КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE

№ 1 (17), 2022

ISSN 2663 - 4023

DOI 10.28925/2663-4023.2022.17.128144
UDC 621.391.15 : 519.7

Anatoliy V.Bessalov
Doctor of Technical Sciences, Professor
Professor of the Department of Information and cyber security Professor of
Borys Grinchenko Kyiv University
ORCID ID: 0000-0002-6967-5001
a.bessalov@kubg.edu.ua

Ludmila V. Kovalchuk
Doctor of Technical Sciences, Professor
Professor of National Technical University of Ukraine "Kyiv Polytechnical University named by Igor Sikorskiy"
ORCID ID: 0000-0003-2874-7950
l.kovalchuk@kpi.ua

Sergey V. Abramov
post-graduate student of Borys Grinchenko Kyiv University, Ukraine
ORCID ID 0000-0002-5145-2782
s.abramov.asp@kubg.edu.ua

RANDOMIZATION OF CSIDH ALGORITHM ON QUADRATIC AND TWISTED EDWARDS CURVES

Abstract. The properties of quadratic and twisted supersingular Edwards curves that form pairs of quadratic twist with order $p+1 \equiv 0 nod 8$ over a prime field F_p are considered. A modification of the CSIDH algorithm based on odd degree isogenies of these curves is considered. A simple model for the implementation of the CSIDH algorithm in 3 minimal odd isogeny degrees 3, 5, 7, with the prime field modulus $p = 839$ and the order $N_E = 840$ of supersingular curves is constructed. At the precipitation stage, the parameters of isogenic chains of all degrees for these two classes of supersingular Edwards curves are calculated and tabulated. An example of the implementation of the CSIDH algorithm as a non-interactive secret sharing scheme based on the secret and public keys of Alice and Bob is given. A new randomized CSIDH algorithm with a random equiprobable choice of one of the curves of these two classes at each step of the isogeny chain is proposed. The choice of the degree of each isogeny is randomized. The operation of the randomized algorithm by an example is illustrated. This algorithm as a possible alternative to "CSIDH with constant time" is considered. A combination of the two approaches is possible to counter side channel attacks. Estimates of the probability of a successful side-channel attack in a randomized algorithm are given. It is noted that all calculations in the CSIDH algorithm necessary to calculate the shared secret d_{AB} are reduced only to calculating the parameter d' of the isogenic curve E' and are performed by field and group operations, in particular, scalar point multiplications and doubling points of the isogeny kernel. In the new algorithm we propose to abandon the calculation of the isogenic function $\phi(R)$ of random point R, which significantly speeds up the algorithm.

Keywords: curve in generalized Edwards form, complete Edwards curve, twisted Edwards curve, quadratic Edwards curve, curve order, point order, isomorphism, isogeny, randomization, w-coordinates, square, non-square.

INTRODUCTION

In the development of the topic of the previous work [1], the present article presents new results in the problems of implementation of the CSIDH algorithm [2]. This post-quantum cryptography (PQC) algorithm differs from other known algorithms by a minimum key length close to the prime field F_p modulus over which group operations are performed. As the most efficient algorithm technology, we propose classes of quadratic and twisted supersingular Edwards curves (SEC) connected as quadratic twist pairs. Compared with the known implementations of CSIDH on complete Edwards curves [3], this technology doubles the space of the curves used and, moreover, does not require time-consuming inversion of the curve parameter d in the transition to quadratic twist.

A well-known problem with the CSIDH algorithm is the vulnerability to a side channel attack, which is based on measuring the time of calculation of the isogeny chain of each degree l_k, proportional to the secret exponent e_k of the key. In a large number of articles [15, 16, etc.], the solution to this problem is proposed by increasing the exponents e_k by fictitious to a known maximum (Constant time CSIDH). It is clear that such redundancy reduces the speed of the algorithm In this article, we propose and justify an alternative approach to counter this attack - randomization of the CSIDH algorithm. It leads to the inevitable increase in the probability of error of the analyst, the only one of which in a long path of measurements thwarts the attack.

The calculation of isogenies of odd degrees for complete and quadratic Edwards curves E_d is carried out according to the formulas defined by Theorems 2–4 of [6]. In our previous work [1], we generalized Theorems [6] to curves in the generalized Edwards form with two parameters a and d, which allowed us to apply quadratic and twisted Edwards curves over the field F_p in this paper to implement the CSIDH model.

Our analysis in this paper is based on the properties of quadratic and twisted Edwards curves connected as quadratic twist pairs [12, 13]. Supersingular curves of these classes with the same order $N_E = p+1 = p+1 = 2^m n, m \geq 3,$ (n - odd) exist only at $p \equiv 3 \bmod 4$. The minimum even cofactor of the order of such curves is 8, then for the CSIDH algorithm with odd $n = \prod_{i=1}^{K} l_i$. field modulus should be selected as $p = 8n - 1.$ In order to adapt the definitions for arithmetic isogeny of Edwards curves and Weierstrass curves, we use a modified law of points addition [10, 11].

Section 1 gives a brief overview of the properties of twisted and quadratic supersingular Edwards curves (SECs) [12,13,14]. In Section 2, specific aspects of the implementation of the CSIDH algorithm model on quadratic and twisted SECs are considered, a modification of the algorithm [2] is given, the parameters of the isogenic curves of the model are calculated and tabulated, an example of Alice and Bob's calculations in the Diffie-Hellman secret sharing scheme is given. In Section 3, the rationale for the randomization of the CSIDH algorithm with a statistical estimate of the probability of a successful side channel attack is given, a new randomized CSIDH algorithm is presented, which also suggests abandoning the calculation of the isogenic function $\phi(R)$ of a random point R of the curve in the CSIDH algorithm.

PROPERTIES OF QUADRATIC AND TWISTED SUPERSINGULAR EDWARDS CURVES

Let us consider some specific properties of supersingular Edwards curves (SECs) [12, 13]. We define an elliptic curve in the *generalized Edwards form* [9, 10] by the equation

$$E_{a,d}: \quad x^2 + ay^2 = 1 + dx^2y^2, \quad a, d \in F_p^*, a \neq d, \ d \neq 1. \tag{1}$$

If a quadratic character $\chi(ad) = -1$, curve (1) is isomorphic to the *complete Edwards curve* [8, 9] with one parameter $\chi(ad) = -1$

$$E_d: \quad x^2 + y^2 = 1 + dx^2y^2, \quad \chi(d) = -1. \qquad (2)$$

SECs of this class exist for $p \equiv 3 \bmod 4$, and their order is $N_E = p + 1 \equiv 0 \bmod 4$.
Let $\chi(ad) = 1, \chi(a) = \chi(d) = 1$, then the curve (1) is isomorphic to the *quadratic Edwards curve* [10]

$$E_d: \quad x^2 + y^2 = 1 + dx^2y^2, \quad \chi(d) = 1,, \ d \neq 1, \qquad (3)$$

In contrast to (2), the parameter d of curve (3) is a square. SEC of class (3) have an order $N_E = p + 1 \equiv 0 \bmod 8$ and exist over a field F_p for $p \equiv 7 \bmod 8$. For both curves (2) and (3) we accept a parameter $a = 1$, and they are called as curves with one parameter. In [9], curve (3) together with curve (2) are defined as *Edwards curves*. At the same time, the difference in the quadratic characters of the parameters d leads to radically different properties of curves (2) and (3) [10, 11].

The *twisted Edwards curve* [9] was defined in [10] as a particular case of curve (1) for $\chi(ad) = 1, \chi(a) = \chi(d) = -1.$ So, complete, quadratic and twisted Edwards curves [10] form 3 non-intersecting classes of curves (1), which allows us to avoid confusion in the definitions adopted in [9].

In the application to the CSIDH algorithm on SECs, we define a pair of quadratic and twisted SECs [10] as a pair of quadratic twist with parameters $\chi(ad) = 1, \bar{a} = ca, \bar{d} = cd, \chi(c) = -1,$ where $a, d -$ are the parameters of a quadratic curve, and respectively, $\bar{a}, \bar{d}$ $-$of a twisted curve. Since SECs exist only for $p \equiv 3 \bmod 4$ [12], we can take $c = -1, a = 1, \bar{a} = -1, \bar{d} = -d$. In other words, the transition from a quadratic to a twisted curve and vice versa we can define $E_d = E_{1,d} \leftrightarrow E_{-1,-d}$. Then the twisted SEC equation for $p \equiv 7 \bmod 8$ from (1) we can written as

$$E_{-1,-d}: \quad x^2 - y^2 = 1 - dx^2y^2, \quad d \in F_p^*, \quad d \neq 1., \chi(d) = 1. \qquad (4)$$

Here, the conditions for the modulus p and order of the curve $N_E = p + 1 \equiv 0 \bmod 8$ are similar to curves (3). For $p \equiv 7 \bmod 8$, of course, also $p \equiv 3 \bmod 4$ holds.

Having fixed the parameter $a = -1$ and running through all admissible values of d , we can determine the set of cardinalities of all $\frac{p-3}{2}$ curves of each of the 3 classes of curves (1) (including isomorphic curves). Any twisted SEC one can reduce to the form (4).

The order $N_E = p + 1 - t$ of an elliptic curve over a prime field F_p is determined based on the trace t of the characteristic equation $\pi^2 + t\pi + p = 0$ of the Frobenius endomorphism, where for some point $P = (x.y)$ the Frobenius endomorphism $\pi(P) = (x^p, y^p)$. For the curve of quadratic twist, the corresponding order will be $N_E{}^t = p + 1 + t$. An elliptic curve is supersingular if and only if, over any extension of a prime field F_p, the trace of the Frobenius equation is $t \equiv 0 \bmod p,$ in this case $\pi^2 = -p,\ \pi = \pm\sqrt{-p}$ in an imaginary quadratic field [13, 15]. A pair of curves E and E^t is sometimes referred to $E[\pi+1],\ E[\pi-1]$ as two solutions of the quadratic Frobenius equation. In an algebraic closure $\overline{F}_p$, a supersingular curve does not contain points of order p. Over a prime field F_p, such a curve always has order $N_E = p+1$.

So, quadratic and twisted SEC as a pair of quadratic twist have the same order $N_E = p+1$ but different structure. All their points are different (except two points $(0,\pm1)$), so isogenies of the same degree have different kernels. Both curves are non-cyclic with respect to points of the 2-nd order (contain 3 points of the 2-nd order each, two of which are exceptional points $D_{1,2} = \left(\pm\sqrt{\frac{a}{d}}, \infty\right)$ [9, 10]). Quadratic SECs (3), in addition, contains two exceptional points of the 4-th order $\pm F_1 = \left(\infty, \pm\frac{1}{\sqrt{d}}\right)$. The presence of a noncyclic subgroup of the 4-th order containing 3 points of the 2-nd order limits the number 8 to the minimum even cofactor of the order $N_E = 8n\ (n - odd)$ of quadratic and twisted Edwards curves [10]. In general, their order is $N_E = 2^m n,\ m \ge 3$. The maximum order of points of these curves is $N_E/2 = 4n.$ It is important that points of even orders are not involved in the calculations of the CSIDH algorithm (after the first multiplication of a random point P of maximum order by 4, we have a point of odd order n).

For the curve (1) J -invariant equal [9, 14]

$$J(a,d) = \frac{16(a^2 + d^2 + 14ad)^3}{ad(a-d)^4}, \quad ad(a-d) \neq 0\ . \tag{5}$$

This parameter distinguishes isogenic (with different J-invariants) and isomorphic (with equal J-invariants) curves. Since the J-invariant retains its value for all isomorphic curves and quadratic twist pairs [15], it is the same for a pair of twisted and quadratic SECs ($a = \pm 1$). It is a useful tool both in finding supersingular curves and in constructing isogeny chain graphs. One of the properties of the J-invariant is

$$J(d) = J(d^{-1}).$$

For the considered classes of SECs, the replacement $d \to d^{-1}$ gives an isomorphism, and for complete Edwards curves (2) it gives a quadratic twist.

CSIDH ALGORITHM ON QUADRATIC AND TWISTED EDWARDS CURVES

The PQC CSIDH (Commutative SIDH) algorithm proposed by the authors of [2] for solving the same key exchange problem (SIDH), but based on isogenic mappings of supersingular elliptic curves as additive Abelian groups. Such a mapping over a prime field F_p as the class group action is defined [2] and is commutative. In comparison with the well-known original CRS scheme (Couveignes (1997), Rostovtsev, Stolbunov (2004)) on non-supersingular curves, the use of isogenies of supersingular curves made it possible to substantial speed up the algorithm and achieve the smallest known key size (512 bits in [2]).

Let the curve E of order $N_E = p+1$ contain points of small odd orders $l_k, k = 1,2,...,K.$ Then there is an isogenic curve E' of the same order as a l_k -degree map: $E \to E' = [l_k]*E$. The repetition of this operation e_k times we denote $[l_k^{e_k}]*E$. The values of the isogeny exponents $e_k \in Z$ determine the length $|e_k|$ of the chain of isogenies of degree l_k . In [2], an interval of exponential values $[-m \le e_i \le m]$ is accepted $m = 5$, which provides a security level of 128 bits for a quantum computer attack. Negative values of the exponent mean a transition to a quadratic twist supersingular curve.

The implementation of the CSIDH algorithm mainly uses fast arithmetic of Montgomery elliptic curves $y^2 = x^3 + Cx^2 + x,\ C \ne \pm 2$ containing 2 points of the 4-th order and, accordingly, having an order $N_E = p+1 = 4n(n - odd)$ [8]. In [3], the CSIDH algorithm implemented on complete SECs of the same order. In this paper, we use quadratic and twisted SECs in the CSIDH algorithm, which have the same speed performance as complete Edwards curves [8, 9]. In [1] we proved 2 theorems for implementation such possibility. With a minimum cofactor of 8, the order of twisted and quadratic SECs is $N_E = 8n$. Thus, for these SECs classes with order $N_E = 8n = p+1,\quad n = \prod_{k=1}^{K} l_k$. the field modulus in the CSIDH algorithm we chosen as $p = 8\prod_{i=1}^{K} l_i - 1 \equiv -1 \bmod 8$.

Non-interactive Diffie-Hellman key exchange includes the following steps [2]:

1. **Choice of parameters.** For small odd primes l_i , compute $n = \prod_{k=1}^{K} l_k$. , where the value K is determined by the security level (in [2] $K = 74, l_{74} = 587$), and choose an appropriate field modulus $p = 2^m \prod_{k=1}^{K} l_k - 1, m \ge 3$ and a starting elliptic curve E_0 .

2. Calculation of public keys. Alice uses her private key $\Omega_A = (e_1, e_2,.., e_K)$ to build an isogenic mapping $\Theta_A = [l_1^{e_1}, l_2^{e_2},.., l_K^{e_K}]$ (class group action [2]) and calculates the isogenic curve $E_A = \Theta_A * E_0$ as her public key. Based on the secret key Ω_B and function Θ_B , Bob performs the same calculations and obtain his public key $E_B = \Theta_B * E_0$. These curves are defined their parameters d_A, d_B up to isomorphism, which are accepted as public keys known to both parties.

3. Sharing secrets. Here the protocol is similar to item 2 with replacements $E_0 \to E_B$ for Alice and $E_0 \to E_A$ for Bob. Knowing Bob's public key, Alice calculates $E_{BA} = \Theta_A * E_B = \Theta_A \Theta_B * E_0$. Similar actions of Bob give a result $E_{AB} = \Theta_B * E_A = \Theta_B \Theta_A * E_0$ that coincides with the first one due to the commutatively of the group operation. The J -invariant of the curve $E_{AB}(E_{BA})$ is accepted the shared secret.

Below we present a modification of Alice's computational algorithm according to item 2 [2] using isogenies of quadratic and twisted SEC.

Algorithm 1: Evaluating the class-group action on twisted and quadratic SEC.

Input: $d_A \in E_A, \chi(d) = 1$ *and a list of integers* $\Omega_A = (e_1, e_2, ...e_K)$.

Output: d_B *such that* $[l_1^{e_1}, l_2^{e_2}, ...l_K^{e_K}]*E_A = E_B$, *where* $E_{A,B}:\quad x^2 + y^2 = 1 + d_{A,B} x^2 y^2$,

```
1. While some $e_k \ne 0$ do
```

```
    2. Sample a random $x \in F_p$,
    3. Set $a \leftarrow 1$,   $E_A : x^2 + y^2 = 1 + d_A x^2 y^2$ if $(x^2 - 1)(dy^2 - 1)$ is a square in $F_p$,
    4. else $a \leftarrow -1$,   $E_A : x^2 - y^2 = 1 - d_A x^2 y^2$,
    5. Let $S = \{k \mid ae_k > 0\}$ . If $S = \emptyset$ then start over to line 2 while $a \leftarrow -a$,
    6. Let $n = \prod_{k \in S} l_k$,  and compute $R \leftarrow [(p+1)/2n]P$,  $P \leftarrow P(x, y)$,
    7. For each $k \in S$ do
        8. Compute $Q \leftarrow [n/l_k]R$
        9. If $Q \neq (1,0)$ Compute an isogeny $\phi : E_A \to E_B$ with $\ker\phi = Q$,
        10. Set $d_A \leftarrow d_B$, $R \leftarrow \phi(R)$, $e_k \leftarrow e_k - a$ ,
        11. Skip $k$ in $S$ and $n \leftarrow n/l_k$ if $e_k = 0$,
12. Return $d_A$ .
```

In comparison with Algorithm 2 in [2], our Algorithm 1, adapted to twisted and quadratic SEC, has some modifications:

1. Checking the square in line 3 use the equation of the quadratic Edwards curve (3).
2. With the order of the twisted Edwards curve $N_E = 8n = p + 1$ with the maximum order $N_E / 2 = 4n$ of the point, to obtain a point of the order n, it is sufficient to double the random point twice. In line 6, this property lied's to reducing one doubling in the scalar product of the point P .
3. Libe 10 has been corrected (you cannot reset the index k before zeroing e_k in line 10).
4. Updating the number $n \leftarrow n/l_k$ and reset k in line11 we perform after zeroing e_k .

According to line 10, exactly $|e_k|$ isogenies we calculate for each l_k until the exponent e_k is set to zero. Depending on its sign, isogenies are calculated in the class of quadratic ($e_k > 0$) or twisted SEC $(e_k < 0)$.

The construction of isogenies of odd prime degrees for quadratic Edwards curves based on Theorem 2 [6], and for twisted Edwards curves - Theorem 1 [1]. In the last work, for the first time, mapping $\phi(P)$ formulas for the curve (1) are given, depending on two parameters a and d . We formulate it below.

Theorem 1[1]. Let $G = \{(1,0), \pm Q_1, \pm Q_2, ..., \pm Q_s\}$ – subgroup of odd order $l = 2s + 1$ of points $\pm Q_i = (\alpha_i, \pm\beta_i)$, of curve $E_{a,d}$ (1) over field F_p .

Define

$$\phi(P) = (x', y') = \left(\prod_{Q \in G} \frac{x_{P+Q}}{x_Q} \frac{x_{P-Q}}{x_{Q,}}, \prod_{Q \in G} \frac{y_{P+Q}}{x_Q} \frac{y_{P-Q}}{x_{-Q,}} \right).$$

Then $\phi(x, y)$ is l -isogeny with kernel G from the curve $E_{a,d}$ to the curve $E_{a',d''}$ with parameters

$$a' = a^l,\ d' = d^l A^8,\ A = \prod_{i=1}^{s} \alpha_i, \tag{6}$$

and the mapping function

$$\phi(x, y) = \left(\frac{x}{A^2} \prod_{ii=1}^{s} \frac{(\alpha_i x)^2 - (a\beta_i y)^2}{1 - (d\alpha_i \beta_i xy)^2}, \frac{y}{A^2} \prod_{i=1}^{s} \frac{(\alpha_i y)^2 - (\beta_i x)^2}{1 - (d\alpha_i \beta_i xy)^2} \right), \tag{7}$$

or

$$\phi(x,y)=\left(\frac{x}{A^2}\prod_{ii=1}^{s}\frac{x^2-a\beta_i^{\ 2}}{1-d\beta_i^{\ 2}x^2},\frac{-y}{A^2}\prod_{i=1}^{s}\frac{x^2-\alpha_i^{\ 2}}{a-d\alpha_i^{\ 2}x^2}\right). \tag{8}$$

The proof of theorem in [1] is given.

Here, functions (7) and (8) include parameters a,d, which makes it possible to construct isogenies of twisted Edwards curves.

To illustrate the basic calculations of Algorithm 1, consider a simple model of the CSIDH algorithm on quadratic and twisted SECs that form quadratic twist pairs with the same order [9, 10]. Such curves exist only for $p\equiv -1 \bmod 8$ and have order $N_E=N_E^{\ t}=p+1=cn\ (n-odd),\ c\equiv 0 \bmod 8.$ Let such a pair of curves contain kernels of the 3-rd , 5-th and 7-th order at the smallest value $n=105$, then the minimum prime $p=839$ and the order of these curves $N_E=8n=840$. The parameter d of the entire family of 418 quadratic Edwards curves can be taken as squares $d=r^2 \bmod p,\ r=2..419.$. Of these, 66 pairs of quadratic and twisted SECs were found with parameters $a=\pm 1$ and $\chi(ad)=1$. The quadratic SEC (3) we denote by E_d, and the twisted SEC (4) as $E_{-1,-d}$. Table 1 shows the parameter d values for pairs of quadratic and twisted SEC. We written they as squares $d=r^2 \bmod p,,r=2..419.$ In this example, the relative share of SECs is about 16%. Note that for each curve in Table 1 there is at least one isomorphic curve with a parameter d^{-1} and the same J-invariant (5).

Table 1.

Parameter d values of quadratic and twisted SECs $(a=\pm 1)$ for $p=839$ and $N_E=840$.

144	**289**	**784**	**2**	**61**	**258**	**508**	**365**	**488**	**30**	**705**
742	**56**	**259**	**180**	**329**	**135**	**640**	**32**	**38**	**28**	**90**
564	**772**	**286**	**40**	**610**	**98**	**475**	**63**	**511**	**43**	**795**
414	**76**	**752**	**800**	**405**	**666**	**112**	**413**	**200**	**236**	**433**
15	**683**	**293**	**750**	**808**	**578**	**288**	**636**	**514**	**276**	**773**
243	**45**	**788**	**172**	**777**	**427**	**21**	**810**	**552**	**420**	**230**

For the first quadratic curve from Table 1, one can construct 3-, 5-, and 7-isogenies and find the parameters $d^{(i)}$ of the chain of isogenic curves $E_d^{(i)}, i = 0,1,2,...,T$ such that $d^{(T)} = d^{(0)}$. The period T of the chain of isogenies divides the number 66=2*3*11 of all SECs. Tables 2, 3, 4 show the results of calculating the parameters $d^{(i)}$ of chains of 3-isogeny, 5-isogeny, and 7-isogeny quadratic SECs, respectively. At each step $i = 0,1,2,...,T$ of the degree $l = 2s+1$ isogeny, the coordinates of the points $\alpha_1,..\alpha_s, s = (l-1)/2$ of the kernel G are calculated, after which the parameter $d^{(i+1)}$ of the isogenic curve $E_d^{(i+1)}$ is calculated using formula (6). In all tables, the numbers i are written in the first line, in the next s lines - the coordinates of the kernel points, then - the line with the parameters $d^{(i)}$. For 3-isogenies with a period, $T = 33$ for completeness, one more table similar to Table 2 is missing, with the second half of the parameters of Table 1. For 5- and 7-isogenies with period $T = 11$, Tables 3 and 4 contain only 1/3 of all isogenies. Next, we will show that the commutability of the function $\Theta_A = [l_1^{e_1}, l_2^{e_2}, .., l_K^{e_K}]$ makes it possible to obtain final results under conditions of incomplete data. The latter circumstance is due to the task of reducing the amount of tabulated data in the article.

For the same purpose, we do not present data for twisted SECs $E_{-1,-d}^{(i)}, i = 0,1,2,...,T-1$ isogenies. Instead, a simple property is used [7]: the sequences $d^{(i)}$ of parameters of isogenies $[l_k^{e_k}], e_k > 0$ and $[l_k^{e_k}], e_k < 0$ on the period $i = 0,1,2,...,T-1$ of isogenies have a reverse (counter) character. In other words, the sequence of parameters $d^{(0)}, d^{(1)}, .., d^{(T)}, d^{(0)} = d^{(T)}$ for the quadratic SEC ($e_k > 0$) is read in reverse order as $d^{(T)}, d^{(T-1)}, .., d^{(0)}, d^{(0)} = d^{(T)}$ for the twisted SEC ($e_k < 0$).

Table 2.

Parameter $d^{(i)}$ values of chain of 3-isogenic quadratic SECs ($a = 1$) for $p = 839$ (period $T = 33$)

i	0	1	2	3	4	5	6	7	8	9	10
$\alpha^{(i)}$	518	558	768	178	502	44	372	136	258	75	487
$d^{(i)}$	**144**	**414**	**405**	**2**	**28**	**259**	**752**	**773**	**15**	**243**	**21**
i	11	12	13	14	15	16	17	18	19	20	21
$\alpha^{(i)}$	697	481	333	248	613	378	663	404	20	377	99
$d^{(i)}$	**433**	**180**	**514**	**578**	**293**	**666**	**38**	**112**	**172**	**683**	**258**
i	22	23	24	25	26	27	28	29	30	31	32
$\alpha^{(i)}$	718	379	327	139	781	41	601	344	561	230	477
$d^{(i)}$	**772**	**488**	**636**	**286**	**508**	**76**	**236**	**43**	**788**	**61**	**289**

Table 3.

Parameter $d^{(i)}$ values of two chains of 5-isogenic quadratic SECs ($a = 1$) for $p = 839$ (period $T = 11$)

i	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
$\alpha_1^{(i)}$	78	343	152	337	318	344	588	222	151	352	390
$\alpha_2^{(i)}$	537	655	632	720	545	837	790	832	748	372	790
$d^{(i)}$	**144**	**76**	**258**	**293**	**243**	**2**	**788**	**636**	**112**	**180**	**752**
$\alpha_1^{(i)}$	327	390	91	125	653	17	251	744	409	586	103
$\alpha_2^{(i)}$	726	552	609	583	655	682	393	764	577	692	531
$d^{(i)}$	**289**	**508**	**683**	**578**	**15**	**405**	**43**	**488**	**38**	**433**	**259**

Table 4.

Parameter $d^{(i)}$ values of two chains of 7-isogenic quadratic SECs ($a = 1$) for $p = 839$ (period $T = 11$)

i	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
$\alpha_1^{(i)}$	9	485	99	161	255	103	367	73	41	422	362
$\alpha_2^{(i)}$	718	700	319	248	705	131	828	258	731	582	820
$\alpha_3^{(i)}$	17	826	678	465	322	324	700	99	229	689	591
$d^{(i)}$	**144**	**293**	**788**	**180**	**76**	**243**	**636**	**752**	**258**	**2**	**112**
$\alpha_1^{(i)}$	314	204	30	86	86	74	324	37	281	284	251
$\alpha_2^{(i)}$	563	416	337	222	489	314	530	164	513	741	544
$\alpha_3^{(i)}$	678	207	313	720	571	430	595	496	418	828	342
$d^{(i)}$	**289**	**578**	**43**	**433**	**508**	**15**	**488**	**259**	**683**	**405**	**38**

Let us take the secret keys of the exponents $\{e_i\}$ of the isogenies of Alice and Bob $\Omega_A = (7,-5, 8)$, $\Omega_B = (-8, 6,-5)$, their functions of the class group actions, respectively $\Theta_A = [3^7, 5^{-5}, 7^8]$, $\Theta_B = [3^{-8}, 5^6, 7^{-5}]$. Compute their public keys d_A, d_B. As the starting curve of the chain of isogenies, we take the curve $E_d{}^{(0)} = E_{144}$. Then, $E_A = E_d{}^{(0)} * \Theta_A$, $E_B = E_d{}^{(0)} * \Theta_B$.

In order to simplify the notation in the algorithm for calculating an isogenic curve $E_A = E_d{}^{(0)} * \Theta_A$, we will use only the parameters $d^{(i)}$, which completely determine the curves $E_d{}^{(i)}(e_k > 0)$ and $E_{-1,-d}{}^{(i)}(e_k < 0)$ as pairs of quadratic twist. The commutability property of the function Θ_A in our case means that there are 3!=6 options for choosing the order of the isogeny degrees. With $E_d{}^{(0)} = E_{144}$, $\Theta_A = [3^7, 5^{-5}, 7^8]$ and choosing the order of degrees of isogenies 3-5-7, the values $d^{(i)}$ of tables 2, 3, 4 we define as

$$\frac{d_0 = 144}{(3)} \xrightarrow{7} \frac{773}{(5)} \xrightarrow{-5} \frac{?}{(7)} \xrightarrow{8} ?$$

Here, under the value $d^{(i)}$ in parentheses, we conditionally put the degree of isogeny, and above the arrow, the value e_k of the exponent of Alice's secret key (the number of steps in the sequence $d^{(i)}$ to the right or left, depending on the sign e_k). This choice of the order of isogeny degrees turned out to be unsuccessful, since the value $d^{(i)} = 773$ is included in the data in Table 2, but is not included in Tables 3 and 4.

In this case, it is more rational to calculate isogenies of higher degrees first (with a smaller amount of data), and at the final stage, 3-isogenies. In this case, we get two paths:

$$\frac{d_0 = 144}{(7)} \xrightarrow{8} \frac{258}{(5)} \xrightarrow{-5} \frac{112}{(3)} \xrightarrow{7} 286,$$

$$\frac{d_0 = 144}{(5)} \xrightarrow{-5} \frac{788}{(7)} \xrightarrow{8} \frac{112}{(3)} \xrightarrow{7} 286.$$

So, Alice's public key is $d_A = 286$. Similarly, we define Bob's public key based on $E_d{}^{(0)} = E_{144}$ and functions $\Theta_B = [3^{-8}, 5^6, 7^{-5}]$

$$\frac{d_0 = 144}{(5)} \xrightarrow{6} \frac{788}{(7)} \xrightarrow{-5} \frac{258}{(3)} \xrightarrow{-8} 514,$$

$$\frac{d_0 = 144}{(7)} \xrightarrow{-5} \frac{636}{(5)} \xrightarrow{6} \frac{258}{(3)} \xrightarrow{-87} 514$$

So, Bob's public key is $d_B = 514$. In the non-interactive CSIDH protocol, the keys d_A, d_B are known to both users. Next, in the secret-sharing scheme, Alice encrypts Bob's public key with her private key and computes $E_{BA} = E_B * \Theta_A$. Bob acts symmetrically and gets

$E_{AB} = E_A * \Theta_B$. In our example, Alice's calculations $E_{BA} = E_{514} * \Theta_A$ with $\Theta_A = [3^7, 5^{-5}, 7^8]$ and choosing the order of degrees of isogenies 3-5-7 give the result

$$\frac{d_B = 514}{(3)} \xrightarrow{7} \frac{683}{(5)} \xrightarrow{-5} \frac{38}{(7)} \xrightarrow{8} 259 \quad \Rightarrow d_{BA} = 259.$$

Accordingly, Bob's calculations $E_{AB} = E_{286} * (\Theta_B = [3^{-8}, 5^6, 7^{-5}])$ can be written as

$$\frac{d_A = 286}{(3)} \xrightarrow{-8} \frac{38}{(5)} \xrightarrow{6} \frac{578}{(7)} \xrightarrow{-5} 259 \quad \Rightarrow d_{AB} = 259.$$

Due to the commutability of the CSIDH $d_{BA} = d_{AB}$. Knowing the secret keys of Alice and Bobs and their sum $\Omega_A + \Omega_B = (-1, 1, 3)$, it is easy to check this result according to the algorithm $E_d^{(0)} * \Theta_A * \Theta_B = E_{144} * [3^{-1}, 5, 7^3]$

$$\frac{d_0 = 144}{(7)} \xrightarrow{3} \frac{180}{(5)} \xrightarrow{1} \frac{752}{(3)} \xrightarrow{-1} 259 \quad \Rightarrow \quad d_{AB} = 259$$

To avoid ambiguity in obtaining isomorphic curves, the J-invariant (5) $J(d_{AB}) = 725$ of the curve E_{259} is taken as the shared secret.

SAMPLE OF RANDOM POINTS AND RANDOMIZATION OF THE CSIDH ALGORITHM

The CSIDH algorithm proposed by the authors of [2] is constructed in such a way that the calculations of isogenic chains according to functions $\Theta_{A,B} = [l_1^{e_1}, l_2^{e_2}, .., l_K^{e_K}]$ are performed in 2 stages: first, a set S is formed with key exponents e_k of one sign, then another. At each stage, the kernels and parameters of exactly $|e_k|$ isogenic curves of isogenies of degrees l_k built on curves of the same class (E_d or $E_{-1,-d}$) are sequentially calculated. This obviously generates a side-channel attack threat based on the measurement of the time of these calculations, proportional to the length $|e_k|$ and degree l_k of each chain $[l_k^{e_k}]$. In this regard, in most articles on this topic, various variants of "constant time CSIDH" are considered, in which the secret exponents are increased to the upper limit by fictitious chains of isogenies. It is clear that such protection is achieved by significant redundancy and algorithm slowdown.

In this work, we propose another method for solving the problem – randomization of paths of isogenic chains. The idea is that any random coordinate of an elliptic curve always generates a random point $P = (x, y)$ of one of the two curves of a quadratic twist pair. Then instead of trying (unsuccessfully with a probability of 1/2) to find a point of a curve of a given class and success with a probability of 1, we determine the class of the curve (in our case it is the curve E_d or $E_{-1,-d}$, one of which belongs the point $P = (x, y)$). Further, in this class, the first isogenic curve $E^{(1)} = [l_k] * E^{(0)}$ of the degree l_k of isogeny corresponding to the sign e_k of the exponent is calculated. The choice l_k is randomized, and the value $|e_k|$ is reduced by 1. At the next step, with a new parameter value $d^{(1)}$, a random point $P=(x,y)$ of one of the curves E_d or $E_{-1,-d}$ is determined again, the isogeny kernel of a randomly chosen degree l_k is determined, and the parameter $d^{(2)}$ is calculated. The process continues until zeroing all e_k .

It should be noted that the classical CSIDH already have a guaranteed level of protection against the type of side channel attack described above. This level determined by the sign of the secret exponent e_k of the key. Since for each component $[l_k]$ of the function Θ the calculation time $[l_k^{+1}]$ and $[l_k^{-1}]$ is the same, the probability of the analyst's success even in the conditions of correctly found values l_k is $2^{-K}=2^{-74}$ (for the data of [2]). With an average length $\frac{m+1}{2}=3$ of the chain of isogenies of each degree l_k, the total length of the chain of isogenies of the function Θ is $3\cdot 74=222$ steps. Let p_1 is the probability of an unmistakable determination of the degree l_k by an analyst at one step of the randomized CSIDH protocol, then its probability of success can be estimated by the value $2^{-74}p_1^{222}, p_1<1$. For example, at $p_1=\frac{1}{2}$, the analyst's probability of success is 2^{-296} , and at $p_1=\frac{3}{4}$, this probability is close to 2^{-165}. This is well below the security level 2^{-128}. Various modifications of the proposed randomization method are possible with insertions of single fictitious exponents into the sample components $[l_k]$ of the function Θ , which will not introduce redundancy into the calculations. Let's not forget that one analyst's mistake destroys all his laborious work.

To illustrate the randomization method based on the data in tables 2, 3, 4 of the previous section, we will give an example of Alice calculating her public key using the secret key $\Omega_A=(7,-5,8)$. In a sequence of isogenies, let the symbol $s=0$ correspond to the random choice of the curve E_d , and the symbol $s=1$ to the choice of $E_{-1,-d}$. In a sufficiently long sequence, these symbols could be considered as equiprobable. In our example, the length of the isogeny chain is 7+5+8=20 with the frequency distribution $\left\{\frac{3}{4},\frac{1}{4}\right\}$, then it is possible to model a short pseudo-random sequence $\Lambda=00101001000101000000$ of length 20 isogeny curves on the way to calculate Alice's public key. Based, as in the previous section, from the starting curve E_{144} , we use the data of tables 2 or 4 for series of symbols 0 of the sequence Λ , and the data of table 3 for series of symbols 1. In the first case, we move to the right along the rows of tables, in the second – to the left. The number of steps is determined by the length of a series of identical symbols in Λ and is written with exponential signs above the arrows of isogenic transitions below. Thus, on the way Λ, in 20 steps, Alice calculates

$$\frac{d_0=144}{(3)}\xrightarrow{2}\frac{405}{(5)}\xrightarrow{-1}\frac{15}{(7)}\xrightarrow{1}\frac{488}{(5)}\xrightarrow{-1}\frac{43}{(7)}\xrightarrow{2}\frac{508}{(5)}\xrightarrow{-1}\frac{289}{(3)}\xrightarrow{2}\frac{43}{(7)}\xrightarrow{3}\frac{405}{(5)}$$

$$\frac{405}{(5)}\xrightarrow{-1}\frac{15}{(3)}\xrightarrow{1}\frac{243}{(5)}\xrightarrow{-1}\frac{293}{(7)}\xrightarrow{5}\frac{636}{(3)}\xrightarrow{1}286 \quad\Rightarrow\quad d_A=286$$

This result, of course, coincides with the result of the previous section. Randomization of the choice of curves, in fact, randomly splits the exponents of the key Ω_A and introduces significant uncertainty into the analyst's task.

Let us now turn to some properties of the curves E_d and $E_{-1,-d}$, which are useful in choosing a random point of one of them. For curves of order $N_E = 8n$, there are 8 times more points of maximum order than points of odd order. For the latter, in turn, the choice of a point of order that divides n is very unlikely.

Equations (3) and (4) will be written as

$$E_d : \quad y^2 = \frac{x^2-1}{dx^2-1}, \quad \chi(d)=1: \qquad\qquad E_{-1,-d} : \quad y^2 = \frac{1-x^2}{dx^2-1}, \quad \chi(d)=1$$

Excluding points of small orders and singular points ($(xy \neq 0),\ (dx^2 \neq 1), (dy^2 \neq 1)$), the choice of a random element $x \in F_p$ generates a random point $P(x,y) \in F_d$ or $P(x,y) \in E_{-1,-d}$. In the first case $\chi((dx^2-1)(x^2-1)) = 1$, in the second case $\chi((dx^2-1)(x^2-1)) = -1$, is performed. According to the above formulas, the y-coordinate of the point $P(x,y)$ is calculated. Below we present Algorithm 2 of a randomized CSIDH implementation .

<u>Randomized</u> **<u>Algorithm 2: Evaluating the class-group action on quadratic and twisted SEC.</u>**

```
Input: $d_A \in E_A, \chi(d)=1$ and a list of integers $\Omega_A = (e_1, e_2, ...e_K)$ .
Output: $d_B$ such that $[l_1^{e_1}, l_2^{e_2}, ...l_K^{e_K}] * E_A = E_B$, where $E_{A,B}: \quad x^2+y^2 = 1+d_{A,B}x^2y^2$,
    1. Let $V_0 = \{k \mid e_k > 0\}$ , $V_1 = \{k \mid e_k < 0\}$, $n_0 = \prod_{k \in V_0} l_k$, , $n_1 = \prod_{k \in V_1} l_k$,
    2. While some $e_k \neq 0$ do
        3. Sample a random $x \in F_p$,
        4. Set $a \leftarrow 1, s \leftarrow 0$ , $E_A : x^2+y^2 = 1+d_Ax^2y^2$ If $\chi((x^2-1)/(dx^2-1)=1$,
        5. Else $a \leftarrow -1, s \leftarrow 1$ $E_A : x^2-y^2 = 1-d_Ax^2y^2$,
        6. Compute $y$-coordinate of the point $P=(x,y) \in E_A$,
        7. Compute $R \leftarrow [(p+1)/2n_s]P$,
        8. Sample a random $l_k \mid k \in V_s$,
        9. Compute $Q \leftarrow [n_s / l_k]R$
        10. If $Q \neq (1,0)$ compute kernel $G$ of $l_k$ - isogeny $\phi : E_A \to E_B$,
        11. Else start over to line 3,
        12. Compute $d_B$ of curve $E_B$, $d_A \leftarrow d_B, e_k \leftarrow e_k - a$ ,
        13. Skip $k$ in $V_s$ and set $n_s \leftarrow (n_s / l_k)$ If $e_k = 0$,
    14. Return $d_A$.
```

This algorithm has 2 important differences from algorithm 1.

Firstly, we do not divide the calculation of isogenies into 2 stages with curves of one class, then another ($a \leftarrow -a$), but we build a random sequence $\{s\}$ with an equiprobable choice of curves E_d or $E_{-1,-d}$, at each step. Together with the doubled acceleration of the procedure for sampling curves, this deprives the analyst of the possibility of orderly construction of subsets V_0, V_1 degrees of isogenies for curves E_d or $E_{-1,-d}$. In addition, for each component $[l_k^{e_k}]$ of the function Θ, the chain of isogenies of length $|e_k|$ is divided into fragments of the general chain, inserted at random times. This inevitably complicates the task of measuring the computation time according to the function $[l_k^{e_k}]$.

Secondly, in Algorithm 2 (line 12) we refuse to calculate the isogenic function $\phi(R)$, which also significantly speeds up the algorithm. The ultimate goal of the CSIDH secret sharing algorithm is to find the common parameter d_{AB} of curve E_{AB}. For each step in the isogeny chain $E \to E'$, it is only necessary to calculate the parameter $d' = \psi(d, Q)$ based on the parameters d and the kernel $< Q >$ of the domain E . This calculation involves two scalar multiplications (SM) of odd-order random points R and $(l_k - 1)/2$ recurrent doublings of points from $< Q >$. Thus, the construction and calculation of a sufficiently complex function $\phi(R)$ is not necessary for the implementation of the CSIDH algorithm. While the order of a point R always contains a factor l_k, the order of its image $\phi(R)$ does not have such a factor, and the point $\phi(R) \in E'$ is useless for finding the kernel of the curve E'. It is used only at the end of the chain of isogenies at $R = Q, \phi(Q) = (1,0)$, but this well-known property does not require verification. Part of the calculations in Algorithm 1 related to the calculation of the function $R = Q, \phi(Q) = (1,0)$ can be saved.

At the beginning of Algorithm 2, two subsets $V_s, s = 0,1$ are formed with degree l_k numbers, together with two factors n_0 and n_1 of number $n = n_0 n_1$. Since the order of the curve is $p + 1 = 8n$, then in line 7 of the algorithm, a point $R = 4n_1 P$ of odd order n_0 is calculated for the curve E_d, and a point $R = 4n_0 P$ of odd order n_1 is calculated for the curve $E_{-1,-d}$. As in Algorithm 1, this minimizes the cost of the next SM that determines the isogeny kernel point Q (line 9). Further, in line 10 of the algorithm, the $(l_k - 1)/2$ coordinates of the points of the kernel G are calculated by doubling the points. Estimates of the cost of these calculations in coordinates $(W : Z)$ are given in [7].

The results of the implementation of the Edwards-CSIDH model [3] in projective coordinates $(W : Z)$ state that it is faster than the Montgomery-CSIDH model in coordinates $(X : Z)$ by 20%. Note that this model in [3] is construct on complete Edwards curves with order $N_E = p + 1 = 4n$. . Based on Theorems 1 and 2 [1], in this paper we have shown how to implement such a model on quadratic and twisted SECs that form pairs of quadratic twist. The main advantage of these classes of Edwards curves over the complete Edwards curves is the doubling of the number of curves in the algorithm with a corresponding increase in security. In addition, the time-consuming inversion of the parameter $d \to d^{-1}$ is not required when going to the complete SEC of quadratic twist. It also speeds up the algorithm.

It can be concluded that the method of randomization of the CSIDH algorithm on quadratic and twisted SECs proposed in this paper provides an efficient and secure alternative to various variants of Constant time CSIDH [15,16, etc.]. Computing of isogenies of odd degrees in $(W : Z)$ coordinates [3] allows you to implement the fastest calculations today when building the PQC protocol CSIDH and similar ones. This article provides an example of such an implementation for a simple model of the CSIDH algorithm. The possibility of refusing to calculate the isogenic function $\phi(R)$ of a random point R is substantiated, which radically speeds up the algorithm. The largest computational costs in the CSIDH algorithm are associated with scalar multiplications SM of random points, which require more experimental evaluation. In further studies, it is planned to obtain such estimates.

REFERENCES

1. Bessalov, A., Sokolov, V., Skladannyi, P., Zhyltsov, O. (2021). Computing of odd degree isogenies on supersingular twisted Edwards curves. *CEUR Workshop Proceedings*, 2923, 1–11.
2. Castryck, W., Lange, T., Martindale, C., Panny, L., Renes, J. (2018). CSIDH: An Efficient Post-Quantum Commutative Group Action. In *Lecture Notes in Computer Science* (pp. 395–427). Springer International Publishing. https://doi.org/10.1007/978-3-030-03332-3_15
3. Kim, S., Yoon, K., Park, Y.-H., Hong, S. (2019). Optimized Method for Computing Odd-Degree Isogenies on Edwards Curves. In *Lecture Notes in Computer Science* (pp. 273–292). Springer International Publishing. https://doi.org/10.1007/978-3-030-34621-8_10.

4 Farashahi, R. R., Hosseini, S. G. (2017). Differential Addition on Twisted Edwards Curves. In *Information Security and Privacy* (pp. 366–378). Springer International Publishing. https://doi.org/10.1007/978-3-319-59870-3_21.

5 Kim, S., Yoon, K., Kwon, J., Hong, S., Park, Y.-H. (2018). Efficient Isogeny Computations on Twisted Edwards Curves. *Security and Communication Networks*, *2018*, 1–11. https://doi.org/10.1155/2018/5747642

6 Moody, D., Shumow, D. (2016). Analogues of Velus formulas for isogenies on alternate models of elliptic curves. *Mathematics of Computation*, *85*(300), 1929–1951.

7 Bessalov, A.V., Tsyhankova, O.V. Abramov, S.V. (2021). Otsenka vychyslytelnoi slozhnosty alhorytma CSIDH na supersynhuliarnykh skruchennykh y kvadratychnykh kryvykh Edvardsa. Radyotekhnyka, 207, 40-51.

8 Bernstein, D. J., Lange, T. (2007). Faster Addition and Doubling on Elliptic Curves. In *Advances in Cryptology – ASIACRYPT 2007* (pp. 29–50). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-540-76900-2_3.

9 Bernstein, D. J., Birkner, P., Joye, M., Lange, T., Peters, C. (2008). Twisted Edwards Curves. In *Progress in Cryptology – AFRICACRYPT 2008* (pp. 389–405). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-540-68164-9_26

10 Bessalov, A.V. (2017). Ellyptycheskye kryvye v forme Edvardsa y kryptohrafyia. Monohrafyia. «Polytekhnyka».

11 Bessalov, A.V., Tsygankova, O.V. (2017). Number of curves in the generalized Edwards form with minimal even cofactor of the curve order. Problems of Information Transmission, 53(1), 92-101.

12 Bessalov, A.V., Kovalchuk, L.V. (2019). Supersingular Twisted Edwards Curves Over Prime Fields. I. Supersingular Twisted Edwards Curves with j-Invariants Equal to Zero and 12^3. *Cybernetics and Systems Analysist, 55*(3), 347–353.

13 Bessalov, A.V., Kovalchuk, L.V. (2019). Supersingular Twisted Edwards Curves over Prime Fields.* II. Supersingular Twisted Edwards Curves with the j-Invariant Equal to 66^3. *Cybernetics and Systems Analysist, 55*(5), 731–741.

14 Washington, L.C. (2008). *Elliptic Curvres. Number Theory and Cryptography. Second Edition*. CRC Press.

15 Onuki, H., Aikawa, Y., Yamazaki, T., Takagi, T. (2020). *A Faster Constant-time Algorithm of CSIDH keeping Two Points.* ASIACRYPT.

16 Jalali, A., Azarderakhsh, R., Kermani, M. M., Jao, D. (2019). Towards Optimized and Constant-Time CSIDH on Embedded Devices. У *Constructive Side-Channel Analysis and Secure Design* (с. 215–231). Springer International Publishing. https://doi.org/10.1007/978-3-030-16350-1_12

Бессалов Анатолій Володимирович
Доктор технічних наук, професор
Професор кафедри інформаційної та кібернетичної безпеки
Київський університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0002-6967-5001
a.bessalov@kubg.edu.ua

Ковальчук Людмила Василівна
Доктор технічних наук, професор
Професор Національного технічного університету України «Київський політехнічний університет імені Ігоря Сікорського»
ORCID ID: 0000-0003-2874-7950
l.kovalchuk@kpi.ua

Абрамов Сергій Вадимович
аспірант Київського університету імені Бориса Грінченка, Україна
ORCID ID 0000-0002-5145-2782
s.abramov.asp@kubg.edu.ua

РАНДОМІЗАЦІЯ АЛГОРИТМУ CSIDH НА КВАДРАТИЧНИХ ТА СКРУЧЕНИХ КРИВИХ ЕДВАРДА

Анотація. Розглянуто властивості квадратичних і кручених суперсингулярних кривих Едвардса, які утворюють пари квадратичних кручень з порядком над простим полем. Розглянуто модифікацію алгоритму CSIDH на основі ізогеній непарного ступеня цих кривих. Побудовано просту модель для реалізації алгоритму CSIDH у 3 мінімальних непарних ступенях ізогенії 3, 5, 7, з простим модулем поля та порядком суперсингулярних кривих. На етапі випадання розраховуються та зводяться в таблицю параметри ізогенних ланцюгів усіх ступенів для цих двох класів суперсингулярних кривих Едвардса. Наведено приклад реалізації алгоритму CSIDH як неінтерактивної схеми обміну секретами на основі секретного та відкритого ключів Аліси та Боба. Запропоновано новий рандомізований алгоритм CSIDH з випадковим рівноімовірним вибором однієї з кривих цих двох класів на кожному кроці ланцюга ізогенії. Вибір ступеня кожної ізогенії є випадковим. Проілюстровано роботу рандомізованого алгоритму на прикладі. Цей алгоритм розглядається як можлива альтернатива "CSIDH з постійним часом". Комбінація двох підходів можлива для протидії атакам на бокових каналах. Наведено оцінки ймовірності успішної атаки побічного каналу в рандомізованому алгоритмі. Зазначається, що всі обчислення в алгоритмі CSIDH, необхідні для обчислення загального секрету, зводяться лише до обчислення параметра ізогенної кривої та виконуються за допомогою польових і групових операцій, зокрема, множення скалярних точок і подвоєння точок ядра ізогенії. У новому алгоритмі ми пропонуємо відмовитися від обчислення ізогенної функції випадкової точки , що значно прискорює роботу алгоритму.

Ключові слова: крива в узагальненому вигляді Едвардса, повна крива Едвардса, скручена крива Едвардса, квадратична крива Едвардса, порядок кривої, точковий порядок, ізоморфізм, ізогенія, рандомізація, w-координати, квадрат, неквадрат.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Bessalov, A., Sokolov, V., Skladannyi, P., Zhyltsov, O. (2021). Computing of odd degree isogenies on supersingular twisted Edwards curves. *CEUR Workshop Proceedings*, 2923, 1–11.

2 Castryck, W., Lange, T., Martindale, C., Panny, L., Renes, J. (2018). CSIDH: An Efficient Post-Quantum Commutative Group Action. In *Lecture Notes in Computer Science* (pp. 395–427). Springer International Publishing. https://doi.org/10.1007/978-3-030-03332-3_15

3 Kim, S., Yoon, K., Park, Y.-H., Hong, S. (2019). Optimized Method for Computing Odd-Degree Isogenies on Edwards Curves. In *Lecture Notes in Computer Science* (pp. 273–292). Springer International Publishing. https://doi.org/10.1007/978-3-030-34621-8_10.

4 Farashahi, R. R., Hosseini, S. G. (2017). Differential Addition on Twisted Edwards Curves. In *Information Security and Privacy* (pp. 366–378). Springer International Publishing. https://doi.org/10.1007/978-3-319-59870-3_21.

5 Kim, S., Yoon, K., Kwon, J., Hong, S., Park, Y.-H. (2018). Efficient Isogeny Computations on Twisted Edwards Curves. *Security and Communication Networks*, *2018*, 1–11. https://doi.org/10.1155/2018/5747642

6 Moody, D., Shumow, D. (2016). Analogues of Velus formulas for isogenies on alternate models of elliptic curves. *Mathematics of Computation*, *85*(300), 1929–1951.

7 Бессалов, А.В., Цыганкова, О.В. Абрамов, С.В. (2021). Оценка вычислительной сложности алгоритма CSIDH на суперсингулярных скрученных и квадратичных кривых Эдвардса. *Радиотехника,* 207, 40-51.

8 Bernstein, D. J., Lange, T. (2007). Faster Addition and Doubling on Elliptic Curves. In *Advances in Cryptology – ASIACRYPT 2007* (pp. 29–50). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-540-76900-2_3.

9 Bernstein, D. J., Birkner, P., Joye, M., Lange, T., Peters, C. (2008). Twisted Edwards Curves. In *Progress in Cryptology – AFRICACRYPT 2008* (pp. 389–405). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-540-68164-9_26

10 Бессалов, А.В. (2017). *Эллиптические кривые в форме Эдвардса и криптография*. Монография. «Политехника».

11 Bessalov, A.V., Tsygankova, O.V. (2017). Number of curves in the generalized Edwards form with minimal even cofactor of the curve order. Problems of Information Transmission, 53(1), 92-101.

12 Bessalov, A.V., Kovalchuk, L.V. (2019). Supersingular Twisted Edwards Curves Over Prime Fields. I. Supersingular Twisted Edwards Curves with j-Invariants Equal to Zero and 12^3. *Cybernetics and Systems Analysist, 55*(3), 347–353.

13 Bessalov, A.V., Kovalchuk, L.V. (2019). Supersingular Twisted Edwards Curves over Prime Fields.* II. Supersingular Twisted Edwards Curves with the j-Invariant Equal to 66^3. *Cybernetics and Systems Analysist, 55*(5), 731–741.

14 Washington, L.C. (2008). *Elliptic Curvres. Number Theory and Cryptography. Second Edition*. CRC Press.

15 Onuki, H., Aikawa, Y., Yamazaki, T., Takagi, T. (2020). *A Faster Constant-time Algorithm of CSIDH keeping Two Points.* ASIACRYPT.

16 Jalali, A., Azarderakhsh, R., Kermani, M. M., Jao, D. (2019). Towards Optimized and Constant-Time CSIDH on Embedded Devices. У *Constructive Side-Channel Analysis and Secure Design* (с. 215–231). Springer International Publishing. https://doi.org/10.1007/978-3-030-16350-1_12