КІБЕРБЕЗПЕКА: освіта, наука, техніка

CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE

№ 1 (5), 2019

ISSN 2663 - 4023

DOI 10.28925/2663-4023.2019.5.4051
UDC 681.3.06

Alla A. Havrylova
Senior Lecturer
Work place: Simon Kuznets Kharkiv National University of Economics, Department of Cyber Security and Information Technology, Kharkiv, Ukraine
OrcID 0000-0002-2015-8927
alla.gavrilova@hneu.net

Olha H. Korol
PhD, Associate Professor department of Cyber Security and Information Technology
Work place: Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine
OrcID 0000-0002-8733-9984
olha.korol@hneu.net

Stanyslav V. Milevskyi
PhD, Associate Professor department of Cyber Security and Information Technology
Work place: Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine
OrcID 0000-0001-5087-7036
milevskiysv@gmail.com

Lala R. Bakirova
Head of Instrument Engineering Department
Work place: Azerbaijan State University of Oil and Industry, Baku, Azerbaijan
OrcID 0000-0003-0584-7916
lala_bekirova@mail.ru

MATHEMATICAL MODEL OF AUTHENTICATION OF A TRANSMITTED MESSAGE BASED ON A MCELIECE SCHEME ON SHORTED AND EXTENDED MODIFIED ELLIPTIC CODES USING UMAC MODIFIED ALGORITHM

Annotation. The subject of the research is a mathematical model of authentication of the transmitted message based on the McEliese scheme on shortened and elongated modified elliptic codes using the modified UMAC algorithm. The aim of this work is to develop such a scheme for the information exchange over Internet communication channels, which would ensure the proper level of verification and integrity of the transmitted information, taking into account the prevention of an increase in the costs of the actions taken. Tasks: analysis of existing ways to increase the resistance to hacking of transmitted messages over telecommunication networks; analysis of a message transfer scheme using blockchain technology; formalized description of a mathematical model for providing clear text authentication using a modified UMAC algorithm, as the formation of key data, a crypto-code construction (CCC) is used on the McEliese scheme on modified elliptic codes (MEC); development of data encryption and decryption algorithms using CCC based on McEliese on the MEC and UMAC algorithm. An approach was proposed to verify the authentication and verification of the information packet during transmission and reception via telecommunication channels, which allows using already known hashing methods to compare generated codegrams and transmitted messages for their correspondence, which increases the level of cryptographic stability of the transmitted data and the reliability of the received data. The developed schemes of algorithms for generating codegrams and their decryption using the proposed approach make it possible to gradually demonstrate the implementation of procedures for generating codegrams and their hash codes using both shortening and lengthening the code. Further research should prove from a practical point of view the effectiveness of using this approach when transmitting a message regarding the preservation of its integrity and authenticity. Therefore, it is necessary to develop a test system that should implement the proposed approach, as well as evaluate the results obtained.

Keywords: decentralized systems; blockchain technology; post-quantum cryptosystems; McEliece crypto code design; elliptic curves; UMAC algorithm.

1. INTRODUCTION

According to the results of the first stage of the selection of the program for standardizing post-quantum cryptosystems published by NIST, out of the 69 proposals made, 26 proposals passed in the second round [1]. This suggests that post-quantum cryptosystems are now one of the main directions of modern cryptography, while symmetric and asymmetric cryptographic algorithms, as well as algorithms based on elliptic curves, are questioned regarding cryptographic strength [2]. Despite the fact that symmetric encryption systems are fast and easy to implement, and asymmetric cryptographic algorithms are built on complex mathematical calculations, the RSA algorithm, based on elliptic curves and the computational complexity of the large number factorization problem, is considered the most reliable today. Using this algorithm, high cryptographic stability of transmitted messages is ensured due to the inability to decrypt these messages in computational time. But at the same time, the basic models of quantum computers are able to cope with this task in a matter of hours. The article proposes a mathematical model based on the McEliece scheme on shortened and elongated modified elliptic codes (MEC) for encoding and decoding information using the modified UMAC algorithm when transmitting and receiving open messages over communication channels. In the process of implementing this model, double verification is provided, which allows ensuring a high level of integrity and reliability of the transmitted message, as well as a high level of speed and cryptographic stability of the hash code in the conditions of post-quantum cryptography.

Formulation of the problem. With the increasing load on the Internet due to the increase in the number of users in it, the degree of cyberattacks by cybercriminals on the operation of this network is also increasing. There is an acute question of ensuring the protection of information in a decentralized system, to which both the Internet at the physical level and the technologies through which users work in it are related. In this system, all participants are independent of each other, but processes are managed jointly. In this regard, their actions must be coordinated in order to obtain the desired result, but without a centralization point.

Therefore, in the conditions of user interaction with each other and the sharing of resources, services, content and devices, it is necessary to constantly monitor and make changes to the principles of organization and operation of protocols that protect the transmission of information from unauthorized access in order to steal and / or distort the transmitted information.

Analysis of recent research and publications. As part of solving the problem of information integrity, cryptographic methods are used, with which it is possible to detect not only random distortions of information, but also its purposeful change. So, the integrity control process is ensured by introducing redundancy into the transmitted information – a test combination of bytes [3]. Such a combination of bytes is calculated according to the algorithms [4], which check to see if the data has been changed unauthorized and what is the measure of the cipher's imitation resistance.

The basis for modern decentralized systems is blockchain technology, therefore, the development of digital information identification algorithms that protect ongoing transactions between network nodes is important for the operation of this system. **There are known authentication methods for digital data transmission, such as checksums, CRC control, hashing and digital signature [5]. The most advanced way out of those listed above is hashing and digital signature. Such algorithms include the UMAC algorithm, which provides authentication and message integrity. This algorithm is based on universal hashing functions, which should guarantee efficiency, security and protection against**

hacks. Despite a number of advantages of those methods that are now used as increasing cryptographic strength, they have a number of disadvantages (tabl. 1).

Table 1

Analysis of existing ways to increase the resistance to hacking of transmitted messages over telecommunication networks

№	The way to increase cryptographic strength	Disadvantage
1	elongation hashes when encrypting message	the process takes a longer time, increasing financial costs
2	formation of new types of information security protocols	is formed after-fact and the process takes a long time, an increase in financial costs
3	use of crypto-code constructions (CCC) on elliptic curves (EC)	the length of the keys increases, but performance is not ensured, increased financial costs
4	use of more powerful computers	has a temporary respite, increased financial costs

It is also important that when creating such algorithms, it must be borne in mind that attacks on the network can be carried out in the future using both optical and post-quantum computers, the latter of which are highly computationally capable.

At the peak of attention, working with cryptocurrencies through blockchain technology requires not only developments that ensure the safety of transactions in the present, but also in the context of a post-quantum future.

This technology today is the basis for the functioning of cryptocurrencies, which in turn are becoming more and more interested not only in business, but in government agencies of different countries. According to a number of experts [6], during data transfer on the principles of blockchain technology, this data can remain open and not encrypted, since it is protected by hash values and electronic digital signature (EDS), which provides a high level of protection, but the level of confidentiality of the host itself is not ensured.

The phenomena of quantum superposition and quantum entanglement for data transmission and processing are based on a polynomial factorization algorithm for a quantum computer [7]. A certain modification of this algorithm allows us to solve the discrete logarithm problem in the group of points of an elliptic curve. The expected high capabilities of this algorithm mean that cryptographic algorithms that use the problems of factorization and the discrete logarithm are potentially unstable in the presence of a full-fledged quantum computer. The emergence of this algorithm contributed to the creation of post-quantum cryptography, which studies algorithms that are resistant to cracking on a quantum computer [8]. Despite the fact that today such a computer does not yet exist, its appearance is not considered too distant for the future, and therefore post-quantum cryptography is an actual area of research at present. One of the most promising areas of post-quantum cryptography is hash-based cryptography. Algorithms of this direction are used to generate and verify digital signatures and use only a cryptographically stable hash function [9]. The SHA-256 cryptographic hash function, which creates a 256-bit hash and is currently used in Bitcoin, can be hacked using this computer. The UMAC model using the AES block symmetric cipher, the encryption reliability of which is highly appreciated by specialists [10], also does not provide universality in post-quantum calculations.

Conversion of the input message into a hash value is carried out using a modular exponentiation using two keyless hash functions – MASH-1 and MASH-2. The construction of the hash functions MASH-1 and MASH-2 is based on the use of an iterative loop function defined through a modular exponentiation (in the simplest case, through a modular squaring). Despite the fact that the existing MASH-1 does not provide high collision properties, and MASH-2 in some cases allows the construction of universal and strictly universal classes of hash functions, the use of such transformations using modular arithmetic guarantees high security (cryptographic strength) and proven stability [10], but do not have high speed.

The structure and information in the blocks obeys the given rules and can be quickly checked [11]. Each block always contains information about one previous block. This allows to build all existing blocks in one chain, which is a distributed database and contains information about all transactions ever performed with Bitcoin (fig. 1).

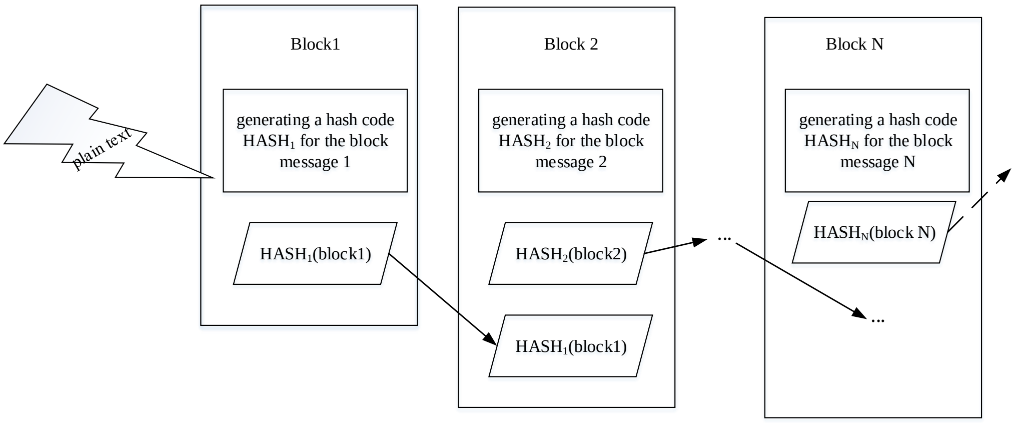
plain text
Block1
generating a hash code HASH$_1$ for the block message 1
HASH$_1$(block1)
Block 2
generating a hash code HASH$_2$ for the block message 2
HASH$_2$(block2)
HASH$_1$(block1)
...
Block N
generating a hash code HASH$_N$ for the block message N
HASH$_N$(block N)
...

Fig. 1. Scheme of message transmission using blockchain technology

From the generated scheme it is seen that the number of blocks included in the chain has a beginning, but does not have a quantitative limit. They are united by the achievement of consensus in the constantly updated storage of information. In aggregate, blocks represent a distributed register, and each block consists of a header containing block metadata and block data that contains a set of transactions and other relevant data [12]. Each transaction includes one or more users of the blockchain network and records information about what happened with the confirmation of its digital signature.

The purpose of this article. The purpose of this article is to analyze the cryptographic strength of existing encryption algorithms and to develop such a scheme for exchanging information over the Internet’s communication channels, which would ensure the proper level of verification and integrity of the transmitted information, taking into account the prevention of an increase in the cost of the actions taken.

As part of this goal the following tasks should be solved:

– the analysis of existing ways to increase the resistance to hacking of transmitted messages over telecommunication networks;

– a message transfer scheme using blockchain technology developed;

– a formalized description of the mathematical model for providing clear text authentication is carried out; the modified UMAC algorithm is used; the crypto-code construction (CCC) on the McEliece scheme on modified elliptic codes (MEC) is used as key data generation;

– an algorithm for encrypting and decrypting data using the KKK based on McEliece on MEC and the algorithm for generating hash values of UMAC has been developed.

2. RESEARCH RESULTS

A mathematical model of encoding and decoding information when transmitting and receiving via communication channels based on the McEliece scheme using shortened and elongated modified elliptic codes (MEC)

When transmitting a message, a modified UMAC algorithm is used to provide plaintext authentication, and a crypto-code structure (CCC) based on a McEliece scheme using modified elliptic codes (MEC) is used as key data generation.

It is necessary to take into account that this model of information transformation in the McEliece system can be built as on shortened (*IV₁=EC–hᵢ*) [3], and on elongated (*IV₁, ,IV₂=EC–hᵣ*) [4] MEC. Additional initialization vectors provide “compensation” for the decrease in the power of the alphabet during the formation of the McEliece CCC on the MEC. This approach ensures the preservation of versatility and provides stability in post-quantum cryptography.

The mathematical model of the crypto-code construction (CCC) on the McEliece scheme using modified elliptic codes (MEC) based on shortening (reduction of information symbols) / extension (adding information symbols) is formally defined by the set of elements listed below [3], [4] (tabl. 2).

Table 2

Definition of model elements

№	**Parameter name**	**Formal description of the parameter taking into account**	
		character shortening	**character extensions**
1	plaintexts set	$M=\{\mathrm{M}_1,\mathrm{M}_2,...,\mathrm{M}_{\mathrm{q}^\mathrm{k}}\}$, где $M_i=\{\mathrm{I}_0,\mathrm{I}_{\mathrm{h}_1},..\ \mathrm{I}_{\mathrm{h}_\mathrm{j}},\mathrm{I}_{\mathrm{k-1}}\}$, $\forall \mathrm{I}_\mathrm{j}\in GF(q)$, h_j – information symbols equal to zero, $\|h\|=\frac{1}{2}k$, т. е. $I_i=0$, $\forall I_i\in h$	$M=\{\mathrm{M}_1,\mathrm{M}_2,...,\mathrm{M}_{\mathrm{q}^\mathrm{k}}\}$, где $M_i=\{\mathrm{I}_0,\mathrm{I}_{\mathrm{h}_{\mathrm{r}_1}},..\ \mathrm{I}_{\mathrm{h}_{\mathrm{r}_\mathrm{j}}},\mathrm{I}_{\mathrm{k-1}}\}$, $\forall \mathrm{I}_\mathrm{j}\in GF(q)$, h_j – information symbols equal to zero, $\|h\|=\frac{1}{2}k$, т.е. $I_i=0$, $\forall I_i\in h$, h_r – extension information symbols k, $\|h\|=\frac{1}{2}k$
2	closed texts (codograms) set	$C=\{\mathrm{C}_1,\mathrm{C}_2,...,\mathrm{C}_{\mathrm{q}^\mathrm{k}}\}$, where $C_i=(c^*_{X_0},c^*_{h_1},...,c^*_{h_j},c^*_{X_{n-1}})$, $\forall c^*_{X_j}\in GF(q)$	$C=\{\mathrm{C}_1,\mathrm{C}_2,...,\mathrm{C}_{\mathrm{q}^\mathrm{k}}\}$, where $C_i=(c^*_{X_0},c^*_{h_{r_1}},...,c^*_{h_{r_j}},c^*_{X_{n-1}})$, $\forall c^*_{X_j}\in GF(q)$
3	direct mappings (based on the use of the public key – the generating matrix) set	$\phi=\{\phi_1,\phi_2,...,\phi_s\}$, where $\phi_i:M\to C_{k-h_r}$, $i=1,2,...,s$	$\phi=\{\phi_1,\phi_2,...,\phi_s\}$,, where $\varphi_i:M\to C_{h_r}$, $i=1,2,...,s$
4	inverse mappings (based on the use of a private (private) key – masking matrices) set	$\phi^{-1}=\{\phi_1^{-1},\phi_2^{-1},...,\phi_s^{-1}\}$, where $\phi_i^{-1}:C_{k-h_r}\to M$, $i=1,2,...,s$;	$\phi^{-1}=\{\phi_1^{-1},\phi_2^{-1},...,\phi_s^{-1}\}$,, where $\varphi_i^{-1}:C_{h_r}\to M$, $i=1,2,...,s$
5	a set of keys parameterizing direct mappings	$K_{a_i}=\{K_{1_{a_i}},K_{2_{a_i}},...,K_{s_{a_i}}\}=\{G_X^{EC_1}{}_{a_i},G_X^{EC_2}{}_{a_i},...,G_X^{ECs}{}_{a_i}\}$, where $G_X^{ECi}{}_{a_i}$ – generating $n\times k$ matrix of disguised as a random code algebraic	

<table>
<tr><td rowspan="2"></td><td rowspan="2">(public key of an authorized user)</td><td colspan="2">geometric block $(n,\ k,\ d)$ -code with elements from $GF(q)$,
a_i – set of coefficients of a polynomial of a curve $a_1 \ldots a_6$, $\forall a_i \in GF(q)$, defining a specific set of curve points from space P^2</td></tr>
<tr><td>$\phi_i : M \xrightarrow{K_{ia_i}} C_{k-h_j};\ \ i = 1, 2, \ldots, s;$</td><td>$\varphi_i : M \xrightarrow{K_{ia_i}} C_{hr},\ \ i = 1, 2, \ldots, s;$</td></tr>
<tr><td>6</td><td>a set of keys that parameterize reverse mappings (private (closed) key of an authorized user)</td><td colspan="2">$K^* = \{\mathrm{K}_1^*, \mathrm{K}_2^*, \ldots, \mathrm{K}_s^*\} = \{\{\mathrm{X,P,D}\}_1, \{\mathrm{X,P,D}\}_2, \ldots, \{\mathrm{X,P,D}\}_s\},\ \{\mathrm{X,P,D}\}_\mathrm{i} = \{X^i, P^i, D^i\}$,
где X^i – a masking non-degenerate randomly uniformly formed by a key source $k \times k$ matrix with elements from $GF(q)$,
P^i – permutation randomly uniformly generated by the key source $n \times n$ matrix with elements from $GF(q)$,
D^i – diagonal formed by key source $n \times n$ matrix with elements from $GF(q)$, i.e.
$\phi_i^{-1} : C \xrightarrow{\mathrm{K}_\mathrm{i}^*} M,\ i = 1, 2, \ldots, s$</td></tr>
</table>

Regardless of the way the code is presented (for both shortened and elongated versions), we will set a number of model parameters as follows.

So, in the CCC based on the McEliece scheme on a modified (shortened / elongated) algebraic (n,k,d)-code with a fast decoding algorithm that “disguises” as random (n,k,d)-code by multiplying the generating matrix G^{EC_i} code for secret masking matrices X, P and D [5], authorized user public key generation is provided:

$$G_X^{EC_i} = X^i \times G^{EC_i} \times P^i \times D^i \tag{1}$$

Formation of a closed text c_X open message M for a given public key can be represented as follows [5]:

$$c_X = i \times G_X^{EC_i} + e, \tag{2}$$

where i – information package for forming a code word, e – **randomly generated vector e (e_0, e_1, ..., e_{n-1}).**

After the generated codogram, it is shortened or lengthened using additional session keys of initialization vectors IV_1, ,IV_2 (depending on the modification algorithm used).

When generating key data in the proposed UMAC algorithm, it is proposed to use the generated cryptogram of CCC McEliece on the MEC, which is used as input to generate the secret key *K* (with length *Keylen*) and random number *Nonce* eight bytes in size. When specifying the size of the generated hash code *Tag* integer *Taglen* used by formula [5]:

$$Tag=Hash\ (K,M,Taglen) \oplus PDF(K,Nonce,Taglen)$$

This authentication code will be part of the hash code of the open message M. Open message M and closed text c_X hashing processes **occurs according to the same procedure for generating UMAC tags using the universal hash function** UHASH (K, M, Taglen) [5].

Let’s consider the UMAC algorithm based on the UHASH function, which is formed in three stages. At the first stage, UHASH-hash is applied to the input message, at the second stage – POLY-hash is applied to this result, and finally, at the third stage, Carter-Wegman-hash is applied to the result. If the length of the input message is no more than 1024 bits, then POLY-hash is not used. Since the Carter-Wegman-hash function returns only a word of 4 bytes in length, then if it is needed to get a hash of more than 4 bytes in length, several iterations of this three-level scheme are performed (tabl. 3).

When transmitting a message to the communication channel, the result of concatenation of three components: the information message *M*, cryptogram c_X and hash code *Y* (fig. 2).

On the receiving side, to verify the integrity of the received message, an authorized user, knowing the initialization vectors IV_1, ,IV_2 performs the following actions (fig. 3):

Table 3

Obtaining hash codes for open messages

Hashing stages	Hashing process	Hash result by sending and receiving parties
UHASH-hash	splitting a message into blocks of 1024 bytes, receiving a message 128 times smaller than the input	$Y_{L1}=Hash_{L1}(K_{L1},M)$ $Y`_{L1}=Hash`_{L1}(K`_{L1},M)$
POLY-hash	verification of data integrity and authenticity of the message, receiving a 16 byte number	$Y_{L2}=Hash_{L2}(K_{L2},Y_{L1})$ $Y`_{L2}=Hash`_{L2}(K`_{L2},Y`_{L1})$
Carter-Wegman-hash	getting a 4-byte value from a 16 byte number	$Y_{L3}=Hash_{L3}(K_{L31},K_{L32},Y_{L2})$ $Y`_{L3}=Hash`_{L3}(K`_{L31},K`_{L32},Y`_{L2})$

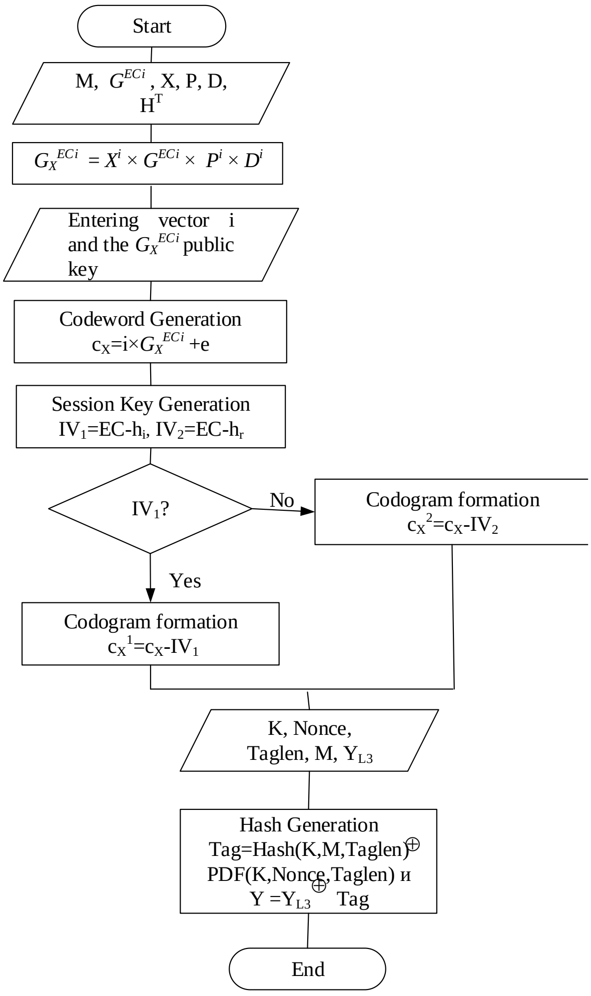
Start
M, G^{ECi}, X, P, D, H^T
$G_X^{ECi} = X^i \times G^{ECi} \times P^i \times D^i$
Entering vector i and the G_X^{ECi} public key
Codeword Generation $c_X=i\times G_X^{ECi}+e$
Session Key Generation IV_1=EC-h_i, IV_2=EC-h_r
IV_1?
No
Codogram formation $c_X^2=c_X-IV_2$
Yes
Codogram formation $c_X^1=c_X-IV_1$
K, Nonce, Taglen, M, Y_{L3}
Hash Generation Tag=Hash(K,M,Taglen)⊕ PDF(K,Nonce,Taglen) и Y =Y_{L3} ⊕ Tag
End

Fig. 2. Formation of an algorithm for encrypting a sender message using a CCC based on McEliece at MEC

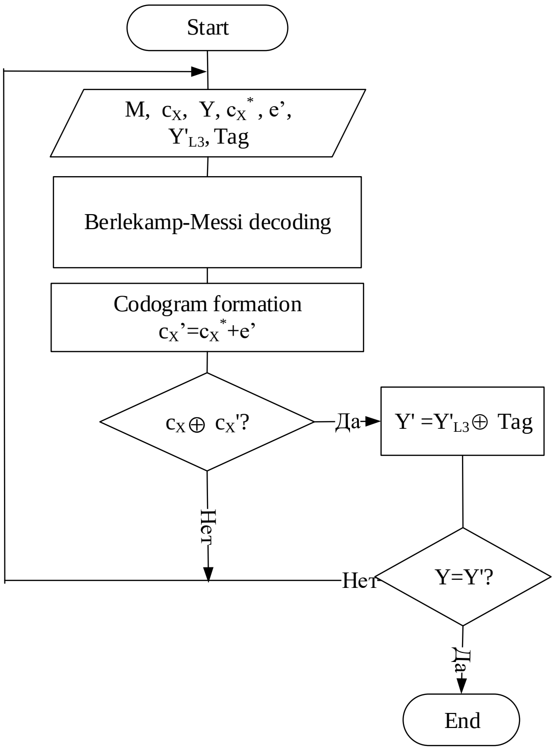

Fig. 3. The algorithm for checking the integrity of the received message

1) based on the Berlekamp-Messi fast decoding algorithm, an error vector is found;

2) the resulting error vector is used to generate a codogram using the CCC McEliece at MEC;

3) verification of the received and generated codogram is carried out on the basis of the

CCC McEliece at MEC. If the codograms (cryptograms) do not match, the message is considered modified and a request for re-sending from the sender is generated;

4) when the codograms match, a hash code *Y'* is created from closed text c_X' according to the scheme given in tabl. 3;

5) verification of the received and generated hash code is carried out. If the hash codes do not match, the message is considered modified and a request for re-sending from the sender is generated.

During the formation of the circuit, the following elements were also used as input data:

- **M – plain text,**
- **G – user private key,**
- **X** – non-degenerate **k×k** matrix over *GF(q),*
- **P** – permutation **n×n** matrix over *GF(q),*
- *D* – diagonal **n×n** matrix over *GF(q),*
- H^T – transposed matrix based on test **r×n** matrix of elliptic code over *GF(q).*

Double verification allows to provide a high level of integrity and reliability of the transmitted message, while the algorithm used provides a high level of speed and cryptographic stability of the hash code in post-quantum cryptography.

Schematically, the process of confirming the integrity of information during transmission from the sending to the receiving side based on verification of codograms and hash codes using the CCC McEliece at MEC is presented in fig. 4.

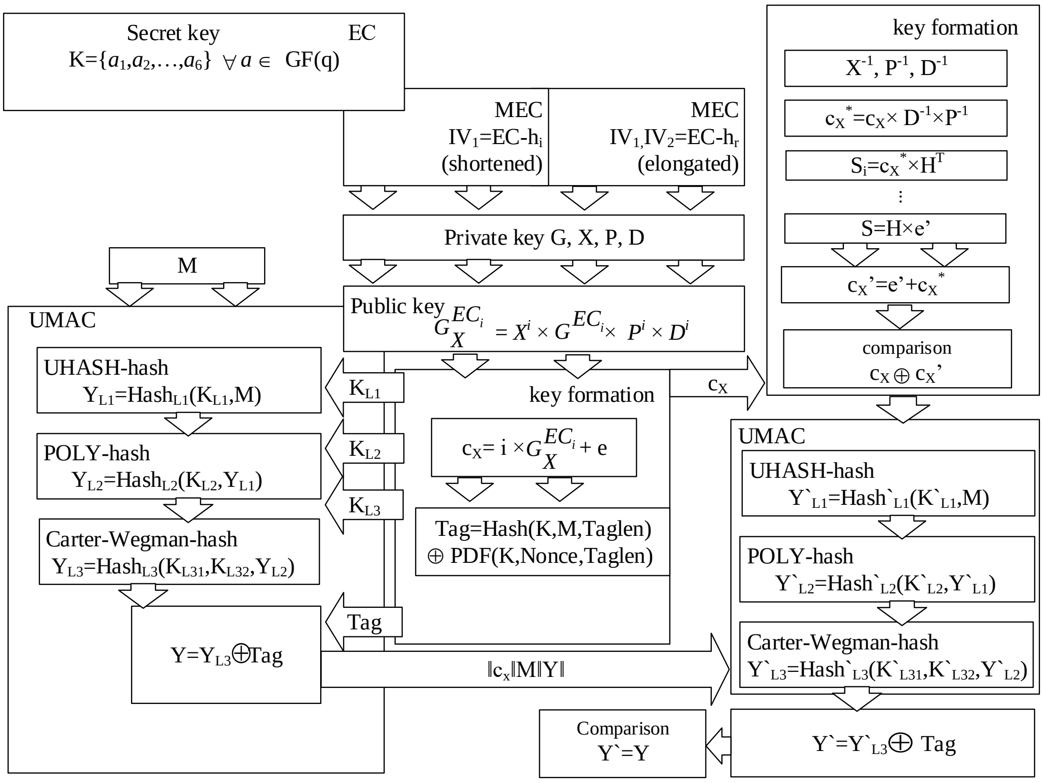
Secret key EC
K={a1,a2,…,a6} ∀a ∈ GF(q)
MEC IV1=EC-hi (shortened)
MEC IV1,IV2=EC-hr (elongated)
Private key G, X, P, D
M
UMAC
Public key $G_X^{EC_i} = X^i \times G^{EC_i} \times P^i \times D^i$
UHASH-hash YL1=HashL1(KL1,M)
POLY-hash YL2=HashL2(KL2,YL1)
Carter-Wegman-hash YL3=HashL3(KL31,KL32,YL2)
KL1
KL2
KL3
Tag
Y=YL3⊕Tag
key formation
$c_X = i \times G_X^{EC_i} + e$
Tag=Hash(K,M,Taglen) ⊕ PDF(K,Nonce,Taglen)
cX
‖cX‖M‖Y‖
key formation
X-1, P-1, D-1
cX*=cX× D-1×P-1
Si=cX*×HT
⋮
S=H×e'
cX'=e'+cX*
comparison cX ⊕ cX'
UMAC
UHASH-hash Y`L1=Hash`L1(K`L1,M)
POLY-hash Y`L2=Hash`L2(K`L2,Y`L1)
Carter-Wegman-hash Y`L3=Hash`L3(K`L31,K`L32,Y`L2)
Y`=Y`L3⊕ Tag
Comparison Y`=Y

Fig. 4. The scheme of transmitting a message from the sender to the recipient and checking the integrity of the received through a comparison of the codograms and hash codes using the CCC McEliece at MEC

3. CONCLUSIONS

In this paper, an approach was proposed to verify the authentication and verification of the information packet during transmission and reception via telecommunication channels, which allows using already known hashing methods to compare generated codegrams and transmitted messages for their correspondence, which increases the level of cryptographic stability of the transmitted data and the reliability of the received data.

The developed schemes of algorithms for the formation of codograms and their decryption using the proposed approach allow to demonstrate step by step he implementation of the procedures for generating codograms and their hash codes using both shortening and lengthening the code. Further research will be to confirm the feasibility of the proposed approach in practice.

REFERENCES

[1] A. Veneduhin, “Post-Quantum Cryptography: NIST 4 Program [Postkvantovaya kriptografiya: programma NIST 4]”, *Bezopasnost*, *Kriptologiya,* Sayt dxdt.ru: zanimatelniy internet-zhurnal. [Online]. Access mode: https://dxdt.ru/2019/02/04/8687/ [04 фев., 2019]. (in Russian)

[2] A.V. Korolkov, “On some applied aspects of quantum cryptography in the context of the development of quantum computing and the advent of quantum computers [O nekotoryh prikladnyh aspektah kvantovoq kriptografii v kontekste razvitiya kvantobyh bychisleniy I poyavleniya kvantovyh komputerov]”, *Voprosy kiberbezopasnosti,* M.: ZAO “Nauchno-proizvodstvennoe obyedineniye “Eshelon", № 1(9), pp. 6–13, 2015 (in Russian).

[3] S.P. Yevseev, H.N. Rzaev, O.G. Korol, and Z.B. Imanova, “Development of a modified asymmetric McElise crypto-code system on shortened elliptic codes [Razrabotka modificirovannoy nesimmetrichnoy kripto-kodovoy sistemy Mak-Elisa ukorochennyh ellipticheskih kodah]”, Vostochno-Evropeyskiy zhurnal peredovyh tehnologiy, № 4/9 (82), pp. 158-165, 2016 (in Russian)/

[4] Serhii Yevseiev, Olha Korol, and Alla Havrylova, “Development of authentication codes of messages on the basis of UMAC with crypto-code McEliece’s scheme on elliptical codes”, *Materials of VIIth International Scientific and Technical Conference* “*Information protection and information systems security*”*: report theses, May 30 –31, 2019,* Lviv: Lviv Polytechnic Publishing House, pp. 86 – 87, 1 electron. opt. disk (DVD), 2019 (in English).

[5] A.A. Kuznetsov, O.G. Korol, and S.P. Yevseev, “Investigation of collision properties of message authentication codes UMAC [Issledovanie kollizionnyh svoystv kodov autentifikacii soobsheniy UMAC]”, *Prikladnaya radioelektronika: nauch.-tehn. zhurnal*, vol. 11, № 2, pp. 171–183, 2012 (in Russian).

[6] A.A. Kuznetsov, O.G. Korol, and V.V. Bosko, “A model for generating message authentication codes using universal hashing functions [Model formirovaniya kodov autentifikacii soobsheniy s ispolzovaniem universalnyh heshiruushih funkciy]”, Zahyst informacii v informaciyno-telekomunikaciynyh systemah, 2016, pp. 117 – 125 (in Russian).

[7] Olga Korol, Lubomyr Parhuts, and Sergey Yevseev, “Development of a model and method for the cascade formation of MAC using modular transformations [Razrabotka modeli i metoda kaskadnogo formirovaniya MAC s ispolzovaniem modularnyh preobrazovaniy]”, Zahiist informatsii, lypen-veresen, t. 15, №3, pp. 186 – 196, 2013 (in Russian).

[8] Y.L. Onanchenko, and A.V. Lysenko, “Analysis of known decoding methods for non-binary block codes [Analiz izvestnyh metodov dekodirovaniya nedvoichnyh blokovyh kodov]”, Visnyk SumDU, Seria Tehnichni nauki, № 3, pp. 100 – 105, 2008 (in Russian).

[9] K.Y. Batenko, and A.N. Prokudin, “Post-quantum digital signature algorithm based on the Merkle tree and GOST RF 34.11–12 “Stribog” [Post-kvantoviy algoritm elektronno-cifrovoy podpisi na osnove dereva Merkla b GOST RF 34.11-12 “Stribog”]”, Molodoy ucheniy, №23, pp. 100-103, 2017. [Online]. Access mode: https://moluch.ru/archive/157/44376/ [30 aug., 2019] (in Russian).

[10] A.A. Kuznetsov, A.I. Pushkarev, I.I. Svatovskiy, and A.V. Shevtsov, “Asymmetric cryptosystems on algebraic codes for the post-quantum period [Nesimmetrichnye kriptosistemy na algebraicheskih kodah dlya postkvantovogo perioda]”, Radiotehnika, 2016, rel. 186, pp. 70 – 90 (in Russian).

[11] P. Kravchenko, B. Skryabin, and O. Dubinina, Blockchain and decentralized systems: textbook. manual for students of higher. Education: in 3 parts [Blokcheyn i decentralizovannye sistemy: ucheb. Posobie dlya studentov vyssh. obrazovaniya: d 3 chastyah], Kharkov: PROMART, part. 1, 2018 (in Russian).

[12] Maryna Yesina, Olga Akolzina, and Ivan Gorbenko, “Conditions and opportunities of Blockchain

applying”, *Materials of VIIth International Scientific and Technical Conference* “*Information protection and information systems security*”*: report theses, May 30–31, 2019*, Lviv: Lviv Polytechnic Publishing House, 1 electron. opt. disk (DVD), pp. 46–47, 2019 (in English).

Гаврилова Алла Андріївна
старший викладач
Харківський національний економічний університет імені Семена Кузнеця, кафедра кібербезпеки та інформаційних технологій, Харків, Україна
OrcID 0000-0002-2015-8927
alla.gavrilova@hneu.net

Король Ольга Григорівна
к.т.н., доц. кафедри кібербезпеки та інформаційних технологій
Харківський національний економічний університет імені Семена Кузнеця, кафедра кібербезпеки та інформаційних технологій, Харків, Україна
OrcID 0000-0002-8733-9984
olha.korol@hneu.net

Мілевський Станіслав Валерійович
к.е.н., доц. кафедри кібербезпеки та інформаційних технологій
Місце роботи: Харківський національний економічний університет імені Семена Кузнеця, кафедра кібербезпеки та інформаційних технологій, Харків, Україна
OrcID 0000-0001-5087-7036
milevskiysv@gmail.com

Бєкірова Лала Рустам Кизи
завідуюча кафедрою приладобудівництва
Азербайджанський університет нафти та промисловості, Баку, Азербайджан
OrcID 0000-0003-0584-7916
lala_bekirova@mail.ru

МАТЕМАТИЧНА МОДЕЛЬ АУТЕНТИФІКАЦІЇ ПОВІДОМЛЕННЯ, ЩО ПЕРЕДАЄТЬСЯ, НА ОСНОВІ СХЕМИ МАК-ЕЛІСА НА УКОРОЧЕНИХ І ПОДОВЖЕННЯ МОДИФІКОВАНИХ ЕЛІПТИЧНИХ КОДАХ З ВИКОРИСТАННЯМ МОДИФІКОВАНОГО АЛГОРИТМА UMAC

Анотація. Предметом дослідження є математична модель забезпечення аутентифікації переданого повідомлення на основі схеми Мак-Еліса на укорочених і подовжених модифікованих еліптичних кодах з використанням модифікованого алгоритму UMAC. Метою даної роботи є розробка такої схеми обміну інформацією по каналах зв'язку мережі Інтернет, яка забезпечила б належний рівень верифікації та цілісності інформації, що передається з урахуванням недопущення збільшення витрат на проведені дії. Завдання, які було вирішено: проведено аналіз існуючих способів підвищення стійкості до зломів переданих повідомлень по телекомунікаційних мережах; проведено аналіз схеми передачі повідомлення з використанням технології блокчейн; розроблено формалізований опис математичної моделі забезпечення аутентифікації відкритого тексту з використанням модифікованого алгоритму UMAC; для формування ключових даних запропоновано використовувати крипто-кодову конструкцію (ККК) на схемі Мак-Еліса на модифікованих еліптичних кодах (МЕС); розроблено алгоритми шифрування і дешифрування даних із застосуванням ККК на основі Мак-Еліса на МЕС і алгоритму UMAC. Був запропонований підхід перевірки аутентифікації і верифікації інформаційної посилки під час передавання або по телекомунікаційних каналах, що дозволяє за допомогою вже відомих методів хешування проводити порівняння сформованих кодограм і переданих повідомлень на їх відповідність, що підвищує рівень криптостійкості переданих даних і ступінь достовірності отриманих даних. Розроблені схеми алгоритмів формування кодограм і їх розшифровки із застосуванням запропонованого підходу дозволяють поетапно продемонструвати здійснення процедур формування кодограм і їх хеш-кодів з використанням як укорочення, так і подовження коду. Подальші дослідження повинні з точки зору практики довести ефективність використання даного підходу при передачі повідомлення відносно його цілісності та автентичності. Тому необхідно розробити тестову систему, яка повинна реалізовувати запропонований підхід, а також оцінити отримані результати

Ключові слова: децентралізовані системи, технологія блокчейн, постквантові криптосистеми, крипто-кодова конструкція на схемі Мак-Еліса, еліптичні криві, алгоритм UMAC.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] А. Венедюхин, “Постквантовая криптография: программа NIST 4”, *Безопасность*, *Криптология,* Сайт dxdt.ru: занимательный интернет-журнал. [Онлайн]. Режим доступа: https://dxdt.ru/2019/02/04/8687/ [04 фев., 2019].

[2] А.В. Корольков, “О некоторых прикладных аспектах квантовой криптографии в контексте развития квантовых вычислений и появления квантовых компьютеров”, *Вопросы кибербезопасности,* М.: ЗАО "Научно-производственное объединение "Эшелон", № 1(9), С. 6–13, 2015,.

[3] С.П. Евсеев, Х.Н. Рзаев., О.Г. Король, и З.Б. Иманова, “Разработка модифицированной несимметричной крипто-кодовой системы Мак-Элиса на укороченных эллиптических кодах”, Восточно-Европейский журнал передовых технологий, № 4/9 (82), С. 158-165, 2016.

[4] Serhii Yevseiev, Olha Korol, and Alla Havrylova, “Development of authentication codes of messages on the basis of UMAC with crypto-code McEliece’s scheme on elliptical codes”, *Materials of VIIth International Scientific and Technical Conference* “*Information protection and information systems security*”*: report theses, May 30 –31, 2019,* Lviv: Lviv Polytechnic Publishing House, 1 electron. opt. disk (DVD), pp. 86 – 87, 2019.

[5] А.А. Кузнецов, О.Г. Король, и С.П. Евсеев, “Исследование коллизионных свойств кодов аутентификации сообщений UMAC”, *Прикладная радиоэлектроника: науч.-техн. Журнал,* Том 11, № 2, С. 171–183, 2012.

[6] А.А. Кузнецов, О.Г. Король, и В.В. Босько, “Модель формирования кодов аутентификации сообщений с использованием универсальных хеширующих функций”, Захист інформації в інформаційно-телекомунікаційних системах, С. 117 – 125, 2016.

[7] Ольга Король, Любомир Пархуць, и Сергей Евсеев, “Разработка модели и метода каскадного формирования MAC с использованием модулярных преобразований”, Захист інформації, липень-вересень, Том 15, №3, С. 186 – 196, 2013.

[8] Е.Л. Онанченко, и А.В. Лысенко, “Анализ известных методов декодирования недвоичных блоковых кодов”, Вісник СумДУ, Серія Технічні науки, № 3, С. 100 – 105, 2008.

[9] К.Е. Батенко, и А.Н. Прокудин, “Пост-квантовый алгоритм электронно-цифровой подписи на основе дерева Меркла и ГОСТ РФ 34.11–12 “Стрибог”, Молодой ученый, 2017, №23, С. 100-103. [Онлайн]. Режим доступа: https://moluch.ru/archive/157/44376/ [30 авг., 2019]

[10] А.А. Кузнецов, А.И. Пушкарев, И.И. Сватовский, и А.В. Шевцов, “Несимметричные криптосистемы на алгебраических кодах для постквантового периода”, Радиотехника, Вып. 186, С. 70 – 90, 2016.

[11] П. Кравченко, Б. Скрябин, и О. Дубинина, Блокчейн и децентрализованные системы: учеб. пособие для студентов высш. образования: в 3 частях, Харьков: ПРОМАРТ, ч. 1, 2018.

[12] Maryna Yesina, Olga Akolzina, and Ivan Gorbenko, “Conditions and opportunities of Blockchain applying”, *Materials of VIIth International Scientific and Technical Conference “Information protection and information systems security*”*: report theses, May 30–31, 2019,* Lviv: Lviv Polytechnic Publishing House, 1 electron. opt. disk (DVD), pp. 46–47, 2019.