Università di Pisa

Corso di Laurea Magistrale in Matematica
Tesi di Laurea Magistrale

Supersingular Isogeny Diffie Hellman: Algorithms and Quantum Security

Candidato:
Agnese Gini

Relatori:
Prof. Carlo Traverso
Prof. Roberto Dvornicich

Controrelatore:
Prof.ssa Ilaria Del Corso

Anno Accademico 2017/2018

A Te.

Contents

Introduction

Quantum computing has drastically changed the concept of computationally hard problem. As a consequence, many classical cryptosystems turn out to be unsafe and the issue of figuring out *quantum resistant* protocols has given rise to an active research area. The USA National Institute of Standards and Technology has initiated a process to solicit the production, evaluation and standardization quantum of resistant public-key cryptographic algorithms; they pointed out that, although we are not able to predict exactly when powerful enough quantum computers will be produced, the recent technological development leads to think that this event is not so far. In this thesis, we focus on a system proposed by David Jao and Luca De Feo in [JDF11] based on elliptic curves over finite fields. An *elliptic curve* is a nonsingular projective curve of genus one and a specified base point. Without loss of generality, to a practical aim, we intend in this thesis elliptic curves as plane nonsingular cubics with fixed Weierstrass coordinates. These varieties are particularly interesting due to the fact that they can be endowed with a group law expressed in terms of regular morphisms. Hence both the geometric and the algebraic structure are compatible, namely they are abelian varieties. The maps between elliptic curves, which respect this double characterization, are called *isogenies* and they have a central role in the cryptosystem we are dealing with. The protocol we study is a public key exchange on the model of the one purposed by Diffie and Hellman in 1976. The Diffie Hellman protocol allows two parties to share a secret that can be deduced from the public keys and either of the two private keys. In its basic form, given g a generator of $\mathbb{F}_p^*$ the private keys are two integer a, b, the public keys are $\alpha = g^a$ and $\beta = g^b$ and the shared secret is $g^{ab} = \alpha^b = \beta^a$. The original method relies on the hardness of computing the discrete logarithms over finite fields. Moreover, in literature, there exist many variants also based on discrete logarithm problem over elliptic curves. The state of art classical attacks to DH protocol run in subexponential time, in the case of finite field, and in exponential time, in the case of elliptic curves. Shor in [Sho94] has proven that a quantum computer can solve the discrete logarithm problem over finite groups in polynomial time. This means that these protocols are not quantum resistant. However, DH model can be adapted to produce a key exchange which is instead safe from both classical and quantum attacks: the *Supersingular Isogeny Diffie Hellman* key exchange (SIDH). Let p be a prime and E_0 a supersingular elliptic curve over $\mathbb{F}_{p^2}$. The private keys are two points R_A, R_B of (public) fixed order $\ell_A^{e_A}$ and $\ell_B^{e_B}$, where ℓ_A and ℓ_B are primes different from p, and the public keys are $E_A = E_0/\langle R_A \rangle$ and $E_B = E_0/\langle R_B \rangle$, i.e. the codomains of the isogenies ϕ_A and ϕ_B whose kernels are the fixed cyclic subgroups. The secret shared key is the j-invariant of the curve $E = E_A/\langle\phi_A(R_B)\rangle = E_B/\langle\phi_B(R_A)\rangle$. Differently form DH to recover E it is necessary that the two parties provide the images of the $E_0[\ell_A^{e_A}]$ and $E_0[\ell_B^{e_B}]$, respectively, as additional information in the public keys. Our aim is to deepen the theoretical bases and the mathematical background in order to investigate the actual security of this system.

In chapter 1, we recall definitions, facts and fundamental notions about elliptic curves. We outline the group law, Tate Module properties, the relation between elliptic curves and complex lattices and we prove that the endomorphism ring of an elliptic curve has to be isomorphic either to $\mathbb{Z}$ or to an order in number field or to an order in a definite quaternion algebra. If the elliptic curve is defined over a finite field, the set of rational points is a finite group and the endomorphism ring of the curve always strictly contains $\mathbb{Z}$. Specifically, when the endomorphism ring is an order in a number field we call the curve *ordinary* curve while when it is an order in a quaternion algebra we call the curve *supersingular*. Note that in the first case the ring is commutative and in the latter it is not.

In chapter 2, we summarize basic knowledge of public key cryptography, we describe the Diffie Hellman protocol and we analyze and discuss the impact of quantum computation in cryptography.

The security of SIDH is based on the fact that, given two elliptic curves defined over a finite field, find an isogeny between them is supposed to be hard also in quantum context. Tate has proved that two elliptic curves are isogenous if and only if the their endomorphism rings are orders in the same $\mathbb{Q}$-algebra. Thus, in chapter 3, we study the endomorphism ring of elliptic curves defined over a finite field: we describe a method to associate connected undirected multigraphs to classes of isogenous curves and we explain how to translate isogenies in terms of paths in that graphs. We also see the connection that such graphs have with classes of ideals and the good properties deriving from it. A consequence of Tate's theorem is that supersingular and ordinary curves can not be isogenous, so it is possible to distinguish the two cases. In particular, we show that in the ordinary case the graphs obtained have regular and rigid structures while the supersingular graphs are more complicated. The results in this chapter are already known but they belong to different areas of mathematics. Our contribution has been to rephrase, organize, fill in and make them coherent in order to obtain a self contained discussion. In chapter 4, we describe the best currently known quantum algorithms to solve the general isogeny problem, i.e. the problem to find an isogeny between fixed elliptic curves. In particular, we show how the non commutativity of the endomorphism ring makes the problem harder for supersingular elliptic curves. First of all, we present a classical algorithm for ordinary case by Galbraith, Hess and Smart (GHS), on which successive algorithms are based. They reduce the problem of recovering an isogeny, between two fixed ordinary elliptic curves, to the problem of finding a fractional ideal such that, through the (endomorphism ring) class group action, brings one in the other. With a classical computer GHS algorithm run in exponential time with respect to the characteristic of the base field. Childs, Jao and Soukharev, in [CJS14], rephrase the strategy of GHS as an abelian hidden shift problem and prove that a quantum computer can solve the ordinary general isogeny problem in subexponential time. In the supersingular case, it is not possible to directly apply such idea, since it is not known an abelian group that acts over the endomorphism ring, which in this case is not commutative. We explain and analyze the idea of Biasse, Childs and Sankar to overcome this problem using the fact that if the curves are defined over $\mathbb{F}_p$, where p is prime, it is possible to adopt the same method of the ordinary case. The resulting complexity is exponential. Therefore, the general isogeny problem can be considered hard.

Finally, in chapter 5 we define the Supersingular Isogeny Diffie Hellman protocol. We discuss the parameters choice in order to maximize the security, in view of the results of the previous chapters, and we give some examples. Indeed proving that the general isogeny problem is easy would imply that the system is not secure. It is not certain if the vice versa is true, since during the key exchange are given additional information about the action of the isogenies over torsion points. On this matter, we examine a recent work of Petit [Pet17], who has shown that, if we consider some variations of the parameters choice, such additional information actually decrease the hardness of the problem. For the original proposal by Jao and De Feo the problem is still open.

In order to clarify some results and the SIDH protocol, we have included some new examples produced, using the computer algebra softwares `Magma` and `Sage`.

Chapter 1

Elliptic Curves

In this chapter we introduce the principal definitions, facts and concepts about elliptic curves. We particularly focus to which are basic to the results in the following chapters. The main references texts to this chapters are [Sil11] and [Was08].

An elliptic curve is a smooth projective curve of genus one with a specified base point. To a practical aim we intend for elliptic curve a curve with fixed Weierstrass coordinates:

Definition 1.0.1. Let E a smooth curve defined over a field K. E is an *elliptic curve* if it is the locus in $\mathbb{P}^2(\overline{K})$ of an equation of the form

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{1.1}$$

with coefficients $a_1, \ldots, a_6 \in K$ and satisfying $O \coloneqq [0,1,0] \in E$.

Let us recall that a projective variety V is defined over a field K if it generating homogeneous polynomials have coefficients in K. Using this definition is not actually a restrain, since each elliptic curve can be represented as a smooth Weierstrass plane cubic curve and also the converse holds. Generally we express E in the affine coordinates $x = X/Z$ and $y = Y/Z$

$$E\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1.2}$$

O is the single point at infinity, thus it is called *point at infinity* or the *base point.* Later we will always assume, up to specify it, that the characteristic of the base field is different from 2 o 3. In this case, up to a change of coordinates, we can suppose our curve having Weierstrass equation

$$y^2 = x^3 + ax + b. \tag{1.3}$$

Moreover, under this assumption, some important invariants could be express in a more comfortable form.

1.1 Group Law

An elliptic curve E can be endowed with a group structure. Since E is defined by a cubic equation, any in line L in $\mathbb{P}^2$ intersect E in exactly three points P, Q, R

by Bézout's Theorem. Obviously if L is tangent to E two of these coincide. The group law is denoted by $+$ and is defined as follows:

Definition 1.1.1. Let $P, Q \in E$, let L be the line through P and Q (if $P = Q$, let L be the tangent line to E at P), and let R be the third point of intersection of $L \cap E$. Let L' be the line through R and O. $P + Q$ is the point such that $L' \cap E = \{O, R, P + Q\}$.

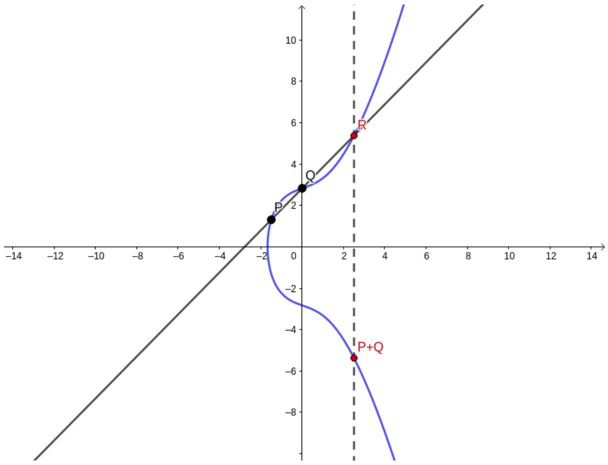

Figure 1.1: Sum of two points of the elliptic curve $y^2 = x^3 + 2x + 8$.

The composition law has the following properties:

Proposition 1.1.2. *Let E be an elliptic curve.*

1. *If a line L intersects E at the (not necessarily distinct) points P, Q, R, then*
$$(P + Q) + R = O$$
2. $P + O = P$ *for all* $P \in E$.
3. $P + Q = Q + P$ *for all* $P, Q \in E$.
4. *Let $P \in E$. There is a point of E, denoted by $-P$, satisfying*
$$P + (-P) = O$$
5. $LetP, Q, R \in E$. *Then*
$$(P + Q) + R = P + (Q + R).$$

Corollary 1.1.3. $(E, +)$ *is an abelian group with identity element O.*

Let us consider the set of point of E defined over K

$$E(K) := \left\{(x, y) \in K^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\right\} \cup \{O\}$$

is a subgroup of E and it is called *K-rational point subgroup of E*. It is a subgroup since, if P and Q have coordinates in K, the equation of the line

connecting them has coefficients in K.
For example, if E has equation $y^2 = x^3 + ax + b$ and $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ both different from the point at infinity. If $P = -Q$ then $Q = (x_1, -y_1)$ and $P + Q = O$, otherwise let

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

then

$$P + Q = (\lambda^2 - x_1 - x_2, -\lambda x_3 - y_1 + \lambda x_1).$$

For $m \in \mathbb{N}$ and $P \in E$, we let

$$[m]P = \underbrace{P + \cdots + P}_{m}$$

$$[-m]P = \underbrace{-P \cdots - P}_{m}$$

$$[0]P = O.$$

Sometimes we briefly denote the multiplication by mP.

1.2 Morphisms and Isogenies

Let us consider a smooth curve C/K, usually the function field of C over an extension L/K is denoted by $L(C)$. If P is a point of C, we can consider the rational function defined in P, i.e. $\bar{K}[C]_P$. Since C is smooth each point is smooth and $\bar{K}[C]_P$ is a discrete valuation ring. The (normalized) valuation in P is usually denoted by

$$\begin{array}{cccc} \operatorname{ord}_P \colon & \bar{K}[C]_P & \longrightarrow & \mathbb{N} \cup \{\infty\} \\ & f & \longmapsto & \sup\left\{d \in \mathbb{Z} \mid \ f \in M_P^d\right\}. \end{array}$$

where M_P it the maximal ideal of $\bar{K}[C]_P$ and it is called *order in* P. Using $\operatorname{ord}_P(f/g) = \operatorname{ord}_P(f) - \operatorname{ord}_P(g)$, we can extend this valuation to $\bar{K}(C)$. Moreover, M_P is principal and we call a generator t *uniformizer* for C at P; in particular any function $t \in \bar{K}(C)$ with $\operatorname{ord}_P(t) = 1$ is an uniformizer.
A *rational map* $\phi \colon C_1 \to C_2$ between two projective curves $C_1 \subseteq \mathbb{P}^n$ and $C_2 \subseteq \mathbb{P}^m$ is a map of the form

$$\phi = [f_0, \ldots, f_m]$$

where the functions $f_0, \ldots, f_m \in \bar{K}(C_1)$ have the property that for every point $P \in C_1$ at which they are all defined,

$$\phi(P) = [f_0(P), \ldots, f_m(P)]$$

If both the curve are defined over K, the Galois $\operatorname{Gal}(\bar{K}/K)$ act on ϕ in the following way

$$\phi^\sigma(P) = [f_0^\sigma(P), \ldots, f_m^\sigma(P)]$$

Notice that we have the formula

$$\phi(P)^\sigma = \phi^\sigma(P^\sigma)$$

for all $\sigma \in \mathrm{Gal}(\bar{K}/K)$ and $P \in C_1$.
If, in addition, there is some $\lambda \in \bar{K}^*$ such that $\lambda f_0, \ldots, \lambda f_n \in K(C_1)$ then ϕ is called *defined* over K. Hence, a rational map ϕ is defined over K if is fixed by the action of $\mathrm{Gal}(\bar{K}/K)$. Note that a rational map is not necessarily a well-defined function at every point of C_1. However, it may be possible to evaluate $\phi(P)$ at points P of C_1 where some f_i is not regular by replacing each f_i by gf_i for an appropriate $g \in \bar{K}(C_1)$. This observation bring us to the following notions:

Definition 1.2.1. A rational map

$$\phi = [f_0, \ldots, f_m] \colon C_1 \to C_2$$

is *regular* at $P \in C_1$ if there is a function $g \in \bar{K}(C_1)$ such that

i. each gf_i is regular at P ;

ii. there is some i for which $(gf_i)(P) \neq 0$.

If such a g exists, then we set

$$\phi(P) = [gf_0(P), \ldots, gf_m(P)].$$

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

We say that C_1 and C_2 are *isomorphic*, if there exist morphisms $\phi \colon C_1 \to C_2$ $\psi \colon C_2 \to C_1$ such that $\psi \circ \phi$ and $\phi \circ \psi$ are the identity maps on C_1 and C_2, respectively. If both curve are defined over K, we say that are *isomorphic over* K if ψ and ϕ can be defined over K. Note that both maps must be morphisms, not merely rational maps.

Let us consider specifically elliptic curves and the following invariants:

Definition 1.2.2. Let $E \colon y^2 = x^3 + ax + b$ an elliptic curve the quantity

$$\Delta = -16(4a^3 + 27b^2)$$

is the *discriminant* of the Weierstrass equation and

$$j(E) = 1728\frac{4a^3}{4a^3 + 27b^2} = -1728\frac{(4a)^3}{\Delta}$$

is the *j-invariant* of the elliptic curve.

The discriminant depends on the choice of coordinates, so on the equation. A curve expressed by Weierstrass equation is non-singular if and only if $\Delta \neq 0$; thus the j-invariant is well defined. Differently from the discriminant, the j-invariant does not depend on the coordinates and it an invariant of the elliptic curve, moreover it is invariant up to isomorphism:

Theorem 1.2.3. *Two elliptic curves are isomorphic over $\bar{K}$ if and only if they have the same j-invariant.*

Proof. Proposition III§1.4 [Sil11]. □

This means that we can uniquely identify the isomorphism classes by j-invariants. Note that the isomorphism provided by Theorem 1.2.3 is defined over the algebraic closure, hence it can happen that two elliptic curves defined over K which have the same j-invariant are not isomorphic over K. For example, let E be the curve given by $y^2 = x^3 + ax + b$ over a finite field K and let $d \in \bar{K}^* \setminus K$ such that $d^2 \in K$ the elliptic curve

$$E_d \colon y^2 = x^3 + ad^2x + bd^3$$

is called *quadratic twist* of E. Easy computations show that $j(E) = j(E_d)$, however the transformation which sends E to E_d $(x, y) \to (\sqrt{d}x', d\sqrt{d}y')$ is not defined over K.

Let us suppose to have $j_0 \in \bar{K}$, $\operatorname{char} K \neq 2, 3$, we can always find an elliptic curve defined over $K(j_0)$ whose j-invariant is j_0. In particular, let us suppose $j_0 \neq 0, 1728$ a possible elliptic curve[1] is

$$E_0 \colon y^2 + xy = x^3 - \frac{36}{j_0 - 1728}x - \frac{1}{j_0 - 1728}.$$

While we have

$$j(y^2 + y = x^3) = 0$$

and

$$j(y^2 = x^3 + x) = 1728.$$

Morphisms between curves have some special properties. The following it is crucial:

Theorem 1.2.4. *Let $\phi \colon C_1 \to C_2$ be a morphism of curves. Then ϕ is either constant or surjective.*

Proof. Theorem II§2.3.[Sil11]. □

Now, let us consider two curves over K and let ϕ a nonconstant rational map defined over K. Then composition with ϕ induces a map between the function fields fixing K,

$$\begin{array}{cccc} \phi^* \colon & K(C_2) & \longrightarrow & K(C_1) \\ & f & \longmapsto & f \circ \phi \end{array}$$

that is injective. It holds that $K(C_1)$ is a finite extension of $\phi^*(K(C_2))$ and so it is well defined the *degree of* ϕ: if ϕ is constant we define $\deg \phi = 0$, otherwise

$$\deg \phi = [K(C_1) \colon \phi^*(K(C_2))]$$

We say that ϕ is *separable, inseparable*, or *purely inseparable* if the field extension $K(C_1)/\phi^*(K(C_2))$ has the corresponding property and we define the separable or inseparable degree consequently. It can be proved that ϕ it is an isomorphism if and only if it has degree one.

[1] We defined here the j-invariant only for curve in reduced Weierstrass form. There exists a general definition, one can use it or equivalently make a change of coordinates and then compute the j-invariant, since itis invariant under isomorphisms.

Assume that $\mathrm{char}(K) = p > 0$ and let $q = p^r$. For any polynomial $f = \sum a_\alpha X^\alpha \in K[X]$, we define

$$f^{(q)} = \sum a_\alpha^q X^\alpha$$

Then for any curve C/K, we can define a new curve $C^{(q)}$ defined over K as the curve whose homogeneous ideal is generated by $f^{(q)}$ for all $f \in I(C)$.

Definition 1.2.5. The natural map

$$\begin{array}{rccc} \pi\colon & C & \longrightarrow & C^{(q)} \\ & [x_0, \dots, x_n] & \longmapsto & [x_0^q, \dots, x_n^q] \end{array}$$

is called the *qth-power Frobenius morphism.*

The next proposition describes two important properties of the Frobenius map:

Proposition 1.2.6.

1. *ϕ is purely inseparable and* $\deg \pi = q$.
2. *Every map $\phi\colon C_1 \to C_2$ of (smooth) curves over a field of characteristic $p > 0$ factors as*
$$\phi\colon C_1 \xrightarrow{\pi} C_1^{(q)} \xrightarrow{\lambda} C_2$$
where q is the inseparable degree of ϕ, the map π is the qth-power Frobenius map, and the map λ is separable.

Proof. Proposition II§2.11 and Corollary II§2.12 [Sil11]. □

We just proved that elliptic curves have both a geometric structure and an algebraic structure of abelian group. This two characterization are compatible, since the equations giving the group law on E are morphisms. Namely, elliptic curves are *abelian variety.* From this point of view we would like to deal with maps which are compatible with both the structures.

Definition 1.2.7. Let (E_1, O_1) and (E_2, O_2) be elliptic curves. An *isogeny* from E_1 to E_2 is a morphism $\phi\colon E_1 \to E_2$ satisfying $\phi(O_1) = O_2$.

The geometrical nature implies that mapping the point at infinity of the first curve to the points it is enough to obtain that for all $P, Q \in E_1$

$$\phi(P + Q) = \phi(P) + \phi(Q)$$

It means that the isogenies are all the morphism such that are also group homomorphisms. Note that by Theorem 1.2.4 we have that an isogeny ϕ is such that either $\phi(E_1) = O_2$ or $\phi(E_1) = E_2$. In particular, in the latter case we will say that E_1 and E_2 are *isogenous.*
By convention the first map is usually denoted as $[0]$ and $\deg[0] = 0$. Since non vanishing isogenies are also morphism, it is well defined the degree of an isogeny and it holds that for all chain of isogenies

$$\deg(\psi \circ \phi) = \deg(\psi)\deg(\phi)$$

We indicate the set of isogenies from E_1 to E_2 by $\mathrm{Hom}(E_1, E_2)$ and we usually use $\mathrm{End}(E)$ for $\mathrm{Hom}(E, E)$ the set of *endomorphisms* of E. If the curve involved are defined over K we denote by $\mathrm{Hom}_K(E_1, E_2)$ the set of isogenies defined over K. Naturally, the homomorphisms' set inherits the structure of abelian group with the sum defined by $(\phi + \psi)(P) = \phi(P) + \psi(P)$. It is also a torsion-free $\mathbb{Z}$ module: for all $m \in \mathbb{Z}$ the multiplication by m-map

$$[m]\colon E \longrightarrow E$$

is a non constant isogeny. We can define the group homomorphism

$$\begin{array}{rccc} [\cdot]\colon & \mathbb{Z} & \longrightarrow & \mathrm{End}(E) \\ & m & \longmapsto & [m] \end{array}$$

which gives to $\mathrm{End}(E)$ the $\mathbb{Z}$ module structure, since if there would exist $\phi \in \mathrm{Hom}(E_1, E_2)$ such that $[m]\phi = [0]$ taking degrees gives $\deg[m]\deg\phi = 0$ so either $m = 0$ or $\phi = [0]$ because $\deg[m] \geq 1$.
The composition of two endomorphisms is already an endomorphism, so we directly obtain the following:

Proposition 1.2.8. *Let E be an elliptic curve. The endomorphism group* $\mathrm{End}(E)$ *is a (not necessarily commutative) ring of characteristic 0 with no zero divisors.*

The kernel of multication by m-map is the set of point such that $[m]P = O$ and it called *m-torsion subgroup of E* and denoted by $E[m]$. The *torsion subgroup of E* is

$$E_{\text{tors}} = \bigcup_{m \geq 1} E[m]$$

If E is defined over K, then $E_{\text{tors}}(K)$ denotes the points of finite order in $E(K)$. The structure of finite torsion groups is known:

Theorem 1.2.9. *Let E be an elliptic curve defined over K and let $m \in \mathbb{Z}$ with* $m \neq 0$.

1. *If $m \neq 0$ in K (if* $\mathrm{char}(K) = p > 0$ *means $p \nmid m$), then*

$$E[m] \simeq {}^{\mathbb{Z}}\!/_{m\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{m\mathbb{Z}}$$

2. *If char$(K) = p > 0$, then one of the following holds:*
   - $\forall\ r \geq 1$ *then* $E[p^r] \simeq \mathbb{Z}/p^r\mathbb{Z}$
   - $\forall\ r \geq 1$ *then* $E[p^r] \simeq \{O\}$

Suppose that $\mathrm{char}(K) = 0$. The map $[\cdot]\colon \mathbb{Z} \to \mathrm{End}(E)$ is often surjective, hence a bijection. When the endomorphism ring is strictly larger than $\mathbb{Z}$ we say that E has *complex multiplication.*
If $\mathrm{char}(K) = p > 0$ and E is defined over the finite field $K = \mathbb{F}_q$, then $E^{(q)} = E$ and π_q is an endomorphism of E, called the *Frobenius endomorphism.* Note that the set of points fixed by it is exactly the finite group $E(\mathbb{F}_q)$.

Let us recall other usefull property of isogenies (the proofs can be found at chapter III of [Sil11]):

Proposition 1.2.10. *Let $\phi\colon E_1 \to E_2$ be a nonzero isogeny.*

1. *$\ker\phi$ is a finite group with cardinality exactly the separable degree of ϕ. Moreover,*
$$\#\phi^{-1}(Q) = \deg_s \phi$$
for all $Q \in E_2$.

2. *If ϕ is separable, then $\#\ker\phi = \deg\phi$ and $\bar{K}(E_1)$ is a Galois extension of $\phi^*(\bar{K}(E_2))$.*

3. *Let $\psi\colon E_1 \to E_3$ be a nonzero isogeny and suppose ϕ to be separable. If*
$$\ker\phi \subset \ker\psi$$
then there is a unique separable isogeny $\lambda\colon E_2 \to E_3$ such that
$$\psi = \lambda \circ \phi$$
$$\begin{tikzcd} E_1 \arrow[r, "\psi"] \arrow[d, "\phi"'] & E_3 \\ E_2 \arrow[ur, dashed, bend right, "\lambda"'] & \end{tikzcd}$$

In practice, most of the time we will be considering separable isogenies, so the previous statements automatically hold. Another crucial property of separable isogenies is that they are completely determined by their kernel:

Theorem 1.2.11. *Let E be an elliptic curve defined over K, and let Φ be a finite subgroup of E which is defined over K, which means it is Gal($\bar{K}/K$)-invariant. There are a unique, up to K-isomorphism, elliptic curve E' and a separable isogeny ϕ defined over K, such that* $\ker\phi = \Phi$ *and $\phi\colon E \to E'$. Often E' is indicated by E/Φ.*

Vélu gave and explicit description of such quotient isogeny:

Theorem 1.2.12 (Vêlu formulae)**.** *Let E be an elliptic curve given by the generalized Weierstrass equation*
$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1.4}$$
with a_i in some field K. Let Φ be a finite subgroup of $E(K)$. Then there exists an elliptic curve E_2 and a separable isogeny ϕ from E to E_2 such that $\Phi = \ker\phi$. For a point $Q = (x_Q, y_Q) \in \Phi$ with $Q \neq 0$, we define
$$g_Q^x := 3x_Q^2 + 2a_2x_Q + a_4 - a_1y_Q \tag{1.5}$$
$$g_Q^y := -2y_Q - a_1x_Q - a_3 \tag{1.6}$$
$$v_Q := \begin{cases} g_Q^x & \text{if } 2Q = O \\ 2g_Q^x - a_1g_Q^y & \text{if } 2Q \neq O \end{cases} \tag{1.7}$$
$$u_Q := (g_Q^y)^2. \tag{1.8}$$

Let Φ_2 be the points of order 2 in Φ. Let us choose $R \subset C$ such that we have disjoint union

$$\Phi = \{O\} \cup \Phi_2 \cup R \cup -R$$

(in other words,for each pair of non-2-torsion points $P, -P \in \Phi$, we put exactly one of them in R). Let S be $R \cup \Phi_2$ and set

$$v = \sum_{Q \in S} v_Q$$

$$w = \sum_{Q \in S} (u_Q + x_Q v_Q)$$

Then E_2 has the equation

$$Y^2 + A_1 XY + A_3 Y = X^3 + A_2 X^2 + A_4 X + A_6, \tag{1.9}$$

where $A_1 = a_1$, $A_2 = a_2$, $A_3 = a_3$, $A_4 = a_4 - 5v$, $A_6 = a_6 - (a_1^2 + 4a_2)v - 7w$. The isogeny $\phi(x, y) = (X, Y)$ is given by

$$X = x + \sum_{Q \in S} \left(\frac{v_Q}{x - x_Q} + \frac{u_Q}{(x - x_Q)^2} \right) \tag{1.10}$$

$$Y = y - \sum_{Q \in S} \left(u_Q \frac{2y + a_1 x + a_3}{(x - x_Q)^3} + v_Q \frac{a_1(x - x_Q) + y - y_Q}{(x - x_Q)^2} + \frac{a_1 u_Q - g_Q^x g_Q^y}{(x - x_Q)^2} \right). \tag{1.11}$$

Proof. Theorem 12.16 [Was08] □

When the base field has positive characteristic, we can obtain separable isogenies also by linear combinations involving the Frobenius morphism:

Proposition 1.2.13. *Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$ and π the Frobenius endomorphism. Let $m, n \in \mathbb{Z}$. Then*

$$m + n\pi \colon E \longrightarrow E$$

is separable if and only if $p \nmid m$. In particular, the map $1 - \pi$ is separable.

Proof. Corollary III§5.5 [Sil11]. □

Note that this also means that if m is not divisible by p then the multication by m is separable and that the endomorphism ring of an elliptic curve defined over a finite field is always larger than $\mathbb{Z}$.

We conclude this section by another central theorem in isogenies' theory:

Theorem 1.2.14. *Let $\phi \colon E_1 \to E_2$ be a nonzero isogeny of degree m. There exists a unique isogeny, called* dual isogeny,

$$\hat{\phi} \colon E_2 \longrightarrow E_1$$

such that $\hat{\phi} \circ \phi = [m]$.
Moreover,

1. $\widehat{\phi \circ \psi} = \hat{\psi} \circ \hat{\phi}$*,*

2. $\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}$*,*

3. $\deg \hat{\phi} = m$*,*

4. $\hat{\hat{\phi}} = \phi$*,*

5. for all $n \in \mathbb{Z}$

$$\widehat{[n]} = [n] \quad \textit{and} \quad \deg[n] = n^2,$$

6. $\hat{\phi}$ *is defined over* K *if and only if* ϕ *is defined over* K*.*

1.3 Tate Module

Let E be an elliptic curve over a field K and let $\ell \geq 2$ a prime of $\mathbb{Z}$, different from p the characteristic of the field. By Theorem 1.2.9 we know that for $n > 0$

$$E[\ell^n] = {}^{\mathbb{Z}}\!\big/_{\ell^n\mathbb{Z}} \times {}^{\mathbb{Z}}\!\big/_{\ell^n\mathbb{Z}}$$

By the natural map

$$[\ell]\colon E[\ell^n] \longrightarrow E[\ell^{n+1}]$$

it is well defined the inverse limit

$$T_\ell(E) = \varprojlim_n E[\ell^n] \tag{1.12}$$

which is called *(ℓ-adic) Tate module of E.*

Each $E[\ell^n]$ torsion group has a structure of $\mathbb{Z}/\ell^n\mathbb{Z}$ module, then Tate module is a $\mathbb{Z}_\ell$-module:

$$T_\ell(E) \simeq \mathbb{Z}_\ell \times \mathbb{Z}_\ell.$$

If we choose a $\mathbb{Z}_\ell$-basis for $T_\ell(E)$, we obtain that

$$\mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(E)) \simeq \mathrm{M}_2(\mathbb{Z}_\ell)$$

and

$$\mathrm{Aut}(T_\ell(E)) \simeq \mathrm{GL}_n(\mathbb{Z}_\ell)$$

The Tate module is a useful tool for studying isogenies. Indeed let us consider an isogeny $\phi\colon E_1 \to E_2$ of elliptic curves and take the restriction, as homomorphism, over the torsion points

$$\phi\colon E_1[\ell^n] \longrightarrow E_2[\ell^n]$$

It induces a $\mathbb{Z}_\ell$-linear map between the Tate modules

$$\phi_\ell\colon T_\ell(E_1) \longrightarrow T_\ell(E_2)$$

and a natural group homomorphism

$$\mathrm{Hom}(E_1, E_2) \longrightarrow \mathrm{Hom}(T_\ell(E_1), T_\ell(E_2))$$

Note that if we consider $E_1 = E_2$ we obtain a ring homomorphism.

Theorem 1.3.1. *Let E_1 and E_2 two elliptic curves defined over K and $\ell \neq \operatorname{char}(K)$ be a prime. The natural map*

$$\begin{array}{ccc} \operatorname{Hom}(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell & \longrightarrow & \operatorname{Hom}(T_\ell(E_1), T_\ell(E_2)) \\ \phi \otimes 1 & \longmapsto & \phi_\ell \end{array}$$

is an injective $\mathbb{Z}_\ell$-module homomorphism.

Proof. Theorem III§7.4 [Sil11]. □

An important consequence is the following statement:

Corollary 1.3.2. *Let E_1 and E_2 be elliptic curves. Then $\operatorname{Hom}(E_1, E_2)$ is a free $\mathbb{Z}$-module of rank at most 4.*

Proof. $\operatorname{Hom}(E_1, E_2)$ is a torsion free module over a principal domain ideal, hence the rank of $\operatorname{Hom}(E_1, E_2)$ over $\mathbb{Z}$ is equal to the rank of $\operatorname{Hom}(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$, i.e. that they are both infinity or if they are finite must coincides. From the Theorem above

$$\operatorname{rk}_{\mathbb{Z}_\ell} \operatorname{Hom}(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \leq \operatorname{rk}_{\mathbb{Z}_\ell} \operatorname{Hom}(T_\ell(E_1), T_\ell(E_2)).$$

We just observed that up to fixing a basis for $T_\ell(E_1)$ and $T_\ell(E_2)$

$$\operatorname{Hom}(T_\ell(E_1), T_\ell(E_2)) \simeq \mathrm{M}_2(\mathbb{Z}_\ell)$$

which has rank 4. □

Through the action of an isogeny over the torsion groups and the Tate module, we can also recover two important quantities:

Proposition 1.3.3. *Let E be an elliptic curve and $\phi \in \operatorname{End}(E)$. Let $\ell \geq 2$ an integer prime different from the characteristic of the base field. Then*

$$\det(\phi_\ell) = \deg(\phi)$$

and

$$\operatorname{Tr}(\phi_\ell) = 1 + \deg(\phi) - \deg(1 - \phi)$$

Proof. Proposition III§8.6 [Sil11]. □

1.4 Endomorphism Ring

Let E be an elliptic curve. In this section we give an initial characterization of which rings may occur as the endomorphism ring of E. In Chapter 2 we will resume the study of the endomorphism ring of elliptic curves defined over finite field and we will describes further properties of these rings.

Let us recall what we stated about $\operatorname{End}(E)$. We saw it is a characteristic 0 ring, then we use Tate module to obtain that it has rank at most 4 as $\mathbb{Z}$-module. Also, by Theorem 1.2.14, the map that associates an isogeny its dual provides an involution for $\operatorname{End}(E)$.
Starting from these properties, we prove that an endomorphism ring is isomorphic to $\mathbb{Z}$ or to one of the following type:

Definition 1.4.1. Let $\mathcal{B}$ be a (not necessarily commutative) $\mathbb{Q}$-algebra that is finitely generated over $\mathbb{Q}$. An order $\mathcal{O}$ of $\mathcal{B}$ is a subring of $\mathcal{B}$ that is finitely generated as a $\mathbb{Z}$-module and such that

$$\mathcal{O} \otimes \mathbb{Q} = \mathcal{B}.$$

Theorem 1.4.2. *Let $\mathcal{O}$ be a ring of characteristic 0, having no zero divisors, and having the following properties:*

i. The rank of $\mathcal{O}$ as $\mathbb{Z}$-module is almost 4;

ii. It has an anti-involution $\alpha \mapsto \hat{\alpha}$ *such that*

$$\widehat{\alpha+\beta} = \hat{\alpha} + \hat{\beta}, \;\; \widehat{\alpha\beta} = \hat{\beta}\hat{\alpha}, \;\; \hat{\hat{\alpha}} = \alpha, \;\; \hat{n} = n \; \forall n \in \mathbb{Z}$$

iii. For $\alpha \in \mathcal{O}$, the product $\alpha\hat{\alpha}$ is a nonnegative integer, and it is 0 if and only if $\alpha = 0$.

Then $\mathcal{O}$ is isomorphic to one of the following type:

1. $\mathbb{Z}$,

2. an order in an imaginary quadratic extension of $\mathbb{Q}$,

3. an order in a define quaternion algebra over $\mathbb{Q}$, i.e. in

$$\mathbb{Q} \oplus \alpha\mathbb{Q} \oplus \beta\mathbb{Q} \oplus \alpha\beta\mathbb{Q}$$

with $\alpha^2, \beta^2 \in \mathbb{Q}$, $\alpha^2 < 0$, $\beta^2 < 0$ and $\beta\alpha = -\alpha\beta$.

Proof. Let $\mathcal{B} = \mathcal{O} \otimes \mathbb{Q}$. Since we have the hypothesis on the rank, it is sufficient to show that $\mathcal{B}$ is respectively isomorphic to $\mathbb{Q}$, to an imaginary quadratic field or to a quaternion algebra of the appropriate form. We can naturally extend the anti-involution over $\mathcal{O}$ to all $\mathcal{B}$ (see also Chapter 2) and define the reduced trace of an element α as $\operatorname{trd}(\alpha) = \alpha + \hat{\alpha}$ and the reduced norm as $\operatorname{nrd}(\alpha) = \alpha\hat{\alpha}$. Let us note the following facts about trace:

- $$\operatorname{trd}\alpha = 1 + \operatorname{nrd}\alpha - \operatorname{nrd}(\alpha - 1), \tag{1.13}$$
  so also $\operatorname{trd}\alpha \in \mathbb{Q}$;
- the trace is $\mathbb{Q}$-linear, since the involution fixes $\mathbb{Q}$;
- if $\alpha \in \mathbb{Q}$ then $\operatorname{trd}(\alpha) = 2\alpha$;
- if $\alpha \in \mathcal{B}$ is such that $\operatorname{trd}(\alpha) = 0$ then $\alpha^2 = -\operatorname{nrd}(\alpha) < 0$, since
  $$0 = (\alpha - \alpha)(\alpha - \hat{\alpha}) = \alpha^2 - \operatorname{trd}\alpha + \operatorname{nrd}\alpha = \alpha^2 + \operatorname{nrd}\alpha$$

If $\mathcal{B} \simeq \mathbb{Q}$ the thesis is trivial. Otherwise there exist $\alpha \in \mathcal{B} \setminus \mathbb{Q}$. Up to replacing α with $\alpha - \operatorname{trd}\alpha/2$, we may assume that $\operatorname{trd}(\alpha) = 0$. By the observation above we have that $\mathbb{Q}(\alpha)$ is a quadratic imaginary field. If $\mathcal{B} = \mathbb{Q}(\alpha)$ the thesis holds. Otherwise there exists $\gamma \in \mathcal{B} \setminus \mathbb{Q}(\alpha)$. Let

$$\beta = \gamma - \frac{1}{2}\operatorname{trd}\gamma - \frac{\operatorname{trd}(\alpha\gamma)}{2\alpha^2}\alpha$$

Then by the outlined properties of the trace and the hypothesis over α we have

$$\operatorname{trd}\beta = \operatorname{trd}\gamma - 2\frac{1}{2}\operatorname{trd}\gamma - 2\frac{\operatorname{trd}(\alpha\gamma)}{2\alpha^2}\operatorname{trd}\alpha = 0$$

By the last point β^2 is a negative rational. Also note that

$$\begin{aligned}\operatorname{trd}(\alpha\beta) &= \alpha\beta + \widehat{\alpha\beta}\\ &= \alpha\beta + \hat{\beta}\hat{\alpha}\\ &= \alpha\beta + \alpha\hat{\beta} - \alpha\hat{\beta} + \hat{\beta}\hat{\alpha}\\ &= (\operatorname{trd}\beta)\alpha + (\operatorname{trd}\alpha)\hat{\beta} = 0\end{aligned}$$

so

$$\alpha = -\hat{\alpha},\ \beta = -\hat{\beta},\ \alpha\beta = -\hat{\beta}\hat{\alpha}$$

and

$$\alpha\beta = -\beta\alpha.$$

Hence to prove that

$$\langle\alpha,\beta\rangle_{\mathbb{Q}} = \mathbb{Q} \oplus \alpha\mathbb{Q} \oplus \beta\mathbb{Q} \oplus \alpha\beta\mathbb{Q}$$

is a quaternion algebra, it is enough to show that $1, \alpha, \beta, \alpha\beta$ are linearly independent. Suppose

$$w + x\alpha + y\beta + z\alpha\beta = 0$$

with $w, x, y, z \in \mathbb{Q}$.

$$\operatorname{trd}(w + x\alpha + y\beta + z\alpha\beta) = 0$$

Taking the trace immidiatly we obtain

$$2w = 0$$

hence $w = 0$. If we multiply by α on the left and β on the right we have

$$(x\alpha^2)\beta + (y\beta^2)\alpha + z\alpha^2\beta^2 = 0$$

but $1, \alpha, \beta$ are linearly independent by construction hence

$$x\alpha^2 = y\beta^2 = z\alpha^2\beta^2 = 0$$

Noting that $\alpha^2 < 0$ and $\beta^2 < 0$ we have the thesis. □

We directly obtain that the endomorphism ring of an elliptic curve E/K is either $\mathbb{Z}$, an order in an imaginary quadratic field, or an order in a quaternion algebra. When $\operatorname{char}(K) = 0$, only the first two are possible, since checking the action of an isogeny over the space of the differential form associated to an elliptic curve, it can be shown that the ring $\operatorname{End}(E)$ must be commutative. On the contrary, when the characteristic is finite the first can not occur since $\pi \notin \mathbb{Z}$.

1.5 Elliptic Curves over Finite Fields

Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$ of characteristic $p > 0$. The group of $\mathbb{F}_q$-rational point is obviously finite. A trivial upper bound is

$$\#E(\mathbb{F}_q) \leq 2q + 1$$

The following theorem gives a better bound:

Theorem 1.5.1 (Hasse). *Let $E/\mathbb{F}_q$ be an elliptic curve defined over a finite field. Then*

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

Proof. Let us fix a Weierstrass equation for E with coefficients in $\mathbb{F}_q$ an π its Frobenius endomorphism. Note that

$$E(\mathbb{F}_q) = \ker(1 - \pi)$$

and $1 - \pi$ is separable by Proposition 1.2.13, hence

$$\#E(\mathbb{F}_q) = \deg(1 - \pi).$$

Let us define $L(\phi, \psi) = \deg(\psi - \phi) - \deg(\phi) - \deg(\psi)$ for $\phi, \psi \in \mathrm{End}(E)$. L is bilinear form positive defined form. Let n, m be two integers. Then

$$0 \leq \deg(m\psi - n\phi) = m^2 \deg(\psi) + mnL(\phi, \psi) + n^2 \deg(\phi).$$

In particular, taking

$$m = -L(\phi, \psi) \quad n = 2\deg(\psi)$$

yields

$$0 \leq \deg(m\psi - n\phi) = L(\phi, \psi)^2 \deg(\psi) - 2\deg(\psi)L(\phi, \psi)^2 + 4\deg(\psi)^2 \deg(\phi)$$

$$L(\phi, \psi)^2 \deg(\psi) \leq 4\deg(\psi)^2 \deg(\phi)$$

$$(\deg(\psi - \phi) - \deg(\phi) - \deg(\psi))^2 \leq 4\deg(\psi)\deg(\phi)$$

considering the square root of the last inequality and putting $\psi = 1$ and $\phi = \pi$, since $\deg \pi = q$ and $\deg 1 = 1$, in particular we have that

$$|\deg(1 - \pi) - q - 1| \leq 2\sqrt{q}$$

□

In 1949, André Weil made a series of conjectures concerning the number of points on varieties defined over finite fields and Hasse Theorem is a special form of it.

Definition 1.5.2. Let us consider V a projective variety defined over $\mathbb{F}_q$, the *V-zeta function* is the power series

$$Z(V/\mathbb{F}_q; T) = \exp\left(\sum_{n=1}^{\infty} \#V(\mathbb{F}_{q^n}) \frac{T^n}{n}\right).$$

Here given any power series $F(T) \in \mathbb{Q}[[T]]$ with no constant term, we intend the power series $\exp(F(T))$ to be the series $\sum_{k\geq 0} F(T)^k/k!$. If we know the zeta series then we can recover the number of of rational points over the extensions by

$$\#V(\mathbb{F}_{q^n}) = \frac{1}{(n-1)!}\frac{d^n}{dT^n}\log Z(V/\mathbb{F}_q;T)_{|T=0}$$

Theorem 1.5.3 (Weil conjecture)**.** *Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$, and let $\#E(\mathbb{F}_q) = q+1-a$. Then*

$$Z(E/\mathbb{F}_q;T) = \frac{1-aT+qT^2}{(1-T)(1-qT)}$$

The proof of Weil conjecture relies some properties of the Frobenius map. In particular, it is a corollary of the following fact:

Theorem 1.5.4. *Let $E/\mathbb{F}_q$ be an elliptic curve and π the qth-power Frobenius endomorphism. Let*

$$a = q+1-\#E(\mathbb{F}_q)$$

be an integer called Frobenius Trace *and*

$$p(T) = T^2 - aT + q.$$

If $\alpha, \beta \in \mathbb{C}$ are the root of $P(T)$, then they are complex conjugates with norm $\sqrt{q}$ and for all $n \geq 1$

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 + \alpha^n - \beta^n.$$

Moreover,

$$\pi^2 - a\pi + q = 0 \quad \textit{in } \mathrm{End}(E).$$

Proof. We observed in Hasse proof that $\#E(\mathbb{F}_q) = \deg(1-\pi)$. Passing to $T_\ell(E)$ for ℓ different from the characteristic of the base field, we have by Proposition 1.3.3

$$\det(\pi_\ell) = \deg(\phi) = q$$

and

$$\mathrm{Tr}(\pi_\ell) = 1 + \deg(\pi) - \deg(1-\pi) = 1 + q - \#E(\mathbb{F}_q) = a$$

Hence the characteristic polynomial of π_ℓ is

$$p(T) = T^2 - aT + q \in \mathbb{Z}[T].$$

We can factor it over $\mathbb{C}$ and we find

$$p(T) = (T-\alpha)(T-\beta)$$

For every rational number $m/n \in \mathbb{Q}$ we have

$$\det\left(\frac{m}{n} - \pi_\ell\right) = \frac{\det(m - \pi_\ell n)}{n^2} = \frac{\deg(m-\pi n)}{n^2}$$

By density we have that $P(T) = \det(T - \pi_\ell) \geq 0$ for all $T \in \mathbb{R}$ so either it has complex conjugate roots or it has a double root. In both cases

$$\alpha\beta = \det \pi_\ell = q \Rightarrow |\alpha| = |\beta| = \sqrt{q}.$$

Note that π_n the q^nth-power Frobenius coincides with π^n, hence

$$\#E(\mathbb{F}_{q^n}) = \deg(1-\pi^n)$$

Through the Jordan normal form of π_ℓ we obtain that

$$\deg(T-\pi^n) = (T-\alpha^n)(T-\beta^n)$$

Then

$$\#E(\mathbb{F}_{q^n}) = \deg(1-\pi^n) = (1-\alpha^n)(1-\beta^n) = q^n + 1 + \alpha^n - \beta^n.$$

The last statement of the theorem follows from Hamilton-Cayley theorem and the following equality

$$\deg(\pi^2 - a\pi + q) = \det(\pi_\ell^2 - a\pi_\ell + q) = \det(0) = 0.$$

□

The facts here we proved emphasize that elliptic curve over finite field must have precise structure. In particular, $E(\mathbb{F}_q)$ is an abelian finite field and Sylow Theorem implies that the following statement holds:

Theorem 1.5.5. *Let E be an elliptic curve over the finite field $\mathbb{F}_q$. Then either*

$$E(\mathbb{F}_q) \simeq \mathbb{Z}/n\mathbb{Z}$$

for some integer $n \geq 1$ or

$$E(\mathbb{F}_q) \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$$

for $n_1, n_2 \in \mathbb{N}$ and $n_1 \mid n_2$.

There are some restrains to the group which can actually realize a subgroup of rational point :

Theorem 1.5.6. *Let $q = p^n$ be a power of a prime number p. Let $N = q+1-a$. There exist an elliptic curve E defined over $\mathbb{F}_q$ such that $\#E(\mathbb{F}_q) = N$ if and only if $|a| \leq 2\sqrt{q}$ and one of the following holds:*

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

Proof. Theorem 4.3 [Was08]. □

Theorem 1.5.7. *Let $q = p^n$ be a power of a prime number p. Let $N = q+1-a$ with $|a| \leq 2\sqrt{q}$ satisfying one of the condition 1-6 of the Theorem 1.5.6. Let*

$$N = \prod_{\ell | N} \ell^{e_\ell}$$

be the prime factorization of N. Then the possible group structures of elliptic curves over $\mathbb{F}_q$ with N points are

$$E(\mathbb{F}_q) = \mathbb{Z}/_{p^e\mathbb{Z}} \times \prod_{\ell \neq p} \left(\mathbb{Z}/_{\ell^{a_\ell}\mathbb{Z}} \times \mathbb{Z}/_{\ell^{e_\ell - a_\ell}\mathbb{Z}} \right)$$

where

1. *if $\gcd(a, p) = 1$ then $0 \leq a_\ell \leq \min\{v_\ell(q-1), \lfloor e_\ell/2 \rfloor\}$ with v_ℓ the ℓ-adic valuation;*
2. *if $a = \pm 2\sqrt{q}$ then $a_\ell = e_\ell/2$, thus*
$$E(\mathbb{F}_q) \simeq \mathbb{Z}/_{(\sqrt{q} \pm 1)\mathbb{Z}} \times \mathbb{Z}/_{(\sqrt{q} \pm 1)\mathbb{Z}};$$
3. *if if $a = 0$ then either the group is cyclic, i.e. all $a_\ell = 0$, or is*
$$E(\mathbb{F}_q) \simeq \mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{((q+1)/2)\mathbb{Z}},$$
4. *if $a = \pm\sqrt{q}$ or $a = \pm p^{(n+1)/2}$ the group is cyclic.*

Only these cases are possible and every case does arise for every q.

Proof. Theorem 9.10.13 [Gal12]. □

Let us consider the endomorphism ring of an elliptic curve E/K where K has characteristic $p > 0$ (it can be infinite). By Theorem 1.2.9 we know that the p-torsion subgroup can be of two type. There is a strictly connection between torsion subgroups and endomorphism ring and the form of p-torsion subgroup influences the structure of the endomorphism ring of the curve.

Theorem 1.5.8. *Let K be a field of characteristic p, and let E/K be an elliptic curve. For each integer $r \geq 1$, let π_r the p^r Frobenius and $\hat{\pi}_r$ its dual. The following condition are equivalent*

a) $E[p^r] = 0$ for one (all) $r \geq 1$.

b) $\hat{\pi}^r$ is (purely) inseparable for one (all) $r \geq 1$.

c) The map $[p]\colon E \to E$ is purely inseparable and $j(E) \in \mathbb{F}_{p^2}$.

d) $\mathrm{End}(E)$ is an order in a quaternion algebra.

If the equivalent conditions above do not hold

$$E[p^r] = \mathbb{Z}/_{p^r\mathbb{Z}} \;\; \forall r \geq 1$$

Further if $j(E) \in \overline{\mathbb{F}}_p$ then $\mathrm{End}(E)$ is an order of a quadratic imaginary field.

Definition 1.5.9. If E has the properties *a*-*b*-*c*-*d* given in the previous theorem, then we say that E is *supersingular*, or that E has *Hasse invariant* 0. Otherwise we say that E is *ordinary*, or that E has *Hasse invariant* 1.

Proof of Theorem 1.5.8. We can suppose K algebricaly close and we fix $\pi = \pi_1$. According to $\pi_r = \pi^r$, the degree is multiplicative and the Frobenius endomorphism is purely inseparable we have that

$$\deg_s(\hat{\pi}_r) = \deg_s([p^r]) = \deg_s([p])^r = \deg_s(\hat{\pi})^r$$

and that

$$\#E[p^r] = \deg_s([p^r])$$

Hence, $E[p^r] = \{0\}$ if and only if $\deg_s([p^r]) = 1$ if and only if $\deg_s(\hat{\pi}) = 1$ if and only if $\hat{\pi}_r$ is purely inseparable, for each r. Let us suppose now $\hat{\pi}$ is purely inseparable. By proposition 1.2.6.2 $\hat{\pi}$ factors as follows

$$\hat{\pi} \colon E^{(p)} \xrightarrow{\pi'} E^{(p^2)} \xrightarrow{\lambda} E$$

where π' is the pth-power Frobenius map of $E^{(p)}$ and the map λ is separable. Checking degrees we obtain that λ must be an isomorphism, then

$$j(E) = j(E^{(p^2)}) = j(E)^{p^2}$$

which means $j(E) \in \mathbb{F}_{p^2}$. Also note that $[p] = \hat{\pi} \circ \pi$ is purely inseparable, too, so *b*) implies *c*).
Note that if $[p]$ is purely inseparable, up to isomorphism, there are only finitely many elliptic curves that are isogenous to E. Indeed, if exists $\psi \colon E \to E'$, since

$$[p] \circ \psi = \psi \circ [p],$$

we have $\#E'[p] = \deg_s[p] = 1$. By the implications we proved $j(E') \in \mathbb{F}_{p^2}$.
Suppose that $\mathrm{End}(E)$ is not an order in a quaternion algebra and *c*) holds. Let us consider

$$\mathcal{B} = \mathrm{End}(E) \otimes \mathbb{Q},$$

it must be isomorphic to a number field. Let $\ell \in \mathbb{Z}$ be a prime different from p, we can also suppose that it remains prime in $\mathrm{End}(E')$ for every elliptic curve E' that it is isogenous to E: there are only finitely many such $\mathrm{End}(E')$ and each is a subring of $\mathcal{B}$ to find such a ℓ it is sufficient to search between inert primes. By Theorem 1.2.9

$$E[\ell^i] \simeq {}^{\mathbb{Z}}\!/_{\ell^i\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{\ell^i\mathbb{Z}}$$

so we can find a sequence of subgroup

$$\Phi_1 \subseteq \Phi_2 \subseteq \cdots \subseteq E \quad \Phi_i \simeq {}^{\mathbb{Z}}\!/_{\ell^i\mathbb{Z}}$$

Let E_i be E/Φ_i, by Theorem 1.2.11 we have the separable isogeny

$$\phi_i \colon E \longrightarrow E'$$

Note that also E' has a finite number of isogenous curves up to isomorphism. Hence we can find $m, n > 0$ such that the natural projection

$$f \colon E_m \longrightarrow E_{m+n} \simeq E_m$$

is an endomorphism and $\ker f = \Phi_{m+n}/\Phi_m \simeq \mathbb{Z}/\ell^n$ is cyclic. Note that $\ker f \subseteq E[\ell^n]$, by Proposition 1.2.10.3 there exist g such that

$$\begin{tikzcd}
E_m \arrow[r, "{[\ell^n]}"] \arrow[d, "f"'] & E_m \\
E_m \arrow[ur, dashed, bend right, "g"'] &
\end{tikzcd}$$

$[\ell^n] = f \circ g$ However we chose ℓ to be prime in $\mathrm{End}(E_m)$, this means by dual isogeny theorem that can not exist isogeny of degree ℓ from E_m and that n must be even. Moreover by the factorization above $[\ell^{n/2}] = f \circ \tilde{g}$ where $\tilde{g}$ is an automorphism. Then $\ker[\ell^{n/2}] = \ker f$ and this is absurd since the latter is cyclic and the fist not.

We have proved $c)$ implies $d)$, it remains to show $d)$ implies $b)$. We will prove the contrapositive. Let suppose $\hat{\pi}_r$ separable for all $r \geq 1$. The map

$$\mathrm{End}(E) \longrightarrow \mathrm{End}\, T_p(E)$$

is injective. Indeed if ϕ go to zero then from the definition of $T_p(E)$ we have $\phi(E[p^r]) = 0$ for all $r \geq 1$; since $[p^r] = \hat{\pi}_r \pi$ and π_r is surjective then

$$\pi_r(\ker \psi) \supseteq \ker \hat{\pi}_r,$$

and thus $\# \ker \psi \geq \# \ker \hat{\pi}_r$, on the other hand, we know by separability that $\# \ker \hat{\pi}_r = \deg \hat{\pi}_r = p^r$. Therefore $\# \ker \psi \geq p^r$ for all $r \geq 1$, which implies that $\psi = 0$.

$$\mathrm{End}(E) \hookrightarrow \mathrm{End}\, T_p(E) \simeq \mathrm{End}(\mathbb{Z}_p) \simeq \mathbb{Z}_p$$

then $\mathrm{End}(E)$ is commutative, which means it may not be an order in a quaternion algebra. □

Note that given a curve E over a finite field and a its Frobenius Trace we have

$$[a] = \pi + \hat{\pi}$$

so $\hat{\pi} = \pi - [a]$. E is supersingular if and only if $\hat{\pi}$ is purely inseparable if and only if $a \equiv 0 \mod p$, where in the last equivalence we use Proposition 1.2.13. Using this fact we can exactly compute the number of supersingular elliptic curve of fixed characteristic, up to isomorphism. In particular, let S_{p^2} the set of the j-invariant corresponding to supersingular curve of $\overline{\mathbb{F}}_p$ and

$$\# S_{p^2} = \lfloor \frac{p}{12} \rfloor + \begin{cases} 0 & \text{if } p \equiv 1 \mod 12, \\ 1 & \text{if } p \equiv 5, 7 \mod 12, \\ 2 & \text{if } p \equiv 11 \mod 12 \end{cases} \tag{1.14}$$

see (Theorem V§4.1 of [Sil11]).

It is worth to specify what does it mean that a curve is defined over a finite field of characteristic p. We said that E is defined over $\mathbb{F}_q$ means that the coefficients of the equation defining it are in $\mathbb{F}_q$. But this does not imply that the curve can not be defined over a smaller or a greater field. Often, the context clarifies if it is intended that the curve it is not defined over any smaller field

or not. Note that, up to isomorphism, there is a unique well-defined minimal field of definition and it is $\mathbb{F}_p(j(E)) \simeq \mathbb{F}_{p^r}$. We say that the elliptic curve E is *essentially* defined on $\mathbb{F}_{p^r}$.
Let us consider an endomorphism of E. It can be defined not only over $\mathbb{F}_q$ or $\mathbb{F}_{p^r}$, but also in their extensions. Since $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ is a cyclic group generate by the qth power map, we have that the group of $\mathbb{F}_q$-rational maps is the centralizer of the qth Frobenius π_q, i.e.

$$\phi \in \mathrm{End}_{\mathbb{F}_q}(E) \iff \phi \circ \pi = \pi \circ \phi.$$

Hence we need to be careful to distinguish $\mathrm{End}(E)$ from $\mathrm{End}_{\mathbb{F}_q}(E)$; the first are endomorphisms over the algebraic closure and the second are endomorphisms defined over $\mathbb{F}_q$. The containment of the latter in the first may be strict.
Let us suppose to have a curve $E_1/\mathbb{F}_q$ and an isomorphism

$$\psi \colon E_1 \longrightarrow E_2$$

(minimally) defined over $\mathbb{F}_{q^s}$ to a curve $E_2/\mathbb{F}_{q^m}$, with $m \mid s$. It is interesting to understand what happens to endomorphism rings. It is well defined the ring homomorphism

$$\begin{array}{rccc} \chi\colon & \mathrm{End}(E_1) & \longrightarrow & \mathrm{End}(E_2) \\ & \phi & \longmapsto & \psi \circ \phi \circ \psi^{-1} \end{array}$$

and it is naturally an isomorphism. Let $\pi_1 \in \mathrm{End}(E_1)$ the qth Frobenius map on E_1, then $\chi(\pi) \in \mathrm{End}_{\mathbb{F}_{q^s}}(E_2)$. In particular, if ψ is defined over $\mathbb{F}_q$ and π_2 is the qth Frobenius map on E, we have that $\psi \circ \pi_1 = \pi_2 \circ \psi$ and

$$\chi(\pi_1) = \psi \circ \pi_1 \circ \psi^{-1} = (\pi_2 \circ \psi) \circ \psi^{-1} = \pi_2.$$

In general, let $\rho = \chi(\pi_1)$. Then

$$\begin{aligned} \rho^2 =& (\psi \circ \pi_1 \circ \psi^{-1}) \circ (\psi \circ \pi_1 \circ \psi^{-1}) \\ =& \psi \circ \pi_1^2 \circ \psi^{-1} = \chi(\pi_1^2) \end{aligned}$$

By induction, we also obtain $\rho^s = \chi(\pi_1^s)$. Then for all $P \in E_2(\mathbb{F}_{q^s})$

$$\rho^s(P) = P$$

Since s is minimal, also the converse it is true and ρ^s is the Frobenius. Moreover, if $Q = \psi^{-1}(P)$ and a is the Frobenius trace, then

$$\pi^2(Q) - a\pi(Q) + qQ = O_1$$

Hence multiplying by ψ we obtain

$$\rho^2(P) - a\rho(P) + qP = O_2.$$

all $P \in E_2(\mathbb{F}_{q^s})$.
We have shown, given E an elliptic curves defined over $\mathbb{F}_q$, $\mathrm{End}(E)$ gives many information about the curves that can be isomorphic to it. Moreover, if E is essentially defined on $\mathbb{F}_{p^r}$, $\mathrm{End}(E)$ must contain a non trivial endomorphism of degree p^r.
Similar arguments lead to the following statement:

Theorem 1.5.10. *Let us suppose to have an elliptic curve $E_1/\mathbb{F}_q$ and a separable isogeny of degree d*

$$\psi\colon E_1 \longrightarrow E_2$$

defined over $\mathbb{F}_{q^s}$ to a curve $E_2/\mathbb{F}_{q^m}$, with $m \mid s$. Let $\hat{\psi}$ the dual isogeny and $\pi_1 \in \mathrm{End}(E_1)$ the qth Frobenius map on E_1. Then

$$\rho = \psi \circ \pi_1 \circ \hat{\psi} \in \mathrm{End}_{\mathbb{F}_{q^s}}(E_2)$$

and all $P \in E_2(\mathbb{F}_{q^s})$ we have that

1. *$\rho^s(P) = [d^s]P$,*
2. *$\rho^2(P) - ad\rho(P) + qd^2P = O_2$.*

1.6 Elliptic Curves over $\mathbb{C}$

There exist a strong connection between elliptic curves and complex lattices. Let us recall that a *lattice* is a discrete subgroup of a real vector space $\mathbb{R}^n$ which contains a base. In particular, a *complex lattice* Λ is lattice in $\mathbb{C} \simeq \mathbb{R}^2$, so it is of the form

$$\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$$

with ω_1, ω_2 $\mathbb{R}$-linearly independent.
Given a complex lattice Λ is well define the quotient group

$$\mathbb{C}\big/\Lambda$$

and it is called *complex torus.* A convex set of class representatives of $\mathbb{C}/\Lambda$ is called a *fundamental parallelogram.*
Two complex lattices Λ_1 and Λ_2 are called to be *homothetic* if there is a complex number $\zeta \in \mathbb{C}^*$ such that $\Lambda_1 = \zeta\Lambda_2$. From a geometrical point of view applying a homothety to a lattice means to zoom and rotate it around the origin.
Let Λ_1 and Λ_2 be lattices in $\mathbb{C}$, and suppose that $\alpha \in \mathbb{C}$ is such that

$$\alpha\Lambda_1 \subseteq \Lambda_2$$

the scalar multiplication by α induces a map

$$\phi_\alpha\colon \mathbb{C}\big/\Lambda_1 \to \mathbb{C}\big/\Lambda_2.$$

We would like to understand the link between complex tori and elliptic curves.

Definition 1.6.1. Let $\Lambda \subseteq \mathbb{C}$ be a lattice. The *Weierstrass $\wp$-function* (relative to Λ) is defined by the series

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

The *Eisenstein series of weight* $2k$ (for Λ) is the series

$$G_{2k}(\Lambda) = \sum_{\omega\in\Lambda\setminus\{0\}} \omega^{-2k}.$$

The following notation

$$g_2(\Lambda) = 60G_4(\Lambda) \quad \text{and} \quad g_3(\Lambda) = 140G_6(\Lambda). \tag{1.15}$$

is useful to define, for example, the *modular j-invariant*

$$j(\Lambda) = \frac{1728 g_2(\Lambda)^3}{g_2(\Lambda)^3 - 27g_3(\Lambda)^2} \tag{1.16}$$

As for the j-invariant for curves this quantity characterize the lattices:

Theorem 1.6.2. *Two complex lattices are homothetic if and only if they have the same modular j-invariant.*

Proof. Theorem I§4.1 [Sil09]. □

Theorem 1.6.3. *Let Λ be a complex lattice and $\wp(z) = \wp(z;\Lambda)$*

1. *$\wp(z)$ is an elliptic function for Λ, i.e.*

   $$\wp(z) = \wp(z+\omega)$$

   for all $z \in \mathbb{C}$ and $\omega \in \Lambda$.

2. *$\wp(z)$s Laurent series around $z = 0$ is*

   $$\frac{1}{z^2} + \sum_{k>0} (2k+1) G_{2k+2}(\Lambda) z^{2k}.$$

3. *For all $z \in \Lambda$*

   $$\wp'(z) = 4\wp(z)^3 - g_2(\Lambda)\wp(z) - g_3(\Lambda). \tag{1.17}$$

4. *The curve*

   $$E_\Lambda \colon y = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$$

   is an elliptic curve over $\mathbb{C}$ and the map

   $$\begin{array}{cccc} \chi\colon & \mathbb{C}/\Lambda & \longrightarrow & E(\mathbb{C}) \\ & 0 & \longmapsto & [0,1,0] \\ & z & \longmapsto & [\wp(z), \wp'(z), 1] \end{array}$$

   is an isomorphism of Riemann surfaces and a group morphism.

Proof. Theorems VI§3.1,VI§3.5 and Proposition VI§3.6 [Sil11]. □

An easy computation shows that $j(E) = j(\Lambda)$. Hence, to an homotety class of complex tori we associated a isomorphism class of elliptic curves. Also the converse it is true.
We can extend the correspondence also to the morphism:

Theorem 1.6.4. *Let E_1, E_2 be elliptic curves over $\mathbb{C}$, with corresponding lattices Λ_1, Λ_2. There is a bijection between the group of isogenies from E_1 to E_2 and the group of maps ϕ_α for all α such that $\alpha\Lambda_1 \subseteq \Lambda_2$.*

Proof. Corollary VI§4.1.1 [Sil11]. □

In particular, we obtain:

Theorem 1.6.5. *The category of elliptic curves over $\mathbb{C}$ with the isogenies and the category of complex lattices up to homothety with*

$$\mathrm{Hom}(\Lambda_1, \Lambda_2) = \{\alpha \in \mathbb{C} \mid \alpha\Lambda_1 \subseteq \Lambda_2\}$$

are equivalent.

1.7 Reduction and Deuring Correspondence

Sometimes we need to pass from a curve defined in characteristic zero to one in finite characteristic, and vice versa. The first operation is know as *reduction*, the latter as *lifting*.

Let us consider a curve $\widetilde{E}/\overline{\mathbb{Q}}$ and p a prime of $\mathbb{Z}$.

$$\widetilde{E}\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6Z$$

$\widetilde{E}$ is actually defined over a number field L, so we can consider a prime $\mathfrak{p}$ over p in the ring of integer $\mathcal{O}_L$ and complete the field. Up to a transformation we can suppose E defined over $(\mathcal{O}_L)_{\mathfrak{p}}$ and that its discriminant has positive valuation respect the place induces by $\mathfrak{p}$, in particular without loss of generality we can suppose discriminant as small as possible.
$\mathcal{O}_L$ is a Dedekind domain, hence the residue field of $\mathfrak{p}$ is just

$$\mathcal{O}_L/\mathfrak{p} \simeq \mathbb{F}_q$$

where $q = p^f$ and f is the inertia degree of $\mathfrak{p}$. Dedekind domains have dimension one then we can, in some sense, forget the completion. Let us consider the natural reduction map

$$\begin{array}{ccc} \mathcal{O}_L & \longrightarrow & \mathbb{F}_q \\ t & \longmapsto & \tilde{t} \end{array}$$

The curve

$$E\colon y^2 + \tilde{a}_1xy + \tilde{a}_3y = x^3 + \tilde{a}_2x^2 + \tilde{a}_4x + \tilde{a}_6$$

is called *reduction of $\tilde{E}$ modulo $\mathfrak{p}$*. It is a curve defined over $\mathbb{F}_q$ but note that it could be singular: if E is an elliptic curve we say that $\tilde{E}$ has *good reduction* modulo $\mathfrak{p}$.

Deuring describes the structures which are preserved in passing between curves in characteristic zero and finite characteristic:

Theorem 1.7.1 (Deuring reduction)**.** *Let $\widetilde{E}/L$ be an elliptic curve defined over a number field with endomorphism ring* $\mathrm{End}(\widetilde{E}) = \mathcal{O}$*, where $\mathcal{O}$ is an order in an imaginary quadratic extension K of $\mathbb{Q}$. Let $\mathfrak{p}$ be a prime of $\overline{\mathbb{Q}}$, over a prime number p, at which $\widetilde{E}$ has good reduction E modulo p.*

- *The curve E is supersingular if and only if p has only one prime of K above it.*
- *If p splits in K, then let f be the conductor of $\mathcal{O}$, so that $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$. Write $f = p^r f_0$, where p^r is the largest power of p dividing f. Then the endomorphism ring of E is as follows.*
  - *(a)* $\mathrm{End}(E) = \mathbb{Z} + f_0\mathcal{O}_K$ *is the order in K with conductor f_0.*
  - *(b) If $(p, f) = 1$ then the reduction map*

$$\begin{array}{ccc} \mathrm{End}(\widetilde{E}) & \to & \mathrm{End}(E) \\ \varphi & \mapsto & \overline{\varphi} \end{array}$$

is an isomorphism.

Proof. Theorem 13§4.12 [Lan87]. □

Theorem 1.7.2 (Deuring lift)**.** *Let E be an elliptic curve over a finite field k of characteristic p and let φ be an endomorphism of E. Then there exists an elliptic curve $\widetilde{E}$ defined over an number field H, an endomorphism $\widetilde{\varphi}$ of $\widetilde{E}$, and a prime $\mathfrak{p}$ over p in H such that E is isomorphic to the reduction of $\widetilde{E}$ at $\mathfrak{p}$, and φ corresponds to the reduction of $\widetilde{\varphi}$ under this isomorphism.*

Proof. Theorem 13§5.14 [Lan87]. □

In general Deuring reduction theorem is formulated in terms of $\bar{\mathbb{F}}_p$, because it is not true that it possible to reduce each curve defined over $\overline{\mathbb{Q}}$ to $\mathbb{F}_p$. The finite field on which the reduction modulo p is defined depends on L and on the place we choose. Let us suppose $\tilde{E}$ is essentially defined over a number field L, p is a rational prime and $\mathfrak{p}$ is a prime over p in L. Let us consider the inertia degree of $\mathfrak{p}$ $f(\mathfrak{p}|p) \geq 1$. $\tilde{E}$ reduces to a curve which is essentially defined over $\mathbb{F}_{p^f}$. A special case is when p splits completely over L: indeed $f(\mathfrak{p}|p) = 1$ for each prime over p, thus E is essentially defined over $\mathbb{F}_p$.

Chapter 2

Post-quantum Cryptography

Basic concepts of cryptography and the links between it and elliptic curves are necessary to understanding to problem we are studying. In this chapter we recall how mathematics can be used to ensure secure communications and we provide some examples. Finally we present and discuss the impact of quantum computation in cryptography.

2.1 Elements of Cryptography

The security of communications has always been a problem in many contexts. Let us suppose two people want to exchange a message over a public channel. Cryptography is the study and analysis of protocols that prevent third parties from reading such private message. We will call the two people, as in literature, Alice and Bob while we will call the adversary Eve (the eavesdropper).
Let us suppose Bob wants to send a secret message to Alice. The idea is the following: he uses a *secret shared key* k to hide his *plaintext message* m and turn it into a *ciphertext* c; Alice, upon receiving c, uses the secret key k to recover m by c. Note that in order to use this scheme there are two issues:

a) Alice and Bob must know k and nobody else.

b) A third part must not have the possibility to recover c from m without knowing k.

Problem a) is known as the *key-exchange* problem and we are going to show how it can be solved. To pass over problem b) we may employ mathematical operations which are quite easy, in order to hide the message (i.e. to *cipher* it), and whose inverse is hard without additional information, to recollect the original message (i.e. to *decipher* it).

Let us formalize the concepts of *(symmetric) cryptosystem.* A (symmetric) cryptosystem is a tuple

$$(\mathcal{A}, \mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$$

where

$\mathcal{A}$: is the alphabet, i.e. the set of admissible symbol to compose a message,

$\mathcal{P}$: is the set of admissible (not blinded) message or *plaintexts*,

$\mathcal{C}$: the set of ciphered messages or *ciphertexts*,

$\mathcal{K}$: the set of *keys*,

$\mathcal{E}$: the set of *encryption functions*

$$E_k \colon \mathcal{P} \to \mathcal{C}$$

with $k \in \mathcal{K}$,

$\mathcal{D}$: the set of *decryption functions*

$$D_k \colon \mathcal{C} \to \mathcal{P}$$

with $k \in \mathcal{K}$.

It is also required that for all $k \in \mathcal{K}$ $D_k \circ E_k = id_{\mathcal{P}}$.

In the situation we described, using a common secret key Bob and Alice can both encrypt and decrypt messages, so Bob and Alice have equal knowledge and abilities. For this reason, this model is called *symmetric.*
Let us suppose now Alice and Bob want to exchange confidential information, however they have never met and they can communicate only through a channel that is being monitored by an adversary. A symmetric cipher is not useful. We need to use a strategy belonging to *public key* or *asymmetric cryptography.* Here we are interested in this type of cryptosystem, which purposed is to allow public secure communications. The mathematical formulation of an asymmetric cipher is similar to the symmetric case, however an element k of the key space is a pair of keys

$$k = (k_{pub}, k_{priv}) \in \mathcal{K}$$

called the *private key* and the *public key*, respectively. For each public key k_{pub} we have an encryption function

$$E_{k_{pub}} \colon \mathcal{P} \to \mathcal{C}$$

and for each private key k_{priv} there is a decryption function

$$D_{k_{priv}} \colon \mathcal{C} \to \mathcal{P}$$

And we require that for all $k \in \mathcal{K}$

$$D_{k_{priv}} \circ E_{k_{pub}} = id_{\mathcal{P}}.$$

The security of an asymmetric system is built on the assumption that it is difficult for Eve to compute the decryption function $D_{k_{priv}}$, even if she knows the public key k_{pub}. Indeed, under this assumption, Alice can send k_{pub} to Bob using an insecure communication channel, and Bob can send back the ciphertext $c = E_{k_{pub}}(m)$, without worrying that Eve will be able to decrypt the message.

To easly decrypt c it is necessary to know the private key, so probably Alice can. The private key is sometimes called Alice's *trapdoor information*, because it provides a trapdoor, i.e. a shortcut, for computing the inverse function of $E_{k_{pub}}$.

Note that *easy* and *hard* are not well defined in a mathematical sense without specification. In this context we have a computational point of view: we intend that an operation is *easy* if there exist an algorithm that perform it in reasonable time, which in general means the time to perform it is polynomial respect to the number of bit of the input; instead, we intend that an operation is *hard* it does not exist any algorithm that attempts to compute it in a reasonable amount of time almost certainly (in probabilistic sense). Let us suppose, for example, to have an algorithm which has input an integer n. We need $y = \log n$ to represent it. If such algorithm is linear in n, it is exponential in its number of bit since $n = 2^y$. This means that we have to consider to be linear algorithms whose complexity is $O(\log n)$. In this text we use for complexity the asymptotic notation. It is the useful to denote by $\widetilde{O}(f(n))$ the complexity up to logarithmic factor. Specifically, $\widetilde{O}(f(n))$ means that may exist an integer $k \geq 0$ such that the complexity is $O(f(n)\log(f(n))^k)$. We say that an algorithm is subexponential in terms of time or space if its complexity is asimptotically the same of the *subexponential function*

$$L_n(a, b) = \exp(b \log(n)^a \log(\log(n))^{1-a})$$

for $0 < a < 1$. Note that $L(0, b) = \log(n)^b$ is a polynomial function while $L(1, b) = n^b$ is exponential.

2.1.1 Diffie Hellman Key Exchange

The first public key encryption models was purposed by Diffie and Hellman in 1976 and the ideas they present are still actual. One of most important and used asymmetric system appear in their article and it is known as *Diffie Hellman key exchange*. Let us present it.

Alice and Bob want to share each other a secret key, for example to use it in a symmetric cipher, but the only communication channel available is insecure and Eve can eavesdrop each message. The first step is for Alice and Bob to agree on a large prime p and a nonzero integer g modulo p and then to make the couple (g, p) public. So Eve knows it, too. Alice random chooses a positive integer a, compute $A \equiv g^a \mod p$ and she sends A by the public channel to Bob; Bob, in turn, chooses a random positive integer b and computes $B \equiv g^b \mod p$, then he sends B by the public channel to Alice. By these information either of them can recover the private shared key

$$K = g^{ab} \mod p,$$

since $K \equiv A^b \equiv B^a \mod p$.

Figure 2.1 summarizes the full protocol:

$$\begin{tikzcd}
& g \arrow[dl, "\_^{b}"'] \arrow[dr, "\_^{a}"] & \\
B \arrow[rr, dashed, bend left] \arrow[dr, "\_^{a}"'] & & A \arrow[ll, dashed, bend left] \arrow[dl, "\_^{b}"] \\
& K &
\end{tikzcd}$$

Public parameters	A large prime p and a nonzero integer g modulo p	
	Alice	**Bob**
Pick random secret	$a \in \mathbb{N}^+$	$b \in \mathbb{N}^+$
Compute public key	$A \equiv g^a \mod p$	$B \equiv g^b \mod p$
Exchange data	A	B
Compute shared secret	$K \equiv B^a \mod p$	$K \equiv A^b \mod p$

Figure 2.1: Diffie Hellman key exchange.

The Diffie Hellman protocol security is based on the fact that the following problem is supposed to be hard:

Problem 1 (Diffie Hellman (DH))**.** *Let p be a prime number and g an integer. Computing the value of $g^{ab} \mod p$ from the known values of $g^a \mod p$ and $g^b \mod p$.*

Problem 1 has been proven to be equivalent to solve the Discrete Logarithm problem in finite fields:

Problem 2 (Discrete Logarithm Problem (DLP))**.** *Let g be a primitive root for $\mathbb{F}_p$ and let h be a nonzero element of $\mathbb{F}_p$. Find an integer c such than*

$$g^c \equiv h \mod p.$$

There exist many algorithms to compute discrete logarithms and the best actually known is the *index calculus*, see [HPS08] Section 3.8. This algorithm in subexponential time solves the discrete logarithm problem in $\mathbb{F}_p^*$. Hence we can suppose Diffie Hellman to be secure, up to take care of the size of p.

Note that the pattern described may be adapted to other group G. The principal example is provided by the elliptic curves. We saw an elliptic curve $E/\mathbb{F}_p$ has an abelian group structure and $E(\mathbb{F}_p)$ is a commutative finite group. Let $P \in E(\mathbb{F}_p)$ be a point and $Q \in \langle P \rangle$, then there exist $n \in \mathbb{Z}$ such that

$$[n]P = Q$$

the *Elliptic Curve Discrete Logarithm Problem* (ECDLP) is the problem of finding an integer n that satisfy this equality. Note that if P is a point of order m, we can consider $n \in \mathbb{Z}/m\mathbb{Z}$ instead $\mathbb{Z}$.

The public parameters in Elliptic Curves Diffie Hellman (ECDH) have to comprehend a large prime p, an elliptic curve E defined over p and a rational point $P \in E(\mathbb{F}_p)$. Figure 2.2 summarizes the procedure:

Public parameters	A large prime p, an elliptic curve E defined over p and a rational point $P \in E(\mathbb{F}_p)$.	
	Alice	**Bob**
Pick random secret	$n_A \in \mathbb{N}^+$	$n_B \in \mathbb{N}^+$
Compute public key	$A := n_A P$	$B := n_B P$
Exchange data	A	B
Compute shared secret	$K = n_A B$	$K = n_B A$

Figure 2.2: Elliptic Curves Diffie Hellman key exchange.

ECDLP is harder then DLP: currently, the best known algorithms to solve the general discrete logarithm problem over elliptic curve groups are fully exponential.

2.1.2 Public Key Encryption

Diffie Hellman protocol is a key exchange method and it does not solve the issue of finding a secure method to exchange confidential information. However, we can obtain from DH a public key encryption method, based on the discrete logarithm problem, which is known as *El Gamal* protocol. We are going to describe it supposing to work over a finite field, but as for the key exchange this method can be extended also to elliptic curves.

The initialization is as follows. Alice publishes information consisting of a public key and an algorithm which gives to Bob the way to encrypt his message (using Alice's public key). Alice does not disclose her private key, which is another number. The private key allows Alice, and only Alice, to decrypt messages that have been encrypted using her public key. In particular Alice fixes a large prime p, for which DLP is hard, and $g \mod p$, which will provide the public parameters. Then she chooses an integer $a \in \mathbb{Z}$ as her private key and she computes

$$A \equiv g^a \mod p$$

A is the public key.
Now suppose that Bob would want to encrypt a message m using Alice's public key A. Let us suppose $m \in \{2, \ldots, p\}$. Bob fixes a random integer k, that is called *ephemeral key* and it must be used to encrypting a single message. He computes

$$c_1 \equiv g^k \mod p$$

and

$$c_2 \equiv mA^k \mod p.$$

Bob's ciphertext is the pair of numbers (c_1, c_2).
Alice in order to decrypt (c_1, c_2) computes

$$x \equiv c_1^a \mod p$$

and

$$y \equiv x^{-1} \mod p.$$

To recover the plaintext text it is sufficient that she computes the class of yc_2:

$$\begin{aligned} c_2 y &\equiv c_2 (c_1^a)^{-1} \mod p \\ &\equiv mA^k c_1^{-a} \mod p \\ &\equiv mA^k g^{-ka} \mod p \\ &\equiv mg^{ka} g^{-ka} \mod p \\ &\equiv m \end{aligned}$$

A public key exchange can be completely described by four functions: *Setup, Key generation, Encryption* and *Decryption.* Let us give the El Gamal's.

Setup: Choose p and $g \in \mathbb{F}_p^*$.

Key generation: Fix $a \in \mathbb{Z}$ and compute $A \equiv g^a \mod p$.
The public key is A.

Encryption: Given a message $m \in \{2, \ldots, p\}$ and a public key A, choose $k \in \mathbb{Z}$ and compute $c_1 \equiv g^k \mod p$ and $c_2 \equiv mA^k \mod p$.
The cyphertext is (c_1, c_2).

Decryption: Given a cyphertext (c_1, c_2) and a private key A, compute the plaintext

$$m = c_2 (c_1^a)^{-1} \mod p.$$

For finite field it easy to encode the message in order to manipulate it directly by the group's operation. In the elliptic curves case it is quite hard because we should transform a message, which is usually a binary string in $\mathcal{P} = \{0,1\}^w$ into a point of a fixed elliptic curve. Another strategy strategy can be adopted, namely the points involved may be transformed in strings. Usually the latter approach is used. An example in which this happens is another large employed public key encryption system: *Elliptic Curve Integrated Encryption Scheme* (ECIES). Let us summarizes it:

Setup: Choose E an elliptic curves defined over a finite field $\mathbb{F}_q$ and P a point of prime order N. Let H_1 and H_2 be two hash functions. Let $\{E_k\}_{k \in \mathcal{K}}$ and $\{D_k\}_{k \in \mathcal{K}}$ the sets of encryption and decryption functions indexed on $\mathcal{K}$ (the keys' set).

Key generation: Fix $s \in \mathbb{Z}$ and compute $A = sP$.
The public key is A and the private key is s.

Encryption: Given a message $m \in \{0,1\}^w$ and a public key, choose $r \in \{0, \ldots, N-1\}$ and compute $R = rP$ and $Z = rA$. Then compute $H_1(R, Z)$ which return two concatenated strings $k_1 || k_2$ of fixed length. Put $c = E_{k_1}(m)$ and $t = H_2(c, k_2)$.
The cyphertext is (R, c, t).

Decryption: Given a cyphertext (R, c, t) and a private key a, compute $Z = sR$ and $H_1(R, Z) = k_1 || k_2$. Control $t = H_2(c, k_2)$, if it is false return an error message; else compute $m = D_{k_1}(c)$.

Respect to El Gamal this protocol is better because it avoid to translate the message into a point and it also check during the decryption that the message has actually sent from the declared sender, preventing active attacks. The details of this and other cryptosystems can be find in [Was08].

2.2 Post-quantum Cryptography

Quantum mechanics had a great impact to modern scientific theories and quantum laws have become important also in information. In particular, it allowed to model a machine based on *quantum logic* instead of *binary logic.* In particular a quantum machine processes the information and performs logic operations by exploiting the laws of quantum mechanics. The unit of quantum information is *qubit*, instead of bit, and a *quantum computer* can be seen as a multisystem of quibits. Here we are not interested to a deep understanding of quantum information, rather we want to achieve its impact over classical cryptography.

2.2.1 Quantum Computation

A *quantum computer* is a system of many qubits, whose evolution can be controlled, and a quantum computation is a unitary transformation that acts on the many-qubit state describing the quantum computer. A single binary digit, i,e a classical bit, is a physical system that can exist in two distinct states which are used to represent 0 and 1. Instead a quantum bit is a two-level quantum system, described by a two-dimensional complex Hilbert space. In that space are chosen a pair of normalized and mutually orthogonal quantum states,

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

which represent a *computational basis*, like 0 and 1 in boolean computation. Any state of the qubit may be written as

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

with $\alpha, \beta \in \mathbb{C}$ such that $|\alpha|^2 + |\beta|^2 = 1$. Thus, a generic state of a qubit may be written as

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + \exp(i\phi)\sin\frac{\theta}{2}|1\rangle$$

for $0 \leq \theta \leq \pi$ and $0 \leq \phi \leq 2\pi$. Therefore, the qubit resides in a vector space, parametrized by continuous variables and a continuum of states is allowed. We remark that, on the contrary, in classical computation bit can only be set equal to 0 or 1 and a system with two states can only be in one state or in the other. A classical computer may be described most conveniently as a finite register of n bits and the state of can be shaped by the binary notation

$$i = \sum_{k=0}^{n} i_k 2^{k-1}.$$

In the same way a quantum computer may be thought of as a quantum register of size n and the state can be represented by

$$\begin{aligned}|\psi\rangle &= \sum_{k=0}^{2^n-1} c_i|i\rangle \\ &= \sum_{i_{n-1}=0}^{1} \cdots \sum_{i_0=0}^{1} c_{i_{n-1},\dots,i_0}|i_{n-1}\rangle \otimes \cdots \otimes |i_0\rangle\end{aligned}$$

with the complex numbers c_i constrained by the normalization condition $\sum_{k=0}^{2^n-1}|c_i|^2 = 1$. A more compact notation is also the following

$$|\psi\rangle = \sum_{i_{n-1},\dots,i_0=0}^{1} c_{i_{n-1},\dots,i_0}|i_{n-1}\cdots i_0\rangle$$

When we perform a computation on a classical computer, different inputs require separate runs. In contrast, a quantum computer can perform a computation for exponentially many inputs on a single run. This potentiality of parallelism is strength of quantum computation.

A quantum computation is composed of three steps:

1. preparation of the input state,
2. implementation of the desired unitary transformation acting on this state,
3. measurement of the output state.

The output of the measurement process is (inherently) probabilistic and the probabilities of the different possible outputs are set by the basic postulates of quantum mechanics. This means that a quantum algorithm must repeat several times the algorithm to obtain the correct solution of our problem with probability as close to one as desired. A quantum algorithms is quite similar to classical probabilistic algorithms, however the use of quantum rules makes it potentially more powerful than classical (deterministic or probabilistic) computers, in a sense with is quite hard to describe here.

Example 2.2.1 (Deutsch's Problem). Let us suppose we want know if a given function $f\colon \{0,1\} \to \{0,1\}$ is constant or not. In is enough to compute $f(0) + f(1) \mod 2$ and we need to apply the evaluation function of twice. With a quantum computer there can be model an algorithm that guess correctly if f is constant with probability $2/3$ in a single evaluation.

There exist different types of quantum algorithm that can be characterized by the use of different tools. We will often employ the *black-box model*, which is model of computation where the input to the problem includes a *black-box* function that can be applied, or equivalently an *oracle* that can be consulted. We also suppose that this is the single way to extract information from the black-box. In the black-box model, the complexity is usually measured in terms of the number of applications of the black-box.

2.2.2 Quantum Algorithm's Impact on Cryptography

The possibility to actually realize a quantum computer has really getting in trouble classical cryptography. In fact, problems which are hard to solve with a classical computer become easy to perform by a quantum computer.

The most well known quantum algorithm is Shor's algorithm to integer factorization problem [Sho94]. Let us describe the idea of this algorithm. Let us suppose we want to factorize $N \in \mathbb{N}$. Let $a \neq N$ be a positive integer and $\gcd(N, a) = d$. If $d \neq 1$ then it is a non trivial factor of N; if $d = 1$ let us suppose to know the order r of a modulo N, since r is a non trivial factor of N we obtain a factorization. This means that the problem of integer factorization can be reduced to the problem of finding the order of an element, which can be solved efficiently on a quantum computer. The latter problem, in fact, is a particular application of the Shor's algorithm that solves the following more general problem:

Problem 3 (Period Finding Problem)**.** *Given a black-box implementing a periodic function $f\colon \mathbb{Z} \to X$ for some finite set X, where $f(x) = f(y)$ if and only if $r \mid x - y$, then find r.*

In particular, he uses the function $f(x) = a^x \mod N$. Note that the same quantum algorithm can efficiently find the order of an element in finite group G, once given a black-box for performing the group arithmetic. It has been proved that, using this method, a quantum computer find the order of $a \mod N$ in $O((\log N)^2 \log\log(N) \log\log\log(N))$, namely the integer factorization problem can be solved polynomially by a quantum computer. We recall that classically the best known heuristic probabilistic algorithm has asymptotic complexity of order $L_N(1/3, 1)$ i.e. it is subexponential. For a general finite group G, it has been estimated a quantum computer compute r at least in $O(\log r)$ black-box multiplications and $O(n + \log^2 r)$ other elementary operations, while classically the complexity is exponential.
Using a similar argument, it can be solved the discrete logarithm problem in $\mathbb{F}_p^*$. We want find an integer c such that

$$g^c \equiv h \mod p.$$

and we can suppose g not to be primitive up to know its order r.
Shor solves this problem by defining the black box function

$$\begin{array}{rccc} f\colon & \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z} & \longrightarrow & \mathbb{F}_p^* \\ & (x, y) & \longmapsto & g^x h^y \end{array}$$

Note that $f(x, y) = f(z, w)$ if and only if the couple $(x - z, y - w)$ is in the additive subgroup of $\mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z}$ generated by $(c, -1)$. Then techniques analogue to which are used to solve the period finding problem give us the chance to recover $(c, -1)$ with quantum complexity $O((\log p)^2 \log\log(p) \log\log\log(p))$, namely polynomially. Also this algorithm can be defined in general for any group G for which arithmetic we have a black box. For example, one can apply this algorithm to compute discrete logarithms in the additive group of an elliptic curve over a finite field. If the elements of the group are represented with strings of length n, the quantum black-box complexity is $O(\log r)$ black-box multiplications and $O(n + log^2 r)$ other elementary operations.

The results just presented implies that large part of the classical cryptosystems become unsafe under quantum attacks. However, there exist classes of protocols that seem to be quantum-resistant. Specifically, they are the systems based on problems that are still hard to quantum computers:

- Hash-based cryptography,
- Code-based cryptography,
- Lattice-based cryptography,
- Multivariate-quadratic-equations cryptography,
- Isogeny-based cryptography.

In this thesis we are dealing with the last one.

2.2.3 Other Algorithms

Shor's methods to solve factorization and discrete logarithm problem permit us to reword both as special cases of the following:

Problem 4 (Abelian Hidden Subgroup Problem)**.** *Let $f\colon G \to X$ be a function from a finite abelian group G to a finite set X such that there exist $K < G$ a subgroup such that $\forall x, y \in G$*

$$f(x) = f(y) \ \textit{ if and only if } \ x - y \in K$$

In other words f is constant on cosets of K and distinct on different cosets. Given f, G, X find K.

Note that also Deutsch's Problem (Example 2.2.1) can be rephrased in terms of this previous one: let $G = \mathbb{Z}/2$, $X = \{0, 1\}$, we obtan $K = \{0\}$ if f is balanced and $K = \{0, 1\}$ if f is constant.
The Abelian Hidden Subgroup problem can also be used to decompose a finite abelian group into a direct sum of cyclic groups if there is a unique representative for each group element. In his PhD thesis Mosca [Mos99] shows the following result:

Theorem 2.2.2. *Let us suppose G be a finite abelian group and $B = \{a_1, \dots, a_k\}$ be a set of generators of prime power order. There exist a polynomial quantum algorithm such that almost certainly return the structure of G.*

The main idea of the algorithm in the theorem is to use the fact that G can be expressed as direct sum of its p-Sylow $G_{p_1}, \dots, G_{p_l}$. If $S_j = B \cap G_{p_j}$ then S_j generates the p_j-Sylow G_{p_j} and so we can first find the decomposition for each of the Sylow p-subgroups of G and then take their product to obtain a decomposition of G. So, without loss of generality let us suppose G a p-group and that the maximal order of the generating element is $q = p^r$. Let us define

$$\begin{array}{rccc} g\colon & \mathbb{Z}/q\mathbb{Z}^k & \longrightarrow & G \\ & (x_1, \dots, x_k) & \longmapsto & a_1^{x_1} \cdots a_k^{x_k} \end{array}$$

If K is the subset hidden by g and $y_1, \dots, y_s \in \mathbb{Z}/q^k/K$ a set of generators of the quotient, then

$$G = \langle g(y_1) \rangle \times \cdots \times \langle g(y_s) \rangle$$

On a quantum computer obtaining this decomposition require performing at most $O(k^3 \log q)$ operation, since abelian hidden subgroup problem can be solved in quantum polynomial time:

Theorem 2.2.3. *There exists a bounded-error quantum algorithm for finding generators for the hidden subgroup $K \leq G$ of f, where $G = \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_s$. This algorithm using $O(s)$ evaluations of f and $O(\log^3 \# G)$ other elementary operations.*

The class group of a number field is an abelian finite group and its decomposition is believed to be hard to find on a classical computer. Hence such a decomposition would easily give the size of the class group, which is also known to be as hard as factoring, assuming the Generalized Riemann Hypothesis.

A problem involving black box functions is also the following:

Problem 5 (Abelian Hidden Shift Problem)**.** *Let A be a known finite abelian group and X a known finite set and let $f_1, f_2 \colon A \to X$ two black-box functions. We say that f_1, f_2* hide a shift *$s \in A$ if f_1 is injective and $f_2(a) = f_1(sa)$ for all $a \in A$. Determine s using queries to such black-box functions.*

Kuperberg proved that:

Theorem 2.2.4 (Kuperberg's algorithm)**.** *The abelian hidden shift problem can be solved in quantum time and query complexity $2^{O(\sqrt{n})}$, where n is the length of the output, uniformly for all finitely generated abelian groups.*

One of the possible consequences of this fact is that, if a given problem can be reworded as an abelian hidden shift problem and n is polynomial, Kuperberg's algorithm solves that problem using a polynomial number of evaluations of the black-box functions.

Another important quantum algorithm by Grover [Gro96] is related to problem of searching an element in an unsorted finite database D. Let us suppose to be able to represent all the element in D through sting of length n, hence we can suppose $D = \{0,1\}^n$. We also suppose to have an oracle able to evaluated an unknown function

$$f \colon D \longrightarrow \{0,1\}$$

A quantum computer can find an element $x \in D$ such that $f(x) = 1$ and $f(y) = 0$ for all $y \neq x$ in D in complexity $O(\sqrt{2^n})$ with success probability greater than $1/2$. Note instead that a classical computer need $O(2^n)$ call of the oracle.

Chapter 3

Endomorphism Rings and Isogeny Graphs

The security of the cryptosystem, we are interested in studying, is closely related to the problem of finding an isogeny between two fixed elliptic curves. In this chapter, first of all we prove that endomorphism rings play a central role, so we try to better understand their structure. Secondly, we show that finding an isogeny can be reduced to the problem of connecting two vertices of a graph. In particular, we will see that it is possible to translate information about isogeny classes of curves, defined over a fixed finite field, in terms of graphs. Finally, we display that these graphs own very useful properties.

3.1 Existence of an Isogeny

First of all we focus on the decisional question whether an isogeny between two fixed elliptic curves exists (or not). Given two elliptic curves over a finite field, we want to prove that saying they are isogenous, i.e.there exists an isogeny between them, is equivalent to say that they have the same number of rational points:

Theorem 3.1.1. *Let $E_1/\mathbb{F}_q$ and $E_2/\mathbb{F}_q$ be elliptic curves defined over a finite field. They are isogenous over $\mathbb{F}_q$ if and only if $\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q)$.*

The proof this condition is necessary is easy. In fact, let us suppose there exists $\phi\colon E_1 \to E_2$ an isogeny. We denote by π_i the q-Frobenius map of E_i. The equality $\pi_2 \circ \phi = \phi \circ \pi_1$ holds because the maps are defined over $\mathbb{F}_q$; then we have

$$(1 - \pi_2) \circ \phi = \phi \circ (1 - \pi_1)$$

so

$$\deg(1 - \pi_2) \deg \phi = \deg \phi \deg(1 - \pi_1)$$

$1 - \pi_i$ is separable by Proposition 1.2.13. Therefore,

$$\#E_2(\mathbb{F}_q) = \deg(1 - \pi_2) = \deg(1 - \pi_1) = \#E_1(\mathbb{F}_q).$$

Note that $\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q)$ if and only if the traces of π_1 is the same of π_2, so if two curves are isogenous than they must have the same Frobenius trace.

Directly from this, by Theorem 1.5.4, we obtain that they have the same zeta function.
The vice versa is based on the classical result by Tate:

Theorem 3.1.2 (Tate Isogeny Theorem[1])**.** *Let $\ell \neq \operatorname{char}(\mathbb{F}_q)$ be a prime and $G = Gal(\bar{\mathbb{F}}_q/\mathbb{F}_q)$. The natural map*

$$\Psi\colon \operatorname{Hom}_{\mathbb{F}_q}(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \to \operatorname{Hom}_G(T_\ell(E_1), T_\ell(E_2))$$

is an isomorphism.

This theorem is a specialization of the general fact proved by Tate for abelian varieties and it is particularly useful because the endomorphism ring of the Tate modules are isomorphic to 2×2 matrix rings with coefficients in the ℓ-adic numbers. Let us give a sketch of the proof of the right arrow of Theorem 3.1.1, to details see [Wat69] chapter 2.

Proof sketch. Let us fix ℓ as in the theorem. We note that $\mathbb{Q}_\ell$ is a $\mathbb{Z}_\ell$-flat module and the cokernels of the Tate's maps are torsion free, hence

$$\operatorname{End}_{\mathbb{F}_q}(E_1) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell \simeq \operatorname{End}_G(T_\ell(E_1)) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell \overset{f_1}{\hookrightarrow} \mathrm{M}_2(\mathbb{Q}_\ell)$$

$$\operatorname{End}_{\mathbb{F}_q}(E_2) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell \simeq \operatorname{End}_G(T_\ell(E_2)) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell \overset{f_2}{\hookrightarrow} \mathrm{M}_2(\mathbb{Q}_\ell)$$

Let us set $V_\ell(E_i) = T_\ell(E_1) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. By Theorem 3.1.2, it is enough to find a G-linear map $V_\ell(E_1) \to V_\ell(E_2)$. We also note that the Frobenius trace of π_1 coincides with the Frobenius trace of π_2 by the hypothesis. In particular, the two maps have the same characteristic polynomial. We can chose ℓ such that both are semisimple, then it exists $\lambda \in \mathrm{GL}_2(\mathbb{Q}_\ell)$ such that $\lambda^{-1} f_2(\pi_2 \otimes 1)\lambda = f_1(\pi_1 \otimes 1)$. Note that this just means that $\lambda \in \operatorname{Hom}_G(V_\ell(E_1), V_\ell(E_2))$, hence $\operatorname{Hom}_{\mathbb{F}_q}(E_1, E_2) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \neq \{0\}$. Up to multiplication, we have found an isogeny over $\mathbb{F}_q$ from E_1 to E_2.

□

Remark 3.1.3. By Schoof's algorithm [Sch95], $\#E(\mathbb{F}_q)$ is computable in polynomial time. Hence, we can decide if an isogeny exists in polynomial time.

Note that Theorem 3.1.1 says us that if $E_1/\mathbb{F}_q$ and $E_2/\mathbb{F}_q$ are elliptic curves defined over a finite field, then for each $n > 0$ there exists an isogeny between them defined over $\mathbb{F}_{q^n}$ if and only if $\#E_1(\mathbb{F}_{q^n}) = \#E_2(\mathbb{F}_{q^n})$. Asking that the two curves are defined over $\mathbb{F}_q$ is stronger than asking they are defined over $\bar{\mathbb{F}}_q$, in particular this brings strict requirement over the rational points set of every extension.

Corollary 3.1.4. *Let $E_1/\mathbb{F}_q$ and $E_2/\mathbb{F}_q$ be elliptic curves defined over a finite field. If they are isogenous then* $\operatorname{End}(E_1) \otimes_{\mathbb{Z}} \mathbb{Q} \simeq \operatorname{End}(E_2) \otimes_{\mathbb{Z}} \mathbb{Q}$.

Proof. Let us suppose there exist $\phi\colon E_1 \to E_2$ an isogeny of degree n. The map

$$\begin{array}{cccc} F_\phi\colon & \operatorname{End}(E_1) & \to & \operatorname{End}(E_2) \\ & \alpha & \mapsto & \phi\alpha\hat{\phi} \end{array}$$

[1] [Sil11] Theorem III.7.7

where $\hat{\phi}$ is the dual isogeny, is well defined and a homomorphism of $\mathbb{Z}$-module. Now, suppose $F_\phi(\alpha) = 0$, i.e. $\phi\alpha\hat{\phi} = 0$, and $\alpha \neq 0$. ϕ is surjective, then $\phi\alpha = 0$, similarly we have $\phi = 0$. However, $\phi \neq 0$ by hypothesis, hence F_ϕ is injective. Tensoring with $\mathbb{Q}$ over $\mathbb{Z}$, we obtain $\mathbb{Q}$-linear map between $\mathbb{Q}$-algebras of dimension 2 or 4:

$$\begin{array}{rccc} \tilde{F_\phi} \coloneqq F_\phi \otimes \frac{1}{n}\colon & \mathrm{End}(E_1) \otimes \mathbb{Q} & \to & \mathrm{End}(E_2) \otimes \mathbb{Q} \\ & \alpha \otimes 1 & \mapsto & \phi\alpha\hat{\phi} \otimes \frac{1}{n} \end{array} \tag{3.1}$$

$\mathbb{Q}$ if flat over $\mathbb{Z}$, then $\tilde{F_\phi}$ is injective. Then

$$\dim_{\mathbb{Q}} \mathrm{End}(E_1) \otimes \mathbb{Q} \leq \dim_{\mathbb{Q}} \mathrm{End}(E_2) \otimes \mathbb{Q}.$$

We can similarly define $F_{\hat{\phi}}\colon \mathrm{End}(E_2) \to \mathrm{End}(E_1)$ and using the same arguments we obtain $\dim_{\mathbb{Q}} \mathrm{End}(E_2) \otimes \mathbb{Q} \leq \dim_{\mathbb{Q}} \mathrm{End}(E_1) \otimes \mathbb{Q}$. Then the two spaces have the same dimension and $\tilde{F_\phi}$ is also a bijection.

□

Note that the main consequence of the previous corollary is that a supersingular and an ordinary curve can not be isogenous. Thus, we are allowed to deal with ordinary and supersingular elliptic curve separately.

3.2 Isogeny Graphs

By the existence of dual isogeny, Theorem 1.2.14, being isogenous is an equivalence relation. Starting from this observation we want to outline a model which represent the relation of being isogenous. We can represent this relation via a graph. First of all, we recall the following:

Definition 3.2.1. A *graph* G is a pair (V, E) where V is a finite set of *vertices* and $E \subseteq V \times V$ is a set of pairs called *edges.* A graph $G = (V, E)$ is called *undirected* if for all $(v, w) \in E$ then $(w, v) \in E$, or equivalently if the pairs in E are unordered. We say that a graph in a *multigraph* if there can exist different edges with the same end node.

Let F a field and $\{E_i\}$ be a complete set of representatives of the rational isomorphism classes of curves defined over F. We can use this set to define a graph: each E_i defines a vertex of the graph and each isogeny connecting E_i and E_j, up to isomorphism over the codomain, gives an edge. We note that the dual map of an isogeny $E_i \to E_j$ gives an edge (E_j, E_i), however we must to take care that if E_j has more automorphisms than E_i there may be multiple edge from E_j to E_i and one edge which represent the dual map for all of them. The graph obtained in this way is direct and we call it *isogeny graph.*
Having unbalanced edges is a rare situation ($j \in \{0, 1728\}$) and we usually treat isogeny graph as an undirected graph. We just observe that being F-isogenous is an equivalence relation, so we think the isogeny graph as the graph induced by this relation, i.e. an undirected multigraph, whose nodes are class of F-isomorphism of F-isogenous curves. Given a couple of nodes, there exists an edge between them if and only if they are isogenous. If F is algebraically closed we can represent each curve by its j-invariant, otherwise is necessary to distinguish curve which has the same j-invariant but are not F-isomorphic. With abuse

of notation sometimes we call isogeny graph the graph whose nodes are all the curve defined over F and sometimes one of the *connected components*, which are just the isogeny classes. This will not cause confusion because, almost always, we will fix a base curve and the elliptic curves which can be reached through a path in the graph must stay in the same connected component. Usually, we are interested only in studying isogenies with fixed degree. In these cases it is better to consider subgraphs. In particular, let ℓ be a prime different from the characteristic of F, we say that two curves are *ℓ-isogenous* if there exist an isogeny of degree ℓ between them. Like above, we can build the *ℓ-isogeny graph*, which is the subgraph of the isogeny graph whose edge has fixed degree ℓ. Note that an isogeny and its dual have the same degree, so being ℓ-isogenous is an equivalence relation, too. Also in this case we will be clear from the context if we refer to all the curves or to a part (a connected component).

Due to Proposition 1.2.6, we can consider only separable isogenies: in what follows we always use *isogeny* for *separable isogeny*. Besides, by Theorem 1.2.11 we will identify an isogeny with its kernel without loss of generality. As direct consequence we have that the following fact holds:

Theorem 3.2.2. *Let E an elliptic curve defined over a finite field F of characteristic p, and let $\ell \neq p$ be a prime. There are $\ell + 1$ distinct isogenies of degree ℓ with domain E defined over the algebraic closure $\bar{F}$.*

Proof. Let $\phi\colon E \to E'$ an isogeny of degree ℓ. The kernel Φ of ϕ has cardinality ℓ, so Φ is cyclic and contained in $E[\ell]$. Due to the fact $\ell \neq p$ we know that $E[\ell] \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$, therefore there are exactly $\ell + 1$ such as subgroup. □

We proved in Corollary 3.1.4 that if two elliptic curves E_1, E_2 over $\mathbb{F}_q$ are isogenous then their endomorphism rings are orders in the same $\mathbb{Q}$-algebra. Hence, it is impossible for an isogeny class to contain both ordinary and supersingular curves. In particular, in the same connected components there are only ordinary or supersingular curves and this cause a differentiation of the resulting graph. For this reason we are going to study separately the ordinary and supersingular case.

3.3 Ordinary Curves

Let E be an ordinary elliptic curve defined over a finite field $F = \mathbb{F}_q$. Its Frobenius endomorphism π satisfies a quadratic equation

$$\pi^2 - t\pi + q = 0. \tag{3.2}$$

Hasse theorem say that $|t| \leq 2\sqrt{q}$, then if we set

$$D_\pi \coloneqq t^2 - 4q$$

the discriminant of the equation (3.2), we have $D_\pi < 0$. The field $K = \mathbb{Q}(\sqrt{D_\pi})$ is an imaginary quadratic field and the ring of integers $\mathcal{O}_K$ is its maximal order. Then, up to isomorphism,

$$\mathbb{Z}[\pi] \hookrightarrow \mathcal{O}_K$$

E is ordinary, so, we can state that

$$\mathbb{Z}[\pi] \subseteq \mathrm{End}(E) \subseteq \mathcal{O}_K$$

This observation brings us to focus on the study of orders in this special case. By the way, the structure of orders inside a quadratic imaginary field is quite simply:

Proposition 3.3.1. *Let K be a quadratic number field and let $\mathcal{O}_K$ be its ring of integers.*

1. *Any order $\mathcal{O} \subset K$ can be written as $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$ for an integer f, called the* conductor *of $\mathcal{O}$.*
2. *If d_K is the discriminant of K, the discriminant of $\mathcal{O}$ is $f^2 d_K$.*
3. *If $\mathcal{O}, \mathcal{O}'$ are the two orders with conductor f, f' , then*
$$\mathcal{O} \subseteq \mathcal{O}' \iff f'|f.$$

If we denote by f_π the conductor of $\mathbb{Z}[\pi]$, there exist an integer a such that

$$\mathcal{O}_K = \mathbb{Z}\left[\frac{\pi - a}{f_\pi}\right].$$

Proposition 3.3.1 let us guess that the isogeny graph has a rigid structure. In order to understand this structure we need to investigate the relationship between containment of orders and isogenies.
Let $\phi\colon E \to E'$ be an isogeny of degree n. Then, as in (3.1), ϕ determines a homomorphism

$$\begin{array}{rlcl} \iota\colon & \mathcal{O}' = \mathrm{End}(E') & \to & K & = \mathrm{End}(E) \otimes \mathbb{Q} \\ & \psi & \mapsto & \phi^{-1}\psi\phi & = \widehat{\phi}\psi\phi \otimes n^{-1} \end{array}$$

This homomorphism does not depend on ϕ: let $\eta\colon E \to E'$ an isogeny of degree k, then

$$\begin{aligned} \widehat{\eta}\psi\eta \otimes k^{-1} =& \widehat{\eta}(\phi\widehat{\phi})\psi(\phi\widehat{\phi})\eta \otimes k^{-1}n^{-2} \\ =& (\widehat{\eta}\phi)\widehat{\phi}\psi\phi(\widehat{\phi}\eta) \otimes k^{-1}n^{-2} \\ =& \widehat{\phi}\psi\phi(\widehat{\eta}\phi)(\widehat{\phi}\eta) \otimes k^{-1}n^{-2} \\ =& \widehat{\phi}\psi\phi \otimes n^{-1} \end{aligned}$$

where the next to last step relies on the commutativity of $\mathcal{O}'$.
For supersingular elliptic curves, the induced embedding of $\mathrm{End}(E')$ in a $\mathbb{Q}$-algebra depends on the isogeny ϕ. For ordinary elliptic curves, it is not restrictive consider the endomorphism rings of all elliptic curves in an isogeny class as embedded in the same number field K.

If we consider isogeny of fixed prime degree, we can prove that the two orders involved must be equal or the containment index is settled:

Proposition 3.3.2. *Let E be an ordinary elliptic curve over the finite field k. Let $\phi\colon E \to E'$ be an isogeny of prime degree ℓ different from the characteristic of k. Then $\mathcal{O} = \mathrm{End}(E)$ contains $\mathcal{O}' = \mathrm{End}(E')$ or $\mathcal{O}'$ contains $\mathcal{O}$ and the index of one in the other divides ℓ.*

Proof. We observe that

$$\mathbb{Z} + \ell^2\mathcal{O} \subseteq \mathbb{Z} + \hat{\phi}\mathcal{O}'\phi \subseteq \mathcal{O}$$

where the index of the first element of this chain is ℓ^2. We note that if equality holds this translates into the equality of $\mathcal{O}$ and $\mathcal{O}'$ in K. If $\mathbb{Z}+\ell^2\mathcal{O} = \mathbb{Z}+\hat{\phi}\mathcal{O}'\phi$ then $\mathcal{O}'$ has index ℓ in $\mathcal{O}$ and if $\mathbb{Z} + \hat{\phi}\mathcal{O}'\phi = \mathcal{O}$ then $\mathcal{O}$ is contained in $\mathcal{O}'$ with index ℓ. □

We have already proved, in the same notations of the Proposition 3.3.2, that

$$[\mathcal{O}\colon \mathcal{O}'] \in \left\{\ell, \frac{1}{\ell}, 1\right\}.$$

In particular, we say that

- ϕ is an *horizontal* ℓ-isogeny if $[\mathcal{O}\colon \mathcal{O}'] = 1$,
- ϕ is a *descending* ℓ-isogeny if $[\mathcal{O}'\colon \mathcal{O}] = \ell$,
- ϕ is an *ascending* ℓ-isogeny if $[\mathcal{O}\colon \mathcal{O}'] = \ell$.

Obviously, we have that:

Lemma 3.3.3. *Let $\phi\colon E \to E'$ be an ℓ-isogeny. ϕ is ascending if and only if $\hat{\phi}$ is descending and ϕ is an horizontal if and only if $\hat{\phi}$ is horizontal, too.*

Definition 3.3.4. Let p an odd prime number and $a \in \mathbb{Z}$, the *Legendre symbol* is a function such that

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue} \mod p \\ 0 & \text{if } a = 0 \\ -1 & \text{if } a \text{ is a quadratic residue} \mod p \end{cases}$$

Furthermore

$$\left(\frac{a}{2}\right) = a \mod 2.$$

A classical and crucial result by Kohel is the following:

Proposition 3.3.5. *(Proposition 23 [Koh96]) Let $E/\mathbb{F}_q$ be an ordinary elliptic curve with endomorphism ring $\mathcal{O} \subseteq K$ of discriminant D and conductor f. Let π the Frobenius and f_π the conductor of $\mathbb{Z}[\pi]$. Let ℓ be a prime different from the characteristic of the field.*

1. *If $\ell \nmid [\mathcal{O}_K\colon \mathcal{O}] = f$ and also*
   - *(a) $\ell \nmid [\mathcal{O}\colon \mathbb{Z}[\pi]] = (f_\pi \mid f)$ there are $1 + \left(\frac{D}{\ell}\right)$ horizontal rational ℓ-isogenies defined over $\mathbb{F}_q$,*
   - *(b) $\ell \mid [\mathcal{O}\colon \mathbb{Z}[\pi]]$ there are $1 + \left(\frac{D}{\ell}\right)$ horizontal rational ℓ-isogenies defined over $\mathbb{F}_q$ and $\ell - \left(\frac{D}{\ell}\right)$ descending.*
2. *If $\ell \mid [\mathcal{O}_K\colon \mathcal{O}]$ and also*
   - *(a) $\ell \nmid [\mathcal{O}\colon \mathbb{Z}[\pi]]$ there are 1 rational ascending ℓ-isogeny defined over $\mathbb{F}_q$,*

(b) $\ell \mid [\mathcal{O}\colon \mathbb{Z}[\pi]]$ *there are* 1 *ascending rational* ℓ*-isogeny defined over* $\mathbb{F}_q$ *and* ℓ *descending.*

Let us remark that in Kohel characterization are involved rational isogenies. Hence we need to take care of the fact that curves which are isomorphic could not be F-isomorphic. However, this not cause greater problem because if an ordinary elliptic curve over F has j invariant different from 0 and 1728 and its frobenius trace is t, then its quadratic twist has frobenius trace $-t$. Thus, they can not be in the same connected component. Moreover, when there are several different isogenies to elliptic curves of the same level then some of the image elliptic curves may actually be isomorphic.

Example 3.3.6. Let

$$E_1/\mathbb{F}_{71} : y^2 = x^3 + 3x + 4$$

be an ordinary elliptic curve over the finite field $\mathbb{F}_{71}$. The frobenius trace of E_1 is -12, so its characteristic polynomial is

$$p_1(x) = x^2 + 12x + 71$$

and $\operatorname{End}(E_1)$ must be an order in $K_1 = \mathbb{Q}(\sqrt{-140}) = \mathbb{Q}(\sqrt{-35})$. Since

$$[\mathcal{O}_{K_1}\colon \mathbb{Z}[\pi_1]] = 2,$$

Proposition 3.3.5 implies that for $\ell \neq 2$ only horizontal isogenies from E_1 are admitted. Computing

$$\left(\frac{D}{3}\right) = 1$$

we obtain that we have exactly 2 3-isogenies.

Proposition 3.3.5 implies the ℓ-isogeny graphs must have a precise form. Now, let's try to understand it better. For example, if ℓ does not divide the conductor f_π does not exist ascending or descending isogeny:

Lemma 3.3.7. *Let* E *be an ordinary elliptic curve such that* $\mathbb{Z}[\pi]$ *is maximal at* ℓ*, i.e.* $\ell \nmid [\mathcal{O}_K\colon \mathbb{Z}[\pi]]$ *. If there exists an* ℓ*-isogeny of* E*, then it is an horizontal isogeny.*

Proof. The conductor of an order in K must divide f_π, so it follows that can occur only the case 1.a of Proposition 3.3.5. □

In what follows, we denote with $v_\ell(a)$ the ℓ-adic valuation of $a \in \mathbb{Z}$. Let us consider now the case in which $\mathbb{Z}[\pi]$ is not maximal at ℓ.

Lemma 3.3.8. *Let* $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$ *such that* $\ell \mid [\mathcal{O}_K\colon \mathbb{Z}[\pi]]$ *and* $\ell \nmid [\mathcal{O}\colon \mathbb{Z}[\pi]]$*, i.e. if* $\ell^n \parallel (f_\pi/f)$ *with* $n \geq 1$ *then* $\ell^n \parallel f$*. Then the only isogeny* $\phi\colon E \to E'$ *is such that* $\ell \mid [\mathcal{O}'\colon \mathbb{Z}[\pi]] = f'$*.*

Proof. From Proposition 3.3.5 we have that there is only an ascending isogeny $\phi\colon E \to E'$. The degree of the isogeny is $\ell = [\mathcal{O}'\colon \mathcal{O}]$, then $f/f' = \ell$. The hypothesis implies that $v_\ell(f_\pi/f) = v_\ell(f_\pi/f) = n$, then $\ell \mid ((f_\pi/f)/f') = f_\pi(f'/f) = f_\pi/\ell$. This means that $\ell \mid [\mathcal{O}'\colon \mathbb{Z}[\pi]]$ and so $v_\ell(f') = n - 1$. □

Lemma 3.3.9. *Let* $\phi\colon E_1 \to E_2$ *is a descending* ℓ*-isogeny and* $\ell \mid [\mathcal{O}_2\colon \mathbb{Z}[\pi]]$*. Then for every* $\beta\colon E_2 \to E_3$*, such that* $\mathcal{O}_1 \neq \mathcal{O}_3$*,* β *is a descending* ℓ*-isogeny. Moreover, there are such* ℓ*-isogenies.*

Proof. α is descending so $[\mathcal{O}_1 \colon \mathcal{O}_2] = \ell$, hance we have that $\ell \mid [\mathcal{O}_K \colon \mathcal{O}_2]$: from Proposition 3.3.5 we know that from E_2 there are 1 ascending ℓ-isogeny and 1 descending.
If γ is the ascending isogeny $[\mathcal{O}_3 \colon \mathcal{O}_2] = \ell$ we obtain that $f_1 = f_3$, but for each conductor there exist an single order, so $\mathcal{O}_1 \simeq \mathcal{O}_3$. So $\beta \neq \gamma$. Therefore β must be the descending ℓ-isogeny. The last part follows from Theorem 3.2.2. □

In other words, if $\beta = \hat{\phi}$ is ascending, then β is a descending ℓ-isogeny. So in the case of Lemma, if E_2 has $\ell + 1$ ℓ-isogenies, $\hat{\phi}$ is an ascending ℓ-isogeny and ℓ others are descending ℓ-isogenies.
A very special case is when there exist more then one horizontal isogeny to the same curve. In this case, in fact, we obtain some information about $\mathcal{O}$.

Lemma 3.3.10. *If there exist two different ℓ-isogenies (up to isomorphism) from a curve E to a curve E', then they are both horizontal ℓ-isogenies. We can also conclude that ℓ splits in $\mathcal{O}$.*

Proof. First of all, we observe that if $\mathcal{O}$ is not maximal at ℓ, we do not may have such isogenies. If it is not maximal and $\ell \nmid [\mathcal{O} \colon \mathbb{Z}[\pi]]$, it's obvious since E because exists only an ℓ-isogeny up isomorphism by Proposition 3.3.5. If $\ell \mid [\mathcal{O} \colon \mathbb{Z}[\pi]]$, there is only one ascending isogeny, so the only possibility would be to have two descending isogenies, this case can not occur yet. Indeed, $[\mathcal{O} \colon \mathcal{O}'] = \ell$ then $\mathcal{O}$ is not maximal at ℓ and if this case would occur, then should be exist two ascending ℓ-isogenies from E', which is impossible because of Proposition 3.3.5. Therefore ℓ does not divide the conductor of $\mathcal{O}$.
If $\ell \mid [\mathcal{O} \colon \mathbb{Z}[\pi]]$ there are $1 + \left(\frac{D}{\ell}\right)$ horizontal ℓ-isogenies and $\ell - \left(\frac{D}{\ell}\right)$ descending. With the same argument of the previous case, the two isogenies can be both descendant or one descendant and one horizontal. So $\left(\frac{D}{\ell}\right)$ must be 1, i.e. ℓ splits in $\mathcal{O}$. If $\ell \mid [\mathcal{O} \colon \mathbb{Z}[\pi]]$, similarly we have the thesis. □

From the previous fact we also obtain a bound for the discriminant of the order:

Corollary 3.3.11. *Suppose there are two ℓ-isogenies α and β distinct up to isomorphism from E to the same curve E' . Then the discriminant D of the endomorphism ring of E is such that $|D| \leq 4q^2$.*

Proof. The isogeny $\hat{\alpha}\beta$ is in $\mathrm{End}(E)$, so it exists an algebraic integer in $\mathcal{O}$ of norm ℓ^2, or equivalently there exist $x, y \in \mathbb{Z}$ such that $4\ell^2 = x^2 + |D|y^2$. □

Remark 3.3.12. Let us suppose ℓ different from the characteristic p of the finite field. $E[\ell]$ is an abelian group of rank two. In particular, once fixed a basis π acts over $E[\ell]$ as a matrix in $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ which characteristic polynomial is

$$\chi(X) = X^2 - tX + q \mod \ell$$

Therefore, there are tree possibilities:

- $\left(\frac{D_\pi}{\ell}\right) = 1$, $\chi(X) = (X - \lambda)(X - \mu)$ splits $\mod \ell$ $(\mu \neq \lambda)$, we will call this case *Elkies* or *split*;
- $\left(\frac{D_\pi}{\ell}\right) = -1$, $\chi(X)$ does not split $\mod \ell$, we will call this case *Atkin* or *inert*;
- $\left(\frac{D_\pi}{\ell}\right) = 0$, $\chi(X) = (X - \lambda)^2 \mod \ell$, we will call this case *ramified.*

If $\ell \nmid f_\pi$, by Kummer Theorem we have each one of these case corresponds to a different type of factorization of $\ell\mathcal{O}_K$, in some sense the name are justified. Using the same notations, let us suppose to be in Elkies case and that we can find a basis $\{P, Q\}$ of $E[\ell]$ onto which π acts as a diagonal matrix

$$M = \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$$

Each of the two eigenspaces of M is the kernel of an isogeny of degree ℓ from E to another curve E'. By Proposition 3.3.5, if $\operatorname{End}(E) = \mathcal{O}_K$ the two isogeny

$$\phi_\lambda \colon E \to {}^{E}\!\big/_{E[\ell] \cap \ker(\pi - \lambda)}$$

$$\phi_\mu \colon E \to {}^{E}\!\big/_{E[\ell] \cap \ker(\pi - \mu)}$$

are horizontal.

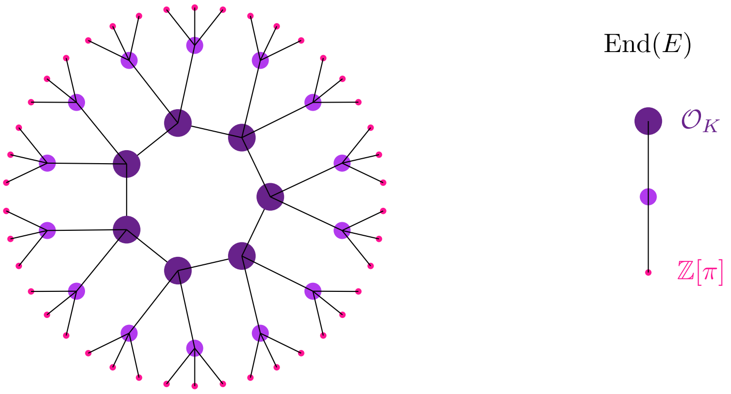

Figure 3.1: A 3-isogenies volcano of ordinary elliptic curves in Elkies case.

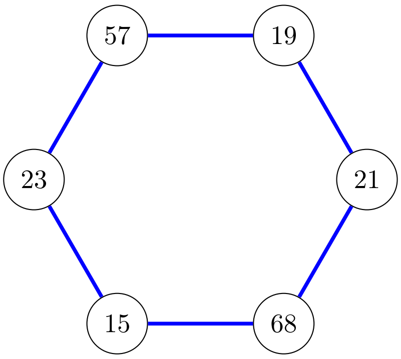

Figure 3.2: Example 3.3.6

This set of lemmas gives us an idea of the graph of ℓ-isogenies of the elliptic curves having the same Frobenius map. It has a structure of a *volcano* truncated at the level of $\mathbb{Z}[\pi]$. The *crater* comes from the horizontal ℓ-isogenies (if

they exist) that we can find when $\mathcal{O}$ is maximal at ℓ, using Proposition 3.3.5. The rest of the volcanic structure comes from the above lemmas. We remark that if $\ell | [\mathcal{O}_K : \mathcal{O}]$ then E does not have any horizontal ℓ-isogeny. The *level* of an elliptic curve in the volcano is the ℓ-adic valuation of its conductor and the *height* of the volcano is equal to the level of a curve with endomorphism ring isomorphic to $\mathbb{Z}[\pi]$ locally at ℓ. In particular, the crater is a cycle of horizontal isogenies in Elkies case, it's reduced to one point in Atkin case and to two points in ramified case.
Finally, we observe that each isogeny of the crater is the root of a tree, which can have also height zero, and that all the tree associated to curves in the same crater have equal number of vertex, then if there are a finite prime number of representatives in an isogeny class the volcano has only the crater.

Let us conclude this section with some explicit examples.

Example 3.3.13. Let us consider the curve $E\colon y^2 + 12xy + 2y = x^3 + x^2 + 4x + 1$ over the finite field $k = \mathbb{F}_{71}$. Its j-invariant is 47 and the j-invariants in its connected component of the isogeny graph are

$$47, 6, 8, 12, 4, 58, 5, 59$$

The frobenius trace of E is 6, so characteristic polynomial is

$$p(x) = x^2 - 6x + 71$$

and $\mathrm{End}(E)$ must be an order in $K = \mathbb{Q}(\sqrt{-62})$. In this special case $\mathcal{O}_K = \mathbb{Z}[\pi]$, hence for each ℓ we have only a crater and checking the Legendre symbol we see the prime 2 is Atkin while 3 is Elkies. With explicit computation we obtain the diagram in Figure 3.3 which is coherent with the theoretical results. We use red dashed edges to the rational 2-isogenies and blue continuous edges to the rational 3-isogenies.

Example 3.3.14. Let us consider the curve $E_1/\mathbb{F}_{71}$ of Example 3.3.6. Its j-invariant is 19 and the j-invariants in its connected component of the isogeny graph are

$$21, 68, 15, 23, 57.$$

Also in this case we have that 3 is an Elkies prime, with the same convention as above we obtain the graph in Figure 3.2.

3.4 Another Interpretation of Ordinary Isogeny Graph

In this section we are going give a further interpretation of the isogeny graph as a Schreier graphs:

Definition 3.4.1. Let G be a group acting freely on a set X, in the sense that there is a map

$$\begin{array}{ccc} G \times X & \to & X \\ (\sigma, x) & \to & \sigma \cdot x \end{array}$$

such that $\sigma \cdot x = x$ if and only if $\sigma = 1$, and $\sigma \cdot (\tau \cdot x) = (\sigma\tau) \cdot x$ for all $\sigma, \tau \in G$ and $x \in X$. Let $S \subseteq G$ be a *symmetric subset*, i.e. one not containing 1 and

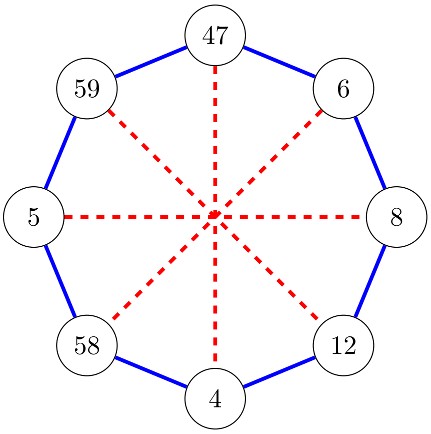

Figure 3.3: Example 3.3.13

closed under inversion. The *Schreier graph* of (S, X) is the graph which vertices are the elements of X, and such that $x, x' \in X$ are connected by an edge if and only if $\sigma \cdot x = x$ for some $\sigma \in S$.

Let us see an example. Take a cyclic group G of order n, then $(\mathbb{Z}/n\mathbb{Z})^*$ acts naturally on G by the law $\sigma \cdot g = g^\sigma$ for any $g \in G$ and $\sigma \in (\mathbb{Z}/n\mathbb{Z})^*$. This action is not free on G, but it is so on the subset P of all generators of G; we can thus build the Schreier graph (S, P), where S is a symmetric subset that generates $(\mathbb{Z}/n\mathbb{Z})^*$.

Example 3.4.2 ([DF17] III§14.1). An example of such graph is in Figure 3.4 for the case $n = 13$, where the set $S \subseteq (\mathbb{Z}/13\mathbb{Z})^*$ has been chosen to contain $2, 3, 5$ and their inverses.

A Schreier graph has many good properties, which will analyze later in this chapter. Now we are interested in understanding how Schreier graphs are related to ordinary isogeny graphs. In particular, we want to show that there is a close relation between isogenies and fractional ideals. To do it, we need to define new objects. Since our purpose in this chapter is to give a fairly comprehensive presentation of the tools we need later, we do not always go into details, which can be found in [Cox97] and [Sil09].

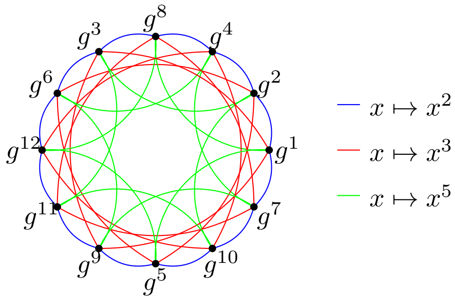

Figure 3.4

3.4.1 The class group of an order in an imaginary quadratic field

Let $\mathcal{O}$ an order in a number field K. A *fractional ideal* is a nonzero subgroup $I \subset K$ such that $xI \subset I$ for all $x \in \mathcal{O}$ and there exists a nonzero $x \in \mathcal{O}$ such that $xI \subset \mathcal{O}$. A fractional ideal is called *principal* if it is of the form $x\mathcal{O}$ for some $x \in K$. For convenience, here we simply call *ideals* the fraction ideals and we use the name *integral ideal* for the fraction ideals in $\mathcal{O}$.

Definition 3.4.3. Let $\mathcal{O}$ an order in a number field K. An ideal I is said to be *invertible* if there is another ideal J such that $IJ = \mathcal{O}$. We say that J is the *inverse* of I and we indicate it I^{-1}.

Note that if $\mathcal{O}$ is not maximal, it is not a Dedekind domain. This cause some problems, because it is equivalent to say that there exist fraction ideal which are not invertible. Then we immediately have that the set of ideals is no longer a group. In particular, it can happen that

$$\mathcal{O} \subsetneq \{b \in K \mid bI \subset I\}$$

We can remedy this issue by introducing the following notion:

Definition 3.4.4. Let $\mathcal{O}$ an order in a number field K. An ideal I is said to be *proper* if

$$\mathcal{O} = \{b \in K \mid bI \subset I\}$$

Proposition 3.4.5. *Let $\mathcal{O}$ an order in a number field K. An ideal I is proper if and only if it is invertible.*

Proof. Proposition 7.4 of [Cox97]. □

We denote by $\mathcal{I}(\mathcal{O})$ the set of the proper fractional ideals of $\mathcal{O}$ and by $\mathcal{P}(\mathcal{O})$ the subset of principal ideals.
We can define an product in $\mathcal{I}(\mathcal{O})$, since given two ideal I, J then IJ is a fractional ideal, too. The neutral element is obviously $\mathcal{O}$ itself. Therefore $\mathcal{I}(\mathcal{O})$ is an abelian group and $\mathcal{P}(\mathcal{O})$ in a subgroup.
Naturally we can consider the quotient by principal ideals:

Definition 3.4.6. Let $\mathcal{O}$ an order in a number field K. The *(ideal) class group* of $\mathcal{O}$ is

$$\mathrm{Cl}(\mathcal{O}) := {}^{\mathcal{I}(\mathcal{O})}\!\big/_{\mathcal{P}(\mathcal{O})}.$$

The goal of this section is to show that the class group acts over the isogeny graph.
The cardinality of $\mathrm{Cl}(\mathcal{O})$, denoted by $h(\mathcal{O})$, is called the *class number* of $\mathcal{O}$. For proper ideals of order in imaginary quadratic field is well defined the complex conjugated of an ideal I, denoted by $\sigma(I)$. There hold many of the properties as in the maximal case, for example:

Lemma 3.4.7. *Let $\mathcal{O}$ an order in the imaginary quadratic number field K. Given $I, J \in \mathcal{O}$, its norm is $\mathrm{N}(I) = |\mathcal{O}/I|$. Then*

- $\mathrm{N}(a\mathcal{O}) = \mathrm{N}^K_{\mathbb{Q}}(a)$ *for all $a \in \mathcal{O}$.*
- $\mathrm{N}(IJ) = \mathrm{N}(I)\,\mathrm{N}(J)$.

- *$I\sigma(I) = \mathrm{N}(I)\mathcal{O}$.*

Proof. Lemma 7.14 [Cox97]. □

Corollary 3.4.8. *Let $\mathcal{O}$ an order in the imaginary quadratic number field K and $I \in \mathcal{I}(\mathcal{O})$. Then $\sigma(I)$ is the inverse of I in $\mathrm{Cl}(\mathcal{O})$.*

It is interesting to understand the behavior of the proper ideals of a fixed order in terms of the maximal order $\mathcal{O}_K$. In fact, further on in this section we will present some results of the complex multiplication theory which, classically, is formulated in terms of $\mathcal{O}_K$.

Definition 3.4.9. Let K a quadratic field and $\mathcal{O}$ an order with conductor f, we say that a non zero ideal $I \in \mathcal{O}$ is *prime to* f provided that $I + f\mathcal{O} = \mathcal{O}$. Furthermore, given a positive integer m, an ideal $I \subseteq \mathcal{O}_K$ is *prime to* m provided that $I + m\mathcal{O}_K = \mathcal{O}_K$

Proposition 3.4.10. *Let K an imaginary quadratic field and $\mathcal{O}$ an order with conductor f. The following facts hold:*

1. *If $I \subseteq \mathcal{O}_K$ is prime to f, then $I \cap \mathcal{O}$ is an $\mathcal{O}$-ideal prime to f of the same norm.*
2. *If $I \subseteq \mathcal{O}$ is prime to f, then $I\mathcal{O}_K$ is an $\mathcal{O}_K$-ideal prime to f of the same norm.*
3. *The map $I \mapsto I \cap \mathcal{O}$ induced an isomorphism between the group of the ideals of $\mathcal{O}_K$ prime to f, i.e. $\mathcal{I}_K(f)$, and the subgroup $\mathcal{I}(\mathcal{O}, f) < \mathcal{I}(\mathcal{O})$ of the proper ideal prime to f.*

Proof. Proposition 7.20 [Cox97]. □

By this Proposition we have that every $\mathcal{O}$-ideal I prime to f has unique decomposition as product of $\mathcal{O}$-ideals prime to f and that holds the following theorem:

Theorem 3.4.11. *Let K an imaginary quadratic field and $\mathcal{O}$ an order with conductor f. The class group $\mathrm{Cl}(\mathcal{O})$ is naturally isomorphic to $\mathcal{I}(\mathcal{O}, f)/\mathcal{P}(\mathcal{O}, f)$ and also to*

$$\mathcal{I}_K(f) \big/ \mathcal{P}_K(f)$$

where $\mathcal{P}_K(f)$ is the subgroup of principal ideals $a\mathcal{O}_K$ such that $a \equiv b \mod f\mathcal{O}_K$ for b integer prime to f.

One of the main consequence, not actually so immediate ([Cox97] Theorem 7.24), of this theorem is that the following sequence is exact

$$1 \to \frac{(\mathcal{O}_K/f\mathcal{O}_K)^*}{\sigma(\mathcal{O}_K^*)(\mathbb{Z}/m\mathbb{Z})^*} \to \mathrm{Cl}(\mathcal{O}) \to \mathrm{Cl}(\mathcal{O}_K) \to 1$$

and so

$$h(\mathcal{O}) = \frac{h(\mathcal{O}_K)}{[\mathcal{O}_K^* : \mathcal{O}^*]} f \prod_{p|f} \left(1 - \left(\frac{D_K}{p}\right)\frac{1}{p}\right)$$

where p are primes. Furthermore, $h(\mathcal{O})$ is always an integer multiple of $h(\mathcal{O}_K)$. Then:

Theorem 3.4.12. *The class group of an order $\mathcal{O}$ in a number field is a finite abelian group.*

3.4.2 Class Group Action over Elliptic Curves with Complex Multiplication

The class group is a fundamental objects in number field theory, the results we use in this section are part of the theory of *complex multiplication.*

Let $E/\mathbb{C}$ an elliptic curve. We recall that in characteristic zero the endomorphism ring can not be isomorphic to an order in quaternion algebra. Thus $\operatorname{End}(E) \simeq \mathbb{Z}$ or an order in a quadratic imaginary number field K (in this case we say that it has *complex multiplication*). Here we suppose to be in the latter case. We fix K as the quadratic number field, $\mathcal{O}_K$ its maximal order and $\mathcal{O} = \operatorname{End}(E)$. By Λ by Theorem 1.6.3.4., for every elliptic curve over $\mathbb{C}$ there is a lattice $\Lambda \subseteq \mathbb{C}$ and an isomorphism

$$\begin{array}{rccc} f\colon & \mathbb{C}/\Lambda & \to & E(\mathbb{C}) \\ & z & \mapsto & (\wp(z,\Lambda), \wp'(z,\Lambda)). \end{array}$$

where $\wp(z,\Lambda)$ is the *Weierstrass $\wp$-function* associated to the lattice. The elliptic curve corresponding to Λ is usually given in terms of the g_i functions (1.15) and it has Weierstrass form

$$E_\Lambda\colon y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda).$$

Note that if E has complex multiplication, there are two way to embed $\mathcal{O}$ in $\mathbb{C}$. It is important to pin down one of these, hence in what follows we suppose to have fixed it an we indicate it as $[\cdot]$.

Definition 3.4.13. Let L a field and $\mathcal{O}$ an order in a ring. The class of all the elliptic curves defined over L with $\operatorname{End}(E) \simeq \mathcal{O}$ up to isomorphism is denoted $\mathcal{ELL}_L(\mathcal{O})$.

Note that by Theorem 1.6.5

$$\mathcal{ELL}_{\mathbb{C}}(\mathcal{O}) = \frac{\{\text{ lattices } \Lambda \text{ with } \operatorname{End}(E_\Lambda) \simeq \mathcal{O}\}}{\text{homothety}}$$

We are interested, now, in relate $\mathcal{O}$-ideals and elliptic curves in $\mathcal{ELL}_{\mathbb{C}}(\mathcal{O})$. For a generic quadratic order, the proof of the main theorem of this section would be long and it use advanced tools. Here, we want to give only a trace and the principal ideas in order to have a deeper comprehension of the theoretical bases of the applications we will present in the following chapters. Therefore, we give all the details in the case $\mathcal{O} = \mathcal{O}_K$ and later, at the end of this subsection, we try to explain how to generalized this construction by the theory shown above.

Let J a nonzero ideal of $\mathcal{O}_K$, up to embedding, it is a lattice in $\mathbb{C}$. Note that from the definition a (fractional) ideal in a quadratic imaginary field is a $\mathbb{Z}$-module of rank 2 not conteined in $\mathbb{R}$. Hence we can form an elliptic curve E_J whose endomorphism ring is

$$\begin{aligned} \operatorname{End}(E_J) =& \{\alpha \in \mathbb{C}\colon \alpha J \subseteq J\} \\ =& \{\alpha \in K\colon \alpha J \subset J\} \\ =& \mathcal{O}_K \end{aligned}$$

where the third equation take advantage from $J \subseteq K$ and the last one is since J is fractional. Thus each nonzero J gives an elliptic curve with complex multiplication by $\mathcal{O}_K$. On the other hand, since homothetic lattices give isomorphic elliptic curves, we see that

$$E_J \simeq E_{cJ}$$

for all $c \in \mathcal{O}_K$. This suggest that we look at the group of fraction ideal modulo principal ideals, i.e. the class group $\mathrm{Cl}(\mathcal{O}_K)$. Note that we have just proven that the map

$$\begin{array}{ccc} \mathrm{Cl}(\mathcal{O}_K) & \to & \mathcal{ELL}_{\mathbb{C}}(\mathcal{O}_K) \\ \text{class of } J & \mapsto & E_J \end{array} \tag{3.3}$$

is well defined. More generally, if Λ is a lattice and $J \neq (0)$ a fractional ideal we can define

$$J\Lambda := \left\{ \sum_{i=1}^{r} a_i \lambda_i \colon a_i \in J,\ \lambda_i \in \Lambda \right\}$$

We want to prove that there exists a simply transitive action of the class group on $\mathcal{ELL}_{\mathbb{C}}(\mathcal{O}_K)$.

Lemma 3.4.14. *Let Λ a lattice with $E_\Lambda \in \mathcal{ELL}_{\mathbb{C}}(\mathcal{O}_K)$, and let I a nonzero ideal of K. Then*

i) $I\Lambda$ is a lattice in $\mathbb{C}$.

ii) The elliptic curve $E_{I\Lambda}$ satisfies $\mathrm{End}(E_{I\Lambda}) \simeq \mathcal{O}_K$.

iii) $E_{I\Lambda} \simeq E_{J\Lambda}$ if and only if $[I] = [J]$ in $\mathrm{Cl}(\mathcal{O}_K)$.

Hence there is a well-defined action of $\mathrm{Cl}(\mathcal{O}_K)$ on $\mathcal{ELL}_{\mathbb{C}}(\mathcal{O}_K)$ by

$$([I], E_\Lambda) \overset{\kappa}{\mapsto} E_{[I]^{-1}\Lambda} \tag{3.4}$$

Proof.

i) $E_\Lambda \in \mathcal{ELL}_{\mathbb{C}}(\mathcal{O}_K)$ so $\mathcal{O}_K\Lambda = \Lambda$. By definition, there exists $d \in \mathcal{O}_K$ such that $dI \subseteq \mathcal{O}_K$. Then $I\Lambda \subseteq \frac{1}{d}\Lambda$ and $I\Lambda$ is a discrete subgroup of $\mathbb{C}$. Similarly, choosing $y \neq 0$ such that $y\mathcal{O}_K \subseteq I$, we find $y\Lambda \subseteq I\Lambda$. Hence $I\Lambda$ spans $\mathbb{C}$, so it is a lattice.

ii) For all $a \in \mathbb{C}$

$$aI\Lambda \subseteq I\Lambda \iff I^{-1}aI\Lambda \subseteq I^{-1}I\Lambda \iff a\Lambda \subseteq \Lambda$$

Then

$$\begin{aligned} \mathrm{End}(E_{I\Lambda}) &= \{a \in \mathbb{C} \colon aI\Lambda \subseteq I\Lambda\} \\ &= \{a \in \mathbb{C} \colon a\Lambda \subseteq \Lambda\} \\ &= \mathrm{End}(E_\Lambda) \\ &= \mathcal{O}_K \end{aligned}$$

iii) The isomorphism class of $E_{I\Lambda}$ is completely determined by the homothety class of $I\Lambda$. In particular, $E_{I\Lambda} \simeq E_{J\Lambda}$ if and only if there exist $c \in \mathbb{C}^*$ such that $I\Lambda = cJ\Lambda$. This condition is equivalent to

$$\Lambda = cI^{-1}J\Lambda$$

and also to

$$\Lambda = c^{-1}IJ^{-1}\Lambda$$

Hence, if $E_{I\Lambda} \simeq E_{J\Lambda}$, then both $cI^{-1}J$ and cIJ^{-1} take Λ to itself. In particular, either of them have to be contained in $\mathcal{O}_K$. Therefore

$$I = cJ.$$

Thus, we see immediately that $c \in K$ and that I and J are in the same class.

The last assertion follows from the following observation:

$$\kappa([I], \kappa([J], E_\Lambda)) = \kappa([I], E_{J^{-1}\Lambda}) = E_{I^{-1}J^{-1}\Lambda} = E_{(JI)^{-1}\Lambda} = \kappa([JI], E_\Lambda)$$

So κ gives a group action of $\mathrm{Cl}(\mathcal{O}_K)$ on $\mathcal{ELL}_{\mathbb{C}}(\mathcal{O}_K)$. □

Theorem 3.4.15. *The action of* $\mathrm{Cl}(\mathcal{O}_K)$ *on* $\mathcal{ELL}_{\mathbb{C}}(\mathcal{O}_K)$

$$\begin{array}{cccc} \kappa\colon & \mathrm{Cl}(O_K) \times \mathcal{ELL}_{\mathbb{C}}(\mathcal{O}_K) & \longrightarrow & \mathcal{ELL}_{\mathbb{C}}(\mathcal{O}_K) \\ & ([I], E_\Lambda) & \longmapsto & E_{[I]^{-1}\Lambda} \end{array} \tag{3.5}$$

is simply transitive. In particular

$$\#\mathcal{ELL}_{\mathbb{C}}(\mathcal{O}_K) = \#\,\mathrm{Cl}(\mathcal{O}_K) = h(\mathcal{O}_K).$$

Proof. Let E_{Λ_1},$E_{\Lambda_2} \in \mathcal{ELL}_{\mathbb{C}}(\mathcal{O}_K)$. To show that the class group acts transitively we must find an ideal I such that $\kappa([I], E_{\Lambda_1}) = E_{\Lambda_2}$. Choose $\lambda_1 \in \Lambda_1$:

$$I_1 = \frac{1}{\lambda_1}\Lambda_1$$

is a lattice. From Theorem VI§5.5[Sil11], we have that I_1 is in K and by assumption it is finitely generate $\mathcal{O}_K$ module, hence it is a fraction ideal of K. Similarly, from $\lambda_2 \in \Lambda_2$, we obtain the ideal I_2 of K. Then

$$\frac{\lambda_2}{\lambda_1} I_2 {I_1}^{-1} \Lambda_1 = \Lambda_2$$

We put $I = {I_2}^{-1} I_1$, so using that homothetic lattices define the same elliptic curve:

$$\kappa([I], E_{\Lambda_1}) = E_{I^{-1}\Lambda_1} = E_{\frac{\lambda_1}{\lambda_2}\Lambda_2} = E_{\Lambda_2}.$$

We proved the action be transitive. From Lemma 3.4.14 ii) we obtain is simply transitive. □

The study of groups $E[m]$, $m \in \mathbb{Z}$, gives many information about the curve. If E has complex multiplication we can extend this notion:

Definition 3.4.16. Let $I \subset \mathcal{I}(\mathcal{O}_K)$ the group of *I-torsion points* is

$$E[I] = \{P \in E \mid [a]P = 0 \; \forall a \in I\}$$

For example,if $I = m\mathcal{O}_K$ $E[m] = E[I]$. Notice that this definition depends on $[\cdot]$. As for the integral points groups, if the ideal I we choose is integral, we can describe the I-torsion points group as the kernel of a map:

Proposition 3.4.17. *Let $E \in \mathcal{ELL}_{\mathbb{C}}(\mathcal{O}_K)$ and I an integral ideal of $\mathcal{O}_K$.*

1. *$E[I]$ is the kernel of the map $E \mapsto \kappa([I], E)$.*
2. *$E[I]$ is a free $\mathcal{O}_K/I$-module of rank one.*

Before prove the Proposition above, in helpful the following observation:

Remark 3.4.18. If I an integral ideal of $\mathcal{O}_K$, then $\Lambda \subseteq I^{-1}\Lambda$, this means that there is a natural homomorphism

$$\begin{array}{cccc} \mu_I\colon & {}^{\mathbb{C}}\!/\!_{\Lambda} & \to & {}^{\mathbb{C}}\!/\!_{\Lambda} \\ & z & \mapsto & z \end{array}$$

which it turn induces a natural isogeny $\phi_I \colon E_\Lambda \to \kappa([I], E_\Lambda)$

Proof. 3.4.17 Let Λ the lattice corresponding to E and fix the isomorphism $E(\mathbb{C}) \simeq E/\Lambda$, we find that

$$\begin{aligned} E[I] \simeq & \{z \in \mathbb{C}/\Lambda \mid az = 0 \forall a \in I\} \\ = & \{z \in \mathbb{C} \mid az \in \Lambda \forall a \in I\}/\Lambda \\ = & \{z \in \mathbb{C} \mid zI \subset \Lambda \forall a \in I\} \\ = & I^{-1}\Lambda/\Lambda \\ = & \ker \mu_I \\ = & \ker \phi_I \end{aligned}$$

This proves 1.
We choose, now, a nonzero lattice element $\lambda \in \Lambda$. By Theorem VI§5.5[Sil11] $(1/\lambda)\Lambda \subseteq K$ and it is finitely generated as $\mathcal{O}_K$-module, then it is a fractional ideal of K. Since homothetic ideals give isomorphic elliptic curves we can suppose Λ a fractional ideal of K. From 1. we know

$$E[I] \simeq {}^{I^{-1}\Lambda}\!/\!_{\Lambda}$$

as $\mathcal{O}_K/I$-module. Let Q an integral ideal dividing I. The fact that $\mathcal{O}_K\Lambda = \Lambda$ implies that

$${}^{I^{-1}\Lambda}\!/\!_{\Lambda} \otimes_{\mathcal{O}_K} {}^{\mathcal{O}_K}\!/\!_{Q} \simeq {}^{I^{-1}\Lambda}\!/\!_{\Lambda + QI^{-1}\Lambda} = {}^{I^{-1}\Lambda}\!/\!_{QI^{-1}\Lambda}$$

By Chinese Remainder Theorem

$${}^{\mathcal{O}_K}\!/\!_{I} = \prod_{P \mid I} {}^{\mathcal{O}_K}\!/\!_{P^{e(P)}}$$

then

$$E[I] = \prod_{P \mid I} {}^{I^{-1}\Lambda}\!/\!_{P^{e(P)}I^{-1}\Lambda}$$

So it is sufficient to prove that

Lemma. *If $J \in \mathcal{I}(\mathcal{O}_K)$ and P^e is a power of an integral prime ideal, then J/P^eJ is a free $\mathcal{O}_K/P^e$-module of rank one.*

Proof. $R = \mathcal{O}_K/P^e$ is a local ring with maximal ideal $M = P/P^e$. Note that we can see the $\mathcal{O}_K/P$-vector space J/P^eJ the R/M-vector space

$$J/P^eJ \Big/ M(J/P^eJ).$$

The dimension of J/PJ over the residue field of P is obviously at most one, if fact two element must be linearly dependent. On the other hand, if the dimension would be zero than $J = MJ$, which is absurd. So the dimension of this space is one. The by Nakayama's lemma applied to J/P^eJ as R-module, J/P^eJ has to be a free R-module of rank one. □

Using the Lemma with $J = I^{-1}\Lambda$, the proof is completed. □

We just proved that given an elliptic curve over $\mathbb{C}$ with complex multiplication by the maximal order $\mathcal{O}_K \subset K$, each ideal I induces an isogeny whose kernel is just I-torsion group; by Lemma 3.4.14 we also have for all integral ideals I that the isogeny ϕ_I is *horizontal*. It hold that isogenies given by integral ideals and principal ideals also have a settled norm:

Corollary 3.4.19. *Let $E \in \mathcal{ELL}_{\mathbb{C}}(\mathcal{O}_K)$.*

- *For all integral ideals I, the map ϕ_I has degree $\mathrm{N}(I)$.*
- *For all $a \in \mathcal{O}_K$ the endomorphism $[a] : E \to E$ has degree $|\,\mathrm{N}_{\mathbb{Q}}^K(a)|$.*

Proof. Both follows immediately from the Proposition 3.4.17:

- From 1. $\deg \phi_I = \#E[I]$ and from 2. $\#E[I] = \mathrm{N}(I)$.
- $\deg\,[a] = \#\ker\,[a] = \#E[a\mathcal{O}_K] = \mathrm{N}_{\mathbb{Q}}^K(a\mathcal{O}_K) = |\,\mathrm{N}_{\mathbb{Q}}^K(a)|$.

□

Remark 3.4.20. Note that the previous facts and proofs can be generalized to every order $\mathcal{O}$ of an imaginary quadratic number field, being careful to use proper $\mathcal{O}$-ideals. In fact, by Theorem 3.4.12 and Lemma 3.4.7, the appropriate proprieties hold.

3.4.3 Integrality of j Invariant and Modular Polynomial

In the previous section we present the action of the class group of an order $\mathcal{O}$ over $\mathcal{ELL}_{\mathbb{C}}(\mathcal{O})$. However, we would be interesting in $\mathcal{ELL}_F(\mathcal{O})$ with $\operatorname{char} F$ prime. By Theorem 1.7.1, it is enough to reduce the simply transitive action to the curves defined over $\overline{\mathbb{Q}}$. Another classical result of complex multiplication theory allow us to do this:

Theorem 3.4.21. *Let $E/\mathbb{C}$ an elliptic curve with complex multiplication. Then $j(E) \in \overline{\mathbb{Q}}$.*

Remember that we consider curves up to isomorphism, Theorem 3.4.21 say us that each elliptic curve defined over the complex numbers is isomorphic to one other defined over the algebraic closure of $\mathbb{Q}$. Therefore, given an order $\mathcal{O}$ in a quadratic imaginary field $\mathcal{ELL}_{\overline{\mathbb{Q}}}(\mathcal{O}) = \mathcal{ELL}_{\mathbb{C}}(\mathcal{O})$, so we can apply Theorem 1.7.1 to each curve, in our context.

There exist different proofs of this Theorem 3.4.21. In the complex analytic one is showed that given two lattices Λ_1, Λ_2, whose induced elliptic curves are isogenous, it can be found a $\mathbb{Q}$-algebraic relation between their j invariants with integral coefficients; so using $\Lambda_1 = \Lambda_2$ the thesis is proved. We will not see details, for which we refer to [Sil09] II§6. However, it's worth to give explicitly these algebraic relations, since they are good tools to efficiently build isogeny graphs.

Let us consider a complex lattice $\Lambda = \langle \omega_1, \omega_2 \rangle$ such that the imaginary part of $\tau = \omega_1/\omega_2$ is greater then zero, we say that such a basis has *positive orientation.* Up to isomorphism of lattices, we can turn to the basis $\langle \tau, 1 \rangle$. In particular, τ define the lattice up to isomorphism and we denote

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

If we multiply the basis of Λ by a matrix in

$$\mathrm{SL}_2(\mathbb{Z}) = \{M \in \mathrm{M}_2(\mathbb{Z}) \mid \det M = 1\}$$

the lattice stay fixed and also the orientation is preserved. In general a matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}_2(\mathbb{Z})$$

acts over a basis of Λ transforming τ in the following way:

$$A(\tau) = \frac{a\tau + b}{c\tau + d} \tag{3.6}$$

Definition 3.4.22. A meromorphic function of a complex variable τ is called *modular*, if is not changed by the action of $\mathrm{SL}_2(\mathbb{Z})$.

Theorem 3.4.23. *The function $j(\tau)$ is modular.*

Proposition 3.4.24. *Any modular function is representable by a fraction of polynomial in $j(\tau)$.*

Let $\mathrm{M}_2^l(\mathbb{Z})$ the matrices of coprime integer elements and determinant l. If $M \in \mathrm{M}_2^l(\mathbb{Z})$ and $A, B \in \mathrm{SL}_2(\mathbb{Z})$ then $AMB \in \mathrm{M}_2^l(\mathbb{Z})$. Therefore, we can define the cosets of $\mathrm{M}_2^l(\mathbb{Z})$ to the group $\mathrm{SL}_2(\mathbb{Z})$ and a set of representatives is

$$\mathcal{S}_l := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}_2^l(\mathbb{Z}) \colon d > 0, 0 \leq b < d \right\}$$

which has cardinality

$$\psi(l) = l \prod_{p \mid l} \left(1 + \frac{1}{p}\right)$$

Definition 3.4.25. The *modular polynomial of order l* is

$$\Phi_l(X, j(\tau)) = \prod_{S \in \mathcal{S}_l} (X - j(S(\tau))) \tag{3.7}$$

The modular polynomials are the integral relations for the j-invariants:

Proposition 3.4.26.

- $\Phi_l(X, j(\tau)) \in \mathbb{Z}[X]$
- $\Phi_l(X, Y) = \Phi_l(Y, X) \in \mathbb{Z}[X, Y]$

Example 3.4.27. The computer algebra system Magma [BCP97] contains a large database of modular polynomials, useful for applications. Here they are lower primes modular polynomials:

$$\begin{aligned}
\Phi_2(X,Y) =& X^3 - X^2Y^2 + 1488X^2Y - 162000X^2 + 1488XY^2 + 40773375XY \\
& + 8748000000X + Y^3 - 162000Y^2 + 8748000000Y - \\
& 157464000000000 \\
\Phi_3(X,Y) =& X^4 - X^3Y^3 + 2232X^3Y^2 - 1069956X^3Y + 36864000X^3 \\
& + 2232X^2Y^3 + 2587918086X^2Y^2 + 8900222976000X^2Y + \\
& + 452984832000000X^2 - 1069956XY^3 + 8900222976000XY^2 \\
& - 770845966336000000XY + 1855425871872000000000X + Y^4 + \\
& 36864000Y^3 + 452984832000000Y^2 + 1855425871872000000000Y
\end{aligned}$$

Modular polynomials gives also information about isogenies:

Theorem 3.4.28. *Let $E_1/\mathbb{C}$ and $E_2/\mathbb{C}$ elliptic curves. There exists a cyclic isogeny, i.e. an isogeny with cyclic kernel, of degree l between them if and only $\Phi_l(j(E_1), j(E_2)) = 0$.*

Proof. Theorem 11.23 [Cox97]. □

Corollary 3.4.29. *Let E_1 and E_2 elliptic curves defined over $\mathbb{F}_q$. Then exist a cyclic isogeny over $\mathbb{F}_q$ of degree l between them if and only*

$$\Phi_l(j(E_1), j(E_2)) = 0$$

and $\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q)$.

Remark 3.4.30. To find the curves related to E via an ℓ-isogeny, we can solve the equation $\Phi_\ell(X, j(E)) = 0$, which gives us their potential invariants. Suppose j' is one of these roots. The curve E' we are looking for is known up to twist and we must find an equation for it. Formulas for computing an equation of E' are given Chapter 1. In section 7 of [Sch95] also the following formula is given. The curve

$$E' \colon y^2 = x^3 + ax + b$$

with

$$a = -\frac{j_0^2}{48j'(j' - 1728)}$$

$$b = -\frac{j_0^3}{864 j'^2 (j' - 1728)}$$
$$j_0 = -\frac{18b \frac{\partial \Phi_\ell}{\partial X}(j(E), j')}{3a \frac{\partial \Phi_\ell}{\partial Y}(j(E), j')} j(E)$$

is in the right class of isomorphism, once reduced. When one of the terms appearing in denominators is equals zero this method fails. So, if we are in one of the bad cases, we can compute $E[\ell]$ explicitly (by division polynomials) over a field extension and checks each of the possible ℓ-cyclic subgroups kernel until the right J is found and then use the method above with E/J. For ordinary elliptic curves $j = 1728$ and $j = 0$ can be avoided, for example by selecting a class of isogeny which they not belong to. Moreover, the term $\frac{\partial \Phi_\ell}{\partial Y}(j(E), j')$ never vanish for small ℓ. In the supersingular case, instead, experimentally is proved that $\frac{\partial \Phi_\ell}{\partial Y}(j(E), j')$ vanishes also in small cases. There exist other approaches, see [Gal12] Chapter 25.2.

Remark 3.4.31. Note that as consequence of fact seen in sections 3.4.2 and 3.4.3 we have that, given an ordinary elliptic curve over a finite field $\mathbb{F}_q$ with complex multiplication by the order $\mathcal{O}$ in the imaginary quadratic field K, the class group $\mathrm{Cl}(\mathcal{O})$ acts freely and transitively over $\mathcal{ELL}_{\bar{\mathbb{F}}_q}(\mathcal{O})$. Note also that, by Theorem 3.4.11 we have an explicit relation with conductors (which are important later for Deuring reduction). Furthermore, let us consider an ordinary curve $E/\mathbb{F}_q$ with endomorphism ring $\mathcal{O}$ with conductor f and $\ell \neq \mathrm{char}\,\mathbb{F}_q$. If $\ell \mid f$, by Proposition 3.3.5 does not exist horizontal isogeny. On the other hand $\ell\mathcal{O} + f\mathcal{O} = \ell\mathcal{O} \subsetneq \mathcal{O}$, so $\ell\mathcal{O} \notin \mathcal{I}(\mathcal{O}, f)$ and $\mathrm{Cl}(\mathcal{O})$ does not contain ideal with norm divisible by ℓ. More details on the construction are given in the proof of Theorem 3.6.6.

3.4.4 Isogeny Graphs as Schreier Graphs

Suppose that that $\ell\mathcal{O}$ splits into prime ideals as $\ell\mathcal{O} = I\sigma(I)$. Set $S = \{I, \sigma(I)\}$, then the Schreier graph of $(S, \mathcal{ELL}_{\mathbb{F}_q}(\mathcal{O}))$ is exactly the graph of horizontal ℓ-isogenies on $\mathcal{ELL}_{\mathbb{F}_q}(\mathcal{O})$. More generally, if we let $S \subset \mathrm{Cl}(\mathcal{O})$ be a symmetric subset, its Schreier graph is a graph of horizontal isogenies. We will see in section 3.6 that this new point of view allows us to solve the problem of finding an isogeny, between fixed curves, just only by considering isogenies of bounded degree. Moreover, this alternative prospective is useful also to discover to which order, in the appropriate number field, the endomorphism ring of an ordinary curve is isomorphic. Let us consider the following examples:

Example 3.4.32.

1. The endomorphism ring $\mathcal{O}_1 = \mathrm{End}(E_1)$, of the curve E_1 in Example 3.3.6, could be either $\mathbb{Z}[\pi_1]$ or $\mathcal{O}_{K_1}$. In Example 3.3.14 we saw that the rational 3-isogeny graph is a crater with 6 nodes. If we compute the class groups we obtain
$$\mathrm{Cl}(\mathcal{O}_{K_1}) \simeq {}^{\mathbb{Z}}\!/_{2\mathbb{Z}} \quad \text{and} \quad \mathrm{Cl}(\mathbb{Z}[\pi_1]) \simeq {}^{\mathbb{Z}}\!/_{6\mathbb{Z}}$$
hence $\mathcal{O}_1 = \mathbb{Z}[\pi_1]$.

2. The endomorphism ring $\mathcal{O} = \mathrm{End}(E)$, of the elliptic curve E in Example 3.3.13, must be a maximal order since the conductor of $\mathbb{Z}[\pi]$ in one. We saw that the number of curve isogenous to E are 8 and all the isogenies are horizontal. If we compute it class group we obtain exactly $\mathrm{Cl}(\mathcal{O}) \simeq \mathbb{Z}/8\mathbb{Z}$.

3.5 Supersingular Curves

The supersingular case is tricker than the ordinary. The endomorphism ring of a supersingular elliptic curve E is an order in a quaternion algebra, which is a non commutative algebra. In order to understand better the shape of the connected components of an isogeny graph and why this case seems to be harder, first of all we give an introduction to the arithmetic of the quaternion algebras; secondly we give the Lenstra's proof that a order which is the endomorphism rings of an elliptic curve is a maximal order and the consequences of this fact. Traditionally supersingular isogeny graph is considered over $\bar{\mathbb{F}}_p$. Note that it suffices to consider elliptic curves defined over $\mathbb{F}_{p^2}$ although the isogenies between them are over $\bar{\mathbb{F}}_p$ in general. Figure 3.5 and figure 3.6 provide two example of supersingular graphs.

3.5.1 Quaternion Algebras

Definition 3.5.1. An algebra $\mathcal{A}$ over a field F is said to be *associative* if it is an unit ring, an F-module with a F-bilinear operation, the multiplication $\cdot$, and if for all $x, y, z \in \mathcal{A}$ holds $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.

Definition 3.5.2. A *central simple algebra* is an associative F-algebra, whose center coincides with F and such that

- $\exists a, b \in \mathcal{A} : ab \neq 0$
- does not exist in $\mathcal{A}$ non trivial bilateral ideals.

If only these two conditions hold $\mathcal{A}$ is said to be *simple.*

Definition 3.5.3. An associative algebra $\mathcal{A}$ is called *division algebra* if there exists $1 \neq 0$ and for all $a \neq 0$ there exists x such that $ax = xa = 1$.

Definition 3.5.4. A *quaternion algebra* $\mathcal{A}$ over a field F is a central simple algebra of dimension 4 over F.

Definition 3.5.5. Let $\mathcal{A}$ be an F-algebra. An *involution* $\bar{\ } : \mathcal{A} \to \mathcal{A}$ is a F-linear map such that

1. $\bar{1} = 1$
2. $\bar{\bar{\alpha}} = \alpha$ for all $\alpha \in \mathcal{A}$
3. $\overline{\alpha\beta} = \bar{\beta}\bar{\alpha}$ for all $\alpha, \beta \in \mathcal{A}$

An involution is also called *standard involution* if $\alpha\bar{\alpha} \in F$.

Definition 3.5.6. Let $\bar{\ } : \mathcal{A} \to \mathcal{A}$ a standard involution. We define the *reduced trace* on $\mathcal{A}$ by

$$\begin{array}{rccc} \mathrm{trd}\colon & \mathcal{A} & \to & F \\ & \alpha & \mapsto & \alpha + \bar{\alpha} \end{array}$$

We define the *reduced trace* on $\mathcal{A}$ by

$$\begin{array}{rccc} \mathrm{nrd}\colon & \mathcal{A} & \to & F \\ & \alpha & \mapsto & \alpha\bar{\alpha} \end{array}$$

If $\mathcal{A}$ is not the zero ring, then $\alpha \in \mathcal{A}$ is a unit (has a two-sided inverse) if and only if $\operatorname{nrd}(\alpha) \neq 0$. Note that for $\alpha \in \mathcal{A}$

$$\alpha^2 - (\alpha + \bar{\alpha})\alpha + \alpha\bar{\alpha} = 0$$

So α is a root of the polynomial

$$x^2 - \operatorname{trd}(\alpha)x + \operatorname{nrd}(\alpha) \in F[x] \tag{3.8}$$

which we call the *reduced characteristic polynomial* of α. The fact that α satisfies its reduced characteristic polynomial is the *reduced Hamilton-Cayley theorem* for an algebra with standard involution. When $\alpha \notin F$, the reduced characteristic polynomial of α is its minimal polynomial, since if α satisfies a polynomial of degree 1 then $\alpha \in F$.

We consider only quaternion algebras over $\mathbb{Q}$, or over one of the completions $\mathbb{Q}_p$ or $\mathbb{R}$ at a place of $\mathbb{Q}$. We define Λ a *lattice in a quaternion algebra* $\mathcal{A}$ over $\mathbb{Q}$ to be a finitely generated $\mathbb{Z}$-module which contains a basis for $\mathcal{A}$ over $\mathbb{Q}$, and adopt the notation Λ for such a lattice. We denote an *order of a quaternion algebra*, also in this case defined to be a lattice which is a subring containing 1, by $\mathcal{O}$. An order is said to be *maximal* if it is not properly contained in another order.

Let p a prime of $\mathbb{Z}$ and $\mathbb{Z}_{(p)}$ the localization to the prime ideal by p, let $\Lambda \subset \mathcal{A}$ be a lattice

$$\Lambda_{(p)} := \Lambda \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$$

Obviously, $\Lambda_{(p)}$ is a $\mathbb{Z}_{(p)}$-lattice. The structure of a lattice in a quaternion algebra is *almost completely local*, in the following sense:

Theorem 3.5.7 (Local-global dictionary for lattices[2])**.** *Let $\mathcal{A}$ be a quaternion $\mathbb{Q}$-algebra, and let $\Lambda \subset \mathcal{A}$ be a lattice. Then the map $N \mapsto (N_{(p)})_p$ establishes a bijection between lattices N and collections of lattices $(N_{(p)})_p$ (indexed by primes p) where $\Lambda_{(p)} = N_{(p)}$ for all but finitely many primes p.*

This property is useful because it allows to bring back global issues to local. In particular, it implies that being a maximal order is a local property:

Lemma 3.5.8. *Let $\mathcal{A}$ be a quaternion $\mathbb{Q}$-algebra and let $\Lambda \subseteq \mathcal{A}$ be a lattice. Then the following are equivalent:*

1. *Λ is an order,*

2. *$\Lambda_{(p)}$ is a $\mathbb{Z}_{(p)}$-order for all primes p.*

Proof. It is enough to prove that $\Lambda = \cap_p \Lambda_{(p)}$. Obviously, $\subseteq$ holds ($\mathbb{Z}$ is a domain). Let us suppose x belongs to the intersection and consider the ideal $(\Lambda \colon x) \subseteq \mathbb{Z}$. Since $\mathbb{Z}$ is PID, each (p) is also maximal. $x \in \Lambda_{(p)}$ then exists $s \in \mathbb{Z} \setminus (p)$ such that $sx \in \Lambda$. In particular, $s \in (\Lambda \colon x)$, so this ideal is not contained in any maximal ideal, so $x \in \Lambda$.

□

[2] [Voi18] Theorem 9.5.1

Proposition 3.5.9. *Let $\mathcal{A}$ be a quaternion $\mathbb{Q}$-algebra and let $\mathcal{O} \subseteq \mathcal{A}$ be a lattice.*

1. *$\mathcal{O}$ is a maximal order,*
2. *$\mathcal{O}_{(p)}$ is a maximal $\mathbb{Z}_{(p)}$-order for all primes p.*

Proof. It follows directly from the previous Lemma and Local-global dictionary Theorem. □

Also considering the completions will be relevant. Let $\mathcal{O} \subseteq \mathcal{A}$ be an order. $\mathbb{Z} \subseteq \mathbb{Z}_{(p)} \subseteq \mathbb{Z}_p$, so with the same argument of the proof of Lemma 3.5.8 we have that

$$\Lambda_p \cap \mathcal{A}_{(p)} = \Lambda_{(p)}$$

In particular, the proposition can be reword:

Proposition 3.5.10. *Let $\mathcal{A}$ be a quaternion $\mathbb{Q}$-algebra and let $\mathcal{O} \subseteq \mathcal{A}$ be a lattice.*

1. *$\mathcal{O}$ is a maximal order,*
2. *$\mathcal{O}_{(p)}$ is a maximal $\mathbb{Z}_{(p)}$-order for all primes p.*
3. *$\mathcal{O}_p$ is a maximal $\mathbb{Z}_p$-order for all primes p.*

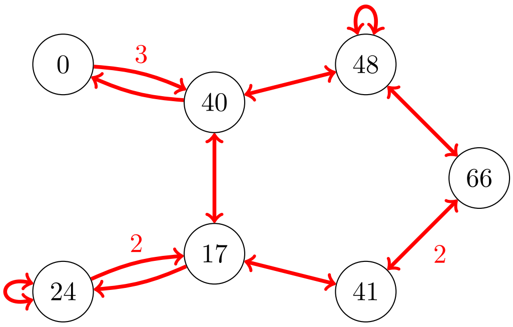

Figure 3.5: Supersingular isogeny graphs of degree 2 $\bar{\mathbb{F}}_{71}$ (labels indicate actual the number of isogenies).

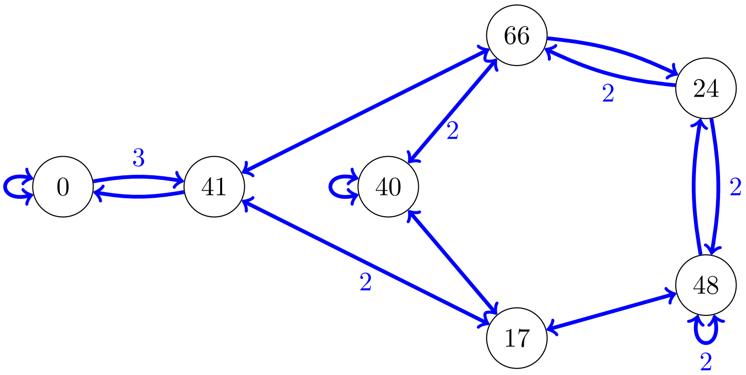

Figure 3.6: Supersingular isogeny graphs of degree 3 $\bar{\mathbb{F}}_{71}$.

The Wedderburn structure theorem ([Voi18] Corollary 7.1.2) implies that a quaternion algebra over a field F is either a *central division algebra* over F or isomorphic to the matrix algebra $\mathrm{M}_2(F)$. In particular, the completion $\mathcal{A}_p = \mathcal{A} \otimes_{\mathbb{Q}} \mathbb{Q}_p$ is either a division ring or the matrix ring $\mathrm{M}_2(\mathbb{Q}_p)$.

Definition 3.5.11. If $\mathcal{A}$ is a quaternion algebra over $\mathbb{Q}$ then a prime p is said to *ramify* if $\mathcal{A}_p = \mathcal{A} \otimes_{\mathbb{Q}} \mathbb{Q}_p$ is a division algebra or *split* if $\mathcal{A}_p$ is isomorphic to $\mathrm{M}_2(\mathbb{Q}_p)$. A quaternion algebra which ramifies at infinity is called *definite*, and one which splits at infinity is called *indefinite.*

Further, if $\mathcal{A}_p \simeq \mathrm{M}_2(\mathbb{Q}_p)$ then every maximal is conjugated to $\mathrm{M}_2(\mathbb{Z}_p)$. Also the converse implication holds: if $\mathrm{M}_2(\mathbb{Z}_p)$ is an order in $\mathcal{A}_p$ then is maximal and p splits. When $\mathcal{A}_p$ is a division ring, the p-adic valuation $v_p\colon \mathbb{Q}_p \to \mathbb{Z} \cup \{\pm\infty\}$ can be extended to a valuation over $\mathcal{A}_p$

$$\begin{array}{rccc} \omega\colon & \mathcal{A}_p & \to & \mathbb{Z} \cup \{\pm\infty\} \\ & \alpha & \mapsto & \frac{v_p(\mathrm{nrd}(\alpha))}{2} \end{array} \tag{3.9}$$

The associated valuation ring is just $\mathcal{O}_p \subseteq \mathcal{A}_p$ and it is the unique maximal order. In particular, it has an unique maximal ideal $P_p \subset \mathcal{O}_p$ satisfying $p\mathcal{O}_p = P_p^2$ ([Voi18]§13.2) .

By the Wedderburn theorem, we can obtain other information. Let α be in $\mathcal{A}$ not in the center F and let $R = F[\alpha]$ (the commutative ring). Then R is of dimension two over F:

- If α is a unit in $\mathcal{A}$, then R is a field extension of F , and $\mathcal{A}$ is a vector space and noncentral algebra over R, hence R/F is necessarily quadratic.
- If α is not invertible, then R must be isomorphic to $\mathrm{M}_2(F)$, so α satisfies its characteristic equation of degree two (3.8).

By Theorem 1.5.8 the quaternion algebras which arise from supersingular elliptic curves are of the form

$$\mathcal{A} = \mathbb{Q} \oplus \alpha\mathbb{Q} \oplus \beta\mathbb{Q} \oplus \alpha\beta\mathbb{Q}$$

with $\alpha^2 < 0$, $\beta^2 < 0$ e $\beta\alpha = -\alpha\beta$. Then they are division algebras over $\mathbb{Q}$, and the maximal subfields of $\mathcal{A}$ are imaginary quadratic extensions of $\mathbb{Q}$. Besides, these algebras are definite.

Let $I \subset \mathcal{A}$ be a lattice in a quaternion $\mathbb{Q}$ algebra $\mathcal{A}$, then

$$\mathcal{O}_L(I) \coloneqq \{\alpha \in \mathcal{A}\colon \alpha I \subseteq I\}$$

is an order, called the *left order of* I; we similarly define the *right order* $\mathcal{O}_R(I)$. If $\mathcal{O} \subset \mathcal{A}$ is an order and $\alpha \in \mathcal{A}$, then α is called *integral* (over $\mathbb{Z}$), if it satisfies a monic polynomial with integer coefficients. Since α satisfies its reduced characteristic polynomial of degree 2, so it is integral if and only if $\mathrm{trd}(\alpha), \mathrm{nrd}(\alpha) \in \mathbb{Z}$. In a number field, the most important order in K is the ring of integers, which is the unique maximal order (under containment). Unfortunately, this is not true in the noncommutative setting: if $\mathcal{O} \subset \mathcal{A}$ is a maximal order and $\alpha \in \mathcal{A}^*$, then $\alpha\mathcal{O}\alpha^{-1} \subset \mathcal{A}$ is a maximal order and, by noncommutativity, we may have

$\alpha\mathcal{O}\alpha^{-1} \neq \mathcal{O}$.
What has been said above suggests that the model developed in the ordinary case has to be hard to generalized. However, in an appropriate sense, the correspondence can be restored thanks to the maximality of the orders associated to supersingular elliptic curves.

3.5.2 The Endomorphism Ring of a Supersingular Elliptic Curve

The endomorphism ring of a supersingular elliptic curve is an order in a quaternion algebra. We want to prove that it have to be a maximal order, so we try to understand why these orders are so special and we see that, thanks to maximality, it is possible to present the category of supersingular curves in terms of left modules of the endomorphism ring of a fixed curve (whose plays the role of base point).

Theorem 3.5.12. *Let E be a elliptic curve over F and suppose that* $\operatorname{rk}_{\mathbb{Z}} \operatorname{End}(E) = 4$. *Then* $\mathcal{B} = \operatorname{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ *is a quaternion algebra over $\mathbb{Q}$ ramified at* $p = \operatorname{char} F$ *and ∞, and* $\operatorname{End}(E)$ *is a maximal order in B.*

Proof. (Lenstra proof in [Voi18] Theorem 42.1.9.)
Let $\mathcal{O} = \operatorname{End} E \subseteq \mathcal{B} = \operatorname{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$. Let $n > 0$ be prime to p. Then we know that the torsion group is

$$E[n] \simeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$$

as abelian groups and its endomorphism ring is $\operatorname{End}(E[n]) \simeq \mathrm{M}_2(\mathbb{Z}/n\mathbb{Z})$.
We claim that the structure map $\mathcal{O}/n\mathcal{O} \to \operatorname{End} E[n]$ is injective, which is to say, $E[n]$ is a faithful module over $\mathcal{O}/n\mathcal{O}$. Indeed, let us suppose $\phi \in \mathcal{O}$ annihilates $E[n]$, since multiplication by n is separable by Proposition 1.2.13, there exists $\psi \in \mathcal{O}$ such that $\phi = n\psi$, so $\phi \equiv 0 \mod n\mathcal{O}$, proving injectivity. Further, since $\#\mathcal{O}/n\mathcal{O} = \#\operatorname{End} E[n] = n^4$, the structure map is an isomorphism:

$$\mathcal{O}/n\mathcal{O} \xrightarrow{\sim} \operatorname{End} E[n] \tag{3.10}$$

Since $\mathcal{O}$ is a free $\mathbb{Z}$-module, if ℓ is a prime different from p we have

$$\mathcal{O}_\ell = \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell = \mathcal{O} \otimes_{\mathbb{Z}} \varprojlim_n \mathbb{Z}/\ell^n\mathbb{Z} \simeq \varprojlim_n \mathcal{O}/\ell^n\mathcal{O}$$

So, the structure map (3.10) induced the following isomorphism of $\mathbb{Z}_\ell$ algebras:

$$\mathcal{O}_\ell \xrightarrow{\sim} \varprojlim_m \operatorname{End} E[\ell^m] \simeq \mathrm{M}_2(\mathbb{Z}_\ell)$$

In particular, $\mathcal{O}_\ell$ is maximal in $\mathcal{B}_\ell \simeq \mathrm{M}_2(\mathbb{Q}_\ell)$ and $\mathcal{B}$ splits at ℓ. Since $\mathcal{B}$ is definite, it follows from the classification theorem ([Voi18] Theorem 14.1.3) that $\mathcal{B}$ ramifies at p and infinity, so $\mathcal{B}_p$ is a division algebra over $\mathbb{Q}_p$.
To conclude, we show that $\mathcal{O}_p$ is maximal. For $\phi \in \mathcal{O}$ an isogeny, let $\deg_i \phi$ be the inseparable degree of ϕ, which is a power of p. We put $\deg_i 0 = \infty$. The map

$$\nu\colon \mathcal{B} \to \mathbb{Q} \cup \{\infty\}$$

$\nu(a \otimes \psi) = \mathrm{ord}_p(a) + \frac{1}{2}\,\mathrm{ord}_p(\deg_i \phi)$ is well defined, since $\deg_i[p] = \deg[p] = p^2$. Factoring an isogeny into its separable and inseparable parts shows that

$$\mathrm{ord}_p(\deg_i \phi) = \mathrm{ord}_p(\deg \phi) = \mathrm{ord}_p(\mathrm{nrd}\,\phi)$$

so ν is precisely the valuation (3.9) on $\mathcal{B}$ obtained by extending the p-adic valuation on $\mathbb{Q}$. To conclude, we show that $\mathcal{O}_{(p)}$ is the valuation ring associated of $\mathcal{B}_{(p)}$ and is therefore maximal. If $\alpha \in \mathcal{O}_{(p)}$ then $\deg \alpha \in \mathbb{Z}_{(p)}$ so α is in the valuation ring. Conversely, let $\alpha \in \mathcal{B}$ be a rational isogeny with $\nu(\alpha) \geq 0$. We write $\alpha = a \otimes \varphi$ where φ is an isogeny not divisible by any integer, i.e. there not exists n such that $\varphi = \varphi' \circ [n]$. Then $\nu(\alpha) = \mathrm{ord}_p(a) + \nu(\varphi) \geq 0$ and $0 \leq \nu(\varphi) \leq 1/2$, since the multiplication by p is purely inseparable by Theorem 1.5.8. Thus $\mathrm{ord}_p(a) \geq -1/2$ and therefore $a \in \mathbb{Z}_{(p)}$, and hence $\alpha \in \mathcal{O}_{(p)}$. Locally $\mathcal{O}$ is maximal so, by Proposition 3.5.10, the thesis is proved. □

For ordinary curves we proved that the isogeny graph has a precise nice form. We saw that fractional proper ideals act as horizontal isogeny. In the non commutative case we must distinguish between left or right ideals, and, for example, the product of two right $\mathcal{O}$-ideals could not be again a right $\mathcal{O}$-ideal. To address this, for lattices $I, J \subset \mathcal{B}$, we say that I is *compatible* with J if the right order of I is equal to the left order of J, so that what comes between I and J in the product IJ matches up. A lattice $I \subset \mathcal{B}$ is *right invertible* if there exists a lattice $I' \subset \mathcal{B}$ such that $II' = \mathcal{O}_L(I)$ with a compatible product, and we call I a *right inverse*. We similarly define notions on the left.
We say $I \subset \mathcal{B}$ is *invertible* if there is a two-sided inverse $I' \subset \mathcal{B}$, i.e.

$$II' = \mathcal{O}_L(I) = \mathcal{O}_R(I') \;\text{ e }\; I'I = \mathcal{O}_L(I') = \mathcal{O}_R(I).$$

If a lattice I has a two-sided inverse, then this inverse is uniquely given by

$$I^{-1} \coloneqq \{\alpha \in \mathcal{B} : I\alpha I \subseteq I\}\,.$$

A *left fractional* $\mathcal{O}$-ideal is a lattice I such that $\mathcal{O} \subset \mathcal{O}_L(I)$; similarly on the right.
Maximal order in number field are Dedekind domain and fractional ideal are all invertible. Similarly lattices which are $\mathcal{O}$-ideal of a maximal order are invertible:

Proposition 3.5.13. *Let $\mathcal{O} \subseteq \mathcal{B}$ be a maximal order. Then a left or right fractional $\mathcal{O}$-ideal is invertible.*

The simplest kind of invertible lattices are the *principal* lattices $I = \mathcal{O}_L(I)\alpha = \alpha\mathcal{O}_R(I)$ with $\alpha \in \mathcal{B}^*$: its inverse is $I^{-1} = \alpha^{-1}\mathcal{O}_L(I) = \mathcal{O}_R(I)\alpha^{-1}$. An important result is that, for a lattice in $\mathcal{B}$, being left-invertible or right-invertible or locally principal is equivalent.
Here, we make a choice to consider lattices as right modules. We say that lattices I, J are in the same *right class* $[I]_R$, if there exists $\alpha \in \mathcal{B}^*$ that $\alpha I = J$ and

$$\mathrm{Cls}_R(\mathcal{O}) \coloneqq \{[I]_R \mid I \subset \mathcal{B} \text{ invertible and } \mathcal{O}_R(I) = \mathcal{O}\}$$

the *right class set* is well defined. Unfortunately, the class set does not have the structure of a group. However, it is a groupoid and it has been proved that it is generated by a finite set of ideals with bounded norm ([Voi18] Proposition

17.5.6).

An easy consequence of the Theorem 3.1.1 is that two supersingular elliptic curves are isogenous. Indeed, suppose E_1 is defined over a finite field $\mathbb{F}_q$ and it has all of its endomorphisms defined over $\mathbb{F}_q$. Let $\pi \in \mathcal{O} = \operatorname{End}(E_1)$ be the q-power Frobenius endomorphism. Then $\mathcal{B} = \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q}$ is a quaternion algebra over $\mathbb{Q}$. Since $\operatorname{End}(E_1)$ is defined over $\mathbb{F}_q$, the endomorphism π commutes with every isogeny $\alpha \in \mathcal{O}$ and so π lies in the center of $\mathcal{O}$; since the center is $\mathbb{Q}$, we have $\pi \in \mathbb{Z}$. But $\deg \pi = q$ so $\pm\sqrt{q} \in \mathbb{Z}$. Therefore, by Theorem 1.5.4 the roots of minimal the polynomial of π are $\alpha = \beta = \pm\sqrt{q}$ and the frobenius is $\mp 2\sqrt{q}$; then by Theorem 1.5.7

$$\#E_1(\mathbb{F}_{q^2}) = q^2 + 1 \mp 2\sqrt{q}$$

and, since $\alpha^2 = \beta^2 = q$,

$$\#E_1(\mathbb{F}_{q^2}) = q^2 + 1 - 2q = (q-1)^2.$$

Given another supersingular curve E_2 we may repeat the above argument over a common larger extension field $\mathbb{F}_q$ to conclude that $\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q)$. It follows that E_1, E_2 are isogenous over $\mathbb{F}_q$.
By the way, given two any supersingular elliptic curves E_1 and E_2 its possible to read $\operatorname{Hom}(E_1, E_2)$ in terms of the endomorphism ring of each curve.

Proposition 3.5.14. *Let E_1, E_2 be supersingular elliptic curves over $\bar{\mathbb{F}}_q$. Then* $\operatorname{Hom}(E_1, E_2)$ *is a $\mathbb{Z}$-module of rank 4 that is invertible as a right* $\operatorname{End}(E_1)$*-module under precomposition and a left* $\operatorname{End}(E_2)$*-module under postcomposition.*

Proof. We may suppose E_1, E_2 defined over $\mathbb{F}_q$. By Theorem 3.1.2

$$\operatorname{rk}_{\mathbb{Z}} \operatorname{Hom}(E_1, E_2) = 4.$$

As in the proof of Theorem 3.1.1, we have that $\operatorname{Hom}(E_1, E_2)$ is a torsion free $\mathbb{Z}$-module with right action by $\mathcal{O}_1 := \operatorname{End}(E_1)$. Let $\psi \in \operatorname{Hom}(E_1, E_2)$ different from zero and $\hat{\psi}$ the dual isogeny. $I = \hat{\psi} \operatorname{Hom}(E_1, E_2) \subset \mathcal{O}_1$ is an integral right ideal; since $\mathcal{O}$ is a maximal order by Theorem 3.5.12, I is necessarily invertible by Proposition 3.5.13. The same then holds for $\operatorname{Hom}(E_1, E_2)$ as a right $\mathcal{O}_1$-module. Similarly we obtain that left $\operatorname{End}(E_2)$-module under postcomposition. □

We say that $\mathcal{O}$ is *connected* to $\mathcal{O}'$ if there exists a locally principal fractional ideal for both the orders $J \subseteq \mathcal{B}$, called a *connecting ideal.* Thus we have already proved that endomorphism ring of supersingular elliptic curves are connected. The relation of being connected is an equivalence relation on the set of orders in $\mathcal{B}$ and it is a remarkable property due to the fact that if $\mathcal{O}$ is connected to $\mathcal{O}'$ then $\operatorname{Cls}(\mathcal{O}) \simeq \operatorname{Cls}(\mathcal{O}')$.

Now, let us fix E a supersingular elliptic curve such that $\mathcal{O} = \operatorname{End}(E)$ an order in the quaternion algebra $\mathcal{B}$ over $\mathbb{Q}$. By Theorem 3.5.12, $\mathcal{O}$ is maximal. Let I be a nonzero integral left $\mathcal{O}$-ideal. Since $\mathcal{O}$ is maximal, necessarily I is locally principal (in particular, invertible). We define, as in the ordinary case, $E[I] \subseteq E$: if there is a nonzero $\alpha \in I$ giving a (separable) isogeny $\alpha \colon E \to E$, then

$$E[I](\bar{\mathbb{F}}_q) = \left\{P \in E(\bar{\mathbb{F}}_q) \colon \alpha(P) = O \ \forall \alpha \in I\right\} \neq \{O\}.$$

We can also define the (separable) isogeny $\phi_I : E \to E/E[I]$ with $\ker(\phi_I) = E[I]$ and $\# \ker \phi_I = \deg \phi_I$.

Lemma 3.5.15. *Let E be a supersingular elliptic curve such that $\mathcal{O} = \operatorname{End}(E)$ an order in the quaternion algebra $\mathcal{B}$ over $\mathbb{Q}$. Let I be a nonzero integral left $\mathcal{O}$-ideal. Then the map*

$$\begin{array}{cccc} \phi_I^* \colon & \operatorname{Hom}(E_I, E) & \to & I \\ & \psi & \mapsto & \psi\phi_I \end{array}$$

is an isomorphism of $\mathcal{O}$-left modules.

Proof. The image of $\operatorname{Hom}(E_I, E)$ under precomposition by ϕ_I lands in $\operatorname{End}(E) = \mathcal{O}$ and factors through ϕ_I so lands in I by definition. The map ϕ_I^* is an injective homomorphism of abelian groups. It compatible with the left $\mathcal{O}$-action, given by postcomposition on $\operatorname{Hom}(E_I, E)$ and left multiplication on I. To conclude, we show it is also surjective. If $\alpha \in I$, then $\alpha(E[I]) = O_E$ by construction. If α is also separable, then it factors through $\phi_I : E \to E_I$ by Proposition 1.2.10.3. In general, we can reduce ourselves at separable case using Proposition 1.2.6. □

Proposition 3.5.16. *The map $\iota \colon \operatorname{End}(E_I) \to \mathcal{B}$ given by*

$$\iota(\beta) = \frac{1}{\deg \phi_I}(\hat{\phi}_I \beta \phi_I)$$

is injective and $\iota(\operatorname{End}(E_I)) = \mathcal{O}_R(I)$.

Proof. Note that in $\mathcal{B}$

$${\phi_I}^{-1} = \frac{\hat{\phi}_I}{\deg \phi_I}$$

The thesis follow directly from the previous lemma. In fact ι defines the induced action on I by right multiplication. Giving an inclusion $\iota(\operatorname{End}(E_I)) \subset \mathcal{O}_R(I)$. For maximality the equality must hold. □

Exactly as in the ordinary case:

Lemma 3.5.17. *If $J = I\beta \subset \mathcal{O}$ with $\beta \in \mathcal{B}^*$, then $E_I \simeq E_J$.*

So far, we have shown how to pass from classes of left $\mathcal{O}$-ideals to (isogenous) supersingular elliptic curves via kernels. We can also go in the other direction. Given a finite subgroup $H < E$, we define

$$I(H) := \{\alpha \in \mathcal{O} \colon \alpha(P) = O \ \forall P \in H\} \subsetneq \mathcal{O}$$

then $I(H)$ is a left $\mathcal{O}$-ideal, nonzero because $\#H \in I(H)$.
If $H_1 \subseteq H_2 \subseteq E$ are two such subgroups, then $I(H_1) \supseteq I(H_2)$.

Lemma 3.5.18. *If $H_1 \subseteq H_2$ and $I(H_1) = I(H_2)$, then $H_1 = H_2$.*

Proof. Let $\phi_1 \colon E \to E/H_1$. We can suppose that ϕ_1 is separable, and let $n = \#H_2$. By the proof of Theorem 3.5.12, the structure map $\mathcal{O}/n\mathcal{O} \to \operatorname{End} E[n]$ is faithful. So if $H_2 > H_1$, then there exists $\alpha \in \mathcal{O}$ such that $\alpha(H_1) = \{O\}$ but $\alpha(H_2) \neq \{O\}$, so $I(H_2) \neq I(H_1)$. □

Voight in [Voi18]§42, using specific properties of orders in quaternion algebra, proves that

$$\deg \phi_I = \operatorname{nrd}(I) \tag{3.11}$$

and

$$I(E[I])$$

We can now show that for each maximal order we can explicitly find an elliptic curve with endomorphism ring isomorphic to it:

Proposition 3.5.19. *For every isogeny $\phi\colon E \to E'$, there exists a left $\mathcal{O}$-ideal I and an isomorphism $\mu\colon E_I \to E'$ such that $\phi = \mu\phi_I$. In particular, for every maximal order $\mathcal{O}' \subset \mathcal{B}$, there exists E such that $\mathcal{O}' \simeq \operatorname{End}(E')$.*

Proof. Let H be the kernel of ϕ. Then $H \subseteq E[I(H)]$, so $\phi_I(H)$ factors through ϕ with $\phi_{I(H)} = \mu\phi$ for some isogeny $\mu\colon E_{I(H)} \to E$. However, $I(H) = I(E[I(H)])$, so $H = E[I(H)]$ by Lemma 3.5.18. Thus $\deg \phi_{I(H)} = \deg \phi$, and so $\deg \mu = 1$ and μ is an isomorphism, with $\phi = \mu^{-1}_{I(H)}$. The second statement follows similarly. □

Lemma 3.5.15 can be generalized:

Lemma 3.5.20. *Let $I, J \subseteq \mathcal{O}$ be nonzero integral left $\mathcal{O}$-ideals. Then the natural map*

$$\operatorname{Hom}(E_I, E)\operatorname{Hom}(E_J, E_I) \to \operatorname{Hom}(E_J, E)$$

is bijective.Furthermore, the induced maps

$$\begin{array}{ccc} \operatorname{Hom}(E_J, E_I) & \to & (I\colon J)_R = I^{-1}J \\ \phi & \to & {\phi_I}^{-1}\psi\phi_I \end{array}$$

is a bijection, too.

Proof. By Lemma 3.5.15, we have $\operatorname{Hom}(E_I, E)\phi_I = I$. Let $m = \deg \phi_I = \operatorname{nrd}(I)$. The left ideal $I \subseteq \mathcal{O}$ is invertible thus $m = \operatorname{nrd}(I) \in I\bar{I}$, hence there exist finitely many $\alpha_i, \beta_i \in \operatorname{Hom}(E_I, E)$ such that

$$[m] = \sum_i (\alpha_i\phi_I)\widehat{(\beta_i\phi_I)} = \sum_i \alpha_i\phi_I\hat{\phi}_I\hat{\beta}_i = \sum_i \alpha_i[m]\hat{\beta}_i$$

therefore

$$[1] = \sum_i \alpha_i\hat{\beta}_i \in \operatorname{End}(E)$$

For $\psi \in \operatorname{Hom}(E_I, E)$, postcomposing with the previous equation gives

$$\psi = \sum_i \alpha_i(\hat{\beta}_i\psi) \in \operatorname{Hom}(E_I, E)\operatorname{Hom}(E_J, E_I)$$

so the natural injective map is bijective. This gives

$$I({\phi_I}^{-1}\operatorname{Hom}(E_J, E_I)\phi_J) = J$$

and the bijective map we wanted. □

Merging all these results, we finally obtain a correspondence for the supersingular elliptic curves:

Theorem 3.5.21. *Let E_0 be a supersingular elliptic curve over $\bar{\mathbb{F}}_q$. Let $\mathcal{O}_0 = \mathrm{End}(E_0)$ and $\mathcal{B} = \mathcal{O}_0 \otimes \mathbb{Q}$. The association $\rho_E \colon E \to \mathrm{Hom}(E, E_0)$ is functorial and it defines an equivalence between the category of $\mathcal{ELL}_{\mathbb{F}_q}(\mathcal{O})$, under isogenies, and invertible left $\mathcal{O}_0$-modules, under left $\mathcal{O}_0$-modules homomorphism.*

Proof. To begin, we need to show $\rho := \mathrm{Hom}(\_, E_0)$ is a functor. The association ρ_E makes sense on objects by Proposition 3.5.14. On morphisms, to an isogeny $\phi \colon E \to E$ we associate

$$\begin{array}{cccc} \phi^* \colon & \mathrm{Hom}(E, E_0) & \to & \mathrm{Hom}(E, E_0) \\ & \psi & \mapsto & \psi\phi \end{array}$$

The map ϕ^* is a homomorphism of left $\mathcal{O}_0$-modules and, since it is compatible with postcomposition with $\mathcal{O}_0$, ρ is functorial.
A functor is an equivalence of category if it is full, faithful and essentially surjective. We claim that ρ is essentially surjective. Let I be an invertible left $\mathcal{O}_0$-module. We know that, tensoring with $\mathbb{Q}$, we get an injection $I \to I \otimes_{\mathbb{Q}} \mathcal{B}$, so up to isomorphism of left $\mathcal{O}_0$-modules, we may suppose $I \subseteq \mathcal{B}$. Scaling by an integer, we may suppose $I \subset \mathcal{O}_0$ is a left $\mathcal{O}_0$-ideal. Let $E_I = E/E[I]$. By Lemma 3.5.15, we have $\mathrm{Hom}(E_I, E_0) \simeq I$ as left $\mathcal{O}_0$-modules, as desired.
Finally, we show that ρ is fully faithful. By Proposition 3.5.19, there is a left $\mathcal{O}_0$-ideals I such that $E \simeq E_{0,I}$; applying this isomorphism, we may suppose without loss of generality that $E = E_{0,I}$. Then by Lemma 3.5.15, we have $I = \mathrm{Hom}(E_{0,I}, E_0)\phi_{0,I}$. Similarly can done with E and J . Then after these identifications, we are reduced to the setting of Lemma 3.5.20:

$$\begin{array}{ccc} \mathrm{Hom}(E_{0,I}, E_{0,J}) & \to & (I \colon J)_R = I^{-1}J \\ \phi & \to & {\phi_{0,I}}^{-1}\psi\phi_{0,I} \end{array}$$

which we know is bijective (note R is for right). □

We just proved that we can study the isogenies between supersingular curves in terms of special ideals in maximal orders of quaternion algebra, in particular by Lemma 3.5.15 we saw that a crucial role in this reduction is played by left ideals. We also noted that finding an isogeny between two supersingular elliptic curves E_1 and E_2, whose endomorphism rings are respectively $\mathcal{O}_1$ and $\mathcal{O}_2$, is equivalent to find an module I such that it is a left $\mathcal{O}_1$-ideal and right $\mathcal{O}_2$-ideal. This restores the algebraic correspondence ideals and isogenies.

For practical applications it useful to have an explicit representation of the connecting module, so we are going to show how to produce it. Now suppose that $\mathcal{O}$ is any maximal order in the quaternion algebra $\mathcal{B}$ ramified at p and ∞. We recall that the reduced norm of a left ideal I satisfies

$$\mathrm{nrd}(I) = \gcd(\{\mathrm{nrd}(\alpha) \mid \alpha \in I\})$$

and $\mathrm{nrd}(I)\mathcal{O} = I\bar{I}$. If I and J are left $\mathcal{O}$-ideals, a homomorphism of I to J is a map $\alpha \mapsto \alpha\gamma$ given by $\alpha \in \mathcal{B}^*$, which is an isomorphism if $J = I\gamma$. We can define

$$\begin{array}{cccc} q_I \colon & I & \longrightarrow & \mathbb{Z} \\ & \alpha & \longmapsto & \frac{\mathrm{nrd}(\alpha)}{\mathrm{nrd}(I)} \end{array} \tag{3.12}$$

Lemma 3.5.22. *Let I be a left $\mathcal{O}$-ideal of reduced norm N and α an element in I. Then $I\gamma$, where $\gamma = \bar{\alpha}/N$, is a left $\mathcal{O}$-ideal of norm $q_I(\alpha)$.*

Proof. By the multiplicativity of the reduced norm, and $\operatorname{nrd}(\alpha) = \operatorname{nrd}(\bar{\alpha})$, we have

$$\operatorname{nrd}(\gamma I) = \operatorname{nrd}(\gamma) \operatorname{nrd}(I) = N \frac{\operatorname{nrd}(\alpha)}{N^2} = \frac{\operatorname{nrd}(\alpha)}{N^2} = q_I(\alpha)$$

Clearly I is a fractional left $\mathcal{O}$-ideal, so it remains to show that $I\gamma \subseteq \mathcal{O}$. Since $\mathcal{O}\alpha \subseteq I$ we have $\bar{\alpha} \subseteq \bar{I}$ and hence $I\bar{\alpha} \subseteq I\bar{I} = N\mathcal{O}$. Then $I\gamma \subseteq \mathcal{O}$. □

Consequently, since the norm correspond to degree of the induce isogeny this lemma means that we can simply reduce the latter in to applications. It is also possible to explicitly find a connecting ideal between two given maximal orders. The proof of this fact involves another family of orders:

Definition 3.5.23. An *Eichler* order $\mathcal{O} \subseteq \mathcal{B}$ is the intersection of two (not necessarily distinct) maximal orders.

By the local-global dictionary for lattices (and orders), the property of being an Eichler order is local. In general the *discriminant* of $\mathcal{B}$ to be the product $\operatorname{disc}\mathcal{B}$ of primes that ramify in $\mathcal{B}$, so $\operatorname{disc}\mathcal{B}$ is a squarefree positive integer. In our case $\operatorname{disc}\mathcal{B} = p$. Since $\mathcal{O}$ is a lattice the $\operatorname{disc}\mathcal{O}$ is the determinant of the matrix of the reduced traces. The order

$$\begin{bmatrix} \mathbb{Z}_q & \mathbb{Z}_q \\ q^e & \mathbb{Z}_q \end{bmatrix} \subseteq \mathrm{M}_2(\mathbb{Z}_q)$$

is called the *standard Eichler order of level* q^e in $\mathrm{M}_2(\mathbb{Q}_q)$. It can be proved that $\mathbb{Z}_q$-order $\mathcal{O}_q \subseteq \mathrm{M}_2(\mathbb{Q}_q)$ is an Eichler order if $\mathcal{O}_q$ is isomorphic to a standard Eichler order. Globally, we say $\mathcal{O} \subset \mathcal{B}$ is a Eichler order of *level* M if $\sqrt{\operatorname{disc}(\mathcal{O})} = N = DM$ with $\gcd(D, M) = 1$ and $\mathcal{O}_q$ is an Eichler order of level q^e for all $q^e || M$. In particular, $\mathcal{O}_q$ is maximal at all primes $q \mid D$. A maximal $\mathbb{Z}_q$-order $\mathcal{O}_q \subseteq \mathrm{M}_2(\mathbb{Z}_q)$ is an Eichler order of level $1 = q^0$.

Lemma 3.5.24. *Suppose that $\mathcal{O}_1$ and $\mathcal{O}_2$ are given maximal orders in B. Then the Eichler order $\mathcal{O}_1 \cap \mathcal{O}_2$ has the same index in each of $\mathcal{O}_1$ and $\mathcal{O}_2$, which we denote M. Let*

$$I(\mathcal{O}_1, \mathcal{O}_2) := \{\alpha \in \mathcal{B} \colon \alpha\mathcal{O}_2\bar{\alpha} \subseteq M\mathcal{O}_1\}$$

be a left $\mathcal{O}_1$-ideal and right $\mathcal{O}_2$-ideal of reduced norm M. Conversely, if I is a left $\mathcal{O}_1$-ideal with right order $\mathcal{O}_2$, such that $I \not\subseteq n\mathcal{O}_1$ for any $n > 1$, then $I = I(\mathcal{O}_1, \mathcal{O}_2)$.

Proof. The first part of the proposition is a classical result regarding Eichler. $I(\mathcal{O}_1, \mathcal{O}_2)$ is a left $\mathcal{O}_1$-module and right $\mathcal{O}_2$-module by construction. Let us recall that for all $\alpha \in \mathcal{B}$

$$\alpha^{-1} = \frac{\overline{\alpha}}{\operatorname{nrd}(\alpha)}.$$

Locally at any prime q, there exists a connecting principal ideals $\mathcal{O}_1$ and $\mathcal{O}_2$ are maximal $\mathbb{Z}_q$-orders such that $\mathcal{O}_1 = \alpha\mathcal{O}_2\alpha^{-1}$, for some $\alpha \in \mathcal{O}_1$ hence also in $\mathcal{O}_2$. Let us remove any integer factors (in the center), the reduced norm of a minimal $\alpha \in \mathcal{O}_1 \cap \mathcal{O}_2$ must be equal the level M at q. Hence

$$\alpha\mathcal{O}_2\alpha^{-1} = \alpha\mathcal{O}_2\frac{\overline{\alpha}}{\operatorname{nrd}(\alpha)} = \mathcal{O}_1$$

and so $\alpha \in I(\mathcal{O}_1, \mathcal{O}_2)$. The global result follows from the local-global principle Theorem 3.5.7. Conversely, since any left $\mathcal{O}_1$-ideal I is locally principal at each prime q, one can find locally α such that $I = \mathcal{O}_1\alpha$; the right order of I is then $\mathcal{O}_1 = \alpha\mathcal{O}_2\alpha^{-1}$. By hypothesis α is not divisible by any integer and we conclude that the Eichler order has level $\mathrm{nrd}(\alpha) = \mathrm{nrd}(I) = M$. From the above construction in terms of a local generator, we conclude $I = I(\mathcal{O}_1, \mathcal{O}_2)$. □

3.6 Expander Graphs

Using random walk on the isogeny graphs is a possible approach to solve the problem of finding an isogeny, but a priori we have no information of how much efficient it is. In this section, we show that isogeny graphs have good properties in this sense.

Let $G = (V, E)$ an undirected graph. The *neighbors* N of a vertex $v \in V$ is the set of the vertices of V connected to it by an edge, in particular is of the form $\{w \in V \mid \{v, w\} \in E\}$. A *path* between two vertices v, w is a sequence of vertices $(v_1 = v, \dots, v_i, \dots, v_t = w)$ such that each $\{v_n, v_{n+1}\} \in E$. The *distance* between two vertices is the length of the shortest path between them; if there is no such path, the vertices are said to be *at infinite* distance. The *diameter* of a connected graph is the largest of all distances between its vertices and the *degree* of a vertex is the number of edges pointing to (or from) it; a graph where every edge has degree k is called *k-regular.* Note that for symmetry we directly obtain:

Proposition 3.6.1. *Let K a imaginary quadratic field and ℓ an Elkies prime. Suppose $\#\mathcal{ELL}_{\mathbb{F}_q}(\mathcal{O}_K)$ is prime number. Then the associated ℓ-isogeny graph of is a 2-regular graph.*

Usually, a graph is represented by a matrix:

Definition 3.6.2. The *adjacency matrix* of a graph G with vertex set $V = \{v_1, \dots, v_n\}$ and edge set E, is the $n \times n$ matrix where the (i, j)-th entry is 1 if there is an edge between v_i and v_j, and 0 otherwise.

Remark 3.6.3. If a graph is undirected, its adjacency matrix is symmetric. Thus it has n real eigenvalues $\lambda_1 \geq \dots \geq \lambda_n$.

Proposition 3.6.4. *If G is a k-regular graph, then its largest and smallest eigenvalues λ_1, λ_n satisfy $k = \lambda_1 \geq \dots \geq \lambda_n \geq -k$.*

If G is a k-regular graph constant vectors are eigenvector of the adjacency matrix with eigenvalue k, which for obvious reasons is called the trivial eigenvalue λ_{triv}. A family of such graphs are called a sequence of expander graphs if all other eigenvalues of their adjacency matrices are bounded away from λ_{triv} by a fixed amount:

Definition 3.6.5. Let $\varepsilon > 0$ and $k \geq 1$. A k-regular graph is called a ε-*expander* if

$$\lambda_2 \leq (1 - \varepsilon)k$$

and a *two-sided ε-expander* if it also satisfies

$$\lambda_n \geq -(1 - \varepsilon)k$$

A sequence $G_i = (V_i, E_i)$ of k-regular graphs with $\#V_i \to \infty$ is said to be a one-sided (resp. two-sided) *expander family* if there is an $\varepsilon > 0$ such that G_i is a one-sided (resp. two-sided) ε-expander for all sufficiently large i.

Note that being ε-expander means that no other eigenvalue is equal to k and also this implies the graph is connected.

Now, we want to prove that:

Theorem 3.6.6. *Let $\mathbb{F}_q$ be a finite field and let $\mathcal{O} \subset K$ be an order in a quadratic imaginary field. Let G be the graph which vertices are elliptic curves over $\mathbb{F}_q$ with complex multiplication by $\mathcal{O}$, and which edges are horizontal isogenies of prime degree bounded by $(\log 4q)^B$ for some fixed $B > 2$. Assume that G is non-empty. Then, under the Generalized Riemann hypothesis, G is a regular graph and there exists an ε, independent of $\mathcal{O}$ and q, such that G is a ε-expander.*

The main idea of this proof is considering, up to correspondences, the Schreier graph $G = (S, \mathcal{ELL}_{\mathbb{F}_q}(\mathcal{O}))$ where S a symmetric subset of $\mathrm{Cl}(\mathcal{O})$ and prove that G is an expander graph if and only if S generates $\mathrm{Cl}(\mathcal{O})$. The last equivalence is based on an important result by Jao, Miller and Venkatesan of 2009 in [JMV09]. Note that since their theorem holds under Generalized Riemann Hypothesis (GHR) that this assumption we will often appear in next chapters.
First of all, we state and prove an analogue of Theorem 3.6.6 over the complex numbers.

Theorem 3.6.7. *Let $\mathcal{O} \subset K$ be an order in a quadratic imaginary field with discriminant D of the Frobenius map. Let G be the graph whose vertices are elements of $\mathcal{ELL}_{\mathbb{C}}(\mathcal{O})$ and whose edges are isogenies of prime degree less than some fixed bound $M \geq (\log|D|)^B$, for some absolute constant $B > 2$. Then, assuming GRH, the graph G is an expander graph.*

Proof sketch. We have seen that the elements of $\mathcal{ELL}_{\mathbb{C}}(\mathcal{O})$ are in bijection with the elements of the group $\mathrm{Cl}(\mathcal{O})$, and that the action of $\mathrm{Cl}(\mathcal{O})$ on $\mathcal{ELL}_{\mathbb{C}}(\mathcal{O})$ defined by equation 3.4 coincides exactly with the translation action of the class group on itself under this bijection. Moreover, for Corollary 3.4.19 isogenies of prime degree less than M correspond to integral ideals of prime norm less than M, and the inverses (i.e. complex conjugates) of these ideals have the same prime norm and thus also yield such isogenies. Hence, the graph G is isomorphic to the Schreier graph $(S, \mathrm{Cl}(\mathcal{O}))$ were S is the set consisting of ideals of prime norm less than $M \geq (\log|D|)^B$. By this equivalence we can directly apply Theorem 1.1 of [JMV09].

□

Using Deuring correspondence we can prove our statement:

Proof sketch (Proof of Theorem 3.6.6). Observe that $(\log 4q)^B \geq (\log(|D|)^B$, since $D = t^2 - 4q$ where the trace t satisfies the Hasse bound $|t| < 2\sqrt{q}$. Hence $(\log 4q)^B$ satisfies the condition for M in theorem 3.6.7. We will now show that the graph G in Theorem 3.6.6 is isomorphic to the graph defined in Theorem 3.6.7. It holds that all elliptic curves in $\mathcal{ELL}_{\mathbb{C}}(\mathcal{O})$ are defined over a determined $H \subset \overline{\mathbb{Q}}$. Hence the identification of the vertices is accomplished by choosing a appropriate place $\mathfrak{p} \subseteq H$ lying over the characteristic p of $\mathbb{F}_q$, and reducing

curves in $\mathcal{ELL}_{\mathbb{C}}(\mathcal{O})$ to obtain an ordinary curve over $\mathbb{F}_q$. Theorem 1.7.1 shows that this identification is surjective. To show that it is injective, consider two non isomorphic curves E_I and E_J in $\mathcal{ELL}_{\mathbb{C}}(\mathcal{O})$, i.e. I and J are not in the same class. By the Chebotarev density theorem[3], there exists an unramified prime ideal F belonging to the same ideal class as IJ^{-1}; note in particular that F can not be principal. This ideal induces an isogeny $\phi\colon E_I \to E_J$ of degree $\mathrm{N}(F)$. If the reductions $\bar{E}_I$ and $\bar{E}_J$ of E_I and E_J modulo $\mathfrak{p}$ would be isomorphic, then $\bar{\phi}$ would represent an endomorphism of $\bar{E}_I$ of degree $\mathrm{N}(F)$. However, we know the endomorphism ring of $\bar{E}_I$ is equal to $\mathcal{O}$, and no element of $\mathcal{O}$ has norm equal to $\mathrm{N}(F)$, since $\mathbb{Q}(\sqrt{D})$ is a quadratic imaginary field[4]. Thus the endomorphism ring $\mathcal{O}$ can not contain any endomorphism of such degree.
Likewise, for each prime $\ell < (\log 4q)^B$ the reduction map modulo $\mathfrak{p}$ sends every isogeny of degree ℓ in characteristic 0 to an isogeny of degree ℓ in characteristic p. All isogenies in characteristic p are obtained in this way, since isogenies of degree ℓ are given by the roots of the modular polynomial $\Phi_\ell(X, Y)$ and this polynomial does not have more roots over the algebraic closure in characteristic p than in characteristic 0.

□

Remark 3.6.8. The strategy of the last proof is quite standard. We will see in next chapters that other facts can be showed by considering the complex case and then reducing modulo p, by Deuring correspondence.

Moreover, it can be proved that the diameter of an expander graph is at most logarithmic in the number of nodes.

Charles and Lauter in [CLG09] proved that supersingular isogeny graphs are special type of expander:

Theorem 3.6.9. *Let $k \geq 1$, and let G_i be a sequence of k-regular graphs. Then*

$$\max(|\lambda_2|, |\lambda_n|) \geq 2\sqrt{k-1} - o(1),$$

as $n \to \infty$. A graph such that $|\lambda_i| \leq 2\sqrt{k-1}$ for any λ_i except for λ_1 is called a Ramanujan graph.

Theorem 3.6.10 ([CLG09]). *Let p, ℓ be distinct primes. The ℓ-isogeny graph of supersingular curves in $\overline{\mathbb{F}}_p$ is connected, $\ell + 1$ regular and has the Ramanujan property.*

The Ramanujan property characterizes the optimal separation between the two largest eigenvalues of the graph adjacency matrix and implies the expansion property.
Expanders graph are largely use in application, in particular a classical results is that the diameter of an expander is bounded by $O(\log n)$ in numbers of nodes, where the constant depends only on k and ε. A *random walk* of length i is a path $(v_1, \ldots, v_i)$, defined by the random process that selects v_i uniformly at random among the neighbors of v_{i-1} . A classical result for expander graphs is that random walks of length close to its diameter terminate on any vertex with probability close to uniform:

[3] See [Cox97]§8.

[4] See [Cox97]§9.

Theorem 3.6.11 (Mixing Theorem)**.** *Let $G = (V, E)$ be a k-regular two-sided ε-expander. Let $S \subset V$ be any subset of the vertices of G, and let v be any vertex in V. Then a random walk of length at least*

$$\frac{\log(2\#V/(\#S)^{1/2})}{\log(1-\varepsilon)}$$

starting from v will land in S with probability at least $\#S/2\#V$. Such length is called the mixing length *of the expander graph.*

Corollary 3.6.12. *Let $\mathbb{F}_q$ be a finite field and let $\mathcal{O} \subset K$ be an order in a quadratic imaginary field. Let $G = (V, E)$ be the graph which vertices are elliptic curves over $\mathbb{F}_q$ with complex multiplication by $\mathcal{O}$, and which edges are horizontal isogenies of prime degree bounded by $(\log 4q)^B$ for some fixed $B > 2$. Assume that G is non-empty. Then, under the generalized Riemann hypothesis, there exists a positive constant C with the following property: for q sufficiently large, a random walk of length*

$$t \geq C\frac{\log(\#V)}{\log\log q}$$

from any starting vertex lands in any fixed subset $S \subset V$ with probability at least $\frac{\#S}{2\#V}$.

Proof. If we prove that $\log(1-\varepsilon)$ is bounded below by a constant (depending on B) times $\log\log q$ once q is sufficiently large, the thesis holds for the mixing theorem. ε depends on $k = \lambda_{triv}$ and on a bound c such that $|\lambda| < c$ for each λ in the set of eigenvalues of the adjacency matrix of G. It is shown in [JMV09] that we can take $1 - \varepsilon = k/c$ and so we have

$$\frac{\log(2\#V/(\#S)^{1/2})}{\log(1-\varepsilon)} \leq \frac{\log(2\#V/(\#S)^{1/2})}{\log(k/c)} \tag{3.13}$$

$\log(\lambda_{triv}) \gg B\log\log q$. □

Similar arguments imply also the following fact:

Corollary 3.6.13. *Let $\mathbb{F}_q$ be a finite field of characteristic p. Let $\ell \neq p$ a prime and $G = (V, E)$ the supersingular ℓ-isogeny graph. Let c be a constant such that $|\lambda| < c$ for each λ eigenvalue of the adjacency matrix of G. Then, under the generalized Riemann hypothesis, there exists a positive constant C such that for q sufficiently large, a random walk of length*

$$t \geq C\frac{\log(2\#V/(\#S)^{1/2})}{\log((\ell+1)/2\sqrt{\ell})}$$

from any starting vertex lands in any fixed subset $S \subset V$ with probability at least $\frac{\#S}{2\#V}$.

Proof. By Theorem 3.6.10, we can replace in (3.13) $k = \ell + 1$ and $c = 2\sqrt{\ell}$. □

Chapter 4

A Quantum Approach to General Isogeny Problem

Problem 6 (General Isogeny Problem). *Let $\mathbb{F}_q$ be a finite field and $j_1, j_2 \in \mathbb{F}_q$. Find, if it exists, an isogeny $\phi\colon E_1 \to E_2$ between two elliptic curves E_1, E_2 over $\mathbb{F}_q$ such that $j(E_i) = j_i$ for $i = 1, 2$.*

The hardness of General Isogeny Problem is crucial to the security of the cryptosystems based on isogenies between elliptic curves over finite field. In chapter 2, we saw how quantum computation has undermined the security of many classical cryptosystems and in particular as protocols, whose security was based on factorization and discrete logarithm, are become unsafe by Shor's algorithm (Section 2.2.2). The aim of this chapter is to give a description of the best known algorithms to solve Problem 6, with the purpose of supporting the effectiveness of isogeny based cryptosystems, also in quantum security scope.
Specifically, we describe three main algorithms. First we present a classical, i.e. non quantum, algorithm by Galbraith, Hess and Smart which is particularly important to display because it contains the key ideas from which the later algorithms start. Then we describe two quantum approaches to Problem 6. As for the endomorphism ring's study, we divide the in ordinary and supersingular case. For the first case we have a quantum subexponential time algorithm, while for the latter an exponential algorithm. It is interesting to see how the noncommutativity get complicated the problem and the idea of Biasse, Childs and Sankar to pass over it.

A crucial observation is that isogenies factor into chains. Let E_1 and E_2 be elliptic curves over $\mathbb{F}_q$ and let $\phi\colon E_1 \to E_2$ be a separable isogeny that is defined over $\mathbb{F}_q$. Let us suppose a decomposition of ϕ's degree be

$$\deg \phi = \prod_{i=1}^{k} p_i \cdot n^2$$

with p_i prime and $p_i \neq p_j$. Then $E[n] \subseteq \ker \phi$ and by Proposition 1.2.10.3 there exists an isogeny λ such that $\phi = \lambda \circ [n]$. The kernel of λ can be written, in turn, as product of k cyclic subgroups

$$\langle P_1 \rangle \times \cdots \times \langle P_k \rangle$$

where $P_i \in E[p_i]$. So, we can represent λ as chain of quotient and, since the orders are coprime, we obtain a decomposition

$$\lambda = \prod_{i=1}^{k} \phi_i \quad \text{where} \quad \deg \phi_i = p_i.$$

Thus

$$\phi = \prod_{i=1}^{k} \phi_i \circ n^2 \quad \deg \phi_i = p_i.$$

In practice this means that an isogeny of large degree can be constructed as a composition of isogenies of small prime degree. Moreover, in the ordinary case by the correspondence with class group we are allowed to search for an isogeny of bounded degree and we can represent it by composition of isogenies of low degree.

4.1 Ordinary General Isogeny Problem

Historically, the general isogeny problem was studied in the ordinary case because, often, it was considered in the context of elliptic curve's discrete logarithm problem (ECDLP). Hence, in literature there can be found different algorithms to solve general isogeny problem for ordinary curves. In this section, first, we present a classical algorithm whose structure is the model of the latter quantum algorithm. The idea of these algorithms is to reshape the problem so that tools of number theory could be employed. If two isogenous curves have isomorphic endomorphism ring, the theory developed in the section 3.3 allow us to reword the ordinary general isogeny problem as group action inverse problem:

Problem 7 (Class Group Action Inverse Problem (ClGAIP))**.** *Let $\mathbb{F}_q$ be a finite field and E_1 and E_2 isogenous ordinary elliptic curves defined over $\mathbb{F}_q$. Let $\mathcal{O}$ be their endomorphism ring. Find the ideal class $[I] \in \mathrm{Cl}(\mathcal{O})$ such that $\kappa([I], E_1)$ and E_2 are isomorphic.*

4.1.1 GHS Algorithm

The first classical algorithm to solve the general isogeny problem for ordinary curves is due to Galbraith and proceeds in two steps:

1. Reduce the problem to the case of elliptic curves whose endomorphism ring is maximal.
2. Construct an isogeny between E_1' and E_2'.

Let us note that, since the isogeny graph is connected, to perform step 1 it is enough a find path to a vertex representing a curve whose endomorphism ring is maximal. Galbraith solves step 2 by constructing isogeny trees, see [Gal99]. An improvement to step 2 is given by Galbraith, Hess and Smart [GHS02] where, instead of isogeny trees, the authors use a random walk on the isogeny graph restricted to curves whose endomorphism ring is the maximal order. Let us fix two ordinary elliptic curve E_1 and E_2 over a finite field, whose are known to be isogenous. Let t be the common Frobenius trace, $D = t^2 - 4q$ and $K = \mathbb{Q}(\sqrt{D})$ the imaginary quadratic field which contains their endomorphism rings as orders. We denote by $\mathcal{O}_K$ the maximal order of K, remember the the class number $h(\mathcal{O}_K) \leq \frac{1}{\pi}\sqrt{|D|}\log|D|$. We can summarize the *GHS algorithm* in 4 steps:

Step 1 Reduce to finding an isogeny between two curves whose endomorphism ring is the maximal order $\mathcal{O}_K$.

Step 2 Use a random walk to determine an ideal of $\mathcal{O}_K$ corresponding to an isogeny between the elliptic curves.

Step 3 Smooth the ideal (using ideas from index calculus algorithms for ideal class groups in quadratic fields).

Step 4 Extract an isogeny corresponding to the smooth ideal output by the previous stage.

Let us specifically describe each stage.

Step 1

Note that if the curves have the maximal order as endomorphism ring, Step 1 can be skipped. Let us suppose to have two ordinary curves $E_1/\mathbb{F}_q$ and $E_2/\mathbb{F}_q$ with

$$\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q) = q + 1 - t$$

for $i = 1, 2$. We can perform step 1 using an algorithm by Kohel [Koh96]. The idea is to construct a chain of isogenies from E_i to E_i' where $\mathrm{End}(E_i') = \mathcal{O}_K$ is the maximal order of K. Let f_π the conductor of $\mathbb{Z}[\pi]$ in $\mathcal{O}_K$ and ℓ a prime dividing f_π. Using information in Proposition 3.3.5, we can climb the ℓ-isogeny volcano until the crater[1]. Then, if the curve E_i'' we reach has endomorphism ring $\mathcal{O}_K$ we put $E_i' = E_i''$, otherwise we select another ℓ dividing f_π and we use the same strategy starting form E_i''. The time and space complexity of this step are $\widetilde{O}(c^3)$ and $\widetilde{O}(c^2)$ with c the maximum conductor of $\mathrm{End}(E_i)$. Since c can be as large as $q^{1/2}$ in the worst case, step 1 has expected running time $\widetilde{O}(q^{3/2})$ and space $\widetilde{O}(q)$.

Step 2

We define a random walk on the isogeny graph. More specifically, we consider pairs of the form $(j, [I])$, where j is the j-invariant of some elliptic curve and $[I]$ is an element of the ideal class group of $\mathcal{O}_K$. Let us recall that in previous chapter we show that the class group act over $\mathcal{ELL}_{\mathbb{F}_q}(\mathcal{O}_K)$. Let us fix a set $\mathcal{F}$ of primes such that the primes $P_\ell \mid \ell\mathcal{O}_K$ generates $\mathrm{Cl}(\mathcal{O}_K)$ and that in $\mathcal{F}$ there should be enough primes such that the walk *looks random*. Often the set $\mathcal{F}$ should be chosen as the set of primes which split in $\mathcal{O}_K$ (some ramified primes

[1] This condition can be checked by $\Phi_\ell(X,Y) \mod p$.

can also be used) which are less than some bound B. The core of the random walk consists by a function

$$f\colon \mathbb{F}_q \longrightarrow \mathcal{F} \times \{0,1\}$$

which should be deterministic but it must have a distribution close to uniform (it can be constructed using the bit of the element in the finite field). In order to save as memory as possible the strategy applied to find the random walk is Pollard like.
We define a step of our random walk given a j-invariant $j_k^{(i)}$ as follows: if

$$(\ell, b) = f(j_k^{(i)})$$

than we factor the modular polynomial $\Phi_\ell(X, j_k^{(i)})$ to obtain one or two new j-invariants. Using the bit b we select one of the j-invariants in a deterministic manner and call it $j_k^{(i+1)}$. Now, we have to update the ideal. Due to remark 3.3.12, we can obtain the ideal P_ℓ from $j_k^{(i+1)}$ by evaluating the Frobenius map over a point $E_{j_k^{(i)}}[\ell]$. Then $[I_k^{(i+1)}] = [I_k^{(i)} P_\ell]$.
Let $T \in \mathbb{N}$ such that $T = O(\sqrt{h(\mathcal{O}_K)}) = O(q^{1/4})$. To find an isogeny from j_1 to j_2, we take a random walk of T steps starting with the initial value $(j_1^{(0)} = j_1, [I_1^{(0)}] = [(1)])$ and store only the final position $(j_1^{(T)}, [I_1^{(T)}])$. Then start a second random walk from $(j_2^{(0)} = j_2, [I_2^{(0)}] = [(1)])$ until a collision $j_1^{(T)} = j_2^{(S)}$ (because of the birthday paradox it must occur). In practice, it could be used a set of distinguished j-invariants and many processors running in parallel (starting on differently randomized j-invariants). Once a collision is found we know that the isogeny from j_1 to j_2 is represented by the class ideal

$$[I] = [I_1^{(T)} {I_2^{(S)}}^{-1}]$$

It is possible to construct a chain of isogenies from E_1 to E_2 by following the paths in the random walk, but this is much longer than necessary. Instead, as we will show in the discussion of Step 3, one can obtain an isogeny which can be easily represented in a short and compact format.

Step 3

Let us suppose to have two j-invariants j_1 and j_2 and an ideal a representing an isogeny between j_1 and j_2 . We can assume that $[I]$ is a reduced ideal[2]. In this stage we will replace I by a smooth ideal. Of course, the ideal I was originally constructed as a smooth product of ideals, but this representation has enormous (exponential) length. Hence we desire a representation which is more suitable for computation. This is accomplished using techniques from index calculus algorithms for imaginary quadratic fields. Here, we are going to give a naive idea of the algorithm, since then in Section 4.1.2 we will discuss more precisely the question of representation of the ideal. Let us choose a factor base $\mathcal{F}'$ as a set of prime ideals of $\mathcal{O}_K$ which are split or ramified in $\mathcal{O}_K$ and of size less

[2] Namely, that the quadratic form associated is reduced, see Appendix A.2

than some bound B, which should be chosen to optimize the performance. In particular, choose (repeatedly) same integer a_i and compute ideals by reducing

$$I \cdot \prod_{P_i \in \mathcal{F}'} P_i^{a_i}$$

until is sufficient to find ideal J whose factorization over the factor base $\mathcal{F}'$ is

$$J = \prod_{P_i \in \mathcal{F}'} P_i^{b_i}$$

Then

$$I \equiv \prod_{P_i \in \mathcal{F}'} P_i^{b_i - a_i} \tag{4.1}$$

The size of the b_i are bounded since the ideal J is reduced. In the original article [GHS02] there was expected heuristically at most $q^{1/4}$ choices of the a_i before obtaining a value of J which is sufficiently smooth. However, we will see that using some adjustments, especially on the choice of primes and the bound, this step can run in subexponential time.

Step 4

We want to construct the isogeny associated to the class $[I]$. Each prime in (4.1) induces an isogeny. Note that by Lemma 3.4.7 if a prime appears in such factorization with negative exponent is enough to consider the isogeny associated to its conjugated. Then using the subgroup $E[J]$ the actual isogeny is determined by Vélu's formulae. Note that the ideal J computed in the previous step will has norm at most $O(\sqrt{|D|})$. Then the smooth representation of the ideal equivalent to I has at most $O(\log |D|)$ not necessarily distinct factors in it, each factor corresponding to an isogeny of degree at most B.

The complexity of the previous algorithm results exponential:

Theorem 4.1.1. *The computation of an isogeny between two ordinary elliptic curves defined over $\mathbb{F}_q$, by GHS algorithm, has average case complexity of $\widetilde{O}(q^{1/4})$ operations.*

Proof sketch. We notice that since the random walk is on a set of size $h(\mathcal{O}_K)$ then we expect a collision to occur after $O(q^{1/4})$ steps. Since each step of the walk in Step 2 requires at most $O((\log q)B^2)$ field operations and it is sufficient chose $B = 6\log(D)^2$, so the complexity for Step 2 is

$$O((\log q)B^2\sqrt{h(\mathcal{O}_K)}) = O((\log q)^6 q^{1/4}) = \widetilde{O}(q^{1/4})$$

To estimate the running time of Step 3 we need to examine the probability of obtaining a smooth number. Standard estimation, see Theorem A.1.2, give an asymptotic smoothness probability to obtain an appropriate factorization in subexponential time. Finally, it remains to evaluate the costs of Vélu method to determine explicitly the isogenies involved, Theorem 1.2.12. Anyway, the exponential complexity of Step 2 overcome the other.

Galbraith and Stolbunov [GS13] improved the complexity of the GHS algorithm by a constant factor by modifying the random walk function so that lower-degree isogenies are used more frequently. Of course, there are many open issues in algorithm we presented above. For example, as it is underlines in [GS13]§3.3, at Step 2 the bit b is chosen uniformly at random. The prime ℓ is typically split and the algorithm chooses one of the two primes over ℓ using that bit. Hence fixed ℓ every step in the walk where it is chosen produces an action by one of the two ideal over ℓ. It has been seen by numerical experiments that this fact produce walks that are far from random. To avoid this problem Galbraith and Stolbunov fix a direction in the graph, which means that for each Elkies prime in $\mathcal{F}$, they establish a priori an eigenvalue of the action Frobenius map over the ℓ-torsion group.
Let us remark that the total complexity of the GHS algorithm is exponential, since the cost of find a connecting path in the graph it is. The goal of the algorithm in the next section is to speed up this step.

4.1.2 A Quantum Algorithm

In 2011 Childs, Jao and Soukharev in [CJS14] proposed the first algorithm to solve the general isogeny problem in subexponential time with a quantum computer. The existence of a subexponential method, in itself, does not undermine the security of the cryptosystems based on isogeny curves, however it opens new possibilities in this direction. In their article, Childs et al. present an improved index calculus algorithm to find a compact and smooth representation of an ideal in the class group of a maximal order that, under GRH, run in subexponential time $L_q(1/2, \sqrt{3}/2)$. Such algorithm can be use to speed up the third step of GHS. Then they describe a quantum algorithm to solve the general isogeny problem between two ordinary elliptic curves, with complex multiplication, by reducing this problem to the abelian hidden shift problem, Problem 5.

Let us consider E_1 and E_2 isogenous ordinary elliptic curves defined over $\mathbb{F}_q$ and let $\mathcal{O}$ be their endomorphism ring. Given two isogenous curves we know that there exist an horizontal isogeny between them if $\mathcal{O}$ is maximal, otherwise it should be necessary climbing the volcano to the crater; so we usually suppose $\mathcal{O}$ maximal. In this section we suppose an horizontal isogeny exists. $\mathcal{O}$ is an order in quadratic imaginary number field, and we denote by D the discriminant of $\mathcal{O}$. We have observed that find an horizontal isogeny is equivalent to find an ideal class $[I] \in \mathrm{Cl}(\mathcal{O})$ such that $\kappa([I], E_1)$ and E_2 are isomorphic, i.e. to Problem 7. Let $f_1, f_2 \colon \mathrm{Cl}(\mathcal{O}) \to \mathcal{ELL}_{\mathbb{F}_q}(\mathcal{O})$ be two functions hiding $[S] \in \mathrm{Cl}(\mathcal{O})$, where $[S]$ is the ideal class such that $j(\kappa([I], E_1)) = j(E_2)$. Specifically, we put

$$f_c([I]) = \kappa([I], j(E_c)).$$

We want to pass from ClGAIP to an abelian hidden shift problem, hence we have to prove that the following fact holds:

Lemma 4.1.2. *The function f_1 is injective and $f_2([I]) = f_1([S][I])$.*

Proof. κ is a group action, then

$$f_2([I]) = \kappa([I], j(E_2))$$

$$
\begin{aligned}
&=\kappa([I],\kappa([S],j(E_1)))\\
&=\kappa([I][S],j(E_1))\\
&=f_1([S][I]).
\end{aligned}
$$

Let us suppose there are two distinct ideal classes $[I],[J]$ such that $f_1([I]) = f_1([J])$, then $\kappa([I],j(E_1)) = \kappa([J],j(E_1))$. The action κ is free and transitive, by Theorem 3.4.15, so it is absurd and f_1 is injective. □

Note that Problem 7 is equivalent to the hidden subgroup problem in the dihedral group[3] $\mathrm{Cl}(\mathcal{O}) \rtimes \mathbb{Z}/2$, where $\mathbb{Z}/2$ acts on I by inversion. Ettinger and Høyer in [EH99] prove that such a problem can be solved by a quantum computer with a polynomial number of valuations:

Theorem 4.1.3 (Theorem 2.3 [EH99]). *Let X be a finite set and $\gamma\colon D_N \to X$ be a function that hides the dihedral subgroup H. There exists a quantum algorithm that, given γ, uses $O(\log N)$ evaluations of γ and outputs a subset $Y \subseteq H$ such that Y is a generating set for H with probability at least $1 - 2/N$.*

Unfortunately, algorithm in theorem 4.1.3 is not efficient in sense we would want: it requires only $O(\log N)$ evaluations of γ, but it does not run in polynomial time. However it implies that our problem has polynomial quantum query complexity.

In order to solve Problem 7 using a quantum algorithm, a primary question is the cost of evaluating the function f_i. Obviously, to find out a way to evaluate the black-box functions coincides to find out a way to evaluate the action κ. In literature, the action of an ideal $[I]$ over an isomorphism class $j(E)$, i.e. $\kappa([I],j(E))$, is denoted by $[I] * j(E)$ and κ is called *isogeny star operator*. In particular, we want to prove that our hidden shift problem can be solved in quantum subexponential time, using Kuperberg approach to abelian hidden shift problem, up to assuming that we can evaluate the isogeny star operator in subexponential time. Now, first we are going to show that this assumption is not restrictive, then we are going to outline a method to construct isogenies in subexponential time.

Computing the isogeny star operator

Let K be a quadratic imaginary number field and $[I]$ an ideal in $\mathrm{Cl}(\mathcal{O})$, let j the j invariant of a class of curves in $\mathcal{ELL}_{\mathbb{F}_q}(\mathcal{O})$ and taken E a curve in such class. We denote $n = \#E(\mathbb{F}_q)$. We wish to evaluate $\kappa([I],j)$. The algorithm proposed is a sort of index calculus algorithm, in fact it include a function which return a compact and smooth representation of an ideal in the class group of a order and then it use this special form to evaluate the operator.

Given an ideal class $[I] \in \mathrm{Cl}(\mathcal{O})$, Algorithm 4.1 produces a relation vector $\mathbf{z} = (z_1,\dots,z_f) \in \mathbb{Z}^f$ for $[I]$, with respect to a factor base $\mathcal{F} = P_1,\dots,P_f$, satisfying

$$[I] = \mathcal{F}^{\mathbf{z}} := P_1^{z_1}\cdots P_f^{z_f}$$

[3] See [EH99].

with the additional property that

$$|\mathbf{z}|_1 = \sum |z_i| < O(\log |D|)$$

for some absolute implied constant. By Corollary 3.6.12, there exist a positive constant $C > 1$ such that a random walk of length

$$t \geq C\frac{\log(h(\mathcal{O}))}{\log\log q}$$

from any starting vertex lands in any fixed subset $S \subset G$ with probability at least $\frac{\#S}{2h(\mathcal{O})}$. We require in Algorithm 4.1 that

$$C\frac{\log(h(\mathcal{O}))}{\log\log q} \leq t \leq C\log(|D|). \tag{4.2}$$

Let us fix, the following notation:

$$L(c) = L_{\max\{|D|,q\}(1/2,c)}.$$

Algorithm 4.1 Computing relation

Input: $[I]$, D, q,n and a parameter z. An integer t as in 4.2.
Output: a relation vector $\mathbf{z} \in \mathbb{Z}^f$ such that $[I] = [\mathcal{F}^{\mathbf{z}}]$.

```
Compute a factor base consisting of split primes of norm less than $L(z)$; discard any primes dividing $qnD$ to obtain a new factor base $\mathcal{F} = \{P_1, \ldots, P_f\}$
$\mathcal{P} \leftarrow \{\mathrm{N}(P) \colon P \in \mathcal{F}\}$
$\ell \leftarrow L\left(\frac{1}{4z}\right)$
for $k = 0, \ldots, \ell$ do
    Select $\mathbf{v} \in \{0..|D|-1\}^f$ uniformly at random subject to the condition that $|\mathbf{v}|_1 = t$
    Calculate the reduced ideal $J_{\mathbf{v}}$ in the ideal class $[I] \cdot [\mathcal{F}^{\mathbf{v}}]$
    Find the prime factorization of the integer $\mathrm{N}(J_{\mathbf{v}})$
    if $\mathrm{N}(J_{\mathbf{v}})$ is $\mathcal{P}$-smooth then
        Factor the ideal $J_{\mathbf{v}}$ over $\mathcal{F}$ to obtain $J_{\mathbf{v}} = \mathcal{F}^{\mathbf{a}}$ for some $\mathbf{a} \in \mathbb{Z}^f$
        return $\mathbf{z} = \mathbf{v} - \mathbf{a}$
    end if
end for
```

Algorithm 4.2 is the main algorithm for evaluating the complex multiplication action. It takes as input a discriminant $D < 0$, $[I]$ an ideal class and a j-invariant $j(E)$ of a curve with complex multiplication induced by an order $\mathcal{O}$ of discriminant D, and it produces as output $\kappa([I], j(E))$. Primes dividing qnD must be eliminated in order to compute the isogenies in the final step of the algorithm.

Algorithm 4.2 Computing $j(E')$

```
Input: $[I]$, $D$, $q$,$n$ and $j$.
Output: $j(\kappa([I], j(E)))$.
Compute a relation $\mathbf{z} \in \mathbb{Z}^f$ such that $[I] = [\mathcal{F}^{\mathbf{z}}]$, by Algorithm 4.1 with any valid choice of $t$
Compute a sequence of isogenies $(\phi_1, \ldots, \phi_s)$ such that the composition $\phi \colon E \to E'$ has kernel $E[\mathcal{F}^{\mathbf{z}}]$ as in GHS
return $j(E')$
```

More than present an exhaustive study of the complexity and the correctness of the algorithms, which are clear in the original article, we want to comment the algorithms above. Here, we suppose to be in a quantum context then step 7 of Algorithm 4.1 can be improved in polynomial time by Shor's algorithm. To perform this step on a classical computer, to obtain the same complexity it is necessary to perform every loop and to use appropriate techniques to find a smooth ideal. The choice of the bound for the number of loops is $L\left(\frac{1}{4z}\right)$ because the probability, under GRH, to produce a smooth ideal (with the bound $L(z)$ over the norm of primes in $\mathcal{F}$) is just $L\left(\frac{1}{4z}\right)$. Note that, also here, the assumption of the GRH depends on the fact that we use that the isogeny graph is expander. An analysis shows that the optimal z is $1/2\sqrt{3}$ and the cost of step 2 of Algorithm 4.2 under approximation $L(\frac{1}{4z} + 3z)$, that dominates the other costs. Finally, it is worth to briefly discuss the question of reduction in step 6 of Algorithm 4.1. A priori the cost of this step could be exponential. Childs et al. in their article solve this setback using quadratic forms. For our purpose is enough to know that each ideal can be represented in terms of reduced primitive positive definite quadratic form, which means that each isogeny is simply representable by the vector of smooth coordinates respect such suitable finite basis in subexponential time. Recalling that $|D| \leq 4q$ we have:

Theorem 4.1.4 ([CJS14] Theorem 3.3)**.** *Under GRH, Algorithm 4.2 has a worst-case running time of at most* $L_q(\frac{1}{2}, \frac{\sqrt{3}}{2})$.

Computing isogenies

We showed that solving the general isogeny problem for ordinary elliptic curve can be reduced to an hidden shift problem by the action the class group and in the previous subsection we present a method to evaluate this action. Now we want to prove that there exists a quantum algorithm to find an isogeny in our hypothesis. We want to apply Kuperberg's algorithm and the result in Theorem 2.2.4. In our case, the acting group is the class group and the outputs are ideal classes. The cost then it depends on the type of representation chosen. However, we saw that is possible to represent the kernel of the isogeny by a finite vector whose length depends on the cardinality of a generating set of the ideal class group. Assuming D known, we decompose $\mathrm{Cl}(\mathcal{O})$ as a direct sum of cyclic groups, with a known generator for each, and then solve the hidden shift problem. So, we obtain:

Theorem 4.1.5. *Assuming GRH, Algorithm 4.3 runs in time* $L_q(\frac{1}{2}, \frac{\sqrt{3}}{2})$ *to solve the general isogeny problem for ordinary elliptic curve defined over a finite field.*

Proof. We can perform step 1 using Mosca quantum algorithm to decompose finite abelian group, which determines the structure of an abelian group given a generating set and a unique representation for the group elements in polynomial time by Theorem 2.2.2. We represent the elements uniquely using reduced quadratic forms, and we use the fact that, under GRH, the set of ideal classes, of norm at most $12\log^2(|D|)$, forms a generating set. By Theorem 2.2.4, step 2 use $2^{O(\sqrt{\log|D|})} = L(0)$ evaluations of the functions f_i: the class number is $O(|D|\log(|D|))$ and a finite group G has at most $O(\log(G))$ generators, so in our case $O(n) \leq O(\sqrt{\log(|D|\log(|D|))}) = O(\sqrt{\log(|D|) + \log\log(|D|)}) = O(\sqrt{\log|D|})$. We stated that the isogeny star operator can be evaluated in $L_q(\frac{1}{2}, \frac{\sqrt{3}}{2})$, under GRH. Using that $|D| \leq 4q$ we have the thesis. □

Algorithm 4.3 Ordinary isogeny computation

Input: A finite field $\mathbb{F}_q$, a discriminant $D < 0$, and Weierstrass equations of isogenous elliptic curves E_1, E_2 with endomorphism ring $\mathcal{O}$.
Output:$[S]$ such that $j(\kappa([I], E_1)) = j(E_2)$.

```
1: Decompose $\mathrm{Cl}(\mathcal{O}) = \langle [I_1] \rangle \oplus \cdots \oplus \langle [I_k] \rangle$ where $n_i = |\langle [I_i] \rangle|$
2: Solve the hidden shift problem defined by the functions
       $f_1, f_2 \colon \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_k \to \mathcal{ELL}_{\mathbb{F}_q}(\mathcal{O})$
   satisfying $f_c(x_1, \ldots, x_k) = \kappa([I_1]^{x_1} \cdots [I_k]^{x_k}, j(E_c))$, giving some
       $(s_1, \ldots, s_k) \in \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_k$
3: return $[I_1]^{s_1} \cdots [I_k]^{s_k}$
```

4.2 Supersingular General Isogeny Problem

We have seen in the previous chapter that two supersingular curves with endomorphism rings in the same quaternion algebra are isogenous. We also have showed that left modules act over supersingular elliptic curves. We could think to use an equivalent approach to the ordinary case, however the fact that class group of orders in number fields are abelian groups is crucial, since it allows to reduce this task to a hidden abelian shift problem. In the supersingular case, the class group of the endomorphism ring is no longer abelian, thus preventing a direct adaptation of this method. In this section we will present a quantum algorithm to solve the general isogeny problem for supersingular curves due to Biasse, Jao and Sankar [BJS14], whose currently is the best known. The central idea is to reduce the problem to two elliptic curves defined over $\mathbb{F}_p$ and then use the fact that the endormorphism ring over $\mathbb{F}_p$ of such curves is an order in the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-p})$, just like the ordinary case. In particular, by this reduction we are allowed to recover the algorithm discussed in the previous section. Algorithm 4.4 summarizes the strategy. We need, now, to explain how to perform these steps: it is better to submit step 1 and 2 and step 3 to two different procedures and to examine them separately. The original article by Biasse et al. includes some mistakes, however we could correct them keeping the same main result.

Algorithm 4.4 Supersingular isogeny computation

Input: Two isogenous supersingular elliptic curves E, E' defined over $\mathbb{F}_q$ of characteristic p.
Output: An isogeny $f\colon E \to E'$.

```
1: Find an isogeny $\phi_1 \colon E \to E_1$ where $E_1$ is defined over $\mathbb{F}_p$.
2: Find an isogeny $\phi_2 \colon E' \to E_2$ where $E_2$ is defined over $\mathbb{F}_p$.
3: Find an isogeny $\alpha \colon E_1 \to E_2$.
4: return $\hat{\phi}_2 \circ \alpha \circ \phi_1$
```

4.2.1 Quantum Search for a Curve Defined over $\mathbb{F}_p$

The j-invariant of a supersingular curve $E/\mathbb{F}_q$ is defined over $\mathbb{F}_{p^2}$, where p is the characteristic of the base field: then all the isomorphism class defined by $j(E)$ is at least defined over $\mathbb{F}_{p^2}$. This fact allows us to suppose that the supersingular curves we take are defined over $\mathbb{F}_{p^2}$. So, given a such curve we are going to describe an isogeny whose image is a curve E_1 defined over $\mathbb{F}_p$.
Let us fix a prime ℓ different from p. By Theorem 3.6.10, the ℓ-isogeny graph of supersingular curves in $\overline{\mathbb{F}}_p$ is connected, $\ell + 1$ regular and has the Ramanujan property. So, by Mixing Theorem we have a bound on the length on the path from a vertex in S_{p^2}, the set of supersingular j-invariants in $\mathbb{F}_{p^2}$, to a vertex in the subset S_p, the set of supersingular j-invariants in $\mathbb{F}_p$. Note that by the observation above S_{p^2} are all the vertices of the graph. Explicitly we obtain:

Lemma 4.2.1. *Let E a curve in S_{p^2}. Then, under GRH, there is a probability at least $\rho(p) = \frac{\pi}{2e^\gamma \sqrt{p} \log\log p}$ that a random path in the 3-isogeny graph of length*

$$t \geq \frac{\log\left(p^{3/4}\frac{\sqrt{e^\gamma}}{\sqrt{3}\pi}\right)}{\log\left(\frac{2}{\sqrt{3}}\right)} + c(p) \tag{4.3}$$

starting from a random supersingular curve passes through a supersingular j-invariant defined over $\mathbb{F}_p$, where γ is the Euler constant and $|c(p)| < \log\log p$.

Proof. We suppose $p \gg 0$. We want to apply Corollary 3.6.13 with $S = S_p$ and $V = S_{p^2}$. In order to estimate a sufficient length of the path necessarily to reach the curve defined over $\mathbb{F}_p$, it is enough to give an upper bound of such quantities. We recall that the 3-isogeny graph is 4-regular and the absolute values of the eigenvalues of the adjacency matrix is less than $2\sqrt{3}$, by the Ramanujan property. A random 3-isogeny walk of length at least

$$\frac{\log\left(2\#S_{p^2}/(\#S_p)^{1/2}\right)}{\log\left(\frac{2}{\sqrt{3}}\right)}$$

starting from a given curve hits a curve defined over $\mathbb{F}_p$ of the vertices G with probability grater then $\#S_p/2\#S_{p^2}$. Let us focus now on the numerator, in particular thanks to monotony we can consider the argument of the logarithm.

Since p is a large prime we can approximate $\#S_{p^2} = p/12$ by (1.14). To obtain an upper bound we need to underestimate $\#S_p$, which coincides with an appropriate class number by (4.5). It has been shown that the best possible lower bound, except for a small constant factor, to the class number of an imaginary quadratic number field $K = \mathbb{Q}(\sqrt{-d})$ is

$$h(d) \geq (1 + o(1)) \frac{\pi}{12e^\gamma} \frac{\sqrt{d}}{\log \log d}.$$

By replacing with the appropriate number field, we obtain that

$$\begin{aligned}\frac{2\#S_{p^2}}{(\#S_p)^{1/2}} \leq & \frac{p/6}{\sqrt{\frac{\pi}{12e^\gamma}\frac{\sqrt{p}}{\log\log p}}} \\ =& \frac{p}{6}\frac{\sqrt{12e^\gamma \log\log p}}{\sqrt{\pi}p^{1/4}} \\ =& p^{3/4}\frac{\sqrt{e^\gamma \log\log p}}{\sqrt{3\pi}}\end{aligned}$$

(for $p \equiv 8 \mod 3$ we would have something smaller but it does not matter). Using the property of logarithm we obtain

$$\log\left(\frac{2\#S_{p^2}}{(\#S_p)^{1/2}}\right) \leq \log\left(p^{3/4}\frac{\sqrt{e^\gamma}}{\sqrt{3\pi}}\right) + \frac{1}{2}\log\log\log p$$

Let us now consider the probability, using the same valuations we obtain

$$\frac{\#S_p}{2\#S_{p^2}} \geq \frac{\pi}{12e^\gamma}\frac{\sqrt{p}}{\log\log p}\frac{6}{p} = \frac{\pi}{2e^\gamma\sqrt{p}\log\log p}.$$

Hence, by replacing all we have the thesis. □

Note that we gave an underestimation of the probability to be sure the result holds; however we expect that correct value is greater, since we take paths whose length that is greater than the minimal in Corollary 3.6.12.
Let us take a random subset of 3-isogeny path whose length is t, as in (4.3), with the same initial point with cardinality $\frac{\log(2)}{\rho(p)}$. The probability a 3-isogeny path starting from a fixed curve does not hit S_p is approximable by

$$(1-\rho(p))^{\frac{\log(2)}{\rho(p)}} = e^{\frac{\log(2)}{\rho(p)}\log(1-\rho(p))} \approx e^{\frac{\log(2)}{\rho(p)}(-\rho(p))} = \frac{1}{2}$$

Considering classical algorithms, a research of an unsorted database D of N elements has a complexity of at least N. By Grover's algorithm, given a condition $C \colon D \to \{0,1\}$, a quantum computer finds an element $x \in D$ such that $C(x) = 1$ and $C(y) = 0$ for all $y \neq x$ in D in complexity $O(\sqrt{N})$ with success probability greater than 1/2. The element of D are encoded by bits sequence then we can suppose $N = 2^n$ and it is assumed condition C to be evaluated in unit time on these states. See Section 2.2.3.
Let E be a supersingular curve over $\mathbb{F}_{p^2}$, we can use Grover's algorithm to find a walk in the 3-isogeny graph from $j(E)$ to a $j \in S_p$. It is sufficient to consider a set of $N = \frac{\log(2)}{\rho(p)}$ walks. In particular, each path of length t can be encoded in

$\{0,1,2,3\}^t$, since each polynomial $\Phi_3(j(E),Y)$ has four roots. By the formula (4.3) the number of bits needed to encode such a path is $O(\log p)$. To choose the subset of path we can take a random injective function

$$f\colon \{1,\dots,N\} \to \{\text{3-isogeny paths of length } t \text{ starting from } E\} \tag{4.4}$$

and then we can define for $x \in \{1,\dots,N\}$

$$x \xmapsto{C_f} \begin{cases} 1 & \text{if } f(x) \text{ pass through } S_p \\ 0 & \text{otherwise.} \end{cases}$$

Note that we proved an x such that $C_f(x) = 1$ exists with probability $1/2$. Now let us summarize our strategy in the following pseudocode:

Algorithm 4.5 Quantum walk to a curve defined over $\mathbb{F}_p$

Input: A supersingular curve E defined over a field of characteristic p.
Output: E' defined over $\mathbb{F}_p$ and $\phi\colon E \to E'$.

```
1: Select
   $t = \left\lceil \frac{\log\left(p^{3/4}\frac{\sqrt{e^{\gamma}}}{\sqrt{3\pi}}\right)}{\log\left(\frac{2}{\sqrt{3}}\right)} + c(p) \right\rceil$
2: Choose a random $f$ as (4.4)
3: By Grover's algorithm find $x$ such that $C_f(x) = 1$.
4: Compute the isogeny path $\phi = \phi_1 \cdots \phi_t$ corresponding to $x$.
5: return $(\phi, \phi(E))$
```

Theorem 4.2.2. *Algorithm 4.5 has an expected run time $\widetilde{O}(p^{1/4})$ with success probability $1/4$.*

Proof. By Lemma 4.2.1 $N = O(1/\rho(p)) = \widetilde{O}(\sqrt{p})$, hence step 2 and 3 has both $\widetilde{O}(p^{1/4})$ time complexity. In our case C_f evaluation Grover's is done in polynomial time, however by looking at the analysis in [Gro96] one note that it affects the cost by the multiplication of a constant of order $O(\log p) = \widetilde{O}(1)$, which here is negligible. Step 4 can be performed polynomially (see Ramark 3.4.30). □

Note that the complexity of this reduction to $\mathbb{F}_p$ algorithm strictly depends on the choice of using 3-isogenies, in fact either of the bound and the cost of constructing isogeny are based on the fact that 3 is small prime.

4.2.2 Computing an Isogeny between Curves Defined over $\mathbb{F}_p$

Let us suppose to have two isogenous supersingular elliptic curves defined over $\mathbb{F}_p$. By Theorem 3.1.1 we know that there exists an isogeny defined over $\mathbb{F}_p$. So, we could decided to work directly over $\mathbb{F}_p$ and to consider $\mathcal{ELL}_{\mathbb{F}_p}(\mathcal{O})$ instead $\mathcal{ELL}_{\overline{\mathbb{F}}_p}(\mathcal{O})$. However, we must take care that the given two curves, the isomorphism between them should be defined over $\mathbb{F}_{p^n}$ with $n > 0$. Note, for example, that the a supersingular elliptic curve and its non-trivial quadratic twist are isogenous, but non isomorphic over $\mathbb{F}_p$ (see Chapter 1). Thus, first of all we investigate $\mathcal{ELL}_{\mathbb{F}_p}(\mathcal{O})$. In this context it is not very precise to represent the vertices in the supersingular isogeny graph over $\mathbb{F}_p$ with j-invariants, then the nodes of our graph must contain more information (such as a subset of the coefficients of the Weierstrass equation). Also, it is not possible to use the modular polynomial to compute the neighbor of a given vertex. Instead we can use the formulae of Vélu Theorem 1.2.12 to compute the image curve under an isogeny whose kernel is a Galois-invariant subgroup G of a curve with order ℓ. Delfs and Galbraith in their article [DG16] have shown that the supersingular $\mathbb{F}_p$-isogeny graph resemble the volcano structure of the ordinary case, in particular there are many craters and the height is grater than zero only when $\ell = 2$. Let us prove this fact.

Let us fix a supersingular elliptic curve E defined over $\mathbb{F}_p$ and π its Frobenius map. As we saw in section 3.5.1, $K = \mathbb{Q}(\pi)$ is an imaginary quadratic field over $\mathbb{Q}$. $\mathrm{End}_{\mathbb{F}_p}(E)$ is the fixed by the action of $\mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$, thus it is an order in K and its conductor is prime to p. We can suppose that $p > 3$, then the trace of Frobenius map t must be zero. Indeed E is supersingular then $t \equiv 0 \mod p$, by Hesse Theorem must hold also that $|t| \leq 2\sqrt{p}$, then $t = 0$. The minimal polynomial of the Frobenius map is

$$\pi^2 + p = 0$$

then $\pi = \pm\sqrt{-p}$ and so $K = \mathbb{Q}(\sqrt{-p})$. Furthermore,

$$\mathbb{Z}[\sqrt{-p}] \subseteq \mathrm{End}_{\mathbb{F}_p}(E) \subset \mathcal{O}_K.$$

There are two cases:

- if $p \equiv 1 \mod 4$ then $\mathcal{O}_K = \mathbb{Z}[\sqrt{-p}]$, then $\mathbb{Z}[\sqrt{-p}] = \mathrm{End}_{\mathbb{F}_p}(E)$,
- if $p \equiv 3 \mod 4$ then $[\mathcal{O}_K \colon \mathbb{Z}[\sqrt{-p}]] = 2$ then $\mathrm{End}\,\mathbb{F}_p(E)$ is $\mathcal{O}_K$ or $\mathbb{Z}[\sqrt{-p}]$.

Directly, we have that the volcano has one level in first case and at most two in the second. We say E is on the *surface* if $\mathrm{End}_{\mathbb{F}_p}(E) = \mathcal{O}_K$, while we say E is on the *floor* if $\mathrm{End}_{\mathbb{F}_p}(E) = \mathbb{Z}[\sqrt{-p}]$. Note that for $p \equiv 1 \mod 4$ surface and floor coincide. As for the general case we say that an isogeny $\phi\colon E \to E'$ is *horizontal* if $\mathrm{End}_{\mathbb{F}_p}(E) = \mathrm{End}_{\mathbb{F}_p}(E')$, otherwise is called *vertical*. Obviously, the following holds:

Lemma 4.2.3. *If there exists a vertical isogeny of degree n then $2 \mid n$. In particular, does not exit vertical isogenies of odd degree.*

Due to the previous remarks, the set of supersingular j-invariants in $\mathbb{F}_p$, that we denote S_p, has cardinality depending on the congruence class of p mod 4. In particular, holds that

$$\#S_p = \begin{cases} \frac{h(-4p)}{2} & \text{if } p \equiv 1 \mod 4, \\ h(-p) & \text{if } p \equiv 7 \mod 8, \\ 2h(-p) & \text{if } p \equiv 3 \mod 8 \end{cases} \tag{4.5}$$

where we are pointing the corresponding order in $\mathbb{Q}(\sqrt{-p})$ by its discriminant ([DG16] Equation 1).

Let us recall that in this context the same invariant j can identify curves not isomorphic over $\mathbb{F}_p$. We denote by $C_{j,p}$ the set of elliptic curves with invariant j up to isomorphism over $\mathbb{F}_p$. Then:

Proposition 4.2.4 (Proposition 2.3 [DG16])**.** *Let $p > 3$ a prime and $j \in \bar{\mathbb{F}}_p$.*

$$\#C_{j,p} = \begin{cases} 6 & j = 0 \textit{ and } p \equiv 1 \mod 3 \\ 4 & j = 1728 \textit{ and } p \equiv 1 \mod 4 \\ 2 & \textit{otherwise.} \end{cases}$$

The j invariant of a supersingular elliptic curve over $\mathbb{F}_p$ is zero if and only if $p \equiv 2 \mod 3$ and is 1728 if and only if $p \equiv 3 \mod 4$. Thus given a j, if it represent a supersingular class of isomorphism, then there are exactly 2 curve in $C_{j,p}$.
A good question is when a supersingular curve is defined over $\mathbb{F}_p$:

Proposition 4.2.5. *Let $p > 3$ and let E be a supersingular elliptic curve over $\bar{\mathbb{F}}_p$. Then E is defined over $\mathbb{F}_p$ if and only if $\mathbb{Z}[\sqrt{-p}] \subseteq \operatorname{End}(E)$.*

Proof. The right implication follows from what we said above. Vice versa, let $\psi \in \operatorname{End}(E)$ such that $\psi^2 = -p$, then $\deg \psi = p$ and $\hat{\psi} \circ \psi = p$. E is supersingular then $E[p^r] = \{O\}$, then $\ker \psi = \{O\}$. The separable degree of ψ is zero and it must be purely inseparable. This means that up to isomorphism it coincide with the Frobenius map (by Decomposition Theorem):

$$\psi \colon E \xrightarrow{\pi} E^{(p)} \xrightarrow{\sim} E$$

So, $j(E) = j(E)^p \in \mathbb{F}_p$. □

In section 3.4 we showed that there is correspondence between ordinary curve with complex multiplication $\mathcal{ELL}_{\bar{\mathbb{F}}_p}(\mathcal{O})$ and $\operatorname{Cl}(\mathcal{O})$: the first step for this equivalence had been showing the correspondence between the class group and the curves defined over the complex numbers; then we saw that the j-invariants are defined over $\bar{\mathbb{Q}}$ and finally by Deuring reduction we got the thesis. In the supersingular case, this does not hold. However we have just seen that if E is defined over $\mathbb{F}_p$ than $\operatorname{End}_{\mathbb{F}_p}(E)$ is an order in an imaginary quadratic field, so we can restore a correspondence:

Theorem 4.2.6. *There exists a one-to-one correspondence between the supersingular elliptic curves defined over $\mathbb{F}_p$ and elliptic curves defined over $\mathbb{C}$ with complex multiplication induced by $\mathcal{O} \in \{\mathcal{O}_K, \mathbb{Z}[\sqrt{-p}]\}$ where $K = \mathbb{Q}(\sqrt{-p})$.*

Proof. Let $\mathcal{E}_p(\mathbb{C})$ the set of elliptic curves defined over $\mathbb{C}$ with complex multiplication induced by $\mathcal{O} \in \{\mathcal{O}_K, \mathbb{Z}[\sqrt{-p}]\}$ and $\mathcal{E}_p(p)$ the set of supersingular elliptic curves defined over $\mathbb{F}_p$. Let us consider the reduction map

$$\begin{array}{ccc} \mathcal{E}_p(\mathbb{C}) & \longrightarrow & \mathcal{E}_p(p) \\ E & \longmapsto & \bar{E} \end{array}$$

It is enough to show that it is a bijection. By Proposition 4.2.4 and (4.5), we have that

$$\#\mathcal{E}_p(\mathbb{C}) = h(\mathcal{O}_K) + h(\mathbb{Z}[\sqrt{-p}]) =$$

$$
\begin{aligned}
&=\begin{cases} h(-4p) & p\equiv 1 \mod 4\\ h(-4p)+h(-p) & p\equiv 3 \mod 4\end{cases}\\
&=\begin{cases} h(-4p) & p\equiv 1 \mod 4\\ 2h(-p) & p\equiv 7 \mod 8\\ 4h(-p) & p\equiv 3 \mod 8\end{cases}\\
&=2\#S_p=\mathcal{E}_p(p)
\end{aligned}
$$

Where the last equality holds since we observed that for each j-invariant of an elliptic curve $C_{j,p}=2$. Hence, if we prove that the reduction map is surjective we automatically have it is a bijection. But surjectivity yields immediately from Theorem 1.7.2. □

In order to adapt the strategy of the ordinary case, the correspondence between the set of the curve is not sufficient, we also need the morphisms behave. Essentially, as we have done in the previous chapter, we have to prove that the reduction map induces an equivalence of category. The delicate issue is if the reduction of an isogeny in characteristic 0, obtained from an isogeny define over $\mathbb{F}_p$, is defined over $\mathbb{F}_p$. It is true:

Proposition 4.2.7. *Let $\bar{E}_1, \bar{E}_2$ be supersingular elliptic curves over $\mathbb{F}_p$ and let (E_1,ψ_1) and (E_2,ψ_2) be the Deuring lifts of $(\bar{E}_1,\pi_1)$ and $(\bar{E}_2,\pi_2)$ to characteristic $\mathbb{C}$. Suppose there is an isogeny $\phi\colon E_1\to E_2$. Then the reduced isogeny $\bar{\phi}\colon E_1\to E_2$ is defined over $\mathbb{F}_p$.*

Proof. Let G be the Galois group of $\bar{\mathbb{F}}_p/\mathbb{F}_p$, we have to prove that for all $\sigma\in G$ $\bar{\phi}^{\sigma}=\bar{\phi}$. We can assume $\bar{\phi}$ defined over $\mathbb{F}_{p^r}$ for some $r\geq 0$ and consider only σ in the Galois group of $\mathbb{F}_{p^r}/\mathbb{F}_p$. This is a finite cyclic group generated by the p-Frobenius σ_0, then it is enough to show that the isogeny is fixed by it.
We can suppose that the embedding of $\mathrm{End}(E_c)$ in $\mathbb{C}$ maps ϕ_c to $i\sqrt{p}$. Then $\phi\circ i\sqrt{p}=i\sqrt{p}\circ\phi$, since in characteristic 0 isogenies correspond to multiplication with a complex number. After reduction the isogeny $\bar{\phi}$ commutes with the Frobenius, i.e. $\bar{\phi}\circ\pi_1=\pi_2\circ\bar{\phi}$. $\bar{E}_1,\bar{E}_2$ are defined over $\mathbb{F}_p$ then for each $Q\in\bar{E}_1$

$$\bar{\phi}^{\sigma_0}(Q)=\bar{\phi}^{\sigma_0}(Q^{\sigma_0})=(\bar{\phi}(Q))^{\sigma_0}=\pi\circ\bar{\phi}(Q)=\bar{\phi}\circ\pi(Q)=\bar{\phi}(Q^{\sigma_0})=\bar{\phi}(Q).$$

□

It remains to prove that every isogeny can be reached by reduction. Let us fix ℓ a prime different from p and $E/\mathbb{F}_p$ a supersingular elliptic curve ($p>3$) and ϕ an ℓ-isogeny defined over $\mathbb{F}_p$. Such a map corresponds to a Galois invariant cyclic subgroup $\langle P\rangle$ of $E[\ell]$, being Galois invariant here specifically means that $\pi(\langle P\rangle)=\langle P\rangle$, then it must exist $a\in\mathbb{Z}$ such that

$$\pi(P)=[a]P$$

This means that we have to search between the eigenspaces of the action induced by Frobenius over $E[\ell]$. Repeating the arguments of Remark 3.3.12, we can consider the minimal polynomial of the Frobenius map restricted to $E[\ell]$

$$x^2+p \mod \ell.$$

If it is irreducible, there are not Galois invariant cyclic subgroup, then no ℓ-isogenies exist. Otherwise π can be represented in one of the following two form:

$$\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix} \text{ or } \begin{pmatrix} \lambda & 0 \\ \gamma & \lambda \end{pmatrix}$$

In first case there are 2 Galois invariant cyclic subgroup, in the latter there are $\ell+1$ if $\gamma = 0$ or only 1 if $\gamma \neq 0$. Note that the polynomial $x^2 + p \mod \ell$ can have a double root if and only if $\ell = 2$. Furthermore $\gamma = 0 \mod 2$ if and only if $E[2] \subseteq \ker(1-\pi)$, since the map of multiplication by 2 is separable and there exists an unique separable ϕ such that $2\phi = 1 - \pi$. ϕ is the quotient of two $\mathbb{F}_p$-isogeny then $\phi \in \mathrm{End}_{\mathbb{F}_p}(E)$. So, $\mathrm{End}_{\mathbb{F}_p}(E) \supsetneq \mathbb{Z}[\pi]$ which means that this case can occur if and only if $p \equiv 3 \mod 4$. Let us fix

$$\mathrm{End}_{\mathbb{F}_p}(E) = \mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$$

integral relation of the generator is $p(x) = x^2 + x + (p+1)/2$ then

- if $p \equiv 7 \mod 8$ (i.e. 2 split in $\mathcal{O}_K$) we have two ideal of norm 2, then there are two horizontal isogenies and one descending;
- if $p \equiv 3 \mod 8$ (i.e. 2 is inert in $\mathcal{O}_K$) there are 3 descending isogenies.

If $\mathrm{End}_{\mathbb{F}_p}(E) = \mathbb{Z}[\pi]$ there is only one 2-isogeny which will be necessarily horizontal if $p \equiv 1 \mod 4$ while one ascending 2-isogeny if $p \equiv 3 \mod 4$. If ℓ is an odd prime, there exist two horizontal isogenies if and only if $\left(\frac{-p}{\ell}\right) = 1$.

Let us summarize what we just proved:

Theorem 4.2.8. *Let $p > 3$ a prime.*

1. *If $p \equiv 1 \mod 4$, there are $h(-4p)$ $\mathbb{F}_p$-isomorphism classes of supersingular elliptic curves over $\mathbb{F}_p$, all having the same endomorphism ring $\mathbb{Z}[\sqrt{-p}]$. From every one there is one outgoing $\mathbb{F}_p$-horizontal 2-isogeny as well as two horizontal ℓ-isogenies for every prime $\ell > 2$ with $\left(\frac{-p}{\ell}\right) = 1$.*
2. *If $p \equiv 3 \mod 4$, there are two levels in the supersingular isogeny graph. From each vertex there are two horizontal ℓ-isogenies for every prime $\ell > 2$ with $\left(\frac{-p}{\ell}\right) = 1$. Furthermore:*
   (a) *If $p \equiv 7 \mod 8$, on each level there are $h(-p)$ vertices. Surface and floor are connected one to one with 2-isogenies and on the surface we also have two horizontal 2-isogenies from each vertex.*
   (b) *If $p \equiv 3 \mod 8$, we have $h(-p)$ vertices on the surface and $3h(-p)$ on the floor. Surface and floor are connected one to three with 2-isogenies, and there are no horizontal 2-isogenies.*

Let us compare this theorem with Proposition 3.3.5:

- Let be $p \equiv 3 \mod 4$.
  - If $\mathrm{End}(E) = \mathcal{O}_K$ the conductor f is one. If $\ell \neq 2$, there exists two isogeny if $\left(\frac{-p}{\ell}\right) = 1$, any if $\left(\frac{-p}{\ell}\right) = -1$. If $\ell = 2$, $\left(\frac{-p}{2}\right) = 0$ then there are two horizontal isogeny and one descending.

- If $\text{End}(E) = \mathbb{Z}[\sqrt{-p}]$ the conductor $f = 2$ is maximal, so there is one ascending 2-isogeny and two horizontal ℓ-isogenies if $\ell \neq 2$.

- Let be $p \equiv 1 \mod 4$. There are always two or zero ℓ-isogenies if ℓ is odd. Since the discriminant is even, we can have only a 2-horizontal isogeny.

The structure of the ℓ isogeny graph then is the same of ordinary case:

Proposition 4.2.9. *There exists a one-to-one correspondence between the ℓ-isogenies defined over $\mathbb{F}_p$ between supersingular elliptic curves defined over $\mathbb{F}_p$ and and ℓ-isogenies between elliptic curves defined over $\mathbb{C}$ with complex multiplication induced by $\mathcal{O} \in \{\mathcal{O}_K, \mathbb{Z}[\sqrt{-p}]\}$ where $K = \mathbb{Q}(\sqrt{-p})$.*

Example 4.2.10. Let us consider the the prime $p = 71$, Figure 3.5 represents the supersingular isogeny graph of degree 2 and Figure 3.6 of degree 3 in $\overline{\mathbb{F}}_{71}$. We note that in $\#S_{p^2} = \#S_p = 7$ and all the j-invariant are defined over $\mathbb{F}_p$. We have that $p \equiv 7 \mod 8$, for $\ell = 3$ we obtain two craters (we use $*$ for the twisted isomorphism class), see Figure 4.1; while for $\ell = 2$ we have two levels as we see in Figure 4.2.

Our aim is to give and algorithm to solve the general isogeny problem between supersingular elliptic curves defined over $\mathbb{F}_p$. We have showed that there is equivalence of category between supersingular elliptic curves defined over $\mathbb{F}_p$ and elliptic curves defined over $\mathbb{C}$ with complex multiplication induced by $\mathcal{O} \in \{\mathcal{O}_K, \mathbb{Z}[\sqrt{-p}]\}$ where $K = \mathbb{Q}(\sqrt{-p})$. Hence, there is a transitive action of $\text{Cl}(\mathcal{O})$ on the $\mathbb{F}_p$-isomorphism classes of supersingular elliptic curves defined over $\mathbb{F}_p$ $\mathcal{E}_p(p)$, then fixed E is well defined

$$\begin{array}{rccc} f_E\colon & \text{Cl}(\mathcal{O}) & \longrightarrow & \mathcal{E}_p(p) \\ & [I] & \longmapsto & \tilde{\kappa}([I], E) \end{array}$$

Similarly to the ordinary case presented in section 4.1.2, we can reduce our problem to the abelian hidden shift problem and use the same algorithm, taking care of the role of $\text{End}(E)$ is replaced by $\text{End}_{\mathbb{F}_p}(E)$. Furthermore, by the fact that the volcano has the special form described above some steps can be optimized:

- In the algorithm to evaluate the isogeny star, analogous to Algorithm 4.1, we can exclude a priori primes whose norm is a prime ℓ such that $\left(\frac{-p}{\ell}\right) \neq 1$.

- In order to have an horizontal isogeny, before starting the computation, we can climb the volcano until the surface. We know that for this operation is enough to compute at most a single 2-isogeny. In particular, if the modular polynomial $\Phi_2(j(E), X)$ has three root modulo p is nothing to do; otherwise if it has one root j', it is the invariant of an isogenous curve on the floor so we compute the ascending isogeny to such curve.

Complexity

Algorithm 4.4 summarizes the method purposed to find an isogeny between supersingular curves E, E' defined over $\mathbb{F}_q$. In step 1 and 2 we reduce the problem to curves defined over $\mathbb{F}_p$ and we saw that each step runs in $\widetilde{O}(p^{1/4})$ by Theorem 4.2.2. We showed that step 3 can be interpreted as an abelian

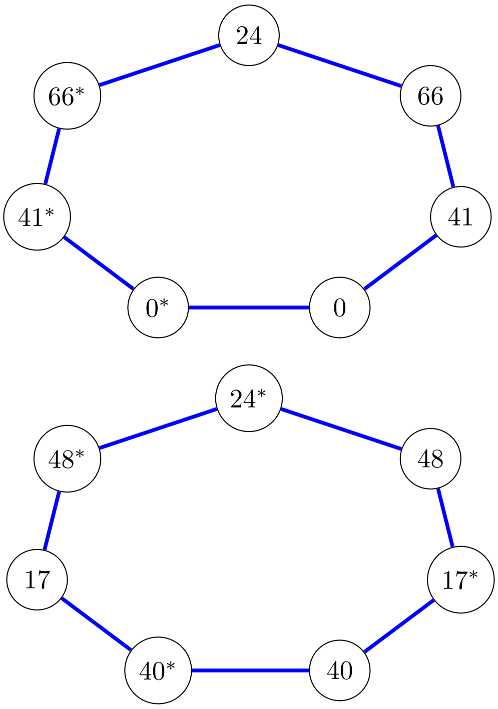

Figure 4.1: Supersingular isogeny graphs of degree 3 over $\mathbb{F}_{71}$

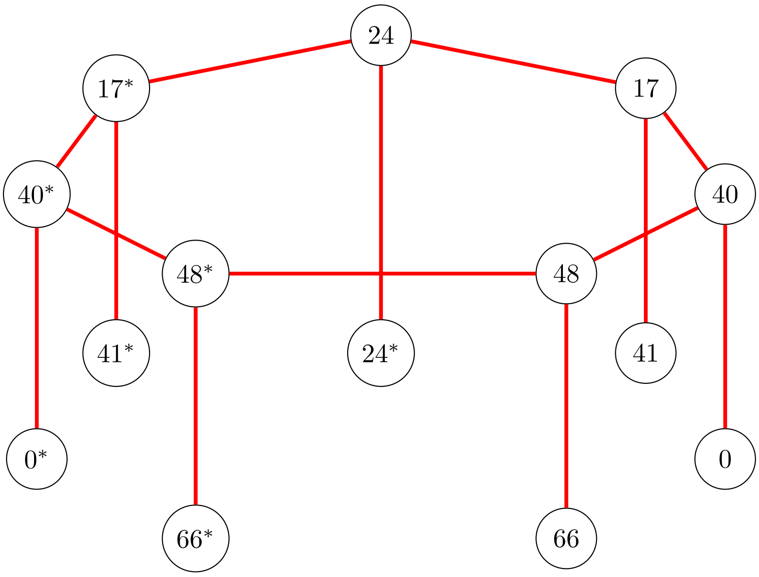

Figure 4.2: Supersingular isogeny graphs of degree 2 over $\mathbb{F}_{71}$

hidden shift problem and, assuming the GRH, it can be performed on a quantum computer in $L_p(1/2, \sqrt{3}/2)$ by Theorem 4.1.5. Moreover, if both curves are defined over $\mathbb{F}_p$ steps 1 and 2 can be skipped. We have just prove the following theorem:

Theorem 4.2.11. *Under the General Riemann Hypothesis, Algorithm 4.4 is correct and run in quantum complexity* $\widetilde{O}(p^{1/4})$*. In particular, if both curves are defined over* $\mathbb{F}_p$*, the quantum complexity decreases to* $L_p\left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$.

Chapter 5

Supersingular Isogeny Diffie Hellman

The hardness of computing isogenies between elliptic curves has encouraged the developing of quantum-resistant cryptographic protocols, whose security relies on this problem. The first one was proposed by Rostovtsev and Stolbunov in 2011 [RS06] and it employed paths in the ordinary isogeny graph. However, using that protocol is unfeasible because arithmetical operations in ordinary curves are slow. This property justify why ordinary curves are a good choice for protocols based on elliptic curve discrete logarithm problem. On the contrary, supersingular curve are discarded in protocol based on discrete logarithm since operations on them are faster. This fact suggest to employ supersingular curves instead ordinary. De Feo and Jao in [JDF11] introduced a candidate quantum resistant system on Diffie Hellman model: the *Supersingular Isogeny Diffie Hellman* key exchange. In this chapter we describe it and a public-key encryption method obtained from. Then we discuss the choice of the parameters and its consequence on the security.

5.1 Key Exchange

In this section we present the Supersingular Isogeny Diffie Hellman (SIDH) key-exchange protocol. Let us fix E_0 a supersingular elliptic curve defined over the finite field $\mathbb{F}_q$. We suppose $q = p^2$ and $p \gg 0$ be a prime of the form $\ell_A^{e_A} \cdot \ell_B^{e_B} \cdot f \pm 1$, where

- ℓ_A and ℓ_B are chosen to be small primes (we take almost always $\ell_A = 2$ and $\ell_B = 3$)
- f a cofactor
- e_A and e_B are positive integers such that $\ell_A^{e_A} \approx \ell_B^{e_B} \approx \sqrt{p}$.

Without loss of generality, we can suppose also that E_0 is such that

$$\#E_0(\mathbb{F}_q) = (\ell_A^{e_A} \cdot \ell_B^{e_B} \cdot f)^2,$$

indeed by Theorem 1.5.7 we know that a curve with this property exists.
Last assumption implies that the torsion subgroups $E_0[\ell_A^{e_A}]$ ed $E_0[\ell_B^{e_B}]$ are $\mathbb{F}_q$-rational. We recall that the group $E_0[\ell^e]$ for $\ell \neq p$ is isomorphic to $(\mathbb{Z}/\ell^e\mathbb{Z})^2$ and it contains $\ell^{e-1}(\ell+1)$ cyclic subgroups of order ℓ^e , each defining an isogeny. We can consider two set of bases $\{P_A, Q_A\}$ and $\{P_B, Q_B\}$ of $E_0[\ell_A^{e_A}]$ ed $E_0[\ell_B^{e_B}]$, respectively. The idea is to use this points to define two secret isogenies ϕ_A and ϕ_B and to obtain a commutative diagram

$$\begin{tikzcd}
& E_0 \arrow[dl, "\phi_B"'] \arrow[dr, "\phi_A"] & \\
E_0/\langle R_B\rangle \arrow[dr] & & E_0/\langle R_A\rangle \arrow[dl] \\
& E_0/\langle R_A, R_B\rangle &
\end{tikzcd}$$

In order to find a shared secret key Alice e Bob, respectively, fix two points $R_A = m_A P_A + n_A Q_A$ and $R_B = m_B P_B + n_B Q_B$ with $m_A, n_A \in \mathbb{Z}/\ell_A^{e_A}$ not both divisible by ℓ_A, idem $m_B, n_B \in \mathbb{Z}/\ell_B^{e_B}$. In this way, they obtain two separable isogenies $\phi_A \colon E_0 \to E_A$ e $\phi_B \colon E_0 \to E_B$ of degree $\ell_A^{e_A}$ e $\ell_B^{e_B}$, with $E_A \simeq E_0/\langle R_A\rangle$ and $E_B \simeq E_0/\langle R_B\rangle$. For $i = A, B$, the ephemeral key is the couple (m_i, n_i) or equivalently the isogeny ϕ_i with $i \in \{A, B\}$, while E_i is published.
Classical Diffie Hellman require commutativity. Here extra information must be communicated as part of the key in order to ensure that both parties arrive at the same common value. Thus, Alice computes $\{\phi_A(P_B), \phi_A(Q_B)\}$ and she makes it public with E_A. Bob proceeds *mutatis mutandis.* Through the public keys

$$(E_A, \phi_A(P_B), \phi_A(Q_B))$$

$$(E_B, \phi_B(P_A), \phi_B(Q_A))$$

and the common setup values $(E_0, p, \ell_A, \ell_B, e_A, e_B)$, both Alice and Bob can compute the secret shared key which is the j-invariant of the curve

$$E = E_0/\langle m_A P_A + n_A Q_A, m_B P_B + n_B Q_B\rangle. \tag{5.1}$$

Indeed Bob can compute the isogeny ϕ_B' from E_A to

$$E_{BA} = E_A/\langle m_B\phi_A(P_B) + n_B\phi_A(Q_B)\rangle$$

and Alice the isogeny ϕ_A' from E_B to

$$E_{AB} = E_B/\langle m_A\phi_B(P_A) + n_A\phi_B(Q_A)\rangle.$$

By the choice of the parameters above, the curves E_{AB} and E_{BA} are isomorphic and $j(E_{AB}) = j(E_{BA})$.

$$\begin{tikzcd}
& E_0 \arrow[dl, "\phi_B"'] \arrow[dr, "\phi_A"] \arrow[dd, dashed] & \\
E_0/\langle R_B \rangle \arrow[dr, "\phi'_A"'] & & E_0/\langle R_A \rangle \arrow[dl, "\phi'_B"] \\
& E_0/\langle R_A, R_B \rangle &
\end{tikzcd}$$

Figure 5.1 summarizes the full protocol.

Public parameters	Primes ℓ_A, ℓ_B, and a prime $p = \ell_A^{e_A} \cdot \ell_B^{e_B} \cdot f \pm 1$, A supersingular elliptic curve E_0 over $\mathbb{F}_{p^2}$ of order $(p \mp 1)^2$, A basis $\{P_A, Q_A\}$ of $E_0[\ell_A^{e_A}]$, A basis $\{P_B, Q_B\}$ of $E_0[\ell_B^{e_B}]$.	
	Alice	**Bob**
Pick random secret	$R_A = m_A P_A + n_A Q_A$	$R_B = m_B P_B + n_B Q_B$
Compute secret isogeny	$\phi_A \colon E_0 \to E_A$	$\phi_B \colon E_0 \to E_B$
Exchange data	$E_A, \phi_A(P_B), \phi_A(Q_B)$	$E_B, \phi_B(P_A), \phi_B(Q_A)$
Compute shared secret	$j\left(E_B/\langle m_A\phi_B(P_A) + n_A\phi_B(Q_A)\rangle\right)$	$j\left(E_A/\langle m_B\phi_A(P_B) + n_B\phi_A(Q_B)\rangle\right)$

Figure 5.1: SIDH Key exchange.

5.2 Public Key Encryption

Directly from the key exchange protocol we can obtain a public key encryption model, as from Diffie Hellman is obtained El Gamal. Using the same notation as above, we define the following four functions:

Setup: Choose $p = \ell_A^{e_A} \cdot \ell_B^{e_B} \cdot f \pm 1$, E_0, $\{P_A, Q_A\}$ and $\{P_B, Q_B\}$. Let $\mathcal{H} := \{H_k \mid k \in \mathcal{K}\}$ be a a family of hash functions indexed by a finite set of keys $\mathcal{K}$, where each H_k is a function from $\mathbb{F}_{p^2}$ to the message space $\{0,1\}^w$.

Key generation: Fix $R_A = m_A P_A + n_A Q_A$ with $m_A, n_A \in \mathbb{Z}/\ell_A^{e_A}$ not both divisible by ℓ_A and compute $E_A, \phi_A(P_B), \phi_A(Q_B)$ and choose a random $k \in \mathcal{K}$.

The public key is the tuple $(E_A, \phi_A(P_B), \phi_A(Q_B), k)$ and the private key is (m_A, n_A, k).

Encryption: Given a message $m \in \{0,1\}^w$ and a public key (E, P, Q, k), choose $R_B = m_B P_B + n_B Q_B$ with $m_B, n_B \in \mathbb{Z}/\ell_B^{e_B}$ not both divisible by ℓ_B and compute $E_B, \phi_B(P_A), \phi_B(Q_A)$. Then compute[1]

$$c = H_k(j(E_{AB})) \oplus m$$

The cyphertext is $(E_B, \phi_B(P_A), \phi_B(Q_A), c)$.

[1] The $\oplus$ operator is the binary sum, i.e. the sum bit to bit.

Decryption: Given a cyphertext (E', P', Q', c) and a private key (m_A, n_A, k), compute the plaintext

$$m = H_k(j(E_{AB})) \oplus c.$$

5.3 Parameters

In practice, one of the main problem of the isogeny based cryptosystem is the time of computation and the space required. There exist other examples of isogeny based protocols, but often they are shown to be impracticable, like [RS06]. Hence the choice of the curves and parameters have to be made in order to make the protocol described feasible, specifically to maximize both speed of performance and safety. The main issues are the choice of the curve E_0, of the primes and the base points of the torsion groups. To choose a random curve, let us consider $E/\mathbb{F}_{p^2}$ such that $\#E(\mathbb{F}_{p^2}) = (p \mp 1)^2$ for a fixed prime p. Starting from E, one can select a random supersingular curve E_0 defined over $\mathbb{F}_{p^2}$ by means of random walks on the $\mathbb{F}_q$-isogeny graph. Since E and E_0 are isogenous, they must have the same number of $\mathbb{F}_q$-rational points and the hypothesis are satisfied.
To find a basis for $E_0[\ell_A^{e_A}]$ we select a random point $P \in E_0(\mathbb{F}_{p^2})$ and multiply it by $(\ell_B^{e_B} f)^2$ to obtain a point P' of order dividing $\ell_A^{e_A}$. The probability that the order is exactly $\ell_A^{e_A}$ is $1/(\ell_A^{2(e_A-1)}(\ell_A^2 - 1))$. By multiplication one can check the order and if it is not correct restart with another random point. To find another point Q the same strategy can be used and to check if they are linearly independent it is enough computing Weil pairing $e_{\ell_A^{e_A}}(P', Q)$ and verifying that the result has order $\ell_A^{e^A}$. Similarly, we can find a base for $E[\ell_B^{e_B}]$. Note that the choice of basis has no effect on the security of the scheme, since one can convert from one basis to another using extended discrete logarithms, which is easy on supersingular curves.
Regarding the isogenies, as we discussed in the previous chapter, if the degrees are powers of small primes we can substantially reduce the cost of Vélu formulae (Theorem 1.2.12) by factoring in small degree isogenies. In particular, if we choose $\ell_A = 2$ and $\ell_B = 3$ there exist special optimized algorithms to compute the isogenies, see for example [JDF11] or [CLN16].
A family of curves, good for our aim, is the family of *Montgomery curves*.

Definition 5.3.1. Let $a, b \in \mathbb{F}_q$ be elements satisfying

$$b(a^2 - 4) \neq 0 \ \text{ in } \ \mathbb{F}_q$$

where we suppose that the characteristic different from 2. A *Montgomery curve* $E_{a,b}$ defined over $\mathbb{F}_q$ is the elliptic curve of equation

$$by^2 = x^3 + ax^2 + x$$

with the point at infinity O.

The j-invariant of the elliptic curve $E_{a,b}$ is

$$\frac{256(a^2-3)^3}{a^2-4}$$

and given two points $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$, with $P \neq \pm Q$ the point $R = P + Q$ has coordinates

$$x_R = b\lambda^2 - (x_P + x_Q) - a$$

and

$$y_R = \lambda(x_P - x_R) - y_P,$$

with $\lambda = (y_P - y_Q)/(x_P - x_Q)$.
Let now consider the *point doubling* and *tripling* formulae over a fixed curve $E_{a,b}$. If $P = (x_P, y_P)$ is a point of odd order then

$$[2]P = \left(\frac{(x_P^2 - 1)^2}{4x_P(x_P^2 + ax_P + 1)}, y_P \frac{(x_2^P - 1)(x_P^4 + 2ax_P^3 + 6x_P^2 + 2ax_P + 1)}{8x_P^2(x_P^2 + ax_P + 1)^2} \right) \tag{5.2}$$

If $P = (x_P, y_P)$ is a point of order coprime with 3 then

$$x_{[3]P} = \frac{(x_P^4 - 4ax_P - 6x_P^2 - 3)^2 x_P}{(4ax_P^3 + 3x_P^4 + 6x_P^2 - 1)^2} \tag{5.3}$$

Formoulae (5.2) and (5.3) lend to optimized implementation respect to the standard one. Moreover, Montgomery curves have very efficient arithmetic on their Kummer line, i.e., by representing points by the coordinates $(X : Z)$ where $x = X/Z$. Using this representation, a point scaled to have Z-coordinate equal to 1 can be doubled at $3M + 2S$, or $2M + 2S$ (where we write M, S for the costs of one multiplication and squaring, respectively, in terms of number of elementary operations in $\mathbb{F}_{p^2}$, and we make the assumption $S \leq M$). For details see [DFJP14] 4.3.

The standard curve purposed in SIKE [JCDF+17] to the National Institute of Standars and Technology U.S. call [oST] is

$$E_0/\mathbb{F}_{p^2} : y^2 = x^3 + x$$

with $\ell_A = 2$ and $\ell_B = 3$ so that $p = 2^{e_2}3^{e_3} - 1$. Note that $E_0(\mathbb{F}_{p2}) = (2^{e_2}3^{e_3})^2$ and that its j-invariant is $j(E_0) = 1728$. Also note that it is a Montgomery curve with $b = 1$ and $a = 0$. For $w \in \{8, 12, 16\}$, the parameters given in Section 1.5 of the documentation of SIKE provide that the prime fields with $p = 2^{e_2}3^{e_3} - 1$ were determined so that $\log_2 p \leq 64w$, i.e., the prime does not exceed $64w$ bits. For each w, these primes were chosen with the aim of maximizing the overall security and achieving a close balance on both sides of the protocol, in particular maximizing the value of $\min\{e_2, \log_2 3^{e_3}\}$ such that $2^{e_2} \approx 3^{e_3}$. A large part of the discussion about the standardization has been the improvement of the performance. A remarkable variation to original protocol is that instead to give two point for each torsion group involved, they give three points in order to be able to work only with the x-coordinates and to benefit from efficient arithmetic over Kummer line.

Let us consider some examples. The following two have parameters of small dimension and they are useful mostly to understanding, while in Appendix B we produce an example in which the parameter selection provides an effective 128-bit secure exchange.

Example 5.3.2. **Setup:**
Alice and Bob fix the prime $p = 71 = 2^3 3^2 - 1$ and the curve

$$E_0/\mathbb{F}_{71^2} \colon y^2 = x^3 + x$$

Here we identify $\mathbb{F}_{71^2}$ with

$$\mathbb{F}_p(\alpha) = {}^{\mathbb{F}_{71}[t]}\!\big/_{(t^2 + 69t + 7)}.$$

The points

$$P_A = (67\alpha + 30, 49\alpha + 17) \text{ and } \quad Q_A = (67, 28)$$

and

$$P_B = (17, 57\alpha + 14) \text{ and } \quad Q_B = (64, 17)$$

form a basis of $E_0[8]$ and $E_0[9]$, respectively.
Alice key generation:
Alice chooses the integers $m_A = 2$ and $n_A = 5$, she computes the point

$$R_A = 2P_A + 5Q_A = (55\alpha + 3, 35\alpha + 60)$$

of order 8 and the isogeny

$$\phi_A \colon E_0 \longrightarrow E_A = E_0/\langle R_A \rangle$$

obtaining the curve $E_A \colon y^2 = x^3 + 22x + 36$ with j-invariant 40.
Then she computes

$$\phi_A(P_B) = (13, 35\alpha + 36) \text{ and } \quad \phi_A(Q_B) = (39, 54)$$

and sends $(E_A, \phi_A(P_B), \phi_A(Q_B))$ to Bob.
Bob key generation:
Bob chooses the integers $m_B = 7$ and $n_B = 6$, he computes the point

$$R_B = 7P_B + 6Q_B = (\alpha + 47, 58\alpha + 45)$$

of order 9 and the isogeny

$$\phi_B \colon E_0 \longrightarrow E_B = E_0/\langle R_B \rangle$$

obtaining the curve $E_B \colon y^2 = x^3 + (62\alpha + 65)x + (58\alpha + 55)$ with j-invariant 40.
Then he computes

$$\phi_B(P_A) = (8\alpha + 6, 34\alpha + 29) \text{ and } \quad \phi_B(Q_A) = (52\alpha + 52, 8\alpha + 32)$$

and sends $(E_B, \phi_B(P_A), \phi_B(Q_A))$ to Alice.
Alice shared key recover:
Alice finds

$$S_A = 2\phi_B(P_A) + 5\phi_B(Q_A) = (16\alpha + 65, 65\alpha + 20)$$

and

$$\phi'_A \colon E_B \longrightarrow E_{AB} = {}^{E_B}\!\big/_{\langle S_A \rangle}$$

And she obtains $j = 66$.
Bob shared key recover:
Bob finds

$$S_B = 7\phi_A(P_B) + 6\phi_A(Q_B) = (30\alpha + 41, 48\alpha + 2)$$

and

$$\phi'_B : E_A \longrightarrow E_{BA} = {}^{E_A}\!\!\diagup_{\langle S_B \rangle}$$

And he obtains $j = 66$.
Note that in this example Alice and Bob find two isomorphic curves during the private key generation. This phenomenon depends one the size of the prime p. Indeed $71 \equiv 11 \mod 12$ hence the number of supersingular j it is 7, by equation (1.14), and the degrees of the isogenies are and $8, 9 > 7$; this means that the paths, which we are considering, certainly have loops in the isogeny graph. See Figures 3.5 and 3.6 and Example 4.2.10.
Let us suppose Bob makes a different choice.
Bob key generation (2):
Bob selects $m_B = 0$ and $n_B = 1$, he computes the point

$$R_B = Q_B = (64, 17)$$

of order 9 and the isogeny

$$\phi_B : E_0 \longrightarrow E_B = E_0/\langle R_B \rangle$$

obtaining the curve $E_B : y^2 = x^3 + 47x + 45$ with j-invariant 41.
Then he computes

$$\phi_B(P_A) = (13\alpha + 18, 51\alpha + 15) \quad \text{and} \quad \phi_B(Q_A) = (58, 52)$$

and sends $(E_B, \phi_B(P_A), \phi_B(Q_A))$ to Alice.
Alice shared key recover (2):
Alice finds

$$S_A = 2\phi_B(P_A) + 5\phi_B(Q_A) = (64\alpha + 18, 35\alpha + 67)$$

and

$$\phi'_A : E_B \longrightarrow E_{AB} = {}^{E_B}\!\!\diagup_{\langle S_A \rangle}$$

And she obtains $j = 48$.
Bob shared key recover(2):
Bob finds

$$S_B = \phi_A(Q_B) = (39, 54)$$

and

$$\phi'_B : E_A \longrightarrow E_{BA} = {}^{E_A}\!\!\diagup_{\langle S_B \rangle}$$

And he obtains $j = 48$.
In this second key exchange we want to underline another possible behavior: the curve E_0 is defined over $\mathbb{F}_p$, Bob chooses a point in $E_0(\mathbb{F}_p)$ and the isogeny ϕ_B results defined over $\mathbb{F}_p$. Potentially, this is a bad thing because such an isogenies is quite easier to recover by a quantum computer[2] (lucky, however, it is sufficiently hard).

[2] See Section 4.2.2.

5.4 Parameters Discussion and Security

If we could efficiently solve the general isogeny problem, the system would be unsafe. In fact, we could for example compute some isogenies ϕ from E_0 and E_A then combining that in order to obtain a degree of degree $\ell_A^{e_A}$ (we will specify what we mean later in this section) and verifying that $\phi_A(P_B)$ $\phi_A(Q_B)$ are correct. Using discrete logarithms, which is easier on supersingular curves, we could compute m_A, n_A and obtain ϕ'_B.

$$\begin{tikzcd}
 & E_0 \arrow[dl, "\phi_B"'] \arrow[dr, "\phi_A"] \arrow[dd, dashed] \arrow[dr, bend left=60, "\phi"] & \\
E_0/\langle R_B\rangle \arrow[dr, "\phi'_A"'] & & E_0/\langle R_A\rangle \arrow[dl, "\phi'_B"] \\
 & E_0/\langle R_A, R_B\rangle &
\end{tikzcd}$$

It is clear that the key space of SIDH depends on the size of the subgroups $E[\ell_A^{e_A}]$ and $E[\ell_B^{e_B}]$, in fact an exhaustive query of an isogeny breaking the cryptosystem employs

$$\min\left\{O(\ell_A^{e_A}), O(\ell_B^{e_B})\right\}.$$

The choice $\ell_A^{e_A} \approx \ell_B^{e_B} \approx \sqrt{p}$ maximizes that complexity, which results $O(\sqrt[4]{p})$. Let us recall that the supersingular isogeny graph has $O(p)$ nodes, by equation (1.14) and since the key spaces are of size $O(\sqrt{p})$ Alice and Bob take random walks much shorter than the diameter of the graph. At this moment, it is not clear how this affects the security of the protocol. In Example 5.3.2 we saw that loops may be a problem, obviously in that case the problem was that the prime was too small. In general, we suppose $p \gg 0$ and there would not be loops since we have suppose the kernel cyclic of order the maximal power of ℓ_A (resp. ℓ_B) in $E_0(\mathbb{F}_q)$.

In order to break our key exchange protocol is enough to solve a more special problem than the general isogeny problem. First of all, the degrees of the isogenies are known in advance and they are smooth. This observation suggest a different approach: the idea is to build a path by constructing two isogeny trees, starting at E_0 and E_A, consisting of all paths of length $e_A/2$; a curve that occurs as a leaf in both trees then immediately leads to the sought isogeny. Due to the sizes, in fact, we expect to find precisely one path. We can see this as an instance of the *claw problem*:

Problem 8 (Claw problem). *Given two functions $f\colon \Omega \to C$ and $g\colon \Omega' \to C$, find a pair $(a, b) \in \Omega \times \Omega'$, called* claw, *such that $f(a) = g(b)$.*

If $\#\Omega = N$ and $\#\Omega' = M$ and $N < M$, on a classical computer this problem can be solved in time $O(M + N)$ and $O(N)$ space by building a hash table for

$f(a)$ for $a \in \Omega$ and comparing with $g(b)$ for all $b \in \Omega'$. In the article [Tan07], it is proven by Tani that, if $N \leq M < N^2$, a quantum computer can find a collision in $O(\sqrt[3]{NM})$. In our context Ω is the set of nodes in the ℓ_A-isogeny graph which can be reached in $e_A/2$ steps from E_0, similarly Ω' is the set of nodes in the ℓ_A-isogeny graph which can be reached in $e_A/2$ steps from E_A. In particular, they have equal size $N = O(\sqrt[4]{p})$, thus we have a quantum complexity $O(\sqrt[6]{p})$. The security of the protocol is not effected by this result, however it stresses that the problem of the security of SIDH should be easier to the general isogeny problem, which we showed in the previous chapter has quantum complexity $\widetilde{O}(\sqrt[4]{p})$.
Taking $\log_2 p = n$ this approach offers a classical security of about $n/4$ bits, and a quantum security of about $n/6$ qubits. For example, to obtain a 128-qubit and 192-bit secure system, we would have to find a 768-bit prime of the form $\ell_A^{e_A} \cdot \ell_B^{e_B} \cdot f \pm 1$, with$e_A \log(\ell_A) \approx e_B \log(\ell_B) \approx 384$. In practice, we usually take $\ell_A = 2$ and $\ell_B = 3$ for efficiency reasons, then an example of one such prime is $p = 2^{387}3^{242} - 1$.
It is wort to recall that Theorem 4.2.11 states that if both curve are defined over $\mathbb{F}_p$ the attack proposed by Biasse et al. run in subexponential time; thus it cautions us to employ curve defined over $\mathbb{F}_p$.

Analyzing security, we have to consider that there are still auxiliary information: the action over the torsion points. Let us formalize the complete problem associated to SIDH:

Problem 9 (Supersingular Isogeny Diffie Hellman (SIDH))**.** *Let E_0 be a supersingular elliptic curve defined over a finite field $\mathbb{F}_q$, with $q = p^2$ and $p \gg 0$ is a prime of the form $\ell_A^{e_A} \cdot \ell_B^{e_B} \cdot f \pm 1$, where ℓ_A e ℓ_B are choosen to be small primes. Let $\phi_A \colon E_0 \to E_A$ be an isogeny whose kernel is equal to $[m_A]P_A + [n_A]Q_A$, and let $\phi_B \colon E_0 \to E_B$ be an isogeny whose kernel is $[m_B]P_B + [n_B]Q_B$, where m_A, n_A (respectively m_B, n_B) are chosen at random from $\mathbb{Z}/\ell_A^{e_A}$ (respectively $\mathbb{Z}/\ell_B^{e_B}$) and not both divisible by ℓ_A (respectively ℓ_B). Given*

$$E_A, E_B, \phi_A(P_B), \phi_A(Q_B), \phi_B(P_A), \phi_B(Q_A)$$

find the j-invariant of

$$E_{AB} = {}^{E_A}\!\big/\!_{\langle m_B\phi_A(P_B) + n_B\phi_A(Q_B)\rangle}.$$

Let us focus now on the issue of the action over the two torsion subgroups. Let us suppose to be an adversary who want to recover the secret shared key. We know the image a basis $\{P_B, Q_B\}$ of $E_0[\ell_B^{e_B}]$, then we can compute ${\phi_A}_{|_{E_0[\ell_B^{e_B}]}}$ by linear combinations. It seems not possible to deduce the complete isogeny from this restriction. In particular, we can not use the quantum computers' capability to solve hidden subgroup, because the degree of ϕ_A is coprime with ℓ_B then it does not annihilate any point in $E_0[\ell_B^{e_B}]$, except for the identity. Note that if we could evaluate ϕ_A over points in $E_0[\ell_A^{e_A}]$, by a quantum computer, we could easily break the scheme since the kernel of ϕ_A a hidden subgroup of $E_0[\ell_A^{e_A}]$. Currently, they do not exist specific attacks in De Feo and Jao's hypothesis which involve torsion points. However, very recently Petit at ASIACRYPT 2017 has presented the first (classical) algorithm which take advantage of it under quite different hypothesis. Despite he does not solve the original problem, this work has opened new possibility in such direction and it provides to put further restrains over the opportunity to choice different parameters.

We stated at the beginning of this section that the role of the general isogeny problem is crucial to the security of SIDH. Petit with Galbraith, Shani and Ti in 2016 described a polynomial algorithm to find an isogeny, of the correct degree, arising in these cryptosystem under the assumption that the endomorphism ring have to be known[3]. It is known, see [PL17], that the problem of computing endomorphism rings of supersingular curves is equivalent to the supersingular general isogeny problem and it is believed that both these problems are hard. The contribution of Galbraith et al. is to prove that the hardness of computing endomorphism rings is necessary for the security of any cryptosystem based the scheme we are studying.

Taking into account of these observations, we decided to conclude this section about the security of SIDH with a more precise description of the two algorithms just cited: the *Reduction to Computation of Endomorphism Ring* of Problem 9 and *Using Torsion Point Images to Compute Isogenies.*

5.4.1 Reduction to Computation of Endomorphism Ring

Let us suppose to be in the hypothesis of Problem 9. We stated that SIDH is more special than Problem 6, in particular if we could easy solve the latter we could easy solve the first, too. Let us recall that, in our context, easy means that there exist an algorithm that solve it in $\widetilde{O}(1)$, i.e. polynomially. Thus, saying that SIDH can be reduced to the problem of computing the endomorphism ring of a supersingular elliptic curve means that there exists a polynomial algorithm such that, given the endomorphism rings of the curves involved, computes an appropriate isogeny. In this section we prove that such an algorithm exists, namely that the following theorem holds:

Theorem 5.4.1. *Let E_0 and E_A be supersingular elliptic curves over $\mathbb{F}_{p^2}$ such that $E_0[\ell_A^{e_A}] \subseteq E(\mathbb{F}_{p^2})$ and there is an isogeny $\phi_A \colon E_0 \to E_A$ of degree $n = \ell_A^{e_A}$. Suppose there is no isogeny $\phi \colon E_0 \to E_A$ of degree less than n. Then, given an explicit description of* $\operatorname{End}(E)$ *and* $\operatorname{End}(E_A)$*, there is an efficient probabilistic algorithm to compute ϕ_A.*

Note that additional hypothesis over the degree of the isogeny is not restrictive in our case. We saw, in the previous chapter, that often an index calculus strategy is a good choice in order to obtain a lower degree isogeny from another. Here we have to be careful since we are handling supersingular curve and the setting is non commutative. Let us suppose to know $\operatorname{End}(E_0) = \mathcal{O}$ and $\operatorname{End}(E_A) = \mathcal{O}_A$ two maximal orders in the same quaternion algebra $\mathcal{B}$ ramified at p and ∞ (Theorem 3.5.12). By Lemma 3.5.24, we know I a $\mathcal{O}$-left ideal and

[3] We intend efficiently computable.

$\mathcal{O}_A$-right ideal that connects E_0 and E_A. Computing an isogeny of the correct degree corresponds to compute an ideal equivalent to I of the correct norm. Hence, by Lemma 3.5.22, we have that such degree can be decreased and an appropriate isogeny can be computed by Theorem 1.2.12. We want to prove that all these steps can be performed in polynomial time. Kohel, Lauter, Petit and Tignol in [KLPT14] precisely describe a probabilistic algorithm whose allows us to reach our goal. Indeed they proved that:

Theorem 5.4.2 (Theorem 7 [KLPT14]). *Let $\mathcal{O}$ be a maximal order in a quaternion algebra $\mathcal{B}$ ramified at p and infinity and let $\ell \neq p$ be a small prime. Then there exists a probabilistic algorithm, under the GRH, which takes as input a left $\mathcal{O}$-ideal and it outputs a left $\mathcal{O}$-ideal, in the same class, of ℓ-power reduced norm.*

The main idea is, first, to consider special type of order: the *p-extremal* maximal orders, which are ones containing π such that $\pi^2 = -p$. For a general order, there exists a unique maximal 2-sided ideal P over p, and this ideal is principal if and only if there exists such an element π. The maximal ideal P is a generator of the 2-sided class group and p-extremal orders are precisely those of trivial 2-sided class number. Note that we just encountered such order, indeed these are the maximal orders which are endomorphism rings of elliptic curves defined over $\mathbb{F}_p$, with Frobenius endomorphism π.

Let q coprime with p and i, j such that $i^2 = -q$ and $j^2 = -p$ and $R = \mathcal{O} \cap \mathbb{Q}(i)$, they also restrict to the case in which $R + jR$ is a subring of the p-extremal order $\mathcal{O}$ and the ideal I has reduced norm N, a large prime coprime to ℓ, $|\operatorname{disc}(R)|$ and p. The central observation is that if I would be of the form $\mathcal{O}(N, \beta)$ it would be sufficient to find $\lambda \in \mathbb{Z}$ such that $\gcd(\lambda, N) = 1$ and

$$\sigma \equiv \lambda\beta \mod N\mathcal{O} \tag{5.4}$$

with $\operatorname{nrd}(\sigma) = N\ell^e$ for some positive integer e. Indeed, let $\gamma := \bar{\sigma}/N$ then $[\gamma I] = [I]$ and

$$\operatorname{nrd}(\gamma I) = \operatorname{nrd}(\gamma)\operatorname{nrd}(I) = \frac{\operatorname{nrd}(\sigma)}{N^2}N = \ell^e.$$

The core of the approach in [KLPT14] is that we have an isomorphism

$$\frac{R + Rj}{N(R + Rj)} \simeq \frac{\mathcal{O}}{N\mathcal{O}},$$

since the index of $R + Rj$ in $\mathcal{O}$ is coprime to N, Obviously, choosing representative elements in $R + Rj$ is convenient to simplify the algorithm. The complex and long part of the proof is to show how to find a special $\mathcal{O}$-base, for which the approximation equation (5.4) can be efficiently solved.

In order to generalize the result, let us observe that we proved that any maximal order $\mathcal{O}_2$ in $\mathcal{B}$ is connected to a p-extremal maximal order $\mathcal{O}_1$, i.e. any supersingular elliptic curves is isogenous to a curve defined over $\mathbb{F}_p$, so by Lemma 3.5.24 is polynomially constructible $I = I(\mathcal{O}_1, \mathcal{O}_2)$. Give a J an $\mathcal{O}_2$ left ideal, it can be found a representative left $\mathcal{O}_1$-ideals for I and IJ by Lemma 3.5.22 such that

$$I_1 = I\bar{\gamma}_1/\operatorname{nrd}(I)$$

with $\gamma_1 \in I$ and

$$I_2 = IJ\bar{\gamma}_2/\operatorname{nrd}(IJ)$$

with $\gamma_2 \in IJ$, where

$$\mathrm{nrd}(\gamma_1) = \mathrm{nrd}(I)\ell^{e_1}$$

and

$$\mathrm{nrd}(\gamma_2) = \mathrm{nrd}(IJ)\ell^{e_2}$$

It follows that $\gamma = \bar{\gamma}_1\gamma_2/\,\mathrm{nrd}(I)$ is an element of J with reduced norm $\mathrm{nrd}(\gamma) = \mathrm{nrd}(J)\ell^{e_1+e_2}$, and hence $J\bar{\gamma}/\,\mathrm{nrd}(J)$ is an ideal of reduced norm $\ell^{e_1+e_2}$ in the same class of J.

Proof 5.4.1. Let use consider Algorithm 5.1:

Algorithm 5.1

Input: ℓ_A, E_0, E_A, $\mathcal{O}$, $\mathcal{O}_A$ as in Theorem 5.4.1.
Output: Isogeny $\phi_A \colon E_0 \to E_A$ of small degree $\ell_A^{n_A}$, or *failure*

```
Compute an ideal $I$ connecting $\mathcal{O}$ and $\mathcal{O}_A$
Compute a Minkowski-reduced basis of $I$
Let $\alpha$ be the non-zero element in $I$ of minimum norm
if $\mathrm{nrd}(\alpha) \neq \mathrm{nrd}(I)\ell_A^{n_A}$ then
    return failure
end if
Compute an ideal $J = I\bar{\alpha}/\,\mathrm{nrd}(I)$
Compute the isogeny $\phi_A$ that corresponds to $J$
return $\phi_A$
```

A maximal order in a quaternion algebra is a lattice of rank 4, so a Minkowski base can be computed in polynomial time. Having an explicit representation of $\mathcal{O}$ and $\mathcal{O}_A$ we observed that we can perform by Lemma 3.5.24 steps 1-2. By Lemma 3.5.22, it is sufficient to find an element α in I of minimal reduced norm by hypothesis. By Theorem 5.4.2 we are able to find some isogenies with ℓ_A-power degree, by a finite number of combinations we can find α with smallest norm in polynomial time. □

5.4.2 Using Torsion Point Images to Compute Isogenies

Let us suppose to have E_0 and E supersingular elliptic curves defined over a finite field $\mathbb{F}_q$, with $q = p^2$ and $p \gg 0$ is a prime of the form $N_1 \cdot N_2 \cdot f \pm 1$. Obviously we will think $N_1 = \ell_A^{e_A}$ and $N_2 = \ell_B^{e_B}$, however the result in this section are more general and it enough to suppose N_1 and N_2 smooth coprime integers. Our aim is to find a secret isogeny $\phi\colon E_0 \to E$ of degree N_1, which for example should be the secret key of De Feo-Jao protocol. We suppose to be aware of the action of ϕ over $E[N_2]$ and we also suppose to know that $N_2 \gg N_1$. Note that, in this sense, the algorithm to find ϕ we are going to describe does not solve Problem 9 with the parameter purpose in the original article ($N_1 \approx N_2$).
We also suppose to know non scalar and/or small degree endomorphisms of E_0 and E, namely to know R_0, R two subrings of $\mathrm{End}(E_0)$, $\mathrm{End}(E)$ respectively. Note that it is not actually a restrain, since it sufficient to compute the Frobenius maps.

Let us summarizes the general strategy:

Step 1 Taken $\theta \in \mathrm{End}(E_0)$, whose degree is coprime with N_2, we define $\psi = \phi\theta\hat{\phi}$ (note that if $\theta \in \mathbb{Z}$ then also ψ is scalar).

Step 2 Using the action of ϕ on the N_2, we evaluate ψ on the $E[N_2]$. Then we find an expression of ψ.

Step 3 We evaluate ψ on $E[N_1]$ and by a discrete logarithm (N_1 is smooth) we compute generators for $H = \ker(\phi\theta\hat{\phi}) \cap E[N_1]$.

Step 4 Observing that the group H contains the kernel of $\hat{\phi}$ as a cyclic subgroup of order N_1, we recover $\hat{\phi}$ and deduce ϕ.

We will see that a single call of this model is not better then approaches which does not take advantage to the awareness of the action over torsion points. However, by a *ad hoc* recursion, we can obtain a polynomial complexity when R_0 contains an endomorphism of small degree and $R = \mathbb{Z}$. In particular we will prove in such hypothesis the following statement holds:

Theorem 5.4.3. *Let N_1 and N_2 be coprime smooth numbers, with $\log N_2 = O(\log^2 N_1)$. Then under plausible heuristic assumptions, we can find ϕ in polynomial time when the initial curve E_0 has a small degree endomorphism.*

Now we proceed in the following way: first we describe every steps in details, then we analyze the complexity of the single call and finally we outline the recursion strategy and the proof Theorem 5.4.3. For Step 1 and 3 it is noting to specify.

Step 2: Computing an Endomorphism from Additional Information

Let C be $\deg\psi$ and note that $\gcd(C, N_2) = 1$, we can also suppose C smooth. Let us fix $\{P_0, Q_0\}$ a basis of $E_0[N_2]$ and $\{\phi(P_0) = P, \phi(Q_0) = Q\}$ a basis[4] of $E[N_2]$. First of all we note that we can evaluate the action of ψ over such torsion group despite we do not know ϕ. In fact, we can let $S \in E[N_2]$ for $m, n \in \mathbb{Z}$

$$S = mP + nQ$$

then

$$\begin{aligned}\psi(S) =& m\psi(P) + n\psi(Q)\\ =& m\psi\phi(P_0) + n\psi\phi(Q_0)\\ =& m\phi\theta\hat{\phi}\phi(P_0) + n\phi\theta\hat{\phi}\phi(Q_0)\\ =& N_1(m\phi\theta(P_0) + n\phi\theta(Q_0))\end{aligned}$$

and by the choice of θ it act as an isomorphisms on $E_0[N_2]$ so we can express $\theta(P_0)$ and $\theta(Q_0)$ in terms of the given basis. Thus the desired quantity can be computed.

Let us consider now $\theta_1, \theta_2 \in R$ and let $\eta = \theta_1\psi + \theta_2$. Obviously we can easily obtain $\eta(E[N_2])$, too. We can also suppose that $\deg\eta = C'N_2$ (see Remark

[4] By hypothesis $\gcd(N_1, N_2) = 1$, hence the restriction of ϕ over the N_2 torsion group is invertible.

5.4.4) with $C' \ll N_2$. So there exist η_1 of degree C' and η_2 of degree N_2 such that

$$\eta = \eta_1 \eta_2$$

Under this assumption, we can compute

$$\eta(P) = \eta_1(\eta_2(P)) = \theta_1(\psi(P)) + \theta_2(P)$$

$$\eta(Q) = \eta_1(\eta_2(Q)) = \theta_1(\psi(Q)) + \theta_2(Q)$$

The kernel of η_2 is a subset of $E[N_2]$, since if $S \in \ker \eta_2$ then $S = aP + bQ$

$$\eta_2(S) = 0 \iff a\eta_2(P) + b\eta_2(Q) = 0$$

We also have $\eta(S) = 0$ then

$$0 = a\eta(P) + b\eta(Q)$$

and using Weil pairing we can compute a and b. Repeating this method we can find whole $\ker \eta_2$, namely η_2 by Theorem 1.2.11.

$$\begin{tikzcd}
E \arrow[r, "\eta_2"] \arrow[rr, bend right, "\eta"'] & E' \arrow[r, "\eta_1"] & E
\end{tikzcd}$$

To find η_1, hence η, we can use a *meet-in-the middle* strategy: we have the two j-invariant $j(E)$ and $j(E')$, so starting two random walks in the isogeny graph from the node representing that invariants we search for a collision. We are solving an instance of the problem 6, however we do not want whichever isogeny but the isogeny η_1. Hence we need to remember to check if the result is correct, using addition information. The efficiency and the correctness of this step depends on the factorization of C'.
We can now compute

$${\theta_1}^{-1}(\eta_1\eta_2 - \theta_2)$$

and assuming $\gcd(\deg\theta_1, C) = 1$ we evaluate this map on the C-torsion to identify $\ker\psi$. This is efficient as C is smooth.

Algorithm 5.2 Computing an Endomorphism from Additional Information

Input: $E, \{P, Q\}, \{\psi(P), \psi(Q)\}, C, N_2, R$ as above and a parameter B .
Output: ψ.

```
Find $C' \in \mathbb{N}$ and $\theta_1, \theta_2 \in R$ such that $\deg(\theta_1\psi + \theta_2) = C'N_2$ and
    $\gcd(\deg\theta_1, C) = 1$, and such that $C'$ is $B$-smooth and as small as possible
Compute $\ker\eta_2$ using the additional information
Compute $\eta_1$ with a meet-in-the-middle approach
Compute $\ker({\theta_1}^{-1}(\eta_1\eta_2 - \theta_2))$ by evaluating all maps on the $C$ torsion
return $\psi$
```

Remark 5.4.4. Let ψ be an endomorphism of E of degree C and let us suppose $R = \mathbb{Z}$ (the most generic case). We define for any $a, b \in R$

$$\eta_{a,b} \coloneqq a\psi + b.$$

Observe that

$$\begin{aligned}\deg \eta_{a,b} =&(a\psi + b)(a\hat{\psi} + b)\\ =&a^2 \deg \psi + b^2 + ab \operatorname{Tr} \psi\\ =&\left(b + a\frac{\operatorname{Tr}\psi}{2}\right)^2 + a^2\left(\deg \psi - \left(\frac{\operatorname{Tr}\psi}{2}\right)^2\right)\end{aligned}$$

Our aim is to find a, b such that $\deg \eta_{a,b} = C'N_2$, where C' is as small and as smooth as possible. We must add two additional hypothesis:

i) $N_2 > 2\sqrt{C}$

ii) If $D := \deg \psi - \left(\frac{\operatorname{Tr}\psi}{2}\right)^2$, we suppose

$$\left(\frac{-D}{N_2}\right) = 1 \tag{5.5}$$

Note that if $N_2 = \ell^e$ a power of a prime number the second condition is equivalent to ask

$$\left(\frac{-D}{\ell}\right) = 1 \tag{5.6}$$

which is satisfied with probability about $1/2$; if N_2 is a powersmooth number with small prime factors, heuristically $1/2$ of these primes satisfy (5.6), so there exist $N_2' \approx \sqrt{N_2}$ such that $N_2' \mid N_2$ and $-D$ is a quadratic residue modulo N_2'. Moreover if $N_2 \approx C$ or bigger, we can use N_2' in the attack instead of N_2 , and still satisfy the first condition. Condition i) and ii) are satisfied for a large set of parameters with the expected forms.
We can evaluate ϕ on the points of $E[N_2]$ and, by the relation $\psi\hat{\psi} = [\deg \psi]$, we can compute also $\hat{\phi}(E[N_2])$. Moreove we can evaluate the trace $\operatorname{Tr}(\psi) = \psi + \hat{\psi}$, obtaining the value $\operatorname{Tr}(\psi) \mod N_2$. By the Cauchy-Schwarz inequality we have that $\operatorname{Tr}(\psi) \leq 2\sqrt{\deg \psi}$, under our first parameter restriction, $N_2 > 2\sqrt{C}$, in this way we have found $\operatorname{Tr}(\psi)$ exactly.
By condition ii), there exists τ such that

$$-D \equiv \tau^2 \mod N_2$$

and it can be efficiently computed using Hensel's lifting lemma. The points (x, y) in the lattice generated by

$$(N_2, 0) \text{ e } (\tau, 1)$$

are the solutions of

$$x^2 + Dy^2 = 0 \mod N_2 \tag{5.7}$$

We compute a reduced basis for the lattice in polynomial time. If (x_0, y_0) is well-chosen short vector in the lattice, we put

$$a = y_0,\ b = x_0 - \frac{\operatorname{Tr}(\psi)}{2}y_0$$

$$C' = \frac{x_0^2 + Dy_0^2}{N_2}$$

To obtain such vector, we use the short basis computed above, then we compute the corresponding C' values and we iterate until we obtain C' such that the meet-in-the-middle strategy would be efficient enough.

Remark 5.4.5. First of all we note that, actually, we are in a special instance of Remark 5.4.4. Our isogeny indeed has the special form

$$\psi = \phi\theta\hat{\phi}$$

then

$$\begin{aligned}\deg\psi_{a,b} &= (a\phi\theta\hat{\phi}+b)(\widehat{a\phi\theta\hat{\phi}}+b)\\ &= (a\phi\theta\hat{\phi}+b)(a\phi\hat{\theta}\hat{\phi}+b)\\ &= a^2N_1^2\deg\theta + ab\phi(\theta+\hat{\theta})\hat{\phi}+b^2\\ &= (aN_1)^2\deg\theta + (aN_1)b\operatorname{Tr}\theta + b^2\\ &= \left(b+\tilde{a}\frac{\operatorname{Tr}\theta}{2}\right)^2 + \tilde{a}^2\left(\deg\theta - \left(\frac{\operatorname{Tr}\theta}{2}\right)^2\right)\end{aligned}$$

where $\tilde{a} = aN_1$. So we can search a short vector in

$$x^2 + D_\theta N_1^2 y^2 = 0 \mod N_2$$

where $D_\theta = \deg\theta - \frac{1}{4}\operatorname{Tr}^2\theta$ and set

$$a = y_0,\ b = x_0 - \frac{\operatorname{Tr}(\theta)}{2}N_1 y_0$$

Another thing to underline is that the condition required became

i) $N_2 > 2\sqrt{\deg\theta}$

ii)
$$\left(\frac{-D}{N_2}\right) = 1$$

Note that first statement is potentially weaker.

Step 4: Recovering ϕ from ψ

In Step 3 we have computed $H = \ker(\phi\theta\hat{\phi}) \cap E[N_1]$, where $\phi\theta\hat{\phi} = \psi$ so we have its kernel directly by Step 2. We observed that $\ker\hat{\phi} \subseteq H$ as a cyclic subgroup of order N_1. Therefore, if H is cyclic, there exists only a cyclic subgroup of order N_1 and so it has to be $\ker\hat{\phi}$. Let us suppose now it is not cyclic, we can take the maximum $M \in \mathbb{N}$ such that $M \mid N_1$ and $E[M] \subseteq H$. From the choice of M there exist two isogenies $\phi_{N_1/M}\colon E \to E_M$ of degree N_1/M and $\phi_M\colon E_0 \to E_M$ of degree M such that

$$\phi = \hat{\phi}_{N_1/M}\phi_M$$

$$\begin{tikzcd} E_0 \arrow[r, "\phi_M"] \arrow[rr, bend right, "\phi"'] & E_M \arrow[r, "\hat{\phi}_{N_1/M}"] & E \arrow[ll, bend right, "\hat{\phi}"'] \end{tikzcd}$$

We are going to show how to deduce ϕ_M and $\phi_{N_1/M}$, and so ϕ.

Lemma 5.4.6.

$$\ker \phi_{N_1/M} = M \cdot H$$

Proof. Observe that $H \simeq \mathbb{Z}/N_1$ and $E_0[M] \simeq \mathbb{Z}/M \times \mathbb{Z}/M$, so

$$\ker \phi_{N_1/M} = {}^{H}\!/_{E_1[M]} \simeq {}^{\mathbb{Z}}\!/_{N_1/M} \simeq M \ker \hat{\phi}$$

The latter is a cyclic subgroup of $M \cdot H$ of order N_1/M, by the choice of M that group is cyclic hence equal to $M \ker \hat{\phi}$ as well. □

Let us study ϕ_M.

Lemma 5.4.7.

$$\theta \ker \phi_M = \ker \phi_M$$

Proof. First of all note that $\gcd(\deg \theta, M) = 1$ then the restriction of θ to ϕ_M is invertible. Without loss of generality we can equivalently prove that $\theta^{-1} \ker \phi_M = \ker \phi_M$.
Holds the follow equality:

$$\ker \phi_M = \ker \phi \cap E_0[M]$$

since the right contentment comes from definitions and we have the equality by cardinality reasons. Similarly

$$\theta^{-1}(\ker \phi_M) = \theta^{-1}(\ker \phi) \cap E_0[M] = \ker(\phi\theta) \cap E_0[M]$$

Note also that $\hat{\phi}(E[M]) = \ker \phi \cap E_0[M]$, since $\hat{\phi}(E[N_1]) = \ker \phi \cap E_0[N_1]$ and $M \mid N_1$; hence the thesis is equivalent to

$$\hat{\phi}(E[M]) = \ker(\phi\theta) \cap E_0[M].$$

$\hat{\phi}(E[N_1])$ is cyclic, so $\hat{\phi}(E[M])$. $E[M] \subseteq E[M] \cap \ker \psi$ if and only if $\hat{\phi}(E[M]) \subseteq \ker(\phi\theta)$. By the definition of M the first condition hold, then we have a contentment. Moreover M is the largest such integer and $\hat{\phi}(E[M])$, so the equality holds. □

Lemma 5.4.8. *Let k be the number of distinct prime factors of M. Then there are at most 2^k cyclic subgroups G of order M in $E_0[M]$ such that $\theta(G) = G$.*

Proof. Let $\{P, Q\}$ be a basis for $E_0[M]$, and let s, r be integers such that $\ker \phi_M = \langle sP + rQ \rangle$. We have $\gcd(s, r, M) = 1$. Let the action of θ on $E_0[M]$ be described by the matrix

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

We can reword the condition of the Lemma above as

$$\langle sP + rQ \rangle = \langle (as + cr)P + (bs + dr)Q \rangle$$

Equivalently, the matrix with coordinates of the generators before and after θ

$$\begin{bmatrix} s & (as + cr) \\ r & (bs + dr) \end{bmatrix}$$

must have rank one, namely

$$(as + cr)r \equiv (bs + dr)s \mod M \tag{5.8}$$

$$cr^2 + (a - d)sr - bs^2 = 0 \mod M \tag{5.9}$$

Equation (5.9) has solutions if and only its discriminant

$$(a - d)^2 - 4bc = (\mathrm{Tr}(\theta))^2 - 4 \deg \theta \mod M$$

is a quadratic residue. However, we assume it is the case, so there are at most two solutions modulo any prime $\ell | M$, and, by Hensel's lifting lemma, a solution modulo a prime $\ell | M$ determines a unique solution modulo any power of dividing M. Hence there are exactly 2^k possibility. □

We remark that, when N_1 is smooth, the proof implicitly provides an efficient algorithm to identify all the candidate kernels. In particular, if N_1 is a prime power, then k is at most one, and we have done.

Complexity

The central idea of the algorithm by Petit is to use the action of the hidden isogeny over a large torsion group, so to reduce the employment of the meet-in-the middle strategy to a lower degree query. Let us prove that a direct use of method Step 1-2-3-4 has a cost of $\widetilde{O}(\sqrt{N_1})$.

First of all we need to show the following lemma:

Lemma 5.4.9. *Let N be a positive integer, let p be a prime and E_1, E_2 two supersingular elliptic curves defined over $\mathbb{F}_{p^2}$ such that there exists an isogeny ϕ of degree N. Assume $N = n_1 \cdot n_2$ where both are B-smooth (B not polynomial in $\log p$). Then the meet-in-the-middle strategy has a time and memory complexity $\widetilde{O}(B \max(n_1, n_2))$.*

Proof. We can factorize N in subexponential time and isogenies of prime degree can be computed in quasilinear time in the degree. The meet-in-the-middle strategy computes $O(n_1)$ isogenies of degree n_1 and $O(n_2)$ isogenies of degree n_2, each of them as a composition of isogenies of degrees at most B. □

Let us focus now on the second step of the main procedure. The cost of algorithm 5.2 is dominated by step 3. Here we suppose to use the method suggested in Remark 5.4.4. Hence it is important to evaluate the norm of a short vector in the lattice

$$x^2 + Dy^2 \equiv 0 \mod N_2.$$

Lemma 5.4.10. *Under plausible heuristic assumptions, the shortest vectors in the lattice we considered have square norm $C'N_2$ where $C' \approx \sqrt{C}$.*

Proof. Note that we are working with the scalar product induced by

$$\begin{bmatrix} 1 & 0 \\ 0 & D \end{bmatrix}$$

Given a 2-dimensional lattice Λ with determinant $\det(\Lambda)$, the Gaussian heuristic predicts that there are about $vol(S)/\det(\Lambda)$ lattice points in a measurable subset S of $\mathbb{R}^2$ of volume[5] $vol(S)$. By Gaussian heuristic, we can estimate the expected

[5] One can think that it is the number of copies of fundamental fitting in S.

length of the shortest vector of Λ when S is convex and symmetric around the original point O. If we take S to be an 2-sphere centered at O, such that it contain a few points, $vol(S)$ is about $\det(\Lambda)$. In the other words, the length of the shortest vector can be approximated by the radius of a sphere whose volume is $\det(\Lambda)$, which is about

$$\sqrt{\frac{1}{e\pi}\det(\Lambda)}.$$

In our case a base of the lattice is $(N_2, 0)$ and $(\tau, 1)$ with $\tau^2 \equiv -D \mod N_2$, hence

$$\det(\Lambda) = \left|\det\begin{pmatrix} N_2 & 0 \\ \tau & 1 \end{pmatrix}\right| = N_2$$

The parameter restrictions assumed say that $D \approx C < N_2^2$ then the $(N_2, 0)$ could not have been minimal. We expect tht a minimal vector (x, y) in the lattice have balanced entries, thus $x^2 \approx Dy^2 = O(C'N_2)$. Then we have $(C'N_2)^2 \approx x^2Dy^2 = D(xy)^2$. Heuristically, $xy \approx N_2$, hence

$$(C'N_2)^2 \approx x^2Dy^2 = D(xy)^2 \approx DN_2^2 \implies C' \approx \sqrt{D} \approx \sqrt{C}.$$

□

We said that we were searching for C' values such that the meet-in-the-middle strategy is efficient enough in the sense of Lemma 5.4.9. We evaluate the number of random necessary trials to find C', heuristically, as the number of trials to find a smooth random number of the same size. Hence we obtain the cost of Step 2:

Proposition 5.4.11. *If $R = \mathbb{Z}$ and*

i) $N_2 > 2\sqrt{C}$

ii) If $D := \deg\psi - \left(\frac{\operatorname{Tr}\psi}{2}\right)^2$, *and we suppose*

$$\left(\frac{-D}{N_2}\right) = 1.$$

Then, heuristically, the complexity of Step 2 is $\widetilde{O}(C^{1/4})$.

Proof. The cost strictly depends on the choice of the smoothness bound, since it is involved both in the complexity of meet-in-the middle and in the query of C'. From the observation above, by Theorem A.1.2, if we fix $B = L_C(a, 1)$ for $a \in (0, 1)$ we find a suitable short vector in $1/L_C(1 - a, 1)$ which is negligible compared to $\widetilde{O}(C^{1/4})$. $\widetilde{O}(C^{1/4})$ is the cost of meet-in-the middle with the same bound taking $n_1 \approx n_2 \approx \sqrt{C'} = C^{1/4}$:

$$\widetilde{O}(B\max(n_1, n_2)) = \widetilde{O}(C^{1/4}L_C(a, 1)) = \widetilde{O}(C^{1/4}).$$

□

Note that, similarly to the general case just analyzed, since in the main protocol $\psi = \phi\theta\hat{\psi}$, by Remark 5.4.5 we obtain $C' = O(N_1\sqrt{D_\theta})$. This complexity it is not different from the one computed now in the general case, however it highlights distinctly the contributes of ϕ and θ.

Let us now consider Step 4. The last operation is an exhaustive research between the subgroups G of order M in $E_0[M]$ such that $\theta(G) = G$. By Lemma 5.4.8 we know that the number of these groups is bounded exponentially by the number k of the factors of M.

Proposition 5.4.12. *Let N_1 be a powersmooth number. Assume ϕ be chosen uniformly at random among all isogenies of degree N_1 from E_0. Then the expected value of k is bounded by $2 \log\log N_1$.*

Proof. We saw in Lemma 5.4.8 that for every prime dividing $M \mid N_1$, there are at most two candidate cyclic subgroups H_ℓ such that $\theta(H_\ell) = H_\ell$. N_1 is smooth so the space of primes dividing N_1 has cardinality at most $\log N_1$, hence the expected value of k is overestimated by

$$\sum_{\substack{\ell \mid N_1, \ell \text{ prime} \\ \ell \leq \log N_1}} \frac{2}{\ell+1} \leq \sum_{\ell \leq \log N_1} \frac{2}{\ell} \approx 2 \int_1^{\log N_1} \frac{d\ell}{\ell} \approx 2 \log\log N_1.$$

□

The previous proposition means that, in our context, the cost of the query is linear.

Our analysis proves the complexity of Step 1-2-3-4 is $\widetilde{O}(C^{1/4})$. So it depends on the degree of $\psi = \phi\theta\hat{\phi}$, namely on the degree of the θ we choose since

$$C = \deg \psi = N_1^2 \deg \theta.$$

When $\deg \theta = 1$ (the most favorable case) we expect to have at best $C' \approx \sqrt{\deg \psi} \approx N_1$ and the main complexity is $\widetilde{O}(\sqrt{N_1})$, worst than a direct employment of a meet-in-the middle approach.
It appear necessary to modify Step 1-2-3-4 strategy and we are going to see that the winning intuition is to apply Step 2 recursively.

Recursion

The complexity of Step 2 dominates the cost and it depends on the degree C of the input isogeny. The idea is to apply a recursion, in order to use the meet-in-the middle strategy only when its cost is polynomial. More precisely, at each call of Step 2 we want to give in input smaller parameters $C' < C/2$ and N_2', a factor of N_2. Before describing the algorithm, let us recall our hypothesis. We suppose that R_0 contains an endomorphism θ of small degree F and $R = \mathbb{Z}$. We also need to require $N_2/N_2' > 2N_1 D_\theta$, which implies that we have to start with parameters such that $\log N_2 = O(\log^2 N_1)$.

Let $\tilde{N}_2$ a factor of N_2 such that $\tilde{N}_2 > KN_1F$ for some $K > 1$ and $-D_\theta$ modulo $\tilde{N}_2$ is a quadratic residue. As in Step 2 and Remark 5.4.5 by a short vector of the lattice generated by $(\tilde{N}_2, 0)$ and $(\tau N_1, 1)$ such that $x^2 + N_1^2 D_\theta y^2 \mod \tilde{N}_2$, we can find $a, b \in \mathbb{Z}$ such that

$$\deg(a\phi\theta\hat{\phi} + b) = N_1'\tilde{N}_2.$$

If $N_1' > N_1/2$ we start again with a new square root of $-D_\theta$ modulo $\tilde{N}_2$ or a new $\tilde{N}_2$. While if $N_1' < N_1/2$ we define $\phi_{N_1'}$ and $\phi_{\tilde{N}_2}$ the isogenies such that

$$a\phi\theta\hat{\phi} + b = \phi_{N_1'}\phi_{\tilde{N}_2}$$

Be careful that we still do not know any of these isogenies but we can evaluate $a\phi\theta\hat{\phi} + b$ on $E[\tilde{N}_2]$. As in Step 2 so we can recover $\phi_{\tilde{N}_2}$.
We evaluate this isogeny on the $N_2' = N_2/\tilde{N}_2$ and we obtain action of $\phi_{N_1'}$ on the N_2' torsion, then we use it to apply this reduction step, recursively, with $\phi_{N_1'}$. We can suppose to have computed a representation of $\phi_{N_1'}$, hence we evaluate

$$\frac{\phi_{N_1'}\phi_{\tilde{N}_2} - b}{a}$$

over $E[N_1']$ (Step 3) and we find $\ker \hat{\phi}$ (Step 4).

By the above discussion on the steps' complexity, all the procedures involved are polynomial (also meet-in-the middle). It remains to check whether the number of reduction steps is polynomial.
We introduce K in order to have exactly this. Let us note that here the basis we use the lattice generated by $(\tilde{N}_2, 0)$ and $(N_1\tau, 1)$ with $\tau^2 \equiv -D_\theta \mod \tilde{N}_2$, hence

$$\det(\Lambda) = \left|\det\begin{pmatrix}\tilde{N}_2 & 0\\ N_1\tau & 1\end{pmatrix}\right| = \tilde{N}_2$$

We saw, in the general case, that the assumption tilde $N_2 > N_1\sqrt{F}$ provides that N_1' must be greater than 1. Similarly in the reduction step, if $K = 1$ we would obtain $N_1' = O(N_1\sqrt{D_\theta})$. If we increase the bound by a factor $K > 1$ to $N_2 > KN_1\sqrt{F}$, the possibility of an unbalanced solution arise. In [Pet17]§4.5, validated by experimental results, Petit stated that actually a small K is sufficient:

Assumption: Let $K > 1$ be a "small" constant and suppose that D_θ is "small". Then the probability that a random powersmooth value $\tilde{N}_2 > KN_1\sqrt{F}$ leads to $N_1' < N_1/2$ is "large".

We can conclude that these steps are executed a polynomial number of times and so 5.4.3 holds.

5.5 Conclusions

In this chapter, we have seen that SIDH can be included in the list of candidate post-quantum resistant cryptosystem. The hardness of supersingular isogeny problem is a necessary condition to the security of this key exchange; on the other hand, we have also shown that this condition seems not to be sufficient, since there exist specific attacks to SIDH, whose complexity is lower than the complexity of the best current algorithm solving the supersingular general isogeny problem. The work of Petit leads us to think that studying the action over torsion subgroups may be the way to obtain more precise results on the security of SIDH. However, this problem remains open.
We note that our work highlights that the issue of security of cryptosystems,

in general, is delicate and subject to change. We saw that quantum computation has undermined systems that were universally considered safe. Hence it is impossible to predict if future quantum algorithms would make the general isogeny problem easy. However, having a complete and formal state of play and understanding the theoretical bases associated to a system is the best way to be prepared to receive all the new stimuli. Our contribution to the study of SIDH has been to provide a coherent and as complete as possible presentation of the arguments related to security of SIDH. In particular, we filled in details and we produced original examples that, put together, provide a global example useful to understand how single topics affect SIDH. Moreover, we correct some mistakes that can be found in the literature.

Appendix A

Further Topics

A.1 Smooth Numbers

Definition A.1.1. Let n be an integer number whose prime factors are all less than or equal to a fixed integer B is called a *B-smooth number.*

The possibility of work with numbers whose factorization has bounded factors is useful in many algorithms. Given n a question is how large we should choose B so that a randomly chosen integer of size approximately n has a good probability of being a B-smooth number. A results by Canfield, Erdos, Pomerance answers this question:

Theorem A.1.2. *Let n, B be positive integers and let $\Pi(n, B)$ be the proportion of integers smaller than n that are B-smooth. For any $0 \leq a \leq 1$ and any large enough n*

$$\Pi(n, L_n(a, 1)) \approx \frac{1}{L_n(1-a, 1)}.$$

A.2 Quadratic Forms

Definition A.2.1. A *binary quadratic form* is expression of type

$$f(x, y) = ax^2 + bxy + cy^2.$$

It is called *integral form* if a, b, and c are integral and not all three coefficients are zero.

A such form is denoted by $f(a, b, c)$. The discriminant of $f(a, b, c)$ is $\Delta = b^2 - 4ac$. In particular, f is said *primitive positive definite* if $\Delta < 0$, $a > 0$ and $\gcd(a, b, c) = 1$.

Binary quadratic forms are used as tool in computational number theory since they are a good way to represent ideals in number fields. Let $\mathcal{O}$ be the order of discriminant D in an imaginary quadratic field K. If $f(x, y) = ax^2 + bxy + cy^2$ is a primitive positive definite quadratic form of discriminant D, then $[a, (-b + y/D)/2]$ is a proper ideal of $\mathcal{O}$. The map sending $f(x, y)$

to $[a, (-b + y/D)/2]$ induces an isomorphism between the group of primitive positive definite quadratic forms of discriminant D, denoted by $\mathrm{Cl}(D)$ and the ideal class group $\mathrm{Cl}(\mathcal{O})$. A primitive positive definite form $f = (a, b, c)$ is said *reduced* if $|b| \leq a \leq c$, and $b \geq 0$ if either $|b| = a$ or $a = c$. The reduced forms generate $\mathrm{Cl}(D)$ and every primitive positive definite form is properly equivalent to a unique reduced form. Reduction problem, i.e. the problem of find the reduced form associated to a given form, is a classical problem and there exists algorithm that solve it with $O(\log(a/\sqrt{|D|})$ arithmetic operations (on numbers of binary length $O(\mathrm{size} f)$). For details we refer to [Cox97] and [BV07].

Appendix B

Example in a Field of Characteristic a 512-bit Prime

Let use consider an example of key exchange by SIDH. We want to provide a conjectured 128-bit and 85-qubit secure system. By arguments in Section 5.4, we need to choose a finite field of characteristic about four times 128 and six times 85. Hence we can select a prime of 512-bit. Moreover that prime has to be of the form

$$\ell_A^{e_A} \cdot \ell_B^{e_B} \cdot f \pm 1$$

where ℓ_A and ℓ_B are chosen to be small primes, f a cofactor and e_A and e_B are positive integers such that $\ell_A^{e_A} \approx \ell_B^{e_B} \approx \sqrt{p}$. Once select the prime, we need to generate a random curve $E_0/\mathbb{F}_{p^2}$ such that

$$\#E_0(\mathbb{F}_q) = (\ell_A^{e_A} \cdot \ell_B^{e_B} \cdot f)^2.$$

We also must compute the torsion subgroups $E_0[\ell_A^{e_A}]$ ed $E_0[\ell_B^{e_B}]$, then we generate a two random bases (as explained in Section 5.3).

$$\{P_A, Q_A\} \quad \text{and} \quad \{P_B, Q_B\}$$

of $E_0[\ell_A^{e_A}]$ ed $E_0[\ell_B^{e_B}]$, respectively. We decided to use one of the primes suggested by De Feo, Jao and Plût in [DFJP14], in order to be able to employ their optimized computing strategy by `Sage`, and we obtained the following common setup:

Setup:

Alice and Bob fix the prime $p = 2^{258}3^{161}186 - 1$ and the curve

$$E_0/\mathbb{F}_{p^2} : y^2 = x^3 + ax^2 + x$$

where

$$\begin{aligned} a =&3062775099938928471858731993023704370407274120922971126768\\ &008668141434106548151117129263687182720927651607061616064\\ &582979130832219792079050438944280505501783\theta+\\ &+22759841571086276511632116203858304809428371341482198988\end{aligned}$$

$$\begin{aligned}
&1048537456879603569265061046276343456591012651096732986643\\
&054721321421270116020988739791933011131313 0
\end{aligned}$$

where we identify $\mathbb{F}_{p^2}$ with

$$\mathbb{F}_p(\theta) = {}^{\mathbb{F}_p[t]}\!\big/_{(t^2+1)}.$$

We have that

$$\#E(\mathbb{F}_{p^2}) = (2^{258}3^{161}186)^2$$

and

$$\begin{aligned}
j(E_0) = & 4872898017236766465429786733175516561839488687446742 75\\
& 307311544848290521605363559307806211232571705426869 46\\
& 5331868077014707894015401730499472351632816576836\theta\\
& + 5101675404862165296513738281281735903772227210636003\\
& 1877704974586823139354805188088535266685479145906212 4\\
& 414017875573289968565689119544687117644076766846679 7
\end{aligned}$$

The points

$$\begin{aligned}
P_A = [& 5065336660123355658857908771404098004252765463991673888937\\
& 1073355085941497308096909802081606249819659764339903910 18\\
& 897155514904878716001697265108615631691 01\theta+\\
& + 2897858213750336643943048116201669940059020915786332252498 8\\
& 12425304217725783404151831575888088262018457030815053661 5\\
& 52863969491826485531450750991815743958624,\\
& 4223629675571759804446469036569982840800393508828726272840958\\
& 848700724082534235065633306440701580393199621161241320789\\
& 7979405248969757269964958157586468403 23\theta+\\
& + 5263645358844430671947095719901301500732042748147878698950 6\\
& 917284181836404599971572378392798156477150570910875167563\\
& 046467749898348323929491673761747090510 08,\\
& 5416636167910333793504782660162461898489106551033536692039428\\
& 1132376404506472992394338992408962690366405580241254891 56\\
& 321528608865948282113837142736160429204\theta\\
& + 4777544602855810320458790465170831588094519004198290308407\\
& 4187380158554295359788668643653166623228411405093531098 72\\
& 083425216822783490444214432792600577889057]
\end{aligned}$$

$$\begin{aligned}
Q_A = [& 8862376052133168485472445823692073168442665504787018720 9\\
& 17468676949837194935292865137900614846047053348391416990 2\\
& 907721826690281061324177101043990042614392 7\theta+\\
& + 2354490613503584141189553483153444098843003015259012439539 1\\
& 680841001430499604488179351083175439267597917576999505883\\
& 174902200003174039582014914796110247114 50,\\
& 5325342396845542419676055240301414726352962564128821882 15\\
& 7697145671342080368545011377703741785637320832137583 5\\
& 293287327478295724669291657890152012415981248 70\theta+\\
& + 4316109637207449203156339114855144607357592206801696 14\\
& 322317668750821227757033960568058035854953645222812 18\\
& 2896141447022594208175461202709401321552159470191 8,
\end{aligned}$$

$$\begin{aligned}
&261326750096882450694546539078034277654588771839084167432\\
&\ 471639237184254244496469109147173195711302020069038853\\
&\ 0730946654144582939665919561924775622769480460 9\theta+\\
&+ 539935183740262029910675887400646628626491269995544652\\
&\ 844959446101187385499214969013437225578635221314828 65\\
&\ 6146264563805146574674439537587236286128602256247]
\end{aligned}$$

$$\begin{aligned}
P_B =&[528297585851969681556956089743300511325973923096912070767\\
&\ 568959860220094054273967937830019114427102467005816315198\\
&\ 5620473423706455421466847464442808360464536\theta+\\
&+ 341331384697248125255439533004824861828041868110648578 7\\
&\ 010047346794273971245642154732577090484825817608603836 4\\
&\ 73737680985234767108973872436388371580678409035,\\
&475315042904087757122284158139003758136562461097908397387 03\\
&\ 748372479418744689494325514522761397789619173665698872 6\\
&\ 91630426288941280759777452362687054096169984\theta+\\
&+ 104281782817771515885613968952895109112902820975841543468\\
&\ 178541225079383063394240829016601244715147730972308587\\
&\ 5164619173419621687305582890252092185596482922,\\
&515875429358167233963013521244727453448869494530001323\\
&\ 118152748375192857502069333597007591452506652408207717\\
&\ 3455717913573984781275599548097144673353656594323\theta+\\
&+ 242528974326687863811087978740357181797047097843645086 62\\
&\ 864604146404906570415270833316027911733269629793562618\\
&\ 3335851494960390445345146057064132325061291730 4]
\end{aligned}$$

$$\begin{aligned}
Q_B =&[580265629322136578400400440161970201648314944586621163281 8\\
&\ 442147583850907311928667222247246793126719745062058868 6\\
&\ 1008758005143149296982714196917310786675889 7\theta+\\
&+ 506096316164392974344532294928266310530560919152947143916\\
&\ 944319722531699934699406934669739092555449581278381855 51\\
&\ 55575233944596704608150753915428645560780337,\\
&265794884776733639909119267377672513591853300560760658155397\\
&\ 543404455010293201164323945966237624399450286861053770 40\\
&\ 3922784487851112633998958926532684975765\theta+\\
&+ 413292453138306652157718527400494716497431346350953084838 2\\
&\ 677864157520260413311062903171355792434521637676109089 38\\
&\ 326489612312003989939584024103448349355855 65,\\
&434491762453121558625734854179220221456738188164127956846733\\
&\ 406649896703212032658982424881326226667197472356217735 17\\
&\ 53300927460437933242896969737470869549 4\theta+\\
&+ 225009658699873604872733918561470233213056691728045101252 6\\
&\ 837960888058770590544948058784202990075151087496611991 71\\
&\ 44578072345848443421087022073070699884488 75]
\end{aligned}$$

form bases of $E_0[2^{258}]$ and $E_0[3^{161}]$, respectively.

Alice and Bob have to generate their private keys. Let us suppose to be Alice. We have to chose a point $R_A = m_A P_A + n_A Q_A \in E_0$ of order $\ell_A^{e_A}$,

where $m_A, n_A \in \mathbb{Z}/\ell_A^{e_A}$ must not be both divisible by ℓ_A. Specifically we put $n_A = 1$ and select m_A random. To generate Bob's secret key, we act similarly but we select m_B not divisible by ℓ_B and $n_B = \ell_B$ and we produce $R_B = m_B P_B + n_B Q_B \in E_0$ of order $\ell_B^{e_B}$.
Now we have to compute the public keys. Hence we compute the isogeny whose kernel is $\langle R_A \rangle$

$$\phi_A \colon E_0 \longrightarrow E_A = E_0/\langle R_A \rangle$$

of degree exactly $\ell_A^{e_A}$. We also compute the image of $E_0[\ell_B^{e_B}]$ by finding the image of a basis

$$\{\phi_A(P_B), \phi_A(Q_B)\}\,.$$

Alice's public key is the tuple $(E_A, \phi_A(P_B), \phi_A(Q_B))$. We proceed in the same way to compute Bob's public key $(E_B, \phi_B(P_A), \phi_B(Q_A))$.

Alice key generation:
Alice chooses the integer

$$\begin{aligned} m_A =& 1821248194471046774965855979524008484838378166695728323\\ &8379257948838392345210 6\\ =& 2 \cdot 43 \cdot 10847 \cdot 43759726443117623 \cdot 186570908564484945811613861\cdot\\ &\cdot 23913465501868410401481875531 \end{aligned}$$

and $n_A = 1$ and she computes the point

$$R_A = m_A P_A + n_a Q_A$$

of order 2^{258} and the isogeny

$$\phi_A \colon E_0 \longrightarrow E_A = E_0/\langle R_A \rangle$$

obtaining the curve $E_A \colon b_A y^2 = x^3 + a_A x^2 + x$

$$\begin{aligned} b_A =& 4053702552556266450471260156223491237893635606348354197\\ &71520739769383532183505494756692442345037972153516 9\\ &0167136510718059086426039322025643056784556433144 18\theta+\\ &+ 1697112375365354384398350202149065162795829711429711 2\\ &7349875926314725936135931457024211192672755310376 03\\ &6450556352104933858005656915121104545255324959145536 5\\ a_A =& 1107549933412895602311300069715463208243466620296230 3\\ &455940556564620363699854666247869254424032381548 2\\ &0073623254765562461529828421160978362059321876523359286\theta+\\ &+ 1323331470630315423945566881875217673375165465173067159\\ &1085814428786298027942722524153387210540945345947573\\ &9485342969379736863814247130868157819098767793818 36 \end{aligned}$$

with j-invariant

$$\begin{aligned} j(E_A) =& 4098417129298443273609277793817493578086035847689954263309559 71\\ &4839668165929350429574859737056319450514778399089815972900 8\\ &20741087356826219877510979701381720\theta+\\ &+ 501177518622304920174682150560965589706941339685211164165359 0\\ &417041393019320417642687808650461684558989209910055768419 53\\ &31625694440280875857379188304110444 38 \end{aligned}$$

Then she computes

$$\begin{aligned}
\phi_A(P_B) =&[394273366973089600799781069539984416176426423910068385606348071156685731630177656522060791682437128693569092336919693149061929633163040734700572482577037205 5\theta+\\
&+ 340605268432575240269028184115795388027400953666911585755763511508192515360897235920242859918935491725252875508532723866646333556486101174353595005458628983 1,\\
&544552635268280848382976481410373758417341584390963933766816297074578095369512014469942934329536120969175131650866134905225383075490959175976864390313949441 8\theta+\\
&+ 291321467540036165705443795469253205346248545211669297912456720499106092152624171891657262626288232146807226307985631906952979348181558382695779050956853308,\\
&207367648766055702854059343054178010497347562301143055592583847410095134130570631443601390411193020893726853588886781859516514750776444100044170132008655794 7\theta+\\
&+ 161749201192590528656274587582897454834003141557376122178642898344056099129134934477517166186594579984908086370787263449779222846991426289064974389204318703 0]\\
\phi_A(Q_B) =&[537330238896037675046379510768239045928281699491905743936745532505729336301977268390315754272080405137678057037646428652502661816429152279987408052864516969 6\theta+\\
&+ 552475284771453776896976052919294326446759413197341085641127837379716768773758754842738865137349370940855102926651223910250548764984408576984818968114021326 0,\\
&333563610257324576048355875521302363840111645208103884488322117057226678326331027547590596433750301235960508084879889749626992135421307100717144928031187895 7\theta+\\
&+ 715326135343470465889156871534863619408722952735242325742291648663184342960248066706276773144046279376110484304555814844497508398456642062497163185248008106,\\
&396504989904007371039571840513049582254572960674345608979484332290635291491353776492172416747550074474964406165774402583747184789035305075315120742349122465 9\theta+\\
&+ 210225323083001435679514034843154790887595531677199960101323718387631404110471111730601971576753651767400171838323817034628951009715819616387496695181330637 0]
\end{aligned}$$

and sends $(E_A, \phi_A(P_B), \phi_A(Q_B))$ to Bob.

Bob key generation:

Bob chooses the integer

$$\begin{aligned}
m_B =&44800328719237831357827871653101361590622864377875882068243945198018222523591\\
=&7 \cdot 9049 \cdot 15756551 \cdot 448870860305610490500352165626717744855695307325794910979712494 87
\end{aligned}$$

and $n_B = 3$ and he computes the point

$$R_B = m_B P_B + n_B Q_B$$

of order 3^{161} and the isogeny

$$\phi_B \colon E_0 \longrightarrow E_B = E_0/\langle R_B \rangle$$

obtaining the curve $E_B \colon b_B y^2 = x^3 + a_B x^2 + x$

$$\begin{aligned}
b_B =& 3202074513519622728586561513749379451279250773928427346493072267697\\
&9669967064010181061633629284076288613111131653300009466621421 37\\
&87827611099023951061187772 6\theta+\\
&+ 1018147507306493650897271337239883842257603350237162581814650481 0\\
&1681362441846341649617002681173654810248087985318320184163466 55\\
&913633572733985617641376612 71\\
a_B =& 5356269702713660910444029031994820087856318698594939527016266180291\\
&2846218521106793643430532008798492977265878000646522115498726 45\\
&86102312979871407561653343 8\theta+\\
&+ 2633779118156083348590273139329457449279350580909044811891321983 0\\
&8255256856782518501542935540524363129617283446474379393349361 53\\
&172954079200170001204855227 85
\end{aligned}$$

with j-invariant

$$\begin{aligned}
j(E_B) =& 2506322248027916937010951099973246674275811574200945250469277586\\
&540567184554298128893736691031021682076828613846981756297467\\
&9260591114673865543284642265571 09\theta+\\
&+ 2238352655958690131138249458434904093017782863729974397941004 7\\
&437056594692066086310607419025378760179344350461542093623046\\
&1278715526199704380450352186690 5833
\end{aligned}$$

Then he computes

$$\begin{aligned}
\phi_B(P_A) =& [3325335658460570301667512194029286324867545617333098206177070 1\\
&579851683213730019482188209407078697845174058962515211573 67\\
&284283213608378411724447125839605 609\theta+\\
&+ 4275473500146862274737975876496968467508203549577320734834256 7\\
&250556695462652161273642692770858420378415218785281660340431\\
&8620284146759976095399581887724204 1,\\
&1302677088727251330341018835510197873100354088550758115322541317\\
&549748509349579626717877941714209770616880080856734354888976\\
&009885065930360260384080057075666 8\theta+\\
&+ 4332806455315034340095195237819506246352835615458857599978115 1\\
&063544779005824642169337382763409451933283776603800604991791\\
&7410741450877201072715571521561973 5,\\
&2534902274386603896755684080419664522332727677838482016489684401\\
&886812621887456794218195642790858208950244519638432353329530\\
&649087089352848157285332312290325\theta+\\
&+ 4837859387315075081630655484908435518503843963597308086945652 5\\
&240502412818697117273425855386063546477819782383996819197982\\
&2790787656580772527211657397497704]
\end{aligned}$$

$$\begin{aligned}
\phi_B(Q_A) =& [2345373032709068343211080714200520551020701526993936066851641 83\\
&236738683087814591577323886730855213072075117259670054233771\\
&382822902590838675976891863098933 09\theta+
\end{aligned}$$

$$\begin{aligned}
&+ 55935945786638149282323166433702493970917379917649450877380041\\
&\ 57583985287185176669855708763531955263401853575450780396514 1\\
&\ 5581073143377056569560015499493414 5,\\
&16246334113283712010674667338761848245187891225352589599072271 94\\
&\ 56423546045720637879526837822883225236014269523902950038520 9\\
&\ 84326924221331911960587660231085 5\theta+\\
&+ 19056903964169194394872806659294572056550329273826764323619459\\
&\ 27763613563997779282536344482122043610029032835209324529479 1\\
&\ 26659355401433459705919239296217478,\\
&12234547235281220550788166196349579680662287864052189765740781 38\\
&\ 95659065318430857859123425912844507851879765530289729523533 4\\
&\ 65768843033766541083137259834064 2\theta+\\
&+ 21418103740295781234084310363766491864668093961985580149645082\\
&\ 95702721013935708988342052006977476554169129782312137196634 8\\
&\ 5382302433851522861438563503376972 7]
\end{aligned}$$

and sends $(E_B, \phi_B(P_A), \phi_B(Q_A))$ to Alice.

In order to find the shared secret key, as Alice, we take Bob's public key $(E_B, \phi_B(P_A), \phi_B(Q_A))$ and using the secret key m_A, n_A we can compute the point

$$S_A = m_A\phi_B(P_A) + n_A\phi_B(Q_A)$$

and the isogeny

$$\phi'_A \colon E_B \longrightarrow E_{AB} = {}^{E_B}\!\diagup_{\langle S_A\rangle}$$

Once we have it done, we directly obtain the j-invariant of E_{AB} which is the shared secret key.
Similarly, as Bob, we can compute the point

$$S_B = n_A\phi_A(P_B) + m_B\phi_A(Q_B)$$

and

$$\phi'_B \colon E_A \longrightarrow E_{BA} = {}^{E_A}\!\diagup_{\langle S_B\rangle}$$

Then we can obtain the the j-invariant of E_{BA} which is the shared secret key.
Alice shared key recover:
Alice finds

$$S_A = m_A\phi_B(P_A) + n_A\phi_B(Q_A)$$

and

$$\phi'_A \colon E_B \longrightarrow E_{AB} = {}^{E_B}\!\diagup_{\langle S_A\rangle}$$

obtaining

$$\begin{aligned}
j(E_{AB}) =&14328144880860551963513352611264649880886726277855099975942060 17\\
&\ 47313113720284515398014039357212157450790642739812298619757 1\\
&\ 96772563675268475210387859093843 9\theta+\\
&+ 11176899002208157313419740867135181672894886276104876365256943\\
&\ 84678012073121827330472351592259679423891217224266852935573 0\\
&\ 6944224601940423737509868375184851 4
\end{aligned}$$

Bob shared key recover:

Bob finds

$$S_B = n_A\phi_A(P_B) + m_B\phi_A(Q_B)$$

and

$$\phi'_B \colon E_A \longrightarrow E_{BA} = {}^{E_A}\!\big/\!_{\langle S_B \rangle}$$

obtaining

$$\begin{aligned} j(E_{BA}) = & 1432814488086055196351335261126464988088672627785509997594206017 \\ & 4731311372028451539801403935721215745079064273981229861975 71 \\ & 9677256367526847521038785909384439\theta + \\ & + 1117689900220815731341974086713518167289488627610487636525 6943 \\ & 8467801207312182733047235159225967942389121722426685293557 30 \\ & 694422460194042373750986837518485 14 \end{aligned}$$

The secret shared key is

$$j = j(E_{AB}) = j(E_{BA}).$$

Bibliography

[BCP97] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[BCS04] G. Benenti, G. Casati, and G. Strini. *Principles of Quantum Computation and Information.* Number v. 1. World Scientific, 2004.

[Ber09] D. Bernstein. *Introduction to post-quantum cryptography*, pages 1–14. Springer Berlin Heidelberg, Berlin, Heidelberg, 2009.

[BJS14] J.-F. Biasse, D. Jao, and A. Sankar. A quantum algorithm for computing isogenies between supersingular elliptic curves. In Willi Meier and Debdeep Mukhopadhyay, editors, *Progress in Cryptology – INDOCRYPT 2014*, pages 428–442, Cham, 2014. Springer International Publishing.

[BV07] J. Buchmann and U. Vollmer. *Binary Quadratic Forms: An Algorithmic Approach.* Algorithms and Computation in Mathematics. Springer Berlin Heidelberg, 2007.

[CJS14] A. Childs, D. Jao, and V. Soukharev. Constructing elliptic curve isogenies in quantum subexponential time. Journal of Mathematical Cryptology 8(1), 2014.

[CLG09] D. X. Charles, K.. Lauter, and E. Goren. Cryptographic hash functions from expander graphs. *Journal of Cryptology*, 22(1):93–113, Jan 2009.

[CLN16] C. Costello, P. Longa, and M. Naehrig. Efficient algorithms for supersingular isogeny diffie-hellman. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology – CRYPTO 2016*, pages 572–601, Berlin, Heidelberg, 2016. Springer Berlin Heidelberg.

[Cox97] D.A. Cox. *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication.* Pure and applied mathematics. Wiley, 1997.

[DF17] L. De Feo. Mathematics of isogeny based cryptography. Notes written for a summer school on Mathematics for post-quantum cryptography in Thiès, Senegal., 2017.

[DFJP14] L. De Feo, D. Jao, and J. Plût. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. Journal of Mathematical Cryptology 8(3), 2014. `https://eprint.iacr.org/2011/506`.

[DG16] C. Delfs and S. D. Galbraith. Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$. *Designs, Codes and Cryptography*, 78(2):425–440, Feb 2016.

[EH99] M. Ettinger and P. Høyer. On quantum algorithms for noncommutative hidden subgroups. In Christoph Meinel and Sophie Tison, editors, *STACS 99*, pages 478–487, Berlin, Heidelberg, 1999. Springer Berlin Heidelberg.

[FM02] M. Fouquet and Fr. Morain. Isogeny volcanoes and the sea algorithm. In Claus Fieker and David R. Kohel, editors, *Algorithmic Number Theory*, pages 276–291, Berlin, Heidelberg, 2002. Springer Berlin Heidelberg.

[Gal99] S. D. Galbraith. Constructing isogenies between elliptic curves over finite fields. *LMS J. Comput. Math*, 2:118–138, 1999.

[Gal12] S. D. Galbraith. *Mathematics of Public Key Cryptography*. Cambridge University Press, New York, NY, USA, 1st edition, 2012.

[GHS02] S. D. Galbraith, F. Hess, and N. P. Smart. Extending the GHS weil descent attack. In Lars R. Knudsen, editor, *Advances in Cryptology — EUROCRYPT 2002*, Berlin, Heidelberg, 2002. Springer Berlin Heidelberg.

[GPST16] S. D. Galbraith, C. Petit, B. Shani, and Y. B. Ti. On the security of supersingular isogeny cryptosystems. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *Advances in Cryptology – ASIACRYPT 2016*, pages 63–91, Berlin, Heidelberg, 2016. Springer Berlin Heidelberg.

[Gro96] L. Grover. A fast quantum mechanical algorithm for database search. In *ANNUAL ACM SYMPOSIUM ON THEORY OF COMPUTING*, pages 212–219. ACM, 1996.

[GS13] S.D. Galbraith and A. Stolbunov. Improved algorithm for the isogeny problem for ordinary elliptic curves. *Applicable Algebra in Engineering, Communication and Computing*, 24(2):107–131, Jun 2013.

[GV17] S. D. Galbraith and V. Vercauteren. Computational problems in supersingular elliptic curve isogenies. Cryptology ePrint Archive, Report 2017/774, 2017. `https://eprint.iacr.org/2017/774`.

[HPS08] J. Hoffstein, J. Pipher, and J.H. Silverman. *An Introduction to Mathematical Cryptography*. Undergraduate Texts in Mathematics. Springer, 2008.

[JCDF$^+$17] D. Jao, C. Costello, L. De Feo, P. Longa, M. Naehrig, and J. Renes. Supersingular isogeny key encapsulation SIKE. 11 2017.

[JDF11] D. Jao and L. De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In Bo-Yin Yang, editor, *Post-Quantum Cryptography*, pages 19–34, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg.

[JMV09] D. Jao, S. D. Miller, and R. Venkatesan. Expander graphs based on grh with an application to elliptic curve cryptography. *Journal of Number Theory*, 129(6):1491 – 1504, 2009.

[KLPT14] D. Kohel, K. Lauter, C. Petit, and J.-P. Tignol. On the quaternion ℓ-isogeny path problem. Cryptology ePrint Archive, Report 2014/505, 2014. `https://eprint.iacr.org/2014/505`.

[Koh96] D. Kohel. *Endomorphism rings of elliptic curves over finite fields*. PhD thesis, University of California at Berkeley, 1996.

[Lan87] S. Lang. *Elliptic Functions*. Graduate texts in mathematics. Springer, 1987.

[Mos99] M. Mosca. *Quantum Computer Algorithms*. PhD thesis, Oxford, 1999.

[Mos08] M. Mosca. Quantum algorithms. `arXiv:0808.0369`, 2008.

[Mur87] M. Murty. On the supersingular reduction of elliptic curves. *Proceedings of the Indian Academy of Sciences - Mathematical Sciences*, 97(1):247–250, Dec 1987.

[oST] National Institute of Standards and Technology. NISTsubmission for post-quantum cryptography. `https://csrc.nist.gov/Projects/Post-Quantum-Cryptography`.

[Pet17] C. 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, Cham, 2017. Springer International Publishing.

[PL17] C. Petit and K. Lauter. Hard and easy problems for supersingular isogeny graphs. Cryptology ePrint Archive, Report 2017/962, 2017. `https://eprint.iacr.org/2017/962`.

[Rei75] I. Reiner. *Maximal orders*. Academic Press, 1975.

[RS06] A. Rostovtsev and A. Stolbunov. Public-key cryptosystem based on isogenies. Cryptology ePrint Archive, Report 2006/145, 2006. `https://eprint.iacr.org/2006/145`.

[Sch95] R. Schoof. Counting points on elliptic curves over finite fields. pages 219–254, 1995.

[Sho94] P. W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. pages 124–134, 1994.

[Sil09] J.H. Silverman. *Advanced topics in the arithmetic of elliptic curves.* Graduate texts in mathematics. Springer-Verlag, 2009.

[Sil11] J.H. Silverman. *The Arithmetic of Elliptic Curves.* Applications of Mathematics. 2011.

[Tan07] S. Tani. An improved claw finding algorithm using quantum walk. In Luděk Kučera and Antonín Kučera, editors, *Mathematical Foundations of Computer Science 2007*, pages 536–547, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg.

[Tsc04] Y. Tschinkel. Supersingular elliptic curves and maximal quaternionionic orders. Mathematisches Institut Georg-august-universität Göttingen, Seminars Summer Term 2004, 2004.

[Voi18] J. Voight. Quaternion algebras. `https://math.dartmouth.edu/~jvoight/quat-book.pdf`, Jan 2018.

[Was08] L. C. Washington. *Elliptic Curves: Number Theory and Cryptography, Second Edition.* Chapman & Hall/CRC, 2 edition, 2008.

[Wat69] W.C. Waterhouse. Abelian varieties over finite fields. pages p. 521–560, 1969.