Evaluation of Cryptographic Strength and Energy Intensity of Design of Modified Crypto-Code Structure of McEliece with Modified Elliptic Codes

Serhii Yevseiev [1], Olha Korol [2], Olga Veselska [3], Serhii Pohasii [4],Vladyslav Khvostenko [5]

[1,2,4,5] Simon Kuznets Kharkiv National University of Economics, Nauky ave., 9-A, Kharkiv, 61166, Ukraine
[3] Akademia Techniczno-Humanistyczna, ul. Willowa 2, Bielsku-Białej, 43309, Poland

Abstract

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 cryptoconversion and besides - 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 elliptic codes, which allows to reduce the field power by 2 times. A comparative assessment of the performance of cryptosystems 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 elliptic codes. It is proposed to use the method of evaluating the cryptographic strength of various cryptosystems based on the entropy approach.

Keywords

Asymmetric McEliece Crypto-Code System, Crypto-Code Construction on Algebro-geometric Codes, Modified (extended) Elliptic Codes, Confidentiality, Integrity.

1. 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

III International Scientific And Practical Conference "Information Security And Information Technologies", September 13–19, 2021, Odesa, Ukraine

EMAIL: serhii.yevseiev@hneu.net (A. 1); olha.korol@hneu.net (A. 2); oveselska@ath.bielsko.pl (A. 3); spogasiy1978@gmail.com (A. 4); vladyslav.khvostenko@gmail.com (A. 5)
ORCID: 0000-0003-1647-6444 (A. 1); 0000-0002-8733-9984 (A. 2); 0000-0002-4914-2187 (A. 3); 0000-0002-4540-3693 (A. 4); 0000-0000-0000-1234 (A. 5)

CEUR Workshop Proceedings (CEUR-WS.org)

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's 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. The construction allows one integrated mechanism to provide the basic requirements for cryptosystems – cryptographic stability, speed of cryptoconversion Pand besides – reliability based on the use of noise-resistant coding.

The analysis showed that for the provision of basic security services, crypto-code constructions are usually used based on the McEliece and Niederreiter schemes. To ensure the level of cryptographic strength in post-quantum cryptography, it is necessary to use the power of the alphabet in a field of 210-213 degrees, which is a significant drawback of their practical application [4]. Even at the current level of computer technology, this is a rather difficult task.

The second drawback is the hacking attack on the McEliece scheme based on linear-fractional transformations and the property of triply transitivity of the automorphism groups of the generalized Reed-Solomon code, proposed in the work of professor Sidelnikov from Moscow State University. The essence of which is to find the elements of the generating matrix and remove the action of masking matrices [4].

The orthogonality of the matrices, which is generative and test, allows us to consider the effectiveness of the attack on the Niederreiter scheme. A promising way to eliminate the identified patterns Sidelnikov proposes to use cascade or algebraic geometry codes – codes built based on the algebra of the theory of noise-resistant coding and geometric parameters of the curve, in particular elliptic curves.

The algebraic-geometric code uses the mathematical apparatus of noise-resistant coding and the parameters of the spatial curve. This allows us to provide resistance to Sidelnikov’s attack and proper (n, k, d) parameters of the error-correcting code, which, under equal conditions of length n, provides bigger values of the d and k parameters (allows to transmit more characters in open text and correct more errors)

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 elliptic codes, which allows to reduce the field power by 2 times. A comparative assessment of the performance of cryptosystems 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 elliptic codes.

2. Analysis of Recent Studies and Publications

The main advantage of symmetric and asymmetric Crypto-Code Systems (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 29 – 212 and cryptostability 230 – 235 group operations when constructed over the field GF(210).

Figure 1 shows the classification of crypto-code structures and the provision of basic security services.

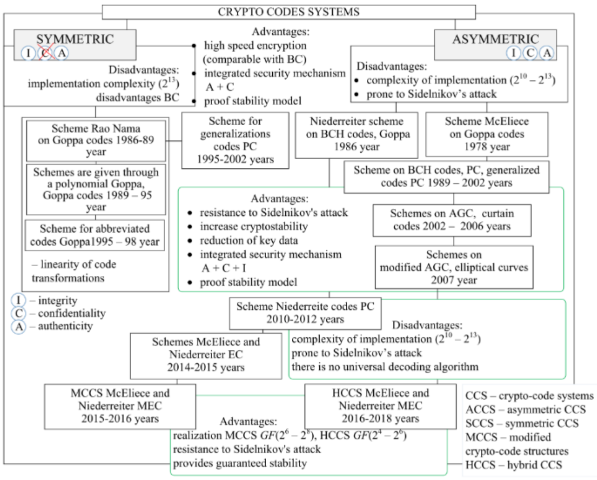

CRYPTO CODES SYSTEMS
SYMMETRIC
I C A
Disadvantages:
implementation complexity (2^13)
disadvantages BC
Advantages:
high speed encryption (comparable with BC)
integrated security mechanism A + C
proof stability model
ASYMMETRIC
I C A
Disadvantages:
complexity of implementation (2^10 – 2^13)
prone to Sidelnikov's attack
Scheme Rao Nama on Goppa codes 1986-89 year
Schemes are given through a polynomial Goppa, Goppa codes 1989 – 95 year
Scheme for abbreviated codes Goppa1995 – 98 year
– linearity of code transformations
Scheme for generalizations codes PC 1995-2002 years
Niederreiter scheme on BCH codes, Goppa 1986 year
Scheme McEliece on Goppa codes 1978 year
Scheme on BCH codes, PC, generalized codes PC 1989 – 2002 years
Advantages:
resistance to Sidelnikov's attack
increase cryptostability
reduction of key data
integrated security mechanism A + C + I
proof stability model
Schemes on AGC, curtain codes 2002 – 2006 years
Schemes on modified AGC, elliptical curves 2007 year
I – integrity
C – confidentiality
A – authenticity
Scheme Niederreite codes PC 2010-2012 years
Disadvantages:
complexity of implementation (2^10 – 2^13)
prone to Sidelnikov's attack
there is no universal decoding algorithm
Schemes McEliece and Niederreiter EC 2014-2015 years
MCCS McEliece and Niederreiter MEC 2015-2016 years
HCCS McEliece and Niederreiter MEC 2016-2018 years
Advantages:
realization MCCS GF(2^6 – 2^8), HCCS GF(2^4 – 2^6)
resistance to Sidelnikov's attack
provides guaranteed stability
CCS – crypto-code systems
ACCS – asymmetric CCS
SCCS – symmetric CCS
MCCS – modified crypto-code structures
HCCS – hybrid CCS

Figure 1: Classification of crypto-code constructions

The main advantage of which is the provision of cryptographic stability, efficiency and reliability in the transmission of information in the post-quantum period.

Table 1 shows the results of comparative studies of the effectiveness of cryptographic information security methods at a fixed level of stability.

Table 1
Results of comparative researches of efficiency of cryptographic methods of information security at the fixed stability level

Methods of cryptographic transformatio n	Security model	Key length [bits	Speed of cryptogra phic 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	$0{,}5·10^6$ (128), $2·10^6$ (256)	$10^6 – 10^8$	Error monitorin g, increasing reliability

In Table 1, there are presented values: average (the complexity of cryptanalysis is the best-known algorithm of at least 2128 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 2512 operations) [4].

Hence, as it follows from the above results of the comparative analysis (Table 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.

In [5–8], the authors propose McEliece crypto-code systems based on various codes. In [9–11], an equilibrium coding method based on m-folded Reed-Solomon codes were proposed; however, the disadvantage is the lack of a practical algorithm for decoding the syndrome on the receiving side and the possibility of hacking based on a rearranged decoder. In [13], there is proposed a modification of the Reed-Solomon codes, which exceeds the Guruswami-Sudan decoding radius 1 – √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 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 the following papers [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. 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 to provide integrated requirements for both reliability and security [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, 20, 21] and the required level of cryptographic strength. But there are remained unresolved questions of practical implementation with the necessary power of the GF(210–213) 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 soon. 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]. Besides, 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). **Fig. 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.

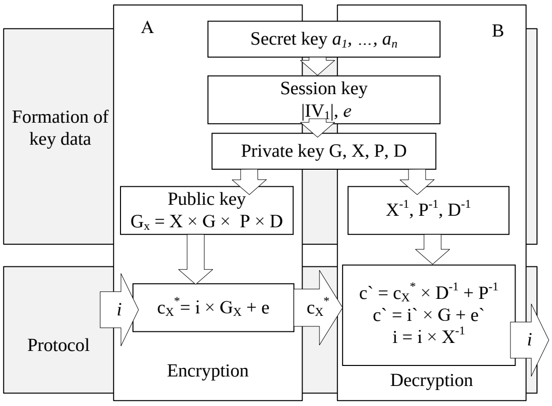


Figure 2: Exchange protocol based on a modified McEliece crypto-code system on modified (shortened) elliptic codes (secret (closed) key – matrices X, P, and D; X – non-degenerate k×k matrix over GF(q); P – permutational n×n matrix over GF(q); D – diagonal n×n matrix over GF(q),\; G^{EC}– generating k×n matrix of elliptic code over GF(q); vector IV_1 (sets of fixed positional sets of clear text {MF})

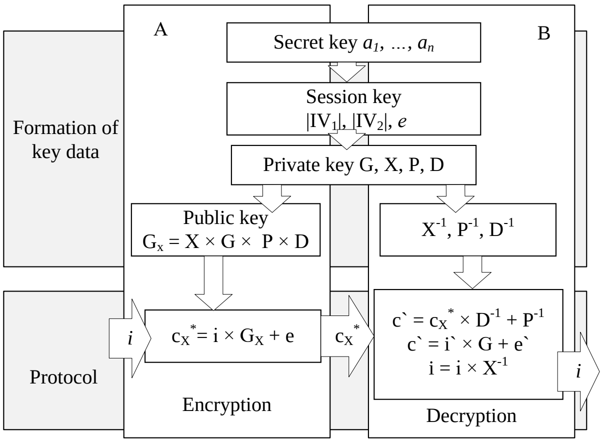


Figure 3: Exchange protocol based on a modified McEliece crypto-code system on modified (extended) elliptic codes (secret (closed) key – matrices X, P, and D; X – non-degenerate k×k matrix over GF(q); P – permutational n×n matrix over GF(q); D – diagonal n×n matrix over GF(q); G^{EC}– generating k×n matrix of elliptic code over GF(q); vector IV_1 (sets of fixed posi-tional sets of clear text {MF}); vector IV_2 (defines the position for adding plaintext characters)

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

Table 2. The main (n, k, d) properties of MEC.

Table 2

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

Property	Shortened MEC	Extended MEC
(n, k, d) code parameters constructed by displaying the view ϕ:X→Pk-1	$n=2\sqrt{q}+q+1-x$, k ≥ α – x, d ≥ n – α, α=3×degF, k + d ≥n	$n=2\sqrt{q}+q+1-x+x_1$, k ≥ α – x + x1, d ≥ n – α, α = 3 × degF
(n, k, d) code parameters constructed by displaying the view ϕ:X→Pr-1	$n=2\sqrt{q}+q+1-x$, k ≥ n – α, d ≥ α, α = 3×degF, k + d ≥ n	$n=2\sqrt{q}+q+1-x+x_1$, k ≥ n – α, d ≥ α, α = 3 × degF

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=(α–x)×m*	*l_I = (α – x + x_1) × 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	$R=(\alpha-x)/\left(2\sqrt{q}+q+1-x\right)$	$R=(\alpha-x+x_1)/\left(2\sqrt{q}+q+1-x+x_1\right)$

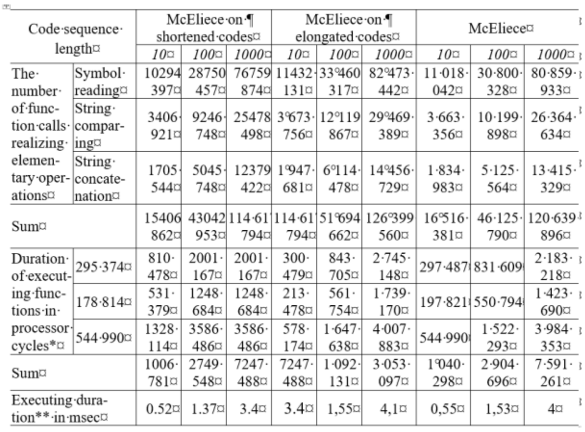
The proposed McEliece MCCS can reduce the power of the alphabet, which al-lows them to be implemented in practice, while ensuring the required level of crypto-graphic strength due to the introduction of additional initialization vectors: IV_1 – defines shortening characters from a code word (cryptograms),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

3. 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.

Table 4.

Research results according to the length of the code sequence in McEliece ACCS on modified elliptic codes in dependency of CPU cycles number.



Code sequence length		McEliece on shortened codes			McEliece on elongated codes			McEliece		
		10	*100*	*1000*	*10*	*100*	*1000*	*10*	*100*	*1000*
The number of func-tion calls realizing elemen-tary oper-ations	Symbol reading	10294 397	28750 457	76759 874	11432 131	33 460 317	82 473 442	11 018 042	30 800 328	80 859 933
	String compar-ing	3406 921	9246 748	25478 498	3 673 756	12 119 867	29 469 389	3 663 356	10 199 898	26 364 634
	String concate-nation	1705 544	5045 748	12379 422	1 947 681	6 114 478	14 456 729	1 834 983	5 125 564	13 415 329
Sum		15406 862	43042 953	114 61 794	114 61 794	51 694 662	126 399 560	16 516 381	46 125 790	120 639 896
Duration of execut-ing func-tions in processor cycles*	295 374	810 478	2001 167	2001 167	300 479	843 705	2 745 148	297 487	831 609	2 183 218
	178 814	531 379	1248 684	1248 684	213 478	561 754	1 739 170	197 821	550 794	1 423 690
	544 990	1328 114	3586 486	3586 486	578 174	1 647 638	4 007 883	544 990	1 522 293	3 984 353
Sum		1006 781	2749 548	7247 488	7247 488	1 092 131	3 053 097	1 040 298	2 904 696	7 591 261
Executing dura-tion** in msec		0.52	1.37	3.4	3.4	1,55	4,1	0,55	1,53	4

Notes:* duration of 1000 operations in processor cycles: reading a character – 27 cycles, com-paring strings – 54 cycles, string concatenation - 297 cycles.

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

Algorithm complexity is calculated from expression [4]:

Per = Utl·CPU_clock/Rate,

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

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

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 (CBP)
McEliece ACCS	100	46 125 790	56	61,5
	1000	120 639 896	56	62,0
	100	51 694 662	56	61,7

McEliece at shortened MEC	1000	126 399 560	56	62,2
McEliece at shortened MEC	100	46 125 790	56	61.5
	1000	120 639 896	56	62.0

Tab. 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.

Analysis of Tables 4 and 5 shows that the use of modified (elongated) elliptic codes allows to save the volume of transmitted data in McEliece a crypto-code sys-tem, but at the same time it provides the required level of cryptographic resistance during the implementation over the smaller field GF(2^6 – 2^8) through the use of en-tropy of initialization vector.

4. Study of the Properties of the McEliece ACCS on the EC and the Modified McEliece on MEC

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 – the length of the public key (in bits);
- l_{K+} – the length of the private key (in bits);
- l_s – the length of the code (in bits);
- O_K - the complexity of the formation of the code (number of group operations);
- O_{SK} – the difficulty of decoding the cryptogram (the number of group operations);
- O_{K+} – the 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 infor-mation sequence (in bits) arriving at the input of the MACCS with the algebraic (n, k, d)-code over GF(2m) (where m − the power of the extended Galois field), we use the expressions:

- $l_I = k \times m$, for ACCS on the EC;
- $l_I = 1/2k \times m$, for MCCS on truncated MEC;
- $l_I = k \times m$, for MACCS on elongated MEC.

In Tab. 6 and in Figure 4 we show the cryptogram formation complexity from the power of the field, where code rate (R) stands for the relative speed of coding R=k/n, the encoder assigns to each message of *k* digits a longer message of *n* digits called a codeword.

From the provided data it can be seen that the cryptogram formation complexity for the chosen power of the GF 26 on the truncated and elongated codes is much lower (by 5 times and more) than in the original realization of MACCS to the EC. Respectively, the speed of the formation of the cryptogram will significantly increase.

- In order to estimate the length of the cryptogram (in bits), we use the expressions:
- ls = n × m, for ACCS on the EC;
- l_s=(2√q+q+1-1/2k)×m, for MCCS on truncated MEC;
- l_s=(2√q+q+1-1/2k+1/2k)×m, for MCCS on elongated MEC.

Table 4.

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

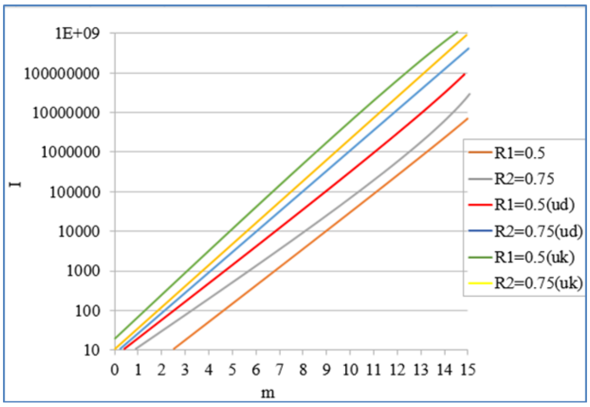


Figure 2: Dependence of the complexity of forming a cryptogram in various GF(2^m)

In Tab. 7 and Figure 5 we show the dependence of the decoding complexity of the cryptogram on the field strength.

Table 5.

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	17564512 7	19364892 4	1e+09	1e+09	1e+09	1e+09

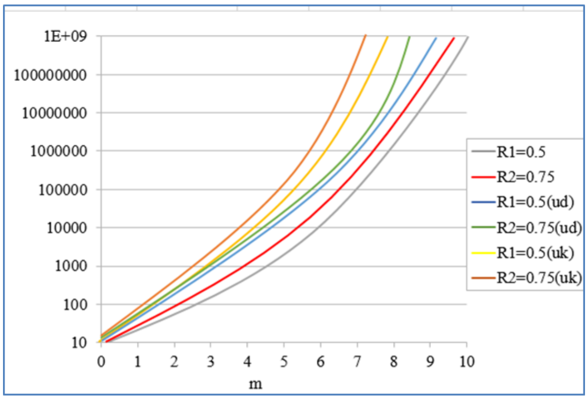


Figure. 3: Dependence of the decryption complexity of the cryptogram in various GF(2^m)

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:

- $l_K = k \times n \times m$, for ACCS on the EC:;
- $l_s = \frac{1}{2k} \times (2\sqrt{q} + q + 1 - 1/2k) \times m,$ for MCCS on truncated MEC;
- $l_s = \frac{1}{2k} \times (2\sqrt{q} + q + 1 - \frac{1}{2k} + \frac{1}{2k}) \times m,$ 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:

- $l_{K+} = n^2 \times k^2 \times m,$ for ACCS on the EC;
- $l_{Ks} = \frac{1}{2k} [\log_2(2\sqrt{q} + q + 1)],$ for MCCS on truncated MEC;
- $l_{Ks} = (\frac{1}{2k} - \frac{1}{2k}) [\log_2(2\sqrt{q} + q + 1)],$ for MCCS on elongated MEC.

In Tab. 8 and Figure 5 there are shown the dependency of the breaking complexity based on the permutation decoding on the field strength.

Table 6.

Dependence of Breaking 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

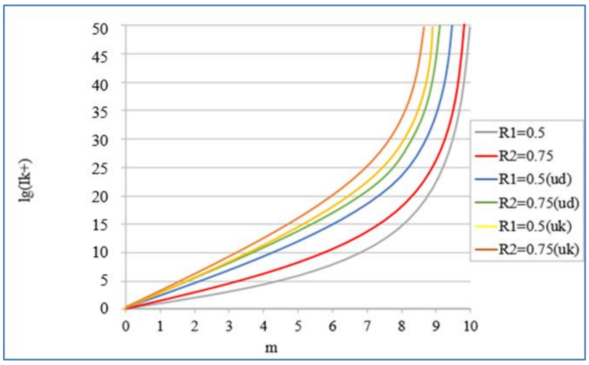


Figure 4: Dependence of breaking complexity in various GF(2^m)

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

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

- for ACCS on the EC:

when implementing systematic coding:

$$O_K = (r+1) \times n,$$

for non-systematic coding:

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

- for MCCS on truncated MEC:

when implementing systematic coding:

$$O_k = (r+1) \times (2\sqrt{q} + q + 1 - 1/2k),$$

for non-systematic coding:

$$O_k = (k+1) \times (2\sqrt{q} + q + 1 - 1/2k);$$

- for MCCS on elongated MEC:

when implementing systematic coding:

$$O_k = (r+1) \times (2\sqrt{q} + q + 1 - \frac{1}{2k} + \frac{1}{2k}),$$

for non-systematic:

$$O_k = (k+1) \times (2\sqrt{q} + q + 1 - \frac{1}{2k} + \frac{1}{2k}).$$

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

- for ACCS on EC:

$$OSK = 2\times n^2+k^2+4t^2 + (t^2 + t - 2)^2/4,$$

- for MCCS on truncated MEC:

$$O_{SK} = 2(2\sqrt{q} + q + 1 - \frac{1}{2k})^2 - \frac{1}{2k^2} + 4t^2 + \frac{(t+t-2)^2}{4}.$$

- for MCCS on elongated MEC:

$$O_{SK} = 2(2\sqrt{q} + q + 1 - \frac{1}{2k} + 1/2k) \quad - k^2 + 4t^2 + \frac{(t+t-2)^2}{4}$$

The complexity of the task of the analysis (decoding) solution is set by expressions:

- for ACCS on EC:

$$O_{K+} = N_{cov} \times \mathrm{n} \times \mathrm{r},$$

where

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

$$t=[(d–1)/2]$$

The potential strength of the cryptosystem is defined by size ρ×t, and noise stability of system – (1 – ρ) × t.

- For MCCS on truncated codes:

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

- For MCCS on elongated codes:

$$O_{MACCS} = N \times (2\sqrt{q} + q + 1 - \frac{1}{2k} + 1/2k) \times r.$$

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

Table 7

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

lg(I_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

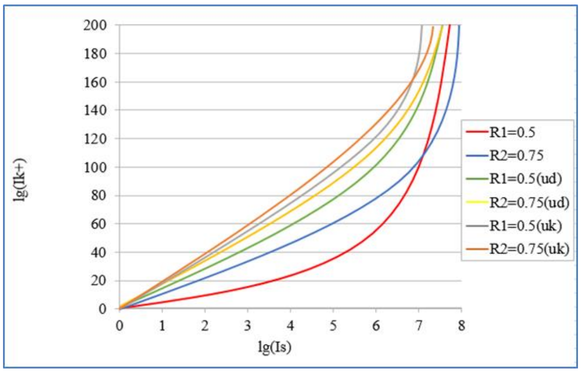


Figure 7: Summary diagram of breaking complexity and encoding complexity for different speeds of the EC (MEC)

Dependences of the volume of open key data for various indicators of firmness are presented in Table 10 and Figure 8.

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

Table 10

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

$\lg(I_{k+})$	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

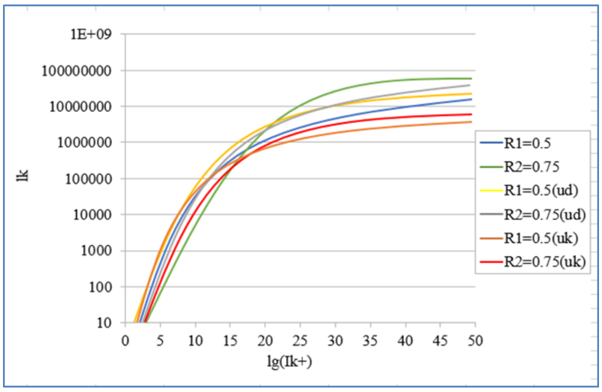


Figure 8: Dependencies of the volume of open key data for various indicators of durability.

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

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

The results of studies of the dependence of the software implementation depend-ing on the field power and the parameters of algebra-geometric codes are also pre-sented, as can be seen from Table 11, the use of modified crypto-code constructions provides a 5-fold reduction in energy costs for the software implementation, that allows for their practical implementation

5. 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 experi-mental estimation of how close the crypto-algorithms approximate the generators of the “random” sequences, statistical tests are used. The NIST STS benchmark pack-age for testing random or pseudorandom number generators is one of the approach-es to realizing the task of evaluating the statistical security of cryptographic primi-tives.

The use of this package makes it possible to conclude 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 [22]. 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 by the event that fulfills the following rules:

1. The rule #1. All q tests were executed, (q =$\overline{(1,189)}$), and if the value of the coefficient rj is inside the confidence interval [0.96, 1.00];
2. The rule #2. All q tests were executed, (q = 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 experimental research about the properties of the developed code cryptosystems the program is developed to realize the offered means of protection of the information.

The following parameters have been selected during the tests:

- length of the test sequence n = 10^6 bits;
- number of tested sequences m = 100. Thus, the volume of the test sample was N = 10^6x100 = 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 Table 12.

As it can be seen from the presented data in Table 12 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.

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.

Table 8
Results of experimental testing

Cryptosystems	The number of tests in which the testing passed more than 99% of the sequences	The number of tests in which tests were over 96% of the sequences	The number of tests in which testing was less than 96% of the sequences
CCS McEliece	149 (78,83%)	189 (100%)	0 (0%)
MCCS McEliece on shortened MEC	151 (79,89%)	189 (100%)	0 (0%)
MCCS McEliece on extended MEC	152 (80,42%)	189 (100%)	0 (0%)
Keccak (SHA-3)	134 (71,9%)	187 (98,9)	2 (1,05)
ANSI X9.17(3-DES)	124(66%)	62(33%)	3(1%)
BBS	132(70%)	55(29%)	2(1%)
SHA-1	134(71%)	54(28%)	1(1%)
Generator based on elliptic curves	146 (77,2%)	188 (100 %)	1(1%)

6. Analysis of Cryptographic Algorithms Based on the Entropy Approach

The proposed express analysis makes it possible, without significant computational and energy costs, at the intuitive level, to compare not only the resistance of various crypto-algorithms (cryptosystems), but their software implementation. The algorithm of the entropy method for assessing crypto-resistance is shown in Figure 9.

Table 13 gives the results of the study into the stability and software effectiveness of the implementation of block and stream ciphers of varying complexity. We applied DES, 3DES, GOST 28147-2015, Kalina-256, AES-256 as block ciphers. To imple-ment a stream cipher, we used pseudo-random sequence generators of two different types: based on the rule “60” of cellular automata in its classical form, without mod-ifications, and the cryptographically resistant generator SecureRandom from Java crypto-libraries, which is marketed as suitable for cryptographic applications.

Table 13
Results of testing the resistance of crypto-algorithms using an express-method

No.	Cipher	Entropy of the input message	Entropy of the encrypted message	Difference	Percentage of entropy, added by the cipher
1	Cellular automata, the rule “60”	0.5023775 (5.023775)	0.6820179 (6.820179)	0.1796404 (1.796404)	35.7580505
2	Crypto-resistant generator SecureRandom from Java crypto-libraries	0.5023767 (5.023767)	0.7999982 (7.999982)	0.2976215 (2.976215)	59.2426958
3	DES	0.469276	0.812043	0.342767	73.0416642
4	3DES	0.469276	0.812043	0.342767	73.0416642
5	GOST 28147-89	0.469276	0.811348	0.342072	72.8935637
6	Kalina-256	0.469276	0.954519	0.485243	103.4024753
7	AES-256	0.469276	0.95454	0.485264	103.4069503

In Table 13, we calculated the entropy of the input and the encrypted text, differ-ence, as well as the percentage of entropy added to the entropy of plaintext by the cipher itself. An analysis of Table 1 allows us to assess the contribution of the cipher in the total entropy of the encrypted message. As they all were tested under identical conditions, it is possible to judge their relative performance.

The AES-like ciphers (SPN-system, substitution-permutation schemes) are worth mentioning. Both such ciphers, Kalina and AES, made the greatest contribution, larger than 103 %, to the entropy of the plaintext. According to the given results, both ciphers have the best diffusing effect. Approximately the same results were demonstrated by the symmetric block cipher (SBC) GOST 28147-2015: 72.89 % against 73.04 % for DES/3DES. This probably confirms conclusions about the max-imally possible degree of dispersion as a characteristic of the architecture.

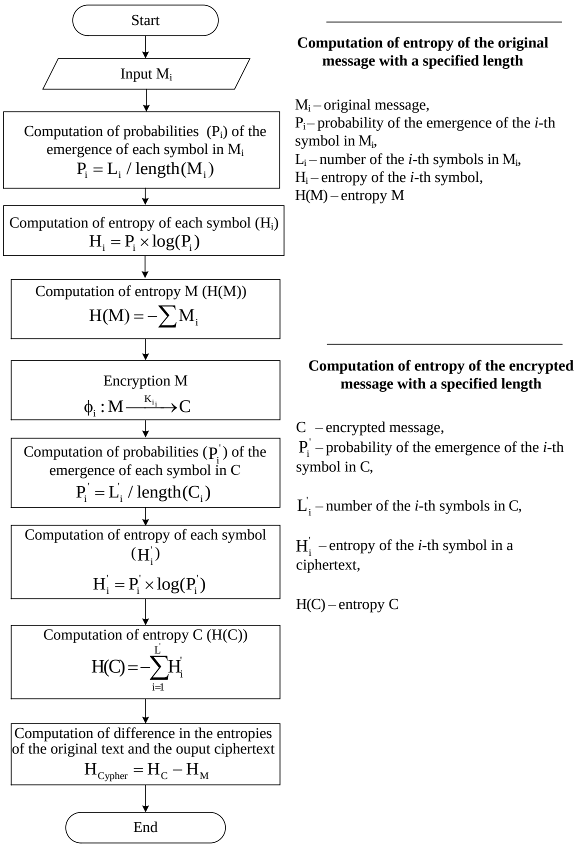

Start
Input M_i
Computation of probabilities (P_i) of the emergence of each symbol in M_i
$P_i = L_i / \text{length}(M_i)$
Computation of entropy of each symbol (H_i)
$H_i = P_i \times \log(P_i)$
Computation of entropy M (H(M))
$H(M) = -\sum M_i$
Encryption M
$\phi_i : M \xrightarrow{K_i} C$
Computation of probabilities (P_i') of the emergence of each symbol in C
$P_i' = L_i' / \text{length}(C_i)$
Computation of entropy of each symbol (H_i')
$H_i' = P_i' \times \log(P_i')$
Computation of entropy C (H(C))
$H(C) = -\sum_{i=1}^{L} H_i'$
Computation of difference in the entropies of the original text and the ouput ciphertext
$H_{Cypher} = H_C - H_M$
End
Computation of entropy of the original message with a specified length
M_i – original message,
P_i – probability of the emergence of the *i*-th symbol in M_i,
L_i – number of the *i*-th symbols in M_i,
H_i – entropy of the *i*-th symbol,
H(M) – entropy M
Computation of entropy of the encrypted message with a specified length
C – encrypted message,
P_i' – probability of the emergence of the *i*-th symbol in C,
L_i' – number of the *i*-th symbols in C,
H_i' – entropy of the *i*-th symbol in a ciphertext,
H(C) – entropy C

Figure 5. Algorithm for testing the cryptosystem for resistance based on the method for the estimation of randomness.

To compare the results, we conducted experiments using stream ciphers based on two different generators with a pseudorandom key sequence. Encryption was per-formed by the rule of addition for modulo two. In the first case, this is a generator based on cellular automata (the rule “60”). This is not a crypto-resistant generator whose sequence does not pass testing for NIST STS 822, while the second one is positioned as the crypto-resistant generator SecureRandom in the Java crypto-library. In both cases, the obtained values for entropy are much smaller than those for classic SBC, which does not allow us to argue about quality encryption with their help. Thus, the presented results suggest that a simple entropy method allows rapid assessment of the quality of ciphers used without referring to expert estimations. Such an express technique is available to anyone with a minimal knowledge of the information theory.

Moreover, in this way, one can evaluate different implementations of ciphers that will make it possible to select the best (optimal) software implementation that matches the terms and requirements of the user. For example, in our computer ex-periments, we used two implementations of the DES algorithm. One of them, given in Table 13 at number 3, demonstrated a 73.04 % increase in entropy after encrypting compared to the original text, another algorithm − 64.4 %. It is obvious that for practical purposes it makes sense to choose the first implementation, since it appears that its scattering characteristics are better. Thus, the express-analysis allows assessment of the quality of implementation of classic (and other) cryptoalgorithms in order to select an optimal crypto library out of many commercially available libraries.

We shall consider the results obtained in terms of maximum cryptographic infor-mation protection. An indicator of such protection is the entropy of the encrypted binary file, given in Table 14.

Table 14

Estimation of maximal cryptographic protection of information.

No.	Cipher	Entropy of the input message	Entropy of the encrypted message	Probability of cryptographic protection, P_c
1	Cellular automata, the rule "60"	0.469276	0.637079949	0.637079949
2	Crypto-resistant generator SecureRandom from Java crypto-libraries	0.469276	0.747287753	0.747287753
3	DES	0.469276	0.812043	0.812043
4	3DES	0.469276	0.812043	0.812043
5	GOST 28147-89	0.469276	0.811348	0.811348
6	Kalina	0.469276	0.954519	0.954519
7	AES-256	0.469276	0.95454	0.95454
8	Perfect cipher		1.000	1.000

It is known that the maximum possible cryptographic protection is provided by the so-called "perfect cipher" by Shannon, which as a result of encryption produces a random number [23,24]. Such a file will have maximum entropy, which in the bina-ry case is equal to unity. We assume that encryption using a given cipher will ensure maximal cryptographic protection; we assume that it equals unity. One can say that the probability of protection using such a cipher is equal to unity. It is natural that imperfect ciphers do not produce such a probability of cryptographic protection. By using such an approach, one can rank all the examined ciphers for the probability of cryptographic protection. This indicator can be employed for various procedures for the assessment of the security of integrated protection systems of different corporate networks, which testifies to its universality.

In Figure 10 there are shown the results of studies of the average entropy of crypto-grams of different BSS of meaningful plaintext with a length of M = 108 bits, with an interval of N = 5 × 106 bits.

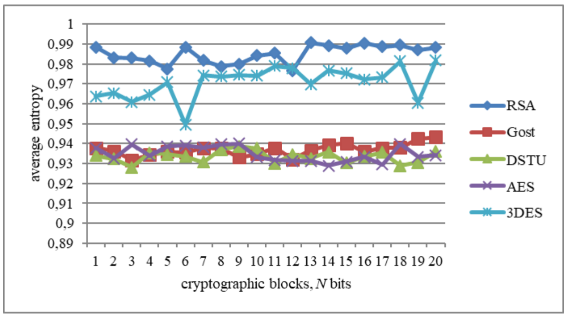


Figure 6. The results of studies of the average entropy of cryptographic blocks

Analysis of Figure 10 practically confirms the possibility of using the express method for the selection of software security mechanisms based on cryptoalgorithms.

7. Conclusions

As a result of the conducted research, it can be concluded that

1. Evaluation by NIST specialists of the computing capabilities of quantum com-puters 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 put forward new requirements for systems for protecting confidential information. At the same time, the use of crypto-code constructions allows us to provide not only the required level of cryptographic stability, but also the reliability of the transmitted information. However, their use in communication devices is associated with significant energy and computation-al costs, which does not allow their practical use. Besides, the proposed Sidelnikov attack does not allow the use of many well-known codes; to counter it, it is pro-posed to use algebraic geometries based on the parameters of elliptic curves.

2. The overall structure of asymmetric crypto-code systems based on the McEliece TCS enabling integrated (with a single device) provision of the required indicators of reliability, efficiency and data security was analyzed. A major shortcoming of ACCS based on the McEliece TCS is a big volume of key data, that constricts their use in different communication system areas (today cryptographic strength on the level of the provable strength model is provided while building ACCS in the Galois field GF(213)). The use of modified (shortened) elliptic (algebraic) codes helps to reduce the volume of key data while maintaining the requirements for cryptographic strength of ACCS. Estimation of the data conversion performance is comparable to the speed of direct and inverse cryptographic conversion of modern BSC, this ensures the cryptographic strength at the level of asymmetric cryptosystems (cryptographic strength is based on the theoretical complexity problem – random code decoding).

3. 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 initializa-tion, 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 infor-mation and communication systems in the conditions of post-quantum cryptog-raphy.

8. References

[1] Report on Post-Quantum Cryptography, http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf, last accessed: 2020/02/19.

[2] Security requirements for cryptographic modules, https://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf, last accessed 2017/12/1.

[3] Grischuk, R.V., Danik, Yu. G.: Basics of Cybersecurity. Zhytomyr: ZhNAEU, p. 636 (2016).

[4] Hryshchuk, R., Yevseiev, S., Shmatko A.: Construction methodology of information secu-rity system of banking information in automated banking systems. Monograph, p. 284, Premier Publishing, Vienna (2018).

[5] Dinh, H., Moore, C., Russell, A.: McEliece and Niederreiter Cryptosystems that Resist Quantum Fourier Sampling Attacks. https://dl.acm.org/citation.cfm?id=2033093, last ac-cessed 2020/03/10.

[6] Baldi, M., Bianchi, M., Chiaraluce, F., Rosenthal, J., Schipani, D., Enhanced public key se-curity for the McEliece cryptosystem. https://arxiv.org/abs/1108.2462, last accessed 2020/03/10.

[7] Zhang, G., Cai, S., Secure error-correcting (SEC) schemes for network coding through McEliece cryptosystem. https://link.springer.com/article/10.1007/s10586-017-1294-5 (2017).

[8] Zhang, G., Cai, S.: Universal secure error-correcting (SEC) schemes for network coding via McEliece cryptosystem based on QC-LDPC codes. https://link.springer.com/article/10.1007/s10586-017-1354-x (2017).

[9] Rossi, M., Hamburg, M., Hutter, M., Marson, M.: A Side-Channel Assisted Cryptanalytic Attack Against QcBits. https://link.springer.com/chapter/10.1007/978-3-319-66787-4_1 (2017).

[10] Dudikevich, V.B., Kuznetsov, O.O., Tomashevsky, B.P.: Crypto-code protection of infor-mation with non-binary equilibrium encoding. The hour zahist of information, No. 2, p. 14–23 (2010).

[11] Dudikevich, V.B., Kuznetsov, O.O., Tomashevsky B.P.: Non-dual equilibrium coding method. Modern information protection. No. 3, p. 57–68 (2010).

[12] Morozov, K., Roy, P.S., Sakurai, K.: On unconditionally binding code-based commitment schemes. https://dl.acm.org/citation.cfm?id=3022327&dl=ACM&coll=DL, last accessed 2019/09/1.

[13] Corbella, I.M., Tillich, J.-P.: Using Reed-Solomon codes in the (U | U + V) construction and an application to cryptography. In: IEEE International Symposium on Information, https://ieeexplore.ieee.org/document/7541435, last accessed 2019/09/1.

[14] Rossi, M., Hamburg, M., Hutter, M., Marson, M.E.: A Side-Channel Assisted Cryptana-lytic Attack Against QcBits. https://link.springer.com/chapter/10.1007/978-3-319-66787-4_1, last accessed 2019/09/1.

[15] Almeida, P., Avelli, D.N.: A new class of convolutional codes and its use in the McEliece Cryptosystem. https://www.researchgate.net/publication/324745076_A_new_class_of_convolutional_codes_and_its_use_in_the_McEliece_Cryptosystem, last accessed 2019/09/1.

[16] Kapshikar, U., Mahalanobis, A.: A Quantum-Secure Niederreiter Cryptosystem using Qua-si-Cyclic Codes. https://www.researchgate.net/publication/327660637_A_Quantum-Secure_Niederreiter_Cryptosystem_using_Quasi-Cyclic_Codes, last accessed 2019/09/1.

[17] Cho, J.Y., Griesser, H., Rafique, D.: A McEliece-Based Key Exchange Protocol for Optical Communication Systems. In: Proceedings of the 2nd Workshop on Communication Securi-ty, WCS 2017, pp. 109-123, https://link.springer.com/chapter/10.1007%2F978-3-319-59265-7_8, last accessed 2019/09/1.

[18] Evseev, S.P., Rzaev, Kh.N., Tsyganenko, A.S.: Analysis of the software implementation of direct and inverse transformation using the method of non-binary equilibrium coding. Bezpeka Informatsii 2016 Volume 22 # 2 – Kiev "Nash Format", pp. 96–203 (2016).

[19] Sidel'nikov, V. M.: Cryptography and coding theory. In conference materials: Moskovskij Universitet i razvitie kriptografii v Rossii, MGU, p. 22 (2002).

[20] Minder, L.: Cryptography based on error correcting codes. Ph.D. thesis, Ecole Polytech-nique Fédérale de Lausanne (2007).

[21] Faure, C., Minder, L.: Cryptanalysis of the McEliece cryptosystem over hyperelliptic codes. In: Eleventh International Workshop on Algebraic and Combinatorial Coding Theory, pp. 99-107, Pamporovo, Bulgaria (2008).

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

[23] Hlobaz, A., Podlaski, K., Milczarski, P.: Enhancements of encryption method used in SDEx. Communications in Computer and Information Science Vol. 718, pp. 134-143, Springer International Publishing (2017).

[24] Milczarski, P., Hlobaz, A., Podlaski, K.: Analysis of enhanced SDEx method. Proceedings of the 2017 IEEE 9th International Conference on Intelligent Data Acquisition and Ad-vanced Computing Systems: Technology and Applications, IDAACS (2017).