CSIDH on Other Form of Elliptic Curves

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 on elliptic curves are of great interest in post-quantum cryptography and appeal to more and more researchers. Many protocols have been proposed such as OIDH, SIDH and CSIDH with their own advantages. We now focus on the CSIDH which based on the Montgomery curves in finite fields $\mathbb{F}_p$ with $p \equiv 3$ (mod8) whose endomorphism ring is $\mathbb{Z}[\sqrt{-p}]$. We try to change the form of elliptic curves into $y^2 = x^3 + Ax^2 - x$ and the characteristic of the prime field into $p \equiv 7$ (mod8) , which induce the endomorphism ring becomes $\mathbb{Z}[\frac{\sqrt{-p}+1}{2}]$. Moreover, many propositionsincluding the formula of isogenies between elliptic curves of the special form and the unique of the representation of $\mathbb{F}_p$-isomorphism class, are given to illustrate the rationality of our idea. An important point to notice that the efficiency can't be reduced because the only difference between our formula of isogenies and that of CSIDH is the sign of some items. Furthermore, we also give a proposition that the protocol based on our case can avoid the collision proposed in [17].

Keywords: CSIDH, Montogomery Curves, Endomorphism Ring, Collision.

1 Introduction

Elliptic curve cryptography (ECC) was proposed [18,19] in 1985. The discrete logarithm problem on elliptic curves (ECDLP) is one of the difficult problems in elliptic curve cryptography. ECC is widely used and studied because of its short key and other advantages before Shor algorithm was proposed in 1994.

The cryptography based on isogeny is first proposed by Couveignes in 1997 [20] and then reproposed by Rostovtsev and Stolbunov independently [23] in 2006, named CRS. All of them focus on the key agreement scheme using the ideal class group of the endomorphism ring of ordinary elliptic curves. However, after the reduction to a hidden shift problem, the scheme have quantum attack of subexponential time. Leaving the quantum attack aside, the efficiency of CRS holds back the development of it. Luca De Feo et al.[26] give a method to accelerate the scheme which requires that the order of the elliptic curves over finite fields must have small primes as factors, which is hard to attain. While the requirement is easy to satisfy on the supersingular elliptic curves over $\mathbb{F}_p$ as long as $p = kl_1 \cdots l_n - 1$ with l_i small primes.

Jao and De Feo take different approach and introduce SIDH[24], relying on the isogenies between supersingular elliptic curves. Because of the non-commutative endomorphism ring, SIDH can thwart the quantum attack by Kuperberg[25]. The practical Supersingular Isogeny Key Encapsulation (SIKE)[27], one of the main contenders in NIST's post-quantum standardization project, is based on SIDH. As a disadvantage, SIDH has active attack [28] when it uses static private keys, which induce the discussion about authenticated key exchange based on SIDH. In addition, it should be combined with a CCA transform such as the FujisakiOkamoto transform to achieve CCA security.

As is mentioned above, the speedup of CRS can perform well on supersingular elliptic curves over $\mathbb{F}_p$. So CSIDH [10] was proposed using supersingular elliptic curves of Montgomery form over finite field $\mathbb{F}_p$ with characteristic $p \equiv 3(\text{mod } 8)$, where "C" stands for commutative. The endomorphism ring of this kind of elliptic curve is $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$. It uses the action of the ideal class group of $\mathbb{F}_p$-isomorphic classes of supersingular elliptic curves $\text{cl}(\mathcal{O}) \times \mathcal{ELL}_p(\mathcal{O}, \pi) \to \mathcal{ELL}_p(\mathcal{O}, \pi)$. There are two advantages of CSIDH. One is that the class group action can be computed efficiently which is the main reason of its high-efficiency. The other is that it provides a non-interactive key exchange with full public-key validation. Although CSIDH has many sparks, there are still many leaks in it. For example, it uses the vector $(e_1, \cdots, e_n) \in \mathbb{Z}^n$ as private key and assume that the group homomorphism $\mathbb{Z}^n \to \text{cl}(\mathcal{O})$ is surjectivity and uniformity. However, Hiroshi Onuki and Tsuyoshi Takagi [17] proposed that $(1, \cdots, 1)$ corresponds to an ideal class of order 3, which means $(e_1, \cdots, e_n)$ and $(e_1 + 3, \cdots, e_n + 3)$ represents the same ideal class in $\text{cl}(\mathcal{O})$.

In this article, we change the characteristic of the prime field into $p \equiv 7(\text{mod } 8)$ and the form of elliptic curves. The form of elliptic curves in CSIDH is $y^2 = x^3 + Ax^2 + x$ called Montgomery curve, while we will use elliptic curves of the form $y^2 = x^3 + Ax^2 - x$. We also prove that the coefficients A can uniquely represent the $\mathbb{F}_p$-isomorphism class as in CSIDH. Moreover, we give the formulas of point-addition on $E : y^2 = x^3 + Ax^2 - x$ and the expressions of isogenies between two elliptic curves $E/K : y^2 = x^3 + Ax^2 - x$ and $E'/K : Y^2 = X^3 + AX^2 - X$. We find that these formulas are similar to those of Montgomery curves only with a few different signs, which inspires us to Implement the change without reduced efficiency. The collisions proposed in [17] are also considered and don't occur in our case.

Organization. The rest of the paper is organized as follows. In Section 2, we recall, besides CSIDH, some basic results on elliptic curves and isogenies over $\mathbb{F}_p$. In Section 3, we propose the computational properties of $E : y^2 = x^3 + Ax^2 - x$ as the analogue of Montgomery curve. In Section 4, we compare the case of $\text{End}_{\mathbb{F}_p} E = \mathcal{O}_K$ with that $\text{End}_{\mathbb{F}_p} E = \mathbb{Z}[\pi]$ in [10], including a important proposition about the relationship between the coefficients and the endomorphism rings and collisions related the ideal class. In Section 5, we give a conclusion.

2 Preliminaries

In this section, we recall some important results on elliptic curves and isogeny. We refer readers to [21,22] for details.

2.1 A New Kind of Projective Coordinates

The projective space is defined to be the set of equivalence classes of (X, Y, Z) with not all of them zero. In general, two triples (X_1, Y_1, Z_1) and (X_2, Y_2, Z_2) are said to be equivalent if there exists constant $k \neq 0$ such that $X_1 = kX_2, Y_1 = kY_2, Z_1 = kZ_2$. Julio López and Ricardo Dahab [16] proposed a new kind of projective coordinates to accelerate the elliptic curve additions over $GF(2^n)$. They redefined such the equivalent relation as the two triples are equivalent if $X_1 = kX_2, Y_1 = k^2Y_2, Z_1 = kZ_2$. In this case, if a point $P = (X, Y, Z)$ with nonzero Z then P can be represented by $(x, y, 1)$, where $x = \frac{X}{Z}$ and $y = \frac{Y}{Z^2}$. And the points for which $Z = 0$ is the point at infinity.

2.2 Some Properties of Elliptic Curve

Proposition 1. *If $\#E(\mathbb{F}_p) = n = 4 \cdot (2k)$ with k an arbitrary constant, then there must be points of order 4 in $E(\mathbb{F}_p)$.*

Proof. According to [11, Theorem 4.1], $E(\mathbb{F}_p) \cong \mathbb{Z}_n$ or $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$ for some integer $n \geq 1$ or for some integer $n_1, n_2 \geq 1$ with n_1 dividing n_2.

If $E(\mathbb{F}_p) \cong \mathbb{Z}_{8k}$, the points of order 4 in $E(\mathbb{F}_p)$ exists obviously. If $E(\mathbb{F}_p) \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$, there are three cases as follows:

- If $2 \nmid n_1$, then $8 \mid n_2$ because $n_1 n_2 = 8k$. So elements of order 4 must exist in $\mathbb{Z}_{n_2}$.
- If $2 \mid n_1$ and $4 \nmid n_1$, then $4 \mid n_2$. So elements of order 4 also exist in $\mathbb{Z}_{n_2}$.
- If $2 \mid n_1$ and $4 \mid n_1$, then elements of order 4 exist in $\mathbb{Z}_{n_1}$.

So if the order of E over $\mathbb{F}_p$ is $4 \cdot (2k)$, then there must be points of order 4 in $E(\mathbb{F}_p)$.

2.3 Isogenies between Supersingular Elliptic Curve over $\mathbb{F}_p$

The l-isogeny only exist when $(\frac{-p}{l}) = 1$, which means $-p$ is a square in $\mathbb{Z}_l$. Otherwise, the characteristic polynomial of Frobenius map $\pi^2 + p = 0 \pmod{l}$ has no root and then there are no edges in the isogeny graph. As suggested by De Feo-Kieffer-Smith in [7], a field of characteristic p, where $p \equiv -1 \pmod{l}$ with l all odd primes up to a bound, should be used to make sure that $l\mathcal{O}$ can decompose into two prime ideals $\mathfrak{l} \cdot \mathfrak{l}^{-1} = (l, \pi - 1) \cdot (l, \pi + 1)$, where π is the Frobenius endomorphism. In this case, the action of the ideal class of $\mathfrak{l}$ (resp. $\mathfrak{l}^{-1}$) can be easily computed by applying Vélu formulae [8] to E (resp. its quadratic twist E^t).

Lemma 1. *Let $E/\mathbb{F}_p$ be an elliptic curve and G a finite $\mathbb{F}_p-$rational subgroup of E. Then there exists a separable isogeny $\phi : E/\mathbb{F}_p \to E_1/\mathbb{F}_p$ defined over $\mathbb{F}_p$ with $E_1 = E\backslash G$ and, up to $\mathbb{F}_p-$isomorphism, the isogeny ϕ and E_1 are unique.*

The $\mathbb{F}_p$-rational isogenies follows the reduction of isogenies over characteristic 0, so we have a correspondence between "$\mathbb{F}_p$-rational l-isogenies between supersingular elliptic curves over $\mathbb{F}_p$" and "l-isogenies between elliptic curves over $\mathbb{C}$ with $\mathrm{End}E \in \{\mathbb{Z}[\sqrt{-p}], \mathcal{O}_K\}$"[3]. So the structure of the supersingular isogeny graph $G(\mathbb{F}_p, l)$, of which the vertices are $\mathbb{F}_p$-isomorphism classes of superingular elliptic curves and the edges are equivalence classes of $\mathbb{F}_p-$rational l-isogenies of these elliptic curves, is similar with the ordinary isogeny graph, a isogeny volcano. The details are summed up in [3, Theorem 2.7]. We now illustrate the case where $p \equiv 3 \pmod 4$ in details and omit the description in other cases.

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

- *If $p \equiv 7 \pmod 8$, there are 2-isogenies connect 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 connect the surface and floor with 1:3 and no horizontal 2-isogenies.*

CSIDH proposed by Castryck W, Lange T, Martindale C, et al. only concentrate on the case where $p \equiv 3 \pmod 8$. They introduce the details about the isogeny graph and give an important proposition about the correspondence between the form of the equation of elliptic curves and their endomorphism ring, along with an example. And we mainly investigate the case $p \equiv 7 \pmod 8$ in later sections. We first compute the $G(\mathbb{F}_{167}, 3)$ using modular polynomials [5,6] to make it visual. There are $h(-167)$=11 supersingular j-invariant in $\mathbb{F}_p$ [3] in total.

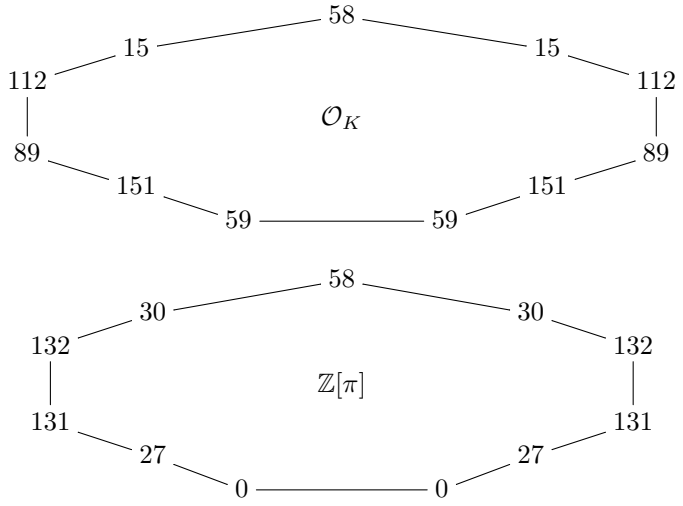

Figure 1. $G(\mathbb{F}_{167}, 3)$. The curves in surface have have endomorphism ring $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{-167}}{2}]$ and those in floor have $\mathbb{Z}[\sqrt{-167}]$ as endomorphism ring.

In the example, $p \equiv -1 (\mathrm{mod}\ 3)$ makes sure that running clockwise through the components corresponds to the repeated action of $[(3, \pi - 1)]$, while running anticlockwise corresponds to that of $[(3, \pi + 1)]$.

3 The Analogue of Montgomery Curve

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

$$x_3(x_1 - x_2)^2 x_1 x_2 = B(x_1 y_2 - x_2 y_1)^2, \tag{1}$$

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

$$x_4(x_1 - x_2)^2 x_1 x_2 = B(x_1 y_2 + x_2 y_1)^2, \tag{2}$$

and

$$x_3 x_4 = \frac{(x_1 x_2 + 1)^2}{(x_1 - x_2)^2}.$$

Proof. There are also similar conclusions in Montgomery Curve and the proofs both begin with the group law

$$x_3 = B\frac{(y_1 - y_2)^2}{(x_1 - x_2)^2} - A - x_1 - x_2.$$

So

$$\begin{aligned} x_3(x_1 - x_2)^2 x_1 x_2 &= B(y_1 - y_2)^2 x_1 x_2 - (A + x_1 + x_2)(x_1 - x_2)^2 x_1 x_2 \\ &= -2Bx_1 x_2 y_1 y_2 + (2A + x_1 + x_2)x_1^2 x_2^2 - x_1 x_2(x_1 + x_2) \\ &= B(x_1 y_2 - x_2 y_1)^2. \end{aligned}$$

Similarly, we can obtain the equation for x_4.

Multiply (1)(2) and use the equation for E to obtain:

$$\begin{aligned} x_3 x_4 &= \frac{B^2(x_2 y_1 - x_1 y_2)^2(x_2 y_1 + x_1 y_2)^2}{x_1^2 x_2^2 (x_1 - x_2)^4} \\ &= \frac{(x_1^2 + Ax_1 - 1)(x_1 x_2^2 + x_2) - (x_2^2 + Ax_2 - 1)(x_1^2 x_2 + x_1)}{(x_1 - x_2)^3} \\ &= \frac{(x_1 x_2 + 1)^2}{(x_1 - x_2)^2}. \end{aligned}$$

Proposition 2. *Let K be a field with* $\mathrm{char(K)} \neq 2$ *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* $a \in K$. ϕ *is a separable isogeny s.t.* $\ker\phi = G$. *Then there is a curve* $E'/K : Y^2 = X^3 + AX^2 - X$ *s.t., up to post-composition by a isomorphism,*

$$\begin{aligned} &\phi : E \to E' \\ &(x, y) \to (f(x), c_0 y f'(x)), \end{aligned}$$

where

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

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

Proof. The proof follows along the proof in [1, Theorem 1]. Write $\phi : (x, y) \to (X, Y)$, where $X = f(x)$ and $Y = c_0 y f'(x)$. X and Y are rational functions on x, y, so $X, Y \in K(E)$, i.e. they are functions on E. And it is obvious that the points in G form the poles of X and Y. Our goal is to show that $F(X, Y) = Y^2 - X^3 - AX^2 + X = 0$.

First we show that if $F(X, Y)$ vanishes at $\mathcal{O}_E$, then $F(X, Y) = 0$. From Lemma 2, we can find that $x_{P+Q}x_{P-Q} = (\frac{x_P x_Q + 1}{x_P - x_Q})^2$ in $E/K : y^2 = x^3 + ax^2 - x$. There is a disjoin union $G = G^+ \cup G^- \cup \{\infty\}$, in other words, for each pair of points $P = (x_P, y_P), P = (x_P, -y_P) \in G$, put exactly one in G^+ and the other in G^-.

$$\begin{aligned} f(x_Q) &= x_Q \prod_{T \in G \setminus \{O_E\}} \frac{x_Q x_T + 1}{x_Q - x_T} = x_Q \prod_{T \in G^+} (\frac{x_Q x_T + 1}{x_Q - x_T})^2 \\ &= x_Q \prod_{T \in G^+} (x_{Q+T} x_{Q-T}) = \prod_{T \in G} x_{Q+T}. \end{aligned}$$

So X, Y will not change under τ_Q, the translation-by-Q, when $Q \in G$. That means if we can obtain that $F(X, Y)|_{\mathcal{O}_E} = 0$, we will have shown $F(X, Y)|_G = 0$, i.e. $F(X, Y)$ vanishes at all points in G. Along with that the points in G form the poles of X and Y, we can get $F(X, Y)$ has no poles. The only possibility is that $F(X, Y) = 0$.

Now we will show $F(X, Y)$ vanishes at $\mathcal{O}_E$. Let $t = \frac{x}{y}$ be the uniformising parameter at $\mathcal{O}_E$ and $s = \frac{1}{y}$. Then

$$y^2 = x^3 + ax^2 - x \Longrightarrow \frac{1}{y} = \frac{x}{y}^3 + a\frac{x}{y}^2 \cdot \frac{1}{y} - \frac{x}{y} \cdot \frac{1}{y^2} \Longrightarrow s = t^3 + at^2 \cdot s - t \cdot s^2.$$

Substituting the expression of s into to $s = t^3 + at^2 \cdot s - t \cdot s^2$, we will get

$$s = t^3 + at^5 + (a^2 - 1)t^7 + a(a^2 - 3)t^9 + (a^4 - 6a^2 + 2)t^{11} + (a^5 - 10a^3 + 10a)t^{13} + O(t^{15}).$$

Invert it and we will have

$$y = \frac{1}{s} = t^{-3}[1 - at^2 + t^4 + at^6 + (a^2 - 1)t^8 + (a^3 - 3a)t^{10} + O(t^{12})],$$

$$x = ty = t^{-2}[1 - at^2 + t^4 + at^6 + (a^2 - 1)t^8 + (a^3 - 3a)t^{10} + O(t^{12})]. \quad (3)$$

$$\frac{dt}{dx} = -\frac{t^3}{2} - \frac{t^7}{2} - at^9 + O(t^{11}) \quad (4)$$

Suppose $G =< P >$. Write

$$X = f(x) = x \prod_{T \in G \setminus \{O_E\}} \frac{xx_T + 1}{x - x_T} \triangleq x \cdot f_1^2(x) \cdots f_d^2(x), \quad (5)$$

where $f_i(x) = \frac{xx_{[i]P}+1}{x-x_{[i]P}} = x_{[i]P} + (x_{[i]P}^2 + 1) \cdot \frac{1}{x-x_{[i]P}}$. Substitution of (3) gives the expression of f_i^2 in terms of t,

$$\frac{1}{x - x_{[i]P}} = t^2 + (a + x_{[i]P})t^4 + [(a + x_{[i]P})^2 - 1]t^6 + O(t^8).$$

So

$$\begin{aligned} f_i^2(t) = x_{[i]P}^2 + 2x_{[i]P}(x_{[i]P}^2 + 1)t^2 + [(x_{[i]P}^2 + 1)(3x_{[i]P}^2 + 2ax_{[i]P} + 1)]t^4 \\ +2(x_{[i]P}^2 + 1)[2x_{[i]P}^3 + 3ax_{[i]P}^2 + a^2x_{[i]P} + a]t^6 + O(t^8). \end{aligned} \quad (6)$$

Substituting (3) and (6) into (5) yields

$$X(t) = \pi t^{-2} + \pi(\sigma - a) + X_2t^2 + X_4t^4 + O(t^6), \quad (7)$$

where $X_2 = \frac{1+4\pi^2+\sigma\pi^2(3\sigma-2a)}{5\pi}$ and $X_4 = \frac{3a-6a^2\pi^2\sigma+5\sigma+4a\pi^2\sigma^2+32a\pi^2+10\pi^2\sigma^3}{35\pi}$. Now define

$$Y = c_0y(t)\frac{df}{dx} = c_0y(t)\frac{dX}{dt}\frac{dt}{dx}. \quad (8)$$

Substitute (7) anf (8) into $F(X, Y)$ and we can get

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

where

$$\begin{aligned} k_0 &= c_0^2\pi^2 - \pi^3, \\ k_1 &= -2c_0^2\pi^2a - 3\pi^3(\sigma - a) - A\pi^2, \\ k_2 &= 2c_0^2\pi(2\pi - X_2) + c_0^2\pi^2a^2 - 3X_2\pi^2 - 3\pi^3(\sigma - a)^2 - 2A\pi^2(\sigma - a) + \pi, \\ k_3 &= 4c_0^2\pi(aX_2 - X_4) - 3X_4\pi^2 - 6X_2\pi^2(\sigma - a) - \pi^3(\sigma - a)^3 - 2AX_2\pi \\ &\quad - A\pi^2(\sigma - a)^2 + \pi(\sigma - a). \end{aligned}$$

The substitution of values of c_0, A, X_2 and X_4 make the coefficients equal 0. So that $F(X, Y) = O(t)$ with t a uniformizer at $(O)_E$, which means that $F(X, Y)$ vanishes at $\mathcal{O}_E$.

Until now, we have shown that X, Y satisfy the equation of E'. Next woe should prove that ϕ is an isogeny, that is to show ϕ is a morphism and $\phi(\mathcal{O}_E) = \mathcal{O}_{E'}$. Because the expression of ϕ is rational and E is smooth, ϕ is a morphism.

Using the new kind of projective embedding, we can embed $E : y^2 = x^3 + ax^2 - x$ into $Y^2 = X^3Z + aX^2Z^2 - XZ^3$ with infinite point $\mathcal{O}_E = (1, 0, 0)$. And $\phi(X, Y, Z) = (\phi_1(X, Z), \phi_2(X, Y, Z), \phi_3(Z))$ where

$$\phi_1(X) = X \prod_{i=1}^{d} (\frac{Xx_{[i]P} + Z}{X - x_{[i]P}Z})^2$$

$$\phi_2(X, Y, Z) = c_0 Y \prod_{i=1}^{d} (\frac{Xx_{[i]P} + Z}{X - x_{[i]P}Z})^2 [1 - 2X \sum_{i=1}^{d} \frac{x_{[i]P}^2 + 1}{(X - x_{[i]P}Z)(Xx_{[i]P} + Z)}]$$

$$\phi_3(Z) = Z$$

So $\phi(1, 0, 0) = (1, 0, 0)$ which indicates ϕ is an isogeny.

From the Proposition 2 and Lemma 1, 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 [1,2] on Montgomery curves, the differences are only on the signs of items.

From other perspective, 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. Then the same conclusion as the Proposition 2 will be directly induced using [1, Theorem 1].

4 Comparision with CSIDH

4.1 Representing $\mathbb{F}_p$-isomorphism classes

In this section, we compare our case with the case in CSIDH, including the vertices representation and collisions related to the ideal class. First, we describe the notation that will be used later. $h(\mathcal{O})$ (resp. $h(\mathcal{O}_K)$) denotes the class number of $\mathcal{O}$ (resp. $\mathcal{O}_K$), which means $h(\mathcal{O}) = \#\mathrm{cl}(\mathcal{O})$(resp. $h(\mathcal{O}_K) = \#\mathrm{cl}(\mathcal{O}_K)$).

In general, the vertices in isogeny graph represent $\mathbb{F}_p$-isomorphism classes of elliptic curves [9], while a new unique representative for $\mathbb{F}_p$ isomorphism class which may serve as a shared key without j-invariants was proposed by [10]. We give a proposition about the unique representation is also suitable for our case.

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

Proof. The proof refers to the proof of [10, Proposition 8] with many key points different.

First, we prove that supersingular elliptic curves of the form $E_A : y^2 = x^3 + Ax^2 - x$ have endomorphism rings defined over $\mathbb{F}_p$ $\mathrm{End}_{\mathbb{F}_p}(E) = \mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{-p}}{2}]$. By [14, Theorem 3.41], we factor prime ideal (2) in $\mathbb{Z}[\frac{1+\sqrt{-p}}{2}]$ and get that $(2)\mathbb{Z}[\frac{1+\sqrt{-p}}{2}] = (2,\omega)(2,\omega+1)$ with $\omega = \frac{1+\sqrt{-p}}{2}$. So there are three 2-torsion $(0,0), P_1$ and P_2 in $E/\mathbb{F}_p$, with P_1 the kernel of isogeny corresponding to $(2,\omega)$ and P_2 the kernel of isogeny corresponding to $(2,\omega+1)$. Since $\omega(P_1) = 0$ and $(\omega+1)(P_2) = 0$, $P_1 \neq P_2$. Hence E_A has full $\mathbb{F}_p$-rational 2-torsion with $(0,0)$ relevant for the only descending isogeny and P_1, P_2 relevant for the two horizontal isogenies [15]. By Theorem 1, $\mathrm{End}_p(E) = \mathrm{End}_p(E_A) = \mathbb{Z}[\frac{1+\sqrt{-p}}{2}]$.

Now assume that $\mathrm{End}_p(E) = \mathbb{Z}[\frac{1+\sqrt{-p}}{2}]$. Since the ideal-class group $\mathrm{cl}(\mathcal{O})$ acts freely and transitively on $\mathcal{E}ll_p(\mathcal{O},\pi)$, there exist $[\mathfrak{a}] \in \mathrm{cl}(\mathcal{O})$ such that $[\mathfrak{a}]E_0 = E$ with $E_0 : y^2 = x^3 - x$. If the representative $\mathfrak{a}$ of the ideal class has norm coprime to $2p$, then there is a separable $\mathbb{F}_p$-isogeny $\varphi_{\mathfrak{a}} : E_0 \to E$ of odd degree. By Proposition 2, given $\ker\varphi$, we can construct $\psi : E_0 \to E_A : y^2 = x^3 + Ax^2 - x$ defined over $\mathbb{F}_p$ with $\ker\psi$=$\ker\varphi$. Because isogeny is unique up to $\mathbb{F}_p$-isomorphism (Lemma 1), E is $\mathbb{F}_p$-isomorphic to E_A.

Finally, we prove the uniqueness of A. Let $E_A \cong E_B : Y^2 = X^3 + BX^2 + X$. Then by [12, Proposition III.3.1(b)] E_A and E_B are related by a linear change of the form

$$x = u^2X + r, \quad y = u^3Y + su^2X + t,$$

with $u \in \mathbb{F}_p^*$ and $r, s, t \in \mathbb{F}_p$. Substitute them into the equation of E_A and subtract $Y^2 - X^3 + BX^2 + X = 0$, we can obtain

$$\begin{aligned} 0 =&(2stu^2 - 3u^2r^2 - 2Au^2r + u^2 - u^6)X + (s^2u^4 - 3u^4r + Au^4 + u^6B)X^2 \\ &+ 2su^5XY + 2u^3ty + (t^2 - r^3 - Ar^2 + r). \end{aligned}$$

Let ∞ be the point at infinity of E_B, then the basis of $\mathcal{L}(5(\infty))$ is $\{1, X, Y, XY, X^2\}$ by Riemann-Roch Theorem[12, Theorem 5.4]. So the coefficients of the equation all equal zero and yield

$$\begin{cases} 2su^5 = 0 & \Rightarrow s = 0, \\ 2tu^3 = 0 & \Rightarrow t = 0, \\ 2stu^2 - 3u^2y^2 - 2Au^2r + u^2 - u^6 = 0 & \Rightarrow 3r^2 + 2Ar - 1 + u^4 = 0, \\ s^2u^4 - 3u^4r + Au^4 + u^6B = 0 & \Rightarrow 3r - A - Bu^2 = 0, \\ t^2 - r^3 - Ar^2 + r = 0 & \Rightarrow r(Ar + r^2 - 1) = 0. \end{cases}$$

Because E_A has full $\mathbb{F}_p$-rational points of order 2, there are two cases as follows:

- $r = 0 \Rightarrow u^4 = 1$. Because -1 is a nonquadratic residue in $\mathbb{F}_p$ when $p \equiv 3 (\mathrm{mod}\ 4)$, $u^2 = 1$. So $A = B$.
- $r^2 - Ar + 1 = 0 \Rightarrow -(r^2+1) = u^4$. We should judge whether $-(r^2+1)$ is a square in $\mathbb{F}_p$ or not.

$$r^2 + 1 = 1 + \frac{(-A \pm \sqrt{A^2+4})^2}{4} = \frac{(A^2+4)(1 \pm \frac{A}{\sqrt{A^2+4}})}{2}.$$

Because $r^2 - Ar + 1 = 0$ has roots, $\triangle = A^2 + 4$ is square in $\mathbb{F}_p$. And 2 is a square in $\mathbb{F}_p$ when $p \equiv 7 \pmod 8$. So the quadratic character of $1 \pm \frac{A}{\sqrt{A^2+4}}$ equals that of $r^2 + 1$. Writing r_1, r_2 are two roots of $r^2 + Ar - 1 = 0$, i.e. $E_A : y^2 = x(x - r_1)(x - r_2)$, implies $r_1 + r_2 = A$ and $r_1 r_2 = -1$ by Vieta's formulas. So

$$1 \pm \frac{A}{\sqrt{A^2+4}} = \frac{2r_1}{r_1 - r_2} \quad or \quad \frac{-2r_2}{r_1 - r_2}.$$

According to Proposition [1], there exist points of order 4 in $E(\mathbb{F}_p)$ since $\#E(\mathbb{F}_p) = p + 1 = 8k$ for $k \in \mathbb{Z}$. So $-r_1$ and $-r_2$ are both squares or r_1 and $r_1 - r_2$ are both squares or r_2 and $r_2 - r_1$ are both squares in $\mathbb{F}_p$ by [13, Theorem 9]. However, since $-1 = r_1 r_2$ is a nonquadratic residue in $\mathbb{F}_p$, $-r_1$ and $-r_2$ have different quadratic characters. The remaining possibilities are r_1 and $r_1 - r_2$ are both squares or r_2 and $r_2 - r_1$ are both squares, which interprets $1 \pm \frac{A}{\sqrt{A^2+4}}$ is quadratic residue in $\mathbb{F}_p$. Conclude the case, we can get that $-(r^2 + 1)$ is a nonquadratic residue in $\mathbb{F}_p$, which induce $-(r^2 + 1) = u^4$ has no root. So this case should be excluded.

From the discussion about the two cases, we can conclude that $r = s = t = 0$, $u^2 = 1$ and $A = B$. Hence the value of A is unique.

This proposition is a $\mathcal{O}_K$-version of the Proposition 8 in [10], which guarantees the valid public keys consisting of coefficient $A \in \mathbb{F}_p$ and efficient public-key validation. So we can also use the coefficients as public keys in our case.

4.2 Avoiding the collision

As for private keys consisting of an exponent vector $(e_1, \cdots, e_n)$, Castryck W. et al assumed the surjectivity of the group homomorphism $\mathbb{Z}^n \to \mathrm{cl}(\mathcal{O})$ and the uniformity of resulting distribution of $\prod_{i=1}^n \mathfrak{l}_i^{e_i}$. However, Hiroshi Onuki and Tsuyoshi Takagi investigated the correspondence between the vectors and the ideal classes and found that $(e_1, \cdots, e_n)$ and $(e_1 + 3, \cdots, e_n + 3)$ represent the same ideal class. We refer the reader to [17, Theorem 3] for precise details. The following proposition implies the collisions don't exit in $\mathrm{cl}(\mathcal{O}_K)$ when $p \equiv 7 (\mathrm{mod} 8)$.

Compare the exact sequence with $\mathcal{O} = \mathbb{Z}[\pi]$

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

when $p \equiv 3 (\mathrm{mod} 8)$ and $p \equiv 7 (\mathrm{mod} 8)$. Since $\mathcal{O}_K^\times$ and $\mathcal{O}^\times$ are $\{\pm 1\}$ in both cases, the exact sequence becomes

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

where $(\mathcal{O}_K/\mathfrak{f})^\times / (\mathcal{O}/\mathfrak{f})^\times \to \mathrm{cl}(\mathcal{O})$ is a monomorphism and $\mathrm{cl}(\mathcal{O}) \to \mathrm{cl}(\mathcal{O}_K)$ is an epimorphism with $\mathfrak{f}$ the conductor of $\mathcal{O}$.

- When $p \equiv 3 \pmod 8$, $h(\mathcal{O}) = 3h(\mathcal{O}_K)$. Since $\mathfrak{f} = 2\mathcal{O}_K = 2\mathcal{O} + (\pi - 1)\mathcal{O}$, we can obtain that $\mathcal{O}_K/\mathfrak{f} \cong \mathbb{F}_4$ and $\mathcal{O}/\mathfrak{f} \cong \mathbb{F}_2$ as illustrate in [17]. Therefor, $\#(\mathcal{O}_K/\mathfrak{f})^\times/(\mathcal{O}/\mathfrak{f})^\times = 3$ and the map $\mathrm{cl}(\mathcal{O}) \to \mathrm{cl}(\mathcal{O}_K)$ is surjective with three elements in kernel.
- When $p \equiv 7 \pmod 8$, $h(\mathcal{O}) = h(\mathcal{O}_K)$. Since $\mathcal{O}_K/\mathfrak{f} \cong \mathcal{O}/\mathfrak{f} \cong \mathbb{F}_2$, the map $\mathrm{cl}(\mathcal{O}) \to \mathrm{cl}(\mathcal{O}_K)$ is surjective with only one element in kernel. So $[\mathfrak{a}]$ is a principal ideal in $\mathcal{O}$ if and only if it is a principal ideal in $\mathcal{O}_K$.

Proposition 4. *When $p \equiv 7 \pmod 8$ and $\mathfrak{l}_i \in \mathrm{cl}(\mathcal{O}_K)$ with $i = 1, \ldots, n$, the ideal class $\mathfrak{l}_1 \cdots \mathfrak{l}_n$ doesn't have order 3 in $\mathrm{cl}(\mathcal{O}_K)$.*

Proof. We first review the case where $p \equiv 3 \pmod 8$, which means $p = 4l_1 \cdots l_n - 1$. So

$$l_1 \ldots l_n \mathcal{O}_K = \frac{p+1}{4}\mathcal{O}_K = \frac{1+\sqrt{-p}}{2}\frac{1-\sqrt{-p}}{2}\mathcal{O}_K.$$

Writing $l_1 \cdots l_n \mathcal{O}_K = (\mathfrak{l}_1 \cdots \mathfrak{l}_n)(\mathfrak{l}_1^{-1} \cdots \mathfrak{l}_n^{-1})$, we can get $\mathfrak{l}_1 \cdots \mathfrak{l}_n = \frac{1-\sqrt{-p}}{2}\mathcal{O}_K$ and $\mathfrak{l}_1^{-1} \cdots \mathfrak{l}_n^{-1} = \frac{1+\sqrt{-p}}{2}\mathcal{O}_K$. Both of them are principal ideals in $\mathcal{O}_K$.

While $p \equiv 7 \pmod 8$, which means $p = 4 \cdot 2l_1 \cdots l_n - 1$,

$$l_1 \ldots l_n \mathcal{O}_K = \frac{1}{2} \cdot \frac{p+1}{4}\mathcal{O}_K = \frac{1}{2} \cdot \frac{1+\sqrt{-p}}{2}\frac{1-\sqrt{-p}}{2}\mathcal{O}_K.$$

The decomposition of the prime ideal (2) in $\mathcal{O}_K$ is $< 2, \frac{\sqrt{-p}-1}{2} >< 2, \frac{\sqrt{-p}+1}{2} >$. Neither of the factors is a principal ideal, which induce that neither $\mathfrak{l}_1 \cdots \mathfrak{l}_n$ nor $\mathfrak{l}_1^{-1} \cdots \mathfrak{l}_n^{-1}$ is principal. Moreover, writing $[\mathfrak{b}_1] =< 2, \frac{\sqrt{-p}-1}{2} >$ and $[\mathfrak{b}_2] =< 2, \frac{\sqrt{-p}+1}{2} >$, we can achieve that neither $[\mathfrak{b}_1]^3$ nor $[\mathfrak{b}_2]^3$ is principal, which results in neither $\mathfrak{l}_1 \cdots \mathfrak{l}_n$ nor $\mathfrak{l}_1^{-1} \cdots \mathfrak{l}_n^{-1}$ doesn't have order 3 in $\mathrm{cl}(\mathcal{O}_K)$.

The proposition only illustrates the fix collision doesn't exist, but doesn't mean there isn't other kinds of collisions between different private keys, for example $(e_1, \cdots, e_n)$ and $(e_1 + i_1, \cdots, e_n + i_n)$ with $i_1 \neq \cdots \neq i_n$ may represent the same ideal class, which needs more exploration.

5 Conclusion

In the article, we discuss a new form of elliptic curves which have endomorphism ring $\mathcal{O}_K$ in fields of characteristic $p \equiv 7 \pmod 8$ and infer that it can be used in CSIDH with a few improvements. To prove the unique representation of the $\mathbb{F}_p$- isomorphism classes, we give some important lemmas and propositions. And then we describe the differences between our case and CSIDH. Although we use a new form of elliptic curve, there is no need to worry the efficiency because the only difference on the isogenious formula between our form and Montgomery curves is just the sign of item. We may make experiments to verify the opinion in the future. As an advantage, we also prove that there doesn't exist the collision described in [17, Theorem 3]. We infer that our propositions can substitute those of CSIDH.

References

1. Craig Costello and Hüseyin Hisil. A Simple and Compact Algorithm for SIDH with Arbitrary Degree Isogenies. Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security.
2. Renes J. Computing isogenies between Montgomery curves using the action of (0, 0)[C]. International Conference on Post-Quantum Cryptography. Springer, Cham, 2018: 229-247.
3. Delfs C, Galbraith S D. Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$ [J]. Designs, Codes and Cryptography, 2016, 78(2): 425-440.
4. Castryck W, Lange T, Martindale C, et al. CSIDH: an efficient post-quantum commutative group action[C]. International Conference on the Theory and Application of Cryptology and Information Security. Springer, Cham, 2018: 395-427.
5. Brker R, Lauter K, Sutherland A. Modular polynomials via isogeny volcanoes[J]. Mathematics of Computation, 2012, 81(278): 1201-1231.
6. Bruinier J H, Ono K, Sutherland A V. Class polynomials for nonholomorphic modular functions[J]. Journal of Number Theory, 2016, 161: 204-229.
7. Luca De Feo, Jean Kieffer, Benjamin 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, Brisbane, QLD, Australia, December 2-6, 2018, Proceedings, Part III,
8. Dustin Moody, Daniel Shumow. Analogues of Vélu's formulas for isogenies on alternate models of elliptic curves. Mathematics of Computation, 2016, 300: 1929–1951.
9. Galbraith S. Isogeny graphs, algorithms and applications[J].
10. Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, Joost 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, Brisbane, QLD, Australia, December 2-6, 2018, Proceedings, Part III.
11. Washington L C. Elliptic curves: number theory and cryptography[M]. Chapman and Hall/CRC, 2008.
12. Silverman J H. The Arithmetic of Elliptic Curves. GTM 106 (1986)[J].
13. Newman B. Growth of torsion of elliptic curves with full 2-torsion over quadratic cyclotomic fields[J]. Journal of Number Theory, 2017, 173: 570-601.
14. Milne J S. Algebraic number theory[M]. JS Milne, 2008.
15. Luca De Feo. Mathematics of Isogeny Based Cryptography. CoRR, abs/1711.04062, 2017.
16. López J, Dahab R. Improved algorithms for elliptic curve arithmetic in $GF(2^n)$[C]. International Workshop on Selected Areas in Cryptography. Springer, Berlin, Heidelberg, 1998: 201-212.
17. Hiroshi Onuki, Tsuyoshi Takagi. On collisions related to an ideal class of order 3 in CSIDH. IACR Cryptology ePrint Archive, 2019, 1209.
18. Koblitz N. Elliptic curve cryptosystems[J]. Mathematics of computation, 1987, 48(177):203-209.
19. Miller V S. Use of elliptic curves in cryptography[C] Conference on the theory and application of cryptographic techniques. Springer, 1985: 417-426.

20. Couveignes J M. Hard Homogeneous Spaces[J]. IACR Cryptology ePrint Archive, 2006, 2006: 291.
21. De Feo L. Mathematics of isogeny based cryptography[J]. arXiv preprint arXiv:1711.04062, 2017.
22. J. H. Silverman. The Arithmetic of Elliptic Curves, volume 106. Springer Science & Business Media, 2009.
23. A. Rostovtsev, A. Stolbunov. Public-key cryptosystem based on isogenies. IACR Cryptology ePrint Archive 2006/145.
24. Jao D, De Feo L. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies[C]. International Workshop on Post-Quantum Cryptography. Springer, Berlin, Heidelberg, 2011: 19-34.
25. Greg Kuperberg. A Subexponential-Time Quantum Algorithm for the Dihedral Hidden Subgroup Problem. SIAM J. Comput., 35(1):170188, 2005.
26. Luca De Feo, Jean Kieffer, Benjamin 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.
27. 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 NISTs post-quantum cryptography standardization process, 2017.
28. Steven D. Galbraith, Christophe Petit, Barak Shani, Yan Bo Ti. On the security of supersingular isogeny cryptosystems. ASIACRYPT 2016, Springer, 2016, pp. 6391.