INdAM Fellowship Programs in Mathematics and/or Applications
cofunded by Marie Skłodowska-Curie Actions
(**INdAM-DP-COFUND-2015**)

Doctoral Thesis Submitted To

Università degli Studi di Roma Tre, Department of Mathematics

Title

Some Objects from Algebraic Geometry and their Application to Post-Quantum Cryptography

By

Manoj Gyawali

Supervisor

Prof. Luca De Feo

Coordinator

Prof. Angelo Felice Lopez

June 3, 2021

Contents

Introduction

Algebraic geometry is concerned with the study of those geometric objects that can be represented as the solutions of a multivariate polynomial system. It is a central branch of mathematics having connections to various other subfields, and its modern areas of research study the geometric objects by constructing more complex algebraic structures on them.
In this manuscript, we are interested in the applications of algebraic geometry to cryptography, in particular to post-quantum cryptography (PQC). One of the main reasons to draw attention toward PQC is the algorithm of Shor [81]. Because of it, all the public key cryptosystems based on the difficulty of the discrete logarithm or integer factorization problems became vulnerable to polynomial-time attacks by quantum computers. Moreover, a competition organized by the United States government agency National Institute of Standards and Technology (NIST) for new post-quantum cryptographic algorithms [66] and its recent third selection round show the flourishing interest in the area of post-quantum cryptography. Participants of the competition can be categorized into lattice-based, code-based, multivariate, hash-based, [11] and isogeny based cryptography. Most of these cryptographic constructions use techniques from algebraic geometry, thereby proving its efficacy in post-quantum cryptography.
In this work, we review some topics related to isogeny based cryptography, and initiate the study of Veronese variety and Grassmannian in the context of post-quantum cryptography. Our study is structured in two parts. The first part is related to the isogeny problems and the second part is devoted to new key exchange and signature protocols based on hard problems occurred in Veronese variety and secant variety of the Grassmannian.
Isogeny based cryptography is appealing in the area of post-quantum cryptography because of its relatively small key size and underlying beautiful mathematical theory. Many variants of the isogeny problems are used in many existing primitives [56, 18, 21, 51, 46]. There are two main hard problems in isogeny based schemes: finding an isogeny between two elliptic curves and computing the endomorphism ring of an elliptic curve. These

two problems are related to each other [59] and there is no sub-exponential algorithm to solve them for supersingular elliptic curves [72]. The computation of a single endomorphism of an elliptic curve E is also closely related to the problem of computing the endomorphism ring of E [58].

Chapter organization and main contributions: In Chapters 1 and 2, we give some preliminaries that will be used in the later chapters. Chapter 1 is mainly related to Chapters 3 and 4, and Chapter 2 provides a background for Chapter 5. Chapter 6 is more or less self-contained.
In Chapter 3, we study an endomorphism computation problem for a supersingular elliptic curve defined over a finite field $\mathbb{F}_p$ under the assumption that the action of the endomorphism is known on a torsion subgroup of the elliptic curve. This problem was first posed in [71], where it is reduced to that of solving a Diophantine equation. We use Simon's algorithm [84] to solve such a quadratic equation. We also use a technique from [61] to improve the size of the parameters under some heuristic assumptions.
In Chapter 4, we study the action of the class group of an imaginary quadratic order $\mathcal{O}$ on the set of elliptic curves with complex multiplication by $\mathcal{O}$. This action has been used to construct several cryptosystems based on isogenies for example [19, 75, 87, 31]. Classical genus theory gives the structure of the 2-torsion subgroup of the class group of $\mathcal{O}$ via some non-trivial quadratic characters. In [20], an interesting connection between genus theory and isogeny graphs was discovered, and was used to break the analogue of the decisional Diffie-Hellman problem for some isogeny-based cryptosystems. In this work, we restrict our attention to the values of the non-trivial characters in the 2-torsion subgroup of the class group $cl(\mathcal{O}_K)$ of a maximal order $\mathcal{O}_K$ of an imaginary quadratic field K and observe how these values give colorings in some Cayley and isogeny graphs obtained from the 2-torsion subgroup $cl(\mathcal{O}_K)[2]$ of $cl(\mathcal{O}_K)$.

In Chapter 5, we propose a new key exchange scheme that we call Quadratic Surface Intersection (QSI) key exchange, joint work with Daniele Di Tullio. We give a naive implementation of the algorithm in the SageMath [35]. We claim hardness of the underlying mathematical problems through empirical evidence.

In Chapter 6, we propose a new signature scheme from the secant variety of the Grassmannian, which is also a joint work with Daniele Di Tullio. This scheme resembles multivariate signature schemes such as [38, 57]. We give an abstract description of the scheme and justify the underlying problem by means of some experimental evidences. We implemented our algorithm

in SageMath [35].

Chapter 1

An introduction to isogeny based post-quantum cryptography

1.1 Overview

Cryptography is a study of methods that deals with secure means of communication between any parties being aware of adversaries. Such a secure communication can be achieved by encryption and decryption of message. A message, which is also called plaintext, is encrypted by an algorithm using some keys then the encrypted message called ciphertext is sent through an insecure channel. Upon receiving the ciphertext, an algorithm decrypts it with the help of some keys to recover the original message. Encryption algorithms should be strong enough to protect private data from malicious adversaries. At the same time, these algorithms should require a reasonable amount of time and memory to be useful for practical purposes.
To meet the security necessities of the present world, many cryptographic schemes have appeared in the literature. These range from private key cryptography, where sender and receiver both have the same keys, to public-key cryptography, where the sender uses the public keys of the receiver to encrypt the message and the receiver retrieves the message by using her/his private keys. Furthermore, a new area of research in cryptography has been carried out extensively, called post-quantum cryptography(PQC).
In this chapter, we mainly discuss some preliminaries of isogeny based cryptography, some of the isogeny schemes, and some of the possible attacks on these schemes.

1.2 Elliptic curve, isogeny and endomorphism ring

There are good references for elliptic curve, isogeny [48, 82, 83, 88, 94] and their application to isogeny based cryptography [29]. We arrange some of the contents from these references that are useful in the isogeny based cryptography.

1.2.1 Elliptic curve

Suppose κ be a perfect field, a field whose every algebraic extension is separable, for example, the finite fields. Let $\bar{\kappa}$ be its algebraic closure. For cryptographic application, we take $\kappa = \mathbb{F}_q$, a finite field of q elements.
We will define an elliptic curve as a smooth projective variety. Before that, it is worthwhile to recall some notions of projective space, variety, and dimension.

Definition 1.2.1. *The n dimensional projective space is defined as*

$$\mathbb{P}^n_{\bar{\kappa}} = (\bar{\kappa}^{n+1} \setminus \mathbf{0}) / \sim,$$

where $\mathbf{0}$ *is a zero vector in* κ^{n+1} *and the equivalence relation* $\sim$ *on* $\bar{\kappa}^{n+1}$ *is defined as*

$$(x_0, ..., x_n) \sim (y_0, ..., y_n) \iff \exists \lambda \in \bar{\kappa}^* = \bar{\kappa} \setminus \{0\} \text{ s.t. } x_i = \lambda y_i \ \ \forall\, i = 0, \ldots, n$$

and an equivalence class is denoted by $[x_0 : ... : x_n]$ *which is called the homogeneous coordinate of* $\mathbb{P}^n_{\bar{\kappa}}$*. The set of* κ*-rational points in* $\mathbb{P}^n_{\bar{\kappa}}$ *is defined to be the set*

$$\mathbb{P}^n_{\kappa} = \{P \in \mathbb{P}^n_{\bar{\kappa}} : \sigma(P) = P \ \forall\, \sigma \in \mathcal{G}_{\bar{\kappa}/\kappa}\},$$

where $\mathcal{G}_{\bar{\kappa}/\kappa}$ *is the Galois group which acts on* $\mathbb{P}^n_{\bar{\kappa}}$ *as follows*

$$\sigma([x_0 : ... : x_n]) = [\sigma(x_0) : ... : \sigma(x_n)] \ \text{ for } \sigma \in \mathcal{G}_{\bar{\kappa}/\kappa}.$$

The n-dimensional affine space $\mathbb{A}^n_{\bar{\kappa}} = \bar{\kappa}^n$ can be identified by the following inclusion

$$\begin{array}{ccc} \mathbb{A}^n_{\bar{\kappa}} & \longrightarrow & \mathbb{P}^n_{\bar{\kappa}} \\ (x_1, \ldots, x_n) & \longmapsto & [x_1 : x_2 : \ldots : x_{i-1} : 1 : x_{i+1} : \ldots : x_n] \end{array}$$

for each $0 \leq i \leq n$. In fact, there is a bijection between the sets

$$U_i = \{[x_0 : \ldots : x_n] \in \mathbb{P}^n_{\bar{\kappa}} : x_i \neq 0\} \subset \mathbb{P}^n_{\bar{\kappa}} \text{ and } \mathbb{A}^n_{\bar{\kappa}},$$

where the inverse map from U_i to $\mathbb{A}^n_{\bar{\kappa}}$ is given by

$$[x_0 : \ldots : x_n] \mapsto \left(\frac{x_0}{x_i}, \frac{x_1}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i}\right).$$

In a projective space, homogeneous polynomials are the well-defined polynomials. A polynomial $G \in \bar{\kappa}[x] = \bar{\kappa}[x_0, \ldots, x_n]$, where $\bar{\kappa}[x]$ is a polynomial ring in variables $x_0, \ldots, x_n$, is called the *homogeneous polynomial* of degree d if

$$G(\lambda x_0, \ldots, \lambda x_n) = \lambda^d G(x_0, \ldots, x_n) \; \forall \; \lambda \in \bar{\kappa}.$$

Such a polynomial G has well-defined zeros in the homogeneous coordinates. An ideal $I \subset \bar{\kappa}[x]$ is called homogeneous if all the generating polynomial of I are homogeneous polynomials.
For any given polynomial in an affine space, we can convert it to a homogeneous polynomial and vice versa.

Definition 1.2.2. *For a polynomial $g \in \bar{\kappa}[x_0, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n]$ of degree d, the homogenization of g by x_i is the polynomial G given by*

$$G(x_0, \ldots, x_n) = x_i^d g\left(\frac{x_0}{x_i}, \frac{x_1}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i}\right)$$

and conversely, the dehomogenization of any homogeneous polynomial $G \in \bar{\kappa}[x]$ by x_i is the polynomial g obtained as

$$g(x_0, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) = G(x_0, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n).$$

The solution set of an ideal of polynomials is defined as an algebraic set.

Definition 1.2.3. *An affine algebraic set is a set of the form*

$$V_I = \{P \in \mathbb{A}^n_{\bar{\kappa}} : g(P) = 0 \; \forall \; g \in I\},$$

where $I \subset \bar{\kappa}[x_1, \ldots, x_n]$ is an ideal. An affine algebraic set V_I is called an affine variety if the ideal I is a prime ideal in $\bar{\kappa}[x_1, \ldots, x_n]$. If V is affine algebraic set, then the ideal of V is defined as $I_V = \{g \in \bar{\kappa}[x_1, \ldots, x_n] : g(P) = 0 \; \forall \; P \in V\}$.

Polynomials or rational functions on any variety constitute the coordinate ring and the function field of the variety respectively.

Definition 1.2.4. *An affine algebraic set $V \subset \mathbb{A}^n_{\bar{\kappa}}$ is said to be defined over a field κ and written as V/κ if its ideal is generated by polynomials whose coefficients lie in κ. The affine coordinate ring of V/κ is denoted as $\kappa[V]$ and is defined as the quotient $\kappa[V] = \frac{\kappa[x_0,\ldots,x_n]}{I_V}$. Similarly, $\bar{\kappa}[V] = \frac{\bar{\kappa}[x_0,\ldots,x_n]}{I_V}$.*

If V is a variety, the quotient $\kappa[V] = \frac{\kappa[x_0,\ldots,x_n]}{I_V}$ is an integral domain and we can define its fraction field. The *function field* of an affine variety V/κ is denoted as $\kappa(V)$ and is the field of fraction of the coordinate ring $\kappa[V]$. Similar definition works if we replace κ by $\bar{\kappa}$.

Definition 1.2.5. *The field extension $\bar{\kappa}(V)/\bar{\kappa}$ is transcendental over $\bar{\kappa}$ and its degree is the dimension of an affine variety V.*

Variety may contain both singular and nonsingular points. We are interested in a variety not containing the singular points.

Definition 1.2.6. *Let V be an affine variety and $g_1,\ldots,g_m \in \bar{\kappa}[x_1,\ldots,x_n]$ are generators of I_V then V is called nonsingular at a point $P \in V$ if the $m \times n$ Jacobian matrix $A = (a_{i,j})_{1\le i\le m, 1\le j\le n}$ with*

$$a_{i,j} = \frac{\partial g_i}{\partial x_j}(P)$$

has rank n-dim$V$, otherwise P is singular point of V. If all the points of V are nonsingular then V is called smooth.

There is a similar definition for algebraic projective variety where we take homogeneous polynomial and homogeneous ideal.

Definition 1.2.7. *Any set of the form*

$$V_I = \{P \in \mathbb{P}^n_{\bar{\kappa}} : G(P) = 0 \ \forall \ \text{homogeneous polynomial } G \in I\},$$

where I is a homogeneous ideal, is called a projective algebraic set. Given a projective set V, the ideal of V is denoted as I_V and is given by

$$I_V = \{G \in \bar{\kappa}[x] : G \text{ is homogeneous and } G(P) = 0 \ \forall \ P \in V\}.$$

Definition 1.2.8. *A projective variety is a projective algebraic set whose homogeneous ideal I_V is a prime ideal in $\bar{\kappa}[x]$.*

Simple examples of projective varieties are the ones defined by linear equations.

Definition 1.2.9. *A linear subspace $L \subset \mathbb{P}^n_{\bar{\kappa}}$ is a projective variety defined by homogeneous polynomials of degree 1. The codimension of L, denoted by* $\mathrm{codim}_{\mathbb{P}^n_{\bar{\kappa}}}(L)$*, can be defined as the minimum number of generators of the ideal I_L.*

Other easy examples of projective algebraic sets are the varieties cut by one equation.

Definition 1.2.10. *A hypersurface is a projective algebraic set $V \subset \mathbb{P}^n_{\bar{\kappa}}$ defined by a single equation $F(X_0, ..., X_n) = 0$.*

Projective variety and its properties can be identified by looking at its affine parts.

Definition 1.2.11. *Let V be a projective variety with homogeneous ideal $I_V = (G_1, \ldots, G_m)$. Then affine parts of V are the varieties $V_i = V \cap U_i$, where $U_i = \{[x_0 : \ldots : x_n] \in \mathbb{P}^n_{\bar{\kappa}} : x_i \neq 0\}$ for all i. The ideal of V_i is generated by the polynomials obtained by dehomogenization of G_i at x_i for all i and $V = \bigcup_i V_i$. The dimension of the projective variety V is the maximum of the dimension of its affine parts V_i, and is smooth if and only if all of its affine parts are smooth.*

For a projective variety, the function field $\kappa(V)$ or $\bar{\kappa}(V)$ is defined as the function field of its affine part $\kappa(V_i)$ or $\bar{\kappa}(V_i)$ for some fixed i after homogenizing each elements. Therefore, the function field of a projective variety V is the field of the rational functions $G = f/h$ such that :

- f and h are homogeneous of the same degree;
- $h \notin I_V$
- with an equivalence relation $f_1/h_1 \sim f_2/h_2$ if $f_1h_2 - f_2g_1 \in I_V$.

Any function $G \in \bar{\kappa}(V)$ is *regular* or *defined at a point* $P \in V$ if $G = f/h$ for some $f, h \in \bar{\kappa}[V]$ with $h(P) \neq 0$. We define rational map between projective varieties and its regularity at points.

Definition 1.2.12. *Let $V_1, V_2 \in \mathbb{P}^n$ be projective varieties. A rational map $\phi : V_1 \to V_2$ is of the form*

$$\phi = [G_0 : \ldots : G_n],$$

where the functions $G_0, \ldots G_n \in \bar{\kappa}(V_1)$ satisfy

$$\phi(P) = [G_0(P) : \ldots : G_n(P)] \in V_2$$

for each point $P \in V_1$ at which all $G_0, \ldots, G_n$ are well defined. Moreover, ϕ is regular (or defined) at $P \in V_1$ if there exists a function $g \in \bar{\kappa}(V_1)$ such that each gG_i is regular at P and $gG_i(P) \neq 0$ for some i. In this case,

$$\phi(P) = [(gG_0)(P) : \ldots : (gG_n)(P)].$$

A rational map that is regular at every point is called a morphism.

Note that a rational function $\phi = [G_0 : \ldots : G_n]$ is defined only up to a scaling by a function in $\bar{\kappa}(V_1)^*$.
Now we define a projective variety of our interest. An *algebraic curve* is a projective variety of dimension one. An elliptic curve can be defined as a smooth projective variety having a group structure and is defined by a single homogeneous equation.

Definition 1.2.13. *Elliptic curve E can be defined as an abelian variety of dimension one, where an abelian variety is a smooth projective variety with a marked point O having the group structure given by rational maps and O is an identity element.*

With this definition, an elliptic curve has both algebraic and geometric structure therefore it can be treated algebraically as an abelian group and geometrically as a smooth projective curve. To make a discussion precise, we consider the Weierstrass form of an elliptic curve and see it as an abelian variety. An elliptic curve can equivalently be defined as a nonsingular curve defined by the Weierstrass equation 1.1 see in [65].

Definition 1.2.14. *(Weierstrass form). Let κ be a field, then an elliptic curve E defined over κ is the set of solutions $[X : Y : Z] \in \mathbb{P}^2_{\bar{\kappa}}$ of the following general Weierstrass equation*

$$Y^2Z + c_1XYZ + c_3YZ^2 = X^3 + c_2X^2Z + c_4XZ^2 + c_6Z^3, \tag{1.1}$$

with $c_1, c_2, c_3, c_4, c_6 \in \kappa$ and $\Delta \neq 0$ where

$$\begin{aligned}
\Delta &= -d_2^2d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6 \\
d_2 &= c_1^2 + 4c_2 \\
d_4 &= 2c_4 + c_1c_3 \\
d_6 &= c_3^2 + 4c_6 \\
d_8 &= c_1^2c_6 + 4c_2c_6 - c_1c_3c_4 + c_2c_3^2 - c_4^2.
\end{aligned}$$

Curve defined by Equation 1.1 meets the line of infinity $Z = 0$ at the point $O = [0 : 1 : 0]$ with multiplicity 3, and the point O is called the point at infinity. The quantity $j(E) = (d_2^2 - 24d_4)^3/\Delta$ is called the *j-invariant* of the elliptic curve E.

Theorem 1.2.15. *1. Weierstrass equation 1.1 defines a nonsingular elliptic curve if and only if $\Delta \neq 0$.*

2. *Two elliptic curves over κ are isomorphic over $\bar{\kappa}$ if and only if they have the same j-invariant.*

3. *Every $j_E \in \bar{\kappa}$ there exists an elliptic curve E defined over the field $\kappa(j_E)$ such that $j(E) = j_E$.*

Proof. See in [82, Proposition 1.4]. □

If characteristic of the field κ is not 2 or 3 then the affine form of Equation (1.1) can be transformed into the following short Weierstrass form

$$y^2 = x^3 + Ax + B \tag{1.2}$$

and hence the discriminant and the j-invariant reduce to $\Delta = -16(4A^3 + 27B^2)$ and $j = -1728\frac{(4A)^3}{\Delta}$ respectively.
Moreover, elliptic curve E over κ can be defined as

$$\{(x, y) \in \bar{\kappa}^2 : y^2 = x^3 + Ax + B\} \cup \{O\}$$

and for a field extension $\kappa \subset K$, the K-rational points of E constitute the set

$$E(K) = \{(x, y) \in K^2 : y^2 = x^3 + Ax + B \text{ with } A, B \in \kappa\} \cup \{O\}.$$

We define a composition law on the Weierstrass form of elliptic curve E, which gives a group structure with identity O. We need the Bézout's theorem to define the composition law.

Bézout's theorem: Let $F(X, Y, Z), G(X, Y, Z) \in \bar{\kappa}[X, Y, Z]$ be two homogeneous polynomials of degree m and n respectively without having a common factor then they intersect at mn points defined over $\bar{\kappa}$ counted with multiplicities.

Composition law on E: Let $P, Q \in E$ be two points, consider a line L_1 passing through P and Q (it will be tangent if $P = Q$) then L_1 meets E at one more point say R by Bézout's theorem. Join again R and O by another line L_2 to get one more intersecting point with E say $P + Q$, which is defined as the composition of P and Q. See Figure 1.1 when E is defined over the real numbers.

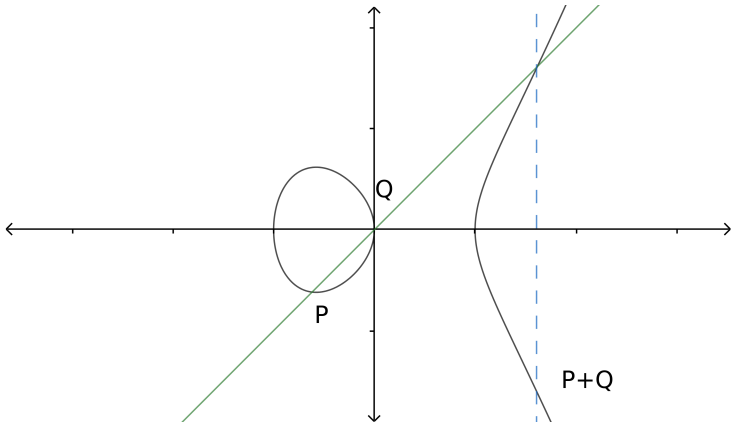

Figure 1.1: Composition law on elliptic curve over the real number $\mathbb{R}$

With the composition law above, E becomes an abelian group.

Theorem 1.2.16. *The elliptic curve E is an abelian group under the composition $'+'$ with the identity element O. Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be any two non-identity points on the elliptic curve given by the affine form of the short Weierstrass equation $E : y^2 = x^3 + Ax + B$. Then the group operation is given explicitly by the following formula*

- *Inverse of any element P is $-P = (x_1, -y_1)$.*
- *Let $P + Q = R := (x_3, y_3)$ where*

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2 \\ y_3 &= -\lambda x_3 - y_1 + \lambda x_1, \end{aligned}$$

and

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } P \neq Q \\ \frac{3x_1^2 + A}{2y_1} & \text{if } P = Q. \end{cases}$$

Proof. See in [82]. □

When an elliptic curve is defined over a finite field then its cardinality and group structure can be determined.

Theorem 1.2.17. *(Hasse) Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$. Then the number of $\mathbb{F}_q$-rational points $\#E(\mathbb{F}_q)$ of E is bounded as*

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

Proof. See in [94]. □

The following theorem gives the group structure of an elliptic curve defined over a finite field.

Theorem 1.2.18. *Let p be a prime and $q = p^n$ and $N = q + 1 - t$. Then there is an elliptic curve defined over $\mathbb{F}_q$ such that $|E(\mathbb{F}_q)| = N$ if and only if $|t| \leq 2\sqrt{q}$ and t satisfies the following*

1. $\gcd(t, p) = 1$
2. *n is even and $t = \pm 2\sqrt{q}$*
3. *n is even, $p \not\equiv 1 \pmod 3$, and $t = \pm\sqrt{q}$*
4. *n is odd, $p = 2$ or 3, and $t = \pm p^{(n+1)/2}$*
5. *n is even, $p \not\equiv 1 \pmod 4$, and $t = 0$*
6. *n is odd and $t = 0$.*

If we have $N = p^\ell n_1 n_2$ with $p \nmid n_1 n_2$ and $n_1 | n_2$ then there is an elliptic curve E defined over $\mathbb{F}_q$ such that

$$E(\mathbb{F}_q) \simeq \mathbb{Z}/p^\ell\mathbb{Z} \oplus \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z}$$

if and only if either $n_1 | q - 1$ in case $(1), (3), (4), (5), (6)$ or $n_1 = n_2$ in the case (2). These are the only possible classifications of $E(\mathbb{F}_q)$.

Proof. See in [95] for the first part and in [74] for the second part. □

1.2.2 Isogenies between elliptic curves

Definition 1.2.19. *Let E_0, E be elliptic curves defined over a field κ. An isogeny $\phi : E_0 \to E$ is a non-constant morphism which sends the identity element of E_0 to the identity element of E.*

Since a morphism between projective curves is either surjective or constant, an isogeny between elliptic curves is a surjective rational map preserving the identity elements.
We define the degree of an isogeny.

Definition 1.2.20. *Let E_1/κ and E_2/κ be elliptic curves defined over a field κ and $\phi : E_1 \to E_2$ be an isogeny. This isogeny induces an injection of function fields that fixes κ,*

$$\phi^* : \kappa(E_2) \to \kappa(E_1), \qquad \phi^* f = f \circ \phi$$

and $\kappa(E_1)/\phi^*\kappa(E_2)$ is a finite extension. Then, the degree of ϕ is defined as

$$deg\ \phi := [\kappa(E_1) : \phi^*\kappa(E_2)]$$

and ϕ is called separable, inseparable, or purely inseparable if the field extension $\kappa(E_1)/\phi^*\kappa(E_2)$ is respectively separable, inseparable, or purely inseparable. The separable and inseparable degrees of ϕ are denoted as $\deg_s \phi$ and $\deg_i \phi$ respectively.

The degree of an isogeny is the product of its separable and inseparable degrees i.e. $\deg \phi = \deg_s \phi \deg_i \phi$. Simple examples of isogenies are multiplication by integers. For each $m \in \mathbb{Z}^*$ the multiplication of m map $[m] : E \to E$ defined as

$$[m](P) = \begin{cases} P + \ldots + P & \text{for } m > 0 \\ [-m](-P) & \text{for } m < 0 \end{cases}$$

are isogenies from E to E.

For each isogeny, there is a corresponding dual isogeny.

Theorem 1.2.21. *Let $\phi : E_1 \to E_2$ be an isogeny of degree m. Then there exists a unique isogeny $\hat{\phi}$ called dual isogeny which satisfies $\hat{\phi} \circ \phi = [m]$ on E_1 and $\phi \circ \hat{\phi} = [m]$ on E_2. Furthermore,*

- *deg $\hat{\phi} = \deg \phi$.*
- $\hat{\hat{\phi}} = \phi$
- *For all $m \in \mathbb{Z}$,*

$$\hat{[m]} = [m], \text{ for } m = 0 \text{ set } [\hat{0}] = [0]$$

- *Let $\psi : E_1 \to E_2$ be another isogeny, then*

$$\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}$$

- *Let $\phi_1 : E_2 \to E_3$ be another isogeny, then*

$$\widehat{\phi_1 \circ \phi} = \hat{\phi} \circ \hat{\phi}_1.$$

Proof. See in [82, Theorem 6.2]. □

The kernel of the multiplication by m map $[m] : E \to E$ is the subgroup

$$E[m] := \{P \in E(\bar{\kappa}) : mP = 0\}$$

called the m-torsion subgroup of E.

The structure of m torsion subgroup $E[m]$ is given by the following theorem.

Theorem 1.2.22. *Let E be an elliptic curve defined over a field κ and let $m \in \mathbb{Z}^*$.*

- *If either $char(\kappa) = 0$ or $char\ (\kappa) = p > 0$ and $p \nmid m$ then*

$$E[m] = \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}.$$

- *If $char\ (\kappa) = p > 0$ then either*

$$E[p^i] = \{O\} \text{ or } E[p^i] = \mathbb{Z}/p^i\mathbb{Z} \text{ for all } i \in \mathbb{N}.$$

Proof. See in [82, Corollary 6.4]. □

Elliptic curve E over a finite field $\mathbb{F}_q$ with $q = p^r$ can be classified as *ordinary* or *supersingular* according to the structure of the p torsion subgroup of E; E is called ordinary if $E[p] \cong \mathbb{Z}/p\mathbb{Z}$ and is called supersingular if $E[p] = \{0\}$.
A supersingular elliptic curve defined over a field of non-zero characteristic p has an isomorphic copy that is defined over a quadratic extension of $\mathbb{F}_p$, and hence all such curves can be enumerated.

Theorem 1.2.23. *Let E be a supersingular elliptic curve defined over a field κ of characteristic $p > 0$. Then the j-invariant of E belongs to $\mathbb{F}_{p^2}$. For $p \geq 5$, the number of all supersingular elliptic curves defined over $\overline{\mathbb{F}}_p$ is*

$$\left\lfloor \frac{p}{12} \right\rfloor + \begin{cases} 0 & \text{if } p \equiv 1 \ (mod\ 12) \\ 1 & \text{if } p \equiv 5, 7 \ (mod\ 12) \\ 2 & \text{if } p \equiv 11 \ (mod\ 12). \end{cases}$$

Proof. [94, Corollary 4.40]. □

Two elliptic curves are called *isogenous* if there is an isogeny between them. The following theorem shows that ordinary elliptic curves are isogenous to only ordinary elliptic curves, and the same is true for supersingular elliptic curves.

Theorem 1.2.24. *Let $\phi : E_1 \to E_2$ be an isogeny of elliptic curves. Then E_1 is ordinary if and only if E_2 is ordinary or equivalently E_1 is supersingular if and only if E_2 is supersingular.*

Proof. See in the lecture note of Sutherland [88, Lecture 14, Theorem 14.2]. □

As we have observed, the kernel of multiplication by m map is the m-torsion subgroup $E[m]$, which is a finite subgroup of E. The kernel of an isogeny is finite and it gives a unique separable isogeny.

Theorem 1.2.25. *Let $\phi : E_1 \to E_2$ be an isogeny. Then the kernel of ϕ is finite and its number of elements is equal to the separable degree of ϕ.*

Proof. See in [82, Theorem 4.10]. □

Conversely, for any finite subgroup of an elliptic curve, there exists a unique separable isogeny of kernel from that subgroup.

Theorem 1.2.26. *Let E be an elliptic curve over a field κ and G be a finite subgroup of E whose order is coprime with the characteristic of κ. Then, there exists an elliptic curve $E^{'}$ and a separable isogeny $\phi : E \to E^{'}$ up to isomorphism such that $\ker \phi = G$.*

Proof. See in [82, Proposition 4.12]. □

Any isogeny from a kernel can be explicitly calculated by the Velú's formula [93]. Using Theorem 1.2.26 repeatedly, any isogeny can be written as the composition of prime degree isogenies.

Endomorphisms are the isogenies from an elliptic curve to itself. We also include zero morphism, denoted by $[0]$ and considering its degree as 0, in the following set

$$\mathrm{End}(E) = \{ \text{ isogenies } \phi : E \to E\} \cup \{[0]\}.$$

For $P \in E$, sum and multiplication of two elements $\phi, \psi \in \mathrm{End}\,(E)$ are defined respectively as

$$\begin{aligned}(\phi + \psi)(P) =& \phi(P) + \psi(P)\\ (\phi\psi)(P) =& \phi(\psi(P)).\end{aligned}$$

The set $\mathrm{End}(E)$ is a ring by the following theorem and is called the *endomorphism ring* of E. We will see that it is an invariant of E that classifies it as ordinary or supersingular.

Theorem 1.2.27. *Let E be an elliptic curve. Then the endomorphism ring $\mathrm{End}(E)$ is a ring of characteristic zero with no zero divisors.*

Proof. See in [82, Proposition 4.2(c)]. □

The above theorem shows that $\mathrm{End}(E)$ is an integral domain.

There is an important endomorphism called Frobenius endomorphism when elliptic curve is defined over a finite field.

Frobenius Endomorphism:

Let E be an elliptic curve defined over a field κ of characteristic $p > 0$ and $q = p^r$. Let $E^{(q)}$ be the elliptic curve whose equation is obtained by raising the coefficients of E to the q-th power. Then there is the natural map $\pi_q : E \to E^{(q)}$ called *q-th power Frobenius map* which is given by

$$\pi_q : [x : y : z] \to [x^q : y^q : z^q].$$

Theorem 1.2.28. *Let E an elliptic curve over a field $\kappa = \mathbb{F}_q$ of characteristic $p > 0$ with $q = p^r$ and $\pi_q : E \to E^{(q)}$ be the q-th power Frobenius map then*

- *π_q is purely inseparable.*
- *deg π_q is q.*
- *Every isogeny $\phi : E_1 \to E_2$ between the elliptic curve over κ can be factored as $\phi = \phi_1 \circ \pi_q$:*

$$E_1 \xrightarrow{\pi_q} E_1^{(q)} \xrightarrow{\phi_1} E_2,$$

where q is the inseparable degree of ϕ and ϕ_1 is a separable isogeny.

Proof. See in [82, Proposition 2.11 and Corollary 2.12]. □

When an elliptic curve is defined over $\mathbb{F}_q$ then $E^{(q)} = E$ and π_q is an endomorphism of E called the *Frobenius endomorphism* of E.

Theorem 1.2.29. *Let E be an elliptic curve defined over a field $\mathbb{F}_q$ with $q = p^r$. Let π_q be the Frobenius endomorphism of E. Then the map*

$$m_1 + m_2\pi_q : E \to E$$

for $m_1, m_2 \in \mathbb{Z}$ is separable if any only if p does not divide m_1 .

Proof. See in [82, Corollary 5.5]. □

1.2.3 Endomorphism algebra

Let E be an elliptic curve defined over a field κ. We know that the endomorphism ring $\mathrm{End}(E)$ is a ring, so it is also a $\mathbb{Z}$ algebra. The *endomorphism algebra* of E is denoted by $\mathrm{End}^0(E)$ and is defined as

$$\mathrm{End}^0(E) := \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q},$$

where $\mathbb{Q}$ is the set of rational numbers. Since both $\mathrm{End}(E)$ and $\mathbb{Q}$ are torsion-free $\mathbb{Z}$ algebras, they are identified canonically (with canonical embeddings $\phi \mapsto \phi \otimes 1$ and $\alpha \mapsto 1 \otimes \alpha$ resp., for $\phi \in \mathrm{End}(E)$ and $\alpha \in \mathbb{Q}$) as the subrings of the algebra $\mathrm{End}^0(E)$.

Definition 1.2.30. *For $\mu \in End^0(E)$, set $\phi \otimes s = s\phi$ for $\phi \in End(E)$ and $s \in \mathbb{Q}$. Define*

- $\widehat{s\mu} = s\hat{\mu}$,
- *reduced norm of μ is $N(\mu) = \mu\hat{\mu}$,*
- *trace of μ is $Tr(\mu) = \mu + \hat{\mu}$.*

It is not hard to show that $\mathrm{End}^0(E)$ is a division ring. The classification of $\mathrm{End}^0(E)$ gives the classification of the ring $\mathrm{End}(E)$. Before the classification of $\mathrm{End}^0(E)$, we define quaternion algebra.

Definition 1.2.31. *A quaternion algebra is a $\mathbb{Q}$-algebra with basis $\{1, a, b, ab\}$ satisfying*

$$a^2, b^2 \in \mathbb{Q}, a^2 < 0, b^2 < 0 \text{ and } ab = -ba.$$

Theorem 1.2.32. *Let E be an elliptic curve over a field κ. Then the endomorphism algebra $End^0(E)$ is isomorphic to one of the following*

- *the field of rational number $\mathbb{Q}$*
- *a quadratic field $\mathbb{Q}(a)$ with $a^2 < 0$*
- *a quaternion algebra $\mathbb{Q}(a, b)$ with $a^2, b^2 < 0$.*

Furthermore, if $End^0(E)$ has dimension $d = 1, 2, 4$ as a $\mathbb{Q}$ vector space then $End(E)$ has rank d as a free $\mathbb{Z}$ module.

Proof. See in [88, Theorem 13.17]. □

The endomorphism ring $\mathrm{End}(E)$ is situated in $\mathrm{End}^0(E)$ not only as a lattice (free module of maximum rank) but also as a subring. For ordinary case, the following theorem gives the precise information of the endomorphism ring.

Theorem 1.2.33. *Let E be an ordinary elliptic curve over the field $\mathbb{F}_q$. Then $End^0(E) = \mathbb{Q}(\pi_q) \cong \mathbb{Q}(\sqrt{d_\pi})$ is an imaginary quadratic field, where $d_\pi = (Tr\ \pi_q)^2 - 4q$ is the discriminant of the characteristic polynomial of π_q.*

Proof. See in [88, Corollary 14.7]. □

For ordinary curve, the endomorphism algebra (an isomorphic copy) can be calculated if the trace of the Frobenius is known, the trace is calculated by Schoof's algorithm. From Theorem 1.2.32, $\mathrm{End}(E)$ is an order in the imaginary quadratic field $K = \mathbb{Q}(\sqrt{d_\pi})$ and

$$\mathbb{Z}[\pi_q] \subset \mathrm{End}(E) \subset \mathcal{O}_K,$$

where $\mathcal{O}_K$ is the maximal order of K, giving only finite number of possibilities for $\mathrm{End}(E)$.

For a supersingular elliptic curve, endomorphism ring is non-commutative in nature. It is a maximal order in a quaternion algebra by the following theorem.

Theorem 1.2.34. *Let E be a supersingular elliptic curve, then $End^0(E)$ is a quaternion algebra.*

Proof. See in [88, Theorem 14.18]. □

1.3 Elliptic curve over $\mathbb{C}$ and complex multiplication

In this section, we explore an elliptic curve defined on the complex plane $\mathbb{C}$ with its endomorphism ring $\mathcal{O}$ (an order in an imaginary quadratic field), the maps between such curves, and the action of class group $cl(\mathcal{O})$ on the set of elliptic curves whose endomorphism ring is $\mathcal{O}$.

1.3.1 Elliptic curve over $\mathbb{C}$

An elliptic curve over the complex plane $\mathbb{C}$ is associated to a lattice in $\mathbb{C}$. We will see that an elliptic curve over $\mathbb{C}$ up to isomorphism corresponds to a lattice in $\mathbb{C}$ up to homothety. In particular, a torus, which is the quotient of $\mathbb{C}$ by a lattice, corresponds to an elliptic curve over $\mathbb{C}$.
A *lattice* $\Lambda = [\omega_1, \omega_2]$ in $\mathbb{C}$, which is generated by two complex numbers $\omega_1, \omega_2 \in \mathbb{C}$ that are independent over the real number $\mathbb{R}$, is defined as an additive subgroup

$$\Lambda = \{m\omega_1 + n\omega_2 : m, n \in \mathbb{Z}\}$$

of $\mathbb{C}$. The *fundamental parallelogram* of the lattice Λ is given by the set

$$\mathcal{F}_\Lambda = \{x\omega_1 + y\omega_2 : x, y \in \mathbb{R} \text{ and } 0 \leq x, y < 1\}.$$

Some special functions for a lattice are useful to connect elliptic curves to lattices.

Definition 1.3.1. *Let Λ be a lattice in the complex plane. An elliptic function relative to the lattice $\Lambda = [\omega_1, \omega_2]$ is a meromorphic complex function $g(z)$ on $\mathbb{C}$ which is doubly periodic i.e.*

$$g(z + \omega_1) = g(z) \text{ and } g(z + \omega_2) = g(z).$$

The set of elliptic functions for a lattice $\Lambda = [\omega_1, \omega_2]$ forms a field $\mathbb{C}(\Lambda)$, which is an extension of $\mathbb{C}$. Elliptic function called Weierstrass $\wp$ is used to parameterize elliptic curves over $\mathbb{C}$. Before defining this, we define a series on a lattice Λ called Eisenstein series.

Definition 1.3.2. *The Eisenstein series of weight $k > 2$, an integer, for a lattice Λ is the series*

$$G_k(\Lambda) = \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{\omega^k}.$$

The series $G_k(\Lambda)$ converges absolutely for integers $k > 2$.

Definition 1.3.3. *The Weierstrass $\wp$ function relative to a lattice Λ is defined as*

$$\wp(z) = \wp(z; \Lambda) := \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \right).$$

It is easy to see that the Weierstrass $\wp$ function is holomorphic outside the points of the lattice Λ and has poles of order two at the points of Λ. Every lattice Λ in $\mathbb{C}$ gives an elliptic curve over $\mathbb{C}$.

Theorem 1.3.4. *Let Λ be a lattice. The map*

$$\phi : \mathbb{C}/\Lambda \to E_\Lambda(\mathbb{C}) \subset \mathbb{P}^2_{\mathbb{C}}$$

given by

$$z + \Lambda \mapsto [\wp(z) : \wp'(z) : 1]$$

is an isomorphism of Riemann surfaces that is also an isomorphism of additive groups, where the elliptic curve is given by

$$E_\Lambda : y^2 = 4x^3 - g_2 x - g_3$$

with coefficients

$$\begin{aligned} g_2 =& g_2(\Lambda) = 60G_4(\Lambda) = 60 \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{w^4} \\ g_3 =& g_3(\Lambda) = 140G_6(\Lambda) = 140 \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{w^6} \end{aligned} \tag{1.3}$$

and with the non-zero discriminant

$$\Delta(\Lambda) = g_2^3 - 27g_3^3.$$

Proof. See in [82, Proposition 3.6]. □

This theorem shows that every lattice Λ defines a torus $\mathbb{C}/\Lambda$ and this gives an elliptic curve over $\mathbb{C}$. We will see that the converse is also true, i.e., each elliptic curve over $\mathbb{C}$ is coming from some lattice Λ.
The *j-invariant of a lattice* Λ is defined as the j-invariant of the corresponding elliptic curve $E_\Lambda(\mathbb{C})$, which is given by

$$j(\Lambda) = 1728\frac{g_2(\Lambda)^3}{\Delta(\Lambda)} = 1728\frac{g_2(\Lambda)^3}{g_2(\Lambda)^3 - 27g_3(\Lambda)^2}.$$

Two elliptic curves over $\mathbb{C}$ are *isomorphic* if and only if they have same j-invariants. There is a similar characterizing notion for lattices which is a homothety. Two lattices Λ_1 and Λ_2 are called *homothetic* if $\Lambda_1 = \alpha\Lambda_2$ for some $\alpha \in \mathbb{C}^*$.

Theorem 1.3.5. *Two lattices Λ_1 and Λ_2 are homothetic if and only if they have the same j- invariant.*

Proof. See in [88, Theorem 16.5]. □

Since a j- invariant defines a lattice uniquely up to homothety, we are interested in lattices up to homothety.
Any lattice $[\omega_1, \omega_2]$ is homothetic to a lattice of the form $[1, \tau]$, where τ belongs to the upper half plane $\mathbb{H} = \{z \in \mathbb{C} : \text{Im}\, z > 0\}$. There is a holomorphic map on the upper half plane called j function, which identifies all the lattices in $\mathbb{C}$ up to homothety.

Definition 1.3.6. *The j function $j : \mathbb{H} \to \mathbb{C}$ is defined as $j(\tau) = j([1, \tau])$. Similarly, the coefficients of the elliptic curve corresponding to the lattice $[1, \tau]$ given in Equation 1.3 are defined as*

$$g_2(\tau) = g_2([1, \tau]) \text{ and } g_3(\tau) = g_3([1, \tau]).$$

The j function is invariant under the action of special linear group.
The *modular group*

$$\Gamma = \text{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z} : ad - bc = 1 \right\},$$

is generated by two matrices $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, acts on the upper half plane $\mathbb{H}$ via linear fractional transformation as

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = \frac{a\tau + b}{c\tau + d}.$$

The j function is uniquely determined up to an equivalence class of $\mathbb{H}/\Gamma$.

Theorem 1.3.7. *The j function is holomorphic on $\mathbb{H}$. Moreover, for $\tau_1, \tau_2 \in \mathbb{H}$, $j(\tau_1) = j(\tau_2)$ if and only if $\tau_1 = \gamma\tau_2$ for some $\gamma \in \Gamma$.*

Proof. See in [28, Theorem 11.2]. □

In particular, j function is invariant under the action of the modular group Γ.

Theorem 1.3.8. *The fundamental region for $\mathbb{H}/\Gamma$ is given by*

$$\mathcal{F}_\Gamma = \{\tau \in \mathbb{H} : |Re(\tau)| \leq 1/2 \text{ and } |\tau| \geq 1\}.$$

The restriction of the j function to the fundamental region: $j|_{\mathcal{F}_\Gamma} \to \mathbb{C}$ is a bijection.

Proof. See in [83, Theorem 4.1]. □

For each j-invariant in $\mathbb{C}$, there exists an elliptic curve of that j-invariant. Since the complex place $\mathbb{C}$ is in bijection with the fundamental region $\mathcal{F}_\Gamma$, the points in the fundamental region represent all the elliptic curves over $\mathbb{C}$ up to isomorphism. Therefore, the following theorem known as uniformization theorem follows from Theorem 1.3.8.

Theorem 1.3.9. *For every elliptic curve E over the complex number $\mathbb{C}$, there exists a lattice Λ such that E is isomorphic to the elliptic curve $\phi(\mathbb{C}/\Lambda) := E_\Lambda$, where ϕ is the isomorphism defined in Theorem 1.3.4.*

1.3.2 Maps of complex tori

Let Λ_1, Λ_2 be latices in $\mathbb{C}$. Let $\alpha \in \mathbb{C}$ such that $\alpha\Lambda_1 \subset \Lambda_2$. Then the scalar multiplication by α map $m_\alpha : z \to \alpha z$ induces a well-defined holomorphic group homomorphism

$$\phi_\alpha : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$$

given by

$$z + \Lambda_1 \mapsto \alpha z + \Lambda_2.$$

The following theorem shows that a choice of a complex number α such that $\alpha\Lambda_1 \subset \Lambda_2$ is equivalent to a choice of holomorphic map between the tori $\mathbb{C}/\Lambda_1, \mathbb{C}/\Lambda_2$ preserving the zero element and this is equivalent to a map between the corresponding elliptic curves $E_{\Lambda_1}, E_{\Lambda_2}$.

Theorem 1.3.10. *Let $\Lambda_1, \Lambda_2 \subset \mathbb{C}$ be two lattices.*

1. *The map*

$$\{\alpha \in \mathbb{C} : \alpha\Lambda_1 \subset \Lambda_2\} \to \{ \text{holomorphic maps } \phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2 \text{ with } \phi(0) = 0\}$$
$$\alpha \mapsto \phi_\alpha$$

   is an isomorphism of additive groups and for $\Lambda_1 = \Lambda_2$ this is an isomorphism of commutative ring.

2. *Let E_{Λ_1} and E_{Λ_2} be elliptic curves corresponding to lattices Λ_1 and Λ_2 respectively, then there is one to one correspondence between*

$$Hom(E_{\Lambda_1}, E_{\Lambda_2}) \to \{ \text{holomorphic maps } \phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2 \text{ with } \phi(0) = 0\}.$$

Proof. See in [82, Theorem 5.3]. □

Furthermore, two elliptic curves E_{Λ_1} and E_{Λ_2} corresponding to lattices $\Lambda_1, \Lambda_2 \subset \mathbb{C}$ respectively are isomorphic over $\mathbb{C}$ if and only if Λ_1 and Λ_2 are homothetic. See Figure 1.2.

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{m_\alpha} & \mathbb{C} \\ \downarrow{\scriptstyle \pi_1} & & \downarrow{\scriptstyle \pi_2} \\ \mathbb{C}/\Lambda_1 & \xrightarrow{\phi_\alpha} & \mathbb{C}/\Lambda_2 \\ \downarrow{\scriptstyle \cong} & & \downarrow{\scriptstyle \cong} \\ E_{\Lambda_1} & \xrightarrow{\phi} & E_{\Lambda_2} \end{array}$$

Figure 1.2: Map between tori and corresponding map between elliptic curves.

1.3.3 Complex multiplication

For a lattice Λ and the corresponding elliptic curve E relative to Λ, Theorem 1.3.10 implies that

$$\{\alpha \in \mathbb{C} : \alpha\Lambda \subset \Lambda\} \cong \text{End}(E).$$

Endomorphism ring for such an elliptic curve E over $\mathbb{C}$ is an order $\mathcal{O}$ in an imaginary quadratic field K. By an *order*, we mean a subring of K that is a free $\mathbb{Z}$ module of rank 2, therefore it is both a lattice and a subring of K.

Definition 1.3.11. *Let $\mathcal{O}$ be an order in an imaginary quadratic field K then two $\mathcal{O}$-ideals $\mathfrak{a}$ and $\mathfrak{b}$ are said to be equivalent if they are homothetic as lattices, more precisely, $\mathfrak{a} = \lambda\mathfrak{b}$ for $\lambda \in K^*$. This can be written as $\alpha\mathfrak{a} = \beta\mathfrak{b}$ for some non-zero $\alpha, \beta \in \mathcal{O}$.*

An elliptic curve of endomorphism ring $\mathcal{O}$ is called an elliptic curve with *complex multiplication (CM)* by $\mathcal{O}$. For any $\mathcal{O}$-ideal $\mathfrak{a}$, the set

$$\mathcal{O}_\mathfrak{a} := \{\alpha \in K : \alpha\mathfrak{a} \subset \mathfrak{a}\}$$

is an order in K. The ideal $\mathfrak{a}$ is called *proper* if $\mathcal{O}_\mathfrak{a} = \mathcal{O}$. In fact, the proper ideals are the invertible ideals, where an $\mathcal{O}$-ideal $\mathfrak{a}$ is called *invertible* if there exists an $\mathcal{O}$-ideal $\mathfrak{a}^{-1}$ such that $\mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}$. Equivalence classes of such ideals form a multiplicative group called class group.

Definition 1.3.12. *Let $\mathcal{O}$ be an order in an imaginary quadratic field K. Then the set of proper $\mathcal{O}$-ideals up to equivalence form a multiplicative group called the class group and is denoted as $cl(\mathcal{O})$.*

Each of the element in the class group $cl(\mathcal{O})$ corresponds to a CM elliptic curve over $\mathbb{C}$ by $\mathcal{O}$.

Theorem 1.3.13. *Let $\mathcal{O}$ be an order in an imaginary quadratic field. Each ideal class in the class group $cl(\mathcal{O})$ represents a homothetic class of lattice Λ in $\mathbb{C}$ such that the corresponding elliptic curve E_Λ has endomorphism ring $\mathcal{O}$; conversely if E_Λ is an isomorphic class of elliptic curve obtained from a homothetic class of lattice Λ, then Λ is homothetic to an element of $cl(\mathcal{O})$.*

Proof. Follows from Theorem 1.3.4 and [28, Corollary 10.20]. □

This theorem gives a bijection, given by $\mathfrak{a} \mapsto j(\mathfrak{a})$, between the class group $cl(\mathcal{O})$ and the set of elliptic curves over $\mathbb{C}$ whose endomorphism ring is $\mathcal{O}$. Finiteness of the class group implies that the set of all elliptic curves over $\mathbb{C}$ whose endomorphism ring are $\mathcal{O}$ is also finite. In fact, more is true. For an imaginary quadratic order $\mathcal{O}$, denote

$$\mathcal{E}_{\mathcal{O}}(\mathbb{C}) = \{j(E) : E \text{ is defined over } \mathbb{C} \text{ and } \mathrm{End}(E) = \mathcal{O}\}.$$

Then the class group $cl(\mathcal{O})$ acts on $\mathcal{E}_{\mathcal{O}}(\mathbb{C})$ and is defined as follows. Let E be such that $j(E) \in \mathcal{E}_{\mathcal{O}}(\mathbb{C})$ and $\mathfrak{a} \in cl(\mathcal{O})$. It is enough to define the action of $\mathfrak{a}$ on E. There exists a lattice $\Lambda \subset \mathbb{C}$ such that $E = E_\Lambda$ by Theorem 1.3.9. Also from Theorem 1.3.13, there exists an ideal class $\mathfrak{b} \in cl(\mathcal{O})$ homothetic to Λ as an ideal and hence $E = E_{\mathfrak{b}}$.
Let $\mathfrak{a}$ be an integral representation of an ideal class. Then the ideal $\mathfrak{a}^{-1}\mathfrak{b}$ belongs to $cl(\mathcal{O})$ and satisfies $\mathfrak{a}^{-1}\mathfrak{b} \supset \mathfrak{b}$. There exists an elliptic curve say $E_{\mathfrak{a}^{-1}\mathfrak{b}}$ corresponding to the ideal $\mathfrak{a}^{-1}\mathfrak{b}$. Define the action of $\mathfrak{a}$ on $E_{\mathfrak{b}}$ as

$$\mathfrak{a} \star E_{\mathfrak{b}} := E_{\mathfrak{a}^{-1}\mathfrak{b}}$$

and in terms of elements of $\mathcal{E}_{\mathcal{O}}(\mathbb{C})$

$$\mathfrak{a} \star j(E_{\mathfrak{b}}) = j(E_{\mathfrak{a}^{-1}\mathfrak{b}}).$$

This is a group action of $cl(\mathcal{O})$ on $\mathcal{E}_{\mathcal{O}}(\mathbb{C})$. Furthermore, for any proper $\mathcal{O}$-ideals $\mathfrak{a}$ and $\mathfrak{b}$, $\mathfrak{a} \star j(E_{\mathfrak{b}}) = j(E_{\mathfrak{a}^{-1}\mathfrak{b}}) = j(E_{\mathfrak{b}})$ if and only if $\mathfrak{b}$ is homothetic to $\mathfrak{a}^{-1}\mathfrak{b}$ by theorem 1.3.7. This gives $\mathfrak{a}$ is principal and hence the action is free.

Theorem 1.3.14. *The action of a class group $cl(\mathcal{O})$ of an imaginary order $\mathcal{O}$ on the set $\mathcal{E}_{\mathcal{O}}(\mathbb{C})$ of elliptic curves that have CM by $\mathcal{O}$ is transitive and free.*

Proof. Follows from the above observations and from Theorem 1.3.13. □

If there is a group action on a set which is both transitive and free then the set is called a *principal homogeneous space*. Therefore, the set $\mathcal{E}_{\mathcal{O}}(\mathbb{C})$ is a

principal homogeneous space or also called $cl(\mathcal{O})$-torsor.

Considering $\lambda = 1$, the inclusion $\lambda\mathfrak{b} \subset \mathfrak{a}^{-1}\mathfrak{b}$ corresponds to a holomorphic map $\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ with $\phi(0) = 0$, where $\Lambda_1 \sim \mathfrak{b}$, $\Lambda_2 \sim \mathfrak{a}^{-1}\mathfrak{b}$ and $\sim$ denote homothety. This corresponds to an isogeny

$$\phi_{\mathfrak{a}} : E_{\mathfrak{b}} \to E_{\mathfrak{a}^{-1}\mathfrak{b}} = \mathfrak{a} \star E_{\mathfrak{b}}.$$

The kernel and the degree of the isogeny $\phi_{\mathfrak{a}}$ are given by a torsion subgroup and the norm of the ideal $\mathfrak{a}$ respectively by Theorem 1.3.16. Before presenting this theorem, we give a definition.

Definition 1.3.15. *Let E be such that $j(E) \in \mathcal{E}_{\mathcal{O}}(\mathbb{C})$. For any $\mathcal{O}$-ideal $\mathfrak{a}$, the $\mathfrak{a}$-torsion subgroup of E is denoted as $E[\mathfrak{a}]$ and is defined as*

$$E[\mathfrak{a}] = \{P \in E(\mathbb{C}) : \alpha(P) = 0 \text{ for all } \alpha \in \mathfrak{a}\}.$$

Theorem 1.3.16. *Let E be an elliptic curve over $\mathbb{C}$ such that $j(E) \in \mathcal{E}_{\mathcal{O}}(\mathbb{C})$. Let $\mathfrak{a}$ be a proper ideal of $\mathcal{O}$ and $\phi_{\mathfrak{a}} : E \to \mathfrak{a} \star E$ be an isogeny. Then the kernel of $\phi_{\mathfrak{a}}$ is $E[\mathfrak{a}]$ and the degree of $\phi_{\mathfrak{a}}$ is the norm of $\mathfrak{a}$.*

Proof. See in [88, Theorem 18.14]. □

Similar properties also hold when elliptic curves are defined over a finite field. Let $\mathcal{O}$ be an order in an imaginary quadratic field $\mathbb{Q}[\sqrt{d_\pi}]$, where d_K is a negative integer. Denote

$$\mathcal{E}_{\mathcal{O}}(\mathbb{F}_p) = \{j(E) : E \text{ is defined over } \mathbb{F}_p \text{ and } \mathrm{End}(E) = \mathcal{O}\}.$$

The following theorem gives the action of the class group $cl(\mathcal{O})$ on the set $\mathcal{E}_{\mathcal{O}}(\mathbb{F}_p)$.

Theorem 1.3.17. *Let $\mathbb{F}_p$ be a finite field. Let $\mathcal{O}$ be an order of an imaginary quadratic field. If the set $\mathcal{E}_{\mathcal{O}}(\mathbb{F}_p)$ is non empty then the action of $cl(\mathcal{O})$ on $\mathcal{E}_{\mathcal{O}}(\mathbb{F}_p)$ is transitive and free.*

Isogeny graph

Let $\mathbb{F}_p$ be a finite field. We can define a relation in the set of isomorphic classes of an elliptic curve over $\overline{\mathbb{F}}_p$ as $E_1 \sim E_2$ if there exists an isogeny between them. This relation is, in fact, an equivalence relation because for each isogeny, there exists a unique dual isogeny by Theorem1.2.21, and we can compose two isogenies. Furthermore, from Theorem 1.2.24 each equivalence class either contains only ordinary elliptic curves or only supersingular elliptic curves. Isogeny graph is usually constructed by fixing a prime ℓ.

Definition 1.3.18. *Let $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ be a graph whose vertex set consists of the $\overline{\mathbb{F}}_p$-isomorphism classes of elliptic curve over $\overline{\mathbb{F}}_p$ and edges set consists of the ℓ isogenies between them that are defined over $\overline{\mathbb{F}}_p$.*

1.4 Isogeny based cryptography

Isogeny based cryptography has a relatively short history, which started with a work of Couveignes titled "hard homogeneous space" in 1996 [27]. Later the hard homogeneous space was upgraded as a post-quantum Diffie Hellman key exchange independently by Rostovtsev and Stolbunov in 2006 and also in 2010 [75, 87], now it is known as the CRS scheme. A hash function by Charles, Goren, and Lauter in 2009 [21] is also considered as one of the initiators of the isogeny based cryptography. An efficient key exchange protocol has been developed by Jao and De Feo in 2011, known as Supersingular Isogeny Diffie Hellman (SIDH), and an extended version including a zero-knowledge identification scheme in 2013 by De Feo, Jao and Plût. An improvement in the CRS scheme was proposed in 2018 [31] as a step towards a practical scheme. Another milestone to efficient isogeny-based cryptography after SIDH is the key exchange scheme by Castryck, Lange, Martindale, Panny, and Renes known as Commutative SIDH (CSIDH) in 2018. Besides these, many other isogeny primitives including signature schemes for example GPS [51], SeaSign [30], Csi-fish [12], SQISign [46] etc and a verifiable delay function [32] have come to the literature.
There are some existing attacks for isogeny schemes, for example, an algorithm by Kohel, Lauter, Petit, and Tignol (KLPT) [59], an attack by Petit to tackle some variants of isogeny problems [71] and its improvement by Kutas, Martindale, Panny, Petit, and Stange [61], which we will discuss briefly later in Chapter 3.

1.4.1 Introduction to public key cryptography

As the name suggests, public-key cryptography uses some public keys that are accessed to everyone, and only private keys are kept private. Public key encryption and digital signature are the main application of public-key cryptography. A seminal paper entitled "New Directions in cryptography" [36] by Diffie and Hellman opened a door of the public key cryptography in 1976 by proposing a key exchange protocol known as Diffie-Hellman (DH) key exchange based on the difficulty of discrete logarithm problem. In both encryption and digital signature, a key exchange scheme is required.

A key exchange scheme is a key sharing mechanism between the communicating parties that helps to agree on a secret key through a public channel.

Diffie Hellman Key Exchange

Diffie-Hellman (DH) key exchange uses a commutative cyclic group, say $(G, \star)$, generated by an element g of a prime order q. Two parties, Alice and Bob, want to agree on a common key through an insecure channel. They first agree on the cyclic group G with a generator g. Alice and Bob choose random numbers K_A and K_B respectively from $\mathbb{F}_q^*$, which is a set of non-zero elements of a finite field of q elements. Alice computes

$$K_A g := \underbrace{g \star g \star \ldots \star g}_{K_A \text{ times}}$$

and sends it to Bob. Bob computes

$$K_B g := \underbrace{g \star g \star \ldots \star g}_{K_B \text{ times}}$$

and sends to Alice. Now, getting each others public keys, both of them get the common secret key

$$S := K_A(K_B g) = K_B(K_A g),$$

where Alice computes $K_A(K_B g)$ and Bob computes $K_B(K_A g)$. The private keys K_A and K_B are secure due to the difficulty of discrete logarithm problem: find K_A from the knowledge of g and $K_A g$ or similarly find K_B from g and $K_B g$.
The common secret key S is secure because of the following problems.

- Decisional Diffie-Hellman problem (DDH) : distinguish the two probability distribution $(K_A g, K_B g, S)$ and $(K_A g, K_B g, K_r g)$ for any random integers $1 \leq K_A, K_B, K_r \leq q$.
- Computational Diffie-Hellman problem (CDH): compute the common key S form the knowledge $K_A g$ and $K_B g$ in the above setting of the key exchange.

Sometimes a comparison can be done between the problems by observing how one affects another. A notion of reduction of a problem is useful in this situation.

Definition 1.4.1. *A problem P_1 is said to reduce to another problem P_2 if to solve a problem P_1, the instance of P_1 can be transformed to the instance of problem P_2 and the solution of P_2 can again be transformed to a solution of problem P_1. It is denoted as $P_1 \leq_R P_2$.*

If $P_1 \leq_R P_2$ then we can say that the problem P_1 is no harder than P_2. For example, the following lemmas are easy-to-prove reductions.

Lemma 1.4.2. *CDH $\leq_R$ DLP.*

Solution of DLP gives a solution to CDH. Therefore, CDH is no harder than DLP.

Lemma 1.4.3. *DDH $\leq_R$ CDH.*

Proof. If there is an algorithm to solve CDH. Then the distribution for DDH can be easily determined. □

Therefore, DDH is no harder than CDH.

A reduction of a discrete logarithm problem to a computational Diffie-Hellman problem is a non-trivial reduction.

Lemma 1.4.4. *[64] DLP $\leq_R$ CDH.*

Encryption scheme

A message can be kept secure by encryption, which changes a message into an unintelligible form called ciphertext by using some keys. Only the party who knows the private key can decrypt the ciphertext and gets the original message. Mainly, an encryption scheme can be divided into three steps: key generation, where users generate keys; encryption, where sender encrypts messages into ciphertext; and decryption, where receiver decrypts the ciphertext and get the original message. Besides the communicating parties, we always suppose a malevolent entity called adversary or attacker whose aim is to obtain private information using the available data.
Security of encryption relies on the following properties :

- One way encryption (OWE): Encryption should be one way, i.e., given a ciphertext c, it should not be able to compute its corresponding message.
- Semantic security: No information on the message can be retrieved from its ciphertext.

- Indistinguishability (IND): An adversary should not be able to distinguish the encryption of any two same length messages.

Mainly, there are the following strategies (attack models) of an adversary.

- Passive attack/ chosen plaintext attack (CPA): An attacker can choose random plaintexts and get corresponding ciphertexts. With this information, the aim is to obtain information related to encryption.
- Lunchtime attack (CCA1): An attacker can ask for decryption of ciphertext until a certain time i.e. until a challenge ciphertext is received.
- Adaptive chosen ciphertext attack (CCA): Attacker can ask for decryption to any chosen ciphertext before or after a challenge ciphertext is received except the challenge ciphertext itself.

Any attack strategy can be applied to any one of the above-mentioned security properties. For example, if encryption is secure from the CCA (respectively CPA) model of attack to indistinguishability (IND) then the encryption is called IND-CCA (respectively IND-CPA) secure.

A public-key encryption method derived from DH key exchange was proposed by Elgamal in 1985 known as ElGamal encryption scheme [40]. We briefly describe the ElGamal system in order to give an example of an encryption scheme.
A cyclic group $(G, \star)$ of order q, a prime number, of generator g is known to both Alice and Bob who are the communicating parties. Suppose Bob wants to send a message m to Alice.
Key generation. Alice generates her private and public keys as follows

- Samples uniformly random $A_S \in \mathbb{F}_q^*$ and computes $A_P = A_S g$.
- Public key is A_P and A_S is the secret key.

Encryption. Bob encrypts a message into a ciphertext.

- Changes a message into an element m of G by a known bijective mapping $f : \mathcal{M}_m \to G$, where $\mathcal{M}_m$ is the message space containing all the possible messages.
- Samples uniformly random $B_S \in \mathbb{F}_q^*$ and computes the common secret $S = B_S A_P$.
- Computes $C_1 = B_S g$, $C_2 = mS$.

- The ciphertext is the pair $C = (C_1, C_2)$.

Bob sends C to Alice.
Decryption. Alice decrypts the ciphertext C as follows

- Computes the common secret $S = A_S C_1 = A_S B_S g$.
- Computes the inverse of $S \in G$ which is S^{-1}. Computes $m = C_2 \star S^{-1}$, this gives message because

$$C_2 \star S^{-1} = (mS) \star S^{-1} = m \star 1_G = m,$$

  where 1_G is the identity element of the group G.
- Retrieves the message by using the known map $f^{-1} : G \to \mathcal{M}_m$.

Digital signature

A document or message that is sent to a receiver may not be in an original form, not been sent by the right person, or there might be some issues that can make the receiver suspect on both the message and the sender. A digital signature is a mathematical scheme that proves the identity of the sender, checks the integrity of data without allowing the signer to deny his/her involvement in the signature generation. A valid digital signature must satisfy the following properties.

1. **Authenticity:** It should verify that the message or document is sent by the right person, not by a defrauder.
2. **Unforgeability:** A signature forgery is a capability of creating a pair of a message and a valid signature to that message different from the signature generated by the authentic signer. The digital signature should prevent such possibility of forging a signature. There are mainly the following types of forgeries:
   i. Existential Forgery: The adversary can forge at least one signature to a message of his choice.
   ii. Selective Forgery: The adversary succeeds in forging the signature to the message chosen by the challenger before the attack.
   iii. Universal Forgery: The adversary is able to produce a valid signature of any given message but not the secret key.
   iv. Total Break: The adversary can compute the signers secret key.

3. **Non-repudiation:** After a message is signed, the signer can not later be denied his involvement.

4. **Integrity:** It ensures that the message has not been changed before reaching to the receiver.

There are many signature schemes which can be used to produce valid signatures. Mainly, the signature scheme consists of three stages: key generation, signing, and verification. As an example of a valid signing method, here we describe a method by Elgamal [40].
Elgamal signature:
Global parameters. These are parameters known to both signer and verifier.

- A collision resistant hash function $\mathcal{H}$.
- A cyclic group $\mathbb{F}_q^* = \langle g \rangle$, where q is a prime number.

Key generation:

- Sample uniformly randomly A_S in $1 < A_S < q - 1$.
- Compute $A_P = g^{A_S} \in \mathbb{F}_q$.
- Public key A_P and secret key is A_S.

Signing: Let m be a message to be signed.

- Sample uniformly randomly B_S in $0 < B_S < q - 1$ with $\gcd(B_S, p - 1) = 1$.
- Compute $S_1 = g^{B_S} \in \mathbb{F}_q$ and $S_2 = (\mathcal{H}(m) - A_S S_1) B_S^{-1} \mod (p - 1)$.
- Ensure $S_2 \not\equiv 0 \mod (p - 1)$, otherwise repeat with new value B_S.
- The pair $S = (S_1, S_2)$ is the signature.

Verification: Accept the signature if the following conditions are satisfied.

- $S_1 \in \mathbb{F}_q^*$ and $0 < S_2 < p - 1$.
- $g^{\mathcal{H}(m)} = A_P^{S_1} S_1^{S_2}$ in $\mathbb{F}_q$.

Otherwise reject the signature.
Why verification works ? Since $\mathcal{H}(m) = B_S S_2 + A_S S_1 \mod (p-1)$,

$$g^{\mathcal{H}(m)} = g^{B_S S_2 + A_S S_1} = (g^{A_S})^{S_1}(g^{B_S})^{S_2} = A_P^{S_1} S_1^{S_2} \text{ in } \mathbb{F}_q.$$

A forgery might be done either by the private key, which is safe by the difficulty of discrete logarithm problem, or by finding collision in the hash function $\mathcal{H}$ i.e. $\mathcal{H}(m_1) = \mathcal{H}(m_2) \mod (p-1)$, which is not possible because $\mathcal{H}$ is a collision resistant hash function.

1.4.2 Complexity notation

We use the term *complexity* of an algorithm $\mathcal{A}$ to mean the computational steps required to perform a task by the algorithm $\mathcal{A}$. The asymptotic steps are expressed with a function in terms of the input size. Big $\mathbb{O}$ notation is used to formalize the *worst-case complexity*, which is the maximum number of steps required by $\mathcal{A}$ and is bounded by a function.
Let $g(n)$ be the number of steps required to run an algorithm, where the argument n is the size of the input, and f is a positive integer valued function then

$$g(n) = \mathbb{O}(f(n))$$

and read as $g(n)$ is big $\mathbb{O}$ of $f(n)$ if there exists a positive integer c and a non negative integer k such that

$$g(n) \leq cf(n) \quad \forall n \geq k.$$

Big $\mathbb{O}$ tilde notation is used to ignore logarithmic factors

$$\mathbb{O}(f(n)\log^k n) = \tilde{\mathbb{O}}(f(n)).$$

An algorithm is called an *efficient algorithm* if its worst-case complexity is polynomial function in an input size.

1.4.3 SIDH and its variants

Supersingular Isogeny Diffie-Hellman (SIDH) is a post-quantum key exchange protocol which was developed by Jao and De Feo in 2011 [56]. This is the only one isogeny scheme that was submitted in a competition of post-quantum cryptography standardization by NIST in the name Supersingular Isogeny Key Encapsulation (SIKE) [6] after modifying it as a key encapsulation mechanism, which is now included in the list of third-round

alternate candidates. Here we briefly describe the SIDH key exchange protocol.
SIDH uses supersingular isogeny graph, where the vertices are the j-invariants of supersingular elliptic curves over $\mathbb{F}_q$ with $q = p^2$. A special prime of the form $p = p_A^{n_1} p_B^{n_2} f \pm 1$ is used. Alice takes a random walk of length n_1 in the supersingular isogeny graph $\mathcal{G}_{p_A}(\overline{\mathbb{F}}_q)$ and Bob takes a random walk of length n_2 in the supersingular isogeny graph $\mathcal{G}_{p_B}(\overline{\mathbb{F}}_q)$. The goal is to reach at the same vertex in $\mathbb{F}_q$ efficiently. A choice of a random walk of length n_1 is equivalent to a choice of a random cyclic subgroup $\langle H_1 \rangle$ of $E[p_A^{n_1}]$ of order $p_A^{n_1}$ because a subgroup defines a separable isogeny uniquely. Similarly, Bob chooses a cyclic subgroup $\langle H_2 \rangle$ of $E[p_B^{n_2}]$ of order $p_B^{n_2}$ to define a random walk of length n_2. Then the group $\langle H_1, H_2 \rangle$ is a cyclic group of order $p_A^{n_1} p_B^{n_2}$ which determines an isogeny walk, driving both Alice and Bob to the same place i.e. to the same j-invariant in $\mathbb{F}_q$.

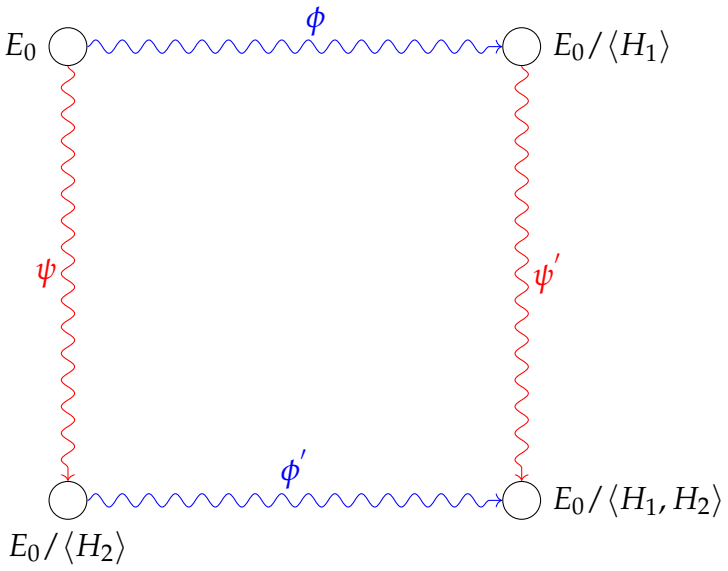

Figure 1.3: Commutative diagram representing the isogeny paths constructed by Alice and Bob.

The selection of the prime $p = p_A^{n_1} p_B^{n_2} f \pm 1$ gives the structure of the elliptic curve as

$$E(\mathbb{F}_q) \simeq (\mathbb{Z}/(p \mp 1)\mathbb{Z})^2 \simeq (\mathbb{Z}/p_A^{n_1}\mathbb{Z})^2 \oplus (\mathbb{Z}/p_B^{n_2}\mathbb{Z})^2 \oplus (\mathbb{Z}/f\mathbb{Z})^2$$

by Theorem 1.2.18. In particular $E[p_A^{n_1}], E[p_B^{n_2}] \subset E(\mathbb{F}_q)$. Therefore the subgroups $\langle H_1 \rangle$ and $\langle H_2 \rangle$ are defined over $\mathbb{F}_q$. In fact, there are $p_A^{n_1 - 1}(p_A + 1)$

cyclic subgroups of $E[p_A^{n_1}] \subset E(\mathbb{F}_q)$ of order $p_A^{n_1}$ and hence each of this subgroup defines unique separable isogeny of degree $p_A^{n_1}$. This shows that an isogeny path for Alice and Bob can be represented by a single group element defined over $\mathbb{F}_q$. Therefore, this choice of prime gives an efficient representation of the chosen isogeny walk. Commutative diagram 1.3 is applicable if there is a way to start a path from $E_0/\langle H_1\rangle$ and $E_0/\langle H_2\rangle$ leading to the same curve $E_0/\langle H_1, H_2\rangle$. The authors found a smart way to do this. We describe this idea together with the precise way to generate parameters.

Parameters that are publicly known include the prime $p = p_A^{n_1} p_B^{n_2} f \pm 1$, a finite field $\mathbb{F}_q$ with $q = p^2$, and a supersingular elliptic curve E_0. Moreover, the bases $\{P_A, Q_A\}$ and $\{P_B, Q_B\}$ of $E[p_A^{n_1}]$ and $E[p_B^{n_2}]$ respectively are also public keys.
Alice chooses two random integers $0 \leq a_1, a_2 \leq p_A^{n_1}$ with $\gcd(p_A^{n_1}, a_1) = 1$ or $\gcd(p_B^{n_2}, a_2) = 1$ and construct a random cyclic group $\langle H_1\rangle = \langle a_1 P_A + a_2 Q_A\rangle$ of E_0 of order $p_A^{n_1}$. Suppose the corresponding isogeny be $\phi : E_0 \to E_A = E_0/\langle H_1\rangle$ with kernel $\langle H_1\rangle$ and codomain is the curve E_A. An insight of the Jao-De Feo to make Diffie Hellman like key exchange is to use the images of the torsion points of each other's secret isogeny. Therefore, Alice computes the images $\phi(P_B), \phi(Q_B)$ on her private isogeny ϕ and sends $E_A, \phi(P_B), \phi(Q_B)$ to Bob.
Similarly, Bob chooses $0 \leq b_1, b_2 \leq p_B^{n_2}$ with $\gcd(p_B^{n_2}, b_1) = 1$ or $\gcd(p, b_2) = 1$, and $\langle H_2\rangle = \langle b_1 P_B + b_2 Q_B\rangle$ of E_0 of order $p_B^{n_2}$, an isogeny $\psi : E_0 \to E_B = E_0/\langle H_2\rangle$ with kernel $\langle H_2\rangle$ and codomain E_B. Bob sends his public keys, which are $E_B, \psi(P_A), \psi(Q_A)$ to Alice.
After getting each other's public keys, Alice computes the isogeny $\phi' : E_B \to E_B/\langle\psi(H_1)\rangle$; Bob computes the isogeny $\psi' : E_A \to E_A/\langle\phi(H_2)\rangle$. It is possible to calculate the image of Alice's (Bob's) secret subgroup by Bob's (Alice's) secret isogeny.

$$\begin{aligned}\langle\psi(H_1)\rangle &= \langle\psi(a_1 P_A + a_2 Q_A)\rangle = \langle a_1\psi(P_A) + a_2\psi(Q_A)\rangle \\ \langle\phi(H_2)\rangle &= \langle\phi(b_1 P_B + b_2 Q_B)\rangle = \langle b_1\phi(P_B) + b_2\phi(Q_B)\rangle.\end{aligned}$$

Both of them get an isomorphism class of elliptic curve $E_A/\phi(\langle H_2\rangle) \simeq E_B/\psi(\langle H_1\rangle)$. Since an isomorphism class of an elliptic curve is identified uniquely by the j-invariant, the j-invariant $j(E_A/\langle\phi(H_1)\rangle) = j(E_B/\langle\phi(H_2)\rangle)$ is the common key. See Figure 1.4.

Hardness assumption of SIDH. A solution of Problem 3.1.1 can be used to break the SIDH. But, the security of SIDH is mainly based on the

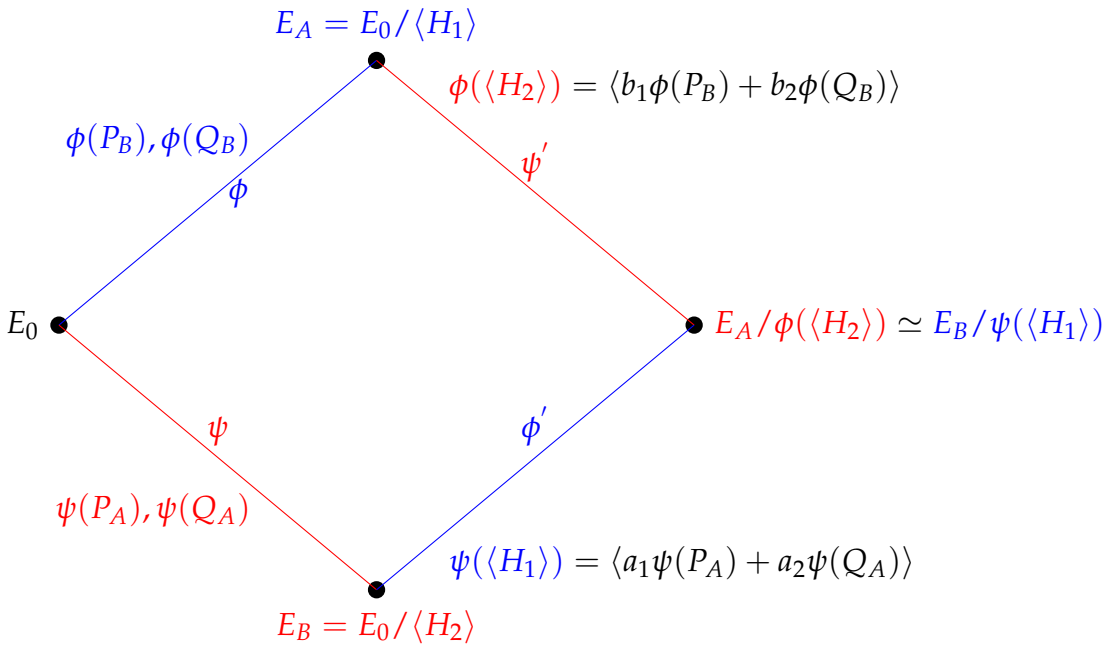

Figure 1.4: Commutative diagram showing the computation of Alice and Bob.

following problem called Supersingular Decision Diffie-Hellman (SSDDH) problem.

Problem 1.4.5. *(SSDDH.) Let $E_0, p_A, p_B, n_1, n_2, P_A, Q_A, P_B, Q_B$ be the parameters chosen for SIDH system with $p_A \neq p_B$ and $p_A^{n_1} \approx p_B^{n_2}$.*
The problem is to determine the distribution of a given tuple that is sampled with probability $1/2$ from one of the following two distributions:

1. $(E_0/\langle H_1 \rangle, \phi(P_B), \phi(Q_B), E_0/\langle H_2 \rangle, \psi(P_A), \psi(Q_A), E_0/\langle H_1, H_2 \rangle)$ *, where*
   - $H_1 \in E_0(\mathbb{F}_q)$ *is a uniformly random point of order* $p_A^{n_1}$*,*
   - $H_2 \in E_0(\mathbb{F}_q)$ *is a uniformly random element of order* $p_B^{n_2}$*,*
   - $\phi : E_0 \to E_0/\langle H_1 \rangle$ *is the isogeny of kernel* $\langle H_1 \rangle$*, and*
   - $\phi : E_0 \to E_0/\langle H_2 \rangle$ *is the isogeny of kernel* $\langle H_2 \rangle$*;*
2. $(E_0/\langle H_1 \rangle, \phi(P_B), \phi(Q_B), E_0/\langle H_2 \rangle, \psi(P_A), \psi(Q_A), E_0/\langle G \rangle)$ *, where* $G \in E_0(\mathbb{F}_q)$ *is a uniformly random point of order* $p_A^{n_1} p_B^{n_2}$*.*

As far as we know, there is only exponential time algorithm to solve SSDDH problem even on the quantum computer.

Variants of SIDH

In SIDH, the elliptic curves in the isogeny walks taken by Alice and Bob are shorter than the walks between any two random curves. For example, Alice has $p_A^{n_1-1}(p_A+1) \approx p^{1/2}$ possible options for E_A. Since there are around $p/12$ supersingular elliptic curves over $\mathbb{F}_q$ with $q = p^2$ by Theorem 1.2.23, the meet at middle approach can determine a path between any two generic elliptic curves in complexity $\tilde{\mathrm{O}}(\sqrt{p})$. But in case of SIDH, there are $\sqrt{p}$ possible elliptic curves between, for example, E_0 and E_A, therefore the meet at middle approach can find a path between them in $O(\sqrt[4]{p})$.
For some choices of parameters, the elliptic curves of Alice and Bob can be selected as the generic elliptic curves that look like uniformly random. In [71], Petit mentioned two variants of SIDH: unbalanced degree and optimal degree variant according to the parameters, and proposed a polynomial-time attack technique on these variants using the torsion point images, which we will discuss in Chapter 3.

Unbalanced degree variant: Parameters used in SIDH are balanced ones i.e. $p_A^{n_1} \approx p_B^{n_2}$, which manages the same level of security to both the parties Alice and Bob. But, there are some situations where one party may require more security than other. Unlike SIDH parameters, in unbalanced variant the prime powers $p_A^{n_1}$ and $p_B^{n_2}$ are chosen such that one of them is larger than other, for example, $p_A^{n_1} \ll p_B^{n_2}$.

Optimal degree variant: In SIDH, the public curves E_A and E_B are not uniformly random in isogeny graph. In optimal degree variant, $p_A^{n_1}$ and $p_B^{n_2}$ are increased to around $\approx p^2$ so as to sample E_A and E_B uniformly random. This also gives freedom to choose two powersmooth (each divisor is less than fixed integer bound) numbers N and M in place of the two prime powers $p_A^{n_1}$ and $p_B^{n_2}$.

1.4.4 Cryptography from hard homogeneous space

Consider a commutative group G acting on a set X freely and transitively and the action is written as gx for $g \in G$ and $x \in X$. Then the set X is called a principal homogeneous space. By looking only at the elements of the set X, the action of G on X is not visible but for each $x, y \in X$ there exists the unique $g \in G$ such that $y = gx$. Couveignes defined in [27], as a homogeneous space is considered a *hard homogeneous space* if the following operations :

- given two any elements g, h check whether they belong to G or not; if yes, check their equality. For example, an equality between $g, h \in G$ can be determined by first computing g^{-1} and checking $g^{-1}h$ is the identity 1_G of G or not, where $g^{-1}h = 1_G$ gives $g = h$,
- given any two elements x, y check whether they belong to X or not and determine their equality,
- sample uniformly randomly the elements of G,
- compute group action of G on X,

should be easy (cryptographically) to compute and the following operations:

- given $x, y \in X$ find $g \in G$ such that $gx = y$, and
- given $w, x, y \in X$ find the unique element $z \in X$ such that $gy = z$, where g should satisfy $gw = x$

should be hard to compute.
Given a hard homogeneous space, a Diffie Hellman like key exchange protocol can be designed. Precisely, let Alice and Bob know a group G and a fixed element $x \in X$. Alice chooses a random element $g \in G$ as a private key and computes gx as a public key; Bob chooses a random element $h \in G$ as a private key and computes hx as a public key; getting hx Alice computes ghx and getting gx Bob computes hgx to share a common secret $ghx = hgx$. See Figure 1.5. By assumption, the set X is a hard homogeneous space, both the private keys are secure.

Diffie Hellman type of key exchange protocols by Couveignes-Rostovtsev-Stolbunov (CRS) and Commutative Supersingular Isogeny Diffie Hellman (CSIDH) are based on the hard homogeneous spaces given by a class group action to a set of elliptic curves over a finite field.

CRS scheme. CRS scheme is a joint outcome of Couveignes [27] approach of hard homogeneous space and further independent development of Rostovtsev and Stolbunov [75, 87] into a key exchange protocol. This is a Diffie-Hellman like key exchange scheme using the underlying group as a class group and its well-defined action on the set of elliptic curves of fixed endomorphism ring.
Let E be an ordinary elliptic curve whose endomorphism ring is the maximal order $\mathcal{O}_K$ of an imaginary quadratic field K. From above notation, let

$$\mathcal{E}_{\mathcal{O}_K}(\mathbb{F}_p) = \{j(E) : E \text{ is defined over } \mathbb{F}_p \text{ and } \mathrm{End}(E) = \mathcal{O}_K\}.$$

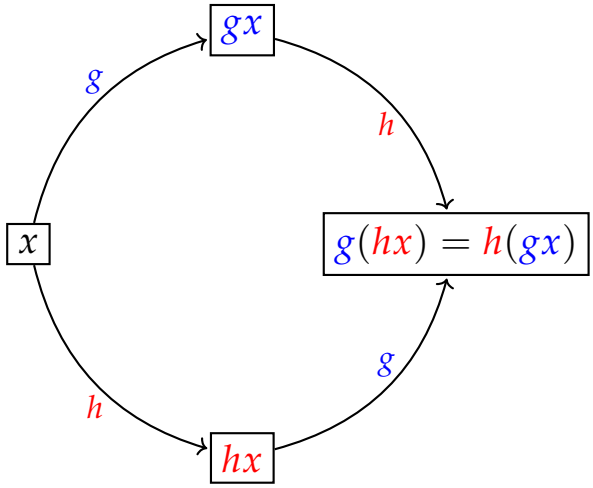

Figure 1.5: Key exchange between Alice and Bob in a homogeneous space X, where underlying group is G and the colors represent the respective calculation done by them.

The Frobenius endomorphism π_p satisfies a characteristic equation with coefficients in $\mathbb{Z}$ i.e. $\pi_p^2 - t\pi_p + p = 0$, where t be its trace and its discriminant $D_\pi = t^2 - 4p$. The discriminant $D_\pi < 0$ when E is ordinary. Number of rational ℓ isogenies (of degree ℓ) with domain E are determined by looking at the Kronecker symbol $(\frac{D_\pi}{\ell})$ for some prime ℓ.

Theorem 1.4.6. *Let $E(\mathbb{F}_p)$ be an elliptic curve and D_π be the discriminant of the Frobenius endomorphism then, for a prime $(\ell, p) = 1$, the followings are the cases of rational isogenies with domain E.*

- *If $(\frac{D_\pi}{\ell}) = 1$ (known as Elkies prime) then there are two isogenies of degree ℓ with domain E.*
- *If $(\frac{D_\pi}{\ell}) = -1$ (known as Atkin prime), then there are no ℓ isogenies.*
- *If $(\frac{D_\pi}{\ell}) = 0$ (ramified primes) then there are 1 or $\ell + 1$ isogenies of degree ℓ.*

Proof. See in [58, Proposition 23]. □

In CRS key exchange scheme, the group $cl(\mathcal{O}_K)$ is used. The discriminant of $\mathcal{O}_K$ is denoted by D_K.
Choose a set $\{\ell_1, \ldots, \ell_k\}$ of Elkies primes, which are primes with $(\frac{D_\pi}{\ell_i}) = 1$ for all $i \leq k$, then

$$\ell_i \mathcal{O}_K = \mathfrak{l}_i \bar{\mathfrak{l}}_i \text{ and } \mathfrak{l}_i^{-1} = \bar{\mathfrak{l}}_i.$$

Precisely, this type of primes give

$$\pi_p^2 - t\pi_p + p = (\pi_p - \alpha_i)(\pi_p - \beta_i) \mod \ell_i$$

and the ideals can be written as

$$\mathfrak{l}_i = (\ell_i, \pi_p - \alpha_i) \text{ and } \bar{\mathfrak{l}}_i = (\ell_i, \pi_p - \beta_i).$$

The number k is chosen so that the set of ideals $\{\mathfrak{l}_1, \ldots, \mathfrak{l}_k\}$ generates the class group $cl(\mathcal{O}_K)$. Under the Riemann hypothesis, k can be chosen in $\mathbb{O}(\log^2 |D_K|)$ [53]. As observed before, the class group action of $cl(\mathcal{O}_K)$ on $\mathcal{E}_{\mathcal{O}_K}(\mathbb{F}_p)$ is transitive and free. Furthermore, each of the ideal $\mathfrak{l}_i$ corresponds an isogeny

$$\phi_{\mathfrak{l}_i} : E \to \mathfrak{l}_i \star E = E_{\mathfrak{l}_i}$$

and its degree is the norm of the ideal $\mathfrak{l}_i$. Therefore, the ideals $\mathfrak{l}_i$ and $\bar{\mathfrak{l}}_i$ give two isogenies starting from the elliptic curve E. This action can be computed by using a fact that the Frobenius π_p acts as a multiplication by α_i map on the ℓ_i torsion subgroup $E[\ell_i]$ of E. Then, its eigenspace gives the kernel of the isogeny $\phi_{\mathfrak{l}_i}$ and the isogeny can be computed by Vélu's formula.
The following homomorphism

$$\begin{aligned} f : \mathbb{Z}^k &\longrightarrow cl(\mathcal{O}_K) \\ (e_1, \ldots, e_k) &\longmapsto \prod_{i=1}^{k} \mathfrak{l}_i^{e_i}, \end{aligned}$$

gives a representation of elements of the class group by the vectors in the lattice $\mathbb{Z}^k$.
Suppose Alice and Bob want to share a common secret. Alice chooses a random vector $\boldsymbol{a} = (a_1, \ldots, a_k)$ in the lattice $\mathbb{Z}^k$ to represent an element

$$\mathfrak{a}_A := \prod_{i=1}^{k} \mathfrak{l}_i^{a_i}$$

of the ideal class $cl(\mathcal{O}_K)$. Alice computes $\mathfrak{a}_A \star E = E_{\mathfrak{a}_A}$. Her private key is the vector $\boldsymbol{a}$ and she publishes $E_{\mathfrak{a}_A}$.
Bob chooses a random vector $\boldsymbol{b} = (b_1, \ldots, b_k) \in \mathbb{Z}^k$ to represent an element

$$\mathfrak{b}_B := \prod_{i=1}^{k} \mathfrak{b}_i^{b_i}$$

of the ideal class $cl(\mathcal{O}_K)$. Bob computes the action $\mathfrak{b}_B \star E = E_{\mathfrak{b}_B}$ and sends it to Alice keeping the vector $\boldsymbol{b}$ as the private key.
Now Alice computes $\mathfrak{a}_A \star E_{\mathfrak{b}_B}$ and Bob computes $\mathfrak{b}_B \star E_{\mathfrak{a}_A}$. Both of them represent same elliptic curve in $\mathcal{E}_{\mathcal{O}_K}(\mathbb{F}_p)$ since

$$E_{\mathfrak{a}_A\mathfrak{b}_B} = \mathfrak{b}_B \star E_{\mathfrak{a}_A} = \mathfrak{b}_B \star (\mathfrak{a}_A \star E) = \mathfrak{a}_A \star (\mathfrak{b}_B \star E) = E_{\mathfrak{b}_B\mathfrak{a}_A}.$$

CSIDH: Commutative SIDH. CSIDH was developed by Castryck, Lange, Martindale, Panny, and Renes in 2018 [18] as an efficient version of CRS scheme but by using supersingular elliptic curves.
Let $\mathrm{End}_p(E)$ be the subring of the full endomorphism ring $\mathrm{End}(E)$ containing endomorphisms that are defined over the base field $\mathbb{F}_p$. If E is supersingular then $\mathrm{End}(E)$ is an order in a quaternion algebra but $\mathrm{End}_p(E)$ is an order $\mathcal{O}$ in an imaginary quadratic field. Therefore, similarly as in CRS scheme, the class group action of $cl(\mathcal{O})$ on the set

$$\mathcal{E}_{\mathcal{O}}(\mathbb{F}_p) = \{j(E) : E \text{ is supersingular curve defined over } \mathbb{F}_p \text{ and } \mathrm{End}_p(E) = \mathcal{O}\}$$

i.e.

$$cl(\mathcal{O}) \times \mathcal{E}_{\mathcal{O}}(\mathbb{F}_p) \to \mathcal{E}_{\mathcal{O}}(\mathbb{F}_p)$$

is transitive and free.
A special prime p of the form $p = 4 \cdot \ell_1 \cdots \ell_k - 1$ with small distinct primes ℓ_i and $p \equiv 3 (\mathrm{mod}\ 8)$ is used. The starting curve is fixed to $E_0 : y^2 = x^3 + x$ over $\mathbb{F}_p$, which is supersingular if and only if $p \equiv 3 (\mathrm{mod}\ 4)$. The trace of the Frobenius endomorphism π_p is zero and π_p satisfies $\pi_p^2 + p = 0$. Then $\mathrm{End}_p(E) = \mathbb{Z}[\pi_p]$ in $\mathbb{Q}(\sqrt{-p})$ and any supersingular elliptic curve over $\mathbb{F}_p$ is $\mathbb{F}_p$-isomorphic to the curve $E_A : y^2 = x^3 + Ax + x$, where $A \in \mathbb{F}_p$ is uniquely determined.
The primes ℓ_i are Elkies primes since $\pi_p^2 \equiv -p \equiv 1 \mod \ell_i$, therefore the ideals are factored as $\ell_i\mathcal{O} = \mathfrak{l}_i\bar{\mathfrak{l}}_i$, where

$$\mathfrak{l}_i = (\ell_i, \pi_p - 1) \text{ and } \bar{\mathfrak{l}}_i = (\ell_i, \pi_p + 1).$$

Now, main speed up comes from an excellent trick as used in [31] for computing the class group action. It is required to find isogenies $\phi_{\mathfrak{l}_i}$ and $\phi_{\bar{\mathfrak{l}}_i}$ corresponding to ideals $\mathfrak{l}_i$ and $\bar{\mathfrak{l}}_i$ respectively. The kernel of the isogeny $\phi_{\mathfrak{l}_i}$ consists of those points in $E[\ell_i]$ that are fixed by the Frobenius π_p and the kernel of $\phi_{\bar{\mathfrak{l}}_i}$ consists of points $P \in E[\ell_i]$ defined over $\mathbb{F}_{p^2}$ such that $\pi_p(P) = -P$. With these setting of the parameters, the CSIDH key exchange is analog to the CRS key exchange protocol.

Chapter 2

Segre and Veronese embedding

In this chapter, we discuss briefly some background of Segre and Veronese embeddings that will be used in Chapter 5. These terminologies are already common in literature such as in [76, 80, 92], we consider that they are taken from those references unless otherwise stated.
Let $\mathbb{P}^n = \mathbb{P}^n_\kappa = (\kappa^{n+1} \setminus \mathbf{0})/\sim$ be the projective space of dimension n for any field κ.

2.1 Quadratic hypersurface

Definition 2.1.1. *A quadratic hypersurface or quadric surface in the projective space $\mathbb{P}^n$ is the zero set of a homogeneous polynomial $G \in \kappa[z_0, \ldots, z_n]$ of the form*

$$G = \sum_{i=0}^{n} c_i z_i^2 + \sum_{i=0}^{n} \sum_{j=i+1}^{n} c_{i,j} z_i z_j.$$

Elliptic curve arises as an intersection of two quadric surfaces. For a general choice of two quadric surfaces $Q_1, Q_2 \subset \mathbb{P}^3_{\bar{\kappa}}$, the intersection $Q_1 \cap Q_2$ is isomorphic to an elliptic curve, whose isomorphism class is determined by the j-invariant.

We will observe quadric surfaces as the images of Segre embeddings. Segre embedding embeds the product of two projective spaces into a bigger projective space .

Definition 2.1.2. *The standard Segre embeddings are the morphisms of the projective varieties*

$$\begin{array}{rcl} \mathbb{P}^n \times \mathbb{P}^m & \xrightarrow{s_{n,m}} & \mathbb{P}^{(m+1)(n+1)-1} \\ ([x_0 : \ldots : x_n], [y_0 : \ldots : y_m]) & \longmapsto & [x_0y_0 : \ldots : x_ny_m] \end{array}$$

where x_iy_j's are ordered according to the standard lexicographical order. The images of these embeddings are called standard Segre varieties and are denoted by $\Sigma_{n,m}$.

Example 2.1.3. *For the Segre embedding*

$$\begin{array}{rcl} \mathbb{P}^1 \times \mathbb{P}^1 & \xrightarrow{s_{1,1}} & \mathbb{P}^3 \\ ([x_0 : x_1], [y_0 : y_1]) & \longmapsto & [x_0y_0 : x_0y_1 : x_1y_0 : x_1y_1], \end{array}$$

we have $s_{1,1}(\mathbb{P}^1 \times \mathbb{P}^1) = \Sigma_{1,1} \subset \mathbb{P}^3$ and $\Sigma_{1,1}$ is a smooth quadric surface defined by the equation

$$z_0z_3 = z_1z_2,$$

where $[z_0 : z_1 : z_2 : z_3]$ is the coordinate of $\mathbb{P}^3$.

Smooth quadric hypersurface are unique up to projective isomorphism.

Lemma 2.1.4. *All the smooth quadric hypersurfaces of $\mathbb{P}^n_{\bar{\kappa}}$ are projectively isomorphic.*

Proof. See in [55, Exercise 5.12]. □

2.2 Curve as an intersection of quadric surfaces

By a bi-homogeneous polynomial of bi-degree (u, v) in $n + m$ variables: $F(x_1, \ldots, x_n, y_1, \ldots, y_m)$, we mean F is homogeneous in x_i of degree u and homogeneous in y_j of degree v.
The intersection of two quadric surfaces in $\mathbb{P}^3$ is a curve of bi-degree $(2, 2)$. Suppose we have two smooth quadric surfaces Q_1, Q_2. From Lemma 2.1.4, we can choose a projective isomorphism $f : \mathbb{P}^3 \to \mathbb{P}^3$ such that $f(Q_1) = \Sigma_{1,1}$. Assume that $Q_1 = \Sigma_{1,1}$, then $Q_1 \cap Q_2 \cong s_{1,1}^{-1}(Q_2) \subset \mathbb{P}^1 \times \mathbb{P}^1$. Let

$$G(z_0, z_1, z_2, z_3) := a_1z_0^2 + a_2z_1^2 + a_3z_2^2 + a_4z_3^2 + a_5z_0z_1 + \ldots + a_{10}z_2z_3$$

be the quadratic form defining Q_2, then $s_{1,1}^{-1}(Q_2)$ is defined in $\mathbb{P}^1 \times \mathbb{P}^1$ by a bi-homogeneous polynomial of bi-degree (2,2)

$$F(x_0, x_1; y_0, y_1) := G(x_0y_0, x_0y_1, x_1y_0, x_1y_1), \tag{2.1}$$

which is called the *pullback* of the polynomial G through $s_{1,1}$.
Since $Q_1 \cap Q_2$ is isomorphic to an elliptic curve, let us denote it by C, we consider C up to isomorphism. We want to find its j-invariant.
A standard result in the theory of algebraic curves is that there is the bijection

$$\left\{\begin{array}{c}\text{genus 1 curves up}\\ \text{to isomorphism.}\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{4-tuples of distinct points of } \mathbb{P}^1\\ \text{up to automorphism.}\end{array}\right\}$$

see for example in [92, 19.5].

Let $\pi : C \to \mathbb{P}^1$ be any degree 2 morphism. Then the 4-tuple of points associated to C are the branch locus of π that are, by definition, the points $P \in \mathbb{P}^1$ such that $\#\pi^{-1}(P) = 1$.

Example 2.2.1. *Let E be the elliptic curve defined by the equation $y^2z = f(x,z)$, where $f(x,z) = (x-az)(x-bz)(x-cz)$, let*

$$\begin{array}{rcl} E & \xrightarrow{\quad\pi\quad} & \mathbb{P}^1 \\ [x:y:z] & \longmapsto & [x:z] \end{array}$$

be a degree 2 map. The branch locus of π is the set $\{[1:0],[a:1],[b:1],[c:1]\}$.

We have $C \subset \mathbb{P}^1 \times \mathbb{P}^1$ and suppose

$$\begin{array}{rcl} C & \xrightarrow{\pi} & \mathbb{P}^1 \\ (P,Q) & \longmapsto & P \end{array}$$

be the projection in the first coordinate. Then the 4-tuple of points in $\mathbb{P}^1$ corresponding to C are the points $P \in \mathbb{P}^1$ such that $\#\pi^{-1}(P) = 1$. Now, we write Equation 2.1 in the following form

$$F(x_0,x_1;y_0,y_1) = y_0^2F_0(x_0,x_1) + y_0y_1F_1(x_0,x_1) + y_1^2F_2(x_0,x_1),$$

which is the defining polynomial of C. Then the branch locus of π is the set of points $P = [X_0,X_1]$ such that the equation

$$F(X_0,X_1;y_0,y_1) = 0$$

has single but repeated solution.

Therefore the discriminant of $F(X_0,X_1;y_0,y_1)$ is zero and hence $[X_0,X_1]$ is the solution of the polynomial

$$H(x_0,x_1) := F_1(x_0,x_1)^2 - 4F_0(x_0,x_1)F_2(x_0x_1).$$

Writing

$$H(x_0, x_1) = q_0 x_0^4 + q_1 x_0^3 x_1 + q_2 x_0^2 x_1^2 + q_3 x_0 x_1^3 + q_4 x_1^4$$

and defining

$$\begin{aligned} S &:= q_0 q_4 - \frac{q_1 q_3}{4} + \frac{q_2^2}{12} \\ T &:= \frac{q_0 q_2 q_4}{6} + \frac{q_1 q_2 q_3}{48} - \frac{q_2^3}{216} - \frac{q_0 q_3^2}{16} - \frac{q_1^2 q_4}{16}, \end{aligned}$$

we get $j(C) = \dfrac{S^3}{S^3 - 27T^2}$, the j invariant of the $(2,2)$ curve C. Also, H is invariant under the action of $\mathcal{GL}(2)$, see for example in [2, 39, 76].

2.3 Segre and Veronese embeddings

We will define a non-standard Segre embedding as the composition of the standard Segre embedding and a projective automorphism of the ambient space of the codomain, which is represented by a square matrix.

Definition 2.3.1. *Let $n, m \in \mathbb{N}$. The non-standard Segre embedding and the Segre variety represented by the matrix M in the general linear group $\mathcal{GL}((m+1)(n+1))$ are respectively defined as*

$$s_{n,m}^M := M \circ s_{n,m}, \quad \Sigma_{n,m}^M := M\Sigma_{n,m}.$$

The smooth quadric surfaces of $\mathbb{P}^3$ are projectively isomorphic, therefore they are $\Sigma_{n,m}^M$ for some m and n.

Example 2.3.2. *Consider a non-standard Segre embedding*

$$\begin{aligned} \mathbb{P}^1 \times \mathbb{P}^1 &\xrightarrow{\quad s_{1,1}^M \quad} \mathbb{P}^3 \\ \left(\begin{bmatrix} x_0 \\ x_1 \end{bmatrix}, \begin{bmatrix} y_0 \\ y_1 \end{bmatrix} \right) &\longmapsto \begin{bmatrix} x_0 y_0 - 4 x_1 y_1 \\ -7 x_1 y_0 + x_1 y_1 \\ x_0 y_0 + 2 x_0 y_1 - x_1 y_0 + 5 x_1 y_1 \\ 8 x_0 y_1 + x_1 y_0 \end{bmatrix} \end{aligned}$$

which is represented by the matrix

$$M = \begin{bmatrix} 1 & 0 & 0 & -4 \\ 0 & 0 & -7 & 1 \\ 1 & 2 & -3 & 5 \\ 0 & 8 & -6 & 0 \end{bmatrix}.$$

We also define the standard and non-standard Veronese embedding.

Definition 2.3.3. *For $n, m \in \mathbb{N}$, the standard Veronese embedding are the morphisms*

$$\begin{array}{ccc} \mathbb{P}^n & \xrightarrow{v_{n,m}} & \mathbb{P}^{\binom{n+m}{m}-1} \\ [x_0 : \cdots : x_n] & \longmapsto & [x_0^m : \cdots : x_n^m] \end{array}$$

where the monomials $(x_0^{i_0} \cdots x_n^{i_n})_{0 \leq i_j \leq m}$ with $\sum_{j=0}^{n} i_j = m$ (of degree m) are ordered by the lexicographical order. The images of these embeddings are called standard Veronese varieties and they are denoted by $V_{n,m}$.

Suppose $z_{i_0,\ldots,i_n}$ be the variable in $\mathbb{P}^{\binom{m+3}{3}-1}$ corresponding to the monomial $x_0^{i_0} \ldots x_n^{i_n}$ in the Veronese map. Suppose,

$$C = c_0, \ldots, c_n, D = d_0, \ldots, d_n, E = e_0, \ldots, e_n, \text{ and } F = f_0, \ldots, f_n$$

be the indices of the coordinates of $\mathbb{P}^{\binom{n+m}{m}-1}$ such that $C + D = E + F$ i.e. $c_0 + d_0 = e_0 + f_0, \ldots, c_n + d_n = e_n + f_n$ then in the images of the Veronese map, we have the following relation of coordinates:

$$z_C \cdot z_D - z_E \cdot z_F = 0 \tag{2.2}$$

Proposition 2.3.4. *The standard Veronese variety is defined by the quadratic equations given in Equation(2.2).*

Proof. See in [80, Example 1.28]. □

Example 2.3.5. *For the Veronese embedding*

$$\begin{array}{ccc} \mathbb{P}^1 & \xrightarrow{v_{1,3}} & \mathbb{P}^3 \\ [x_0 : x_1] & \longmapsto & [x_0^3 : x_0^2 x_1 : x_0 x_1^2 : x_1^3] \end{array}$$

we have, $v_{1,3}(\mathbb{P}^1) = V_{1,3} \subset \mathbb{P}^3$, the image is defined by the following quadratic equations

$$-z_2^2 + z_1 z_3, -z_1 z_2 + z_0 z_3, -z_1^2 + z_0 z_2 \tag{2.3}$$

where $[z_0 : z_1 : z_2 : z_3]$ is the coordinate of $\mathbb{P}^3$.

Similarly we define non-standard Veronese embedding as the composition of the standard Veronese embedding and a projective automorphism of the ambient space of the variety.

Definition 2.3.6. *Let $n, m \in \mathbb{N}$. Let $M \in \mathcal{GL}(\binom{n+m}{m})$. Then*

$$v_{n,m}^{M} := M \circ v_{n,m}, \quad V_{n,m}^{M} := MV_{n,m}$$

are defined respectively as the Veronese embedding and the Veronese variety represented by the matrix M.

We use the composition of the Segre embedding $s_{1,1}^{M}$ and the Veronese embedding $v_{3,m}^{M'}$ in the application to cryptography. We define the composition $v_{3,m}^{M'} \circ s_{1,1}^{M}$ as a σ-embedding represented by a $\binom{m+3}{3} \times (m+1)^2$ matrix.

Example 2.3.7. *Let $\kappa = \mathbb{F}_3 = \{0, 1, 2\}$ and $m = 2$ then $\binom{m+3}{3} = 10$. Consider a non-standard Segre embedding*

$$\begin{array}{ccc} \mathbb{P}^1 \times \mathbb{P}^1 & \xrightarrow{\quad s_{1,1}^{M} \quad} & \mathbb{P}^3 \\ \left(\begin{bmatrix} x_0 \\ x_1 \end{bmatrix}, \begin{bmatrix} x_2 \\ x_3 \end{bmatrix} \right) & \longmapsto & \begin{bmatrix} -x_0x_2 + x_0x_3 + x_1x_3 \\ x_1x_2 + x_0x_3 - x_1x_3 \\ x_0x_2 - x_1x_2 + x_1x_3 \\ -x_0x_2 + x_0x_3 + x_1x_3 \end{bmatrix} \end{array}$$

which is represented by the matrix

$$M = \begin{bmatrix} 2 & 1 & 0 & 1 \\ 0 & 1 & 1 & 2 \\ 1 & 0 & 2 & 1 \\ 2 & 1 & 0 & 1 \end{bmatrix}.$$

Suppose

$$v_{3,2}^{M'} := M' \circ v_{3,2},$$

where the map $v_{3,2} \circ s_{1,1}^{M}$

$$\mathbb{P}^1 \times \mathbb{P}^1 \xrightarrow{\quad v_{3,m} \circ s_{1,1}^{M} \quad} \mathbb{P}^9$$

maps to

$$[x_0^2x_2^2 + x_0^2x_2x_3 + x_0x_1x_2x_3 + x_0^2x_3^2 - x_0x_1x_3^2 + x_1^2x_3^2 : -x_0x_1x_2^2 - x_0^2x_2x_3 - x_0x_1x_2x_3 + x_1^2x_2x_3 + x_0^2x_3^2 - x_1^2x_3^2 : -x_0^2x_2^2 + x_0x_1x_2^2 + x_0^2x_2x_3 - x_0x_1x_2x_3 - x_1^2x_2x_3 + x_0x_1x_3^2 + x_1^2x_3^2 : x_0^2x_2^2 + x_0^2x_2x_3 + x_0x_1x_2x_3 + x_0^2x_3^2 - x_0x_1x_3^2 + x_1^2x_3^2 : x_1^2x_2^2 - x_0x_1x_2x_3 + x_1^2x_2x_3 + x_0^2x_3^2 + x_0x_1x_3^2 + x_1^2x_3^2 : x_0x_1x_2^2 - x_1^2x_2^2 + x_0^2x_2x_3 + x_0x_1x_2x_3 - x_1^2x_2x_3 + x_0x_1x_3^2 - x_1^2x_3^2 : -x_0x_1x_2^2 - x_0^2x_2x_3 - x_0x_1x_2x_3 + x_1^2x_2x_3 + x_0^2x_3^2 - x_1^2x_3^2 : x_0^2x_2^2 + x_0x_1x_2^2 + x_1^2x_2^2 - x_0x_1x_2x_3 + x_1^2x_2x_3 + x_1^2x_3^2 : -x_0^2x_2^2 + x_0x_1x_2^2 + x_0^2x_2x_3 - x_0x_1x_2x_3 - x_1^2x_2x_3 + x_0x_1x_3^2 + x_1^2x_3^2 : x_0^2x_2^2 + x_0^2x_2x_3 + x_0x_1x_2x_3 + x_0^2x_3^2 - x_0x_1x_3^2 + x_1^2x_3^2].$$

Now applying the automorphism of $\mathbb{P}^9$ *given by*

$$M' = \begin{bmatrix} 2 & 1 & 1 & 1 & 1 & 2 & 2 & 1 & 2 & 1 \\ 2 & 1 & 0 & 0 & 1 & 2 & 1 & 2 & 1 & 1 \\ 2 & 1 & 0 & 0 & 2 & 1 & 2 & 1 & 2 & 1 \\ 2 & 1 & 2 & 1 & 1 & 1 & 0 & 2 & 2 & 1 \\ 2 & 1 & 0 & 0 & 1 & 0 & 0 & 2 & 0 & 2 \\ 1 & 0 & 2 & 0 & 2 & 1 & 0 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 & 2 & 1 & 1 & 2 & 1 & 0 \\ 2 & 0 & 2 & 1 & 1 & 0 & 2 & 0 & 2 & 1 \\ 1 & 1 & 0 & 0 & 2 & 2 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 2 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

we get the σ*-embedding* $v_{3,m}^{M'} \circ s_{1,1}^{M}$*, which maps to*

$$[x_0^2x_2^2 + x_0^2x_2x_3 + x_0x_1x_2x_3 + x_0^2x_3^2 - x_0x_1x_3^2 + x_1^2x_3^2 : -x_0x_1x_2^2 - x_0^2x_2x_3 - x_0x_1x_2x_3 + x_1^2x_2x_3 + x_0^2x_3^2 - x_1^2x_3^2 : -x_0^2x_2^2 + x_0x_1x_2^2 + x_0^2x_2x_3 - x_0x_1x_2x_3 - x_1^2x_2x_3 + x_0x_1x_3^2 + x_1^2x_3^2 : x_0^2x_2^2 + x_0^2x_2x_3 + x_0x_1x_2x_3 + x_0^2x_3^2 - x_0x_1x_3^2 + x_1^2x_3^2 : x_1^2x_2^2 - x_0x_1x_2x_3 + x_1^2x_2x_3 + x_0^2x_3^2 + x_0x_1x_3^2 + x_1^2x_3^2 : x_0x_1x_2^2 - x_1^2x_2^2 + x_0^2x_2x_3 + x_0x_1x_2x_3 - x_1^2x_2x_3 + x_0x_1x_3^2 - x_1^2x_3^2 : -x_0x_1x_2^2 - x_0^2x_2x_3 - x_0x_1x_2x_3 + x_1^2x_2x_3 + x_0^2x_3^2 - x_1^2x_3^2 : x_0^2x_2^2 + x_0x_1x_2^2 + x_1^2x_2^2 - x_0x_1x_2x_3 + x_1^2x_2x_3 + x_1^2x_3^2 : -x_0^2x_2^2 + x_0x_1x_2^2 + x_0^2x_2x_3 - x_0x_1x_2x_3 - x_1^2x_2x_3 + x_0x_1x_3^2 + x_1^2x_3^2 : x_0^2x_2^2 + x_0^2x_2x_3 + x_0x_1x_2x_3 + x_0^2x_3^2 - x_0x_1x_3^2 + x_1^2x_3^2],$$

and its 10×9 *matrix representation*

$$M'' = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 & 2 & 1 \\ 0 & 2 & 0 & 2 & 2 & 1 & 1 & 0 & 2 \\ 2 & 1 & 0 & 1 & 2 & 2 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 2 & 1 \\ 0 & 0 & 1 & 0 & 2 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 1 & 1 & 2 & 0 & 1 & 2 \\ 0 & 2 & 0 & 2 & 2 & 1 & 1 & 0 & 2 \\ 1 & 1 & 1 & 0 & 2 & 1 & 0 & 0 & 1 \\ 2 & 1 & 0 & 1 & 2 & 2 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 2 & 1 \end{bmatrix}.$$

is obtained with respect to the monomial basis

$$\{x_0^2x_2^2, x_0x_1x_2^2, x_1^2x_2^2, x_0^2x_2x_3, x_0x_1x_2x_3, x_1^2x_2x_3, x_0^2x_3^2, x_0x_1x_3^2, x_1^2x_3^2\}.$$

2.3.1 Automorphism of Veronese Variety

It is easy to construct the automorphisms of the Veronese variety. This can be obtained by using the homomorphism of general linear groups. Suppose we have the standard Veronese embedding $v_{n,m} : \mathbb{P}^n \to \mathbb{P}^{\binom{n+m}{m}-1}$.

Consider an action of $A = (a_{ij})_{0 \le i,j \le n} \in \mathcal{GL}(n+1)$ on the coordinates of $\mathbb{P}^n$ as

$$x_i \mapsto L_i := \sum_{j=0}^{n} a_{ij}x_j, \;\; 0 \le i \le n$$

This action on coordinates induces a natural action on the monomials of degree $\sum_{k=0}^{n} e_k = m$ as

$$x_0^{e_0} \cdots x_n^{e_n} \mapsto L_0^{e_0} \cdots L_n^{e_n}$$

and can be represented by a matrix in $\mathcal{GL}(\binom{n+m}{m})$. More precisely, this matrix is obtained by the action of A on the homogeneous polynomials of degree m, written with respect to the monomial basis of the Veronese map. This gives a natural group homomorphism

$$\phi_{n,m} : \mathcal{GL}(n+1) \to \mathcal{GL}(\binom{n+m}{m}).$$

Example 2.3.8. *Take* $n = 1$ *and* $m = 2$. *Then the Veronese map is*

$$\begin{array}{ccc} \mathbb{P}^1 & \xrightarrow{\quad v_{1,2} \quad} & \mathbb{P}^3 \\ [x_0 : x_1] & \longmapsto & [x_0^2 : x_0x_1 : x_1^2]. \end{array}$$

Consider $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{GL}(2)$ *acting on the coordinates* $[x_0 : x_1] \in \mathbb{P}^1$ *as*

$$\begin{aligned} x_0 &\mapsto ax_0 + bx_1 \\ x_1 &\mapsto cx_0 + dx_1. \end{aligned}$$

This corresponds to an action on the monomials of degree 2 as

$$\begin{aligned} x_0^2 &\mapsto a^2x_0^2 + 2abx_0x_1 + b^2x_1^2 \\ x_0x_1 &\mapsto acx_0^2 + (ad + bc)x_0x_1 + bdx_1^2 \\ x_1^2 &\mapsto c^2x_0^2 + 2cdx_0x_1 + d^2x_1^2. \end{aligned}$$

This gives the following matrix with respect to the monomial basis $\{x_0^2, x_0x_1, x_1^2\}$

$$\phi_{n,m}(A) = \begin{pmatrix} a^2 & 2ab & b^2 \\ ac & ad + bc & bd \\ c^2 & 2cd & d^2 \end{pmatrix}.$$

The image of $\phi_{n,m}$ is a subgroup of $\mathcal{GL}(\binom{n+m}{m})$, which contains the automorphisms of the ambient space $\mathbb{P}^{\binom{n+m}{m}-1}$ that fix the Veronese variety $V_{n,m}$.
The automorphisms of the Veronese variety $V_{n,m}^M$ are given by the following proposition.

Proposition 2.3.9. $\mathrm{Aut}(V_{n,m}^M) = M \,\mathrm{Im}(\phi_{n,m}) M^{-1}$ *for any* $M \in \mathcal{GL}(\binom{m+3}{3})$.

Proof. It follows from the equality

$$\mathrm{Aut}(MV) = M \,\mathrm{Aut}(V) M^{-1}$$

for any projective subvariety V. □

Chapter 3

Computing isogenies from torsion images

After a theorem of Tate [89], which states that two elliptic curves over a finite field $\mathbb{F}_p$ are isogenous over $\mathbb{F}_p$ if and only if they have the same number of $\mathbb{F}_p$-rational points, a natural question is to find an isogeny between them. An algorithm proposed first by Schoof [77, 78], and later improvements by Elkies [41], Atkin [3], now known as Schoof-Elkies-Atkin (SEA), count the number of points on an elliptic curve over a finite field and hence give an efficient way to determine whether two elliptic curves are isogenous or not. Moreover, having a wide range of application in isogeny based cryptography as discussed in Section 1.4 and point counting algorithms, computing isogeny between elliptic curves over finite fields have appealed many researchers. The small degree isogenies, in size $\mathcal{O}(\log(p))$, which are useful in point counting, were studied, for example, in [4, 41] [25, 26, 43, 44, 42, 45].
The large degree isogenies, in size $\mathcal{O}(p)$ are useful in isogeny based cryptography. A study of such isogenies was initiated by Galbraith in [47] and further improved in [49] and in [34]. The quantum variants of such isogeny problems were studied in [22, 13] and the specialized versions to compute isogeny for the supersingular elliptic curve was developed by Petit in [71] under the assumption that some information of the isogeny, more specifically, the image on a torsion subgroup under the isogeny, are known. This work was further improved in [61] and got some weak instances of some variants of SIDH but not that of the SIDH itself. Their work leverages the SIDH scenario.

In this chapter, we first review an isogeny computation problem introduced by Petit, and give a polynomial-time algorithm to construct an endomorphism of a supersingular elliptic curve defined over $\mathbb{F}_p$ given only

the action on torsion subgroup under certain parameter restriction and heuristic assumptions. Our main contributions in this chapter are Theorem 3.2.23, Theorem 3.3.4 and Algorithm 3.3.5.

3.1 Isogeny computation using torsion images

In this section, we review a technique to compute an isogeny using torsion point images from [71].
The following problem is the general type of isogeny problem for supersingular elliptic curves.

Problem 3.1.1. *Let E_0, E be two supersingular elliptic curves defined over the finite field $\mathbb{F}_{p^2}$ and there is an isogeny $\phi : E_0 \to E$ between them. Compute an efficient expression of ϕ.*

Solutions of Problem 3.1.1 can break the SIDH. But, a more specific problem that occurs in SIDH is the following:

Problem 3.1.2. *Let E_0, E be supersingular elliptic curves defined over $\mathbb{F}_{p^2}$. Let M, N be integers with gcd(M,N)=1 and suppose $\phi : E_0 \to E$ be a degree M isogeny whose images are known on N-torsion subgroup $E_0[N]$ of E_0 i.e. $\phi(P)$ for all $P \in E_0[N]$ are known. Compute an efficient expression of ϕ.*

In SIDH, the isogeny ϕ is known on the basis of $E_0[N]$ but these images on the basis can be used to evaluate ϕ on the whole $E_0[N]$. Any algorithm that can solve Problem 3.1.2 can break the SIDH due to [50]. Therefore, such a problem is interesting in SIDH/SIKE like environment.

We summarize the main idea to deal with Problem 3.1.2 from [71]. Suppose E_0, E be supersingular elliptic curves defined over $\mathbb{F}_{p^2}$ and $\phi : E_0 \to E$ be a degree M isogeny which is known on the N-torsion subgroup of E_0 with $\gcd(N, M) = 1$. Unlike SIDH, where small prime powers are used instead of M and N, here we suppose M and N be any powersmooth numbers, where a number $M = \prod p_i^{a_i}$ is called a B-powersmooth for some integer B if $p_i^{a_i} < B$. Furthermore, the prime p is not restricted to the special form $p = MNf \pm 1$. If M and N are chosen arbitrarily, then the M, N-torsion points may not be defined in $\mathbb{F}_{p^2}$. Therefore, we consider M, N are powersmooth numbers so that the M, N-torsion points can be represented efficiently as described by an algorithm in [51].

There are three main steps:

1. (Find an endomorphism of E_0). Search for a non-scalar endomorphism μ of E_0 and an integer d such that the corresponding endomorphism $\nu = \phi \circ \mu \circ \hat{\phi} + [d]$ of E is of degree Ne with $e \geq 1$ be an integer as small as possible. See Figure 3.1.
2. (Compute an endomorphism of E). Compute ν in the form $\nu = \psi \circ \nu_N$, where ν_N and ψ are isogenies of degree N and e respectively.
3. (Obtain ϕ from $\nu - [d] = \phi \circ \mu \circ \hat{\phi}$). Recover the kernel of ϕ from that of $\nu - [d]$.

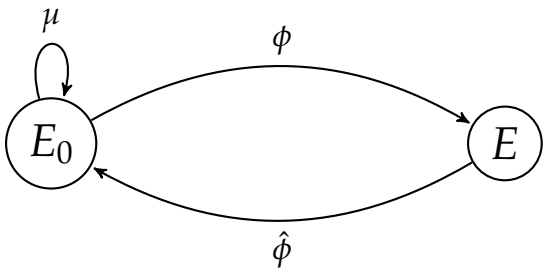

Figure 3.1: Torsion point attack

3.1.1 Find an endomorphism of E_0

A suitable non-scalar endomorphism of E_0 is calculated so that the endomorphism $\nu = \phi \circ \mu \circ \hat{\phi} + [d]$ of E is of degree Ne with e small. This degree expression helps to find the endomorphism ν explicitly.

When E_0 is special curve. E_0 is called *special* if it is defined over $\mathbb{F}_p$ and $\mathrm{End}(E_0)$ contains a small degree non-scalar endomorphism. Suppose E_0 be a special curve and ι be a trace zero endomorphism of E_0 of degree r. In this case $\mathbb{Z}[\pi_p, \iota] \subset \mathrm{End}(E_0)$, where π_p is the p-th power Frobenius map.
Let us write

$$\nu = \phi \circ \mu \circ \hat{\phi} + d \in \mathrm{End}(E),$$

where $\mu = a\iota\pi_p + b\pi_p + c\iota \in \mathrm{End}(E_0)$, such that the degree

$$\deg \nu = M^2 pra^2 + M^2 pb^2 + M^2 rc^2 + d^2 = Ne. \tag{3.1}$$

In this case, the attack works for the optimal degree variant explained in 1.4.3 under the following parameters restrictions

- $N > M^4 \approx p^4$
- N is a square modulo M^2.

Under these restrictions, a way to solve Equation 3.1 is to start with assigning value $e = 1$, if this fails then replace it by another bigger square in $\mathbb{Z}/M^2\mathbb{Z}$. For chosen e, find a value of d satisfying the congruence relation

$$d^2 = Ne \pmod{M^2}.$$

Choose a value of d such that

$$r\frac{Ne - d^2}{M^2} \text{ is square } (\text{mod } p).$$

Now, with given e and d, assign some values of c until the right hand side of the equation

$$ra^2 + b^2 = \frac{Ne - d^2 - M^2rc^2}{M^2p}$$

is positive and hence can be solved efficiently by using Cornacchia's algorithm [23]. Values of a, b, c determine μ and together with the value of d ensure that the degree of ν is Ne.

3.1.2 Find an endomorphism of E

From the discussion in the previous subsection, an endomorphism μ of E_0 can be found such that the degree of the endomorphism $\nu = \phi \circ \mu \circ \hat{\phi} + [d] \in \text{End}(E)$ is of the form Ne. The knowledge of the degree expression Ne helps to find the endomorphism ν in a form $\nu = \psi \circ \nu_N$ such that $\deg \psi = e$ and $\deg \nu_N = N$. Since the action of the isogeny ϕ is known on N-torsion subgroup of E_0, this can be used to get the action of the endomorphism ν on the N-torsion subgroup of E.
Suppose $\nu_N : E \to E^{'}$. Using the action of ν on N-torsion points, it is easy to compute the kernel of ν_N of order N. Now, by meet in middle attack, applying between $E^{'}$ and E, the isogeny ψ can be recovered easily whenever e is small. See Figure 3.2.

3.1.3 Obtain ϕ from $\nu - [d]$

Once the endomorphism $\nu = \phi \circ \mu \circ \hat{\phi} + [d]$ of E is known, $\ker \phi$ can be recovered from the kernel of $\nu - [d] = \phi \circ \mu \circ \hat{\phi}$. Suppose $\deg \mu$ is coprime with M.

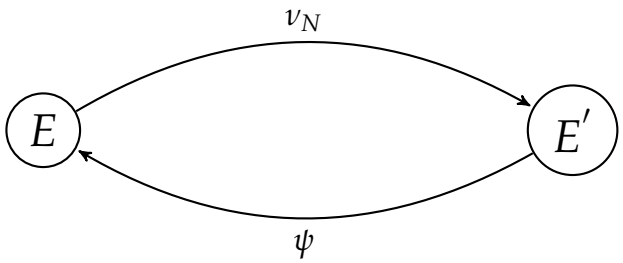

Figure 3.2: An endomorphism $\nu = \psi \circ \nu_N$ of E of degree Ne, where deg $\psi = e$ and deg $\nu_N = N$.

Suppose $H = \ker(\phi \circ \mu \circ \hat{\phi}) \cap E[M]$. Since $\hat{\phi} : E \to E_0$ is an isogeny of degree M, its kernel $\ker \hat{\phi}$ is a cyclic subgroup of order M. When H is cyclic then $H = \ker \hat{\phi}$ and $\ker \phi$ can be recovered from H. Suppose H is not cyclic. Let m be the largest integer such that $E[m] \subset H$. Then the isogeny ϕ can be seen as a composition of an isogeny $\phi_m : E_0 \to E_m$ and $\hat{\phi}_{M/m} : E_m \to E$ as

$$\phi = \hat{\phi}_{M/m} \circ \phi_m,$$

see Figure 3.3.

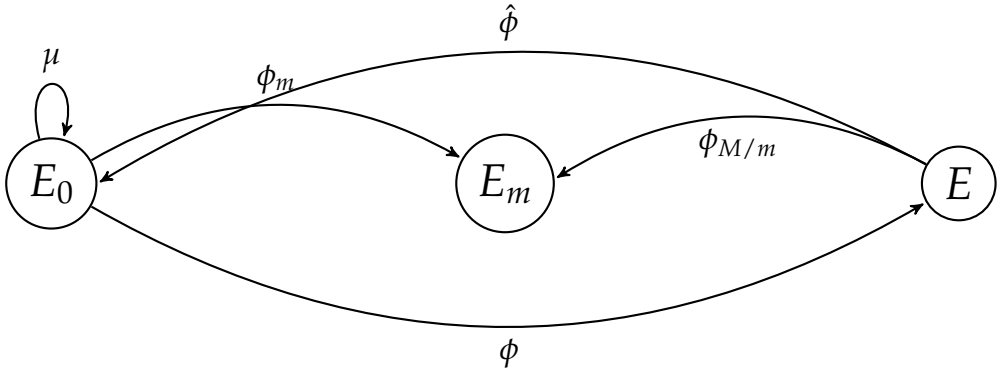

Figure 3.3: The isogeny $\phi = \hat{\phi}_{M/m} \circ \phi_m : E_0 \to E$ as the composition of two isogenies $\phi_m : E_0 \to E_m$ and $\hat{\phi}_{M/m} : E_m \to E$.

Then the kernel of $\phi_{M/m}$ is obtained by intersecting the kernel of ν with $E[M]$.

Lemma 3.1.3. *The kernel of $\phi_{M/m}$ is mH, where*

$$H = \ker(\phi \circ \mu \circ \hat{\phi}) \cap E[M].$$

Proof. See in [71, Lemma 4]. □

Now, it remains to find the kernel of ϕ_m, which can be obtained by a few possible attempts when m has few prime factors due to the following lemma.

Lemma 3.1.4. *The endomorphism μ stabilizes the subgroup ker $\phi_m \subset E_0$ i.e.*

$$\mu(ker\ (\phi_m)) = \ ker(\phi_m)$$

and if t be the number of distinct prime divisors of m then the number of cyclic subgroups of $E_0[m]$ of order m that are stabilized by μ is 2^t.

Proof. See in [71, Lemma 5]. □

By assumption M is smooth, therefore it is easier to find the kernel of ϕ_m.

3.1.4 An improvement in isogeny computation using torsion images

The isogeny computation algorithm discussed above works well with some restriction of parameters and when E_0 is special curve. More specifically, the following is true from [71].

Proposition 3.1.5. *Let M and N are two relatively prime powersmooth numbers such that $N \approx M^4 > p^4$ and N is a square modulo M^2. Let $\phi : E_0 \to E$ be a degree M isogeny whose action on N-torsion points are known. Then ϕ can be computed in polynomial time when E_0 is special.*

On the other hand, SIKE requires $M \approx N \approx p^{1/2}$. In [61], the parameters assumption $N \approx M^4 > p^4$ is relaxed to $N > M^3 > p^{3/2}$ or $N > M^2 > p^2$. This improvement is coming from a small tweak in the following equation

$$\deg \nu = \ \deg\ (\phi \circ \mu \circ \hat{\phi} + d) = M^2pra^2 + M^2pb^2 + M^2rc^2 + d^2 = Ne$$

by changing N by N^2 as follows

$$M^2pra^2 + M^2pb^2 + M^2rc^2 + d^2 = N^2e. \tag{3.2}$$

Furthermore, the following theorem given in [61] ensures that the change of N by N^2 does not affect the complexity of the algorithm.

Theorem 3.1.6. *Let M, N be coprime powersmooth integers. Let E_0 be a supersingular elliptic curve over $\mathbb{F}_{p^2}$. Suppose $\phi : E_0 \to E$ be a degree M isogeny whose*

action on N-torsion points of E_0 is known. Moreover, suppose there exists a trace zero endomorphism μ of E_0 and an integer d with $\gcd(d, N) = 1$ *such that*

$$deg\ (\phi \circ \mu \circ \hat{\phi} + [d]) = N^2 e.$$

Then ϕ can be computed in complexity $\mathbb{O}(\sqrt{e}\ polylog(p))$.

Torsion point attack is further improved for SIDH variants in [33] that includes many weak parameter sets. For instance, they provide polynomial-time algorithm when the curve E_0 has j-invariant 1728, $N > pM$, $p > M$ or $N > \sqrt{p}M^2$, $p > M$, M has at most $\mathbb{O}(\log\log p)$ distinct prime factors and N is at most polynomial in M. Further impact of this torsion point attack covers an attack to a group key agreement [5] and to B-SIDH [24].
Moreover, for some variants of SIDH, the abelian group action on the SIDH key space can be computed using torsion point information [62].

3.2 Simon's Algorithm for dimension 5

We describe an algorithm of Denis Simon [84] to solve quadratic equations in dimension 5. We will further analyze the complexity when the factorization of the determinant is known.
Before that we give a brief preliminary from [16, 79].

3.2.1 Hilbert symbol and Witt invariant

Definition 3.2.1. *Let K be either the field $\mathbb{R}$ of real numbers or the field $\mathbb{Q}_p$ of p-adic numbers for prime p. Let $a, b \in K^*$ then the Hilbert symbol $(a, b)_K$ is defined as*

$$(a,b)_K = \begin{cases} 1 & \text{if } ax^2 + by^2 - z^2 = 0 \text{ has a solution } (x,y,z) \neq (0,0,0) \text{ in } K^3 \\ -1 & \text{otherwise.} \end{cases}$$

Hilbert symbol has the following properties.

Lemma 3.2.2. *Let $a, b, c \in K^*$, where $K = \mathbb{R}$ or $\mathbb{Q}_p$ then*

- $(a, b)_K = (b, a)_K$.
- $(a^2, b)_K = 1$.
- $(a, -a)_K = (a, 1 - a)_K = 1$ *if* $a \neq 1$.
- $(a, a)_K = (a, -1)_K$.

- $(a, bc)_K = (a, b)_K (a, c)_K$.

Proof. See in [79, Proposition 2]. □

The last property of the previous lemma shows the bilinearity of the Hilbert symbol.

Theorem 3.2.3. *The Hilbert symbol is a nondegenerate bilinear form on the $\mathbb{F}_2$-vector space K^*/K^{*2}.*

Proof. Follows from Lemma 3.2.2. □

Definition 3.2.4. *Let V be a module over a commutative ring R. A function $Q : V \to R$ is called a quadratic form on V if*

- *$Q(rx) = r^2 Q(x)$ for $r \in R$ and $x \in V$*
- *the function $(x, y) \mapsto Q(x + y) - Q(x) - Q(y)$ is a bilinear form. The pair (V, Q) is called a quadratic module.*

If $R = K$ is a field of characteristic $\neq 2$ then V is a K-vector space and we can define a scalar product on V as

$$x \cdot y = \frac{1}{2}\{Q(x + y) - Q(x) - Q(y)\}.$$

The map $(x, y) \mapsto x \cdot y$ is a symmetric bilinear form on V. We have

$$Q(x) = x \cdot x.$$

This gives a correspondence between quadratic forms and symmetric bilinear forms.

Definition 3.2.5. *(Matrix of a quadratic form.) Let $(e_i)_{1 \leq i \leq n}$ be a basis of V. The matrix of Q with respect to this basis is the symmetric matrix*

$$A = (a_{ij}) \text{ where } a_{ij} = e_i \cdot e_j.$$

If $x = \sum x_i e_i \in V$, then

$$Q(x) = \sum_{i,j} a_{ij} x_i x_j$$

is a quadratic form in $x_1, \ldots x_n$.
If the basis (e_i) is changed by an invertible matrix B then the new matrix A' of Q with respect to new basis is BAB^t and

$$\det(A') = \det(A) \det(B^2).$$

Definition 3.2.6. *An element x of a quadratic module (V,Q) is called isotropic if* $Q(x) = 0$. *A subspace of V is called isotropic if all the elements are isotropic.*

Definition 3.2.7. *(Orthogonal sum.) Let* $(V_1, Q_1), \ldots, (V_n, Q_n)$ *be quadratic modules. The orthogonal sum* $V_1 \oplus \ldots \oplus V_n$ *is defined to be the direct sum of modules* V_i *with quadratic form* $Q := Q_1 \oplus \ldots \oplus Q_n$ *defined by*

$$Q(x_1 \oplus \cdots \oplus x_n) = \sum_i Q_i(x_i).$$

Definition 3.2.8. *Let* (V, Q) *be a quadratic module over a field K. Two elements* $x, y \in V$ *are orthogonal if* $x \cdot y = 0$. *If* V_1 *and* V_2 *are two vector subspaces of V they are said to be orthogonal if*

$$x \cdot y = 0 \text{ for all } x \in V_1 \text{ and } y \in V_2.$$

A basis $(e_1, \ldots, e_n)$ of a quadratic module (V, Q) is called orthogonal if its elements are pairwise orthogonal. In this case, the matrix of Q with respect to this basis is a diagonal matrix

$$\begin{pmatrix} a_1 & 0 & \ldots & 0 \\ 0 & a_2 & \ldots & 0 \\ & \ldots\ldots & & \\ 0 & 0 & \ldots & a_n \end{pmatrix} \tag{3.3}$$

If $x = \sum x_i e_i$ then $Q(x) = a_1 x_1^2 + \ldots + a_n x_n^2$.
Let $f(X) = \sum_{i=1}^{n} a_{ii} X_i^2 + 2 \sum_{i<j} a_{ij} X_i X_j$ be a quadratic form in n variables over a field K, taking $a_{ij} = a_{ji}$ if $i > j$ then the matrix $A = (a_{ij})$ is symmetric. Then the pair (K^n, f) is a quadratic module associated to f.

Definition 3.2.9. *Two quadratic forms* f *and* f' *are called equivalent if the corresponding modules are isomorphic.*

Theorem 3.2.10. *[79] Let* f *be a quadratic form in n variables. Then there exist* $a_1, \ldots, a_n \in K$ *such that* f *is equivalent to* $a_1 X_1^2 + \ldots + a_n X_n^2$.

Proof. See in [79, Theorem 1']. □

The *rank* of a quadratic form f is the number of indices i such $a_i \neq 0$ and the *signature* is (r, s), where r and s are the number of a_i's that are positive and negative respectively. A quadratic form with signature $(n, 0)$ (respectively $(0, n)$) is positive (negative) definite.

Definition 3.2.11. *(Witt invariant.) Let K be the field $\mathbb{Q}_p$ for some prime p and (V, Q) be a quadratic module of rank n and discriminant Δ. Suppose $e = \{e_1, \ldots, e_n\}$ be an orthogonal basis for V. Suppose $a_i = e_i \cdot e_i$ then $\Delta = a_1 \cdots a_n$ and the Witt invariant of (V, Q) denoted as $\epsilon_p(Q)$ and is defined as*

$$\epsilon_p(Q) = \prod_{i<j} (a_i, a_j)_{\mathbb{Q}_p}.$$

Theorem 3.2.12. *The number $\epsilon_p(Q)$ does not depend on the choice of the orthogonal basis of V.*

Proof. See in [79, Theorem 5]. □

3.2.2 Solution for dimension 5

Let $Q_0(X) = X^t Q_0 X$ be a quadratic form over $\mathbb{Z}^5$, where $Q_0 = (b_i \cdot b_j) \in \mathcal{M}_5(\mathbb{Z})$ be its symmetric matrix according to a basis $\{b_1, \cdots, b_5\}$.

Algorithm 3.2.13. *[84] (Simon's algorithm for dimension 5.) Let $Q_0 \in \mathcal{M}_5(\mathbb{Z})$ be a symmetric matrix of determinant $\Delta_0 \neq 0$ whose factorization is known. This algorithm either finds an isotropic subspace of Q_0 of maximal dimension or no solution.*

1. *Compute the signature (r, s) of Q_0. If $r = 0$ or $s = 0$ then there is no real solution. Ensure $s < r$, if $r < s$ replace Q_0 by $-Q_0$ and exchange r and s.*

2. *For each prime divisor p of Δ_0, use Minimization algorithm 3.2.22 to minimize Q_0 (its discriminant). Call Q and Δ as the minimized matrix and the minimized determinant respectively.*

3. *If $\Delta = \pm 1$, apply Algorithm 3.2.15 to find a isotropic subspace of dimension s for Q. Retrieve an isotropic subspace for Q_0 with the same dimension.*

4. *Suppose $\delta = -8|\Delta|$. Calculate generators $\mathfrak{a}_1, \mathfrak{a}_2, \ldots \mathfrak{a}_r$ of the 2-sylow subgroup of the class group $cl(\delta)$ of primitive quadratic forms with discriminant δ using the algorithm from [14].*

5. *For all divisors p of Δ and for all generators $\mathfrak{a}_i$, find Witt invariants $\epsilon_p(\mathfrak{a}_i)$ and an element $\mathfrak{a} = \prod \mathfrak{a}_i^{\alpha_i}$ such that*

$$\epsilon_p(\mathfrak{a}) = -\left((-1)^{(n-1)/2+s} \times 2, p\right)_{\mathbb{Q}_p}$$

for all p dividing Δ.

6. *Write the quadratic form as* $\mathfrak{a} = (a, 2b, c)$ *and*

$$Q_2' = \begin{pmatrix} a & b \\ b & c \end{pmatrix}.$$

7. *Define* $Q_7 = Q \oplus -Q_2'$. *Let* E *be the subspace* $\mathbb{Q}^5$ *of* $\mathbb{Q}^7$. *Minimize* Q_7 *using Minimization algorithm 3.2.22. Suppose* Q_7' *be the corresponding minimized matrix, with determinant* ± 1.

8. *Use Algorithm for unimodular 3.2.14 to find a isotropic subspace* F *for* Q_7' *of dimension* $m = min(r, s+2) \geq 3$.

9. *Find the intersection* $G = E \cap F$ *of dimension* $v = m - 2 \geq 1$ *and find a subspace of dimension* v, *which is isotropic for* Q_0.

3.2.3 Algorithm for unimodular matrix

In this subsection, we describe the Simon's algorithm to solve a quadratic form of determinant ± 1.

Algorithm 3.2.14. *(A solution in unimodular case.) Let* $Q \in \mathcal{M}_5(\mathbb{Z})$ *be a symmetric matrix with determinant* $\Delta = \pm 1$ *and signature* (r, s). *The following algorithm determines a non trivial solution of* $Q(x) = 0$ *if it exists.*

1. *If* $r = 0$ *or* $s = 0$ *there is no solution.*

2. *Use the reduction algorithm from [85]. This algorithm either reduces the quadratic form* Q *or stops with some isotropic vector, if such a vector is found, return it.*

3. *Find the Gram-Schmidt orthogonal basis* $(b_k^*)_{1 \leq k \leq 5}$ *associated to* Q.

4. *Set* $d_0 = 1$. *For* $k = 1 \ldots 5$, *compute*

$$d_k = det(Q_{i,j})_{1 \leq i \leq k, 1 \leq j \leq k}.$$

5. *If* $\frac{d_i}{d_{i-1}} = -\frac{d_j}{d_{j-1}}$ *for some* $i \neq j$ *then return* $b_i^* + b_j^*$.

The following recursive algorithm is used to find a maximal isotropic subspace of dimension $m = 1$ or 2 with basis a $\{b_1, ..., b_{2m-1}\}$.

Algorithm 3.2.15. *(Isotropic subspace in unimodular case.) Let $Q \in \mathcal{M}_5(\mathbb{Z})$ be a symmetric matrix with determinant $\Delta = \pm 1$ and signature (r, s). The following algorithm finds a basis $\{b_1, ..., b_{2m-1}\}$ of $\mathbb{Z}^5$ such that in this basis Q takes the form $Q = H^{\oplus m} \oplus D$ where $m = min(r, s)$, D is a positive or negative definite quadratic form of dimension $5 - 2m$, and $H = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ or $= \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$.*

1. *If $r = 0$ or $s = 0$ or $n \leq 1$, return $D = Q$*
2. *Using Algorithm 3.2.14 find a solution of $x_1^t Q x_1 = 0$. Choose a new basis $x_1 \dots x_5$ including x_1.*
3. *Find a new basis of Q such that Q has the form $Q = H \oplus Q'$ where*

$$H = \begin{pmatrix} 0 & 1 \\ 1 & \epsilon \end{pmatrix}$$

   with $\epsilon = 0$ or 1. Q' has dimension 3, determinant $det(Q') = -det(Q)$ and signature $(r - 1, s - 1)$.
4. *Apply again this algorithm for Q', denote the resulting matrix by R. Return $H \oplus R$.*

3.2.4 An algorithm for minimization :

Let $Q \in \mathcal{M}_5(\mathbb{Z})$ be a symmetric matrix of determinant $\Delta \neq 0$. An aim of this algorithm is to minimize the determinant of Q, reducing either to ± 1 or as small as possible by using linear algebra over Q keeping the coefficient in $\mathbb{Z}$.
We work successively for each divisor of Δ. Let p be a divisor of Δ and $\text{val}_p(\Delta) = v$ be the valuation of Δ at p. Further assume that $\overline{Q}$ is the reduction of Q mod p and $d = \dim_{\mathbb{F}_p} \ker \overline{Q}$ be the dimension of $\ker \overline{Q}$. Then $1 \leq d \leq 5$ and $d \leq v$. After a linear transformation on Q, assume first d columns are divisible by p and then we can write as

$$Q = \begin{pmatrix} p\tilde{Q} & p* \\ p* & U \end{pmatrix}$$

where $\tilde{Q} = (\frac{1}{p} Q_{i,j})_{1 \leq i,j \leq d}$ and $U \in \mathcal{M}_{5-d}(\mathbb{Z})$, is an invertible matrix modulo p.
The following lemmas, which are proved in [84], are used for the minimization of the determinant, which will be used according to the values of d and v. Here we only give the idea from [84] to compute a matrix M corresponding to a basis change of Q.

Lemma 3.2.16. *If $d = 5$, then $Q' = \frac{1}{p}Q \in \mathcal{M}_5(\mathbb{Z})$ and $\det Q' = p^{-5}\Delta$.*

Lemma 3.2.17. *If $d < v$, then there exists an integer $\tilde{d}$ with $1 \leq \tilde{d} \leq d$ and a matrix $M \in \mathcal{M}_5(\mathbb{Q})$ such that $Q' = M^t Q M \in \mathcal{M}_5(\mathbb{Z})$ with $\det Q' = p^{-2\tilde{d}}\Delta$.*

Proof. Let $\tilde{d}$ be the dimension of the matrix $\tilde{Q}$ modulo p, then $1 \leq \tilde{d} \leq d$. By a change of basis we get the first $\tilde{d}$ columns of $\tilde{Q}$ are divisible by p. Extend this basis change to Q. The required matrix M can be taken as a diagonal matrix with first $\tilde{d}$ coefficients equal to $1/p$ and the remaining coefficients equal to 1. □

Lemma 3.2.18. *If $d = v$ is even and $d \geq 2$, then there exists a matrix $M \in \mathcal{M}_5(\mathbb{Q})$ such that $Q' = \frac{1}{p}M^t Q M \in \mathcal{M}_5(\mathbb{Z})$, $Q' \notin \mathcal{M}_n(p\mathbb{Z})$ with $\det Q' = p^{5-2d}\Delta$.*

Proof. The Matrix M can be taken as a diagonal matrix with first d coefficients equal to 1 and the remaining coefficients equal to p. □

Lemma 3.2.19. *If $d = v$ and $d \geq 3$, then there exists a matrix $M \in \mathcal{M}_5(\mathbb{Q})$ such that $Q' = M^t Q M \in \mathcal{M}_5(\mathbb{Z})$ with $\det Q' = p^{-2}\Delta$.*

Proof. By a change of the basis, the first coefficient of $\tilde{Q}$ is divisible by p. Extend this basis to Q. Then we can choose M as a diagonal matrix with first coefficient $1/p$ and remaining coefficients equal to 1. □

Lemma 3.2.20. *If $d = v = 2$ and if $-\det \tilde{Q}$ is a square modulo p, then there exists a matrix $M \in \mathcal{M}_5(\mathbb{Q})$ such that $Q' = M^t Q M \in \mathcal{M}_5(\mathbb{Z})$ with $\det Q' = p^{-v}\Delta$.*

Proof. Similar to Lemma 3.2.19. □

Let m be the maximum dimension of a isotropic subspace for $\overline{U} \mod p$.

Lemma 3.2.21. *Let $d = v = 1$. If $m = (5-d)/2$, then there exists a matrix $M \in \mathcal{M}_5(\mathbb{Q})$ such that $Q' = \frac{1}{p}M^t Q M \in \mathcal{M}_5(\mathbb{Z})$ with $\det Q' = p^{-v}\Delta$.*

Proof. We can choose M as a diagonal matrix with first $d + m$ coefficients equal to 1 and the remaining coefficients equal to p □

Algorithm 3.2.22. *(Minimization algorithm.) This algorithm provides linear transformations on Q to minimize the determinant $\Delta \neq 0$ of a symmetric matrix $Q \in \mathcal{M}_5(\mathbb{Z})$. For each divisor p of Δ, perform the following transformations.*

1. *Apply Lemmas 3.2.16,3.2.17,3.2.18,3.2.19,3.2.20, and 3.2.21 as long as they are applicable.*

2. *Return the new matrix $Q \in \mathcal{M}_5(\mathbb{Z})$ and the matrix $M \in \mathcal{M}_5(\mathbb{Q})$ of the corresponding basis change.*

We observe the following

Theorem 3.2.23. *Simon's algorithm for a quadratic equation of dimension 5 3.2.13 requires time polynomial in* $\log|\Delta|$*, where* Δ *is the determinant of the matrix* Q *representing the quadratic form, when the entries of* Q *are in* $\tilde{\mathbf{O}}(\Delta)$ *and the factorization of* Δ *is known.*

Proof. Simon's algorithm to solve a symmetric quadratic form of dimension 5 discussed in 3.2 consists of three main algorithms: Algorithm for minimization 3.2.22, Algorithm for unimodular case 3.2.14 and algorithm from [14] to compute generators of the 2-Sylow subgroups.
In the algorithm for minimization, we need to perform linear transformations (Lemmas 3.2.16 to 3.2.21) on 5×5 matrix Q for each of the prime divisor of the determinant of Q, this can be done in polynomial time.
The algorithm for unimodular case uses an algorithm from [85] to find a solution. If a solution exists, this algorithm finds a solution in polynomial running time [85] when the discriminant of the Gram matrix is known. Other steps require some linear transformations on Q and computation of Gram-Schmidt orthogonal basis, which are easy to compute.
In order to obtain generators of the 2-Sylow subgroups of the class group $cl(\Delta)$, we can use algorithm from [14], which requires polynomial time in $\log|\Delta|$. □

3.3 Endomorphism under known torsion images

Given an elliptic curve E, computation of an endomorphism of E is an interesting problem both in number theory and in isogeny based cryptography. If we can compute the endomorphism ring of a supersingular elliptic curve, then there is a polynomial-time attack using quaternion algebra [51, 59] to the pure isogeny problems like the Problem 3.1.1. Briefly, to solve Problem 3.1.1, construct the endomorphism ring of both the curves E_0 and E, find a connecting ideal joining two endomorphism rings and translate the ideal into an isogeny path to get an isogeny between E_0 and E_1 as given in [59]. As observed in [50] such an isogeny is sufficient to break the SIDH.
In this section, we consider an endomorphism computation problem but with some extra information as studied in [71]. To be precise, the action of an endomorphism on some torsion subgroup is given. Such a problem looks like the following

Problem 3.3.1. *Let E be a supersingular elliptic curve defined over a finite field $\mathbb{F}_{p^2}$. Let M, N be integers with gcd(M,N)=1 and ϕ be an endomorphism of E of degree M whose action on N-torsion subgroup of E is known. Compute an efficient expression of ϕ.*

3.3.1 Endomorphism of E when only $\mathbb{Z} \subset \mathbf{End}(E)$ is known

In this subsection, we briefly recall an idea from [71] to solve Problem 3.3.1 under the assumption that only endomorphisms that are multiplication by integers are known.
Suppose, E be a supersingular elliptic curve defined over a finite field $\mathbb{F}_{p^2}$. Let ϕ be an endomorphism of E of degree M whose action on N-torsion subgroup of E is known, where $\gcd(N, M) = 1$.
Write $\nu = a\phi + d$ with $a, d \in \mathbb{Z}$ such that the degree of ν is Ne i.e

$$\deg \nu = a^2 \deg \phi + d^2 + ad \ \mathrm{Tr}\phi = Ne$$

or

$$(d + a \ \mathrm{Tr}\phi/2)^2 + a^2(\deg\phi - (\ \mathrm{Tr}\phi/2)^2) = Ne \tag{3.4}$$

Solve Equation 3.4 for a, d such that e is as small as possible. One way to solve this equation is to impose the following condition on parameters

i. $N > 2\sqrt{M}$,

ii. there exists u such that $u^2 \equiv -B \mod N$, where $B = \deg\phi - (\mathrm{Tr}\phi/2)^2$.

First, Tr ϕ can be calculated under the assumption (i). We have $\hat{\phi} \circ \phi = [M]$ and $\phi + \hat{\phi} =$ Tr ϕ. The action of ϕ is known on $E_0[N]$ by assumption. Also ϕ is bijective on $E_0[N]$ because $\gcd(N, M) = 1$, therefore the inverse ϕ^{-1} is well defined and the images of the dual $\hat{\phi}$ is known on $E[N]$. As a result, the trace $\mathrm{Tr}\phi$ is known on $E_0[N]$ and some discrete logarithm solutions are enough to obtain $\mathrm{Tr}\phi \mod N$. Furthermore, the relation $\mathrm{Tr}\phi \leq 2\sqrt{\deg \phi}$ yields $\mathrm{Tr}\phi$ since $N > 2\sqrt{M}$.
Second, Equation 3.4 can be solved under the assumption in (ii). Consider a lattice Λ generated by two vectors $(N, 0)$ and $(u, 1)$. Any point in Λ satisfies the equation $x^2 + By^2 \equiv 0 \mod N$. A reduced basis can be computed by taking a weighted inner product norm weighted the second component by $\sqrt{B}$. Then we can choose a short vector so that the parameters give solution to Equation 3.4 with e small.
Under the following heuristic assumption on the size of the solution of $x^2 + By^2 \equiv 0 \mod N$:

$$xy \approx N \text{ and } x^2 \approx By^2 \approx Ne,$$

a solution is expected to exist with $e \approx \sqrt{M}$.
Any such solution ensures the degree of the endomorphism $\nu = a\phi + d$ in the form Ne and using the technique from Subsection 3.1.2, ν can be expressed as $\nu = \psi \circ \nu_N$ with $\deg \psi = e$ and $\deg \nu_N = N$. Therefore, the required endomorphism is in the form $\phi = (\psi \circ \nu_N - d)/a$.

3.3.2 An endomorphism of $E/\mathbb{F}_p$ under some known torsion images

In this section, we propose a new algorithm to solve Problem 3.3.1 for computing an endomorphism but considering the elliptic curve E to be defined over a finite $\mathbb{F}_p$.
Let E be a supersingular elliptic curve defined over the finite field $\mathbb{F}_p$. Let ϕ be an endomorphism of E of degree M whose action on N-torsion subgroup of E is known, where $\gcd(N, M) = 1$. Suppose $\pi_p : (x, y) \to (x^p, y^p)$ be the p^{th}-power Frobenius endomorphism of E. We fix parameters as $N > 2\sqrt{Mp}$. With this parameters restriction, we hope to get a solution as in Lemmas 3.3.2 and 3.3.3. More precisely, we want to find a solution of Equation 3.5 with $e = \mathbb{O}(1)$.
Substitute $\phi' = \phi - \frac{\mathrm{Tr}\phi}{2}$ with ϕ so that $\mathrm{Tr}\phi' = 0$. Let

$$\delta := \deg \phi' = M - \frac{1}{4}(\mathrm{Tr}\phi)^2.$$

Consider an endomorphism of the form

$$\nu = (a\phi' + b)\pi_p + c\phi' + d$$

of degree

$$\begin{aligned}\deg \nu =& (a^2\delta + b^2)p + (c^2\delta + d^2) + \mathrm{Tr}((a\phi' + b)\pi_p(-c\phi' + d)) \\ =& (a^2\delta + b^2)p + (c^2\delta + d^2) + (ad - bc)\mathrm{Tr}(\phi'\pi_p),\end{aligned}$$

where $a, b, c, d \in \mathbb{Z}$. The relation $N > 2\sqrt{Mp}$ allows us to evaluate $\mathrm{Tr}(\phi'\pi_p)$ as in Subsection 3.3.1. We want the degree of ν to be Ne i.e.

$$(a^2\delta + b^2)p + (c^2\delta + d^2) + (ad - bc)\mathrm{Tr}(\phi'\pi_p) = Ne \tag{3.5}$$

with e is as small as possible. Now, the problem is to find, $a, b, c, d, e \in \mathbb{Z}$ satisfying Equation (3.5). Since there is no known method to solve this

equation in integer, we modify this equation by introducing a new variable f as

$$p\delta a^2 + pb^2 + \delta c^2 + d^2 + \mathrm{Tr}(\phi^{'}\pi_p)ad - \mathrm{Tr}(\phi^{'}\pi_p)bc - Nf^2 = 0 \qquad (3.6)$$

Now, the problem of finding an endomorphism μ reduces to a problem of solving a homogeneous quadratic equation 3.6 in $a, b, c, d, f \in \mathbb{Z}$. A problem is to solve this equation such that f is as small as possible. If we get such a solution, then there exists an endomorphism ν of degree $\deg \nu = Nf^2$.
Equation 3.6 represents a quadratic form, say its matrix be Q with integer entries such that

$$X^t Q X = 0, \qquad (3.7)$$

where

$$Q = \begin{pmatrix} p\delta & 0 & 0 & \mathrm{Tr}(\phi^{'}\pi_p)/2 & 0 \\ 0 & p & -\mathrm{Tr}(\phi^{'}\pi_p)/2 & 0 & 0 \\ 0 & -\mathrm{Tr}(\phi^{'}\pi_p)/2 & \delta & 0 & 0 \\ \mathrm{Tr}(\phi^{'}\pi_p)/2 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & -N \end{pmatrix},$$

which is a symmetric matrix of determinant $\Delta = -N(p\delta - (\mathrm{Tr}(\phi^{'}\pi_p))^2)^2$.
We solve for an integer solution $X^t \in \mathbb{Z}^5$ with f is small.
The symmetric quadratic form can be solved for integer values by using the algorithm given in Section 3.2 or in [85] of Denis Simon when the factorization of Δ is known. This algorithm is implemented in a computer algebra system PARI/GP [9] by the author himself and is given in his website. If the factorization of Δ is unknown then still the quadratic form can be solved by using an algorithm of Castel [17].
From the knowledge of the degree expression as $\deg\nu = Nf^2$, we can calculate $\nu = \psi_{f^2} \circ \nu_N$, where the degree N isogeny ν_N can be computed by using the torsion images of ν on $E[N]$ and the degree f^2 isogeny by the meet in the middle technique as in Section 3.1.2.

Parameters sizes are estimated based on some heuristic assumptions.

Lemma 3.3.2. *There do not exist solutions of Equation 3.6 when $Mp < N$ and heuristically there exist values of M and N with $Mp \approx N$ such that a solution of Equation 3.6 with $f = \mathbb{O}(1)$ is expected to exist, in particular when $N \approx p^2$ and $M \approx p^3$.*

Proof. From Equation 3.5, we have

$$(a^2\delta + b^2)p + (c^2\delta + d^2) + (ad - bc)\mathrm{Tr}(\phi^{'}\pi_p) = Nf^2.$$

For the minimal solution, we expect heuristically the parameters sizes as

$$a^2pM \approx b^2p \approx c^2M \approx d^2 \approx f^2N \text{ and } abcd \approx N \text{ where } \delta \approx M.$$

This gives,

$$a \approx fN^{1/2}p^{-1/2}M^{-1/2},\ b \approx fN^{1/2}p^{-1/2}$$

$$c \approx fN^{1/2}M^{-1/2} \text{ and } d \approx fN^{1/2}.$$

Therefore,

$$N \approx abcd \approx f^4N^2M^{-1}p^{-1}$$

or,

$$f^4 \approx \frac{Mp}{N}.$$

For the a choice $M \approx p^2$ and $N \approx p^3$, we get
$f^4 = \mathbb{O}(1)$. □

Now, we use the technique used in [61] to improve the size of the parameters. We replace N by N^2 in Equation 3.5

$$(a^2\delta + b^2)p + (c^2\delta + d^2) + (ad - bc)\mathrm{Tr}(\phi^{'}\pi_p) = N^2f^2. \tag{3.8}$$

Following the similar size estimation as in Lemma 3.3.2, we get the parameters as follows

Lemma 3.3.3. *There do not exist solutions of Equation 3.8 when $Mp < N^2$ and heuristically there exist values of M and N with $Mp \approx N^2$ such that a solution of Equation 3.8 with $f = \mathbb{O}(1)$ is expected to exist, in particular when $N \approx p$ and $M \approx p$.*

From any integer solution of Equation 3.8, we learn the degree expression as $\deg \nu = N^2f^2$. We want to decompose the endomorphism ν as the composition of two isogenies of degree N and one isogeny of degree f^2. For this, we use the technique from Theorem 3.1.6 and hence we have the following theorem.

Theorem 3.3.4. *Let E be a supersingular elliptic curve defined over a finite field $\mathbb{F}_p$. Let ϕ be an endomorphism of E of degree M whose action on N-torsion subgroup of E is known, where $\gcd(N, M) = 1$ and $N > 2\sqrt{Mp}$. Suppose $\pi_p : (x, y) \to (x^p, y^p)$ be the p^{th}-power Frobenius endomorphism of E. Substitute, $\phi' = \phi - \frac{Tr\phi}{2}$. Then an endomorphism of the form*

$$\nu = (a\phi' + b)\pi_p + c\phi' + d$$

of E with $deg(\nu) = N^2e$ and $\gcd(a\ Tr(\phi'\pi_p) + 2d, N) = h$, where h is a small integer and $e = \mathbb{O}(1)$, is expected to determine according to the heuristic assumption of Lemma 3.3.3. Also with $deg(\nu) = Ne$, $e = \mathbb{O}(1)$ and under the assumption of Lemma 3.3.2, such endomorphism is expected to obtain. In those cases, ϕ can be computed in complexity $\mathbb{O}(\ polylog(p))$.

Proof. When $\deg(\nu) = Ne$, the endomorphism ϕ can be determined as in Subsection 3.1.2.
Suppose $\deg(\nu) = N^2e$. By using the action of ϕ on $E[N]$ and under the assumption $N > 2\sqrt{Mp} > 2\sqrt{M}$, the trace $\mathrm{Tr}\phi$ can be computed and hence the action of ν on $E[N]$ can be computed. Since the degree of ν is N^2e, it can be written as the composition $\nu = \nu'_N \circ \phi_e \circ \nu_N$, where ν'_N, ν_N are isogenies of degree N and ϕ_e is of degree e isogeny. The isogeny ν_N can be computed by using the action of ν on N torsion subgroup of E as in Subsection 3.1.2. To compute the isogeny ν'_N, we use the fact that $\nu(E[N]) \subseteq \ker \nu'_N$ this is true because $\widehat{\nu'_N} \circ \nu = [N] \circ \phi_e \circ \nu_N$. Furthermore, if ν is decomposes as $\nu' \circ [s]$ for some endomorphism ν' and a divisor s of N then s divides h because $\gcd(a\ \mathrm{Tr}(\phi'\pi_p) + 2d, N) = h$. Now by the brute force search for the possible h isogenies, $\ker \nu'_N$ can be calculated. Finally, for each possible ν'_N, a generic meet in middle search can be applied to recover ϕ_e. □

Solutions of Equation 3.8 gives an expression of the degree of the endomorphism $\nu = (a\phi' + b)\pi_p + c\phi' + d$ as N^2f^2. Now, using the fact that it is known on the N-torsion subgroup of E, Theorem 3.3.4 can be used to compute ν in a form $\nu'_N \circ \phi_{f^2} \circ \nu_N$, where ν'_N, ν_N are of degree N and ϕ_{f^2} is of degree f^2 isogenies under an assumption $\gcd(a\ \mathrm{Tr}(\phi'\pi_p) + 2d, N) = h$ with h small. An expression of ϕ' takes the form

$$\phi' = \frac{\nu'_N \circ \phi_{f^2} \circ \nu_N - (b\pi_p + d)}{a\pi_p + c}$$

and using $\phi' = \phi - \mathrm{Tr}(\phi)/2$, the required endomorphism ϕ is given by

$$\phi = \frac{2(\nu'_N \circ \phi_{f^2} \circ \nu_N - (b\pi_p + d)) + (a\pi_p + c)\mathrm{Tr}(\phi)}{a\pi_p + c}.$$

More natural representation of ϕ can be computed by computing its kernel. A basis of the kernel can be computed by supposing $\gcd(M, \deg(a\pi_p + c)) = 1$ and evaluating ϕ on M torsion subgroup of E.
The endomorphism ring of a supersingular elliptic curve over $\mathbb{F}_p$ can be computed in $\tilde{\mathrm{O}}(p^{1/4})$ by the algorithm given in [34]. A solution of Problems 3.6 and 3.8 will not be useful unless the cofactor f^2 satisfies $f^2 = \mathrm{O}(\sqrt{p})$. For the parameters as in Lemmas 3.3.2 and 3.3.3, we use Simon's algorithm to solve Equations 3.6, 3.8. We repeat Simon's algorithm or Castel's algorithm [17] by replacing $T = N$ or N^2 by kT with small integer k unless a solution with $f = \mathrm{O}(1)$ is obtained. A target is to find a solution with f is as small as possible but these algorithms return only a solution satisfying the equations. We hope, under some heuristic, to get a better solution in multiple attempts. We leave for further research for extracting a solution by these algorithms with the last variable f is as small as possible. We summarize the steps in the following algorithm.

Algorithm 3.3.5. *(Computation of an endomorphism)*

1. *Compute Trϕ.*
   Action of ϕ on $E[N]$ is known. Since $\gcd(N, M) = 1$ *therefore $\phi\big|_{E[N]}$ is a bijective map. From $\phi\hat{\phi} = [\deg \phi]$, the action of $\hat{\phi}$ is also known on $E[N]$. Therefore, the Trϕ is also known on $E[N]$ and can be recovered under the assumption $N > 2\sqrt{Mp} > 2\sqrt{M}$.*

2. *Suppose $\phi' = \phi - \frac{Tr\phi}{2}$ and $\delta = deg\ \phi' = M - \frac{1}{4}(Tr\phi)^2$.*

3. *Compute $Tr(\phi'\pi_p)$ as in Step 1 (under the assumption $N > 2\sqrt{Mp}$).*

4. *Consider an endomorphism of E in the form*

$$\nu = (a\phi' + b)\pi_p + c\phi' + d$$

   such that the degree $\deg \nu$ *is of the form deg $\nu = Tf^2$, where $T = N$ or N^2, $\pi_p : (x, y) \to (x^p, y^p)$ is the p^{th}-power Frobenius endomorphism of E and f be an integer to be determined. This gives an equation*

$$p\delta a^2 + pb^2 + \delta c^2 + d^2 + Tr(\phi'\pi_p)ad - Tr(\phi'\pi_p)bc - Tf^2 = 0. \quad (3.9)$$

5. *Equation 3.9 for $a, b, c, d, f \in \mathbb{Z}$ by using Simon's algorithm 3.2. For $T = N^2$ (3.8), choose a and d such that* $\gcd(a\,Tr(\phi^{'}\pi_p) + 2d, N) = h$, *with h is small integer.*

6. *If necessary replace T by kT with small integer k and use Simon's algorithm until kf^2 is as small as possible.*

7. *If $T = kN$ then express ν in a form $\nu = \psi_{kf^2} \circ \nu_N$ such that deg $\psi_{kf^2} = kf^2$ and deg $\nu_N = N$ as in Section 3.1.2. If $T = kN^2$ then express ν in the form $\nu = \nu_N^{'} \circ \phi_{kf^2} \circ \nu_N$, where $\nu_N^{'}, \nu_N$ are of degree N and ϕ_{kf^2} is of degree kf^2 isogenies, by using Theorem 3.3.4.*

8. *The required endomorphism ϕ is given by*

$$\phi = \begin{cases} \frac{2(\nu_N^{'} \circ \phi_{kf^2} \circ \nu_N - (b\pi_p + d)) + (a\pi_p + c)Tr(\phi)}{a\pi_p + c} & \text{if } T = kN^2 \\ \frac{2(\phi_{kf^2} \circ \nu_N - (b\pi_p + d)) + (a\pi_p + c)Tr(\phi)}{a\pi_p + c} & \text{if } T = kN \end{cases} .$$

3.3.3 Conclusion

In this chapter, we proposed a polynomial-time algorithm 3.3.5 to construct an endomorphism of a supersingular elliptic curve defined over $\mathbb{F}_p$ using the torsion information of the endomorphism under certain parameter restriction and heuristic assumptions. This problem was first proposed in [71] and might be interested in computational number theory. While dealing with this problem, we studied Simon's algorithm to solve quadratic equation of dimension 5 and analyzed its complexity (Theorem 3.2.23). We believe that this could be useful to solve certain type of norm equation in an endomorphism ring, and Theorem 3.3.4 could be useful to generate some useful endomorphisms. However, we haven't realized any concrete cryptographic application so far.

Chapter 4

Genus theory and its application on isogeny graph

Genus theory gives the structure of 2-torsion subgroup of the class group of an imaginary quadratic order $\mathcal{O}$ with an aid of existing non-trivial characters in the class group of $\mathcal{O}$. Castryck, Sotáková and Vercauteren use genus theory, in particular, the non-trivial characters to break the decisional Diffie-Hellman problem lying in the action of the ideal class group of $\mathcal{O}$ on a set of elliptic curves [20]. They observed an excellent application of the genus theory to get some information on an ideal class from the corresponding isogeny graph.
In this chapter, we first recall some preliminaries of quadratic forms and genus theory, then we study the values of the non-trivial characters in the 2-torsion subgroup of the maximal order $\mathcal{O}_K$ of an imaginary quadratic field K, and observe how these values give a coloring in the isogeny graph obtained from the 2-torsion subgroup $cl(\mathcal{O}_K)[2]$ of $cl(\mathcal{O}_K)$. We also summarize the idea of Castryck et al. in the class group action, which was a motivation of our work.

4.1 Introduction

In this section, we present some background for the genus theory and see how this gives the structure of 2-torsion subgroup of a class group. Here we mostly follow [28] and restrict our attention to binary quadratic form.

4.1.1 Binary quadratic form

We simply write quadratic form for a quadratic form of two variables.

Definition 4.1.1. *A (binary) quadratic form is a quadratic polynomial expression $Q(x,y) = ax^2 + bxy + cy^2$, where $a, b \in \mathbb{Z}$. The quadratic form Q is called the primitive form if $\gcd(a,b,c) = 1$ and the quantity $\Delta = b^2 - 4ac$ is called the discriminant of Q.*

An equivalence relation on a set of quadratic forms is defined as follows.

Definition 4.1.2. *Two forms $Q(x,y)$ and $R(x,y)$ are equivalent if there are integers p,q,r,s such that $Q(x,y) = R(px+qy, rx+sy)$ and $ps - qr = \pm 1$ and they are called properly equivalent if $ps - qr = 1$.*

We say an integer n is *represented properly* by a form $Q(x,y)$ if the equation $n = Q(x,y)$ has an integer solution (x,y) with $\gcd(x,y) = 1$. If the discriminant $\Delta > 0$ then $Q(x,y)$ represents both positive and negative integers in which case $Q(x,y)$ is called *indefinite* form. If $\Delta < 0$ then the form represents only positive integers or only negative integers in which case $Q(x,y)$ is called *positive definite* or *negative definite* respectively.

Lemma 4.1.3. *[28, Lemma 2.5] Let $\Delta \equiv 0, 1 \mod 4$ be an integer and n be an odd integer such that $\gcd(\Delta, n) = 1$. Then n is properly represented by a primitive form of discriminant Δ if and only if Δ is a quadratic residue modulo n.*

The following theorem gives a group structure to the set of properly equivalent quadratic forms which we call *form class group*.

Theorem 4.1.4. *[28, Theorem 3.9] Let $\Delta \equiv 0, 1 \mod 4$ be a negative integer, and let $cl(\Delta)$ be the set of classes of primitive positive definite forms of discriminant Δ. Then $cl(\Delta)$ is finite abelian group under Dirichlet composition which is called the form class group.*
Furthermore, the identity element of $cl(\Delta)$ is the class containing the principal form

$$\begin{cases} x^2 - \dfrac{\Delta}{4}y^2 & \text{if } \Delta \equiv 0 (mod\ 4) \\ x^2 + xy + \dfrac{1-\Delta}{4}y^2 & \text{if } \Delta \equiv 1 (mod\ 4) \end{cases}$$

and the inverse of the class containing the form $ax^2 + bxy + cy^2$ is the class containing $ax^2 - bxy + cy^2$.

We are interested in the 2-torsion elements of the form class group.

Definition 4.1.5. *[68] A quadratic form $Q(x,y) = ax^2 + bxy + cy^2$ is called an ambiguous form if $a|b$.*

The following two lemmas give the relations between the ambiguous form and the quadratic forms of order at most 2.

Lemma 4.1.6. *The class of a quadratic form $Q = ax^2 + bxy + cy^2$ has order at most 2 if and only if Q is properly equivalent to $Q' = ax^2 - bxy + cy^2$.*

Proof. Follows from Theorem 4.1.4. □

Lemma 4.1.7. *[68] A class of a quadratic form is an ambiguous one (class containing an ambiguous form) if and only if it is self-inverse.*

The following theorem gives that the form class group corresponds to the ideal class group of an order of a quadratic imaginary field and hence the 2-torsion quadratic forms corresponds to the 2-torsion ideal classes.

Theorem 4.1.8. *[28] Let K be an imaginary quadratic field of discriminant Δ_K and $Q(x,y) = ax^2 + bxy + cy^2$ be a primitive positive definite quadratic form of discriminant Δ_K, then $I = [a, (-b + \sqrt{\Delta_K})/2]$ is an ideal of the maximal order $\mathcal{O}_K$ of K and the map sending $Q(x,y)$ to the ideal I induces an isomorphism between the form class group $cl(\Delta_K)$ and the ideal class group $cl(\mathcal{O}_K)$. Furthermore, a positive integer m is represented by a quadratic form if and only if m is the norm of some ideal $\mathfrak{a}$ in the corresponding ideal class.*

We will see that the 2-torsion ideal classes are generated by the ramified primes.

Lemma 4.1.9. *[28, Corollary 5.17] Let K be a quadratic field of discriminant Δ_K, and p be a prime then p ramifies in K if and only if p divides Δ_K.*

We are interested in the relation between the primes above the ramified primes in an imaginary quadratic field K.

Lemma 4.1.10. *Let $p_1, \ldots, p_r$ be the odd prime divisors of the discriminant Δ_K of an imaginary quadratic field $K = \mathbb{Q}(\sqrt{d_K})$, where d_K is a square-free negative integer. Let $(p_i) = \mathfrak{p}_i^2$ in the maximal order $\mathcal{O}_K$ of K for $i = 1, \ldots, r$. Then the 2-torsion elements of the class group $cl(\mathcal{O}_K)[2]$ are generated by the prime above the ramified primes in K. Furthermore,*

i. If $\Delta_K \equiv 1 \mod 4$ then

$$\prod_{i=1}^{r} \mathfrak{p}_i = (\sqrt{d_K})$$

and any $r-1$ elements of $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ generate $cl(\mathcal{O}_K)[2]$.

ii. Let $\Delta_K \equiv 0 \mod 4$, *write* $\Delta_K = 4d_K$. *If* $d_K \equiv 2 \mod 4$, *write* $(2) = (2, \sqrt{d_K})^2$ *then*

$$(2, \sqrt{d_K}) \prod_{i=1}^{r} \mathfrak{p}_i = (\sqrt{d_K}).$$

If $d_K \equiv 3 \mod 4$, *then the product of primes above the odd prime divisors is principal ideal i.e.*

$$\prod_{i=1}^{r} \mathfrak{p}_i = (\sqrt{d_K}).$$

Proof. There is a one to one correspondence between the form class group of discriminant Δ_K and the ideal class group of the maximal order $\mathcal{O}_K$ of K by Theorem 4.1.8. This theorem implies that the 2-torsion form classes correspond to the 2-torsion ideal classes. We now show that these 2-torsion ideal classes are generated by the ramified primes. From Lemmas 4.1.6, 4.1.7, the class of a quadratic form Q has order ≤ 2 if and only if Q is properly equivalent to an ambiguous form, say $Q' = cx^2 + dxy + ey^2$ with $c|d$. By Theorem 4.1.8, the form Q' corresponds to an ideal $J = [c, (-d + \sqrt{\Delta_K})/2]$ of Δ_K with $c|d$. Using $c|d$, we have $\sqrt{\Delta_K} \in J$ and hence the norm of J divides the discriminant Δ_K of the field. Also from Lemma 4.1.9, a prime is ramified in K if and only if it divides the discriminant of K, which implies all the primes occurring in the norm of J are ramified. As a consequence, the 2-torsion forms in the form class group correspond to 2-torsion ideals in the ideal class group, and they are generated by the prime ideals above the ramified primes.
Moreover, for each of the odd prime divisor p_i of Δ_K we can write $(p_i) = \mathfrak{p}_i^2 = (p_i, \sqrt{d_K})^2$ and if 2 divides Δ_K then

- $(2) = (2, \sqrt{d_K})^2$ if d_K is even. This is because $(2, \sqrt{d_K})^2 = (4, 2\sqrt{d_K}, d_K) \subset (2)$.
- $(2) = (2, 1 + \sqrt{d_K})^2$ if d_K is odd. This is because $(2, 1 + \sqrt{d_K})^2 = (4, 2(1 + \sqrt{d_K}), 2\sqrt{d_K} + d_K + 1) \subset (2)$ when d_K is even.

i. Suppose $d_K \equiv 1 \mod 4$ then $\Delta_K = d_K = p_1 \cdots p_r$. This gives

$$\prod_{i=1}^{r} \mathfrak{p}_i = (p_1, \sqrt{d_K}) \cdots (p_r, \sqrt{d_K}) = (\sqrt{d_K}),$$

which implies

$$\mathfrak{p}_i \sim \prod_{j=1, j\neq i}^{r} \mathfrak{p}_j \text{ for } i = 1, \dots r$$

and hence $\{\mathfrak{p}_1, \dots \mathfrak{p}_r\} \setminus \{\mathfrak{p}_i\}$ generates $cl(\mathcal{O}_K)[2]$ for any i.

ii. Suppose $\Delta_K \equiv 0 \mod 4$, write $\Delta_K = 4d_K$. If $d_K \equiv 3 \mod 4$ then

$$\prod_{i=1}^{r} \mathfrak{p}_i = (p_1, \sqrt{d_K}) \cdots (p_r, \sqrt{d_K}) = (\sqrt{d_K}),$$

since

$$d_K = p_1 \cdots p_r \text{ and } \Delta_K = 4d_K$$

for odd prime divisors $p_1, \dots, p_r$.
For $d_K \equiv 2 \mod 4$, we can take $(2) = (2, \sqrt{d_K})^2$ then we have,

$$(2, \sqrt{d_K}) \prod_{i=1}^{r} \mathfrak{p}_i = (2, \sqrt{d_K}) \cdot (p_1, \sqrt{d_K}) \cdots (p_r, \sqrt{d_K}) = (\sqrt{d_K}),$$

since

$$d_K = 2p_1 \cdots p_r \text{ and } \Delta_K = 4d_K.$$

□

4.1.2 Genus theory

Characters play an important role in determining the structure of the 2-torsion class group. The following lemma ensures the existence and the uniqueness of the characters in $(\mathbb{Z}/\Delta\mathbb{Z})^*$.

Lemma 4.1.11. *[28, Lemma 1.14] Let $\Delta \equiv 0, 1 \mod 4$ be a nonzero integer. There exists a unique homomorphism $\chi : (\mathbb{Z}/\Delta\mathbb{Z})^* \to \{\pm 1\}$ given by Legendre symbol as $\chi([p]) = \left(\frac{\Delta}{p}\right)$ for odd primes not dividing Δ and $\chi([-1]) = \pm 1$ according to $\Delta > 0$ and $\Delta < 0$.*

The following theorem tells when a value in $(\mathbb{Z}/\Delta\mathbb{Z})^*$ is represented by a quadratic from of discriminant Δ.

Theorem 4.1.12. *[28] Let $\Delta \equiv 0, 1 \mod 4$ be a negative integer and χ be the character as in Lemma 4.1.11. Then for an odd prime not dividing Δ, $[p] \in ker(\chi)$ if and only if p is represented by one of the quadratic forms in $cl(\Delta)$. Furthermore, the values in $(\mathbb{Z}/\Delta\mathbb{Z})^*$ represented by the principal form of discriminant Δ form a subgroup H of $ker(\chi)$.*

Two forms of discriminant Δ are defined to be in the *same genus* if they represent the same values in $(\mathbb{Z}/\Delta\mathbb{Z})^*$. Since equivalent forms represent same values, they belong to the same genus. The *genus for a coset* $H^{'}$ of H in $\ker(\chi)$ is defined to be a set consisting of all forms of discriminant Δ that represents the values of $H^{'}$ modulo Δ.

Lemma 4.1.13. *[28, Lemma 3.13] The map $\Phi : cl(\Delta) \rightarrow ker(\chi)/H$ sending the class of a quadratic form to the values it represents in $(\mathbb{Z}/\Delta\mathbb{Z})^*$ i.e. the coset of H in $ker(\chi)$, is a group homomorphism.*

By Theorem 4.1.8, we can view the map Φ as a map from the ideal class group $cl(\Delta)$ to $(\mathbb{Z}/\Delta\mathbb{Z})^*$ sending an ideal class to its norm.
The following proposition gives the cardinality of the 2-torsion subgroup of the class group $cl(\Delta)$.

Proposition 4.1.14. *[28, Proposition 3.11] Let $\Delta \equiv 0, 1 \mod 4$ be a negative integer, and r be the number of odd primes dividing Δ. Define the number of assigned characters μ as follows: if $\Delta \equiv 1 \mod 4$, then $\mu = r$ and if $\Delta \equiv 0 \mod 4$, then $\Delta = -4n$, where $n > 0$, and μ id determined by the following table*

n	μ	*assigned characters*
$n \equiv 3 \mod 4$	r	$\chi_1, \ldots, \chi_r$
$n \equiv 1 \mod 4$	$r+1$	$\chi_1, \ldots, \chi_r, \delta$
$n \equiv 2 \mod 8$	$r+1$	$\chi_1, \ldots, \chi_r, \delta\epsilon$
$n \equiv 6 \mod 8$	$r+1$	$\chi_1, \ldots, \chi_r, \epsilon$
$n \equiv 4 \mod 8$	$r+1$	$\chi_1, \ldots, \chi_r, \delta$
$n \equiv 0 \mod 8$	$r+2$	$\chi_1, \ldots, \chi_r, \delta, \epsilon$

where

$$\begin{aligned} \chi_i(a) &= \left(\frac{a}{p_i}\right) \text{ defined for a prime to } p_i, i = 1, \ldots, r \\ \delta(a) &= (-1)^{(a-1)/2} \text{ defined for a odd} \\ \epsilon(a) &= (-1)^{(a^2-1)/8} \text{ defined for a odd.} \end{aligned}$$

Then the class group $cl(\Delta)$ has exactly $2^{\mu-1}$ elements of order ≤ 2.

The *principal genus*, the genus consisting the principal form, corresponds to the classes of squares in the class group by the following theorem.

Theorem 4.1.15. *[28] Let $\Delta \equiv 0, 1 \mod 4$ be a negative integer. Then there are $2^{\mu-1}$ genera of forms of discriminant Δ and the principal genus corresponds to the classes in $cl(\Delta)^2$.*

All the μ characters defined in Proposition 4.1.14 constitute a map

$$\Psi : (\mathbb{Z}/\Delta\mathbb{Z})^* \to \{\pm 1\}^{\mu}$$

defined by all the μ characters in its coordinates i.e.

$$[a] \mapsto (\chi_1(a), \ldots, \chi_\mu(a)),$$

where $\chi_i = \epsilon, \delta,$ or $\delta\epsilon$ for $r < i \leq \mu$ according to Proposition 4.1.14. An important observation is that Ψ is a homomorphism.

Lemma 4.1.16. *[28, Lemma 3.17] The homomorphism $\Psi : (\mathbb{Z}/\Delta\mathbb{Z})^* \to \{\pm 1\}^{\mu}$ is surjective and its kernel is the subgroup H of values represented by the principal form and hence Ψ induces an isomorphism*

$$(\mathbb{Z}/\Delta\mathbb{Z})^*/H \xrightarrow{\sim} \{\pm 1\}^{\mu}.$$

This lemma guarantees that the map Ψ is uniquely determined by the values in $(\mathbb{Z}/\Delta\mathbb{Z})^*$ up to the values that are represented by the principal form of discriminant Δ.

4.2 Graph coloring in some Cayley graphs

4.2.1 Graph coloring

Definition 4.2.1 (Graph Coloring)**.** *A procedure of labeling each vertex of a graph G by colors in such a way that no two adjacent vertices admit the same colors is called graph coloring. The minimum number of colors required to color a graph G is called the chromatic number of the graph.*

We are interested in colorings of a special Cayley graph.

Definition 4.2.2. *(Cayley graph) [60] Let G be a group and X be a generating set of G such that X does not contain the identity element of G and $X = X^{-1} = \{x^{-1} : x \in X\}$. Then the Cayley graph $\Gamma = (G, E)$ is an undirected graph in which the vertices are the elements of G and edges set E consists the edges joining g and gx for any $g \in G$ and $x \in X$, i.e. $E = \{(g, gx) : g \in G, x \in X\}$.*

We will see some examples of Cayley graph.

Definition 4.2.3. *(Hypercube graph)[54] The n-cube or n-dimensional hypercube Q_n is defined recursively by the cartesian product of two graphs as*

$$\begin{aligned} Q_1 &= K_2 \\ Q_n &= K_2 \times Q_{n-1}, \end{aligned}$$

where K_2 is a complete graph with two vertices and one edge. See Figure 4.1 for Q_1 and Q_2 and Figure 4.2 for Q_3.

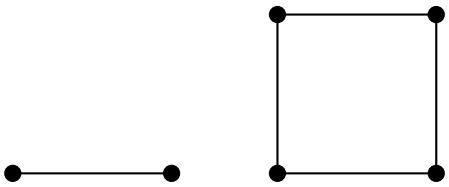

Figure 4.1: Q_1 and Q_2

Example 4.2.4. *The n-dimensional hypercube Q_n can be constructed by the 2^n nodes of the n-dimensional boolean vectors (vectors with binary coordinates 0 or 1) or equivalently by the binary strings of length n, and two nodes are adjacent whenever they differ in exactly one coordinate. In short, the n-cube is the Cayley graph with the group $G = (\mathbb{Z}/2\mathbb{Z})^n$ and a generating set*

$$X = \{(1, 0, \ldots, 0), (0, 1, \ldots, 0), \ldots, (0, 0, \ldots, 1)\}.$$

We extend the definition for Q_0 as a graph having a single vertex and no edge. An n-cube is composed of many hypercubes.

Lemma 4.2.5. *An n-cube is composed of a number $H_{m,n} = 2^{n-m}\binom{n}{m}$ of m-dimensional hypercubes .*

Example 4.2.6. *A 4-cube contains 8 cubes (3-cubes), 24 squares (2-cubes), 32 lines (1-cubes) and 16 vertices (0-cubes).*

We call the *hypercube with longest diagonals*, i.e. the graph obtained from a hypercube by adding edges joining the *farthermost opposite vertices* (with respect to Hamming distance) of the hypercube by Q_n^d. For example, if we identify the vertices with binary string $x_1x_2 \ldots x_n$, then the farthermost opposite vertex can be obtained by the mapping, say an *opposite map*, from a set of n length binary strings to itself:

$$x_1x_2 \ldots x_n \mapsto \bar{x}_1\bar{x}_2 \ldots \bar{x}_n,$$

where

$$\bar{x}_i = \begin{cases} 1 & \text{if } x_i = 0 \\ 0 & \text{if } x_i = 1. \end{cases}$$

See Figure 4.6 for Q_3^d.
From Lemma 4.2.5, the number of $(n-1)$-hypercubes in an n-hypercube is $2n$. Now looking only at the two distinct (no vertices in common) $(n-1)$-cubes and joining their farthermost opposite vertices in their respective $(n-1)$-cubes, we get a graph that we denote as $Q_n^{d,n-1}$. In other words,

$$Q_n^{d,n-1} = K_2 \times Q_{n-1}^d.$$

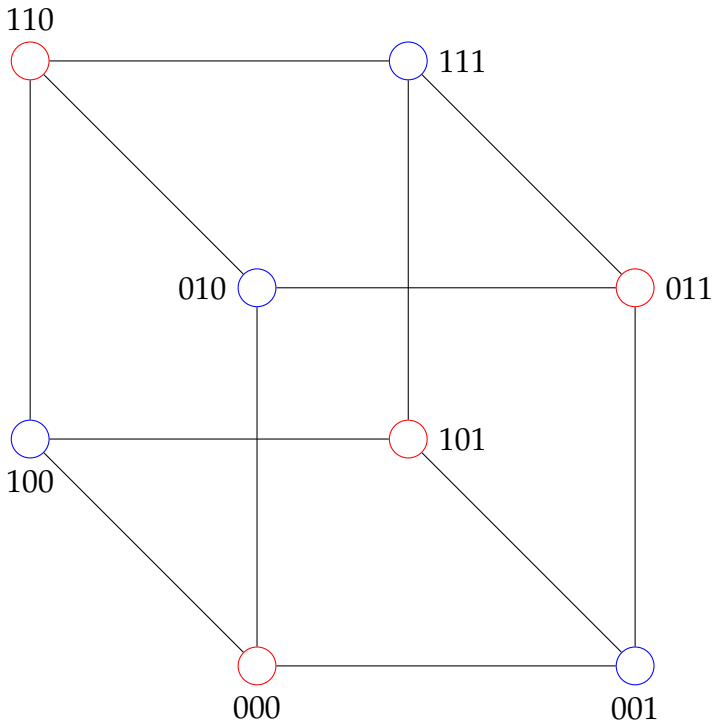

Figure 4.2: Coloring of 3-cube (Q_3)

See $Q_4^{d,3}$ in Figure 4.10.

The chromatic number of hypercube graph is 2 [54]. An idea of a proof is to define the weight, which is the integer $\sum_i x_i$, to each vertex where the vertex is represented by a binary string $x_1 x_2 \dots x_n$ as in Example 4.2.4. Then color the vertices of even weight by the first color and the vertices of odd weight with the second color, see Figure 4.2 for a valid coloring in Q_3.

4.2.2 Coloring a Cayley graph

Let K be a quadratic imaginary field of discriminant $\Delta_K \equiv 0, 1 \mod 4$ and $cl(\mathcal{O}_K)[2]$ be the 2-torsion subgroup of the class group $cl(\mathcal{O}_K)$ of its maximal order $\mathcal{O}_K$.
By the isomorphism between the class group of an order in K and the form class group of discriminant Δ_K, we move from one to another class group according to context.
Suppose $p_1, \dots p_r$ be distinct odd prime divisors of Δ_K and μ is the number of assigned characters, which is r or $r+1$ as in Proposition 4.1.14.

We define the genus coloring map.

Definition 4.2.7. *(Genus coloring map) A map $T : cl(\Delta_K) \to \{\pm 1\}^{\mu}$ defined by the composition $T = \Psi' \circ \Phi$, where $\Phi : cl(\Delta_K) \to ker(\chi)/H$ sends the class of a quadratic form of discriminant Δ_K to the coset it represents and Ψ' is an isomorphism deduced from Ψ from Lemma 4.1.16. The map T, which gives μ tuple of values in $\{\pm 1\}^{\mu}$, is defined as a genus coloring map.*

The kernel of T is the kernel of Φ, which is the set of squares in $cl(\Delta_K)$ by Theorem 4.1.15. If we are considering the map T from the corresponding ideal class group then it maps an ideal class to a tuple of Legendre/Kronecker symbols attached to its norm. We will apply the genus coloring map to a Cayley graph.

Now we define the Cayley graph in our context. We construct Cayley graph with the group $G = cl(\mathcal{O}_K)[2]$ and the generating set $X = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ of G, where $\mathfrak{p}_i$ are the primes above the ramified primes p_i in K for $i = 1, \ldots, n$. We color the vertices of the Cayley graph by the map T, then T assigns values to each of the ideal classes in G which we say coloring of the vertices.
We name the Cayley graph constructed by taking the group $G = \langle \mathfrak{p}_1, \ldots, \mathfrak{p}_n \rangle$ and the generating set $X = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ as a $\{p_1, \ldots, p_n\}$ graph. We are interested in the following question:

Problem 4.2.8. *Determine whether the coloring of the $\{p_1, \ldots, p_n\}$ graph obtained by the genus coloring map T is valid or not. If coloring is not valid in general, then identify the cases when the coloring is valid.*

We will study Problem 4.2.8 for the $\{p_1, \ldots, p_n\}$ graph associated with the 2-torsion subgroup of the class group of the maximal order $\mathcal{O}_K$ of an imaginary quadratic field K.
Coloring of the $\{p_1, \ldots, p_n\}$ graph depends on the relation between the ramified primes in K because this determines when two ideals belong to the same genus. Two ideal classes have the same value (color) by the genus coloring map T if and only if they belong to the same genus.

Lemma 4.2.9. *Let $cl(\mathcal{O}_K)[2]$ be the 2-torsion subgroup of the class group of the maximal order $\mathcal{O}_K$ of an imaginary quadratic field K. Then for any $\mathfrak{p}, \mathfrak{q} \in cl(\mathcal{O}_K)[2]$ belong to the same genus if and only if $\mathfrak{pq} \in cl(\mathcal{O}_K)^2$.*

Proof. Let $\mathfrak{p}, \mathfrak{q} \in cl(\mathcal{O}_K)[2]$ such that $\mathfrak{p}, \mathfrak{q}$ belong to the same coset $H' \in$

$cl(\mathcal{O}_K)/cl(\mathcal{O}_K)^2$. Let T be the genus coloring map. Then,

$$\begin{aligned} & \mathfrak{p}, \mathfrak{q} \in H^{'} \\ \iff & T(\mathfrak{p}) = T(\mathfrak{q}) \\ \iff & T(\mathfrak{pq}) = e, \text{ where } e \text{ is the identity of } \{\pm 1\}^{\mu} \\ \iff & \mathfrak{pq} \in cl(\mathcal{O}_K)^2, \text{ the kernel of } T. \end{aligned}$$

□

We study $\{p_1, \ldots, p_n\}$ and $\{p_1, \ldots, p_{n-1}\}$ graphs by taking ramified primes p_i. The former is interesting because those are all the ramified primes, and the latter is interesting because those $n-1$ primes are sufficient to generate the 2-torsion class group. We start with some examples of colorings in small graphs where, coloring is valid without further restrictions except the assumption that each of the prime ideal belongs to a different genus than the principal one.

Example 4.2.10. *Let $\Delta_K \equiv 1 \mod 4$ be the discriminant of the imaginary quadratic field K. Let p_1, p_2 be the odd prime divisors of the discriminant Δ_K of K. Let $(p_i) = \mathfrak{p}_i^2$ in the maximal order $\mathcal{O}_K$ of K for $i = 1, 2$. Then the colorings given by T in $\{p_1\}, \{p_2\}$ and $\{p_1, p_2\}$ graphs are valid colorings if and only if $\mathfrak{p}_i \notin cl(\Delta_K)^2$ for $i = 1, 2$.*

Proof. By Lemma 4.1.10 $\mathfrak{p}_1 \sim \mathfrak{p}_2$, therefore we can write $cl(\mathcal{O}_K)[2] = \langle \mathfrak{p}_1 \rangle$. Suppose $\mathfrak{p}_1 \notin cl(\mathcal{O}_K)^2$. Then $\mathfrak{p}_1$ and the principal ideal class $[(1)]$ lie in different genera. By genus theory, there are $2^{\mu-1} = 2$ colors $(1,1)$ and $(-1,-1)$ for the 2 genera, which are cosets of $cl(\mathcal{O}_K)^2$ in $cl(\mathcal{O}_K)$. Therefore, we have

$$T(\mathfrak{p}_1) = T(\mathfrak{p}_2) = (-1,-1) \text{ and } T([(1)]) = (1,1),$$

Figure 4.3: $\{p_1\} = \{p_2\} = \{p_1, p_2\}$ graph

which shows that the coloring in the $\{p_1\} = \{p_2\} = \{p_1, p_2\}$ graph is valid, see Figure 4.3.

□

Example 4.2.11. *Let $\Delta_K \equiv 1 \mod 4$ be the discriminant of the imaginary quadratic field K. Let p_1, p_2, p_3 are odd prime divisors of Δ_K. Let $(p_i) = \mathfrak{p}_i^2$ for $i = 1, \ldots, 3$. The colorings given by the genus coloring map T have following possible cases:*

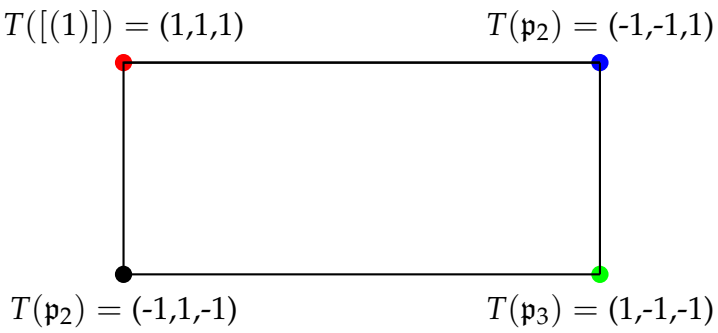

Figure 4.4: $\{p_1, p_2\}$ graph for $\mu = 3$

- *If any one of the $\mathfrak{p}_i$ is square then the coloring is not valid in $\{p_1, p_2, p_3\}$, $\{p_1, p_2\}, \{p_1, p_3\}$ and $\{p_2, p_3\}$ graph.*
- *If none of the $\mathfrak{p}_i$ are squares, then the colorings in $\{p_1, p_2, p_3\}, \{p_1, p_2\}, \{p_1, p_3\}$ and $\{p_2, p_3\}$ graphs are valid colorings.*

Proof. There are $\#cl(\mathcal{O}_K)[2] = 4$ genera and hence 4 possible colorings

$$(1,1,1), (1,-1,-1), (-1,-1,1), (-1,1,-1).$$

Suppose $cl(\mathcal{O}_K)[2] = \langle \mathfrak{p}_1, \mathfrak{p}_2 \rangle$. Other generating sets give similar coloring situation.

- If one of $\mathfrak{p}_1$ or $\mathfrak{p}_2 \in cl(\mathcal{O}_K)^2$, the coloring map does not give a valid coloring in $\{p_1, p_2\}$ graph.
- Suppose $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3 \notin cl(\mathcal{O}_K)^2$. Then

  $$\mathfrak{p}_1\mathfrak{p}_2 = \mathfrak{p}_3 \notin cl(\mathcal{O}_K)^2$$

  and therefore $\mathfrak{p}_1$ and $\mathfrak{p}_2$ lie in different genera and hence have different color. For example

  $$T([(1)]) = (1,1,1), T(\mathfrak{p}_1) = (-1,-1,1), T(\mathfrak{p}_2) = (-1,1,-1) \text{ and}$$
  $$T(\mathfrak{p}_1\mathfrak{p}_2) = (1,-1,-1).$$

  In this case, the colorings in $\{p_1, p_2\}$ and in $\{p_1, p_2, p_3\}$ graphs are valid, see Figure 4.4 and Figure 4.5.

□

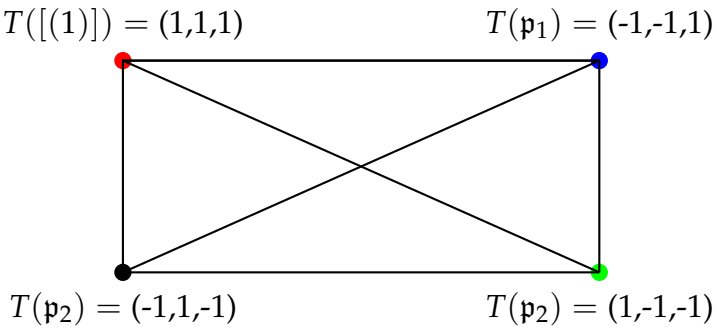

Figure 4.5: $\{p_1, p_2, p_3\}$ graph for $\mu = 3$

Example 4.2.12. *Suppose* $K = \mathbb{Q}(\sqrt{-3 \cdot 13 \cdot 17}) = \mathbb{Q}(a)$. *Then the class group is of order* 16 *with structure* $C_8 \times C_2 = \langle x \rangle \times \langle y \rangle$, *where* x *and* y *are generators of* C_8 *and* C_2 *respectively in the structure of the class group. Let*

$$(3) = \mathfrak{p}_1^2, (13) = \mathfrak{p}_2^2, \text{ and } (17) = \mathfrak{p}_3^2,$$

where

$$\mathfrak{p}_1 = (3, 1/2a + 3/2), \mathfrak{p}_2 = (13, 1/2a + 13/2), \mathfrak{p}_3 = (17, 1/2a + 17/2).$$

Here $y \sim \mathfrak{p}_3$ *and* $\mathfrak{p}_2 \in cl(\mathcal{O}_K)^2$, *the principal genus, since* $x^4 \sim \mathfrak{p}_2$. *Also* $\mathfrak{p}_1\mathfrak{p}_3 = \mathfrak{p}_2 \in cl(\mathcal{O}_K)^2$, *therefore* $\mathfrak{p}_1$ *and* $\mathfrak{p}_3$ *belong to the same genus. We have,*

$T(\mathfrak{p}_1) = (-1, 1, -1), T(\mathfrak{p}_2) = (1, 1, 1), T(\mathfrak{p}_3) = (-1, 1, -1)$.

Hence, coloring in the $\{p_1, p_3\}$ *graph is valid but not in* $\{p_1, p_2\}$, $\{p_2, p_3\}$ $\{p_1, p_2, p_3\}$ *graphs.*

Example 4.2.13. *Suppose* $K = \mathbb{Q}(\sqrt{-3 \cdot 5 \cdot 17}) = \mathbb{Q}(a)$. *Then the class group is of order* 12 *with structure* $C_6 \times C_2 = \langle x \rangle \times \langle y \rangle$, *where* x *and* y *are generators of* C_6 *and* C_2 *respectively in the structure of the class group. Let*

$$(3) = \mathfrak{p}_1^2, (5) = \mathfrak{p}_2^2, \text{ and } (17) = \mathfrak{p}_3^2.$$

$$\mathfrak{p}_1 = (3, 1/2a + 3/2), \mathfrak{p}_2 = (5, 1/2a + 5/2), \mathfrak{p}_3 = (17, 1/2a + 17/2).$$

$x^3 \sim \mathfrak{p}_3$ *and* $y \sim \mathfrak{p}_2$. *Here* $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3 \notin cl(\mathcal{O})^2$ *and*

$$T(\mathfrak{p}_1) = (1, -1, -1), T(\mathfrak{p}_2) = (-1, 1, -1), T(\mathfrak{p}_3) = (-1, -1, 1).$$

Therefore, colorings in the $\{p_1, p_2\}$, $\{p_1, p_3\}$, $\{p_2, p_3\}$ *and* $\{p_1, p_2, p_3\}$ *graphs are valid.*

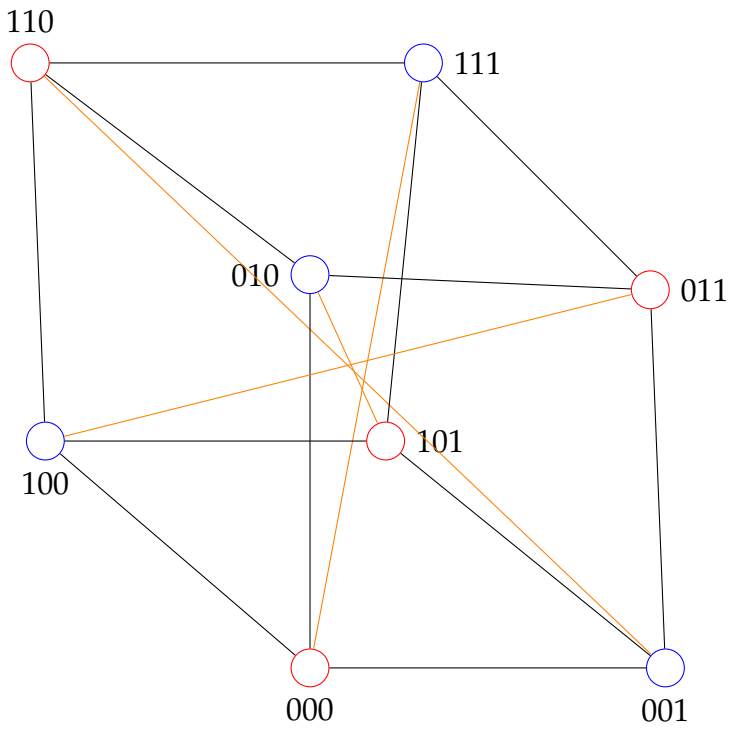

Figure 4.6: 3 cube with longest diagonals

Now, we observe the general case. In many cases, the $\{p_1, \ldots, p_n\}$ graph is a hypercube graph which can be colored with 2 colors and, in some cases, the graph resembles the hypercube but having more edges, which might require more than two colors to color the graph. As observed before, the chromatic number of any hypercube is 2, but if we add more edges in this cube, then the resulting graph may or may not be 2-colorable.

Lemma 4.2.14. *The chromatic number of the graph Q_n^d is 2 when n is odd and is greater than 2 and at most 4 when n is even.*

Proof. Let n is odd then the opposite map sends vertices of even weight to vertices of odd weight and vice versa. Therefore, coloring the vertices of even weight to one color and those of odd weight by another color gives a valid coloring with chromatic number two. For example see Figure 4.6 for $n = 3$.
Let n is even. Then Q_n^d has cycles of odd length and hence is not 2 colorable by using the argument that a graph is 2 colorable if and only if it does not have a cycle of odd length [54].
Furthermore, when n is even, the opposite map does not change the parity

of the weight of the vertices. Giving two colors for even and odd weighted vertices in the n-hypercube as above and while adding the longest diagonals, we assign two more colors; one for one of the opposite vertices of even weight and one for that of odd weight vertices, we see that the graph can be colored with 4 colors. □

Chromatic number of Q_n^d is known when n is even.

Proposition 4.2.15. *The chromatic number of Q_n^d is 4 when n is even.*

Proof. See the discussion in [86, pp. 308-309]. □

Lemma 4.2.16. *Let $\Delta_K \equiv 1 \mod 4$ be the discriminant of the imaginary quadratic field K. Let $p_1, \ldots, p_r$ be the odd prime divisors of the discriminant Δ_K of K and $\mathcal{O}_K$ be the maximal order of K. Let $(p_i) = \mathfrak{p}_i^2$ in $\mathcal{O}_K$. Using the coloring map T, the coloring in $\{p_1, \ldots, \tilde{p}_i, \ldots, p_r\}$, a set without p_i, graph for any $1 \leq i \leq r$ is valid if and only if none of the $\mathfrak{p}_j$, with $j \neq i$ belongs to the principal genus.*

Proof. By definition of the $\{p_1, \ldots, \tilde{p}_i, \ldots, p_r\}$ graph, there is an edge between any two elements $A, B \in cl(\mathcal{O}_K)[2]$ if and only if $B = \mathfrak{p}A$ for some $\mathfrak{p} \in X = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_{r-1}\}$. Adjacent vertices A and B have different colors if and only of $A\mathfrak{p}A \notin cl(\mathcal{O})^2$ by Lemma 4.2.9 which is true if and only if $\mathfrak{p} \notin cl(\mathcal{O})^2$. □

Theorem 4.2.17. *Let $\Delta_K \equiv 1 \mod 4$ be the discriminant of the imaginary quadratic field K. Let $p_1, \ldots, p_r$ be the odd prime divisors of the discriminant Δ_K of K and $\mathcal{O}_K$ be the maximal order of K. Let $(p_i) = \mathfrak{p}_i^2$ in $\mathcal{O}_K$. Then, there are the following possible cases if the coloring is done by the coloring map T.*

i. From p_i's, consider any set with $r-1$ elements, without loss of generality, let this set be $\{p_1, \ldots, p_{r-1}\}$. Then the $\{p_1, \ldots, p_{r-1}\}$ graph is $(r-1)$ hypercube graph Q_{r-1}. If $\mathfrak{p}_i \notin cl(\mathcal{O}_K)^2$ for $i = 1, \ldots, r-1$ then the coloring is valid and only attains the chromatic number of the $(r-1)$-hypercube if all the $\mathfrak{p}_i$ belong to the same genus. For $r = 4$, see in `https://github.com/mgyawali/Graph_coloring`.

ii. The $\{p_1, \ldots, p_r\}$ graph is $(r-1)$-hypercube with longest diagonals Q_{r-1}^d. Suppose $\mathfrak{p}_i \notin cl(\mathcal{O}_K)^2$ for $i = 1, \ldots, r$ and $r \geq 2$. Then the coloring is valid, the chromatic number is 2 when r is even and all of these r prime ideals belong to a non-principal genus; and the chromatic number is 4 when r is odd and these r prime ideals belong to two different non-principal genera.

Proof. i. Suppose $\mathfrak{p}_i \notin cl(\mathcal{O}_K)^2$ for $i = 1, \ldots, r-1$. Then the $\{p_1, \ldots, p_{r-1}\}$ graph admits a valid coloring by Lemma 4.2.16. Now we prove how the coloring map provides the chromatic number of the $(r-1)$-hypercube.

Recalling a representation of the vertices of an n-hypercube by the binary strings of length n from Example 4.2.4, we can see the lattice view of the graph, see Example 4.7 for $r = 5$, divided in labels, where we say a string $A = x_1 x_2 \ldots x_n$ lie in level m for $0 \leq m \leq n$ if A has m number of 1's. Now we can see the lattice view of the $\{p_1, \ldots, p_{r-1}\}$ graph, which is a $r-1$ cube and there are product of k prime ideals in level k.

Suppose all the $\mathfrak{p}_i$ belong to the same genus. The coloring to each of the vertices are determined when the coloring of the prime ideals $\mathfrak{p}_1, \ldots \mathfrak{p}_{r-1}$, which are $T(\mathfrak{p}_1), \ldots T(\mathfrak{p}_{r-1})$, are assigned because T is homomorphism.

We have the color $(1, \ldots, 1)$ having all the coordinate 1 to the vertex at level 0, which is denoted as a binary string of length n as $00 \ldots 0$ corresponding to the principal ideal class $[(1)]$. Since all the prime ideals $\mathfrak{p}_1, \ldots \mathfrak{p}_{r-1}$ belong to the same genus, the complete character T maps each of these primes to the same values in $\{\pm 1\}^{r-1}$ and thus all have same color i.e.

$$T(\mathfrak{p}_1) = T(\mathfrak{p}_2) = \ldots = T(\mathfrak{p}_{\mu-1})$$

in the level 1. In the second level, the vertices are formed with the product of two prime ideals, therefore

$$T(\mathfrak{p}_i \mathfrak{p}_j) = (1, \ldots, 1) \text{ for all } i \neq j,$$

which is different than the color in level 1. In level 3, we have the product of three prime ideals, therefore the color at this level must be equal to the color at level 1,

$$T(\mathfrak{p}_i \mathfrak{p}_j \mathfrak{p}_k) = \mathfrak{p}_1 \text{ for any choice of three prime ideals.}$$

In general, in level $i \geq 1$ and for any i choices of prime ideals $\mathfrak{p}_1, \ldots \mathfrak{p}_i$, we have

$$T(\mathfrak{p}_1 \cdots \mathfrak{p}_i) = (1, \ldots, 1) \text{ if } i \text{ is even}$$
$$T(\mathfrak{p}_1 \cdots \mathfrak{p}_i) = T(\mathfrak{p}_1) \text{ if } i \text{ is odd.}$$

Hence, the graph is 2-colorable, see in 4.9 for $r = 4$ and in 4.7 for $r = 5$.

ii. The $\{p_1, \ldots, p_r\}$ graph is also a $r-1$ hypercube graph with 2^{r-1} vertices as above but there are $2^{r-2}(r-1) + 2^{r-2} = 2^{r-2}r$ edges, so there are 2^{r-2} more edges than $\{p_1, \ldots, p_{r-1}\}$ graph and these extra edges are the longest diagonals by using the fact $\mathfrak{p}_r = \mathfrak{p}_1 \cdots \mathfrak{p}_{r-1}$ from Lemma 4.1.10.
When r is odd, then all the $\mathfrak{p}_i$ can not belong to the same genus because the relation $\mathfrak{p}_r = \mathfrak{p}_1 \cdots \mathfrak{p}_{r-1}$ implies that if $r-1$ prime ideals belong to the same genus then the r^{th} of them must belong to the principal genus which is a contradiction. Hence, at least two of the prime ideals must belong to different genera and attains at least four colors that are similar to the proof of the part (i).
Suppose r is even, and all of the r prime ideals belong to a non-principal genus. Then, the graph is 2-colorable that can be proved similarly as in part (i), see Figure 4.8 for $r = 4$.

□

From Theorem 4.2.17, the $\{p_1, \ldots, p_r\}$ graph is either $(r-1)$-hypercube or $(r-1)$-hypercube with longest diagonals when $\Delta_K \equiv 1 \mod 4$.
Now consider the case where $\Delta_K \equiv 0 \mod 4$. In this case, 2 is also ramified. We have $\#cl(\mathcal{O}_K)[2] = 2^{\mu-1}$, where μ is the number of distinct prime divisors and $cl(\mathcal{O}_K)[2] = \langle \mathfrak{c}, \mathfrak{p}_1, \ldots, \mathfrak{p}_r \rangle$, where $\mathfrak{c}$ is prime above 2. In this case, the graph is still hypercube but with some more edges as in the previous cases.

Lemma 4.2.18. *The graph $Q_n^{d,n-1}$ has chromatic number 2 when $n > 3$ is even.*

Proof. Similar arguments as in Lemma 4.2.14. See also Figures 4.10 and 4.11 for particular cases when $n = 4$, where the extra edges than a 4 hypercube are the edges connecting to opposite vertices to one lower dimensional hypercube i.e. 3 hypercubes. In this example, the graph is $Q_4^{d,3}$. □

When $n > 2$ is even, then in Lemma 4.2.14, we conjectured that the chromatic number of Q_n^d has chromatic number 4. When n is odd, then $n-1$ is even and from the relation $Q_n^{d,n-1} = K_2 \times Q_{n-1}^d$, we expect that the chromatic number of $Q_n^{d,n-1}$ is also 4 because K_2 does not change the chromatic number.

Theorem 4.2.19. *Let $\Delta_K \equiv 0 \mod 4$ be the discriminant of imaginary quadratic field $K = Q(\sqrt{d_K})$. Let $p_1, \ldots, p_r$ be the odd prime divisors of the discriminant Δ_K of the maximal order $\mathcal{O}_K$. Let $(p_i) = \mathfrak{p}_i^2$, $(2) = \mathfrak{c}^2$ in $\mathcal{O}_K$. Write $\Delta_K = 4d_K$.*

i. When $d_K \equiv 3 \mod 4$,

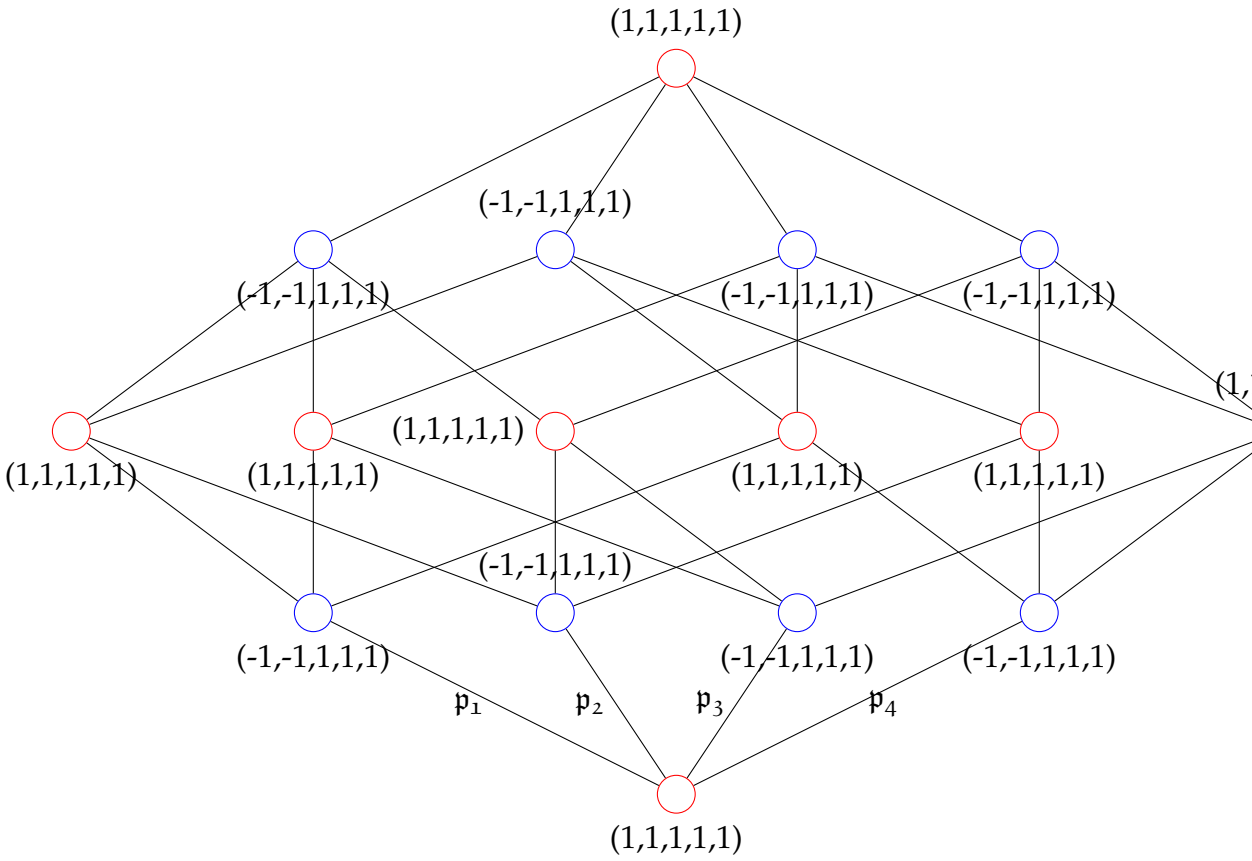

Figure 4.7: A $\{p_1, \ldots, p_4\}$ graph for $\mu = 5$

- *Let* $\mathfrak{c}, \mathfrak{p}_i \notin cl(\mathcal{O}_K)^2$ *for* $i = 1, \ldots, r-1$. *The* $\{2, p_1 \ldots, p_{r-1}\}$ *graph is* Q_r *and coloring is valid for any choice of* $r-1$ *odd prime divisors and the chromatic number* 2 *is attained when all the prime ideals belong to the same non-principal genus.*
- *Let* $\mathfrak{c}, \mathfrak{p}_i \notin cl(\mathcal{O}_K)^2$ *for* $i = 1, \ldots, r$. *Then the* $\{2, p_1 \ldots, p_r\}$ *graph is* $Q_r^{d,r-1}$ *and the coloring is valid. Moreover, when* r *and all the prime ideals belong to the same genus, then the chromatic number is* 2 *(see Fig 4.11). When* r *is odd, and if one of the prime ideals in* $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ *belongs to a genus which is different from the genus of the remaining ideals, then the graph attains 4 colors.*

ii. When $d_K \equiv 2 \mod 8$, *coloring in* $\{2, p_1, \ldots, p_r\}$ *graph and any* r *subset graph have similar cases as in Theorem 4.2.17 for* $\mu = r + 1$.

iii. When $d_K \equiv 6 \mod 8$, *coloring behavior is similar in* $\{2, p_1, \ldots, p_r\}$ *graph*

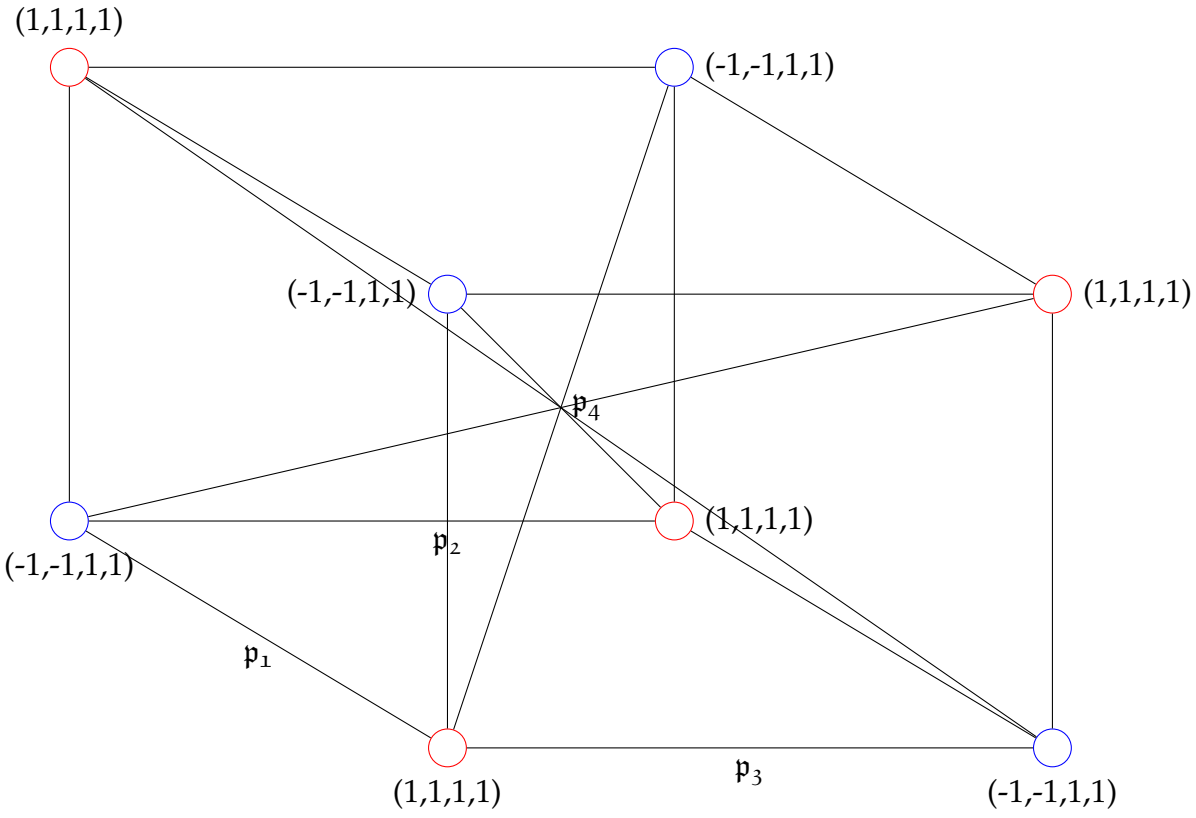

Figure 4.8: A $\{p_1, p_2, p_3, p_4\}$ graph for $\mu = 4$

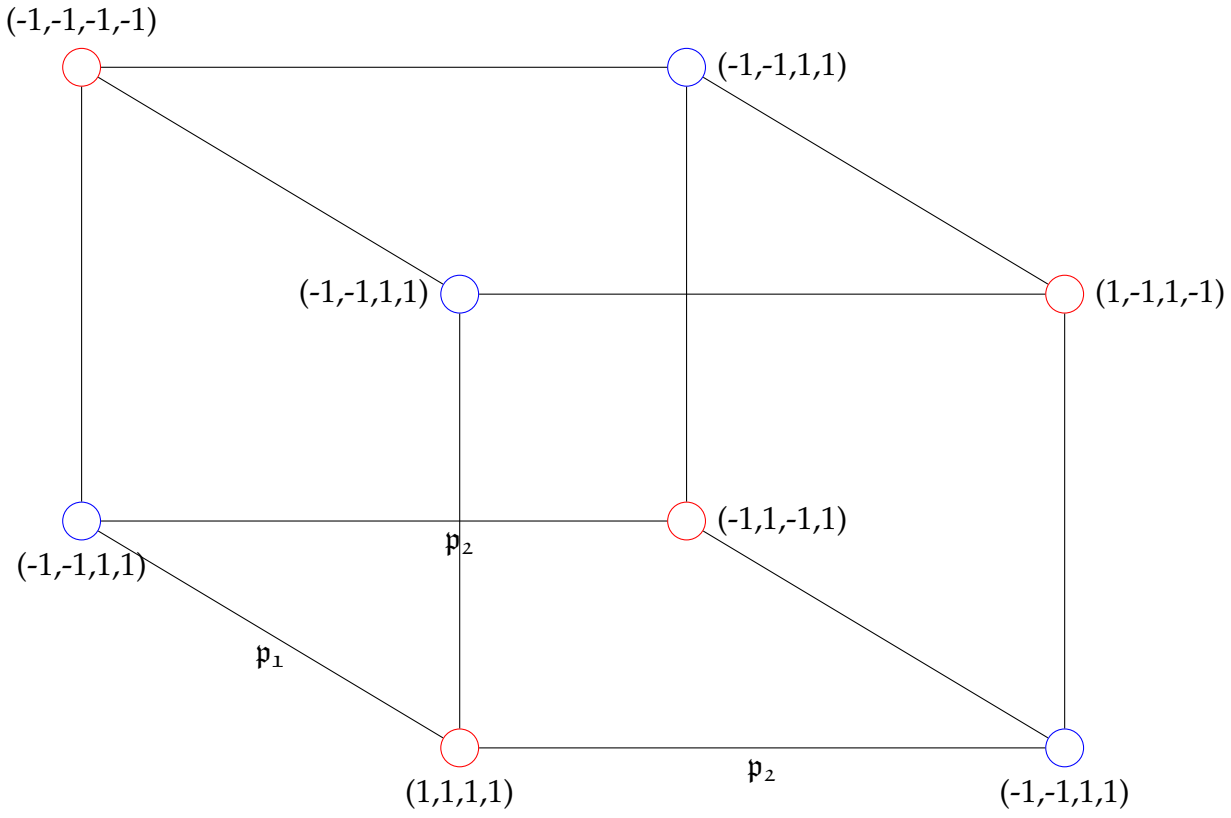

Figure 4.9: A $\{p_1, p_2, p_3\}$ graph for $\mu = 4$

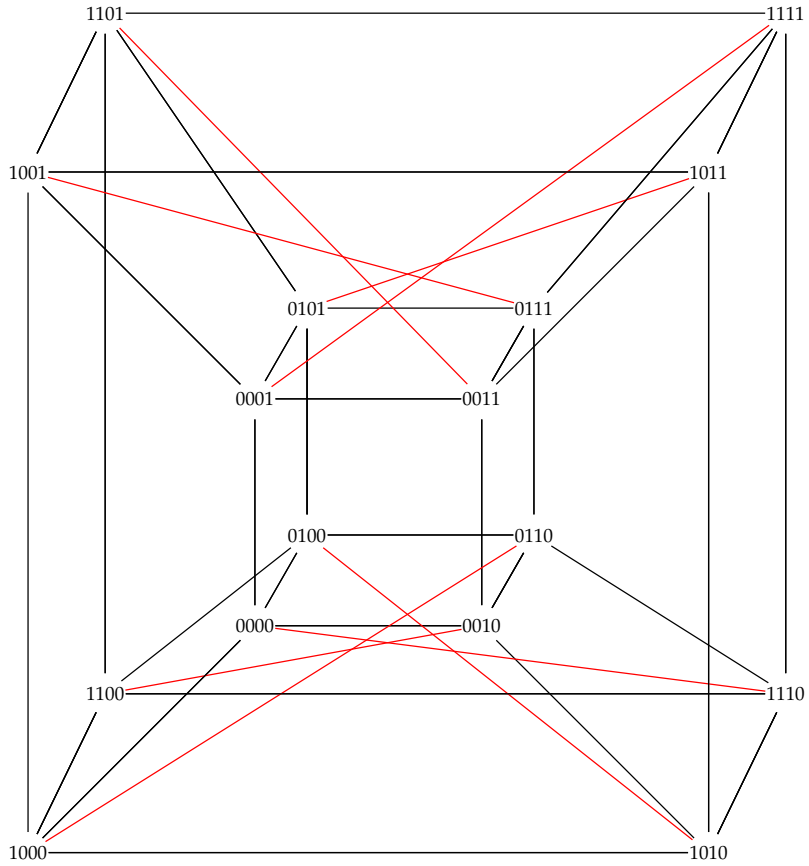

Figure 4.10: 4-cube with edges connecting to opposite vertices in two distinct 3-cube: $(Q_4^{d,3})$.

as in the case of Theorem 4.2.17 for $\mu = r + 1$.

Proof. i. Suppose $d_K \equiv 3 \mod 4$. Then there are $r+1$ characters and $\#cl(\mathcal{O}_K)[2] = 2^r$ by Proposition 4.1.14. Also by Lemma 4.1.10, we have

$$\prod_{i=1}^{r} \mathfrak{p}_i = (\sqrt{d_K}).$$

These facts imply that the rest of the arguments are similar to Theorem 4.2.17.

ii. When $d_K \equiv 2 \mod 8$, coloring in $\{2, p_1, \ldots, p_r\}$ graph and any r subset graph have similar cases as in Theorem 4.2.17 since $\mu = r + 1$ and $(2, \sqrt{d_K})\mathfrak{p}_1 \cdots \mathfrak{p}_r = (\sqrt{d_K})$ and $\#cl(\mathcal{O}_K[2]) = 2^r$.

iii. When $d_K \equiv 6 \mod 8$, coloring is valid in $\{2, p_1, \ldots, p_r\}$ graph as in the case of Theorem 4.2.17 by using the fact that $\mu = r + 1$ and $(2, \sqrt{d_K})\mathfrak{p}_1 \cdots \mathfrak{p}_r = (\sqrt{d_K})$ and $\#cl(\mathcal{O}_K[2]) = 2^r$.

□

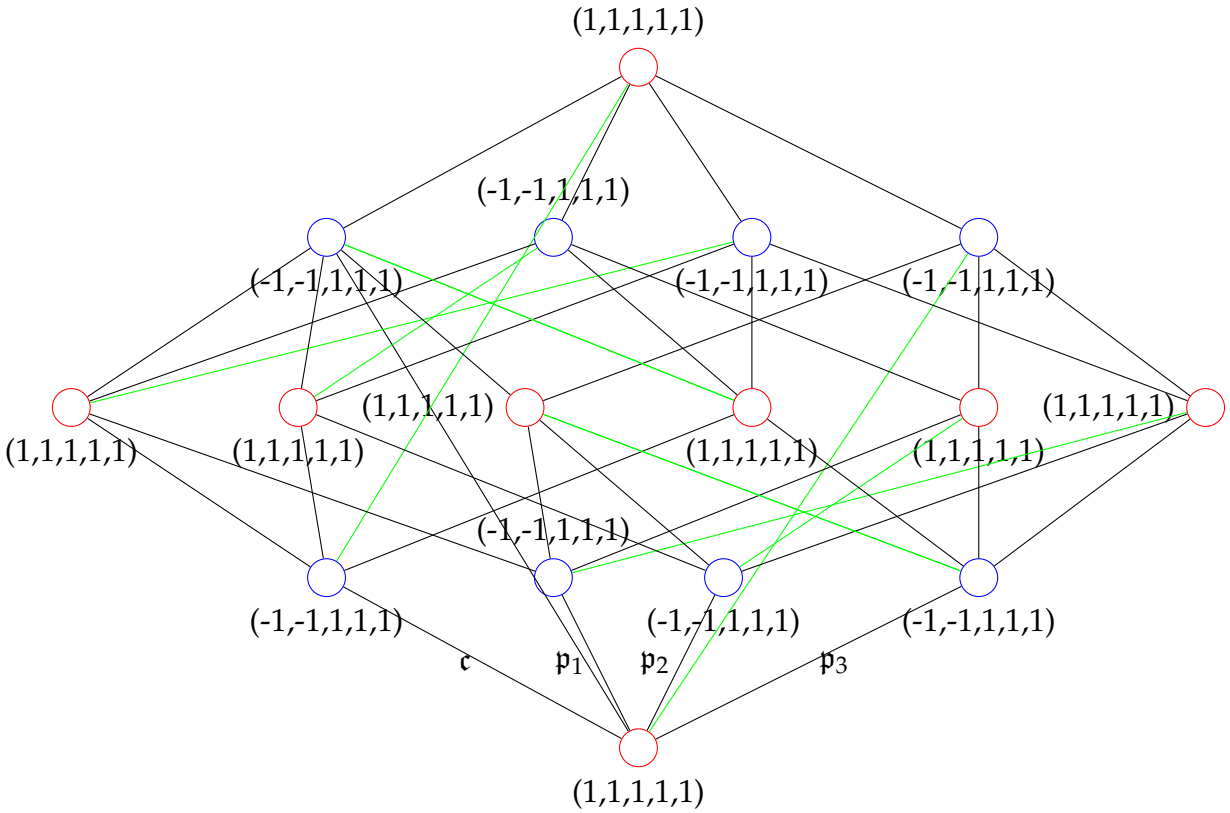

Figure 4.11: $\{2, p_1, p_2, p_3, p_4\}$ graph for $r = 4$ when $\Delta \equiv 0 \mod 4$

4.3 Isogeny Graph

In this section, we study isogeny graph from ramified primes.
We revisit the isogeny graph.

Definition 4.3.1. *(Isogeny graph). An isogeny graph is a graph with a vertex set consisting of isomorphic classes of elliptic curves, and the edges set consisting of isogenies between the elliptic curves.*

We are interested in the isogeny graph with isogenies of degree equal to the norm of ramified primes. Let E be an elliptic curve over the finite field $\mathbb{F}_q$ whose endomorphism ring is the maximal order $\mathcal{O}_K$ of the imaginary quadratic field $K = \mathbb{Q}(\sqrt{d_K})$. Let p_i be divisors of d_K for $i = 1, \ldots, n$ and $\mathfrak{p}_i$ be the prime above p_i. With the class group action from Theorem 1.3.17, the $\{p_1, \ldots p_n\}$ isogeny graph can be defined as a graph with vertices set $Ell_q(\mathcal{O})$ and the edges are given by the set

$$\{(E_0, E = \mathfrak{p}_i \star E_0) | \text{ for } E_0, E \in Ell_q(\mathcal{O}) \text{ and for } \mathfrak{p}_i \in \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}\}.$$

Lemma 4.3.2. *Let $\Delta_K \equiv 1 \mod 4$ be the discriminant of the imaginary quadratic field K. Let $p_1, \ldots, p_r$ be the odd prime divisors of the discriminant Δ_K of K and $\mathcal{O}_K$ be the maximal order of K and h be the class number. Then the $\{p_1, \ldots, p_{r-1}\}$ and $\{p_1, \ldots, p_r\}$ isogeny graph are partitioned into $\frac{h}{2^{r-1}}$ connected components and each connected component is Q_{r-1} in the former case and that of Q_{r-1}^d in the latter case.*

Proof. Follows from Theorem 1.4.6. □

Lemma 4.3.3. *Let $\Delta_K \equiv 0 \mod 4$ be the discriminant of imaginary quadratic field $K = Q(\sqrt{d_K})$. Let $p_1, \ldots, p_r$ be the odd prime divisors of the discriminant Δ_K of the maximal order $\mathcal{O}_K$ and h be the class number. Let $(p_i) = \mathfrak{p}_i^2$, $(2) = \mathfrak{c}^2$ in $\mathcal{O}_K$. Write $\Delta_K = 4d_K$.*

i. When $d_K \equiv 3 \mod 4$, then the $\{2, p_1, \ldots, p_{r-1}\}$ and $\{2, p_1, \ldots, p_r\}$ isogeny graphs are partitioned into $\frac{h}{2^r}$ connected components and each connected component is Q_r in the former graph and that of $Q_r^{d,r-1}$ in the latter graph.

ii. When $d_K \equiv 2 \mod 8$ the $\{2, p_1, \ldots, p_r\}$ isogeny graph is similar as in Lemma 4.3.2.

iii. When $d_K \equiv 6 \mod 8$, the $\{2, p_1, \ldots, p_r\}$ isogeny graph is as in Lemma 4.3.2.

Coloring of the $\{p_1, \ldots, p_n\}$ isogeny graph by the genus coloring map T can be obtained if we fix an elliptic curve E_0; color it as an identity action and the rest of the curves admit colors according to the class group action, for instance if $E = \prod_{i=1}^k \mathfrak{p}_i E_0$ for some $1 \leq k \leq n$ then coloring of E is given by the value $T(\prod_{i=1}^k \mathfrak{p}_i)$.
Since the components of the isogeny graph from the ramified primes are Q_n, Q_n^d and $Q_n^{d,n-1}$, they have similar coloring properties as described in Theorems 4.2.17 and 4.2.19.
As a consequence of Theorem 4.2.17, we have the following

Corollary 4.3.4. *Let $\Delta_K \equiv 1 \mod 4$ be the discriminant of the imaginary quadratic field K. Let $p_1, \ldots, p_r$ be the odd prime divisors of the discriminant Δ_K of K and $\mathcal{O}_K$ be the maximal order of K. Let $(p_i) = \mathfrak{p}_i^2$ in $\mathcal{O}_K$. If none of the two ideals $\mathfrak{p}_i$ belongs to a genus then the coloring in a component of the $\{p_1, \ldots, p_r\}$ isogeny graph represents all the possible colors for all the genera of $cl(\mathcal{O}_K)$.*

4.4 Decisional Diffie-Hellman for class group actions

Let $\mathcal{O}$ be an imaginary quadratic order and the class group $cl(\mathcal{O})$ is acting on the set

$$\mathcal{E}_{\mathcal{O}}(\mathbb{F}_p) = \{j(E) : E \text{ is defined over } \mathbb{F}_p \text{ and } \mathrm{End}(E) = \mathcal{O}\}.$$

Decisional Diffie-Hellman problem for class group is: distinguish the two probability distributions

- $(\mathfrak{a} \star E, \mathfrak{b} \star E, (\mathfrak{a}\mathfrak{b}) \star E)$ and
- $(\mathfrak{a} \star E, \mathfrak{b} \star E, \mathfrak{c} \star E)$,

where $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ are random elements in $cl(\mathcal{O})$. Castryck, Sotáková and Vercauteren's idea is to distinguish the two distributions through the non-trivial characters [20].

Fix an elliptic curve E with $j(E) \in \mathcal{E}_{\mathcal{O}}(\mathbb{F}_p)$ as a base curve. Then by the transitive action of $cl(\mathcal{O})$ to the set $\mathcal{E}_{\mathcal{O}}(\mathbb{F}_p)$, each ideal class $\mathfrak{a}$ can be associated to an elliptic curve E' and the isogeny $\phi : E \to E'$ such that $E' = \mathfrak{a} \star E$ and norm $N(\mathfrak{a}) = \deg(\phi)$. The idea developed in [20] is to calculate the coloring $T(E')$ associated with the vertex $E' \in \mathcal{E}_{\mathcal{O}}(\mathbb{F}_p)$ of the isogeny graph from only the curves E, E' or without knowing the connecting ideal $\mathfrak{a}$. Since the map T as in Subsection 4.2.2 is composed of characters associated to each divisor p_i of the discriminant $\Delta_{\mathcal{O}}$, they devise a technique to determine the norm $N(\mathfrak{a}) (\mathrm{mod}\ p_i)$ up to a square factor for each p_i.

The curves E and E' have the same endomorphism ring $\mathcal{O}$ and hence lie on the same level of their corresponding volcanoes by [58], by walking down from E and E' to their respective surfaces give elliptic curves E_0 and E_0' having the same endomorphism ring $\mathcal{O}_0 \subset \mathcal{O}$. Moreover, since the class group $cl(\mathcal{O}_0)$ acts transitively on $\mathcal{E}_{\mathcal{O}}(\mathbb{F}_p)$, there exists an ideal $\mathfrak{b} \subset \mathcal{O}_0$ such that $E_0' = \mathfrak{b} \star E_0$, a representative can be chosen with $\gcd(N(\mathfrak{b}), \Delta_{\mathcal{O}_0}) = 1$.

Let $\phi^{'} : E_0 \to E_0^{'}$ be the isogeny corresponding to the ideal $\mathfrak{b}$ of degree equal to the norm $N(\mathfrak{b})$. At the floor, we have

$$E_0(\mathbb{F}_p)[m^\infty] \cong \mathbb{Z}/p_i^v\mathbb{Z} \cong E_0^{'}(\mathbb{F}_p)[m^\infty].$$

Choose $P \in E_0[p_i](\mathbb{F}_p)$, $P^{'} \in E_0[p_i](\mathbb{F}_p)$ and $Q, Q^{'}$ of order p_i^v such that

$$p_i^{v-1}Q = P \text{ and } p_i^{v-1}Q^{'} = P^{'}.$$

Then, there exists $k \in \{1, \ldots, p_i - 1\}$ such that $k\phi^{'}(P) = P^{'}$. Then

$$k\phi^{'}(P) = p_i^{v-1}(k\phi^{'}(Q)) = P^{'} = p_i^{v-1}Q^{'}$$

gives $k\phi^{'}(Q) = Q^{'}$ and by Tate pairing

$$\mathcal{T}_{p_i}(P^{'}, Q^{'}) = \mathcal{T}_{p_i}(k\phi^{'}(P), k\phi^{'}(Q)) = \mathcal{T}_{p_i}(P, Q)^{k^2 \deg(\phi^{'})},$$

which gives $N(\mathfrak{a}) (\text{mod } p_i)$ up to a square factor and hence the character associated to p_i is computed as

$$\left(\frac{N(\mathfrak{b})}{p_i}\right) = \left(\frac{\deg(\phi^{'})}{p_i}\right) = \left(\frac{\log_{T_{p_i}(P,Q)} T_{p_i}(P^{'}, Q^{'})}{p_i}\right).$$

Chapter 5

A new candidate: Quadratic Surface Intersection (QSI) key exchange

Currently, there are five major post-quantum areas of research in cryptography, four of them are discussed in [11] including lattice-based, codes based, multivariate, hash-based, and one is isogeny based cryptography.
In this section, we present a new candidate for a key exchange protocol that we call QSI key exchange, joint work with Daniele Di Tullio [90], and an encryption scheme derived from it. Mainly, the key exchange is based on the difficulty of recovering a Veronese variety, which is hidden by an automorphism of the ambient space. This problem reduces to a problem of solving a large system of high degree polynomial equations in many variables or finding the primary decomposition of an ideal generated by some multivariate polynomials, which we claim a post-quantum problem. We leave the detailed security analysis and an optimization of the proposed scheme towards an efficient key exchange candidate for future research.
We have implemented our algorithm in the computer algebra system SageMath [35] and is available at
`https://github.com/mgyawali/QSI-Key-Exchange`

5.1 QSI Key Exchange

5.1.1 A high-level overview of the key exchange

QSI key exchange is not an exact analog of Diffie-Hellman like key exchange, where Alice and Bob have a similar way of constructing public

and private keys, but in QSI one of the users say Bob makes use of Alice's public keys to generate his private key. Later they become successful to share a common secret by using their private data.
In summary, Alice chooses a non-standard Veronese variety that is contained in a large projective space and a quadric surface lying in it. The selection of the quadric surface is equivalent to the choice of a σ-embedding (the composition of Segre and Veronese map). Alice chooses two σ-embeddings; she keeps one σ-embedding as a private key and publishes another σ-embedding (equivalently, another quadric) whose image is contained in the Veronese variety. She also publishes some automorphisms of the variety. Now, Bob can generate a private σ- embedding (his quadric surface) by using the public σ-embedding and some automorphism of the variety. Both of them publish hyperplanes containing the images of their private σ-embeddings. By using their private σ-embeddings, they compute the pullback of each other's hyperplanes through their private embeddings to recover the intersection of the quadric surfaces, which is a $(2,2)$ homogeneous curve, and finally compute the common j-invariant of the curve.

5.1.2 QSI algorithm

Let $\mathbb{P}^n_\kappa = \mathbb{P}^n$ be the projective space of dimension n, where $\kappa = \mathbb{F}_q$ is a finite field with q elements and $m \in \mathbb{N}^+$ be the degree of the Veronese embedding $v^{M_A}_{3,m}$.

- Alice chooses a non-standard Veronese embedding

$$v^{M_A}_{3,m} : \mathbb{P}^3 \to M_A \cdot V_{3,m} \subset \mathbb{P}^{\binom{m+3}{3}-1}$$

  represented by a random matrix $M_A \in \mathcal{GL}(\binom{m+3}{3})$.

- Alice constructs some automorphisms of the variety $M_A \cdot V_{3,m}$. These automorphisms of the variety are chosen by the map $\phi_{n,m}$ as described in Subsection 2.3.1. Precisely, she selects some automorphisms of $\mathbb{P}^3$, i.e. $A'_1, \ldots, A'_r \in \mathcal{GL}(4)$ of order $q^4 - 1$ (with the characteristic polynomials irreducible over $\mathbb{F}_q$) and then she computes

$$A_i := M_A \phi_{n,m}(A'_i) M_A^{-1}$$

  as some automorphisms of the variety. For example, we fix $r = 2$.

- Alice selects a secret quadric surface inside $M_A \cdot V_{3,m}$, equivalently a σ-embedding

$$\sigma^{(s)}_A : \mathbb{P}^1 \times \mathbb{P}^1 \to M_A \cdot V_{3,m} \subset \mathbb{P}^{\binom{m+3}{3}-1}$$

represented by a $\binom{m+3}{3} \times (m+1)^2$ matrix $M_A^{(s)}$ as described in Example 2.3.7, because a choice of a quadric surface in $\mathbb{P}^3$ and its embedding to the large projective space $\mathbb{P}^{\binom{m+3}{3}-1}$ are done through the composition of Veronese and Segre embeddings.

- She constructs a hyperplane $H_A \subset \mathbb{P}^{\binom{m+3}{3}-1}$ containing the $\mathrm{Im}(\sigma_A^{(s)})$, which can be obtained by choosing a vector in $\mathrm{coker}(M_A^{(s)}) \subset \mathbb{F}_q^{\binom{m+3}{3}}$.
- She constructs a public quadric surface inside $M_A \cdot V_{3,m}$, equivalently a σ-embedding

$$\sigma_A^{(p)} : \mathbb{P}^1 \times \mathbb{P}^1 \to M_A \cdot V_{3,m} \subset \mathbb{P}^{\binom{m+3}{3}-1},$$

which is represented by a $\binom{m+3}{3} \times (m+1)^2$ matrix $M_A^{(p)}$.

Alice's public key:

- Two Automorphisms of the variety given by matrices $A_1, A_2 \in \mathcal{GL}(\binom{m+3}{3})$.
- The $\binom{m+3}{3} \times (m+1)^2$ matrix $M_A^{(p)}$.
- The hyperplane H_A.

Alice's secret key:

- The σ-embedding $\sigma_A^{(s)}$ or equivalently its representing matrix $M_A^{(s)}$ of size $\binom{m+3}{3} \times (m+1)^2$.

Bob's key generation

- Bob chooses $b_1, b_2, b_3, b_4 \in \{0, \ldots, q^4 - 1\}$ and then computes

$$M_B' = A_1^{b_1} A_2^{b_2} A_1^{b_3} A_2^{b_4}.$$

- Bob computes the matrix $M_B := M_B' \cdot M_A^{(p)}$ as a matrix of a σ-embedding $\sigma_B^{(s)} : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^{\binom{m+3}{3}}$ which is, in fact, the private quadratic surface of Bob lying in the Veronese variety chosen by Alice.
- Bob computes a hyperplane $H_B \subset \mathbb{P}^{\binom{m+3}{3}-1}$ containing the $\mathrm{Im}(\sigma_B^{(s)})$.

Bob keeps $\sigma_B^{(s)}$ or M_B as a private key and publishes H_B.
Key Exchange:

- Bob computes the pullback ${\sigma_B^{(s)}}^* H_A$. It is a curve of bi-degree (m, m) in $\mathbb{P}^1 \times \mathbb{P}^1$.
- He uses a factorization algorithm to find a component of bi-degree (2,2) and computes its j-invariant $j_B \in \mathbb{F}_q$.
- The probability that the residue curve of bi-degree $(m-2, m-2)$ is reducible is negligible, so the j_B is well determined except for $m = 4$, it which case there are two bi-degree $(2, 2)$ curve.
- Alice computes the pullback ${\sigma_A^{(s)}}^* H_B$. She finds the component of bi-degree (2,2), then she computes its j-invariant $j_A \in \mathbb{F}_q$.

$j_A = j_B$ is the common key of Alice and Bob.

Lemma 5.1.1. *Two j-invariants are equal i.e.* $j_A = j_B$.

Proof. Since $\mathbb{P}^3$ is isomorphic to the Veronese variety in $\mathbb{P}^{\binom{m+3}{3}-1}$, an embedding $\mathbb{P}^1 \times \mathbb{P}^1$ in $\mathbb{P}^{\binom{m+3}{3}-1}$ contained in the Veronese variety is equivalent to give an embedding of $\mathbb{P}^1 \times \mathbb{P}^1$ into $\mathbb{P}^3$, whose image is a quadric surface. Alice and Bob have two different embeddings $\sigma_A^{(s)}$ and $\sigma_B^{(s)}$ whose images are contained in the Veronese Variety, viewing these images as quadric surfaces, denote them as Q_A and Q_B respectively. We need to find the intersection $Q_A \cap Q_B$ which is a genus 1 curve and is isomorphic with the curves of Alice and Bob. Thus, identifying the Veronese variety as $\mathbb{P}^3$, the embedding of Alice can be assumed as

$$\sigma_A^{(s)} : \mathbb{P}^1 \times \mathbb{P}^1 \to Q_A \subset \mathbb{P}^3$$

and similarly quadratic surface of Bob as

$$\sigma_B^{(s)} : \mathbb{P}^1 \times \mathbb{P}^1 \to Q_B \subset \mathbb{P}^3.$$

The pullback of Q_B through the σ-embedding of Alice: ${\sigma_A^{(s)}}^* Q_B$, which is isomorphic to $Q_A \cap Q_B$ as in the discussion of Subsection 2.2. Providing a hyperplane section of the Veronese variety is equivalent to giving a surface S_A or S_B of $\mathbb{P}^3$ of degree m and having Q_A or Q_B as the component. The pullback gives the (2, 2) bi-degree component and is isomorphic to $Q_A \cap Q_B$ at least in the general case.

□

5.1.3 Toy Example

Example 5.1.2. ***Key Generation:*** *A finite field $\mathbb{F}_q$ with $q = 16411$, $m = 2$. Then $\binom{m+3}{3} = 10$. Alice chooses a Veronese embedding*

$$v_{3,m}^{M_A} : \mathbb{P}^3 \to M_A \cdot V_{3,m} \subset \mathbb{P}^9$$

represented by a random 10×10 matrix

$$M_A = \begin{bmatrix} 6434 & 8624 & 1442 & 8172 & 13226 & 12669 & 9492 & 11160 & 2354 & 14514 \\ 5392 & 9365 & 1565 & 3457 & 14505 & 8874 & 9738 & 9536 & 4162 & 7052 \\ 9995 & 3409 & 12388 & 2962 & 13538 & 3814 & 8079 & 14920 & 2982 & 3167 \\ 3655 & 8237 & 1820 & 12771 & 15351 & 11681 & 6626 & 463 & 12211 & 10377 \\ 9818 & 15886 & 11814 & 11548 & 8164 & 7285 & 3865 & 4837 & 15330 & 12963 \\ 1377 & 7570 & 10743 & 8013 & 3980 & 6998 & 6942 & 13032 & 13042 & 13066 \\ 13067 & 8075 & 8684 & 6162 & 11588 & 10876 & 8172 & 40 & 2874 & 5514 \\ 1420 & 11397 & 14649 & 7628 & 9902 & 5803 & 4539 & 9387 & 13157 & 6504 \\ 5479 & 12138 & 680 & 8772 & 5036 & 11603 & 4928 & 6922 & 7011 & 15716 \\ 5020 & 14199 & 11398 & 13653 & 6829 & 2800 & 2834 & 10248 & 7818 & 1773 \end{bmatrix}.$$

In order to choose automorphisms of the Veronese variety $M_A \cdot V_{3,m}$, she takes two random matrices $A_1^{'}, A_2^{'} \in \mathcal{GL}(4)$, where

$$A_1^{'} = \begin{bmatrix} 15790 & 6966 & 6845 & 4231 \\ 8011 & 3668 & 8257 & 831 \\ 605 & 3986 & 7888 & 1157 \\ 4462 & 16388 & 7343 & 14432 \end{bmatrix} \text{ and } A_2^{'} = \begin{bmatrix} 5758 & 201 & 14881 & 3246 \\ 1376 & 211 & 9310 & 7851 \\ 9861 & 13210 & 1243 & 15 \\ 5776 & 13711 & 9047 & 5442 \end{bmatrix}$$

and computes

$$A_i = M_A \phi_{n,m}(A_i^{'}) M_A^{-1} \quad \text{for } i = 1, 2.$$

Therefore,

$$A_1 = \begin{bmatrix} 15018 & 7379 & 11744 & 11490 & 10844 & 10009 & 12890 & 11191 & 1666 & 16235 \\ 436 & 6517 & 11689 & 1035 & 3948 & 8946 & 795 & 15753 & 3926 & 15920 \\ 15677 & 6798 & 4533 & 4266 & 490 & 14025 & 13668 & 860 & 5535 & 8840 \\ 4283 & 6514 & 6363 & 9652 & 12681 & 11618 & 16094 & 12376 & 12056 & 7575 \\ 2808 & 61 & 193 & 4741 & 9627 & 2813 & 12310 & 15657 & 4608 & 2378 \\ 2978 & 16021 & 5513 & 1185 & 10587 & 13067 & 8342 & 4232 & 16273 & 7589 \\ 11071 & 12641 & 1141 & 2329 & 8739 & 2990 & 13833 & 8438 & 11187 & 13591 \\ 6272 & 9096 & 12928 & 788 & 2799 & 10686 & 9829 & 7755 & 14429 & 7948 \\ 7864 & 1517 & 6114 & 9107 & 13263 & 4237 & 1312 & 4171 & 11821 & 3308 \\ 15726 & 7489 & 1756 & 8055 & 8245 & 4124 & 8820 & 10566 & 13627 & 1083 \end{bmatrix}$$

and

$$A_2 = \begin{bmatrix} 13369 & 15770 & 9803 & 10390 & 15295 & 14706 & 12527 & 9354 & 7794 & 14856 \\ 8447 & 9124 & 6458 & 12871 & 9932 & 6220 & 10477 & 9907 & 7816 & 6399 \\ 12520 & 9907 & 5244 & 11892 & 8717 & 12287 & 6801 & 7262 & 1980 & 2350 \\ 10666 & 2429 & 10820 & 3502 & 4264 & 1076 & 3684 & 4255 & 13409 & 12313 \\ 9194 & 4290 & 4445 & 14167 & 4100 & 3093 & 4026 & 5614 & 5983 & 2029 \\ 14093 & 2842 & 14268 & 7988 & 4402 & 10580 & 5060 & 12625 & 14393 & 10063 \\ 420 & 664 & 11556 & 7209 & 13025 & 8693 & 4869 & 550 & 15038 & 5438 \\ 14547 & 11245 & 7577 & 13783 & 8462 & 16111 & 3996 & 6680 & 8069 & 5781 \\ 8898 & 8774 & 15705 & 3270 & 11632 & 6559 & 12836 & 13643 & 12300 & 8008 \\ 8574 & 2669 & 14730 & 14024 & 11160 & 13511 & 7697 & 10874 & 9888 & 12951 \end{bmatrix}.$$

She keeps the secret embedding

$$\sigma_A^{(s)} : \mathbb{P}^1 \times \mathbb{P}^1 \to M_A \cdot V_{3,m} \subset \mathbb{P}^9$$

whose representing matrix is the following 10×9 *matrix*

$$M_A^{(s)} = \begin{bmatrix} 1320 & 2620 & 11135 & 2352 & 4340 & 5297 & 416 & 12442 & 1908 \\ 1896 & 1525 & 6976 & 10295 & 15677 & 5531 & 8803 & 13595 & 11350 \\ 3114 & 3038 & 4343 & 4194 & 3410 & 3268 & 13487 & 885 & 11904 \\ 3276 & 2264 & 7342 & 15211 & 11771 & 8806 & 11059 & 11378 & 10608 \\ 1196 & 15628 & 8778 & 15495 & 1815 & 7911 & 12916 & 4073 & 12975 \\ 13875 & 3785 & 8803 & 1247 & 7024 & 6443 & 9817 & 502 & 9134 \\ 10985 & 6007 & 1464 & 12419 & 1703 & 1835 & 15245 & 12758 & 14087 \\ 8343 & 11091 & 10245 & 1960 & 13606 & 6551 & 14556 & 5822 & 8517 \\ 3923 & 6315 & 11634 & 7502 & 6454 & 3700 & 13878 & 10216 & 4533 \\ 1295 & 11283 & 2418 & 1477 & 15007 & 7063 & 15300 & 5917 & 2092 \end{bmatrix}.$$

Alice's public keys consist of a hyperplane H_A *in* $\mathbb{P}^9$ *:*

$$x_0 + 1469x_1 - 8066x_2 + 2363x_3 + 2680x_4 - 1980x_5 + 5540x_6 + 2285x_7 - 5203x_8 + 7674x_9$$

containing the image of $\sigma_A^{(s)}$*, the embedding*

$$\sigma_A^{(p)} : \mathbb{P}^1 \times \mathbb{P}^1 \to M_A \cdot V_{3,m} \subset \mathbb{P}^9$$

represented by the 10×9 *matrix*

$$M_A^{(p)} = \begin{bmatrix} 8590 & 8461 & 6748 & 15978 & 3543 & 12505 & 3129 & 627 & 16239 \\ 15293 & 13594 & 10715 & 12397 & 46 & 4798 & 12438 & 13145 & 14163 \\ 7602 & 769 & 5417 & 3304 & 7795 & 14719 & 15833 & 6416 & 11489 \\ 7632 & 13392 & 10345 & 322 & 10751 & 5896 & 16313 & 16225 & 14235 \\ 7749 & 15238 & 12591 & 2855 & 5074 & 771 & 2812 & 8788 & 8135 \\ 4852 & 11438 & 4357 & 5462 & 371 & 5418 & 13730 & 14255 & 12231 \\ 14594 & 176 & 15387 & 2185 & 3097 & 6726 & 16198 & 1553 & 99 \\ 9265 & 15959 & 1594 & 16353 & 16183 & 13447 & 3785 & 11208 & 1609 \\ 1115 & 10396 & 2580 & 1153 & 531 & 10719 & 8208 & 11221 & 4900 \\ 8475 & 15417 & 15063 & 16139 & 16064 & 5343 & 11934 & 5658 & 15627 \end{bmatrix}$$

and automorphisms A_1, A_2.

Bob chooses a random integers $b_1 = 6739, b_2 = 6338, b_3 = 14612, b_4 = 6950$*; computes an automorphism*

$$M_B^{'} = A_1^{b_1} A_2^{b_2} A_1^{b_3} A_2^{b_4} = \begin{bmatrix} 8402 & 8088 & 3256 & 9623 & 16339 & 15102 & 7293 & 12071 & 15793 & 8979 \\ 12150 & 13336 & 594 & 3969 & 7180 & 2239 & 11310 & 9534 & 5091 & 13870 \\ 14874 & 5084 & 13249 & 12808 & 7354 & 2911 & 2559 & 165 & 5762 & 4748 \\ 11762 & 12983 & 12932 & 6250 & 14281 & 9673 & 573 & 6454 & 5011 & 909 \\ 13865 & 3904 & 4003 & 2096 & 5504 & 5870 & 13008 & 7737 & 5252 & 11114 \\ 4497 & 14177 & 10640 & 5234 & 10054 & 11048 & 2128 & 7427 & 14868 & 13717 \\ 7523 & 13487 & 7464 & 796 & 10253 & 2102 & 8736 & 10399 & 1582 & 5422 \\ 13783 & 10771 & 1723 & 3461 & 68 & 14176 & 15622 & 2233 & 3743 & 15586 \\ 8951 & 14717 & 6121 & 4899 & 9838 & 10902 & 2187 & 13328 & 3436 & 12577 \\ 2073 & 1183 & 13888 & 4233 & 12205 & 6095 & 15837 & 9761 & 15699 & 5154 \end{bmatrix}$$

of the variety $M_A \cdot V_{3,m}$*. He calculates*

$$M_B = M_B^{'} M_A^{(p)} = \begin{bmatrix} 10316 & 70 & 5132 & 5007 & 2548 & 7354 & 732 & 15368 & 4469 \\ 5158 & 10610 & 12687 & 4020 & 10647 & 12187 & 7885 & 10061 & 12566 \\ 3263 & 3196 & 12137 & 3814 & 6090 & 10420 & 105 & 4761 & 15514 \\ 6142 & 8180 & 13169 & 11135 & 2750 & 15611 & 14406 & 14894 & 6055 \\ 15633 & 4970 & 9093 & 14779 & 7475 & 15556 & 8779 & 451 & 14227 \\ 14863 & 3370 & 2268 & 920 & 369 & 9234 & 10790 & 2659 & 8773 \\ 9388 & 1235 & 8573 & 16249 & 16013 & 7724 & 2767 & 8031 & 2984 \\ 15445 & 12709 & 8615 & 5043 & 11409 & 2875 & 2516 & 11029 & 9782 \\ 11591 & 10626 & 11760 & 10191 & 7664 & 14341 & 10404 & 8175 & 12554 \\ 13748 & 3883 & 2870 & 8980 & 15814 & 12948 & 9672 & 8447 & 276 \end{bmatrix}$$

as a representing matrix of the secret σ*-embedding*

$$\sigma_B^{(s)} : \mathbb{P}^1 \times \mathbb{P}^1 \to M_A \cdot V_{3,m} \subset \mathbb{P}^{\binom{m+3}{3}}.$$

He also computes a hyperplane H_B in $\mathbb{F}^9$ given by

$$x_0 - 5404x_1 + 3650x_2 + 465x_3 + 6073x_4 + 7863x_5 - 162x_6 - 7294x_7 - 7707x_8 + 8095x_9$$

containing the image of $\sigma_B^{(s)}$.

Key Exchange:

Bob computes the pullback

$$\begin{aligned} C_1 := {\sigma_B^{(s)}}^* H_A = {} & 4094x_0^2x_2^2 + 433x_0x_1x_2^2 + 262x_1^2x_2^2 + 1048x_0^2x_2x_3 + 5309x_0x_1x_2x_3 \\ & - 4413x_1^2x_2x_3 + 5200x_0^2x_3^2 - 4806x_0x_1x_3^2 - 1129x_1^2x_3^2, \end{aligned}$$

which is a bi-degree (2,2) curve and computes its j-invariant $j_B = j(C_1) = 4026 \in \mathbb{F}_q$.

Alice computes the pullback

$$\begin{aligned} C_2 := {\sigma_A^{(s)}}^* H_B = {} & -7091x_0^2x_2^2 - 5735x_0x_1x_2^2 - 2687x_1^2x_2^2 + 1479x_0^2x_2x_3 + 6077 \\ & x_0x_1x_2x_3 + 8150x_1^2x_2x_3 + 1351x_0^2x_3^2 + 7198x_0x_1x_3^2 + 4625x_1^2x_3^2 \end{aligned}$$

and computes its j-invariant $j_A = j(C_2) = 4026 \in \mathbb{F}_q$, which is the common key.

5.2 Public-key encryption

The QSI key exchange technique can be used to design a public key cryptosystem, similar to the ElGamal public key encryption scheme.
Suppose Bob wants to send a message m to Alice.

- **Public parameters to both parties**
  A finite field $\mathbb{F}_q$, $m \in \mathbb{N}^+$ and a family of hash functions $\mathcal{H} = \{H_k : k \in \mathcal{K}\}$ from the finite field F_q to the message space $\{0,1\}^w$, and $\mathcal{K}$ be a finite set.

- **Encryption**
  Bob has access to the Alice's public data $(A_1, A_2, M_A^{(p)}, H_A, k)$. He computes a random ephemeral key, a σ embedding $\sigma_B^{(s)} : \mathbb{P}^1 \times \mathbb{P}^1 \to M_A \cdot V_{3,m} \subset \mathbb{P}^{\binom{m+3}{3}-1}$. He first computes the j-invariant of the bi-degree (2,2) curve j_B as described before. Then he encrypts the message $m \in \{0,1\}^w$ as
  $$c = H_k(j_B) \bigoplus m.$$
  The ciphertext is (H_B, c).

- **Decryption**
  Alice gets the ciphertext (H_B, c) and using her private embedding $\sigma_A^{(s)} : \mathbb{P}^1 \times \mathbb{P}^1 \to M_A \cdot V_{3,m} \subset \mathbb{P}^{\binom{m+3}{3}-1}$, she first recovers the $(2,2)$ curve and its j-invariant j_A, and recovers the message m as

$$m = H_k(j_A) \bigoplus c.$$

5.3 Attacks against QSI

5.3.1 Underlying cost of the key exchange

We first observe the space complexity of public and private keys.
Keys of Alice:

- Two public square matrices A_1, A_2 of size $\binom{m+3}{3}$ require $\mathcal{O}(m^6 \log q)$ space.
- Public matrix $M_A^{(p)}$ of size $\binom{m+3}{3} \times (m+1)^2$ requires $\mathcal{O}(m^5 \log q)$.
- Public hyperplane H_A, a vector of length $\binom{m+3}{3}$, requires $\mathcal{O}(m^3 \log q)$.
- Private σ-embedding $\sigma_A^{(s)}$ or its matrix $M_A^{(s)}$ of size $\binom{m+3}{3} \times (m+1)^2$ requires $\mathcal{O}(m^5 \log q)$.

Keys of Bob:

- Private σ-embedding $\sigma_B^{(s)} : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^{\binom{m+3}{3}}$ or its matrix M_B of size $\binom{m+3}{3} \times (m+1)^2$ requires $\mathcal{O}(m^5 \log q)$.
- Public hyperplane H_B, a vector of length $\binom{m+3}{3}$, occupies $\mathcal{O}(m^3 \log q)$.

Now, we analyze asymptotic steps required to share a common key.

- Number of steps to produce $A_1, A_2, \sigma_A^{(s)}$ is bounded by $\mathcal{O}(\mathbf{M}(\log q)m) + \mathcal{O}(m^9)$, where $\mathbf{M}(x)$ denote the number of steps required to multiply two x-bits integers.
- To compute the hyperplanes H_A and H_B, it requires to solve a system of linear equation which takes at most $\mathcal{O}(m^{3\omega})$ steps [69], where $2 < \omega \leq 3$ is the matrix multiplication exponent.

- For private σ-embedding of Bob $\sigma_B^{(s)}$, it needs $\mathbb{O}(m^{3\omega}\log m)$.
- To both Alice and Bob
  - Pull back of hyperplane by private σ-embeddings in $\mathbb{O}(\mathbf{M}(\log q)m^3)$.
  - Factorization of bi-degree (m, m) can be computed efficiently by the method given in [10].

5.3.2 Brute force attempts

We give the approximate steps needed to attack the keys.

- The number of quadric hypersurfaces contained in H_A i.e. amount of brute-force needed to find $\sigma_A^{(s)}$:
  We count $M_A^{(s)}$ such that H_A is in coker$M_A^{(s)}$ i.e. $H_A M_A^{(s)} = 0$. This implies that the columns of $M_A^{(s)}$ are in the kernel of H_A, which is isomorphic with $\mathbb{F}_q^{\binom{m+3}{3}-1}$, therefore choosing $(m+1)^2$ elements of $\mathbb{F}_q^{\binom{m+3}{3}-1}$ require total of $q^{(\binom{m+3}{3}-1)(m+1)^2}$ attempts.
- Possible number of $\sigma_B^{(s)}$ (necessarily depending on r):
  For $r = 2$, choices of b_i for $i = 1, \ldots, 4$ determine $\sigma_B^{(s)}$ therefore there are q^{16} choices.
- Running over all possibilities for $\sigma_B^{(s)}$, the number of distinct options for ${\sigma_B^{(s)}}^* H_A$ is q^{16}.
- Similarly, the number of distinct options for ${\sigma_B^{(s)}}^* H_A$ is $q^{(\binom{m+3}{3}-1)(m+1)^2}$.
- Valid j-invariants (i.e. amount of brute-force needed to find $j_A = j_B$) : Since j-invariants are defined in $\mathbb{F}_q$ so there are q choices.

Since the j-invariants belong to the base field $\mathbb{F}_q$, we have to choose $q \approx 2^{128}$ for the classical 128-bit security level. This attack suggests that small values of m could work but we will see that the brute force is not the best attack.

5.3.3 Other possible attack strategies

Here we summarize other possible attack strategies against QSI. One of the possibilities is a direct key recovery attack targeting the private keys, more

precisely, to the secret σ-embeddings or the Veronese variety hidden by the automorphism of the ambient space. We state the following underlying problem of the proposed key exchange scheme.

Problem 5.3.1. *Let $\kappa = \mathbb{F}_q$ be the field of cardinality q. Suppose*

$$v_{3,m}^{M} : \mathbb{P}^3 \to M \cdot V_{3,m} \subset \mathbb{P}^{\binom{m+3}{3}-1}$$

be a non-standard Veronese embedding represented by a random matrix $M \in \mathcal{GL}(\binom{m+3}{3})$ with its variety $M \cdot V_{3,m}$ and let

$$\sigma^{(p)} : \mathbb{P}^1 \times \mathbb{P}^1 \to M \cdot V_{3,m} \subset \mathbb{P}^{\binom{m+3}{3}-1}$$

$$\sigma^{(s)} : \mathbb{P}^1 \times \mathbb{P}^1 \to M \cdot V_{3,m} \subset \mathbb{P}^{\binom{m+3}{3}-1}$$

be σ-embeddings represented by $\binom{m+3}{3} \times (m+1)^2$ matrices $M^{(p)}$ and $M^{(s)}$ respectively. A hyperplane H containing $\mathrm{Im}(\sigma^{(s)})$ is represented by a vector in $coker(M^{(s)}) \subset \mathbb{F}^{\binom{m+3}{3}}$. Furthermore, let A_1 and A_2 in $\mathcal{GL}(\binom{m+3}{3})$ be two matrices of order $q^4 - 1$ representing automorphisms of the variety $M \cdot V_{3,m}$. Given:

- *the finite field $\mathbb{F}_q$,*
- *the degree of the Veronese embedding $m \in \mathbb{N}^+$,*
- *two automorphisms of the variety given by matrices A_1, A_2,*
- *the matrix $M^{(p)}$ and*
- *a hyperplane H containing the image of $\sigma^{(s)}$,*

determine $\sigma^{(s)}$(equivalently its corresponding matrix) or the matrix M representing the non-standard Veronese variety $M \cdot V_{3,m}$.

Problem 5.3.1 of determining the Veronese variety, say $V = M \cdot V_{3,m}$ and the σ-embedding $\sigma^{(s)}$ reduce to a problem of solving multivariate and high degree polynomial equations. Since A_i are automorphisms of V, we have

$$A_i M = M\phi_{3,m}(A) \tag{5.1}$$

for some matrix $A \in \mathcal{GL}(4)$. Consider $A = (a_{ij})$ be 4×4 and $M = (m_{ij})$ be $\binom{m+3}{3} \times \binom{m+3}{3}$ matrices of unknowns. Substituting these matrices in Equation 5.1, we get a system of multivariate polynomial equations of bi-degree $(1, m)$ in variables m_{ij} and a_{ij}, and elimination of the variables a_{ij} changes the system into a system with very high degree equations and

large number of variables as m gets bigger.

Likewise, an attempt to find $\sigma^{(s)}$ such that $\mathrm{Im}(\sigma^{(s)}) \subset V$ also reduces to the similar multivariate problem. The condition $\mathrm{Im}(\sigma^{(s)}) \subset V$ implies that

$$\sigma^{(s)} = M \circ v_{3,m} \circ A \circ s_{1,1}$$

for some $A \in \mathrm{Aut}(\mathbb{P}^3)$ since $\sigma^{(s)}$ is a composition of non-standard Segre and Veronese. As before, the matrix M_σ, representing the embedding $M \circ v_{3,m} \circ A \circ s_{1,1}$, is a matrix whose components are bi-homogeneous polynomials of bi-degree $(1, m)$ in the set of variables $\{m_{ij}\}$ and $\{a_{ij}\}$, where a_{ij} and m_{ij} are as above. Now, imposing the given vector representing the hyperplane H as a co-kernel of M_σ, we get a system of a multivariate polynomials of bi-degree $(1, m)$ in the variables m_{ij} and a_{ij} as above.

Shared Secret Recovery: Another underlying problem of the QSI key exchange is a problem of recovering the common secret, which is the bi-degree $(2, 2)$ homogeneous curve embedded as a curve of degree $4m$ in the Veronese variety.

Problem 5.3.2. *Let $\kappa = \mathbb{F}_q$ be the finite field with q elements. Suppose that $V \subset \mathbb{P}^{\binom{m+3}{3}-1}$ is a 3-dimensional non-standard Veronese variety. Assume the homogeneous ideal of V is known but it's isomorphism with $\mathbb{P}^3$ is not known. Let H_1 and H_2 be two hyperplanes of $\mathbb{P}^{\binom{m+3}{3}-1}$. Find the irreducible decomposition of the curve $V \cap H_1 \cap H_2$ as a curve of degree $4m$ and a curve of degree $m^3 - 4m$.*

The equivalent problem in terms of defining ideals can be stated as the problem of primary decomposition of the ideal $I = (I_V, L_{H_1}, L_{H_2})$ where I_V is the homogeneous ideal of V; L_{H_1} and L_{H_2} are the linear equations defining the hyperplanes H_1 and H_1. Here, the Gröbner basis of the ideal I gives the information of the shared secret.
The Veronese variety V is defined by $m(m^2-1)(m^3+12m^2+59m+66)$ homogeneous polynomials of degree 2.

Proposition 5.3.3. *[90] The Veronese variety $V_{3,m}$ is an intersection of $N(V_{3,m}) = m(m^2-1)(m^3+12m^2+59m+66)$ linearly independent quadric hypersurfaces in $\binom{m+3}{3}$ variables. .*

These defining polynomials can be obtained by some linear algebra. Therefore, the main difficulty lies in the computation of irreducible components of the variety $V \cap H_1 \cap H_2$, or equivalently to find the primary

decomposition of the ideal generated by the quadratic polynomials defining V and the two linear polynomials defining H_1 and H_2.
The Veronese variety V is of degree m^3.

Proposition 5.3.4. *The Veronese variety $V_{3,m} \subset \mathbb{P}^{\binom{n+m}{3}-1}$ is a 3-dimensional projective variety of degree m^3.*

Proof. In general $\deg(V_{n,m}) = m^n$, see for example in [80, 4.2.7] □

It follows that the curve $V \cap H_1 \cap H_2$ is curve of degree m^3 and it is reducible with a component of degree $4m$ because of the following proposition.

Proposition 5.3.5. *[90] The image of a curve of bi-degree $(2,2)$ through a σ-embedding $\mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^{\binom{m+3}{3}-1}$ is a curve of degree $4m$.*

Once the irreducible component of $V \cap H_1 \cap H_2$ of degree $4m$ is known, then one can evaluate the j-invariant of the component of degree $4m$, which is the common secret to both Alice and Bob.

Attack to the Private Keys: Suppose Eve wants to attack Bob's private key. She chooses $e_1, e_2, e_3, e_4 \in \{0, \ldots, q^4 - 1\}$ and then computes

$$M'_E = A_1^{e_1} A_2^{e_2} A_1^{e_3} A_2^{e_4}.$$

She further computes the matrix $M_E := M'_E \cdot M_A^{(p)}$ as a matrix of a σ-embedding $\sigma_E : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^{\binom{m+3}{3}}$ and imposes the condition

$$H_B \in \operatorname{coker}(M_E).$$

This may require q^{16} attempts. But, the possible quadric surfaces of $\mathbb{P}^3$ form a 9 dimensional projective space therefore the brute force attack requires only q^9 attempts. This shows q^9 trials can generate a σ-embedding say σ_E such that its image coincide with the image of the private σ-embedding of Bob i.e. $\operatorname{Im}(\sigma_E) = \operatorname{Im}(\sigma_B^{(s)})$.

5.3.4 Gröbner basis computation

The number of steps required to compute Gröbner algorithms (Faugère F4, F5 [37]) is bounded by

$$\mathcal{O}\left(ld\binom{N+d-1}{d}^{\omega}\right) \tag{5.2}$$

for a graded monomial ordering up to degree d, where N is the number of variables, l is the number of equation in the system of homogeneous polynomials, and ω is the matrix multiplication exponent [7, 8]. In Shared Secret Recovery in Section 5.3.3, we have $N = \binom{m+3}{3}$ and $l = N(V_{3,m}) + 2$, where $N(V_{3,m})$ given in Proposition 5.3.3. The complexity is determined by the highest degree of the polynomials that occurs in the reduction process of the Gröbner basis algorithms, this degree is also called the *degree of regularity* in the literature. We were unable to determine how the degree of regularity depends on the parameter m, and hence we cannot give a precise estimate for the complexity of the Gröbner basis attack. It is expected that the degree of regularity grows at least linearly in m, implying that the complexity of the F4/F5 algorithms grows at least exponentially. Experimentally, the running time increases rapidly and becomes inaccessible even with some values in $m \leq 10$, therefore we hope that a value of m around 20 will be safe for at least 128 bit classical security.
We have posted a code to compute the Gröbner basis of the ideal $I = (I_{V_1}, L_{H_1}, L_{H_2})$ at `https://github.com/mgyawali/QSI-Key-Exchange`, which is written for Magma [15].
Our experiment was done on the computer of the University of L'Aquila [70].
Finite field is $\mathbb{F}_q$ and m is the degree of the Veronese embedding.
Algorithm used : Faugère F4
Monomial basis order : Graded Reverse Lexicographical
Magma V2.24-2
Time required for some values of m is given in Table 5.1.

$q = 65521$				$q =$NextPrime(2^{128})	
m	Time 1(sec)	Time 2(sec)	Time 3(sec)	m	Time(sec)
3	0.440	0.450	0.449	3	3.110
4	20.519	19.629	20.359	4	161.2
5	613.620	608.470	623.980	5	Aborted
6	Aborted (after 6 hours)				

Table 5.1: Gröbner basis computation

Large values of m makes the key exchange excessively slow. We believe that some variants or some technique to accelerate the system could be possible in future. Therefore, we leave the complete security analysis and development of some possible variants for the future research.

Chapter 6

Signature scheme from the secant variety of the Grassmannian

6.1 Introduction

Multivariate public key authentication schemes like Rainbow [38], one of the three NIST post-quantum signature finalists [67], is known for relatively fast signing and verification but large public key size in comparison to other post-quantum signature schemes. In this chapter, we purpose a new multivariate signature scheme, a joint work with Daniele Di Tullio [91], based on the difficulty of finding points inside the shifted secant variety of the Grassmannian when only the implicit equations are known. A purpose of the proposed signature scheme is to start a new line of work toward an efficient signature scheme with small key size. But, we leave the detail security analysis for the future research.

The main idea of the signature scheme can be summarized as follows:

1. Alice chooses a secret projective variety Y, which is a shifted (through an automorphism of the ambient space) Secant variety of the Grassmannian.

2. She publishes a set of equations vanishing on the variety.

3. A message is encoded into a linear subspace L of the ambient space. A signature is a point P lying in the intersection $Y \cap L$.

4. Alice can quickly sign a message by using the Plücker embedding of the Grassmannian and her secret automorphism.

5. Signature P can be verified easily by checking whether it satisfies or not the set of public equations and the system of linear equations defining L.

We have implemented our algorithm in a computer algebra system SageMath [35] and is available at
`https://github.com/mgyawali/SSGrass`.

6.2 Preliminaries

In this section, we describe some background required to explain the signature scheme. There are good references for the materials covered in this section, for example, see in [1, 39, 76, 80, 92].

6.2.1 Grassmannian

Projective space $\mathbb{P}^n_\kappa = \mathbb{P}^n$ of dimension n parameterizes the lines through the origin that are contained in $\mathbb{A}^{n+1}$. Equivalently, it parametrizes the 1-dimensional subspaces of a κ-vector space V of dimension $n+1$. The Grassmannian is an immediate generalization of this concept.

Definition 6.2.1. *Let V be a n dimensional vector space over κ. For $1 \leq d \leq n$, the Grassmannian of d-subspaces of V is the set*

$$G(d, V) = \{W \leq V : \dim(W) = d\}.$$

When $V = \kappa^n$, this is denoted by $G(d, n)$.

Recalling from the basic linear algebra, two ordered sets of linearly independent vectors of V, $\mathcal{B} = \begin{pmatrix} \vec{v}_1 \\ \vdots \\ \vec{v}_d \end{pmatrix}$ and $\mathcal{B}' = \begin{pmatrix} \vec{w}_1 \\ \vdots \\ \vec{w}_d \end{pmatrix}$, generate the same subspace $W \subset V$ if and only if there is an invertible matrix $M \in \mathcal{GL}(d)$ such that

$$\mathcal{B}' = M \cdot \mathcal{B}.$$

The following proposition implies that Grassmannian can be identified by a set of matrices of some fixed rank up to a certain equivalence relation.

Proposition 6.2.2. *Let $\mathcal{G}(d,n)$ be the set of $d \times n$ matrices A of rank d modulo the equivalence relation*

$$A \sim A' \iff \exists M \in \mathcal{GL}(d) : A = MA'.$$

Then there is a bijection

$$\mathcal{G}(d,n) \leftrightarrow G(d,n),$$

which maps the class of a matrix A to the vector space spanned by the rows of A.

From now on, we will not distinguish $\mathcal{G}(d,n)$ and $G(d,n)$.
Similar to the case of the projective space, affine charts can also be defined for the Grassmannian. Let S any subset of $\{1,...,n\}$ such that $\#S = d$ and denote by $U_S \subset G(d,n)$ the subset of matrices for which the $d \times d$ minors corresponding to S is non-zero. Note that $G(d,n)$ is covered by these subsets U_S. Furthermore any $[M] \in U_S$ admits a unique representative for which the $d \times d$ sub-matrix corresponding to S is the identity matrix: in fact if M_S is such a sub-matrix, then we can take $M_S^{-1}M$ as a representative. It follows that U_S is identified with $\mathbb{A}^{d(n-d)}$.

Example 6.2.3. *Suppose that $S = \{1,...,d\}$, then denoting by* HJ *the operator of horizontal joint of two matrices (having the same number of rows), we have the following characterization*

$$U_S = \{\mathrm{HJ}(I_d, B) : B \in \mathrm{Mat}_{d\times(n-d)}(\kappa)\}.$$

We want to characterize $G(d,n)$ as a projective variety, i.e., as an object defined by polynomial equations in a projective space. The first aim is to find the projective space on which it lies. We will observe this with the help of an exterior power of a vector space.

Definition 6.2.4. *Let V be an n-dimensional κ-vector space, $0 < d \leq n$. Then the d-th exterior power of V, denoted by $\bigwedge^d V$, is the vector space spanned by the tensors of the form $v_1 \wedge v_2 \cdots \wedge v_d$, where $\wedge$ satisfies the following properties:*

- *it is d-linear:*

$$a \cdot (v_1 \wedge ... \wedge v_d) = (av_1) \wedge v_2 ... \wedge v_d = ... = v_1 \wedge ... \wedge v_{d-1} \wedge (av_d),$$

$$v_1 \wedge ... \wedge (v_i + v_i') \wedge ... \wedge v_d = v_1 \wedge ... \wedge v_i \wedge ... \wedge v_d + v_1 \wedge ... \wedge v_i' \wedge ... \wedge v_d;$$

- *it is antisymmetric:*

$$v_{\sigma(1)} \wedge ... \wedge v_{\sigma(d)} = (-1)^{\mathrm{sgn}(\sigma)} v_1 \wedge ... \wedge v_d,$$

for any $\sigma \in \mathcal{S}_d$, where $\mathcal{S}_d$ denotes the d-th symmetric group.

Remark 6.2.5. *Note that the antisymmetric condition implies, for characteristic* > 2*, that*

$$\dim(\text{Span}(v_1, ..., v_d)) < d \Rightarrow v_1 \wedge ... \wedge v_d = 0. \tag{6.1}$$

In characteristic 2, when there is no distinction between symmetry and antisymmetry, it is possible to define the "antisymmetric" property by the symmetric one with Condition 6.1.

Fix a basis $\{e_1, \ldots, e_n\}$ of the vector space V, then the set

$$\{e_{i_1} \wedge \cdots \wedge e_{i_d} : 1 \leq i_1 < \ldots \leq i_d \leq n\} \tag{6.2}$$

forms a basis for $\bigwedge^d(V)$, with dimension $\binom{n}{d}$.

Lemma 6.2.6. *Let W be a d-dimensional subspace of an n-dimensional vector space V over κ. Let $\mathcal{U} = \begin{bmatrix} u_1 \\ \vdots \\ u_d \end{bmatrix}$ and $\mathcal{W} = \begin{bmatrix} w_1 \\ \vdots \\ w_d \end{bmatrix}$ be two bases of W and M be a $d \times d$ invertible matrix such that*

$$\mathcal{U} = M\mathcal{W}.$$

Then

$$u_1 \wedge \cdots \wedge u_d = \det(M) \cdot w_1 \wedge \cdots \wedge w_d.$$

This lemma shows that whatever the bases we choose for W, the corresponding wedge product is uniquely determined up to a scalar multiplication. Therefore, the following map

$$\iota : G(d, V) \to \mathbb{P}(\bigwedge^d V)$$

given by $W \mapsto [v_1 \wedge \cdots \wedge v_d]$, where $\{v_1, \ldots v_d\}$ is a basis of $W \in G(d, V)$, is well defined.

Proposition 6.2.7. *The map $\iota : G(d, V) \to \mathbb{P}(\bigwedge^d V)$ defined above is an isomorphism onto the image, called Plücker embedding.*

Proof. See in [63, Theorem 5.2.1] □

By Proposition 6.2.7, the Grassmannian $G(d, V)$ can be seen as a subset of a projective space.

Fix a basis $\{e_1, ..., e_n\}$ of V, then Set 6.2 is a basis of $\bigwedge^d V$. In fact, the Plücker embedding maps $[M]$ to the sequence of its minors of rank d.

The image $\iota(G(d, V))$ is a projective variety defined by a set of quadratic equations.

Theorem 6.2.8. *The image of the Plücker embedding $\iota(G(d,V)) \subset \mathbb{P}(\bigwedge^d(V))$ is a projective variety defined by quadratic equations, called Plücker relations. Call $\{X_{i_1,\dots,i_d}\}_{1\leq i_1<\dots<i_d\leq n}$ the coordinates of $\mathbb{P}(\bigwedge^2 V)$, then for any couple of ordered sequences*

$$1 \leq i_1 < i_2 < \dots < i_{d-1} \leq n, \;\; 1 \leq j_1 < j_2 < \dots < j_{d+1} \leq n$$

the following equations hold:

$$\sum_{l=1}^{d+1} X_{i_1,\dots,i_{d-1},j_l} X_{j_1,\dots,\hat{j_l},\dots,j_{d+1}} = 0,$$

where $j_1,\dots,\hat{j_l},\dots,j_{d+1}$ is the sequence obtained by discarding j_l by the sequence $j_1,\dots,j_{d+1}$.

Proof. See in [63, Theorem 5.2.3] □

6.2.2 Grassmannian of planes and its secant variety.

In this section, we focus on the case $d = 2$. This case is interesting because both the Grassmannian and its secant variety are defined by sparse equations.

Definition 6.2.9. *Let $X \subset \mathbb{P}^n$ be a projective variety. The secant variety of X, denoted by $\mathrm{Sec}(X)$ is the smallest projective variety containing the locus*

$$\bigcup_{P,Q\in X} l_{P,Q},$$

where $l_{P,Q}$ denotes the line joining P and Q.

This definition implies that $\mathrm{Sec}(X)$ contains elements of the form $[ax_1 + bx_2]$, where $x_1, x_2 \in \mathbb{A}^{n+1}$ are such that $[x_1], [x_2] \in X$, $a, b \in \kappa$. When $X = G(d,n)$, $\mathrm{Sec}(X)$ parameterizes the tensors which can be written as sum of two indecomposable tensors.

Definition 6.2.10. *Let A be an antisymmetric matrix, then the square root of its determinant i.e. $\sqrt{\det(A)}$ is called the Pfaffian of A.*

We observe that there exists a correspondence between elements of $\bigwedge^2 V$ and $n \times n$ antisymmetric matrices: for any $t \in \bigwedge^2 V$, write $t =$

$\sum_{1\leq i<j\leq n} t_{ij} e_i \wedge e_j$. Then the corresponding $n \times n$ antisymmetric matrix is $M_t = (m_{ij})$, where

$$m_{ij} = \begin{cases} t_{ij} \text{ if } i < j \\ 0 \text{ if } i = j \\ -t_{ij} \text{ if } i > j. \end{cases}$$

The rank of the matrix M_t is strictly related to the minimum number of simple tensors in which t can be decomposed.

Proposition 6.2.11. *Let $t \in \bigwedge^2 V$ and M_t be its associated antisymmetric matrix. Then*

$$\text{rank}(M_t) = 2n_t,$$

where n_t is the minimum number of simple tensors in which t can be decomposed.

Remark 6.2.12. *An antisymmetric matrix can have only an even rank and there is an alternative criteria for detecting its rank.*

Definition 6.2.13. *Let $A = (a_{ij})$ be an $n \times n$ matrix and $B = (b)_{ij}$ be its sub-matrix of order $m \times m$. Then B is centred at the diagonal if there exists a sequence $1 \leq s_1 < ... < s_m \leq n$ such that*

$$b_{ij} = a_{s_i, s_j}.$$

A minor of A is called centred at the diagonal if it is the determinant of a sub-matrix of A centred at the diagonal.

Remark 6.2.14. *If A is (anti)symmetric, then so is any sub-matrix centred at the diagonal.*

Proposition 6.2.15. *Let M be an antisymmetric matrix. Then the* $\text{rank}(M) \leq r - 2$ *if and only if all the $r \times r$ minors that are centered at the diagonal vanish.*

There is an immediate consequence for the description of $G(2, n)$ and $\text{Sec}(G(2, n))$.

Corollary 6.2.16. *Let $[t] \in \mathbb{P}(\bigwedge^2 V)$. Then:*

- *$t \in G(2, V)$ if and only if* $\text{rank}(M_t) = 2$ *if and only the Pfaffians of the 4×4 centered at the diagonal sub-matrices vanish;*
- *$t \in \text{Sec}(G(2, V))$ if and only if* $\text{rank}(M_t) \leq 4$ *if and only the Pfaffians of the 6×6 centered at the diagonal sub-matrices vanish.*

In particular, $\mathrm{Sec}(G(2,V))$ is defined by $\binom{n}{6}$ cubic polynomials, which are quite sparse. For example, the Pfaffian

$$\mathrm{pf}\begin{pmatrix} 0 & X_0 & X_1 & X_2 & X_3 & X_4 \\ -X_0 & 0 & X_5 & X_6 & X_7 & X_8 \\ -X_1 & -X_5 & 0 & X_9 & X_{10} & X_{11} \\ -X_2 & -X_6 & -X_9 & 0 & X_{12} & X_{13} \\ -X_3 & -X_7 & -X_{10} & -X_{12} & 0 & X_{14} \\ -X_4 & -X_8 & -X_{11} & -X_{13} & -X_{14} & 0 \end{pmatrix}$$

is a polynomial with 15 non-zero monomials. Therefore, one expects that if we shift $\mathrm{Sec}(G(2,n))$ by a sparse automorphism of $\mathbb{P}^n$ then we will have a variety defined by sparse cubic equations.

The dimension of $\mathrm{Sec}(G(2,n))$ is known.

Proposition 6.2.17. *Let $d = dim(G(2,n))$ be the dimension of $G(2,n)$ (so $d = 2(n-2)$), then* $\dim(\mathrm{Sec}(G(2,n))) = 2d-3$.

6.2.3 Points in linear sections of the Grassmannian

A better approach for generating random points inside a linear section of $G(d,n)$ is not by using Gröbner bases, but by using the affine charts and the Plucker embedding. If we fix a subset $S \subset \{1,...,n\}$ of cardinality d, then the Plücker map restricts to an embedding

$$\mathbb{A}^{d(n-d)} \to \mathbb{P}^{\binom{n}{d}-1}.$$

Let $L \subset \mathbb{P}^{\binom{n}{d}-1}$ be a linear subspace of codimension $n-d$. Then it is possible to find points inside $L \cap G(2,n)$ by just using linear algebra. To illustrate the procedure, we consider the case in which $S = \{1,...,d\}$. Suppose

$$L = \begin{cases} L_1(X) = 0 \\ \vdots \\ L_{n-d}(X) = 0 \end{cases}$$

then we can choose a vector of unknowns

$$\vec{x} = (1,0,...,0,x_{d+1},...,x_n)$$

and $d-1$ random vectors of κ^n

$$\begin{aligned} \vec{a}_1 &= (0,1,...,0,a_{1,d+1},...,a_{1,n}) \\ &\vdots \\ \vec{a}_{d-1} &= (0,...,0,1,a_{d-1,d+1},...,a_{d-1,n}) \end{aligned}$$

and solve the linear system in $x_{d+1}, ..., x_n$:

$$\begin{cases} L_1(\vec{x} \wedge \vec{a}_1 \wedge \cdots \wedge \vec{a}_{d-1}) = 0 \\ \vdots \\ L_{n-d}(\vec{x} \wedge \vec{a}_1 \wedge \cdots \wedge \vec{a}_{d-1}) = 0. \end{cases}$$

In general, this system has a unique solution $\vec{x}_0$, then

$$P = [\vec{x}_0 \wedge \vec{a}_1 \wedge \cdots \wedge \vec{a}_{d-1}]$$

is a point of $G(d, n) \cap L$.

6.3 New signature scheme

In this section we present a signature scheme, which consists of three parts: key generation, signing and verification. We propose a signature scheme using $\mathrm{Sec}(G(2, n))$, but it can be easily adapted to $G(d, n)$ as well. We use a vector space V of dimension n over a finite field $\kappa = \mathbb{F}_{2^\ell}$ of characteristic 2 then V is identified with κ^n.

6.3.1 Key generation

The private key consists of a random automorphism ϕ of $V = \kappa^n$, which is sparse and defined over $\mathbb{F}_2$. The public key is a set of cubic equations vanishing on $\phi(\mathrm{Sec}(G(2, n)))$.
Private key generation:

1) Alice chooses a random upper triangular, invertible and sparse $\binom{n}{2} \times \binom{n}{2}$ matrix M'_A.
2) Alice chooses two random $\binom{n}{2} \times \binom{n}{2}$ permutation matrices A_1, A_2;
3) Alice defines $M_A = A_1 M'_A A_2$ and then the private key is

$$K_A^{\mathrm{pri}} = (M_A, M_A^{-1}).$$

If a polynomial $F(X)$, where $X = \begin{pmatrix} X_0 \\ \vdots \\ X_n \end{pmatrix}$, vanishes on a variety $Y \subset \mathbb{P}^n$ and M is an invertible $(n+1) \times (n+1)$ matrix, then $F(M^{-1}X)$ vanishes on MY. This fact gives an easy way to generate the public key.
Public key generation:

1) Alice chooses a random subset $\{F_1(X), ..., F_m(X)\}$ of the set of $\binom{n}{6}$ Pfaffians defining $\mathrm{Sec}(G(2,n))$.

2) She computes $G_i(X) = F_i(M_A X)$ for $i \in \{1, ..., m\}$ and a set

$$K_A^{\mathrm{pub}} = \{G_1(X), ..., G_m(X)\}$$

denoting the public key. Note that G_i vanishes on $M_A^{-1}\,\mathrm{Sec}(G(2,n))$ for $i \in \{1, ..., m\}$.

6.3.2 Signature generation and verification

A message D is encoded into a linear subspace of $\mathbb{P}^{\binom{n}{2}-1}$ cut by $n-2$ linear equations $\{L_1 = 0, ..., L_{n-2} = 0\}$ defined over $\mathbb{F}_2$.

1) Alice choose a random vector $\vec{a} \in \kappa^n$ of the form $\vec{a} = (0, 1, a_3, ..., a_n)$ and a vector of unknowns $\vec{x} = (1, 0, x_3, ..., x_n)$;

2) Alice computes

$$L_1'(X) = L_1(M_A^{-1}X), ..., L_{n-2}'(X) = L_{n-2}(M_A^{-1}X)$$

and imposes the condition

$$L_i'(\vec{x} \wedge \vec{a}) = 0, \quad \forall i \in \{1, ..., n-2\}, \tag{6.3}$$

where $\vec{x} \wedge \vec{a}$ is identified with its coordinates with respect to the basis $\{e_i \wedge e_j : 1 \leq i < j \leq n\}$. Here 6.3 is a linear system in $\{x_3, ..., x_n\}$, which has a unique solution $(b_3, ..., b_n) \in \kappa^{n-2}$ in general;

3) Let $\vec{b} = (1, 0, b_3, ..., b_n)$, then $P = [M_A^{-1}(\vec{a} \wedge \vec{b})] \in D \cap (M_A^{-1}G(2,n))$. So the point P satisfies the system of equations:

$$\begin{cases} G_1(X) = 0 \\ \quad \vdots \\ G_m(X) = 0 \\ L_1(X) = 0 \\ \quad \vdots \\ L_{n-2}(X) = 0 \end{cases}$$

and $P \in G(2,n) \cap D$.

4) Alice repeats the procedure in $1) - 3)$ and finds another point $Q \in (M_A^{-1}G(2,n)) \cap D$;

5) Alice chooses two random vectors of $\vec{v}_P, \vec{v}_Q \in \kappa^{\binom{n}{2}}$ such that $[v_P] = P, [v_Q] = Q$ and defines $S_A = [v_P + v_Q] \in D \cap (M_A^{-1}\,\mathrm{Sec(G(2,n))})$ to be the signature of D.

If Bob wants to verify the signature, he has to verify

$$G_i(S_A) = 0 \text{ for } i \in \{1, ..., m\}$$
$$L_i(S_A) = 0 \text{ for } i \in \{1, ..., n-2\}.$$

6.3.3 A toy example

Here we give a toy example with $n = 6, \kappa = \mathbb{F}_2$. The ambient space of $G(2,6)$ is $\mathbb{P}^{14}$, $\mathrm{Sec}(G(2,6))$ is a degree 3 hypersurface defined by the equation (for $n = 6$, there is only one equation)

$$\begin{aligned} &X_4X_7X_9 + X_3X_8X_9 + X_4X_6X_{10} + X_2X_8X_{10} + X_3X_6X_{11} + \\ &X_2X_7X_{11} + X_4X_5X_{12} + X_1X_8X_{12} + X_0X_{11}X_{12} + X_3X_5X_{13} + \\ &X_1X_7X_{13} + X_0X_{10}X_{13} + X_2X_5X_{14} + X_1X_6X_{14} + X_0X_9X_{14} = 0. \end{aligned} \tag{6.4}$$

The private key is given by the two matrices:

$$M_A = \begin{bmatrix} 0&0&0&0&0&0&0&0&1&0&0&0&0&1&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0 \\ 1&0&0&0&0&0&1&1&0&0&0&1&0&0&0 \\ 0&0&0&0&0&0&0&0&1&0&0&0&1&0&0 \\ 0&1&1&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&1&0&0&0&0&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&1&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&1 \\ 0&0&0&0&0&0&0&0&1&1&0&1&0&0 \\ 0&0&0&0&0&1&0&0&1&1&0&0&0&0 \\ 0&0&0&1&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&1&0&0&0&0&0&0&0 \\ 1&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 1&0&0&0&0&0&0&0&0&1&0&0&0&0&1 \end{bmatrix}$$

and

$$M_A^{-1} = \begin{bmatrix} 0&0&0&0&0&0&0&0&0&0&0&0&0&1&0 \\ 0&0&0&0&1&0&1&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&1&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&1&0&0&0&0&0&0&0&0&0 \\ 0&1&0&1&0&0&0&0&1&0&1&0&0&1&1 \\ 0&0&0&0&0&0&0&0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&0&1&0&0&0&0&0&0&0 \\ 0&1&0&1&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&1&0&0&0&0&1&1 \\ 0&1&0&0&0&0&0&0&1&1&0&0&0&1&1 \\ 0&0&1&0&0&0&0&1&0&0&0&0&1&1&0 \\ 0&1&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 1&1&0&1&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&1&0&0&0&0&0&0 \end{bmatrix}.$$

Applying the transformation of coordinates $X \mapsto M_A X$ to (6.4), we get the K_A^{pub} given by the equation

$$\begin{aligned}
&X_0^2X_4 + X_1X_2X_5 + X_2^2X_5 + X_0X_4X_6 + X_1X_4X_6+\\
&X_2X_4X_6 + X_0X_3X_7 + X_0X_4X_7 + X_3X_6X_7 + X_3X_7^2+\\
&X_1X_2X_8 + X_2^2X_8 + X_2X_3X_8 + X_0X_4X_8 + X_0X_5X_8+\\
&X_3X_6X_8 + X_0X_8^2 + X_1X_2X_9 + X_2^2X_9 + X_0X_4X_9+\\
&X_4X_6X_9 + X_1X_7X_9 + X_2X_7X_9 + X_4X_7X_9 + X_8X_9^2+\\
&X_1X_7X_{10} + X_2X_7X_{10} + X_0X_8X_{10} + X_8X_9X_{10} + X_0X_4X_{11}+\\
&X_3X_7X_{11} + X_4X_9X_{11} + X_0X_2X_{12} + X_2X_3X_{12} + X_0X_4X_{12}+\\
&X_0X_7X_{12} + X_1X_7X_{12} + X_2X_7X_{12} + X_0X_8X_{12} + X_2X_9X_{12}+\\
&X_8X_9X_{12} + X_0X_5X_{13} + X_3X_6X_{13} + X_0X_8X_{13} + X_9^2X_{13}+\\
&X_0X_{10}X_{13} + X_9X_{10}X_{13} + X_0X_{12}X_{13} + X_9X_{12}X_{13} + X_0X_4X_{14}+\\
&X_0X_5X_{14} + X_4X_6X_{14} + X_5X_6X_{14} + X_4X_7X_{14} + X_5X_7X_{14}+\\
&X_0X_8X_{14} + X_6X_8X_{14} + X_7X_8X_{14} + X_0X_9X_{14} + X_6X_9X_{14}+\\
&X_7X_9X_{14} + X_4X_{11}X_{14} + X_5X_{11}X_{14} + X_8X_{11}X_{14} + X_9X_{11}X_{14}+\\
&X_2X_{12}X_{14} + X_6X_{12}X_{14} + X_9X_{12}X_{14} + X_{10}X_{12}X_{14} + X_{12}^2X_{14}+\\
&X_9X_{13}X_{14} + X_{10}X_{13}X_{14} + X_{12}X_{13}X_{14} = 0.
\end{aligned} \tag{6.5}$$

Suppose Alice wants to sign a message D, corresponding to the system of linear equations:

$$\begin{cases}
L_1 = X_0 + X_2 + X_3 + X_4 + X_5 + X_7 + X_{10} + X_{11} + X_{12} & = 0\\
L_2 = X_2 + X_4 + X_6 + X_{13} + X_{14} & = 0\\
L_3 = X_3 + X_4 + X_{10} + X_{11} + X_{13} + X_{14} & = 0\\
L_4 = X_1 + X_2 + X_3 + X_4 + X_5 + X_6 + X_9 + X_{12} + X_{13} + X_{14} & = 0.
\end{cases}$$

Alice shifts the message D through the matrix M_A^{-1}, by computing $L_i'(X) = L_i(M_A^{-1}X)$. She obtains the system

$$D_A : \begin{cases}
X_1 + X_4 + x_6 + X_9 + X_{10} + x_{12} + X_{13} & = 0\\
X_0 + X_1 + X_3 + X_5 + X_6 + X_7 + X_8 + X_9 + X_{10} + X_{14} & = 0\\
X_0 + X_2 + X_3 + X_4 + X_5 + X_6 + X_7 + X_8 + X_9 + X_{13} + X_{14} & = 0\\
X_1 + X_2 + X_3 + X_4 + X_5 + X_6 & = 0.
\end{cases}$$

Alice chooses a vector of unknowns $\vec{x} = (1, 0, x_3, x_4, x_5, x_6)$ and two random vectors $\vec{a}_1 = (0, 1, 1, 1, 1, 1), \vec{a}_2 = (0, 1, 1, 0, 0, 1)$. The condition that $\vec{x} \wedge \vec{a}_1 \in$

D_A corresponds to the linear system

$$\begin{cases} x_6 & = 0 \\ x_3 + x_5 + 1 & = 0 \\ x_4 + x_6 & = 0 \\ x_3 + x_4 & = 0 \end{cases}$$

whose solution is $(0, 0, -1, 0)$. Call $x_1 = (1, 0, 0, 0, -1, 0), P_1 = [x_1 \wedge a_1]$. Similarly, the condition that $\vec{x} \wedge \vec{a}_2 \in D_A$ corresponds to the linear system

$$\begin{cases} x_4 + x_5 & = 0 \\ x_3 + x_5 + x_6 & = 0 \\ x_3 + x_4 + x_5 & = 0 \\ x_3 + x_4 & = 0 \end{cases}$$

whose solution is $(0, 0, 0, 0)$. Call $x_2 = (1, 0, 0, 0, 0, 0), P_2 = [x_2 \wedge a_2]$. Then

$$P_1 = [1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1],$$

$$P_2 = [1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0].$$

$P_1, P_2 \in G(2, 6) \cap D_A$. Call $P = [x_1 \wedge a_1 + x_2 \wedge a_2]$, then

$$P = [0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1]$$

is a point of $\mathrm{Sec}(G(2, 6)) \cap D_A$. It follows that

$$S_A = M_A^{-1} \cdot P = [0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0]$$

is a point of $M_A^{-1} \mathrm{Sec}(G(2, 6)) \cap D$. Therefore, it satisfies Equation (6.5) and $L_i(S_A) = 0$ for $i \in \{1, 2, 3, 4\}$.

6.4 Security analysis

Suppose, Frank wants to forge a signature of Alice for a message $D = \{L_1, ..., L_{n-2}\}$. Generic techniques, for instance, by using Grobner basis to solve the polynomial system like

$$\begin{cases} G_i = 0 \text{ for } i \in \{1, ..., m\} \\ L_i = 0 \text{ for } i \in \{1, ..., n-2\} \end{cases}$$

takes exponential time in general but it depends heavily on the nature of the problem. Faugère's $\mathbf{F}_4$ and $\mathbf{F}_5$ [37] are currently the best algorithm to compute Gröbner basis. The number of steps required to compute Gröbner basis is bounded by

$$\mathcal{O}\left(ld\binom{N+d-1}{d}^{\omega}\right) \tag{6.6}$$

for a graded monomial ordering upto degree d, where N is the number of variables, l is the number of equation in the system of homogeneous polynomials, and ω is the matrix multiplication exponent [8]. In our context, we estimate according to our experimental evidences.
If Alice produces around $\binom{n}{6}$ signatures, Frank is able to compute a basis of the vector space of cubic equations vanishing on $M_A^{-1}\,\mathrm{Sec}(G(2,n))$. This fact allows Frank to use two possible approaches:

1) Trying to reconstruct the matrix M_A;

2) Apply a Gröbner basis approach, after having a full set of equations defining $\mathrm{Sec}(G(2,n))$.

We need to study the complexity of the second approach: in general, it is possible to give a very rough upper bound but the number of steps required may be very less in practice, so it is preferable an empirical analysis. We expect that the value of n will not be too large for efficiency reason otherwise we may require larger base field to make the message space large enough. In fact, if we have a valid signature P defined over κ for a message D, then the probability that it is also a valid signature for another message D' is $\frac{1}{(\#\kappa)^{n-2}}$. So signatures defined over a smaller field must be considered invalid for smaller values of n. In our case, $N = \binom{n}{2}$ and experimentally we believe $d = n^2$ in the equation 6.6, this gives an exponential complexity.

Secant varieties of Grassmannian are varieties with many extra structure. For an attacker, it is tempting to try and exploit this structure in order to recover the secret linear change of the variables transforming the disguised variety $M_A^{-1}\,\mathrm{Sec}(G(2,n))$. The same is true for the hidden Veronese variety $M_A \cdot V_{3,m}$ in Subsection 5.1.2. There are some attempts to parameterize algebraic varieties [73] and certain types of surfaces [52]. It would be an interesting problem to see an impact of this technique to the Secant variety of the Grassmannian and Veronese variety over a field of non-zero characteristics.

n	Time	Memory uses
10	637.889 seconds	7457.69 MB
11	240327.910 seconds	260880.47MB
12	Aborted in two weeks	462414.7MB (In two weeks running time)

Table 6.1: Gröbner basis computation

6.4.1 Gröbner basis computation

The variety $M_A^{-1}\,\mathrm{Sec}(G(2,n))$ has dimension $2d-3$, where $d = 2(n-2) = \dim(G(2,n))$. So, if we want to find points on $(M_A^{-1}\,\mathrm{Sec}(G(2,n))) \cap D$, where D is a codimension $n-2$ linear subspace of $\mathbb{P}^{\binom{n}{2}-1}$, in general, we need to intersect with other $2d-3-(n-2) = 2d-n-1$ hyperplanes. In our code, we will consider hyperplanes of the form $X_i = c_i X_{i_0}$, where $c_i \in \kappa$. If we dehomogenize with respect to the variable X_{i_0} (i.e. we set $X_{i_0} = 1$), it is equivalent to put $2d-n$ conditions of the form $X_i = c_i$. We assume that the forger Frank knows a basis of the vector space of cubic forms vanishing on $M_A^{-1}\,\mathrm{Sec}(G(2,n))$.
We have posted a MAGMA [15] code at `https://github.com/mgyawali/SSGrass`. We implemented the code in a machine with the processor Intel(R) Xeon(R) CPU E7-4850 v3 @ 2.20GHz and 1.585 TB RAM and got timings as in Table 6.1.
Finite field : $\mathbb{F}_{2^{13}}$
Order: Graded Reverse Lexicographical
Algorithm used : Faugère F4
Magma V2.23-8 a

6.5 Estimated key sizes

6.5.1 Private key size

The private key consists of the two matrices M_A and M_A^{-1}, which are, by construction, sparse binary matrices with around $2n$ components equal to 1. So they require storage of around $4n$ bits.

6.5.2 Public key size

The public key is given by a set of m equations of the form

$$\{F_i(M_A X) : i \in \{1, ..., m\}\},$$

where $\{F_1, ..., F_m\}$ is a subset of the $\binom{n}{6}$ Pfaffian cubic polynomials defining $\mathrm{Sec}(G(2, n))$. The Pfaffians have 15 non-zero terms, which are square-free. The number of non-zero terms of the shifted Pfaffians, in general, is variable. Since the matrix M_A is sparse, we expect that they are also sparse. In the particular case when all the rows of M_A have exactly two components equal to 1, each shifted Pfaffian has several non-zero terms which are less than or equal to $120 = 15 \cdot 2^3$. Therefore, it is expected that the size of the public key in this case is around $120m$ bits.

6.5.3 Message size

If $\kappa = \mathbb{F}_{2^\ell}$ then the size of the message, which is a set of $n - 2$ hyperplanes of $\mathbb{P}^{\binom{n}{2}-1}$, is $\binom{n}{2} \cdot (n - 2)$ bits.

6.5.4 Signature size

The signature is a point of $\mathbb{P}^{\binom{n}{2}-1}$ defined over κ, so it occupies $\ell \cdot \left(\binom{n}{2} - 1\right)$ bits.

Bibliography

[1] Richand Joseph Abdelkerim. Geometry of the dual grassmannian. PhD thesis, University of Illinois at Chicago, 2011.

[2] Abdelmalek Abdesselam. A computational solution to a question by beauville on the invariants of the binary quintic. *Journal of Algebra*, 303(2):771–788, 2006.

[3] Arthur O. L. Atkin. The number of points on an elliptic curve modulo a prime. Preprint, 1988.

[4] Arthur O. L. Atkin. The number of points on an elliptic curve modulo a prime. Preprint, 1992.

[5] Reza Azarderakhsh, Amir Jalali, David Jao, and Vladimir Soukharev. Practical supersingular isogeny group key agreement. Cryptology ePrint Archive, Report 2019/330, 2019.

[6] Reza Azarderakhsh, Brian Koziel, Matt Campagna, Brian LaMacchia, Craig Costello, Patrick Longa, Luca De Feo, Michael Naehrig, Basil Hess, Joost Renes, Amir Jalali, Vladimir Soukharev, David Jao, and David Urbanik. Supersingular isogeny key encapsulation, 2017.

[7] Magali Bardet, Jean-Charles Faugère, and Bruno Salvy. On the degree of regularity of Gröbner basis computation of semi regular overdetermined algebraic equations. *In International Conference on Polynomial System Solving 2004*, pages 71– 75, 2004.

[8] Magali Bardet, Jean-Charles Faugère, and Bruno Salvy. On the complexity of the **F**5 Gröbner basis algorithm. *Journal of Symbolic Computation*, 70:49–70, 2015.

[9] Christian Batut, Karim Belabas, Dominique Bernardi, Henri Cohen, and Michel Olivier. Users guide to pari-gp. Université de Bordeaux I.

[10] Laurent Bernardin and Michael B. Monagan. Efficient multivariate factorization over finite fields. In Mora T. and Mattson H., editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. AAECC 1997. Lecture Notes in Computer Science*, volume 1255, pages 15–28. Springer, Berlin, Heidelberg., 1997.

[11] Daniel J. Bernstein, Johannes Buchmann, and Erik Dahmen. *Post-Quantum Cryptography*. Springer-Verlag Berlin Heidelberg, 2009.

[12] Ward Beullens, Thorsten Kleinjung, and Frederik Vercauteren. CSI-FiSh: Efficient isogeny based signatures through class group computations. In Steven D. Galbraith and Shiho Moriai, editors, *Advances in Cryptology – ASIACRYPT 2019*, pages 227–247, Cham, 2019. Springer International Publishing.

[13] Jean-François Biasse, David Jao, and Anirudh Sankar. A quantum algorithm for computing isogenies between supersingular elliptic curves. In *International Conference in Cryptology in India*, pages 428–442. Springer, 2014.

[14] Wieb Bosma and Peter Stevenhagen. On the computation of quadratic 2- class group. *J. Théorie Nombres bordeaux*, 8(2):283–313, 1996.

[15] John Cannon, Wieb Bosma, Claus Fieker, and Allan Steel (eds.). Handbook of magma functions, version 2.19, 2013.

[16] John William S. Cassels. *Rational Quadratic Forms*. Rational Quadratic Forms L.M.S. vol.13. ACADEMIC PRESS, 1978.

[17] Pierre Castel. Solving quadratic equations in dimension 5 or more without factoring. *Open Book Series*, 1(1):213–233, 2013.

[18] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: An efficient post-quantum commutative group action. In Thomas Peyrin and Steven D. Galbraith, editors, *Advances in Cryptology – ASIACRYPT 2018*, pages 395–427. Springer International Publishing, 2018.

[19] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: An efficient post-quantum commutative group action. Cryptology ePrint Archive, Report 2018/383, 2018.

[20] Wouter Castryck, Jana Sotáková, and Frederik Vercauteren. Breaking the decisional Diffie-Hellman problem for class group actions using

genus theory. In Ristenpart T. Micciancio D., editor, *Advances in Cryptology CRYPTO 2020*, Lecture Notes in Computer Science, vol 12171, pages 92–120. Springer, Cham, 2020.

[21] Denis X. Charles, Eyal Z. Goren, and Kristin E. Lauter. Cryptographic hash functions from expander graphs. *Journal of Cryptology*, 22(1):93–113, January 2009.

[22] Andrew Childs, David Jao, and Vladimir Soukharev. Constructing elliptic curve isogenies in quantum subexponential time. *Journal of Mathematical Cryptology*, 8(1):1–29, 2014.

[23] Henri Cohen. *A Course in Computational Algebraic Number Theory*. Springer, 2010.

[24] Craig Costello. B-sidh: supersingular isogeny diffie-hellman using twisted torsion. Cryptology ePrint Archive, Report 2019/1145, 2019.

[25] Jean-Marc Couveignes. Computing l-isogenies using the p-torsion. In *ANTS-II: Proceedings of the Second International Symposium on Algorithmic Number Theory*, volume 7, Springer-Verlag, London, UK, 1996. AMS International Press.

[26] Jean-Marc Couveignes. Isomorphism between artin-schreier towers. *Mathematics of Computation*, 69(232):1625–1631, 2000.

[27] Jean-Marc Couveignes. Hard homogeneous spaces. Cryptology ePrint Archive, Report 2006/291, 2006.

[28] David A. Cox. *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*. Pure and Applied Mathematics. Wiley, second edition, 2013.

[29] Luca De Feo. Mathematics of isogeny based cryptography, 2017.

[30] Luca De Feo and Steven D. Galbraith. SeaSign: Compact isogeny signatures from class group actions. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2019*, pages 759–789, Cham, 2019. Springer International Publishing.

[31] Luca De Feo, Jean Kieffer, and Benjamin Smith. Towards practical key exchange from ordinary isogeny graphs. Cryptology ePrint Archive, Report 2018/485, 2018.

[32] Luca De Feo, Simon Masson, Christophe Petit, and Antonio Sanso. Verifiable delay functions from supersingular isogenies and pairings. In Steven D. Galbraith and Shiho Moriai, editors, *Advances in Cryptology – ASIACRYPT 2019*, pages 248–277, Cham, 2019. Springer International Publishing.

[33] Victoria de Quehen, Péter Kutas, Chris Leonardi, Chloe Martindale, Lorenz Panny, Christophe Petit, and Katherine E. Stange. Improved torsion point attacks on SIDH variants. Cryptology ePrint Archive, Report 2020/633, 2021.

[34] Christina Delfs and Steven D. Galbraith. Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$. *Designs, Codes and Cryptography*, 78(2):425–440, February 2016.

[35] The Sage Developers. The sage mathematics software system (version 9.0), 2020. `https://www.sagemath.org`.

[36] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. 22(6):644–654, 1976.

[37] Jintai Ding, Albrecht Petzoldt, and Dieter S. Schmidt. *Multivariate Public Key Cryptosystems*, volume 80 of *Advances in Information Security*. Springer, second edition, 2020.

[38] Jintai Ding and Dieter Schmidt. Rainbow, a new multivariate polynomial signature scheme. In J. Ioannidis, A. Keromytis, and M. Yung, editors, *Applied Cryptography and Network Security. ACNS 2005. Lecture Notes in Computer Science*, volume 3531, pages 164–175. Springer, Heidelberg, 2005.

[39] Igor Dolgachev. *Lectures on Invariant Theory*. Cambridge University Press, 2003.

[40] Taher Elgamal. A public-key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 31(4):469–472, 1985.

[41] Noam D. Elkies. Elliptic and modular curves over finite fields and related computational issues. In *Computational perspectives on number theory (Chicago, IL, 1995)*, volume 7 of *Studies in Advanced Mathematics*, Providence, RI, 1998. AMS International Press.

[42] Luca De Feo. Fast algorithms for towers of finite fields and isogenies. PhD thesis, École Polytechnique, 2010.

[43] Luca De Feo. Fast algorithms for computing isogenies between ordinary elliptic curves in small characteristic. *Journal of Number Theory*, 131(5):873–893, 2011.

[44] Luca De Feo and Éric Schost. Fast arithmetics in artin-schreier towers over finite fields. *Journal of Symbolic Computation*, 47(7):771–792, 2012.

[45] Luca De Feo, Cyril Hugounenq, Jérôme Plût, and Éric Schost. Explicit isogenies in quadratic time in any characteristic. *LMS J. Comput. Math.*, 19(A):267–282, 2016.

[46] Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, and Benjamin Wesolowski. SQISign: Compact post-quantum signatures from quaternions and isogenies. In Moriai S. and Wang H., editors, *Advances in Cryptology ASIACRYPT 2020. Lecture Notes in Computer Science*, volume 12491, pages 64–93. Springer, Cham., 2020.

[47] Steven D. Galbraith. Constructing isogenies between elliptic curves over finite fields. *LMS Journal of Computation and Mathematics*, 2:188–138, 1999.

[48] Steven D. Galbraith. *The mathematics of Public Key Cryptography*, volume 151. Cambridge University Press, New York, 2012.

[49] Steven D. Galbraith, Florian Hess, and Nigel P. Smart. Extending the ghs weil descent attack. In Knudsen L.R., editor, *Advances in Cryptology EUROCRYPT 2002. Lecture Notes in Computer Science*, volume 2332, pages 164–175. Springer, Berlin, Heidelberg, 2002.

[50] Steven D. Galbraith, Christophe Petit, Barak Shani, and Yan Bo Ti. On the security of supersingular isogeny cryptosystems. In *Advances in Cryptology–ASIACRYPT 2016: 22nd International Conference on the Theory and Application of Cryptology and Information Security*, pages 63–91. Springer, 2016.

[51] Steven D. Galbraith, Christophe Petit, and Javier Silva. Identification protocols and signature schemes based on supersingular isogeny problems. In Tsuyoshi Takagi and Thomas Peyrin, editors, *Advances in Cryptology – ASIACRYPT 2017*, pages 3–33. Springer International Publishing, 2017.

[52] Willem A De Graaf, Michael Harrison, Jana Pílniková, and Josef Schicho. A lie algebra method for rational parametrization of Severi-Brauer surfaces. *Journal of Algebra*, 303(2):514–529, 2006.

[53] James L. Hafner and Kevin S. McCurley. A rigorous subexponential algorithm for computation of class groups. *Journal of the American Mathematical Society*, 2(4):837–850, 1989.

[54] Frank Harary, John P. Hayes, and Horng-Jyh Wu. A survay of the theory of hypercube graphs. *Computers & Mathematics with Applications*, 15(4):277–289, 1988.

[55] Robin Hartshorne. *Algebraic Geometry*. Springer, 1977.

[56] David Jao and Luca De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In Yang BY., editor, *Post-Quantum Cryptography. PQCrypto 2011*, volume 7071, pages 19–34, Springer, Berlin, Heidelberg, 2011. Lecture Notes in Computer Science.

[57] Aviad Kipnis, Jacques Patarin, and Louis Goubin. Unbalanced oil and vinegar schemes. In Stern J., editor, *EURO-CRYPT 1999, Lecture Notes in Computer Science*, volume 1592, pages 206–222. Springer,, 1999.

[58] David Kohel. Endomorphism rings of elliptic curve over finite fields. PhD thesis, University of California, Berkeley, 1996. `http://iml.univ-mrs.fr/~kohel/pub/thesis.pdf`.

[59] David R. Kohel, Kristin Lauter, Christophe Petit, and Jean-Pierre Tignol. On the quaternion-isogeny path problem. *LMS Journal of Computation and Mathematics*, 17(A):418–432, 2014.

[60] Elena Konstantinova. Some problems on Cayley graphs. *Linear Algebra and its Applications*, 429(11-12):2754–2769, 2008.

[61] Péter Kutas, Chloe Martindale, Lorenz Panny, Christophe Petit, and Katherine E. Stange. Weak instances of SIDH variants under improved torsion-point attacks. Cryptology ePrint Archive, Report 2020/633, 2020.

[62] Péter Kutas, Simon-Philipp Merz, Christophe Petit, and Charlotte Weitkämper. Improved torsion point attacks on SIDH variants. Cryptology ePrint Archive, Report 2021/282, 2021.

[63] Venkatraman Lakshmibai and Justin Brown. *The Grassmannian Variety: Geometric and Representation-Theoretic Aspects*, volume 42 of *Developments in Mathematics*. Springer, 2015.

[64] Ueli M. Maurer and Stefan Wolf. The Diffie-Hellman protocol. *Designs, Codes and Cryptography*, 19:147–171, 2000.

[65] James S. Milne. Abelian varieties, 1991. `https://www.jmilne.org/math/CourseNotes/AV110.pdf`.

[66] National Institute of Standards and Technology. Post-quantum cryptography standardization, August 2016. `https://csrc.nist.gov/News/2016/Post-Quantum-Cryptography-Proposed-Requirements`.

[67] National Institute of Standards and Technology. Post-quantum cryptography standardization, July 2020. `https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization`.

[68] Gordon Pall. Discriminantal divisors of binary quadratic form*. *Journal of Number Theory*, 1(4):525–533, 1969.

[69] Richard Peng and Santosh Vempala. Solving sparse linear systems faster than matrix multiplication. In *Proceedings of the 2021 ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 504–521.

[70] Donato Pera. Design and performance evaluation of a linux hpc cluster. *Task Quarterly*, 22(2), 2018.

[71] Christophe Petit. Faster algorithms for isogeny problems using torsion point images. In Tsuyoshi Takagi and Thomas Peyrin, editors, *Advances in Cryptology – ASIACRYPT 2017*, pages 330–353. Springer International Publishing, 2017.

[72] Christophe Petit and Kristin Lauter. Hard and easy problems for supersingular isogeny graphs. Cryptology ePrint Archive, Report 2017/962, 2017.

[73] Jana Pílniková. Parametrizing algebraic varietiesusing lie algebras. Ph.D. thesis, Research Institute for Symbolic Computations Johannes Kepler University Linz, Austria, 2006.

[74] Kenneth Alan Ribet. On modular representations of $\mathcal{G}_{\bar{\mathbb{Q}}/\mathbb{Q}}$ arising from modular forms. *Invent. Math.*, 100(2):431–476, 1990.

[75] Alexander Rostovtsev and Anton Stolbunov. Public-key cryptosystem based on isogenies. Cryptology ePrint Archive, Report 2006/145, April 2006.

[76] George Salmon. *Higher Algebra, fifth ed.* Reprinted by Chelsea, New York, 1965.

[77] René Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Math. Comp.*, 44(170):483–494, 1985.

[78] René Schoof. Counting points on elliptic curves over finite fields. *J. Theory Nombres Bordeaux*, 7(1):219–254, 1995.

[79] Jean-Pierre Serre. *A course in arithmetic*. Springer, 1993.

[80] Igor R. Shafarevich. *Basic Algebraic Geometry 1 Varieties in Projective Space, Third ed.* Springer, New York, 2013.

[81] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997. `https://arxiv.org/abs/quant-ph/9508027`.

[82] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1992.

[83] Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*, volume 151 of *Graduate Texts in Mathematics*. Springer, New York, January 1994.

[84] Denis Simon. Quadratic equations in dimensions 4, 5 and more. Preprint, 2005.

[85] Denis Simon. Solving quadratic equations using reduced unimodular quadratic forms. *Mathematics of Computation*, 74(251):1531–1543, 2005.

[86] Marie Sokolová. The chromatic number of extended odd graphs is four. *časopis pro pěstování matematiky*, 112(3):308–311, 1987.

[87] Anton Stolbunov. Constructing public-key cryptographic schemes based on class group action on a set of isogenous elliptic curves. *Advances in Mathematics of Communications*, 4(2), 2010.

[88] Andrew Sutherland. Elliptic curve. MIT Open CourseWare, 2019. `https://ocw.mit.edu/courses/mathematics/18-783-elliptic-curves-spring-2019/index.htm`.

[89] John Tate. Endomorphisms of abelian varieties over finite fields. *Invent mathematicae*, 2(2):134–144, 1966.

[90] Daniele Di Tullio and Manoj Gyawali. A post-quantum key exchange protocol from the intersection of quadric surfaces. Cryptology ePrint Archive, Report 2020/628, 2020. `https://eprint.iacr.org/2020/628.pdf`.

[91] Daniele Di Tullio and Manoj Gyawali. A post-quantum signature scheme from the secant variety of the grassmannian. Cryptology ePrint Archive, Report 2020/1141, 2020. `https://eprint.iacr.org/2020/1141`.

[92] Ravi Vakil. *The rising sea - Foundations of Algebraic Geometry*. 2017. `http://math.stanford.edu/~vakil/216blog/FOAGnov1817public.pdf`.

[93] Jacques Vélu. Isogénies entre courbes elliptiques. *Comptes Rendus de l'Académie des Sciences de Paris*, 273:238–241, 1971.

[94] Lawrence C. Washington. *Elliptic Curves: Number Theory and Cryptography, second edition*. Pure and Applied Mathematics. Chapman & Hall/CRC, 2008.

[95] William C. Waterhouse. Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup.*, 4(2):521–560, 1969.