CiSJ

computing@computingonline.net
www.computingonline.net

Print ISSN 1727-6209
On-line ISSN 2312-5381
International Journal of Computing

CODE-BASED HYBRID CRYPTOSYSTEM: COMPARATIVE STUDIES AND ANALYSIS OF EFFICIENCY

Yurii Gorbenko [1,2], Anastasiia Kiian [1], Andriy Pushkar'ov [3], Oleksandr Korneiko [4], Serhii Smirnov [5], Tatyana Kuznetsova [1]

[1] V. N. Karazin Kharkiv National University, Svobody sq., 6, Kharkiv, 61022, Ukraine, nastyak931@gmail.com
[2] JSC "Institute of Information Technologies", Bakulin St., 12, Kharkiv, 61166, Ukraine, gorbenkou@iit.kharkov.ua
[3] State Service of Special Communication and Information Protection, Solomianska 13 str., Kyiv, 03680, Ukraine
[4] National Academy of Internal Affairs, 1 Solomjanska Square, Kyiv, 03035, Ukraine, alex_korneiko@meta.ua
[5] Central Ukrainian National Technical University, University Avenue 8, Kropyvnytskyi, 25006, Ukraine,
smirnov.ser.81@gmail.com

Paper history:
Received 20 November 2018
Received in revised form 15 September 2019
Accepted 20 December 2019
Available online 31 December 2019

Keywords:
Algebraic codes;
Code-based cryptography;
McEliece cryptosystem;
Niederreiter cryptosystem;
Public-key cryptosystem;
Post-quantum cryptosystem.

Abstract: In this paper the basic principles of construction and operation of McEliece and Niederreiter cryptosystems based on the use of error-correcting codes were considered. A new hybrid cryptosystem that combines the rules of encryption according to the above-mentioned schemes is proposed. Also, this paper presents the analysis and comparative studies from the standpoint of stability, the volume of public and private keys, length of ciphertext and relative speed of information transmission of the new proposed scheme and McEliece and Niederreiter cryptosystems. It is considered from an analytical point of view and with the help of graphic images. Comparative studies revealed that the hybrid cryptosystem retains the positive aspects of its predecessors, as well as allows us to increase the relative transmission rate with the preservation of the stability indicator to the classical and quantum cryptanalysis. One disadvantage is the increase in decoding time by adding information extracted as in Niederreiter scheme, but the increase in this indicator is not critical. Despite the demonstrated benefits, it remains open to all cryptosystems to reduce the amount of the used key data, which, in the case of quantum computers to maintain stability, still needs to be increased once.

1. INTRODUCTION

A vast majority of modern cryptographic systems are based on mechanisms which provide protection due to the complexity of solving a particular mathematical problem such as discrete logarithm, factorization, etc. [1-2]. By contrast, cryptosystems based on coding are not currently widely used, but in the near future everything can change radically. This change is due to the desire of the world community to create a full-scale quantum computer, which will be able to accelerate the performance of usual computer operations in dozens or even hundreds of times [3]. With this in mind, research into the post-quantum cryptography, cryptography representing algorithms that are resistant to quantum and classical cryptanalysis, became relevant.

There are five main areas of research: hash-based cryptography, lattice-based cryptography, multivariate cryptography, supersingular elliptic curve isogeny cryptography and code-based cryprography [4]. In our study, we focus on the latter direction, taking into account several factors. Firstly, code-based systems can provide such benefit as channel error control. Secondly, the high speed of cryptography and the resistance to classical and quantum cryptanalysis are distinguished by code-based systems from their competitors [5].

The most popular cryptosystems based on the use of coding are McEliece and Niederreiter schemes. After analyzing their structures, advantages and disadvantages, we offer a new, so-called hybrid cryptosystem that combines principles of encryption of two above-mentioned systems and provides additional significant benefits that will be considered in the future.

2. RESEARCH OF PRINCIPLES OF CRYPTOSYSTEMS CONSTRUCTION

2.1 McELIECE CRYPTOSYSTEM

McEliece cryptosystem is a so-called classic cryptosystem based on the use of codes. It was proposed more than 30 years ago and it is still considered to be resistant not only to classical, but also to quantum cryptanalysis. A feature of this scheme can be defined as masking the fast decoding rule by means of matrix multiplication of generating matrix of algebraic block code on a random matrix (which is a secret key) [6]. An attacker, who only knows a public key, has to use a complex algorithm for non-algebraic decoding. This algorithm is defined as an NP-complete task. An authorized user who has a private key removes the effect of masking matrices and applies a fast algebraic decoding algorithm. Next, we define an encryption algorithm using in McEliece scheme:

1). Let's fix a finite field $GF(q)$,a matrix G, which is a generating matrix of (n,k,d) code over $GF(q)$, a matrix X is a non-degenerate $k \times k$ matrix with elements from $GF(q)$, matrices P and D, which are permutational and diagonal $n \times n$ matrices respectively (for binary codes, D isn't used).

2). Let's form a matrix $G_X = X \cdot G \cdot P \cdot D$. It's the public key of the McEliece scheme. In this case, matrices X ,P and D are the private key.

3). A cryptogram is formed according to the following rule:

$$c_X^* = I \cdot G_X + e, \tag{1}$$

where e is an error vector, the Hamming weight which meets the requirement:

$$w_h(e) \le t = \left\lfloor \frac{d-1}{2} \right\rfloor, \tag{2}$$

where I is the k-bit informational vector over the field $GF(q)$.

After completing the above steps, we receive a codeword $c_X = I \cdot G_X$, which is influenced by the error vector. In this case, vector e should be considered as a one-time private key. Its weight determines the complexity of decoding influenced the codeword (cryptogram) [7].

A decryption algorithm can be described by the following steps:

1) Construct the vector $\bar{c}^* = c_X^* \cdot D^{-1} \cdot P^{-1}$. Matrix $\Lambda = D^{-1} \cdot P^{-1}$ keeps the distance and weight according to Hamming. This means that the constructed vector cannot be suitable in more than $w_h(e)$ digits. For binary codes, this step is slightly different, because in this case, we do not use the matrix D and the construction of the corresponding vector is reduced to the multiplication $\bar{c}^* = c_X^* \cdot P^{-1}$

2) Using an algorithm of polynomial complexity, we decode the vector $\bar{c}^* = I' \cdot G + e'$, i.e. find I'.

3) Calculate the initial k-bit information vector $I = I' X^{-1}$[6-7].

Consequently, McEliece decryption is performed by removing the masking matrices and using a polynomial complexity algorithm [8].

2.2 NIEDERREITER CRYPTOSYSTEM

The next step is to consider peculiarities of functioning of the theoretical code-based scheme Niederreiter. It is also based on the benefits of using masking matrices, as in the McEliece scheme [7-9]. In order to define an encryption algorithm that runs in this scheme:

1) We fix a finite field $GF(q)$. The check matrix of algebraic (n,k,d) code over $GF(q)$ is denoted by H (in the original article, it was suggested to use the generic Reed-Solomon codes).

2) Let's form a private key containing the following components: X is a non-degenerate $(\mathrm{n-k}) \times (\mathrm{n-k})$ matrix with elements of GF(q), P is a permutation $n \times n$ matrix, and D is a diagonal $n \times n$ matrix (this matrix is not used for binary codes).

3) Then, we calculate a public key in accordance with the rule:

$$H_x = X \cdot H \cdot P \cdot D. \tag{3}$$

4) Formation of the cryptogram is accomplished by multiplying the vector *e* by the transposed public key:

$$s_X = e \cdot H_X^T. \tag{4}$$

The cryptogram consists of *(n-k)* elements [10]. Vector *e* stores information that we want to encrypt. The information vector is further transformed using equilibrium coding. Upon receiving a message, a legitimate user, in the same way as in McEliece cryptosystem, removes the action of masking matrices and, using the fast decoding algorithm, receives the vector *e*, which, after equilibrium coding, represents the initially transmitted information [11].

2.3. A NEW HYBRID CRYPTOSYSTEM

Taking into account the proved stability of the considered cryptosystems (more details will be discussed in the next section), we propose a new hybrid cryptosystem, which has the same advantages as its predecessors, and even improves their performance. A basis of the proposed system is the combination of encryption information according to McEliece and Niederreiter schemes. Private keys of the hybrid scheme are similar to the first two schemes, matrix X (it has $k \times k$ elements), matrix P (it has $n{\times}n$ elements) and, in the case of non-binary coding, matrix D (size $n{\times}n$) [7, 11].

The public key is the matrix $G_X = X \cdot G \cdot P \cdot D$. In order to encrypt the information vector is divided into two components (I_1 and I_2). After that, the cryptogram is formed:

$$c_X^* = I_1 \cdot G_X + e. \tag{5}$$

In this case, the first component of information is multiplied by public key, as in the transformation according to McEliece. The second information component is converted according to the Niederreiter scheme, namely, I_2 of length m is transformed into an encoded information vector e of length n (for example, using equilibrium coding). For the generated vector, the following conditions must be fulfilled [7]:

$$w_h(e) \le t = \left\lfloor \frac{d-1}{2} \right\rfloor, \tag{6}$$

$$m = \left\lfloor \log_q \left(\sum_{i=0}^{t} (q-1)^i \frac{n!}{i!(n-i)!} \right) \right\rfloor. \tag{7}$$

In order to provide a maximum stability, it is recommended to maximize the Hamming weight of the vector *e*, because overcoming all possible values of this vector is much more complicated. Decryption in the hybrid scheme occurs, just like in the McEliece scheme described in the previous section, with the only difference that information is extracted not only from the vector *I*, but also from the error vector *e* [12-14]. This fact allows us to significantly increase the relative speed of information transmission, which will be discussed further.

3. COMPARATIVE ANALYSIS OF CRYPTOSYSTEMS

Comparing the effectiveness of cryptosystems, we will use such factors as the relative speed of information transmission, resistance to classical and quantum cryptanalysis, the volume of key data that needs a cryptosystem, and the length of the ciphertext according to each alternate.

3.1. RELATIVE SPEED OF INFORMATION TRANSMISSION

First, let's consider the relative speed of information transmission. It describes an amount of information contained in a cryptogram of length *n* relative to the total length of this cryptogram.

An estimation of the relative speed for the McEliece scheme is the simplest, since it is known that any cryptogram formed by this algorithm has the length *n*, whereas the initial information vector has the length of *k* bit. Consequently, the relative transmission speed in this case [12-14] is equal to

$$R = \frac{\log_2 2^k}{n} = \frac{k}{n}. \tag{8}$$

The relative speed of information transmission for the Niederreiter scheme is discussed in detail in [7]. According to this data, it equals

$$R = \frac{\left\lfloor \log_2 \left(\frac{n!}{t!(n-t)!} \right) \right\rfloor}{n-k}. \tag{9}$$

Using a hybrid cryptosystem, the formed ciphertext has the length n, whereas information is encoded with a combination of the principles of McEliece and Niederreiter, dividing it into two components I_1 and I_2, with I_1 having the length of *k* bit and I_2 converted by equilibrium encoding, so the maximum possible hidden amount of bits defined as in the Niederreiter scheme equals

$$\log_q \left(\sum_{i=0}^{t} (q-1)^i \frac{n!}{i!(n-i)!} \right) = n-k.$$

That is, an estimate of the relative speed of information transmission for hybrid cryptosystem can be defined as:

$$R = \frac{k + \left\lfloor \log_2 \left(\frac{n!}{t!(n-t)!} \right) \right\rfloor}{n}. \tag{10}$$

From the above data, one can immediately conclude that in terms of relative speed, the hybrid system is far ahead of its predecessors, due to encoding two components [7].

3.2. STABILITY TO CLASSICAL CRYPTANALYSIS

It should be noted immediately that the researchers proved that the stability of McEliece and Niederreiter is equivalent. The proof is as follows. Assume that we know the syndrome $c = eH_x$. We can calculate $b = aE + e$, in this case $c = bH_x$ and b is treated as a ciphertext in the McEliece system. Provided that an attack with complexity W is found for the McEliece system, there is a known algorithm for computing vector a, which is the secret information in the McEliece scheme. Then the vector e containing the secret information in the Niederreiter system can be represented in the form of $e = aE + b$, that is, the complexity of determining the vector e coincides with the complexity of determining the vector a. Otherwise, when there is an effective attack on the Niederreiter scheme, possibly using a ciphertext $(aE + e)D^T = eD^T$, the vectors e and a are calculated. It should be noted that from the above point of view, the equivalence of the estimates of stability of McEliece and Niederreiter cryptosystems and the hybrid cryptosystem [15] follows. The security of all three cryptosystems is based on the inability to solve such fundamental problems of coding theory as the general problem of decoding linear codes and the problem of finding a codeword with a given weight [16-19]. Considering the possibility of attacking, it's worth mentioning that, despite the fact that the McEliece cryptosystem based on Goppa codes, is still considered resistant, as Robert McEliece pointed out in his original article, there are two main ways that an intruder can use to attack a cryptosystem [6]: 1) An attacker may try to recover a private key from the public key, and then decrypt the message; 2) An attacker can directly decode a message without having to study the structure of the Goppa code.

A large number of researchers are engaged in the realization of these types of attacks, but the optimal effective version hasn't been yet invented. Also, the assessment of the stability of each cryptosystem to attacks can be made by determining the minimum number of sets covering all errors (roof sets). Their number is calculated according to the formula:

$$N \geq \frac{C_n^t}{C_{n-k}^t} = \frac{\frac{n!}{t!(n-t)!}}{\frac{(n-k)!}{t!(n-k-t)!}} = \frac{n!(n-k-t)!}{(n-t)!(n-k)!}. \quad (11)$$

In this case C_n^t represents the total number of error combinations, and C_{n-k}^t is the maximum number of error combinations that can be covered by this set [7]. The assessment from this point of view is somewhat underestimated, because the computational complexity of the formation of candidate words is not taken into account, which is calculated with respect to the chosen set.

3.3. STABILITY TO QUANTUM CRYPTANALYSIS

Now there are various quantum algorithms, among which the most popular are the quantum Schor's algorithm and the quantum Grover's algorithm for finding an element in unsorted base, quantum algorithms for cryptanalysis for transformations in factor-ring, and others [20]. Several sources say that the Shor's quantum algorithm is not efficient enough for the McEliece cryptosystem security breakdown. The most effective quantum algorithm in relation to the McEliece scheme is Grover's algorithm. It is correctly considered not as a "database", but as a search for the roots of a function. From this point of view, it is worth considering the application of the Grover's algorithm within the scope of the set decoding attack [21]. Grover's algorithm is a general constructive transformation of conditional chains in the quantum chain of finding roots. The detailed implementation of the quantum attack decoding the data set is demonstrated in [22, 23]. It is worth noting that basic set decoding attack performs a search of the root of the function in a random manner. The search uses roughly average $\frac{C_n^k}{0,29C_{n-t}^k} \approx c^{n/\lg n}$ passes of the function. Using Grover's algorithm, this estimate is transformed into

$$\sqrt{\frac{C_n^k}{0,29C_{n-t}^k}} \approx c^{(1/2)n/\lg n} \quad (12)$$

Each iteration is a quantum function performed in $O(n^3)$ qubits operations. Each iteration also requires $n^{O(1)}$ qubits operations. The total time for finding S is equal to $c^{(1/2+O(1))n/\lg n}$ of a quantum computer. When you find S, you can calculate m and e, using minor incremental efforts [24].

We will show the relative speed of information transmission and stability to both types of cryptanalysis on the examples given in Table 1. It should be noted that in the table above, the following notation is used: "M" for the McEliece cryptosystem; "N" for the Niederreiter cryptosystem; "H" for the Hybrid Cryptosystem. Then the data presented in the table for the better visual perception can be represented using a graphic image (Fig. 1-2). Analyzing the reviewed data, we can conclude that with the same code parameters, all three cryptosystems provide the same level of stability to the classical cryptanalysis. However, the results of resistance to quantum cryptanalysis are different: the resistance to quantum cryptanalysis of the McEliece cryptosystem begins to decrease when the code's relative speed drops below the limit of 0.66. At the same time, it is obvious that with the increasing correction ability of the hybrid cryptosystem and the decreasing relative speed the stability to quantum cryptanalysis also increases. However, the further research has shown that this trend will change under the same condition that affects the stability of the McEliece scheme, namely, the reduction of the relative speed of information transmission below the limit of 0.66.

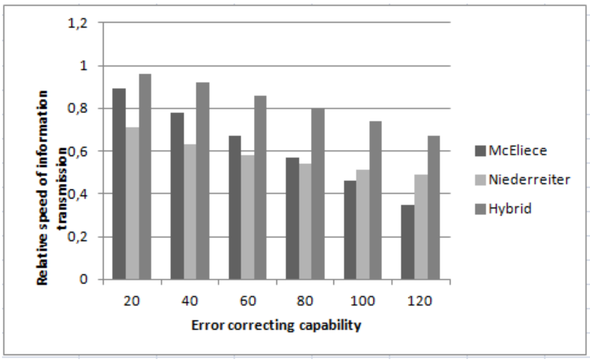

Figure 1 – Comparison of the relative speed of transmission of cryptosystems

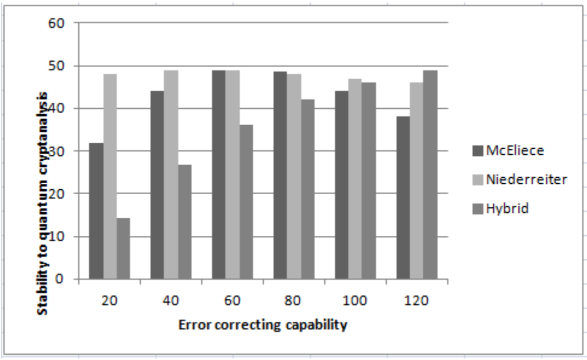

Figure 2 – Comparison of stability of cryptosystems to quantum cryptanalysis

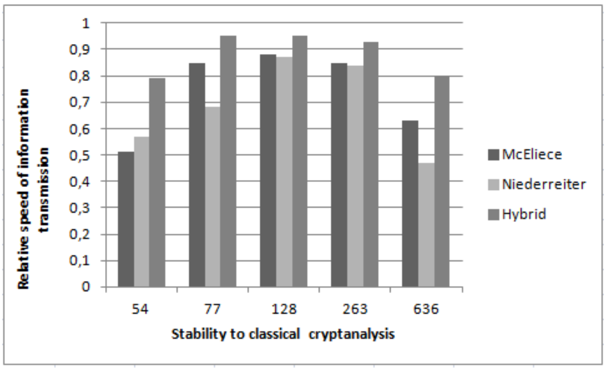

Figure 3 – Dependence between relative speed and stability of cryptosystems

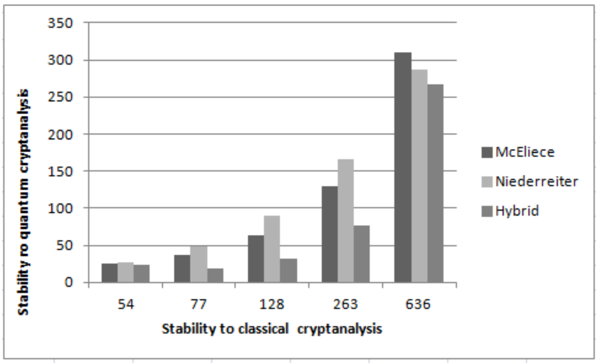

Figure 4 – Dependence between the magnitude of stability to classical and quantum cryptanalysis

3.4. COMPARISON OF KEY DATA AND LENGTH OF CIPHERTEXT

The next step is to compare the volume of key data and length of the ciphertext, which is formed according to each of three cryptosystems.

Since the binary case of using cryptosystems is considered in the work, therefore, when evaluating the volume of key parameters, matrix *D* will not be taken into account, and consideration will be given without taking into account the secret polynomial of the Goppa code. The key parameters and method of ciphertext formation coincide in the case of hybrid scheme and McEliece scheme, so their estimates can be considered equivalent. The private key of these schemes consists of matrices *X* and *P*. The matrix *X* has dimensions of $k \times k$, and the volume that occupies matrix *P* is determined by the vector of a permutation of *n* elements. The size of the public key of both schemes is determined by the matrix $G_X = X \cdot G \cdot P$, which has the dimension $n \times k$. The length of the formed ciphertext is determined by the length of the cryptogram $c_X^* = I_1 \cdot G_X + e$ consisting of *n* elements. Consequently, for the McEliece cryptosystem and hybrid cryptosystem, the length of the private key is equal to $l_{\text{pr.k.}} = k \cdot k + n$, the public key- $l_{p.k} = k \cdot n$ and the constituted ciphertext $l_{text} = n$. Hence, we can also note the disadvantage of cryptosystems, which is in an increased length of ciphertext relative to the initial information vector. It is known that for Niederreiter cryptosystem, matrices X and P also generate a secret key. Size of the matrix P is determined, as in the previous case, but the matrix X is different and has the dimensions of $(n-k)\times(n-k)$. The public key of this scheme is the matrix $H_X = X \cdot H \cdot P$ consisting of $n \times (n-k)$ elements. The length of syndrome $s_X = e \cdot H_X^T$ is equal to $(n-k)$. Consequently, for Niederreiter cryptosystem, the following estimates are true: the amount of the private key $l_{pr.k} = (n-k)\cdot(n-k)+n$, the volume of the public key $l_{p.k} = n\cdot(n-k)$, the length of the ciphertext $l_{text} = n-k$.

Having analyzed the above information, one can conclude that the volume of the secret key in the McEliece and hybrid scheme varies with the secret keys in the Niederreiter scheme $n^2 - 2\cdot n\cdot k$, the difference from the generated encryption text is equal to k elements, but at the same time, size of the public key in Niederreiter scheme is greater than n^2 elements. We will illustrate this fact by the examples shown in Table 2. For the consideration of different levels of security, the code parameters most commonly found in the scientific literature were chosen. For a more visual understanding, we shall present the data listed in the table using histograms (Fig. 3-5). Having analyzed the above data, one can conclude that to provide a similar level of stability to quantum cryptanalysis, compared with the usual cryptanalysis (for example, comparing the parameters for the code parameter n = 16384, n = 8192), it is necessary to increase the volume of key data more than three times. It is also worth noting that the stability of cryptosystems to quantum cryptanalysis depends directly on the indicators of their relative speed. Because of the advantage in the latter indicator, the hybrid cryptosystem has shown decent results in stability to quantum cryptanalysis, but the decrease in resistance is not critical compared to other schemes.

However, the obvious advantage of the hybrid cryptosystem, which is worth reminding, in terms of cryptosystem's efficiency, is that it allows one to encrypt a larger amount of information using the same number of keys, while providing an adequate level of protection [25-31]. This research might be useful for the improvement of various methods of information security [10-13], as well as other practical use [32-36].

Table 1. Dependence of stability and relative speed on the error-correcting ability of the code

Parameters of code	Relative speed of information transmission			Resistance to classical cryptanalysis, bit			Resistance to quantum cryptanalysis, bit		
	M.	N.	H.	M.	N.	H.	M.	N.	H.
(2048,1828,41)	0,89	0,71	0,96	65,5			32	47,9	14,2
(2048, 1608,81)	0,78	0,63	0,92	90			44	49	26,7
(2048,1388, 121)	0,67	0,58	0,86	100			49	49	36
(2048,1168, 161)	0,57	0,54	0,8	100			48,7	48,1	42
(2048,948, 201)	0,46	0,51	0,74	92			44	47	46
(2048,728, 241)	0,35	0,49	0,67	78,9			38	46	49

Table 2. Comparison of performance indicators of cryptosystems

McEliece cryptosystem					
Parameters of code	Key volume, bit	Length of ciphertext, bit	Relative speed	Resistance to classical cryptanalysis, bit	Resistance to quantum cryptanalysis, bit
(1024,524,101)	812176	1024	0,51	54	25,8
(2048,1751,55)	6654097	2048	0,85	77	37,6
(4096,2584,253)	27754896	4096	0,88	128	62,6
(8192,6957,191)	105399785	8192	0,85	263	130
(16384,10322,867)	275675716	16384	0,63	636	310
Niederreiter cryptosystem					
(1024,524,101)	763024	500	0,57	54	26,7
(2048,1751,55)	698513	297	0,68	77	49
(4096,3604,83)	2261392	492	0,87	128	90,2
(8192,6957,191)	11650537	1235	0,84	263	166
(16384,10322,867)	136084036	6062	0,47	636	286
Hybrid cryptosystem					
(1024,524,101)	812176	1024	0,79	54	24,2
(2048,1751,55)	6654097	1945	0,95	77	18,9
(4096,3604,83)	27754896	3892	0,95	128	31,8
(8192,6957,191)	105399785	7618	0,93	263	77
(16384,10322,867)	275675716	13107	0,8	636	267

4. CONCLUSION

After analyzing the entire spectrum of information related to code-based cryptosystems, we can draw a number of conclusions. Firstly, the research found that the use of algebraic codes in the context of post-quantum cryptography is a promising direction, since they allow us to provide a higher speed of cryptographic transformation, an error control that can occur in the communication channel, as well as resistance to the classical and quantum cryptanalysis. Due to the above mentioned advantages of using codes for the purpose of constructing algorithms of post-quantum cryptography, a new hybrid algorithm, which combines principles of encryption in accordance with the cryptosystems of McEliece and Niederreiter, was proposed. In turn, a further comparative analysis of all three cryptosystems has shown that using the proposed scheme, the key data occupies the same volumes as the key data of McEliece cryptosystem. The Hybrid cryptosystem provides a higher relative transmission speed and equal resistance to cryptanalysis as McEliece cryptosystem. One disadvantage is an increase in decoding time by adding information extracted as in Niederreiter scheme, but the increase in this indicator is not critical. Despite the demonstrated benefits, it remains open in all cryptosystems how to reduce the amount of the used key data, which, in the case of quantum computers to maintain stability, still needs to be increased once. This direction remains an actual vector of research in the core of modern cryptography [26-29].

5. REFERENCES

[1] A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997, 794 p.

[2] N. Ferguson and B. Schneier, *Practical Cryptography*, John Wiley & Sons, 2003, 432 p.

[3] D. Moody, "Post-quntum cryptography: NIST's plan for the future," *Proceedings of the Seventh International Conference on Post-Quntum Cryptography*, Japan, 2016, [Online]. Available at: https://pqcrypto2016.jp

[4] N. Koblitz and A.J. Menezes, "A Riddle wrapped in an enigma," [Online], Available at: https://eprint.iacr.org/2015/1018.pdf

[5] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, New York, Oxford, 1977, 762 p.

[6] R. J. McEliece, *A Public-key Cryptosystem based on Algebraic Coding Theory*, DSN Progress Report 42-44, Jet Propulsion Lab., January-February, 1978, pp. 114-116.

[7] S. Heyse, "Implementation of McEliece based on quasi-dyadic Goppa codes for embedded devices," *in Post-Quantum Cryptography, ser. Lecture Notes in Computer Science, B.-Y. Yang*, Ed. Springer Berlin / Heidelberg, 2011, vol. 7071, pp. 143-162.

[8] M. Finiasz and N. Sendrier, "Security bounds for the design of codebased cryptosystems," *in M. Matsui, ed., Advances in Cryptology, ASIACRYPT 2009, volume 5912 of Lecture Notes in Computer Science*, Springer Berlin Heidelberg, 2009, pp. 88 -105

[9] N. Courtois, M. Finiasz, and N. Sendrier, "How to achieve a McEliece-based digital signature scheme," *Proceedings of the Advances in Cryptology – ASIACRYPT 2001*, vol. 2248, pp. 157–174.

[10] H. Niederreiter, "Knapsack-type cryptosystems and algebraic coding theory," *Problem Control and Inform Theory*, vol. 15, pp. 19-34, 1986.

[11] A. Kuznetsov, A. Pushkar'ov, N. Kiyan and T. Kuznetsova, "Code-based electronic digital signature," *Proceedings of the 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Kyiv, Ukraine, 2018, pp. 331-336. DOI: 10.1109/DESSERT.2018.8409154

[12] A. Kuznetsov, M. Lutsenko, N. Kiian, T. Makushenko and T. Kuznetsova, "Code-based key encapsulation mechanisms for post-quantum standardization," *Proceedings of the 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Kyiv, Ukraine, 2018, pp. 276-281. DOI: 10.1109/DESSERT.2018.8409144

[13] A. Kuznetsov, A. Kiian, M. Lutsenko, I. Chepurko and S. Kavun, "Code-based cryptosystems from NIST PQC," *Proceedings of the 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Kyiv, Ukraine, 2018, pp. 282-287. DOI: 10.1109/DESSERT.2018.8409145

[14] Vladimir M. Sidelnikov and Sergey O. Shestakov, "On insecurity of cryptosystems based on generalized Reed-Solomon codes," *Discrete Mathematics and Applications*, vol. 2, issue 4, pp. 439-444, 1992.

[15] Y. X. Li, R. H. Deng and X. M. Wang, "On the equivalence of McEliece's and Niederreiter's public-key cryptosystems," *IEEE Transactions on Information Theory*, vol. 40, no. 1, pp. 271-273, Jan. 1994.

[16] A. A. Kuznetsov, Yu. I. Gorbenko, D. I. Prokopovych-Tkachenko, M. S. Lutsenko, M. V. Pastukhov. "NIST PQC: Code-based cryptosystems," *Telecommunications and Radio Engineering*, vol. 78, issue 5, pp. 429-441, 2019. DOI: 10.1615/TelecomRadEng.v78.i5.50

[17] O. Al Rasheed and P. Ivaniš, "Complexity and performance of QC-MDPC code-based McEliece cryptosystems," *Proceedings of the 2015 12th International Conference on Telecommunication in Modern Satellite, Cable and Broadcasting Services (TELSIKS)*, Nis, 2015, pp. 31-34. DOI: 10.1109/TELSKS. 2015.7357731

[18] M. Baldi, P. Santini and F. Chiaraluce, "Soft McEliece: MDPC code-based McEliece cryptosystems with very compact keys through real-valued intentional errors," *Proceedings of the 2016 IEEE International Symposium on Information Theory (ISIT)*, Barcelona, 2016, pp. 795-799. DOI: 10.1109/ISIT.2016.7541408

[19] Q. Wang, X. Qiu, Q. Zhang and C. Tang, "Key privacy in McEliece public key cryptosystem," *Proceedings of the 2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications*, Changsha, 2011, pp. 824-828. DOI: 10.1109/TrustCom.2011.109

[20] D. Bernstein, J. Buchmann and E. Dahmen, *Post-Quantum Cryptography*, Springer-Verlag, Berlin-Heidleberg, 2009, 245 p.

[21] J. Proos and C. Zalka. "Shor's discrete logarithm quantum algorithm for elliptic curves," *Quantum Info. Comput.*, vol. 3, issue 4, pp. 317-344, 2003.

[22] D.J. Bernstein, T. Lange, C. Peters, "Attacking and defending the McEliece cryptosystem," *in Buchmann J., Ding J. (eds) Post-Quantum Cryptography. PQCrypto 2008. Lecture Notes in Computer Science*, vol 5299, Springer, Berlin, Heidelberg, 2008, pp. 31-46.

[23] L. Grover, "A fast quantum mechanical algorithm for database search," *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing (STOC'96)*, ACM Press, New York, 1996, pp. 212-219.

[24] N. Sendrier, "Decoding one out of many," *in Yang, B.Y., ed.: PQCrypto 2011*, volume 7071 of LNCS, Springer, 2011, pp. 51-67.

[25] S. H. Odin Hashemi and G. A. Hodtani, "A modified McEliece public-key cryptosystem based on irregular codes of QC-LDPC and QC-MDPC," *Proceedings of the 2019 27th Iranian Conference on Electrical Engineering (ICEE)*, Yazd, Iran, 2019, pp. 1373-1376. DOI: 10.1109/IranianCEE.2019.8786376

[26] F. P. Biasi, P. S. L. M. Barreto, R. Misoczki, W. V. Ruggiero, "Scaling efficient code-based cryptosystems for embedded platforms," *J. Cryptograph. Eng.*, vol. 4, no. 2, pp. 123-134, 2014.

[27] P. Farkaš, "Two countermeasures against reaction attacks on LEDApkc and other QC-MDPC and QC-LDPC based McEliece cryptosystems in ARQ setting heuristic discussion," *Proceedings of the 2018 26th International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, Split, 2018, pp. 1-5.

[28] I. von Maurich and T. Güneysu, "Lightweight code-based cryptography: QC-MDPC McEliece encryption on reconfigurable devices," *Proceedings of the 2014 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, Dresden, 2014, pp. 1-6.

[29] T. Eisenbarth, T. Ğuneysu, S. Heyse, and C. Paar, "MicroEliece: McEliece for embedded devices," *in CHES, ser. Lecture Notes in Computer Science*, C. Clavier and K. Gaj, Eds., vol. 5747, Springer, 2009, pp. 49-64.

[30] I. Gorbenko, A. Kuznetsov, M. Lutsenko and D. Ivanenko, "The research of modern stream ciphers," *Proceedings of the 2017 4th International Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkov, 2017, pp. 207-210. DOI: 10.1109/INFOCOMMST.2017.8246381

[31] E. Persichetti, "Compact McEliece Keys based on Quasi-Dyadic Srivastava codes," *J. Mathematical Cryptology*, vol. 6, no. 2, pp. 149-169, 2012.

[32] A. Andrushkevych, Y. Gorbenko, O. Kuznetsov, R. Oliynykov, M. A. Rodinko, "Prospective lightweight block cipher for green IT engineering," *in: Kharchenko V., Kondratenko Y., Kacprzyk J. (eds), Green IT Engineering: Social, Business and Industrial Applications. Studies in Systems, Decision and Control*, vol 171, Springer, Cham, 2019, pp. 95-112.

[33] R. Misoczki, J.-P. Tillich, N. Sendrier, and P. S. L. M. Barreto, "MDPCMcEliece: New McEliece variants from moderate density parity-check codes," *Proceedings of the IEEE International Symposium on Information Theory (ISIT'2013)*, 2013, pp. 2069-2073.

[34] I. Gorbenko, O. Kuznetsov, Y. Gorbenko, A. Alekseychuk and V. Tymchenko, "Strumok keystream generator," *Proceedings of the 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Kyiv, Ukraine, 2018, pp. 294-299.

[35] S. Heyse, I. von Maurich, and T. Ğuneysu, "Smaller keys for code-based cryptography: QC-MDPC McEliece implementations on embedded devices," *in CHES, ser. Lecture Notes in Computer Science*, G. Bertoni and J.-S. Coron, Eds., vol. 8086. Springer, 2013, pp. 273-292.

[36] C. Chen, T. Eisenbarth, I. von Maurich, R. Steinwandt, "Differential power analysis of a McEliece cryptosystem," *Proceedings of the 13th Int. Conf. Appl. Cryptogr. Netw. Secur. (ACNS)*, June 2015, pp. 1-19.

Yurii I. Gorbenko, *Candidate of Sciences (Engineering), Academician of the Academy of Applied Radioelectronics Sciences, Researcher of the Department security information systems and technologies of the V. N. Karazin Kharkiv National University. Areas of scientific interests: applied cryptology.*

Anastasiia Kiian, *Researcher of the Department security information systems and technologies of the V. N. Karazin Kharkiv National University. Areas of scientific interests: cryptography, information theory and coding.*

Andriy I. Pushkar'ov, *Head of the State Service of Special Communication and Information Protection of Ukraine. Areas of scientific interests: cryptography, information theory and coding, authentication, cybersecurity.*

Oleksandr V. Korneiko, *Candidate of Sciences (Engineering), Full Professor, Head of the Department of Informatics technologies and cybersecurity of the National Academy of Internal Affairs. Areas of scientific interests: applied cryptology.*

Serhii A. Smirnov*, Candidate of Sciences (Engineering), Associate Professor of Cybersecurity & Software Academic Department Central Ukrainian National Technical University, Ukraine, Kropyvnytskyi. Areas of scientific interests: applied cryptology.*

Tatyana Y. Kuznetsova, *Researcher of the Department security information systems and technologies of the V. N. Karazin Kharkiv National University. Areas of scientific interests: security information systems and technologies.*