UDC 004.056.5

Lavryk I. V. ORCID: 0000-0002-3433-9083 (MITIT)
DScTech, S. R. F Chevardin V. E. 0000-0002-1070-4568 (MITIT)
Marchuk O. V. ORCID: 0000-0003-4224-5113 (MITIT)

ASSESSMENT OF THE SECURITY LEVEL OF MODERN STANDARDIZED CRYPTOGRAPHIC TRANSFORMATIONS

Лаврік І. В., Чевардін В. Є., Марчук О. В. Оцінка рівня безпеки сучасних стандартизованих криптографічних перетворень.

Сучасні системи криптографічного захисту інформації, які будуються на основі математичних перетворень в кільці, групі та групі точок еліптичних кривих, більше не вважаються перспективним напрямком для подальшого розвитку систем захисту інформації. Це пов'язано з появою реального квантового комп'ютера, що призвело до активізації нового етапу розвитку криптосистем, який умовно називають постквантовими стабільними криптографічними алгоритмами.

У даній статті наводиться оцінка рівня безпеки існуючих стандартизованих криптосистем і перспективних криптоалгоритмів, потенційно стійких до квантового криптоаналізу. Рівень безпеки існуючих асиметричних криптосистем для квантового криптоаналізу є поліноміальним. Показано залежність криптографічної стійкості алгоритму від розміру загальносистемних параметрів. Наведені обмеження для проведення квантового криптоаналізу на теперішній час.

У статті наведені значення загальносистемних параметрів криптосистеми на основі еліптичних кривих, які можуть дати час для переходу до постквантової криптографії. Також показані такі криптосистеми, як SIKE, SIDH, які мають запас криптостійкості до квантового криптоаналізу та можливість побудови на їх основі постквантового алгоритму електронного цифрового підпису та інкапсуляції ключів.

Ключові слова: *постквантова криптографія, квантовий криптоаналіз, алгоритм Шора, RSA, ECC.*

Modern systems of cryptographic protection of information, which are based on mathematical transformations in the ring, group, and group of points of elliptic curves are no longer considered a promising area for further development of information security systems. This is due to the emergence of the real quantum computer, which led to the activation of a new stage in the development of cryptosystems, which are conventionally called post-quantum stable cryptographic algorithms.

This article provides an assessment of the existing standardized cryptosystems security level and promising crypto-algorithms potentially resistant to quantum cryptanalysis. The security level of existing asymmetric cryptosystems for quantum cryptanalysis is polynomial. The dependence of the algorithm security level on the size of the system-wide parameters is shown. The limitations for conducting quantum cryptanalysis at the present time are given.

The article gives the values of system-wide parameters of the elliptic curves cryptosystem, which can give time for the transition to post-quantum cryptography. Also shown are such cryptosystems as SIKE, SIDH, which have a margin of cryptoresistance to quantum cryptanalysis and the possibility of building a post-quantum electronic digital signature and key encapsulation algorithm of on their basis.

Keywords: *postquantum cryptography, quantum cryptanalysis, Shor's algorithm, RSA, ECC.*

1. Statement of the problem and relevance of the research

Nowadays, the security level is one of the main indicators of information security which is transmitted and processed in information systems. The security level of the algorithm is based on the complexity of solving certain mathematical problems (factorization of large integers, solving a discrete logarithm, etc.). The complexity of computing these problems on modern computers is sub-exponential or exponential. However, the appearance of the first quantum computer made it obvious the possibility of using Shor's [1] and Grover's [2] cryptanalysis algorithms to solve certain mathematical problems with polynomial complexity, which endangered the existing cryptographic information protection algorithms [3].

The creation of a quantum computer capable of computing Shor's cryptanalysis algorithm or Grover's unordered database search algorithm for standardized cryptosystems may cause threats to the security of critical infrastructure objects.

2. Main part.

Well-known algorithms for asymmetric transformation in a ring, a group, and a group of elliptic curve points are RSA, DSA, ECC, ECDSA, ECRSA, and others similar to them. Most attacks on such cryptosystems are aimed at finding the private key. Thus, for the RSA cryptosystem, the resistance against such kind of attack is based on the complexity of the factorization of module N. It is believed that the best factorization algorithm is the algorithm of the general lattice of the numerical field or its modification. The time complexity [5] of such algorithms is subexponential and is calculated by expression (1):

$$O(\exp(\delta + o(1)(lnN)^{\gamma})\,(lnlnN)^{1-\gamma}),\ \delta = 1.92, \gamma = \frac{1}{3}. \quad (1)$$

Shor's algorithm has polynomial complexity. It can decompose a large prime number into prime factors in a time approximately equal to (2):

$$O(4n^3), \quad (2)$$

it requires the following number of qubits (3):

$$O(2n), \quad (3)$$

where n – module size.

Example 1:

Let`s evaluate the RSA-512 cryptographic algorithm cryptanalysis complexity for Shor's algorithm (2, 3):

$$O(4n^3) = O(4 \times 512^3) = O(536870912) \approx O(11{,}5 \times 10^{10}).$$

The required number of qubits to implement the specified algorithm:

$$O(2n) = 2 \times 512 = 1024.$$

Table 1 shows the estimation values of the quantum cryptanalysis algorithm parameters for the RSA cryptosystems.

Table 1

Module size, bits	Required number of qubits	The complexity of quantum cryptanalysis	The complexity of quantum cryptanalysis
512	1024	$0{,}5 \times 10^{8}$	$1{,}6 \times 10^{19}$
768	1536	$1{,}8 \times 10^{9}$	$9{,}9 \times 10^{22}$
1024	2048	$4{,}3 \times 10^{9}$	$1{,}2 \times 10^{26}$
2048	4096	$3{,}4 \times 10^{10}$	$1{,}35 \times 10^{35}$
3072	6144	$11{,}5 \times 10^{10}$	5×10^{41}
15360	30720	$1{,}5 \times 10^{13}$	$9{,}2 \times 10^{80}$

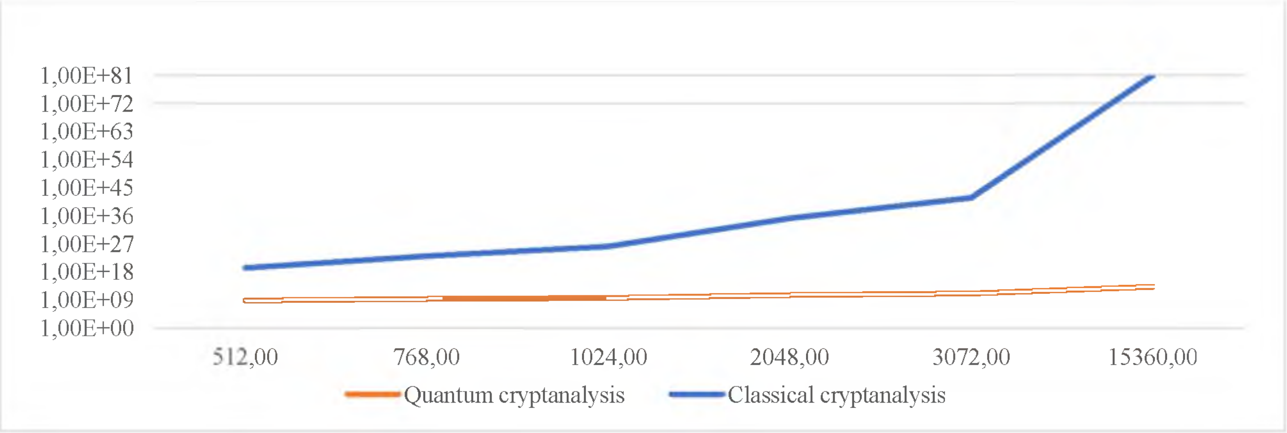

Fig. 1. Complexity of RSA cryptanalysis

From the results of analytical evaluations (Table 1) and the graph (Fig. 1), we can see that even with a key length of 15360 bits, only $1{,}5 \times 10^{13}$ operations are needed on a quantum computer, which means that this algorithm can be broken in polynomial time.

Problems of the elliptic curves discrete logarithm can be solved using ρ-Pollard's and λ-methods, it`s complexity is estimated by expression (4):

$$O(\sqrt{q}), \tag{4}$$

where $q = 2n$, and n – base point size.

In addition, in the general case, Shor's quantum algorithm is capable to solve the logarithmic equation [4] with an approximate complexity:

$$O(360n^3). \tag{5}$$

For this, you need to use a quantum computer with the number of the qubits equal to:

$$O(7n + 4log_2 n + 10). \tag{6}$$

Example:

Let`s evaluate the complexity of classical and quantum algorithms of discrete logarithms in a group of points of an elliptic curve with the base point order size ord(E) = 110 bits.

The complexity of classical cryptanalysis for the specified algorithm will be:

$$O(\sqrt{q}) = \sqrt{2^{110}} = 36\,028\,797\,018\,963\,968 \approx 3{,}6 \times 10^{16}.$$

The complexity of quantum cryptanalysis for the specified algorithm will be:

$$O(360n^3) = 479\,160\ \ 000 \approx 0{,}5 \times 10^9.$$

For this implementation, you need to use a quantum computer with the number of the qubits equal to:

$$O(7n + 4log_2 n + 10) = 7 \times 110 + 4log_2 110 + 10 = 807.125\ldots \approx 808.$$

Table 2 shows the parameter estimation values of the quantum cryptanalysis algorithm for cryptosystems on elliptic curves.

Table 2

Basepoint size, bits	Required number of qubits	The complexity of quantum cryptanalysis	The complexity of quantum cryptanalysis
110	808	$0{,}5 \times 10^9$	$3{,}6 \times 10^{16}$
163	1181	$1{,}5 \times 10^9$	$3{,}4 \times 10^{24}$
224	1610	4×10^9	$5{,}2 \times 10^{33}$
256	1834	6×10^9	$3{,}4 \times 10^{38}$
509	3609	$4{,}7 \times 10^{10}$	$4{,}1 \times 10^{76}$
571	4044	$6{,}7 \times 10^{10}$	$8{,}8 \times 10^{85}$
1024	7218	$3{,}8 \times 10^{11}$	$1{,}3 \times 10^{154}$
2048	14390	$3{,}1 \times 10^{12}$	$1{,}8 \times 10^{308}$

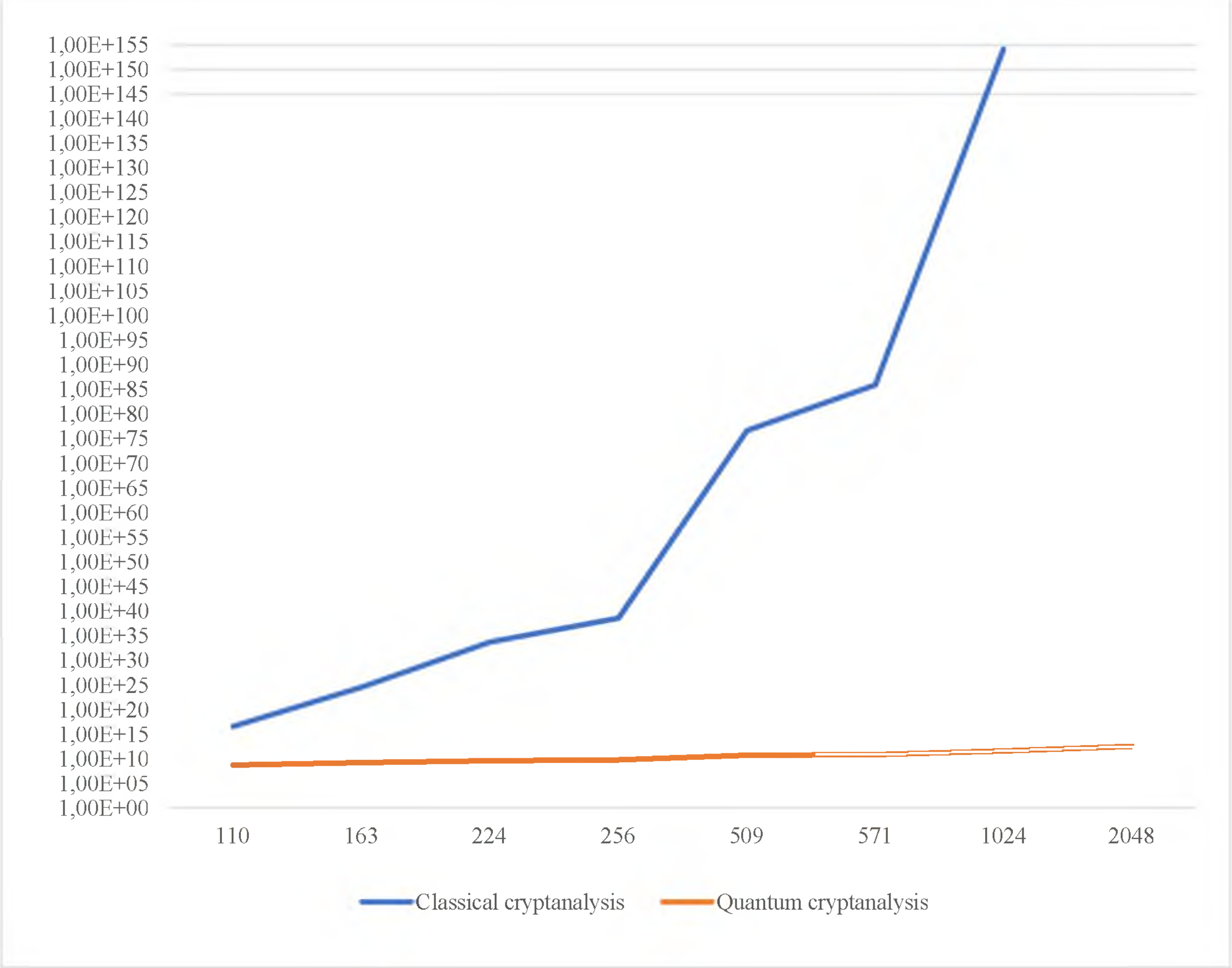

Fig. 2. Complexity of ECC cryptanalysis

From the results of analytical evaluations (Table 2) and the graph (Fig. 2), we can see that increasing the base point order size does not significantly increase cryptographic stability during quantum cryptanalysis, unlike classical cryptanalysis. This allows an attacker to perform quantum cryptanalysis in polynomial time.

Also, a comparison of analytical estimates, based on NIST recommendations [10] (Table 1, Table 2) shows that ECC requires a much smaller length of keys to ensure a comparable security level , which is provided by long RSA keys [6], but the implementation of ECC quantum cryptanalysis requires a smaller qubits number (Table 3).

Table 3

RSA key length, bits	Required number of qubits	ECC key length, bits	Required number of qubits
2048	4096	224	1610
3072	6144	256	1834

In both cases, quantum cryptanalysis requires a large number of qubits, which makes it impossible. However, eventually, such a computer will be created, so the transition to new algorithms resistant to quantum cryptanalysis must be done in advance.

New cryptographic transformations and the possibilities of their application published in open sources over the last 10 years are listed in Table 4 [8].

Table 4

Algorithm, Main cryptographic assumption	Used operations	Public Key length (bits) depending on the selected parameters	Private Key length (bits) depending on the selected parameters	Ability to create a digital signature	Ability to encrypt/ decrypt data
NTRU, NTRU PRIME, Falcon lattice-based	Matrix multiplication	NTRU – 699–2401 NTRU PRIME – 897–2067 Falcon – 897, 1793	NTRU – 935–2983 NTRU PRIME – 1125–3059 Falcon – 1281, 2305	+	+
Rainbow multivariable polynomials	Matrix multiplication, solving a linear system of equations	60192–1930600	64–1408736	+	–
SPHINCS+, Picnic hash-based	Hash functions (sha256/512, sha2, sha3)	SPHINCS+ – 64–128 Picnic – 33–65	SPHINCS+ – 7856–49856 Picnic – 49–97	+	–
McElice Codes usage	Matrix multiplication, decoding	McElice – 261120–1357824	McElice – 6452–14080	+	+
SIKE, SIDH (supersingular) isogeny walk problem	Operations with elliptic curves	SIDH – 134–564 SIKE – 197–564	SIDH – 28–48 SIKE – 350–644	–	+
Based on isomorphic transformations in the elliptic curves group of points [7]	Operations with elliptic curves	Dual_EC_DRBG – 256–521	Dual_EC_DRBG – 256–521	+	–

3. SIDH analysis.

One of the current areas of research is the development of new cryptographic algorithms using existing platforms and libraries of software functions that will meet the growing requirements for cryptographic stability of algorithms in the face of the increasing power of quantum computers. Algorithms based on the isogeny of the elliptic curve are a promising direction for the development of postquantum cryptosystems. So, let`s take a closer look at operations, used in SIDH algorithm.

Let the elliptic curve be given by the Weierstrass equation:

$$y^2 = x^3 + Ax + B \; mod \; p, \tag{7}$$

where $A = 1, B = 1, p = 19$ The order of the curve is equal to $\#E_p = 21$. The points of this curve are shown in Table 5.

Table 5

P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11
(0,1)	(0,18)	(2,7)	(2,12)	(5,6)	(5,13)	(7,3)	(7,16)	(9,6)	(9,13)	(10,2)
P12	P13	P14	P15	P16	P17	P18	P19	P20	P21	-
(10,17)	(13,8)	(13,11)	(14,2)	(14,17)	(15,3)	(15,16)	(16,3)	(16,16)	*O*	-

Curve (7) has 2 subgroups with orders 3 and 7. For example, for a group of order 3, these are the points: (2,7), (2,12), O.

Definition 1. Group [11].

The set G with the binary operation “*” defined on it is called a group if:

1) operation “*” is associative, that means that for any $a,\ b,\ c \in G,\ \ a * a * (b * c) = (a * b) * c\ \ c;$

2) there is a neutral (single) element $e \in G$, that $e * a = a * e = a$ for all $a \in G$;

3) for every element $a \in G$ exists opposite element a^{-1} : $a * a^{-1} = a^{-1} * a = e$.

Definition 2. Subgroup [11].

A subgroup H of a group G is a subset of H, which is also a group concerning the same group operation defined in group G.

Definition 3. Lagrange's theorem [11].

Let G be a finite group. Then,

$$|G| = (G{:}\,H) \times |H|. \tag{8}$$

Definition 4. Bijection.

A bijection is a mapping in which each element of one set corresponds to exactly one element of another set, with an inverse mapping having the same property defined.

Definition 5. Isomorphism, homomorphism, automorphism.

The mapping $f{:}\,H \rightarrow G$ is called:

– homomorphism, if for any

$$h_1, h_2 \in H{:}\, f(h_1 \cdot h_2) = f(h_1) \times f(h_2); \tag{9}$$

– isomorphism, if f is homomorphism and bijection;

– automorphism, if f is an isomorphism and $H = G$.

Definition 6. Isogeny [11].

The isogeny of the elliptic curve is a non-constant rational mapping of the curve E_1 over a finite field F into the curve E_2, which is also called a group homomorphism and is given as:

$$(x;\ y) \rightarrow (f1(x;\ y)/f2(x;\ y), g1(x;\ y)/g2(x;\ y)), \tag{10}$$

where *f1, f2, g1, g2* – are polynomials.

Example:

Let`s obtain the isogeny of the elliptic curve (7).

The isogeny of the curve can be obtained using the Vélu algorithm with the isogeny nucleus C: $\{O, (2,7), (2,12)\}$, where the nucleus of isogeny is a cyclic subgroup of simple order. We obtain the isogeny curve by the Vélu algorithm. Let us take curve (7).

Vélu algorithm for C: $\{\boldsymbol{O}, \mathbf{(2,7)}, \mathbf{(2,12)}\}$

1. Dropping a point at infinity.
2. Finding C_2 is a set of points of a pair order. R – the rest of the points. There are no points of a pair order in sub-group C.
3. Breaking R into two parts R_+ and R_-. For R_+we choose the point (2;7). Point (2;12) is opposite, because $7 = -12 \bmod 19$
4. Set S = {(2,7)} Cycle consist of one step because the S set includes one point.

$$Q = (2,7), \text{ coordinates are } x_Q = 2, y_Q = 7.$$

$$g_Q^x = 3 * 2^2 + 1 = 13$$

$$g_Q^y = -2 * 7 = 5$$

$$v_Q = 2 * 13 = 7$$

$$u_Q = 5^2 = 6$$

$$v = 7$$

$$w = 6 + 2 * 7 = 1$$

$$A' = 1 - 5 * 7 = 4$$

$$B' = 1 - 7 * 1 = 13$$

We calculate rational reflection $(s, y) \to (\alpha, \beta)$, using the nucleus $(x, y) \to (\alpha, \beta)$ of the curve (7).

$$\alpha = x + \sum\nolimits_{Q \in S} \left(\frac{v_Q}{(x - x_Q)} + \frac{u_Q}{(x - x_Q)^2} \right)$$

$$\alpha = x + \frac{7}{x - 2} + \frac{6}{(x - 2)^2} = \frac{x^3 - 4x^2 + 11x - 8}{x^2 - 4x + 4}$$

$$\beta = y - \sum\nolimits_{Q \in S} \left(u_Q \frac{2y}{(x - x_Q)^3} + v_Q \frac{y - y_Q}{(x - x_Q)^2} - \frac{g_Q^x g_Q^y}{(x - x_Q)^2} \right)$$

$$\beta = \frac{x^3 y - 6x^2 y + 5xy - 6y}{x^3 - 6x^2 + 12x - 8}$$

Reflection $\varphi: (x, y) \to (\alpha, \beta\ )$

We calculate rational reflection$(s, y) \to (\alpha, \beta)$, using the nucleus $(x, y) \to (\alpha, \beta)$ of curve $E_1: y^2 = x^3 + x + 1\ mod\ 19$ on curve $E_2: y^2 = x^3 + 4x + 13\ mod\ 19$.

Table 6

№	*Point coordinates of* E_1curve	*Point coordinates of* E_2curve
1.	(0,1)	(17, 15)
2.	(7,16)	
3.	(14,17)	
4.	(0,18)	(17, 4)
5.	(7,3)	
6.	(14,2)	
7.	(5,6)	(8, 5)
8.	(10,2)	
9.	(16,16)	
10.	(5,13)	(8, 14)
11.	(10,17)	
12.	(16,3)	
13.	(9,6)	(14, 1)
14.	(13,11)	
15.	(15,3)	
16.	(9,13)	(14, 18)
17.	(13,8)	
18.	(15,16)	
19.	(2,7)	*O*
20.	(2,12)	
21.	*O*	

Vélu algorithm for C: $\{\boldsymbol{O}, \mathbf{(10,2)}, \mathbf{(10,17)}, \mathbf{(14,2)}, \mathbf{(14,7)}, \mathbf{(15,3)}, \mathbf{(15,16)}\}$

1. Dropping a point at infinity.

2. Finding C_2 is a set of points of a pair order. R – the rest of the points. There are no points of a pair order in sub-group C.

3. Breaking R into two parts R_+ and R_-. For R_+we choose points (10, 2), (14, 2), (15, 3). Points (10, 17), (14, 17), (15, 16) are opposite, because $2 = -17$ mod 19 and $3 = -16$ mod 19

4. Set $S = \{(10,2),(14,2),(15,3)\}$
The cycle consists of three steps because the S set includes three points.

First step:

$$Q = (10,2), \text{ coordinates are } x_Q = 10, y_Q = 2.$$
$$g_Q^x = 3 * 10^2 + 1 = 16$$
$$g_Q^y = -2 * 2 = 15$$
$$v_Q = 2 * 16 = 13$$
$$u_Q = 15^2 = 16$$

Second step:

$$Q = (14,2), \text{ coordinates are } x_Q = 14, y_Q = 2.$$
$$g_Q^x = 3 * 14^2 + 1 = 0$$
$$g_Q^y = -2 * 2 = 15$$
$$v_Q = 2 * 0 = 0$$
$$u_Q = 15^2 = 16$$

Third step:

$$Q = (15,3), \text{ coordinates are } x_Q = 15, y_Q = 3.$$
$$g_Q^x = 3 * 15^2 + 1 = 11$$
$$g_Q^y = -2 * 3 = 13$$
$$v_Q = 2 * 11 = 3$$
$$u_Q = 13^2 = 17$$
$$v = 13 + 0 + 3 = 16$$
$$w = (16 + 10 * 13) + (16 + 14 * 0) + (17 + 15 * 3) = 15$$
$$A' = 1 - 5 * 16 = 16$$
$$B' = 1 - 7 * 15 = 10$$

We calculate rational reflection$(s, y) \to (\alpha, \beta)$:

$$\alpha = x + \sum_{Q \in S} \left(\frac{v_Q}{(x - x_Q)} + \frac{u_Q}{(x - x_Q)^2} \right),$$

$$\alpha = x + \left(\frac{13*(x-10)+16}{(x-10)^2} + \frac{0*(x-14)+16}{(x-14)^2} + \frac{3*(x-15)+17}{(x-15)^2} \right),$$

$$\beta = y - \sum_{Q \in S} \left(u_Q \frac{2y}{(x - x_Q)^3} + v_Q \frac{y - y_Q}{(x - x_Q)^2} - \frac{g_Q^x g_Q^y}{(x - x_Q)^2} \right),$$

$$\beta = y - \left(\begin{array}{c} \frac{13y+(13y-7)(x-10)-12(x-10)}{x^3-11x^2+15x-12} + \frac{13y}{x^3-4x^2+18x-8} + \\ + \frac{15y+(3y-9)(x-15)-10(x-15)}{x^3-7x^2+10x-12} \end{array} \right),$$

Reflection $\varphi: (x, y) \to (\alpha, \beta\ )$

Table 7

Point of E_2	**(12, 7)**						
Point of E_1	(0,1)	(2,7)	(5,13)	(7,3)	(9,13)	(16,16)	(13,11)
Point of E_2	**(12, 12)**						
Point of E_1	(0,18)	(2,12)	(5,6)	(7,16)	(9,6)	(16,3)	(13,8)
Point of E_2	**O**						
Point of E_1	(10,2)	(10,17)	(14,2)	(14,17)	(15,3)	(15,16)	O

The general idea of the protocol is that with the help of publicly available parameters Alice and Bob perform separate calculations of isogenies of degree l_A^a and l_B^b, respectively, calculating the isogeny of large order over the secret nucleus (Fig. 4).

Public SIDH parameters include:

- A prime number p of the form $l_A^a l_B^b \cdot f \pm 1$, where l_A^a and l_B^b are small prime numbers, a and b are natural integers, and f is a cofactor.
- Supersingular elliptic curve, $E_0(F_{p^2})$.
- Points $\{P_A, Q_A\}$ generated from $E_0[l_A^a]$ over $\mathbb{Z}/l_A^a\mathbb{Z}$ and points $\{P_B, Q_B\}$ generated from $E_0[l_B^b]$ over $\mathbb{Z}/l_B^b\mathbb{Z}$.

The protocol consists of two rounds which can be divided into the following steps:

Calculating the secret nucleus $R = \langle [m]P + [n]Q \rangle$ for base points $\{P, Q\}$, where m and n are private keys.

Calculation of isogeny over the secret nucleus, $\varphi: E \to E/\langle R \rangle$, using the Vélu algorithm for the supersingular curve E.

Calculate the mappings of the base points of the base of the other side, $\{\varphi(P_{opp}), \varphi(Q_{opp})\}$, for the first round.

Thus, for the first round, Alice and Bob calculate the isogeny $\varphi_A: E_0 \to E_A = E_0/\langle [m_A]P + [nA]Q$. They apply isogeny to the base points of the other side. After the first round, Alice sends Bob $(E_A, \{\varphi_A(P_B), \varphi_A(Q_B)\})$. Bob sends Alice $(E_B, \{\varphi_B(P_A), \varphi_B(Q_A)\})$ through the unprotected channel. The second round consists of a similar calculation of isogeny, but with the public keys, they exchanged. Alice calculates $\varphi'_A: E_B \to E_{AB} = E_B/\langle [m_A]\varphi_B(P_A) + [n_A]\varphi_B(Q_A) \rangle$, Bob calculates $\varphi'_B: E_A \to E_{BA} = E_A/\langle [m_B]\varphi_A(P_B) + [n_B]\varphi_A(Q_B) \rangle$ To obtain a general secret, Alice calculates the j-invariant of E_{AB}, and Bob of E_{BA}.

The safety assumption is based on the difficulty of calculating isogeny between supersingular elliptic curves for which there is no subexponential algorithm known for quantum computers. Alice generates private keys $m_A, n_A \in \mathbb{Z}/l_A^a\mathbb{Z}$, which are not divisible by l_A^a. Bob also generates private keys $m_B, n_B \in \mathbb{Z}/l_B^b\mathbb{Z}$, which are not divisible by l_B^b .

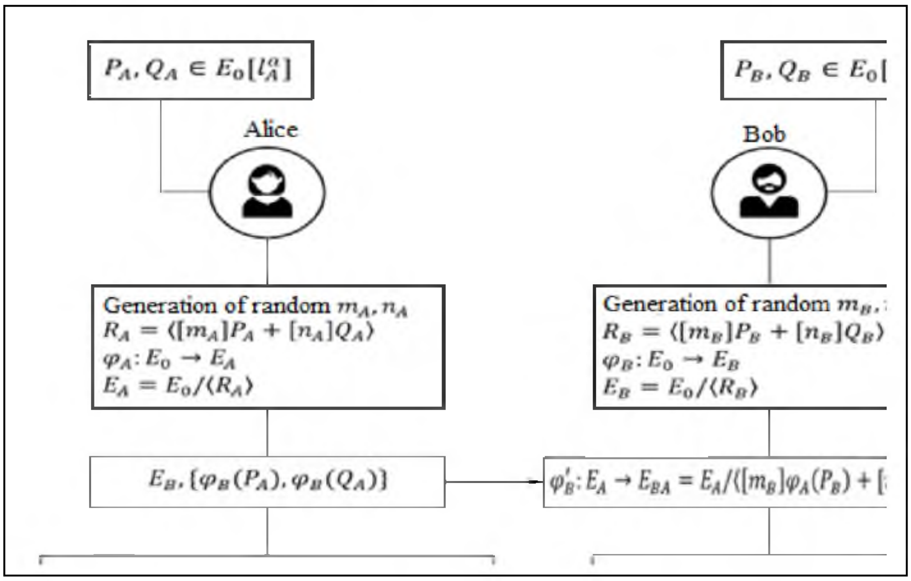
$P_A, Q_A \in E_0[l_A^a]$
Alice
$P_B, Q_B \in E_0[$
Bob
Generation of random m_A, n_A
$R_A = \langle [m_A]P_A + [n_A]Q_A \rangle$
$\varphi_A: E_0 \to E_A$
$E_A = E_0/\langle R_A \rangle$
Generation of random $m_B,$
$R_B = \langle [m_B]P_B + [n_B]Q_B \rangle$
$\varphi_B: E_0 \to E_B$
$E_B = E_0/\langle R_B \rangle$
$E_B, \{\varphi_B(P_A), \varphi_B(Q_A)\}$
$\varphi'_B: E_A \to E_{BA} = E_A/\langle [m_B]\varphi_A(P_B) + [$

Fig. 3. SIDH algorithm scheme

Research on the security level, done with algorithms based on elliptic curves isogenies in [9] shows that for classical cryptanalysis needed time is equal to $3{,}4 \times 10^{38}$ with classical memory $1{,}8 \times 10^{19}$, and that a quantum key recovery on AES-128 costs $1{,}2 \times 10^{24}$ gates (which allows for

$1{,}1 \times 10^{12}$ queries and $1{,}2 \times 10^{24}$ quantum time), and neglect polynomial factors. Then this would require $p \sim 5280$ bits, that is, multiplying by 10 the parameter size.

4. Conclusion.

This paper provides an assessment of the security level of the existing standardized cryptosystems, the main cryptographic assumption of which is based on the complexity of integer factorization and solving the problem of discrete logarithms and promising crypto-algorithms potentially resistant to quantum cryptanalysis. The security level of existing asymmetric cryptosystems to quantum cryptanalysis is polynomial, and system-wide parameters size increasing will not significantly increase the security level. The current limitation for quantum cryptanalysis is the required number of qubits.

The length of the system-wide parameters of a cryptosystem based on elliptic curves can be increased to 2048 bits, in this case, a quantum computer must have 14390 qubits to crack such a cryptosystem. It gives some time for the transition to post-quantum cryptography. It should also be noted that such cryptosystems as the SIKE, SIDH algorithms have a margin of crypto resistance to quantum cryptanalysis and the possibility of building a post-quantum algorithm of electronic digital signature and key encapsulation on their basis.

The work also presented potential candidates for the post-quantum cryptography standard, their differences, and the possibilities of their application

REFERENCES

1. Shor P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer / P. W. Shor // S IAM J. Comput. 1997. 26 (5). P. 1484–1509.

2. Grover L. K. A fast quantum mechanical algorithm for database search / L. K. Grover // Proceeding of the 28th ACM Symposium on Theory of Computation, New York: ACM Press. 1996. P. 212–219.

3. Lily Chen. Report on Post-Quantum Cryptography / Lily Chen, Stephen Jordan, Yi-Kai Liu, Dustin Moody, Rene Peralta, Ray Perlner, Daniel Smith-Tone // NISTIR 8105. 2016. P. 2.

4. Shor, P. W. Algorithms for quantum computation: Discrete logarithms and factoring / Shor, P. W. // In: Proceedings 35th Annual Symposium on Foundations of Computer Science. 1994. P. 124–134.

5. Горбенко Ю. І. Аналіз можливостей квантових комп'ютерів та квантових обчислень для криптоаналізу сучасних криптосистем / Ю. І. Горбенко, Р. С. Ганзя // Восточно-Европейский журнал передовых технологий. Харків, 2014. Том 6, № 1 (67). С. 8–15.

6. Kerry Maletsky. RSA vs. ECC Comparison foe Embedded systems / Kerry Maletsky // Microchip. 2020.

7. Чевардін В. Е. Метод генерации псевдослучайных последовательностей на основе изоморфных трансформаций эллиптической кривой / В. Е. Чевардін, А. В. Бессалов // Прикладна радіоелектроніка. 2012. Том 11. № 2. С. 234–237.

8. liboqs. Open-source C library for quantum-safe cryptographic algorithms. URL: https://github.com/open-quantum-safe/liboqs.

9. Xavier Bonnetain. Quantum Security Analysis of CSIDH / Xavier Bonnetain, Andre Schrottenloher // Advances in Cryptology – EUROCRYPT 2020. Pp. 493–522.

10. NIST SP 800-57 § 5.6.1. P. 62–64. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-57p1r3.pdf.

11. Applied algebra. Part 1. Basics of abstract algebra: tutorial / L. V. Kovalchuk, Y. Y. Yaremchuk. Vinnytsya: VNTU, 2015. 99 p.