UDC 004.056.55 DOI: 10.30748/soi.2020.162.09

O. Tsyhanenko

Simon Kuznets Kharkiv National University of Economics, Kharkiv

DEVELOPMENT OF DIGITAL SIGNATURE ALGORITHM BASED ON THE NIEDERRITER CRYPTO-CODE SYSTEM

The development of computing resources in the post-quantum period calls into question the provision of the required level of stability of symmetric and asymmetric cryptography algorithms. The advent of a full-scale quantum computer based on the Shore and Grover algorithms greatly increases the capabilities of cybercriminals and reduces the resilience of cryptosystems used in protocols for basic security services. The article analyzes the main requirements for resistance to post-quantum cryptography algorithms. In such conditions, it is necessary to use modified cryptosystems that provide an integrated required level of stability and efficiency of cryptocurrencies. One such mechanism is the crypto-code constructs of McEliece and Niederriter, which provide the required indicators of durability, efficiency and reliability. The paper analyzes the construction of the crypto-code structure of the Niederriter on elliptical (EC), modified elliptical codes (MEC) shortened and / or extended, and defective codes, practical algorithms for their implementation. An advanced protocol for the formation of a digital signature using Niederriter crypto-code constructions is proposed.

Keywords: *post-quantum period, digital signature, Niederreiter crypto-code constructions, elliptical codes.*

Introduction

Formulation of the problem. The entry of mankind into the era of high technologies has made it possible to single out cyberspace (an abstract concept based on computer networks and Internet technologies) into a separate component of security and put it before information security and security of information. To ensure security, as a rule, symmetric cryptosystems with temporary strength are used, but fast (by 3–5 orders of magnitude) crypto transformations, in comparison with asymmetric cryptosystems that provide a provable level of security (strength is based on NP-complete problems), which allows them to be used in transmission key data of symmetric cryptosystems and form digital signature protocols (DS) providing the service of authenticity (authenticity of the message source). The rapid development of computing means provides a 2-fold increase in computing capabilities every 18 months, which significantly increases the scope of services in cyberspace. However, the analysis by US NIST specialists of traditional cryptography algorithms [1–3] and asymmetric cryptography algorithms, digital signature protocols (including algorithms using elliptic curves) showed that the computational capabilities in the post-quantum period are the use of full-scale quantum computers and the Grover and Shor hacking algorithms [4] – allow for polynomial time to break the cryptosystem data used in computer systems and networks of cyberspace, which casts doubt on the quality of providing basic security services: confidentiality, integrity and authenticity. In works [4–7] it is indicated that with the growth of computing capabilities, there is not only an expansion of IT services in almost all spheres of human activity, but also a significant increase in hybrid, providing a synergistic effect, attacks with elements of social engineering. Thus, a scientific and technical problem arises to provide basic security services based on alternative approaches that ensure, first of all, the cryptographic strength of the algorithms used.

Analysis of recent research and publications [1–4; 8–14] showed that with the advent of a full-scale quantum computer, the security of modern cryptosystems providing basic security services is being questioned. Therefore, NIST USA specialists are holding a competition for post-quantum cryptography algorithms. Among the algorithms-contestants that passed to the second round there are also crypto-code constructions (CCC). Thus, the consideration of the use of the Niederreiter CCC on algebraic geometric codes (AGC) (codes on elliptic curves and / or their modifications, on defective codes) in practical algorithms of security services for their modification / improvement is an urgent task.

The purpose of this article is to build a digital signature algorithm based on Niederreiter's crypto-code construction at AGC.

To solve this goal, it is necessary to solve the following tasks:

– analyze the requirements for post-quantum cryptography algorithms;

– research on the Niederreiter's crypto-code construction, practical algorithms.

Statement of basic materials

Research of requirements for post-quantum cryptography algorithms.

When implementing a full-scale quantum computer, Shor's algorithm allows factoring the number N into factors in the time $O(lg^3N)$ using $O(lg\ N)$-bits register, which is significantly faster than any classical factorization method. The advantages of using quantum registers are significant memory savings (N quantum bits can contain 2^N bits of information), the interaction between qubits makes it possible to affect the entire register in one operation (quantum parallelism).

Thus, Shor's algorithm called into question the very existence of asymmetric cryptography, since on its basis it is possible to effectively solve problems of discrete logarithm and other problems on the complexity of which cryptographic algorithms are based. This conclusion was confirmed in March 2018 in the report of the US NIST (Report on Post-Quantum Cryptography) [1–2], which notes that the emergence of full-scale quantum computers casts doubt on the cryptographic strength of asymmetric cryptography algorithms, and in February 2019, experts NIST USA, at the opening of the competition for post-quantum cryptography algorithms, stated that the algorithms on elliptic curves are also being questioned. Thus, humanity enters the so-called post-quantum period - a period of time in the future when classical methods will be significantly improved and quantum computers with the register lengths (in qubits) necessary for successful cryptanalysis and the mathematical and software necessary for their implementation will be created. The main problems that can be solved on a quantum computer include the following:

1) Shor's quantum factorization algorithm;

2) quantum Grover's algorithm for finding an element in an unsorted base;

3) Shor's quantum algorithm for solving the discrete logarithm in a finite field;

4) quantum algorithm for solving the discrete logarithm in the EC Shor point group;

5) quantum cryptanalysis algorithms for transformations into factor ring;

6) quantum crypto analysis algorithm Xiong and Wang and its improvement and the like.

Tabl. 1 shows the results of a comparative analysis of the complexity of factorization for classical and quantum algorithms, in tabl. 2 – the complexity of the implementation of Shor's method of discrete logarithm to the group of points EC.

Table 1

Comparative analysis of the complexity of factorization for classical and quantum algorithms

Module size N, bit	Number of qubits required $2n$	Complexity of the quantum algorithm $4n^3$	Complexity of the classical algorithm
512	1024	$0.54 \cdot 10^9$	$1.6 \cdot 10^{19}$
3072	6144	$12 \cdot 10^{10}$	$5 \cdot 10^{41}$
15360	30720	$1.5 \cdot 10^{13}$	$9.2 \cdot 10^{80}$

Table 2

The complexity of the implementation of Shor's method of discrete logarithm to the point group EC

Algorithm for calculating the discrete logarithmic equation			
Base point order size, bit	Number of qubits required $f(n) = 7n + 4\log_2 n + 10$	Complexity of the quantum algorithm $360n^3$	Complexity of the classical algorithm
163	1210	$1.6 \cdot 10^9$	$3.4 \cdot 10^{24}$
256	1834	$6 \cdot 10^9$	$3.4 \cdot 10^{38}$
571	4016	$6.7 \cdot 10^{10}$	$8.8 \cdot 10^{85}$
1024	7218	$3.8 \cdot 10^{11}$	$1.3 \cdot 10^{154}$

Presented in tabl. 1–2, the results of comparisons indicate a significant reduction in energy costs for the implementation of breaking cryptoalgorithms of asymmetric cryptography, which include DS algorithms when using a quantum computer, which significantly reduces the level of “trust” in algorithms and protocols for providing basic security services: confidentiality, integrity and authenticity.

In the conditions of post-quantum cryptography, NIST experts suggest considering attacks of a special type (SIDE-CHANEL ATTACKS). The implementation of these attacks is aimed at finding vulnerabilities in the practical implementation of the cryptosystem, primarily the means of cryptographic protection.

The following classification of special attacks based on the following features was proposed:

– control of the computing process;

– the way to access the system or tool;

– the method of direct attack and the like.

Protection against special attacks can be based on features:

– fixed number of calls to the hash function, data randomization;

– independence of keys from values and the like.

The main NIST requirements for safety in the post-quantum period are:

Safety requirements:

– replacement of the ES standard FIPS 186;

– replacement of key distribution standards SP 800-56A, SP 800-56B;

– using the new standard in protocols: TLS, SSH, IPSec etc.;

– security model for encryption and distribution is a “semantically secure encryption” scheme. Security model – IND-CCA2;

Safety conditions:

– attacker access to less than 2^{64} selected cipher-text-key pairs;

Resilience requirements:

1) 128-bit classic security / 64-bit quantum security (AES-128 security margin);

2) 128-bit classic security / 80-bit quantum security (SHA-256 / SHA3-256 safety margin) SHA-384 / SHA3-384);

3) 256-bit classic security / 128-bit quantum security (AES-256 security margin).

Thus, NIST USA suggests considering the following models:

– for symmetric cryptography algorithms - under the conditions of the security model IND-CCA2 (Indistinguishability Adaptive Ciphertext Attack), which determines the resistance to an adaptive attack based on the selected text cipher;

– for electronic digital signature - under the conditions of the security model EUF-CMA (existentially unforgeable under adaptive chosen message attacks);

– for the key encapsulation protocol - under the conditions of the security model Canetti-Krawczyk (CК-safety).

As a preliminary criterion, NIST proposes an approach in which quantum attacks are limited to a set of fixed runtimes, or “depths,” of the scheme. This parameter is named MAXDEPTH

Possible values for the range MAXDEPTH:

– 2^{40} logical gates, that is, the approximate number of gates that will be sequentially executed per year;

– 2^{64} logic gates that modern classical computing architectures can execute sequentially in ten years;

– not more than 2^{96} logical gates, that is, an approximate number of gates, how atomic-scale qubits with the speed of light propagation time can perform over millennia.

Thus, the analysis showed that the use of EDS based on asymmetric cryptoalgorithms in the post-quantum period cannot provide a guaranteed level of cryptographic strength, and, accordingly, can be subject to a special type of attack based on a full-scale quantum computer.

Research on Niederreiter's crypto-code constructs

A special place among symmetric and asymmetric cryptosystems is occupied by asymmetric cryptosystems based on crypto-code constructions by McEliece and Niederreiter, who are participants in the NIST competition for a post-quantum algorithm and integrately provide not only the required level of cryptographic strength (when they are implemented in $GF(2^{10}–2^{13})$, but also the reliability of the transmitted information based on error-correcting codes (a transmission method with forward error correction is implemented). However, a significant drawback is the difficulty of their practical implementation in the alphabet $GF\,(2^{10}–2^{13})$, as well as significant energy costs. In addition, in the work of V.M. Sidelnikov [10] proposed a practical algorithm for cracking these structures using cyclic noise-immune codes. The essence of which is to find the elements of the generating matrix and remove the action of the masking matrices. The orthogonality of the generating and test matrices allows us to consider the effectiveness of the attack on the Niederreiter scheme. Sidelnikov proposes to use cascade or algebraic geometric codes as a promising direction for eliminating the revealed regularities - codes built on the basis of the algebra of the theory of error-correcting coding and geometric parameters of a curve, in particular, elliptic curves.

The general classification of crypto-code structures (CCC) is given in [4] (Fig. 1).

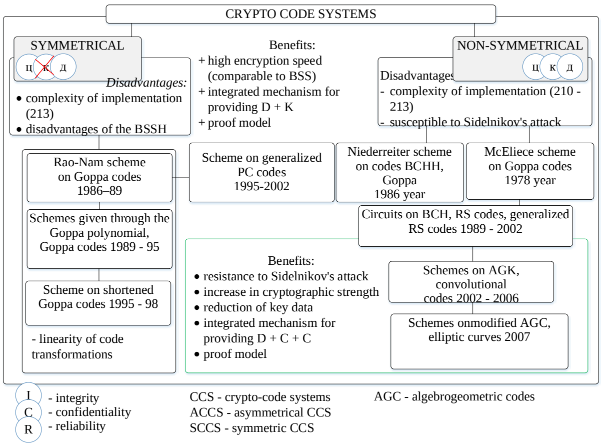
CRYPTO CODE SYSTEMS
SYMMETRICAL
ц
к
д
Disadvantages:
• complexity of implementation (213)
• disadvantages of the BSSH
Benefits:
+ high encryption speed (comparable to BSS)
+ integrated mechanism for providing D + K
+ proof model
NON-SYMMETRICAL
ц
к
д
Disadvantages
- complexity of implementation (210 - 213)
- susceptible to Sidelnikov's attack
Rao-Nam scheme on Goppa codes 1986–89
Scheme on generalized PC codes 1995-2002
Niederreiter scheme on codes BCHH, Goppa 1986 year
McEliece scheme on Goppa codes 1978 year
Schemes given through the Goppa polynomial, Goppa codes 1989 - 95
Circuits on BCH, RS codes, generalized RS codes 1989 - 2002
Scheme on shortened Goppa codes 1995 - 98
- linearity of code transformations
Benefits:
• resistance to Sidelnikov's attack
• increase in cryptographic strength
• reduction of key data
• integrated mechanism for providing D + C + C
• proof model
Schemes on AGK, convolutional codes 2002 - 2006
Schemes onmodified AGC, elliptic curves 2007
I - integrity
C - confidentiality
R - reliability
CCS - crypto-code systems
ACCS - asymmetrical CCS
SCCS - symmetric CCS
AGC - algebrogeometric codes

Fig. 1. General classification of crypto-code constructions

The analysis carried out in works [4; 8–9] showed that these cryptosystems allow providing a provable (mathematically) level of security (strength is based on the NP-complete problem – decoding a random code), ensure the efficiency of crypto transformations at the level of encryption speed with traditional cryptography algorithms and reliability, due to the use of error-correcting codes. In addition, the report of NIST specialists [1– 2] noted that it is crypto-code constructions that allow providing the required level of cryptographic strength in post-quantum cryptography.

The known methods of their construction on the basis of noise-resistant (algebraic geometric codes, AGK), mathematical models and practical algorithms are considered in works [4; 11–12].

Based on McEliese's crypto-code construction, first proposed in [11]. As a secret (private key), the generating matrix of the linear (n, k, d) code on $GF(q)$ – G, and *masking matrices:* non-degenerate $k \times k$-matrix on $GF(q)$ – X, diagonal $n \times n$-matrix D, permutation $n \times n$-matrix – P. The permutation matrix implements the permutation of vector coordinates in the form of matrix multiplication.

The public key is the matrix $G_X = X \cdot G \cdot P \cdot D$.

Encryption:

$$c_X^* = i \cdot G_X + e ,$$

where vector $c_X = i \cdot G_X$ belongs to (n, k, d) code with the generator matrix G_X, i – k-bit information vector, vector e –error vector of weight $\leq t$, serves as an additional secret parameter (session key).

On the receiving side, the receiver, knowing the public key, and using the Berlekemp-Messi decoding algorithm (polynomial complexity), receives the original text. The exchange protocol between authorized users based on the McEliece crypto-code construction on algebraic geometric (elliptic, EC) codes is shown in Fig. 2.

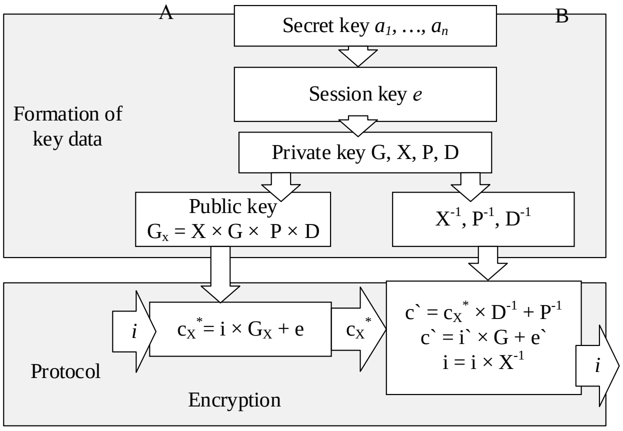

Fig. 2. An exchange protocol in an asymmetric cryptosystem based on the McEliece CCC

To eliminate the drawback - the Sidelnikov attack implementation, it is proposed to use algebraic geometric codes, codes built on curves (as an example, on elliptic curves).

Singular (supersingular) curves of 3 kinds are used to form the AGC (EC).

Algebrogeometric code along the curve X over *GF*(*q*) – this is a linear code of length $n \le N$, code words $C(c_1, c_2, …, c_n)$ of which are given by the equality:

$$\sum_{i=0}^{k-1} i_j F_j(P_i) = c_i \ ,$$

where $P_i(X_i, Y_i, Z_i)$ – projective points of the curve *X*, i.e. (X_i, Y_i, Z_i) – solutions of a homogeneous algebraic equation defining the curve *X*, $i = \overline{1, n}$; $F_j(P_i)$ – values of the generator functions at the points of the curve.

This definition is equivalent to the matrix representation of the algebraic geometric code [4]:

$$G\ (i_0, i_1, ..., i_{k-1})^T = (c_0, c_1, ..., c_{n-1}) \ ,$$

where *G* – generator matrix of dimension *k*×*n*, *k* = α – *g*+1, α=*degX*·*degF* of view

$$G = \begin{pmatrix} F_0(P_0) & F_0(P_1) & ... & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & ... & F_1(P_{n-1}) \\ ... & ... & ... & ... \\ F_{k-1}(P_0) & F_{k-1}(P_1) & ... & F_{k-1}(P_{n-1}) \end{pmatrix} =$$

$$= \left\| F_j\ (P_i) \right\|_{n,k} .$$

However, the construction of the CCC on EC does not eliminate the disadvantage of significant energy consumption in practical implementation. To eliminate the disadvantage, it is proposed to use modified EC (MEC), proposed in works [4; 8].

Consider a *cryptosystem based on Niederreiter's crypto-code construction*, first proposed in [12]. Private (private) key check matrix *H* -linear (*n*, *k*, *d*) code on *GF*(*q*), *masking matrices:* non-degenerate *r* × *r*-matrix on *GF*(*q*) – *X*, diagonal *n* × *n*-matrix *D*, permutation *n* × *n*-matrix – *P*. Opened (public) key matrix $H_X = X \cdot H \cdot P \cdot D$. Rule encryption

$$S_X = e \cdot H_X^T \ ,$$

where vector *e* – is a vector of length *n* and weight ≤ *t*, is computed in advance based on the equilibrium coding and is a transformed input sequence. On the receiving side, the recipient finds from q^k solutions of expression $S_X = c_X^* \cdot H_X^T$. Next, decryption is used based on the Berlekamp-Messi algorithm.

The scheme of the exchange protocol in an asymmetric cryptosystem based on the Niederreiter crypto-code construction on elliptic codes is presented in the form of Fig. 3. To use the EC in the Niederreiter CCC, the equilibrium coding of *m*-ary codes is used – the block diagram of the algorithm is shown in Fig. 4.

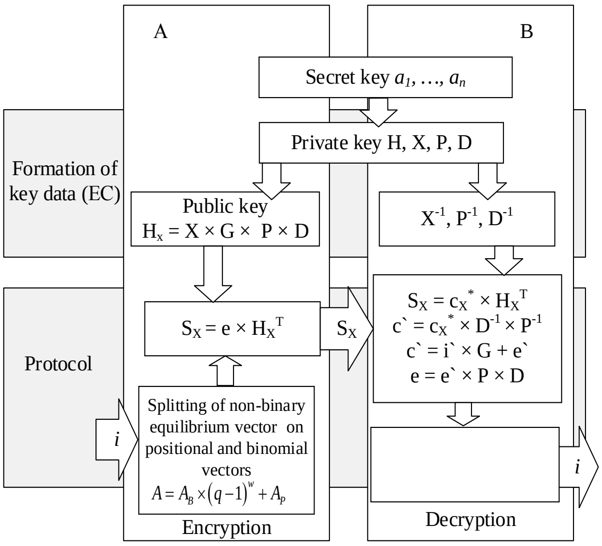

Fig. 3. An exchange protocol in an asymmetric cryptosystem based on the Niederreiter CCC on the EC

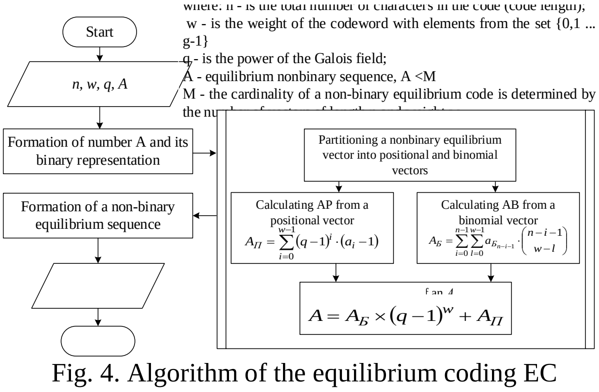
where: n - is the total number of characters in the code (code length);
w - is the weight of the codeword with elements from the set {0,1 ... g-1}
q - is the power of the Galois field;
A - equilibrium nonbinary sequence, A <M
M - the cardinality of a non-binary equilibrium code is determined by the nu
Start
n, w, q, A
Formation of number A and its binary representation
Formation of a non-binary equilibrium sequence
Partitioning a nonbinary equilibrium vector into positional and binomial vectors
Calculating AP from a positional vector
$A_П = \sum_{i=0}^{w-1} (q-1)^i \cdot (a_i - 1)$
Calculating AB from a binomial vector
$A_Б = \sum_{i=0}^{n-1}\sum_{l=0}^{w-1} a_{Б_{n-i-1}} \cdot \binom{n-i-1}{w-l}$
$A = A_Б \times (q-1)^w + A_П$

Fig. 4. Algorithm of the equilibrium coding EC in the crypto-code construction of the Niederreiter

Fig. 5 shows a practical encryption algorithm in the Niederreiter CCC in the EC.

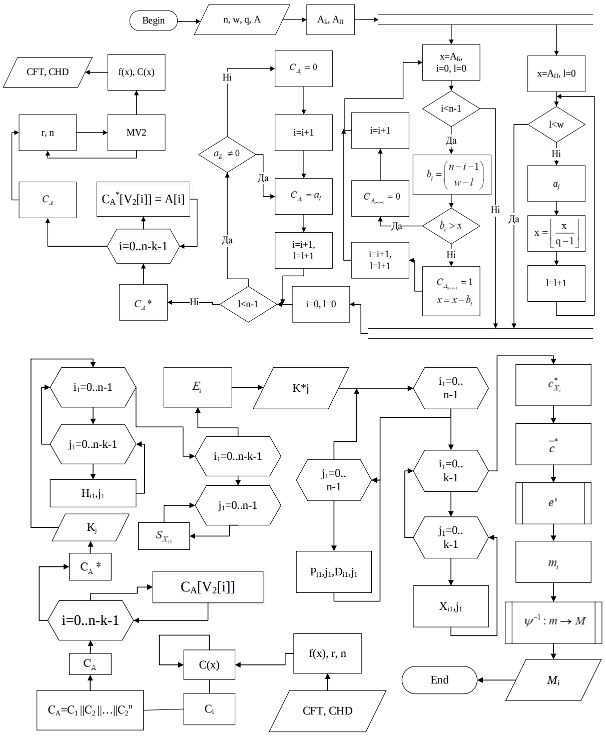

Fig. 5. CCC encryption algorithm on the EC

To reduce energy costs while maintaining stability, a modification of the Niederreiter CCC is used on modified (shortened and / or elongated) elliptical codes (MEC). In fig. 6–9 shown the exchange protocols and encryption algorithms in the Niederreiter MCCC on modified (shortened and / or extended) MECs, respectively.

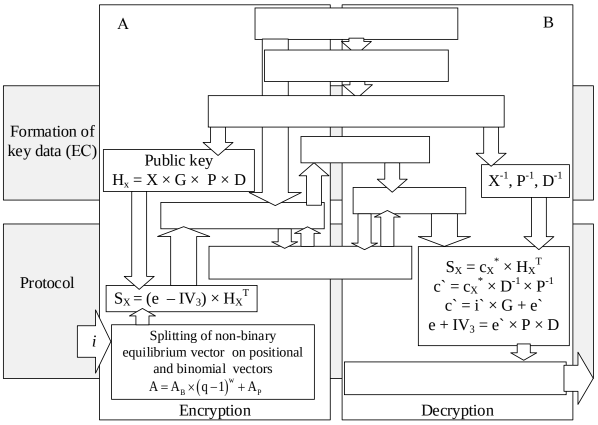

Fig. 6. An exchange protocol
in an asymmetric cryptosystem based
on the Niederreiter CCC on shortened MEC

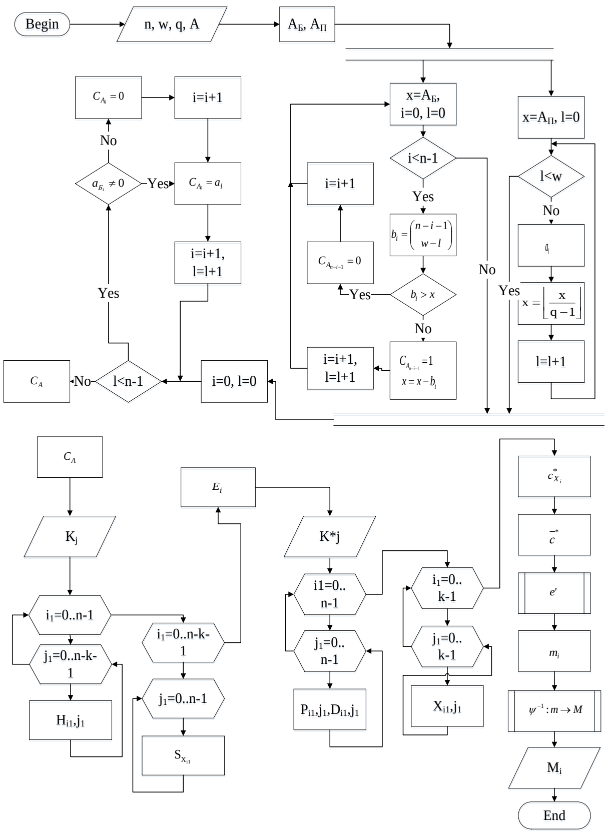

Fig. 7. CCC encryption algorithm on shortened MEC

This approach makes it possible to reduce the level of CCC formation over GF (2^2–2^4).

For the Niederreiter CCC, an additional initialization vector is used that defines the codewords that satisfy the decoding algorithm.

The algorithm for forming a cryptogram in the modified Niederreiter CCC on MEC, taking into account the revealed regularity, is presented as a sequence of steps:

Step 1. Input of information to be encoded, one of the elements of the set of suitable plain texts. Public key introduction H_X^{EC}.

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

Step 3. Formation of the initialization vector IV_1.

Step 4. Formation of the truncated error vector:

$$e_x = e(A) - IV_2.$$

Step 5. Formation of a codogram:

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

The algorithm for decoding the codogram in the modified Niederreiter CCC on MEC is presented as a sequence of steps:

Step 1. Introduction of the codogram S_X, that is decoded. Private key introduction – matrices *X*, *P*, *D*.

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

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

Step 3. Removing the action of diagonal and adjustable matrices: $\bar{c}^* = c_X^* \cdot D^{-1} \cdot P^{-1}$.

Step 4. Decoding vector $\bar{c}^*$. Forming vector e_x’.

Step 5. Transforming vector e_x’: $e_x = e_x$’$\times P \times D$.

Step 6. The formation of the desired error vector are e: $e = e_x + IV_2$.

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

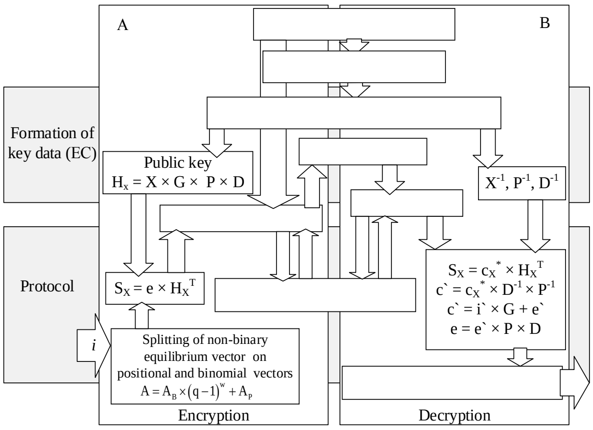
A
B
Formation of key data (EC)
Protocol
Public key $H_x = X \times G \times P \times D$
X^{-1}, P^{-1}, D^{-1}
$S_X = e \times H_X^T$
$S_X = c_X^* \times H_X^T$
$c` = c_X^* \times D^{-1} \times P^{-1}$
$c` = i` \times G + e`$
$e = e` \times P \times D$
i
Splitting of non-binary equilibrium vector on positional and binomial vectors
$A = A_B \times (q-1)^w + A_P$
Encryption
Decryption

Fig. 8. An exchange protocol
in an asymmetric cryptosystem
based on the Niederreiter CCC on extended MEC

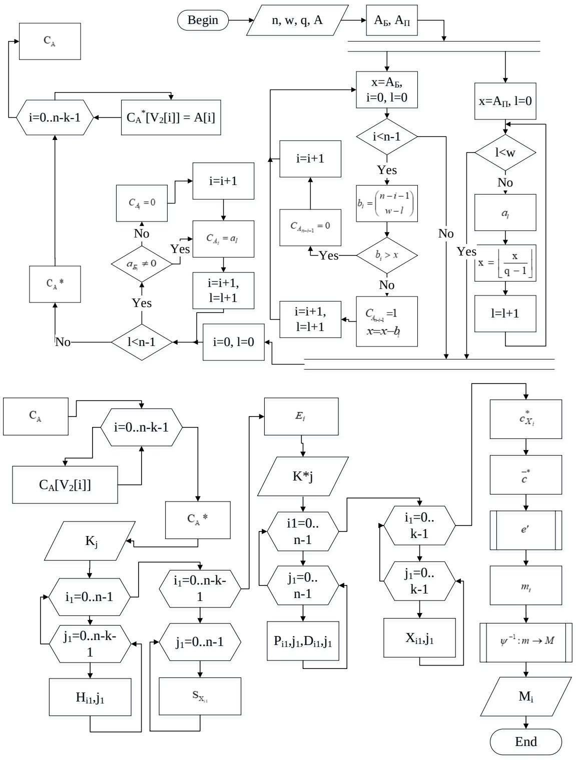

Fig. 9. CCC encryption algorithm on extended MEC

To further reduce the level of energy consumption while preserving the cryptographic strength of the cryptosystem, in [4; 9], it is proposed to use hybrid crypto-code constructions of McEliece and Niederreiter on defective codes.

Fig. 10 shows a block diagram of one step of the universal mechanism for causing damage.

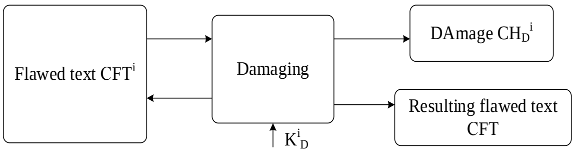

Fig. 10. Block diagram of one step damage mechanism

Cryptographic harmed texts are texts obtained in the following ways [13–14]:

– *approach 1*: damage to the original text, followed by encryption of the damaged text and / or its damage (Fig. 11);

– *approach 2*: damage to the ciphertext (Fig. 12);

– *approach 3*: causing damage to the original text and ciphertext of the damaged text (Fig. 13).

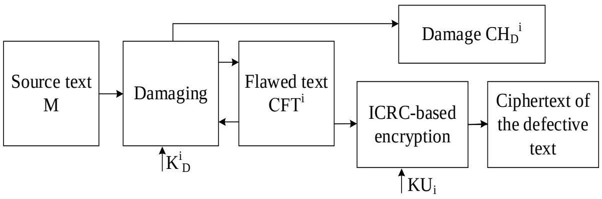

Fig. 11. Structural diagram of building a hybrid cryptosystem based on damage to the original text (approach 1)

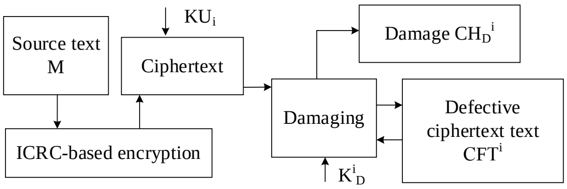

Fig. 12. Structural diagram of the construction of a hybrid cryptosystem based on damage to ciphertext (approach 2)

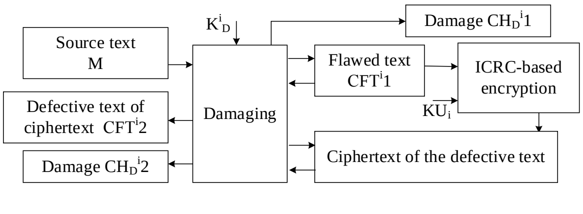

Fig. 13. Structural diagram of the construction of a hybrid cryptosystem based on damage to the original text and ciphertext (approach 3)

To determine the optimal method, let us analyze the ratio of the number of required additional operations to implement the approach to the size of the resulting outgoing data using the example of the Niederreiter CCC.

The dependence of the group operations of the implementation of the NCCC on the field strength is given in Tabl. 3.

Table 3

Dependence of the software implementation on the field strength (the number of thousands of additional operations before encryption / after / amount)

Ap-proach	2^5	2^7	2^9	2^{11}
1	1002/–/1002	3285/–/3285	6322/–/6322	11078/–/8247
2	–/1501/1501	–/4289/4289	–/9296/9296	–/15908/15908
3	992/1487/2479	2952/4428/7380	5793/8690/14483	10086/15130/25216

Tabl. 4 shows the length of the transmitted data.

Table 4

Length of transmitted data in bytes

Ap-proach	2^5	2^7	2^9	2^{11}
1	500902	902403	1642357	2374489
2	375298	667029	1072313	1652979
3	627533	1044069	1868102	2716713

The ratio of these values shows the bit rate ratio for each additional operation (Table 5).

Table 5

Number of bits per additional operation

Ap-proach	2^5	2^7	2^9	2^{11}
1	2.5E-04	4.55E-04	4.812E-04	4.341E-04
2	4.999E-04	8.038E-04	**10.836E-04**	**12.03E-04**
3	4.938E-04	8.836E-04	9.691E-04	11.602E-04

Thus, the use of the approach when damaging the ciphertext with a modified CCC on MEC, shown in Fig. 12 (second approach) increases the throughput starting from the GF field (29). This method is the optimal approach for constructing a hybrid Niederreiter CCC (McEliece) on a MEC.

The information core of a certain text is understood as a defective CFT text, obtained by a cyclical transformation of the universal mechanism of causing damage C_m.

Universal damage mechanism C_m can be described by [4]:

$$CFT / CH_{FT} = E_1 (M, KU^{EC}),$$

$$CHD / CH_D = E_2 (M, KU^{EC}),$$

$$M = E_{1,2}^{-1} (CFT / CH_{FT}, CHD / CH_D, KU^{EC}),$$

where $CFT / CH_{FT} = CFT / CH^i_{FT}, \dots, CFT / CH^m_{FT}$,

$$KU^{EC} = (K^i_D, \dots, K^m_D, KU_1^{EC}, \dots, KU_m^{EC}),$$

$$CHD / CH_D = CHD / CH^i_D, \dots, CHD / CH^m_D.$$

Thus, as a result, we have two ciphertext: (damage (CH_D) and defective text (FTC)). Each of which makes no sense either in the alphabet of the original text, or in the alphabet of the ciphertext. In fact, the ciphertext of the original message (M) is represented as a combination of two defective ciphertexts, each of which, separately, cannot recover the original text. To restore the original sequence, there is no need to know intermediate defective sequences.

Development of a modified digital signature protocol based on crypto-code constructions

To ensure the service of authenticity in cyberspace, the DSS (Digital Signature Standard) protocol is used, which describes DSA (Digital Signature Algorithm) based on RSA and ElGamal algorithms. The main difference between asymmetric cryptoalgorithms is a relatively higher level of security in the El-Gamal algorithm and the ability to use elliptic curves to form the DS. However, the DS protocol on RSA provides faster DS shaping. Crypto resistance is based on the security of the applied algorithms RSA (NP-complete problem – factorization of a number), El-Gamal&#39;s algorithm (NP-complete problem - finding a discrete algorithm in a group of numbers, or in a group of points of an elliptic curve, depending on the use of the EC equation). However, in the current trends in the development of the post-quantum period, these algorithms may not provide the required level of cryptographic strength, and can be cracked in polynomial time. Therefore, a modified DSS protocol based on CCC is proposed, the block diagram is shown in Fig. 14.

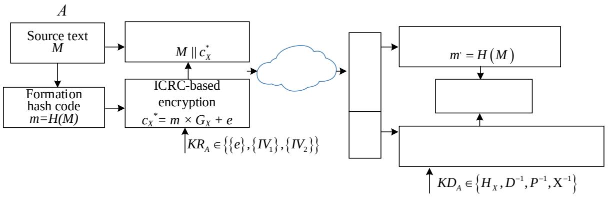
A
Source text M
$M \| c_X^*$
Formation hash code m=H(M)
ICRC-based encryption $c_X^* = m \times G_X + e$
$KR_A \in \{\{e\},\{IV_1\},\{IV_2\}\}$
$m' = H(M)$
$KD_A \in \{H_X, D^{-1}, P^{-1}, X^{-1}\}$

Fig. 14. Modified protocol DSS

The sender uses personal data as key data: Session key CCC – e (error vector), and initialization vectors (IV_1 – shortening symbols, IV_2 – extension symbols *MEC*). The receiver uses the MEC orthogonal parity check matrix and inverse masking matrices as the sender's public key.

Thus, the use of CCC in the DSS protocol will provide the required level of resistance in the post-quantum period and the synergy and / or hybridity of modern attacks.

Conclusion

1. The analysis of computing resources in the post-quantum period casts doubt on the use of traditional cryptography and public-key cryptography algorithms to provide security services. Further development and emergence of the quantum computer will allow cyber attackers to combine threats to achieve synergy and / or hybridity. In such conditions, it is necessary to modify

and / or develop fundamentally new algorithms that provide the required level of cryptographic strength.

2. The scheme of the modified DSA protocol based on modified (hybrid) crypto-code constructions provides the required level of resistance to modern threats of the post-quantum period. The studies carried out confirm that the use of MEC (EC) provides speed at the level of the speed of crypto-transformations of symmetric cryptoalgorithms, provable cryptographic strength based on the complexity-theoretic problem of decoding a random code (provided by 10^{30} – 10^{35} group operations), and reliability based on the use of a shortened algebraic geometric code (provided by $P_{ош}$=10^{-9} – 10^{-12}). To further reduce the power of the alphabet (Galois fields to GF (2^4 – 2^6) it is proposed to use systems based on defective codes that allow simultaneous formation of multichannel cryptosystems.

References

1. The National Institute of Standards and Technology (2010), *Guide for Cybersecurity Event Recovery*, available at: https://nvlpubs.nist.gov/nistpubs/.../NIST.SP.800-184.pdf (Accessed Februray 1, 2020).

2. The National Institute of Standards and Technology (2001), *Security requirements for cryptographic modules*, available at: https://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf (Accessed Februray 1, 2020).

3. Cichonski, J., Franklin, J.M. and Bartock, M. (2017), *Guide to LTE Security*, available at: https://csrc.nist.gov/publications/drafts/800-187/sp800_187_draft.pdf (Accessed Februray 1, 2020).

4. Hryshchuk, R., Yevseiev, S. and Shmatko, A. (2018), *Construction methodology of information security system of banking information in automated banking systems: monograph*, Premier Publishing s. r. o., Vienna, 284 p.

5. Ankur Lohachab Anu Lohachab Ajay Jangra (2020), A Comprehensive Survey of Prominent Cryptographic Aspects for Securing Communication in Post-Quantum IoT Networks, *Internet of Things*, available at: https://www.sciencedirect.com/science/article/pii/S2542660520300159 (Accessed Februray 1, 2020). https://doi.org/10.1016/j.iot.2020.100174.

6. Petrenko, K., Mashatan, A. and Shirazi, F. (2019), Assessing the quantum-resistant cryptographic agility of routing and switching IT network infrastructure in a large-size financial organization, *Journal of Information Security and Applications*, Vol. 46, pp. 151-163. https://doi.org/10.1016/j.jisa.2019.03.007.

7. Shubhani Aggarwal, Rajat Chaudhary, Gagangeet Singh Aujla, Neeraj Kumar, Kim-Kwang Raymond Choo and Albert Y. Zomaya (2019), Blockchain for smart communities: Applications, challenges and opportunities, *Journal of Information Security and Applications*, Vol. 144, pp. 13-48. https://doi.org/10.1016/j.jnca.2019.06.018.

8. Yevseiev, S., Kots, H. and Liekariev, Y. (2016), Developing of multi-factor authentication method based on Niederreiter-McEliece modified crypto-code system, *Eastern-European Journal of Enterprise Technologies*, No. 6/4(84), pp. 11-23.

9. Yevseiev, S., Kots, H., Minukhin, S., Korol, O. and Kholodkova, A. (2017), The development of the method of multifactor authentication based on hybrid crypto-code constructions on defective codes, *Eastern-European Journal of Enterprise Technologies*, No. 5/9(89), pp. 19-35.

10. Sidel'nikov, V.M. (2002), "Kriptografija i teorija kodirovanija" [Cryptography and coding theory], *Materialy konferencii "Moskovskij universitet i razvitie kriptografii v Rossii"*, MGU, Moscow, pp. 1-22.

11. McEliece, R.J. (1978), A Public-Key Criptosystem Based on Algebraic Theory, *DGN Progres Report 42-44*, Jet Propulsi on Lab., Pasadena, CA, pp. 114-116.

12. Niederreiter, H. (1986), Knapsack-Type Cryptosystems and Algebraic Coding Theory, *Probl. Control and Inform. Theory*, Vol.15, pp. 19-34.

13. Mishhenko, V.A. and Vilanskij, Ju.V. (2007), "*Ushherbnye teksty i mnogokanal'naja kriptografija*" [*Damaged texts and multichannel cryptography*], Jenciklopediks, Minsk.

14. Mishhenko, V.A., Vilanskij, Ju.V. and Lepin, V.V. (2006), "*Kriptograficheskij algoritm MV 2*" [*Cryptographic algorithm MV 2*], Minsk.

15. Rukhin, A. and Soto, J. (2010), *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, NIST Special Publication, 131 p.

Список літератури

1. The National Institute of Standards and Technology. Guide for Cybersecurity Event Recovery [Electronic resource]. – 2010. – Available at: https://nvlpubs.nist.gov/nistpubs/.../NIST.SP.800-184.pdf (Accessed Februray 1, 2020).

2. The National Institute of Standards and Technology. Security requirements for cryptographic modules [Electronic resource].– 2001. – Available at: https://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf (Accessed Februray 1, 2020).

3. Cichonski J. Guide to LTE Security [Electronic resource] / J. Cichonski, J.M. Franklin, M. Bartock. Available at: https://csrc.nist.gov/publications/drafts/800-187/sp800_187_draft.pdf (Accessed Februray 1, 2020).

4. Hryshchuk R. Construction methodology of information security system of banking information in automated banking systems: monograph / R. Hryshchuk, S. Yevseiev, A. Shmatko. – Vienna: Premier Publishing s. r. o., 2018. – 284 p.

5. Ankur Lohachab. A Comprehensive Survey of Prominent Cryptographic Aspects for Securing Communication in Post-Quantum IoT Networks / Ankur Lohachab Anu Lohachab Ajay Jangra // Internet of Things. – 2020. Available at: https://www.sciencedirect.com/science/article/pii/S2542660520300159 (Accessed Februray 1, 2020) https://doi.org/10.1016/j.iot.2020.100174.

6. Petrenko K. Assessing the quantum-resistant cryptographic agility of routing and switching IT network infrastructure in a large-size financial organization / K. Petrenko, A. Mashatan, F. Shirazi // Journal of Information Security and Applications. – 2019. – Vol. 46. – P. 151-163. https://doi.org/10.1016/j.jisa.2019.03.007.

7. Blockchain for smart communities: Applications, challenges and opportunities / Shubhani Aggarwal, Rajat Chaudhary, Gagangeet Singh Aujla, Neeraj Kumar, Kim-Kwang Raymond Choo and Albert Y. Zomaya // Journal of Information Security

and Applications. – 2019. – Vol. 144. – P. 13-48. https://doi.org/10.1016/j.jnca.2019.06.018.

8. Yevseiev S. Developing of multi-factor authentication method based on Niederreiter-McEliece modified crypto-code system / S. Yevseiev, H. Kots, Y. Liekariev // Восточно-европейский журнал передовых технологий. – 2016. – № 6/4(84). – С. 11-23.

9. The development of the method of multifactor authentication based on hybrid crypto-code constructions on defective codes / S. Yevseiev, H. Kots, S. Minukhin, O. Korol, . Kholodkova // Восточно-европейский журнал передовых технологий. – 2017. – № 5/9(89). – С. 19-35.

10. Сидельников В.М. Криптография и теория кодирования / В.М. Сидельников // Материалы конференции "Московский университет и развитие криптографии в России". – М.: МГУ, 2002. – С. 1-22.

11. McEliece R.J. A Public-Key Criptosystem Based on Algebraic Theory / R.J. McEliece // DGN Progres Report 42-44. – Jet Propulsi on Lab. Pasadena, CA. – 1978. – P. 114-116.

12. Niederreiter H. Knapsack-Type Cryptosystems and Algebraic Coding Theory / H. Niederreiter // Probl. Control and Inform. Theory. – 1986. – Vol. 15. – P. 19-34.

13. Мищенко В.А. Ущербные тексты и многоканальная криптография / В.А. Мищенко, Ю.В. Виланский. – Минск: Энциклопедикс, 2007.

14. Мищенко В.А. Криптографический алгоритм MV 2 / В.А. Мищенко, Ю.В. Виланский, В.В. Лепин. – Минск, 2006.

15. Rukhin A. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications / A. Rukhin. – NIST Special Publication. – 131 p.

Received by Editorial Board 14.08.2020
Signed for printing 22.09.2020

Відомості про автора:

Циганенко Олексій Сергійович
аспірант
Харківського національного
економічного університету ім. С. Кузнеця,
Харків, Україна
https://orcid.org/0000-0002-5784-8438

Information about the author:

Oleksii Tsyhanenko
Doctoral Student
of Simon Kuznets
Kharkiv National University of Economics,
Kharkiv, Ukraine
https://orcid.org/0000-0002-5784-8438

РОЗРОБКА АЛГОРИТМУ ЦИФРОВОГО ПІДПИСУ НА ОСНОВІ КРИПТО-КОДОВОЇ СИСТЕМИ НІДЕРРАЙТЕРА

О.С. Циганенко

Розвиток обчислювальних ресурсів в постквантовий період ставить під сумнів забезпечення необхідного рівня стійкості алгоритмів симетричної та несиметричної криптографії. Поява повномасштабного квантового комп'ютера на основі алгоритмів Шора і Гровера значно збільшує можливості кіберзлочинців і знижує стійкість використовуваних криптосистем в протоколах забезпечення основних послуг безпеки. У статті аналізуються основні вимоги до стійкості до алгоритмів постквантовій криптографії. В таких умовах необхідно використання модифікованих криптосистем, що забезпечують інтегрований необхідний рівень стійкості і оперативності криптоперетворень. Одним з таких механізмів є крипто-кодові конструкції Мак-Еліса і Нідеррайтера, що забезпечують необхідні показники стійкості, оперативності та достовірності. У роботі проводиться аналіз побудови крипто-кодової конструкції Нідеррайтера на еліптичних (ЕС), модифікованих еліптичних кодах (МЕС) укорочених і / або подовжених, і збиткових кодах, практичні алгоритми їх реалізації. Пропонується удосконалений протокол формування цифрового підпису з використанням крипто-кодових конструкцій Нідеррайтера.

Ключові слова: *постквантовий період, цифровий підпис, крипто-кодові конструкції Нідеррайтера, еліптичні коди.*

РАЗРАБОТКА АЛГОРИТМА ЦИФРОВОЙ ПОДПИСИ НА ОСНОВЕ КРИПТО-КОДОВОЙ СИСТЕМЫ НИДЕРРАЙТЕРА

А.С. Цыганенко

Развитие вычислительных ресурсов в постквантовый период ставит под сомнение обеспечение требуемого уровня стойкости алгоритмов симметричной и несимметричной криптографии. Появление полномасштабного квантового компьютера на основе алгоритмов Шора и Гровера значительно увеличивает возможности киберпреступников и снижает стойкость используемых криптосистем в протоколах обеспечения основных услуг безопасности. В статье анализируются основные требования к стойкости к алгоритмам постквантовой криптографии. В таких условиях необходимо использование модифицированных криптосистем, обеспечивающих интегрировано требуемый уровень стойкости и оперативности криптопреобразований. Одним из таких механизмов являются крипто-кодовые конструкции Мак-Элиса и Нидеррайтера, обеспечивающие требуемые показатели стойкости, оперативности и достоверности. В работе проводится анализ построения крипто-кодовой конструкции Нидеррайтера на эллиптических (ЕС), модифицированных эллиптических кодах (МЕС) укороченных и/или удлиненных, и ущербных кодах, практические алгоритмы их реализации. Предлагается усовершенствованный протокол формирования цифровой подписи с использованием крипто-кодовых конструкций Нидеррайтера.

Ключевые слова: *постквантовый период, цифровая подпись, крипто-кодовые конструкции Нидеррайтера, эллиптические коды.*