UDC 004.056 doi: https://doi.org/10.20998/3083-6298.2025.02.10

Vadym Stetsenko[1], Pierre Murr[2], Andrii Tkachov[1], Oleksandr Laptiev [3], Marharyta Melnyk[4]

[1] National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine
[2] International University of Science and Technology in Kuwait, Ardiya Government Area, Kuwait
[3] Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
[4] Science Entrepreneurship Technology University, Kyiv, Ukraine

McELIECE AND NIEDERREITER CRYPTOCODE STRUCTURE MODELS

Abstract. The relevance of the research lies in ensuring information security by creating cryptographic solutions that combine high performance, resistance to quantum attacks and the possibility of effective implementation in resource-limited devices. **The subject of study** is the approaches and strategies for using code cryptosystems, in particular the McEliese and Niederreiter crypto-code constructions, as basic mechanisms for building cryptographic systems resistant to attacks. **The purpose of the article** is to substantiate the prospects of using code cryptosystems as basic mechanisms for building cryptographic systems resistant to attacks on quantum computers. To develop algorithms for generating and decoding cryptograms, to analyze their algorithmic complexity. **Research results**. The prospects for using code cryptosystems as basic mechanisms for building cryptographic systems are substantiated. The algorithms for generating and decoding cryptograms were developed, their algorithmic complexity was analyzed, and the potential for integrating such structures into real systems was assessed. **Conclusion.** The study allows reveal advantages of a systematic approach in planning speed of action thanks to previous calculation syndromes. The solutions for algorithmic difficulties indicate a high efficiency crypto protection, which makes them suitable for use in modern information systems.

Keywords: crypto-code construction, cybersecurity, cryptosystem, algorithmic complexity, model, confidentiality, integrity

Introduction

The relevance of the problem and analysis of literary sources. In the context of intensive development of quantum computing, cloud technologies and mass use of IoT devices, ensuring cryptographic stability of information systems becomes a critically important task. Traditional public-key cryptosystems, such as RSA or ECC, are vulnerable to attacks on quantum computers due to the Shor and Grover algorithms. This makes the development of post-quantum cryptographic systems based on mathematical problems that remain difficult even for quantum computers relevant. Among such approaches, a special place is occupied by code cryptosystems, in particular the McEliese and Niederreiter crypto-code constructions, which are based on the complexity of decoding linear codes in the general case.

In recent years, significant progress has been observed in the study and optimization of code cryptosystems. Thus, in work [1], modifications of the McEliese cryptosystem based on elliptic codes are analyzed, which allow to increase the encryption performance and reduce the size of the keys. The authors demonstrate that the use of algebrogeometric codes, in particular codes on elliptic curves, provides high coding density and decoding efficiency, which is important for use in resource-dependent environments. Another important direction is the study of the computational complexity of crypto-code constructions. In work [2], a detailed analysis of the algorithmic complexity of the coding and decoding processes in Niederreiter-type cryptosystems is carried out, in particular using systematic and non-systematic approaches. The authors show that systematic coding allows to reduce the time of cryptogram formation due to the preliminary calculation of syndromes, which increases the system speed. This is consistent with the results given in the downloaded document, which compares the complexity of operations for different implementation options. Particular attention is paid to the security of cryptosystems based on elliptic codes. The study [3] considers vulnerabilities associated with the error localization procedure, in particular the use of Chen's algorithm, which is mentioned in the downloaded material. The authors propose a modified approach to checking the roots of the error locator polynomial, which reduces the probability of a successful information rack attack. In addition, the work [4] investigated the integration of crypto-code structures into practical data protection systems, in particular in blockchain technologies and electronic voting systems. It is shown that the use of codes with high error correction capabilities allows to simultaneously ensure confidentiality, integrity and resistance to quantum attacks. Thus, the analysis of scientific sources indicates a growing interest in code cryptosystems, especially based on elliptic and algebrogeometric codes. The relevance of the topic lies in the need to create cryptographic solutions that combine high performance, resistance to quantum attacks and the possibility of effective implementation in resource-limited devices. The results presented in the downloaded document regarding algorithmic complexity and decoding procedures are relevant and correspond to current trends in the development of post-quantum cryptography.

The purpose of the research is to substantiate the prospects of using code cryptosystems, in particular the McEliese and Niederreiter crypto-code constructions, as basic mechanisms for building cryptographic systems resistant to attacks on quantum computers. To investigate the resistance of such systems to known attacks, in particular at the stage of error localization using the Chen algorithm, and to propose ways to improve security and performance. To develop algorithms for generating and decoding cryptograms, to analyze their algorithmic complexity.

1. McEliece and Niederreiter's crypto-code construction models

The mathematical model of an asymmetric cryptosystem for information protection using algebrogeometric block codes based on the McEliese crypto-code construction is formally defined by the set of the following elements:

– set of information sequences $M=\{\mathrm{M}_1,\mathrm{M}_2,...,\mathrm{M}_{\mathrm{q}^k}\}$, where $M_i=\{\mathrm{I}_0,\mathrm{I}_{\mathrm{h}_1},..\ \mathrm{I}_{\mathrm{h}_j},\mathrm{I}_{\mathrm{k-1}}\}$, $\forall \mathrm{I}_j \in GF(q)$;

– set of cryptograms (codograms) $C=\{\mathrm{C}_1,\mathrm{C}_2,...,\mathrm{C}_{\mathrm{q}^k}\}$, where $C_i=(c^*_{X_0},c^*_{h_1},...,c^*_{h_j},c^*_{X_{n-1}})$, $\forall c^*_{X_j}\in GF(q)$;

– cryptographic transformation – formation of a cryptogram (codogram): $\phi=\{\phi_1,\phi_2,...,\phi_s\}$, where $\phi_i: M\to C_k$, $i=1,2,...,s$;

– set of inverse cryptotransformations – decoding codegrams : $\phi^{-1}=\{\phi_1^{-1},\phi_2^{-1},...,\phi_s^{-1}\}$, where $\phi_i^{-1}: C_k\to M$, $i=1,2,...,s$;

– set of public keys:

$$K_{a_i}=\{K_{1_{a_i}},K_{2_{a_i}},...,K_{s_{a_i}}\}= =\{G_X^{EC_1}{}_{a_i},G_X^{EC_2}{}_{a_i},...,G_X^{ECs}{}_{a_i}\},$$

where $G_X^{ECi}{}_{a_i}$ is the public key of the crypto conversion:

$\phi_i: M\xrightarrow{K_{ia_i}} C_{k-h_j}$; $i=1,2,...,s$;

$G_X^{ECu}=X^u\times G^{EC}\times P^u\times D^u$, $u\in\{1,2,...,s\}$;

– a $_i$ – the set of coefficients of the polynomial ES, ∀a $_i$ ∈GF(q);

– set of private (private) keys – masking matrices:

$$K^*=\{\mathrm{K}_1^*,\mathrm{K}_2^*,...,\mathrm{K}_s^*\}= =\{\{\mathrm{X,P,D}\}_1,\{\mathrm{X,P,D}\}_2,...,\{\mathrm{X,P,D}\}_s\}= =\{X^i,P^i,D^i\};$$

$G_X^{ECu}=X^u\cdot G^{EC}\cdot P^u\cdot D^u$, $u\in\{1,2,...,s\}$,

where G^{EC} – generating $n\times k$ matrix algebrogeometric block (n,k,d) code with elements from $GF(q)$, based on use chosen by the user coefficients of the polynomial of the curve a $_1$ ... a $_6$, ∀a $_i$ ∈GF(q) , uniquely specifying a specific set of points curve from spaces P ^{2}.

The formal mathematical description of the formation of a cryptogram is determined by the expression:

$$C_j=\phi_u\left(M_i,G_X^u\right)=M_i\cdot\left(G_X^u\right)^T+e, \quad (1)$$

where the weight of the vector e is determined by:

$$0\le w(e)\le t=\left\lfloor\frac{d-1}{2}\right\rfloor. \quad (2)$$

On the receiving side, due to knowledge of the private (private) key, the authorized user uses bijective transformations and a decoding algorithm. Berlekamp - Messi [6-9]:

$$M_i=\phi_u^{-1}\left(C_j,\{\mathrm{X,P,D}\}_\mathrm{u}\right). \quad (3)$$

– removes the effect of masking matrices P^u and D^u :

$$C=C_j\times\left(D^u\right)^{-1}\times\left(P^u\right)^{-1}= =\left(M_i\times\left(X^u\times G\times P^u\times D^u\right)^T+e\right)\times \times\left(D^u\right)^{-1}\times\left(P^u\right)^{-1}= =M_i\times\left(X^u\right)^T\times\left(G\right)^T+e\times\left(D^u\right)^{-1}\times\left(P^u\right)^{-1}.$$

– decodes the received vector using the Berlekamp - Messy algorithm [10,11]:

$$C=M_i\times\left(X^u\right)^T\times\left(G^{EC}\right)^T+e\times\left(D^u\right)^{-1}\times\left(P^u\right)^{-1}.$$

– removes the masking matrix $\left(X^u\right)$:

$$\left(M_i\times\left(X^u\right)^T\right)\times\left(X^u\right)^{-1}=M_i.$$

Let us consider a formal description of the mathematical model of the asymmetric Niederreiter cryptosystem, which is formally defined by a set of elements [12,13]:

– set of plaintexts $M=\left\{M_1,M_2,...M_{q^k}\right\}$;

– set of closed texts (syndromes) $S=\left\{S_0,S_1,...S_{q^r}\right\}$, $\forall S_i\in GF(q), i\in\overline{1\ldots q^r}$;

– set of direct cryptotransformations: $\varphi=\left\{\varphi_1,\varphi_2,...,\varphi_r\right\}$, where $\varphi_i: M\to S_r$, $i=1,2,...,e$;

– set of inverse cryptotransformations: $\varphi^{-1}=\left\{\varphi_1^{-1},\varphi_2^{-1},...,\varphi_r^{-1}\right\}$, where $\varphi_i^{-1}: S_r\to M$, $i=1,2,...,e$;

– set of public keys: $KU_{a_i}=\left\{KU_{1_{a_i}},KU_{2_{a_i}},...,KU_{r_{a_i}}\right\}= =\left\{H^{EC_1}_{X_{a_i}},H^{EC2}_{X_{a_i}},...,H^{ECr}_{X_{a_i}}\right\}$, where $H^{EC_i}_{X_{a_i}}$ is a check r×n matrix with elements $GF(q)$, a_i – a set of coefficients of the polynomial of the curve $a_1 \ldots a_6$, a_i GF (q), which uniquely defines a specific set of points of the curve from the space P^2;

– set of private (private keys: $KR = \{\{X,P,D\}_1,\{X,P,D\}_2,...,\{X,P,D\}_r\} = = \{X^i,P^i,D^i\}$.

Based on equilibrium coding, the information sequence is converted into an error vector, which is used in the mathematical model of cryptogram formation.

The formal description of the mathematical model of cryptogram formation is determined by the rule:

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

and the Hamming weight (number of non-zero elements) of the vector e does not exceed the correcting ability of the algebraic block (n,k,d) code used:

$$\forall i: 0 \le w(M_i) \le t = \left\lfloor \frac{d-1}{2} \right\rfloor.$$

The cardinality of the sets M and C is determined by the admissible spectrum of weights $w(M_i)$, , i.e. in the general case (for all admissible values of $w(M_i)$) we have:

$$m = \sum_{i=0}^{t} (q-1)^i \times C_n^i, \quad (4)$$

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

The public key is formed by multiplying the check matrix of the algebrogeometric code by the masking matrix:

$$H_X^{ECu} = X^u \times H \times P^u \times D^u,\ u \in \{1,2,...,s\}, \quad (5)$$

where H^{EC} is the verification $n \times (n-k)$ matrix of the algebrogeometric block (n,k,d) code with elements from $GF(q)$.

On the receiving side, the authorized user uses a private (private key):

$$S^*_r = c^*_{X_i} \cdot H^T_{X_j}, \quad (6)$$

that is finds a vector $c^*_{X_i}$:

$$c^*_{X_i} = c_{X_i} \times H^T_{X_j} = 0.$$

Next, a decoding sequence is used, as in the McEliece crypto-code construction.

To restore the information equilibrium sequence, M_i it is sufficient to multiply the vector again M_i^u by the masking matrices D^u and P^u, but in a different order:

$$M_i = M_i^u \times P^u \times D^u = = M_i \times \left(D^u\right)^{-1} \times \left(P^u\right)^{-1} \times P^u \times D^u = M_i. \quad (7)$$

When decrypting a cryptogram (after obtaining the error vector), the inverse equilibrium coding algorithm is used.

McEliese and Niederreiter crypto-code constructions based on ES.

First, we will consider algorithm for forming a cryptogram (codogram) in the McAleese crypto-code construction.

The algorithm for forming a codegram is presented as a sequence of the following steps:

Step 1. Enter the information to be encrypted. Enter the public key G_X^{EC}.

Step 2. Encoding information with an elliptic code. Formation of a codeword with X elliptic code given by the matrix G_X^{EC}.

Step 3. Formation of an error vector e, the weight of which does not exceed ≤t – the ability of the elliptic code to detect and correct errors.

Step 4. Formation of the codegram:

$$c^*_X = c_X + e.$$

Step 5. Completion of work. The end.

Cryptogram (codogram) decoding algorithm in McAleese crypto-code construction on the receiving side is described by the following steps:

Step 1. Enter the codegram c^*_X, which is to be decoded. Input of the private key – matrices X, P, D.

Step 2. Removing the action of diagonal and permutation matrices:

$$\bar{c}^* = c^*_X \times D^{-1} \times P^{-1}.$$

Step 3. Vector decoding $\bar{c}^*$. Formation of vector i'.

Step 4. Removing the action of the matrix X: i = i ' · X-1. Formation of the desired information vector i.

Step 5. Completion of work. The end.

The main stage of the developed algorithm for decoding codegrams is vector decoding (step 3). Let us present, with minor changes, the scheme for decoding the algebra of algebrogeometric codes proposed in [7], and estimate the complexity of the algorithm for decoding elliptic codes.

The task of decoding an algebrogeometric code is to find the error vector e = (e_0, e_1, …, e_{n-1}) for the known syndrome sequence S = (S_0, S_1, …, S_{r-1}).

Let us consider as generating functions homogeneous monomials of degree *degF*. Each such monomial is written in the form:

$$f_{lmp} = x^l y^m z^p,\ l + m + p = degF. \quad (8)$$

On the set of projective points of the curve *X*, represented in homogeneous coordinates in the form *P (X, Y, 1)*, the values of the generating functions will take the form, $f_{lm} = X_i^l Y_i^m$, *i = 0. n – 1*, *l + m≤ degF*. The verification matrix *H* is written as:

$$H = \begin{pmatrix} 1 & 1 & ... & 1 \\ X_0 & X_1 & ... & X_{n-1} \\ ... & ... & ... & ... \\ Y_0^{\deg F} & Y_1^{\deg F} & ... & Y_{n-1}^{\deg F} \end{pmatrix} \quad (9)$$

Elements of a syndrome sequence as elements of a vector $\|S_{lm}\|_r$, we calculate according to the rule:

$$S_{lm} = \sum_{i=0}^{n-1} c_i^* X_i^l Y_i^m = \sum_{i=0}^{n-1} e_i X_i^l Y_i^m \text{ , } l + m \le deg, \quad (10)$$

or, in matrix form,

$$\|S_{lm}\|_r = H \left\|c_n^*\right\|_n^T = \left\|X_i^l Y_i^m\right\|_{n,r} \|e_i\|_n^T . \quad (11)$$

Thus, the problem of decoding an algebrogeometric code constructed by mapping projective points *P (X, Y, 1)* by a curve with homogeneous monomials of degree *degF* is equivalent to the problem of solving a system of *r = d + g – 1* nonlinear equation in *3t* variables.

To solve this problem, we will use an artificial technique, which consists in introducing into consideration a polynomial of error locators, the solutions of which uniquely localize (indicate the location of) the errors that have occurred.

Let us define the polynomial of error locators of an algebrogeometric code as a polynomial in two variables, degree *≤(t – 1)*:

$$a_{00} + a_{10}x + ... + y^{t-1} = 0, \quad (12)$$

where *t* is the number of errors that the algebraic-geometric code can correct.

Multiplying both parts of the polynomial (12) by e_i and summing over all *i = 0... n – 1*, the value at the point *(x = X*$_i$*, y = Я*$_i$*),* we obtain the recurrent expression:

$$a_{00}S_{00} + a_{10}S_{10} + ... + S_{0\,t-1} = 0, \quad (13)$$

which defines a system of linear equations with respect to the unknown coefficients of the polynomial of error locators.

In matrix form, the system of linear equations is written as:

$$\begin{pmatrix} S_{00} & S_{10} & ... & S_{1\,t-2} \\ S_{10} & S_{20} & ... & S_{2\,t-2} \\ ... & ... & ... & ... \\ S_{1\,t-2} & S_{0\,t-2} & ... & S_{2\,2t-4} \end{pmatrix} \times$$

$$\times \begin{pmatrix} a_{00} \\ a_{10} \\ ... \\ a_{1\,t-2} \end{pmatrix} = \begin{pmatrix} -S_{0\,t-1} \\ -S_{1\,t-1} \\ ... \\ -S_{1\,2t-3} \end{pmatrix} . \quad (14)$$

After finding the coefficients of the error locator polynomial, the error localization procedure consists in substituting all possible locators and selecting those that reduce the error locator polynomial to zero. This procedure is known in the literature as Chen's procedure [20-25]. When decoding algebraic geometric codes, all pairs of locator polynomials are substituted, identifying all projective points of the curve given in homogeneous coordinates *P (X, Y, 1)*.

Fig. 1 and Fig. 2 show the algorithms for cryptogram formation and decoding based on Niederreiter's crypto-code construction.

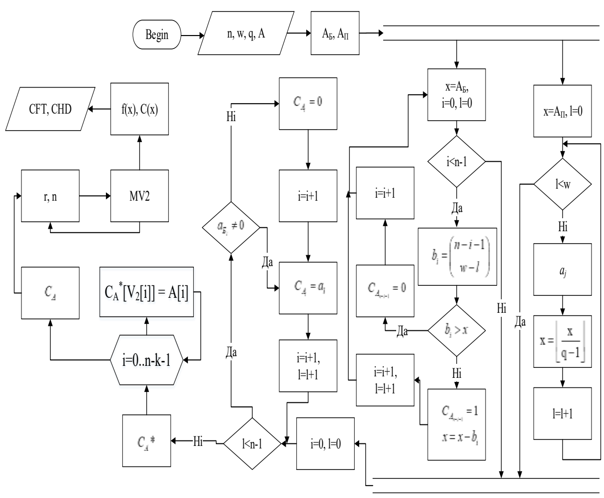

Fig. 1. Encryption algorithm in the Niederreiter crypto-code on elliptic codes

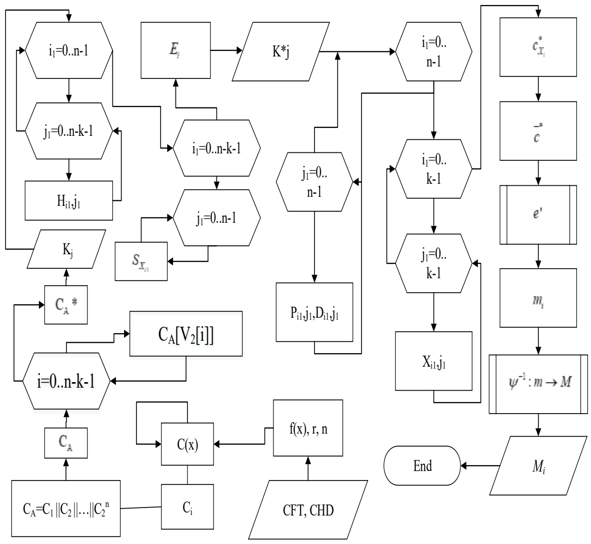

Fig. 2. Decryption algorithm in the Niederreiter crypto-code system using elliptic codes

During the research, asymmetric crypto-code structures based on elliptic codes were developed, as well as algorithms for generating and decoding codegrams. Based on the obtained relations that determine the relationship between the parameters of elliptic codes and asymmetric crypto-code structures, an analysis of the computational complexity of the processes of encoding and decoding codegrams was carried out. The results of experimental studies showed that asymmetric crypto-code structures based on elliptic codes are characterized by high performance and demonstrate potential stability.

2. Coding complexity research materials

Table 1 presents the results of research into the algorithmic complexity of systematic and non-systematic coding algorithms using elliptic codes in McEliese and Niederreiter crypto-code constructions.

Table 1 – **Algorithmic complexity of systematic and non-systematic coding algorithms in crypto-code constructions**

Parameter of Coding	*Complexity in Crypto-Code Construction*		
	Mac-Eliece (coding, number of addition and multiplication operations)		*Niederreiter (number of addition and multiplication operations)*
	systematic	*non-systematic*	
Computation of syndrome vector	k×r	k×n	-
Computation of parity-check vector	k×r	k×n	-
Complexity of systematic coding algorithm without considering the complexity of generator function computation	O(3×degF×n)	O(3×degF×n)	-
Complexity of cryptogram generation algorithm	O((r+l) ×n) or O(4×degF×n)	O((k+l) ×n) or O(4×degF×n)	O(3×degF×n) or O(d×n)
Complexity of cryptogram decoding algorithm	$O(2×n^2+k^2+4t^2+(t^2+t-2)^2/4)$	$O(2×n^2+k^2+4t^2+(t^2+t-2)^2/4)$	$O(5×n^2+4t^2+(t^2+t-2)^2/4)$

During the research, asymmetric crypto-code structures based on elliptic codes were developed, as well as algorithms for generating and decoding codegrams. Based on the obtained relations that determine the relationship between the parameters of elliptic codes and asymmetric crypto-code structures, an analysis of the computational complexity of the processes of encoding and decoding codegrams was carried out. The results of experimental studies showed that asymmetric crypto-code structures based on elliptic codes are characterized by high performance and demonstrate potential stability.

3. Discussion of results

The conducted research highlights the feasibility and efficiency of using code-based cryptosystems, particularly the McEliece and Niederreiter constructions, as a reliable foundation for post-quantum cryptographic mechanisms. The comparative analysis of systematic and non-systematic coding demonstrated that systematic approaches provide advantages in reducing encryption time through pre-computed syndromes, which is critical for high-speed applications. At the same time, the study of vulnerabilities, such as those linked to Chen's algorithm, revealed the need for modified error localization procedures that significantly enhance cryptographic resilience.

The obtained results confirm that code-based constructions not only ensure confidentiality and integrity of data but also exhibit strong resistance against quantum algorithms such as Shor and Grover. This makes them highly relevant for integration into practical systems, including blockchain networks and electronic voting platforms. Moreover, the demonstrated potential for implementation in resource-constrained environments, such as IoT devices and embedded systems, emphasizes the practical importance of the proposed solutions.

4. Conclusions and prospects for further development

In the course of the work, the prospects of using code cryptosystems, in particular the McEliese and Niederreiter crypto-code constructions, as a basis for building cryptographic solutions resistant to threats arising in connection with the development of quantum computing were substantiated. In the context of the vulnerability of traditional public-key cryptosystems, such as RSA and ECC, to quantum attacks based on the Shor and Grover algorithms, post-quantum cryptographic mechanisms based on difficult-to-solve mathematical problems, in particular the complexity of decoding linear block codes, acquire special importance. In this context, considerable attention is paid to algebrogeometric codes, in particular codes on elliptic curves, which combine high cryptographic stability with the efficiency of implementation in resource-dependent environments.

The scientific research focuses on the analysis of mathematical models of crypto-code constructions, the development and optimization of encryption and decryption algorithms, as well as on the assessment of their computational complexity and resistance to existing attacks. Special attention is paid to the error localization procedure, in particular, to vulnerabilities associated with the use of Chen's algorithm, for which modified approaches aimed at increasing crypto-resistance are proposed. A comparison of systematic and unsystematic coding was carried out, which allowed to identify advantages of a systematic approach in planning speed thanks to previous calculation syndromes. Obtained results of algorithmic difficulties indicate a high efficiency proposed decisions that make them suitable for use in modern information systems. In addition, research has been conducted possibility integration of such structures into practical applications, particularly in blockchain technology and systems electronic voting, where they provide not only confidentiality and integrity data, but also resilience to future quantum attacks.

Thus, the work makes a significant contribution contribution to development post-quantum cryptography, offering comprehensive, well-founded and practically oriented approach to creation secure and efficient cryptosystems based on theories coding. A promising direction is the implementation of code cryptosystems in resource-intensive environments, in particular in IoT devices, embedded systems, and mobile platforms, where minimizing key sizes and computational costs is important.

In this context, further research should focus on creating compact implementations of codes with high remediation capabilities, which will allow for effective data protection even on devices with limited computing resources.

References

1. Alsadie, D., Baldi, M., Chiaraluce, F. and Santini, P. (2021), "Enhancing the McEliece Cryptosystem Based on Polar Codes and Its Application to IoT", *IEEE Access,* 9, pp. 145678–145692, https://doi.org/10.1109/ACCESS.2021.3123456
2. Gaborit, P., Hauteville, A. and Tillich, J.-P. (2022), "Quantum Security Analysis of the Niederreiter Cryptosystem", *Designs , Codes and Cryptography*, 90(3), pp. 557–581, https://doi.org/ 10.1007/s10623-022-01002-4
3. Couvreur, A. and Lequesne, M. (2023), "On the Security of Algebraic Geometry Codes Against Sidorenko Attacks", *IEEE Transactions on Information Theory*, 69(5), pp. 2890–2905, https://doi.org/10.1109/TIT.2023.3234567
4. Banegas, G. and Urbanowicz, J. (2024), "Code-Based Cryptography for Post-Quantum Blockchain Applications", *Cryptography*, 8(1), 12, https://doi.org / 10.3390/cryptography8010012
5. Kuchuk, H., Mozhaiev , O., Kuchuk, N., Tiulieniev, S., Mozhaiev, M., Gnusov, Y., Tsuranov, M., Bykova, T., Klivets , S. and Kuleshov, A. (2024), "Devising a method for the virtual clustering of the Internet of Things edge environment", *Eastern-European Journal of Enterprise Technologies* , vol. 1(9(127), pp. 60–71, doi: https://doi.org/10.15587/1729-4061.2024.298431
6. Hu, N. (2024), "Internet of things edge data mining technology based on cloud computing model", *International Journal of Innovative Computing, Information and Control* , vol. 20(6), pp. 1749–1763, doi : http://dx.doi.org/10.24507/ijicic.20.06.1749
7. Hunko, M., Tkachov, V., Kovalenko, A. and Kuchuk, H. (2023), "Advantages of Fog Computing: A Comparative Analysis with Cloud Computing for Enhanced Edge Computing Capabilities", *KhPI Week 2023 - Conference Proceedings* , pp. 1–5, doi: https://doi.org/10.1109/KhPIWeek61412.2023.10312948
8. Ding, H., Ding, X., Xia, F. and Zhou, F. (2023), "An Efficient Method for Implementing Applications of Smart Devices Based on Mobile Fog Processing in a Secure Environment", *International Journal of Advanced Computer Science and Applications* , vol.14(10), pp. 93–105, doi: https://doi.org/10.14569/IJACSA.2023.0141011
9. Kuchuk, H. and Malokhvii, E. (2024), "Integration of iot with Cloud, Fog and Edge computing: a review", *Advanced Information Systems* , vol. 8, no. 2, pp. 65–78, doi : https://doi.org/10.20998/2522-9052.2024.2.08
10. Routray, K. and Bera, P. (2024), "Fog-Assisted Dynamic IoT Device Access Management Using Attribute-Based Encryption", *ACM International Conference Proceeding Series*, pp. 346–352, doi: https://doi.org/10.1145/3631461.3631466
11. Mani Kiran, Ch.V.N.S., Jagadeesh Babu, B. and Singh, M.K. (2023), "Study of Different Types of Smart Sensors for IoT Application Sensors", *Smart Innovation, Systems and Technologies* , vol. 290, pp. 101–107, doi: https://doi.org/10.1007/978-981-19-0108-9_11
12. Kuchuk, N., Kashkevich, S., Radchenko, V., Andrusenko, Y. and Kuchuk, H. (2024), "Applying edge computing in the execution of IoT operative transactions", *Advanced Information Systems*, vol. 8, no. 4, pp. 49–59, doi: https://doi.org/10.20998/2522-9052.2024.4.07
13. Petrovska I., Kuchuk, H. and Mozhaiev M. (2022), "Features of the distribution of computing resources in cloud systems", *2022 IEEE 3rd KhPI Week on Advanced Technology* , doi: https://doi.org/10.1109/KhPIWeek57572.2022.9916459
14. Li, G., Liu, Y., Wu, J., Lin, D. and Zhao, Sh. (2019), "Methods of Resource Scheduling Based on Optimized Fuzzy Clustering

in Fog Computing", *Sensors* , vol. 19(9), doi: https://doi.org/10.3390/s19092122
15. Deng, R., Lu, R., Lai, C., Luan, T.H. and Liang, H. (2016), " Optimal workload allocation in fog-cloud computing toward balanced delay and power consumption", *IEEE Internet Thing* , Vol. 3, no. 6, pp. 1171–1181, doi: https://doi.org/10.1109/JIOT.2016.2565516
16. Kuchuk, N. , Kovalenko, A. , Ruban, I. , Shyshatskyi , A., Zakovorotnyi, O. and Sheviakov, I. (2023), " Traffic Modeling for the Industrial Internet of NanoThings ", *2023 IEEE 4th KhPI Week on Advanced Technology* , doi: http://dx.doi.org/10.1109/KhPIWeek61412.2023.10312856
17. Saurabh and Dhanaraj, R.K. (2024), "Enhance QoS with fog computing based on sigmoid NN clustering and entropy-based scheduling", *Multimed Tools Appl*, vol. 83, pp. 305–326, doi: https://doi.org/10.1007/s11042-023-15685-3
18. Petrovska, I., Kuchuk, N., Pochebut, M., Kuchuk, H., Mozhaiev, O. and Onishchenko, Y. (2023), "Sequential Series-Based Prediction Model in Adaptive Cloud Resource Allocation for Data Processing and Security", *The 13th IEEE Int. Conf. on Dependable Systems, Services and Technologies*, DESSERT'2023, Athens, Greece, pp. 1–6, doi: https://doi.org/10.1109/DESSERT61349.2023.10416496
19. Kaur, M., Sandhu, R. and Mohana, R. (2023), "A Framework for QoS Parameters-Based Scheduling for IoT Applications on Fog Environments", *Wireless Personal Communications*, vol. 132(4), pp. 2709–2736, doi: https://doi.org/10.1007/s11277-023-10740-6
20. Thomas, P. and Jose, D.V. (2023), "Towards Computation Offloading Approaches in IoT-Fog-Cloud Environment: Survey on Concepts, Architectures, Tools and Methodologies", *Lecture Notes in Networks and Systems* , 613 LNNS, pp. 37–52, doi: https://doi.org/10.1007/978-981-19-9379-4_4
21. Taneja, M. and Davy, A. (2017), "Resource aware placement of IoT application modules in fog-cloud computing paradigm", *Proc. 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM),* pp. 1222–1228, doi: https://doi.org/10.23919/INM.2017.7987464
22. Yin, B., Shen, W., Cheng, Y., Cai, L.X. and Li, Q. (2017), "Distributed resource sharing in fog-assisted big data streaming", *Proc. IEEE Int. Conf. Commun*., pp. 1–6, doi: https://doi.org/10.1109/ICC.2017.7996724
23. Aazam, M., St-Hilaire, M., Lung, C.-H., Lambadaris, I. and Huh, E.-N. (2018), "IoT resource estimation challenges and modeling in fog", *Fog Computing in the IoT* , Springer, pp. 17–31, doi https://doi.org/10.1007/978-3-319-57639-8_2
24. Kuchuk, H., Kalinin, Y., Dotsenko, N., Chumachenko, I. and Pakhomov, Y. (2024), "Decomposition of integrated high-density IoT data flow", *Advanced Information Systems* , vol. 8, no. 3, pp. 77–84, doi: https://doi.org/10.20998/2522-9052.2024.3.09
25. Truong, N.B., Lee, G.M. and Ghamri-Doudane, Y. (2015), "Software defined networking based vehicular adhoc network with fog computing", *2015 IFIP/IEEE International Symposium on Integrated Network Management*, pp. 1202–1207, doi: https://doi.org/10.1109/INM.2015.7140467

Received 24.07.2025
Accepted for publication 11.08.2025

ВІДОМОСТІ ПРО АВТОРІВ/ ABOUT THE AUTHORS

Стеценко Вадим Олегович – аспірант кафедри кібербезпеки, Національний технічний університет "Харківський політехнічний інститут", Харків, Україна;
Vadym Stetsenko – PhD student of Cybersecurity Department, National Technical University "Kharkiv polytechnic institute", Kharkiv, Ukraine;
e- mail: 4all2dream@gmail.com; ORCID Author ID: https://orcid.org/0009-0008-5315-5539;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=59185285700.

Мурр П'єр – доцент кафедри комп'ютерної інженерії, Міжнародний університет науки і технологій у Кувейті, Ардія, Кувейт;
Pierre Murr – PhD, Assistant professor, Computer Engineering Department, International University of Science and Technology in Kuwait, Ardiya, Kuwait;
e- mail: murrpierre@gmail.com; ORCID Author ID: https://orcid.org/0009-0007-4094-0223.

Ткачов Андрій Михайлович – кандидат технічних наук, старший науковий співробітник, доцент кафедри кібербезпеки, Національний технічний університет "Харківський політехнічний інститут", Харків, Україна;
Andrii Tkachov – Candidate of Technical Science, Senior research fellow, Associate professor of Cybersecurity Department, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine;
e- mail: andrii.tkachov@khpi.edu.ua; ORCID Author ID: https://orcid.org/0000-0003-1428-0173;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57416821200.

Лаптєв Олександр Анатолійович – доктор технічних наук, старший науковий співробітник, доцент кафедри кібербезпеки та захисту інформації, Київський національний університет імені Тараса Шевченка, Київ, Україна;
Oleksandr Laptiev – Doctor of Technical Sciences, Senior Researcher, Associate Professor the Department of Cyber Security and Information Protection, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine;
e- mail: olaptiev@knu.ua; ORCID Author ID: https://orcid.org/0000-0002-4194-402X;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57216163849.

Мельник Маргарита Олександрівна – кандидат технічних наук, доцент кафедри кібербезпеки та захисту інформації, Університет науки, підприємництва та технологій, Київ, Україна;
Marharyta Melnyk — PhD, assistant professor Department of Cyber Security and information protection, Science Entrepreneurship Technology University, Kyiv, Ukraine;
e- mail: Margaritochek@gmail.com; ORCID Author ID: https://orcid.org/0000-0003-0619-7281.

МОДЕЛІ КРИПТО-КОДОВИХ КОНСТРУКЦІЙ МАК-ЕЛІСА Й НІДЕРРАЙТЕРА

В.О. Стеценко, П. Мурр, А. М. Ткачов, О. А. Лаптєв, М. О. Мельник

Анотація. Актуальність дослідження полягає в забезпеченні інформаційної безпеки шляхом створення криптографічних рішень, що поєднують високу продуктивність, стійкість до квантових атак та можливість ефективної реалізації в пристроях з обмеженими ресурсами. **Предметом дослідження** є підходи та стратегії використання кодових криптосистем, зокрема криптокодових конструкцій Мак-Еліса та Нідеррайтера, як базових механізмів побудови криптографічних систем, стійких до атак. **Метою статті** є обґрунтування перспектив використання кодових криптосистем як базових механізмів побудови криптографічних систем, стійких до атак на квантові комп'ютери. Розробити алгоритми генерації та декодування криптограм, проаналізувати їх алгоритмічну складність. **Результати дослідження**. Обґрунтовано перспективи використання кодових криптосистем як базових механізмів побудови криптографічних систем. Розроблено алгоритми генерації та декодування криптограм, проаналізовано їх алгоритмічну складність та оцінено потенціал інтеграції таких структур у реальні системи. **Висновки.** Дослідження дозволяє виявити переваги системного підходу в плануванні швидкості дій завдяки попереднім синдромам обчислень. Рішення алгоритмічних труднощів свідчать про високу ефективність криптозахисту, що робить їх придатними для використання в сучасних інформаційних системах.

Ключові слова: крипто-кодова конструкція, кібербезпека, криптосистема, алгоритмічну складність, модель, конфіденційність, цілісність.