curves). This approach provides not only opposition to Sidelnikov's attack, but also the ability to reduce key data based on the use of the coefficients of the equation of the curve as a secret parameter [4]. In addition, US NIST experts consider the security (cryptographic strength) of cryptosystems in post-quantum cryptography only if they built in the Galois field GF (2^{10}–2^{13}). However, the level of computing capabilities of modern information and communication systems does not allow them to be fully implemented. To reduce energy costs, the authors propose using modified crypto-code constructions on modified (extended codes). Figure 2 shows the exchange protocol based on the modified McEliece crypto-code system on modified (shortened) elliptic codes, in Fig. 3 – on modified (extended) codes.

The main code characteristics and parameters of cryptosystems are given in Tabl. 2–3.

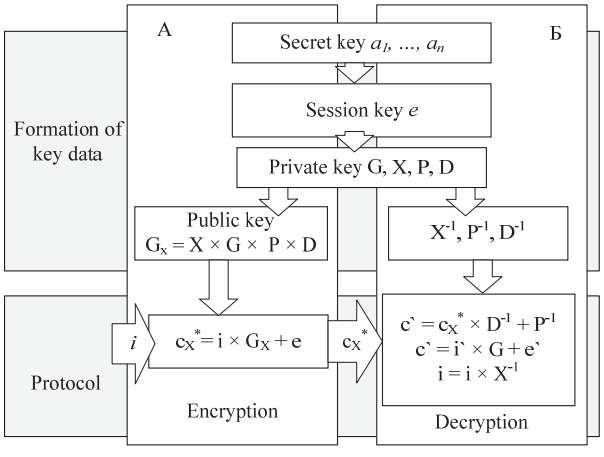

Fig. 2. Exchange protocol based on a modified McEliece crypto-code system on modified (shortened) elliptic codes

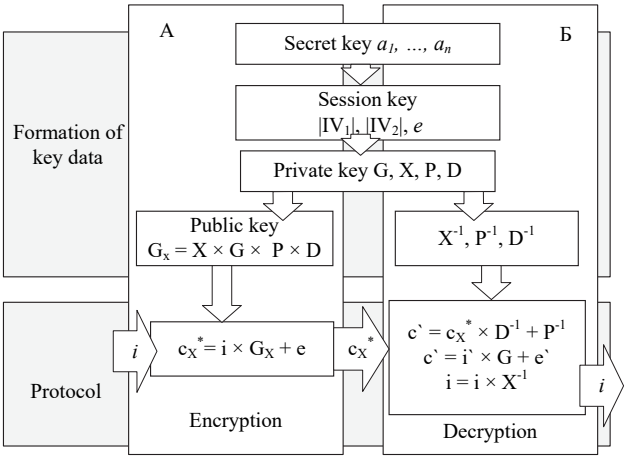

Fig. 3. Exchange protocol based on a modified McEliece crypto-code system on modified (extended) elliptic codes

Table 2

The main (*n, k, d*) properties of *MEC*

Property	Shortened MEC	Extended MEC
(*n, k, d*)code parameters constructed by displaying the viewφ:X→P^{k-1}	$n = 2\sqrt{q} + q + 1 - x$, $k \geq \alpha - x$, $d \geq n - \alpha$, $\alpha = 3 \times \deg F$, $k + d \geq n$	$n = 2\sqrt{q} + q + 1 - x + x_1$, $k \geq \alpha - x + x1$, $d \geq n - \alpha$, $\alpha = 3 \times \deg F$
(*n, k, d*) code parameters constructed by displaying the viewφ:X→P^{r-1}	$n = 2\sqrt{q} + q + 1 - x$, $k \geq n - \alpha$, $d \geq \alpha$, $\alpha = 3 \times \deg F$, $k + d \geq n$	$n = 2\sqrt{q} + q + 1 - x + x_1$, $k \geq n - \alpha$, $d \geq \alpha$, $\alpha = 3 \times \deg F$

Table 3

Basic parameters of McEliece MACCS on *MEC*

Property	Shortened MEC	Extended MEC
dimension of the secret key	$l_{K+} = x \times \left\lceil \log_2 \left(2\sqrt{q} + q + 1\right) \right\rceil$	$l_{K+} = (x - x_1) \times \log_2 \left(2\sqrt{q} + q + 1\right)$
dimension of information vector	$l_I = (\alpha - x) \times m$	$l_I = (\alpha - x + x1) \times m$
dimension of the cryptogram	$l_S = \left(2\sqrt{q} + q + 1 - x\right) \times m$	$l_S = \left(2\sqrt{q} + q + 1 - x + x_1\right) \times m$
relative transmission speed	$R = (\alpha - x) / \left(2\sqrt{q} + q + 1 - x\right)$	$R = (\alpha - x + x_1) / \left(2\sqrt{q} + q + 1 - x + x_1\right)$

The proposed McEliece MCCS can reduce the power of the alphabet, which allows them to be implemented in practice, while ensuring the required level of cryptographic strength due to the introduction of additional initialization vectors: IV_1 – defines shortening characters from a code word (cryptograms), IV_2 – defines elongation characters (plain text) of a code word (cryptogram), see also Fig. 3. Consider the results of a study of the basic properties of the proposed crypto-code systems.

Statement of basic materials

Evaluation of energy costs for program implementation and the complexity of the proposed McEliece MACCS code transformation. To estimate time and speed parameters it is common to use the unit of measurement CPB (cycles per byte) – the number of processor cycles, which should be spent to process 1 byte of incoming information.

Algorithm complexity is calculated from expression [4]:

$$Per = Utl \cdot CPU\_clock / Rate, \quad (1)$$

where *Utl* – utilization of the *CPU* core (%) and *Rate* – algorithm bandwidth (bytes/sec).

In Tabl. 4 there are shown dependency research results of code length sequence of algebrogeometric code in McEliece TCS from number of processor cycles due to executing elementary operations in program realization of crypto-code systems.

Tabl. 5 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.

In order to estimate the parameters of asymmetric code-theoretic schemes using elliptic codes, let us introduce the following notation:

- l_I – length of the information sequence (block) arriving at the input of the crypto-code structure (in bits);
- l_K – length of the public key (in bits);
- l_{K+} – length of the private key (in bits);
- l_s –length of the code (in bits);
- O_K – complexity of the formation of the code (number of group operations);
- O_{SK} – difficulty of decoding the cryptogram (the number of group operations);
- O_{K+} – complexity of solving the analysis problem (the number of group operations).

For the construction of graphs, conditional abbreviations (prefixes) were used:

- u_k – MACCS with truncated MEC;
- u_d – MACCS with elongated MEC.

In calculating the parameters of cryptosystems, the Galois fields were used:

- for McEliece TCS – $GF(2^{10})$;
- for MACCS with truncated / elongated MEC – $GF(2^6)$.

In the next step, we perform a comparative analysis of the parameters of the McEliece asymmetric code-theoretic scheme (MACS) using EC, with the parameters of the modified MACCS McEliece on MEC. To estimate the length of the information sequence (in bits) arriving at the input of the MACCS with the algebraic (*n*, *k*, *d*)-code over $GF(2^m)$ (where m − the power of the extended Galois field), we use the expressions:

Table 4

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: reading a character – 27 cycles, comparing strings – 54 cycles, string concatenation – 297 cycles.*

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

Table 5

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

Crypto-code systems	Code sequence length	Algorithm bandwidth, Rate (byte / 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

- $l_I = k \times m$, (2)

– for ACCS on the EC;

- $l_I = 1/2k \times m$, (3)

– for MCCS on truncated MEC;

- $l_I = k \times m$, (4)

– for MACCS on elongated MEC.

In Tabl. 6 and in Fig. 4 we show the cryptogram formation complexity from the power of the field.

Table 6

Dependence of the complexity of forming a cryptogram in various $GF(2^m)$

$GF(2^m)$	R					
	0.5	**0.75**	**0.5(u_d)**	**0.75(u_d)**	**0.5(u_k)**	**0.75(u_k)**
3	31	87	242	603	817	968
4	76	340	760	980	2140	6282
5	335	872	2241	6121	8706	11461
6	582	2170	**6348**	**9830**	**10722**	**60760**
7	1023	6172	17092	61751	83000	210170
8	5237	10673	67016	105265	207422	605005
9	10563	50487	98765	510780	710920	1018079
10	**52704**	**103822**	497309	908243	4572881	5561379

From the provided data it is visible that the cryptogram formation complexity for the chosen power of the GF 2^6 on the truncated and elongated codes is much lower (by 5 times and more), than in original realization of MACCS to the EC. Respectively, the speed of formation of the cryptogram will significantly increase.

In order to estimate the length of the cryptogram (in bits), we use the expressions:

- $l_s = n \times m$, (5)

– for ACCS on the EC;

- $l_s = \left(2\sqrt{q} + q + 1 - \frac{1}{2k}\right) \times m$, (6)

– for MCCS on truncated MEC;

- $l_s = \left(2\sqrt{q} + q + 1 - \frac{1}{2k} + \frac{1}{2k}\right) \times m$, (7)

– for MCCS on elongated MEC.

In Tabl. 7 and in Fig. 5 we show the dependence of the decoding complexity of the cryptogram on the field strength.

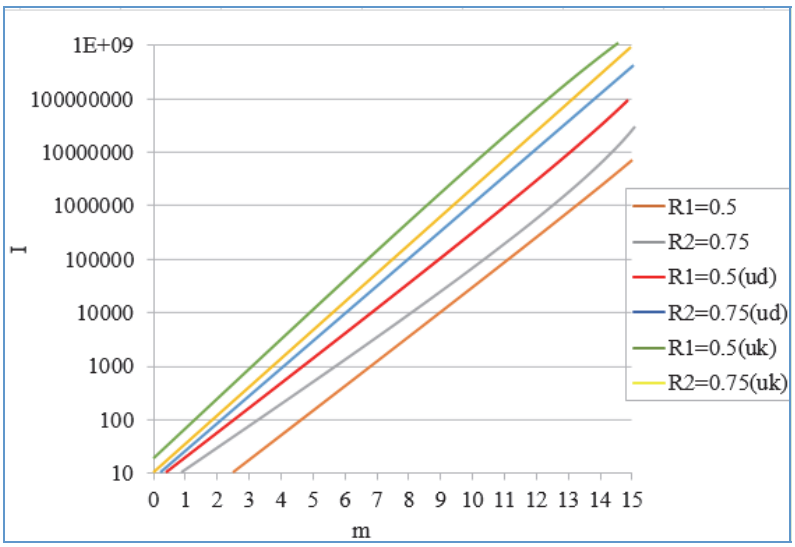

Fig. 4. Dependence of the complexity of forming a cryptogram in various $GF(2^m)$

Table 7

Dependence of the decryption complexity of the cryptogram in various $GF(2^m)$

$GF(2^m)$	R					
	0.5	**0.75**	**0.5(u_d)**	**0.75(u_d)**	**0.5(u_k)**	**0.75(u_k)**
1	43	57	78	81	82	96
2	67	98	456	457	457	556
3	120	640	1024	1168	1280	5127
4	680	2378	7672	8232	11028	23674
5	2092	7512	21073	42082	78634	277830
6	12397	61246	**103862**	**281472**	**760553**	**5220573**
7	127523	136495	642648	752018	4566721	19768512
8	1203984	1494284	3564898	3957812	12948312	52694229
9	10637991	12768954	54678128	67458242	92516734	102564872
10	**175645127**	**193648924**	1e+09	1e+09	1e+09	1e+09

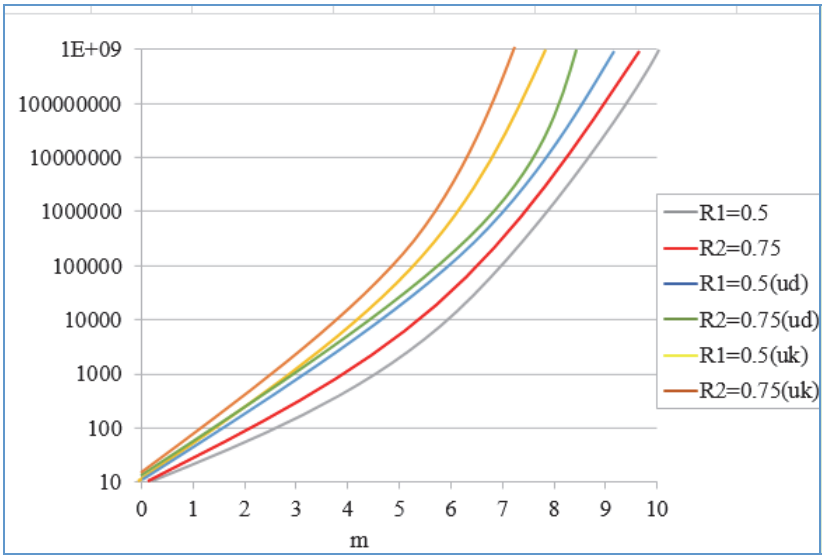

Fig. 5. Dependence of the decryption complexity of the cryptogram in various $GF(2^m)$

Analysis of calculation results, as in the case of cryptogram formation, shows a significant increase in the decoding rate when using truncated and elongated MEC.

The length of the public key (in bits) is determined by the sum of the elements of the matrix and is given by the expressions:

- $l_K = k \times n \times m,$ (8)

– for ACCS on the EC;

$$\bullet\ l_s = \frac{1}{2k}\times\left(2\sqrt{q}+q+1-\frac{1}{2k}\right)\times m, \qquad (9)$$

– for MCCS on truncated MEC;

$$\bullet\ l_s = \frac{1}{2k}\times\left(2\sqrt{q}+q+1-\frac{1}{2k}+\frac{1}{2k}\right)\times m, \qquad (10)$$

– for MCCS on elongated MEC.

The length of the private key (in bits) is determined by the sum of the elements of the matrices *X*, *P*, *D* (in bits) and is given by the expressions:

$$\bullet\ l_{K+} = n^2\times k^2\times m, \qquad (11)$$

– for ACCS on the EC;

$$\bullet\ l_{Ks} = \frac{1}{2k}\left[\log_2\left(2\sqrt{q}+q+1\right)\right], \qquad (12)$$

– for MCCS on truncated MEC;

$$\bullet\ l_{Ks} = \left(\frac{1}{2k}-\frac{1}{2k}\right)\left[\log_2\left(2\sqrt{q}+q+1\right)\right], \qquad (13)$$

– for MCCS on elongated MEC.

In Tabl. 8 and in Fig. 6 there are shown the dependency of the hacking complexity based on the permutation decoding on the field strength.

The analysis of Fig. 7 shows that reducing the field power to 2^6 have not led to a significant reduction in the complexity of breaking cryptograms by permutation decoding.

Table 8

Dependence of hacking complexity in various GF(2^m)

GF(2^m)	**R**					
	0.5	**0.75**	**0.5(u_d)**	**0.75(u_d)**	**0.5(u_k)**	**0.75(u_k)**
1	1.056	1.38	2.786	2.835	4.122	4.257
2	2.237	3.017	4.978	5.961	6.233	6.781
3	2.868	4.867	7.568	8.120	8.234	9.764
4	4.843	6.613	9.87	12.1	12.647	13.32
5	6.22	8.03	12.017	14.224	14.742	16.892
6	7.891	12.245	**14.983**	**17.483**	**18.767**	**19.76**
7	8.995	13.13	17.14	20.32	21.102	22.93
8	10.37	15.16	19.55	23.23	24.05	26.11
9	11.74	17.18	21.96	26.15	27.002	29.302
10	13.19	19.23	24.37	29.06	29.95	32.484

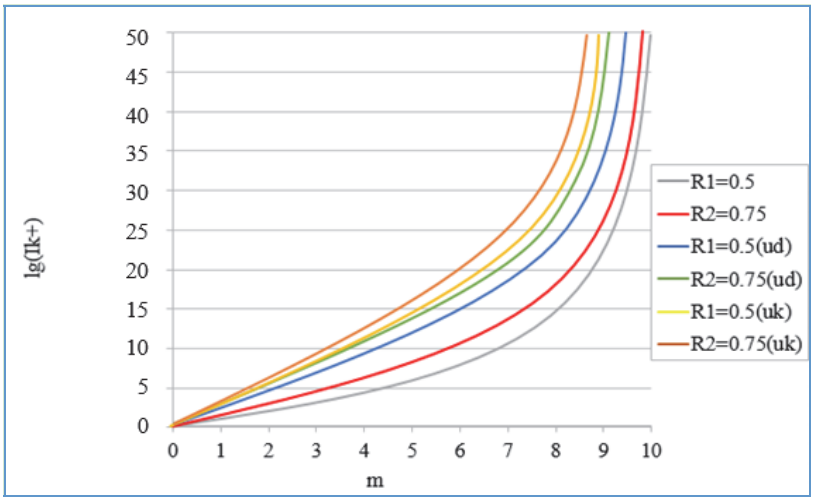

Fig. 6. Dependence of hacking complexity in various *GF*(2^m)

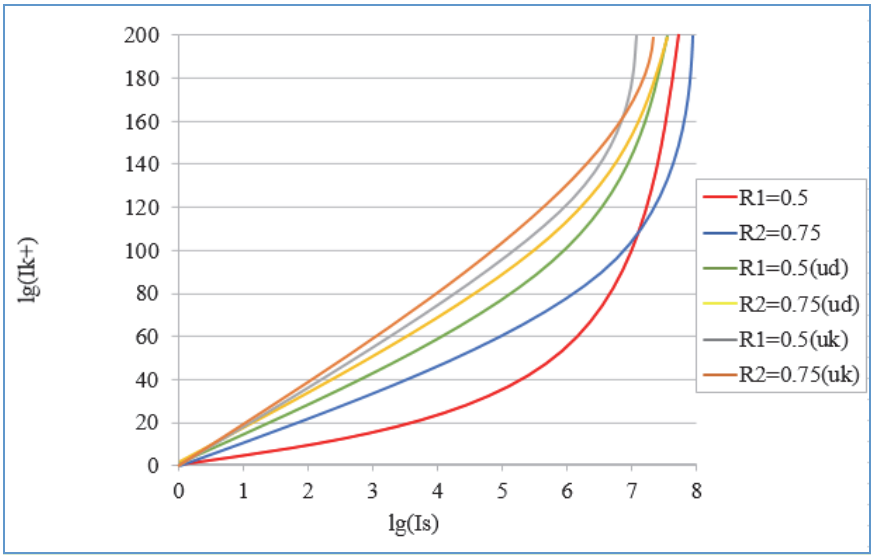

Fig. 7. Summary diagram of hacking complexity and encoding complexity for different speeds of the EC (MEC)

The complexity of the cryptogram formation is estimated by the expressions:

- for ACCS on the EC: when implementing systematic coding:

$$O_K = (r+1) \times n; \quad (14)$$

- for non-systematic coding:

$$O_K = (k+1) \times n; \quad (15)$$

- for MCCS on truncated MEC: when implementing systematic coding:

$$O_K = (r+1) \times \left(2\sqrt{q} + q + 1 - \frac{1}{2k}\right), \quad (16)$$

- for non-systematic coding:

$$O_K = (k+1) \times \left(2\sqrt{q} + q + 1 - \frac{1}{2k}\right); \quad (17)$$

- for MCCS on elongated MEC: when implementing systematic coding:

$$O_K = (\mathrm{r}+1) \times \left(2\sqrt{q} + q + 1 - \frac{1}{2k} + \frac{1}{2k}\right), \quad (18)$$

- for non-systematic:

$$O_K = (\mathrm{k}+1) \times \left(2\sqrt{q} + q + 1 - \frac{1}{2k} + \frac{1}{2k}\right). \quad (19)$$

The complexity of decoding of a pattern is defined by expressions:

- for ACCS on EC:

$$O_{Sk} = 2 \times n^2 + k^2 + 4t^2 + \frac{(t^2 + t - 2)^2}{4}; \quad (20)$$

- for MCCS on truncated MEC:

$$O_{Sk} = 2\left(2\sqrt{q} + q + 1 - \frac{1}{2k}\right)^2 - \frac{1}{2k^2} + 4t^2 + \frac{(t+t-2)^2}{4}, \quad (21)$$

- for MCCS on elongated MEC:

$$O_{Sk} = 2\left(2\sqrt{q} + q + 1 - \frac{1}{2k} + \frac{1}{2k}\right) - k^2 + 4t^2 + \frac{(t+t-2)^2}{4}. \quad (22)$$

Complexity of the task of the analysis (decoding) solution are set by expressions:

- for ACCS on EC:

$$O_{K+} = N \,\mathrm{cov} \times n \times r, \quad (23)$$

where $N_{\mathrm{cov}} \geq \frac{C_n^t}{C_{n-k}^t} = \frac{n(n-1)\ldots(n-t-1)}{(n-k)(n-k-1)\ldots(n-k-t-1)}$,

$\tau=[(d-1)/2]$.

The potential firmness of cryptosystem is defined by size $\rho \times t$, and noise stability of system – $(1-\rho) \times t$.

- For MCCS on truncated codes:

$$O_{MACCS} = N \times \left(2\sqrt{q} + q + 1 - \frac{1}{2k}\right) \times \mathrm{r}. \quad (24)$$

- For MCCS on elongated codes:

$$O_{MACCS} = N \times \left(2\sqrt{q} + q + 1 - \frac{1}{2k} + \frac{1}{2k}\right) \times \mathrm{r}. \quad (25)$$

In Tabl. 9 and in Fig. 7 it is presented dependence of complexity of breaking and complexity of coding for various speeds of the EC (MEC).

Dependences of volume of open key data for various indicators of firmness are presented in Tabl. 10 and in Fig. 8.

The results of the research of the capacitor characteristic at program realization from field power are presented in Tabl. 11.

Table 9

Summary diagram of hacking complexity and encoding complexity for different speeds of the EC

lg(l_s)	**0.5**	**0.75**	**0.5(u_d)**	**0.75(u_d)**	**0.5(u_k)**	**0.75(u_k)**
1	4.75	12.1	15.6	18.23	19.12	19.82
2	10.52	21.76	32.47	35.67	38.63	39.18
3	18.22	33.17	43.75	51.61	56.88	58.03
4	21.42	51.75	59.43	72.81	78.92	80.52
5	38.77	61.09	68.26	87.32	94.91	104.56
6	54.13	78.37	**101.72**	**112.46**	**120.83**	**128.79**
7	82.14	83.72	156.75	164.72	182.39	189.74
8	165.84	179.13	223.64	231.57	276.27	287.33
9	358.33	371.09	421.97	428.63	459.81	476.52
10	**672.37**	**684.94**	716.41	722.26	783.46	794.28

Table 10

Dependencies of the volume of open key data for various indicators of durability

lg(l_{k+})	***R***					
	0.5	**0.75**	**0.5(u_d)**	**0.75(u_d)**	**0.5(u_k)**	**0.75(u_k)**
5	30	87	240	602	968	799
20	2278137	4351076	926137	987234	1034682	1897092
35	12329538	14097276	4253109	5237688	6126273	6832018
50	22541273	77520337	43076332	60122407	8602376	7027160

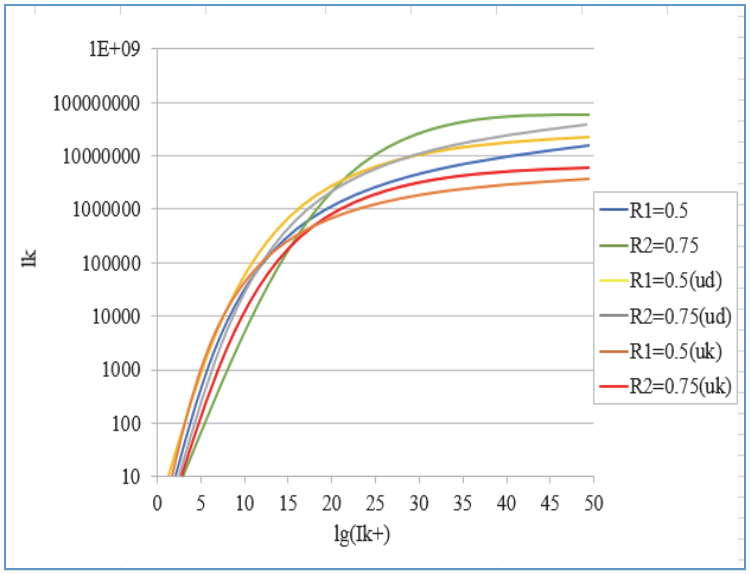

Fig. 8. Dependencies of the volume of open key data for various indicators of durability

Table 11

The dependence of the program implementation rate on the power of the field (the number of group operations)

Cryptosystems	**2^5**	**2^6**	**2^7**	**2^8**	**2^9**	**2^{10}**
ACCS McEliece on EC	10018042	18048068	32847145	47489784	63215578	**82467897**
MACCS McEliece on truncated MEC	10007947	**17787431**	28595014	44079433	61974253	79554764
MACCS McEliece on elongated MEC	11156138	**18561228**	33210708	48297112	65171690	84051337

Results of Studies of the Proposed Public-Key Cryptosystems Based on the NIST-STS 822 Package. One of the main components of the evaluation of the stability of cryptographic algorithms is the estimation of its statistical security. It is believed that the algorithm is statistically secure if the sequence it generates by its properties is not inferior to a random sequence - such sequences are called “pseudorandom”. For the experimental estimation of how close the cryptoalgorithms approximate the generators of the “random” sequences, statistical tests are used. The NIST STS benchmark package for testing random or pseudorandom number

generators is one of the approaches to realizing the task of evaluating the statistical security of cryptographic primitives. The use of this package makes it possible to draw conclusions with a high degree of probability as to how much sequence that is generated by the investigated primitive is statistically secure. A set of NIST STS tests was proposed during the contest for a new national standard for US block coding in 2000 and developed by the staff of the National Institute of Standard and Technologies [20]. This set was used to study the statistical properties of candidates for a new block cipher. To date, the test methodology, which is offered by NIST, is the most common for developers of cryptographic means of information protection. The test procedure for an individual binary sequence S is as follows:

1. A null hypothesis H_0 is advanced-the assumption that the given binary sequence S is random.

2. From the S sequence, the test statistics from (S) are calculated.

3. Using the special function and test statistics, a probability value $P=f(c(S)),\ P\in[0,1]$.

4. The value of probability P is compared with the level of significance

$\alpha\in[0.001,0.01]$. If $P\geq\alpha$, then the H_0 hypothesis is accepted. Otherwise, an alternative hypothesis is adopted.

In accordance with the methodology, the decision to pass statistical testing is taken in the event that the following rules are fulfilled:

1. The rule #1. All q tests were tested, ($q = \overline{1,189}$), and if the value of the coefficient r_j is inside the confidence interval [0.96, 1.00];

2. The rule #2. All q tests were tested, ($q = \overline{1,189}$), and if for all tests by the Pearson χ^2 criterion the condition is met $P(\chi^2)>0.0001$.

For carrying out of experimental research of properties of the developed code cryptosystems it is developed the program realization of the offered means of protection of the information, the following parameters are selected during the testing:

- length of the test sequence $n = 10^6$ bits;
- number of tested sequences $m = 100$. Thus, the volume of the test sample was $N = 10^6 \times 100 = 10^8$ bits;
- significance level $\alpha = 0.01$;
- number of tests $q = 189$.

Authors have obtained the results of statistical testing and statistical portraits of the developed means of information protection. The final values and results of the best world crypto-algorithms are summarized in Tabl. 12.

As it can be seen from the presented data in Tab. 10, the proposed crypto-code systems on the modified codes are not inferior to the statistical characteristics of the randomness of the code sequence formation to the world standards of providing basic services: confidentiality, integrity and accessibility, while ensuring the required level of reliability of data transmission.

Table 12

Results of experimental testing

Generator	Number of tests, in which testing passed ≥99% of the sequences	Number of tests, in which testing passed more than ≥96% of the sequences
BBS	134 (71%)	189 (100%)
FIPS 197	126 (67%)	189 (100%)
Developed modified crypto-code protection of information	136 (73%)	189 (100%)

Consequently, the practical application of the developed information protection means allows to obtain good statistical properties of the generated sequences and to effectively ensure the security and reliability of the data being processed and transmitted.

Conclusion

In a result of conducted research it can be concluded that:

1. Evaluation by NIST specialists of the computing capabilities of quantum computers requires a review of the use of traditional encryption algorithms to provide basic security services based on symmetric and asymmetric cryptography. The growth and synergy of modern threats puts forward new requirements for systems for protecting confidential information. At the same time, the use of crypto-code constructions allows to provide not only the required level of cryptographic stability, but also the reliability of the transmitted information. Such crypto-code constructions, as estimated by US NIST experts, can provide cryptographic stability in post-quantum cryptography provided that they are constructed in the Galois GF field (2^{10}–2^{13}), while providing an additional approach to data transmission based on direct error correction (based on the use of error-correcting codes in designs), the speed of cryptographic conversions is comparable to the encryption speed of block-symmetric cipher algorithms, which provides the required level of speed and reliability of data transfer. However, their use in communication devices is associated with significant energy and computational costs, which does not allow their practical use. In addition, the proposed Sidelnikov attack does not allow the use of many well-known codes; to counter it, it is proposed to use algebraic geometries based on the parameters of elliptic curves.

2. The use of modified crypto-code constructions in modified (shortened, elongated) elliptic codes allows to reduce the level of the alphabet with the required

level of cryptographic strength. For this, additional session keys are used (initial initialization, which specify the symbols of correlation and / or extension), as well as valid codewords on the receiving side. The alphabetical index of the cryptosystem without reducing the cryptographic strength of the system as a whole ensures their practical application and use in the protocols of Internet resources and information and communication systems in the conditions of post-quantum cryptography.

References

1.*Report on Post-Quantum Cryptography*, available at: www.nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf.

2.The Information Technology Laboratory, *Security requirements for cryptographic modules*, available at: https://csrc.nist.gov/publications/fips/fips 140-2/fips1402.pdf (accessed 1 December 2017).

3.Grischuk, R.V. and Danik, Yu.G. (2016), "*Osnovy kiberbezpeky*" [*Basics of Cybersecurity*], ZhNAEU, Zhytomyr, 636 p.

4.Hryshchuk, R., Yevseiev, S. and Shmatko, A. (2018), *Construction methodology of information security system of banking information in automated banking systems: monograph*, PremierPublishing s.r.o., Vienna, 284 p., https://doi.org/0.29013/R.HRYSHCHUK_S.YEVSEIEV_A.SHMATKO.CMISSBIABS.284.2018.

5.Dinh, Hang, Moore, Cristopher and Russell, Alexander (2011), *McEliece and Niederreiter Cryptosystems that Resist Quantum Fourier Sampling Attacks*, available at: https://dl.acm.org/citation.cfm?id=2033093 (accessed 1 September 2018).

6.Baldi, Marco, Bianchi, Marco, Chiaraluce, Franco, Rosenthal, Joachim and Schipani, Davide (2011), *Enhanced public key security for the McEliece cryptosystem*, available at: https://arxiv.org/abs/1108.2462 (accessed 1 September 2018).

7.Guangzhi Zhang and Shaobin Cai (2017), S*ecure error-correcting (SEC) schemes for network coding through McEliece cryptosystem*, available at: https://link.springer.com/article/10.1007/s10586-017-1294-5.

8.Guangzhi Zhang and Shaobin Cai (2017), *Universal secure error-correcting (SEC) schemes for network coding via McEliece cryptosystem based on QC-LDPC codes*, available at: https://link.springer.com/article/10.1007 /s10586-017-1354-x.

9.Rossi, M'elissa, Hamburg, Mike, Hutter, Michael and Marson, Mark E. (2017), *A Side-Channel Assisted Cryptanalytic Attack Against QcBits*, available at: https://link.springer.com/chapter/10.1007/978-3-319-66787-4_1 (Accessed 1 September 2019).

10. Dudikevich, V.B., Kuznetsov, O.O. and Tomashevsky, B.P. (2010), "Krypto-kodovyy zakhys tinformatsiyi z nedviykovym rivnovahovym koduvannyam" [Crypto-code protection of information with non-binary equilibrium encoding], *Modern information protection*, No. 2, pp. 14-23.

11. Dudikevich, V.B., Kuznetsov, O.O. and Tomashevsky, B.P. (2010), "Metod nedviykovoho rivnovahovoho koduvannya" [Non-dual equilibrium coding method], *Modern information protection*, No. 3, pp. 57-68.

12. Morozov, Kirill, Roy, ParthaSarathi and Sakurai, Kouichi (2017), *On unconditionally binding code-based commitment schemes*, available at: https://dl.acm.org/citation.cfm?id=3022327&dl=ACM&coll=DL (accessed 1 September 2019).

13. Marquez-Corbella, Irene and Tillich, Jean-Pierre (2016), Using Reed-Solomon codes in the (U | U + V) construction and an application to cryptography, *IEEE International Symposium on Information*. https://doi.org/:10.1109/ISIT.2016.7541435.

14. Rossi, M'elissa, Hamburg, Mike, Hutter, Michael and Marson, Mark E. (2017), *A Side-Channel Assisted Cryptanalytic Attack Against QcBits*, available at: https://link.springer.com/chapter/10.1007/978-3-319-66787-4_1 (accessed 1 September 2019).

15. Almeida, Paulo and Napp, Diego (2018), *A new class of convolutional codes and its use in the McEliece Cryptosystem*, available at: https://www.researchgate.net/publication/324745076_A_new_class_of_convolutional_codes_and_its_use_in_the_McEliece_Cryptosystem (accessed on September 1, 2019).

16. Kapshikar, Upendra and Mahalanobis, Ayan (2018), *A Quantum-Secure Niederreiter Cryptosystem using Quasi-Cyclic Codes*, available at: https://www.researchgate.net/publication/327660637_A_Quantum-Secure_Niederreiter_Cryptosystem_using_Quasi-Cyclic_Codes (accessed 1 September 2019).

17. Cho, JooYeon, Griesser, Helmut and Rafique, Danish (2017), *A McEliece-Based Key Exchange Protocol for Optical Communication Systems*, available at: https://link.springer.com/chapter/10.1007%2F978-3-319-59265-7_8 (accessed 1 September 2019).

18. Evseev, S.P., Rzaev, Kh.N. and Tsyganenko, A.S. (2016), "Analiz programnoy realizatsii pryamogo i obratnogo preobrazovaniya po metodu nedvoichnogo ravnovesnogo kodirovaniya" [Analysis of the software implementation of direct and inverse transformation using the method of non-binary equilibrium coding], *Bezpeka Informatsii*, Vol. 22, No. 2, pp. 196-203.

19. Sidel'nikov, V.M. (2002), "Kriptografija i teorija kodirovanija" [Cryptography and coding theory], *Materialy konferencii "Moskovskij universitet i razvitie kriptografii v Rossii"*, MGU, Moscow, pp. 1-22.

20. Rukhin, A. and Soto, J. (2000), *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, NIST Special Publication 800-22, 09.2000.

Список літератури

1.Report on Post-Quantum Cryptography [Electronic resource]. – Available at: http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR. 8105.pdf.

2.The Information Technology Laboratory. Security requirements for cryptographic modules [Electronic resource]. – Available at: https://csrc.nist.gov/publications/fips/fips 140-2/fips1402.pdf (accessed 1 December 2017).

3.Грищук Р.В. Основи кібербезпеки / Р.В. Грищук, Ю.Г. Даник. – Житомир: ЖНАЕУ, 2016. – 636 с.

4.Hryshchuk R. Construction methodology of information security system of banking information in automated banking systems: monograph / R. Hryshchuk, S. Yevseiev, A. Shmatko. – Vienna: PremierPublishing s.r.o. – 2018. – 284 p. https://doi.org/0.29013/R.HRYSHCHUK_S.YEVSEIEV_A.SHMATKO.CMISSBIABS.284.2018.

5.Hang Dinh. McEliece and Niederreiter Cryptosystems that Resist Quantum Fourier Sampling Attacks [Electronic resource] / Hang Dinh, Cristopher Moore, Alexander Russell. – Available at: https://dl.acm.org/citation.cfm?id=2033093 (accessed 1 September 2018).

6.Enhanced public key security for the McEliece cryptosystem [Electronic resource] / Marco Baldi, Marco Bianchi, Franco Chiaraluce, Joachim Rosenthal, Davide Schipani. – Available at: https://arxiv.org/abs/1108.2462 (accessed 1 September 2018).

7.Guangzhi Zhang. Secure error-correcting (SEC) schemes for network coding through McEliece cryptosystem [Electronic resource] / Guangzhi Zhang, Shaobin Cai. – Available at: https://link.springer.com/article/10.1007/s10586-017-1294-5.

8.Guangzhi Zhang. Universal secure error-correcting (SEC) schemes for network coding via McEliece cryptosystem based on QC-LDPC codes [Electronic resource] / Guangzhi Zhang, Shaobin Cai. – Available at: https://link.springer.com/article/10.1007/s10586-017-1354-x.

9.A Side-Channel Assisted Cryptanalytic Attack Against QcBits [Electronic resource] / M'elissa Rossi, Mike Hamburg, Michael Hutter, Mark E. Marson. – Available at: https://link.springer.com/chapter/10.1007/978-3-319-66787-4_1 (accessed 1 September 2019).

10. Дудикевич В.Б. Крипто-кодовий захист інформації з недвійковим рівноваговим кодуванням / В.Б. Дудикевич, О.О. Кузнєцов, Б.П. Томашевський // Сучасний захист інформації. – 2010. – № 2. – С. 14-23.

11. Дудикевич В.Б. Метод недвійкового рівноважового кодування / В.Б. Дудикевич, О.О. Кузнєцов, Б.П. Томашевський // Сучасний захист інформації. – 2010. – № 3. – С. 57-68.

12. Морозов Кирилл. О безоговорочно обязательных схемах обязательств на основе кода [Электронный ресурс] / Кирилл Морозов, Партха Саратхи Рой, Куичи Сакурай. – Режим доступа: https://dl.acm.org/citation.cfm?id =3022327&dl=ACM&coll=DL (accessed 1 September 2019).

13. Marquez-Corbella Irene. Using Reed-Solomon codes in the (U | U + V) construction and an application to cryptography / Irene Marquez-Corbella, Jean-Pierre Tillich // IEEE International Symposium on Information. https://doi.org/10.1109/ISIT.2016.7541435.

14. A Side-Channel Assisted Cryptanalytic Attack Against QcBits [Electronic resource] / M'elissa Rossi, Mike Hamburg, Michael Hutter, Mark E. Marson. – Available at: https://link.springer.com/chapter/10.1007/978-3-319-66787-4_1 (accessed 1 September 2019).

15. Almeida Paulo. A new class of convolutional codes and its use in the McEliece Cryptosystem. [Electronic resource] / Paulo Almeida, Diego Napp. – Available at: https://www.researchgate.net/publication/324745076_A_new_class_of_convolutional_codes_and_its_use_in_the_McEliece_Cryptosystem (accessed 1 September 2019).

16. Kapshikar Upendra. A Quantum-Secure Niederreiter Cryptosystem using Quasi-Cyclic Codes [Electronic resource] / Upendra Kapshikar, Ayan Mahalanobis. – Available at: https://www.researchgate.net/ publication/327660637_A_Quantum-Secure_Niederreiter_ Cryptosystem_using_Quasi-Cyclic_Codes (accessed 1 September 2019).

17. Joo Yeon Cho. A McEliece-Based Key Exchange Protocol for Optical Communication Systems [Electronic resource] / Joo Yeon Cho, Helmut Griesser, Danish Rafique. – Available at: https://link.springer.com/chapter/10.1007%2F978-3-319-59265-7_8 (accessed 1 September 2019).

18. Евсеев С. Анализ программной реализации прямого и обратного преобразования по методу недвоичного равновесного кодирования / С. Евсеев, Х. Рзаев, А. Цыганенко // Безпека інформації. – 2016. – Том 22, № 2. – С. 196-203.

19. Сидельников В.М. Криптография и теория кодирования / В.М. Сидельников // Материалы конференции "Московский университет и развитие криптографии в России". – М.: МГУ, 2002. – С. 1-22.

20. Rukhin A. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications / A. Rukhin, J. Soto. – NIST Special Publication. – 2000.

Received by Editorial Board 10.10.2019
Signed for printing 19.11.2019

Відомості про автора:

Євсеєв Сергій Петрович
доктор технічних наук старший науковий співробітник
завідувач кафедри
Харківського національного економічного
університету ім. С. Кузнеця,
Харків, Україна
https://orcid.org/0000-0003-1647-6444

Information about the author:

Serhii Yevseiev
Doctor of Technical Sciences Senior
Research Head of the Department
of Simon Kuznets Kharkiv National
University of Economics,
Kharkiv, Ukraine
https://orcid.org/0000-0003-1647-6444

ДОСЛІДЖЕННЯ КРИТЕРІЮ МОДИФІКОВАНОЇ НЕСИМЕТРИЧНОЇ КРИПТО-КОДОВОЇ КОНСТРУКЦІЇ МАК-ЕЛІСА НА ПОДОВЖЕНИХ ЕЛІПТИЧНИХ КОДАХ

С.П. Євсеєв

Розвиток обчислювальної техніки в епоху постквантовой криптографії висуває нові вимоги до криптографічних механізмів для надання базових послуг безпеки. Поява повномасштабного квантового комп'ютера ставить під сумнів криптографічну силу криптосистем, заснованих на симетричній криптографії і криптографії з відкритим ключем. Однією з багатообіцяючих областей, на думку американських експертів NIST, є використання кріпто-кодових конструкцій Мак-Еліса або Нідеррейтера. Конструкція дозволяє за допомогою одного інтегрованого механізму забезпечити основні вимоги до криптосистем – криптографічний стабільність, швидкість криптоперетворень і, крім того, – надійність, засновану на використанні завадостійкого кодування. Однак їх використання ускладнене через великий обсяг потужності алфавіту і можливості злому на основі атаки Сидельникова. У статті пропонується використовувати нециклічні шумостійкі коди на еліптичних кривих в модифікованій криптосистемі Мак-Еліса, які не схильні до атаки Сидельникова. Досліджено основні критерії побудови модифікованого кріптокода на основі схеми Мак-Еліса на подовжених еліптичних кодах. Пропонується знизити енергоємність в пропонованому проекті кріптокода за рахунок зменшення потужності поля Галуа, забезпечуючи при цьому рівень криптографічної стабільності модифікованої криптосистеми в цілому з її програмною реалізацією. Для зменшення потужності поля пропонується використовувати модифіковані еліптичні коди, що дозволяє зменшити потужність поля в 2 рази. Проведена порівняльна оцінка продуктивності криптовалюти в пропонованому проекті криптосистеми. Результати досліджень статистичної стійкості на основі пакету NIST STS 822 підтверджують криптографічну стійкість пропонованої криптосистеми на модифікованих подовжених еліптичних кодах.

Ключові слова: *крипто-кодова система Мак-Еліса, модифіковані (подовжені) еліптичні коди.*

ИССЛЕДОВАНИЕ КРИТЕРИЯ МОДИФИЦИРОВАННОЙ НЕСИММЕТРИЧНОЙ КРИПТО-КОДОВОЙ КОНСТРУКЦИИ МАК-ЭЛИСА НА УДЛИНЕННЫХ ЭЛЛИПТИЧЕСКИХ КОДАХ

С.П. Евсеев

Развитие вычислительной техники в эпоху постквантовой криптографии выдвигает новые требования к криптографическим механизмам для предоставления базовых услуг безопасности. Появление полномасштабного квантового компьютера ставит под сомнение криптографическую силу криптосистем, основанных на симметричной криптографии и криптографии с открытым ключом. Одной из многообещающих областей, по мнению американских экспертов NIST, является использование криптокодовых конструкций Мак-Элиса или Нидеррейтера. Конструкция позволяет с помощью одного интегрированного механизма обеспечить основные требования к криптосистемам – криптографическую стабильность, скорость криптопреобразования и, кроме того, – надежность, основанную на использовании помехоустойчивого кодирования. Однако их использование затруднено из-за большого объема мощности алфавита и возможности взлома на основе атаки Сидельникова. В статье предлагается использовать нециклические шумоустойчивые коды на эллиптических кривых в модифицированной криптосистеме Мак-Элиса, которые не подвержены атаке Сидельникова. Исследованы основные критерии построения модифицированного криптокода на основе схемы Мак-Элиса на удлиненных эллиптических кодах. Предлагается снизить энергоемкость в предлагаемом проекте криптокода за счет уменьшения мощности поля Галуа, обеспечивая при этом уровень криптографической стабильности модифицированной криптосистемы в целом с ее программной реализацией. Для уменьшения мощности поля предлагается использовать модифицированные эллиптические коды, что позволяет уменьшить мощность поля в 2 раза. Проведена сравнительная оценка производительности криптовалюты в предлагаемом проекте криптосистемы. Результаты исследований статистической устойчивости на основе пакета NIST STS 822 подтверждают криптографическую стойкость предлагаемой криптосистемы на модифицированных удлиненных эллиптических кодах.

Ключевые слова: *крипто-кодовая система Мак-Элиса, модифицированные (расширенные) эллиптические коды.*