On collisions related to an ideal class of order 3 in CSIDH

Hiroshi Onuki and Tsuyoshi Takagi

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

Abstract. CSIDH is an isogeny-based key exchange, which is a candidate for post quantum cryptography. It uses the action of an ideal class group on $\mathbb{F}_p$-isomorphic classes of supersingular elliptic curves. In CSIDH, the ideal classes are represented by vectors with integer coefficients. The number of ideal classes represented by these vectors determines the security level of CSIDH. Therefore, it is important to investigate the correspondence between the vectors and the ideal classes. Heuristics show that integer vectors in a certain range represent "almost" uniformly all of the ideal classes. However, the precise correspondence between the integer vectors and the ideal classes is still unclear. In this paper, we investigate the correspondence between the ideal classes and the integer vectors and show that the vector $(1, \ldots, 1)$ corresponds to an ideal class of order 3. Consequently, the integer vectors in CSIDH have collisions related to this ideal class. Here, we use the word "collision" in the sense of distinct vectors belonging to the same ideal class, i.e., distinct secret keys that correspond to the same public key in CSIDH. We further propose a new ideal representation in CSIDH that does not include these collisions and give formulae for efficiently computing the action of the new representation.

Keywords: CISDH · post-quantum cryptography · isogeny-based cryptography · ideal class groups · supersingular elliptic curve isogenies.

1 Introduction

Once a large-scale quantum computer is built, many of the public-key cryptosystems currently in use will no longer be secure. For this reason, research on post-quantum cryptography (PQC) has been increasingly important. In 2017, the National Institute of Standards and Technology (NIST) started the process of PQC standardization [19]. Candidates for NIST's PQC standardization include supersingular isogeny key encapsulation (SIKE) [13], which is a cryptosystem based on isogenies between elliptic curves.

Isogeny-based cryptography was first proposed by Couveignes [7] in 1997 and independently rediscovered by Rostovtsev and Stolbunov [23, 26]. Their proposed scheme is a Diffie-Hellman-style key exchange based on isogenies between ordinary elliptic curves over a finite field and typically called CRS. In 2011, Jao and

De Feo [12] proposed another isogeny-based key-exchange, supersingular isogeny Diffie-Hellman (SIDH). In 2018, Castryck, Lange, Martindale, Panny, and Renes [3] proposed commutative SIDH (CSIDH), which incorporates supersingular elliptic curves in the CRS scheme.

Diffie and Hellman [10] constructed their famous key-exchange scheme on the multiplicative group of a finite field. Koblitz [14] and Miller [17] proposed to use the group of points on an elliptic curve for the key-exchange scheme. The structures of these groups can be easily determined. Let G be a cyclic subgroup of one of these groups, g a generator of G, and N the order of G. Then, a secret key is an integer x, and the corresponding public key is the group element g^x. If one takes x from the interval $[0, N-1]$, the correspondence $x \mapsto g^x$ is one-to-one. Buchmann and Williams [2] proposed a Diffie-Hellman-style key-exchange using the ideal class group of an quadratic imaginary field with a large discriminant. In their scheme, a secret key is an integer x, and the corresponding public key is the ideal class $\mathfrak{a}^x$, where $\mathfrak{a}$ is a public ideal class. Unlike the former two schemes, it is hard to determine the structure of the ideal class group, and thus, the correspondence between the integer x and the ideal class $\mathfrak{a}^x$ is unclear. However, Buchmann and Williams claimed that by using the heuristics of Cohen and Lenstra [4], a randomly chosen ideal class has a large order with high probability and it is unlikely that different integers generate the same ideal class. CSIDH uses the free and transitive action of the ideal class group $\mathrm{cl}(\mathcal{O})$ of an order $\mathcal{O}$ of an imaginary quadratic field on the set of $\mathbb{F}_p$-isomorphism classes of supersingular elliptic curves whose endomorphism ring is isomorphic to $\mathcal{O}$. An ideal class in CSIDH is represented by an ideal of the form $\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n}$, where $\mathfrak{l}_i$ are prime ideals whose action can be efficiently computed and e_i are integer. By using this correspondence, a secret key in CSIDH is represented by an integer vector (e_i). The corresponding public key is the elliptic curve $(\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n}) * E$, where E is a public elliptic curve. By using the heuristics of Cohen and Lenstra and the Gaussian heuristic, Castryck et al. claimed that if one takes e_i from a certain range, s/he can expect that all the ideal classes in $\mathrm{cl}(\mathcal{O})$ are uniformly represented by these vectors. However, the precise correspondence between these vectors and the ideal classes is still unclear. It is important to investigate the correspondence between integer vectors and ideal classes, because the number of ideal classes represented by the integer vectors determines the security level of CSIDH.

In this paper, we investigate this correspondence and show that the ideal representation in CSIDH has collisions related to an ideal class of order 3. In particular, the vectors $(e_1, e_2, \ldots, e_n)$ and $(e_1+3, e_2+3, \ldots, e_n+3)$ represent the same ideal class. The order of the ideal class group $\mathrm{cl}(\mathcal{O})$ is three times the class number of $\mathbb{Q}(\sqrt{-p})$. Therefore, $\mathrm{cl}(\mathcal{O})$ always contains ideal classes of order 3. We show that the ideal class represented by $(1, \ldots, 1)$ has order 3; thus, the action of the ideal class represented by $(3, \ldots, 3)$ is trivial. Furthermore, we propose a new ideal representation in CSIDH that does not include these collisions and give formulae for computing the actions of the ideal classes represented by $(1, \ldots, 1)$ and $(-1, \ldots, -1)$. In particular, the actions of these ideal classes can be computed by isogenies of degree 4, and thus, they can be efficiently computed. By using these formulae, our representation can be computed more efficiently than the representation proposed by [3]. As an additional result, we give formulae for odd-degree isogenies between Montgomery curves using 4-torsion points. The computation of our formulae is faster than that of the previous formulae if the degree is less than 9.

Organization. The rest of this paper is organized as follows. In Section 2, we give a preliminaries on isogenies, ideal class groups, and CSIDH. In Section 3, we describe our theoretical results. In particular, we show that the ideal class represented by the vector $(1, \dots, 1)$ has order 3 and its action can be computed by using an isogeny of degree 4. Section 4 gives formulae for the action on Montgomery curves of this ideal class and its inverse. We conclude the paper in Section 5. Appendix gives formulae for odd-degree isogenies between Montgomery curves.

Related work. Beullens, Kleinjung, and Vercauteren [1] computed the ideal class group structure of CSIDH-512, which is a parameter set of CSIDH proposed in [3], and they proposed a method to uniformly sample ideal classes from this group. However, to obtain the structure of the ideal class group of CSIDH-512, they used an algorithm that has subexponential time in the ideal class group size. Therefore, their method may not be applicable to a larger CSIDH.

2 Preliminaries

We denote multiplication by $m \in \mathbb{Z}$ on an elliptic curve by $[m]$. For a group element g, we denote the group generated by g by $\langle g \rangle$.

In this section, we briefly introduce isogenies between elliptic curves, ideal class groups in number fields, the action of ideal classes on elliptic curves, and CSIDH. We refer the reader to the textbook of Silverman [25, 24] for an exposition on elliptic curves and Neukirch [20] for a description of ideal class groups. For details on CSIDH, the reader can consult Castryck et al. [3].

2.1 Isogenies

Since we use only elliptic curves defined over a finite prime field $\mathbb{F}_p$ with $p > 3$, we describe definitions and properties related isogenies between these curves.

An *isogeny* is a rational map between elliptic curves that is a group homomorphism. Let E and E' be elliptic curves defined over $\mathbb{F}_p$, and $\varphi : E \to E'$ an isogeny defined over $\mathbb{F}_p$. If φ is a nonzero isogeny, then φ induces an injection between function fields $\varphi^* : \bar{\mathbb{F}}_p(E') \to \bar{\mathbb{F}}_p(E)$, where $\bar{\mathbb{F}}_p$ is an algebraic closure of $\mathbb{F}_p$. In this case, we define the *degree* of φ by the degree of a field extension $\bar{\mathbb{F}}_p(E)/\varphi^*(\bar{\mathbb{F}}_p(E'))$ and say that φ is *separable* or *inseparable* if this field extension has the corresponding property. If φ is the zero map, we define the degree of

φ to be 0. We denote the degree of φ by $\deg\varphi$. For a nonzero separable isogeny $\varphi : E \to E'$, the degree of φ is finite and the cardinality of the kernel of φ is equal to $\deg\varphi$. Thus, a nonzero separable isogeny has a finite kernel. Conversely, a finite subgroup of an elliptic curve E determines a separable isogeny from E.

Proposition 1 (Lemma 6 of [3]). *Let E be an elliptic curve defined over $\mathbb{F}_p$ and Φ a finite subgroup of E that is stable under the action of the p-th power Frobenius map. Then there exists an elliptic curve E' defined over $\mathbb{F}_p$ and a separable isogeny $\varphi : E \to E'$ defined over $\mathbb{F}_p$ with kernel Φ. The codomain E' and the isogeny φ are unique up to $\mathbb{F}_p$-isomorphism.*

In the rest of this paper, we regard two elliptic curves as being the same if they are $\mathbb{F}_p$-isomorphic and denote the codomain of an isogeny $\varphi : E \to E'$ with kernel Φ by E/Φ.

For a nonzero separable isogeny $\varphi : E \to E'$, there exists a unique isogeny $\hat{\varphi} : E' \to E$ such that $\hat{\varphi} \circ \varphi = [\deg\varphi]$. We call the isogeny $\hat{\varphi}$ the *dual isogeny* of φ. We have $\deg\hat{\varphi} = \deg\varphi$. For a given elliptic curve E and subgroup Φ, one can explicitly calculate the curve E' and isogeny $\varphi : E \to E'$ by using Vélu's formula [27].

2.2 Ideal class groups

Let K be a number field of degree n. An *order* in K is a subring of K whose rank as a $\mathbb{Z}$-module is n. It is known that the integral closure of $\mathbb{Z}$ in K is the unique maximal order in K. We denote the maximal order by $\mathcal{O}_K$. Let $\mathcal{O}$ be an order of K. A *fractional ideal* of $\mathcal{O}$ is a finitely generated $\mathcal{O}$-submodule of K. A fractional ideal $\mathfrak{a}$ is *invertible* if there exists a fractional ideal $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b} = \mathcal{O}$, *integral* if $\mathfrak{a} \subseteq \mathcal{O}$, and *principal* if there exists $\alpha \in K$ such that $\mathfrak{a} = \alpha\mathcal{O}$. The set of invertible ideals of $\mathcal{O}$ forms an abelian group. We denote this group by $I(\mathcal{O})$. The subgroup of $I(\mathcal{O})$ consisting of principal ideals is denoted by $P(\mathcal{O})$. The *ideal class group* of $\mathcal{O}$ is the quotient group

$$\mathrm{cl}(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O}).$$

We denote the equivalent class of $\mathfrak{a}$ by $\{\mathfrak{a}\}$. It is known that $\mathrm{cl}(\mathcal{O})$ is a finite group. The order of $\mathrm{cl}(\mathcal{O}_K)$ is called the *class number* of K and denoted by h_K.

The *conductor* of $\mathcal{O}$ is the set $\{\alpha \in \mathcal{O}_K \mid \alpha\mathcal{O}_K \subseteq \mathcal{O}\}$. Note that the conductor of $\mathcal{O}$ is contained in $\mathcal{O}$ and can be regarded as an integral ideal of both $\mathcal{O}_K$ and $\mathcal{O}$. We need the following theorem, which provides a relation between the ideal class group of the maximal order and of an order.

Theorem 1. *Let K be a number field, $\mathcal{O}$ an order of K, and $\mathfrak{f}$ the conductor of $\mathcal{O}$. Then there is an exact sequence*

$$1 \to \mathcal{O}_K^\times/\mathcal{O}^\times \to (\mathcal{O}_K/\mathfrak{f})^\times/(\mathcal{O}/\mathfrak{f})^\times \to \mathrm{cl}(\mathcal{O}) \to \mathrm{cl}(\mathcal{O}_K) \to 1. \tag{1}$$

Proof. See [20, Theorem 12.12 in Chapter 1].

2.3 The class group action

Let $p > 3$ be a prime number and E an elliptic curve defined over $\mathbb{F}_p$. We denote the $\mathbb{F}_p$-rational endomorphism ring of E by $\mathrm{End}_{\mathbb{F}_p}(E)$. The ring $\mathrm{End}_{\mathbb{F}_p}(E)$ contains the p-th power Frobenius endomorphism ϕ, which satisfies the characteristic equation

$$\phi^2 - t\phi + p = 0, \tag{2}$$

where $t \in \mathbb{Z}$ is called the *trace of Frobenius*. The curve E is *supersingular* if and only if $t = 0$. The $\mathbb{F}_p$-rational endomorphism ring $\mathrm{End}_{\mathbb{F}_p}(E)$ is isomorphic to an order in an imaginary quadratic field. For an order $\mathcal{O}$ in an imaginary quadratic field and $\pi \in \mathcal{O}$, we define $\mathcal{E}\ell\ell_p(\mathcal{O}, \pi)$ to be the set of $\mathbb{F}_p$-isomorphism classes of elliptic curves E defined over $\mathbb{F}_p$ such that there is an isomorphism $\mathcal{O} \to \mathrm{End}_{\mathbb{F}_p}(E),\ \alpha \mapsto [\alpha]$ that maps π to the Frobenius endomorphism.

Let $E \in \mathcal{E}\ell\ell_p(\mathcal{O}, \pi)$ and $\mathfrak{a}$ be an integral ideal of $\mathcal{O}$. We define the $\mathfrak{a}$-torsion subgroup $E[\mathfrak{a}]$ of E by

$$E[\mathfrak{a}] := \{P \in E \mid [\alpha]P = \infty,\ \text{for all } \alpha \in \mathfrak{a}\}.$$

The subgroup $E[\mathfrak{a}]$ is finite, since $E[\mathfrak{a}] \subseteq E[\mathrm{N}(\mathfrak{a})]$, where N is the absolute norm. Therefore, by Proposition 1, there exists a unique elliptic curve $E/E[\mathfrak{a}]$ and an isogeny $\varphi_{\mathfrak{a}} : E \to E/E[\mathfrak{a}]$ with kernel $E[\mathfrak{a}]$. We denote the elliptic curve $E/E[\mathfrak{a}]$ by $\mathfrak{a} * E$. If $\mathfrak{a}$ is a principal ideal generated by $\alpha \in \mathcal{O}$, then $\varphi_{\mathfrak{a}}$ is a composition of the endomorphism $[\alpha]$ and an $\mathbb{F}_p$-automorphism of E, and $\mathfrak{a} * E = E$. This correspondence induces an action of $\mathrm{cl}(\mathcal{O})$ on $\mathcal{E}\ell\ell_p(\mathcal{O}, \pi)$. The following theorem describe the details.

Theorem 2 (Theorem 7 of [3]). *Let $\mathcal{O}$ be an order in an imaginary quadratic field and $\pi \in \mathcal{O}$ such that $\mathcal{E}\ell\ell_p(\mathcal{O}, \pi)$ is non-empty. Then the ideal class group $\mathrm{cl}(\mathcal{O})$ acts freely and transitively on the set $\mathcal{E}\ell\ell_p(\mathcal{O}, \pi)$ via the map*

$$\begin{aligned} \mathrm{cl}(\mathcal{O}) \times \mathcal{E}\ell\ell_p(\mathcal{O}, \pi) &\to \mathcal{E}\ell\ell_p(\mathcal{O}, \pi) \\ (\{\mathfrak{a}\}, E) &\mapsto \mathfrak{a} * E, \end{aligned}$$

in which $\mathfrak{a}$ is chosen as an integral representative.

2.4 CSIDH

Let $p > 3$ be a prime of the form $4\ell_1 \cdots \ell_n - 1$, where $\ell_1, \ldots, \ell_n$ are distinct odd primes. Let $\pi = \sqrt{-p}$ and $\mathcal{O} = \mathbb{Z}[\pi]$. The primes ℓ_i split in $\mathcal{O}$ as $\ell_i\mathcal{O} = \mathfrak{l}_i\bar{\mathfrak{l}}_i$, where $\mathfrak{l}_i = \ell_i\mathcal{O} + (\pi - 1)\mathcal{O}$ and $\bar{\mathfrak{l}}_i = \ell_i\mathcal{O} + (\pi + 1)\mathcal{O}$. The isogeny defined by $\mathfrak{l}_i$ has degree ℓ_i, and its dual isogeny is the isogeny defined by $\bar{\mathfrak{l}}_i$. The action of $\mathrm{cl}(\mathcal{O})$ on $\mathcal{E}\ell\ell_p(\mathcal{O}, \pi)$ is used in CSIDH. Note that $\mathcal{E}\ell\ell_p(\mathcal{O}, \pi)$ is not empty, since the elliptic curve defined by $y^2 = x^3 + x$ is contained in this set (see §4 in [3] for details). Therefore, by Theorem 2, the cardinality of $\mathcal{E}\ell\ell_p(\mathcal{O}, \pi)$ is equal to that of $\mathrm{cl}(\mathcal{O})$.

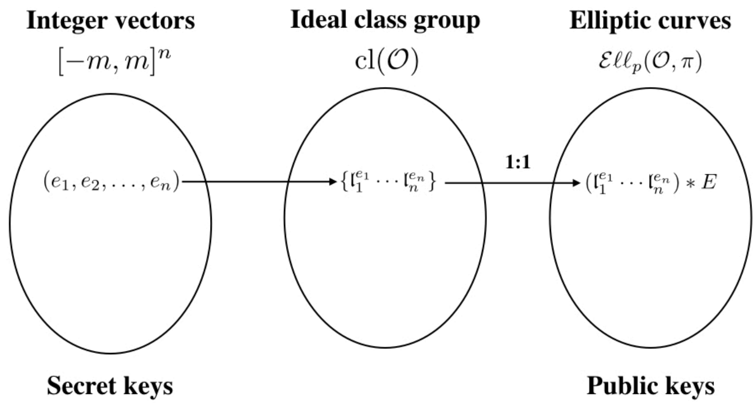

Figure 1. Correspondence of keys in CSIDH

For an elliptic curve $E \in \mathcal{E}\ell\ell_p(\mathcal{O},\pi)$, the torsion subgroups of the above ideals can be written as

$$E[\mathfrak{l}_i] = E[\ell_i] \cap E(\mathbb{F}_p), \tag{3}$$
$$E[\bar{\mathfrak{l}}_i] = E[\ell_i] \cap \{Q \in E \mid [\pi]Q = -Q\}. \tag{4}$$

Since the actions of $\mathfrak{l}_i$ and $\bar{\mathfrak{l}}_i$ on $\mathcal{E}\ell\ell_p(\mathcal{O},\pi)$ can be efficiently computed (see §8 in [3]), Castryck et al. [3] represented an ideal class in $\mathrm{cl}(\mathcal{O})$ by the product of these ideals; i.e., they represented it by an ideal of the form

$$\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n} \quad \text{for} \quad -m \le e_i \le m, \tag{5}$$

where m is an integer such that $(2m+1)^n \ge \sqrt{p}$. This representation induces a correspondence between integer vectors and ideal classes. Castryck et al. [3] showed that one can expect that this correspondence is "almost" surjective and uniform. (See §7.1 in [3] for details.) A secret key in CSIDH is expressed by an integer vector $(e_1, \dots, e_n)$, and we call this vector "secret exponents." A public key in CSIDH is an elliptic curve in $\mathcal{E}\ell\ell_p(\mathcal{O},\pi)$. By Theorem 2, there is a one-to-one correspondence between $\mathrm{cl}(\mathcal{O})$ and $\mathcal{E}\ell\ell_p(\mathcal{O},\pi)$. Figure 1 illustrates this situation.

The protocol of CSIDH is as follows: Alice and Bob share an elliptic curve $E \in \mathcal{E}\ell\ell_p(\mathcal{O},\pi)$ as a public parameter. Alice chooses her secret exponents $(e_1, \dots, e_n)$ and computes the curve $\mathfrak{a} * E$, where $\mathfrak{a} = \prod_i \mathfrak{l}_i^{e_i}$. She sends the curve to Bob as her public key. Bob proceeds in the same way by choosing his secret ideal $\mathfrak{b} = \prod_i \mathfrak{l}_i^{e_i'}$. Then, both parties can compute the shared secret $\mathfrak{a}\mathfrak{b} * E = \mathfrak{b}\mathfrak{a} * E$. Note that $\mathrm{cl}(\mathcal{O})$ is commutative.

3 Collisions related to an ideal class of order 3

First, we describe the notation that will be used in the rest of this paper. We will consider a slightly more general setting than that of CSIDH. Let $p > 3$ be a prime such that $p \equiv 3 \pmod 8$. Then $(p+1)/4$ is an odd integer, so it can be factorized as $\ell_1^{r_1} \cdots \ell_n^{r_n}$, where ℓ_i are distinct odd primes and r_i are positive integers. Let $\pi = \sqrt{-p}$, $K = \mathbb{Q}(\pi)$, and $\mathcal{O} = \mathbb{Z}[\pi]$. As in CSIDH, the primes ℓ_i split in $\mathcal{O}$ as $\ell_i\mathcal{O} = \mathfrak{l}_i\bar{\mathfrak{l}}_i$, where $\mathfrak{l}_i = \ell_i\mathcal{O} + (\pi - 1)\mathcal{O}$, $\bar{\mathfrak{l}}_i = \ell_i\mathcal{O} + (\pi + 1)\mathcal{O}$.

3.1 An ideal class of order 3

We prove two main theorems of this paper. The first theorem implies that there are two distinct secret exponents that represent the same ideal class.

Theorem 3. *The ideal classes* $\{\mathfrak{l}_1^{r_1} \cdots \mathfrak{l}_n^{r_n}\}$ *has order* 3 *in* $\mathrm{cl}(\mathcal{O})$.

Proof. The unit groups $\mathcal{O}_K^\times$ and $\mathcal{O}^\times$ are $\{\pm 1\}$. Therefore, by Theorem 1, we obtain the exact sequence

$$1 \to (\mathcal{O}_K/\mathfrak{f})^\times/(\mathcal{O}/\mathfrak{f})^\times \to \mathrm{cl}(\mathcal{O}) \to \mathrm{cl}(\mathcal{O}_K) \to 1, \tag{6}$$

where $\mathfrak{f}$ is the conductor $\mathfrak{f}$ of $\mathcal{O}$. Note that the maximal order $\mathcal{O}_K = \mathbb{Z}[\frac{1+\pi}{2}]$. Since $\mathfrak{f} = 2\mathcal{O}_K = 2\mathcal{O} + (\pi-1)\mathcal{O}$, it can be easily checked that $\mathcal{O}_K/\mathfrak{f} \cong \mathbb{F}_4$ and $\mathcal{O}/\mathfrak{f} \cong \mathbb{F}_2$. Therefore, the group $(\mathcal{O}_K/\mathfrak{f})^\times/(\mathcal{O}/\mathfrak{f})^\times$ is of order 3. The ideal $\mathfrak{l}_1^{r_1} \cdots \mathfrak{l}_n^{r_n}\mathcal{O}_K$ is a principal ideal of $\mathcal{O}_K$ because $\frac{\pi-1}{2}$ generates this ideal in $\mathcal{O}_K$. Therefore, the exact sequence (6) indicates that the ideal class $\{\mathfrak{l}_1^{r_1} \cdots \mathfrak{l}_n^{r_n}\}$ comes from $(\mathcal{O}_K/\mathfrak{f})^\times/(\mathcal{O}/\mathfrak{f})^\times$, so its order divides 3. We assume that the order of $\{\mathfrak{l}_1^{r_1} \cdots \mathfrak{l}_n^{r_n}\}$ is 1; i.e., $\mathfrak{l}_1^{r_1} \cdots \mathfrak{l}_n^{r_n}$ is principal in $\mathcal{O}$. Then, there exist $\alpha \in \mathcal{O}$ such that $\mathfrak{l}_1^{r_1} \cdots \mathfrak{l}_n^{r_n} = \alpha\mathcal{O}$. As we stated above, $\mathfrak{l}_1^{r_1} \cdots \mathfrak{l}_n^{r_n}\mathcal{O}_K = \frac{\pi-1}{2}\mathcal{O}_K$, so we have $\alpha = \pm\frac{\pi-1}{2}$. This contradicts $\alpha \in \mathcal{O}$. Consequently, the ideal class $\{\mathfrak{l}_1^{r_1} \cdots \mathfrak{l}_n^{r_n}\}$ has order 3 in $\mathrm{cl}(\mathcal{O})$. □

The following corollary directly follows from this theorem and shows that there are collisions in the ideal representation in CSIDH if $m \geq 2$. Figure 2 illustrates the assertion in the corollary.

Corollary 1. *In CSIDH, the secret exponents*

$$(e_1, e_2 \ldots, e_n) \quad \textit{and} \quad (e_1 + 3, e_2 + 3, \ldots, e_n + 3)$$

represent the same ideal class.

The second main theorem claims that the ideal class of $\mathfrak{l}_1^{r_1} \cdots \mathfrak{l}_n^{r_n}$ has a simple representative. We define the ideals of $\mathcal{O}$ as follows:

$$\mathfrak{c} = 4\mathcal{O} + (\pi - 1)\mathcal{O}, \tag{7}$$
$$\bar{\mathfrak{c}} = 4\mathcal{O} + (\pi + 1)\mathcal{O}. \tag{8}$$

It can be easily checked that $\mathfrak{c}\bar{\mathfrak{c}} = 4\mathcal{O}$.

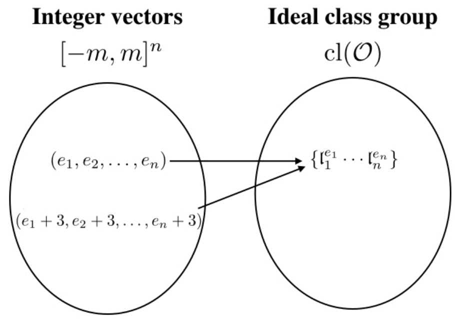

Figure 2. Collision in the ideal representation

Theorem 4. *The ideals* $\mathfrak{c}$ *and* $\bar{\mathfrak{c}}$ *are invertible and*

$$\mathfrak{c}\mathfrak{l}_1^{r_1} \cdots \mathfrak{l}_n^{r_n} = (\pi - 1)\mathcal{O}, \tag{9}$$
$$\bar{\mathfrak{c}}\bar{\mathfrak{l}}_1^{r_1} \cdots \bar{\mathfrak{l}}_n^{r_n} = (\pi + 1)\mathcal{O}. \tag{10}$$

Proof. It can be easily shown that

$$\mathfrak{c}\left(\mathcal{O} + \frac{\pi+1}{4}\mathcal{O}\right) = \mathcal{O}, \quad \bar{\mathfrak{c}}\left(\mathcal{O} + \frac{\pi-1}{4}\mathcal{O}\right) = \mathcal{O}. \tag{11}$$

Therefore, $\mathfrak{c}$ and $\bar{\mathfrak{c}}$ are invertible.

By definition, the ideal $\mathfrak{c}\mathfrak{l}_1^{r_1} \cdots \mathfrak{l}_n^{r_n}$ is generated by $4\prod_i \ell_i^{r_i}$ and multiple by $\pi - 1$. Since $4\prod_i \ell_i^{r_i} = p + 1 = -(\pi-1)(\pi+1)$, the ideal $(\pi-1)\mathcal{O}$ contains $\mathfrak{c}\mathfrak{l}_1^{r_1} \cdots \mathfrak{l}_n^{r_n}$.

Next, we show the inclusion $\mathfrak{c}\mathfrak{l}_1^{r_1} \cdots \mathfrak{l}_n^{r_n} \supseteq (\pi-1)\mathcal{O}$. There exists an integer $N > 0$ such that $(\pi-1)^N \in \mathfrak{c}\mathfrak{l}_1^{r_1} \cdots \mathfrak{l}_n^{r_n}$, since the ideals $\mathfrak{c}$ and $\mathfrak{l}_i$ contain $\pi - 1$. By the congruence

$$(\pi-1)^N \equiv (-2)^N \pmod{\pi+1}, \tag{12}$$

there exists $\alpha \in \mathcal{O}$ such that $(\pi-1)^N - \alpha(\pi+1) = (-2)^N$. Since $(\pi-1)^N$ and $-(\pi-1)(\pi+1) = 4\prod_i \ell_i^{r_i}$ are contained in $\mathfrak{c}\mathfrak{l}_1^{r_1} \cdots \mathfrak{l}_n^{r_n}$, we have

$$(-2)^N(\pi-1) = (\pi-1)^{N+1} - \alpha(\pi-1)(\pi+1) \in \mathfrak{c}\mathfrak{l}_1^{r_1} \cdots \mathfrak{l}_n^{r_n}.$$

On the other hand, we have $(\prod_i \ell_i^{r_i})(\pi-1) \in \mathfrak{c}\mathfrak{l}_1^{r_1} \cdots \mathfrak{l}_n^{r_n}$. Since 2 and $\prod_i \ell_i^{r_i}$ are relatively prime, it follows that $\pi - 1 \in \mathfrak{c}\mathfrak{l}_1^{r_1} \cdots \mathfrak{l}_n^{r_n}$. This proves equation (9). The second equation is the complex conjugate of the first. □

In terms of the ideal class group, Theorem 4 says that

$$\{\mathfrak{l}_1^{r_1} \cdots \mathfrak{l}_n^{r_n}\} = \{\bar{\mathfrak{c}}\}, \tag{13}$$
$$\{\bar{\mathfrak{l}}_1^{r_1} \cdots \bar{\mathfrak{l}}_n^{r_n}\} = \{\mathfrak{c}\}. \tag{14}$$

Note that $\{\mathfrak{l}_1^{r_1}\cdots\mathfrak{l}_n^{r_n}\}^{-1} = \{\bar{\mathfrak{l}}_1^{r_1}\cdots\bar{\mathfrak{l}}_n^{r_n}\}$ and $\{\mathfrak{c}\}^{-1} = \{\bar{\mathfrak{c}}\}$. An application of this theorem to CSIDH is that the action of $\{\mathfrak{l}_1^{r_1}\cdots\mathfrak{l}_n^{r_n}\}$ on $\mathcal{E}\ell\ell_p(\mathcal{O},\pi)$ can be computed via an isogeny of degree 4.

Corollary 2. *Let $E \in \mathcal{E}\ell\ell_p(\mathcal{O},\pi)$. Then, the torsion subgroups $E[\mathfrak{c}]$ and $E[\bar{\mathfrak{c}}]$ are cyclic groups of order 4 and*

$$(\mathfrak{l}_1^{r_1}\cdots\mathfrak{l}_n^{r_n}) * E = \bar{\mathfrak{c}} * E, \tag{15}$$

$$(\bar{\mathfrak{l}}_1^{r_1}\cdots\bar{\mathfrak{l}}_n^{r_n}) * E = \mathfrak{c} * E. \tag{16}$$

Proof. Since $E[\mathfrak{c}] = E[4]\cap E[\pi-1] = E[4]\cap E(\mathbb{F}_p)$ and $\#E(\mathbb{F}_p) = p+1 = 4\prod_i \ell_i^{r_i}$, we have $\#E[\mathfrak{c}] = 4$. Therefore, the isogeny defined by $\mathfrak{c}$ has degree 4. It can be easily checked that $\mathfrak{c}\bar{\mathfrak{c}} = 4\mathcal{O}$; i.e., the composition of isogenies defined by $\mathfrak{c}$ and $\bar{\mathfrak{c}}$ is multiplication by 4. Therefore, the isogeny defined by $\bar{\mathfrak{c}}$ is the dual isogeny of the isogeny defined by $\mathfrak{c}$, so it has degree 4. Thus, we have $\#E[\bar{\mathfrak{c}}] = 4$.

Consequently, we have that $E[\mathfrak{c}]$ and $E[\bar{\mathfrak{c}}]$ are cyclic of order 4 or isomorphic to $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$. We assume $E[\mathfrak{c}] \cong \mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$. This means that $E[\mathfrak{c}] = E[2]$; i.e., the action of the ideal class of $\mathfrak{c}$ on $\mathcal{E}\ell\ell_p(\mathcal{O},\pi)$ is trivial. Therefore, by Theorem 2, $\mathfrak{c}$ is principal. Furthermore, by Theorem 4, $\mathfrak{l}_1^{r_1}\cdots\mathfrak{l}_n^{r_n}$ is also principal. This contradicts Theorem 3 that says the order of $\{\mathfrak{l}_1^{r_1}\cdots\mathfrak{l}_n^{r_n}\}$ is 3. Thus, $E[\mathfrak{c}]$ is cyclic of order 4. The statement for $E[\bar{\mathfrak{c}}]$ can be proven similarly.

Equations (15) and (16) directly follow from equations (13) and (14). □

3.2 Ideal representation without the collisions stated in Section 3.1

For simplicity, we use the setting in CSIDH in this subsection; i.e., we assume $r_1 = \cdots = r_n = 1$.

Corollary 1 says that if one uses the secret exponents $(e_1,\ldots,e_n)$ in the intervals $[-m,m]^n$ with $m \geq 2$ in CSIDH, then there are collisions in the ideal representation. For example, CSIDH-512, which is a parameter set of CSIDH with a prime p about 512 bits proposed by Castryck et al. [3], uses the intervals $[-5,5]^{74}$, so it contains collisions.

On the other hand, for CSIDH-512, Beullens, Kleinjung, and Vercauteren [1] proposed a method to choose ideal classes uniformly. However, their method relies on knowledge of the structure of the ideal class group; in particular, it needs a list of secret exponents which represent the identity element of the ideal class group. To obtain the structure of the ideal class group, they used the algorithm due to Hafner and McCurley [11]. Since that algorithm is subexponential time in the discriminant of the target number field, their method can not be applied to a CSIDH when a large base field is used. Therefore, the ideal representation proposed in [3] is still important.

For the general case, one way to avoid the collisions stated in Section 3.1 is to use different intervals for each e_i in which there is at least one interval of the form $[-1,1]$. De Feo, Kieffer, and Smith [9] and Meyer, Campos, and Reith [15] proposed using different intervals for each e_i for speeding up the computation of the action of the ideal classes. One can expect that this representation is "almost" surjective and uniform, from a similar argument to the one in §7.1 in [3] (for the case of using different intervals, see §5.4 in [21]).

We propose another representation that is more efficiently computable than the method described in the above paragraph. Our representation uses $\mathfrak{c}$ instead of $\mathfrak{l}_n$ and is of the form

$$\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_{n-1}^{e_{n-1}} \mathfrak{c}^f \quad \text{for} \quad -m_i \leq e_i \leq m_i,\ f \in \{-1, 0, 1\}, \tag{17}$$

where $m_1, \ldots, m_{n-1}$ are positive integers such that $\prod_i (2m_i + 1) \geq \sqrt{p}$. By Corollary 2, the action of $\mathfrak{c}$ can be efficiently computed by an isogeny of degree 4. We give the formulae for computing this isogeny between Montgomery curves in Section 4.2. The reason for choosing $\mathfrak{l}_n$ as a replacement is that the cost of the isogeny associated with $\mathfrak{l}_n$ is the highest in the prime ideals $\mathfrak{l}_1, \ldots, \mathfrak{l}_n$.

To show the validity of our representation, recall the exact sequence (6)

$$1 \to (\mathcal{O}_K/\mathfrak{f})^\times/(\mathcal{O}/\mathfrak{f})^\times \to \mathrm{cl}(\mathcal{O}) \to \mathrm{cl}(\mathcal{O}_K) \to 1.$$

We denote the image of $(\mathcal{O}_K/\mathfrak{f})^\times/(\mathcal{O}/\mathfrak{f})^\times$ in $\mathrm{cl}(\mathcal{O})$ by G. As we stated in the proof of the Theorem 3, G is a group of order 3 generated by $\{\bar{\mathfrak{l}}_1^{r_1} \cdots \bar{\mathfrak{l}}_n^{r_n}\} = \{\mathfrak{c}\}$. We define a set

$$M = \bigoplus_{i=1}^{n-1} ([-m_i, m_i] \cap \mathbb{Z}). \tag{18}$$

Then, we want to show the map

$$M \to \mathrm{cl}(\mathcal{O})/G, \quad (e_i) \mapsto \text{the image of } \mathfrak{l}_1^{e_1} \ldots \mathfrak{l}_{n-1}^{e_{n-1}} \tag{19}$$

is "almost" uniform and surjective. We can do so by using the same discussion as in §7.1 in [3]. Therefore, the map

$$M \times \{-1, 0, 1\} \to \mathrm{cl}(\mathcal{O}), \quad (e_1, \ldots, e_{n-1}; f) \mapsto \{\mathfrak{l}_1^{e_1} \ldots \mathfrak{l}_{n-1}^{e_{n-1}} \mathfrak{c}^f\} \tag{20}$$

is also "almost" uniform and surjective.

4 Formulae for Montgomery curves

Here, we give formulae for computing the action of our new representation on Montgomery curves [18]. A Montgomery curve defined over $\mathbb{F}_p$ is an elliptic curve defined by

$$By^2 = x^3 + Ax^2 + x, \tag{21}$$

where $A, B \in \mathbb{F}_p$. We denote this curve by $E_{A,B}$ or E_A if $B = 1$. Castryck et al. [3] showed that all curves in $\mathcal{E}\ell\ell_p(\mathcal{O}, \pi)$ can be defined as unique Montgomery curves and proposed an implementation of CSIDH on Montgomery curves.

4.1 Existing formulae

First, let us recall the formulae for computing an isogeny between Montgomery curves presented by De Feo, Jao, and Plût [8] and Costello and Hisil [5]. We will use these formulae for proving our new formulae.

Theorem 5. *Let $E_{A,B}$ be a Montgomery curve over $\mathbb{F}_p$. Let $P_+, P_- \in E_{A,B}$ such that the x-coordinate of P_+ is 1 and the x-coordinate of P_- is -1. Then the points P_+ and P_- have order 4, and the elliptic curve $E_{A,B}/\langle P_+\rangle$ is defined by*

$$\frac{B}{2-A}y^2 = x^3 + 2\frac{A+6}{A-2}x^2 + x, \tag{22}$$

and the elliptic curve $E_{A,B}/\langle P_-\rangle$ is defined by

$$\frac{B}{2+A}y^2 = x^3 - 2\frac{A-6}{A+2}x^2 + x. \tag{23}$$

Proof. The first assertion can be easily checked by using the duplication formula for Montgomery curves [18]. For the second, see equation (20) in [8].

For the third, we use an isomorphism between a Montgomery curve and its twist. Let i be a square root of -1 in $\bar{\mathbb{F}}_p$. For $a, b \in \mathbb{F}_p$, we define the isomorphism

$$t_{a,b} : E_{a,b} \to E_{-a,b}, \quad (x, y) \mapsto (-x, iy). \tag{24}$$

Then, $t_{A,B}(P_-)$ is a point of $E_{-A,B}$ whose x-coordinate is 1. Let φ be the isogeny $E_{-A,B} \to E_{-A,B}/\langle t_{A,B}(P_-)\rangle$. By the second assertion of this theorem, we have $E_{-A,B}/\langle t_{A,B}(P_-)\rangle = E_{A',B'}$, where

$$A' = 2\frac{A-6}{A+2},\ B' = \frac{B}{2+A}. \tag{25}$$

Then the composition

$$t_{A',B'} \circ \varphi \circ t_{A,B} : E_{A,B} \to E_{-A',B'} \tag{26}$$

is the isogeny defined over $\mathbb{F}_p$ with kernel $\langle P_-\rangle$. This proves the third assertion. □

Theorem 6. *Let $E_{A,B}$ be a Montgomery curve defined over $\mathbb{F}_p$, $P \in E_{A,B}$ a point of order $\ell = 2d + 1$, and φ the isogeny from $E_{A,B}$ with kernel $\langle P\rangle$. For $i \in \mathbb{N}$, we denote the x-coordinate of $[i]P$ by x_i. Then, the codomain of φ is $E_{A',B'}$, where*

$$A' = \left(6\sum_{i=1}^{d}\frac{1}{x_i} - 6\sum_{i=1}^{d}x_i + A\right)\left(\prod_{i=1}^{d}x_i\right)^2 \quad \text{and} \quad B' = B\left(\prod_{i=1}^{d}x_i\right)^2, \tag{27}$$

and φ maps

$$(x, y) \mapsto (f(x), yf'(x)), \tag{28}$$

where

$$f(x) = x \prod_{i=1}^{d} \left(\frac{x x_i - 1}{x - x_i} \right)^2, \tag{29}$$

and $f'(x)$ is its derivative.

Proof. This is a special case of Theorem 1 of [5]. □

4.2 New formulae

Here, we give formulae for isogenies corresponding to the ideals $\mathfrak{l}_1^{r_1} \cdots \mathfrak{l}_n^{r_n}$ and $\bar{\mathfrak{l}}_1^{r_1} \cdots \bar{\mathfrak{l}}_n^{r_n}$ between Montgomery curves. By Corollary 2, these isogenies can be computed by the actions of the ideals $\mathfrak{c}$ and $\bar{\mathfrak{c}}$. First, we give generators of the torsion subgroups $E[\mathfrak{c}]$ and $E[\bar{\mathfrak{c}}]$.

Lemma 1. *Let $A \in \mathbb{F}_p$ such that $E_A \in \mathcal{E}\ell\ell_p(\mathcal{O}, \pi)$, P_+ be a point of E_A of x-coordinate 1, and P_- be a point of E_A of x-coordinate -1. Then*

$$E_A[\mathfrak{c}] = \langle P_- \rangle, \tag{30}$$

$$E_A[\bar{\mathfrak{c}}] = \langle P_+ \rangle. \tag{31}$$

Proof. By definition, we have

$$E_A[\mathfrak{c}] = E_A[4] \cap E_A(\mathbb{F}_p), \tag{32}$$

$$E_A[\bar{\mathfrak{c}}] = E_A[4] \cap \{Q \in E_A \mid [\pi]Q = -Q\}. \tag{33}$$

Furthermore, by Theorem 5, the points P_- and P_+ have order 4. Therefore, it suffices to show that $P_- \in \mathbb{F}_p$ and $[\pi]P_+ = -P_+$.

By Corollary 2, $E_A[\mathfrak{c}]$ is cyclic of order 4. Therefore, the 2-torsion subgroup $E_A[2]$ is not contained in $E_A(\mathbb{F}_p)$. This means the equation

$$x^3 + Ax^2 + x = 0 \tag{34}$$

has only one solution $x = 0$ in $\mathbb{F}_p$. Thus, the discriminant $A^2 - 4$ of $x^2 + Ax + 1$ is not a square in $\mathbb{F}_p$. Therefore, one of $A - 2$ or $A + 2$ is a square in $\mathbb{F}_p$, and the other is not. Since the y-coordinate of P_- is a square root of $A - 2$, while that of P_+ is a square root of $A + 2$, one of P_- or P_+ is in $E_A(\mathbb{F}_p)$ and the other is not. Since the x-coordinate of P_+ is in $\mathbb{F}_p$, if $P_+ \notin E_A(\mathbb{F}_p)$, then $[\pi]P_+ = -P_+$. Therefore, it suffices to prove $P_- \in E_A(\mathbb{F}_p)$.

Since $p \equiv 3 \pmod 8$, -2 is a square in $\mathbb{F}_p$. Therefore, the lemma holds in the case $A = 0$. For the general case, we consider an isogeny from E_0 to E_A. Let P'_- be a point of E_0 whose x-coordinate is -1. By Theorem 2, there exists an integral invertible ideal $\mathfrak{a}$ such that $E_A = \mathfrak{a} * E_0$. By changing a representative of the ideal class if necessary, we may assume that the absolute norm of $\mathfrak{a}$ is odd; i.e., the isogeny defined by $\mathfrak{a}$ has odd degree. By substituting $x = -1$ into equation (29) in Theorem 6, it follows that this isogeny maps P'_- to P_-. (Note that for $b \in \mathbb{F}_p^\times$, E_{A,b^2} is isomorphic over $\mathbb{F}_p$ to E_A by $(x, y) \mapsto (x, by)$.) Since P'_- is defined over $\mathbb{F}_p$, P_- is also defined over $\mathbb{F}_p$. □

Next, we give formulae for the isogenies corresponding to the ideals $\mathfrak{l}_1^{r_1}\cdots\mathfrak{l}_n^{r_n}$ and $\bar{\mathfrak{l}}_1^{r_1}\cdots\bar{\mathfrak{l}}_n^{r_n}$.

Theorem 7. *Let $A \in \mathbb{F}_p$ such that $E_A \in \mathcal{E}\ell\ell_p(\mathcal{O},\pi)$. We define*

$$A' = -2\frac{A+6}{A-2}, \quad A'' = 2\frac{A-6}{A+2}. \tag{35}$$

Then

$$(\mathfrak{l}_1^{r_1}\cdots\mathfrak{l}_n^{r_n}) * E_A = E_{A'}, \quad (\bar{\mathfrak{l}}_1^{r_1}\cdots\bar{\mathfrak{l}}_n^{r_n}) * E_A = E_{A''}. \tag{36}$$

Proof. By Corollary 2, we have $\mathfrak{l}_1^{r_1}\cdots\mathfrak{l}_n^{r_n} * E_A = \bar{\mathfrak{c}} * E_A$. The above lemma says that $\mathfrak{c} * E_A = E_A/\langle P_+\rangle$. Therefore, by Theorem 5, $\mathfrak{l}_1^{r_1}\cdots\mathfrak{l}_n^{r_n} * E_A$ can be defined by

$$\frac{1}{2-A}y^2 = x^3 + 2\frac{A+6}{A-2}x^2 + x. \tag{37}$$

For $a, b \in \mathbb{F}_p$, the Montgomery curve $E_{a,-b^2}$ is $\mathbb{F}_p$-isomorphic to E_{-a} by $(x,y) \mapsto (-x, by)$. Since $P_- \in E_A(\mathbb{F}_p)$, the element $A-2$ is a square in $\mathbb{F}_p$. Therefore, the curve defined by equation (37) is $\mathbb{F}_p$-isomorphic to the curve defined by

$$y^2 = x^3 - 2\frac{A+6}{A-2}x^2 + x. \tag{38}$$

This proves the first assertion of the theorem. One can prove the second similarly. □

By using Corollary 2 and Theorem 7, we can compute the action of the ideal representation proposed in Section 3.2. The action of $\mathfrak{l}_1^{e_1}\cdots\mathfrak{l}_{n-1}^{e_{n-1}}\mathfrak{c}^f$ on a Montgomery curve $E_A \in \mathcal{E}\ell\ell_p(\mathcal{O},\pi)$ can be computed as follows:

(i) Set $A' = 2\frac{A-6}{A+2}$ if $f = 1$, $A' = A$ if $f = 0$, and $A' = -2\frac{A+6}{A-2}$ if $f = -1$.
(ii) Compute $(\mathfrak{l}_1^{e_1}\cdots\mathfrak{l}_{n-1}^{e_{n-1}}) * E_{A'}$ by using Algorithm 2 in [3].

5 Conclusion

We showed that the ideal class of $\mathfrak{l}_1^{r_1}\cdots\mathfrak{l}_n^{r_n}$ has order 3 in the ideal class group and the same class of the ideal $\bar{\mathfrak{c}}$. In CSIDH, the former means that the secret exponents $(e_1, e_2 \ldots, e_n)$ and $(e_1+3, e_2+3, \ldots, e_n+3)$ generate the same public key. The latter means that the action of the secret exponents $(1, \ldots, 1)$ can be computed by an isogeny of degree 4. We gave formulae for computing this action on Montgomery curves. Furthermore, we proposed a new ideal representation for CSIDH that does not contain the collisions we found. Our new ideal representation can be computed efficiently by using the formula for computing the action of the secret exponents $(1, \ldots, 1)$.

Appendix Odd-degree isogenies using 4-torsion points

We give new formulae for computing odd-degree isogenies between Montgomery curves by calculating the images of P_+ and P_-.

Theorem 8. *We use the same notation as in Theorem 6 and assume $B = 1$. Further, we assume that the group $\langle P \rangle$ is stable under the action of the p-th power Frobenius endomorphism. Then, there exists $A' \in \mathbb{F}_p$ such that $E_{A'} = E_A/\langle P \rangle$. Furthermore, A' satisfies the equations*

$$A' + 2 = (A + 2)\left(\left(1 + 2\sum_{i=1}^{d} \frac{x_i + 1}{x_i - 1}\right)\prod_{i=1}^{d} x_i\right)^2, \tag{39}$$

$$A' - 2 = (A - 2)\left(\left(1 + 2\sum_{i=1}^{d} \frac{x_i - 1}{x_i + 1}\right)\prod_{i=1}^{d} x_i\right)^2. \tag{40}$$

Proof. Let $b = \prod_{i=1}^{d} x_i$. Then we have $b \in \mathbb{F}_p$, because the group $\langle P \rangle$ is stable under the action of the p-th power Frobenius map. Theorem 6 says that the isogeny with kernel $\langle P \rangle$ is given by

$$E_A \to E_{A',b^2}, \quad (x, y) \mapsto (f(x), yf'(x)), \tag{41}$$

where A' is defined in Theorem 6. We have $E_{A',b^2} = E_{A'}$ because $E_{A',b^2} \to E_{A'}$, $(x, y) \mapsto (x, by)$ is a $\mathbb{F}_p$-isomorphism. This proves the first assertion.

Let $P_+, P_- \in E_A$ be the same as in Lemma 1. We denote the y-coordinate of P_+ by y_+. Note that $y_+^2 = A+2$. The image of P_+ under the isogeny $E_A \to E_{A'}$ is $(1, by_+f'(1))$. One can easily check that

$$f'(1) = 1 + 2\sum_{i=1}^{d} \frac{x_i + 1}{x_i - 1}. \tag{42}$$

Substituting $(1, by_+f'(1))$ into equation of $E_{A'}$ yields equation (39). By considering the image of P_-, we obtain equation (40). □

As same as the other formulae for isogenies between Montgomery curves [8, 6, 5, 22, 16], our formulae can avoid inversions by using a projective coordinate of A. For $x \in \mathbb{F}_p$, we call a pair $X, Z \in \mathbb{F}_p$ such that $x = X/Z$ a projective coordinate of x and denote it by $(X : Z)$. The following corollary gives a projectivized variant of equation (40) in the above theorem. Note that a projectivized variant of equation (39) can be obtained in the same way.

Corollary 3. *We use the same notation as in Theorem 8. Let $(a : c)$ be a projective coordinate of A and $(X_i : Z_i)$ a projective coordinate of x_i. We define*

$$c' = c(\prod_{i=1}^{d} S_i \prod_{i=1}^{d} Z_i)^2), \tag{43}$$

$$a' = (a - 2c)((\prod_{i=1}^{d} S_i + 2\sum_{i=0}^{d} D_i \prod_{j \neq i} S_j)\prod_{i=1}^{d} X_i)^2 + 2c', \tag{44}$$

where $S_i = X_i + Zi,\ D_i = X_i - Z_i$. *Then* $(a' : c')$ *is a projective coordinate of* A'.

Proof. This follows immediately from equation (40). □

By Corollary 2, we obtain an algorithm (Algorithm 1) for computing the coefficient of the codomain of an odd-degree isogeny. We assume that the elements X_i, Z_i, S_i and D_i are precomputed. These elements are used in the computation for the image of a point under an isogeny. In CSIDH, one needs to compute not only the coefficient of the codomain of an isogeny, but also the image of a point under that isogeny. Therefore, it is natural to separate the computation of these elements from that of an isogeny.

Algorithm 1 Odd-degree isogeny

Require: A projective coordinate $(a : c)$ of the coefficient of a Montgomery curve, projective coordinates $(X_i : Z_i)$ of the x-coordinate of $[i]P$, where $P \in E_{a/c}$ has odd order $\ell = 2d + 1$, $S_i = X_i + Z_i$, and $D_i = X_i - Z_i$ for $i = 1, \ldots, d$.
Ensure: a projective coordinate $(a' : c')$ such that $E_{a'/c'} = E_{a/c}/\langle P \rangle$.

$X \leftarrow X_1,\ Z \leftarrow Z_i,\ F \leftarrow D_1,\ G \leftarrow S_1$
for $i = 2$ to d **do**
  $X \leftarrow XX_i$.
  $Z \leftarrow ZZ_i$.
  $F \leftarrow FS_i + GD_i$.
  $G \leftarrow GS_i$.
end for
$c' \leftarrow c(GZ)^2$.
return $((a - 2c)((G + 2F)X)^2 + 2c' : c')$.

The cost of Algorithm 1 is

$$(5d - 1)\mathbf{M} + 2\mathbf{S} + (d + 5)\mathbf{a}, \tag{45}$$

where $\mathbf{M}$, $\mathbf{S}$, and $\mathbf{a}$ mean multiplication, squaring, and addition or subtraction on the field $\mathbb{F}_p$, respectively.

On the other hand, the costs of the similar algorithms in the previous studies are as follows. Castryck et al. [3] used the formula from Costello and Hisil [5] and Renes [22]. The cost is

$$(6d - 2)\mathbf{M} + 3\mathbf{S} + 4\mathbf{a}. \tag{46}$$

Meyer and Reith [16] proposed an algorithm that exploits the correspondence between Montgomery curves and twisted Edwards curves. The cost is

$$2d\mathbf{M} + 6\mathbf{S} + 6\mathbf{a} + 2w(\ell), \tag{47}$$

where $w(\ell)$ is the cost of the ℓ-th power on $\mathbb{F}_p$. If we use the binary algorithm for exponentiation, we obtain $w(\ell) = (h-1)\mathbf{M} + (t-1)\mathbf{S}$, where h and t are the Hamming weight and the bit length of ℓ, respectively.

For comparing the above costs, we assume that $\mathbf{S} = 0.8\mathbf{M}$ and $\mathbf{a} = 0.05\mathbf{M}$ as in [16]. We conclude that Algorithm 1 is the fastest if $\ell \leq 7$ and the algorithm in [16] is the fastest if $\ell > 7$. Table 1 shows the costs of these algorithms for small degrees.

Table 1. Costs of odd-degree isogeny computations

degree	Algorithm 1	Algorithm in [3]	Algorithm in [16]
3	5.90**M**	6.70**M**	10.70**M**
5	10.95**M**	12.80**M**	14.30**M**
7	16.00**M**	18.90**M**	18.30**M**
9	21.05**M**	25.00**M**	19.90**M**
11	26.10**M**	31.00**M**	23.90**M**

References

1. W. Beullens, T. Kleinjung, F. Vercauteren: CSI-FiSh: Efficient Isogeny based Signatures through Class Group Computations. IACR Cryuptography ePrint Archive 2019/498; `https://eprint.iacr.org/2019/498`
2. J. Buchmann, H. C. Williams: A Key-Exchange System Based on Imaginary Quadratic Fields. Journal of Cryptology **1**, 107–118 (1988).
3. W. Castryck, T. Lange, C. Martundale, L. Panny, J. Renes: CSIDH: An efficient post-quantum commutative group action. ASIACRYPT 2018, LNCS 11274, 395–427 (2018).
4. H. Cohen and H. W. Lenstra, Jr.: Heuristics on class groups of number fields. Number Theory, Noordwijkerhout 1983, 33–62 (1984).
5. C. Costello, H. Hisil: A simple and compact algorithm for SIDH with arbitrary degree isogenies. ASIACRYPT 2017, LNCS 10625, 303–329 (2017).
6. C. Costello, P.Longa, M. Naehrig: Efficient algorithms for supersingular isogeny Diffie-Hellman. CRYPTO 2016, LNCS 9814, 572–601 (2016).
7. J-M. Couveigne: Hard homogeneous spaces. IACR Cryptology ePrint Archive 2006/291; `https://eprint.iacr.org/2006/291`.
8. L. De Feo, D. Jao, and J. Plût: Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. Journal of Mathematical Cryptology **8**(3), 209—247 (2014).
9. L. De Feo, J. Kieffer, B. Smith: Towards practical key exchange from ordinary isogeny graphs. ASIACRYPT 2018, LNCS 11274, 365–394 (2018).
10. W. Diffie, M. Hellman: New Directions in Cryptography, IEEE Transactions on Information Theory **22**(6), 644-–654 (1976).
11. James L. Hafner, Kevin S. McCurley: A rigorous subexponential algorithm for computation of class groups. Journal of the American Mathematical Society, 2:837-–850 (1989).
12. D. Jao, L. De Feo: Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. PQCrypto 2011, LNCS 7071, 19–34 (2011).

13. D. Jao, R. Azarderakhsh, M. Campagna, C. Costello, L. De Feo, B. Hess, A. Jalali, B. Koziel, B. LaMacchia, P. Longa, M. Naehrig, J. Renes, V. Soukharev, D, Urbanik: Supersingular isogeny key encapsulation. Submission to the NIST Post-Quantum Cryptography Standardization project; `https://sike.org`.
14. N. Koblitz: Elliptic Curve Cryptosystems. Mathematics of Computation **48**(177), 203–209 (1987).
15. M. Meyer, F. Campos, S. Reith: On Lions and Elligators: An efficient constant-time implementation of CSIDH. PQCrypto 2019, LNCS 11505, 307–325 (2019).
16. M. Meyer, S. Reith: A faster way to the CSIDH. INDOCRYPT 2018, LNCS 11356, 137–152 (2018).
17. V. Miller: Use of Elliptic Curves in Cryptography. CRYPTO 1985, LNCS 218, 417–426 (1986).
18. P. L. Montgomery: Speeding the Pollard and elliptic curve methods of factorization. Mathematics of Computation **48**(177), 24–264 (1987).
19. National Institute of Standards and Technology (NIST): NIST Post-Quantum Cryptography Standardization; `https://csrc.nist.gov/Projects/Post-Quantum-Cryptography`, (2016).
20. J. Neukirch: Algebraic Number Theory, Springer-Verlag (1999).
21. H. Onuki, Y, Aikawa, T. Yamazaki, T. Takagi: A Faster Constant-time Algorithm of CSIDH keeping Two Points IACR Cryptography ePrint Archive 2019/353; `https://eprint.iacr.org/2019/353`
22. J. Renes: Computing isogenies between Montgomery curves using the action of (0, 0). PQCrypto 2018, LNCS 10786, 229—247 (2018).
23. A. Rostovtsev, A. Stolbunov: Public-key cryptosystem based on isogenies. IACR Cryptology ePrint Archive 2006/145; `https://eprint.iacr.org/2006/145`.
24. J. H. Silverman: Advanced topics in the arithmetic of elliptic curves. GTM 151, Springer (1994).
25. J. H. Silverman: The arithmetic of elliptic curves. GTM 106, Springer, 2nd edition (2009).
26. A. Stolbunov: Constructing public-key cryptographic schemes based on class group action on a set of isogenous elliptic curves, Advances in Mathematics of Communications **4**(2), 215–235 (2010).
27. J. Vélu: Isogénies entre courbes elliptiques. Comptes Rendus de l ' Académie des Sciences de Paris, Series A **273**, 238—241 (1971).