How to Construct CSIDH on Edwards Curves

Tomoki Moriya[1], Hiroshi Onuki[1], and Tsuyoshi Takagi[1]

Department of Mathematical Informatics, The University of Tokyo, Japan
{tomoki_moriya,onuki,takagi}@mist.i.u-tokyo.ac.jp

Abstract. CSIDH is an isogeny-based key exchange protocol proposed by Castryck, Lange, Martindale, Panny, and Renes in 2018. CSIDH is based on the ideal class group action on $\mathbb{F}_p$-isomorphic classes of Montgomery curves. In order to calculate the class group action, we need to take points defined over $\mathbb{F}_{p^2}$. The original CSIDH algorithm requires a calculation over $\mathbb{F}_p$ by representing points as x-coordinate over Montgomery curves. Meyer and Reith proposed a faster CSIDH algorithm in 2018 which calculates isogenies on Edwards curves by using a birational map between a Montgomery curve and an Edwards curve. If we try to calculate the class group action on Edwards curves in a similar way on Montgomery curves, we have to consider points defined over $\mathbb{F}_{p^4}$. Therefore, it is not a trivial task to calculate the class group action on Edwards curves over $\mathbb{F}_p$.

In this paper, we prove a number of theorems on the properties of Edwards curves. By using these theorems, we devise a new CSIDH algorithm that uses only Edwards curves while calculating over $\mathbb{F}_p$. This algorithm is as fast as (or a little bit faster than) the algorithm proposed by Meyer and Reith.

Keywords: Isogeny-based cryptography · Montgomery curves · Edwards curves · CSIDH · Post-quantum cryptography.

1 Introduction

Currently, there are two popular public-key cryptosystems: RSA [18], whose security is based on the computational complexity of the Prime Factorization Problem, and Elliptic Curve Cryptography [15, 13], whose security is based on the computational complexity of the Discrete Logarithm Problem. However, Shor pointed out in 1994 that both the Prime Factorization Problem and the Discrete Logarithm Problem can be solved in polynomial time by using a quantum computer [19, 20]. This means we should develop new cryptosystems which cannot be broken by quantum computers. We call such cryptosytems post quantum cryptography (PQC).

Isogeny-based cryptography is a public-key cryptosystem based on the computational complexity of the Isogeny Problem, which is a problem arising when we calculate isogenies between given two elliptic curves. It is considered to be a candidate of PQC. Jao and De Feo proposed a Diffie-Hellman type isogeny-based key exchange protocol, called SIDH (Supersingular Isogeny Diffie-Hellman), in 2011 [11]. SIKE (Supersingular Isogeny Key Encapsulation) [1], which is derived from SIDH, has been selected as a candidate of NIST PQC standardization [17]. The SIDH calculation uses supersingular elliptic curves over $\mathbb{F}_{p^2}$. Castryck, Lange, Martindale, Panny, and Renes proposed another Diffie-Hellman type of isogeny-based key exchange protocol, called CSIDH (Commutative Supersingular Isogeny Diffie-Hellman), in 2018 [4]. Its calculation uses supersingular elliptic curves over $\mathbb{F}_p$.

CSIDH is based on the commutative group action on $\mathbb{F}_p$-isomorphism classes of supersingular Montgomery curves defined over $\mathbb{F}_p$. In order to calculate this group action, we need to generate a point in $\ker(\pi_p - 1)$ or in $\ker(\pi_p + 1)$ and determine which set the point belongs to, where π_p is the p-Frobenius map. Castryck et al. showed that if we take a random element from $\mathbb{F}_p$ as an x-coordinate of a point in a Montgomery curve and determine whether y-coordinate of the point belongs to $\mathbb{F}_p$ or not, then we can get a point in $\ker(\pi_p - 1)$ or in $\ker(\pi_p + 1)$ and determine which set the point belongs to. Castryck et al. also showed that a Montgomery coefficient is unique up to $\mathbb{F}_p$-isomorphism. Since it is known that a group operation of a Montgomery curve can be calculated using only the x-coordinates of the points [16] and that isogenies between Montgomery curves can be also calculated by using only the x-coordinates of the points of the kernel [5, 14], we can calculate the original CSIDH algorithm over $\mathbb{F}_p$.

Table 1. Comparing CSIDH algorithms on Montgomery curves and Edwards curves

	group operations	calculation of isogenies	kernel points
Montgomery	✓	✓	✓
Edwards	✓	✓	not trivial

Meyer and Reith proposed a faster CSIDH algorithm in 2018 [14]. This algorithm calculates isogenies over not Montgomery curves but rather Edwards curves, by using a birational map between a Montgomery curve and an Edwards curve. In this algorithm, the method for generating a point in $\ker(\pi_p - 1)$ or in $\ker(\pi_p + 1)$ and determining which set the point belongs to is the same as in the original CSIDH algorithm proposed by Castryck et al. Hence, a question arises: How do we calculate the CSIDH algorithm on *purely* Edwards curves over $\mathbb{F}_p$?

There is a special coordinate (the w-coordinate) on Edwards curves for calculating the group operation [9] and isogenies [12] efficiently. However, if we take a random element from $\mathbb{F}_p$ as the w-coordinate of a point on an Edwards curve, the point is sometimes defined outside of $\mathbb{F}_{p^2}$ (defined over $\mathbb{F}_{p^4}$). Since the points in $\ker(\pi_p - 1)$ and those in $\ker(\pi_p + 1)$ are defined over $\mathbb{F}_{p^2}$, it is not a trivial task to run the CSIDH algorithm using only Edwards curves over $\mathbb{F}_p$.

We summarize the above discussion in Table 1.

1.1 Our results

In this paper, we prove three important theorems about Edwards curves and use them to construct a new CSIDH algorithm. First, we show that if we take a random element from $\mathbb{F}_p^{\times 2}$ (the set of square elements in $\mathbb{F}_p$) as the w-coordinate of a point P and determine whether the w-coordinate of $2P$ is square in $\mathbb{F}_p$ or not, then we can generate a point in $\ker(\pi_p - 1)$ or in $\ker(\pi_p + 1)$ and determine which set the point belongs to. Specifically, if the w-coordinate of $2P$ is square, then this coordinate represents a point in $\ker(\pi_p + 1)$, and if the w-coordinate of $2P$ is not square, then the reciprocal of this coordinate represents a point in $\ker(\pi_p - 1)$. Second, we show that there is no difference between the probability of generating a point in $\ker(\pi_p - 1)$ and the probability of generating a point in $\ker(\pi_p + 1)$ in the previous way. Finally, we show that an Edwards coefficient is unique up to an $\mathbb{F}_p$-isomorphism, like a Montgomery coefficient.

By using these theorems, we can construct a new CSIDH algorithm that only uses Edwards curves (Algorithm 1). Moreover, we show that our algorithm is as fast as (or a little bit faster than) the algorithm proposed by Meyer and Reith, which as far as we know, is the state of the art.

2 Preliminaries

2.1 Basic mathematical concepts

Here, we explain basic mathematical concepts behind isogeny-based cryptography.

Let $\mathbb{L}$ be a field, and $\mathbb{L}'$ be an algebraic extensional field of $\mathbb{L}$. An elliptic curve E defined over $\mathbb{L}$ is a non-singular algebraic curve defined over $\mathbb{L}$ of genus one. Denote by $E(\mathbb{L}')$ the $\mathbb{L}'$-rational points of the elliptic curve E. $E(\mathbb{L}')$ is an abelian group [21, Ⅲ. 2]. A supersingular elliptic curve E over a finite field $\mathbb{L}$ of characteristic p is defined as an elliptic curve which satisfies $\#E(\mathbb{L}) \equiv 1 \pmod{p}$, where $\#E(\mathbb{L})$ is the cardinality of $E(\mathbb{L})$.

Let E, E' be elliptic curves defined over $\mathbb{L}$. Define an isogeny $\phi\colon E \to E'$ over $\mathbb{L}'$ to be a rational map over $\mathbb{L}'$ which is a non-zero group homomorphism from $E(\overline{\mathbb{L}})$ to $E'(\overline{\mathbb{L}})$, where $\overline{\mathbb{L}}$ is the algebraic closure of $\mathbb{L}$. A separable isogeny with $\# \ker \phi = \ell$ is called an ℓ-isogeny. Denote by $\mathrm{End}_{\mathbb{L}'}(E)$ the endomorphism ring of E over $\mathbb{L}'$. It is represented as $\mathrm{End}_p(E)$ when $\mathbb{L}'$ is a prime field $\mathbb{F}_p$. An isogeny $\phi\colon E \to E'$ defined over $\mathbb{L}'$ is called an isomorphism over $\mathbb{L}'$, if ϕ has an inverse isogeny over $\mathbb{L}'$.

If G is a finite subgroup of $E(\overline{\mathbb{L}})$, then there exists an isogeny $\phi\colon E \to E'$ whose kernel is G, and E' is unique up to an $\overline{\mathbb{L}}$-isomorphism [21, Proposition Ⅲ.4.12]. This isogeny can be efficiently calculated by using Vélu formulas [22]. We denote a representative of E' by E/G.

$E[k]$ $(k \in \mathbb{Z}_{>0})$ is defined as the k-torsion subgroup of $E(\overline{\mathbb{L}})$. For an endomorphism ϕ of E, we sometimes denote $\ker \phi$ by $E[\phi]$.

Let $\mathbb{L}$ be a number field, and $\mathcal{O}$ be its order. A fractional ideal $\mathfrak{a}$ of $\mathcal{O}$ is a finitely generated $\mathcal{O}$-submodule of $\mathbb{L}$ which satisfies $\alpha\mathfrak{a} \subset \mathcal{O}$ for some $\alpha \in \mathcal{O} \setminus \{0\}$. An invertible fractional ideal $\mathfrak{a}$ of $\mathcal{O}$ is defined as a fractional ideal of $\mathcal{O}$ which satisfies $\mathfrak{a}\mathfrak{b} = \mathcal{O}$ for some fractional ideal $\mathfrak{b}$ of $\mathcal{O}$. The fractional ideal $\mathfrak{b}$ is represented as $\mathfrak{a}^{-1}$. If a fractional ideal $\mathfrak{a}$ is contained in $\mathcal{O}$, then $\mathfrak{a}$ is called an integral ideal of $\mathcal{O}$.

Let $I(\mathcal{O})$ be a set of invertible fractional ideals of $\mathcal{O}$. $I(\mathcal{O})$ is an abelian group derived from multiplication of ideals with the identity $\mathcal{O}$. Let $P(\mathcal{O})$ be a subgroup of $I(\mathcal{O})$ defined by $P(\mathcal{O}) = \{\mathfrak{a} \mid \mathfrak{a} = \alpha\mathcal{O} \text{ (for some } \alpha \in \mathbb{L}^{\times})\}$. We call an abelian group $\mathrm{cl}(\mathcal{O})$ defined by $I(\mathcal{O})/P(\mathcal{O})$ an ideal class group of $\mathcal{O}$.

The $\mathbb{F}_p$-endomorphism ring $\mathrm{End}_p(E)$ of a supersingular elliptic curve E defined over $\mathbb{F}_p$ is isomorphic to an order in an imaginary quadratic field [7]. Denote by $\mathcal{E}\ell\ell_p(\mathcal{O})$ the set of $\mathbb{F}_p$-isomorphism classes of elliptic curves E whose $\mathbb{F}_p$-endomorphism ring $\mathrm{End}_p(E)$ is isomorphic to $\mathcal{O}$.

2.2 Montgomery curves

Let $\mathbb{L}$ be a field whose characteristic is odd. An elliptic curve E defined by the following equation is called a Montgomery curve:

$$E\colon bY^2Z = X^3 + aX^2Z + XZ^2 \quad (a, b \in \mathbb{L} \text{ and } b(a^2-4) \neq 0).$$

In this paper, we denote the Montgomery curve $Y^2Z = X^3 + aX^2Z + XZ^2$ by $E_{\mathcal{M},a}$. The identity of E is $(0 : 1 : 0)$, and the inverse point of $(X : Y : Z)$ is $(X : -Y : Z)$.

Montgomery showed that the group calculations of Montgomery curves can be efficiently computed by using x-coordinates [16]. Define a function x as

$$x(X : Y : Z) = \frac{X}{Z}.$$

The function x is not defined at the point $(0 : 1 : 0)$. If P and Q satisfy $x(P) = x(Q)$, then $P = Q$ or $P = -Q$. Next define a function $\mathbf{x}$ as $\mathbf{x}(X : Y : Z) = (X : Z)$. We call $\mathbf{x}(P)$ the projective x-coordinates of P.

Let P be a point on E. Let $A/C = a$ and $B/C = b$. Let $(X : Z) = \mathbf{x}(P)$. The projective x-coordinates $(X' : Z')$ of $2P$ are calculated as follows [16]:

$$X' = 4C(X + Z)^2(X - Z)^2, \quad Z' = 4XZ(4C(X - Z)^2 + (A + 2C)4XZ). \tag{1}$$

The computational cost is $4\mathbf{M}$+$2\mathbf{S}$+$4\mathbf{a}$. If $Z = 1$, the computational cost is $4\mathbf{M}$+$1\mathbf{S}$+$5\mathbf{a}$. (We denote field multiplications by $\mathbf{M}$, field squarings by $\mathbf{S}$, and field additions or subtractions or doublings by $\mathbf{a}$.)

Let P_1 and P_2 be points on E_d, and $(X_1 : Z_1) = \mathbf{x}(P_1)$, $(X_2 : Z_2) = \mathbf{x}(P_2)$. Let $(X_0 : Z_0) = \mathbf{x}(P_1 - P_2)$. The projective x-coordinates $(X_3 : Z_3)$ of $P_1 + P_2$ are calculated as follows [16]:

$$X_3 = Z_0(X_1X_2 - Z_1Z_2)^2, \quad Z_3 = X_0(X_1Z_2 - X_2Z_1)^2. \tag{2}$$

The computational cost is $4\mathbf{M} + 2\mathbf{S} + 6\mathbf{a}$. If $Z_0 = 1$, the computational cost is $3\mathbf{M} + 2\mathbf{S} + 6\mathbf{a}$.

Costello and Hisil proposed efficient calculations for odd-degree isogenies by using x-coordinates [5], and Meyer and Reith improved them [14]. Let ℓ be an odd number and s be the number which satisfies that $\ell = 2s + 1$. Let P be a point on E, and $(X : Z) = \mathbf{x}(P)$. Let Q be an ℓ-order point on E, and $(X_1 : Z_1) = \mathbf{x}(Q)$. Let $(X_k : Z_k) = \mathbf{x}(kQ)$. Let $E' = E/\langle Q\rangle$ and ϕ be an isogeny $\phi \colon E \to E'$ with $\ker\phi = \langle Q\rangle$. The projective x-coordinates $(X' : Z')$ of $\phi(P)$ are calculated as follows [5]:

$$X' = X \cdot \prod_{i=1}^{s}(XX_i - ZZ_i)^2, \quad Z' = Z \cdot \prod_{i=1}^{s}(XZ_i - ZX_i)^2. \tag{3}$$

The computational cost is $(4s)\mathbf{M} + 2\mathbf{S} + (4s + 2)\mathbf{a}$. Let $A/C = a$. The curve coefficient $a' = A'/C'$ of E' is calculated as follows [14]:

$$\begin{aligned} \tilde{a} = A + 2C, \quad \tilde{d} = A - 2C, \quad \tilde{a}' = \tilde{a}^{\ell} \cdot \prod_{i=1}^{s}(X_i + Z_i)^8, \\ \tilde{d}' = \tilde{d}^{\ell} \cdot \prod_{i=1}^{s}(X_i - Z_i)^8, \quad A' = 2(\tilde{a}' + \tilde{d}'), \quad C' = \tilde{a}' - \tilde{d}'. \end{aligned} \tag{4}$$

The computational cost is $(2s+2)\mathbf{M} + 6\mathbf{S} + (2s+6)\mathbf{a}$ and that of the two s-th powers. Since $X_i + Z_i$ and $X_i - Z_i$ are also used for calculating $\phi(P)$, the computational cost of calculating $\phi(P)$ and E' is $(6s + 2)\mathbf{M} + 8\mathbf{S} + (4s + 8)\mathbf{a}$ and that of the two s-th powers.

Appendix A.1 describes why the computational costs are as above.

2.3 Edwards curves

In 2007, Edwards introduced a new form of an elliptic curve [8]. Bernstein and Lange extended these curves to another form in 2007, called Edwards curves [3]. For representing points at infinity, Hisil, Wong, Carter, and Dawson proposed projective closures of Edwards curves in $\mathbb{P}^3$ in 2018 [10].

Let $\mathbb{L}$ be a field. If an elliptic curve E is defined by the following equation, E is called an Edwards curve [10]:

$$E\colon X^2+Y^2=Z^2+dT^2, \quad XY=ZT \quad (d\in\mathbb{L} \text{ and } d\neq 0,1).$$

In this paper, we denote the Edwards curve $X^2+Y^2=Z^2+dT^2,\ XY=ZT$ by E_d. The identity of E_d is $(0:1:1:0)$, which we will denote by 0_d for simplicity, while the inverse point of $(X:Y:Z:T)$ is $(-X:Y:Z:-T)$. We obtain the group addition formulas as follows [10]:

$$\begin{aligned}&(X_1:Y_1:Z_1:T_1)+(X_2:Y_2:Z_2:T_2)\\ &=((X_1Y_2+Y_1X_2)(Z_1Z_2-dT_1T_2):(Y_1Y_2-X_1X_2)(Z_1Z_2+dT_1T_2)\\ &\quad:(Z_1Z_2-dT_1T_2)(Z_1Z_2+dT_1T_2):(Y_1Y_2-X_1X_2)(X_1Y_2+Y_1X_2)).\end{aligned} \tag{5}$$

For simplicity, we will sometimes consider an Edwards curve to be an affine curve defined by the following equation:

$$E\colon x^2+y^2=1+dx^2y^2 \quad (d\in\mathbb{L} \text{ and } d\neq 0,1),$$

where $x=X/Z$ and $y=Y/Z$. In this equation, only $(\pm\sqrt{d}:0:0:1)$ and $(0:\pm\sqrt{d}:0:1)$ are points at infinity. $(\pm\sqrt{d}:0:0:1)$ are points of order 2, and $(0:\pm\sqrt{d}:0:1)$ are points of order 4. Hence, if the order of a point P on E_d is neither 2 nor 4, P can be represented in affine coordinates (x,y).

Farashahi and Hosseini showed that the group calculations of Edwards curves can be efficiently performed by using the w-coordinate [9]. Define a function w as

$$w(X:Y:Z:T)=\begin{cases}\frac{dT^2}{Z^2} & (\text{if } Z\neq 0)\\ \infty & (\text{if } Z=0 \text{ (points at infinity)})\end{cases}.$$

In affine coordinates, $w(x,y)=dx^2y^2$. We call $w(P)$ the w-coordinate of P. If P and Q satisfy that $w(P)=w(Q)$, then $P+Q$ or $P-Q$ is an element of

$$\{0_d,(0:-1:1:0),(1:0:1:0),(-1:0:1:0)\}.$$

In this paper, we will denote $\{0_d,(0:-1:1:0),(1:0:1:0),(-1:0:1:0)\}$ by $\mathcal{G}_4$ for simplicity. Note that $\mathcal{G}_4$ is a cyclic group of order 4. Define a function $\mathbf{w}$ as $\mathbf{w}(X:Y:Z:T)=(dT^2:Z^2)$. We call $\mathbf{w}(P)$ the projective w-coordinates of P.

Let P be a point on E_d, and $(W:Z)=\mathbf{w}(P)$. Let $D/C=d$. The projective w-coordinates $(W':Z')$ of $2P$ are calculated as follows [9]:

$$W'=4WZ(D(W+Z)^2-4CWZ), \quad Z'=D(W+Z)^2(W-Z)^2. \tag{6}$$

The computational cost is $4\mathbf{M}+2\mathbf{S}+4\mathbf{a}$. If $Z=1$, the computational cost is $4\mathbf{M}+1\mathbf{S}+5\mathbf{a}$.

Let P_1 and P_2 be points on E_d, and $(W_1 : Z_1) = \mathbf{w}(P_1)$, $(W_2 : Z_2) = \mathbf{w}(P_2)$. Let $(W_0 : Z_0) = \mathbf{w}(P_1 - P_2)$. The projective w-coordinates $(W_3 : Z_3)$ of $P_1 + P_2$ are calculated as follows [9]:

$$W_3 = Z_0(W_1Z_2 - W_2Z_1)^2, \quad Z_3 = W_0(W_1W_2 - Z_1Z_2)^2. \tag{7}$$

The computational cost is $4\mathbf{M} + 2\mathbf{S} + 6\mathbf{a}$. If $Z_0 = 1$, the computational cost is $3\mathbf{M} + 2\mathbf{S} + 6\mathbf{a}$.

Kim, Yoon, Park, and Hong proposed efficient calculations for odd-degree isogenies by using projective w-coordinates [12]. Let ℓ be an odd number and s be the number which satisfies $\ell = 2s + 1$. Let P be a point on E_d, and $(W : Z) = \mathbf{w}(P)$. Let Q be an ℓ-order point on E_d, and $(W_1 : Z_1) = \mathbf{w}(Q)$. Let $(W_k : Z_k) = \mathbf{w}(kQ)$. Let $E_{d'} = E_d/\langle Q \rangle$, and ϕ be an isogeny $\phi \colon E_d \to E_{d'}$ with $\ker \phi = \langle Q \rangle$. The projective w-coordinates $(W' : Z')$ of $\phi(P)$ are calculated as follows [12]:

$$W' = W \cdot \prod_{i=1}^{s} (ZW_i - ZW_i)^2, \quad Z' = Z \cdot \prod_{i=1}^{s} (WW_i - ZZ_i)^2. \tag{8}$$

The computational cost is $(4s)\mathbf{M} + 2\mathbf{S} + (4s+2)\mathbf{a}$. The projective curve coefficient $d' = D'/C'$ is calculated as follows [12]:

$$D' = D^{\ell} \cdot \prod_{i=1}^{s} (W_i + Z_i)^8, \quad C' = C^{\ell} \cdot \prod_{i=1}^{s} (2Z_i)^8. \tag{9}$$

The computational cost is $(2s + 2)\mathbf{M} + 6\mathbf{S} + (s + 4)\mathbf{a}$ and that of the two s-th powers. Since $W_i + Z_i$ is also used for calculating $\phi(P)$, the computational cost of calculating $\phi(P)$ and $E_{d'}$ is $(6s + 2)\mathbf{M} + 8\mathbf{S} + (4s + 6)\mathbf{a}$ and that of the two s-th powers.

Appendix A.2 describes why the computational costs are as above.

An Edwards curve has a following property.

Theorem 1. *Let p be a prime and $p \geq 3$. The Edwards curve E_d defined over $\mathbb{F}_p$ is $\mathbb{F}_p$-isomorphic to the Montgomery curve,*

$$E_{\mathcal{M}} \colon \frac{4}{1-d} Y^2 Z = X^3 + \frac{2(1+d)}{1-d} X^2 Z + XZ^2.$$

Proof. Bernstein, Birkner, Joye, Lange, and Peters show that there is a birational map between E_d and $E_{\mathcal{M}}$ [2]. This birational map becomes an isomorphism.

The proof of this theorem is given in Appendix B. □

It is known that there is a birational map between a Montgomery curve and an Edwards curve [2]. However, we need an isomorphism for constructing the CSIDH algorithm using only Edwards curves.

Corollary 1. *Let p be a prime, $p \geq 3$, and $p \equiv 3 \pmod 4$. An Edwards curve E_d defined over $\mathbb{F}_p$ is $\mathbb{F}_p$-isomorphic to the Montgomery curve,*

$$E_{\mathcal{M}} \colon Y^2 Z = X^3 + \left(\frac{1-d}{p}\right) \cdot \frac{2(1+d)}{1-d} X^2 Z + XZ^2,$$

where $\left(\frac{1-d}{p}\right)$ is the Legendre symbol.

Corollary 1 is easily proven from Theorem 1.

Corollary 2. *Let p be a prime, $p \geq 3$, and $p \equiv 3 \pmod 8$. Let $E_{\mathcal{M},a}$ be a supersingular Montgomery curve $Y^2Z = X^3 + aX^2Z + XZ^2$ defined over $\mathbb{F}_p$. If $a-2$ is square, then $E_{\mathcal{M},a}$ is $\mathbb{F}_p$-isomorphic to the Edwards curve,*

$$E_{\frac{a+2}{a-2}} \colon X^2 + Y^2 = Z^2 + \frac{a+2}{a-2}T^2, \quad XY = ZT,$$

and if $a-2$ is not square, then $E_{\mathcal{M},a}$ is $\mathbb{F}_p$-isomorphic to the Edwards curve,

$$E_{\frac{a-2}{a+2}} \colon X^2 + Y^2 = Z^2 + \frac{a-2}{a+2}T^2, \quad XY = ZT.$$

Proof. As $E_{\mathcal{M},a}$ is supersingular, $\#E_{\mathcal{M},a}(\mathbb{F}_p) = \#\tilde{E}_{\mathcal{M},a}(\mathbb{F}_p) = p + 1 \equiv 4 \pmod 8$, where $\tilde{E}_{\mathcal{M},a}$ is a quadratic twist of $E_{\mathcal{M}}$. From Table 1 of [6], $(a-2)(a+2)$ is not square.

If $a-2$ is square, the Edwards curve $E_{\frac{a+2}{a-2}}$ is $\mathbb{F}_p$-isomorphic to $E_{\mathcal{M},a}$ by Corollary 1. If $a-2$ is not square, since $a+2$ is square, the Edwards curve $E_{\frac{a-2}{a+2}}$ is $\mathbb{F}_p$-isomorphic to $E_{\mathcal{M},a}$ by Corollary 1.

This completes the proof of Corollary 2. □

By using Corollary 1 and Corollary 2, it is easy to convert an Edwards curve into a Montgomery curve and convert a Montgomery curve into an Edwards curve.

3 CSIDH [4]

CSIDH (Commutative Supersingular Isogeny Diffie-Hellman) was proposed by Castryck et al. in 2018 [4].

CSIDH is based on the action of $\mathrm{cl}(\mathbb{Z}[\pi_p])$ on $\mathcal{E}\ell\ell_p(\mathbb{Z}[\pi_p])$. Let the prime p be $4 \cdot \ell_1 \cdots \ell_n - 1$, where the $\ell_1, \ldots, \ell_n$ are small distinct odd primes, for Alice and Bob to calculate the action efficiently. Alice and Bob let random elements of $\mathrm{cl}(\mathbb{Z}[\pi_p])$ be secret keys and calculate the actions on $E_{\mathcal{M},0} \colon Y^2Z = X^3 + XZ^2$. They publish the obtained elliptic curves as public keys. Finally, they calculate the actions on the public keys, respectively. The obtained elliptic curves are identical up to $\mathbb{F}_p$-isomorphism by the commutativity of $\mathrm{cl}(\mathbb{Z}[\pi_p])$; therefore, the values of the Montgomery coefficients are the same as in Theorem 3. Let their values be $\mathrm{SK}_{\mathrm{shared}}$.

3.1 CSIDH protocol

Before explaining the protocol of CSIDH, we should state the following important theorems.

Theorem 2 ([23, Theorem 4.5]). *Let $\mathcal{O}$ be an order of an imaginary quadratic field and E be an elliptic curve defined over $\mathbb{F}_p$. If $\mathcal{E}\ell\ell_p(\mathcal{O})$ contains the $\mathbb{F}_p$-isomorphism class of supersingular elliptic curves, then the action of the ideal class group $\mathrm{cl}(\mathcal{O})$ on $\mathcal{E}\ell\ell_p(\mathcal{O})$,*

$$\begin{aligned} \mathrm{cl}(\mathcal{O}) \times \mathcal{E}\ell\ell_p(\mathcal{O}) &\longrightarrow \mathcal{E}\ell\ell_p(\mathcal{O}) \\ ([\mathfrak{a}], E) &\longmapsto E/E[\mathfrak{a}] \end{aligned}$$

is free and transitive, where $\mathfrak{a}$ is an integral ideal of $\mathcal{O}$, and $E[\mathfrak{a}]$ is the intersection of the kernels of elements in the ideal $\mathfrak{a}$.

Denote a representative of $E/E[\mathfrak{a}]$ by $[\mathfrak{a}]E$.

Theorem 3 ([4, Proposition 8]). *Let p be a prime satisfying $p \equiv 3 \pmod 8$. Let E be a supersingular elliptic curve defined over $\mathbb{F}_p$. Then, $\mathrm{End}_p(E) = \mathbb{Z}[\pi_p]$ holds if and only if there uniquely exists $a \in \mathbb{F}_p$ such that E is $\mathbb{F}_p$-isomorphic to a Montgomery curve $E_{\mathcal{M},a}$, where π_p is the p-Frobenius map.*

The exact protocol is as follows. Let Alice and Bob want to share a secret key denoted by $\mathrm{SK}_{\mathrm{shared}}$.

Setup. Let p be a prime which satisfies $p = 4 \cdot \ell_1 \cdots \ell_n - 1$, where $\ell_1, \ldots, \ell_n$ are small distinct odd primes. Let the public parameters be p and $E_{\mathcal{M},0}$.

Key generation. One randomly chooses a integer vector $(e_1, \ldots, e_n)$ from $\{-m, \ldots, m\}^n$. Define $[\mathfrak{a}] = [\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n}] \in \mathrm{cl}(\mathbb{Z}[\pi_p])$, where $\mathfrak{l}_i = (\ell_i, \pi_p - 1)$, $\mathfrak{l}_i^{-1} = (\ell_i, \pi_p + 1)$, and m is the smallest integer which satisfies $2m + 1 \geq \sqrt[n]{\#\mathrm{cl}(\mathbb{Z}[\pi_p])} \approx p^{1/2n}$. One calculates the action of $[\mathfrak{a}]$ on $E_{\mathcal{M},0}$ and the Montgomery coefficient $a \in \mathbb{F}_p$ of $[\mathfrak{a}]E_{\mathcal{M},0} \colon Y^2Z = X^3 + aX^2Z + XZ^2$.
Let the integer vector $(e_1, \ldots, e_n)$ be the secret key, and $a \in \mathbb{F}_p$ be the public key.

Key exchange. Alice and Bob have pairs of keys, $([\mathfrak{a}], a)$ and $([\mathfrak{b}], b)$, respectively. Alice calculates the action $[\mathfrak{a}]E_{\mathcal{M},b} = [\mathfrak{a}][\mathfrak{b}]E_{\mathcal{M},0}$. Bob calculates the action $[\mathfrak{b}]E_{\mathcal{M},a} = [\mathfrak{b}][\mathfrak{a}]E_{\mathcal{M},0}$. Denote the Montgomery coefficient of $[\mathfrak{a}][\mathfrak{b}]E_{\mathcal{M},0}$ by SK_{Alice} and the Montgomery coefficient of $[\mathfrak{b}][\mathfrak{a}]E_{\mathcal{M},0}$ by SK_{Bob}.

From the commutativity of $\mathrm{cl}(\mathbb{Z}[\pi_p])$ and Theorem 3, $\mathrm{SK}_{Alice} = \mathrm{SK}_{Bob}$ holds. Let these values be the shared key $\mathrm{SK}_{\mathrm{shared}}$.

3.2 Evaluating the class group action on Montgomery curves [4]

In this subsection, we explain how to evaluate the class group action on Montgomery curves. Algorithm 2 in Appendix D is the algorithm for evaluating the class group action.

The inputs of the algorithm are a Montgomery coefficient $a \in \mathbb{F}_p$ and a list of integers $(e_1, \ldots, e_n)$. The output is a Montgomery coefficient $a' \in \mathbb{F}_p$ that satisfies $E_{\mathcal{M},a'} = [\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n}]E_{\mathcal{M},a}$. Let p be a prime satisfying $p = 4 \cdot \ell_1 \cdots \ell_n - 1$, where $\ell_1, \ldots, \ell_n$ are small distinct odd primes.

We calculate a' by repeating the calculations of the actions of $[\mathfrak{l}_i]$ or $[\mathfrak{l}_i]^{-1}$ (i.e., repeating the calculations of ℓ_i-isogenies).

Sampling points For calculating the class group action, we first sample a point which belongs to $\ker(\pi_p - 1)$ or $\ker(\pi_p + 1)$. We take a uniformly random element of $\mathbb{F}_p$. Let the element be x, and P be a point in $E_{\mathcal{M},a}$ such that $x(P) = x$. We calculate $x^3 + ax^2 + x$, which is a square of $y(P)$, where $y(P)$ is the y-coordinate of P. If $x^3 + ax^2 + x$ is square in $\mathbb{F}_p$, then $P \in \ker(\pi_p - 1)$, and if $x^3 + ax^2 + x$ is not square in $\mathbb{F}_p$, then $P \in \ker(\pi_p + 1)$. If $x^3 + ax^2 + x$ is square, we define S to be a set of i such that the sign of e_i is $+1$, and if $x^3 + ax^2 + x$ is not square, we define S to be a set of i such that the sign of e_i is -1. If $S = \emptyset$, we repeat this procedure with another sample point.

Scalar multiplication Next, we calculate $P_1 = \frac{p+1}{k}(P)$, where $k = \prod_{i \in S} \ell_i$. The calculation uses the Montgomery ladder algorithm [16].

Calculation of isogenies We calculate $P_2 = \frac{k}{\ell_i} P_1$. The order of P_2 is 1 or ℓ_i. If P_2 is not the identity, we get a point of order ℓ_i. Then, we calculate an ℓ_i-isogeny,

$$\phi \colon E_{\mathcal{M},a} \longrightarrow E_{\mathcal{M},a}/\langle P_2 \rangle,$$

by using the formulas in [5, 14]. Denote the Montgomery coefficient of $E_{\mathcal{M},a}/\langle P_2 \rangle$ by $a' \in \mathbb{F}_p$. From Theorem 3, a' is unique. We redefine e_i as $e_i - 1$ (if $e_i > 0$) or $e_i + 1$ (if $e_i < 0$), k as k/ℓ_i, P_1 as $\phi(P_1)$, and a as a'.

We repeat this calculation for all $i \in S$. After that, if the list of integers $(e_1, \ldots, e_n)$ is not the zero vector, we return to the **Sampling points** part.

Output If the list of integers $(e_1, \ldots, e_n)$ is the zero vector, we output the Montgomery coefficient $a' \in \mathbb{F}_p$.

4 Main theorems used for our algorithm

Here, we state and prove three theorems needed to construct the algorithm for evaluating the class group action based on Edwards curves.

The lemmas used in the proofs of the theorems are proven in Appendix C.

Theorem 4. *Let $p \equiv 3 \pmod 8$. Let P be a point on an Edwards curve E_d such that the w-coordinate $w(P) \in \mathbb{F}_p$, the order of P is not a power of 2, and $w(P)$ is square. If $w(2P)$ is square, there exists P' such that $P' \in E_d[\pi_p + 1]$, $w(2P) = w(P')$, and $\frac{p+1}{4} P' = 0_d$. If $w(2P)$ is not square, there exists P' such that $P' \in E_d[\pi_p - 1]$, $1/w(2P) = w(P')$, and $\frac{p+1}{4} P' = 0_d$.*

Proof. Let (x, y) be the coordinates of P. Let P_{odd} and P_{2power} be points of E_d such that $P = P_{odd} + P_{2power}$, the order of P_{odd} is odd, and the order of P_{2power} is a power of 2. The existence of P_{odd} and P_{2power} are guaranteed by Lemma 6. By Lemma 7, one of the following holds.

- $(\pi_p - 1)(P_{2power}) \in \mathcal{G}_4$ and $P_{odd} \in E[\pi_p - 1]$.
- $(\pi_p + 1)(P_{2power}) \in \mathcal{G}_4$ and $P_{odd} \in E[\pi_p + 1]$.

It is easy to check that $(\pi_p + 1)\mathcal{G}_4 = \{0_d, (0, -1)\}$ and $(\pi_p - 1)\mathcal{G}_4 = \{0_d\}$. Therefore,

$$(\pi_p^2 - 1)(P_{2power}) = \begin{cases} 0_d & \text{(if } P_{odd} \in E[\pi_p + 1]\text{)}, \\ 0_d \text{ or } (-1, 0) & \text{(if } P_{odd} \in E[\pi_p - 1]\text{)}. \end{cases}$$

As $\pi_p^2 + p = 0$, $\pi_p^2 - 1 = -p - 1$. Since P_{2power} is a point whose order is a power of 2,

$$4P_{2power} = \begin{cases} 0_d & \text{(if } P_{odd} \in E[\pi_p + 1]\text{)}, \\ 0_d \text{ or } (-1, 0) & \text{(if } P_{odd} \in E[\pi_p - 1]\text{)}. \end{cases}$$

Hence, if $P_{odd} \in E[\pi_p + 1]$, then

$$2P_{2power} = 0_d, (0, -1), (\pm\sqrt{d} : 0 : 0 : 1),$$

and if $P_{odd} \in E[\pi_p - 1]$, then

$$2P_{2power} = 0_d, (0, -1), (\pm\sqrt{d} : 0 : 0 : 1), (1, 0), (-1, 0), (0 : \pm\sqrt{d} : 0 : 1).$$

It is easy to check that if $w(2P_{2power}) = 0$, then $w(2P) = w(2P_{odd})$, and if $w(2P_{2power}) = \infty$, then $w(2P) = 1/w(2P_{odd})$. Therefore, if $w(2P)$ is square, then $w(2P_{odd})$ is square, and if $w(2P)$ is not square, then $w(2P_{odd})$ is not square. By Lemma 5, if $w(2P)$ is square, then $2P_{odd} \in E_d[\pi_p + 1]$, and if $w(2P)$ is not square, then $2P_{odd} \in E_d[\pi_p - 1]$.

Denote $w(P)$ by w. By the Edwards addition formula (5), we have

$$w(2P) = \frac{4dx^2y^2(y^2 - x^2)^2}{(1 - dx^2y^2)^2(1 + dx^2y^2)^2} = \frac{4w(y^2 - x^2)^2}{(1 - w)^2(1 + w)^2}.$$

Since w is square, if $w(2P)$ is square, then $y^2 - x^2 \in \mathbb{F}_p$, and if $w(2P)$ is not square, then $y^2 - x^2 \notin \mathbb{F}_p$. As

$$2P = \left(\frac{2xy}{1 + dx^2y^2}, \frac{y^2 - x^2}{1 - dx^2y^2}\right),$$

if $w(2P)$ is square, then the y-coordinate of $2P$ is an element of $\mathbb{F}_p$, and if $w(2P)$ is not square, then the y-coordinate of $2P$ is not an element of $\mathbb{F}_p$.

In the case that $w(2P)$ is square, $y(2P) \in \mathbb{F}_p$ and $2P_{odd} \in E_d[\pi_p + 1]$. Therefore, $y(2P_{odd}) \in \mathbb{F}_p$. Assume that $2P_{2power} = (\sqrt{d} : 0 : 0 : 1)$ or $(-\sqrt{d} : 0 : 0 : 1)$. It is easy to check that

$$y(2P) = \pm\frac{1}{\sqrt{d} \cdot y(2P_{odd})}.$$

As $y(2P_{odd}) \in \mathbb{F}_p$, $y(2P) \notin \mathbb{F}_p$ by Lemma 1. This is a contradiction. We conclude that $2P_{2power}$ is 0_d or $(0, -1)$. Therefore, $w(2P) = w(2P_{odd})$. As $(\pi_p^2 - 1)(2P_{odd}) = 0_d$,

$$\frac{p + 1}{4}(2P_{odd}) = 0_d.$$

In the case that $w(2P)$ is not square, $y(2P) \notin \mathbb{F}_p$ and $2P_{odd} \in E_d[\pi_p - 1]$. Therefore, $y(2P_{odd}) \in \mathbb{F}_p$. Assume that

$$2P_{2power} = 0_d, (0, -1), (1, 0), (-1, 0).$$

It is easy to check that $y(2P) = \pm y(2P_{odd})$. As $y(2P_{odd}) \in \mathbb{F}_p$, $y(2P) \in \mathbb{F}_p$. This is a contradiction. We conclude that $2P_{2power}$ is $(\pm\sqrt{d} : 0 : 0 : 1)$ or $(0 : \pm\sqrt{d} : 0 : 1)$. Therefore, it is easy to check that $w(2P) = 1/w(2P_{odd})$. As $(\pi_p^2 - 1)(2P_{odd}) = 0_d$,

$$\frac{p + 1}{4}(2P_{odd}) = 0_d.$$

Let P' be $2P_{odd}$. This completes the proof of Theorem 4. □

Theorem 5. *Let $p \equiv 3 \pmod 8$. Let P be a point on an Edwards curve E_d such that the w-coordinate $w(P) \in \mathbb{F}_p$, the order of P is not a power of 2, and $w(P)$ is square. The number of points P such that $w(2P)$ is square is the same as the number of points P such that $w(2P)$ is not square.*

Proof. Let the coordinates of P be (x, y). Let P_{odd} and P_{2power} be points of E_d such that $P = P_{odd} + P_{2power}$, the order of P_{odd} is odd, and the order of P_{2power} is a power of 2. The existence of P_{odd} and P_{2power} are guaranteed by Lemma 6. As shown in the proof of Theorem 4, we have

$$2P_{2power} = 0_d, (0, -1), (\pm\sqrt{d} : 0 : 0 : 1), (0 : \pm\sqrt{d} : 0 : 1).$$

If $2P_{2power}$ is 0_d or $(0, -1)$, $w(P_{2power})$ is 0 or ∞, since it is easy to check that

$$P_{2power} = 0_d, (0, -1), (\pm 1, 0), (\pm\sqrt{d} : 0 : 0 : 1), (0 : \pm\sqrt{d} : 0 : 1).$$

If $2P_{2power}$ is $(\pm\sqrt{d} : 0 : 0 : 1)$ or $(0 : \pm\sqrt{d} : 0 : 1)$, $w(P_{2power})$ is ± 1 since

$$w(2P_{2power}) = \frac{4w(P_{2power})((1 + w(P_{2power}))^2 - 4w(P_{2power})/d)}{(1 - w(P_{2power}))^2(1 + w(P_{2power}))^2}.$$

Assume that $w(P_{2power})$ is -1. $w(2P_{2power}) = \infty$. As shown in the proof of Theorem 4, $(\pi_p - 1)(P_{odd}) = 0_d$. Let the coordinates of P_{odd} be (x_o, y_o). It is easy to check that

$$P_{2power} = \left(\sqrt{\sqrt{\frac{1}{d}}}, \sqrt{-\sqrt{\frac{1}{d}}}\right) + Q',$$

where Q' is a point of E_d such that $w(Q') = 0$ or $w(Q') = \infty$. From the addition formula of Edward curves,

$$P = P_{odd} + P_{2power} = \left(\frac{x_o\sqrt{-\sqrt{\frac{1}{d}}} + y_o\sqrt{\sqrt{\frac{1}{d}}}}{1 + dx_oy_o\sqrt{\frac{-1}{d}}}, \frac{y_o\sqrt{-\sqrt{\frac{1}{d}}} - x_o\sqrt{\sqrt{\frac{1}{d}}}}{1 - dx_oy_o\sqrt{\frac{-1}{d}}}\right) + Q'.$$

Therefore,

$$w(P) = \frac{(2x_oy_o + (y_o^2 - x_o^2)\sqrt{-1})^2}{(1 + dx_o^2y_o^2)^2} \text{ or } \frac{(1 + dx_o^2y_o^2)^2}{(2x_oy_o + (y_o^2 - x_o^2)\sqrt{-1})^2}.$$

As $p \equiv 4 \pmod 3$, -1 is not square. Since P_{odd} is not 0_d, $x_o \neq 0$ and $y_o \neq 0$. If we assume that $x_o^2 = y_o^2$, then it is easy to check that $2x_o^2 = 1 + dx_o^4$, and

$$x_o^2 = \frac{1 \pm \sqrt{1 - d}}{d} \notin \mathbb{F}_p \quad \text{(by Lemma 2)}.$$

Since $x_o^2 \in \mathbb{F}_p$, $x_o^2 \neq y_o^2$. Therefore, $(2x_oy_o + (y_o^2 - x_o^2)\sqrt{-1})^2$ does not belong to $\mathbb{F}_p$. Hence, $w(P) \notin \mathbb{F}_p$. This is a contradiction. We conclude $w(P_{2power})$ is 0 or ∞ or 1.

If $w(2P)$ is square, as shown in the proof of Theorem 4, $w(P_{odd})$ is square and $2P_{2power} = 0_d$ or $(0, -1)$. Therefore, $w(P_{2power})$ is 0 or ∞. If $w(2P)$ is not square, as shown in the proof of Theorem 4, $w(P_{odd})$ is not square and $2P_{2power} = (\pm\sqrt{d} : 0 : 0 : 1)$ or $(0 : \pm\sqrt{d} : 0 : 1)$. Therefore, $w(P_{2power})$ is 1.

We prove that if $P_{odd} \in E_d[\pi_p - 1]$, then $w(P_{odd} + Q)$ is square for all points Q at which $w(Q)$ is 1. It is easy to check that

$$Q = \left(\sqrt{1 + \sqrt{-1}r}, \sqrt{1 - \sqrt{-1}r}\right) + Q',$$

where $r = \sqrt{\frac{1-d}{d}}$, and Q' is a point such that $w(Q') = 0$ or $w(Q') = \infty$. By Lemma 1 and Lemma 2, $r \in \mathbb{F}_p$. Let the coordinates of P_{odd} be (x_o, y_o). Denote $\left(\sqrt{1+\sqrt{-1}r}, \sqrt{1-\sqrt{-1}r}\right)$ by R. Note that

$$P_{odd} + R = \left(\frac{x_o\sqrt{1-\sqrt{-1}r} + y_o\sqrt{1+\sqrt{-1}r}}{1+\sqrt{d}x_oy_o}, \frac{y_o\sqrt{1-\sqrt{-1}r} - x_o\sqrt{1+\sqrt{-1}r}}{1-\sqrt{d}x_oy_o}\right).$$

Therefore,

$$w\left(P_{odd} + R\right) = \frac{d(-2x_oy_o\sqrt{-1}r + (y_o^2 - x_o^2)\sqrt{1+r^2})^2}{(1-dx_o^2y_o^2)^2} = \frac{(-2x_oy_o\sqrt{-d}r + (y_o^2 - x_o^2))^2}{(1-dx_o^2y_o^2)^2}.$$

By Lemma 1, $\sqrt{-d} \in \mathbb{F}_p$. As $P_{odd} \in E_d[\pi_p - 1]$, $x_o, y_o \in \mathbb{F}_p$. Therefore, $w\left(P_{odd} + R\right)$ belongs to $\mathbb{F}_p$ and is square. Since $w(P_{odd}+Q) = w(P_{odd}+R)$ or $1/w(P_{odd}+R)$, $w(P_{odd}+Q)$ belongs to $\mathbb{F}_p$ and is square.

Let S_+ be the set of points P of E_d such that both $w(P)$ and $w(2P)$ are square and the order of P is not a power of 2, and let S_- be the set of points P of E_d such that $w(P)$ is square, $w(2P)$ is not square, and the order of P is not a power of 2. We shall prove that there is a bijection $\phi\colon S_+ \to S_-$. Define $\phi\colon S_+ \to S_-$ as follows.

$$\phi(P) := f(P_{odd}) + P_{2power} + R,$$

where P_{odd} and P_{2power} are points of E_d such that $P = P_{odd} + P_{2power}$, the order of P_{odd} is odd, the order of P_{2power} is a power of 2, R is defined as above, and f is the bijection in Lemma 8. As has already been shown, if $P \in S_+$, then $w(P_{2power})$ is 0 or ∞. As $f(P_{odd}) \in E_d[\pi_p - 1]$ and $w(P_{2power} + R) = 1$, $w(\phi(P))$ is square. Since $w(2\phi(P)) = 1/w(2f(P_{odd}))$ and $2f(P_{odd}) \in E_d[\pi_p - 1]$, $w(2\phi(P))$ is not square. As $f(P_{odd})$ is not 0_d, the order of $\phi(P)$ is not a power of 2. From Lemma 6 and the above, ϕ is well-defined. Define $\psi\colon S_- \to S_+$ as follows.

$$\psi(P) := f^{-1}(P_{odd}) + P_{2power} - R,$$

where P_{odd} and P_{2power} are points of E_d such that $P = P_{odd} + P_{2power}$, the order of P_{odd} is odd, and the order of P_{2power} is a power of 2. As has already een shown, if $P \in S_-$, then $w(P_{2power}) = 1$. As $w(P_{2power} - R)$ is 0 or ∞, $w(\psi(P)) = w(f^{-1}(P_{odd}))$ or $1/w(f^{-1}(P_{odd}))$. Since $f^{-1}(P_{odd}) \in E_d[\pi_p + 1]$, $w(f^{-1}(P_{odd}))$ is square by Lemma 4. Hence, $w(\psi(P))$ and $w(2\psi(P))$ are square. As $f^{-1}(P_{odd})$ is not 0_d, the order of $\psi(P)$ is not a power of 2. From Lemma 6 and the above, ψ is well-defined. It is easy to check that $\psi = \phi^{-1}$.

This completes the proof of Theorem 5. □

Theorem 6. *Let $p \equiv 3 \pmod 8$ and E be a supersingular elliptic curve defined over $\mathbb{F}_p$. Then $\mathrm{End}_p(E) \cong \mathbb{Z}[\pi_p]$ holds if and only if there exists $d \in \mathbb{F}_p$ such that E is $\mathbb{F}_p$-isomorphic to an Edwards curve E_d. Moreover, if such a d exists, then it is unique.*

Proof. The first half of this theorem follows from Corollary 1, Corollary 2, and Theorem 3.

Let us prove the uniqueness of d. Let $d_1, d_2 \in \mathbb{F}_p$ such that E_{d_1} and E_{d_2} are supersingular Edwards curves, $\mathrm{End}_p(E_{d_1}) \cong \mathbb{Z}[\pi_p]$, $\mathrm{End}_p(E_{d_2}) \cong \mathbb{Z}[\pi_p]$, and $E_{d_1} \cong E_{d_2}$ over $\mathbb{F}_p$.

As $1 - d_1$ and $1 - d_2$ are not square by Lemma 2,

$$E_{d_i} \cong Y^2Z = X^3 - \frac{2(1+d_i)}{1-d_i}X^2Z + XZ^2 \quad (i = 1, 2)$$

holds by Corollary 1. Therefore,

$$\frac{2(1+d_1)}{1-d_1} = \frac{2(1+d_2)}{1-d_2}$$

holds by the uniqueness of coefficients in Theorem 3. This equation reduces to $d_1 = d_2$.

This completes the proof of Theorem 6. □

5 Evaluating the class group action on Edwards curves

Algorithm 1 Evaluating the class group action on Edwards curves

```
Input: $d \in \mathbb{F}_p$ such that Edwards curve $E_d$ is supersingular and a list of integers $(e_1, \dots, e_n)$
Output: $d'$ such that $[\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n}]E_d = E_{d'}$
 1: while some $e_i \neq 0$ do
 2:     $w \leftarrow 0$
 3:     while $w = 0$ or $w = 1$ or $w = -1$ do
 4:         Sample a random $w \in \mathbb{F}_p$
 5:     end while
 6:     $w \leftarrow w^2$   (Theorem 4, 5)
 7:     $\mathbf{w}(P) \leftarrow (w : 1)$
 8:     Compute $\mathbf{w}(2P)$   (Theorem 4)
 9:     $(W : Z) \leftarrow \mathbf{w}(2P)$
10:     Set $s \leftarrow +1$ if $W$ is a square in $\mathbb{F}_p$, else $s \leftarrow -1$
11:     Let $S = \{i \mid \mathrm{sign}(e_i) = s\}$
12:     if $S = \emptyset$ then
13:         Go to line 2
14:     end if
15:     $\mathbf{w}(P) \leftarrow (W : Z)$, $k \leftarrow \prod_{i \in S} \ell_i$
16:     $\mathbf{w}(P) = (W : Z) \leftarrow \mathbf{w}(((p+1)/4k)P)$   (Theorem 4)
17:     if $s = 1$ then
18:         $\mathbf{w}(P) \leftarrow (Z : W)$   (Theorem 4)
19:     end if
20:     for all $i \in S$ do
21:         $\mathbf{w}(Q) \leftarrow \mathbf{w}((k/\ell_i)P)$
22:         if $K \neq 0_d$ then
23:             Compute an $\ell_i$-isogeny $\phi\colon E_d \to E_{d'}$ with $\ker \phi = \langle Q \rangle$
24:             $d \leftarrow d'$, $\mathbf{w}(P) \leftarrow \mathbf{w}(\phi(P))$, $k \leftarrow k/\ell_i$, $e_i \leftarrow e_i - s$
25:         end if
26:     end for
27: end while
28: return $d$   (Theorem 6)
```

In this section, we propose the method for evaluating the class group action based on Edwards curves. The theorems proved in the previous section will be used to construct the method. The algorithm is described in Algorithm 1. All of its calculations are done over $\mathbb{F}_p$.

The inputs of the algorithm are an Edwards coefficient $d \in \mathbb{F}_p$ and a list of integers $(e_1, \dots, e_n)$. The output of this algorithm is an Edwards coefficient $d' \in \mathbb{F}_p$ such that $E_{d'} = [\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n}]E_d$. Let p be a prime which satisfies $p = 4 \cdot \ell_1 \cdots \ell_n - 1$, where the $\ell_1, \dots, \ell_n$ are small distinct odd primes.

Sampling points To sample a point that belongs to $E_d[\pi_p - 1]$ or $E_d[\pi_p + 1]$, we take a uniformly random element of $\mathbb{F}_p$. Denote this element by w. If w is 0 or ± 1, we take a random element again. (We reject any point whose order is a power of 2 by Lemma 9 in Appendix C.) Then, we calculate w^2. Let P be a point in E_d such that $w(P) = w^2$. By Theorem 4, if $w(2P)$ is square in $\mathbb{F}_p$, then there exists a point P' such that $w(P') = w(2P)$, $\frac{p+1}{4}P' = 0_d$, and $P' \in E_d[\pi_p + 1]$. If $w(2P)$ is not square in $\mathbb{F}_p$, then there exists a point P' such that $w(P') = 1/w(2P)$, $\frac{p+1}{4}P' = 0_d$, and $P' \in E_d[\pi_p - 1]$. Thus, we calculate $w(2P)$ by using the doubling formulas on Edwards curves and determine whether $w(2P)$ is square or not. If $w(2P)$ is square, we can use $w(2P)$ as an element of $E_d[\pi_p + 1]$. If $w(2P)$ is not square, we can use $1/w(2P)$ as an element of $E_d[\pi_p - 1]$. If $w(2P)$ is square, we define S as a set of i such that the sign of e_i is -1. If $w(2P)$ is not square, we define S as a set of i such that the sign of e_i is $+1$. If $S = \emptyset$, we go back to the **Sampling points** calculation.

From Theorem 5, the probability of getting points in $E_d[\pi_p - 1]$ is equal to the probability of getting points in $E_d[\pi_p + 1]$.

Scalar multiplication From Theorem 4, it suffices to calculate $w(\frac{p+1}{4k}(P'))$ instead of $w(\frac{p+1}{k}(P))$, where $k = \prod_{i \in S} \ell_i$. To calculate $w(\frac{p+1}{4k}(P'))$ efficiently, we use Algorithm 3 in Appendix D.

If $w(2P)$ is not square, the proof of Theorem 4 indicates that $P' = 2P + Q$, where Q is a point at infinity. Since $\frac{p+1}{4k}$ is odd and the order of a point at infinity is 2 or 4, $w(\frac{p+1}{4k}(P')) = 1/w(\frac{p+1}{4k}(2P))$.

Calculation of isogenies By Theorem 6, we can calculate isogenies by using the same strategy as the original CSIDH algorithm. To do so, we can use the formulas on Edwards curves [12].

Output If the list of integers $(e_1, \ldots, e_n)$ is the zero vector, we output the Edwards coefficient $d' \in \mathbb{F}_p$.

Remark 1. To determine whether $w(2P)$ is square or not, we only need to consider W, where $(W : Z) = \mathbf{w}(2P)$.

Recall the isogenies formulas on Edwards curves:

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

As ℓ is odd, if D is not square, then D' is also not square. At the beginning of the algorithm, we let $(D : C) = (d : 1)$. Hence, we can assume that D is not square. Let the projective w-coordinates of P be $(W' : Z')$, the projective w-coordinates of $2P$ be $(W : Z)$, and the projective coordinates of d be $(D : C)$. Z is not square, since

$$\mathbf{w}(2P) = (4W'Z'(D(W' + Z')^2 - 4CW'Z') : D(W' + Z')^2(W' - Z')^2).$$

Therefore, if W is square, then $w(2P)$ is not square. Moreover, if W is not square, then $w(2P)$ is square.

5.1 Computational savings

Our proposed CSIDH algorithm using only Edwards curves is as fast as (or a little bit faster than) the algorithm proposed by Meyer and Reith [14]. In this subsection, we explain computational savings of our algorithm relative to the algorithm of Meyer and Reith.

On Edwards curves, the **Sampling points** calculation costs $1\mathbf{S}$ for taking a uniformly random element of $(\mathbb{F}_p)^2$ and requires one doubling on Edwards curves with $Z = 1$ (the cost of $4\mathbf{M} + 1\mathbf{S} + 5\mathbf{a}$) for determining the set which the point belongs to. On the other hand, on Montgomery curves, **Sampling points** calculation entails calculating $Cx^3 + Ax^2 + Cx$ (the cost of $3\mathbf{M} + 1\mathbf{S} + 2\mathbf{a}$) for determining the set which the point belongs to, where $(A : C)$ is a projective coordinates of a. Therefore, our algorithm saves a cost of $-\mathbf{M} - \mathbf{S} - 3\mathbf{a}$ per **Sampling points** calculation.

The **Scalar multiplication** part entails multiplication by $\frac{p+1}{4k}$ on Edwards curves and multiplication by $\frac{p+1}{k}$ on Montgomery curves. Therefore, per **Scalar multiplication**, the proposed algorithm saves the cost of a doubling on Edwards curves with $Z = 1$ and the cost of doubling on Edwards curves with $Z \neq 1$ (i.e., $8\mathbf{M} + 3\mathbf{S} + 9\mathbf{a}$).

The probability that $S = \emptyset$ after performing the **Sampling points** calculation is at most $\frac{1}{2}$, by Theorem 5. Hence, we expect the proposed algorithm to save at least

$$\frac{1}{2}(-\mathbf{M} - \mathbf{S} - 3\mathbf{a}) + \frac{1}{2}(8\mathbf{M} + 3\mathbf{S} + 9\mathbf{a} - \mathbf{M} - \mathbf{S} - 3\mathbf{a}) = 3\mathbf{M} + \frac{1}{2}\mathbf{S} + \frac{3}{2}\mathbf{a},$$

per **Sampling points** and **Scalar multiplication** calculation.

The difference between **Calculation of isogenies** on Edwards curves and on Montgomery curves is only in calculating the isogenies. The computational cost of calculating $(2s+1)$-degree isogenies on Edwards curves is $(6s+2)\mathbf{M}+8\mathbf{S}+(4s+6)\mathbf{a}$ and that of the two s-th powers, while the computational cost on Montgomery curves is $(6s+2)\mathbf{M}+8\mathbf{S}+(4s+8)\mathbf{a}$ and that of the two s-th powers. Therefore, the proposed algorithm saves $2\mathbf{a}$ per isogeny calculation.

From the above, we conclude that our proposed CSIDH algorithm using only Edwards curves is as fast as or a little bit faster than the algorithm proposed by Meyer and Reith.

6 Conclusion

We proved three important theorems (Theorem 4, Theorem 5, and Theorem 6) on Edwards curves and used them to make a new CSIDH algorithm. Theorem 4 shows that if $w(P)$ and $w(2P)$ are square, then $w(2P)$ can be treated as a point in $E_d[\pi_p + 1]$, and if $w(P)$ is square and $w(2P)$ is not square, then $1/w(2P)$ can be treated as a point in $E_d[\pi_p - 1]$. Theorem 5 claims that the number of points such that $w(P)$ and $w(2P)$ are square is equal to the number of points such that $w(P)$ is square and $w(2P)$ is not square. Theorem 6 proves that an Edwards coefficient d is unique up to $\mathbb{F}_p$-isomorphism. The new CSIDH algorithm built from these three theorems uses only Edwards curves over $\mathbb{F}_p$.

Finally, we compared complexities of the new algorithm and the sate of the art one of Meyer and Reith. We showed that our proposed algorithm is as fast as (or a little bit faster than) the one of Meyer and Reith.

Appendix A How to compute the calculations and isogenies

Here, we explain how to compute the calculations and isogenies on Montgomery curves and Edwards curves.

A.1 Montgomery curves

The doublings formula (1) can be computed as

$$t_1 \leftarrow X+Z, \quad t_2 \leftarrow X-Z, \quad t_1 \leftarrow t_1^2, \quad t_2 \leftarrow t_2^2, \quad s \leftarrow t_1 - t_2, \quad t_2 \leftarrow t_2 \cdot (4C),$$
$$X' \leftarrow t_1 \cdot t_2, \quad t_1 \leftarrow (A+2C) \cdot s, \quad t_1 \leftarrow t_1 + t_2, \quad Z' \leftarrow s \cdot t_1.$$

If $Z = 1$, the doublings formula (1) can be computed as

$$t_1 \leftarrow X+1, \quad t_1 \leftarrow t_1^2, \quad s \leftarrow 2 \cdot X, \quad s \leftarrow 2 \cdot s, \quad t_2 \leftarrow t_1 - s, \quad t_2 \leftarrow t_2 \cdot (4C),$$
$$X' \leftarrow t_1 \cdot t_2, \quad t_1 \leftarrow (A+2C) \cdot s, \quad t_1 \leftarrow t_1 + t_2, \quad Z' \leftarrow s \cdot t_1.$$

The addition formula (2) can be computed as

$$t_1 \leftarrow X_1 + Z_1, \quad s_1 \leftarrow X_2 + Z_2, \quad t_2 \leftarrow X_1 - Z_1, \quad s_2 \leftarrow X_2 - Z_2, \quad t \leftarrow t_1 \cdot s_2,$$
$$s \leftarrow t_2 \cdot s_1, \quad X_3 \leftarrow t + s, \quad Z_3 \leftarrow t - s, \quad X_3 \leftarrow X_3^2 \cdot Z_0, \quad Z_3 \leftarrow Z_3^2 \cdot X_0.$$

The formula for calculating $\phi(P)$ (3) can be computed as

$$t_i \leftarrow X_i + Z_i, \quad s_i \leftarrow X_i - Z_i, \quad t_i \leftarrow t_i \cdot (X - Z), \quad s_i \leftarrow s_i \cdot (X + Z),$$
$$X' \leftarrow \prod_{i=1}^{s} (t_i - s_i), \quad Z' \leftarrow \prod_{i=1}^{s} (t_i + s_i), \quad X' \leftarrow X \cdot (X')^2, \quad Z' \leftarrow Z \cdot (Z')^2.$$

The formula for calculating E' (4) can be computed as

$$c \leftarrow 2 \cdot C, \quad a \leftarrow A + c, \quad d \leftarrow A - c,$$
$$a' \leftarrow \prod_{i=1}^{s} (X_i + Z_i), \quad d' \leftarrow \prod_{i=1}^{s} (X_i - Z_i), \quad a' \leftarrow (a')^4, \quad d' \leftarrow (d')^4,$$
$$a' \leftarrow a^s \cdot a', \quad d' \leftarrow d^s \cdot d', \quad a' \leftarrow a \cdot (a')^2, \quad d' \leftarrow d \cdot (d')^2,$$
$$A' \leftarrow 2 \cdot (a' + d'), \quad C' \leftarrow a' - d'.$$

A.2 Edwards curves

The doublings formula (6), addition formula (7), and formula for calculating $\phi(P)$ (8) can be computed similarly as the formulas on Montgomery curves.

The formula for calculating E' (9) can be computed as

$$D' \leftarrow \prod_{i=1}^{s} (W_i + Z_i), \quad C' \leftarrow \prod_{i=1}^{s} Z_i, \quad D' \leftarrow (D')^4, \quad C' \leftarrow (C')^4,$$
$$D' \leftarrow D^s \cdot D', \quad C' \leftarrow (2 \cdot 2 \cdot 2 \cdot 2 \cdot C)^s \cdot C', \quad D' \leftarrow D \cdot (D')^2, \quad C' \leftarrow C \cdot (C')^2.$$

Appendix B Proof of Theorem 1

In this section, we prove Theorem 1.

Theorem 1. *Let p be a prime and $p \geq 3$. The Edwards curve E_d defined over $\mathbb{F}_p$ is $\mathbb{F}_p$-isomorphic to the Montgomery curve,*

$$E_{\mathcal{M}}\colon \frac{4}{1-d}Y^2Z = X^3 + \frac{2(1+d)}{1-d}X^2Z + XZ^2.$$

Proof. Define a rational map $\psi\colon E_d \to E_{\mathcal{M}}$,

$$(X : Y : Z : T) \mapsto (X + T : Y + Z : X - T).$$

ψ is a morphism, because all points except for $(0 : -1 : 1 : 0)$ are simply regular, and from the following equation, $(0 : -1 : 1 : 0)$ is also regular.

$$\frac{(Z-Y)Z}{X}(X+T, Y+Z, X-T) = (Z^2 - Y^2, XZ - dYT, (Z-Y)^2).$$

$\psi(0_d) = (0 : 1 : 0)$ holds, so ψ is an isogeny defined over $\mathbb{F}_p$.

Define a rational map $\phi\colon E_{\mathcal{M}} \to E_d$,

$$(X : Y : Z : T) \mapsto (X(X+Z) : Y(X-Z) : Y(X+Z) : X(X-Z)).$$

ϕ is a morphism, because all points except for $(0 : 1 : 0)$ and $(0 : 0 : 1)$ are simply regular, and from the following two equations, $(0 : 1 : 0)$ and $(0 : 0 : 1)$ are also regular.

$$\frac{1}{X}(X(X+Z), Y(X-Z), Y(X+Z), X(X-Z))$$
$$= \left(X + Z, \frac{bY^2 - X^2 - aXZ - Z^2}{bY}, \frac{bY^2 + X^2 + aXZ + Z^2}{bY}, X - Z\right),$$

and

$$\frac{1}{Y}(X(X+Z), Y(X-Z), Y(X+Z), X(X-Z))$$
$$= \left(\frac{bYZ(X+Z)}{X^2 + aXZ + Z^2}, X - Z, X + Z, \frac{bYZ(X-Z)}{X^2 + aXZ + Z^2}\right),$$

where $b = \dfrac{4}{1-d}$ and $a = \dfrac{2(1+d)}{1-d}$.

$\phi(0 : 1 : 0) = 0_d$ holds, so ϕ is an isogeny defined over $\mathbb{F}_p$.

As $\psi \circ \phi = \mathrm{id}_{E_{\mathcal{M}}}$ and $\phi \circ \psi = \mathrm{id}_{E_d}$ hold, E_d is $\mathbb{F}_p$-isomorphic to $E_{\mathcal{M}}$. □

Appendix C Proofs of the lemmas

Here, we prove the lemmas used in the theorems in Section 4 and Lemma 9.

Lemma 1. *Let $p \equiv 3 \pmod 8$. If an Edwards curve E_d defined over $\mathbb{F}_p$ is supersingular and satisfies $\mathrm{End}_p(E_d) \cong \mathbb{Z}[\pi_p]$, then d is not square.*

Proof. There exists a Montgomery curve $E_{\mathcal{M}}$ which is $\mathbb{F}_p$-isomorphic to E_d, by Corollary 1. If $E_{\mathcal{M}}[2] \subset E_{\mathcal{M}}(\mathbb{F}_p)$, Table 1 of [6] shows that the order of $E_{\mathcal{M}}$ or its quadratic twist can be divided by 8; however, both orders are $p+1 \equiv 4 \pmod 8$. $E_{\mathcal{M}}$ has the only one point of order 2 over $\mathbb{F}_p$. Therefore, E_d also has only one point of order 2 over $\mathbb{F}_p$.

Points of order 2 in E_d are $(0:-1:1:0)$ and $(\pm\sqrt{d}:0:0:1)$. Since $(0:-1:1:0)$ is a $\mathbb{F}_p$-rational point, d is not square. □

Lemma 2. *Let $p \equiv 3 \pmod 8$. If an Edwards curve E_d defined over $\mathbb{F}_p$ is supersingular and satisfies $\mathrm{End}_p(E_d) \cong \mathbb{Z}[\pi_p]$, then $1-d$ is not square.*

Proof. As $p \equiv 3 \pmod 8$, $\#E_d(\mathbb{F}_p) = p+1 \equiv 4 \pmod 8$.

By Lemma 1, there are no points at infinity on $E_d(\mathbb{F}_p)$. Hence, in this proof, we consider E_d to be an affine curve.

If a point (x,y) belongs to $E_d(\mathbb{F}_p)$, the points,

$$(-x,y),(x,-y),(-x,-y),(y,x),(-y,x),(y,-x),(-y,-x),$$

also belong to $E_d(\mathbb{F}_p)$. If $x \neq 0$, $y \neq 0$, $x \neq y$, and $x \neq -y$ hold, these eight points are different. If $x=0$ or $y=0$, the four points,

$$(0,1),(0,-1),(1,0),(-1,0),$$

are different. If $x=y$ or $x=-y$, x is a root of the equation,

$$2x^2 = 1 + dx^4.$$

Therefore,

$$x^2 = \frac{1 \pm \sqrt{1-d}}{d}.$$

Assume that $1-d$ is square. Note that

$$\frac{1+\sqrt{1-d}}{d} \cdot \frac{1-\sqrt{1-d}}{d} = \frac{1-(1-d)}{d^2} = \frac{1}{d}.$$

By Lemma 1, d is not square. Hence, one of $\frac{1+\sqrt{1-d}}{d}$ or $\frac{1-\sqrt{1-d}}{d}$ is square, and the other one is not square. Therefore, if $x=y$ or $x=-y$, the four points,

$$(x,x),(x,-x),(-x,x),(-x,-x),$$

are different, where x is $\sqrt{\frac{1+\sqrt{1-d}}{d}}$ or $\sqrt{\frac{1-\sqrt{1-d}}{d}}$.

From the above, $\#E_d(\mathbb{F}_p) \equiv 4+4 \equiv 0 \pmod 8$ holds. This is a contradiction. Therefore, $1-d$ is not square. □

Lemma 3. *If P is a point of E_d such that $w(P) \in \mathbb{F}_p$, then $(\pi_p+1)(P) \in \mathcal{G}_4$ or $(\pi_p-1)(P) \in \mathcal{G}_4$.*

Proof. Since $\pi_p(w(P)) = w(\pi_p(P))$, $w(\pi_p(P)) = w(P)$. Therefore, $(\pi_p+1)(P) \in \mathcal{G}_4$ or $(\pi_p-1)(P) \in \mathcal{G}_4$. □

Lemma 4. *Let p be a prime and $p \equiv 3 \pmod 8$. Let P be a point of E_d, not a point at infinity, and $w(P) \neq 0$. If $P \in E_d[\pi_p + 1]$, then $w(P) \in \mathbb{F}_p$ and is square in $\mathbb{F}_p$, and if $P \in E_d[\pi_p - 1]$, then $w(P) \in \mathbb{F}_p$ and is not square in $\mathbb{F}_p$.*

Proof. Denote the coordinates of P by (x, y) (affine coordinates). As $w(P) \neq 0$, $x \neq 0$ and $y \neq 0$. If $P \in E_d[\pi_p + 1]$, then $(x^p, y^p) = (-x, y)$. Therefore, $x^p = -x$ and $y \in \mathbb{F}_p$. As $(x^2)^p = x^2$ and $x \notin \mathbb{F}_p$, $x^2y^2 \in \mathbb{F}_p$ and x^2y^2 is not square. If $P \in E_d[\pi_p - 1]$, then $(x^p, y^p) = (x, y)$. Therefore, $x, y \in \mathbb{F}_p$. Thus, $x^2y^2 \in \mathbb{F}_p$ and x^2y^2 is square. Since d is not square by Lemma 1, Lemma 4 holds. □

Lemma 5. *Let p be a prime and $p \equiv 3 \pmod 8$. Let $P \in E_d[\pi_p - 1]$ or $E_d[\pi_p + 1]$, not a point at infinity, and $w(P) \neq 0$. If $w(P)$ is square in $\mathbb{F}_p$, then $P \in E_d[\pi_p + 1]$, and if $w(P)$ is not square in $\mathbb{F}_p$, then $P \in E_d[\pi_p - 1]$.*

Proof. This lemma obviously holds by Lemma 4. □

Lemma 6. *Let P be a point of E_d. Then, points P_{odd} and P_{2power} uniquely exist such that $P = P_{odd} + P_{2power}$, the order of P_{odd} is odd, and the order of P_{2power} is a power of 2.*

Proof. Note that $P \in E_d(\mathbb{F}_q)$, where q is a power of p. Therefore, P has finite order. By the fundamental theorem of finite abelian groups, there exist points P_{odd} and P_{2power} such that $P = P_{odd} + P_{2power}$, the order of P_{odd} is odd, and the order of P_{2power} is a power of 2.

Assume that $P_{odd} + P_{2power} = P'_{odd} + P'_{2power}$, where the orders of P_{odd} and P'_{odd} are odd, and the orders of P_{2power} and P'_{2power} are powers of 2. As $P_{odd} - P'_{odd} = -P_{2power} + P'_{2power}$,

$$P_{odd} - P'_{odd} = 0_d \text{ and } P_{2power} - P'_{2power} = 0_d.$$

Therefore, uniqueness holds. □

Lemma 7. *Let P be a point of E_d such that $w(P) \in \mathbb{F}_p$. Let P_{odd} and P_{2power} be points of E_d such that $P = P_{odd} + P_{2power}$, the order of P_{odd} is odd, and the order of P_{2power} is a power of 2. Then, one of the following holds.*

- *$P_{odd} \in E_d[\pi_p - 1]$ and $(\pi_p - 1)(P_{2power}) \in \mathcal{G}_4$.*
- *$P_{odd} \in E_d[\pi_p + 1]$ and $(\pi_p + 1)(P_{2power}) \in \mathcal{G}_4$.*

Proof. By Lemma 3, $(\pi_p \pm 1)(P) \in \mathcal{G}_4$. In the case that $(\pi_p - 1)(P) \in \mathcal{G}_4$, $(\pi_p - 1)(P_{odd}) = 0_d$, since the order of P_{odd} is odd and $\mathcal{G}_4$ is a cyclic group of order 4. Then, $(\pi_p - 1)(P_{2power}) = (\pi_p - 1)(P) \in \mathcal{G}_4$.

Similarly, in the case that $(\pi_p + 1)(P) \in \mathcal{G}_4$, $P_{odd} \in E_d[\pi_p + 1]$ and $(\pi_p + 1)(P_{2power}) \in \mathcal{G}_4$ hold. □

Lemma 8. *Let p be a prime and $p \equiv 3 \pmod 8$. There exists a bijection,*

$$f \colon E_d[\pi_p + 1] \cap E_d[(p + 1)/4] \longrightarrow E_d[\pi_p - 1] \cap E_d[(p + 1)/4],$$

such that $f(0_d) = 0_d$.

Proof. We will prove that the cardinality of $E_d[\pi_p + 1] \cap E_d[(p + 1)/4]$ and the cardinality of $E_d[\pi_p - 1] \cap E_d[(p + 1)/4]$ are finite and equal and that 0_d belongs to both sets.

Since E_d is supersingular and $\pi_p - 1$ and $\pi_p^2 - 1$ are separable, $\deg(\pi_p^2 - 1) = \#E_d(\mathbb{F}_{p^2}) = (p + 1)^2$ and $\deg(\pi_p - 1) = \#E_d(\mathbb{F}_p) = p + 1$. Therefore, $\deg(\pi_p + 1) = p + 1$. As $\pi_p - 1$

and $\pi_p + 1$ are separable, $\#E_d[\pi_p - 1] = p + 1$ and $\#E_d[\pi_p + 1] = p + 1$. As the set $E_d[\pi_p - 1] \cap E_d[(p+1)/4]$ is the set of all points of order odd in $E_d[\pi_p - 1]$,

$$\#(E_d[\pi_p - 1] \cap E_d[(p+1)/4]) = \frac{p+1}{4}.$$

Similarly,

$$\#(E_d[\pi_p + 1] \cap E_d[(p+1)/4]) = \frac{p+1}{4}.$$

We have proven that $\#(E_d[\pi_p + 1] \cap E_d[(p+1)/4])$ and $\#(E_d[\pi_p - 1] \cap E_d[(p+1)/4])$ are finite and equal.

It is obvious that 0_d belongs to $E_d[\pi_p + 1] \cap E_d[(p+1)/4]$ and $E_d[\pi_p - 1] \cap E_d[(p+1)/4]$. This completes the proof of Lemma 8. □

We used Lemmas 1 to 8 to prove the theorems in Section 4.

Lemma 9. *Let $p \equiv 3 \pmod 8$. Let P be a point on E_d such that $w(P) \in \mathbb{F}_p$ and the order of P is a power of 2. Then, $w(P)$ is 0 or ± 1.*

Proof. By Lemma 7, $(\pi_p - 1)(P) \in \mathcal{G}_4$ or $(\pi_p + 1)(P) \in \mathcal{G}_4$. As $(\pi_p - 1)\mathcal{G}_4 = \{0_d\}$, $(\pi_p + 1)\mathcal{G}_4 = \{0_d, (0, -1)\}$, and $\pi_p^2 - 1 = -p - 1$, we have

$$4P = 0_d, (0, -1).$$

Therefore, it is easy to check that

$$2P = 0_d, (0, -1), (\pm 1, 0), (\pm\sqrt{d} : 0 : 0 : 1), (0 : \pm\sqrt{d} : 0 : 1).$$

Hence, $w(2P) = 0$ or $w(2P) = \infty$. Since

$$w(2P) = \frac{4w(P)((1 + w(P))^2 - 4w(P)/d)}{(1 - w(P))^2(1 + w(P))^2},$$

$w(P) = 0, \frac{d-2\pm 2\sqrt{1-d}}{d}, 1, -1$. From Lemma 2, $1 - d$ is not square. Therefore, $w(P) = 0, \pm 1$. □

We use Lemma 9 for rejecting points whose order is a power of 2 in the **Sampling points** calculation of Algorithm 1.

Appendix D Algorithms

Algorithm 2 Evaluating the class group action on Montgomery curves [4]

```
Input: $a \in \mathbb{F}_p$ such that $E_{\mathcal{M},a}$ is supersingular and a list of integers $(e_1, \ldots, e_n)$
Output: $a'$ such that $[\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n}] E_{\mathcal{M},a} = E_{\mathcal{M},a'}$
1: while some $e_i \neq 0$ do
2:     Sample a random $x \in \mathbb{F}_p$
3:     $\mathbf{x}(P) \leftarrow (x : 1)$
4:     Set $s \leftarrow +1$ if $x^3 + ax^2 + x$ is a square in $\mathbb{F}_p$, else $s \leftarrow -1$
5:     Let $S = \{i \mid \mathrm{sign}(e_i) = s\}$
6:     if $S = \emptyset$ then
7:         Go to line 2
8:     end if
9:     $k \leftarrow \prod_{i \in S} \ell_i$, $\mathbf{x}(P) \leftarrow \mathbf{x}(((p+1)/k)P)$
10:    for all $i \in S$ do
11:        $\mathbf{x}(Q) \leftarrow \mathbf{x}((k/\ell_i)P)$
12:        if $K \neq (0 : 1 : 0)$ then
13:            Compute an $\ell_i$-isogeny $\phi\colon E_{\mathcal{M},a} \to E_{\mathcal{M},a'}$ with $\ker \phi = \langle Q \rangle$
14:            $a \leftarrow a'$, $\mathbf{x}(P) \leftarrow \mathbf{x}(\phi(P))$, $k \leftarrow k/\ell_i$, $e_i \leftarrow e_i - s$
15:        end if
16:    end for
17: end while
18: return $a$
```

Algorithm 3 The Edwards ladder using P and $2P$

```
Input: $E_d$, $k = \sum_{i=0}^{\ell-1} k_i 2^i$ with $k_{\ell-1} = 1$, $(W_0 : 1) = \mathbf{w}(P)$, and $(W : Z) = \mathbf{w}(2P)$ s.t. $P \in E_d$
Output: $(W' : Z') = \mathbf{w}(kP)$
$(W_1 : Z_1) \leftarrow (W_0 : 1)$ and $(W_2 : Z_2) \leftarrow (W : Z)$
for $i = \ell - 2$ down to $0$ do
    if $k_i = 0$ then
        $(W_1 : Z_1) \leftarrow 2(W_1 : Z_1)$ (doubling on $E_d$)
        $(W_2 : Z_2) \leftarrow (W_1 : Z_1) + (W_2 : Z_2)$ (addition on $E_d$ by using $W_0$)
    else
        $(W_2 : Z_2) \leftarrow 2(W_1 : Z_1)$ (doubling on $E_d$)
        $(W_1 : Z_1) \leftarrow (W_1 : Z_1) + (W_2 : Z_2)$ (addition on $E_d$ by using $W_0$)
    end if
end for
return $(W_1 : Z_1)$
```

References

1. Reza Azarderakhsh, Matthew Campagna, Craig Costello, LD Feo, Basil Hess, A Jalali, D Jao, B Koziel, B LaMacchia, P Longa, et al. Supersingular isogeny key encapsulation. *Submission to the NIST Post-Quantum Standardization project*, 2017.
2. Daniel J Bernstein, Peter Birkner, Marc Joye, Tanja Lange, and Christiane Peters. Twisted Edwards Curves. In *International Conference on Cryptology in Africa–AFRICACRYPT 2008*, pages 389–405. Springer, 2008.
3. Daniel J Bernstein and Tanja Lange. Faster Addition and Doubling on Elliptic Curves. In *International Conference on the Theory and Application of Cryptology and Information Security–ASIACRYPT 2007*, pages 29–50. Springer, 2007.

4. Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: an efficient post-quantum commutative group action. In *International Conference on the Theory and Application of Cryptology and Information Security–ASIACRYPT 2018*, pages 395–427. Springer, 2018.
5. Craig Costello and Huseyin Hisil. A simple and compact algorithm for SIDH with arbitrary degree isogenies. In *International Conference on the Theory and Application of Cryptology and Information Security–ASIACRYPT 2017*, pages 303–329. Springer, 2017.
6. Craig Costello and Benjamin Smith. Montgomery curves and their arithmetic: The case of large characteristic fields. *IACR Cryptology ePrint Archive*, 2017:212, 2017. `https://ia.cr/2017/212`.
7. Christina Delfs and Steven D Galbraith. Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$. *Designs, Codes and Cryptography*, pages 425–440, 2016.
8. Harold Edwards. A normal form for elliptic curves. *Bulletin of the American Mathematical Society*, pages 393–422, 2007.
9. Reza Rezaeian Farashahi and Seyed Gholamhossein Hosseini. Differential Addition on Twisted Edwards Curves. In *Australasian Conference on Information Security and Privacy*, pages 366–378. Springer, 2017.
10. Huseyin Hisil, Kenneth Koon-Ho Wong, Gary Carter, and Ed Dawson. Twisted Edwards Curves Revisited. In *International Conference on the Theory and Application of Cryptology and Information Security–ASIACRYPT 2008*, pages 326–343. Springer, 2008.
11. David Jao and Luca De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In *International Workshop on Post-Quantum Cryptography–PQCrypto 2011*, pages 19–34. Springer, 2011.
12. Suhri Kim, Kisoon Yoon, Young-Ho Park, and Seokhie Hong. Optimized Method for Computing Odd-Degree Isogenies on Edwards Curves. *IACR Cryptology ePrint Archive*, 2019:110, 2019. `https://ia.cr/2019/110`.
13. Neal Koblitz. Elliptic curve cryptosystems. *Mathematics of computation*, pages 203–209, 1987.
14. Michael Meyer and Steffen Reith. A faster way to the CSIDH. In *International Conference on Cryptology in India–INDOCRYPT 2018*, pages 137–152. Springer, 2018.
15. Victor S Miller. Use of elliptic curves in cryptography. In *Conference on the theory and application of cryptographic techniques–CRYPTO 1985*, pages 417–426. Springer, 1985.
16. Peter L Montgomery. Speeding the Pollard and elliptic curve methods of factorization. *Mathematics of computation*, pages 243–264, 1987.
17. National Institute of Standards and Technology. Post–quantum cryptography standardization, December 2016. `https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization`.
18. Ronald L Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, pages 120–126, 1978.
19. Peter W Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. Ieee, 1994.
20. Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, pages 303–332, 1999.
21. Joseph H Silverman. *The arithmetic of elliptic curves*, volume 106. Springer Science & Business Media, 2009.
22. Jacques Vélu. Isogénies entre courbes elliptiques. *CR Acad. Sci. Paris, Séries A*, pages 305–347, 1971.
23. William C Waterhouse. Abelian varieties over finite fields. In *Annales scientifiques de l'École Normale Supérieure*, pages 521–560, 1969.