Computing of Odd Degree Isogenies on Supersingular Twisted Edwards Curves

Anatoly Bessalov[a], Volodymyr Sokolov[a], Pavlo Skladannyi[a], and Oleksii Zhyltsov[a]

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

Abstract

An overview of the properties of three classes of curves in generalized Edwards form $E_{a,d}$ with two parameters is given. The known formulas for the odd degree isogenies on curves E_d with one parameter are generalized to all classes of curves in Edwards form, and Theorem 1 on the isogenic mapping of the points of these curves is proved. The analysis of the known effective method for computing isogenies in Farashahi-Hosseini *w*-coordinates, justified for the curve E_d, is given. Theorem 2 proves the applicability of this method to the class of twisted Edwards curves. Examples of 3- and 5-isogenies of twisted Edwards curves are given. Methods for bypassing the exceptional points of such curves in PQC cryptosystems like CSIDH are proposed.

Keywords

Generalized Edwards form curve, complete Edwards curve, twisted Edwards curve, quadratic Edwards curve, curve order, points order, isomorphism, isogeny, w-coordinate, quadratic residue, quadratic nonresidue.

1. Introduction

Recently, there has been significant progress in the prospects for post-quantum cryptography (PQC) on isogenies of supersingular elliptic curves. An effective alternative to the well-known Supersingular Isogeny Diffie-Hellman (SIDH) [1] protocol is the new faster algorithm with a very short key length—Commutative SIDH (CSIDH) [2]. It offers a non-interactive key exchange protocol based on Alice and Bob's secret keys. Instead of the extended field F_{p^2} in SIDH, operations in CSIDH are performed over a prime field F_p, which for the given p halves the length of the field elements and key sizes. Instead of the acyclic curve in SIDH with subgroups of 2^i and 3^k of higher orders in CSIDH, the elliptic curve contains cyclic subgroups of simple odd-order $l_1,l_2,..,l_{\max}$, where $l_{\max}$ is specified by the security level.

The implementation of SIDH and CSIDH algorithms was mainly based on the fastest arithmetic of isogenies of curves in Montgomery form or mixed arithmetic of curves in Montgomery and Edwards form. In [3], a new effective method for computing odd degree isogenies on Edwards curves based on Farashahi-Hosseini *w*-coordinates [4] was proposed. This work, in turn, is based on Montgomery's method of differential points addition and adapts it to Edwards curves. The formulae for computing of odd degree isogenies on Edwards curves [5] also contain components of differential points addition, which allowed in [3, 4] with the help of *w*-coordinates to align the speeds of performing the corresponding operations on the curves in the Montgomery and Edwards forms. The results of the implementation of the CSIDH algorithm on Edwards curves [3] are already ahead of the closest competitor.

To work of the authors [3] was preceded their article [6], in which, in particular, an efficient algorithm for computing 3-isogenies in projective coordinates was developed with the minimal computation cost for today. However, for 5-isogenies, as our analysis showed [7], computations in classical projective coordinates became almost three times more complicated. There are reasons to

Cybersecurity Providing in Information and Telecommunication Systems, January 28, 2021, Kyiv, Ukraine
EMAIL: a.bessalov@kubg.edu.ua (A.1); v.sokolov@kubg.edu.ua (A.2); p.skladannyi@kubg.edu.ua (A.3); o.zhyltsov@kubg.edu.ua (A.4)
ORCID: 0000-0002-6967-5001 (A.1); 0000-0002-9349-7946 (A.2); 0000-0002-7775-6039 (A.3); 0000-0002-7253-5990 (A.4)

consider the use of Farashahi-Hosseini w-coordinates and the method [3] as a method for optimal computation of odd degree isogenies on Edwards curves.

Complete Edwards curves E_d with one parameter d, defined in [8] ($\chi(d) = -1$), have well-known advantages: maximum exponentiation rate of a point, the universality of points addition law, affine coordinates of a neutral element of a group. The introduction of the second parameter a on the curve $E_{a,d}$ in [9] expanded the class of curves in the Edwards form and gave rise, according to the classification adopted in [10], to two new classes: twisted and quadratic Edwards curves. The last class, together with complete ones in terminology [9], is called Edwards curves E_d.

The computing of odd degree isogenies on Edwards curves E_d is carried out using the formulas defined by Theorems 2–4 in [5]. Although Theorem 3 of this paper is formulated for normalized Edwards curves $E_{a,d} \to E_{1,d/a}$, its existence condition for $\sqrt{a}$ is not satisfied in the class of twisted Edwards curves over a prime field F_p. In other words, isogenic mapping $E_{a,d} \to E'_{a,d}$ remained unknown for this class. One of the goals of this paper is to fill this gap and to prove Theorem 1 with a generalization of results known for curves E_d to curves $E_{a,d}$ over a prime field F_p.

Further, in the work [3], based on Farashahi-Hosseini w-coordinates, a method for computing of odd degree isogenies for Edwards curves E_d were developed and implemented, and Theorems were proved for isogenic mappings of these curves. But the question remained whether this method works in the existing conditions of twisted Edwards curves $E_{a,d}$. Theorem 2 in this article puts an end to this question as well.

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

Sect. 2 gives a brief overview of the properties of three classes of Edwards curves according to the classification [10]. In Sect. 3, we consider the properties of odd degree isogenies and prove Theorem 1 for a rational mapping $E_{a,d} \to E'_{a',d'}$ expressed by functions of two and one variables, and give examples of isogenies on twisted Edwards curves. In Sect. 4, based on Theorem 1, Theorem 2 is formulated and proved for the isogenic mapping of the curve $E_{a,d}$ in Farashahi-Hosseini w-coordinates. Estimates of the cost of computing isogenies in projective coordinates $(W:Z)$ [3] are given. Examples are considered for classes of quadratic and twisted Edwards curves and methods are proposed to bypass the exceptional points of the 2nd order on twisted Edwards curves.

2. Classes of Curves in the Generalized Edwards Form

The elliptic curve in the generalized Edwards form [10] is determined by the equation

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

In contrast to the equation of this curve in [9], here we multiply the parameter a by y^2 instead of x^2. With the quadratic character $\chi(ad) = -1$, the curve (1) is isomorphic to the complete Edwards curve [8] with one parameter d

$$E_d: x^2 + y^2 = 1 + dx^2y^2, \chi(d) = -1, d \neq 0,1. \quad (2)$$

In the case $\chi(a) = \chi(d) = 1$, there is an isomorphism of the curve (1) with quadratic Edwards curve [10]

$$E_d: x^2 + y^2 = 1 + dx^2y^2, \chi(d) = 1, d \neq 0,1, \quad (3)$$

which, in contrast to (2), has the parameter d defined as a square. This difference leads to radically different properties of curves (2) and (3) [10], which are summarized below. Despite this, in world literature, these classes of curves are often combined by the general term *Edwards curves* [9].

In our paper [13], we proposed to change places of x and y coordinates in the form (1) of the Edwards curve. The modified universal law of addition of the points of the curve (1) has the form:

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1x_2 - ay_1y_2}{1 - dx_1x_2y_1y_2}, \frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}\right). \quad (4)$$

If two points from (4) coincide, we have

$$2(x_1, y_1) = \left(\frac{x_1^2 - ay_1^2}{1 - dx_1^2y_1^2}, \frac{2x_1y_1}{1 + dx_1^2y_1^2}\right). \tag{5}$$

Determining the inverse point as $-P = (x_1, -y_1)$ we obtain according to (4) the coordinates of the neutral element $O = (1,0)$ of the group of points. In addition to the neutral element O, the axis X also always contains the point $D_0 = (-1,0)$ of the 2nd order, such that $2D_0 = (1,0) = O$. Depending on the properties of the parameters a and d, we can get two exceptional points of the 2nd order and two exceptional points of 4th order with the coordinates:

$$D_{1,2} = \left(\pm\sqrt{\frac{a}{d}}, \infty\right), \pm F_1 = \left(\infty, \pm\frac{1}{\sqrt{d}}\right), \tag{6}$$

where we put the sign ∞ when dividing by 0. They arise in the cases $\chi(ad) = 1$ and $\chi(d) = 1$, respectively.

Depending on the properties of the parameters a and d, the curves in the generalized Edwards form (1) are divided into 3 disjoint classes [10]:

- Complete Edwards curves with the conditions C1: $\chi(ad) = -1$.
- Twisted Edwards curves with the conditions C2.1: $\chi(a) = \chi(d) = -1$.
- Quadratic Edwards curves with the conditions C2.2: $\chi(a) = \chi(d) = 1$ [14–16].

Basic properties of curves of these classes:

1. For the points of the 2nd order, the class of complete Edwards curves over a prime field is the class of cyclic curves (with one point of the 2nd order), while twisted and quadratic Edwards curves form classes of acyclic curves (three points of the second-order each). The maximum order of points of curves of the two last classes is equal to ${}^{N_E}/_2$.
2. The class of complete Edwards curves does not contain exceptional points.
3. Twisted Edwards curves contain two exceptional points of the 2nd order $D_{1,2} = \left(\pm\sqrt{\frac{a}{d}}, \infty\right)$, and quadratic Edwards curves, besides them, contain two more exceptional points of the 4th order $\pm F_1 = \left(\infty, \pm\frac{1}{\sqrt{d}}\right)$.
4. Twisted and quadratic Edwards curves form quadratic twist pairs based on parameters transformations: $\tilde{a} = ca, \tilde{d} = cd, \chi(c) = -1$.
5. In the classes of twisted and quadratic Edwards curves, the replacement $a \leftrightarrow d$ gives the isomorphism of curves $E_{a,d} \sim E_{d,a}$.
6. Complete and quadratic Edwards curves are isomorphic to the curves with the parameter $a = 1$: $E_{a,d} \sim E_{1,d/a} = E_{\tilde{d}}$. The introduction of the new parameter a into the equation of the curve (1) is necessary only for the class of twisted Edwards curves.

For the curve (1) *J*-invariant is equal to [17]

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

This parameter distinguishes between isogenic (with different *J*-invariants) and isomorphic (with equal *J*-invariants) curves.

3. Odd Degree Isogenies on Twisted Edward Curves

The isogeny from the elliptic curve $E(K)$ over the field K to the curve $E'(K)$ is a homomorphism $\phi: E(K) \to E'(K)$ that is given by rational functions. This means that for all $P, Q \in E(K), \phi(P + Q) = \phi(P) + \phi(Q)$ and that there are rational functions [17]

$$\phi(x,y) = \left(\frac{p(x)}{q(x)}, y\frac{f(x)}{g(x)}\right) = (x', y'), \tag{7}$$

mapping the points of curve E to the points of the curve E'. The maximum of the degrees $l = \deg\phi(x,y) = \max\{\deg p(x), \deg q(x)\}$ is called the degree of isogeny and its kernel $\ker\phi = G$ is the subgroup $G \subseteq E$, the points of which are mapped by the function $\phi(x,y)$ into the neutral element O of the group E'. The degree of separable isogeny is equal to the order l of its kernel.

Isogeny compresses the set of the curve E points by a factor l (l points of the curve E are mapped to one point of the curve E'). At $G = O$ isogeny becomes the isomorphism with the degree 1.

The construction of odd degree isogenies on Edwards curves is based on Theorem 2 [5]. Let's formulate it taking into account the modification (4) of the points addition law of the curve (1) at $a = 1$.

Theorem 2 [5]. Let $G = \{(1,0), \pm Q_1, \pm Q_2, .., \pm Q_s\}$ the subgroup of odd order $l = 2s + 1$ of the points $\pm Q_i = (\alpha_i, \pm\beta_i)$ on the curve E_d.

We define

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

Then $\phi(x, y)$ is l-isogeny with the kernel G from the curve E_d to the curve $E'_{d'}$ with the parameter $d' = A^8 d^l$ and the mapping function

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

Its proof is given in [5]. Its important consequence is that isogenic curves are in the same classes as curves E_d (i.e., complete Edwards curves are mapped to complete curves, twisted curves—to twisted ones, and quadratic curves—to quadratic ones). This essentially distinguishes odd degree isogenies from 2-isogenies (for them, the complete Edwards curves are mapped to quadratic ones).

The formula (8) for the function $\phi(x, y)$ directly follows from the definition $\phi(P)$ in the statement of the Theorem and the addition law (4) for the arbitrary point $(x_P, y_P) = (x, y)$ with the kernel points $\pm Q_i = (\alpha_i, \pm\beta_i)$, so for coordinates pairs we have

$$\frac{x_{P+Q_i}}{x_{Q_i}} \frac{x_{P-Q_i}}{x_{-Q_i}} = \frac{1}{\alpha_i^2} \frac{(\alpha_i x)^2 - (\beta_i y)^2}{1 - (d\alpha_i\beta_i xy)^2}, \qquad \frac{y_{P+Q_i}}{y_{Q_i}} \frac{y_{P-Q_i}}{y_{-Q_i}} = \frac{1}{\alpha_i^2} \frac{(\alpha_i y)^2 - (\beta_i x)^2}{1 - (d\alpha_i\beta_i xy)^2}.$$

The factors x and y before the products in the coordinates of the function $\phi(x, y)$ take into account the neutral element $O = (1,0)$ of the isogeny kernel. It is obvious from (8) that the property $\phi(1,0) = (1,0)$ holds, i.e. the neutral element is mapped into itself. For all points of the kernel $\phi(\pm Q_i) = \phi(\alpha_i, \pm\beta_i) = (1,0)$ is also true.

Theorem 2[5] and the mapping (8) are valid only for the classes of complete and quadratic Edwards curves with the parameter $a = 1$. The authors of [5] further formulated and proved Theorem 3 for curves $E_{a,d}$ in the form (1), relying on the property of normalization of this curve with isomorphism $E_{a,d} \sim E_{1,d/a}$ with the change of the coordinate $y \to {}^{y}\!/_{\sqrt{a}}$. For the class of twisted Edwards curves ($\chi(a) = \chi(d) = -1$) over a prime field F_p such a change does not exist, and the results of Theorem 3[5] are applicable only for the curves E_d over the extended fields $F_{p^m}, m \geq 2$. For the PQC protocol SIDH [1] with implementation on the curves E_d over the fieldF_{p^2} Theorem 3 [5] may be useful. But for the CSIDH protocol [2] with curves over the field F_p, this theorem does not give results for the whole class of twisted Edwards curves. In this paper, we fill this gap and for the first time present mapping formulas $\phi(P)$ for the curve (1) that depends on two parameters a and d.

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

We define

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

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

$$\phi(x, y) = \left(\frac{x}{A^2} \prod_{i=1}^{s} \frac{(\alpha_i x)^2 - a^2(\beta_i y)^2}{1 - (d\alpha_i\beta_i xy)^2}, \frac{y}{A^2} \prod_{i=1}^{s} \frac{(\alpha_i y)^2 - (\beta_i x)^2}{1 - (d\alpha_i\beta_i xy)^2}\right), \tag{9}$$

or

$$\phi(x,y) = \left(\frac{x}{A^2}\prod_{i=1}^{s}\frac{x^2 - a\beta_i^2}{1 - d\beta_i x^2}, \frac{-y}{A^2}\prod_{i=1}^{s}\frac{x^2 - \alpha_i^2}{a - d\alpha_i x^2}\right). \tag{10}$$

Proof. The formula (9) follows directly from the definition $\phi(P)$ and the points addition law (4) of the curve (1).

From (1) it is true that $y^2 = (1 - x^2)/(a - dx^2), \alpha_i^2 + a\beta_i^2 = 1 + d\alpha_i^2\beta_i^2$. Then, in the numerator of the first coordinate x' in (9), each factor is transformed as:

$$U_i = \alpha_i^2 x^2 - \beta_i^2 y^2 = \alpha_i^2 x^2 - a^2\beta_i^2 \frac{1 - x^2}{a - dx^2} = \frac{a(\alpha_i^2 + a\beta_i^2)x^2 - a^2\beta_i^2 - d\alpha_i^2 x^4}{a - dx^2} =$$
$$= \frac{a(1 + d\alpha_i^2\beta_i^2)x^2 - a^2\beta_i^2 - d\alpha_i^2 x^4}{a - dx^2} = \frac{a(x^2 - a\beta_i^2) - d(\alpha_i^2 x^4 - \alpha_i^2\beta_i^2 x^2)}{a - dx^2} =$$
$$= \frac{(x^2 - a\beta_i^2)(a - d\alpha_i^2 x^2)}{a - dx^2}.$$

Similarly, we transform the factors of the common denominator of coordinates x' and y' into (9):

$$Z_i = 1 - (d\alpha_i\beta_i xy)^2 = 1 - d^2\alpha_i^2\beta_i^2 x^2 \frac{1 - x^2}{a - dx^2} = \frac{a - dx^2 - d^2\alpha_i^2\beta_i^2 x^2 + d^2\alpha_i^2\beta_i^2 x^4}{a - dx^2} =$$
$$= \frac{a - d(\alpha_i^2 + a\beta_i^2)x^2 + d^2\alpha_i^2\beta_i^2 x^4}{a - dx^2} = \frac{(1 - a\beta_i^2 x^2)(a - d\alpha_i^2 x^2)}{a - dx^2}.$$

After reducing the common factors for the x'-coordinate, we obtain

$$\frac{U_i}{Z_i} = \frac{(\alpha_i x)^2 - a^2(\beta_i y)^2}{1 - (d\alpha_i\beta_i xy)^2} = \frac{x^2 - a\beta_i^2}{1 - d\beta_i^2 x^2}.$$

The second coordinate y' in (9) as factors in the numerator

$$V_i = (\alpha_i y)^2 - (\beta_i x)^2 = \frac{\alpha_i^2(1 - x^2) - \beta_i^2 x^2(a - dx^2)}{a - dx^2} =$$
$$= \frac{-x^2(\alpha_i^2 + a\beta_i^2 x^2) + d\beta_i^2 x^4 + \alpha_i^2}{a - dx^2} = \frac{-x^2(1 + d\alpha_i^2\beta_i^2) + d\beta_i^2 x^4 + \alpha_i^2}{a - dx^2} =$$
$$= \frac{-(x^2 - \alpha_i^2)(1 - d\beta_i^2 x^2)}{a - dx^2}.$$

Then

$$\frac{V_i}{Z_i} = \frac{(\alpha_i y)^2 - (\beta_i x)^2}{1 - (d\alpha_i\beta_i xy)^2} = -\frac{x^2 - \alpha_i^2}{a - d\alpha_i^2 x^2}.$$

As a result, the function (9) can be written in the equivalent form (10)

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

depending on the parameters a and d. Formulas for the parameters of the isogenic curve $a' = a^l, d' = A^8 d^l, A = \prod_{i=1}^{s}\alpha_i$ are proved in Theorem 3 [5]. The theorem is proved.

For the curves E_d with the parameter $a = 1$ the formula (10) is given in Theorem 4 [5]. In this paper, we generalized it for the curves $E_{a,d}$ (1) with the arbitrary value $a \neq d$, which allows us to compute the isogenies of twisted Edwards curves ($\chi(a) = \chi(d) = -1$).

Let's note that the rational function (10) corresponds to the classical form (7). Its obvious advantage over (9) is its simplicity and minimal computational complexity in affine coordinates. Also, the degree of isogeny as the maximum degree of the polynomial $p(x)$ in (7) is immediately defined as $l = 2s + 1$. The form (1) of the Edwards curve with the addition law (4) adapts it to the definitions of isogenies in the Weierstrass form [17].

Let's consider examples of isogenies of the supersingular twisted Edwards curve (STEC). Such curves exist only at $p \equiv -1 \bmod 8$ and have the order $N_E = p + 1 \in \{8n, 16n, \ldots\}$ (n is odd). The curve, for example, contains kernels of the 3rd and 5th order at the smallest value $n = 15$, then the minimum prime number is $p = 239$ and the order of such curve is $N_E = 16n = 240$. The parameters of the entire family of 118 twisted Edwards curves can be taken as quadratic non-residues

$a = -1, d = -m^2 \bmod p, m = 2..119$. Of these, there are 30 STEC's with the parameters $(-d)$, given in Table 1. They are written as squares in ascending order $m = 5..118$.

Table 1
Values of the parameter $(-\boldsymbol{d})$ of STEC at $\boldsymbol{p} = \mathbf{239}$, $\boldsymbol{a} = -\mathbf{1}$, and $\boldsymbol{N_E} = \mathbf{240}$

25	64	121	196	50	183	4	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 first curve (1) $E_{-1,-25} = E_{a,d}^{(0)}$ from Table 1 we can construct 3- and 5-isogenies and find chains of isogenic curves $E_{-1,di}^{(i)}, i = 1,2, \ldots, \pi$ such that $E_{a,d}^{(\pi)} = E_{a,d}^{(0)}$. Then the chain of mappings $\phi^{(2)} \circ \phi^{(3)} \circ \ldots \circ \phi^{(\pi)}$ gives dual isogeny $E_{-1,d1}^{(1)} \rightarrow E_{-1,d0}^{(0)}$. The parameter a of all isogenic STEC's can be fixed as the quadratic non-residue $a = -1$, since according to Theorem 3 [5] $a^{(i+1)} = \left(a^{(i)}\right)^l = -1$ 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[5], $A = \prod_{k=1}^{s} \alpha_k = 149, A^8 = 8, d^{(1)} = A^8 (d^{(0)})^3 = A^8 d^3 = -3$. The calculated parameters $-d^{(i)}, J(d^{(i)})$ of the chain of 3-isogenous curves with the starting value $d = -25$ are given in Table 2. The period of the chain $\pi = 5$ divides the number of all STEC's equal to 30. Specifying the starting value $d = -2$ not included in Table 2, it is possible to obtain a different sequence $-d^{(i)} \in \{2,61,62,193,5,2\}$ with period 5 with the elements from Table 1 for all STEC's. For 3-isogenies, we can calculate 6 tables similar to Table 2 with disjoint values $-d^{(i)}$ Table 1. We note that all *J*-invariants $J(d^{(i)})$ of adjacent 3-isogenic curves (except the last pair) are different, i.e. they are not isomorphic. However, inside the chain, there may be isomorphic curves with equal *J*-invariants.

The kernel of 5-isogeny on the curve $E_{-1,-25}$ is the subgroup of points of the 5th order $\pm Q_1 = (\alpha_1, \pm\beta_1) = (-95, \pm 28)$, $\pm Q_2 = (\alpha_2, \pm\beta_2) = (-72, \pm 119)$, and $5Q_1 = O = (1,0)$. It is uniquely determined by the coordinates α_1, α_2 of two points and equation (1). Then for each 5-isogenic curve, we compute $A^{(i)} = \alpha_1^{(i)} \alpha_2^{(i)}, d^{(i+1)} = \left(A^{(i)}\right)^8 \left(d^{(i)}\right)^5, i = 0,1, \ldots$. The results of calculations of the parameters of the chain of 5-isogenic curves are given in Table 3. The period of this chain is $\pi = 15$, so we can build one more similar table (up to a cyclic shift) with the other half of the parameters of Table 1. The data of Tables 2 and 3 are used to construct the graphs of isogenies.

Table 2
Values of parameters of the chain of 3-isogenous SSCE at $\boldsymbol{p} = \mathbf{239}$, $\boldsymbol{a} = -\mathbf{1}$

i	0	1	2	3	4	5
$\alpha^{(i)}$	149	227	152	174	179	149
$-d^{(i)}$	25	3	10	50	110	25
$J(d^{(i)})$	225	105	55	105	225	225

Table 3
Values of parameters of the chain of 5-isogenous SSCE at $\boldsymbol{p} = \mathbf{239}$, $\boldsymbol{a} = -\mathbf{1}$

i	0	1	2	3	4	5	6	7
$\alpha_1^{(i)}, \alpha_2^{(i)}$	–95,–72	69, −53	57,–8	103, −102	107,– 34	118, −55	25, −18	41, −52
$-d^{(i)}$	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
$\alpha_1^{(i)}, \alpha_2^{(i)}$	103, −88	79, −91	51,108	−68, −43	13, −	−103, −46	−48,−8	−93, −72
$-d^{(i)}$	183	110	5	121	10	62	201	25
$J(d^{(i)})$	218	225	113	327	55	217	113	225

The mapping (10) of the points $P=(x,y)$ of the curve $E_{-1,-25}$ with the kernel $G=\{(1,0),\pm Q_1=(-90,\pm 64)\}$ of 3-isogeny has the form:

$$\phi_3(x,y)=\left(\frac{x}{A^2}\frac{x^2-a\beta^2}{1-d\beta^2x^2},\frac{-y}{A^2}\frac{x^2-\alpha^2}{1+d\alpha^2x^2}\right)=$$
$$=\left(\frac{x}{90^2}\frac{x^2+64^2}{1+25^2 64^2x^2},\frac{-y}{90^2}\frac{x^2-90^2}{1-25^2 90^2x^2}\right).$$

The point of the maximum 120th order $P=(3{,}75)$ of the curve $E_{-1,-25}$ is mapped by this function to the point $P'=(-116{,}94)$ of the 40th order of the curve $E'_{-1,-3}$. The point of the maximum odd 15th order $P=(-44,-12)$ is mapped to the point $P'=(-18,-114)$ of the 5th order, the point $P=(-95{,}28)$ of the 5th order is mapped to the point $P'=(25,-66)$ of the 5th order, and the point $P=(-90{,}64)$ of the 3rd order is mapped to the point $P'=(1{,}0)=O$. As we can see, the function $\phi_3(x,y)$ reduces by 3 times the orders of the domain points, which are multiples of 3, and does not change the orders of the other points. In subgroups of orders multiples of 3, three points are mapped into one (surjection property).

For the same curve $E_{-1,-25}$ with the kernel of the 5th order $G=\{(1{,}0),\pm Q_1=(-95,\pm 28),\pm Q_2=(-72,\pm 119)\}$ 5-isogeny in the form (10) is written as

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

The point of the 120th order $P=(3{,}75)$ of the curve $E_{-1,-25}$ is mapped by this function to the point $P'=(-116{,}94)$ of the 24th order of the curve $E'_{-1,-2}$. The point $P=(8,-16)$ of the 30th order is mapped to the point $P'=(18,-7)$ of the 6th order. The point of the 5th order $P=(-95{,}28)$ is mapped to the point $P'=(1{,}0)=O$, Here, too, in subgroups of orders multiples of 5, five points are mapped into one.

4. The Computing of Isogenies on Supersingular Twisted Edwards Curves in Projective Coordinates of Farashai-Hosseini

Significant progress has been made in the efficiency of computing odd degree isogenies on Edwards curves in paper [3]. It is based on the idea of the method of differential addition (i.e., the addition of two points with the known difference) on the curve in the Farashahi-Hosseini projective coordinates [4]. Since the formulae of isogenies [5] contain the coordinates of the point pairs $P\pm Q$ as multipliers, it is possible to obtain results for the isogenies similar to the results of the differential addition on the curve.

In the paper [3], Theorem 1 was proved, which determines the odd degree isogenic mapping from Edwards curve E_d to the curve E'_d in Farashahi-Hosseini coordinates $w(x,y)=dx^2y^2$ (or $w(x,y)=x^2/y^2$). As in the paper [5], it is proved only for the Edwards curve E_d ($a=1$), and it is not known whether its results are applicable in the class of twisted Edwards curves $E_{a,d}$ ($\chi(a)=\chi(d)=-1$). Below we prove this theorem for all curves in the generalized form $E_{a,d}$ (1). Instead of the formula (8) taken as a basis in [3], we proceed from the more laconic formula (10) obtained above in Theorem 1.

Theorem 2. Let $G=\{(1{,}0),\pm Q_1,\pm Q_2,\dots,\pm Q_s\}$ is the subgroup of odd order $l=2s+1$ of the points $\pm Q_i=(\alpha_i,\pm\beta_i)$ of the curve $E_{a,d}$ (1). Let $w_i=d\alpha_i^2\beta_i^2, w=dx^2y^2, P=(x,y)\in E_{a,d}$. Then $w(\phi(x,y))=w(x',y')$ is l-isogeny with the kernel G from the curve $E_{a,d}$ to the curve $E'_{a',d'}$ with the parameters $a'=a^l, d'=A^8d^l, A=\prod_{i=1}^{s}\alpha_i$, and the mapping function

$$w(\phi)=w\prod_{i=1}^{s}\frac{(w-w_i)^2}{(1-ww_i)^2}. \qquad (11)$$

Proof. From the equation of the curve (1) we have $\alpha_i^2+a\beta_i^2=1+d\alpha_i^2a\beta_i^2$. The factors under the sign of the product of isogeny (10) have the form:

$$\frac{U_i}{Z_{xi}}=\frac{x^2-a\beta_i^2}{1-d\beta_i^2x^2},\qquad \frac{V_i}{Z_{yi}}=\frac{x^2-\alpha_i^2}{a-d\alpha_i^2x^2}.$$

Let’s denote the products of numerators and denominators:

$$S_i = U_iV_i = \left(x^2 - a\beta_i^2\right)\left(x^2 - \alpha_i^2\right), \qquad R_i = Z_{xi}Z_{yi} = \left(1 - d\beta_i^2x^2\right)\left(a - d\alpha_i^2x^2\right).$$

Then, taking into account $\alpha_i^2 + a\beta_i^2 = 1 + w_i$ and the multiplying of these equations by dy^2 and y^2 respectively, we obtain:

$$S_idy^2 = -U_iV_i = dy^2\left(x^2 - a\beta_i^2\right)\left(x^2 - \alpha_i^2\right) = x^2w - x^2y^2\left(\alpha_i^2 + a\beta_i^2\right) + ad\alpha_i^2\beta_i^2y^2 =$$
$$= wx^2 - w(1 + w_i) + aw_iy^2,$$
$$R_iy^2 = y^2\left(1 - d\beta_i^2x^2\right)\left(a - d\alpha_i^2x^2\right) = ay^2 - dx^2y^2\left(\alpha_i^2 + a\beta_i^2\right) + ww_ix^2 =$$
$$= ay^2 - w(1 + w_i) + ww_ix^2.$$

Substitution in the last equations $ay^2 = 1 + w - x^2$ gives:

$$S_idy^2 = wx^2 - w(1 + w_i) + aw_iy^2 = wx^2 - w - ww_i + w_i(1 + w - x^2) =$$
$$= (w - w_i)(x^2 - 1),$$
$$R_iy^2 = ay^2 - w(1 + w_i) + ww_ix^2 = (1 + w - x^2) - w - ww_i + ww_ix^2 =$$
$$= (1 - ww_i)(x^2 - 1).$$

Then

$$\frac{S_i}{R_i} = d^{-1}\frac{w - w_i}{1 - ww_i}, \qquad \prod_{i=1}^{s}\left(\frac{S_i}{dR_i}\right)^2 = d^{-2s}\prod_{i=1}^{s}\left(\frac{S_i}{R_i}\right)^2 = d^{-2s}\prod_{i=1}^{s}\frac{(w - w_i)^2}{(1 - ww_i)^2}.$$

As a result, for l-isogeny (10) taking into account the value of the parameter of the isogenic curve

$$w\big(\phi(P)\big) = d'(x' \cdot y')^2 = A^8d^{2s+1}x^2y^2A^{-8}\prod_{i=1}^{s}\left(\frac{S_i}{dR_i}\right)^2 =$$
$$= dx^2y^2\prod_{i=1}^{s}\left(\frac{S_i}{R_i}\right)^2 = w\prod_{i=1}^{s}\frac{(w - w_i)^2}{(1 - ww_i)^2}.$$

The theorem is proved.

We emphasize that isogeny (11) for w-coordinate $E_{a,d}$ (1) does not depend on the parameter a and is equally valid for quadratic and twisted Edwards curves forming quadratic twist pairs [10]. In other words, function (11) maps the curve points of one of these two classes to the curve points of the same class.

Let’s take as an example the 3-isogeny of the twisted curve $E_{-1,-25}$ of the previous section and its point $P = (3{,}75)$ of the 120th order. For it, we will receive the coordinate $w = -25 \cdot 3^2 \cdot 75^2 = 119$. For the kernel point $Q_1 = (149{,}64)$, respectively, $w_1 = -25 \cdot 149^2 \cdot 64^2 = -60$. According to the formula (11) $w(\phi(P)) = 78$ the point of the isogenic curve $E'_{-1,-3}$, calculated by the formula (10), is the point of the 40th order $P' = (-116{,}94)$. For it, the coordinate $w\big(\phi(P)\big) = d'(x'y')^2 = 78$ coincides with the calculations by formula (11).

Let’s now turn to the quadratic curve $E_{1,25} = E_{25}$ as a pair of quadratic torsion of the curve $E_{-1,-25}$. All points of this pair of curves have different coordinates (except for the points $(\pm 1{,}0)$) and, accordingly, the curve E_{25} has the different kernel of the 3rd degree $G = \{(1{,}0), \pm Q_1 = (97, \pm 14)\}$. Characteristically, the parameter of the isogenic curve $d' = d^{(1)} = A^8d^{(0)3} = 97^825^3 = 110$ also changes. For the curve E_{25} the mapping (10) of the point of the 120th $P = (20{,}108)$ is the point of the 40th order $P' = (-16{,}57)$ on the isogenic curve E_{110}. For point P we obtain the coordinate $w = 25 \cdot 20^2 \cdot 108^2 = 113$, for the point of the kernel $w_1 = 25 \cdot 97^2 \cdot 14^2 = 44$, respectively. According to formula (11) $w(\phi(P)) = 100$. For the point $P' = (-24{,}57)$ the w-coordinate is $w\big(\phi(P)\big) = 110 \cdot 24^2 \cdot 57^2 = 100$. This corresponds to Theorem 2 and the formula (11).

The implementation of computing of isogenies (11) is given in [3]. To calculate the parameters $d^{(i)}$ of the chain of isogenies in projective coordinates, an additional parameter C is introduced into the equation of the curve E_d (2) or (3). For STEC (1) at $p \equiv 3 \bmod 4$, we accept $a = -1$, $d^{(i=m)} = -m^2 \bmod p, m \in \{2..(p-1)/2\}$ and define the curve:

$$E_{C,D}\colon Cx^2 - Cy^2 = C + Dx^2y^2, D = dC, \chi(d) = -1. \tag{12}$$

To calculate the parameter d' of the isogenic curve the formula [5] is used:

$$d' = A^8d^l, A = \prod_{i=1}^{s}\alpha_i\,, l = 2s + 1. \tag{13}$$

To express the parameter A with the replacement $\alpha_i \to w_i$ in [3], the idea of doubling the kernel points is proposed, which does not change the points of subgroups G of odd order l. From the law of doubling (5) we have

$$2(\alpha_i, \beta_i) = \left(\frac{\alpha_i^2 - a\beta_i^2}{1 - d\alpha_i^2\beta_i^2}, \frac{2\alpha_i\beta_i}{1 + d\alpha_i^2\beta_i^2}\right).$$

By squaring the second coordinate, we obtain

$$\left(\frac{2\alpha_i\beta_i}{1 + w_i}\right)^2 = \frac{4d^{-1}w_i}{(1 + w_i)^2} = \beta_k^2 \Rightarrow d\alpha_k^2\beta_k^2 = \frac{4\alpha_k^2 w_i}{(1 + w_i)^2} \Rightarrow \alpha_i^2 = \frac{(1 + w_i)^2}{4}.$$

Here we take into account that for each point of the kernel (α_i, β_i) there exists the reverse point $(\alpha_i, -\beta_i) = (\alpha_k, \beta_k)$ and for such a pair of points $w_i = w_k$. Then the formula (13) takes the form

$$d' = d^l \prod_{i=1}^{s} \frac{(1 + w_i)^8}{4^4}. \tag{14}$$

Transition to projective coordinates $(W{:}\,Z)$ allows avoiding inversions in the formula (11), thus for the curve (12)

$$W' = W \prod_{i=1}^{s} (WZ_i - W_iZ)^2, Z' = Z \prod_{i=1}^{s} (ZZ_i - WW_i)^2.$$

Here $4sM + 2M + 2S$ operations in the field are performed for every s (M is multiplication, S is squaring). If we enter intermediate formulas:

$$H = (W + Z)(W_i - Z_i),$$
$$J = (W - Z)(W_i + Z_i),$$

then

$$2W' = W \prod_{i=1}^{s} (H_i - J_i)^2, 2Z' = Z \prod_{i=1}^{s} (H_i - J_i)^2.$$

And we need only $4sM + 2S$ operations when calculating one isogeny (11).

For calculating the parameter $d' = {}^{D'}/_{C'}$ of the isogenic curve (12) in projective coordinates according to (14) we obtain

$$D' = D^l \prod_{i=1}^{s} (Z_i + W_i)^8, C' = C^l \prod_{i=1}^{s} (2Z_i)^8.$$

Therefore, for the small degrees of isogenies $l = 2s + 1 \leq 9 (s \leq 4)$ in each of these formulae, it is enough to perform three squares, within which to substitute values D and C at different steps. Herewith the cost of calculations is determined by the linear function $2(s + 1)M + 6S$. With the degree of isogeny $l > 9$ additional operations M and S are required, the number of which needs an estimate.

Within the limits of the linear trend (lower value), the total cost of calculating l-isogenies in Farashahi-Hosseini coordinates [3] is $2(3s + 1)M + 8S$ (the formula of the trend is obtained in this paper). For example, at $l = 3$ and $l = 5$ we obtain $8M + 8S$ and $14M + 8S$, respectively. The calculation of these isogenies in the classical projective coordinates $(X{:}\,Z)$ gives in [6] the best result $6M + 5S$ for 3-isogenies and the worst result $21M + 12S$ for 5-isogenies in [7]. With the growth of l the calculations of isogenies in coordinates $(X{:}\,Z)$ become significantly more complicated.

Supersingular twisted and quadratic Edwards curves with the same order $N_E = p + 1$, as follows from Sect. 2, have different structures [10]. STEC has only two exceptional points of the 2nd order, and in the class of quadratic curves, two more exceptional points of the 4th order (6) are added to them as well as two non- exceptional points of the 4th order $\pm F_0 = (0, \pm 1)$. It is easier to bypass exceptional points in the STEC class, which makes them preferable to quadratic ones in cryptosystems.

For this purpose, for STEC with the order of the curve with the minimum even cofactor $N_E = 8n$ (n is odd), it is sufficient to select the base point P of Alice and Bob as the point of order n or maximum order $4n$ at the stage of selection of system-wide parameters. In the latter case, quadratic curves are not acceptable, because the mappings to points of the 4th order are possible. At the same time, it is clear for the twisted Edwards curves that with such a choice no chain of isogenies of odd degrees will generate the point of the 2nd order. Another solution to this problem may be to select the point P from one of the three subgroups of the curve that don`t contain exceptional points (they are replaced in this subgroup by the ordinary point of the 2nd order $D_0 = (-1,0)$).

The results of the implementation of the Edwards-CSIDH model [3] in projective coordinates $(W{:}\,Z)$ claim that it is 20% faster than the Montgomery-CSIDH model in coordinates $(X{:}\,Z)$. It should be noted that this model is built on complete Edwards curves with the order $N_E = p + 1 = 4n$ With the same success, it can be realized on supersingular twisted Edwards curves with the order $N_E = 8n$. Quadratic Edwards curves with redundant exceptional points of the 4th order are outside the recommended range.

5. Conclusions

It can be concluded that the method of computing odd degree isogenies in coordinates $(W{:}\,Z)$, proposed in [3], using supersingular complete and twisted Edwards curves, allows implementing the fastest calculations to date in the construction of the PQC of protocol CSIDH and the like. The theorems proved in this paper open a class of twisted Edwards curves for their implementation.

6. References

[1] D. Jao, L. de Feo, Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies, Lect. Notes Comput. Sci. 7071 (2011) 19–34. doi:10.1007/978-3-642-25405-5_2.

[2] W. Castryck, et al., CSIDH: An efficient post-quantum commutative group action, in: Advances in Cryptology—ASIACRYPT, 2018, pp. 395–427. doi:10.1007/978-3-030-03332-3_15.

[3] S. Kim, et al., Optimized method for computing odd-degree isogenies on Edwards curves, in: Advances in Cryptology—ASIACRYPT, 2019, pp. 273–292. doi:10.1007/978-3-030-34621-8_10.

[4] R. R. Farashahi, S. G. Hosseini, Differential addition on twisted Edwards curves, Lect. Notes Comput. Sci. 10343 (2017) 366–378. doi:10.1007/978-3-319-59870-3_21.

[5] D. Moody, D. Shumow, Analogues of Velu’s formulas for isogenies on alternate models of elliptic curves, Math. Computation 85(300) (2015) 1929–1951. doi:10.1090/mcom/3036.

[6] S. Kim, et al., Efficient isogeny computations on twisted Edwards curves, Secur. Commun. Netw. 2018 (2018). 1–11. doi:10.1155/2018/5747642.

[7] A. Bessalov, V. Sokolov, P. Skladannyi, Modeling of 3- and 5-isogenies of supersingular Edwards curves, in: Proceedings of the 2nd International Workshop on Modern Machine Learning Technologies and Data Science, June 2–3, 2020, no. I, vol. 2631, pp. 30–39.

[8] D. J. Bernstein, T. Lange, Faster addition and doubling on elliptic curves, Lect. Notes Comput. Sci. 4833 (2007) 29–50. doi:10.1007/978-3-540-76900-2_3.

[9] D. J. Bernstein, et al., Twisted Edwards curves, Lect. Notes Comput. Sci. 5023 (2008) 389–405. doi:10.1007/978-3-540-68164-9_26.

[10] A. V. Bessalov, Edwards Elliptic Curves and Cryptography, 2017. [Publication in Russian].

[11] A. V. Bessalov, L. V. Kovalchuk, Supersingular twisted Edwards curves over prime fields. II. Supersingular twisted Edwards curves with the J-invariant equal to 66^3, Cybern. Syst. Anal. 55(5) (2019) 731–741. doi:10.1007/s10559-019-00183-y.

[12] A. V. Bessalov, O. V. Tsygankova, Number of curves in the generalized Edwards form with minimal even cofactor of the curve order, Probl. Inf. Transm. 53(1) (2017) 92–101. doi:10.1134/s0032946017010082. [Publication in Russian].

[13] A. V. Bessalov, O. V. Tsygankova, Interrelation of families of points of high order on the Edwards curve over a prime field, Probl. Inf. Transm. 51(4) (2015) 391–397. doi:10.1134/s0032946015040080. [Publication in Russian].

[14] 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.

[15] A. V. Bessalov, Calculation of parameters of cryptic curves Edwards over the fields of 5th and 7th characteristic, Cybersecur. Educ. Sci. Tech. 1 (2018) 94–104. doi:10.28925/2663-4023.2018.1.94104. [Publication in Ukrainian].

[16] A. Bessalov, et al., 3- and 5-isogenies of supersingular Edwards curves, Cybersecur. Educ. Sci. Tech. 4(8) (2020) 6–21. doi:10.28925/2663-4023.2020.8.621.

[17] L. Washington, Elliptic Curves. Discrete Mathematics and Its Applications, 2008. doi:10.1201/9781420071474.