CSIDH on Elliptic Curves of the Form $y^2 = x^3 + Ax^2 - x$

Xuejun Fan[1,2], Song Tian[1,2], Bao Li[1,2], and Xiu Xu[1,2]

1 School of Cyber Security, University of Chinese Academy of Sciences.
2 State Key Laboratory of Information Security, Institute of Information Engineering,
Chinese Academy of Sciences, Beijing, China.
fanxuejun@iie.ac.cn

Abstract. Isogenies between elliptic curves over a common finite field are of great interest in post-quantum cryptography. Many protocols have been proposed such as Supersingular Isogeny Diffie-Hellman key exchange (SIDH) and Commutative Supersingular Isogeny Diffie-Hellman key exchange (CSIDH). The CSIDH uses supersingular elliptic curves of Montgomery form over finite fields $\mathbb{F}_p$ with $p \equiv 3 \pmod 8$ whose endomorphism rings are $\mathbb{Z}[\sqrt{-p}]$. While we consider the supersingular elliptic curves over $\mathbb{F}_p$ with $p \equiv 7 \pmod 8$ and show that they can be expressed uniquely in the form of $y^2 = x^3 + Ax^2 - x$ if and only if their endomorphism rings are isomorphic to $\mathbb{Z}[\frac{\sqrt{-p}+1}{2}]$, which is our first contribution. The original motivation is to avoid the collisions in CSIDH where 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. Wouter Castryck and Thomas Decru also show a similar idea and propose CSURF. While we use a different way from theirs to prove that the coefficients A can be the unique representation of the $\mathbb{F}_p$-isomorphism classes. We also give formulae of 2-isogenies corresponding to the ideal class $[(2, \frac{\pi\pm1}{2})]$ in different ways and compare the cost of them. As our second contribution, we find collisions in the ideal representation in CSURF where the vectors $(e_0, e_1, \ldots, e_n)$ and $(e_0 + 1, e_1 + 2, e_3 + 1, \ldots, e_n + 1)$ represent the same ideal class, and then give a new ideal class representative that will avoid the duplications. The new ideal class representative can also help to avoid the computation of the largest isogeny in the protocol and thus offer a speed-up of about 6.02%. Moreover, we try to change the direction of the loop computing the action of ideal classes and get a speed-up of about 28.69%.

Keywords: CSIDH, Montogomery Curves, Endomorphism Ring, Collision, Ideal Class Representative.

1 Introduction

Elliptic curve cryptography was proposed by Koblitz [12] and Miller [13] in 1985. It relies on the assumption that the elliptic curve discrete logarithm problem (ECDLP) is hard. However, Shor's algorithm makes ECDLP easy on a quantum computer [1]. It was Couveignes [14] who first realized in 1997 that computing isogenies between elliptic curves over finite fields can be considered to be an intractable problem on a quantum computer. Basing on this problem, he proposed a key agreement scheme which was rediscovered by Rostovtsev and Stolbunov [15] independently in 2006. Their key agreement scheme, which we will call CRS, uses the action of the ideal class groups of the endomorphism rings of ordinary elliptic curves. As pointed out by Childs, Jao and Soukharev [23], the underlying hard problem can be phrased as a hidden shift problem which is amenable to Kuperberg's algorithm [17]. In contrast with the ordinary case, supersingular elliptic curves do not admit such an action of an abelian group. This difficulty is resolved by Jao and De Feo [16] by means of publishing the images of certain points under secrete isogenies. The resulting scheme named supersingular isogeny Diffie-Hellman key exchange (SIDH), on which one of the most competitive algorithms in NIST's post-quantum standardization project called supersingular isogeny key encapsulation (SIKE) [19] is based.

In order to achieve reasonable efficiency in CRS, one should use elliptic curves whose order is a product of small primes. So far there is no known efficient algorithms to generate such kind of ordinary elliptic curves. Though some improvements have been made by Luca De Feo et al. [18], the result is still not satisfactory. Recently, a CRS style key exchange based on supersingular elliptic curves has been proposed by Castryck, Lange, Martindale, Panny and Renes [9]. They notice that the set of $\mathbb{F}_p$-isomorphism classes of supersingular elliptic curves over a prime field $\mathbb{F}_p$ is also a "homogeneous space" under the ideal class group of certain order in imaginary quadratic number field, and that it is much easier to choose supersingular elliptic curves which are suitable for implementation. Their scheme, which is named commutative supersingular isogeny Diffie-Hellman (CSIDH), is fairly efficient and thus receives lots of attention. For example, it is possible to construct reasonably efficient signature scheme [24].

The supersingular elliptic curves that CSIDH uses are over finite prime fields $\mathbb{F}_p$ with $p \equiv 3 \pmod 8$. Their endomorphism rings (over $\mathbb{F}_p$) are isomorphic to $\mathbb{Z}[\sqrt{-p}]$, which is shown to be equivalent to that the curves can be expressed uniquely in Montgomery form. In this article, we consider the supersingular elliptic curves over $\mathbb{F}_p$ with $p \equiv 7 \pmod 8$ and show that they can be expressed uniquely in the form of $y^2 = x^3 + Ax^2 - x$ if and only if their endomorphism rings are isomorphic to $\mathbb{Z}[\frac{\sqrt{-p}+1}{2}]$. This implies that the coefficient A can be used to represent the $\mathbb{F}_p$-isomorphism class or public key. We also use different ways to compute the 2-isogenies between the supersingular elliptic curves of the form $y^2 = x^3 + Ax^2 - x$. Moreover, we find explicit collisions when elliptic curves $E_A : y^2 = x^3 + Ax^2 - x$ over $\mathbb{F}_p$ with $p \equiv 7 \pmod 8$ are used, namely, the vector $(e_0, e_1, \ldots, e_n)$ and the $(e_0 + 1, e_1 + 2, e_2 + 1, \ldots, e_n + 1)$ represent the same ideal class. To avoid the trivial duplications, we offer re-expressions of the ideal classes which also gives a speed-up for about 6.02% comparing to the original implementation. To get a higher performance, we change the direction of the loop in the implementation of CSURF and gain a speed-up of about 28.69% comparing to the original implementation.

The type of curves we consider is also studied by Castryck et al. in [20], where they name the corresponding curves Montgomery$^-$ curves. We emphasize that the proof of the link between Montgomery$^-$ form and endomorphism rings is different from theirs, and that the formulae for 2-isogenies, the analysis of the collision problem and the change of loop direction are new results.

Organization. In Section 2, we recall, besides CSIDH and CSURF, some basic results on ideal class groups and isogenies over $\mathbb{F}_p$ that will be used in later sections. In Section 3, we give some essential conclusions about the case of $\mathrm{End}_{\mathbb{F}_p}E = \mathcal{O}_K$ as the analogue of $\mathrm{End}_{\mathbb{F}_p}E = \mathbb{Z}[\pi]$ in [9], including the formulae of ℓ-isogenies and 2-isogenies, and the bijection between the coefficients and the $\mathbb{F}_p$-isomorphism classes. In Section 4, we discuss the collisions in CSURF and offer a new ideal class representative, and then change the direction of the loop, which brings a speed-up. In Section 5, we give a conclusion.

2 Preliminaries

2.1 The Ideal Class Group and Its Action

Let $K = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic field. An order of K is a subring $\mathcal{O}$ which is also a lattice. It is well know that K has a unique maximal order $\mathcal{O}_K$, which is the ring of integers. An order $\mathcal{O}$ can be expressed as $\mathbb{Z} + f\mathcal{O}_K$ for an integer $f > 0$. The integer f is called the conduct of $\mathcal{O}$.

Let $\mathcal{O}$ be an order of K. A fractional ideal $\mathfrak{a}$ of $\mathcal{O}$ is an $\mathcal{O}$-module of the form $\alpha\mathfrak{a}'$, where $\alpha \in K^*$ and $\mathfrak{a}'$ is an integral ideal of $\mathcal{O}$. It is said to be invertible if there exists a fractional ideal $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b} = \mathcal{O}$. All invertible fractional ideals of $\mathcal{O}$ form an abelian group $I(\mathcal{O})$. A fractional ideal of form $\alpha\mathcal{O}$ with $\alpha \in K^*$ is called a principal fractional ideal. All principal fractional ideals are invertible and form a subgroup $P(\mathcal{O})$ of $I(\mathcal{O})$. The quotient of $I(\mathcal{O})$ by $P(\mathcal{O})$, denoted by $\mathrm{cl}(\mathcal{O})$, is called the ideal class group of $\mathcal{O}$. We will denote by $[\mathfrak{a}]$ the class of an invertible fractional ideal $\mathfrak{a}$.

Now let E be a supersingular elliptic curve over $\mathbb{F}_p$ with $p > 3$. Let π be its Frobenius endomorphism. Then its endomorphism algebra is $\mathbb{Q}[\pi] \simeq \mathbb{Q}(\sqrt{-p})$, which implies that its $\mathbb{F}_p$-rational endomorphism ring $\mathrm{End}_{\mathbb{F}_p}(E)$ is an order of the imaginary quadratic field $\mathbb{Q}(\pi)$. According to [21, Theorem 4.2], the conduct of $\mathrm{End}_{\mathbb{F}_p}(E)$ is prime to p. So $\mathrm{End}_{\mathbb{F}_p}(E)$ is isomorphic to either $\mathbb{Z}[\sqrt{-p}]$ or the maximal order of $\mathbb{Q}(\sqrt{-p})$.

If $\mathfrak{a}$ is any integral ideal of $\mathcal{O} = \mathrm{End}_{\mathbb{F}_p}(E)$, then we can define a finite group scheme

$$E[\mathfrak{a}] = \cap_{\phi\in\mathfrak{a}}\mathrm{Ker}(\phi)$$

and an isogeny

$$\psi_{\mathfrak{a}} : E \to E/E[\mathfrak{a}]$$

with kernel $E[\mathfrak{a}]$. If $\mathfrak{a}$ is invertible as a fractional ideal of $\mathcal{O}$, then the $\mathbb{F}_p$-rational endomorphism ring of $E/E[\mathfrak{a}]$ is isomorphic to $\mathcal{O}$, and its $\mathbb{F}_p$-isomorphism class depends only on the class of $\mathfrak{a}$ in $\mathrm{cl}(\mathcal{O})$. In this way, we actually have a well-defined action of $\mathrm{cl}(\mathcal{O})$ on the set $\mathcal{ELL}(\mathcal{O})$ of $\mathbb{F}_p$-isomorphism classes of supersingular elliptic curves over $\mathbb{F}_p$ whose $\mathbb{F}_p$-rational endomorphism rings are isomorphic to $\mathcal{O}$. And it turns out that the action is simply transitive.

We are interested in ℓ-isogenies for primes $\ell \neq p$, which correspond to prime ideals of $\mathcal{O}$ of norm ℓ. Of course, they might not exist if $-p$ is a non-square in $\mathbb{Z}/\ell\mathbb{Z}$. Let $G(\mathbb{F}_p, \ell)$ be the supersingular ℓ-isogeny graph. The vertices correspond to the $\mathbb{F}_p$-isomorphism classes of supersingular elliptic curves, which are often denoted by the corresponding j-invariants. The edges correspond to the equivalence classes of $\mathbb{F}_p$-rational ℓ-isogenies between different elliptic curves. The following theorem gives a general picture of $\mathbb{F}_p$, where by the surface (resp. the floor) we mean that the corresponding curves have $\mathbb{F}_p$-rational endomorphism rings isomorphic to $\mathbb{Z}[\frac{1+\sqrt{-p}}{2}]$ (resp. $\mathbb{Z}[\sqrt{-p}]$).

Theorem 1. *When $p \equiv 3 \pmod 4$, there are two levels in $G(\mathbb{F}_p, \ell)$ and for $\ell > 2$ with $(\frac{-p}{\ell}) = 1$, there are two horizontal ℓ-isogenies from each vertex.*

- *If $p \equiv 7 \pmod 8$, there are 2-isogenies connecting the surface and floor with 1:1 and in the surface there are also two horizontal 2-isogenies from each vertex.*
- *If $p \equiv 3 \pmod 8$, there are 2-isogenies connecting the surface and floor with 1:3 and no horizontal 2-isogenies.*

We give the example of $G(\mathbb{F}_{167}, 3)$ by using modular polynomials [4,5] (See Figure 1). There are 11 supersingular j-invariants in $\mathbb{F}_{167}$ in total [3]. Each j-invariant in $G(\mathbb{F}_{167}, 3)$ corresponds to two $\mathbb{F}_p$-isomorphism classes. Note that both E and E^t have $p + 1$ points, so they are isogeneous over $\mathbb{F}_{167}$. This is very different from the ordinary case where $\#E(\mathbb{F}_p) \neq \#E^t(\mathbb{F}_p)$. Running clockwise corresponds to the repeated action of $[(3, \pi - 1)]$, while running anticlockwise corresponds to that of $[(3, \pi + 1)]$. The dotted lines we add in the graph mean that there are 2-isogenies between the corresponding curves on the surface and those on the floor.

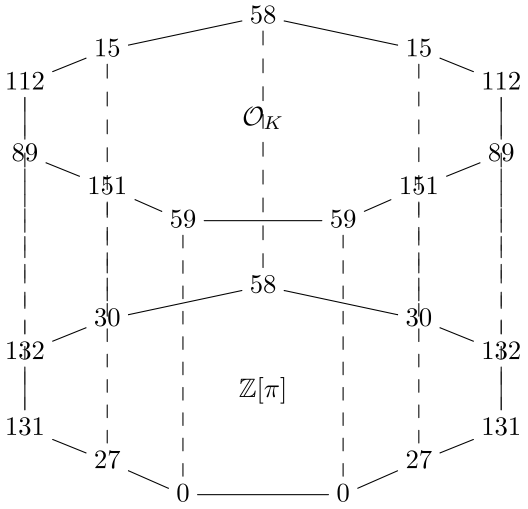

Figure 1. $G(\mathbb{F}_{167}, 3)$. The curves on surface have endomorphism ring $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{-167}}{2}]$ and those on floor have $\mathbb{Z}[\sqrt{-167}]$ as endomorphism ring.

As is shown in [6], if the two eigenvalues λ and μ of the Frobenius map π satisfy that $\lambda^r \equiv 1 \pmod{\ell}$ and $\mu^r \not\equiv 1 \pmod{\ell}$, then the isogeny corresponds to $[\ell, \pi - \lambda]$ can be computed over $\mathbb{F}_{p^r}$. So we can compute the action of $[(3, \pi - 1)]$ over the base field $\mathbb{F}_p$. As for $[(3, \pi+1)]$, we can compute it through its quadratic twist E^t by $[(3, \pi + 1)]E = ([(3, \pi - 1)]E^t)^t$ to compute efficiently by using $\mathbb{F}_p$-rational points.

2.2 CSIDH and CSURF

CSIDH uses the commutative group action $\mathrm{cl}(\mathcal{O}) \times \mathcal{ELL}(\mathcal{O}) \to \mathcal{ELL}(\mathcal{O})$ with $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$ and $p \equiv 3 \pmod 8$. Every $\mathbb{F}_p$-isomorphism class in $\mathcal{ELL}(\mathcal{O})$ can be represented by a Montgomery elliptic curve $E_A : y^2 = x^3 + Ax^2 + x$ over $\mathbb{F}_p$. Since the coefficient A is unique, it is used to denote the $\mathbb{F}_p$-isomorphism class. The prime p is chosen to be of the form $p = 4 \cdot l_1 \cdots l_n - 1$ with $l_1, \ldots, l_n$ small primes. So there are prime ideals $\mathfrak{l}_i = (l_i, \pi - 1)$ of $\mathcal{O}$ of norm l_i. In CSIDH, vectors $(e_1, \cdots, e_n) \in [-m, m]^n$, which represent the ideal classes $[\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n}]$, are used as private keys. The protocol with starting curve $E_0/\mathbb{F}_p : y^2 = x^3 + x$ works as follows (see Figure 2).

Generation/Exchange: As her private key, Alice chooses a uniformly random vector $(e_1, \cdots, e_n)$. She then computes the Montgomery elliptic curve $E_A = [\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n}]E_0$ and sends Bob the coefficient A. Likewise, as his private key, Bob chooses a uniformly random vector $(e'_1, \cdots, e'_n)$. He then computes the Montgomery elliptic curve $E_B = [\mathfrak{l}_1^{e'_1} \cdots \mathfrak{l}_n^{e'_n}]E_0$ and sends Alice the coefficient B.

Key Agreement: After receiving the coefficient from each other, they check the supersingularity of the receiving curves. And then Alice calculates $[\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n}]E_B$

by using her own secret key and Bob's public key B. In the same way, Bob calculates $[\mathfrak{l}_1^{e_1'} \cdots \mathfrak{l}_n^{e_n'}]E_A$. Because of the commutativity of the class group, Alice and Bob can get the same elliptic curve $E_S = [\mathfrak{l}_1^{e_1+e_1'} \cdots \mathfrak{l}_n^{e_n+e_n'}]E_0$ and its coefficient $S \in \mathbb{F}_p$ as their shared secret.

$$\begin{tikzcd}
\mathit{Alice} & \mathit{Bob} \\
(e_1, \cdots, e_n) & (e_1', \cdots, e_n') \\
E_A = [\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n}]E_0 \arrow[r, "A"] & (\mathit{TEST}) \\
(\mathit{TEST}) & E_B = [\mathfrak{l}_1^{e_1'} \cdots \mathfrak{l}_n^{e_n'}]E_0 \arrow[l, "B"'] \\
E_S = [\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n}]E_B & E_S = [\mathfrak{l}_1^{e_1'} \cdots \mathfrak{l}_n^{e_n'}]E_A.
\end{tikzcd}$$

Figure 2. CSIDH. The "(TEST)" represents that each party will test the supersingularity of the received curve by testing its order over $\mathbb{F}_p$.

CSURF changes the form of the curves into Montgomery$^-$ elliptic curves over $\mathbb{F}_p$ with $p = 4 \cdot 2 \cdot l_1 \cdots l_n - 1$, which implies the endomorphism ring becomes $\mathcal{O}_K = \mathbb{Z}[\frac{1+\pi}{2}]$. And the whole protocol is similar with CSIDH apart from the different beginning elliptic curve, $E_0/\mathbb{F}_p : y^2 = x^3 - x$, and range of the exponent vectors. As in Figure 1, there is a one-to-one correspondence between the surface and floor, hence the alteration of endomorphism ring does not influence the security level of the protocol.CSURF implemented almost all of 2-isogenies corresponding to the ideal classes $[(2, \frac{\pi \pm 1}{2})]$ on isomorphic Montgomery curves, while we give other formulae of 2-isogenies corresponding to the ideal classes $[(2, \frac{\pi \pm 1}{2})]$ between Montgomery$^-$ curves in Section 3.2. And we find collisions in its private keys and propose a new representation to avoid them in Section 4.1.

3 CSIDH on elliptic curves $E_A : y^2 = x^3 + Ax^2 - x$

In this section, we show that it is possible to construct CSIDH over finite fields $\mathbb{F}_p$ with $p \equiv 7 \pmod 8$. First we give a formula to compute odd degree isogenies between elliptic curves of the form $y^2 = x^3 + Ax^2 - x$. Then we use this formula to show that the elements in $\mathcal{ELL}(\mathbb{Z}[\frac{1+\sqrt{-p}}{2}])$ can also be represented uniquely by coefficients of certain representatives. Finally, we study different ways of computing 2-isogenies.

3.1 Unique Representation for $\mathbb{F}_p$-isomorphism class

As for the formula of isogenies, if the elliptic curve has a form less general than Weierstrass form, the formula from Vélu, which is used commonly to compute isogeny, is not guaranteed to preserve the form. [2] obtained the formulae for isogenies on Montgomery curves, which streamlines code and enhances the efficiency of SIDH. As for CSIDH, it uses Montgomery elliptic curves for its x-only arithmetic and the unique representative formed by Montgomery coefficients.

Hence we get the formulae for ℓ-isogenies on elliptic curves of this form without any loss of efficiency.

Proposition 1. *Let K be a field with* char*$(K)\neq 2$ and $\sqrt{-1}\notin K$. Let $G\subseteq E(\overline{K})$ be a finite subgroup of order $2d+1$ in an elliptic curve $E/K : y^2=x^3+ax^2-x$ with $a\in K$. Let ϕ be a separable isogeny with* ker*$\phi=G$. Then there is a curve $E'/K : Y^2=X^3+AX^2-X$ such that, up to post-composition by an isomorphism,*

$$\phi : E\to E' : (x,y)\mapsto (f(x), c_0yf'(x)),$$

where

$$f(x)=x\prod_{T\in G\setminus\{O_E\}}\frac{xx_T+1}{x-x_T},\quad c_0^2=\prod_{T\in G\setminus\{O_E\}}x_T.$$

Moreover, we write $\sigma=\sum_{T\in G\setminus\{O_E\}}(x_T+\frac{1}{x_T})$ and $A=c_0^2(a-3\sigma)$.

The proofs of Proposition 1 are discussed in Appendix B, which are similar to those of Montgomery curves. We can conclude that, for elliptic curves in form of $E/\mathbb{F}_p : y^2=x^3+ax^2-x$ with $a\in\mathbb{F}_p$, given a finite $\mathbb{F}_p$-subgroup G of odd degree, there exists an $A\in\mathbb{F}_p$ and a separable isogeny $\phi : E\to E' : Y^2=X^3+AX^2-X$ defined over $\mathbb{F}_p$ with kernel G. In comparison to [2] on Montgomery curves, the differences are only on the signs of items. While when $i=\sqrt{-1}\in K$, there is a morphism:

$$\psi : E_A : y^2=x^3+Ax^2-x\longrightarrow E_{mon} : -iY^2=X^3+iAX^2+X,$$
$$(x,y)\longmapsto (X,Y)=(ix,y).$$

So $E_A : y^2=x^3+Ax^2-x$ and Montgomery curve $E_{mon} : BY^2=X^3+A'X^2+X$ are isomorphic, which immediately implies the same conclusion as the Proposition 1 by [2, Theorem 1]. The conclusion will also be used in the latter proposition.

In general, the nodes in isogeny graph represent $\mathbb{F}_p$-isomorphism classes of elliptic curves [8], while a new unique representative for $\mathbb{F}_p$-isomorphism class which may serve as a shared key instead of j-invariants was proposed by [9]. However, Castryck W. et al [9] only consider the finite field $\mathbb{F}_p$ with $p\equiv 3 \pmod 8$, where the unique representation for elliptic curves of the form $y^2=x^3+Ax^2-x$ doesn't exist. So we change the characteristic into $p\equiv 7 \pmod 8$ and prove the one-to-one correspondence between the $\mathbb{F}_p$-isomorphism classes and the coefficients A.

Proposition 2. *Let $p\equiv 7 \pmod 8$ be a prime and let $E/\mathbb{F}_p$ be a supersingular elliptic curve. Then $\mathrm{End}_{\mathbb{F}_p}(E)=\mathbb{Z}[\frac{1+\sqrt{-p}}{2}]$ if and only if E is $\mathbb{F}_p$-isomorphic to $E_A : y^2=x^3+Ax^2-x$ with a unique $A\in\mathbb{F}_p$.*

Proof. Let $E_A : y^2=x^3+Ax^2-x$ be a supersingular elliptic curve over $\mathbb{F}_p$. We have to show that $\mathrm{End}_{\mathbb{F}_p}(E_A)$ is isomorphic to $\mathbb{Z}[\frac{1+\sqrt{-p}}{2}]$. For this, we only need to show that $E_A(\mathbb{F}_p)[2]=\{P\in E_A(\mathbb{F}_p)|2P=0\}$ has 4 points. If $P=(x_0,y_0)\in$

$E_A(\mathbb{F}_p)$ is not a two-torsion point, then by the group law we have an $\mathbb{F}_p$-rational point

$$(-\frac{1}{x_0}, \frac{y_0}{x_0^2}) = (x_0, y_0) + (0,0).$$

Since $p \equiv 7 \pmod 8$, $x_0 \neq -\frac{1}{x_0}$, so P, $-P$, $P+(0,0)$ and $-P+(0,0)$ are pairwise distinct points. This implies that

$$\#E_A(\mathbb{F}_p) \equiv \#E_A(\mathbb{F}_p)[2] \pmod 4.$$

Since $\#E_A(\mathbb{F}_p) = p+1 \equiv 0 \pmod 8$, $\#E_A(\mathbb{F}_p)[2] = 4$ as required.

Now assume that $\mathrm{End}_{\mathbb{F}_p}(E)$ is isomorphic to $\mathbb{Z}[\frac{1+\sqrt{-p}}{2}]$. Since the elliptic curve $E_0 : y^2 = x^3 - x$ over $\mathbb{F}_p$ is supersingular, $\mathcal{O} = \mathrm{End}_{\mathbb{F}_p}(E_0)$ is also isomorphic to $\mathbb{Z}[\frac{1+\sqrt{-p}}{2}]$, so there exists an ideal class $[\mathfrak{a}] \in \mathrm{cl}(\mathcal{O})$ such that $[\mathfrak{a}]E_0 = E$. As we can always choose an $\mathcal{O}$-ideal $\mathfrak{b} \in [\mathfrak{a}]$ whose norm is relatively prime to $2p$, E is $\mathbb{F}_p$-isomorphic to $E_0/E_0[\mathfrak{b}]$, which by Proposition 1 is of the form $E_A : y^2 = x^3 + Ax^2 - x$.

It remains to show the uniqueness of A. Let $\phi : E_B : Y^2 = X^3 + BX^2 - X \to E_A$ be an $\mathbb{F}_p$-isomorphism. Then by [10, Proposition III.3.1(b)] we can write

$$\phi((X,Y)) = (u^2X + r, u^3Y + su^2X + t),$$

where $u \in \mathbb{F}_p^*$ and $r, s, t \in \mathbb{F}_p$. Since $(u^3Y + su^2X + t)^2 - (u^2X + r)^3 - A(u^2X + r)^2 + (u^2X + r)$ is divisible by $Y^2 - X^3 - BX^2 + X = 0$, we have

$$\begin{cases} s = t = 0, \\ 3r^2 + 2Ar - 1 + u^4 = 0, \\ -3r - A + Bu^2 = 0, \\ r(Ar + r^2 - 1) = 0. \end{cases}$$

Next we prove that $r = 0$. As we have seen, $\#E_B(\mathbb{F}_p)[2] = 4$, so we can write $X^3 + BX^2 - X = X(X - b_1)(X - b_2)$ with $b_1, b_2 \in \mathbb{F}_p$. We may assume that b_1 is a square. Then $b_2 = -1/b_1$ is a non-square. Since $E(\mathbb{F}_p) \cong \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z}$ for integers $n_1|n_2$ and $\#E(\mathbb{F}_p) = p + 1 \equiv 0 \pmod 8$, E, E_A and E_B have points of order 4. If $P = (x_0, y_0) \in E_B(\mathbb{F}_p)$ is a point of order 4, then $x(2P) = (\frac{x_0^2+1}{2y_0})^2 \neq 0$ is a square in $\mathbb{F}_p$, so $2P = (b_1, 0)$ and $u^2b_1 + r = x(2\phi(P)) \neq 0$ is a square. If $\phi((b_2, 0))$ was $(0,0)$, then we would have $u^2b_2 + r = 0$ and $r = x(\phi((0,0))) = -1/(u^2b_1 + r)$, so $b_2 = 1/((u^2b_1 + r)u^2)$ is a square, which is impossible. It follows from $r = 0$ that $u^4 = 1$, so $u^2 = 1$ and $A = B$.

This proposition guarantees the valid public keys consisting of coefficients $A \in \mathbb{F}_p$ and efficient public-key validation. So the coefficients can serve as shared secrets instead of taking j-invariants, which frees the computation from j-invariants to equations of elliptic curves. Wouter Castryck and Thomas Decru[20] also propose the same conclusion at the same time. But we emphasize that the different proof. Our proof is a $\mathcal{O}_K$-version of the Proposition 8 in [9], while their proof uses the bijection between the Montgomery curves on floor and Montgomery$^-$ curves on surface.

3.2 Formulae for 2-isogenies

Proposition 1 gives the formulae of isogenies of odd degree for elliptic curves in the form of $y^2 = x^3 + Ax^2 - x$. For the 2-isogenies corresponding to the ideal classes $[(2, \frac{\pi \pm 1}{2})]$, we have following Lemma which is proved in [20, Lemma 5]. We highlight that for a A square in $\mathbb{F}_p$ we denote by $\sqrt{A}$ the unique square root which is again a square, which can be computed through $A^{\frac{p+1}{4}}$, and the non-square can be gotten by changing the sign.

Lemma 1. *Let $p \equiv 7 \pmod 8$ and consider $E_A : y^2 = x^3 + Ax^2 - x \in \mathcal{ELL}(\mathcal{O}_K)$. Then*

$$E_A[(2, \frac{\pi - 1}{2})] = \langle (\frac{-A + \sqrt{A^2+4}}{2}, 0) \rangle, \quad E_A[(2, \frac{\pi + 1}{2})] = \langle (\frac{-A - \sqrt{A^2+4}}{2}, 0) \rangle.$$

Castryck and Decru [20] used the rescalings to Montgomery curves and computed 2-isogenies between them. In this section, we study different ways of computing 2-isogenies: direct formulae, resacling to Edwards curves and using the map between the special points. Finally we compare the computational cost of them.

Direct Derivation Now we give direct formulae for the 2-isogenies, corresponding to the above ideal classes of norm 2, between the curves of the form $y^2 = x^3 + Ax^2 - x$.

Proposition 3. *Let $E_A : y^2 = x^3 + Ax^2 - x$ be an elliptic curves over a field of characteristic $p \equiv 7 \pmod 8$. Let $G^- = E_A[(2, \frac{\pi-1}{2})]$ and $G^+ = E_A[(2, \frac{\pi+1}{2})]$, ϕ^+ and ϕ^- be the separable isogenies such that $\ker(\phi^+) = G^+$ and $\ker(\phi^-) = G^-$. Then, up to composition with a isomorphism, there are curves $E_{A'} : y^2 = x^3 + A'x^2 - x$ and $E_{A''} : y^2 = x^3 + A''x^2 - x$ such that*

$$\phi^- : E_A \to E_{A'} : (x, y) \mapsto (\frac{x^2 + \frac{x}{M}}{2\sqrt{\Theta N}(x - M)} - \frac{\sqrt{\Theta N}}{2}, \frac{x^2 - 2Mx - 1}{(4\Theta N)^{\frac{3}{4}}(x - M)^2} y),$$

where $M = \frac{-A+\sqrt{A^2+4}}{2}$, $N = \sqrt{M^2+1}$, $\Theta = -2N + 2M + \frac{1}{M}$ and $A' = \frac{\Theta - 4N}{2\sqrt{\Theta N}}$. And

$$\phi^+ : E_A \to E_{A''} : (x, y) \mapsto (\frac{x^2 + \frac{x}{\tilde{M}}}{2\sqrt{\tilde{\Theta}\tilde{N}}(x - \tilde{M})} - \frac{\sqrt{\tilde{\Theta}\tilde{N}}}{2}, \frac{x^2 - 2\tilde{M}x - 1}{(4\tilde{\Theta}\tilde{N})^{\frac{3}{4}}(x - \tilde{M})^2} y),$$

where $\tilde{M} = \frac{-A-\sqrt{A^2+4}}{2}$, $\tilde{N} = \sqrt{\tilde{M}^2+1}$, $\tilde{\Theta} = -(2\tilde{N} + 2\tilde{M} + \frac{1}{\tilde{M}})$ and $A'' = \frac{4\tilde{N} - \tilde{\Theta}}{2\sqrt{\tilde{\Theta}\tilde{N}}}$.

Proof. Note that $[(2, \frac{\pi-1}{2})]^{-1} = [(2, \frac{\pi+1}{2})]$ and quadratic twisting swaps the roles of $(\frac{-A+\sqrt{A^2+4}}{2}, 0)$ and $(\frac{-A-\sqrt{A^2+4}}{2}, 0)$, so we can simply flip the sign of A and focus on the isogeny with kernel $E_A[(2, \frac{\pi-1}{2})]$.

Let $M = \frac{-A+\sqrt{A^2+4}}{2}$, it can be easily verified that the isogeny φ^- with kernel $\langle(M,0)\rangle$ of degree 2 can be written as

$$\varphi^- : E_A \to E' : (x,y) \mapsto (\frac{x^2+\frac{x}{M}}{x-M}, y\frac{x^2-2Mx-1}{(x-M)^2}),$$

where E' is of the form $y^2 = x^3 + (-4M - \frac{2}{M})x^2 + \frac{1}{M^2}x$. To put everything back to the curve of the form $y^2 = x^3 + A'x^2 - x$, we now give the isomorphism from elliptic curves E' to elliptic curves $E_{A'} : y^2 = x^3 + A'x^2 - x$:

$$\omega^- : E' \to E_{A'} : (x,y) \mapsto (\frac{1}{2\sqrt{\Theta\sqrt{M^2+1}}}x - \sqrt{\frac{\Theta}{4\sqrt{M^2+1}}}, (\frac{1}{4\Theta\sqrt{M^2+1}})^{\frac{3}{4}}y),$$

where $\Theta = -2\sqrt{M^2+1} + 2M + \frac{1}{M}$ and $A' = \frac{\Theta - 4\sqrt{M^2+1}}{2\sqrt{\Theta\sqrt{M^2+1}}}$. So $\phi^- = \omega^- \circ \varphi^-$ can be written as

$$\phi^- : E_A \to E_{A'} : (x,y) \mapsto (\frac{x^2+\frac{x}{M}}{2\sqrt{\Theta N}(x-M)} - \sqrt{\frac{\Theta}{4N}}, \frac{x^2-2Mx-1}{(4\Theta N)^{\frac{3}{4}}(x-M)^2}y),$$

where $N = \sqrt{M^2+1}$, $\Theta = -2N + 2M + \frac{1}{M}$ and $A' = \frac{\Theta-4N}{2\sqrt{\Theta N}}$. Then ϕ^+ can be easily derived using the quadratic twist and hence the two assertions are proved.

The implementation only uses the coefficients of the elliptic curves, so we conclude Proposition 3 and get the following lemma. To reduce the computational cost in each loop, knowing the initial value of A, we can make some precomputation to simplify the resulting coefficients.

Lemma 2. *Let $A \in \mathbb{F}_p$ such that $E_A : y^2 = x^3 + Ax^2 - x \in \mathcal{ELL}(\mathcal{O}_K)$. We define*

$$A' = \frac{-6N + 2M + \frac{1}{M}}{2\sqrt{(-2N + 2M + \frac{1}{M})N}}, \quad A'' = \frac{6\tilde{N} + 2\tilde{M} + \frac{1}{\tilde{M}}}{2\sqrt{-(2\tilde{N} + 2\tilde{M} + \frac{1}{\tilde{M}})\tilde{N}}}$$

where $M = \frac{-A+\sqrt{A^2+4}}{2}$, $\tilde{M} = \frac{-A-\sqrt{A^2+4}}{2}$, $N = \sqrt{M^2+1}$ and $\tilde{N} = \sqrt{\tilde{M}^2+1}$. Then

$$[(2, \frac{\pi-1}{2})]E_A = E_{A'}, \quad [(2, \frac{\pi+1}{2})]E_A = E_{A''}.$$

We can work with the XZ-only projective Montgomery coordinates and the projective parameters $(A:1) = (a:c)$ as in [25] to get further speed-up.

Rescaling to Edwards Curves Apart from the direct formula, we also try the rescaling to Edwards curves. First we give the 2-isogeny withe kernel $\langle(M,0)\rangle$ between the X coordinate of $Y^2 = X^3 + AX^2 - X$ and the y coordinate of

$ax^2 + y^2 = 1 + dx^2y^2$ which will be used to compute the first 2-isogeny and the final rescaling.

$$X = \frac{uy + \frac{1}{u}}{y - 1}, \quad y = \frac{X + \frac{1}{u}}{X - u},$$

where u is the X coordinate of the point of order 4 in $E : Y^2 = X^3 + AX^2 - X$ satisfying $u^2 - 2Mu - 1 = 0$ and $u^2 = -\sqrt{\frac{d}{a}}$. And then we give the 2-isogeny with kernel $\langle(0, -1)\rangle$ between Edwards curves which will be used from the second to $|e_i|$-th 2-isogeny in the loop.

Proposition 4. *Let $E_{a,d} : ax^2 + y^2 = 1 + dx^2y^2$ be an elliptic curves over a field. Let $G = \langle(0, -1)\rangle$ and ϕ be the separable isogenies such that* $\ker(\phi) = G$. *Then, up to composition with a isomorphism, there are curves $E_{a'} : a'x'^2 + y'^2 = 1 + x'^2y'^2$ such that*

$$\phi : E_{a,d} \to E_{a'} : (x, y) \mapsto (\alpha xy, \beta\frac{y^2 - B_1}{y^2 - B_2}),$$

where $\alpha = \frac{\sqrt{a}}{B_1}$, $\beta = -\frac{B_2}{B_1}$, $a' = \beta^2$. The values of B_1, B_2 can be solved through $B_1 + B_2 = \frac{2a}{d}$ and $B_1B_2 = \frac{a}{d}$.

Proof. Write $x' = \alpha xy$ and $y' = \beta\frac{y^2 - B_1}{y^2 - B_2}$ with $B_1 + B_2 = \frac{2a}{d} = 2B_1B_2$. Substituting them to the equation of elliptic curves $a'x'^2 + y'^2 = 1 + x'^2y'^2$, we can get

$$\begin{cases} a' = \beta^2, \\ B_1^2\beta^2 = B_2^2, \\ 2\alpha^2\beta^2(B_2 - B_1) = (\beta^2 - 1)d, \cdot \\ \beta\dfrac{1 - B_1}{1 - B_2} = 1. \end{cases}$$

So $\alpha = \frac{\sqrt{a}}{B_1}$, $\beta = -\frac{B_2}{B_1}$, $a' = \beta^2$ with $B_1 + B_2 = \frac{2a}{d}$ and $B_1B_2 = \frac{a}{d}$.

Map the Point of Special Order Apart from the direct derivation of the isogenies, the correspondence between the points of special orders are always used to obtain the isogenies. Now to get the specific 2-isogenies between elliptic curves of the form $y^2 = x^3 + Ax^2 - x$, we used the ∞ and the points of order 2 and 4. Since we only need the coefficients of the resulting curves, we now give the resulting coefficients directly.

Proposition 5. *Let $A \in \mathbb{F}_p$ such that $E_A : y^2 = x^3 + Ax^2 - x \in \mathcal{ELL}(\mathcal{O}_K)$. Let $M = \frac{-A+\sqrt{A^2+4}}{2}$, $\overline{M} = \frac{A+\sqrt{A^2+4}}{2}$. Define*

$$A' = \frac{1}{b} - b \quad \textit{and} \quad A'' = -(\frac{1}{\overline{b}} - \overline{b})$$

where $b = -2(M+\sqrt{1+M^2})\sqrt{M}\sqrt{\sqrt{1+M^2}}$ *and* $\overline{b} = -2(\overline{M}+\sqrt{1+\overline{M}^2})\sqrt{\overline{M}}\sqrt{\sqrt{1+\overline{M}^2}}$. *Then*

$$[(2, \frac{\pi-1}{2})]E_A = E_{A'} \quad \textit{and} \quad [(2, \frac{\pi+1}{2})]E_A = E_{A''}$$

Proof. Write $E_A : y^2 = x(x-M)(x-\tilde{M})$ where $M = \frac{-A+\sqrt{A^2+4}}{2}$ is square. Let $P_0(x_0, y_0)$ be the point of order 4 in E_A satisfying that $x_0^2 - 2Mx_0 - 1 = 0$. Assume that the points of order 2 in $E_{A'} : Y^2 = X^3 + A'X^2 - X$ are $(0,0)$, $(b_1, 0)$ and $(b_2, 0)$, so

$$A' = -(b_1+b_2), \quad b_1 = -\frac{1}{b_2}.$$

Then we can write the x coordinate map of the 2-isogeny between E_A and $E_{A'}$ as $X = \frac{\alpha M(x+\frac{1}{x_0})^2}{x-M}$, which maps ∞ and $(M,0)$ to ∞, $(0,0)$ and $(-A-M, 0)$ to $(b_1, 0)$, (x_0, y_0) and $(x_0, -y_0)$ to $(b_2, 0)$, $(-\frac{1}{x_0}, \frac{y_0}{x_0^2})$ and $(-\frac{1}{x_0}, -\frac{y_0}{x_0^2})$ to $(0,0)$. So

$$\begin{cases} \alpha^2 = \dfrac{x_0^4}{x_0^4-1} \quad \text{where} \quad x_0^4 - 1 = 4x_0^2 M(x_0 - M), \\ b_1 = \dfrac{-\alpha}{x_0^2}, \quad b_2 = \dfrac{x_0^2}{-\alpha}. \end{cases}.$$

We must ensure that $x_0 - a$ is a square, so $x_0 = M + \sqrt{M^2+1}$ and finally we can obtain $b_2 = -2(M+\sqrt{1+M^2})\sqrt{M}\sqrt{\sqrt{1+M^2}}$ and $A' = -(b_2 - \frac{1}{b_2})$. The proof of the 2-isogenies with kernel $\langle(\frac{-A-\sqrt{A^2+4}}{2}, 0)\rangle$ is omitted here because it can be easily obtained by changing the sign and using the quadratic twist.

Comparation Finally we compare the computational cost of the 2-isogeny corresponding to $[(2, \frac{\pi-1}{2})]$ in Table 1.

Table 1. Compare the Computational Cost

Methods	Rescaling	Rescaling Cost	Each Loop
To Mon. [20]	Yes	F2: 3S+4s+3F+2M+8A FR: 2S+1s+3F+1M+5A	1S+1s+3A+2M
Direct [Pro.3]	No	-	3S+2s+6A+5M+3F
Edw. [Pro.4]	Yes	F2: 1S+1s+1F+2M+3A FR: 2S+1s+1F+3M+3A	1S+1s+3A+2M+1F
Points [Pro.5]	No	-	4S+2s+5A+3M+2F

We use many abbreviations for the concision. The “Rescaling” represents whether rescalings are needed, the “Rescaling Cost” (resp. the “Each Loop”) is the cost of the rescaling process (resp. the cost of each loop to compute $|e_i|$ isogenies of degree l_i). “F2” and “FR” are the cost of the first 2-isogeny and that of the final rescaling respectively. And “S”,“s”,“F”,“M” and “A” represent “Square root”, “Square”, “Fraction”,“Multiplication” and “Addition” respectively.

4 Some Improvements to CSURF

We improve the implementation of CSURF from two way. One is offering a new ideal representation and gaining a speed-up of about 6.02%, the other is changing the direction of the loop and also gaining a speed-up of about 28.69%

4.1 Collisions in CSURF and A New Ideal Representation

In CSIDH, Castryck W. et al assumed the surjectivity of the group homomorphism

$$\mathbb{Z}^n \to \mathrm{cl}(\mathcal{O}), \quad (e_1, \cdots, e_n) \mapsto \prod_{i=1}^{n} [\mathfrak{l}]_i^{e_i}$$

and the uniformity of resulting distribution $\prod_{i=1}^{n} [\mathfrak{l}]_i^{e_i}$, with $\mathcal{O} = \mathbb{Z}[\pi]$. However, Hiroshi Onuki and Tsuyoshi Takagi [11] found that $(e_1, \cdots, e_n)$ and $(e_1 + 3, \cdots, e_n + 3)$ represented the same ideal class in CSIDH-512. But the collisions don't exist in $\mathrm{cl}(\mathcal{O}_K)$ when $p \equiv 7(\mathrm{mod}\ 8)$. So in CSURF [20], the authors chose a finite field $\mathbb{F}_p$ with $p = 4 \cdot 2 \cdot 3 \cdot (3 \cdot \ldots \cdot 389) - 1$ and a near-optimal set $I = [-137, 137] \times [-4, 4]^3 \times [-5, 5]^{46} \times [-4, 4]^{25}$ to sample exponent vectors, which can avoid the collisions in [11]. By assuming the surjectivity and the uniformity, they claimed that the near-optimal interval I resulted in $2^{255.995}$ distinct secret vectors. Now we give another kind of collisions in CSURF.

We consider a more general case than CSURF and describe the notation first. Let $p = 4 \cdot 2 \cdot l_1^{r_1} \ldots l_n^{r_n} - 1$ be a prime, where l_i are distinct odd primes and r_i are positive integers. The imaginary quadratic field $K = Q(\pi)$ with Frobenius map π has maximal order $\mathcal{O}_K = \mathbb{Z}[\frac{1+\pi}{2}]$ and equation order $\mathcal{O} = \mathbb{Z}[\pi]$. As in CSURF-512, π has two eigenvalues $\lambda = 1$ and $\mu = -1$ in $\mathbb{Z}/l_i\mathbb{Z}$, so the primes l_i split in $\mathcal{O}$ as $l_i\mathcal{O} = \mathfrak{l}_i \cdot \bar{\mathfrak{l}}_i$ for $i = 1, \cdots, n$, where $\mathfrak{l}_i = l_i\mathcal{O} + (\pi - 1)\mathcal{O}$ and $\bar{\mathfrak{l}}_i = l_i\mathcal{O} + (\pi + 1)\mathcal{O}$. The decomposition also exists in $\mathcal{O}_K$.

We now define ideals of $\mathcal{O}_K$ as $\mathfrak{l}_0 = 2\mathcal{O}_K + \frac{\pi-1}{2}\mathcal{O}_K$, $\bar{\mathfrak{l}}_0 = 2\mathcal{O}_K + \frac{\pi+1}{2}\mathcal{O}_K$.

Proposition 6. *In the general case of CSURF,*

$$\mathfrak{l}_0\mathfrak{l}_1^{r_1} \cdots \mathfrak{l}_n^{r_n} = \frac{\pi - 1}{2}\mathcal{O}_K, \qquad \bar{\mathfrak{l}}_0\bar{\mathfrak{l}}_1^{r_1} \cdots \bar{\mathfrak{l}}_n^{r_n} = \frac{\pi + 1}{2}\mathcal{O}_K.$$

Proof. Note that $\mathfrak{l}_i = \langle l_i, (\pi - 1)\rangle = \langle l_i, \frac{\pi-1}{2}\rangle$, so

$$\begin{aligned}\mathfrak{l}_0\mathfrak{l}_1^{r_1} \cdots \mathfrak{l}_n^{r_n} =& \langle 2, \frac{\pi - 1}{2}\rangle \cdot \langle l_1, \frac{\pi - 1}{2}\rangle^{r_1} \cdot \ldots \cdot \langle l_n, \frac{\pi - 1}{2}\rangle^{r_n} \\ =& \langle 2l_1^{r_1} \cdots l_n^{r_n}, \frac{\pi - 1}{2}\rangle = \langle \frac{1 - \pi^2}{4}, \frac{\pi - 1}{2}\rangle \\ =& \langle \frac{\pi - 1}{2}\rangle.\end{aligned}$$

and $\bar{\mathfrak{l}}_0\bar{\mathfrak{l}}_1^{r_1} \cdots \bar{\mathfrak{l}}_n^{r_n} = \overline{\langle \frac{\pi-1}{2}\rangle} = \langle \frac{\pi+1}{2}\rangle$, from which the statement follows.

The above proposition shows that $\mathfrak{l}_0\mathfrak{l}_1^{r_1}\cdots\mathfrak{l}_n^{r_n}$ is principal ideal, so in CSURF the action of the ideal class corresponding to the vector $(1, 2, 1, \ldots, 1)$ is trivial. This directly implies the following corollary, which shows explicit collisions of the ideal class representation in CSURF.

Corollary 1. *In CSURF, the exponent vectors*

$$(e_0, e_1, e_2, \ldots, e_n) \quad \textit{and} \quad (e_0 + 1, e_1 + 2, e_2 + 1, \ldots, e_n + 1)$$

represent the same ideal class.

In general, one way to avoid the above collisions is to change the interval where we sample the exponents. For CSIDH, Meyer et al.[22] used different intervals for e_i to gain a speed-up. To guarantee the security level and the "almost" surjective and uniform representation, we change the interval and get a new representation which omits $[\mathfrak{l}_{74}]$. The final representation is of the form

$$[\mathfrak{l}_0^{e_0}\mathfrak{l}_1^{e_1}\cdots\mathfrak{l}_{73}^{e_{73}}] \quad \text{for} \quad I' = [-141, 141] \times [-4, 4]^3 \times [-6, 6]^{13} \times [-5, 5]^{33} \times [-4, 4]^{24}.$$

There are $283 \cdot 9^{27} \cdot 13^{13} \cdot 11^{33} \approx 2^{255.999}$ distinct secret vectors in I' which guarantees the 256-bit size class group. The interval from which we sample isogenies of degrees $3, 5$ and 7 is relatively small because of the high failure probability of finding torsion points. Intuitively, we economize on the computation of largest isogeny of degree 389 which will induce a speed-up. To evaluate the performance, we change the the source code of CSURF-512 which can be found at https://github.com/TDecru/CSURF and gain a speed-up of about 6.02%. The estimate is based on 2000 experiments in both settings in the computer algebra system Magma.

4.2 Change the Direction of the Loop

As the original implementation of CSIDH, CSURF goes through the primes in ascending order in its implementation, starting with small degree isogenies. Michael Meyer and Steffen Reith [25] gave some faster ways to implement CSIDH, one of which is changing the direction of the loop. Going through the primes in descending order can eliminate the larger factors of $p+1$ first, and therefore end up with multiplications by significantly smaller factors as we proceed through the loop. To verify the point in CSURF, we change the the source code of CSURF-512 and gain a speed-up of about 28.69% comparing to the original performance. The experiments are also implemented in the computer algebra system Magma.

5 Conclusion

In the article, we consider a new form of supersingular elliptic curves over $\mathbb{F}_p$ with $p \equiv 7 \pmod 8$. We show that the curves are uniquely isomorphic to a curve in the form of $y^2 = x^3 + Ax^2 - x$ if and only if they have endomorphism ring $\mathcal{O}_K$ and hence A can be a unique representation of the $\mathbb{F}_p$- isomorphism classes, which implies they can replace the curves in CSIDH. To prove the unique representation and efficient computation, we give some important lemmas and propositions. To our knowledge, Wouter Castryck and Thomas Decru also use curves of the same form in their protocol CSURF and obtain a speed-up, but we prove the uniqueness of the representative of $\mathbb{F}_p$-isomorphism classes from a different perspective. We also offer some formulae for the 2-isogenies with comparation. Moreover, we show there exists another kind of collisions in the ideal representation in CSURF. And to avoid the collisions, we offer a new representation which enhances the efficiency for about 6.02%. We also try to change the direction of the loop in the implementation of CSURF, which gives a speed-up of about 28.69%.

References

1. P W. Shor Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer[M]. Society for Industrial and Applied Mathematics, 1997.
2. C. Costello, H. Hisil. A Simple and Compact Algorithm for SIDH with Arbitrary Degree Isogenies. Advances in Cryptology-ASIACRYPT2017-23rd International Conference on the Theory and Applications of Cryptology and Information Security.
3. C. Delfs , S D. Galbraith. Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$ [J]. Designs, Codes and Cryptography, 2016, 78(2): 425-440.
4. R. Broker, K. Lauter, A. Sutherland . Modular polynomials via isogeny volcanoes[J]. Mathematics of Computation, 2012, 81(278): 1201-1231.
5. J H. Bruinier, K. Ono , A V. Sutherland. Class polynomials for nonholomorphic modular functions[J]. Journal of Number Theory, 2016, 161: 204-229.
6. L. De Feo, J. Kieffer, B. Smith. Towards Practical Key Exchange from Ordinary Isogeny Graphs. Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security.
7. D. Moody, D. Shumow. Analogues of Vélu's formulas for isogenies on alternate models of elliptic curves. Mathematics of Computation, 2016, 300: 1929–1951.
8. S. Galbraith. Isogeny graphs, algorithms and applications[J].
9. W. Castryck, T. Lange, C. Martindale, L. Panny, J. Renes. CSIDH: An Efficient Post-Quantum Commutative Group Action, Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security.
10. J H. Silverman. The Arithmetic of Elliptic Curves. GTM 106 (1986)[J].
11. H. Onuki, T. Takagi. On collisions related to an ideal class of order 3 in CSIDH. IACR Cryptology ePrint Archive, 2019, 1209.
12. N. Koblitz Elliptic curve cryptosystems[J]. Mathematics of computation, 1987, 48(177):203-209.
13. V S. Miller Use of elliptic curves in cryptography[C] Conference on the theory and application of cryptographic techniques. Springer, 1985: 417-426.
14. J M. Couveignes Hard Homogeneous Spaces[J]. IACR Cryptology ePrint Archive, 2006, 2006: 291.
15. A. Rostovtsev, A. Stolbunov. Public-key cryptosystem based on isogenies. IACR Cryptology ePrint Archive 2006/145.

16. D. Jao, L. De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies[C]. International Workshop on Post-Quantum Cryptography. Springer, Berlin, Heidelberg, 2011: 19-34.
17. G. Kuperberg. A Subexponential-Time Quantum Algorithm for the Dihedral Hidden Subgroup Problem. SIAM J. Comput. 35(1): 170-188, 2005.
18. L. De Feo, J. Kieffer, B. Smith. Towards Practical Key Exchange from Ordinary Isogeny Graphs. Advances in Cryptology - ASIACRYPT 2018 - 24th International Conferenceon the Theory and Application of Cryptology and Information Security.
19. R. Azarderakhsh, M. Campagna, C. Costello, L. De Feo, B. Hess, A. Jalali, D. Jao, B. Koziel, B. LaMacchia, P. Longa, M. Naehrig, J. Renes, V. Soukharev, D. Urbanik. Supersingular Isogeny Key Encapsulation Submission to the NIST¡¯s post-quantum cryptography standardization process, 2017.
20. W. Castryck, T. Decru. CSIDH on the Surface[M]. Post-Quantum Cryptography, 11th International Conference, PQCrypto 2020.
21. W C. Waterhouse. Abelian varieties over finite fields[J]. Annales Scientifiques de l École Normale Supérieure, 1971, 2(4):56-62(7).
22. M. Meyer, F. Campos, S. Reith. On Lions and Elligators: An efficient constant-time implementation of CSIDH. PQCrypto 2019, LNCS 11505, 307-325 (2019).
23. A. Childs, D. Jao, V. Soukharev. Constructing elliptic curve isogenies in quantum subexponential time[J]. Journal of Mathematical Cryptology, 2014, 8(1):1-29.
24. W. Beullens, T. Kleinjung, F. Vercauteren. CSI-FiSh: Efficient Isogeny Based Signatures Through Class Group Computations. Advances in Cryptology-ASIACRYPT 2019-25th International Conferenceon the Theory and Application of Cryptology and Information Security.
25. M. Meyer, S. Reith. A Faster Way to the CSIDH. Progress in Cryptology - INDOCRYPT 2018 - 19th International Conference on Cryptology in India, New Delhi, India, December 9-12, 2018, Proceedings.

A Lemma 3

Montgomery elliptic curves appeal to people by their properties. One can use x throughout and use the Montgomery Ladder to compute $[l]E$ efficiently. The following lemma shows that the specific elliptic curves have similar properties.

Lemma 3. *Let E be an elliptic curve given by an equation $y^2 = x^3 + Ax^2 - x$. $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ are two points on E with $x_1 \neq x_2$ and $x_1x_2 \neq 0$. Then $P_1 + P_2 = (x_3, y_3)$ satisfies*

$$x_3(x_1 - x_2)^2 x_1 x_2 = B(x_1y_2 - x_2y_1)^2, \tag{1}$$

$P_1 - P_2 = (x_4, y_4)$ satisfies

$$x_4(x_1 - x_2)^2 x_1 x_2 = B(x_1y_2 + x_2y_1)^2, \tag{2}$$

and

$$x_3x_4 = \frac{(x_1x_2 + 1)^2}{(x_1 - x_2)^2}.$$

Proof. By the group law on E, we have $x_3 = \frac{(y_1-y_2)^2}{(x_1-x_2)^2} - A - x_1 - x_2$. So

$$\begin{aligned} x_3(x_1-x_2)^2 x_1 x_2 &= (y_1-y_2)^2 x_1 x_2 - (A + x_1 + x_2)(x_1-x_2)^2 x_1 x_2 \\ &= (y_1-y_2)^2 x_1 x_2 - (\frac{y_1^2}{x_1} - \frac{y_2^2}{x_2})(x_1-x_2)x_1x_2 = (x_1y_2 - x_2y_1)^2. \end{aligned}$$

Since $P_1 - P_2 = P_1 + (-P_2)$, the equation (2) can be obtained by replacing x_3 and y_2 in (1) by x_4 and $-y_2$ respectively. Then we have

$$x_3x_4 = \frac{((x_2y_1)^2 - (x_1y_2)^2)^2}{x_1^2x_2^2(x_1-x_2)^4} = \frac{(x_1x_2(1+x_1x_2)(x_1-x_2))^2}{x_1^2x_2^2(x_1-x_2)^4} = \frac{(x_1x_2+1)^2}{(x_1-x_2)^2}.$$

B Proof of Proposition 1

It is similar to the proof of [2, Theorem 1]. Assume that $G = \langle P \rangle$ is a cyclic group of order $2d+1$. Let $x_i = x(iP)$ for $i = 1, \ldots, 2d$. Then by Lemma 3, we see that

$$X = x\prod_{i=1}^{2d} \frac{xx_i+1}{x-x_i} = x\prod_{i=1}^{d}(\frac{xx_i+1}{x-x_i})^2 = x\prod_{i=1}^{d}(\tau_{iP}^* x)\cdot(\tau_{-iP}^* x) = \prod_{Q\in G}\tau_Q^* x,$$

where $\tau_Q : E \to E$ is the translation by $Q \in E$. One can show that $Y = c_0 y X'$ is a multiple of $\sum_{Q\in G}\tau_Q^* y$, so it is also invariant under translation by elements of G. We also see that the only poles of $F(X,Y) = Y^2 - X^3 - AX^2 + X$ are at the points in G. Therefore if $F(X,Y)$ vanishes at ∞, then it is zero.

To show that $F(X,Y)$ vanishes at ∞, we consider its Laurent series expansion. Let $t = \frac{x}{y}$ and $s = \frac{1}{y}$. Then dividing $y^2 = x^3 + ax^2 - x$ by y^3 yields

$$s = t^3 + ast^2 - s^2t.$$

Substituting the value for s into the right hand side, we obtain

$$\begin{aligned} s &= t^3 + a(t^3 + at^2s - ts^2)t^2 - (t^3 + at^2s - ts^2)^2 t \\ &= t^3 + at^5 + (a^2-1)t^7 + (a^3-3a)t^9 + O(t^{11}). \end{aligned}$$

So

$$\begin{aligned} y &= \frac{1}{s} = t^{-3}(1 - at^2 + t^4 + at^6 + O(t^8)), \\ x &= ty = t^{-2}(1 - at^2 + t^4 + at^6 + O(t^8)). \end{aligned}$$

Then we have

$$(\frac{xx_i+1}{x-x_i})^2 = (x_i + (x_i^2+1)t^2 + (a+x_i)(x_i^2+1)t^4 + (x_i^2+1)((a+x_i)^2-1)t^6 + O(t^8))^2,$$

so

$$X = x\prod_{i=1}^{d}(\frac{xx_i+1}{x-x_i})^2 = X_{-2}t^{-2} + (\sigma - a)X_{-2} + X_2t^2 + X_4t^4 + O(t^6), \qquad (3)$$

where

$$X_{-2} = \prod_{i=1}^{d} x_i^2, \sigma = 2\sum_{i=1}^{d}(x_i + \frac{1}{x_i}), X_2 = \frac{1+(3\sigma^2 - 2a\sigma + 4)X_{-2}^2}{5X_{-2}},$$
$$X_4 = \frac{3a + 5\sigma + (-6a^2\sigma + 4a\sigma^2 + 32a + 10\sigma^3)X_{-2}^2}{35X_{-2}}.$$

A calculation shows that

$$F(X,Y) = Y^2 - X^3 - AX^2 + X = k_0t^{-6} + k_1t^{-4} + k_2t^{-2} + k_3 + O(t),$$

where

$$k_0 = (c_0^2 - X_{-2})X_{-2}^2, \quad k_1 = (-2c_0^2a - 3(\sigma - a)X_{-2} - A)X_{-2}^2,$$
$$k_2 = (4c_0^2 + c_0^2a^2 - 2A(\sigma - a) - 3X_2)X_{-2}^2 - 2c_0^2X_{-2}X_2 - 3X_{-2}^3(\sigma - a)^2 + X_{-2},$$
$$k_3 = 4c_0^2X_{-2}(aX_2 - X_4) - 3X_4X_{-2}^2 - 6X_2X_{-2}^2(\sigma - a) - X_{-2}^3(\sigma - a)^3 - 2AX_2X_{-2}$$
$$- AX_{-2}^2(\sigma - a)^2 + X_{-2}(\sigma - a).$$

It is easy to check that $k_1 = k_2 = k_3 = k_4 = 0$ when $c_0^2 = \prod_{i=1}^{d} x_i^2$, and $A = c_0^2(a - 3\sum_{T\in G\setminus\{O_E\}}(x_T - \frac{1}{x_T}))$. Since the curve $E_A : y^2 = x^3 - Ax^2 + x$ is nonsingular, it is an elliptic curve. The rational map ϕ defines a morphism which maps the identity element of E to that of E_A, so it is an isogeny.