Implementation of the CSIDH Algorithm Model on Supersingular Twisted and Quadratic Edwards Curves

Anatoly Bessalov[1], Volodymyr Sokolov[1], Pavlo Skladannyi[1], Natallia Mazur[1], and Dmytro Ageyev[1]

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

Abstract

The properties of twisted and quadratic supersingular Edwards curves forming pairs of quadratic torsion with the order $p + 1$ over the simple field F_p are considered. A modification of the CSIDH algorithm using the isogenies of these curves in replacement of the extended arithmetic's of the isogenies of curves in the Montgomery form is presented. The isogeny parameters of the CSIDH algorithm model are calculated and tabulated on the basis of the theorems proved in the previous work. The example of Alice's and Bob's calculations according to the non-interactive Diffy-Hellman circuit, illustrating the separation of their secrets, is considered. The use of the known projective $(W:Z)$-coordinates for the given classes of curves provides the fastest execution of the CSIDH algorithm to-date.

Keywords

Generalized Edwards form curve, complete Edwards curve, twisted Edwards curve, quadratic Edwards curve, curve order, point order, isomorphism, isogeny, w-coordinates, quadratic residue, quadratic non-residue.

1. Introduction

This article is a continuation of the previous work [1]. Problems of post-quantum cryptography (PQC) today are successfully solved by various algorithms, among which the most promising, in particular, are algorithms based on isogenies of supersingular elliptic curves (SEC) [2, 3]. An efficient alternative to the SIDH [2] (Supersingular Isogeny Diffi-Hellman) protocol is the CSIDH [3] (Commutative SIDH) algorithm with the minimum known key length. Instead of the extended field F_{p^2} in the SIDH, operations in the CSIDH are performed over a simple field F_p, which for the given F_p halves the length of field elements and key sizes.

The implementations of the SIDH and CSIDH algorithms were mainly based on the fast arithmetic of isogenies of curves in the Montgomery form. In [4] (2019), a new efficient method for calculating isogenies of odd degrees for Edwards curves based on the Farashahi-Hosseini *w*-coordinates [5] is proposed. This work, in turn, is based on Montgomery's method of differential addition of points and adapts it to Edwards curves. The optimization of the arithmetic of isogenies on Edwards curves in projective coordinates $(W:Z)$ in [4] significantly accelerated the algorithms of their previous work [6] and allowed the authors to obtain a 20% gain in the speed of operations compared to the implementation of the algorithm on the Montgomery curves.

Formulas for calculating isogenies of odd degrees of Edwards curves [7] also contain components of differential addition of points, which served as the basis for the method proposed in [4]. Calculations in classical projective coordinates, as our analysis showed for isogeny of small degrees [8], become much more complicated with increasing degree of isogeny and lose in cost to $(W:Z)$-coordinates.

Complete Edwards curves E_d with one parameter ($\chi(d) = -1$), defined in [9], have well-known advantages: maximum speed of exponentiation of a point, universality of the law of addition of points,

CPITS-II-2021: Cybersecurity Providing in Information and Telecommunication Systems, October 26, 2021, Kyiv, Ukraine
EMAIL: a.bessalov@kubg.edu.ua (A. Bessalov); v.sokolov@kubg.edu.ua (V. Sokolov); p.skladannyi@kubg.edu.ua (P. Skladannyi); n.mazur@kubg.edu.ua (N. Mazur); dmytro.aheiev@nure.ua (D. Ageyev)
ORCID: 0000-0002-6967-5001 (A. Bessalov); 0000-0002-9349-7946 (V. Sokolov); 0000-0002-7775-6039 (P. Skladannyi); 0000-0001-7671-8287 (N. Mazur); 0000-0002-2686-3854 (D. Ageyev)
© 2022 Copyright for this paper by its authors.
Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).
CEUR Workshop Proceedings (CEUR-WS.org)

CEUR-WS.org/Vol-3187/short10.pdf

affine coordinates of a neutral element of a group of points. The introduction of the 2nd parameter a of the curve $E_{a,d}$ in [10] expanded the class of curves in the Edwards form and gave rise, according to the classification adopted in [11, 12], to two new classes: twisted and quadratic Edwards curves. They form quadratic torsion pairs that are used in this article to implement the CSIDH algorithm.

The calculation of isogenies of odd degrees for complete and quadratic Edwards curves E_d is carried out by the formulas defined by Theorems 2–4 in [7]. In our previous work [1], we generalized theorems [7] to curves in the generalized Edwards form with two parameters a and d, which allowed us to apply in this article twisted and quadratic Edwards curves over the field F_p for the implementation of the CSIDH model.

Our analysis in this paper is based on the properties of twisted and quadratic Edwards curves connected as pairs of quadratic torsion [13, 14]. Supersingular curves of these classes with the same order $N_E = p + 1 = 2^m n$, $m \geq 3$ (n is odd) exist only at $p \equiv 3\text{mod}4$. The minimum even cofactor of the order of such curves is eight; then, for the CSIDH algorithm with odd $n=\prod_{i=1}^{K} l_i$, the modulus of the field F_p should be chosen as $p = 8n – 1$. In order to adapt the definitions for the arithmetic of isogenies of Edwards curves and curves in the Weierstrass form, we use a modified law of addition of points [11,12].

Section 1 gives a brief overview of the properties of twisted and quadratic supersingular Edwards curves [13–15]. **Section 2** discusses specific aspects of the implementation of the CSIDH algorithm model on twisted and quadratic Edwards curves, provides a modification of the algorithm [3], calculates and tabulates the parameters of isogenous curves of the model, gives an example of Alice's and Bob's calculations in the Diffie-Hellman secret sharing scheme. Aspects of the performance of model using (W:Z)-coordinates [4,1] are summarized.

2. Properties of Twisted and Quadratic Supersingular Edwards Curves

A number of general properties of Edwards curves were considered in the previous work [1]. Here we turn to the specific properties of the supersingular Edwards curves (SEC) [13, 14]. The elliptic curve in the generalized Edwards form [11] is determined by the equation

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

With the quadratic character $\chi(ad) = –1$, the curve (1) is isomorphic to the complete Edwards curve [9] with one parameter d

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

In case of $\chi(ad) = 1$, $\chi(a) = \chi(d) = 1$ the curve (1) is isomorphic to the Edwards quadratic curve [11]

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

Having, in contrast to (2), the parameter d, defined as the square. For both curves (2) and (3) usually take $a = 1$. In the work [10] the curve (3) together with the curve (2) are called the Edwards curves. The difference in the quadratic characters of these curves leads to their radically different properties [11, 12].

The twisted Edwards curve was defined in [11] as a special case of the curve (1) for $\chi(ad) = 1$, $\chi(a) = \chi(d) = –1$.

We define a pair of twisted and quadratic Edwards curves [11] as a pair of quadratic torsion with parameters $\chi(ad) = 1$, $a' = ca$, $d' = cd$, $\chi(c) = –1$. As the SEC exists only at $p \equiv 3\text{mod}4$ [11], then we can accept $c = –1$, $a' = –a = –1$, $d' = –d$, where a and d are quadratic curve parameters and, respectively, a',d'-twisted curve parameters. In other words, the transition from a quadratic to a twisted torsion curve and vice versa can be defined as $E_d = E_{1,d} \leftrightarrow E_{–1,–d}$. So the equation of the twisted SEC at $p \equiv 3\text{mod}4$ from (1) can be written as

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

The order N_E of the elliptic curve over the simple field F_p is defined based on the trace t of the characteristic Frobenius equation $t\varphi^2 + t\phi + p = 0$ as $N_E = p + 1 – t$. For the curve of the quadratic torsion E^t the respective order will be equal to $N'_E = p + 1 + t$. An elliptic curve is supersingular if and only if over any extension of a simple field F_p the trace of Frobenius equation is $t \equiv 0\text{mod}p$, where in $\varphi^2 = -p, \varphi = \pm\sqrt{-p}$ [14,15]. In other words, in the algebraic closure $\bar{F}_p$ a supersingular curve doesnot

contain the points of the order p. Over a simple field F_p such curve always has the order $N_E = p + 1$, and over any extension of this field $N_E \equiv 1 \bmod p$.

So, twisted and quadratic SEC as a pair of quadratic torsion have the same order $N_E = p + 1$, but a different structure. Except two points $(0,\pm 1)$ all their points do not coincide; therefore, isogenies of the same degrees have different kernels and are calculated independently. Both curves are non-cyclic with respect to the points of even order (they contain three points of the 2nd order, two of which are singular points. Both curves are $D_{1,2} = (\pm\sqrt{\frac{a}{d}}, \infty)$ [11]). Besides, the quadratic SEC contains two singular points of the 4th order $\pm F_1 = (\infty, \pm\frac{1}{\sqrt{d}})$. The presence of three points of the 2nd order limits to eight the minimum cofactor of the order $N_E = 8n$ (n is odd) of twisted and quadratic Edwards curves [11]. The maximum order of the points of these curves is $N_E / 2$. Points of even orders are not involved in the calculations of the CSIDH algorithm.

For the curve (1) J-invariant equals [13,15]

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

This parameter distinguishes between isogenous (with different J-invariants) and isomorphic (with equal J-invariants) curves. Since the J-invariant retains its value for all isomorphic curves and pairs of quadratic torsion [15], it is the same for a pair of twisted and quadratic SEC ($a = \pm 1$), therefore, in what follows we will use J-invariant $J(d)$. It is a useful tool both for finding supersingular curves and for constructing graphs of isogenous chains. One of the properties of the J-invariant $J(d)$ is

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

For the classes of SEC under consideration, the replacement $d \to d^{-1}$ gives an isomorphism, and for complete Edwards curves—quadratic torsion [16].

3. Modification of the CSIDH Algorithm on Twisted and Quadratic Edwards Curves

The PQC CSIDH (Commutative SIDH) algorithm was proposed by the authors [3] to solve the same key exchange problem (SIDH [2]), but on the basis of isogenous mappings of elliptic curves, on the whole, as additive Abelian groups. This mapping over a simple field F_p is defined as the class of group action and is commutative. In comparison with the well-known original CRS scheme (Couveignes (1997), Rostovtsev, Stolbunov (2004) on nonsupersingular curves, the use of isogenies of supersingular curves made it possible to dramatically speed up the algorithm and obtain the smallest known key size (512 bits in [3]).

Let the curve E of the order N_E contain points of small odd orders l_i, $i = 1,2,\ldots,K$. Then there is an isogenous curve E' of the same order N_E as the mapping of the degree l_i: $E \to E' = [l_i]*E$. The repetition of this operation e_i times will denote $\left[l_i^{e_i}\right] * E$. The exponents of isogenies $e_i \in Z$ determine the length of the chain of isogenies of l_i degree. In the work [3] an interval of exponential values $-m \le e_i \le m$, $m = 5$, $K = 74$ is adopted, which provides a security level of 128 bits when attacking a quantum computer. Negative values of the exponent e_i indicate a transition to a quadratic torsion curve.

The implementation of the CSIDH algorithm mainly uses Montgomery's fast arithmetic of elliptic curves $y^2 = x^3 + Cx^2 + x$, $C \neq \pm 2$, containing two points of the 4th order and, respectively, having the order $N_E = 4n$ (n is odd) [9]. In the work [4] the algorithm is built on complete SEC of the same order. In this work, for the first time, we propose to use in the CSIDH algorithm twisted and quadratic SEC, which have the same record-breaking speed performance indicators as the complete Edwards curves [11].

This possibility arises on the basis of the theorems we proved in [1]. With a minimum cofactor of eight, the order of twisted and quadratic SEC is $N_E = 8n$. Thus, for these classes of SEC with the order $N_E = 8n = p + 1, n = \prod_{i=1}^{K} l_i$ the field modulus in the CSIDH algorithm should be chosen as $p \equiv -1 \bmod 8$.

Diffie-Hellman non-interactive key exchange scheme includes the following stages [3]:

1. The choice of parameters. For small simple odd l_i. $n = \prod_{i=1}^{K} l_i$ is calculated, where the value K is determined by the safety level and the appropriate modulus of the field $p = 2^m \prod_{i=1}^{K} l_i - 1, m \geq 3$ and starting elliptical curve E_0 are selected.

2. Calculation of public keys. Alice with her private key $\Omega_A = (e_1, e_2, e_3, \ldots, e_K)$ constructs an isogenous function $a = [l_1^{e_1}, l_2^{e_2}, l_3^{e_3}, \ldots, l_K^{e_K}]$ and calculates an isogenous curve $E_A = a * E_0$ **as her public key.** Bob, with the secret key Ω_B and function b, performs the same calculations and gets his public key $E_B = b * E_0$**.** These curves are determined by their parameters up to isomorphism.

3. Key exchange. Here the protocol is similar to item two with the replacement $E_0 \longrightarrow E_B$ for Alice and $E_0 \longrightarrow E_A$ for Bob. Knowing Bob's public key, Alice calculates $E_{BA} = a * E_B = ab * E_0$**.**

Similar actions of Bob give the result $E_{AB} = b * E_A = ba * E_0$, which coincides with the first due to the commutativity of the group operation. The J-invariant of the curve (E_{BA}) is taken as the shared secret.

Below we present a modification of Alice's computation algorithm according to item 2 [3] using isogenies of twisted and quadratic 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 $E_{A,B}: \quad x^2 - y^2 = 1 - d_{A,B} x^2 y^2$,

1. **While** some $e_i \neq 0$ **do**
   2. Sample a random $x \in F$.
   3. Set $s \leftarrow 1$, E_A: $x^2 - y^2 = 1 - d_A x^2 y^2$, **if** $(x^2 - 1)/(1 - dx^2)$ is a square in F_p.
   4. **Else** $s \leftarrow -1$, E_A^t: $x^2 + y^2 = 1 + d_A x^2 y^2$.
   5. Let $S = \{i \mid se_i > 0\}$. If $S = \emptyset$ then start over to line 2 while $s \leftarrow -s$.
   6. Let $k = \prod_{i \in S} l_i$ and compute $R \leftarrow [(p + 1)/2k]P$, $P = (x,y)$.
   7. **For** each $i \in S$ **do**
      8. Compute $Q \leftarrow [k/l_i]R$.
      9. **If** $Q \neq (1,0)$, compute an isogeny φ: $E_A \rightarrow E_B$ with $\ker \varphi = Q$.
         10. Set $d_A \leftarrow d_B$, R $\leftarrow \varphi(R)$, $k \leftarrow k/l_i$, and finally $e_i \leftarrow e_i - s$.
11. **Return** d_A.

In comparison with Algorithm 2 in the work [3] in our algorithm 1, adapted to twisted and quadratic SEC, modifications were made:

1. The repeated selection of a random point (Item 5) is performed until it falls after the original curve E_A into the curve (E^t_A) of quadratic torsion ($y^2 \rightarrow -y^2$). The check of quadraticity y^2 in Item 3 is performed for the twisted Edwards curve equation (4).

2. The set S of indices of positive and negative exponentials $\{e_i\}$ is formed twice according to Item 5.

3. For twisted Edwards curve order $N_E = 8n = p + 1$ with the maximum order of the point $N_E / 2 = 4n$ to get the point of the order n it is enough to double a random point P twice. In item 6 this property is taken into account by decreasing one doubling in the point product. According to Item 10 for each l_i exactly e_i of isogenies is calculated until the exponent e_i is zeroed. Depending on its sign, isogenies are calculated in the twisted class ($e_i > 0$) or quadratic SEC class ($e_i < 0$).

The construction of isogenies of odd simple degrees for quadratic Edwards curves is based on the Theorem 2 [7], for the twisted Edwards curves—on the Theorem 1 [1]. In the last work, the formulas of mapping $\phi(P)$ for the curve (1), depending on two parameters a and d, are presented for the first time. They are formulated below.

Theorem 1 [1]. Let us $G = \{(1,0), \pm Q_1, \pm Q_2, \ldots, \pm Q_S,\}$ is subgroup of odd simple order $l = 2s + 1$ of the points $\pm Q_1 = (\alpha_i, \pm\beta_i)$ of the curve E_d over the field F_p.

We define

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

Then $\phi(x,y)$ is an l-isogeny with the kernel G from the curve $E_{a,d}$ into the curve $E_{a',d'}$ with parameters $a' = a^l$, $d' = A^8 d^l$, $A = \prod_{i=1}^{s} \alpha_i$, and the mapping function

$$\phi(x,y)=\left(\frac{x}{A^2}\prod_{i=1}^{s}\frac{(\alpha_i x)^2-a^2(\beta_i y)^2}{1-(d\alpha_i\beta_i xy)^2},\frac{y}{A^2}\prod_{i=1}^{s}\frac{(\alpha_i y)^2-(\beta_i x)^2}{1-(d\alpha_i\beta_i xy)^2}\right) \quad (6)$$

or

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

Its proof is given in [1].

Let's consider a simple model for the implementation of the CSIDH algorithm on twisted and quadratic SEC that form pairs of quadratic torsion with the same order. Such curves exist only at $p\equiv -1 \bmod 8$ and have the order $N_E = N^t_E = p + 1 = cn(n - odd)$, $c \equiv 0 \bmod 8$. Let such pair of curves contain the kernels of the 3rd and 5th order at the minimum value $n = 15$, then the minimal simple is $p = 239$ and the order of these curves is $N_E = 16n = 240$. The parameter d of the whole family of 118 quadratic Edwards curves can be taken as squares $d = r^2 \bmod p$, r=2..119. Of these, 30 pairs of quadratic and twisted SEC were found with parameters $a = \pm 1$ and ad. Let us denote a quadratic SEC as E_d and a twisted SEC (4) as $E_{-1,-d}$. Table 1 shows the values of parameters for pairs of quadratic and twisted SCEs. They are written as squares in ascending order $d = r^2 \bmod p$, r=5..119.

Table 1

Values of parameter d of quadratic and twisted SECs ($a = \pm 1$) at $p = 239$ and $N_E = 240$

25	64	121	196	50	183	5	10	87	176
24	153	11	110	48	187	120	193	27	160
213	44	2	201	61	3	206	192	80	62

For the 1st curve $E_{-1,-25} = E^{(0)}_{-1,-d}$ from Table 1 we can construct 3- and 5-isogenies and find chains of isogenous curves $E^{(i)}_{-1,-d}$, $i = 1,2,\ldots,\pi$, such as $E^{(\pi)}_{-1,-d} = E^{(0)}_{-1,-d}$. The parameter a of all isogenous twisted SEC can be fixed as quadratic non-deduction $a = -1$, because, according to theorem 1, $a^{(i+1)} = (a^{(i)})^l = -1$ for all odd degrees l.

The curve $E_{-1,-25}$ contains the point of the 3rd order $Q_1 = (149,64)$, then, according to Theorem 3 [7] $A = \prod_{k=1}^{s}\alpha_k = 149$, $A^8 = 8$, $d^{(1)} = A^8(d^{(0)})^3 = 3$. Calculated parameters $d^{(i)}$, $J(d^{(i)})$ of the chain of 3-isogenous curves with the start value $d = 25$ are given in the first half of Table 2. The period of the chain $\pi = 5$ divides the number of all twisted SEC, equal to 30. By setting a different start value d = 2 from Table 1, we can get another sequence of parameters $d^{(i)} \in \{2,61,62,193,5,2\}$ with period 5 with values from Table1. Parameters of the 2nd chain are given in the second half of Table 2. For 3-isogenies it is possible to calculate 3 tables similar to Table 2 with non-overlapping values $d^{(i)}$ of Table 1. The data in Table 2 are used for twisted SEC when constructing the function $[l_1^{e_1}, l_2^{e_2}]$, $l_1 = 3, e_1 > 0$.

With negative values of exponents $e_1 < 0$ the results of similar calculations for quadratic SEC with other kernels Q of the 3rd order are given in Table 3. We emphasize that in comparison with Table 2, the same values of the parameters $d^{(i)}$ on the period of the chain are run in reverse order here.

The kernel of the 5-isogeny on the curve $E_{-1,-25}$ is the subgroup of points of the 5th order $Q_1 = (\alpha_1,\beta_1) = (-95,28)$, $2Q_1 = Q_2 = (\alpha_2,\beta_2) = (-72,-119)$, $3Q_1 = -2Q_1 = (\alpha_2,-\beta_2)$, $4Q_1 = -Q_1 = (\alpha_1,-\beta_1)$, $5Q_1 = O = (1,0)$. It is unequivocally determined by the coordinates α_1,α_2 of two points and the equation (4). For each 5-isogenous curve we calculate $A^{(i)} = \alpha_1^{(i)}\alpha_2^{(i)}$, $d^{(i+1)} = (A^{(i)})^8(d^{(i)})^5$, $i = 0,1,\ldots$ The results of calculating the parameters of the chain of 5-isogenic twisted SCEs are given in Table 4.The period of this chain is $\pi = 15$ and we can construct one more similar table (up to cyclic shift) with the other half of parameters of Table 1. For quadratic SEC, the results of similar calculations are summarized in Table 5. The data from Tables 4, 5 are used for twisted , $(e_2 > 0)$ and quadratic SECs $(e_2 < 0)$ when constructing the function $[l_1^{e_1}, l_2^{e_2}]$, $l_2 = 5$.

Table 2

Values of parameters of 2 chains of 3-isogeneous twisted SECs ($a = -1$) at $p = 239$

i	0	1	2	3	4	5	0	1	2	3	4	5
$\alpha^{(i)}$	149	227	152	174	179	149	137	177	221	129	66	137
$\beta^{(i)}$	25	3	10	50	110	25	193	5	2	61	62	193
$J(d^{(i)})$	225	105	55	105	225	225	215	113	218	235	217	215

Table 3

Values of parameters of 2 chains of 3-isogeneous quadratic SECs ($a = 1$) at $p = 239$

i	0	1	2	3	4	5	0	1	2	3	4	5
$\alpha^{(i)}$	97	116	157	197	113	97	172	101	61	17	109	193
$\beta^{(i)}$	25	110	50	10	3	25	193	62	61	2	5	193
$J(d^{(i)})$	225	225	105	55	105	225	215	217	235	218	113	215

Table 4

Values of parameters of a chain of 5-isogeneous twisted SECs ($a = -1$) at $p = 239$

i	0	1	2	3	4	5	6	7
$\alpha_1^{(i)},\alpha_2$	–95,–72	69,–53	57,–8	103,–102	107,–34	118,184	25,221	41,187
$-d^{(i)}$	25	2	11	50	193	187	3	61
$J(d^{(i)})$	225	218	215	105	215	215	105	235
i	8	9	10	11	12	13	14	15
$\alpha_1^{(i)},\alpha_2$	103,151	79,148	51,108	171,196	13,193	136,193	191,231	144,167
$-d^{(i)}$	183	110	5	121	10	62	201	25
$J(d^{(i)})$	218	225	113	327	55	217	113	225

Table 5

Values of parameters of a chain of 5-isogeneous twisted SECs ($a = -1$) at $p = 239$

i	0	1	2	3	4	5	6	7
$\alpha_1^{(i)},\alpha_2$	84,204	4,236	82, 230	31,201	42,204	22,206	17,237	16,211
$-d^{(i)}$	25	201	62	10	121	5	110	183
$J(d^{(i)})$	225	113	217	55	327	113	225	218
i	8	9	10	11	12	13	14	15
$\alpha_1^{(i)},\alpha_2$	175,223	138,229	50,156	116,203	27,156	104,207	5,11	84,204
$-d^{(i)}$	61	3	187	193	50	11	2	25
$J(d^{(i)})$	235	105	215	215	105	215	218	225

We will accept private keys of exponential isogeny $\{e_i\}$ of Alice and Bob $\Omega_A = (1,-2)$, $\Omega_A = (-4,3)$, their isogenous functions, respectively, $a = [3^1, 5^{-2}], b = [3^{-4}, 5^3]$. Let`s calculate their public keys d_A,d_B. *As a start curve of the chain of isogenies* we accept the curve $E^{(0)} = E_{-1,-25}$. *Alice calculates* the parameters of 3-isogenous curves $E^{(i)}$: one 3- isogenous twisted SEC, two 5-isogenous quadratic SECs at random.

1. **Calculation from left to right.** From Table 2 at the first step we immediately get $d^{(0)} = 25 \rightarrow d^{(1)} = 3 \Longrightarrow E^{(1)} = E_{-1,-3}$. For calculation of 5-isogenous curves we pass to the class of quadratic torsion—to the quadratic curve $E^{(1)} = E_{1,3} = E_3$. According to Table 5 we get $d^{(1)} = 3 \rightarrow d^{(2)} = 187 \rightarrow d^{(3)} = 193 \Longrightarrow E_3 \rightarrow E_{187} \rightarrow E_{193} \Longrightarrow E^{(3)} = E_{193}$. Returning to the class of twisted SECs gives $E^{(3)} = E_{-1,-193}$. So Alice's public key is $d_A = 193$. The default for the twisted SEC class is $a_A = -1$.

2. **Calculation from right to left.** For this case, at first in the class of quadratic curves, Alice calculates two 5-isogenous quadratic curves from Table 5 $E_{25} \rightarrow E_{201} \rightarrow E_{62} \Longrightarrow E^{(2)} = E_{62}$. Then she goes to the twisted curve $E_{-1,-62}$ and calculates one 3-isogenous curve. From Table 2 we get the final result $E^{(2)} = E_{-1,-62} \rightarrow E^{(3)} = E_{-1,-193} \Longrightarrow d_A = 193$. This example illustrates the commutability of isogenous mappings in the CSIDH algorithm.

Bob's public key is calculated in the same way. At $e_1 = -4$ the first isogenous curve is the quadratic curve $E^{(4)} = E_3$ from Table 3. Calculation of the next three 5-isogenous twisted curves ($e_2 = 3$) in accordance with Table 4 gives the curve $E^{(7)} = E_B = E_{-1,-110}$ and the value of Bob's public key $d' = d^{(3)} = d_B = 110$. Calculations from right to left give the same result.

Further, in the secret sharing scheme, Alice knowing Bob's public key calculates the isogenous curve $E_{BA} = [3^1,5^{-2})*E_{-1,-110}$. From Table 2 for twisted SECs we get $d^{(0)} = 110 \to d^{(1)} = 25$, then from Table 5 for quadratic SECs is $d^{(1)} = 25 \to d^{(2)} = 201 \to d^{(3)} = 62$. As a result, $E_{BA} = E_{-1,-62} \Longrightarrow d_{BA} = 62$.

Calculations of Bob in the secret sharing $E_{AB} = [3^{-4},5^3)*E_{-1,-193}$. From Table 3 for quadratic SEC we get $d^{(0)} = 193 \to d^{(1)} = 62 \to d^{(2)} = 61 \to d^{(3)} = 2 \to d^{(4)} = 5$, then from Table 4 for twisted SECs is $d^{(4)} = 5 \to d^{(5)} = 121 \to d^{(6)} = 10 \to d^{(7)} = 62$. As a result, $E_{AB} = E_{BA} = E_{-1,-62} \Longrightarrow d_{AB} = 62$. Alice's and Bob's results are identical.

According to Algorithm 1, isogenous functions (7) with kernels of degrees l_i along with dot products of points can be effectively used to calculate points of corresponding simple orders in chains of isogenous curves.

The mapping (7) of the points $P = (x,y)$ of the curve $E_A = E_{-1,-25}$ with the kernel of 3-isogeny $G = \{(1,0),\pm Q = (149,\pm 64)\}$ has the form

$$\phi_3(x,y) = \frac{x}{A^2}\cdot\frac{x^2-a\beta^2}{1-d\beta^2x^2}\cdot\frac{y}{A^2}\cdot\frac{x^2-\alpha^2}{1+d\alpha^2x^2} = \left(\frac{x}{149^2}\cdot\frac{x^2+64^2}{1+25^2 64^2 x^2}, \frac{y}{149^2}\frac{x^2-149^2}{1-25^2 149^2 x^2}\right)$$

The point of maximum odd 15th order $P = (-44,-12)$ of the curve $E_{-1,-25}$ is mapped to the point $P' = (221,125)$ of the 5thorder of the curve $E_{-1,-3}$, the point of the 5th order $P = (144,28)$ is mapped to the point $P' = (25,183)$ of the 5th order, and the point of the 3rd order $P = (149,64)$ is mapped to the neutral element of the group—the point $P' = (1,0) = O$. As we see, the function $\phi_3(x,y)$ reduces the orders of points of the preimage that are multiples of three and does not change the orders of other points.

For the same curve $E_{-1,-25}$ with the kernel of the 5th order $G = \{(1,0),\pm Q_1 = (-95,\pm 28),\pm Q_2 = (-72,-119)\}$ of the 5th isogeny in the form (7) is written as

$$\phi_5(x,y) = \left(\frac{x}{A^2}\cdot\frac{x^2+28^2}{1+25^2 64^2 x^2}\cdot\frac{x^2-95^2}{1-25^2 95^2 x^2}, \frac{y}{A^2}\cdot\frac{x^2+119^2}{1+25^2 119^2 x^2}\cdot\frac{x^2-72^2}{1-25^2 72^2 x^2}\right), A^2 = (95\cdot 72)^2 = 155$$

The point of the 15th order $P = (-44,-12)$ of the curve $E_{-1,-25}$ is mapped into the point $P' = (-18,7)$ of the 3rd order of the curve $E'_{-1,-2}$. The point of the 3rd order $P = (149,64)$ is mapped into the point $P' = (-18,-7)$ of the 3rd order of isogenous curve, the point of the 5th order $P = (-95,28)$ is mapped into the point $P' = (1,0) = O$. Here the function $\phi_3(x,y)$ reduces the orders of the preimage points, which are multiples of 5, by 5 times, without changing the orders of other points.

Calculations of the isogenies of twisted and quadratic SEC in projective Farashahi-Hosseini coordinates [6] $(W:Z)$ with replacement $w(x,y) = dx^2y^2$ based on the method proposed in [4] were considered in the previous paper [1] using Theorems 1 and 2 proved there.

The results of the implementation of the Edwards-CSIDH model [4] in projective coordinates claim that it is faster than the Montgomery-CSIDH model in coordinates $(X:Z)$ by 20%.

We note that the Edwards-CSIDH model [4] is built on complete Edwards curves with the order $N_E = p + 1 = 4n$ (n is odd). On the basis of Theorems 1 and 2 [1] in this paper we have shown how to implement such a model on twisted and quadratic SEC forming pairs of quadratic torsion.

The advantage of these classes of curves over the complete Edwards curves is the absence of the laborious inversion of the parameter $d \to d^{-1}$, which is necessary in the transition to the complete curve of quadratic torsion. This only speeds up the execution of the algorithm. However, with the same maximum order of the point $4n$, the order of these curves $N_E = 8n$ is twice as large as compared to the complete ones, which is hardly significant.

4. Conclusions

It can be concluded that the method for calculating isogenies of odd degrees in coordinates $(W:Z)$, proposed in [4], using full and twisted supersingular Edwards curves, allows us to implement the fastest computations for today when constructing the PQC CSIDH protocol and the like. The theorems proved

in [1] open up classes of twisted and quadratic Edwards curves for their implementation. This article is the first to show such an implementation for a simple model of the CSIDH algorithm.

5. References

[1] Bessalov, A., Sokolov, V., Skladannyi, P., Zhyltsov, O. Computing of odd degree isogenies on supersingular twisted edwards curves. CEUR Workshop Proceedings, 2021, 2923, pp. 1–11.

[2] D.Jao, and L. de Feo, Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies, Post-Quantum Cryptography pp. 19–34 (2011).

[3] Castryck, W., Lange, T., Martindale, C., Panny, L., Renes, J.: CSIDH: An efficient post-quantum commutative group action. In: Peyrin, T., Galbraith, S. (eds.) Advances in Cryptology { ASIACRYPT 2018. pp. 395–427. Springer International Publishing, Cham (2018).

[4] Suhri Kim, Kisoon Yoon, Young-Ho Park, and Seokhie Hong. Optimized Method for Computing Odd-Degree Isogenies on Edwards Curves. Security and Communication Networks, 2019 (2019).

[5] Farashahi, R.R., Hosseini, S.G.: Differential addition on twisted Edwards curves. In: Pieprzyk, J., Suriadi, S. (eds.) Information Security and Privacy. pp. 366{378. Springer International Publishing, Cham (2017).

[6] Suhri Kim, Kisoon Yoon, Jihoon Kwon, Seokhie Hong, and Young-Ho Park Efficient Isogeny Computations on Twisted Edwards Curves Hindawi Security and Communication NetworksVolume.

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

[8] A. Bessalov, V. Sokolov, P. Skladannyi. Modeling of 3- and 5-Isogenies of Supersingular Edwards Curves // Proceedings of the 2nd International Workshop on Modern Machine Learning Technologies and Data Science (MoMLeT&DS'2020), June 2–3, 2020: abstracts. — No. I, vol. 2631. — Aachen : CEUR, 2020. — P. 30–39.

[9] Bernstein D.J., Lange T. Faster Addition and Doubling on Elliptic Curves // Advances in Cryptology—ASIACRYPT'2007 (Proc. 13th Int. Conf. on the Theory and Application of Cryptology and Information Security. Kuching, Malaysia. December 2–6, 2007. Lect. Notes Comp. Sci. V. 4833. Berlin: Springer, 2007. P. 29–50.

[10] Bernstein Daniel J. , Birkner Peter , Joye Marc , Lange Tanja, Peters Christiane. Twisted Edwards Curves.// IST Programme under Contract IST–2002–507932 ECRYPT,and in part by the National Science Foundation under grant ITR–0716498, 2008.

[11] Bessalov A.V. Elliptic curves in Edwards form and cryptography. Monograph. Polytechnic, Kyiv, 2017. 272p.

[12] Bessalov A.V., Tsygankova O.V. Number of curves in the generalized Edwards form with minimal even cofactor of the curve order. Problems of Information Transmission, Volume 53, Issue 1 (2017), p. 92–101. doi:10.1134/S0032946017010082

[13] Bessalov, A.V., Kovalchuk, L.V. Supersingular Twisted Edwards Curves Over Prime Fields. I. Supersingular Twisted Edwards Curves with j-Invariants Equal to Zero and 123. Cybernetics and Systems Analysist, 2019, 55(3), стр. 347–353.

[14] Bessalov, A.V., Kovalchuk, L.V.Supersingular Twisted Edwards Curves over Prime Fields. II. Supersingular Twisted Edwards Curves with the j-Invariant Equal to 663. Cybernetics and Systems Analysist, 2019, 55(5), стр. 731–741.

[15] Washington, L.C. Elliptic Curvres. Number Theory and Cryptography. Second Edition. CRC Press, 2008.

[16] A. Bessalov, et al., Analysis of 2-isogeny properties of generalized form Edwards curves, in: Proceedings of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems, July 7, 2020, vol. 2746, pp. 1–13.