AUT Journal of Mathematics and Computing

AUT J. Math. Comput., 7(1) (2026) 19-31
https://doi.org/10.22060/AJMC.2024.23144.1245

Original Article

Supersingular elliptic curves, binary quadratic forms and isogenies

Leila Goodarzi, Hassan Daghigh*

Faculty of Mathematical Sciences, University of Kashan, Kashan, Iran

ABSTRACT: Many of researchers have explored the construction of isogenies between particular elliptic curves, largely due to the extensive range of their practical applications. In this paper, we use the relationship between supersingular elliptic curves over $\mathbb{F}_p$ and binary quadratic forms to generate isogenies connecting supersingular elliptic curves over $\mathbb{F}_p$.

Review History:

Received:30 May 2024
Revised:09 October 2024
Accepted:16 October 2024
Available Online:01 January 2026

Keywords:

Elliptic curve
Isogeny
Supersingular
Binary quadratic forms

MSC (2020):

14H52; 94A60

1. Introduction

Encryption based on isogenies is a relatively new research area in cryptography that utilizes the mathematical concept of isogeny to create secure encryption protocols. An isogeny refers to a rational map between two elliptic curves, which simultaneously functions as a group homomorphism.

The strength of isogeny-based encryption lies in its conjectured resistance against quantum attacks [23]. Unlike conventional encryption algorithms, which are based on the hardness of factoring large numbers or computing discrete logarithms, isogeny-based encryption relies on the hardness of computing isogenies between elliptic curves. This makes it a promising candidate for post-quantum cryptography. However, it is still an emerging field and further research needs to be conducted to fully understand its security properties and potential applications.

Isogenies play a crucial role in cryptography. Isogeny-based schemes are considered as one of the strongest post-quantum schemes [15]. They are used in introducing hash functions [6], as well as in studying the structure of elliptic curve cryptosystems. The Supersingular Isogeny Diffie-Hellman (SIDH) protocol was introduced in 2014 [9]. Although this protocol was broken [4], the attack did not solve the isogeny problem.

*Corresponding author.
E-mail addresses: lgoudarzi22@gmail.com (L. Goodarzi), hassan@kashanu.ac.ir (H. Daghigh)

Within the framework of the well-known paper, SQISign: Compact Post-Quantum Signatures from Quaternions and Isogenies, a new class of signatures has been proposed that relies on isogeny graphs of a certain class of elliptic curves, yielding a compact size of signatures and keys. The authors demonstrate that their scheme is intended for, and indeed achieves NIST's postquantum security level, with much smaller signature and public key sizes than most current post-quantum signature schemes [10]. These applications underscore the applicability of isogenies in the current cryptographic applications.

In 1941, Deuring established the existence of a bijective correspondence between the categories of maximal orders in certain quaternion algebras and the categories of supersingular elliptic curves $E/\mathbb{F}_{p^2}$ [12]. In 1982, Ibukiyama introduced two types of maximal orders and proved that these orders correspond to classes of supersingular elliptic curves defined over $\mathbb{F}_p$ [14]. In 2018, the CSIDH (Commutative Supersingular Isogeny Diffie-Hellman) cryptographic protocol was proposed by Castryck et al. The CSIDH protocol utilizes the group action of an ideal class group on the set of supersingular elliptic curves defined over $\mathbb{F}_p$ [5].

In 2022, in paper [22], Xiao et al. created a correspondence between $\mathbb{F}_p$-isomorphism classes of supersingular elliptic curves and primitive reduced binary quadratic forms. They demonstrate the compatibility between the composition of isogenies of supersingular elliptic curves and the composition of quadratic forms. Additionally, the authors claimed that the security of CSIDH relies on the difficulty of computing the correspondence. However, the specific details of how to utilize this correspondence are not explicitly addressed, and no algorithm for the correspondence is provided.

In the following, we first review this correspondence and then examine the method of constructing this correspondence. In section two, we will review the basic definitions of elliptic curves and binary quadratic forms. In section three, we will explore the correspondence between elliptic curves and binary quadratic forms, and additionally, we will present an algorithm for its implementation. Then, we provide an example of this correspondence. In section four, we discuss constructing an isogeny between two given isogenous curves using the correspondence.

In this paper, we seek answers to the following questions:
How can we determine the degree of isogeny between two isogenous elliptic curves using this correspondence?
How can we construct the isogeny using this correspondence?

2. Preliminaries

In this section, we begin by providing a concise overview of the fundamental definitions related to elliptic curves. For more details, one can see [17, 21]. Then, we review the basic concepts of binary quadratic forms. For more information, one can see [2, 8].

2.1. Elliptic Curves

Let $\mathbb{F}_q$ be the finite field of order q where q is a power of a prime number p and $p \neq 2, 3$. Let $\overline{\mathbb{F}}_q = \bigcup_{n\geq 1} \mathbb{F}_{q^n}$ be the algebraic closure of $\mathbb{F}_q$. An elliptic curve over $\mathbb{F}_q$ is defined by an equation $E : y^2 = x^3 + ax + b$, where $a, b \in \mathbb{F}_q$ and $4a^3 + 27b^2 \neq 0$. The set of $\mathbb{F}_q$-rational points on E is denoted by

$$E(\mathbb{F}_q) = \{(x, y) \in \mathbb{F}_q^2 : y^2 = x^3 + ax + b\} \cup \{O\}.$$

Where, O represents the point at infinity on the curve, that is, $O = (0 : 1 : 0)$ in the projective form $Y^2Z = X^3 + aXZ^2 + bZ^3$. The set $E(\mathbb{F}_q)$ forms an abelian group under the law of chord and tangent with O as the identity element. The j-invariant of the curve E is defined as $j(E) = 1728 \cdot \frac{4a^3}{4a^3+27b^2}$.

The collection of n-torsion points on E, where $n > 1$, is defined as

$$E[n] := \{P \in E(\overline{\mathbb{F}}_q) : nP = O\}.$$

If $gcd(p, n) = 1$, then $E[n]$ is the direct product of two cyclic groups of order n, hence $\#E[n] = n^2$.

Let E and E' be two elliptic curves over $\mathbb{F}_q$. An isogeny from E to E' is a morphism $\varphi : E \longrightarrow E'$ such that $\varphi(O) = O'$. For every isogeny $\varphi : E \longrightarrow E'$, there exist explicit rational functions $R_1(x, y)$ and $R_2(x, y)$ such that $\varphi(x, y) = (R_1(x, y), R_2(x, y))$.

Let $p > 3$ be a prime number. Consider a non-square element $\mu \in \mathbb{F}_p$. For an elliptic curve $E : y^2 = x^3 + ax + b$, we define its quadratic twist as follows:

$$\text{If } j(E) \neq 1728, \quad \overline{E} : y^2 = x^3 + a\mu^2 x + b\mu^3.$$

$$\text{If } j(E) = 1728, \quad \overline{E} : y^2 = x^3 + a\mu x.$$

Quadratic twists have the same j-invariant but are not isomorphic over $\mathbb{F}_p$.

Theorem 2.1. *(Hasse's Theorem) Let $E/\mathbb{F}_q$ be an elliptic curve. Then,*

$$|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}.$$

Proof. See page 138, Theorem 1.1 of [17]. □

Theorem 2.2. *(Tate's Theorem) Let $E/\mathbb{F}_q$ and $E'/\mathbb{F}_q$ be two elliptic curves. Then, E and E' are $\mathbb{F}_q$-isogenous if and only if $\#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q)$.*

Proof. See Theorem C4.1 of [18]. □

Let $\varphi : E_1 \longrightarrow E_2$ be a non-constant morphism. Then, φ is a surjective map. If φ is a non-constant morphism, we define the degree of φ to be,

$$\deg(\varphi) := [\overline{K}(E_1) : \varphi^*(\overline{K}(E_2))],$$

where $\overline{K}(E_1)$ is the field of functions on E_1 over $\overline{K}$, and

$$\varphi^* : \overline{K}(E_2) \longrightarrow \overline{K}(E_1),$$

is defined by $\varphi^*(f) = f \circ \varphi$. The degree of the constant map is considered 0.

We call an isogeny φ separable if the extension $\overline{K}(E_1)/\varphi^*(\overline{K}(E_2))$ is separable. If this extension is inseparable, we call φ inseparable.

We denote the set of isogenies from E_1 to E_2 by $Hom(E_1, E_2)$. For two isogenies φ and ψ, $\varphi + \psi$ is also an isogeny defined by $(\varphi + \psi)(P) = \varphi(P) + \psi(P)$. Therefore, $Hom(E_1, E_2)$ forms a group.

Let $\varphi : E_1 \longrightarrow E_2$ be a non-zero separable isomorphism. Then,

$$\deg(\varphi) = \# \ker(\varphi).$$

Example 2.1. *Let $char(K) = p$ and E/K be an elliptic curve. Then, for every $n \in \mathbb{Z}$, the multiplication map by n, denoted by $[n]_E$, on the elliptic curve E, is defined as follows:*

$$[n]_E P = nP.$$

The multiplication map by n is an isogeny, and the kernel of $[n]$ equals $E[n]$.

Theorem 2.3. *Let E/K be an elliptic curve and $m \in \mathbb{Z}$ with $m \neq 0$.*

a) $\deg[m] = m^2$.

b) *If $char(K) = 0$ or $char(K) = p > 0$ and $p \nmid m$, then*

$$E[m] = \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}.$$

c) *If $char(K) = p > 0$, then one of the following two cases holds:*
   1. *For every $e = 1, 2, 3, \ldots,$ $E[p^e] = \{O\}$.*
   2. *For every $e = 1, 2, 3, \ldots,$ $E[p^e] = \frac{\mathbb{Z}}{p^e\mathbb{Z}}$.*

According to Theorem 2.3, the group $E[p]$ has either one or p elements. If $E[p]$ has one element, E is called supersingular. If $E[p]$ has p elements, E is called ordinary.

An endomorphism of E is an isogeny from E to itself. We denote the set of endomorphisms of an elliptic curve E as $End(E)$. End(E) is a ring under point-wise addition and composition of functions.

Let E be an elliptic curve defined over a field K with characteristic p, and let $q = p^n$. Let $E^{(q)}$ be the elliptic curve obtained by raising the coefficients of the Weierstrass equation of E to the q-th power. The Frobenius morphism π_q is defined as:

$$\begin{aligned} \pi_q : E &\longrightarrow E^{(q)} \\ (x, y) &\mapsto (x^q, y^q) \end{aligned}$$

If E is defined over $\mathbb{F}_q$, then we have $E^{(q)} = E$, and thus, π_q is an endomorphism of E called the Frobenius endomorphism. Then, $P \in E(\mathbb{F}_q)$ if and only if $\pi_q(P) = P$.

Remark 2.4. *Let K be a field of characteristic zero. The map*

$$\begin{aligned}[\cdot] : \mathbb{Z} &\longrightarrow End(E)\\ n &\longrightarrow [n]\end{aligned}$$

is one-to-one. If $End(E)$ is strictly larger than $\mathbb{Z}$, we say E has complex multiplication. If K is a finite field, then $End(E)$ is always larger than $\mathbb{Z}$ because it contains the Frobenius map. (Remark 3.4.3, page 69 of [17])

A quaternion algebra over $\mathbb{Q}$ is a four-dimensional central simple algebra over $\mathbb{Q}$. It is generated by elements $1, i, j, ij$ with $i^2 = a, j^2 = b, ij = -ji$, where a and b are elements of $\mathbb{Q}^\times$. For a quaternion algebra to be ramified at a prime p, it means that when you localize the algebra at p, it does not split into the matrix algebra $M_2(\mathbb{Q}_p)$, but remains a division algebra. Similarly, being ramified at infinity means that when you extend scalars to the real numbers $\mathbb{R}$, the algebra does not split into $M_2(\mathbb{R})$ but remains a division algebra. An order in a quaternion algebra over $\mathbb{Q}$ is a subring that has a basis over $\mathbb{Z}$. An order in a quadratic imaginary field is a subring that contains the integers and is finitely generated over $\mathbb{Z}$.

If E is an elliptic curve over a field K, then $End(E)$ is isomorphic to either $\mathbb{Z}$, an order in a quadratic imaginary field, or an order in a quaternion algebra over $\mathbb{Q}$.

The endomorphism ring $End(E)$ of a supersingular elliptic curve E over $\mathbb{F}_{p^2}$ is isomorphic to a maximal order in the quaternion algebra $B_{p,\infty}$ (a quaternion algebra defined over $\mathbb{Q}$ and ramified at p and ∞).

Let $E/\mathbb{F}_q$ be an elliptic curve. Then, we call $t = q + 1 - \#E(\mathbb{F}_q)$ the trace of the Frobenius map π_q. The Frobenius map satisfies the equation $x^2 - tx + q = 0$.

Let $p \geq 5$ and $E/\mathbb{F}_p$ be an elliptic curve over a finite field $\mathbb{F}_p$ and $t = p + 1 - \#E(\mathbb{F}_p)$. Then E is supersingular if and only if $t = 0$.

Corollary 2.5. *Let $E/\mathbb{F}_p$ be a supersingular elliptic curve over a finite field $\mathbb{F}_p$. Then the Frobenius map satisfies the equation $x^2 + p = 0$.*

2.2. Binary Quadratic Forms

Definition 2.6. *A binary quadratic form f is a function defined as $f(x, y) = ax^2 + bxy + cy^2$, where $a, b, c \in \mathbb{Z}$. Usually, f is represented as (a, b, c). We say f is primitive if $gcd(a, b, c) = 1$. The discriminant of f is defined as $D = b^2 - 4ac$. The discriminant can always be written as $D = dk^2$, where d is square-free. If $k = 1$, then D is called a fundamental discriminant.*

Definition 2.7. *Two forms $f(x, y)$ and $g(x, y)$, are called equivalent if there exist integers p, q, r, s such that*

$$f(x, y) = g(px + qy, rx + sy), \quad ps - qr = 1.$$

Then, we write $f \sim g$.

Definition 2.8. *A quadratic form (a, b, c) is called reduced if it satisfies the following conditions:*

1. $-a < b \leq a$,
2. $a \leq c$,
3. *If $a = c$, then $b \geq 0$.*

Definition 2.9. *An integer $n \in \mathbb{Z}$ is represented by the quadratic form $f(x, y) = ax^2 + bxy + cy^2$ if there exist $x_n, y_n \in \mathbb{Z}$ such that $f(x_n, y_n) = n$. If $gcd(x_n, y_n) = 1$, we say n is represented specially.*

Definition 2.10. *For any quadratic form $f(x, y) = ax^2 + bxy + cy^2$, we can observe that:*

$$4af(x, y) = (2ax + by)^2 - Dy^2.$$

If $D > 0$, then f represents both positive and negative integers and is called an indefinite form.
If $D < 0$ and $a > 0$, the form f represents only positive integers and is called a positive definite form.
If $D < 0$ and $a < 0$, the form f represents only negative integers and is called a negative definite form.

Note that all forms we consider are positive definite.

Theorem 2.11. *Every primitive positive definite form is equivalent to a unique reduced form.*

Proof. See page 145, Proposition 2.8 of [8]. □

Definition 2.12. *Consider two quadratic forms $f(x,y) = ax^2 + bxy + cy^2$ and $g(x,y) = a'x^2 + b'xy + c'y^2$ with discriminant D, such that $gcd(a, a', \frac{b+b'}{2}) = 1$. Then, the Dirichlet composition of f and g is defined as:*

$$h(x,y) = aa'x^2 + b''xy + \frac{b''^2 - D}{4aa'}y^2,$$

where

$$b'' \equiv b \pmod{2a}, \quad b'' \equiv b' \pmod{2a'}, \quad b''^2 \equiv D \pmod{4aa'}.$$

Example 2.2. *Consider the quadratic forms $f = (14, 10, 21)$ and $g = (9, 2, 30)$ of discriminant $D = -1076$, then $b'' = 38$ and the composition of f and g is $f * g = h = (126, 38, 5)$.*

For the Dirichlet composition of two reduced forms, we can consider the coefficients of x^2 in two forms to be coprime. By transforming the forms into equivalent forms, we can consider such a composition. Then, we call this composition the normalized Dirichlet composition. According to Proposition 8.3 in [8], the Dirichlet composition of two primitive positive definite quadratic forms is also a positive definite form.

Theorem 2.13. *We define the class group of forms with discriminant D as:*

$$Cl(D) = \{ \text{ Classes of equivalent forms with discriminant } D \ \}.$$

Then, $Cl(D)$ forms an Abelian group under the operation of the normalized Dirichlet composition.

The identity element of the class group is the form $(1, \alpha, (\frac{\alpha - D}{4})); D \equiv \alpha \pmod 4$, which is called the principal form. Additionally, the inverse of the reduced form (a, b, c) equals $(a, -b, c)$.

Proof. See page 51 of [8]. □

Definition 2.14. *Let $\mathcal{O}$ be an imaginary quadratic order in $\mathbb{Q}(\sqrt{D})$. Every ideal in $\mathcal{O}$ has the form $< \alpha, \beta >= \mathbb{Z}\alpha + \mathbb{Z}\beta$, where $\alpha, \beta \in \mathcal{O}$.*

The following proposition concerns the relationship between the ideal class group $Cl(\mathcal{O})$ and the class group of quadratic forms $Cl(D)$.

Proposition 2.15. *Let $\mathcal{O}$ be an order with discriminant D in an imaginary quadratic field K. Then*

a) *If $f(x,y) = ax^2 + bxy + cy^2$ is a primitive positive definite quadratic form with discriminant D, then $< a, (-b + \sqrt{D})/2 >$ is an ideal of $\mathcal{O}$.*

b) *The map that sends $f(x,y)$ to $< a, (-b + \sqrt{D})/2 >$ induces a well-defined injective map $\tau : Cl(D) \longrightarrow Cl(\mathcal{O})$.*

c) *A positive integer m is represented by a form $f(x,y)$ if and only if m is precisely the norm of an ideal $\mathbf{a}$ in the corresponding ideal class in $Cl(\mathcal{O})$.*

d) *Let $\mathbf{a} = [\alpha, \beta]$ be a proper $\mathcal{O}$-ideal such that $Im(\beta/\alpha) > 0$. Then, $f(x,y) = \frac{N(\alpha x - \beta y)}{N(\mathbf{a})}$ is a positive definite quadratic form with discriminant D. In fact, the map that sends $\mathbf{a}$ to f is the inverse of τ in part b.*

Proof. See page 227, Theorem 5.2.4 of [7] and section 7.B of [8]. □

3. The correspondence

In this section, we first introduce the correspondence between supersingular elliptic curves over $\mathbb{F}_p$ and binary quadratic forms based on the article [22]. Then, we present an algorithm for implementing this correspondence.

In the following, we represent $End_{\mathbb{F}_p}(E)$ as $End(E)$. If E is a supersingular elliptic curve defined over $\mathbb{F}_p$, then as stated in 2.5, there exists an element α in $End(E)$ with minimal polynomial is $x^2 + p$. Alternatively, $End(E)$ includes a subring $\mathbb{Z}[\sqrt{-p}]$. Ibukiyama has presented a comprehensive explanation of all maximal orders $\mathcal{O}$ in $B_{p,\infty}$ that include a root of $x^2 + p = 0$.

Let q be a prime integer such that

$$q \equiv 3 \pmod 8 \quad \text{and} \quad \left(\frac{p}{q}\right) = -1. \tag{1}$$

Then, $B_{p,\infty}$ can be written as: $B_{p,\infty} = \mathbb{Q} + \alpha\mathbb{Q} + \beta\mathbb{Q} + \alpha\beta\mathbb{Q}$, where $\alpha^2 = -p$, $\beta^2 = -q$, and $\alpha\beta = -\beta\alpha$.
Let r be an integer such that

$$r^2 + p \equiv 0 \pmod q, \tag{2}$$

We define:

$$\mathcal{O}(q,r) = \mathbb{Z} + \frac{1+\beta}{2}\mathbb{Z} + \frac{\alpha(1+\beta)}{2}\mathbb{Z} + \frac{(r+\alpha)\beta}{q}\mathbb{Z}.$$

If $p \equiv 3 \pmod 4$, we choose an integer r' such that

$$r'^2 + p \equiv 0 \pmod{4q}, \tag{3}$$

and define:

$$\mathcal{O}'(q,r) = \mathbb{Z} + \frac{1+\alpha}{2}\mathbb{Z} + \beta\mathbb{Z} + \frac{(r'+\alpha)\beta}{2q}\mathbb{Z}.$$

$\mathcal{O}(q,r)$ (resp.$\mathcal{O}'(q,r)$) is independent of choices of r (resp. r') up to isomorphism [14]. So we can show $\mathcal{O}(q,r)$ (resp.$\mathcal{O}'(q,r)$) with $\mathcal{O}(q)$ (resp. $\mathcal{O}'(q)$). $\mathcal{O}(q)$ (resp. $\mathcal{O}'(q)$) is a maximal order of $B_{p,\infty}$. For a supersingular elliptic curve E defined over $\mathbb{F}_p$, the endomorphism ring $End(E)$ is isomorphic to $\mathcal{O}(q)$ or $\mathcal{O}'(q)$, by selecting an appropriate value for q.

Theorem 3.1. *Let $j \in \mathbb{F}_p$ be a j-invariant of a supersingular elliptic curve E_j defined over $\mathbb{F}_p$. Then:*

1. $End(E_0) \cong \mathcal{O}(3)$.
2. $End(E_{1728}) \cong \mathcal{O}'(1)$.
3. *If $j \neq 0, 1728$,*
   (a) *If $\frac{1+\pi}{2} \in End(E_j)$, then $End(E_j) \cong \mathcal{O}'(q)$.*
   (b) *If $\frac{1+\pi}{2} \notin End(E_j)$, then $End(E_j) \cong \mathcal{O}(q)$.*

Proof. See [14]. □

Theorem 3.2. *Let p be a prime number and E be a supersingular elliptic curve over $\mathbb{F}_p$,*

a) *Let $p \equiv 3 \pmod 4$. If $End(E) \cong \mathcal{O}'(q)$, then there exists a reduced quadratic form f with discriminant $-p$ such that f and f^{-1} both represent q.*

b) *If $End(E) \cong \mathcal{O}(q)$, then there exists a reduced quadratic form f with discriminant $-16p$ such that f and f^{-1} both represent q.*

Proof. According to [22],

a) If the integer r satisfies 2, then $f = (q, r, \dfrac{r^2+p}{4q})$.

b) If the integer r' satisfies 3, then $f = (q, 4r, \dfrac{4r^2+4p}{q})$. □

Definition 3.3. *Let $\mathcal{O}$ be an imaginary quadratic order with discriminant D. Then the Hilbert class polynomial H_D is defined as:*

$$H_D(x) := \prod_{j(E) \in Ell_O(\mathbb{C})} (x - j(E)),$$

Where:

$$Ell_{\mathcal{O}}(\mathbb{C}) = \{j(E) | End(E/\mathbb{C}) \cong \mathcal{O}\}.$$

Theorem 3.4. *Suppose p is a prime number and $f = (a,b,c)$ is a reduced quadratic form representing the prime number q satisfying (1).*

a) *If the discriminant of f is $-p$, then there is a unique j-invariant $j \in \mathbb{F}_p$ such that $End(E(j)) \cong \mathcal{O}'(q)$. Furthermore, f^{-1} is also associated with the same j-invariant.*

b) *If the discriminant of f is $-16p$, then there is a unique supersingular j-invariant in $\mathbb{F}_p$ such that $End(E(j)) \cong \mathcal{O}(q)$. Additionally, f^{-1} is also associated with the same j-invariant.*

Proof. a) According to Lemma 1 of [22], the desired j-invariant is the common root of the Hilbert class polynomials $H_{-4a}(x)$ and $H_{-4c}(x)$.
b) According to Lemma 2 of [22], the desired j-invariant is the common root of the Hilbert class polynomials $H_{-a}(x)$ and $H_{-c}(x)$. □

Consider the isogenies of supersingular elliptic curves over the field $\mathbb{F}_p$. As discussed in Section 2.2 of [16], these isogenies correspond to ideals in imaginary quadratic orders. Therefore, based on 2.15, these isogenies can be shown by quadratic forms.

Let E_1 and E_2 be elliptic curves defined over $\mathbb{F}_p$. Also, assume that $\phi : E_1 \longrightarrow E_2$ is an isogeny defined over $\mathbb{F}_p$. Since any isogeny can be expressed as a composition of prime degree isogenies, we only consider isogenies of prime degree l. If we take l_i as a prime factor of $\#E(\mathbb{F}_p)$, then $E(\mathbb{F}_p)$ has subgroups of order l_i. Therefore, using the Velu formula, we can construct isogenies of degree l_i [20].

Theorem 3.5. *Let $E_1/\mathbb{F}_p$ and $E_2/\mathbb{F}_p$ be supersingular elliptic curves, and let $\varphi : E_1 \longrightarrow E_2$ be an l-isogeny where $l \neq 2$ is a prime number. Then, one of the following conditions holds:*
1) $End(E_1) \cong End(E_2) \cong \mathcal{O}(q)$,
2) $End(E_1) \cong End(E_2) \cong \mathcal{O}'(q)$.

Proof. See section 4.2 of [22] □

Remark 3.6. *For $(\frac{-p}{l}) = 1$, there exist two l-isogenies $\phi : E_1 \longrightarrow E_2$ and $\phi' : E_1 \longrightarrow E_2'$ defined over $\mathbb{F}_p$. If the isogeny ϕ corresponds to g_l, then the isogeny ϕ' corresponds to the form g_l^{-1}.*

Theorem 3.7. *Consider the assumptions of the Theorem 3.5.*
In case 1, if the elliptic curve E_1 corresponds to the quadratic form $(q_1, 4r_1, \frac{4r_1^2+4p}{q_1})$, then there are two l-isogenies from E_1 which one corresponds to the quadratic form $g_l = (l, 2b, \frac{b^2+p}{l})^2$, where $b^2 \equiv -4p \pmod{l}$, and the elliptic curve E_2 corresponds to the form $(q_1, 4r_1, \frac{4r_1^2+4p}{q_1}) \cdot g_l$, and the other one corresponds to the quadratic form g_l^{-1} and the elliptic curve E_2 corresponds to the form $(q_1, 4r_1, \frac{4r_1^2+4p}{q_1}) \cdot g_l{}^{-1}$.
In case 2, if the elliptic curve E_1 corresponds to the quadratic form $(q_1, r_1, \frac{r_1^2+p}{4q_1})$, then there are two l-isogenies from E_1 which one corresponds to the quadratic form $g_l = (l, b, \frac{b^2+p}{4l})^2$, where $b^2 \equiv -p \pmod{4l}$, and the elliptic curve E_2 corresponds to the form $(q_1, r_1, \frac{r_1^2+p}{4q_1}) \cdot g_l$, and the other one corresponds to the quadratic form g_l^{-1} and the elliptic curve E_2 corresponds to the form $(q_1, r_1, \frac{r_1^2+p}{4q_1}) \cdot g_l{}^{-1}$.

Proof. See Theorems 4 and 5 of [22]. □

Corollary 3.8. *According to Theorem 3.7, we have a correspondence between elliptic curves and quadratic forms: $\varphi \longleftrightarrow g_l$, where $\varphi : E_1 \longrightarrow E_2$, $E_1 \longleftrightarrow f_1, E_2 \longleftrightarrow f_1 g_l$.*

In this algorithm, first we find the supersingular j-invariants corresponding to suitable q values. Then, we associate elliptic curves with corresponding quadratic forms.

Algorithm 1

Step 1. Find all the supersingular j-invariants in the field $\mathbb{F}_p$.
Step 2. Choose a random prime number q that satisfies the following two conditions:

$$(\frac{-p}{q}) = 1, \qquad q \equiv 3 \pmod{8}.$$

Step 3. Find the j-invariant $j_q \in \mathbb{F}_p$ such that $End(E_{j_q}) \cong \mathcal{O}(q)$.
Step 3.1. Find r such that $r^2 \equiv -p \pmod{q}$.
Step 3.2. Suppose $R(D)$ is the set of roots of the Hilbert class polynomial H_D in $\mathbb{F}_p$.
Calculate $j_q = R(-q) \cap R\left(-\frac{4r^2+4p}{q}\right)$.
Step 3′.1. Find r' such that $r'^2 \equiv -p \pmod{4q}$.
Step 3′.2. Calculate $j_q = R(-4q) \cap R\left(-\frac{r'^2+p}{q}\right)$.
Step 4. Compute the reduced quadratic form $f = (q, 4r, \frac{4r^2+4p}{q})$ corresponding to j_q obtained in Step 3.
Step 4′. Compute the reduced quadratic form $f = (q, r', \frac{r'^2+p}{4q})$ corresponding to j_q obtained in Step 3′.

The following lemma shows that in the above algorithm steps 3.1 and 3′.1 are quite easy to be done.

Lemma 3.9. *Let q be a prime number and $q \equiv 3 \pmod 4$. Suppose a is such that $(\frac{a}{q}) = 1$. Then $b \equiv a^{\frac{q+1}{4}}$ is a square root of a modulo q, i.e., $b^2 \equiv a \pmod q$.*

Proof. By Fermat's little theorem, we have $a^{q-1} \equiv 1 \pmod q$. Thus, $a^{\frac{q-1}{2}} \equiv \pm 1 \pmod q$. By Gauss's lemma, if $(\frac{a}{q}) = 1$, then $a^{\frac{q-1}{2}} \equiv 1 \pmod q$. Therefore, $a^{\frac{q+1}{2}} \equiv a \pmod q$. Hence, $b^2 \equiv (a^{\frac{q+1}{4}})^2 \equiv a^{\frac{q+1}{2}} \equiv a \pmod q$. □

Corollary 3.10. *If p and q are prime numbers and q satisfies (1), then the congruence $r^2 \equiv -p \pmod q$ has a solution $r \equiv (-p)^{\frac{q+1}{4}} \pmod q$.*

The following lemma guarantees the fast succes in step 2 in the above algorithm.

Lemma 3.11. *If p is a prime number and $E/\mathbb{F}_p$ is a supersingular elliptic curve, then it is easy to find a suitable q satisfying (1) such that $End(E) \cong \mathcal{O}(q)$.*

Proof. According to the properties of the Legendre symbol, we have $(\frac{-p}{q}) = (\frac{-1}{q})(\frac{p}{q}) = -(\frac{p}{q})$. If $p \equiv 1 \pmod 4$, by the law of quadratic reciprocity, we have $(\frac{q}{p}) = (\frac{p}{q}) = -1$. The value of $(\frac{q}{p})$ depends only on the residue of q modulo p. These residues are half square and half non-square modulo p. To have $(\frac{q}{p}) = -1$, it is sufficient for the residue of q modulo p to be one of the non-residues. Combining this condition with $q \equiv 3 \pmod 8$, according to the Chinese remainder theorem, we can find a value of q modulo $8p$. Among the residues modulo $8p$, $\frac{p-1}{2}$ satisfies both conditions in (1). By Dirichlet's theorem, the density of prime numbers in these classes is $\frac{\frac{p-1}{2}}{4p}$. Therefore, by choosing an arbitrary prime number q, the probability that q satisfies both conditions in (1) is greater than $\frac{1}{9}$. Hence, it is possible to find an appropriate q in a short time, as the success probability in choosing q for m times is given by $1 - (\frac{8}{9})^m$. □

For the step 3.2 and $3'.2$, the book [3] covers various computational techniques for finding roots of Hilbert class polynomials.

4. Creating isogeny using correspondence:

In Chapter 25 of Mathematics of Public Key Cryptography, Steven Galbraith thoroughly exposes the algorithms for the computation of isogenies between elliptic curves [13]. For instance, one of the methods uses the j-invariant, which is not clean due to presenting a problem on the determination of the degree of the isogeny. This approach is more effective in fields of certain characteristics. Besides, the SEA (Schoof-Elkies-Atkin) algorithm is also described, which is one of the most effective algorithms but also the most computationally intensive one since it involves computations with modular polynomials over large prime fields. The efficiency of this method, however, may be limited in certain situations and conseqeuently, other methods like, p-adic algorithms may also be used in such cases. Other algorithms like Stark's, Galbraith's and Galbraith-Hess-Smart (GHS) algorithms were also mentioned which their complexity arises from the need to compute large polynomials. These algorithms may not perform well in special cases, such as when the characteristic of the field is small.

In this section first we find an l-isogenous curve with a fixed given curve E using correspondence. We also present an algorithm to find an isogeny between two given isogenous supersingular elliptic curves, $E_1/\mathbb{F}_p$ and $E_2/\mathbb{F}_p$.

Theorem 4.1. *Let $p > 3$ be a prime and $E/\mathbb{F}_p$ be a supersingular elliptic curve, then $End(E)$ is an order in $K = \mathbb{Q}(\sqrt{-p})$. Let $\mathcal{O}_K$ be the ring of integers of K, then:*

$$\mathbb{Z}[\sqrt{-p}] \subseteq End(E) \subseteq \mathcal{O}_K,$$

We consider two situations:
If $p \equiv 1 \pmod 4$, we have $End(E) = \mathbb{Z}[\sqrt{-p}]$.
If $p \equiv 3 \pmod 4$, then $End(E)$ is $\mathbb{Z}[\sqrt{-p}]$ or $\mathbb{Z}[\dfrac{1+\sqrt{-p}}{2}]$.

Proof. See Theorem 2.1 of [11]. □

Lemma 4.2. *Let $p > 5$ be a prime number, and $E/\mathbb{F}_p$ be a supersingular elliptic curve. Then $E[2] \subset E(\mathbb{F}_p)$ if and only if*

$$End(E) = \mathbb{Z}[\frac{1+\sqrt{-p}}{2}].$$

Proof. See Lemma 3.6 of [1]. □

Mapping the elliptic curve E to a quadratic form

How to map an elliptic curve $E/\mathbb{F}_p$ to an equivalent quadratic form?

Assume that $E/\mathbb{F}_p$ is a supersingular elliptic curve. If $p \equiv 1 \pmod 4 \Longrightarrow -p \equiv 3 \pmod 4 \Longrightarrow \frac{1+\sqrt{-p}}{2} \notin End(E)$, according to 3.1, $End(E) \cong \mathcal{O}(q)$, but if $p \equiv 3 \pmod 4$, then End(E) is $\mathcal{O}(q)$ or $\mathcal{O}'(q)$. To see if $End(E)$ is $\mathcal{O}(q)$ or $\mathcal{O}'(q)$, based on Lemma 4.2, we must check if $E[2]$ is contained in $E(\mathbb{F}_p)$.

Now, we find a suitable q such that satisfies (1).

If $End(E) \cong \mathcal{O}(q)$, we choose a suitable r satisfying $r^2 \equiv -p \pmod q$, and we set:

$$f = (q, 4r, \frac{4r^2 + 4p}{q}),$$

Then, we calculate the reduced form of f.

If $End(E) \cong \mathcal{O}'(q)$, we choose a suitable r' satisfying $r'^2 \equiv -p \pmod{4q}$, and we set:

$$f = (q, r', \frac{r'^2 + p}{4q}),$$

Then, we calculate the reduced form of f.

Computing the isogeny in the quadratic form representation

We calculate isogeny in the quadratic form representation. For a prime number l, let g_l be the quadratic form corresponding to the l-isogeny.

If $End(E) \cong \mathcal{O}(q)$, then

$$g_l = (l, 2b, \frac{b^2 + 4p}{l})^2,$$

where b is a solution of $b^2 \equiv -4p \pmod l$.

If $End(E) \cong \mathcal{O}'(q)$, then

$$g_l = (l, b, \frac{b^2 + p}{4l})^2,$$

where b is a solution of $b^2 \equiv -p \pmod{4l}$.

Mapping the resulting quadratic form back to an elliptic curve

We calculate the quadratic form $f_1 = g_l f$. According to 3.8, the quadratic form f_1 corresponds to an elliptic curve E_1, which is l-isogenous to E.

To transform the quadratic form f_1 into an elliptic curve, we first consider the reduced quadratic form (a, b, c). Then,

If $p \equiv 3 \pmod 4$, according to Theorem 3.4, the Hilbert polynomials $H_{-4a}(x)$ and $H_{-4c}(x)$ have a common root j in $\mathbb{F}_p$, and the elliptic curve $E(j)$ corresponds to the form f_1.

If $p \equiv 1 \pmod 4$, according to 3.4, the Hilbert polynomials $H_{-a}(x)$ and $H_{-c}(x)$ have a common root j in $\mathbb{F}_p$, and $E(j)$ is the elliptic curve corresponding to the form f_1.

Example 4.1. *Let $p = 101$. Then, the set of supersingular j-invariants is:*

$$\{0, 3, 21, 57, 59, 64, 66\}.$$

Note that if we consider elliptic curves defined over the field $\mathbb{F}_p$, considering quadratic twists of the curves up to isomorphism, we will have twice this set of curves. The curves and their corresponding forms are as follows:

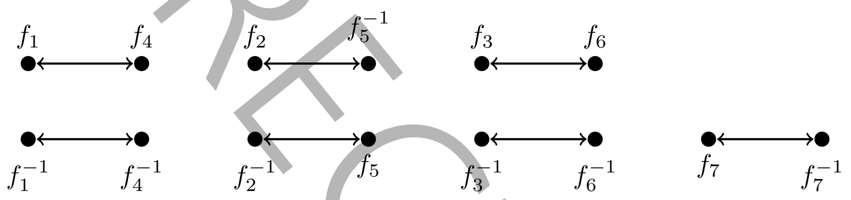
$E_1 : y^2 = x^3 + 1$	$f_1 = (3, -2, 135),$	$\tilde{E_1} : y^2 = x^3 + 63$	$f_1^{-1} = (3, 2, 135)$
$E_2 : y^2 = x^3 + 12x + 65$	$f_2 = (11, -10, 39),$	$\tilde{E_2} : y^2 = x^3 + 50x + 27$	$f_2^{-1} = (11, 10, 39)$
$E_3 : y^2 = x^3 + 89x + 20$	$f_3 = (7, 6, 59),$	$\tilde{E_3} : y^2 = x^3 + 98x + 48$	$f_3^{-1} = (7, -6, 59)$
$E_4 : y^2 = x^3 + 18x + 54$	$f_4 = (12, 8, 35),$	$\tilde{E_4} : y^2 = x^3 + 41x + 75$	$f_4^{-1} = (12, -8, 35)$
$E_5 : y^2 = x^3 + 25x + 8$	$f_5 = (15, -2, 27),$	$\tilde{E_5} : y^2 = x^3 + 33x + 16$	$f_5^{-1} = (15, 2, 27)$
$E_6 : y^2 = x^3 + 72x + 20$	$f_6 = (15, -8, 28),$	$\tilde{E_6} : y^2 = x^3 + 28x + 67$	$f_6^{-1} = (15, 8, 28)$
$E_7 : y^2 = x^3 + 77x + 42$	$f_7 = (8, 4, 51),$	$\tilde{E_7} : y^2 = x^3 + 81x + 14$	$f_7^{-1} = (8, -4, 51)$

Example 4.2. *Consider the forms corresponding to the elliptic curves in Example 4.1. To obtain the graphs of l-isogenies, we combine the forms corresponding to the l-isogenies with corresponding forms to the elliptic curves.*

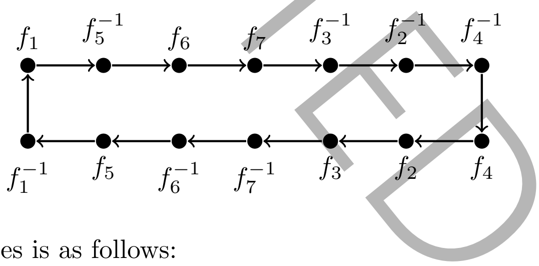
Table 1:

Corresponding forms with elliptic curves	$*g_2 = (4,0,101)$	$*g_3 = (9,2,45)$	$*g_{17} = (13,-10,33)$
$f_1 = (3,2,135)$	$(12,8,35)$	$(15,-2,27)$	$(11,10,39)$
$f_1^{-1} = (3,-2,135)$	$(12,-8,35)$	$(3,2,135)$	$(12,8,35)$
$f_2 = (11,10,39)$	$(15,-2,27)$	$(7,6,59)$	$(15,8,28)$
$f_2^{-1} = (11,-10,39)$	$(15,2,27)$	$(12,-8,35)$	$(3,-2,135)$
$f_3 = (7,6,59)$	$(15,8,28)$	$(8,-4,51)$	$(8,4,51)$
$f_3^{-1} = (7,-6,59)$	$(15,-8,28)$	$(11,-10,39)$	$(15,2,27)$
$f_4 = (12,8,35)$	$(3,2,135)$	$(11,10,39)$	$(15,-2,27)$
$f_4^{-1} = (12,-8,35)$	$(3,-2,135)$	$(12,8,35)$	$(3,2,135)$
$f_5 = (15,2,27)$	$(11,-10,39)$	$(3,-2,135)$	$(12,-8,35)$
$f_5^{-1} = (15,-2,27)$	$(11,10,39)$	$(15,8,28)$	$(7,6,59)$
$f_6 = (15,8,28)$	$(7,6,59)$	$(8,4,51)$	$(8,-4,51)$
$f_6^{-1} = (15,-8,28)$	$(7,-6,59)$	$(15,2,27)$	$(11,-10,39)$
$f_7 = (8,4,51)$	$(8,-4,51)$	$(7,-6,59)$	$(15,-8,28)$
$f_7^{-1} = (8,-4,51)$	$(8,4,51)$	$(15,-8,28)$	$(7,-6,59)$

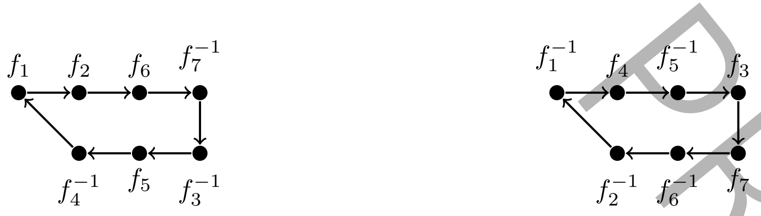
The meaning of $*$ is composition of quadratic forms, for example $f_1 * g_2 = (12,8,35)$. According to the results in the table 1, the graph of 2-isogenies is as follows:



Furthermore, the graph of 3-isogenies is as follows:



In addition, the graph of 17-isogenies is as follows:



Theorem 4.3. *If the supersingular elliptic curves $E_1/\mathbb{F}_p$ and $E_2/\mathbb{F}_p$ are associated with the quadratic forms f_1 and f_2 respectively, then the quadratic form $g = f_2 \cdot f_1^{-1}$ corresponds to an isogeny $\varphi : E_1 \longrightarrow E_2$.*

Proof. Straightforward from Theorem 3.7. □

Question 4.4. *Two isogenous supersingular elliptic curves $E_1/\mathbb{F}_p$ and $E_2/\mathbb{F}_p$ are given.*

a) Find the degree of the isogeny.
b) Find an isogeny $\varphi : E_1 \to E_2$.

To answer this question using correspondence, we provide the following algorithm.

Algorithm 2

```
1. Compute the quadratic forms $f_1$ and $f_2$ corresponding to the elliptic curves $E_1$ and $E_2$.
2. Compute the list of powers $g_{l_i}$ and composition of them, where $l_i$ are prime factors of $\#E(\mathbb{F}_p)$.
3. Calculate $g = f_2 \cdot f_1^{-1}$ and compare $g$ with the list from step 2.
4. If $g = g_{l_1}^{m_1} \cdot g_{l_2}^{m_2} \dots g_{l_k}^{m_k}$, then the degree of the isogeny is $l_1^{m_1} \cdot l_2^{m_2} \dots l_k^{m_k}$.
5. Create the isogeny using Velu formula step by step.
```

Example 4.3. *Consider the elliptic curves E_5 and E_6 in Example 4.1. Then, the list of powers of g_{l_i} and composition of them is as follows:*

$$g_2 = (4,0,101), \quad g_2^2 = (1,0,404), \quad g_3 = (9,2,45), \quad g_3^2 = (5,-2,81), \quad g_3^3 = (17,-4,24),$$

$$g_3^4 = (21,-20,24), \quad g_3^5 = (20,-8,21), \quad g_3^6 = (13,10,33), \quad g_{17} = (13,-10,33),$$

$$g_2 \cdot g_3 = (13,-10,33), \quad g_3 \cdot g_{17} = (20,8,21), \quad g_2 \cdot g_{17} = (9,2,45),$$

$$g_2^2 = (1,0,404), \quad g_3^{14} = (1,0,404), \quad g_{17}^7 = (1,0,404),$$

$$h(-16p) = 28.$$

The class group $Cl(-16p)$ is an abelian group of order 28, and the quadratic form $(3,2,135)$ generates it.

Suppose we want to find the degree of isogeny $\psi : E_1 \longrightarrow E_7$.

$$f_7 \cdot f_1^{-1} = (17,-4,24) = {g_{17}}^3.g_2,$$

So the degree of ψ is 2.17^3.

Now, we want to find the degree of the isogeny $\varphi : E_5 \longrightarrow E_6$.

$$f_6 \cdot f_5^{-1} = (21,-20,24) = g_3^4,$$

Therefore, the degree of the isogeny is 3^4, meaning there are four arrows in the 3-isogeny graph between E_5 and E_6 (Example 4.2). Now, to compute the isogeny, we can construct the 3-isogenies step by step, using the Velu formula. The set of 3-torsion points on E_5 is equal to:

$$\{(0,1),(12,4),(12,97)\},$$

The point $(12,4)$ is the kernel of the isogeny $\varphi_1 : E_5 \longrightarrow \tilde{E}_1$, where

$$\varphi_1(x,y) = \left(\frac{x^3 - 24x^2 + 48x + 4}{x^2 - 24x + 43}, \frac{x^3y - 36x^2y + 23xy + 22y}{x^3 - 36x^2 + 28x - 11} \right),$$

Now we obtain the set of 3-torsion points on $\tilde{E}_1$ as follows:

$$\{(0,1),(0,7),(0,94)\},$$

The point $(0,7)$ is the kernel of the isogeny $\varphi_2 : \tilde{E}_1 \longrightarrow E_1$, where

$$\varphi_2(x,y) = \left(\frac{x^3 - 6}{x^2}, \frac{x^3y + 12y}{x^3} \right),$$

Now, the set of 3-torsion points on E_1 consists of:

$$\{(0,1),(7,38),(7,63)\},$$

The point $(7,38)$ is the kernel of the isogeny $\varphi_3 : E_1 \longrightarrow \tilde{E}_5$, where

$$\varphi_3(x,y) = \left(\frac{x^3 - 14x^2 + 40x - 19}{x^2 - 14x + 49}, \frac{x^3y - 21x^2y - 46xy - 40y}{x^3 - 21x^2 + 46x - 40} \right),$$

The 3-torsion points on $\tilde{E}_5$ are equal to:

$$\{(0,1),(46,44),(46,57)\},$$

The point $(46,44)$ is the kernel of the isogeny $\varphi_4 : \tilde{E}_5 \longrightarrow E_6$, where

$$\varphi_4(x,y) = \left(\frac{x^3 + 9x^2 - 46x + 35}{x^2 + 9x - 5}, \frac{x^3y - 37x^2y + 26xy + 26y}{x^3 - 37x^2 - 15x + 28} \right),$$

Now, by considering the composition of these isogenies, that is $\varphi = \varphi_4 \circ \varphi_3 \circ \varphi_2 \circ \varphi_1$, we have an isogeny of degree 3^4 from E_5 to E_6. Calculations are done using SAGE software [19].

Lemma 4.5. *Let $E_1/\mathbb{F}_p$ and $E_2/\mathbb{F}_p$ be two supersingular elliptic curves and $End(E_1) \cong End(E_2) \cong \mathcal{O}'$. If E_1 and E_2 be $l-$isogenous and the class number be $4k+3$, then the square root of $f_1.f_2^{-1} = h$ is h^{2k+2} and so one can find l directly.*

Proof.

$$(h^{2k+2})^2 = h^{4k+4} = h.$$

According to the format of g_l we can find l simply. □

Example 4.4. *Let $p = 439$, $E_1 : y^2 = x^3 + 425x + 196$ and $E_2 : y^2 = x^3 + 292x + 293$. If $\varphi : E_1 \longrightarrow E_2$ be a l-isogeny, then $f_1 = (4, 3, 28)$ and $f_2 = (10, 9, 13)$. The class number is 15, and*

$$f_2 \cdot f_1^{-1} = (8, 3, 14) = h,$$

$$h^8 = (5, 1, 22),$$

So $l = 5$.

References

[1] S. Arpin, C. Camacho-Navarro, K. Lauter, J. Lim, K. Nelson, T. Scholl, and J. Sotáková, *Adventures in supersingularland*, Exp. Math., 32 (2023), pp. 241–268.

[2] D. A. Buell, *Binary Quadratic Forms: Classical Theory and Modern Computations*, Springer New York, NY, 1 ed., 1989.

[3] J. P. Buhler and P. Stevenhagen, eds., *Algorithmic number theory: lattices, number fields, curves and cryptography*, vol. 44 of Mathematical Sciences Research Institute Publications, Cambridge University Press, Cambridge, 2008.

[4] W. Castryck and T. Decru, *An efficient key recovery attack on SIDH*, in Advances in cryptology—EUROCRYPT 2023. Part V, vol. 14008 of Lecture Notes in Comput. Sci., Springer, Cham, 2023, pp. 423–447.

[5] W. Castryck, T. Lange, C. Martindale, L. Panny, and J. Renes, *CSIDH: an efficient post-quantum commutative group action*, in Advances in cryptology—ASIACRYPT 2018. Part III, vol. 11274 of Lecture Notes in Comput. Sci., Springer, Cham, 2018, pp. 395–427.

[6] D. X. Charles, K. E. Lauter, and E. Z. Goren, *Cryptographic hash functions from expander graphs*, J. Cryptology, 22 (2009), pp. 93–113.

[7] H. Cohen, *A course in computational algebraic number theory*, vol. 138 of Graduate Texts in Mathematics, Springer-Verlag, Berlin, 1993.

[8] D. A. Cox, *Primes of the form $x^2 + ny^2$—Fermat, class field theory, and complex multiplication*, AMS Chelsea Publishing, Providence, RI, 2022. Third edition [of 1028322] with solutions, With contributions by Roger Lipsett.

[9] L. De Feo, D. Jao, and J. Plût, *Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies*, J. Math. Cryptol., 8 (2014), pp. 209–247.

[10] L. De Feo, D. Kohel, A. Leroux, C. Petit, and B. Wesolowski, *SQISign: compact post-quantum signatures from quaternions and isogenies*, in Advances in cryptology—ASIACRYPT 2020. Part I, vol. 12491 of Lecture Notes in Comput. Sci., Springer, Cham, [2020] ©2020, pp. 64–93.

[11] C. Delfs and S. D. Galbraith, *Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$*, Des. Codes Cryptogr., 78 (2016), pp. 425–440.

[12] M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Hansischen Univ., 14 (1941), pp. 197–272.

[13] S. D. Galbraith, *Mathematics of public key cryptography*, Cambridge University Press, Cambridge, 2012.

[14] T. Ibukiyama, *On maximal orders of division quaternion algebras over the rational number field with certain optimal embeddings*, Nagoya Math. J., 88 (1982), pp. 181–195.

[15] P. Longa, *A note on post-quantum authenticated key exchange from supersingular isogenies.* Cryptology ePrint Archive, Paper 2018/267, 2018.

[16] L. Luo, G. Xiao, and Y. Deng, *On two problems about isogenies of elliptic curves over finite fields*, Commun. Math. Res., 36 (2020), pp. 460–488.

[17] J. H. Silverman, *The arithmetic of elliptic curves*, vol. 106 of Graduate Texts in Mathematics, Springer New York, NY, 2nd ed., 2009.

[18] J. Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math., 2 (1966), pp. 134–144.

[19] The Sage Developers, *Sagemath, the sage mathematics software system (version 8:2).* `http://www.sagemath.org`, 2018.

[20] J. Vélu, *Isogénies entre courbes elliptiques*, C. R. Acad. Sci. Paris Sér. A-B, 273 (1971), pp. A238–A241.

[21] L. C. Washington, *Elliptic Curves: Number Theory and Cryptography*, Chapman and Hall/CRC, 2nd ed., 2008.

[22] G. Xiao, Z. Zhou, Y. Deng, and L. Qu, *Endomorphism rings of supersingular elliptic curves over $\mathbb{F}_p$ and binary quadratic forms*, Adv. Math. Commun., 19 (2025), pp. 698–715.

[23] Élise Tasso, L. D. Feo, N. E. Mrabet, and S. Pontié, *Resistance of isogeny-based cryptographic implementations to a fault attack.* Cryptology ePrint Archive, Paper 2021/850, 2021.

Please cite this article using:

Leila Goodarzi, Hassan Daghigh, Supersingular elliptic curves, binary quadratic forms and isogenies, AUT J. Math. Comput., 7(1) (2026) 19-31
https://doi.org/10.22060/AJMC.2024.23144.1245