Modeling of 3- and 5-Isogenies of Supersingular Edwards Curves

Anatoly Bessalov[1[0000-0002-6967-5001]], Volodymyr Sokolov[1[0000-0002-9349-7946]], and Pavlo Skladannyi[1[0000-0002-7775-6039]]

Borys Grinchenko Kyiv University, Kyiv, Ukraine
{a.bessalov,v.sokolov,p.skladannyi}@kubg.edu.ua

Abstract. An analysis is made of the properties and conditions for the existence of 3- and 5-isogenies of complete and quadratic supersingular Edwards curves. For the encapsulation of keys based on the SIDH algorithm, it is proposed to use isogeny of minimal odd 3 and 5 degrees, which allows bypassing the problem of singular points of the 2nd and 4th orders, characteristic of 2-isogenies. A review of the main properties of the classes of complete, quadratic and twisted Edwards curves over a simple field is given. Formulas for the isogeny of odd degrees are reduced to a form adapted to curves in Weierstrass form. To do this, the modified law of addition of curve points in the generalized Edwards form is used, which preserves the horizontal symmetry of the curve's return points. Examples of the calculation of 3- and 5-isogenies of complete Edwards supersingular curves over small simple fields are given, and the properties of the isogeny composition for computing isogenies with large-order kernels are discussed. Formulas of upper bounds for the complexity of computing isogeny of odd degrees 3 and 5 in the classes of complete and quadratic Edwards curves in projective coordinates are obtained. Algorithms for calculating 3- and 5-isogenies of Edwards curves with complexity and $12M+5S$, respectively, are constructed. The conditions for the existence of supersingular complete and quadratic Edwards curves of the order $4\cdot 3^m\cdot 5^n$ and $8\cdot 3^m\cdot 5^n$ are found. Some parameters of the cryptosystem were determined during the implementation of the SIDH algorithm at the quantum security level of 128 bits.

Keywords: Generalized Edwards Curve, Complete Edwards Curve, Twisted Edwards Curve, Quadratic Edwards Curve, Curve Order, Point Order, Isomorphism, Isogeny, Degree of Isogeny, Kernel of Isogeny, Quadratic Residue, Quadratic Non-residue.

1 Introduction

One of the well-known prospects of post-quantum cryptography (PQC) is the algorithms based on the isogeny of supersingular elliptic curves with as many subgroups of their points as possible (in particular, the SIDH algorithm [1]). The problem of the discrete logarithm of classical elliptic cryptography is replaced by the problem of finding one of the isogenous sets of subgroups of such a non-cyclic curve that is sufficiently resistant to the attacks of a quantum computer. To date, the growing interest in isogeny

is associated with the shortest key length in the proposed algorithms in comparison with other well-known candidates for post-quantum cryptography at a given level of strength.

This paper deals with the properties of 3- and 5-isogenies of two classes of these curves, in particular the conditions of their existence. Section 2 provides a brief review of the literature on this topic. In Sect. 3, we touch upon the issue of how to solve the problem of singular points that occurs when programming the SIDH algorithm on Edwards curves using 2-isogenies. Instead of 2- and 3-isogenies, it is proposed to construct an algorithm on 3- and 5-isogenies of points of odd orders, which allows circumventing singular points. Sect. 4 gives a brief overview of the properties of three classes of Edwards curves according to the new classification. In Sect. 5, we prove a formula for the isogeny of odd degrees expressed by rational functions of one variable and give examples. In Sect. 6, the conditions for the existence of 3- and 5-isogenies and the requirements for the curve parameters for the SIDH algorithm are defined [1]. Algorithms for 3- and 5-isogenous Edwards curves are presented in Sect. 7 and the results of mathematical modeling are presented in Sect. 8.

2 Review of the Literature

The properties of isogeny for curves in the form of Weierstrass are sufficiently studied. Effective construction methods and isogeny properties of promising classes of curves in the Edwards form are less known.

Edwards curves with one parameter, defined in [2], have very attractive advantages for cryptography: maximum point exponentiation speed, completeness, and universality of the point addition law, affine coordinates of a neutral element of a group of points, increased security against side-channel attacks. The programming of group operations becomes more efficient and accelerates due to the absence of a singular point at infinity as the zero of an abelian group of points. The introduction of the second parameter of the curve in [3] expanded the class of curves in the Edwards form and generated curves with new properties that are interesting for cryptographic applications.

Along with the properties noted above, curves in the Edwards form proved to be the fastest technology in calculating isogeny. In [4], experimental estimates of the rate of calculation of isogeny on Edwards curves are presented, more than three times higher than the indices for curves in the Weierstrass form. Since the procedure for finding an isogenic point usually includes the scalar product of the point, the complex gain in the speed of the algorithms on the Edwards curves becomes significant.

3 Statement of the Problem

Well-known implementations of the SIDH algorithm mainly use curves in the forms of Weierstrass and Montgomery. Our attempt to programmatically implement the SIDH algorithm using 2- and 3-isogenies of curves in the Edwards form encountered the problem of the presence of 4 singular points at infinity of the 2^{nd} and 4^{th} orders in the class of quadratic Edwards curves, to which all Edwards curves are mapped over the field

F_{p^2} set over the field F_p. These points exist in all subgroups of even orders, the number of which exceeds half of all subgroups of the curve. The appearance of any singular point in the calculation of isogeny significantly slows down the software implementation of the SIDH algorithm on Edwards curves. To get around this problem, we propose using isogenies of minimal odd degrees 3 and 5 for points of odd order of the curve. Although the transition from 2- to 5-isogeny complicates the calculation algorithm, such a smooth implementation of the algorithm is faster.

Among the numerous works on this problem, we single out articles [4, 5], in which isogeny formulas for curves in the Edwards form were first obtained. Our analysis in this paper is based on their results using the properties of supersingular curves [6]. To adapt the definitions for the arithmetic of isogeny of Edwards curves and curves in the Weierstrass form, we use the modified law of addition of points [7].

4 Classes of Curves in the Generalized Edwards Form

The elliptic curve in the generalized Edwards form [3, 8] is determined by the equation

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

In contrast to the equation of this curve in [3], here we multiply the parameter *a* by y^2 instead of x^2. If it is quadratic $\chi(ad) = -1$, the curve (1) is isomorphic to the complete Edwards curve [1] with one parameter d.

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

In case $\chi(ad) = 1$ and $\chi(a) = \chi(d) = 1$, then there is an isomorphism of the curve (1) with a quadratic Edwards curve

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

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

Curves with different values *d* are isomorphic if they have the same j-invariant equal to the curve (1)

$$j(a, d) = \frac{16(a^2+d^2+14ad)}{ad(a-d)^4}. \quad (4)$$

This parameter is basic in the structure of graphs of isogenic curves, the vertices of which define classes of isomorphic curves.

In our article [7], we proposed interchanging the coordinates x and y in the form of the Edwards curve. Then the modified universal law of addition of points of the curve (1) has the form:

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1x_2 - ay_1y_2}{1 - dx_1x_2y_1y_2}, \frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}\right). \quad (5)$$

If two points coincide, we obtain from (2) the law of doubling points

$$2(x_1, y_1) = \left(\frac{x_1^2 - ay_1^2}{1 - dx_1^2 y_1^2}, \frac{2x_1 y_1}{1 + dx_1^2 y_1^2}\right). \quad (6)$$

Using the modified laws (4), (6) allows us to preserve the generally accepted horizontal symmetry (relative to the axis *x*) of the reverse points. Defining now the reverse point as $-P = (x_1, -y_1)$ we obtain, according to (4), the coordinates of the neutral element of the group of points $O = (x_1, y_1) + (x_1, -y_1) = (1,0)$.

In addition to the neutral element *O*, the axis *X* also always contains the second-order point $D_0 = (-1,0)$, for which, in accordance with (6) $D_0 = (-1,0), 2D_0 = (1,0) = O$.

Depending on the properties of the parameters *a* and *d*, you can get two more singular points of the 2nd order and two or more points of the 4th order.

As follows from (1), points $\pm D_0 = \left(0, \pm\frac{1}{\sqrt{a}}\right)$ of the fourth-order may lie on the axis *y*, for which $\pm 2F_0 = D_0 = (-1,0)$. These points exist over the simple field F_p if the parameter is *a* square (quadratic residue).

From equation (1) we define the squares:

$$x^2 = \frac{1 - ay^2}{1 - dy^2}, y^2 = \frac{1 - x^2}{a - dx^2}, \quad (7)$$

generating singular points at infinity (we put the sign ∞ when dividing by 0):

$$D_{1,2} = \left(\pm\sqrt{\frac{a}{d}}, \infty\right), \pm F_{11} = \left(\infty, \pm\frac{1}{\sqrt{d}}\right). \quad (8)$$

They arise in cases $\chi(ad) = 1$ and $\chi(d) = 1$ respectively. This, for example, is always performed in the extension of the field F_{p^2}. According to the rules of terminal transition and the doubling law (6), we can verify that $2D_{1,2} = O, \pm 2F_1 = D_0 = (-1,0)$. In other words, under the conditions of their existence, singular points $D_{1,2}$ are points of the 2nd order and singular points $\pm F_1$ are points of the 4th order.

Depending on the properties of the parameters *a* and *d*, the curves in the generalized Edwards form (1) are divided into 3 disjoint (non-isomorphic) classes:

- Complete Edwards curves with the condition C1: $\chi(ad) = -1$.
- Twisted Edwards curves with the condition C2.1: $\chi(a) = \chi(d) = -1$.
- Quadratic Edwards curves with the condition C2.2: $\chi(a) = \chi(d) = 1$.

The main properties of these classes of curves [7]:

1. Concerning the points of the second order, the first class of complete Edwards curves over a simple field is the class of cyclic curves (with one point of the second order), twisted and quadratic Edwards curves form classes of non-cyclic curves (3 points of the second-order each). The maximum order of the points of the curves of the last classes does not exceed $N_E/2$.

2. The class of complete Edwards curves does not contain singular points.

3. Twisted Edwards curves contain only two second-order singular points $D_{1,2} = \left(\pm\sqrt{\frac{a}{d}};\infty\right)$, and Edwards quadratic curves, in addition to them,—two other fourth-order singular points $\pm F_{11} = \left(\infty;\pm\frac{1}{\sqrt{d}}\right)$.

4. Edwards twisted and quadratic curves form quadratic torsion pairs based on a parameter transformation $\tilde{a} = ca, \tilde{d} = cd, \chi(c) = -1$.

5. In the classes of twisted and quadratic Edwards curves, the replacement $a \leftrightarrow d$ gives the isomorphism $E_{a,d} \sim E_{d,a}$.

6. Complete and quadratic Edwards curves are isomorphic to the curves with parameter $a = 1$: $E_{a,d} \sim E_{1,d/a}$.The introduction of the new parameter into the equation of curve (1) is justified only for the class of twisted Edwards curves.

7. The twisted Edwards curves for $p \equiv 1 \bmod 4$ do not have the 4th order points.

We emphasize that in the extension of the simple field F_{p^2} all 3 classes of Edwards curves defined over a simple field acquire the properties of quadratic curves (3). Therefore, we consider mainly curves E_d of the form (2) and (3).

5 Isogenies of Odd Degrees of Edwards Curves

The isogeny of the elliptic curve $E(K)$ over the field K into the curve $E'(K)$ is the homomorphism $\phi: E(\overline{K}) \to E'(\overline{K})$, defined by rational functions. That means that for all $\phi(P+Q) = \phi(P) + \phi(Q)$ there exists the rational function [9]

$$\phi(x,y) = \left(\frac{p(x)}{q(x)}, y\frac{f(x)}{g(x)}\right) = (x', y'), \tag{9}$$

mapping curve points E to curve points E'. The degree of isogeny is called the maximum of the degrees $l = \deg\phi(x,y) = \max\{\deg p(x), \deg q(x)\}$ and its kernel $\ker\phi = G$ is subgroup $G \subseteq E$, the points of which are reflected 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 curve E points l times (curve E points l are displayed in one point of the curve E'). At $G = O$ isogeny becomes the isomorphism with the degree 1.

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

Theorem 2 [4]. Let's $G = \{(0,1), \pm Q_1, \pm Q_2, \dots, \pm Q_s\}$, the subgroup of the odd order $l = 2s+1$ of points $\pm Q_i = (\alpha_i, \pm\beta_i)$ of the curve E_d. Let's define

$$\phi(P) = \left(\prod_{Q\in G}\frac{x_{P+Q}}{x_Q}, \prod_{Q\in G}\frac{y_{P+Q}}{x_Q}\right), \tag{10}$$

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

$$\phi(x,y) = \left(\frac{x}{A^2}\prod_{i=1}^{s}\frac{(\alpha_i x)^2 - (\beta_i y)^2}{1-(d\alpha_i\beta_i xy)^2}, \frac{y}{A^2}\prod_{i=1}^{s}\frac{(\alpha_i y)^2 - (\beta_i x)^2}{1-(d\alpha_i\beta_i xy)^2}\right), \tag{11}$$

Its proof is given in [4]. An important consequence of this is that isogenic curves lie in the same classes as curves E_d (i. e., complete Edwards curves are mapped to complete and quadratic curves—to quadratic). This significantly distinguishes the isogeny of odd degrees from the 2-isogeny (for them, the complete Edwards curves are mapped into quadratic ones).

The formula (11) for the function $\phi(x, y)$ directly follows the definition $\phi(P)$ in the statement of the theorem, the law (4) of the addition of points $(x_P, y_P) = (x, y)$ with the points $\pm Q_i = (\alpha_i, \pm\beta_i)$, wherein, for pairs of coordinates we have

$$\frac{x_{P+Q_i}}{x_{Q_i}}\frac{x_{P-Q_i}}{x_{-Q_i}} = \frac{1}{\alpha_i^2}\frac{(\alpha_i x)^2-(\beta_i y)^2}{1-(d\alpha_i\beta_i xy)^2}, \frac{y_{P+Q_i}}{x_{Q_i}}\frac{y_{P-Q_i}}{x_{-Q_i}} = \frac{1}{\alpha_i^2}\frac{(\beta_i x)^2-(\alpha_i y)^2}{1-(d\alpha_i\beta_i xy)^2}. \quad (12)$$

The multipliers *x* and *y* before the products in the coordinates of the function $\phi(x, y)$ take into account the neutral element $O = (1_i, 0)$ of the kernel of isogeny.

From (11) the property $\phi(0,1) = (0,1)$ it is obvious that, i. e. the neutral element is mapped in itself. For all points of the kernel $\phi(\pm Q_i = (\alpha_i, \pm\beta_i)) = (1,0)$ is also true.

The mapping (11) can be reduced to the form (9), then the determination of the degree of isogeny becomes obvious. From (2) and (3) let's express $y^2 = \frac{1-x^2}{1-dx^2}$, and substitute this value in (11). Then in the numerator of the first coordinate (11)

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

$$= \frac{(1+d\alpha_i^2\beta_i^2)x^2-\beta_i^2-d\alpha_i^2x^4}{1-dx^2} = \frac{x^2-\beta_i^2-d(\alpha_i^2x^4-\alpha_i^2\beta_i^2x^2)}{1-dx^2} = \frac{(x^2-\beta_i^2)(1-d\alpha_i^2x^2)}{1-dx^2}. \quad (13)$$

Similarly, we transform the denominator of the first coordinate (11)

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

$$= \frac{1-d(\alpha_i^2+d\beta_i^2)x^2+d^2\alpha_i^2\beta_i^2x^4}{1-dx^2} = \frac{(1-d\alpha_i^2x^2)(1-d\beta_i^2x^2)}{1-dx^2}. \quad (14)$$

After reducing the common factors, we obtain

$$\frac{(\alpha_i x)^2-(\beta_i y)^2}{1-(d\alpha_i\beta_i xy)^2} = \frac{x^2-\beta_i^2}{1-d\beta_i^2x^2}. \quad (15)$$

Similar calculations can be carried out with the second coordinate (11). As a result, the function (11) can be written in the equivalent form

$$\phi(x, y) = \left(\frac{x}{A^2}\prod_{i=1}^{s}\frac{x^2-\beta_i^2}{1-dx^2\beta_i^2}, -\frac{y}{A^2}\prod_{i=1}^{s}\frac{x^2-\alpha_i^2}{1-dx^2\alpha_i^2}\right), \quad (16)$$

corresponding to the classical form (9). This form is given in [4] without proof. Its obvious advantage over (11) is simplicity and minimal computational complexity. Besides, the degree of isogeny as the maximum degree of the polynomial $p(x)$ in (9) is immediately determined as $l = 2s + 1$.

6 Requirements for Cryptosystem Parameters

The search for a suitable value of the characteristic of the field p in the SIDH problem using 3- and 5-isogeny of Edwards curves must meet some necessary conditions.

Statement 1. 3- and 5-isogenies exist for supersingular complete and quadratic Edwards curves E_d, respectively, at $p \equiv -1 \bmod 60$ and $p \equiv -1 \bmod 120$.

Proof. Points of the 3rd and 5th orders exist on the complete supersingular Edwards curve of the $p + 1 = 4 \cdot 3^m \cdot 5^n$ order under the conditions that $p \equiv -1 \bmod 4$, $p \equiv -1 \bmod 3$, and $p \equiv -1 \bmod 5$, and which come down to one condition $p \equiv -1 \bmod 60$.

The minimum even cofactor of the order N_E of the quadratic Edwards curve is the number 8, at the same time at $p + 1 = 8 \cdot 3^m \cdot 5^n$ the condition $p \equiv -1 \bmod 120$ is true.

Statement 2. For odd $l = 2s + 1$ of l-isogeny of P points of odd order of the curve, there are points of odd order.

Proof. The Edwards curve E_d of the order $N_E = 2^c \cdot n$, $c \geq 2$, contains the points P of the odd order $n = l \cdot m$. Thus, l-isogeny and isogenous curve E' of the same order N_E exist. l-isogeny is a homomorphism that compresses l times the points $< P >$ into a subgroup of points of odd order of the curve E'. This subgroup does not contain any points of even order. At $m = 1$ n-isogeny maps all points $< P >$ into neutral element O of the order 1.

Statement 3. At $p \equiv 1 \bmod 4$ *supersingular Edwards curves do not exist.*

Proof. At $p \equiv 1 \bmod 4$ the order of supersingular curve is $p + 1 \equiv 2 \bmod 4$, at the same time for any Edwards curve the number 4 divides the order of the curve.

The value of module p is determined by the security requirements. In the product $3^m \cdot 5^n$ both factors have the same order at $3^m \approx 5^n$, then $m \approx 1.465n$. This balances the number of corresponding cyclic subgroups.

128-bit quantum security with complexity estimate $\sqrt[6]{p}$ (instead of $\sqrt[4]{p}$ for a regular computer) is provided with the length of module $\log_2 p = 6 \cdot 128 = 768$ bit. In the field F_{p^2} each coordinate of the point has the length $2 \log_2 p = 1536$ bit. The key length estimate in the SIDH system is $6 \log_2 p = 4608$ bit. 256-bit quantum security level doubles all of these estimates.

7 Algorithms for 3- and 5-Isogenous Edwards Curves

The calculation of the 3- and 5-isogenes of the Edwards curves (2) and the parameter $d' = A^8 \cdot d^l$ of the isogeous curve is performed using the following algorithms with the cost $6M + 5S$ and $21M + 12S$ respectively.

These algorithms are distinguished by the greatest simplicity and low cost of computing among the known ones. In contrast to the 3-isogeny calculation algorithm given in [9] and instead of (11) we use the simpler expression (16) for the function $\phi(x, y)$ together with the simpler equation for the parameter $d' = A^8 \cdot d^l$.

In fact, when calculating 3-isogeny, we use an algorithm close to that proposed in [9], with the same effectiveness $6M + 5S$. Our algorithm for computing 5-isogeny is almost three times slower than for 3-isogeny, and probably has reserves to increase efficiency.

7.1 3-Isogene Edwards Curve Calculation Algorithm

Entry: point $P = (X:Z)$ and point of 3rd order $Q_1 = (X_1:Z_1)$ of kernel of curve E_d with parameter d.

1. $s_1 \leftarrow X_1^2$
2. $s_2 \leftarrow Z_1^2$
3. $t_1 \leftarrow (X + Z_1)^2 - s_0 - s_2$
4. $t_2 \leftarrow t_1 + s_1$
5. $t_3 \leftarrow t_1 + s_2$
6. $t_4 \leftarrow 2t_1$
7. $t_5 \leftarrow 4s_1 + s_2 + t_4$
8. $t_6 \leftarrow 4s_2 + s_1 + t_4$
9. $D' \leftarrow t_3 \cdot t_5$
10. $C' \leftarrow t_2 \cdot t_6$
11. $u_1 \leftarrow X_1 \cdot Z$
12. $u_2 \leftarrow X \cdot Z_1$
13. $u_3 \leftarrow (u_1+u_2)^2$
14. $u_4 \leftarrow (u_1-u_2)^2$
15. $F \leftarrow (X + Z) \cdot u_3$
16. $G \leftarrow (X - Z) \cdot u_4$
17. $2X' \leftarrow F + G$
18. $2Z' \leftarrow F - G$

Exit: point of curve $E'_{\bar{d}}P' = (X':Z')$ and parameter $(D':C')$ of isogenic curve $C'E'_{d'}$.

7.2 5-Isogene Edwards Curve Calculation Algorithm

Entry: point $P = (X:Z)$ and point of 5th orders $Q_1 = (X_1:Z_1)$ and $Q_2 = (X_2:Z_2)$ of kernel of curve E_d with parameter d.

1. $s_0 \leftarrow X^2$
2. $s_1 \leftarrow X_1^2$
3. $s_2 \leftarrow X_2^2$
4. $s_3 \leftarrow Z^2$
5. $s_4 \leftarrow Z_1^2$
6. $s_5 \leftarrow Z_2^2$
7. $t_0 \leftarrow d \cdot s_0$
8. $t_1 \leftarrow d \cdot s_1$
9. $t_2 \leftarrow d \cdot s_2$
10. $G_1 \leftarrow s_1 - s_4$
11. $F_1 \leftarrow t_1 - s_4$
12. $G_2 \leftarrow s_2 - s_5$

13. $F_2 \leftarrow t_2 - s_5$
14. $H_1 \leftarrow -s_0 \cdot F_1 + s_3 \cdot G_1$
15. $I_1 \leftarrow -t_0 \cdot G_1 + s_3 \cdot F_1$
16. $H_2 \leftarrow -s_0 \cdot F_2 + s_3 \cdot G_2$
17. $I_2 \leftarrow -t_0 \cdot G_2 + s_3 \cdot F_2$
18. $L_1 \leftarrow s_1 \cdot s_2$
19. $L_2 \leftarrow s_4 \cdot s_5$
20. $X' \leftarrow X \cdot L_2$
21. $X' \leftarrow X' \cdot H_1$
22. $X' \leftarrow X' \cdot H_2$
23. $Z' \leftarrow Z \cdot L_1$
24. $Z' \leftarrow Z' \cdot I_1$
25. $Z' \leftarrow Z' \cdot I_2$
26. $D \leftarrow d^2$
27. $D \leftarrow D^2$
28. $D \leftarrow D \cdot d$
29. $L \leftarrow L_1^2$
30. $L \leftarrow L^2$
31. $L \leftarrow L \cdot D$
32. $C \leftarrow L_2^2$
33. $C' \leftarrow C^2$

Exit: point of curve $E'_{\bar{d}}P' = (X' : Z')$ and parameter $(D' : C')$ of isogenic curve $C'E'_{d'}$.

8 Implementation of the SIDH Algorithm

Below are three field module values of the field p found by brute force with a length of about 768 bits for the implementation of the SIDH algorithm on the 3- and 5-isogeny of complete Edwards curves (see Table 1).

Table 1. Automatic search results by SIDH algorithm.

#	m	n	$p = 4 \times 3^m \times 5^n - 1$	$\log p$, bit
1	238	165	0×50f6d0ab1dad4fb9048ca2e5357e7fa140806f49f72b711a651962 fd24d6ae30953eeb9cafca76f39eae708b2bfa6926d7df2937074b00 4fa4d966e8ecd7469bc771d4dd084b5a9f358a2c83e4f67398f1b79 72610af76087956accd41b0c33	763
2	243	168	0×25869530ff4e3ece49cacad3ea2e345995ec4714b12e4378f2d1a7 30421dfc56067c5ca5ec3dffe7e410ebab910f1cd27fd7af93404254 11e9f0bf417f1dbafadd8d935fbe0324ed80899da7d593f60de8304e 6f2585c2dde7751b31562d544edeb	778
3	247	156	0×d0e0e81c7cf2831a189cf43da28062552d4a98e390e7b3f3bb8bd 34b91e364d7849480255df7222b93e45fe7640850a6e60e1afd64a0 7ee55f821e7009ec557cfbd9abca5dd1b758d06ec0939ca37cc685f9 37196f3bd26aa01ae966c35eb	756

9 Conclusions and Future Work

Thus, the use of 3- and 5-isogeny of Edwards curves for points of odd order with a fixed resistance to attacks by a quantum computer will allow bypassing the problems of singular points inherent to 2-isogenies of these curves. Estimates of the complexity of computing the 3- and 5-isogeny of Edwards curves, comparable to *w* the complexity of group operations, allow us to implement the fastest post-quantum cryptography algorithms. Experimental estimates of the computational efficiency of these isogenies in the implementation of the SIDH algorithm are planned to be considered in the next paper.

References

1. Jao, D., de Feo, L.: Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. Lect. Notes Comput. Sci.: 19–34 (2011). https://doi.org/10.1007/978-3-642-25405-5_2
2. Bernstein, D. J., Lange, T.: Faster addition and doubling on elliptic curves. Lect. Notes Comput. Sci. **4833**: 29–50 (2007). https://doi.org/10.1007/978-3-540-76900-2_3
3. Bernstein, D. J., Birkner, P., Joye, M., Lange, T., Peters, C.: Twisted Edwards Curves. Lect. Notes Comput. Sci.: 389–405 (2008). https://doi.org/10.1007/978-3-540-68164-9_26
4. Moody, D., Shumow, D.: Analogues of Velu's formulas for isogenies on alternate models of elliptic curves. Math. Computation **85**(300), 1929–1951 (2015). https://doi.org/10.1090/mcom/3036
5. Ahmadi, O., Granger, R.: On isogeny classes of Edwards curves over finite fields. J. Number Theory **132**(6), 1337–1358 (2012). https://doi.org/10.1016/j.jnt.2011.12.013
6. Bessalov, A. V., Tsygankova, O. V.: Edwards supersingular complete curves over a simple field. Radio eng. **191**: 88–98 (2017). [Publication in Russian]
7. Bessalov, A. V., Tsygankova, O. V.: Interrelation of families of points of high order on the Edwards curve over a prime field. Probl. Inf. Transm. **51**(4): 391–397 (2015). https://doi.org/10.1134/s0032946015040080. [Publication in Russian]
8. Bessalov, A. V.: Calculation of parameters of cryptic criviae Edwards over the fields of characteristics 5 and 7. Cybersecur. Educ. Sci. Tech. **1**: 94–104 (2018). https://doi.org/10.28925/2663-4023.2018.1.94104
9. Washington, L.: Elliptic Curves. Discrete Mathematics and Its Applications. (2008). https://doi.org/10.1201/9781420071474