На основі практичної реалізації класичної схеми Нідеррайтера на недвійковий кодах виявлена закономірність для практичної реалізації – фіксація допустимих позиційних векторів перетворення відкритого тексту на основі рівноважного кодування. Отримання множини позиційних векторів вектора помилки при фіксованому наборі матриць маскування (особистого ключа одержувача) дозволяє реалізувати алгоритм розкодування класичної крипто-кодової схеми Нідеррайтреа на недвійковий кодах. Для цього необхідна модифікація крипто-кодової конструкції (ККК). Пропонується використовувати додатковий параметр ключових даних – вектор ініціалізації (множина неприпустимих позиційних векторів вектора помилки). Для протистояння атакам Сидельникова пропонується використовувати модифіковані (укорочені) алгебро-геометричні (еліптичні) коди (МЕС). Для цього необхідно використовувати другий додатковий вектор ініціалізації (множина позицій укорочення вектора помилки). На основі модифікації класичної схеми Нідеррайтера на недвійкових кодах пропонуються прикладні алгоритми формування та розшифрування криптограми в модифікованої крипто-кодової конструкції Нідеррайтера на основі модифікованих (укорочених) еліптичних кодів і програмна реалізація. Для подтвержденія рентабельності запропонованої крипто-кодової конструкції наведені результати порівняльної оценкі енерговитрат на реалізацію класичної схеми Нідеррайтреа на еліптичних кодах і реалізацію запропонованої конструкції на модифікованих еліптичних кодах. Отримані результати підтверджують можливість практичної реалізації крипто-кодової системи Нідеррайтера на основі запропонованих алгоритмів. При цьому гарантується необхідний рівень криптостійкості крипто-кодової конструкції, захист криптосистеми від атак Сидельникова і збільшення швидкості криптоперетворень в 3–5 разів в порівнянні з класичною схемою Нідеррайтрера

Ключові слова: модифікована крипто-кодова конструкція Нідеррайтера, модифіковані укорочені еліптичні коди, рівноважне кодування

UDC 621.391
DOI: 10.15587/1729-4061.2018.150903

PRACTICAL IMPLEMENTATION OF THE NIEDERREITER MODIFIED CRYPTO-CODE SYSTEM ON TRUNCATED ELLIPTIC CODES

S. Yevseiev
Doctor of Technical Science, Senior Researcher*
E-mail: serhii.yevseiev@hneu.net
O. Tsyhanenko
Postgraduate student*
S. Ivanchenko
Doctor of Technical Science, Associate Professor
Department No. 1
Institute of Special Communication and Information Security
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute"
Verkhnokliuchova str., 4, Kyiv, Ukraine, 03056
V. Aleksiyev
Doctor of Technical Sciences, Professor*
D. Verheles
PhD, Deputy Head
State Research Institute of Special Communication
and Information Protection
Maksyma Zalizniaka str., 3, Kyiv, Ukraine, 03142
S. Volkov
PhD, Associate Professor
Department of Automated Systems and Cybersecurity
Odessa State Academy of Technical Regulation and Quality
Kovalska str., 15, Odessa, Ukraine, 65020
R. Korolev
PhD, Senior Lecturer
Department of Combat Use and Operation of Automated Control Systems
Ivan Kozhedub Kharkiv National Air Force University
Sumska str., 77/79, Kharkiv, Ukraine, 61023
H. Kots
PhD, Associate Professor*
O. Milov
PhD, Associate Professor*
O. Shmatko
PhD, Senior Lecturer
Department of Software Engineering and
Information Technology Management
National Technical University "Kharkiv Polytechnic Institute"
Kyrpychova str., 2, Kharkiv, Ukraine, 61002
*Department of Cyber Security and Information Technology
Simon Kuznets Kharkiv National University of Economics
Nauky ave., 9-A, Kharkiv, Ukraine, 61166

1. Introduction

The entry of humanity into the era of high technology has significantly expanded the use of computational capabilities and technologies of artificial intelligence. Along with technical progress, computer crime is also growing, new types of attacks and new types of cyber-terrorism are emerging [1–3]. Threats acquire the character of synergism and hybridity, which leads to the need for a radical revision of the algorithms used in the Internet space and computer systems and networks [4–6]. The increase in processed data volumes in critical systems of state and commercial use places new

requirements to ensuring the reliability and performance of computer systems, security and reliability of transmitted and processed data [1, 7–9]. The emergence of quantum data processing technologies ("quantum computers – machines that use quantum mechanical phenomena to solve mathematical problems" [10–12]) threatens the use of traditional cryptography and public key cryptography algorithms [12–15]. In the 2018 report, NIST (USA) experts warn about the possibility of hacking many public-key cryptosystems in the context of creating full-scale quantum computers [12].

This will seriously undermine the confidentiality and integrity of digital communications on the Internet and elsewhere [12]. One of the promising areas proposed by NIST experts is the development of cryptographic systems that are protected from both quantum and classical computers based on McEliece and Niederreiter crypto-code systems [12–15].

This approach will reduce the risks and problems with the introduction of new algorithms for post-quantum cryptography and can interact with existing communication protocols and networks [12, 16, 17].

An analysis of the research results into the capabilities of quantum computers requires the development of a new methodology for the distribution of key data based on the use of asymmetric cryptography algorithms [12–14, 17]. The introduction of full-scale quantum computers will allow hacking of RSA, ECC, DSA cryptographic systems with brute force attacks in polynomial time. Thus, the development of cryptographic information protection tools (CIPT) currently requires new solutions to eliminate the vulnerabilities of post-quantum computing and ensuring data security to hybrid attacks. Such algorithms relate to the section of quantum-resistant cryptography. Due to the emergence of new schemes, not enough attention is paid to the well-known, asymmetric crypto-code systems (ACCS) based on the McEliece and Niederreiter schemes, which are also quantum-resistant [12].

The main difference between McEliece and Niederreiter's schemes from asymmetric cryptography algorithms is the use of noise-tolerant coding methods when masking the user's private key matrices. In both schemes, the masking matrices are: X^i – masking nondegenerate randomly equiprobably formed by the key source $k \times k$ matrix with elements from GF(q), P^i – permutable randomly equiprobably formed by the key source $n \times n$ matrix with elements from GF(q), D^i – diagonal formed by the key source $n \times n$ matrix with elements from GF(q). The product of these matrices and the generating matrix of the error-correcting code forms a public key. Cryptoresistance depends on the power of the GF(q) field and is ensured at the power of the field $GF(2^{10}–2^{13})$, which is a difficult practical task even with modern resources [18, 19]. In addition, in [20], an attack on the McEliece and Niederreiter schemes based on linear fractional transformations is shown, which make it possible to find the generating (check) matrix and hack the cryptosystem.

A promising direction is the development of McEliece and Niederreiter schemes on algebraic-geometry codes (codes based on elliptic curve parameters) or cascade codes [20].

2. Literature review and problem statement

In [15, 21, 22], an equilibrium coding method based on m-th codes (Reed-Solomon codes) was 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 permutation decoder.

In [13, 24], the use of alternant 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 [16, 23, 24], the authors use quasi-cyclic low-density parity-check (QC-LDPC) codes [25] and maximum rank distance codes [16, 23] to build McEliece and Niederreiter cryptosystems, respectively. In [24], the construction of the McEliece and Niederreiter schemes based on the alternant Goppa codes is considered. However, these codes are binary, which significantly increases the possibility of their hacking on the basis of a permutation decoder in a finite number of steps, described in [20].

In decision feedback computer networks, the authors suggest the use of the McEliece crypto-code system in the G.709 optical transport network (OTN) infrastructure to provide integrated requirements for reliability [17]. In [28], the authors proposed to use the Niederreiter asymmetric crypto-code system on elliptic codes [28]. This approach provides protection against possible attacks described in [20] and the required level of cryptographic strength. But the questions of practical implementation with the necessary power of the $GF(2^{10}–2^{13})$ field to ensure a guaranteed level of cryptographic strength remained unresolved.

Thus, the analysis showed that crypto-code systems 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, the analysis of open publications over the past two years has shown that the proposed versions of the Niederreiter cryptosystem on binary and non-binary block codes do not take into account the possibility of the Sidelnikov attack [20]. Such systems are impractical to use in Internet technologies because of their vulnerabilities and high energy costs in practical implementation. The use of algebraic codes in the Niederreiter crypto-code system is difficult due to the lack of a decoding algorithm, the difficulty of practical implementation and the need to build algebraic-geometry or cascading codes in $GF(2^{10}–2^{13})$ to provide the required level of cryptographic strength. Therefore, it is advisable to conduct a study on the development of the algorithm for decoding algebraic-geometric codes in the classical Niederreiter scheme, reducing energy consumption for their practical implementation.

3. The aim and objectives of the study

The aim of the study is to develop algorithms for the practical implementation of the Niederreiter crypto-code system on modified shortened elliptic codes, taking into account the revealed regularity of the necessary fixation of admissible position vectors of the plaintext into the error vector.

To achieve this aim, the following objectives were considered:

– to analyze the regularities of the necessary fixation of the position vectors of the plaintext for the formation of the error vector during the equilibrium coding of non-binary codes;

– to develop algorithms for the practical implementation of the Niederreiter crypto-code system on modified (shortened) elliptic codes.

4. Analysis of the pattern of necessary fixation of position vectors of plaintext for the formation of the error vector

The main advantage of the Niederreiter ACCS is the high speed of information conversion (the relative coding speed is close to 1). In [21, 22], an algorithm for equilibrium coding on non-binary codes and an algorithm for generating cryptograms in the Niederreiter crypto-code system on Reed-Solomon codes are proposed. However, the authors did not provide an information decoding algorithm, and the proposed cryptosystem could not be implemented over $GF(2^{10}–2^{13})$. To reduce energy costs with a guaranteed level of security, the Niederreiter modified crypto-code system (MCCS) on modified (shortened) elliptic codes (*MEC*) was proposed in [8]. This approach provides a reduction in the field power and allows you to implement the classic version of the Niederreiter scheme with a guaranteed level of cryptographic strength.

However, during the experimental study of the Niederreiter crypto-code system on *MEC*, it was determined that the use of non-binary codes with the classical Niederreiter ACCS requires fixing a subset of plaintexts for which the error localization procedure, with selected *X*, *P* and *D*, cannot be performed.

Let the $M_C=\{M_1,M_2,...M_{q^k}\}$, set of all plaintexts (n, k, d) be a block code. Define the set of fixed plaintexts.

$$M_F=\{M_1,M_2,...M_n\},$$

where

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

which are not suitable for further cryptogram generation. This set is proposed to be used as an initialization vector (IV_1). The second initialization vector forms the position vector for shortening the error vector:

$$IV_2=|h|=½,$$

where – the shortening elements (h_e is the error vector symbol, equal to zero, $|h1/2=|e$, that is, $e_i=0$, $\forall e_i\in h$).

In the classical Niederreiter scheme at the first stage of cryptogram generation, the plaintext characters are converted into error vector symbols based on the equilibrium coding algorithm. The resulting error vector at the second stage of cryptogram generation is "shortened" based on the code shortening algorithm and multiplied by the check matrix of the algebraic-geometric (elliptical) code:

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

where H_X^{ECu} is the check $n\times(n-k)$ matrix of the algebraic-geometric block (n, k, d) code with elements from $GF(q)$,

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

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

After the formation of key matrices of the private key, an authorized user needs to form elements of the set of fixed plaintexts that are not suitable for the subsequent formation of the cryptogram (the syndrome from the error vector).

Fig. 1 shows the algorithm for the formation of the initialization vector IV_1 (sets of fixed position sets of the plaintext $\{M_F\}$).

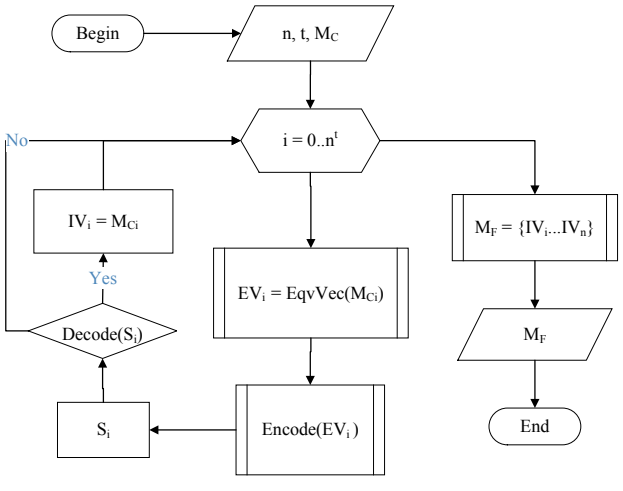

Fig. 1. Algorithm for the formation of a set of fixed plaintext sets

The set of usable plaintexts is determined by the formula:

$$M=M_C-M_F.$$

Thus, the proposed algorithm for generating a set of position plaintext sets $\{M_F\}$ allows you to "weed out" the error vector sets that do not allow the use of the classical version of information decoding on the receiving side.

In addition, the use of algebraic-geometric codes on elliptic curves makes it possible to eliminate the possibility of finding the elements of the check matrix by the algorithm proposed by V. Sidelnikov in [20], which significantly enhances the competitive advantages of the proposed crypto-code system.

Consider the algorithms for the practical implementation of cryptogram formation and decoding on the basis of the Niederreiter crypto-code system on *MEC*, taking into account the identified patterns.

5. Development of coding/decoding algorithms on shortened elliptic codes, taking into account the identified patterns

The algorithm for generating a cryptogram in the Niederreiter modified CCS on *MEC*, taking into account the identified patterns, is presented as a sequence of steps (Fig. 2).

Step 1. Entering the information to be encoded, one of the elements of the set of suitable plaintexts. The introduction of the public key H_X^{EC}.

Step 2. Formation of the error vector e, the weight of which does not exceed $\leq t$ – corrects the ability of the elliptic code based on the non-binary equilibrium coding algorithm.

Step 3. Formation of the initialization vector IV_1.

Step 4. Formation of the shortened error vector: $e_x = e(A) - IV_2$.

Step 5. Formation of the codogram:

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

The algorithm for decoding the codogram in the Niederreiter modified CCS on *MEC* will be represented as a sequence of steps (Fig. 3):

Step 1. Introduction of the S_X codogram, which is decoded. Introduction of the private key – matrices X, P, D.

Step 2. Finding one of the possible solutions of the equation

$$S^*_{r-h_e} = \bar{c}^* \times \left(H_X^{EC}\right)^T.$$

Step 3. Removing the action of the diagonal and permutation matrices:

$$\bar{c}^* = c_X^* \cdot D^{-1} \cdot P^{-1}.$$

Step 4. Decoding the vector $\bar{c}^*$. Formation of the vector e_x'.

Step 5. Converting the vector e_x'

$$e_x = e_x' \times P \times D.$$

Step 6. Forming the desired error vector e: $e = e_x + IV_2$.

Step 7. Transformation of the vector e based on the use of a non-binary equilibrium code into an information sequence.

Thus, the proposed algorithms make it possible to practically implement the classic Niederreiter scheme on *MEC*. This approach allows the use of the proposed Niederreiter MCCS in Internet protocols and provides a guaranteed level of cryptographic security.

We will conduct a comparative assessment of the energy consumption of the developed practical algorithms for the implementation of the Niederreiter MCCS on *MEC* with the algorithms of the classical Niederreiter scheme on *EC*.

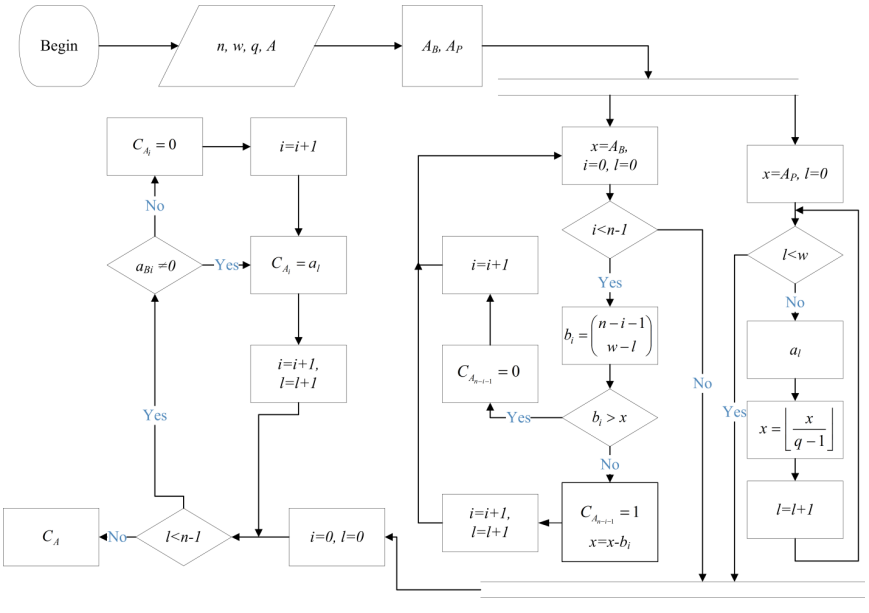

Fig. 2. Algorithm for the formation of codograms in the Niederreiter MCCS on *MEC*

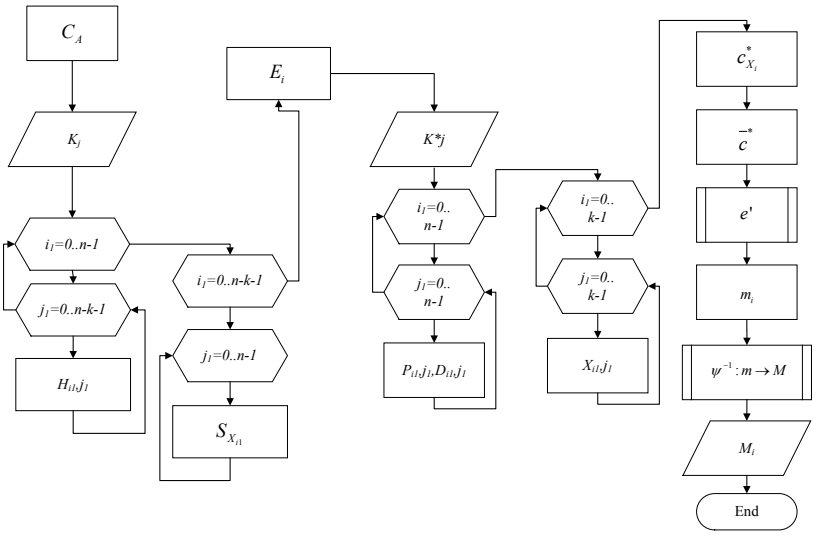

Fig. 3. Algorithm for decoding codograms in the Niederreiter MCCS on modified elliptic codes

We give an example of the implementation of the proposed Niederreiter crypto-code system on *MEC*.

Initial data: plaintext dictionary value – 11072; private key of the authorized user (masking matrix):

$$X=\begin{vmatrix}4&4&2&3\\3&6&2&1\\6&7&3&3\\2&0&0&5\end{vmatrix},$$

$$P=\begin{vmatrix}0&0&0&0&1&0&0\\1&0&0&0&0&0&0\\0&0&0&0&0&0&1\\0&1&0&0&0&0&0\\0&0&1&0&0&0&0\\0&0&0&1&0&0&0\\0&0&0&0&0&1&0\end{vmatrix},$$

$$D=\begin{vmatrix}2&0&0&0&0&0&0\\0&3&0&0&0&0&0\\0&0&5&0&0&0&0\\0&0&0&3&0&0&0\\0&0&0&0&1&0&0\\0&0&0&0&0&1&0\\0&0&0&0&0&0&5\end{vmatrix}.$$

For the formation of the initialization vector (formation of a set of fixed plaintexts), we define the vector of code words that are not suitable later for forming a cryptogram in the classical Niederreiter scheme on *EC* in the $GF(2^3)$ field.

Using the procedure of non-binary equilibrium coding with parameters n=15 and w=2, we transform it to a form that satisfies the modified elliptic code over the field 2^4.

11072 – {49} [000010000010000],
{47} [3 4] – [000030000040000].

We define the initialization vector as IV=[0 6 7 8 9 11 12 13], respectively, after reducing $e=e-$IV, we have e=0003040. After the reduction, we use the code above 23 with the parameters (7,3,5). Multiplying the private key matrix gives the public key:

$$H_x=\begin{bmatrix}7&5&5&2&3&4&1\\5&0&0&2&1&7&2\\4&2&7&7&4&2&5\\5&3&5&5&3&2&5\end{bmatrix}.$$

Find the parcel $S_x=e\times H_x^m$

$$S_x=[0\,0\,0\,3\,0\,4\,0]\times\begin{bmatrix}7&5&4&5\\5&0&2&3\\5&0&7&5\\2&2&7&5\\3&1&4&3\\4&7&2&2\\1&2&5&5\end{bmatrix}=[5\,6\,3\,4].$$

On the receiving side, we find one of q^k solutions of the expression $x\times H_x^m=S_x$.

Fixing the part x_1=1, x_2=1, x_3=1 of the vector and solving a system of linear equations, we get:

$$\begin{bmatrix}2&3&4&1&4&5\\2&1&7&2&1&6\\7&4&2&5&0&3\\5&3&2&5&6&4\end{bmatrix}=3\,0\,6\,2,$$

x=[1 1 1 3 0 6 2].

Find

$C_x^*x\times D^{-1}\times P^{-1}$, C_x^*=[1 3 0 6 1 2 1].

Find

$S_x^*=C_x^*\times H^T$, S_x^*=(5, 2, 0, 6);

Find the error locator polynomial

$$\Lambda(x)=x^2+a_1x+a_0=0,$$

$$\begin{bmatrix}S_0&S_1\\S_1&S_2\end{bmatrix}\times\begin{bmatrix}a_0\\a_1\end{bmatrix}=\begin{bmatrix}S_2\\S_3\end{bmatrix},\ \begin{bmatrix}5&2&0\\2&0&6\end{bmatrix},\ a_0=5;\ a_1=1;$$

Find error locators according to the Chen procedure. The result is a vector where zeros correspond to errors [5 0 3 0 2 2 3]. If the number of errors $<t$, then this information parcel is not included in the set of usable plaintexts $e=e^*\times P$=[0 0 0 1 0 1 0].

We find, so if

$$i\times\begin{bmatrix}7&5&5&2&3&4&1\\5&0&0&2&1&7&2\\4&2&7&7&4&2&5\\5&3&5&5&3&2&5\end{bmatrix}=\begin{bmatrix}5\\6\\3\\4\end{bmatrix},$$

and localizing the error vector, we get the system $\begin{bmatrix}2&4&5\\2&7&6\end{bmatrix}$, by solving which we get i_0=3; i_1=4; which, when combined with the error vector, gives i=[0 0 0 3 0 4 0]. If the system has more than one solution or root 0, then this information parcel is not included in the set of usable plaintexts.

Next, using the initialization vector IV, we restore the initial information parcel i_0=3; i_1=4000030000040000], which in turn, according to the procedure for restoring the equilibrium code [000030000040000], is 11072.

After converting the plaintext to the error vector based on equilibrium coding, it is necessary to fix elements of the set of plaintexts corresponding to the position vector {0 0 0 1 0 1 0}.

Based on the algorithm in Fig. 1, we obtain sets of position vectors of the set $\{M_F\}$ (for $GF(2^3)$ – 21 vectors).

Thus, for the set of keys, it is necessary to fix the vectors corresponding to the position vectors {1 1 0 0 0 0}, {1 0 1 0 0 0}, {1 0 0 0 1 0 0}, {0 1 0 0 1 0 0}, {1 0 0 0 0 0 1}, {0 0 1 0 0 0 1}, {0 0 0 1 0 1 0} and {0 0 0 0 1 0 1}. This set forms the initialization vector IV_1.

Thus, the presented example confirms the theoretical proposals in the practical modification of the Niederreiter crypto-code system on *MEC*.

6. Discussion of the study results of energy costs for the Niederreiter crypto-code system practical implementation

One of the main criteria for the use of cryptographic protocols is the cryptographic resistance of the system to modern attacks. Asymmetric cryptosystems relate to models of provable security, which is based on theoretical and complexity problems. However, their cryptographic strength with increasing computing power in the era of high technology is limited to individual indicators. In relation to crypto-code systems, this indicator is the power of the field in which the matrices of the closed (masking matrix) and open (generating matrix) keys are formed. Reducing the field power leads to a decrease in cryptographic strength of the entire crypto-code system. In addition, the use of classical error-correcting codes is subject to the attack of V. Sidelnikov and can be used by intruders. Compensation for the field power reduction and an effective mechanism to fight the V. Sidelnikov's attack is the use of algebraic-geometry codes – codes that are built on the algorithms of the noise-tolerant coding theory using elements (derived points) of the third-kind geometric curve. The approach of forming shortened elliptic codes proposed in this paper increases the entropy of the transmitted codeword (serves as an additional session key) and, accordingly, increases the cryptographic strength of the transmitted data and the system as a whole.

In [8], the results of estimating the complexity of the formation of the cryptogram M of its decoding, assessing the complexity of hacking by the most effective decoding method (permutation decoder) are presented. The analysis of the results in [8] confirms the guaranteed level of cryptographic strength in the implementation of the Niederreiter CCS on *MEC*, an increase in the rate of crypto-transformations – coding by 3 times, decoding by 5 times due to a decrease in the field power during the practical implementation of Niederreiter CCS. Additional key data – initialization vectors IV_1, IV_2 provide an additional level of cryptographic strength and are used as session keys. However, their use increases the total number of operations in the implementation of CCS.

To evaluate the proposed coding and decoding algorithms in the Niederreiter CCS on *MEC*, it is proposed to use the approach described in [18].

To estimate the time and speed indicators, it is customary to use the unit of measurement cpb, where *cpb* (*cycles per byte*) is the number of processor cycles that need to be spent for processing 1 byte of incoming information.

The complexity of the algorithm is calculated by the formula [18]:

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

where Utl is the core utilization (%); $Rate$ is the algorithm bandwidth (byte/sec).

Table 1 shows the results of studies of the dependence of the length of the *EC* (*MEC*) code sequence of the code in the Niederreiter CCS on the number of processor cycles for performing elementary operations in the software implementation of crypto-code systems.

Table 2 shows the results of studies assessing the time and speed indicators of the procedures for the formation and decoding of information in the Niederreiter CCS on *EC* (*MEC*).

The analysis of Tables 1, 2 showed a reduction in energy costs in the implementation of crypto-code systems on *MEC* despite the complexity of the general algorithm. This is due to the fact that the fixation of the set of plaintexts occurs once during key generation. Thus, despite the need for additional energy consumption for the algorithm for generating initialization vectors IV_1, IV_2 (forming the set of fixed position plaintext sets $\{M_F\}$ and the set of shortening positions), the total cost of practical implementation of the Niederreiter MCCS on *MEC* does not exceed the cost of the classical scheme.

The main advantages of the proposed approach are the possibility of implementing a crypto-code system on almost any platform (achieved by reducing the field power), ensuring the required level of cryptographic strength of the system as a whole (achieved using modified (shortened) elliptical codes and additional session keys – IV_1, IV_2 initialization vectors). Alternative solutions proposed in [16, 23, 24] do not take into account the possibility of hacking a cryptosystem by the V. Sidelnikov's attack, and therefore cannot provide a guaranteed level of system security in general.

Table 1

The results of studies of the *EC* (*MEC*) code sequence length dependence of the code in the Niederreiter CCS on the number of processor cycles

Code sequence length		*Niederreiter* on *EC*			*Niederreiter* on *MEC*		
		10	100	1,000	10	100	1,000
Number of function calls implementing elementary operations	Character reading	1,160 342	2,502 422	15,923 222	1,148 738	2,477 397	15,763 989
	String comparison	381 020	777 560	4 742 960	377 209	759 784	4 695 530
	String concatenation	192 770	411 380	2 597 480	190 842	407266	2 571 505
Sum		1 734 132	3 691 362	23 263 662	1 716 790	3 654 448	23 031 025
Duration of the functions * in processor cycles	Character reading	31 329	67 565	429 927	31 015	64 889	425 627
	String comparison	20 575	41 988	256 120	21 369	41 568	253 558
	String concatenation	57 253	122 180	771 452	56 680	120 958	763 737
Sum		109 157	231 733	1 457 498	108 065	229 415	1 442 923
Duration of execution ** in ms		0.06	0.12	0.77	0.07	0.12	0.75

*Note: * – duration of 1,000 operations in processor cycles: character reading – 27 cycles, string comparison – 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 of 5 % is taken*

Table 2

The results of studies assessing the time and speed indicators of the procedures for the formation and decoding of information

Code	Number of calls	Code sequence length	Algorithm throughput rate (bytes/sec)	Core utilization (%)	Algorithm complexity, *Per(cpb)*
EC	functions implementing elementary operations	100	46,125,790	56	61.5
		1,000	120,639,896	56	62.0
MEC		100	48,659,872	56	62.5
		1,000	117,421,311	56	63.5

The proposed approach can be used in Internet protocols and is an alternative to using RSA cryptosystems in them.

A promising direction for further research is the further reduction of energy costs for the practical implementation of the Niederreiter MCCS on *MEC*.

7. Conclusions

1. Experimental studies of the Niederreiter crypto-code system on *MEC* revealed the main reason for the impossibility of the practical decoding algorithms implementation when using non-binary codes in the classical scheme. It has been found that it is necessary to fix a subset of plaintexts for which the error localization procedure, with the X, P and D (private key) masking matrices selected by the sender, cannot be performed. The obtained practical result allows us to "weed out" the sets of the error vector, which, however, allow using the classical variant of information decoding on the receiving side when using the classical Niederreiter scheme on m-th codes.

2. The proposed algorithms for coding and decoding modified (shortened) elliptic codes in the Niederreiter crypto-code system ensures its practical implementation. Reducing the field power when building the classic Niederreiter scheme allows reducing the amount of transmitted data by shortening the error vector before generating the syndrome on the sender side and, accordingly, the energy costs of its implementation. The use of algebraic-geometric codes (codes on elliptic curves) and their modifications eliminates the possibility of V. Sidelnikov's attack (finding the check matrix of the error-correcting code), which significantly enhances the cryptographic strength of the system in post-quantum cryptography. This approach ensures the competitiveness of the proposed Niederreiter crypto-code system and makes it possible to consider as an alternative to RSA in Internet technology protocols.

References

1. Grishchuk R. V., Danik Yu. G. Osnovy kiberbezopasnosti: monografiya / Yu. G. Danik (Ed.). Zhitomir: ZHNAEU, 2016. 636 p.
2. Kiberprostranstvo i informacionnyy terrorizm. URL: http://vpoanalytics.com/2016/02/15/kiberprostranstvo-i-informacionnyj-terrorizm/
3. Security requirements for cryptographic modules. URL: https://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
4. Zabezpechennia informatsiynoi bezpeky derzhavy: monohrafyia / Ivanchenko I. S., Khoroshko V. O., Khokhlachova Yu. Ye., Chyrkov D. V. Kyiv: PVP "Zadruha", 2013. 170 p.
5. Bezpeka bankivskoi diyalnosti: monohrafiya / Kazakova N. F., Panfilov V. I., Skachek L. M., Skopa O. O., Khoroshko V. O. Kyiv: PVP "Zadruha", 2013. 282 p.
6. Leonenko G. P., Yudin A. Yu. Problemy obespecheniya informacionnoy bezopasnosti sistem kriticheski vazhnoy informacionnoy infrastruktury Ukrainy // Information Technology and Security. 2013. Issue 1. P. 44–48.
7. Evseev S., Korol' O., Koc G. Analysis of the legal framework for the information security management system of the NSMEP // Eastern-European Journal of Enterprise Technologies. 2015. Vol. 5, Issue 3 (77). P. 48–59. doi: https://doi.org/10.15587/1729-4061.2015.51468
8. Yevseiev S., Tsyhanenko O. Development of asymmetrical crypto-coded construction of niderraiter on modified codes // Systemy obrobky informatsiyi. 2018. Issue 2 (153). P. 127–135. doi: https://doi.org/10.30748/soi.2018.153.16
9. Kazakova N., Pleshko E., Aivazova K. International regulation of regulatory of documents as well standardization in area audit of information security // Visnyk Skhidnoukrainskoho natsionalnoho universytetu imeni Volodymyra Dalia. 2013. Issue 15. P. 172–181.
10. Approaches to selection of combinatorial algorithm for optimization in network traffic control of safety-critical systems / Kuchuk G., Kharchenko V., Kovalenko A., Ruchkov E. // 2016 IEEE East-West Design & Test Symposium (EWDTS). 2016. doi: https://doi.org/10.1109/ewdts.2016.7807655
11. Multiservice network security metric / Mozhaev O., Kuchuk H., Kuchuk N., Mozhaev M., Lohvynenko M. // 2017 2nd International Conference on Advanced Information and Communication Technologies (AICT). 2017. doi: https://doi.org/10.1109/aiact.2017.8020083
12. Report on Post-Quantum Cryptography / Chen L., Jordan S., Liu Y.-K., Moody D., Peralta R., Perlner R., Smith-Tone D. // NIST. 2016. doi: https://doi.org/10.6028/nist.ir.8105
13. Dinh H., Moore C., Russell A. McEliece and Niederreiter Cryptosystems that Resist Quantum Fourier Sampling Attacks // CRYPTO'11 Proceedings of the 31st annual conference on Advances in cryptology. Santa Barbara, 2011. P. 761–779. URL: https://dl.acm.org/citation.cfm?id=2033093
14. Achieving 128-bit Security Against Quantum Attacks in OpenVPN. URL: https://internetscriptieprijs.nl/wp-content/uploads/2017/04/1-Simon-de-Vries-UT.pdf
15. A Side-Channel Assisted Cryptanalytic Attack Against QcBits / Rossi M., Hamburg M., Hutter M., Marson M. E. // Lecture Notes in Computer Science. 2017. P. 3–23. doi: https://doi.org/10.1007/978-3-319-66787-4_1

16. Enhanced public key security for the McEliece cryptosystem / Baldi M., Bianchi M., Chiaraluce F., Rosenthal J., Schipani D. 2014. URL: https://arxiv.org/pdf/1108.2462.pdf
17. Cho J. Y., Griesser H., Rafique D. A McEliece-Based Key Exchange Protocol for Optical Communication Systems // Lecture Notes in Electrical Engineering. 2017. P. 109–123. doi: https://doi.org/10.1007/978-3-319-59265-7_8
18. Development of mceliece modified asymmetric crypto-code system on elliptic truncated codes / Yevseiev S., Rzayev K., Korol O., Imanova Z. // Eastern-European Journal of Enterprise Technologies. 2016. Vol. 4, Issue 9 (82). P. 18–26. doi: https://doi.org/10.15587/1729-4061.2016.75250
19. Evseev S. P., Korol O. H. Teoretyko-metodolohichni zasady pobudovy hibrydnykh krypto-kodovykh konstruktsiy na zbytkovykh kodakh. Informacionnaya ekonomika: etapy razvitiya, metody upravleniya, modeli: monografiya. Kharkiv, VSHEM – HNEU im. S. Kuzneca, 2018. P. 233–280.
20. Sidel'nikov V. M. Kriptografiya i teoriya kodirovaniya // Materialy konferencii "Moskovskiy universitet i razvitie kriptografii v Rossii". Moscow, 2002.
21. Dudykevych V. B., Kuznetsov O. O., Tomashevskyi B. P. Krypto-kodovyi zakhyst informatsiyi z nedviykovym rivnovahovym koduvanniam // Suchasnyi zakhyst informatsiyi. 2010. Issue 2. P. 14–23.
22. Dudykevych V. B., Kuznietsov O. O., Tomashevskyi B. P. Metod nedviikovoho rivnovahovoho koduvannia // Suchasnyi zakhyst informatsiyi. 2010. Issue 3. P. 57–68.
23. Zhang G., Cai S. Secure error-correcting (SEC) schemes for network coding through McEliece cryptosystem // Cluster Computing. 2017. doi: https://doi.org/10.1007/s10586-017-1294-5
24. Morozov K., Roy P. S., Sakurai K. On unconditionally binding code-based commitment schemes // Proceedings of the 11th International Conference on Ubiquitous Information Management and Communication – IMCOM '17. 2017. doi: https://doi.org/10.1145/3022227.3022327
25. Zhang G., Cai S. Universal secure error-correcting (SEC) schemes for network coding via McEliece cryptosystem based on QC-LDPC codes // Cluster Computing. 2017. doi: https://doi.org/10.1007/s10586-017-1354-x
26. Moufek H., Guenda K. A New variant of the McEliece cryptosystem based on the Smith form of convolutional codes // Cryptologia. 2017. Vol. 42, Issue 3. P. 227–239. doi: https://doi.org/10.1080/01611194.2017.1362061
27. Biswas B., Sendrier N. McEliece Cryptosystem Implementation: Theory and Practice // Lecture Notes in Computer Science. 2008. P. 47–62. doi: https://doi.org/10.1007/978-3-540-88403-3_4
28. Yevseiev S., Rzayev Kh., Tsyhanenko A. Analysis of the software implementation of the direct and inverse transform in non-binary equilibrium coding method // Ukrainian Scientific Journal of Information Security. 2016. Vol. 22, Issue 2. P. 196–203.
29. Niederreiter H. Knapsack-Type Cryptosystems and Algebraic Coding Theory // Problems of Control and Information Theory. 1986. Vol. 15, Issue 2. P. 19–34.
30. A statistical test suite for random and pseudorandom number generators for cryptographic applications / Rukhin A., Sota J., Nechvatal J., Smid M., Barker E., Leigh S. et. al. // NIST Special Publication. 2000. doi: https://doi.org/10.6028/nist.sp.800-22