Modeling CSIKE Algorithm on Non-Cyclic Edwards Curves

Anatoly Bessalov[1], Volodymyr Sokolov[1], Pavlo Skladannyi[1], Serhii Abramov[1], and Oleksii Zhyltsov[1]

[1] *Borys Grinchenko Kyiv University, 18/2 Bulvarno-Kudriavska str., Kyiv, 04053, Ukraine*

Abstract

An original key encapsulation scheme is proposed as a modification of the CSIDH algorithm built on the isogenies of non-cyclic Edwards curves. The corresponding CSIKE algorithm uses only one public key of the recipient. A brief review of the properties of non-cyclic quadratic and twisted supersingular Edwards curves is given. We use a new scheme for modeling the CSIKE algorithm on isogenies of 4 degrees 3, 5, 7, 11 for $p = 9239$. In contrast to the CSIDH models of previous works, this scheme does not use precomputations and tabulation of the parameters of isogenic chains, but uses one known supersingular starting curve E_d with the parameter $d = 2$. Examples of calculations of isogenic chains by Alice and Bob at three stages of CSIKE operation using a randomized algorithm are given. It also proposes to abandon the calculation of the isogenic function $\phi(R)$ of a 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.

1. Introduction

The post-quantum cryptography (PQC) algorithm CSIDH [1] has a well-known advantage over others—the minimum key length, close to the modulus of the prime field F_p, on which group operations are performed. The main criticism of CSIDH relates to its vulnerability to a side channel attack built on measuring the time it takes to compute a chain of isogenies of each prime degree l_k proportional to l_k and the secret exponent e_k of the key. In a large number of papers [2, 3], the solution to this problem is proposed by increasing the exponents e_k by fictitious ones up to a known maximum (Constant time CSIDH). In this paper, we use CSIDH and CSIKE algorithm randomization as an alternative approach to counter this attack. Note that in the key exchange problem today preference is given to key encapsulation schemes. The main goal of this work is to present the original CSIKE (Commutative Supersingular Isogeny Key Encapsulation) algorithm with an illustration of how its model works on the minimum 4 degrees of isogeny. Instead of two public keys in CSIDH, the CSIKE algorithm uses one recipient's public key.

In [4,5], the solution of such a problem is proposed on the basis of the well-known KEM (Key Encapsulation Mechanism) scheme, built on the ElGamal encryption algorithm. Its implementation is complex and time-consuming. We propose a simpler, faster and more efficient CSIKE encryption algorithm with one public key as a modification of CSIDH with inversion of the recipient's private key [6–8].

As the most efficient technology of the algorithm, classes of non-cyclic quadratic and twisted supersingular Edwards curves (SEC) forming the quadratic twist pairs are proposed [9–11]. In comparison with the known implementations of CSIDH on complete Edwards curves [12], this technology doubles the space of curves used and, moreover, does not require laborious inversion of the curve parameter d in the transition to quadratic twist.

Computing odd degree isogenies on complete and quadratic Edwards curves is carried out

CPITS-2022: Cybersecurity Providing in Information and Telecommunication Systems, October 13, 2022, Kyiv, Ukraine
EMAIL: a.bessalov@kubg.edu.ua (A. Bessalov); v.sokolov@kubg.edu.ua (V. Sokolov); p.skladannyi@kubg.edu.ua (P. Skladannyi); s.abramov.asp@kubg.edu.ua (S. Abramov); o.zhyltsov@kubg.edu.ua (O. Zhyltsov)
ORCID: 0000-0002-6967-5001 (A. Bessalov); 0000-0002-9349-7946 (V. Sokolov); 0000-0002-7775-6039 (P. Skladannyi); 0000-0002-5145-2782 (S. Abramov); 0000-0002-7253-5990 (O. Zhyltsov)

according to the formulas of Theorems 2–4 of [13]. In the fundamental papers [14, 15], some classes of Edwards curves, in our opinion, received unfortunate terms, which leads to ambiguous interpretations. We use the classification of curves in the generalized Edwards form with two parameters a and d [16, 17] with their division into three non-intersecting classes of curves (Section 2). In [8], we generalized the theorems of [12] to curves in the generalized Edwards form, which made it possible in [9–11] to apply quadratic and twisted Edwards curves over a field F_p to implement the simplest models of the CSIDH algorithm. To illustrate their work, we used pre-computation and tabulation of the parameters of isogenic chains, which is possible in a limited volume of the article with the number of isogeny degrees not more than three. For a real cryptosystem, this makes no sense. In this article, without pre-computations, we give examples of the CSIKE algorithm work with the construction of random isogenic SEC chains and a starting curve E_d with a parameter $d = 2$ known from [19]. Such modeling is much closer to the operation of a real algorithm with a large number of isogeny degrees.

An analysis of the properties of quadratic and twisted Edwards curves that form pairs of quadratic twist is given in [18, 19]. Supersingular curves of these classes with the same order $N_E = p + 1 = 2^m n$, $m \geq 3$ (n is odd) exist only for $p \equiv 3\text{mod}4$. The minimum even cofactor of the order of such curves is 8; then, for the CSIDH and CSIKE algorithms with an odd $n = \prod_{i=1}^{K} l_i$ the field F_p modulus, it should be chosen as $p = 8n - 1$. In order to adapt the definitions for the arithmetic of the isogenies of Edwards curves and curves in the Weierstrass form, we use a modified point addition law [16].

Section 2 gives a brief overview of the properties of noncyclic twisted and quadratic supersingular Edwards curves (SEC) [18, 19]. Section 3 gives a description of the CSIDH [1] algorithm with its adaptation to classes of non-cyclic SEC, and a theorem [8] on the isogenies of such curves. In Section 4, we present the original CSIKE scheme and give an example of Alice's calculations at the first stage of her work on a model with isogeny degrees 3, 5, 7, 11 over a prime field F_p at $p = 9239$. In Section 5, the rationale for the randomization method of the CSIDH algorithm is given, a new randomized CSIKE 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 algorithm. Examples of calculations by Alice and Bob at three stages of the model of the randomized CSIKE algorithm are given.

2. Brief Review of the Properties of Non-Cyclic Supersingular Edwards Curves

We define an elliptic curve in the generalized Edwards form [16, 17] by the equation

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

If the quadratic character is $\chi(ad) = -1$, curve (1) is isomorphic to the complete Edwards curve [14, 15] with one parameter d

$$E_d: x^2 + y^2 = 1 + dx^2y^2, \chi(d) = -1. \tag{2}$$

Otherwise $\chi(ad) = 1$, $\chi(a) = \chi(d) = 1$, the curve (1) is isomorphic with the quadratic Edwards curve [16]

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

having, in contrast to (2), the parameter d defined as a square. For both curves (2) and (3) one usually takes $a = 1$. In [15], curve (3) together with curve (2) are called Edwards curves. At the same time, the difference in the quadratic characters of these curves leads to radically different properties [16, 17]. In particular, the order of cyclic SKE (2) $N_E \equiv 0\text{mod}4$, and non-cyclic SEC (3) $N_E \equiv 0\text{mod}8$.

The twisted Edwards curve is defined in [16] as a special case of curve (1) for $\chi(ad) = 1$, $\chi(a) = \chi(d) = -1$. Only this class of Edwards curves requires the second parameter a in equation (1). In [15], all curves in the form (1) are called twisted.

Let us define a pair of quadratic and twisted Edwards curves [16, 17] as a pair of quadratic twist with parameters $\chi(ad) = 1$, $a' = ca$, $d' = cd$, $\chi(c) = -1$. Since SEC exist only for $p \equiv 3\text{mod}4$ [18], we can take $c = -1$, $a' = -a = -1$, $d' = -d$ where a and d are the parameters of a quadratic curve, respectively a' and d', of a twisted curve. In other words, the transition from a quadratic to a twisted torsion curve and vice versa can be defined as $E_d = E_{1,d} \leftrightarrow E_{-1,-d}$. Accordingly, the

twisted SEC equation for $p \equiv 3\text{mod}4$ from (1) can be written as

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

Over a prime field F_p, a supersingular 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 2nd order (contain 3 points of the 2nd order each, two of which are exceptional points $D_{1,2} = \left(\pm\sqrt{\frac{a}{d}}, \infty\right)$ [15, 16]). Quadratic SEC (3), in addition, contains two exceptional points of the 4th order $\pm F_1 = \left(\infty, \pm\frac{1}{\sqrt{d}}\right)$ The presence of a noncyclic subgroup of the 4th order containing 3 points of the 2nd order limits the number 8 to the minimum even cofactor of the order $N_E = 8n$ (n is odd) of quadratic and twisted Edwards curves [16]. In general, their order is $N_E = 2^m n$, $m \geq 3$. 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).

3. CSIDH Algorithm on Quadratic and Twisted Edwards Curves

The PQC CSIDH (Commutative Supersingular isogeny Diffie-Hellman) algorithm proposed by the authors of [1] for solving the key exchange problem based on isogenic mappings of supersingular elliptic curves as additive Abelian groups. Such a commutative mapping over a prime field F_p as the class group action is defined [1]. It provides the smallest known key size (512 bits in [1]).

Let the curve E of order $N_E = p + 1$ contain points of small odd orders l_k, $k = 1, 2, \ldots, K$. 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 [1], an interval of exponential values $[-m \leq e_i \leq m]$ 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 in [1] uses fast arithmetic of Montgomery elliptic curves $y^2 = x^3 + Cx^2 + x$, $C \neq \pm2$ containing two points of the 4th order and, accordingly, having an order $N_E = p + 1 = 4n$ (n is odd) [14]. In [12] the CSIDH algorithm implemented on complete SEC of the same order. In [9–11] and this paper, we use quadratic and twisted SECs in the CSIDH algorithm, which have the same speed performance as complete Edwards curves [12]. In [8] we proved two theorems for implementation such possibility. With a minimum cofactor of 8, the order of twisted and quadratic SEC is $N_E = 8n$. Thus, for these SEC classes with order $N_E = 8n = p + 1, n = \prod_{k=1}^{K} l_k$ the field modulus in the CSIDH algorithm we chosen as $p = \prod_{k=1}^{K} l_k - 1 \equiv -1\text{mod}8$.

Non-interactive Diffie-Hellman key exchange includes the following steps [1]:

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 [1] $K = 74$, $l_{74} = 587$), and choose an appropriate field modulus $p = 2^m \prod_{k=1}^{K} l_k - 1$, $m \geq 3$ and a starting elliptic curve E_0.

2. *Calculation of public keys.* Alice uses her private key $\Omega_A = (e_1, e_2, \ldots, e_K)$ to build an isogenic mapping $\Theta_A = [l_1^{e_1}, l_2^{e_2}, \ldots, l_K^{e_K}]$ (class group action [1]) 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 [1] 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* $\Omega_A = (e_1, e_2, \ldots, e_K)$.
Output: d_B *such that* $[l_1^{e_1}, l_2^{e_2}, \ldots, l_K^{e_K}]*E_A = E_B$, *where* $E_{A,B}$: $x^2 + ay^2 = 1 + ad_{A,B}x^2y^2$.

1. **While** *some* $e_k \neq 0$ **do**
2. *Sample a random* $x \in F_p$,
3. *Set* $a \leftarrow 1$, E_A: $x^2 + y^2 = 1 + d_Ax^2y^2$ **if** $(x^2 - 1)(dy^2 - 1)$ *is a square in* F_p,
4. **Else** $a \leftarrow -1$, E_A: $x^2 - y^2 = 1 - d_Ax^2y^2$,
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* ϕ: $E_A \rightarrow E_B$ *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 [1], 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. Lite 10 has been corrected (you cannot reset the index k before zeroing e_k in line 10).

3. Updating the number $n \leftarrow n/l_k$ and reset k in line 11 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 [13], and for twisted Edwards curves—Theorem 1 [8]. 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.

4. CSIDH Algorithm on Quadratic and Twisted Edwards Curves

The classic non-interactive Diffie-Hellman algorithm is based on the use of two public keys. The same task of forming a shared secret can be solved in a protocol with one transmission session and one public key of the recipient, which is more secure. To do this, Alice generates a shared secret, encrypts it with Bob's public key, and sends him the encrypted key (the encapsulation key). Bob decrypts it with his private key. This protocol is called key encapsulation.

Based on CSIDH, we propose its modification—the Commutative Supersingular Isogeny: Key Encapsulation (CSIKE) algorithm, which, like [4, 5], includes three stages:

1. *Key generation.* Alice, using a random number generator, finds a secret vector $\Omega_\kappa = (e_1, e_2, \ldots, e_K)$, builds an isogenic map $\Theta_\kappa = [l_1^{e_1}, l_2^{e_2}, \ldots, l_K^{e_K}]$ and calculates an isogenic curve $E_\kappa = \Theta_\kappa * E_0$ whose parameter d is taken as $d = \kappa$.

2. *Key encapsulation.* This is the procedure for Alice to encrypt a key with Bob's public key E_B. To do this, Alice computes an isogenic curve $\Theta_\kappa * E_B = E_{\kappa B}$. The parameter $d_{\kappa B}$ of this curve as an encrypted key is sent to Bob.

3. *Key decapsulation.* Bob's decryption of the curve $E_{\kappa B}$ with his secret key Ω_B is reduced to his calculation of the isogenic curve $\overline{\Theta_B} * E_{\kappa B} = E_\kappa$, where the inverse function $\overline{\Theta_B}$ is constructed by inverting all signs of the exponent of Bob's secret key: $\Omega_B \rightarrow (-\Omega_B)$.

Consider a simple implementation model of the CSIKE algorithm on quadratic and twisted SEC that form pairs of quadratic twist with the same order $p + 1$. Such curves exist only for $p \equiv -1 \bmod 8$ and have order $N_E = N_E{}^t = p + 1 = cn$ (n is odd), $c \equiv 0 \bmod 8$.

Let such a pair of curves contain points of prime order 3, 5, 7, 11, then $n = 1155$, the minimum prime $p = 8n - 1 = 9239$ and the order of these curves $N_E = 8n = 9240$. The number of supersingular curves at a rough estimate $2\sqrt{p}$ in this model is close to 200; therefore, the parameters of all such curves and their exact number are assumed to be unknown. Unlike previous models [9–11], which use precomputation and tabulation of the parameters of isogenic chains on a period, in this paper we proceed only from the known starting curve E_0 and Algorithm 1, which brings the model closer to

a real cryptosystem. As a starting curve E_0, we can take the Edwards curve (3) for $d = 2$ which is supersingular with J-invariant $J = 66^3$ [18]. Let us pose the problem of calculating isogeny chains at stage 1 of the CSIKE algorithm.

Let's take the secret key vector $\Omega_\kappa = (4,-3, -3,2)$, then the group action class function, respectively $\Theta_\kappa = [3^4,5^{-3},7^{-3},11^2)]$. According to this function, Alice calculates the secret key κ. For the starting curve, we take $E_d^{(0)} = E_2$, then $E_\kappa = E_2{*}\Theta_\kappa$. In our example, the length of the chain of isogenies, equal to the sum of the absolute values of the exponents, is 12. At each step, you can choose any of the 4 degrees of isogenies, then there are 2^{24} paths leading to one result. A result can be considered reliable if it is found in at least two ways.

If the calculations are carried out according to the function Θ_κ and algorithm 1 from left to right, first for curves $E_d^{(i)}$ ($e_k > 0$), then for curves $E_{-1,-d}^{(i)}$ ($e_k < 0$), it is possible to construct two chains of length 6 each.

Example 1. The starting curve is the SEC $E_d^{(0)}$, $d = 2$. Let us consider Alice's calculations at the first step according to Algorithm 1. For isogenies of degrees 3 and 11, we first need to find a random point $R33$ of the curve E_2 of order $n_0 = 3 \cdot 11 = 33$. According to Algorithm 1, we determine a random point $P = (503,2304)$ having the maximum order $4n$. By doubling twice, we obtain a point $R = 4P = (8779,5631)$ of order n. Next, we find a point $R33 = 35R = (5412,-3772)$ of the 33rd order. The kernel of the 3-isogeny is the point $Q3 = 11R33 = (-6153,3016)$ of the 3rd order. Finally, using formula (6), we determine the parameter of the isogenic curve $d^{(1)} = 5861$.

In order to simplify the notation in the algorithm for calculating an isogenic curve $E_\kappa = E_2{*}\Theta_\kappa$, 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. For the first chain of length 6 curves $E_d^{(i)}$ ($e_k > 0$), Alice's calculations can be written as

$$\frac{d^{(0)} = 2}{(3)} \xrightarrow{1} \frac{d^{(1)} = 5861}{(3)} \xrightarrow{1} \frac{7935}{(3)} \xrightarrow{1} \xrightarrow{1} \frac{7745}{(3)} \xrightarrow{1} \frac{4900}{(11)} \xrightarrow{1} \frac{393}{(11)} \xrightarrow{1} 4637 = d^{(6)}.$$

Here, under the value $d^{(i)}$ in brackets, we conditionally set the degree of isogeny, and above the arrow, the value a of parameter of the curve E_d or $E_{-1,-d}$.

Continuation of calculations for isogenic curves of degrees 5 and 7 gives the results

$$\frac{d^{(6)} = 4637}{(5)} \xrightarrow{-1} \frac{d^{(7)} = 259}{(5)} \xrightarrow{-1} \frac{6813}{(5)} \xrightarrow{-1} \xrightarrow{-1} \frac{1941}{(7)} \xrightarrow{-1} \frac{7805}{(7)} \xrightarrow{-1} \frac{5308}{(7)} \xrightarrow{-1} 443 = d^{(12)}.$$

So, the secret key shared with Bob, calculated by Alice, is $\kappa = 443$. By changing the order of the degrees of isogenies from the highest to the lowest (in the same class of curves), we obtain the second path of the chain with the results

$$\frac{d^{(0)} = 2}{(11)} \xrightarrow{1} \frac{7327}{(11)} \xrightarrow{1} \frac{50}{(3)} \xrightarrow{1} \xrightarrow{1} \frac{8935}{(3)} \xrightarrow{1} \frac{4647}{(3)} \xrightarrow{1} \frac{8262}{(3)} \xrightarrow{1} 4637 = d^{(6)},$$

$$\frac{d^{(6)} = 4637}{(7)} \xrightarrow{-1} \frac{3376}{(7)} \xrightarrow{-1} \frac{4550}{(7)} \xrightarrow{-1} \xrightarrow{-1} \frac{445}{(5)} \xrightarrow{-1} \frac{2431}{(5)} \xrightarrow{-1} \frac{3880}{(5)} \xrightarrow{-1} 443 = d^{(12)}.$$

It can be seen that only the parameters $d^{(0)}d^{(12)}$, and $d^{(6)} = 4637$, coincide on the first and second calculation paths. The last result is explained by the fact that it completes a chain of length 6 for all curves $E_d^{(i)}$ ($e_k > 0$) and is the same when the degrees of 3- and 11-isogenies are interchanged. However, such a collision event reduces the security of the CSIDH and CSIKE algorithms. We propose an approach free from this shortcoming [11].

5. Randomization of the CSIKE Algorithm

The CSIDH algorithm proposed by the authors of [1] (Algorithm 1 in Section 3) is constructed in such a way that the calculations of isogenic chains according to functions $\Theta_{A,B} = [l_1^{e_1}, l_2^{e_2}, \dots, l_K^{e_K}]$ are performed in two stages: first, a set S with key exponents e_k of one sign is formed, then another. At each stage, the kernels and parameters of exactly $|e_k|$ isogenic curves of isogenies of degrees l_k constructed on curves of the same class (E_d or $E_{-1,-d}$) are successively calculated. This obviously gives rise to the threat of a side channel attack based on the measurement of the time of these calculations, proportional to the length $|e_k|$ and degree l_k of each chain. In this regard, in a large number of articles on this topic, various variants of "constant time CSIDH" are considered, in which the secret exponents e_k are increased to the

upper bound m by fictitious chains of isogenies. It is clear that such protection is achieved by significant redundancy and algorithm slowdown.

In [11], we proposed an alternative approach to solving the problem—randomization of the path of isogenic chains. Along with counteracting side channel attacks, this method makes it possible to practically avoid the collisions described in the final part of Section 4. The idea is that any random coordinate x of an elliptic curve always generates a random point $P = (x,y)$ of one of the two curves E_d or $E_{-1,-d}$ a pair of quadratic twist. Then one can avoid fruitless attempts to find a point of a curve of a given class and immediately determine the class of the curve and the y-coordinate of a point $P = (x,y)$ of this class. 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 of the exponent e_k 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 $d^{(1)}$ value, 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.

Some estimates of the probability of a successful time attack by an analyst who calculates the secret exponents e_k of isogenic chains of degree l_k are given in [11]. Below we provide Algorithm 2 of CSIKE (CSIDH) Randomized Implementation.

Randomized algorithm 2: Evaluating the class-group action on quadratic and twisted SEC.

Input: $d_A \in E_A$, $\chi(d) = 1$ *and a list of integers* $\Omega_A = (e_1, e_2, \ldots, e_K)$.
Output: d_B *such that* $[l_1^{e_1}, l_2^{e_2}, \ldots, l_K^{e_K}]*E_A = E_B$, *where* $E_{A,B}$: $x^2 + ay^2 = 1 + ad_{A,B}x^2y^2$.

1. *Let* $S_0 = \{k \mid e_k > 0\}$, $S_1 = \{k \mid e_k < 0\}$, $n_0 = \prod_{k \in S_0} l_k$, $n_1 = \prod_{k \in S_1} l_k$,
2. **While** *some* $e_k \neq 0$ **do**
3. *Sample a random* $x \in F_p$,
4. *Set* $a \leftarrow 1$, $\lambda \leftarrow 0$, E_A: $x^2 + y^2 = 1 + d_Ax^2y^2$ **if** $\chi((x^2 - 1)/(dx^2 - 1)) = 1$,
5. **Else** $a \leftarrow -1$, $\lambda \leftarrow 1$, 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* $R \leftarrow [(p + 1)/2n_\lambda]P$,
8. *Sample a random* $l_k \mid k \in S_\lambda$,
9. *Compute* $Q \leftarrow [n_\lambda/l_k]R$
10. **If** $Q \neq (1,0)$ *compute kernel G of* l_k*-isogeny* ϕ: $E_A \rightarrow E_B$,
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* S_λ *and set* $n_\lambda \leftarrow n_\lambda/l_k$ if $e_k = 0$,
14. **Return** d_A.

This algorithm has two important differences from Algorithm 1. Firstly, we do not divide the calculation of isogenies into two stages with curves of one class, then another ($a \leftarrow -a$), but build a random sequence $\{\lambda\}$ with an equiprobable choice of curves E_d or $E_{-1,-d}$, at each step. Together with the twofold acceleration of the procedure for selecting curves, this deprives the analyst of the possibility of orderly construction of two subsets S_0,S_1 of isogeny degrees. 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, which are inserted at random times. This inevitably complicates the task of measuring the computation time according to the function $[l_k^{e_k}]$. A rough lower bound for the number of paths of isogenic chains for the data of [1] is 2^{1300}.

Secondly, as in [11], in Algorithm 2 (section 12) we refuse to calculate the isogenic function $\phi(R)$, which 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 chain of isogenies $E \rightarrow E'$, it is only necessary to calculate the parameter $d' = \psi(d,Q)$ based on the parameter d and the kernel $<Q>$ of the domain E. This calculation involves two scalar multiplications SM of odd-order n_λ 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 and CSIKE algorithms. A significant part of the calculations in Algorithm 1 related to the calculation of the function $\phi(R)$ can be saved.

At the beginning of Algorithm 2, two subsets $S_\lambda, \lambda = 0,1$ are formed with degree numbers l_k, 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 step 7 of the algorithm, a point $R = 4n_1P$ of odd order n_0 is calculated for the curve E_d, and a point $R = 4n_0P$ of odd order n_1 is calculated for the curve $E_{-1,-d}$. As in Algorithm 1, this minimizes the cost of the next scalar multiplication that determines the degree l_k isogeny kernel point Q (Item 9). Further, in step 10 of the algorithm, the $(l_k - 1)/2$ coordinates of the points of the kernel $<Q>$ are calculated by doubling the points.

Example 2. To illustrate the randomization method based on the data of Example 1, let's give an example of Alice calculating the secret key κ, as well as its encapsulation with Bob's public key and Bob's decapsulation of the encrypted key in the randomized CSIKE algorithm (Algorithm 2).

In order for the reader to be able to check the calculations of the first stage, we have summarized their key results in Table 1. In its upper half we write the results for the first six isogenic curves ($i = 1..6$), and in the lower half for the rest ($i = 7..12$).

The first line of the table specifies the number i of the isogenic curve, then given the coordinates of a random point P, a point R of odd order, its order, the degree l of isogeny, the coordinates of the point Ql of the kernel, the parameters α_1, α_2, …, α_s of the kernel points and, finally, the parameter $d^{(i)}$ calculated by the formula (6).

We note right away that in this example we practically do not change the x-coordinates of the point P, and the choice of the curve E_d or $E_{-1,-d}$ at each step is due to a change in the flow parameter $d^{(i)}$. For $i = 8$ and $x = 100$, the order of the point R turned out to be 11, and this degree of isogeny has been exhausted by previous calculations. We took $x = 101$ and continued the calculations until the final step $i = 12$. Here, the curve $E_{-1,-d}$ with 5-isogeny is found at $x = 104$. The number of degrees of freedom at the end of the calculations naturally decreases. Random points R with small probabilities L_k/n may not have the maximum order n, which sometimes leads to a return to the beginning of the cycle.

Table 1

Results of calculating the parameters $d^{(i)}$ of a chain of isogenies of length 12 at p = 9239 based on Algorithm 2 and the function $\Theta_\kappa = (3^4, 5^{-3}, 7^{-3}, 11^2)$

i	**1**	**2**	**3**	**4**	**5**	**6**
P	(100,8575)	(100,1188)	(100,6058)	(100,36)	(100,8756)	(100,6475)
R=4P	(2355,3000)	(7437,8394)	(1314,6857)	(1999,6221)	(5518,5326)	(6757,8503)
OrdR	3*7*11	5*7*11	5*11	3*5*7*11	3*5*7*11	3*5*7*11
l	7	11	11	3	5	3
R	(3765,1727)	(79,5609)	(3770,1401)	(6068,2793)	(8212,2432)	(–500,8513)
α_1	3765	79	3770	–3171	8212	–500
α_2	4218	2380	–1364	—	2592	—
α_3	4670	387	8468	—	—	—
α_4	—	–7876	–7225	—	—	—
α_5	—	–33	–8620	—	—	—
$d^{(i)}$	**5135**	**8326**	**35**	**2590**	**8588**	**3466**
i	**7**	**8**	**9**	**10**	**11**	**12**
P	(100,8968)	(101,8248)	(101,6278)	(101,5375)	(101,401)	(104,6408)
R=4P	(1283,6372)	(6731,5854)	(8362,524)	(-943,4106)	3690,6330)	(7842,6474)
OrdR	3*5*7*11	3*5*7*11	3*5*7*11	3*5*7*11	3*5*7*11	3*5*7*11
l	3	7	7	3	5	5
Ql	(1442,6713)	(407,556)	(5751,3010)	(–885,2008)	(1072,2627)	(6577,715)
α_1	1442	407	5751	–885	1072	6577
α_2	—	–2358	1789	—	8878	8979
α_3	—	–398	–550	—	—	—
$d^{(i)}$	**7327**	**8326**	**389**	**2431**	**3880**	**443**

According to the results of calculations in Table 1, Alice determines the secret key $\kappa = 443$.

With a random choice of the x-coordinate of the point P, another chain of isogenies was defined with parameters $d^{(i)}$

$$\underset{(3)}{d^{(0)} = 2} \overset{1}{\to} \underset{(5)}{5861} \overset{-1}{\to} \underset{(7)}{1919} \overset{-1}{\to} \overset{-1}{\to} \underset{(11)}{2992} \overset{1}{\to} \underset{(7)}{2755} \overset{-1}{\to} \underset{(7)}{3880} \overset{-1}{\to} 6365 = d^{(6)},$$

$$\underset{(11)}{d^{(6)} = 6365} \overset{1}{\to} \underset{(3)}{4684} \overset{1}{\to} \underset{(5)}{5734} \overset{-1}{\to} \overset{-1}{\to} \underset{(3)}{7113} \overset{1}{\to} \underset{(5)}{623} \overset{1}{\to} \underset{(3)}{1507} \overset{-1}{\to} 443 = d^{(12)} = \kappa.$$

This secret key $\kappa = 443$ is the same as the result of the previous section and Table 1. Randomizing the choice of curves essentially randomly splits the key exponents Ω_κ and introduces significant uncertainty into the side channel attack problem.

Consider next the stages of encapsulation and decapsulation. Let Bob's secret key be $\Omega_B = (3,–2,2,–3)$, and the class group action, respectively, be $\Theta_B = [3^3,5^{-2},7^2,11^{-3}]$. Then he calculates his public key of one of the possible isogeny chains of length 10

$$\underset{(5)}{d^{(0)} = 2} \overset{-1}{\to} \underset{(3)}{2723} \overset{1}{\to} \underset{(3)}{1919} \overset{1}{\to} \overset{1}{\to} \underset{(3)}{7971} \overset{1}{\to} \underset{(11)}{4014} \overset{-1}{\to} \underset{(5)}{5164} \overset{-1}{\to} 6482 = d^{(6)},$$

$$\underset{(7)}{d^{(6)} = 6482} \overset{1}{\to} \underset{(11)}{393} \overset{-1}{\to} \overset{-1}{\to} \underset{(7)}{4900} \overset{1}{\to} \underset{(11)}{1821} \overset{-1}{\to} 2504 = d^{(10)}.$$

Bob thus has a public key $d_B = 2504$. Knowing it, Alice encrypts it at the encapsulation step using the secret function of the group action class. $\Theta_\kappa = [3^4,5^{-3},7^{-3},11^2]$. To do this, she calculates an isogenic curve $\Theta_\kappa * E_B = E_{\kappa B}$. Her calculations yield an encrypted encapsulation key

$$\underset{(3)}{d_B = 2504} \overset{1}{\to} \underset{(7)}{3276} \overset{-1}{\to} \underset{(5)}{7327} \overset{-1}{\to} \overset{-1}{\to} \underset{(7)}{6250} \overset{-1}{\to} \underset{(11)}{1787} \overset{1}{\to} \underset{(3)}{667} \overset{-1}{\to} 9033 = d^{(6)},$$

$$\underset{(11)}{d^{(6)} = 9033} \overset{1}{\to} \underset{(3)}{833} \overset{1}{\to} \underset{(5)}{894} \overset{-1}{\to} \overset{-1}{\to} \underset{(3)}{6661} \overset{1}{\to} \underset{(5)}{6163} \overset{-1}{\to} \underset{(3)}{5881} \overset{1}{\to} 5154 = d^{(12)}.$$

This key $d_{\kappa B} = 5154$ is sent to Bob. To decapsulate $d_{\kappa B}$, Bob uses his reverse secret key $\overline{\Theta_B} = [3^{-3},5^2,7^{-2},11^3]$. He calculates $\overline{\Theta_B} * E_{\kappa B}$ and obtain

$$\underset{(5)}{d_{\kappa B} = 5154} \overset{1}{\to} \underset{(7)}{667} \overset{-1}{\to} \underset{(7)}{9033} \overset{-1}{\to} \overset{-1}{\to} \underset{(3)}{3282} \overset{-1}{\to} \underset{(3)}{7190} \overset{-1}{\to} \underset{(11)}{6813} \overset{1}{\to} 8001 = d^{(6)},$$

$$\underset{(3)}{d^{(6)} = 8001} \overset{-1}{\to} \underset{(11)}{583} \overset{1}{\to} \overset{1}{\to} \underset{(5)}{5734} \overset{1}{\to} \underset{(11)}{8704} \overset{1}{\to} 443 = d^{(10)}.$$

As a result, both parties have a common secret key $\kappa = 443$ to work in a symmetric cryptosystem. The security level of the algorithm is evaluated similarly to CSIDH [1], but under the conditions of an attack with a known one public key instead of two.

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 $4n$ than points of odd order n. For the latter, in turn, the choice of a point of order that divides n is unlikely.

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

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

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

Excluding points of small even orders, and singular points ($(xy \neq 0)$, $(dx^2 \neq 1)$, $(dy^2 \neq –1)$), the choice of a random element $x \in F_d$ 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.

The results of the implementation of the Edwards-CSIDH model [12] 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 [12] is built on complete Edwards curves with order $N_E = p + 1$ (n is odd). Based on theorems [8] and the randomization method [11], in this paper we have shown how to implement a simple CSIKE model on non-cyclic quadratic and twisted SKEs that form quadratic twist pairs. The advantage of these classes of Edwards curves over the complete ones

at fixed p 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 quadratic twist complete curve.

6. Conclusions

The paper presents the original PQC CSIKE algorithm, which implements a scheme for encrypting a shared secret with a single public key of the recipient. The algorithm, in contrast to the well-known KEM scheme [2, 3], does not use the ElGamal encryption scheme, but is built as a modification of CSIDH using the recipient's reverse secret key. Such an implementation is undoubtedly much faster than the KEM scheme. An illustration of CSIKE operation on a model with isogenies of degrees 3, 5, 7, and 11 at and order $N_E = 9240$ of SEC is given. In the absence of precalculation of the SEC parameters d (they were used in previous works [9–11]), all isogenic curves were calculated from the starting curve E_d with the parameter [19].

7. References

[1] W. Castryck, et al., CSIDH: An efficient Post-Quantum Commutative Group Action. in Advances in Cryptology, ASIACRYPT, 2018.

[2] H. Onuki, et al., A Faster Constant-time Algorithm of CSIDH keeping Two Points. ASIACRYPT, 2020.

[3] A. Jalali, et al., Towards Optimized and Constant-Time CSIDH on Embedded Devices, IACR Cryptology ePrint Archive 2019/297.

[4] M. Qi, An Efficient Post-Quantum KEM from CSIDH, Journal of Mathematical Cryptology, 16, 2022, pp. 103–113. doi: 10.1515/jmc-2022-0007.

[5] K. Yoneyama, Post-Quantum Variants of ISO/IEC Standards: Compact Chosen Ciphertext Secure Key Encapsulation Mechanism From Isogeny, in 5th ACM Workshop on Security Standardisation Research Workshop, 2019, p. 13–21.

[6] A. Bessalov, V. Sokolov, P. Skladannyi, Modeling of 3- and 5-Isogenies of Supersingular Edwards Curves, in 2nd International Workshop on Modern Machine Learning Technologies and Data Science, no. I, vol. 2631, 2020, pp. 30–39.

[7] A. Bessalov, et al., Analysis of 2-Isogeny Properties of Generalized Form Edwards Curves, in Workshop on Cyberse-curity Providing in Information and Telecommunication Systems, vol. 2746, 2020, pp. 1–13.

[8] A. Bessalov, et al., Computing of Odd Degree Isogenies on Supersingular Twisted Edwards Curves, CEUR Workshop Proceedings, vol. 2923, 2021, pp. 1–11.

[9] A. Bessalov, et al., Implementation of the CSIDH Algorithm Model on Supersingular Twisted and Quadratic Edwards Curves. CEUR Workshop Proceeding, vol. 3187, 2021, pp. 302–309.

[10] A. Bessalov V. How to Construct CSIDH on Quadratic and Twisted Edwards Curves. Cybersecurity: Education, Science, Technique, vol. 3, no. 15, 2022, pp. 148–163.

[11] A. Bessalov, L. Kovalchuk, S. Abramov, Randomization of CSIDH Algorithm on Quadratic and Twisted Edwards Curves, Cybersecurity: Education, Science, Technique, vol. 1, no. 17, 2022, pp. 128–144.

[12] S. Kim, et al., Optimized Method for Computing Odd-Degree Isogenies on Edwards Curves. Security and Communication Networks, 2019.

[13] D. Moody, D. Shumow, Analogues of Velus formulas for isogenies on alternate models of elliptic curves. Mathematics of Computation, vol. 85, no. 300, 2016, pp. 1929–1951.

[14] D. J. Bernstein, T. Lange, Faster Addition and Doubling on Elliptic Curves, in Advances in Cryptology—ASIACRYPT, Lect. Notes Comp. Sci., vol. 4833, 2007, pp. 29–50.

[15] D. J. Bernstein, et al., Twisted Edwards curves, in: AFRICACRYPT, vol. 5023, 2008, pp. 389–405.

[16] A. V. Bessalov, Elliptic Curves in Edwards form and Cryptography, Monograph, Kyiv, 2017.

[17] A. Bessalov, O. Tsygankova, Number of Curves in the Generalized Edwards form with Minimal even Cofactor of the Curve Order, Problems of Information Transmission, vol. 53, iss. 1, 2017, pp. 92–101. doi: 10.1134/S003294601701008213.

[18] A. Bessalov, L. Kovalchuk, Supersingular Twisted Edwards Curves Over Prime Fields, I. Supersingular Twisted Edwards Curves with j-Invariants Equal to Zero and 123,

Cybernetics and Systems Analysist, vol. 55, no. 3, 2019, pp. 347–353.
[19] A. Bessalov, L. Kovalchuk, Supersingular Twisted Edwards Curves over Prime Fields, II. Supersingular Twisted Edwards Curves with the j-Invariant Equal to 663, Cybernetics and Systems Analysist, vol. 55, no. 5, 2019, pp. 731–741.
[20] L. C. Washington, Elliptic Curves. Number Theory and Cryptography, 2nd ed., CRC Press, 2008.