MASTER'S THESIS

UTRECHT UNIVERSITY

MATHEMATICAL SCIENCES

# Supersingular Isogeny Graphs and Orientations in Cryptography

*Author:*
Anne Wouda

*Supervisor:*
Dr. Valentijn Karemaker

*Second Supervisor:*
Dr. Stefano Marseglia

August 8, 2022

**Abstract**

We discuss the theory of isogeny graphs; we mainly consider *supersingular isogeny graphs*, where the vertices of the graphs are given by $j$-invariants of supersingular elliptic curves over some finite field and the edges denote the $\ell$-degree isogenies between the elliptic curves that have those $j$-invariants. We look at some cryptographic protocols, both key exchange protocols and a $\Sigma$-protocol, that use supersingular isogeny graphs. Finally, we introduce orientations, which are injective ring homomorphisms that embed quadratic orders into the endomorphism algebras of (supersingular) elliptic curves. We consider the key exchange protocol OSIDH, which uses orientations and we construct a 3-move protocol that uses orientations and could potentially be a $\Sigma$-protocol.

# Contents

# 1 Introduction

In this thesis, we will look at supersingular isogeny graphs, orientations and their applications in cryptography. Supersingular isogeny graphs gained a lot of interest from mathematicians and cryptographers lately, mainly due to some characteristics that are promising for use in cryptographic protocols. For example [1], [2] and [3] study isogeny-based cryptography and even introduce isogeny-based cryptographic protocols. Over the past years, the arrival of a quantum computer has become more and more realistic [4] and with that come some problems with current standard cryptographic protocols. In particular, some of these protocols will or might be broken, because algorithms that attack the security of those protocols, but run too slowly on current computers, might run in e.g. polynomial time on quantum computers. One example of such an algorithm is Schor's algorithm, which can factor integers. This was enough reason for the National Institute of Standards and Technology to start a competition in 2016 to find protocols that will be resistant against quantum attacks, so that they can be used as new standardised protocols. One of the submissions for a quantum resistant key exchange protocol is SIKE, which is based on Supersingular Isogeny Diffie-Hellman (SIDH), which was introduced in 2011 in [3]. As the name suggests, SIDH uses supersingular isogeny graphs.

Supersingular isogeny graphs are graphs whose vertices are $j$-invariants of supersingular elliptic curves over a finite field and whose edges are isogenies of prime degree $\ell$. As we will see, there are some good reasons to believe that these graphs can form a good basis for post-quantum cryptography. The goal of this thesis is to explore and understand the theory of supersingular isogeny graphs and some of their applications in cryptography.

In Chapter 2 we will start by looking at the theory of elliptic curves and isogenies. After that, we discuss some basic graph theory in Chapter 3 and look at key exchange protocols in Chapter 4, we will mainly consider key exchange protocols that resemble the standard Diffie-Hellman protocol. Then we introduce isogeny graphs and we discuss and prove some of the most important properties of supersingular isogeny graphs in Chapter 5, so we can see why supersingular isogeny graphs can be useful primitives. In Chapter 6 we will also discuss some cryptographic protocols based on isogeny graphs; the Rostovtsev-Stolbunov protocol, SIDH and SQISign. The first one uses ordinary isogeny graphs and the others use supersingular isogeny graphs.

Finally, we will look at the theory of orientations in Chapter 7, which are embeddings into the endomorphism algebras of (supersingular) elliptic curves. We will see a key exchange protocol called OSIDH, which stands for Oriented Supersingular Isogeny Diffie-Hellman, which uses orientations. We will also introduce a 3-move protocol that uses orientations; this protocol is potentially a $\Sigma$-protocol.

# 2 Elliptic curves

Before we introduce (supersingular) isogeny graphs, we will discuss some basics. In this section we will give a short overview of the theory of elliptic curves and isogenies.

## 2.1 Elliptic curves

**Definition 2.1.** An *elliptic curve* $E$ over a field $k$ with $\text{char}(k) \neq 2$ is a nonsingular curve given by a Weierstrass equation of the form

$$E : y^2 = x^3 + \alpha x^2 + \beta x + \gamma, \quad \text{with } \alpha, \beta, \gamma \in k.$$

If $\text{char}(k) \neq 2, 3$, $E$ can be given by an equation of the form

$$E : y^2 = x^3 + ax + b, \quad \text{with } a, b \in k.$$

When considering $E$ in projective coordinates there is an extra point compared to when we consider $E$ in affine coordinates. This is the point $[0, 1, 0]$, we denote it by $\mathcal{O}$. This point is called the point at infinity.

In more general terms we may say that an elliptic curve is a smooth projective curve of genus one. One of the reasons elliptic curves are so useful is because one can define a group law on the points of an elliptic curve over $k$, where $\mathcal{O}$ is the unit element. This group law is not quite obvious from the equation for the elliptic curve and its construction is completely geometric. In this section we will only see the equations for adding points, but [5, p. 51] explains the construction of the group law in more detail. The explicit formulas for the group law for addition of points on the curve, are as follows; let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ with $x_1 \neq x_2$, be points on the elliptic curve $E$, given by the equation $E : y^2 = x^3 + \alpha x^2 + \beta x + \gamma$, denote $P_1 + P_2 = (x_3, -y_3)$. The coordinates $x_3$ and $y_3$ are given by

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - \alpha - x_1 - x_2 \quad \text{and} \quad y_3 = \frac{y_2 - y_1}{x_2 - x_1} x_3 + \nu, \tag{1}$$

here $\nu$ is given by

$$\nu = y_1 - \frac{y_2 - y_1}{x_2 - x_1} x_1 = y_2 - \frac{y_2 - y_1}{x_2 - x_1} x_2.$$

Now consider the case where $x_1 = x_2$ but $y_1 \neq y_2$. In this case $P_1$ and $P_2$ are each other's (additive) inverse, so adding them together gives the unit element, which is point at infinity; $P_1 + P_2 = \mathcal{O}$. We can also construct an explicit formula for the

case where we want to add a point $P = (x, y)$ to itself. This formula, which gives the $x$-coordinate of $2P = (x', y')$ is called the duplication formula:

$$x' = \frac{x^4 - 2\beta x^2 - 8\gamma x + \beta^2 - 4\alpha\gamma}{4x^3 + 4\alpha x^2 + 4\beta x + 4\gamma}. \tag{2}$$

Consider an elliptic curve over a field $k$. In this thesis, we will generally assume that the field $k$ does not have characteristic 2 or 3. This means that $E$ can be given by an equation of the form

$$E : y^2 = x^3 + ax + b, \quad \text{with } a, b \in k.$$

We define the following quantities.

**Definition 2.2.** Let $E/k$ be an elliptic curve over a field with $\text{char}(k) \neq 2, 3$. The *discriminant* of the elliptic curve $E$ is denoted by $\Delta(E)$ and it equals

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

The *j-invariant* of the elliptic curve $E$ is denoted by $j(E)$ and it equals

$$j(E) = 1728\frac{4a^3}{4a^3 + 27b^2} = 1728\frac{4a^3}{-\Delta(E)/16}.$$

As mentioned before, elliptic curves are nonsingular, which means that they do not have any nodes or cusps. For elliptic curves this is equivalent to saying that $\Delta(E) \neq 0$, this is proven in [5, Proposition III.1.4 (a)]. Also, the $j$-invariant of two curves $E$ and $E'$ can tell us whether the curves "look alike" in a certain sense. To make this more precise, we need the concept of isomorphisms of elliptic curves, which will be introduced in the next section.

## 2.2 Isogenies

Another important concept for (supersingular) isogeny graphs are isogenies. In this section we will define isogenies and list some of their most important properties.

**Definition 2.3.** Let $E_1, E_2$ be elliptic curves over a field $k$ given by

$$E_1 : y^2 = x^3 + ax + b \quad \text{and} \quad E_2 : y^2 = x^3 + a'x + b'.$$

A *morphism* $\phi : E_1 \to E_2$ is a mapping $\phi(x, y) = (\phi_x(x, y), \phi_y(x, y))$ where $\phi_x$ and $\phi_y$ are functions on $E_1$ such that $\phi_y^2 = \phi_x^3 + a'\phi_x + b'$.

**Definition 2.4.** Given two elliptic curves $E_1$ and $E_2$ over a field $k$, we say that $E_1$ and $E_2$ are *isomorphic* if there exist morphisms $\phi : E_1 \to E_2$ and $\psi : E_2 \to E_1$ such that $\psi \circ \phi$ and $\phi \circ \psi$ are the identity maps on $E_1$ and $E_2$, respectively. The maps $\phi$ and $\psi$ are called *isomorphisms*.

**Theorem 2.5.** *Let $E_1$ and $E_2$ be elliptic curves over a field $k$. The curves $E_1$ and $E_2$ are isomorphic over the algebraic closure $\overline{k}$ of $k$, if and only if $j(E_1) = j(E_2)$.*

*Proof.* For the proof we refer to [5, p. 45]. □

**Definition 2.6.** Let $E_1$ and $E_2$ be elliptic curves. An *isogeny* from $E_1$ to $E_2$ is a morphism

$$\phi : E_1 \to E_2 \quad \text{where} \quad \phi(O_1) = O_2.$$

All isogenies satisfy $\phi(E_1) = \{O_2\}$ or $\phi(E_1) = E_2$. In other words, all isogenies are either constant or surjective (more generally, this holds for all morphisms between elliptic curves). We say that two curves $E_1$ and $E_2$ are *isogenous* if there exists a non-constant isogeny between them. Being isogenous is an equivalence relation, so in particular, when there is an isogeny from $E_1$ to $E_2$, we know that there is also an isogeny from $E_2$ to $E_1$. We will discuss this in more detail at the end of this section.

Two elliptic curves given by $E_1 : f_1(x,y) := y^2 - (x^3 + ax^2 + bx + c) = 0$ and $E_2 : f_2(x,y) := y^2 - (x^3 + a'x^2 + b'x + c') = 0$ over a field $k$, have *function fields* $k(E_1)$ respectively $k(E_2)$ that equal the field of fractions of the affine coordinate rings $k[x,y]/(f_1(x,y))$ and $k[x,y]/(f_2(x,y))$, respectively. Given an isogeny $\phi$ between elliptic curves, i.e., $\phi : E_1 \to E_2$, we define the map $\phi^*$ as follows:

$$\phi^* : k(E_2) \to k(E_1), \quad \phi^* f = f \circ \phi.$$

**Theorem 2.7.** *Let $E_1/k$ and $E_2/k$ be elliptic curves and let $\phi : E_1 \to E_2$ be a non-constant isogeny.*

*(i) The map $\phi^*$ induces an injection of function fields $k(E_2)$ in $k(E_1)$, fixing $k$.*

*(ii) Let $\phi$ be non-constant. Then $k(E_1)$ is a finite extension of $\phi^*(k(E_2))$.*

*Proof.* For the proof we refer to [6, Theorem II.6.8]. □

We say an isogeny $\phi$ is *separable*, when the extension $k(E_1)/\phi^*(k(E_2))$ is separable. Similarly we say that $\phi$ is *(purely) inseparable* when the extension $k(E_1)/\phi^*(k(E_2))$ is (purely) inseparable.

**Definition 2.8.** Let $\phi : E_1 \to E_2$ be a morphism of elliptic curves over $k$. If $\phi$ is constant, we define the degree of $\phi$ as $\deg(\phi) = 0$. Otherwise we define the *degree* of $\phi$ as

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

We call the *separable* and *inseparable degrees* of the extension $\deg_s(\phi)$ and $\deg_i(\phi)$, respectively.

By Theorem 2.7(ii), we know that the degree is finite. The degree is multiplicative, so for maps $\phi$ and $\psi$, we have that $\deg(\phi \circ \psi) = \deg(\phi) \cdot \deg(\psi)$. Also, the degree as a map from $\mathrm{Hom}(E_1, E_2)$ to $\mathbb{Z}$, is a positive definite quadratic form, this is proven in [5, Corollary III.6.3].

**Theorem 2.9.** *Let $E_1$ and $E_2$ be elliptic curves over $k$ and let $\phi : E_1 \to E_2$ be an isogeny. Then*

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

*for all points $P, Q \in E_1(\bar{k})$.*

*Proof.* The proof is given in [5, Theorem III.4.8]. □

**Theorem 2.10.** *Let $\phi : E_1 \to E_2$ be a non-zero isogeny.*

*(i) The group $\ker(\phi) := \phi^{-1}(\mathcal{O})$, is defined to be the kernel of $\phi$ and it is a finite group.*

*(ii) For every $Q \in E_2$, we have $\#\phi^{-1}(Q) = \deg_s(\phi)$.*

*(iii) Suppose $\phi$ is separable. Then $\#\ker(\phi) = \deg_s(\phi)$.*

*Proof.* The fact that $\ker(\phi)$ is a group follows from Theorem 2.9, and (iii) follows directly from (ii) with $Q = \mathcal{O}$. The rest of the proof needs the theory of orders and divisors, which we do not want to go into here. The proof can be found in [5, Theorem III.4.9] and [5, Theorem III.4.10]. □

Next we will see two isogenies that occur often when studying elliptic curves: the *multiplication-by-m-map* and the *Frobenius map*.

**Definition 2.11.** An *endomorphism* is an isogeny from an elliptic curve to itself.

**Definition 2.12.** Let $E$ be an elliptic curve over $k$. For each $m \in \mathbb{Z}$, we define the *multiplication-by-m* map as follows

$$[m] : E \to E, \quad [m]P \mapsto \underbrace{P + P + \cdots + P}_{m \text{ times}}.$$

As mentioned, the multiplication-by-$m$ map is an example of an endomorphism. Another endomorphism is given in the next definition.

**Definition 2.13.** Let $E$ be an (elliptic) curve in $\mathbb{P}^2$ given by

$$E : Y^2Z = X^3 + aXZ^2 + bZ^3.$$

The elliptic curve $E^{(q)}$ is given by

$$E^{(q)} : Y^2Z = X^3 + a^qXZ^2 + b^qZ^3.$$

**Definition 2.14.** Let $E/k$ be an elliptic curve and let $\text{char}(k) = p > 0$. The *$p$-power Frobenius endomorphism* $\pi$ is defined as

$$\pi : E \to E^{(p)}, \quad [X, Y, Z] \mapsto [X^p, Y^p, Z^p].$$

The Frobenius endomorphism has degree equal to $p$ and is purely inseparable.

**Theorem 2.15.** *Let $\psi$ be an isogeny over a field $k$ of characteristic $p > 0$. Then*

$$\psi = \psi_{\text{sep}} \circ \pi^n,$$

*where $\psi_{\text{sep}}$ is some separable isogeny and $\pi$ is the $p$-power Frobenius endomorphism.*

*Proof.* For the proof we refer to [5, Corollary II.2.12]. □

**Theorem 2.16.** *Let $\phi : E_1 \to E_2$ be a non-constant isogeny of degree $m$. Then there exists a unique isogeny*

$$\widehat{\phi} : E_2 \to E_1 \quad \text{satisfying} \quad \widehat{\phi} \circ \phi = [m].$$

*This isogeny is called the dual isogeny.*

*Proof.* For the proof we refer to Theorem 6.1(a) in [5, Theorem III.6.1(a)]. □

The next theorem illustrates some useful properties of the dual isogeny.

**Theorem 2.17.** *Let $\phi : E_1 \to E_2$ be an isogeny.*

*(i) Let $\deg(\phi) = m$. Then $\hat{\phi} \circ \phi = [m]$ on $E_1$ and $\phi \circ \widehat{\phi} = [m]$ on $E_2$.*

*(ii) Let $\psi : E_2 \to E_3$ be another isogeny. Then $\widehat{\psi \circ \phi} = \widehat{\phi} \circ \widehat{\psi}$.*

*(iii) Let $\lambda : E_1 \to E_2$ be another isogeny. Then $\widehat{\phi + \lambda} = \widehat{\phi} + \widehat{\lambda}$.*

*(iv)* *For all* $m \in \mathbb{Z}$, $\widehat{[m]} = [m]$ *and* $\deg[m] = m^2$.

*(v)* *We have that* $\deg(\phi) = \deg(\widehat{\phi})$.

*(vi)* *We have that* $\hat{\hat{\phi}} = \phi$.

*Proof.* For the proof we refer to [5, Theorem 6.2]. □

The multiplication-by-$m$ map is a non-constant map. This can be shown by considering the duplication formula and the formula for multiplying a point by three. The multiplication-by-$m$ map is an endomorphism. The kernel of the multiplication-by-$m$ map is denoted by $E[m]$ and its points correspond to the $m$-torsion points on $E(\overline{k})$.

**Proposition 2.18.** *Let $E$ be an elliptic curve over a field $k$ and let $m \neq 0$ be an integer. The kernel of the multiplication-by-m map, denoted $E[m]$, is of the form*

*(i)* $E[m] \cong (\mathbb{Z}/m\mathbb{Z})^2$, *if* $\mathrm{char}(k)$ *does not divide m.*

*(ii)* $E[p^i] \cong \begin{cases} \mathbb{Z}/p^i\mathbb{Z} \\ \{\mathcal{O}\} \end{cases}$ , *if* $\mathrm{char}(k) = p$.

*Proof.* (i) If $[m]$ is separable then $\#\ker([m]) = \deg([m]) = m^2$. We know that if $m \neq 0$ in $k$, then $[m]$ is separable by [5, Corollary 5.4]. In particular, for all divisors $d$ of $m$, it holds that $d \neq 0$ in $k$. So for $d$ the same thing holds, namely $\#E[d] = \deg([d]) = d^2$. We can factor $m$ as $m = \prod_{i=1}^{t} p_i^{e_i}$, where the $p_i$ are primes. Using this factorisation and the fact that $E[m]$ is an abelian group, we can write

$$E[m] \cong G_1 \times \cdots \times G_t,$$

where the $G_i$ have order $p_i^{2e_i}$, since $\#E[m] = m^2$. For any divisor $p^e$ of $m$, we know by the above that $\#E[p^e] = p^{2e}$, hence there are $p^{2e}$ elements of order $p^e$. Therefore the $G_i$ have to be of the form $(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^2$. This shows that

$$E[m] \cong (\mathbb{Z}/p_1^{e_1}\mathbb{Z})^2 \times \cdots \times (\mathbb{Z}/p_t^{e_t}\mathbb{Z})^2 \cong (\mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_t^{e_t}\mathbb{Z})^2.$$

By the Chinese remainder theorem we conclude that

$$E[m] \cong (\mathbb{Z}/m\mathbb{Z})^2.$$

(ii) The following holds:

$$\begin{aligned}\#E[p^i] &= \deg_s([p^i]) \\ &= \deg_s((\pi \circ \widehat{\pi})^i) \\ &= \deg_s(\pi \circ \widehat{\pi})^i \\ &= \deg_s(\widehat{\pi})^i.\end{aligned}$$

In general, an isogeny can be separable, inseparable or purely inseparable. In this case, we only have to distinguish two cases, since the (total) degree of the isogeny is a prime $p$:

$$p = \deg(\widehat{\pi}) = \deg_i(\widehat{\pi}) \cdot \deg_s(\widehat{\pi}).$$

This shows that either the inseparable or the separable degree of $\widehat{\pi}$ equals 1, so that $\widehat{\pi}$ is either separable or purely inseparable. So we distinguish two cases; the case where $\hat{\pi}$ is purely inseparable and the case where $\widehat{\pi}$ is separable. Firstly, if $\widehat{\pi}$ is purely inseparable, that means that $\deg(\widehat{\pi}) = \deg_i(\widehat{\pi})$. Therefore $\deg_s(\widehat{\pi}) = 1$, so $E[p^i] = \{O\}$.
Secondly, if $\widehat{\pi}$ is separable, then $\deg_s(\widehat{\pi}) = p$. Therefore $\#E[p^i] = p^i$, which holds for all $i$. So for all $i$, there are $p^i$ elements that have order $p^i$. This implies that $E[p^i] \cong \mathbb{Z}/p^i\mathbb{Z}$.

□

The next theorem shows that for all finite subgroups $G$ of $E(\bar{k})$, there exists a unique separable isogeny from $E$ to some curve $E'$ that has kernel $G$. It also gives explicit formulas with which the isogeny and the curve $E'$ can be computed. These formulas are very useful when constructing (supersingular) isogeny graphs, as we will see in Section 5.

**Theorem 2.19** (Vélu's formulas)**.** *Let $E$ be an elliptic curve given by $E : y^2 = x^3 + ax + b$. Suppose that $G \subset E(\bar{k})$ is a finite subgroup. Then there exists a unique separable isogeny $\phi : E \to E/G$ with kernel $G$. It is given by*

$$\phi(P) = \left( x(P) + \sum_{Q \in G \setminus \{O\}} x(P+Q) - x(Q), y(P) + \sum_{Q \in G \setminus \{O\}} y(P+Q) - y(Q) \right).$$

*The curve $E/G$ is given by $E/G : y^2 = x^3 + a'x + b'$, where*

$$\begin{aligned}a' &= a - 5 \sum_{Q \in G \setminus \{O\}} (3x(Q)^2 + a) \\ b' &= b - 7 \sum_{Q \in G \setminus \{O\}} (5x(Q)^3 + 3ax(Q) + b).\end{aligned}$$

*Proof.* Vélu showed this in [7]. □

## 2.3 Endomorphism rings

The upcoming part will contain relevant information about the endomorphism rings of elliptic curves, concluding with a theorem (Theorem 2.27) that shows the structure of the endomorphism ring of an elliptic curve. We will start by listing some facts about endomorphism rings.

The set of isogenies defined over $\overline{k}$ between two elliptic curves $E_1/k$ and $E_2/k$ is denoted by $\mathrm{Hom}(E_1, E_2)$. Defining addition in this set as $(\phi + \psi)(P) := \phi(P) + \psi(P)$ gives it a group structure.

**Definition 2.20.** The *endomorphism ring* of an elliptic curve $E/k$ is defined as

$$\mathrm{End}(E) := \mathrm{Hom}(E, E).$$

The endomorphism ring consists of all isogenies going from an elliptic curve $E$ to itself. It has the structure of a ring, where we define multiplication of elements as composition of maps, i.e. $\phi \cdot \psi = \phi \circ \psi$.

**Definition 2.21.** Let $k$ be a field and let $A$ be a vector space over $k$, equipped with a bilinear map $A \times A \to A$, we the map by $\cdot$ here. Then $A$ is an algebra over $k$ if for all $x, y, z \in A$ and for all $a, b \in k$ the following hold:

- $(x + y) \cdot z = x \cdot z + y \cdot z$
- $z \cdot (x + y) = z \cdot x + z \cdot y$
- $(ax) \cdot (by) = (ab)(x \cdot y)$.

**Definition 2.22.** Let $\mathcal{K}$ be a $\mathbb{Q}$-algebra that is finitely generated over $\mathbb{Q}$. An *order* $\mathcal{O}$ of $\mathcal{K}$ is a subring of $\mathcal{K}$ that is finitely generated as a $\mathbb{Z}$-module and satisfies $\mathcal{O} \otimes \mathbb{Q} = \mathcal{K}$.

**Definition 2.23.** A *quaternion algebra over* $\mathbb{Q}$ is an algebra of the form

$$\mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k,$$

where the multiplication satisfies

$$i^2, j^2 \in \mathbb{Q}, \quad i^2 < 0, \quad j^2 < 0, \quad ij = -ji = k.$$

It is important to note that a quaternion algebra is not commutative.

Given an elliptic curve $E$ over a field $k$ with characteristic $p \geqslant 0$, the multiplication-by-$[m]$ map is non-constant whenever $m \neq 0$ (from [5, Theorem III.4.2.(a)]). This implies the following theorem.

**Theorem 2.24.** *Let $E_1, E_2$ be elliptic curves over $k$. Then $\mathrm{Hom}(E_1, E_2)$ is a torsion-free $\mathbb{Z}$-module.*

*Proof.* We have seen that $\mathrm{Hom}(E_1, E_2)$ has a group structure. Moreover, the multiplication-by-$[m]$ map can be used to give scalar multiplication

$$\begin{aligned} \mathbb{Z} \times \mathrm{Hom}(E_1, E_2) &\to \mathrm{Hom}(E_1, E_2) \\ (m, \phi) &\mapsto [m] \circ \phi. \end{aligned}$$

Also, whenever $[m] \circ \phi = [0]$ for non-trivial $m$, $\deg([m]) \cdot \deg(\phi) = 0$. Since $m$ is non-trivial, $\deg([m]) \geqslant 1$, hence $\phi$ must be the zero map. Therefore $\mathrm{Hom}(E_1, E_2)$ is torsion-free. □

Now consider $\mathrm{Hom}(E, E) =: \mathrm{End}(E)$, for some elliptic curve $E/k$. As mentioned, using composition as the multiplication in $\mathrm{End}(E)$, we give $\mathrm{End}(E)$ a ring structure.

**Theorem 2.25.** *Let $E$ be an elliptic curve over $k$. Then $\mathrm{End}(E)$ is a domain.*

*Proof.* By the previous theorem, $\mathrm{Hom}(E, E)$ is torsion-free, hence $\mathrm{End}(E)$ has characteristic zero. Moreover, $\mathrm{End}(E)$ is an integral domain, since for $\phi, \psi \in \mathrm{End}(E)$,

$$\phi \circ \psi = [0]$$

implies that $\deg(\phi) \cdot \deg(\psi) = 0$, hence either $\phi$ or $\psi$ has to be the zero map. □

For an endomorphism ring of an elliptic curve $\mathrm{End}(E)$, we define the (reduced) trace and (reduced) norm maps as follows

$$T(\phi) := \phi + \hat{\phi} \quad \text{and} \quad N(\phi) := \phi\hat{\phi}.$$

Note that the norm map defined as above coincides with multiplication by the degree of $\phi$, i.e. $N(\phi) = \phi\hat{\phi} = \phi \circ \hat{\phi} = [\deg(\phi)]$. As mentioned before, the degree map is a positive definite quadratic form.

We will now define the concept of ramification. We denote the $p$-adic numbers by $\mathbb{Q}_p$.

**Definition 2.26.** Let $\mathcal{K}$ be a quaternion algebra over $\mathbb{Q}$ and let $p$ be a prime. We say $\mathcal{K}$ is *split at p* or *unramified at p* if $\mathcal{K}_p := \mathbb{Q}_p \otimes \mathcal{K} \cong M_{2\times 2}(\mathbb{Q}_p)$. We say that $\mathcal{K}$ is *non-split at p* or *ramified at p* if $\mathcal{K}_p$ is not isomorphic to $M_{2\times 2}(\mathbb{Q}_p)$.
Similarly we say that $\mathcal{K}$ is *split at infinity* if $\mathcal{K}_\infty := \mathbb{R} \otimes \mathcal{K} \cong M_{2\times 2}(\mathbb{R})$. We say that $\mathcal{K}$ is *ramified at infinity* if $K_\infty$ is not isomorphic to $M_{2\times 2}(\mathbb{R})$.

**Theorem 2.27** (Deuring)**.** *Let $E$ be an elliptic curve over a field $k$ of characteristic $p$. Then the endomorphism ring* $\mathrm{End}(E)$ *is isomorphic to one of the following:*

*(i)* $\mathbb{Z}$*, this only happens if* $p = 0$*;*

*(ii) An order $\mathcal{O}$ in a quadratic imaginary field, in this case we say that $E$ has complex multiplication by $\mathcal{O}$;*

*(iii) An order in a quaternion algebra over $\mathbb{Q}$ ramified at $p$ and the point at infinity, this only happens when $p > 0$. In this case we say that $E$ is supersingular.*

*Proof.* For the proof we refer to [5, Corollary III.9.4]. □

**Definition 2.28.** Let $E$ be an elliptic curve over a field $k$ of characteristic $p$. If the endomorphism ring of $E$ is isomorphic to an order $\mathcal{O}$ in an imaginary quadratic field, we say that $E$ is *ordinary* and that $E$ has *complex multiplication by* $\mathcal{O}$.
If the endomorphism ring of $E$ is isomorphic to an order in a quaternion algebra over $\mathbb{Q}$ ramified at $p$ and $\infty$, we say that $E$ is *supersingular*.

## 2.4 Supersingular elliptic curves

In this section we will consider supersingular elliptic curves in more detail.

**Theorem 2.29.** *Let $\phi : E \to E'$ be a non-constant isogeny. The elliptic curve $E$ is supersingular if and only if $E'$ is supersingular.*

*Proof.* This follows from [8, Exercise 42.1].

□

**Theorem 2.30.** *Let $E/k$ be an elliptic curve and let* $\mathrm{char}(k) = p > 0$*. Recall that we denote the $p^r$-th power Frobenius map as $\pi_r$. The following are equivalent:*

*(i) $E$ is supersingular.*

*(ii) $\widehat{\pi}_r$ is purely inseparable for $r = 1$, or equivalently, for all $r \geqslant 1$.*

*(iii) $[p]$ is purely inseparable and $j(E) \in \mathbb{F}_{p^2}$.*

*(iv) $E[p^r] = \{\mathcal{O}\}$ for $r = 1$, or equivalently, for all $r \geqslant 1$.*

*Proof.*

(ii) $\Leftrightarrow$ (iv) : By Proposition 2.11 in [5, p. 25], the $p^r$-th Frobenius endomorphism is purely inseparable for all $r$, i.e., $\deg_s(\pi_r) = 1$. Also, $\deg([p^r]) = \deg(\pi_r) \cdot \deg(\widehat{\pi}_r)$. When taking the separable degrees, we see that $\deg_s([p^r]) = \deg_s(\pi_r) \cdot \deg_s(\widehat{\pi}_r) = \deg_s(\widehat{\pi}_r)$. This gives

$$\deg_s(\widehat{\pi}_r) = \deg_s([p^r]) = \#\ker([p^r]) = \#E[p^r].$$

Hence, when $\widehat{\phi}_r$ is purely inseparable, $\#E[p^r] = 1$ so $E[p^r] = \{O\}$. When $E[p^r] = \{O\}$, the above shows that $\deg_s(\widehat{\pi}_r) = 1$. This proves the direction from (ii) to (iv) and vice versa.

(i) $\Rightarrow$ (ii) : The proof of this implication will use some knowledge of Dieudonné modules, we do not want to introduce them in this paper, but more information can be found in [5, p. 87]. We will prove the contrapositive statement, so we start by assuming that $\widehat{\pi}_r$ is separable for all $r \geqslant 1$. By Proposition 2.18, this shows that $E[p^r] \cong \mathbb{Z}/p^r\mathbb{Z}$ for all $r$. We consider the map

$$T_p : \mathrm{End}(E) \to \mathrm{End}(T_p(E)),$$

which sends $\psi$ to $\psi_p$. Suppose that $\psi_p = 0$, then $\psi(E[p^r]) = 0$ for all $r \geqslant 1$. In particular this implies that $\#\ker(\psi) \geqslant p^r$ for all $r \geqslant 1$. However, all non-constant isogenies have finite kernel, therefore $\psi = 0$. This shows that $T_p$ is injective. By [5, p. 88], we have that $T_p(E) \cong \mathbb{Z}_p$, using the assumption that $\widehat{\pi}_r$ is separable for all $r \geqslant 1$. Therefore also $\mathrm{End}(T_p(E)) \cong \mathbb{Z}_p$, which is commutative. Since $T_p$ is injective, the above implies that $\mathrm{End}(E)$ is commutative as well. This proves the statement.

(ii) $\Rightarrow$ (iii) : Again by Proposition 2.11 in [5, p. 25], we know that $\pi$ is purely inseparable. We assume in (ii) that $\widehat{\pi}$ is also purely inseparable. Since $[p] = \pi \circ \widehat{\pi}$ and the degree is multiplicative, this implies that $[p]$ is also purely inseparable.

Since $[p]$ is purely inseparable, we know that $[p]$ has separable degree equal to 1. We know that $[p]$ can be written as the composition of a separable isogeny and a power of the Frobenius endomorphism by Theorem 2.15. Hence

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

where $\psi$ is some separable isogeny and $\pi$ is the Frobenius endomorphism. Since $[p]$ is purely inseparable, $\psi$ has degree one and thus it is an isomorphism. The isogeny $\psi$ is a map from $E^{(p^2)}$ to $E$, so $j(E) = j(E^{p^2}) = j(E)^{p^2}$,

where the last equality holds since $\text{char}(k) = p$. This means that $j(E)$ is fixed by the field automorphism $\sigma : x \mapsto x^{p^2}$. In other words, it belongs to a subfield in which $x^{p^2} - x = 0$, so either the field is $\mathbb{F}_p$ or it is $\mathbb{F}_{p^2}$. This shows that $j(E)$ is in $\mathbb{F}_{p^2}$ (and sometimes even in $\mathbb{F}_p$).

(iii) $\Rightarrow$ (i) : Let $E, E'$ be elliptic curves over $k$ and let $E$ be a curve on which $[p]$ is purely inseparable and $j(E) \in \mathbb{F}_{p^2}$. Suppose that $\psi : E \to E'$ is an isogeny. We write $[p]_E$ for the multiplication-by-$p$ map on $E$ and $[p]_{E'}$ for the multiplication-by-$p$ map on $E'$. We know that $[p]_{E'} \circ \psi = \psi \circ [p]_E$. Since $[p]_E$ on $E$ is purely inseparable, this shows that $[p]_{E'}$ on $E'$ is purely inseparable as well. We saw in the proof of the previous implication that this implies $j(E') \in \mathbb{F}_{p^2}$. Therefore, there can only be finitely many elliptic curves that are isogenous to $E$.

Suppose for contradiction that $E$ is not supersingular. Then $\text{End}(E) \otimes \mathbb{Q}$ is isomorphic to $\mathbb{Q}$ or an imaginary quadratic extension of $\mathbb{Q}$, i.e. $\mathbb{Q}(\sqrt{d})$ where $d < 0$ (this follows from Theorem 2.27). We claim that in both cases, there are infinitely many primes $\ell$ such that there is no endomorphism of degree $\ell$. If $\text{End}(E) \otimes \mathbb{Q} \cong \mathbb{Q}$ then $\text{End}(E) \cong \mathbb{Z}$ and the isomorphism is given by $m \mapsto [m]$. This implies that every endomorphism in $\text{End}(E)$ has degree equal to a square, meaning that there are no isomorphisms of prime degree. Now we suppose that $\text{End}(E) \otimes \mathbb{Q} \cong \mathbb{Q}(\sqrt{d})$ for some $d < 0$. Let $\phi \in \text{End}(E)$ and note that $\phi$ is a root of the polynomial

$$f(x) := x^2 - \text{tr}(\phi)x + \deg(\phi).$$

Then the discriminant $D_f$ of the polynomial above has to be the square of an element in $\text{End}(E)$, since $\phi$ is a root of $f$. Suppose that $\phi$ has degree $\ell$, then we have $D_f = \text{tr}(\phi)^2 - 4\ell = u^2 d$, for some $u \in \mathbb{Q}$. This is true since $\text{End}(E)$ is isomorphic to an order $\mathcal{O}$ in $\mathbb{Q}(\sqrt{d})$, which in particular implies that $\mathcal{O}$ is a $\mathbb{Z}$-lattice in $\mathbb{Q}(\sqrt{d})$ and that it spans $\mathbb{Q}(\sqrt{d})$ over $\mathbb{Q}$. Therefore elements in $\mathcal{O}$ are of the form $\alpha + \beta\sqrt{d}$.

The above implies that $d$ is a square modulo $\ell$. By quadratic reciprocity, assuming $d < 0$ and $d$ and $\ell$ coprime, we can consider the cases where $\ell = \pm 1 \bmod 4$ and where $\ell$ is a square mod $d$ or not a square mod $d$. These cases fully determine whether $d$ is a square modulo $\ell$. Hence whether $d$ is a square modulo $\ell$ or not depends on the residue class of $\ell$ modulo $4d$. There is at least one residue class such that $d$ is not a square modulo $\ell$. Dirichlet's theorem on primes in arithmetic progressions then

implies that there are infinitely many primes for which $d$ is not a square modulo $\ell$.

Therefore we can take $\ell_1, \ell_2, \ldots$ to be an infinite sequence of primes, not equal to $p$, such that there are no endomorphisms in $\mathrm{End}(E)$ of degree $\ell_i$. By Theorem 2.19, we can construct a separable isogeny $\phi_i$ that has kernel $G_i \subset E[\ell_i] \cong (\mathbb{Z}/\ell_i\mathbb{Z})^2$ with $\ell_i$ elements, so $\deg(\phi_i) = \ell_i$. We denote the target curve by $E_i$, so $\phi : E \to E_i$. By Theorem 2.29 we know that the $E_i$ are also supersingular and by the above there can only be finitely many elliptic curves isogenous to $E$, hence there must be some $m$ and $n$ such that $E_m \cong E_n$. Let $\alpha$ be the isomorphism between $E_m$ and $E_n$. Now consider the endomorphism $\psi := \widehat{\phi}_n \circ \alpha \circ \phi_m$, which has degree $\ell_m \ell_n$. Note that $\mathrm{End}(E)$ cannot be isomorphic to $\mathbb{Z}$ since we assume that the characteristic is not 0. Therefore we must have that $\mathrm{End}(E) \otimes \mathbb{Q} \cong \mathbb{Q}(\sqrt{d})$, the isogeny $\psi$ is a root of the polynomial

$$g(x) := x^2 - \mathrm{tr}(\psi)x + \deg(\psi).$$

In particular this implies that the discriminant $D_g = \mathrm{tr}(\psi)^2 - 4\ell_1\ell_2$ is a square in $\mathcal{O}$. By the same argument as before this implies that $d$ has to be a square modulo $\ell_1$ and $\ell_2$, which is a contradiction.

□

In Theorem 2.30, we saw some equivalent characterizations for supersingular elliptic curves. In Definition 2.28 we defined a supersingular elliptic curve to be an elliptic curve whose endomorphism ring is isomorphic to an order in a quaternion algebra ramified only at $p$ and at infinity. The next theorem, initially proved by Deuring, gives a slightly stronger result.

**Theorem 2.31.** *Let $E$ be a supersingular elliptic curve defined over a field $k$ of characteristic $p > 0$. Then* $\mathrm{End}(E)$ *is isomorphic to a maximal order in a quaternion algebra ramified only at $p$ and at infinity.*

*Proof.* For the proof we refer to [9, Theorem 4.2]. □

With this theorem, we can change part (iii) of Theorem 2.27 by replacing "an order" with "a maximal order".

# 3 Graphs

## 3.1 Graph theory

In this section we will briefly go over some basic graph theory and highlight some important results.

**Definition 3.1.** An *undirected graph* is a pair $(V, E)$, where $V$ is a set whose elements are called vertices, and where $E \subset V \times V$ is a collection of unordered pairs $(v, w)$ of elements $v, w \in V$, called the edges.

We can also consider *directed graphs*. These also consist of a vertex set $V$ and an edge set $E$, however the edge set consists of ordered pairs of elements in $V \times V$. We will be considering undirected graphs in the rest of this section.

**Definition 3.2.** Two vertices $v, w \in V$ are said to be *connected by an edge* if $(v, w) \in E$. The neighbours of a vertex $v \in V$ are the vertices of $V$ connected to $v$ by an edge.

**Definition 3.3.** A *path* between two vertices $v, w \in V$ is a sequence of vertices $v \to v_1 \to \cdots \to v_n \to w$ where each vertex $v_i$ is connected to the next vertex $v_{i+1}$.
We define the *length of a path* to be the number of edges in the path. The *distance* between two vertices, denoted by $\mathrm{d}(v, w)$, is defined as the length of the shortest path between the vertices. If there is no such path, the vertices are said to be at infinite distance.

**Definition 3.4.** A graph is *connected* if any two vertices in $V$ have a path connecting them. If this is not the case, the graph is called disconnected.

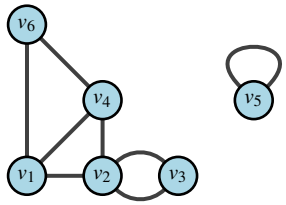
**Definition 3.5.** The *diameter* of a graph, denoted $\delta(G)$, is defined to be the largest of all distances between the vertices in $V$, i.e.

$$\delta(G) := \max_{v,w \in V} \{\mathrm{d}(v, w)\}$$

**Definition 3.6.** The *degree* of a vertex is the number of distinct edges pointing to (or from) the vertex. A graph where every edge has the same degree $k$ is called *$k$-regular*.

**Definition 3.7.** The *adjacency matrix* of a graph $G = (V, E)$ with $V = \{v_1, \ldots, v_n\}$, is the $n \times n$-matrix where the $(i, j)$-th entry equals the number of edges between the vertices $v_i$ and $v_j$.
An undirected graph therefore has a symmetric adjacency matrix. Symmetric matrices have $n$ real eigenvalues $\lambda_1 \geqslant \cdots \geqslant \lambda_n$.

**Example 3.8.** We give an example of a graph and its characteristics.




The vertices of the graph are the elements $v_i$ for $i \in \{1, \ldots, 6\}$. The edges are the black lines between the vertices. We can see for example that $v_4$ is connected to $v_2$, but $v_4$ is not connected to $v_5$ or $v_3$. However, there is a path from $v_4$ to $v_3$, e.g. the path given by $v_4 \to v_2 \to v_3$, but there is no path from $v_4$ to $v_5$. Note that the distance from $v_4$ to $v_3$ equals 2, i.e. $\mathrm{d}(v_4, v_3) = 2$. This is true since $v_4$ and $v_3$ are not connected to each other, so their distance cannot equal 1, but the path $v_4 \to v_2 \to v_3$ has length 2. The distance between $v_4$ and $v_5$ is infinite, since there is no path between the vertices. The graph is disconnected, because there is no path from $v_5$ to another vertex. This also implies that the diameter of the graph is infinite. If we were to delete $v_5$ from the graph, the diameter of the graph would be 3, since the maximum of the distances between any pair of vertices in the graph would equal 3. Note that the vertex $v_5$ has degree 1 and that the vertex $v_2$ has degree 4. The graph is not $k$-regular, since the degree of the vertices is not the same for all vertices. The adjacency matrix of the graph looks as follows:

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

**Proposition 3.9.** *If $G = (V, E)$ is a $k$-regular undirected graph, then its largest and smallest eigenvalues satisfy*

$$k = \lambda_1 \geqslant \lambda_2 \geqslant \cdots \lambda_n \geqslant -k.$$

*Proof.* We can view the adjacency matrix $A$ as a self-adjoint operator, since the matrix is symmetric and real. In particular this means that $A$ does the following

$$\begin{aligned} A : L^2(V) &\to L^2(V) \\ f &\mapsto Af, \end{aligned}$$

where

$$Af(v) = \sum_{\substack{w \in V \\ \{v,w\} \in E}} f(w).$$

We define 1 to be the constant function sending every vertex to 1. It follows that $A \cdot 1 = k \cdot 1$, since $A \cdot 1$ maps any $v \in V$ to the sum of 1 over its neighbours, which equals $k$ since the graph we are considering is $k$-regular. Therefore $k$ is an eigenvalue of $A$ with eigenvector 1.
Next we look at the operator norm of $A$. It equals the supremum of $|\langle Af, g\rangle|$, for $f, g$ with norm less than or equal 1, i.e. $\|f\|_2 \leqslant 1$ and $\|g\|_2 \leqslant 1$. Therefore for some $f, g \in L^2(V)$ with norm 1, we have

$$\begin{aligned}
\|A\|_{\text{op}} &\leqslant |\langle Af, g\rangle| \\
&= |\sum_{v \in V} \sum_{\substack{w \in V \\ \{v,w\} \in E}} f(w)\overline{g(v)}| \\
&\leqslant \frac{1}{2} \sum_{\substack{v,w \in V \\ \{v,w\} \in E}} |f(w)|^2 + |g(v)|^2 \\
&\leqslant \frac{1}{2} \cdot k \cdot \|f\|^2 + \frac{1}{2} \cdot k \cdot \|g\|^2 = k.
\end{aligned}$$

Therefore the operator norm is bounded by $k$. In particular, we can calculate the operator norm by taking the supremum over $\frac{\|Ax\|}{\|x\|}$ for non-zero $x$. Therefore for any eigenvalue $\lambda$ of $A$, we have

$$|\lambda| = \frac{|\lambda|\|x\|}{\|x\|} = \frac{\|Ax\|}{\|x\|} \leqslant k.$$

This shows that every eigenvalue has absolute value bounded by $k$.

□

## 3.2 Expander graphs and Ramanujan graphs

**Definition 3.10.** Let $\varepsilon > 0$ and $k \geqslant 1$. Let $G$ be a finite $k$-regular graph consisting of $n$ vertices. $G$ is called a *one-sided $\varepsilon$-expander* if

$$\lambda_2 \leqslant (1 - \varepsilon)k;$$

and it is called a *two-sided $\varepsilon$-expander* if it also satisfies

$$\lambda_n \geqslant -(1 - \varepsilon)k.$$

A sequence of $k$-regular graphs $G_i = (V_i, E_i)$ with $\#V_i \to \infty$ is said to be a *one-sided (resp. two-sided) expander family* if there exists an $\varepsilon > 0$ such that $G_i$ is a one-sided (resp. two-sided) $\varepsilon$-expander for all sufficiently large $i$.

**Definition 3.11.** Let $G = (V, E)$ be a graph. Let $F \subset V$ be a subset of the set vertices. The *boundary of* $F$, denoted by $\delta F \subset E$, is the subset of the edges of $G$ that go from $F$ to $V \backslash F$. The *edge expansion ratio of* $G$, denoted by $h(G)$, is the quantity

$$h(G) = \min_{\substack{F \subset V \\ \#F \leqslant \#V/2}} \frac{\#\delta F}{\#F}.$$

This expansion ratio tells us that even for a small set $S \subset V$, we have at least $h(G) \cdot \#S$ edges going from $S$ to its complement. Suppose that we are considering random walks on the graph, i.e. we know a starting position but we do not know where the walk ends. Then the higher the edge expansion ratio, the more difficult it is to determine where a random walk ended, since at a given vertex there are more edges that can be chosen to walk over. Therefore, if we want to let the random walks look as "random as possible" we like to have a large edge expansion ratio.

**Theorem 3.12** (Alon, Dodziuk, Milman, Tanner)**.** *Suppose that $G = (V, E)$ is a $k$-regular graph, then*

$$\frac{k - \lambda_2}{2} \leqslant h(G) \leqslant \sqrt{2k(k - \lambda_2)}.$$

*Proof.* The proof is given in [10, Proposition 1.84]. □

The theorem above gives a bound for the edge expansion ratio in terms of the largest eigenvalue of $G$ that does not equal $k$, i.e. $\lambda_2$. In particular, $h(G)$ is large if and only if $\lambda_2$ is small. Therefore, if we want random walks to look as "random as possible", we want $\lambda_2$ to be as small as possible. This motivates the introduction of so-called *Ramanujan graphs*.

**Definition 3.13** (Big O notation)**.** Suppose $f$ is a real or complex valued function and suppose that $g$ is a real valued function. We say $f(x) = O(g(x))$ if there exist some real number $M > 0$ and a real number $x_0$ such that $|f(x)| \leqslant Mg(x)$ for all $x \geqslant x_0$.

**Theorem 3.14.** *Let $k \geqslant 1$ and let $(G_n)$ be a sequence of $k$-regular graphs with $n$ vertices. We denote the eigenvalues of $G_n$ by $\lambda_{n,j}$ for $j \in \{1, \ldots, n\}$. Then*

$$\max\{|\lambda_{n,2}|, |\lambda_{n,n}|\} \geqslant 2\sqrt{k-1} - O(1),$$

*as $n \to \infty$.*

*Proof.* This is proven in [11, Theorem 5.3] □

**Definition 3.15.** A graph such that $|\lambda_i| \leqslant 2\sqrt{k-1}$ for every $\lambda_i$ except for $\lambda_1$, is called a *Ramanujan graph*.

This means that Ramanujan graphs are graphs for which the eigenvalues are as small as possible. In particular this means that Ramanujan graphs are "the best possible" expander graphs, since a small $\lambda_2$ gives a large edge expansion ratio $h(G)$. As mentioned before, this gives the graph nice randomness properties. This was used for example by [1] to create a hash function using supersingular isogeny graphs. These graphs are Ramanujan, as we will see in Section 5. This hash function uses its input as "directions" on a supersingular isogeny graph, i.e. it converts the input into a walk on the graph, starting at a certain vertex. The output of the hash function is a vertex on the graph. A good hash function needs to generate a random looking output (by definition), hence the rapid mixing property of the isogeny graph (which is Ramanujan) makes the output look random. Randomness is important in many aspects of cryptography; when choosing a secret key for example, we need "sufficient" randomness, otherwise an adversary might be able to guess the secret key with too large probability. Hence the aforementioned fact that supersingular isogeny graphs are Ramanujan potentially makes them very useful for cryptographic protocols.

The rapid mixing property of Ramanujan graphs is the reason for the observed randomness. We will formalise what it means to have "rapid mixing".

**Definition 3.16.** Let $G$ be a $k$-regular undirected graph and denote its adjacency matrix by $A$. Then the *normalized adjacency matrix for $G$* is given by

$$P := \frac{1}{k} \cdot A.$$

We label the vertices of $G = (V, E)$ by $v_i$ for $i \in \{1, \ldots, n\}$. When we consider $P(v_i, v_j)$, we look at the $i, j$-th entry in the matrix $P$. We view this value as the probability that, in one step, a random walk that starts at $v_i$ ends at $v_j$.

We are considering the case where we choose a random vertex, according to some probability distribution $\mathbf{p}$ on the vertices, and then take a random walk of length 1. Given a starting point $v_i$, we know that the probability of the walk ending at $v_j$ equals $P(v_i, v_j)$. Therefore, the probability of a random walk of length 1 (when we are not given a starting point) terminating at a vertex $v_j$ equals

$$\sum_{v_i \subset V} \mathbf{p}(v_i) P(v_i, v_j).$$

Note that we can consider the distribution $\mathbf{p}$ to be some vector in $\mathbb{R}^n$ such that $p(v_i) \geqslant 0$ for all $i$ and such that $\sum_{v_i \in V} p(v_i) = 1$. Then, using the fact that $P$ is symmetric, we have that the probability distribution after one step is described by the vector

$$\mathbf{p}^T \cdot P = P \cdot \mathbf{p}.$$

Iterating this, we see that for a random walk of length $r$, where the starting point is chosen according to the distribution $\mathbf{p}$, the endpoint of the walk is distributed according to

$$P^r \cdot \mathbf{p}.$$

Let $\mathbf{u}$ be the uniform distribution. Viewing the distributions as vectors in $\mathbb{R}^n$, we can consider the distance between the distribution of the endpoint of a random walk and the uniform distribution. We measure this distance using the *total variation distance*.

**Definition 3.17.** Let $\mathbf{p}$ and $\mathbf{q}$ be distributions over the set of vertices $V$. We define the *total variation distance* or *statistical distance* as

$$\max_{S \subset V} \left( \sum_{v \in S} \mathbf{p}(v) - \sum_{v \in S} \mathbf{q}(v) \right).$$

Distributions with disjoint support have total variation equal to 1, this is also the largest possible value. Hence two distributions that have total variation 1 are maximally far from each other in the sense of this measure of distance. One can show that the total variation distance equals $\frac{1}{2} \cdot ||\mathbf{p} - \mathbf{q}||_1$, where $|| \cdot ||_1$ stands for the 1-norm or "taxicab norm". The 1-norm of a vector $\mathbf{v}$ of length $n$ equals:

$$||\mathbf{v}||_1 =:= \sum_{i=1}^{n} |v_i|.$$

**Proposition 3.18.** *Let* $\mathbf{p}$ *and* $\mathbf{q}$ *be distributions over the set of vertices* $V$*. The total variation distance equals*

$$\max_{S \subset V} \left( \sum_{v \in S} \mathbf{p}(v) - \sum_{v \in S} \mathbf{q}(v) \right) = \frac{1}{2} ||\mathbf{p} - \mathbf{q}||_1.$$

*Proof.* Recall that $||\mathbf{p}-\mathbf{q}||_1 := \sum_{v\in V} |\mathbf{p}(v)-\mathbf{q}(v)|$. Let $A \subset V$ and consider the set $B \subset V$ where $B := \{v \in V \ : \ \mathbf{p}(v) \geqslant \mathbf{q}(v)\}$. We have the following

$$\mathbf{p}(A)-\mathbf{q}(A) \leqslant \mathbf{p}(A\cap B)-\mathbf{q}(A\cap B) \leqslant \mathbf{p}(B)-\mathbf{q}(B),$$

where we use the definition of $B$. Also,

$$\mathbf{q}(A)-\mathbf{p}(A) \leqslant \mathbf{q}(A\cap B^c)-\mathbf{p}(A\cap B^c) \leqslant \mathbf{q}(B^c)-\mathbf{p}(B^c) = \mathbf{p}(B)-\mathbf{q}(B).$$

Therefore we have that

$$|\mathbf{p}(A)-\mathbf{q}(A)| \leqslant \mathbf{p}(B)-\mathbf{q}(B), \tag{3}$$

for all sets $A \subset V$. Note that $|\mathbf{p}(A)-\mathbf{q}(A)| = |\sum_{v\in A}\mathbf{p}(v) - \sum_{v\in A}\mathbf{q}(v)|$ and note that $|\mathbf{p}(A)-\mathbf{q}(A)|$ is maximal when $A = B$ or $A = B^c$, by (3). Therefore

$$\begin{aligned}
\max_{S\subset V}\left(\sum_{v\in S}\mathbf{p}(v)-\sum_{v\in S}\mathbf{q}(v)\right) &= \frac{1}{2}|\mathbf{p}(B)-\mathbf{q}(B)| + \frac{1}{2}|\mathbf{p}(B^c)-\mathbf{q}(B^c)| \\
&= \frac{1}{2}(\mathbf{p}(B)-\mathbf{q}(B)) + \frac{1}{2}(\mathbf{q}(B^c)-\mathbf{p}(B^c)) \\
&= \frac{1}{2}\sum_{v\in B}(\mathbf{p}(v)-\mathbf{q}(v)) + \frac{1}{2}\sum_{w\in B^c}(\mathbf{q}(w)-\mathbf{p}(w)) \\
&= \frac{1}{2}\sum_{v\in B}|\mathbf{p}(v)-\mathbf{q}(v)| + \frac{1}{2}\sum_{w\in B^c}|\mathbf{p}(w)-\mathbf{q}(w)| \\
&= \frac{1}{2}\sum_{v\in V}|\mathbf{p}(v)-\mathbf{q}(v)| = \frac{1}{2}||\mathbf{p}-\mathbf{q}||_1.
\end{aligned}$$

□

**Theorem 3.19.** *Let $G$ be a $k$-regular graph with $n$ vertices and let $P$ be its normalized adjacency matrix. Then for every distribution $\mathbf{p}$ over the vertices and for every $r$, we have that*

$$||P^r\mathbf{p}-\mathbf{u}||_1 \leqslant \sqrt{n}\left(\frac{\lambda_2}{k}\right)^r,$$

*where $\mathbf{u}$ is the uniform distribution.*

*Proof.* The proof is given in [12, Lemma 1]. □

**Theorem 3.20.** *Let $G$ be a $k$-regular $\varepsilon$-expander graph and let $P$ be its normalized adjacency matrix. Then it takes $O\left(\frac{\log n}{1-\lambda_2}\right)$ steps before*

$$||P^r\mathbf{p} - \mathbf{u}||_1 < \frac{1}{n}.$$

*We call the amount of steps necessary to reach this the* mixing time *of the graph.*

*Proof.* By Theorem 3.19 and the fact that $k \geqslant \lambda_2$ we have that

$$||P^r\mathbf{p} - \mathbf{u}||_1 \leqslant \sqrt{n} \cdot \lambda_2^r.$$

If we want the right-hand side to be less than $1/n$ we need

$$r > \frac{\log\left(\frac{1}{n\sqrt{n}}\right)}{\log(\lambda_2)} = \frac{\log(n\sqrt{n})}{\log\left(\frac{1}{\lambda_2}\right)}.$$

Note that

$$\log(1/\lambda_2) = \sum_{i=1}^{\infty}(-1)^{i+1}\frac{(1/\lambda_2 - 1)^i}{i}.$$

Hence $\log(1/\lambda_2) = O(1/\lambda_2 - 1) = O(1 - \lambda_2)$. Also note that $\log(n\sqrt{n}) = \frac{3}{2}\log(n)$, therefore $\log(n\sqrt{n}) = O(\log(n))$. We conclude that $r$ has to be of the order

$$O\left(\frac{\log(n)}{1-\lambda_2}\right).$$

□

Again we see that a small value for $\lambda_2$ has an advantage for the randomness property of the graph, since the smaller $\lambda_2$ is, the faster the graph mixes. Ramanujan graphs are defined to be expander graphs with eigenvalues as small as possible, hence they mix as fast as is possible for a graph.

# 4 Key Exchange

In *secret key encryption* (also *private key encryption* or *symmetric key encryption*) two people try to communicate over a channel using the same key and without letting anyone else, i.e. some eavesdropper, gain "too much" information on their message or key. A natural question to ask is the following: how do the two parties agree on a key, without leaking too much information about the key? This is where the so called *key exchange protocols* come into play. In this section we will look at some (standard) key exchange protocols. In Section 6 we will see how isogeny graphs can be useful for key exchange protocols.

In 1976 Diffie and Hellman published a cryptographic protocol for key exchange, called the *Diffie-Hellman key exchange* (although Hellman later suggested it be called the *Diffie-Hellman-Merkle key exchange*, since the protocol was based on a concept by Merkle). It is based on the assumption that given a cyclic group $G$, a generator $g$ for the group and an element $x \in G$, it is hard to find $a$ such that $x = g^a$. This is called the *discrete logarithm assumption*. Diffie-Hellman key exchange is illustrated in the figure below. Here $x \leftarrow\!\!\$\ S$ means that $x$ is chosen uniformly at random from a set $S$.

Diffie-Hellman key exchange

**Public parameters** : A group $(\mathbb{Z}/p\mathbb{Z})^*$, where $p$ is prime
$g \in (\mathbb{Z}/p\mathbb{Z})^*$ where $g$ is a generator

| **Alice** | | **Bob** |
|---|---|---|
| $a \leftarrow\!\!\$\ \{1, \dots p-1\}$ | | $b \leftarrow\!\!\$\ \{1, \dots p-1\}$ |
| $A := g^a$ | | $B := g^b$ |
| | $\xrightarrow{A}$ | |
| | $\xleftarrow{B}$ | |
| $k := B^a$ | | $k := A^b$ |

Figure 1: Diffie-Hellman

There are some necessary constraints to eliminate the possibility of 'simple' attacks on this protocol, but we will not go into those here. Note that since $g^{ab} = g^{ba}$ Alice and Bob indeed agree on the same key, without simply leaking the key to a potential eavesdropper.

This protocol can easily be generalized to the case where $(\mathbb{Z}/p\mathbb{Z})^*$ is a cyclic group of prime order in which the discrete logarithm problem is assumed to be hard. To do this we can replace the group $(\mathbb{Z}/p\mathbb{Z})^*$ by some cyclic group $G = \langle g \rangle$. For example, we can take the cyclic group to be the points on an elliptic curve over a finite field $\mathbb{F}_p$ where $p$ is prime. The protocol that generalizes the Diffie-Hellman protocol using elliptic curves is called the Elliptic Curve Diffie-Hellman protocol, it is illustrated in the figure below.

Elliptic Curve Diffie-Hellman

**Public parameters** : A finite field $\mathbb{F}_p$, where $p$ is prime
An elliptic curve $E/\mathbb{F}_p$ with $\#E(\mathbb{F}_p)$ prime
A generator $P$ of $E(\mathbb{F}_p)$

| **Alice** | | **Bob** |
|---|---|---|
| $a \leftarrow\$ \{1, \ldots, \#E(\mathbb{F}_p)\}$ | | $b \leftarrow\$ \{1, \ldots, \#E(\mathbb{F}_p)\}$ |
| $A := [a]P$ | | $B := [b]P$ |
| | $\xrightarrow{A}$ | |
| | $\xleftarrow{B}$ | |
| $k := [a]B$ | | $k := [b]A$ |

Figure 2: ECDH

Since the multiplication-by-$m$ map is commutative, Alice and Bob end up with the same key. Also, the discrete logarithm problem is assumed to be hard in the group of points of an elliptic curve. Elliptic Curve Diffie-Hellman (ECDH) is used for example in TLS. TLS (Transport Layer Security) is a cryptographic protocol that is widely used, e.g. for secure web browsing, but also for other applications like e-mail, instant messaging and file transfers.

Next we will define the concept of Schreier graphs, which are useful for key exchange protocols in which the secrets are random walks.

**Definition 4.1** (Schreier graphs)**.** Let $G$ be a group acting freely on a set $X$, i.e., there is a map

$$G \times X \to X$$
$$(\sigma, x) \mapsto \sigma \cdot x$$

such that $\sigma \cdot x = x$ if and only if $\sigma = 1$, and $\sigma \cdot (\tau x) = (\sigma \cdot \tau) \cdot x$, for all $\sigma, \tau \in G$ and for all $x \in X$. Let $S \subset G$ be a symmetric subset, i.e., a subset not containing 1 and closed under inversion. The *Schreier graph* of $(S, X)$ is the graph whose vertices are the elements of $X$. Two elements $x, x' \in X$ are connected by an edge if and only if $\sigma \cdot x = x'$ for some $\sigma \in S$.

Schreier graphs are undirected and regular graphs and often they are good expander graphs as well [13, Exercise III.2]. To construct a key exchange protocol we restrict to cyclic groups of order $p$, where $p$ is a prime, and we pick a generator $g$ for $G$, so $G = \mathbb{Z}/p\mathbb{Z} = \langle g \rangle$. We choose $D = \{s_1, \ldots, s_n\} \subset (\mathbb{Z}/p\mathbb{Z})^\times$ such that whenever $\sigma \in D$, $\sigma^{-1} \notin D$. Let $S := D \cup D^{-1}$. If we consider $G \backslash \{1\}$, we see that $S$ acts freely on $G \backslash \{1\}$. We also say that $G$ is a *principal homogeneous space* for $(\mathbb{Z}/p\mathbb{Z})^\times$ under the action

$$\sigma(g) = g^\sigma \quad \text{for } \sigma \in D \text{ and } g \in G \backslash \{1\}.$$

Hence we can consider the Schreier graph $(S, G \backslash \{1\})$, where a walk from a vertex $g_0$ corresponds to the action of an element $\sigma_1, \ldots, \sigma_n$ for $\sigma_i \in S$ on $g_0$, such that the end point of the walk equals $g_0^{\sigma_1 \cdots \sigma_n}$. We call such a sequence $\rho := (\sigma_1, \ldots, \sigma_n)$ a *directed route*. We denote $\rho(g)$ for the vertex where the walk defined by $\rho$ and $g$ ends. When considering two directed routes $\rho, \rho'$ on the Schreier graph $G$ and $g$ is a vertex, we can see that $\rho'(\rho(g))) = \rho(\rho'(g))$. This commutativity gives us a simple way to generalize Diffie-Hellman using a Schreier graph:

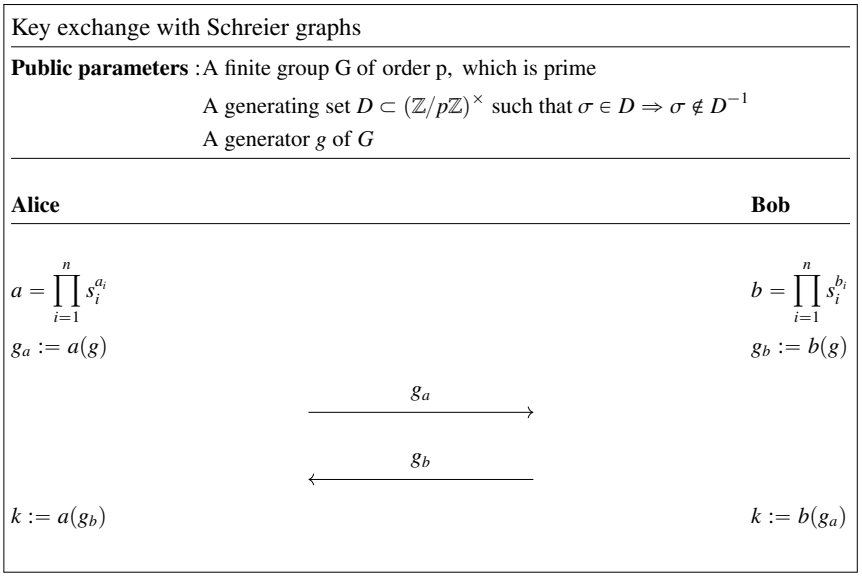



Figure 3: Key exchange with Schreier graphs

We can clearly see the similarities between the (standard) Diffie-Hellman protocol and the protocol based on Schreier graphs. One can imagine that for this protocol to be safe, it is necessary that the walks that Alice and Bob take look "random enough". Since if the walks are too predictable, an adversary (or eavesdropper) could for example try some of the walks that they think might be the ones Alice or Bob took and then try to find the key $k$ by starting a walk at $g_a$ or $g_b$.

A protocol that uses these Schreier graphs is the Rostovtsev-Stolbunov protocol. In this protocol we consider the set $\mathrm{Ell}_q(\mathcal{O})$, which is the set of $\overline{\mathbb{F}}_q$-isomorphism classes of elliptic curves that have complex multiplication by some fixed order $\mathcal{O} \subset \mathbb{Q}(\sqrt{d})$, where $d < 0$. It turns out that the class group of $\mathcal{O}$ acts freely on $\mathrm{Ell}_q(\mathcal{O})$ (we will not specify the group action, but more details can be found in [14]). The vertices of the graph hence correspond to the $j$-invariants belonging to the isomorphism class of elliptic curves and the edges correspond to isogenies. This protocol can be used for key exchange, but unfortunately it is too slow to use in practice. The Rostovtsev-Stolbunov protocol uses ordinary elliptic curves since the class group of an order in an imaginary quadratic field is commutative. For supersingular elliptic curves this is not true in general, therefore we would have to make some larger adaptations to define a key exchange protocol using supersingular isogeny graphs in a similar way. In the upcoming sections we will see how we can instantiate a key exchange protocol using supersingular elliptic curves.

# 5 Isogeny graphs

Isogeny graphs from both ordinary and supersingular elliptic curves have been considered for use in cryptographic protocols. The main differences between these type of graphs lies in the fact that the endomorphism ring of supersingular elliptic curves is isomorphic to a (maximal) order in a quaternion algebra, which is non-commutative.

**Definition 5.1.** Let $p$ be a prime. An *isogeny graph* is a (multi-)graph that has vertex set $V$, consisting of the isomorphism classes of elliptic curves over $\overline{\mathbb{F}_p}$ that are isogenous and the edge set $E$ consists of the isogenies between the elements of the isomorphism classes.

We first direct our attention to isogeny graphs of ordinary elliptic curves, i.e. the vertices consist of isomorphism classes of ordinary elliptic curves.

## 5.1 Ordinary isogeny graphs

In this section we will consider ordinary isogeny graphs.

**Theorem 5.2.** *Let $\mathbb{F}_q$ be a finite field, let $\mathcal{O} \subset \mathbb{Q}[\sqrt{-d}]$, where $d > 0$, be an order in an imaginary quadratic field. Denote by $\mathrm{Ell}_q(\mathcal{O})$ the set of elliptic curves defined over $\mathbb{F}_q$ that have complex multiplication by $\mathcal{O}$, i.e., their endomorphism rings are isomorphic to $\mathcal{O}$. Assume that $\mathrm{Ell}_q(\mathcal{O})$ is non-empty. Then the class group $\mathrm{Cl}(\mathcal{O})$ acts freely and transitively on it (alternatively we can say that the action is simply transitive); in other words, there is a map*

$$\begin{aligned} \mathrm{Cl}(\mathcal{O}) \times \mathrm{Ell}_q(\mathcal{O}) &\to \mathrm{Ell}_q(\mathcal{O}) \\ (\mathfrak{a}, E) &\mapsto \mathfrak{a} \cdot E \end{aligned}$$

*such that $(1) \cdot E = E$ and $\mathfrak{a} \cdot (\mathfrak{b} \cdot E) = (\mathfrak{a}\mathfrak{b}) \cdot E$ for all $\mathfrak{a}, \mathfrak{b} \in \mathrm{Cl}(\mathcal{O})$ and for all $E \in \mathrm{Ell}_q(\mathcal{O})$. Also, the map is such that for any $E, E' \in \mathrm{Ell}_q(\mathcal{O})$ there is a unique $\mathfrak{a} \in \mathrm{Cl}(\mathcal{O})$ such that $E' = \mathfrak{a} \cdot E$.*

*Proof.* For the proof we refer to [9, Theorem 4.5], we will only give an outline of the proof here. For an element $\mathfrak{a}$ in the class group, we define

$$E[\mathfrak{a}] := \{P \in E(\overline{\mathbb{F}_q}) \mid \sigma(P) = 0_E \ \forall \sigma \in \mathfrak{a}\}.$$

The map in question is given by

$$\mathfrak{a} \cdot E := E/E[\mathfrak{a}].$$

Let $B$ be the endomorphism algebra of an ordinary elliptic curve $E$, i.e., $B = \mathrm{End}(E) \otimes \mathbb{Q}$, and let $\mathcal{O}$ be an order in $B$ that is possibly an endomorphism ring. It can be shown that the ideal class group $\mathrm{Cl}(\mathcal{O})$ operates freely on the isomorphism classes of curves with endomorphism ring $\mathcal{O}$. This follows from [9, Theorem 3.11]. What's left to show is that the action is transitive and this is equivalent to showing that there is only one orbit. The fact that there is only one orbit follows by proving that all subgroups of an (ordinary) elliptic curve $E$ can be written as $H = E[\mathfrak{a}]$ for some $\mathcal{O}$-ideal $\mathfrak{a}$. □

The fact that the class group acts on $\mathrm{Ell}_q(\mathcal{O})$ in this way gives us a way to choose an isogeny graph that is also a Schreier graph. There are a couple of conditions that need to be met for such isogeny graphs to be (useful) Schreier graphs, but we will not go into detail on those conditions here, for more details we refer to [14]. After making this into a Schreier graph, the key exchange protocol that was explained in Figure 3 can be executed using an ordinary isogeny graph. This protocol was first described such that it could be efficiently implemented by Rostovtsev and Stolbunov, it is also called the Rostovtsev-Stolbunov protocol [15].

What happens essentially in this protocol is the following: first a starting point $E$ in the graph is chosen and primes $\ell_i$ are fixed. Alice chooses a random exponent $a_i$ for each $\ell_i$ and computes a curve $E_A$ that is $\prod \ell_i^{a_i}$-isogenous to $E$. Bob does the same with exponents $b_i$ and arrives at some curve $E_B$. Alice and Bob publish $E_A$ and $E_B$, respectively, but they keep their exponents $a_i$ and $b_i$ a secret. Alice now computes a curve $E_{BA}$ that is $\prod \ell_i^{a_i}$-isogenous to $E_B$ and Bob computes a curve $E_{AB}$ that is $\prod \ell_i^{b_i}$-isogenous to $E_A$. Since the endomorphism ring of ordinary elliptic curves is commutative, the curves $E_{AB}$ and $E_{BA}$ are isomorphic, hence Alice and Bob have arrived at the same point in the isogeny graph.

However, the Rostovtsev-Stolbunov protocol turns out to be too slow to be useful (in this form) in practice. Also, Childs, Jao and Soukharev showed that the protocol could be broken with a sub-exponential quantum attack [16]. Therefore the parameters of the protocol need to be scaled up asymptotically to make it safe, but this makes the protocol even slower than it already was.

As we mentioned, the main differences between ordinary and supersingular isogeny graphs lies in the fact that the endomorphism ring of supersingular elliptic curves is isomorphic to a (maximal) order in a quaternion algebra, which is non-commutative, whereas the endomorphism ring of an ordinary elliptic curve is commutative. The commutativity of the endomorphism ring of ordinary elliptic curves is the reason that the Rostovtsev-Stolbunov protocol could be quite 'sim-

ple'. If we would want to do something similar with supersingular elliptic curves, we would have to do some more work because we do not have the commutativity of the class group of the endomorphism ring. In the next section we will direct our attention to *supersingular isogeny graphs*.

## 5.2 Supersingular isogeny graphs

**Definition 5.3.** Let $p$ be a prime and let $\ell$ be a prime such that $\ell \neq p$. The *supersingular isogeny graph* $G(p,\ell)$ is a graph that has vertex set $V$, which consists of the isomorphism classes of supersingular elliptic curves over $\mathbb{F}_{p^2}$. Furthermore, the edge set $E$ consists of all isogenies of degree $\ell$ between the isomorphism classes up to post-composition by an automorphism.

**Remark 5.4.** One can use the so called *modular polynomials* to solve the question whether two given $j$-invariants are $\ell$-isogenous. Modular polynomials $\Phi_\ell(x,y)$ are the polynomials such that when setting $\Phi_\ell(x,y) = 0$, they represent a classical modular curve called $X_0(\ell)$. We denote the $\ell$-th modular polynomial by $\Phi_\ell(x,y)$. The following holds:

$$\Phi_\ell(j_1,j_2) = 0 \quad \text{if and only if } j_1 \text{ and } j_2 \text{ are } \ell - \text{isogenous.}$$

This can be found in e.g. [17, Section 2.3]. In [18] the following is stated

$$\Phi_2(X,1728) = (X-1728)(X-66^3)^2 \quad \text{and} \quad \Phi_2(X,0) = (X-2^4\cdot 3^3\cdot 5^3)^3,$$

this implies that $j = 1728$ has an edge with itself and two edges with $66^3$ and that $j = 0$ has three edges with $2^4\cdot 3^3\cdot 5^3$.

**Remark 5.5.** Because of the existence and uniqueness of the dual isogeny in Theorem 2.16, we can make $G(p,\ell)$ into an "almost" undirected graph, in particular, it is undirected except at $j = 0$ and $j = 1728$; consider any edge between the isomorphism classes of two elliptic curves $E_1$ and $E_2$, where $E_1$ and $E_2$ do not have $j$-invariant 0 or 1728. This edge corresponds to an isogeny $\phi$. By Theorem 2.16 there exists a unique isogeny $\widehat{\phi}$ going from $E_2$ to $E_1$, such that $\widehat{\phi}\circ\phi = [\deg(\phi)] = [\ell]$. The isogeny $\widehat{\phi}$ corresponds to an edge from $E_2$ to $E_1$, since $\deg(\widehat{\phi}) = \deg(\phi) = \ell$. However, something else happens at the $j$-invariants $j = 0$ and $j = 1728$. Indeed, we will see that supersingular isogeny graphs are $\ell + 1$ regular and connected and we saw Remark 5.4 that in the graph $G(p,2)$, the vertex $j = 0$ always has three edges going to the vertex with $j = 2^4\cdot 3^3\cdot 5^3$. If the isogeny graph were undirected, that would mean that three edges would have to go back to the vertex $j = 0$, but then the graph would have a disconnected component consisting of the vertices $j = 0$ and $j = 2^4\cdot 3^3\cdot 5^3$ and three edges between them. The problem

here lies in the way we define the edges of the supersingular isogeny graph. Some papers say that the edges of the supersingular isogeny graph are isogenies 'up to isomorphism', what this means precisely is not always specified. In [19], two isogenies $\phi : E_1 \to E_2$ and $\phi' : E_1' \to E_2'$ are said to be equivalent (i.e. represent the same edge in the graph) if there exists isomorphisms $\alpha : E_1' \to E_1$ and $\beta : E_2 \to E_2'$ such that

$$\phi' = \beta \circ \phi \circ \alpha.$$

Note that if we define the edges in this way, the supersingular isogeny graphs will in general not be $\ell + 1$-regular, because according to 5.4, $j = 0$ will only have one edge (going to $j = 2^4 \cdot 3^3 \cdot 5^3$) and $j = 1728$ will only have two edges (going to $j = 1728$ and $j = 66^3$). We use another definition for the edges, which is also in line with the definition of *Brandt matrices* (which we will see later on). Using this definition we preserve the $\ell$+1 regularity.

We say in Definition 5.3 that two isogenies $\phi$ and $\phi'$ are equivalent if there exists an automorphism $\alpha$ such that

$$\phi = \alpha \circ \phi'.$$

This gives an interesting situation at the $j$-invariants $j = 0$ and $j = 1728$, since their automorphism groups are larger than those of other $j$-invariants. In fact, an elliptic curve with $j$-invariant 0 has automorphism group $\mathbb{Z}/6\mathbb{Z}$ and an elliptic curve with $j$-invariant 1728 has automorphism group $\mathbb{Z}/4\mathbb{Z}$, whereas elliptic curves with other $j$-invariants have automorphism group $\mathbb{Z}/2\mathbb{Z}$. We consider what happens at $j = 0$ in a 2-isogeny graph. We denote the elements of the automorphism group for $j = 0$ as $[1], [-1], [\zeta_3], [2\zeta_3], [-\zeta_3], [-2\zeta_3]$ (hence $[-\zeta_3]$ generates the automorphism group). For $j \neq 0, 1728$, the automorphism group consists of $[1], [-1]$. Suppose $\phi : E \to E'$ is an isogeny of degree 2 and $j(E) = 0$ and $j(E') = 2^4 \cdot 3^3 \cdot 5^3$. Then we can consider this isogeny composed with automorphisms of $E$, we get

$$\begin{aligned}
\phi_1 &:= \phi \circ [1] \\
\phi_2 &:= \phi \circ [\zeta_3] \\
\phi_3 &:= \phi \circ [2\zeta_3] \\
\phi_4 &:= \phi \circ [-1] \\
\phi_5 &:= \phi \circ [-\zeta_3] \\
\phi_6 &:= \phi \circ [-2\zeta_3].
\end{aligned}$$

The only post-compositions of automorphisms we can make at $j(E')$ are with $[1]$ and $[-1]$. Therefore $\phi_1 \sim \phi_4$ and $\phi_2 \sim \phi_5$ and $\phi_3 \sim \phi_6$, but there are no other equivalences than this. Therefore we have three edges going from $j(E)$ to $j(E')$.

However, considering the duals of $\phi_1, \phi_2$ and $\phi_3$, we see that

$$\widehat{\phi_1} = \widehat{\phi} \quad \text{and} \quad \widehat{\phi_2} = [2\zeta_3] \circ \widehat{\phi} \quad \text{and} \quad \widehat{\phi_3} = [\zeta_3] \circ \widehat{\phi}.$$

Since $[\zeta_3]$ and $[2\zeta_3]$ are automorphisms of $E$, we have that all these duals are equivalent, and therefore we only have a single edge going from $j(E')$ to $j(E)$ in a 2-isogeny graph with $p > 5$. Something similar happens at $j = 1728$, where there is up to equivalence one extra automorphism compared to other $j$-invariants. Therefore we get two edges going out of $j = 1728$ (if the characteristic is not 2 or 3), but only one comes back. Note that at all other $j$-invariants, the graph does not have this problem, since the automorhpism groups are all $\mathbb{Z}/2\mathbb{Z}$.

Defining isogeny graphs in this way, the number of edges originating at $j = 0$ and $j = 1728$ agrees with the multiplicity of the zeroes in the *modular polynomials*. In Example 5.6 we will be able to see how the edges look at $j = 0$ and $j = 1728$ in the isogeny graph $G(59, 2)$.

**Example 5.6.** We will construct the supersingular isogeny graph $G(59, 2)$. Silverman shows in [5, Theorem V.4.1(c)] that the number of isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$ equals

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

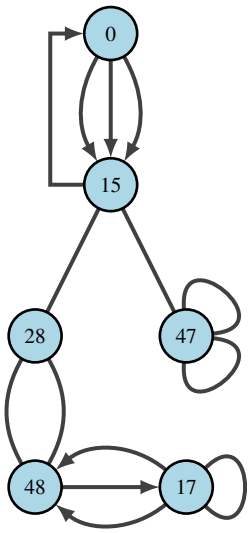
Therefore we expect 6 isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_{59}$. Using Magma (the code can be found in the Appendix), we can determine that the isomorphism classes can be represented by the following $j$-invariants:

$$\{0, 15, 17, 28, 47, 48\},$$

where $1728 \bmod 59 \equiv 17$ and $54000 \bmod 59 \equiv 15$ and $66^3 \bmod 59 \equiv 48$, these numbers are interesting because from Remark 5.4 we know that they have edges with $j = 0$ and $j = 1728$. Using the modular polynomial $\Phi_2(j_1, j_2)$ in Magma, we can determine whether there exists a degree 2 isogeny between the $j$-invariants $j_1$ and $j_2$. We find the following:

$$\begin{aligned} j = 0 \quad & 2 - \text{isogenous to } j = 15; \\ j = 15 \quad & 2 - \text{isogenous to } j = 0, 28, 47; \\ j = 17 \quad & 2 - \text{isogenous to } j = 17, 48; \\ j = 28 \quad & 2 - \text{isogenous to } j = 15, 48; \\ j = 47 \quad & 2 - \text{isogenous to } j = 15, 47; \\ j = 48 \quad & 2 - \text{isogenous to } j = 17, 28. \end{aligned}$$

Using our knowledge about the edges at $j = 0$ and $j = 1728$ from Remark 5.4 and the fact that the rest of the graph is 3-regular, we construct the following graph for $G(59, 2)$:




**Lemma 5.7.** *Let $E/k$ be an elliptic curve over a finite field, where* $\text{char}(k) = p$. *Let $\ell \neq p$ be a prime, then there are $\ell + 1$ subgroups of order $\ell$ in $E[\ell]$.*

*Proof.* Since $\ell$ is a prime not equal to $p$, by Proposition 2.18 we know that $E[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^2$. All elements in $E[\ell]$ have order $\ell$, except for 0, hence there are $\ell^2 - 1$ elements that generate subgroups of order $\ell$. However if $(x, y)$ generates a subgroup of order $\ell$, then all elements in this subgroup, except for the zero element, generate the same subgroup of order $\ell$. Hence for every subgroup of order $\ell$ there are $\ell - 1$ elements that generate the same subgroup. Therefore there are $\frac{\ell^2-1}{\ell-1} = \ell + 1$ subgroups of order $\ell$ in $E[\ell]$. □

**Lemma 5.8.** *The vertices of a supersingular isogeny graph $G(p, \ell)$ can be viewed as the subgroups $H$ of order $\ell$ of the group of points on some supersingular elliptic curve $E$ over a field of characteristic $p$.*

*Proof.* Note that by Theorem 2.30, all supersingular elliptic curves $E$ over a field of characteristic $p$ have $j(E) \in \mathbb{F}_{p^2}$. Generally, the vertices of an isogeny graph are labeled with the corresponding $j$-invariants. Let $j_1$ be one of the $j$-invariants occurring in the vertex set. Pick $E_1$ such that $j(E_1) = j_1$ and choose a subgroup $H_1$ of $E_1$ of order $\ell$. We can pick such a subgroup because Lemma 5.7 tells us that there are $\ell + 1$ of them. We connect the vertices $j_1$ and $j_2$, where $j_2 := j(E_2)$,

with $E_2 = E_1/H_1$. Hence we consider the edge set to consist of $E/H$, where $E$ is a supersingular elliptic curve and where $H$ is a subgroup of $E$ of order $\ell$. This characterization of the edge set $E$ of $G(p,\ell)$ is equivalent to the characterization in the definition because of the following. First note that $E_1/H_1$ indeed is a supersingular elliptic curve by Theorem 2.29. Given an elliptic curve $E_1$ and a subgroup $H_1$, by Theorem 2.19 there is a unique (up to isomorphism) elliptic curve $E_2$ and a unique separable isogeny $\phi$, such that $\phi : E_1 \to E_2$ and $\ker(\phi) = H_1$. Now suppose that we have such a separable isogeny $\phi : E_1 \to E_1/H_1$ where $H_1$ is a subgroup of order $\ell$. This is an isogeny of degree $\ell$, since $\deg(\phi) = \deg_s(\phi) = \#\ker(\phi) = \ell$. For the implication the other way; suppose that $\phi : E_1 \to E_2$ is an isogeny of degree $\ell$. Then $\ell = \deg(\phi) = p^n \cdot \deg_s(\phi)$ by Theorem 2.15. Moreover, $\ell \neq p$ gives that $\ell = \deg_s(\phi) = \#\ker(\phi)$. Also, $\ker(\phi)$ is a subgroup of $E_1$, therefore we have $\phi : E_1 \to E_1/\ker(\phi)$ and $\ker(\phi)$ has order $\ell$. This shows that every isogeny of degree $\ell$ can be written as a separable isogeny from a curve $E$ to $E/H$, where $H$ is a subgroup of order $\ell$ and vice versa. □

## 5.3 Supersingular isogeny graphs are Ramanujan

Lemma 5.8 and Lemma 5.7 together show that supersingular isogeny graphs $G(p,\ell)$ are $\ell + 1$-regular. In this section we will prove even more characteristics of supersingular isogeny graphs; we will prove (part of) the following theorem:

**Theorem 5.9.** *The supersingular isogeny graph $G(p,\ell)$ is $(\ell+1)$-regular, connected and Ramanujan.*

This theorem gives another reason why supersingular isogeny graphs are useful for cryptographic protocols. As mentioned in Section 3, Ramanujan graphs are "optimal" expander graphs, and expander graphs have the property that random walks of certain minimal length on the graph terminate on any vertex with probability close to uniform. Generally this would make it hard for an adversary to distinguish the random walk from a uniformly sampled element.

The main goal of this section will be to give an outline of the proof of the statement in Theorem 5.9. To this end, we will first see how we can use the endomorphism ring of supersingular elliptic curves to gain information about the vertices and edges of a supersingular isogeny graph (from now on to be called isogeny graph). Also, from now on we will denote the identity element of an elliptic curve $E$ by $0_E$, to avoid confusion with the notation of an order.

### 5.3.1 The endomorphism ring of supersingular isogeny graphs

**Definition 5.10.** Let $\mathbb{A}$ be a quaternion algebra and let $\mathfrak{a} \subset \mathbb{A}$ be an non-trivial ideal. The *left order of* $\mathfrak{a}$ is defined as the ring $\mathcal{O}(\mathfrak{a}) := \{x \in \mathbb{A} \mid x\mathfrak{a} \subset \mathfrak{a}\}$.
Let $\mathcal{O}$ be an order in a quaternion algebra $\mathbb{A}$. We say that $\mathfrak{a}$ is a *left $\mathcal{O}$-ideal* if $\mathcal{O} \subset \mathcal{O}(\mathfrak{a})$.

**Definition 5.11.** Let $E$ be an elliptic curve defined over some finite field $\mathbb{F}_q$ of characteristic $p$. Let $\mathfrak{a} \subset \mathcal{O}$ be an ideal. Then the $\mathfrak{a}$-*torsion group* of $E$ is defined as follows

$$E[\mathfrak{a}] := \{P \in E(\overline{\mathbb{F}_q}) \mid \sigma(P) = 0_E \ \forall \sigma \in \mathfrak{a}\}.$$

Note that the group $E[\mathfrak{a}]$ can also be described as the intersection of the kernels of all elements in $\mathfrak{a}$, i.e. $E[\mathfrak{a}] = \bigcap\{\ker(\alpha) \ : \ \alpha \in \mathfrak{a}\}$.

**Definition 5.12.** The separable isogeny $\phi_\mathfrak{a}$ is defined to be the isogeny with domain $E$ and kernel $E[\mathfrak{a}]$, i.e.

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

We denote the isomorphism class of the image of $\phi_\mathfrak{a}$ by $\mathfrak{a} \cdot E$.

By the third isomorphism theorem, we know that, up to isomorphism, there is a unique isogeny with given kernel and it is clear that there is a unique image curve. By [9, Theorem 3.11] we know that $E/E[\mathfrak{a}] \cong E/E[\mathfrak{b}]$ if and only if $[\mathfrak{a}] = [\mathfrak{b}]$. Therefore the isogeny $\phi_\mathfrak{a}$ is well-defined.

**Definition 5.13.** The *reduced norm* of an ideal $\mathfrak{a}$ in a quaternion algebra $\mathbb{A}$, denoted by $\mathcal{N}(\mathfrak{a})$, is defined as follows

$$\mathcal{N}(\mathfrak{a}) := \gcd(\{\mathcal{N}(\alpha) \ : \ \alpha \in \mathfrak{a}\}),$$

here $\mathcal{N}(\alpha) = \overline{\alpha}\alpha$. In the case where we consider the endomorphism algebra of a supersingular elliptic curve this means that $\mathcal{N}(\alpha) = \widehat{\phi} \circ \phi$, as defined in Section 2.

**Definition 5.14.** Let $E$ be a supersingular elliptic curve over a finite field $\mathbb{F}_q$ with endomorphism ring $\mathcal{O}$ and let $H$ be a subgroup of $E(k)$. We define

$$I(H) := \{\alpha \in \mathcal{O} \ : \ \alpha(P) = 0_E \ \forall P \in H\}.$$

The set $I(H)$ is a left $\mathcal{O}$-ideal which is non-empty since it contains $[\#H]$.

**Lemma 5.15.** *Let $E$ be a supersingular elliptic curve over a finite field $\mathbb{F}_q$ and let $H_1, H_2$ be finite subgroups of $E(k)$ such that $H_1 \subset H_2$ and $I(H_1) = I(H_2)$. Then $H_1 = H_2$.*

*Proof.* For the proof we refer to [8, Lemma 42.2.15] □

**Lemma 5.16.** *Let $E$ be a supersingular elliptic curve over a finite field $\mathbb{F}_q$ and let $\mathfrak{a}$ be an $\mathcal{O}$-ideal. Then*

$$I(E[\mathfrak{a}]) = \mathfrak{a}.$$

*Proof.* For the proof we refer to [8, Proposition 42.2.16]. □

**Theorem 5.17.** *Let $E$ be a supersingular elliptic curve over a finite field $k$ and let $\mathcal{O} = \mathrm{End}(E)$. Then every subgroup of $E(k)$ is of the form $E[\mathfrak{a}]$, for some left $\mathcal{O}$-ideal $\mathfrak{a}$. The rank of $E[\mathfrak{a}]$ equals the reduced norm $\mathcal{N}(\mathfrak{a})$.*

*Proof.* We will give the outline of the proof of the fact that every subgroup of $E(k)$ is of the form $E[\mathfrak{a}]$ for some left $\mathcal{O}$-ideal $\mathfrak{a}$. Suppose that we have some subgroup $H$ of $E(k)$, in particular $H$ is finite since $k$ is a finite field. We define $\mathfrak{a} := I(H)$, then it is clear that $H \subset E[\mathfrak{a}]$. Also $I(H) = \mathfrak{a} = I(E[\mathfrak{a}])$, where the second equality follows from Lemma 5.16. Now using Lemma 5.15 we can conclude that $H = E[\mathfrak{a}]$. Hence every subgroup of $E(k)$ is of the form $E[\mathfrak{a}]$ for some left $\mathcal{O}$-ideal $\mathfrak{a}$.
For the rest of the proof we refer to [9, Theorem 3.15].

□

**Lemma 5.18.** *The degree of $\phi_\mathfrak{a}$ equals the reduced norm of the ideal $\mathfrak{a}$ it is associated to, i.e.*

$$\deg(\phi_\mathfrak{a}) = \mathcal{N}(\mathfrak{a}).$$

*Proof.* The isogeny $\phi_\mathfrak{a}$ is separable, hence its degree equals the number of elements in its kernel. The kernel, $\ker(\phi_\mathfrak{a}) = E[\mathfrak{a}]$, has rank equal to $\mathcal{N}(\mathfrak{a})$ by Theorem 5.17. We conclude that $\deg(\phi_\mathfrak{a}) = \mathcal{N}(\mathfrak{a})$. □

**Remark 5.19.** We already showed that the $j$-invariants in the isogeny graph $G(p, \ell)$ could be viewed as the isomorphism classes of $E/H$, where $H$ is a subgroup of a supersingular elliptic curve $E$ with $\ell$ elements. The results above show that every such subgroup $H$ is of the form $E[\mathfrak{a}]$ for a left $\mathcal{O}$-ideal $\mathfrak{a}$ where $E[\mathfrak{a}]$ has rank $\ell$. By Theorem 5.17, this rank equals the reduced norm of $\mathfrak{a}$, which in turn equals the degree of $\phi_\mathfrak{a}$ by Lemma 5.18, showing that the isogeny corresponding to $E \to E/H$, denote by $\phi_\mathfrak{a}$, indeed has degree $\ell$. Vice versa, any $E[\mathfrak{a}]$ for a left $\mathcal{O}$-ideal $\mathfrak{a}$ of reduced norm $\ell$, is a finite subgroup of $E$, since it equals the intersection of the kernels of the elements in $\mathfrak{a}$. Moreover, this subgroup has rank $\ell$ since it equals $\mathcal{N}(\mathfrak{a}) = \ell$.

Therefore $j$-invariants can be viewed as $E/E[\mathfrak{a}]$ for a supersingular elliptic curve $E$ and some left $\mathcal{O}$-ideal of reduced norm $\ell$, where $\mathcal{O} = \mathrm{End}(E)$. So, the isomorphism class (as $\mathcal{O}$-modules) of every left $\mathcal{O}$-ideal $\mathfrak{a}$ of reduced norm $\ell$ corresponds to a vertex. This gives a useful relation between the vertices and edges of an isogeny graph and (the ideals of) the endomorphism ring $\mathcal{O}$.

**Theorem 5.20.** *Let $\phi_\mathfrak{a}$ be as above and define $E_\mathfrak{a} := E/E[\mathfrak{a}]$. Then the pullback map*

$$\begin{aligned}\phi_\mathfrak{a}^* : \mathrm{Hom}(E_\mathfrak{a}, E) &\to \mathfrak{a} \\ \psi &\mapsto \psi\phi_\mathfrak{a}\end{aligned}$$

*defines an isomorphism of left $\mathcal{O}$-modules.*

*Proof.* For the proof we refer to [8, Theorem 42.2.8]. □

Theorem 5.20 says that every left $\mathcal{O}$-ideal $\mathfrak{a}$ is of the form $\mathrm{Hom}(E_\mathfrak{a}, E)\phi_\mathfrak{a}$. In other words, every element $\alpha \in \mathfrak{a}$ corresponds to an element $\psi \circ \phi_\mathfrak{a}$, where $\psi \in \mathrm{Hom}(E_\mathfrak{a}, E)$.

**Corollary 5.21.** *Let $\psi \in \mathrm{Hom}(E_\mathfrak{a}, E)$ and denote by $\alpha$ the image under $\phi_\mathfrak{a}^*$ of $\psi$ in $\mathfrak{a}$. Then*

$$\deg(\psi) = \mathcal{N}(\alpha)/\mathcal{N}(\mathfrak{a}).$$

*Proof.* Since $\phi_\mathfrak{a}^*(\psi) = \alpha$, we have that $\alpha = \psi \circ \phi_\mathfrak{a}$. Taking the norm of $\alpha$ we obtain

$$\mathcal{N}(\alpha) = \deg(\psi) \cdot \deg(\phi_\mathfrak{a}).$$

Using Lemma 5.18 we obtain the desired result. □

Theorem 5.20 gives a way to relate isogenies that have image $E$ to left $\mathcal{O}$-ideals. More generally, it is possible to relate isogenies between any two elliptic curves to the set of ideals of the form $\mathfrak{b}^{-1}\mathfrak{a}$, using the following theorem.

**Theorem 5.22.** *Let $\mathfrak{a}, \mathfrak{b} \subset \mathcal{O}$ be two nonzero left $\mathcal{O}$-ideals. Then there is a bijection*

$$\begin{aligned}\mathrm{Hom}(E_\mathfrak{a}, E_\mathfrak{b}) &\to \mathfrak{b}^{-1}\mathfrak{a} \\ \psi &\mapsto \phi_\mathfrak{b}^{-1} \circ \psi \circ \phi_\mathfrak{a}.\end{aligned}$$

*Proof.* For the proof we refer to [8, Lemma 42.2.22] □

**Corollary 5.23.** *Let $\psi \in \mathrm{Hom}(E_\mathfrak{a}, E_\mathfrak{b})$ and denote by $\alpha$ the element in $\mathfrak{b}^{-1}\mathfrak{a}$ that $\psi$ corresponds to. Then*

$$\deg(\psi) = \mathcal{N}(\alpha) \cdot \frac{\mathcal{N}(\mathfrak{b})}{\mathcal{N}(\mathfrak{a})}.$$

*Proof.* The endomorphism $\psi$ corresponds to an element $\alpha$ of the form $\alpha = \phi_\mathfrak{b}^{-1} \circ \psi \circ \phi_\mathfrak{a}$. Therefore

$$\mathcal{N}(\alpha) = \deg(\phi_\mathfrak{a}) / \deg(\phi_\mathfrak{b}) \cdot \deg(\psi).$$

By Lemma 5.18 we have that $\phi_\mathfrak{a} = \mathcal{N}(\mathfrak{a})$ and $\phi_\mathfrak{b} = \mathcal{N}(\mathfrak{b})$. Rewriting the above gives

$$\deg(\psi) = \mathcal{N}(\alpha) \cdot \frac{\mathcal{N}(\mathfrak{b})}{\mathcal{N}(\mathfrak{a})}.$$

□

**Theorem 5.24.** *Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals of $\mathcal{O}$. Then $E/E[\mathfrak{a}] \cong E/E[\mathfrak{b}]$ if and only if $\mathfrak{a}$ and $\mathfrak{b}$ are isomorphic as $\mathcal{O}$-modules if and only if $\mathfrak{a} = \mathfrak{b}\lambda$ for some invertible $\lambda \in \mathcal{O}$. We say $\mathfrak{a} \sim \mathfrak{b}$, i.e. the ideals are equivalent, if such a $\lambda$ exists.*

*Proof.* For the proof we refer to [9, Theorem 3.11] and [9, Theorem 3.15]. □

The next theorem is a consequence of (amongst others) the above statements and says something more about the connection between an isogeny graph and the endomorphism ring of a supersingular elliptic curve.

**Theorem 5.25** (Deuring correpondence)**.** *Let $E_0$ be a supersingular elliptic curve over a finite field $\mathbb{F}_q$ with endomorphism ring $\mathrm{End}(E_0) \cong \mathcal{O}_0$. There is a bijection between isomorphism classes of supersingular elliptic curves over $\mathbb{F}_q$ and the left class set $\mathrm{Cl}_L(\mathcal{O}_0)$. Under this bijection, if $E \mapsto I$, then $\mathrm{End}(E) \cong \mathcal{O}_R(I)$ and $\mathrm{Aut}(E) \cong \mathcal{O}_R(I)^\times$.*

*Proof.* The theorem is stated in [14, p. 25]. The proof uses the results from Theorem 5.20 and Theorem 5.22. For the full proof we refer to [8, p.778]. □

### 5.3.2 Proving supersingular isogeny graphs are Ramanujan

In this section we will introduce a theorem by Pizer that shows that supersingular isogeny graphs are Ramanujan. We will first discuss some necessary definitions and notation before we state Pizer's theorem.

**Definition 5.26.** Let $\mathbb{A}$ be the quaternion algebra over $\mathbb{Q}_p$, where $p$ is an odd prime. An order $\mathcal{O}$ of $\mathbb{A}$ is said to *level* $p^2$ if $\mathcal{O}$ is isomorphic over $\mathbb{Z}_p$ to the order

$$\left\{ \begin{pmatrix} \alpha & \beta \\ u\beta^\sigma & \alpha^\sigma \end{pmatrix} \ : \ \alpha \in \mathbb{Z}_p + \mathbb{Z}_p \sqrt{p}, \beta \in (\sqrt{p}) \right\},$$

where $u$ is a quadratic non-residue modulo $p$ and $\sigma$ denotes conjugation of $\mathbb{Q}_p(\sqrt{p})/\mathbb{Q}_p$.

**Definition 5.27.** Let $p$ be a prime, let $M$ be a positive integer and let $B_{p,\infty}$ be the unique (up to isomorphism) quaternion algebra over $\mathbb{Q}$ ramified only at $p$ and $\infty$. When $\mathcal{O}$ is an order in $B_{p,\infty}$ and $\ell$ is a prime we define $\mathcal{O}_\ell = \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ and $(B_{p,\infty})_\ell = B_{p,\infty} \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$.
An order $\mathcal{O}$ in $B_{p,\infty}$ is said to have *level* $p^2M$ if

(i) $\mathcal{O}_p$ is an order of level $p^2$ in $(B_{p,\infty})_p$;

(ii) $\mathcal{O}_\ell$ is isomorphic over $\mathbb{Z}_\ell$ to $\begin{pmatrix} \mathbb{Z}_\ell & \mathbb{Z}_\ell \\ M\mathbb{Z}_\ell & \mathbb{Z}_\ell \end{pmatrix}$ for all primes $\ell \neq p$.

If we have representatives of the distinct left $\mathcal{O}$-ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_H$, then all right orders of the $\mathfrak{a}_i$

$$\{x \in B_{p,\infty} \ : \ x\mathfrak{a}_i \subset \mathfrak{a}_i\}$$

are orders of level $p^2M$.

We write $\mathfrak{a}_1, \ldots, \mathfrak{a}_H$ for the distinct left $\mathcal{O}$-ideal classes. Here $H$ is the class number of $\mathcal{O}$. It is given by

$$H = \frac{p^2 - 1}{12} M \prod_{q|M} (1 + 1/q),$$

where $q$ is prime. Both the fact that the distinct left $\mathcal{O}$-ideal classes have level $p^2M$ and the equation above come from [20, p. 187]. In Pizer's theorem we will consider graphs with adjacency matrices that are *Brandt matrices*. Brandt matrices are defined as follows.

**Definition 5.28.** Let $M$ be a positive integer coprime to $p$ and let $\mathcal{O}$ be an order of level $p^2M$ in a quaternion algebra over $\mathbb{Q}$ ramified at $p$ and infinity. Again, we write $\mathfrak{a}_1, \ldots, \mathfrak{a}_H$ for the distinct left $\mathcal{O}$-ideal classes. The *Brandt matrix* is denoted by $\mathcal{B}(p^2, M; \ell)$ or $\mathcal{B}(\ell)$, where $\ell$ is coprime to $p$. Its entries $b_{ij}(\ell)$ are defined as follows. Consider the two left $\mathcal{O}$-ideals $\mathfrak{a}_i$ and $\mathfrak{a}_j$. Let $e_j$ denote the number of units in the right order of $\mathfrak{a}_j$, i.e. in $\mathcal{O}(\mathfrak{a}_j)$. Then $b_{ij}(\ell)$ equals $e_j^{-1}$ times the number of elements $\alpha \in \mathfrak{a}_j^{-1}\mathfrak{a}_i$ with $\mathcal{N}(\alpha) = \ell\mathcal{N}(\mathfrak{a}_i)/\mathcal{N}(\mathfrak{a}_j)$, here $\mathcal{N}(\cdot)$ denotes the reduced

norm. In other words, the $ij$th entry of the Brandt matrix denotes the number of elements with which one can go from $\mathfrak{a}_j$ to $\mathfrak{a}_i$ up to units, with normalized reduced norm $\ell$.

We will show that the adjacency matrix of an isogeny graph is a Brandt matrix in order to apply Pizer's Theorem 5.30.

**Theorem 5.29.** *Let $G(p,\ell)$ be a supersingular isogeny graph. The adjacency matrix of $G(p,\ell)$ is $\mathcal{B}(\ell)$.*

*Proof.* We know by Theorem 5.25 that there is a one-to-one correspondence between the class group $\mathrm{Cl}(\mathcal{O})$ and the isomorphism classes of supersingular elliptic curves sending a representative $\mathfrak{a}_i$ to $\mathfrak{a}_i \cdot E$, such that $\mathrm{End}(\mathfrak{a}_i \cdot E) \cong \mathcal{O}(\mathfrak{a}_i)$. We write $E_i$ for $E_{\mathfrak{a}_i}$, by [21, p. 124] we know that there is an isomorphism as left $\mathrm{End}(E_i)$ and as right $\mathrm{End}(E_j)$ modules: $\mathrm{Hom}(E_j, E_i) \cong \mathfrak{a}_j^{-1}\mathfrak{a}_i$, Theorem 5.22 illustrates the map. In other words: there is a one-to-one correspondence between isogenies $E_j \to E_i$ and elements in the ideal $\mathfrak{a}_j^{-1}\mathfrak{a}_i$. If $\alpha$ is a nonzero element in $\mathfrak{a}_j^{-1}\mathfrak{a}_i$, it is sent by the isomorphism to some isogeny $\phi_\alpha$ in $\mathrm{Hom}(E_j, E_i)$. The degree of $\phi_\alpha$ is given by $\deg(\phi_\alpha) = \frac{N(\alpha)}{N(\mathfrak{a}_i)/N(\mathfrak{a}_j)}$ by Corollary 5.23. By the definition of a Brandt matrix the $\alpha \in \mathfrak{a}_j^{-1}\mathfrak{a}_i$ that contribute to the Brandt matrix have $\frac{N(\alpha)}{N(\mathfrak{a}_i)/N(\mathfrak{a}_j)}) = \ell$, therefore the corresponding isogeny $\phi_\alpha : E_j \to E_i$ has degree $\ell$. The same reasoning holds the other way around, therefore the Brandt matrix $\mathcal{B}(\ell)$ as defined above equals the adjacency matrix of $G(p,\ell)$.
We have skipped one detail, since we have not yet explained what it means to divide by the units in $\mathfrak{a}_j$ in the endomorphism ring. The units in $\mathfrak{a}_j$ have norm 1 and therefore they correspond to elements in the endomorphism ring of degree 1, i.e. they correspond to the isomorphisms. In the supersingular isogeny graph, we defined two isogenies $\phi$ and $\phi'$ to be equivalent if there exists an automorphism $\alpha$ such that $\alpha\phi = \phi'$. Therefore in order to count the isogenies properly we have to divide by the number of isomorphisms in the endomorphism ring of the target curve. □

**Theorem 5.30** (Pizer)**.** *Let $\mathcal{O}$ be an order of level $N = p^2M$ in a quaternion algebra $\mathbb{A}$, ramified at $p$ and at infinity, with class number*

$$H = \left(\frac{p^2-1}{12}\right) M \prod_{q|M}(1 + 1/q),$$

*here the $q$ are primes. Let $\ell$ be a prime with $\ell < p/4$ and $\ell \nmid N$. Then the associated multigraph $G(\ell) = G(p^2, M; \ell)$ that has adjacency matrix $\mathcal{B}(\ell)$, is defined and is an $\ell + 1$-regular connected Ramanujan graph.*

*Proof.* For the proof we refer to [22, p. 131]. □

Theorem 5.29 shows that supersingular isogeny graphs have an adjacency matrix that is a Brandt matrix, therefore Theorem 5.30 implies that supersingular isogeny graphs are $\ell + 1$-regular connected Ramanujan graphs.

# 6 Supersingular elliptic curves in cryptography

As mentioned before, supersingular elliptic curves are interesting objects for cryptography. In this chapter we will see some applications of them in cryptography. We will start with some prerequisites. After that we will look at a key exchange protocol called Supersingular Isogeny Diffie-Hellman (SIDH), identification protocols and a signature scheme called SQISign. Many definitions in this section come from [23].

## 6.1 Prerequisites

In this section we will discuss some prerequisites for understanding the upcoming cryptographic protocol.

**Definition 6.1** (Negligible function)**.** We say $\mu : \mathbb{N} \to \mathbb{R}$ is a *negligible function* if for every positive polynomial $f$ there exists a number $N > 0$ such that for all $\lambda > N$:

$$|\mu(\lambda)| < \frac{1}{f(\lambda)}.$$

Intuitively, this means that a negligible function goes to zero faster than any polynomial goes to zero.

**Theorem 6.2.** *Suppose we have a supersingular elliptic curve $E$ over some finite field $\mathbb{F}_{p^2}$ where $p$ is a prime of the form $p = \ell_1^{e_1} \cdot \ell_2^{e_2} \cdot f \pm 1$, where $\ell_1$ and $\ell_2$ are distinct (small) primes and $f$ is some integer cofactor. We choose $E$ such that $E[\ell_i^{e_i}]$ consists only of $\mathbb{F}_{p^2}$-rational points. Let $\langle P_1, Q_1 \rangle$ be a basis for $E[\ell_1^{e_1}]$ and let $\langle P_2, Q_2 \rangle$ be a basis for $E[\ell_2^{e_2}]$. Let $m, n, m', n'$ be integers and let $K := [m]P_1 + [n]Q_1$ and $K' := [m']P_2 + [n']Q_2$. Define $\phi : E \to E/\langle K \rangle$ and $\phi' : E \to E/\langle K' \rangle$ to be the unique (separable) isogenies with kernel $\langle K \rangle$ and $\langle K' \rangle$ respectively. We define $P_1' := \phi'(P_1)$, $Q_1' := \phi'(Q_1)$, $P_2' := \phi(P_2)$ and $Q_2' := \phi(Q_2)$. We define $\psi, \psi'$ to be isogenies such that*

$$\psi : E/\langle K' \rangle \to (E/\langle K' \rangle)/\langle [m]P_1' + [n]Q_1' \rangle =: E_1$$

*and*

$$\psi' : E/\langle K \rangle \to (E/\langle K \rangle)/\langle [m']P_2' + [n']Q_2' \rangle =: E_2.$$

*Then*

$$E_1 \cong E_2.$$

*Proof.* First note that since $\phi$ and $\phi'$ are isogenies,

$$[m]\phi'(P_1) + [n]\phi'(Q_1) = \phi'([m]P_1 + [n]Q_1) = \phi'(K)$$

and that

$$[m']\phi(P_2) + [n']\phi(Q_2) = \phi([m']P_2 + [n']Q_2) = \phi(K').$$

Note that the curve $E_1 \cong (\psi \circ \phi')(E)$ and similarly that $E_2 \cong (\psi' \circ \phi)(E)$, since isogenies are surjective. Therefore we have that

$$\ker(\psi' \circ \phi) = \langle K, K' \rangle \quad \text{and} \quad \ker(\psi \circ \phi') = \langle K, K' \rangle.$$

Therefore we have two isogenies with domain $E$ that have the same kernel. By the third isomorphism theorem this implies that

$$E_1 \cong E/\ker(\psi \circ \phi') \cong E/\ker(\psi' \circ \phi) \cong E_2,$$

again using the fact that isogenies are surjective. Therefore the curves $E_1$ and $E_2$ are isomorphic (and the isogenies differ only by an automorphism). □

Generally, the cofactor $f$ can (and will) be chosen to be 1. If we would want to have a larger set of useable primes $p$ for the protocol, we could take another value for $f$. We will see in the next section why we choose a prime $p$ of the form $\ell_1^{e_1} \cdot \ell_2^{e_2} \cdot f \pm 1$.

## 6.2 Supersingular Isogeny Diffie-Hellman (SIDH)

In this section we describe the supersingular isogeny Diffie-Hellman protocol (SIDH), which is a key exchange protocol that resembles the Diffie-Hellman key exchange protocol. SIDH is used in SIKE (which stands for supersingular isogeny key encapsulation). SIKE basically applies a transformation to SIDH that allows its users to reuse the same (private) secret key. It was submitted to the NIST standardization process on post-quantum cryptography and is currently one of the final contenders.

We start by setting the public parameters. Alice and Bob agree on a prime $p = \ell_1^{e_1} \cdot \ell_2^{e_2} \cdot f \pm 1$ where $\ell_1$ and $\ell_2$ are small primes (often $\ell_1 = 2$ and $\ell_2 = 3$) such that $\ell_1^{e_1} \approx \ell_2^{e_2}$ and $f$ is some integer cofactor. As mentioned, the cofactor is introduced to make the set of primes that can be chosen larger, however in practice it is (as far as is known at this moment) sufficient to choose $f = 1$. They also fix a supersingular elliptic curve $E$ over $\mathbb{F}_{p^2}$ such that

$$E(\mathbb{F}_{p^2}) \cong (\mathbb{Z}/\ell_1^{e_1}\mathbb{Z})^2 \oplus (\mathbb{Z}/\ell_2^{e_2}\mathbb{Z})^2 \oplus (\mathbb{Z}/f\mathbb{Z})^2.$$

They also agree on bases $\langle P_1, Q_1 \rangle$ for $E[\ell_1^{e_1}]$ and $\langle P_2, Q_2 \rangle$ for $E[\ell_2^{e_2}]$.

The secrets are the following. Alice chooses integers $m_A, n_A$ and Bob chooses integers $m_B, n_B$. These integers are Alice' and Bob's private secret keys. Subsequently, Alice computes $A := \langle [m_A]P_1 + [n_A]Q_1 \rangle$ and Bob computes $B := \langle [m_B]P_2 + [n_B]Q_2 \rangle$. Note that $A \subset E[\ell_1^{e_1}]$ and that $B \subset E[\ell_2^{e_2}]$. Alice and Bob now have secret isogenies, $\phi_A$ and $\phi_B$ respectively, such that

$$\phi_A : E \to E/A$$
$$\phi_B : E \to E/B.$$

They can compute the isogenies and the target curves using Vélu's formulas. Alice publishes $E_A := E/A$ and Bob publishes $E_B := E/B$.

Alice and Bob need some more information from each other to get to the same curve. Alice computes $P_2' := \phi_A(P_2)$ and $Q_2' := \phi_A(Q_2)$ and Bob computes $P_1' := \phi_B(P_1)$ and $Q_1' := \phi_B(Q_1)$ and they both publish their results. Alice will compute $E/\langle [m_a]P_1' + [n_A]Q_1' \rangle$ and Bob will compute $E/\langle [m_B]P_2' + [n_B]Q_2' \rangle$. Because of Theorem 6.2 these two curves are isomorphic, so Alice and Bob have arrived at the same vertex, which will be their shared secret key.

How do Alice and Bob choose a curve $E$ such that $E(\mathbb{F}_{p^2}) \cong (\mathbb{Z}/\ell_1^{e_1}\mathbb{Z})^2 \oplus (\mathbb{Z}/\ell_2^{e_2}\mathbb{Z})^2 \oplus (\mathbb{Z}/f\mathbb{Z})^2$? From [18, p.5] we know that every supersingular elliptic curve is isomorphic to a supersingular elliptic curve $E$ for which the trace of the Frobenius map $\pi_E$ satisfies $\pi_E = -2p$. The explicit representatives for such an elliptic curve are also given in [18]. Using [5, Theorem 2.3.1], we know that

$$\#E(\mathbb{F}_{p^2}) = p^2 + 1 - \mathrm{tr}(\pi_E).$$

If we chose $E$ such that $\pi_E = -2p$, we have $\#E(\mathbb{F}_{p^2}) = (p+1)^2$. Combining this with Proposition 2.18, we obtain

$$E(\mathbb{F}_{p^2}) \cong (\mathbb{Z}/(p+1)\mathbb{Z}) \oplus (\mathbb{Z}/(p+1)\mathbb{Z})$$

Choosing $p = \ell_1^{e_1} \cdot \ell_2^{e_2} \cdot f - 1$ gives

$$\begin{aligned} E(\mathbb{F}_{p^2}) &\cong (\mathbb{Z}/(\ell_1^{e_1}\ell_2^{e_2}f)\mathbb{Z}) \oplus (\mathbb{Z}/(\ell_1^{e_1}\ell_2^{e_2}f)\mathbb{Z}) \\ &\cong (\mathbb{Z}/\ell_1^{e_1}\mathbb{Z})^2 \oplus (\mathbb{Z}/\ell_2^{e_2}\mathbb{Z})^2 \oplus (\mathbb{Z}/f\mathbb{Z})^2, \end{aligned}$$

where we use the fact that $\ell_1$, $\ell_2$ and $f$ are coprime.

Supersingular Isogeny Diffie-Hellman (SIDH)

**Public parameters** : Prime $p = \ell_1^{e_1} \cdot \ell_2^{e_2} \cdot f \pm 1$
Supersingular elliptic curve $E/\mathbb{F}_{p^2}$
Basis $\langle P_1, Q_1 \rangle$ for $E[\ell_1^{e_1}]$
Basis $\langle P_2, Q_2 \rangle$ for $E[\ell_2^{e_2}]$

| **Alice** | | **Bob** |
|---|---|---|
| $A := \langle [m_A]P_1 + [n_A]Q_1 \rangle$ | | $B := \langle [m_B]P_2 + [n_B]Q_2 \rangle$ |
| $\phi_A : E \to E/A =: E_A$ | | $\phi_B : E \to E/B =: E_B$ |
| | $\xrightarrow{E_A}$ | |
| | $\xrightarrow{P'_2 := \phi_A(P_2), Q'_2 := \phi_A(Q_2)}$ | |
| | $\xleftarrow{E_B}$ | |
| | $\xleftarrow{P'_1 := \phi_B(P_1), Q'_1 := \phi_B(Q_1)}$ | |
| $A' := \langle [m_A]P'_1 + [n_A]Q'_1 \rangle$ | | $B' := \langle [m_B]P'_2 + [n_B]Q'_2 \rangle$ |
| $E_{AB} = E_B/A'$ | | $E_{BA} = E_A/B'$ |
| **Output** : $j(E_{AB})$ | | **Output** : $j(E_{BA})$ |

Figure 4: An illustration of SIDH

## 6.3 The supersingular $\ell$-isogeny path problem

In this section we introduce the $\ell$-isogeny path problem, which is interesting for the security of some cryptographic protocols based on supersingular isogenies, like the hash function introduced by Charles, Goren and Lauter [1].

**Problem 1** (The supersingular $\ell$-isogeny path problem)**.** Let $p, \ell$ be primes such that $p \neq \ell$. Let $E_0$ and $E_1$ be supersingular elliptic curves over $\mathbb{F}_{p^2}$. Compute an isogeny

$$\phi : E_0 \to E_1,$$

such that $\phi$ has degree $\deg(\phi) = \ell^e$ for some non-zero $e$.

If we can (efficiently) compute such an isogeny $\phi$, it means that we have found a path of length $e$ in the supersingular isogeny graph $G(p, \ell)$ between two vertices. It

turns out to be quite hard to solve this problem efficiently when considering elliptic curves and isogenies. However the Deuring correspondence gives a way to turn this into a problem in the quaternions.

**Problem 2** (The quaternion $\ell$-isogeny path problem)**.** Let $p, \ell$ be primes such that $p \neq \ell$. Let $\mathcal{O}$ be a maximal order in a quaternion algebra $\mathbb{A}$ and let $I$ be a left $\mathcal{O}$-ideal. Find a left $\mathcal{O}$-ideal $J$ such that $J \sim I$ with norm $\ell^e$ for some non-zero $e$.

In [24] a probabilistic algorithm was proposed that can solve the quaternion $\ell$-isogeny path problem efficiently, this algorithm is referred to as the KLPT algorithm. The algorithm uses the Deuring correspondence, i.e., the correspondence between supersingular elliptic curves and their endomorphism rings as mentioned in Theorem 5.25.

In table 6.3 we summarize the Deuring correspondence as discussed in Subsection 5.3.1 and Theorem 5.25. We fix a supersingular elliptic curve $E/\mathbb{F}_{p^2}$ and we write $B_{p,\infty}$ for the (unique) quaternion algebra in which the endomorphism ring is an order. We write $\mathcal{O}_i$ for the order that $\mathrm{End}(E_i)$ is isomorphic to.

Table 1: The Deuring correspondence

| Supersingular $j$-invariants over $\mathbb{F}_{p^2}$ | Maximal orders in $B_{p,\infty}$ |
|---|---|
| $j(E)$ | $\mathcal{O} \cong \mathrm{End}(E)$ |
| $(E_1, \phi)$ with $\phi : E \to E_1$ | $I_\phi$ integral left $\mathcal{O}$-ideal and right $\mathcal{O}_1$-ideal |
| $\alpha \in \mathrm{End}(E)$ | Principal ideal $\mathcal{O}\alpha$ |
| $\deg(\phi)$ | $\mathcal{N}(I_\phi)$ |
| $\phi : E \to E_1$ and $\psi : E \to E_1$ | Equivalent ideals $I_\phi \sim I_\psi$<br>i.e. $I_\phi = \lambda I_\psi$ for some $\lambda$ |
| Supersingular $j$-invariants over $\mathbb{F}_{p^2}$ | $\mathrm{Cl}(\mathcal{O})$ |

## 6.4 Σ-protocols

In this section we define Σ-protocols, following [25]. A Σ-protocol is a 3-move cryptographic protocol between two parties: a so called "Prover" and "Verifier". The idea of such a protocol is that the Prover identifies himself to the Verifier in a way in which they, i.e. the Prover, do not give away too much information. For example, if someone wants to have access to their bank account, they generally need to sign in using their password. However, if some malicious party managed to build a website that looks exactly like that of the bank, logging into this website would mean giving away your password to someone else. Σ-protocols are designed so that the person trying to prove their identity does not have to give away sensitive secret information like a password. The idea of a Σ-protocol is that the Prover shows enough knowledge of its identity, without giving all of it away, so that the Verifier knows with enough certainty that the Prover is who they pretend to be.

In this section we will use the notation $\{0,1\}^*$, which is defined to be the set of arbitrary length bitstrings. In other words, it is the union of all bitstring of length $n$, so $\{0,1\}^* := \bigcup_{n\in\mathbb{N}} \{0,1\}^n$. We will also use the notation $|x|$ for a bitstring $x$, where $|x|$ denotes the length of the bitstring. Finally, as we mentioned before, when we write $c \xleftarrow{\$} C$ that means that an element $c$ is chosen uniformly at random from a set $C$.

**Definition 6.3.** We say an algorithm $A$ runs in *polynomial time*, if there exists a polynomial $p \in \mathbb{N}[x]$ such that for every input $x \in \{0,1\}^*$ the computation of $A(x)$ terminates within at most $p(|x|)$ steps.
An algorithm $A$ running in time $p$ is said to be *probabilistic*, if $A$ on input $x$ additionally has access to at most $p(x)$ 'unbiased random bits' (i.e., equal to 0 with probability 1/2 and equal to 1 with probability 1/2) to be used within the computation. For a *probabilistic polynomial-time algorithm*, we write PPT in short.

We will now define the notion of a Σ-protocol (the name comes from the observation that the communication between the two parties follows the shape of a Σ).

**Definition 6.4** (Σ-protocol)**.** We let $C$ be a set and $R$ be a binary relation $R \subset \{0,1\}^* \times \{0,1\}^*$ such that whenever $(x,w) \in R$, then $|w| \leqslant p(|x|)$, where $p$ is some polynomial. $\Pi$ is a protocol consisting of three moves (a 3-move protocol) between a Prover $P$ and a Verifier $V$, where the Prover and Verifier are PPT algorithms. $P$ gets as input some $(x,w) \in R$ and $V$ only gets $x$. The protocol $\Pi$ is a Σ-protocol with challenge space $C$ if

- $P$ sends a message $a$ to $V$

- $V$ sends back a random $\lambda$-bitstring $c \xleftarrow{\$} C$ to $P$
- $P$ responds by sending some $z$ to $V$.

Additionally, when the communication has ended, the Verifier outputs a bit $b \in \{0,1\}$, where 0 corresponds to "reject" and 1 corresponds to "accept" by computing a deterministic function with inputs $x, (a,c,z)$. We denote the output of the Verifier by $\langle P,V\rangle(x;w)$ and we denote the protocol transcript by $\Pi(x;w)$. Also, the protocol needs to satisfy the following three conditions

- *Completeness:* For every $(x,w) \in R$, $\Pr[\langle P,V\rangle(x;w) = 1] = 1$.
- *Special soundness:* There exists a polynomial time algorithm $\mathcal{E}$ (also called the *extractor*) such that on input of two accepting transcripts $(a,c,z)$ and $(a,c',z')$ for $x$ with $c \neq c'$, outputs a witness $\tilde{w}$ such that $(x,\tilde{w}) \in R$.
- *Special honest verifier zero-knowledge:* There exists a PPT algorithm $\mathsf{Sim}$ such that on input of $x$, $\mathsf{Sim}$ outputs a transcript $(\tilde{a},\tilde{c},\tilde{z})$ such that the transcript has the same probability distribution as the honest protocol transcript $\Pi(x;w)$.

**Definition 6.5.** We define the language of a relation $R \subset X \times W$ to be

$$L_R := \{x \in X \mid \exists w \in W \ : \ (x,w) \in R\}.$$

**Definition 6.6.** Let $\kappa : \{0,1\}^* \to [0,1]$ be a function. A protocol $(P,V)$ is a *proof of knowledge* for the relation $R$ with *knowledge error* $\kappa$ if the following are satisfied:

- *Completeness:* For every $(x,w) \in R$, $\Pr[\langle P,V\rangle(x;w) = 1] = 1$.
- *Knowledge soundness:* There exists a probabilistic polynomial time algorithm $K$, called the *knowledge extractor*, such that for every Prover $P^*$ and every $x \in L_R$, $K$ satisfies the following condition. Let $\varepsilon(x)$ be the probability that $V$ accepts on input $x$ after interacting with $P^*$. If $\varepsilon(x) > \kappa(x)$, then on input $x$ and (oracle) access to $P^*$, $K$ outputs some $\tilde{w}$ such that $(x,w) \in R$ with probability at least $\varepsilon(|x|) - \kappa(|x|)$.

The "knowledge soundness" property is in fact equivalent to the following: let $K$, $\varepsilon$ and $\kappa$ be as before. There exists a constant $c > 0$ such that if $\varepsilon(x) > \kappa(x)$, then on input $x$ and (oracle) access to $P^*$, $K$ outputs a witness $w$ such that $(x,w) \in R$ within an expected number of steps bounded by

$$\frac{|x|^c}{\varepsilon(x) - \kappa(x)}. \tag{4}$$

One of the nice properties of Σ-protocols is mentioned in the next theorem, which shows that every Σ-protocol is in fact a proof of knowledge (with a certain knowledge error).

**Theorem 6.7.** *Let* $\Pi$ *be a* Σ*-protocol for a relation* $R$ *with challenge length* $\lambda$*. Then* $\Pi$ *is a proof of knowledge with knowledge error* $2^{-\lambda}$*.*

*Proof.* For the proof we refer to [25, Theorem 6.3.2]. □

We will give an example of a Σ-protocol, but in order to understand the requirements of such a protocol better, we will first give some examples of protocols that do not meet the requirements of a Σ-protocol.

**Example 6.8.** We consider the relation $R = \{(h, w) \in G \times \mathbb{Z}_q \mid h = g^w\}$, where $G$ is a cyclic group with generator $g$. Note that the related language $L_R = \{h \in G \mid \exists\, w : (h, w) \in R\}$ equals $G$. The prover gets as input a pair $h, w$, the verifier only knows $h$. The goal of the Prover is to prove knowledge of a witness $w$. We will make some first attempts to construct a Σ-protocol:

- A first naive attempt is to let $a$ and $c$ be arbitrary messages and let $z = w$. This way a verifier can simply compute whether $g^z = h$ holds. However, this is not a Σ-protocol, since the special honest verifier zero-knowledge property is not met, since that would require the algorithm Sim to be able to find a witness for any given $h$. This illustrates the idea of special honest verifier zero-knowledge, which basically says that an honest verifier learns nothing from the protocol transcript, since it could have simulated the transcript in its head without knowledge of the witness.

- A smarter way to go about this is to choose the first message, i.e. $a$, in such a way that the verifier can use it to check whether the prover has knowledge of $w$. Suppose that the prover samples a random $r$ and sets $a = g^r$. Let $z = r + w$ and let the verifier output 1 if and only if $g^z = h \cdot g^r$. This clearly satisfies correctness. However a malicious party is capable of computing $h^{-1} = g^{-w}$, since $h$ is public. It can send $a = g^r h^{-1}$ for some random $r$, to the verifier. The verifier will reply with some $c$ and after that the prover will send $z = r - w + w = r$. The verifier will accept this transcript, even though the prover did not need knowledge of a witness for this transcript. In particular, given two such transcripts there is no information about the witness to be extracted, unless one is capable of finding the discrete logarithm in polynomial time, which is generally assumed to not be possible. This implies that there can not be an extractor and hence the protocol is not special sound.

Often the properties of a Σ-protocol can be proven to be true using some kind of hardness assumption, e.g. assuming that the discrete logarithm problem is hard with respect to some group. We give an example of a Σ-protocol called Schnorr's identification scheme below.

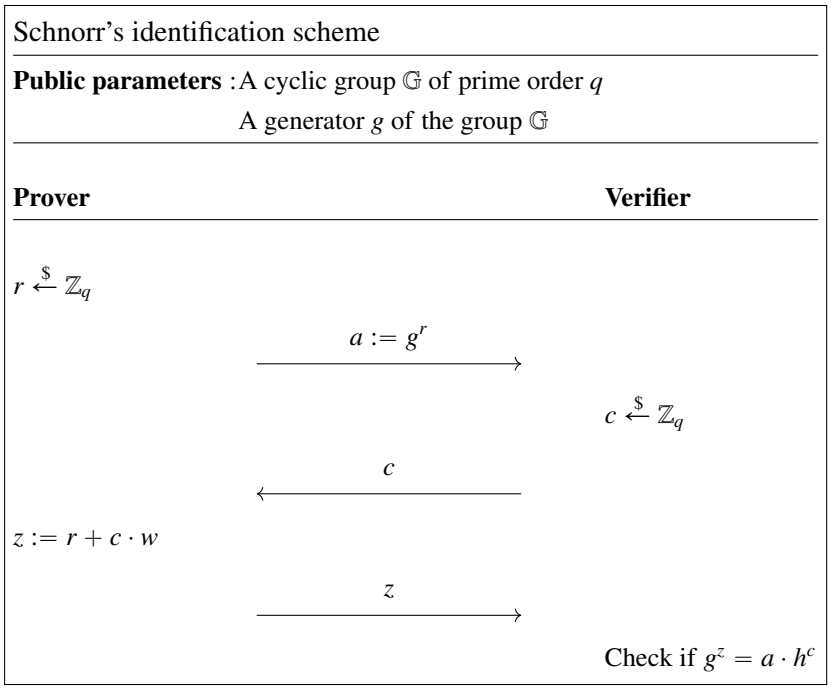



Figure 5: Schnorr's identification scheme

**Theorem 6.9.** *We define R to be the following relation*

$$R := \{(h, w) \in \mathbb{G} \times \mathbb{Z}_q \mid h = g^w\}.$$

*We assume that the discrete logarithm problem is hard with respect to $\mathbb{G}$, i.e. given an element $h \in \mathbb{G}$ it is hard to find $w$ such that $h = g^w$. Then the protocol in Figure 5 is a Σ-protocol for R with challenge space $\mathbb{Z}_q$.*

*Proof.* It is clear that the protocol is a 3-move protocol as described in the definiton of Σ-protocols. We will prove that the protocol satisfies completeness, special soundness and special honest verifier zero-knowledge.

- *Completeness:* We want to show that the verifier always accepts when the prover has the required information and executes the protocol correctly. This

means that the prover, given some $h$, knows a $w$ such that $h = g^w$. The prover has computed $z := r + c \cdot w$, so

$$g^z = g^{r+c\cdot w} = g^r \cdot (g^w)^c = a \cdot h^c.$$

The verifier will always output 1 if this is the case, therefore the verifier will always output 1 when the prover has the required knowledge and follows the protocol, i.e. $\Pr[\langle P, V\rangle(h; w) = 1] = 1$ for all $(h, w) \in R$.

- *Special soundness:* We want to show there exists a polynomial time algorithm $\mathcal{E}$ that, given two transcripts $(a, c, z)$ and $(a, c', z')$ with $c \neq c'$, outputs a witness $\tilde{w}$ such that $(h, \tilde{w}) \in R$. Suppose that we have two such transcripts $(a, c, z)$ and $(a, c', z')$. Then

$$z = r + c \cdot w \quad \text{and} \quad z' = r + c' \cdot w.$$

In particular this means that $(z - z') \cdot (c - c')^{-1} \equiv w \bmod q$. Note that $c - c'$ is invertible since $c \neq c'$ and $q$ is prime. Therefore we can let $\mathcal{E}$ be such that it outputs $\tilde{w} = (z - z') \cdot (c - c')^{-1}$, which can be computed in polynomial time. Then

$$g^{\tilde{w}} \equiv g^w \equiv h,$$

so $\tilde{w}$ is indeed a witness for $h$.

- *Special honest verifier zero-knowledge:* We want a probabilistic polynomial time algorithm $\mathsf{Sim}$ that on input of $h$ can generate some $(\tilde{a}, \tilde{c}, \tilde{z})$ that 'looks like' a protocol transcript, i.e. such that the outputs of $\mathsf{Sim}$ are distributed the same as the outputs of honest protocol executions. The PPT algorithm $\mathsf{Sim}$ operates as follows: on input $h$, $\mathsf{Sim}$ samples $\tilde{z}, \tilde{c} \xleftarrow{\$} \mathbb{Z}_q$ uniformly at random. It then sets $\tilde{a} := g^{\tilde{z}} \cdot h^{-\tilde{c}}$. This makes that $\tilde{a}$ looks like an element from $\mathbb{G}$ that is chosen uniformly at random. Also $\tilde{z}$ is the unique element in $\mathbb{Z}_q$ such that $g^{\tilde{z}} = \tilde{a} \cdot h^{\tilde{c}}$, so the generated transcript will be accepted if and only if $g^{\tilde{z}} = \tilde{a} \cdot h^{\tilde{c}}$, which is exactly what is true for a real protocol transcript as well.

□

## 6.5 Identification protocol and signature scheme based on supersingular isogeny graphs

We will now look at a Σ-protocol and a signature scheme based on supersingular isogeny graphs introduced in [2] by De Feo, Kohel, Leroux, Petit and Wesolowski. The signature scheme is called SQISign (for *Short Quaternion and Isogeny Signature*) and seems to be a quantum-proof signature scheme which also has relatively short public key and signature size.

**Definition 6.10.** Let $R$ be a ring. Let $I$ be a subset of $R$ that is an additive subgroup such that for all $r \in R$ and for all $a \in I$ it holds that $ra \in I$, then we say that $I$ is a *left ideal of* $R$. We can analogously define the notion of *right ideals of* $R$.

**Definition 6.11.** Let $I$ be a subset of a ring $R$, we say that $I$ is a *2-sided ideal of* $R$ if $I$ is both a left $R$-ideal and a right $R$-ideal. If $R$ is a commutative ring, all ideals are 2-sided. The *2-sided class group* is defined analogously to the class group, but is defined instead only using the 2-sided ideals.

**Proposition 6.12.** *Let $\mathcal{O}$ be an order in a quaternion algebra ramified only at $p$ and at $\infty$. Then there exists a unique maximal 2-sided ideal $\mathfrak{P}$ over $p$. Furthermore, $\mathfrak{P}$ is principal if and only if there exists an element $\pi$ in $\mathcal{O}$ such that $\pi^2 = -p$.*

*Proof.* This is stated in [24, Section 2.3]. □

**Proposition 6.13.** *Let $\mathcal{O}$ be as above and let $\mathfrak{P}$ be its unique maximal 2-sided ideal. Then $\mathfrak{P}$ is a generator of the 2-sided class group.*

*Proof.* This is stated in [24, Section 2.3]. □

**Definition 6.14.** Let $R$ be some non-commutative ring. The *$p$-extremal orders* are the orders $\mathcal{O}$ that have an element $\pi$ such that $\pi^2 = -p$. By the above this is equivalent to $\mathcal{O}$ having trivial 2-sided class group.

**Remark 6.15.** By [9, Theorem 4.1.5] we know that for every prime $p$ there exists a supersingular elliptic curve $E$ over $\mathbb{F}_p$ such that its Frobenius endomorphism $\pi$ has $\mathrm{tr}(\pi) = 0$. Therefore $\pi$ satisfies

$$\pi^2 + \deg(\pi) = 0 \quad \text{so} \quad \pi^2 = -p.$$

By the same Theorem in [9], such elliptic curves do not have their full endomorphism ring defined over their field of definition, which in this case is $\mathbb{F}_p$. Also, by [9, Theorem 4.2.3] we have that: if $\mathrm{End}(E) \otimes \mathbb{Q}$ is the endomorphism algebra of a supersingular elliptic curve $E$ for which not all endomorphisms are defined,

then the orders in $\mathrm{End}(E) \otimes \mathbb{Q}$ which are endomorphism rings of elliptic curves in the isogeny class of $E$, are the orders which contain $\pi$ (and are maximal at $p$), so all these elliptic curves have endomorphism rings that are $p$-extremal orders.

**Definition 6.16.** Let $A \subset B$ be a ring extension where $B$ is free of rank $n$ as an $A$-module. We define $M_x : B \to B$ as the multiplication-by-$x$ map, i.e. $M_x(b) = xb$, which is an $A$-linear map. We define

$$\mathrm{Tr}_{B/A}(x) = \mathrm{trace}(M_x).$$

**Definition 6.17.** Let $\mathcal{O}$ be an order in a quaternion algebra of free-rank $n$, having $\mathbb{Z}$-basis $x_1, \ldots, x_n$. Then the discriminant of $\mathcal{O}$ is

$$\mathrm{disc}(\mathcal{O}) = \det(\mathrm{Tr}_{\mathcal{O}/\mathbb{Z}}(x_i x_j))_{i,j=1}^{n}.$$

**Definition 6.18.** Let $\mathcal{O}$ be as in Definition 6.17 and additionally let $\mathcal{O}$ have a distinguished quadratic subring $S$. For a maximal order $\mathcal{O}$, we define

$$\mathrm{d}(\mathcal{O}) := \min\{\mathrm{disc}(S) \ : \ \mathbb{Z} \neq S \subsetneq \mathcal{O}\}.$$

**Definition 6.19.** Let $\mathcal{O}$ be a $p$-extremal maximal order. Among all $p$-extremal maximal orders, we say that $\mathcal{O}$ is a *special $p$-extremal maximal order* if $\mathrm{d}(\mathcal{O})$ is minimal.

**Definition 6.20.** Let $m$ be a natural number and let $B$ be a positive real number. Then $m$ is called *$B$-smooth* if it has no prime divisors larger than $B$. We say $m$ is *smooth* if it is $B$-smooth for sufficiently small $B$.

**Definition 6.21.** Let $\phi : E \to E'$ be an isogeny. We say $\phi$ is a *cyclic isogeny* if $\ker(\phi)$ is a cyclic group, i.e. $\ker(\phi)$ is generated as a group by one element.

**Lemma 6.22.** *Let $E, E'$ be elliptic curves over a finite field $\mathbb{F}_q$. If $\phi : E \to E'$ is a cyclic isogeny of degree $n$ coprime to $q$, then $\widehat{\phi}$ is also a cyclic isogeny.*

*Proof.* Note that $E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ by Theorem 2.18. Therefore in $E/\ker(\phi)$ there is a point of order $n$, because $\phi$ cannot send all points of order $n$ to zero since it is cyclic but $E[n]$ is not. Let $\phi(P)$ be a point of order $n$ in $E' \cong E/\ker(\phi)$ such that $P \notin \ker(\phi)$. Note that

$$\widehat{\phi}(\phi(P)) = [\deg(\phi)]P = nP = 0_E.$$

Therefore $\phi(P)$ is in the kernel of $\widehat{\phi}$ and $\phi(P)$ has order $n = \deg(\widehat{\phi}) = |\ker(\widehat{\phi})|$. Therefore $\phi(P)$ generates the kernel of $\widehat{\phi}$, so $\widehat{\phi}$ is a cyclic isogeny as well. □

## The Σ-protocol in SQISign

**Parameters:** The setup of the scheme is as follows. A prime $p$ is chosen and then a supersingular elliptic curve $E_0$ over $\mathbb{F}_p$ with special extremal endomorphism ring $\mathcal{O}_0$ is chosen. We choose $D_c$ to be an odd smooth number of $\lambda$ bits and $D = 2^e$ where $e$ is above the diameter of the supersingular 2-isogeny graph. The prover wants to prove knowledge of a secret $\tau$.

**Key generation:** The key pair, consisting of a public key and a secret key, is generated as follows. A random isogeny walk starting at $E_0$ is chosen. This isogeny walk is denoted by $\tau$ and ends at some vertex corresponding to an elliptic curve $E_A$. The public key is the curve $E_A$ and the secret key is the isogeny $\tau$, i.e. the key pair is $(\mathsf{pk}, \mathsf{sk}) = (E_A, \tau)$.

**The protocol:**

- First the Prover $P$ picks a random (secret) $\psi : E_0 \to E_1$. It sends $E_1$ to the Verifier $V$.
- The Verifier $V$ picks a cyclic isogeny $\phi : E_1 \to E_2$ of degree $D_c$ and sends a description of $\phi$ to $P$.
- The prover $P$ constructs from $\phi \circ \psi \circ \widehat{\tau} : E_A \to E_2$ some new isogeny $\sigma : E_A \to E_2$ of degree $D$ such that $\widehat{\phi} \circ \sigma$ is cyclic.
- The Verifier $V$ accepts when $\sigma$ is an isogeny from $E_A \to E_2$ of degree $D$ and $\widehat{\phi} \circ \sigma$ is cyclic.

An illustration of the three-move protocol is given on the next page.

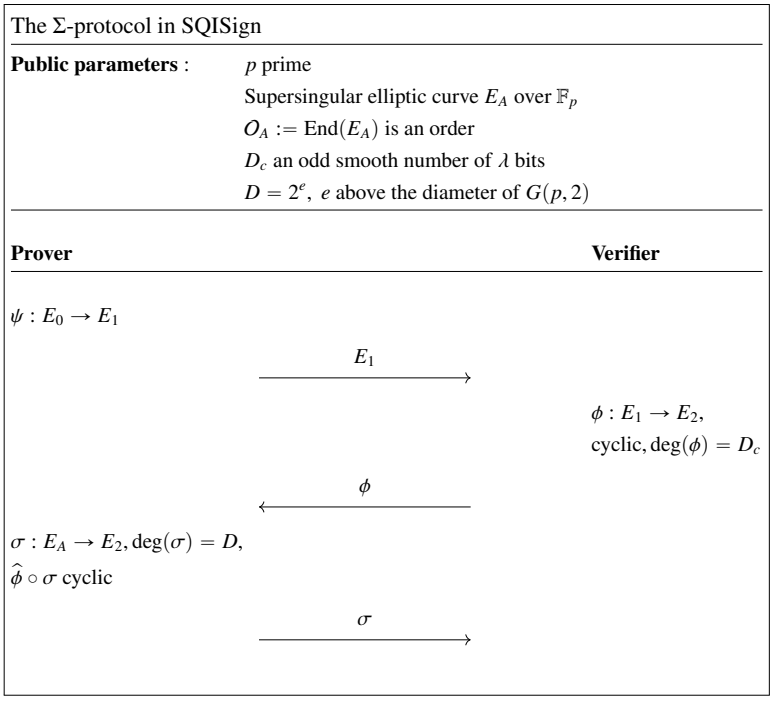



Figure 6: The Σ-protocol in SQISign

### 6.5.1 Completeness

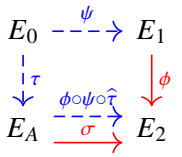
In this section we will analyze the completeness property of the Σ-protocol introduced in the previous section. The most important tool to prove completeness lies in an algorithm proposed in [2, p. 24], called SigningKLPT. In the algorithm we take $O_0$ to be a special extremal maximal order and $O$ to be a maximal order. Viewing the algorithm as a black box, it looks as follows:

SigningKLPT$(I, I_\tau)$
**Input:** $I_\tau$ is a left $O_0$-ideal and a right $O$-ideal of norm $\mathrm{N}_\tau$. $I$ is a left $O$-ideal.
**Output:** An ideal $J \sim I$ of norm $\ell^e$, where $e$ is fixed.

In the Σ-protocol we consider a 2-isogeny graph, so we take $\ell = 2$ in the algorithm above. The algorithm is shown to be correct and to terminate heuristically in probabilistic polynomial time in [2].

What we need for completeness, is that whenever an honest prover $P$ executes the protocol and indeed has the information $\tau$, the verifier $V$ will always accept. The

verifier always accepts when it is given an isogeny $\sigma : E_A \to E_2$ of degree $2^e$ such that $\widehat{\phi} \circ \sigma$ is cyclic. Therefore we want the prover $P$ to be able to construct such an isogeny $\sigma$ every time it has the information $\tau$. The isogenies and elliptic curves in question are given in the diagram below. The blue dashed lines correspond to secret isogenies and the red lines correspond to public isogenies.




As mentioned before, we want $P$ to be able to construct an isogeny $\sigma$, where $\sigma$ is as described above, whenever $P$ really knows $\tau$. Note that when $P$ indeed has knowledge of $\tau$, $P$ knows the isogeny $\phi \circ \psi \circ \widehat{\tau}$. Denote by $\mathcal{O}_A$ the order corresponding to the endomorphism ring of $E_A$ and by $\mathcal{O}_0$ the order corresponding to the endomorphism ring of $E_0$. By the Deuring correspondence, as illustrated in Table 6.3, such an isogeny correponds to an ideal $I_{\phi\circ\psi\circ\widehat{\tau}}$ that is a left $\mathcal{O}_A$-ideal. We denote by $I_\tau$ the ideal corresponding to the isogeny $\tau$, so $I_\tau$ is a left $\mathcal{O}_0$-ideal and a right $\mathcal{O}_A$-ideal. The prover can now run $\mathsf{SigningKLPT}(I_{\phi\circ\psi\circ\widehat{\tau}}, I_\tau)$ and it will obtain an ideal $J \sim I_{\phi\circ\psi\circ\widehat{\tau}}$ of norm $2^e$. Such an ideal $J$ corresponds to an isogeny $\sigma : E_A \to E_2$ with $\deg(\sigma) = \mathcal{N}(I_{\phi\circ\psi\circ\widehat{\tau}}) = 2^e$. Therefore the prover will be able to output an isogeny that will be accepted by the verifier, due to the correctness of $\mathsf{SigningKLPT}$ (the cyclicity also follows from the algorithm, we refer to [2] for the details).

### 6.5.2 Special soundness

In this section we will analyse the special soundness property of the $\Sigma$-protocol in $\mathsf{SQISign}$. We define the relation $R$ as follows:

$$R := \{(E_A, \alpha) \ : \ \alpha \text{ is a cyclic endomorphism of smooth degree}\}.$$

We assume that the following problem is hard. This will help us prove the special soundness of the given protocol.

**Problem 3** (Supersingular Smooth Endomorphism Problem)**.** Given a prime $p$ and a supersingular elliptic curve $E/\mathbb{F}_{p^2}$, find a (non-trivial) cyclic endomorphism of $E$ of smooth degree.

This problem can be shown to be equivalent to the *Endomorphism Ring Problem* (given $E/\mathbb{F}_{p^2}$ compute endomorphisms that form a $\mathbb{Z}$-basis of $\mathrm{End}(E)$), which is

assumed to be hard. We will also need the following lemma to prove the special soundness of the protocol.

**Lemma 6.23.** *Given two accepting transcripts $(E_1, \phi, \sigma)$ and $(E_1, \phi', \sigma')$, where $\phi$ and $\phi'$ are not equivalent (i.e. they do not represent the same path in the isogeny graph, we denote this by $\phi \nsim \phi'$), the composition $\widehat{\sigma}' \circ \phi' \circ \widehat{\phi} \circ \sigma$ is a non-scalar endomorphism of $E_A$ and it has smooth degree.*

*Proof.* We know that $\phi$ and $\phi'$ have degree $D_c$, so also their duals have degree $D_c$. Also we know that $\sigma$ and $\sigma'$ have degree $D$, so their duals also have degree $D$. This means that

$$\deg(\widehat{\sigma}' \circ \phi' \circ \widehat{\phi} \circ \sigma) = \deg(\widehat{\sigma}') \cdot \deg(\phi') \cdot \deg(\phi) \cdot \deg(\sigma) = (DD_c)^2.$$

Since $D$ and $D_c$ are smooth numbers, their product is also smooth, so the given composition of endomorphisms indeed has smooth degree.
What's left to show is that the composition $\widehat{\sigma}' \circ \phi' \circ \widehat{\phi} \circ \sigma$ is a non-scalar endomorphism. Suppose for contradiction that it is a scalar endomorphism. Since its degree is $(DD_c)^2$, we have that

$$\widehat{\sigma}' \circ \phi' \circ \widehat{\phi} \circ \sigma = [DD_c].$$

Since $\widehat{\sigma}' \circ \phi'$ and $\widehat{\sigma}' \circ \phi'$ have the same degree and $\widehat{\sigma}' \circ \phi' \circ \widehat{\phi} \circ \sigma = [\deg(\widehat{\sigma}' \circ \phi')]$, we conclude that $\widehat{\sigma}' \circ \phi'$ and $\widehat{\phi} \circ \sigma$ are duals, by the uniqueness of the dual isogeny. This implies

$$\widehat{\sigma}' \circ \phi' = \widehat{\sigma} \circ \phi.$$

In particular this implies that $\ker(\widehat{\sigma}' \circ \phi') = \ker(\widehat{\sigma} \circ \phi)$. Suppose that $\ker(\sigma) = \ker(\sigma')$, this implies that $\sigma = \sigma'$. However the equality $\widehat{\sigma}' \circ \phi' = \widehat{\sigma} \circ \phi$ then implies that $\phi = \phi'$, which is not possible. Therefore we must have that $\ker(\sigma) \neq \ker(\sigma')$. However, $\sigma$ and $\sigma'$ are of degree $2^e$, which by assumption is coprime to $p$. Therefore $\sigma$ and $\sigma'$ are separable isogenies. Hence

$$\#\ker(\sigma) = \deg_s(\sigma) = \deg(\sigma) = \deg(\sigma') = \deg_s(\sigma') = \#\ker(\sigma').$$

We know that $\ker(\sigma)$ and $\ker(\sigma')$ are cyclic subgroups of $E[2^e] \cong (\mathbb{Z}/2^e\mathbb{Z})^2$. Since both have (separable) degree $2^e$ that implies that $\ker(\sigma') \cong \ker(\sigma) \cong \mathbb{Z}/2^e\mathbb{Z}$. This implies that $\sigma$ and $\sigma'$ only differ by an isomorphism and since $\widehat{\sigma}' \circ \phi' = \widehat{\sigma} \circ \phi$, we conclude that $\phi'$ and $\phi$ also differ only by an isomorphism. In particular, this shows that $\phi \sim \phi'$, which is a contradiction. □

**Corollary 6.24.** *The Σ-protocol used in SQISign satisfies special soundness.*

*Proof.* This follows directly from Lemma 6.23. Since $\widehat{\sigma}' \circ \phi' \circ \widehat{\phi} \circ \sigma$ is a cyclic endomorphism of $E_A$ of smooth degree it follows that

$$(E_A, \widehat{\sigma}' \circ \phi' \circ \widehat{\phi} \circ \sigma) \in R.$$

Also note that this isogeny can be computed in (probabilistic) polynomial time. Therefore we define the extractor $\mathcal{E}$ to be such that it outputs $\widehat{\sigma}' \circ \phi' \circ \widehat{\phi} \circ \sigma$ as witness for $E_A$. □

**Theorem 6.25.** *If there is an adversary that breaks the soundness of the protocol with probability w and expected running time r for the public key $E_A$, then there is an algorithm for the* Supersingular Smooth Endomorphism Problem *on $E_A$ with expected running time $O\left(\frac{r}{w-1/C}\right)$, where C is the size of the challenge space.*

*Proof.* As mentioned, the endomorphism $\widehat{\sigma}' \circ \phi' \circ \widehat{\phi} \circ \sigma$ given in Lemma 6.23 is a cyclic endomorphism of $E_A$ that has smooth degree. Therefore a witness for $E_A$ gives a solution to the Supersingular Smooth Endomorphism Problem of $E_A$. The special soundness of the protocol implies that it also has knowledge soundness with knowledge error $1/C$ where $C$ is the size of the challenge space (this follows from e.g. [26, Theorem 1]). In other words, the number of steps necessary to output a witness is bounded by

$$\frac{|x|^c}{\varepsilon(x) - 1/C}.$$

The running time $r$ is of the size of a power of the length of the input and the probability of breaking the soundness of the protocol $w$ is equal to $\varepsilon(x)$, i.e. the probability that the verifier accepts after interaction with the (possibly malicious) prover. Therefore the expected running time is

$$O\left(\frac{r}{w - 1/C}\right).$$

□

Note that if we had proven already that the protocol is a Σ-protocol, we could have used Theorem 6.7 and (4) to prove Theorem 6.25.

### 6.5.3 Zero-Knowledge

In this subsection we will prove the zero-knowledge property of the Σ-protocol. We will not give the full proof, but give the proof of an easier statement where we

use an assumption on the public key $E_A$. This assumption can be proven to be true, as is done in [2, Section 7].

**Definition 6.26.** Let $X = \{X_\lambda\}_{\lambda\in\mathbb{N}}$ and $Y = \{Y_\lambda\}_{\lambda\in\mathbb{N}}$ be families of random variables. We say $X$ and $Y$ are *computationally close* or *computationally indistinguishable*, if for all probabilistic polynomial time adversaries $\mathcal{A}$, there exists a negligible function $f$ (defined in Definition 6.1) such that for all $\lambda \in \mathbb{N}$:

$$|\Pr[\mathcal{A}(x) \ : \ x \leftarrow X_\lambda] - \Pr[\mathcal{A}(x) \ : \ x \leftarrow Y_\lambda]| \leqslant f(\lambda).$$

We will denote $X \sim Y$ if $X$ and $Y$ are computationally indistinguishable.
We define *computational Honest-Verifier Zero-Knowledge* analogous to Honest-Verifier Zero-Knowledge, only we require the distributions to be computationally indistinguishable, instead of indistinguishable.

The above definition means as much as: the probability that a PPT adversary outputs the same value for an element from $X_\lambda$ as an element from $Y_\lambda$ is quite large, which implies that it is hard for any PPT adversary to distinguish the family of random variables $X$ from the other family of random variables, $Y$.

**Lemma 6.27.** *Let $\mathcal{D}(E_A)$ denote the distribution of the isogenies $\sigma$ in the SQISign identification protocol. If we assume that for any SQISign public key $E_A$, there exists a probabilistic polynomial time algorithm $S$, taking $E_A$ as input, whose output distribution is (computationally) indistinguishable from $\mathcal{D}(E_A)$, then the SQISign identification protocol is (computationally) Honest-Verifier Zero-Knowledge.*

*Proof.* For the Honest-Verifier Zero Knowledge property to hold we need to construct a PPT algorithm $\mathsf{Sim}$ that on input $x$ outputs a transcript whose distribution is (computationally) indistinguishable from the distribution of the honest protocol transcript. We construct $\mathsf{Sim}$ as follows: on input of some elliptic curve $E_A$, $\mathsf{Sim}$ lets $S$ generate a $\tilde{\sigma}$ by giving it input $E_A$, i.e. $S(E_A) = \tilde{\sigma} : E_A \to \tilde{E}_2$. Also $\mathsf{Sim}$ generates a uniformly random $\widehat{\tilde{\phi}} : \tilde{E}_2 \to \tilde{E}_1$ of degree $D_c$, i.e. $\tilde{\phi}$ is chosen uniformly at random from the set of isogenies going from $E_2 \to E_1$ and have degree $D_c$. Finally it outputs

$$\mathsf{Sim}(E_A) = (\tilde{E}_1, \tilde{\phi}, \tilde{E}_2, \tilde{\sigma}).$$

We check if this transcript distribution is (computationally) indistinguishable from the distribution of an honest protocol transcript, we denote $(E_1, \phi, E_2, \sigma)$ for an honest protocol transcript. Note that $\phi$ and $\tilde{\phi}$ are both chosen uniformly at random

from the set of isogenies of degree $D_c$ with domain some elliptic curve $E_1$ and $\tilde{E}_1$, respectively. We denote the distribution of $\phi$ and $\tilde{\phi}$ by $\mathcal{D}(\phi)$ and $\mathcal{D}(\tilde{\phi})$, respectively, so $\mathcal{D}(\phi)$ and $\mathcal{D}(\tilde{\phi})$ are identical. By assumption on $S$, $\tilde{\sigma}$ has the same distribution as $\sigma$ from the honest protocol transcript. What's left to show is that the elliptic curves in the output of the simulator have the same distribution as the elliptic curves in the output of the honest protocol transcript. If we choose $D$ and $D_c$ sufficiently large, then the walk corresponding to $\psi$ and $\widehat{\tilde{\phi}}$ consist of sufficiently many steps which means that the distribution of the endpoint of a random walk is approximately the uniform distribution, which follows from Theorem 3.20. Sufficiently large here means that the number of steps in the walk should be $O\left(\frac{\#V}{\log(1-\lambda_2)}\right)$, as is stated in Theorem 3.20 as well. In particular this means that the curve $\tilde{E}_1$ and $E_1$ are both chosen according to a uniform random distribution. Finally, the elliptic curve $\tilde{E}_2$ is chosen by $S$, which by assumption gives as output something with the same distribution as $\mathcal{D}(E_A)$ hence the distribution of $\tilde{E}_2$ computationally indistinguishable from the distribution of $E_2$ (from an honest protocol). □

For more information on the distribution $\mathcal{D}(E_A)$ we refer to [2, Section 7.2].

Lemma 6.27 shows that the SQISign identification protocol satisfies (computational) Honest-Verifier Zero Knowledge under the assumption that there is a PPT algorithm that on input $E_A$ outputs an isogeny and a target curve whose distribution are (computationally) indistinguishable from the distribution in which they occur in the honest protocol transcript. It is shown in [2, Section 7] that this assumption holds.

### 6.5.4 The signature scheme SQISign

In the previous subsections we have seen that the introduced 3-move protocol, the SQISign identification scheme, is indeed a Σ-protocol. In this section we will introduce (digital) signature schemes and we will show how to construct a signature scheme from a Σ-protocol. For this we will use the Σ-protocol that we discussed in the previous subsections. The signature scheme we construct is the SQISign scheme introduced in [2].

**Definition 6.28** ((Digital) Signature scheme)**.** A *(digital) signature scheme* consists of three polynomial-time algorithms $(\mathsf{Gen}, \mathsf{Sign}, \mathsf{Ver})$ such that:

1. The *key generation algorithm* $\mathsf{Gen}$ takes as input some parameter $\overbrace{(1, \ldots, 1)}^{\lambda}$

and outputs a pair of keys $(\mathsf{pk}, \mathsf{sk})$, i.e. the *public key* and the *secret key*.

2. The *signing algorithm* $\mathsf{Sign}$ takes as input a private key $\mathsf{sk}$ and a message $m$, and outputs a signature $\sigma$.

3. The *verification algorithm* $\mathsf{Ver}$ is a deterministic algorithm which takes as input a public key $\mathsf{pk}$, a message $m$ and a signature $\sigma$. It outputs a bit $b \in \{0, 1\}$, where 0 means *invalid* and 1 means *valid*.

Furthermore, we require a correctness guarantee: $\mathsf{Ver}(\mathsf{pk}, m, \mathsf{Sign}(\mathsf{sk}, m)) = 1$ except with negligible probability (i.e. with probability $1 - f(\lambda)$ where $f$ is a negligible function).

There are several definitions of security for signature schemes, one of those is called *existential unforgeability against chosen message attacks*, abbreviated as EUF-CMA. If a signature scheme satisfies EUF-CMA security, this basically means that any PPT adversary that can query messages and receive a valid signature, cannot produce a forgery, that is, a message-signature pair $(m, \sigma)$, that gets accepted by the verifying algorithm $\mathsf{Ver}$ (and $m$ was not previously queried). We will not give the formal definition of this type of security here, but it can be found in any textbook on basic cryptography, e.g., [27].

To be complete we will give the definitions of a hash-function and a random oracle. Both are used a lot in cryptographic proofs and/or protocols so it is no surprise that they show up in the signature scheme that we will consider. However, we will not go into the theory behind hash functions and random oracles deeply, since there is a lot of theory, but it is not strictly necessary for what we are considering here.

**Definition 6.29** (Hash-function)**.** A *hash function* $H$ is a deterministic function $H : \{0, 1\}^* \to \{0, 1\}^{c_\lambda}$, where $\lambda$ is some security parameter and $c_\lambda$ is some constant depending on $\lambda$.

**Definition 6.30** (Random Oracle)**.** A *random oracle* is a theoretical black box that responds to every unique query with a truly random response chosen uniformly from its set of possible outputs.

Theoretically, a truly random function can be seen as a function $g : A \to B$, where $A$ and $B$ are sets and $g$ is such that even when we know all $g(x_i)$ for $x_i \in A \setminus \{x\}$, we could not predict $g(x)$ better than just picking some $y \in B$ at random. In the optimal case, a hash function behaves like a truly random function. Random oracles are often used in proofs where it is not enough to use a (cryptographic) hash-function. Security proofs that use a random oracle will often

state something in terms of: "the protocol is secure in the random oracle model". Sometimes a proof in the random oracle model is called a "heuristic proof".

The next definition gives a signature scheme that is built from a Σ-protocol. It was introduced by Fiat and Shamir in [28].

**Definition 6.31** (Fiat-Shamir)**.** Given a Σ-protocol for a relation $R$ with challenge space $C$ and some public hash function $H : \{0,1\}^* \to \{0,1\}^{c_\lambda}$, where $\lambda$ is a security parameter, the *Fiat-Shamir transform* is as follows.

- The signing algorithm has access to both the secret and public key, which in this case corresponds to $x$ and $w$. It starts by generating an $a$ according to the Σ-protocol, like a prover would do. Next it sets $c := H(x||a)$ (here $x||a$ means that we concatenate the bitstrings $x$ and $a$) and using the partial transcript $(a,c)$ it generates a $z$ in the same way a prover would do when given $(a,c)$. Finally:

$$\mathsf{Sign}(x,w) = (a,z).$$

- The verification algorithm computes $H(x||a)$ and checks whether $(a, H(x||a), z)$ is accepted by the verifier in the Σ-protocol. In other words

$$\mathsf{Ver}(x,a,z) = \begin{cases} 1 & \text{if} \quad \langle \mathrm{P}, \mathrm{V} \rangle(x;w) = 1 \text{ given the transcript } (a, H(x||a), z) \\ 0 & \text{if} \quad \langle \mathrm{P}, \mathrm{V} \rangle(x;w) = 0 \text{ given the transcript } (a, H(x||a), z). \end{cases}$$

We leave out the proof that the Fiat-Shamir transform is in fact a digital signature scheme. Fiat and Shamir suggested to use a random oracle for $H$. Indeed it turns out that this gives EUF-CMA security, as long as the underlying Σ-protocol satisfies a certain type of security (we will not go into this here, the precise statement is given in [29, Theorem 1]). However there has been a lot of research to find instantiations for $H$ that render the Fiat-Shamir transform secure in the standard model (i.e. where we do not have to assume that $H$ is a random oracle) for many widely-used protocols.

We can now introduce the signature scheme, SQISign, from [2]. Recall the Σ-protocol introduced in Section 6.5, SQISign is basically a Fiat-Shamir transform of this Σ-protocol. To be precise, it is as follows:

## SQISign

**Parameters:** A prime $p$ is chosen and then a supersingular elliptic curve $E_0$ over $\mathbb{F}_p$ with special extremal endomorphism ring $\mathcal{O}_0$ is chosen. We choose $D_c = \prod_{i=1}^{n} \ell_i^{e_i}$ to be an odd smooth number of $\lambda$ bits and $D = 2^e$ where $e$ is above the diameter of the supersingular 2-isogeny graph. We let $\mu(D_c) = \prod_{i=1}^{n} \ell_i^{e_i-1}(\ell_i + 1)$. We consider a cryptographically secure hash function $H : \{0,1\}^* \to [1, \mu(D_c)]$ and we let $\Phi_{D_c}$ be an arbitrary function that maps an elliptic curve $E$ and an element $s \in [1, \mu(D_c)]$ to a non-backtracking sequence of isogenies of total degree $D_c$, starting at $E$.

**Key generation:** The key pair, consisting of a public key and a secret key, is generated as follows. A random isogeny walk starting at $E_0$ is chosen. This isogeny walk is denoted by $\tau$ and ends at some vertex corresponding to an elliptic curve $E_A$. The public key is the curve $E_A$ and the secret key is the isogeny $\tau$, i.e. the key pair is $(\mathsf{pk}, \mathsf{sk}) = (E_A, \tau)$.

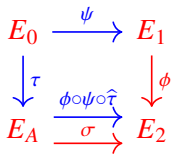
**The protocol:**

- Sign: It gets as input $(\mathsf{sk}, m)$. First it chooses a random (secret) isogeny $\psi : E_0 \to E_1$, like the prover in the $\Sigma$-protocol would do. Then it sets $s := H(j(E_1), m)$ and outputs the isogeny $\Phi_{D_c}(E_1, s) =: \phi : E_1 \to E_2$, in the $\Sigma$-protocol this would correspond to the answer of a verifier. From $\mathcal{O}_A$ and $\phi \circ \psi : E_0 \to E_2$ it constructs an isogeny $\sigma : E_A \to E_2$ of degree $D$ such that $\widehat{\phi} \circ \sigma$ is cyclic. It outputs:

$$\mathsf{Sign}(\mathsf{sk}, m) = (E_1, \sigma).$$

- Verify: It gets as input $(\mathsf{pk}, m, E_1, \sigma)$. It calculates $s = H(j(E_1, m)$ and then computes $\Phi_{D_c}(E_1, s) = \phi$. It then checks whether $\sigma$ is indeed an isogeny from $E_A$ to $E_2$ of degree $D$ and checks whether $\widehat{\phi} \circ \sigma$ is a cyclic isogeny, if so, it outputs 1, else it outputs 0.

The protocol can be illustrated as the diagram below. Here the red parts denote public information and the blue ones secret information. It is important to keep in mind that the signature $\sigma$ does not equal $\phi \circ \psi \circ \widehat{\tau}$. However, $\sigma$ is constructed *using* $\phi \circ \psi \circ \widehat{\tau}$ as input in Algorithm 5 in [2, Section 6].



# 7 Orientations and OSIDH

## 7.1 Orientations

In this section we will discuss the notion of orientations. We will introduce an orientation on elliptic curves and isogenies and using these orientations we will look at isogeny graphs where both the elliptic curves and the isogenies have a certain orientation.

**Definition 7.1.** Let $k$ be the algebraic closure of some field of characteristic $p$, where $p$ is a prime. Let $K$ be an imaginary quadratic field and let $E$ be an elliptic curve over $k$. A *$K$-orientation on the elliptic curve $E/k$* is an injective ring homomorphism (i.e. an embedding)

$$\iota : K \hookrightarrow \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

**Theorem 7.2.** *Let $K = \mathbb{Q}(\sqrt{d})$ be an imaginary quadratic field and let $\left(\frac{m,n}{\mathbb{Q}}\right)$ be the quaternion algebra over the rationals given by*

$$\left(\frac{m,n}{\mathbb{Q}}\right) = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}ij,$$

*where $i^2 = m$, $j^2 = n$ and $ij = -ji$. Then there exists an embedding, i.e. an injective ring homomorphism*

$$\iota : K \hookrightarrow \left(\frac{m,n}{\mathbb{Q}}\right),$$

*if and only if there exists an $\omega \in \left(\frac{m,n}{\mathbb{Q}}\right)$ such that $\omega^2 = d$.*

*Proof.* First suppose that there exists such $\omega$. We define a map $\iota$ from $K = \mathbb{Q}(\sqrt{d})$ to $\left(\frac{m,n}{\mathbb{Q}}\right)$ as follows

$$\mathbb{Q}(\sqrt{d}) \to \left(\frac{m,n}{\mathbb{Q}}\right) \quad \text{with} \quad a + b\sqrt{d} \mapsto a + b\omega,$$

where $a, b$ are rationals. Note that $\iota$ is a ring homomorphism since

$$\begin{aligned} \iota(a + b\sqrt{d}) + \iota(a' + b'\sqrt{d}) &= a + b\omega + a' + b'\omega \\ &= a + a' + (b + b')\omega \\ &= \iota((a + b\sqrt{d}) + (a' + b'\sqrt{d})), \end{aligned}$$

and

$$\begin{aligned}\iota(a+b\sqrt{d})\cdot\iota(a'+b'\sqrt{d}) &= (a+b\omega)\cdot(a'+b'\omega)\\ &= aa'+a'b+ab'\omega+\omega^2\\ &= \iota(aa'+a'b\sqrt{d}+ab'\sqrt{d}+d)\\ &= \iota((a+b\sqrt{d})\cdot(a'+b'\sqrt{d})),\end{aligned}$$

for all $a,a',b,b' \in \mathbb{Q}$. Also $\iota$ is injective, since $\iota(a+b\sqrt{d}) = 0$ if and only if $a = b = 0$. Hence the kernel of $\iota$ is trivial, so $\iota$ is injective. Therefore $\iota$ gives an embedding of $K$ into $\left(\frac{m,n}{\mathbb{Q}}\right)$.
For the other direction, we suppose that there exists an embedding

$$\iota : K = \mathbb{Q}(\sqrt{d}) \hookrightarrow \left(\frac{m,n}{\mathbb{Q}}\right).$$

Since embeddings of number fields necessarily leave $\mathbb{Q}$ unchanged, we have that $\iota\left(\frac{a}{b}\right) = \frac{a}{b}$ for all $\frac{a}{b} \in \mathbb{Q}$. Moreover, this means that if we set $\omega = \iota(\sqrt{d})$, then

$$\omega^2 = \iota(\sqrt{d})^2 = \iota(d) = d.$$

□

Theorem 7.2 gives a necessary and sufficient condition for the existence of a $K$-orientation on a supersingular elliptic curve, since endomorphism algebras of supersingular elliptic curves are rational quaternion algebras.

**Example 7.3.** Let $E$ be an elliptic curve given by $y^2 = x^3 + x$ over some finite field $k$. This curve has $j$-invariant $j(E) = 1728$, and by [5, Example V.4.5] we know that curves with $j = 1728$ are supersingular if and only if $p \equiv 3 \mod 4$. Now suppose that $k$ has characteristic $p \equiv 3 \mod 4$, then $E$ is supersingular. Consider the field $K = \mathbb{Q}(i)$, where $i$ is such that $i^2 = -1$. By Theorem 7.2 we know that there exists an embedding of $K$ into $\mathrm{End}^0(E)$ if and only if there is some element that acts as $-1$. Consider the isogeny

$$\sigma : (x,y) \mapsto (-x, ay),$$

where $a$ is such that $a^2 = -1$. Note that the image of $\sigma$ is exactly the elliptic curve $E$, hence $\sigma$ is an endomorphism. Also note that

$$\sigma^2(x,y) = (x,-y) = -(x,y),$$

therefore applying $\sigma$ twice corresponds to the multiplication by $-1$. Denote the isomorphism from $\left(\frac{m,n}{\mathbb{Q}}\right)$ to $\mathrm{End}^0(E)$ by $\psi$. Then we have an embedding

$$K \hookrightarrow \left(\frac{m,n}{\mathbb{Q}}\right) \quad \text{with} \quad a+bi \mapsto a+b\psi^{-1}(\sigma),$$

and composing this embedding with the isomorphism $\psi$ we have an embedding $\iota$ of $K$ into $\mathrm{End}^0(E)$. Hence we have a $\mathbb{Q}(i)$-orientation on the (supersingular) elliptic curve $E$ over a field of characteristic $p$ where $p \equiv 3 \mod 4$.

**Definition 7.4.** Let $k, K$ and $E$ be as before and let $\mathcal{O}$ be an order in $K$. We say that a $K$-orientation is an *$\mathcal{O}$-orientation* if $\iota(\mathcal{O}) \subset \mathrm{End}(E)$.
We say that an $\mathcal{O}$-orientation is *primitive* if $\iota(\mathcal{O}) = \mathrm{End}(E) \cap \iota(K)$. Note that in this case $\iota$ gives an isomorphism between the order $\mathcal{O}$ and the endomorphism ring of $E$ considered in the image of $K$ under $\iota$.
If $\iota$ is a $K$-orientation on $E$, respectively a (primitive) $\mathcal{O}$-orientation on $E$, we say that the pair $(E,\iota)$ is a *$K$-oriented elliptic curve*, respectively a *(primitive) $\mathcal{O}$-oriented elliptic curve*.

Throughout this section we will assume that $k, K, E$ are as introduced in Definition 7.1.

**Definition 7.5.** Let $(E,\iota)$ be a $K$-oriented elliptic curve, let $F$ be some elliptic curve over $k$ and let $\phi : E \to F$ be an isogeny of degree $\ell$. We define a *$K$-orientation $\phi_*(\iota)$ on $F$* by

$$\phi_*(\iota)(\alpha) = \frac{1}{\ell}\phi \circ \iota(\alpha) \circ \widehat{\phi},$$

for $\alpha \in K$.
Given two $K$-oriented elliptic curves $(E,\iota_E)$ and $(F,\iota_F)$, an isogeny $\phi : E \to F$ is *$K$-oriented* if $\phi_*(\iota_E) = \iota_F$. We denote this by $\phi : (E,\iota_E) \to (F,\iota_F)$.

**Proposition 7.6.** *Suppose $E$ has a primitive $\mathcal{O}$-orientation, denoted by $\iota_E$, and there is an isogeny $\phi : E \to F$ of degree $\ell$. Then $F$ admits an induced primitive $\mathcal{O}'$-orientation by an order $\mathcal{O}'$ satisfying*

$$\mathbb{Z} + \ell\mathcal{O} \subseteq \mathcal{O}' \quad \text{and} \quad \mathbb{Z} + \ell\mathcal{O}' \subseteq \mathcal{O}.$$

*Proof.* The induced orientation on $F$ is defined as $\iota_F(\alpha) := \frac{1}{\ell}\phi \circ \iota_E(\alpha) \circ \widehat{\phi}$, for $\alpha \in K$. Rewriting this, by multiplying both sides with $\phi$ and its dual, gives $\iota_E(\alpha) = \frac{1}{\ell}\widehat{\phi}\circ\iota_F(\alpha)\circ\phi$. We claim that $\iota_E^{-1}(\psi) = \frac{1}{\ell}\iota_F^{-1}(\phi\circ\psi\circ\widehat{\phi})$, for $\psi \in \mathrm{End}(E)$. It can be checked that indeed $\iota_E^{-1}(\iota_E(\alpha)) = 1$ and that $\iota_E(\iota_E^{-1}(\psi)) = [1]$. Similarly,

we can check that $\iota_F^{-1}(\psi) = \frac{1}{\ell}\iota_E^{-1}(\widehat{\phi} \circ \psi \circ \phi)$, by checking that $\iota_F^{-1}(\iota_F(\alpha)) = 1$ and that $\iota_F(\iota_F^{-1}(\psi)) = [1]$.
Note that $\mathcal{O} = \iota_E^{-1}(\mathrm{End}(E))$ and that $\mathcal{O}' = \iota_F^{-1}(\mathrm{End}(F))$. Let $\psi \in \mathrm{End}(E)$ and $a \in \mathbb{Z}$, then

$$a + \ell\iota_E^{-1}(\psi) \in \mathbb{Z} + \ell\mathcal{O}.$$

We have that

$$\begin{aligned} a + \ell\iota_E^{-1}(\psi) &= a + \ell\frac{1}{\ell}\iota_F^{-1}(\phi \circ \psi \circ \widehat{\phi}) \\ &= a + \iota_F^{-1}(\phi \circ \psi \circ \widehat{\phi}). \end{aligned}$$

Since $a \in \iota_F^{-1}(\mathrm{End}(F))$ and since $\phi \circ \psi \circ \widehat{\phi} \in \mathrm{End}(F)$, we conclude that $a + \ell\,\iota_E^{-1}(\psi) \in \iota_F^{-1}(\mathrm{End}(F)) = \mathcal{O}'$, so

$$\mathbb{Z} + \ell\mathcal{O} \subseteq \mathcal{O}'.$$

The other inclusion can be proven in the same way. □

**Proposition 7.7.** *Let $\phi : (E, \iota_E) \to (F, \iota_F)$ be a K-oriented isogeny of degree $\ell$. Let $\mathcal{O} = \mathrm{End}(E) \cap \iota_E(K)$ and let $\mathcal{O}' = \mathrm{End}(F) \cap \iota_F(K)$ so that $\iota_E$ is a primitive $\mathcal{O}$-orientation and $\iota_F$ a primitive $\mathcal{O}'$-orientation. We can distinguish three cases:*

- *we say $\phi$ is* horizontal *if $\mathcal{O} = \mathcal{O}'$;*
- *we say $\phi$ is* ascending *if $\mathcal{O} \subsetneq \mathcal{O}'$. In this case $[\mathcal{O}' : \mathcal{O}] = \ell$;*
- *we say $\phi$ is* descending *if $\mathcal{O} \supsetneq \mathcal{O}'$. In this case $[\mathcal{O} : \mathcal{O}'] = \ell$.*

*Proof.* The proof of this statement is also given in [30, Proposition 21]. We use [30, Proposition 5]. This proposition says that if $E$ and $F$ are isogenous and if $E$ has an endomorphism ring that is an order in a quadratic imaginary extension of $\mathbb{Q}$, then there exists unique relatively prime integers $m_E$ and $m_F$ such that

$$\mathbb{Z} + m_E \cdot \iota_E(\mathrm{End}(E)) = \mathbb{Z} + m_F \cdot \iota_F(\mathrm{End}(F)),$$

where the degree of every isogeny from $E$ to $F$ is divisible by $m_E m_F$. Therefore, we must have that $m_E m_F$ divides $\ell$, which is prime. So either $m_E = m_F = 1$ or $m_E = \ell$ and $m_F = 1$ or $m_E = 1$ and $m_F = \ell$. Hence we have one of the three following cases:

$$\mathbb{Z} + \ell\mathcal{O}' = \mathbb{Z} + \mathcal{O} \quad \text{or} \quad \mathbb{Z} + \ell\mathcal{O} = \mathbb{Z} + \mathcal{O}' \quad \text{or} \quad \mathbb{Z} + \mathcal{O} = \mathbb{Z} + \mathcal{O}'. \tag{5}$$

This implies that either $\mathcal{O} = \mathcal{O}'$, or $\mathcal{O} \subsetneq \mathcal{O}'$ with $[\mathcal{O}' : \mathcal{O}] = \ell$ or $\mathcal{O} \supsetneq \mathcal{O}'$ with $[\mathcal{O} : \mathcal{O}'] = \ell$.

□

**Definition 7.8.** A $K$-oriented isogeny $\phi : (E, \iota_E) \to (F, \iota_F)$ is a *$K$-oriented isomorphism* if there exists a $K$-oriented isogeny $\psi : (F, \iota_F) \to (E, \iota_E)$ such that $\psi \circ \phi = \mathrm{id}_E$ and $\phi \circ \psi = \mathrm{id}_F$. In this case we say that $(E, \iota_E)$ and $(F, \iota_F)$ are *$K$-isomorphic* and we write $(E, \iota_E) \cong (F, \iota_F)$.

We now return to the subject of isogeny graphs. In particular, we consider supersingular isogeny graphs. Let $E_0/k$ be a supersingular isogeny graph and let $\ell \neq p$.

**Definition 7.9.** An *$\ell$-isogeny chain of length $n$ from $E_0$ to $E$* is a sequence of isogenies of degree $\ell$:

$$E_0 \xrightarrow{\phi_0} E_1 \xrightarrow{\phi_1} E_2 \xrightarrow{\phi_2} \cdots \xrightarrow{\phi_{n-1}} E_n = E.$$

We say that the chain is *without backtracking* if $\ker(\phi_{i+1} \circ \phi_i) \neq E_i[\ell]$ for all $i \in \{0, \ldots, i-1\}$. Furthermore we say the chain is *ascending* (or *descending* or *horizontal*) if all isogenies $\phi_i$ are ascending (respectively descending or horizontal).

We can consider $\ell$-isogeny chains to be walks in an isogeny graph. Since $\widehat{\phi_i}$ is the unique isogeny such that composition with $\phi_i$ gives $[\ell]$, "without backtracking" means that the walk, considered in the isogeny graph, does not go back immediately to the vertex it came from.

**Lemma 7.10.** *The composition of isogenies in an $\ell$-isogeny chain is cyclic if and only if the $\ell$-isogeny chain is without backtracking.*

*Proof.* It is clear that backtracking implies that the composition is not cyclic, since then the kernel will contain $(\mathbb{Z}/\ell\mathbb{Z})^2$, which is not a cyclic group. Now suppose that the composition is not cyclic, that implies that there is an $i$ such that $\ker(\phi_{i+1} \circ \phi_i)$ is not cyclic. That means that $\ker(\phi_{i+1} \circ \phi_i)$ is a non-cyclic subgroup of $E_i[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^2$. In particular this implies that there is an element $(a, b) \in \ker(\phi_{i+1} \circ \phi_i)$ such that $a$ and $b$ are both not the unit element. But every element in $\mathbb{Z}/\ell\mathbb{Z}$ for a prime $\ell$ generates the entire group. Hence $\ker(\phi_{i+1} \circ \phi_i) = (\mathbb{Z}/\ell\mathbb{Z})^2 = E_i[\ell]$ and therefore the chain is with backtracking. □

**Remark 7.11.** Note that descending $\ell$-isogeny chains automatically do not have backtracking, since the unique isogeny $\psi$ that satisfies $\psi \circ \phi_i = E_i[\ell]$ is the dual isogeny of $\phi_i$, which is ascending. The same holds for ascending $\ell$-isogeny chains.

**Theorem 7.12.** *Let $(E_i, \phi_i)$ be a descending $\ell$-isogeny chain, such that $E_0$ is equipped with an $\mathcal{O}_K$-orientation, where $\mathcal{O}_K$ is the maximal order of $K$. For each $i$ let $\iota_i : K \hookrightarrow \mathrm{End}^0(E_i)$ be the induced $K$-orientation on $E_i$. We denote $\mathcal{O}_i = \mathrm{End}(E_i) \cap \iota_i(K)$, where $\mathcal{O}_0 := \mathcal{O}_K$. Then $\iota_i$ induces an isomorphism*

$$\iota_i : \mathbb{Z} + \ell^i \mathcal{O}_K \cong \mathcal{O}_i.$$

*Proof.* We know that $\mathcal{O}_1$ has index $\ell$ in $\mathcal{O}_K$, by Proposition 7.7, and similarly $\mathcal{O}_{i+1}$ has index $\ell$ in $\mathcal{O}_i$. By the multiplicativity of the index this implies that

$$[\mathcal{O}_K : \mathcal{O}_i] = [\mathcal{O}_K : \mathcal{O}_1] \cdot [\mathcal{O}_1 : \mathcal{O}_2] \cdots [\mathcal{O}_{i-1} : \mathcal{O}_i] = \ell^i.$$

For imaginary quadratic fields it holds that the conductor of an order $\mathcal{O}$ equals its index in the ring of integers, i.e. it equals $[\mathcal{O}_K : \mathcal{O}]$. In particular this implies that $\mathcal{O}_i = \mathbb{Z} + [\mathcal{O}_K : \mathcal{O}_i]\mathcal{O}_K$, so $\mathcal{O}_i = \mathbb{Z} + \ell^i \mathcal{O}_K$. □

Next we will introduce the concept of *isogeny ladders*. We use the same notation as in Theorem 7.12. Let $q$ be prime (in $\mathbb{Z}$) different from $p$ and $\ell$ that splits in $\mathcal{O}_K$. Let $\mathfrak{q}$ be a prime over $q$ in $\mathcal{O}_K$. Set $\mathfrak{q}_i = \iota_i(\mathfrak{q}) \cap \mathcal{O}_i$. We define

$$C_i := E_i[\mathfrak{q}_i] = \{P \in E_i[q] \mid \psi(P) = 0 \quad \forall \psi \in \mathfrak{q}_i\}.$$

Define $F_i := E_i/C_i$ and let $\psi_i : E_i \to F_i$ be an isogeny of degree $q$. Suppose that we have an $\ell$-isogeny chain $(E_i, \phi_i)$ and $q$-isogenies $\psi_i$ as defined. Then for all $i$ there is a unique $\phi_i' : F_i \to F_{i+1}$ with kernel $\psi_i(\ker(\phi_i))$ such that the following diagram commutes.

$$\begin{array}{ccc} E_i & \xrightarrow{\phi_i} & E_{i+1} \\ \downarrow{\scriptstyle \psi_i} & & \downarrow{\scriptstyle \psi_{i+1}} \\ F_i & \xrightarrow{\phi_i'} & F_{i+1} \end{array}$$

Furthermore, because the diagram commutes and $\psi_i$ have degree $q$ and $\phi_i$ have degree $\ell$, we know that the isogenies $\phi_i'$ all have degree $\ell$ too.

**Definition 7.13.** An *$\ell$-ladder of degree $q$* is a commutative diagram of $\ell$-isogeny chains $(E_i, \phi_i)$ and $(F_i, \phi_i')$ of length $n$ connected by $q$-isogenies $(\psi_i : E_i \to F_i)$.

$$\begin{array}{ccccccccc} E_0 & \xrightarrow{\phi_0} & E_1 & \xrightarrow{\phi_1} & E_2 & \xrightarrow{\phi_2} & \cdots & \xrightarrow{\phi_{n-1}} & E_n = E \\ \downarrow{\scriptstyle \psi_0} & & \downarrow{\scriptstyle \psi_1} & & \downarrow{\scriptstyle \psi_2} & & & & \downarrow{\scriptstyle \psi_n} \\ F_0 & \xrightarrow{\phi_0'} & F_1 & \xrightarrow{\phi_1'} & F_2 & \xrightarrow{\phi_2'} & \cdots & \xrightarrow{\phi_{n-1}'} & F_n = F \end{array}$$

We say that the ladder is *ascending* if $(E_i, \phi_i)$ is ascending and similarly we call it *descending* or *horizontal* if the chain $(E_i, \phi_i)$ is descending, respectively horizontal. We say the ladder is *level* if $\psi_0$ is a horizontal $q$-isogeny.

**Remark 7.14.** Note that given an $\ell$-isogeny chain of length $n$ where $E_0$ has an orientation on it, the choice of an isogeny $\psi_0 : E_0 \to F_0$ for some curve $F_0$ gives a unique choice for all other $\psi_i$ and all $F_i$, since the kernels of the $\psi_i$ are given by $E_i[\mathfrak{q}_i]$. Here we define $\mathfrak{q}_i = \iota_i(\mathfrak{q}) \cap \mathrm{End}(E_i) \cap \iota_i(K)$. This way, given an $\ell$-isogeny chain of length $n$ where $E_0$ is oriented by some order in $K$, we can *push forward* an isogeny $\psi_0$ to an $\ell$-ladder of length $n$.

**Lemma 7.15.** *An $\ell$-ladder $\psi : (E_i, \phi_i) \to (F_i, \phi_i')$ of oriented elliptic curves is level if and only if* $\mathrm{End}((E_i, \iota_i))$ *is isomorphic to* $\mathrm{End}(F_i, \iota_i')$ *for all* $0 \leqslant i \leqslant n$. *In particular, if the $\ell$-ladder is level, then $(E_i, \phi_i)$ is descending (or ascending, or horizontal) if and only if $(F_i, \phi_i')$ is descending (or ascending, or horizontal).*

*Proof.* This is stated in [31, Lemma 6]. □

In [31] the authors state that the class group of an order $\mathcal{O}$ acts transitively and freely on the set of $K$-isomorphism classes of primitive $\mathcal{O}$-oriented supersingular elliptic curves. This set is denoted by $\mathrm{SS}_{\mathcal{O}}^{pr}(p)$. In [32] it was shown that this claim had to be slightly modified. The author proved the following Theorem 7.17.

To understand the Theorem we will first say something about *reductions*. We do not want to go into detail about the subjects used here. For more information on the subject we refer to [33, Section II.1]. Let $L$ be a number field containing $K = \mathbb{Q}(\sqrt{d})$ for some $d < 0$. Let $E$ be an elliptic curve over $L$ with $\mathrm{End}(E) \cong \mathcal{O}$, where $\mathcal{O}$ is an order in $K$. Let $[\cdot]_E : \mathcal{O} \to \mathrm{End}(E)$ be an isomorphism such that $(E, [\cdot]_E)$ is normalized, i.e., for any invariant differential $\omega$ on E,

$$([\alpha]_E)^*\omega = \alpha\omega \quad \forall \alpha \in \mathcal{O}.$$

Let $\mathfrak{p}$ be a prime ideal of $L$ lying above a prime $p$ at which $E$ has good reduction. A pair $(E, [\cdot]_E)$ determines a $K$-oriented elliptic curve $(\tilde{E}, [\cdot]_{\tilde{E}})$ by the reduction modulo $p$ where $[\cdot]_{\tilde{E}} : K \to \mathrm{End}_0(\tilde{E})$ is defined by

$$[\alpha]_{\tilde{E}} = [\alpha]_E \bmod p \quad \forall \alpha \in \mathcal{O}.$$

The above can be found in [32, Section 3.3.2].

**Definition 7.16.** We define $\mathcal{J}_{\mathcal{O}}$ as the set of $j$-invariants of elliptic curves over $\mathbb{C}$ with $\mathrm{End}(E) \cong \mathcal{O}$.
We let $L$ be a number field and $\mathfrak{p}$ be a prime ideal of $L$ lying above a prime $p$ such that for all $j \in \mathcal{J}_{\mathcal{O}}$ there exists an elliptic curve over $L$ whose $j$-invariant is $j$ and which has good reduction at $\mathfrak{p}$.
We define $Ell(\mathcal{O})$ as the set of isomorphism classes of all elliptic curves $E$ over $L$

such that $j(E) \in \mathcal{J}_{\mathcal{O}}$ and $E$ has good reduction at $\mathfrak{p}$.
We define the reduction modulo $\mathfrak{p}$ map as

$$\rho : Ell(\mathcal{O}) \to \mathrm{SS}_{\mathcal{O}}^{pr}(p) \quad \text{by} \quad E \mapsto (\tilde{E}, [\cdot]_{\tilde{E}}).$$

**Theorem 7.17.** *Let $K$ be an imaginary quadratic field such that $p$ does not split in $K$, and let $\mathcal{O}$ be an order in $K$ such that $p$ does not divide the conductor of $\mathcal{O}$. Then the ideal class group $\mathrm{Cl}(\mathcal{O})$ acts freely and transitively on $\rho(Ell(\mathcal{O}))$.*

*Proof.* The proof is given in [32, Theorem 3.4]. □

**Proposition 7.18.** *For all $(F, \iota) \in \mathrm{SS}_{\mathcal{O}}^{pr}(p)$ we have*

$$(F, \iota) \in \rho(Ell(\mathcal{O})) \quad \text{or} \quad (F^{(p)}, \iota^{(p)}) \in \rho(Ell(\mathcal{O})).$$

*Proof.* The proof is given in [32, Proposition 3.3]. □

Proposition 7.18 tells us that $\rho$ is surjective up to the $p$-th power Frobenius map, hence the class group $\mathrm{Cl}(\mathcal{O})$ acts transitively and freely on $\mathrm{SS}_{\mathcal{O}}^{pr}(p)$ up to the $p$-th power Frobenius map.

**Example 7.19.** We consider an elliptic curve $E$ over the finite field $\mathbb{F}_{59}$, with $j(E) = 0$. By Example V.4.4 of [5], we know that an elliptic curve with $j$-invariant 0 is supersingular if and only if $\mathrm{char}(k) \equiv 2 \bmod 3$, therefore the elliptic curve we chose is supersingular. By [34, p.11] we have that

$$\mathrm{End}(E) \cong \mathbb{Z} + \mathbb{Z}\left[\frac{1+i}{2}\right] + \mathbb{Z}[j] + \mathbb{Z}\left[\frac{3+i+3j+k}{6}\right],$$

where $i^2 = -3$, $j^2 = -59$ and $ij = k = -ji$. We let $K = \mathbb{Q}(\sqrt{-3})$ and since $-3 \equiv 1 \bmod 4$, we have that the ring of integers of $K$ equals

$$\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right].$$

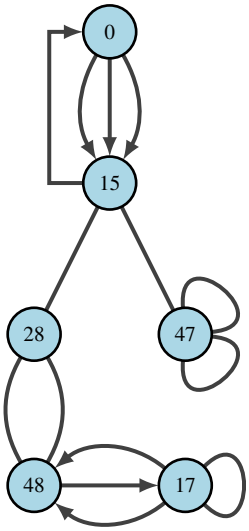
We define a $\mathbb{Q}(\sqrt{-3})$-orientation on $E$ by

$$\iota : \mathbb{Q}(\sqrt{-3}) \hookrightarrow \mathrm{End}(E) \otimes \mathbb{Q} \quad \text{where} \quad a + b\iota(\sqrt{-3}) = a + bi.$$

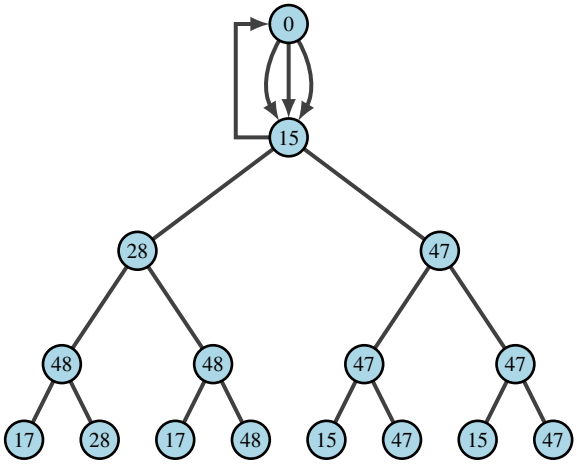
We define $\zeta_3 := \frac{1+\sqrt{-3}}{2}$, note that

$$\iota(\mathbb{Z}[\zeta_3]) = \mathrm{End}(E) \cap \iota(\mathbb{Q}(\sqrt{-3})).$$

Therefore $E$ has a primitive $\mathbb{Z}[\zeta_3]$-orientation, given by $\iota$. For a cube root of unity $\zeta_3$, we know that $\mathbb{Z}[\zeta_3]$ has class number 1. We already constructed the isogeny graph $G(59, 2)$ in Example 5.6 in Section 5. It looks as follows:




We can view the possible 2-isogeny chains by considering paths in the supersingular isogeny graph $G(2, 59)$. The descending 2-isogeny chains starting at the vertex $j = 0$ and having length 4 can be illustrated as below. We let the edges between 0 and 15 be as in the isogeny graph, since the graph is not 2-regular at these vertices. This way we obtain a tree structure:




We know that for a primitve $p^k$-th root of unity, a prime $q \neq p$ splits (and is unramified) in $\mathbb{Z}[\zeta_n]$. We choose the following 2-isogeny chain from the graph: $[0, 15, 28, 48, 17]$. We choose a prime ideal over the split prime 7 in $\mathbb{Z}[\zeta_3]$, we denote it by $\mathfrak{p}_7$. We will consider the action of this prime ideal on the given 2-isogeny chain, in order to construct a 2-isogeny ladder. To construct such a ladder

we can use the so called *modular polynomials*, as introduced in Chapter 5. Since the class number of $\mathbb{Z}[\zeta_3]$ equals 1, the ladder will look like:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & 15 & \longrightarrow & 28 & \longrightarrow & 48 & \longrightarrow & 17 \\ \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & F_1 & \longrightarrow & F_2 & \longrightarrow & F_3 & \longrightarrow & F_4. \end{array}$$

For $F_1$ we solve

$$\Phi_2(0,X) = 0 \quad \text{and} \quad \Phi_7(15,X) = 0.$$

Subsequently we solve

$$\Phi_2(F_1,X) = 0 \quad \text{and} \quad \Phi(28,X) = 0.$$

Continuing like this, we can construct a ladder. At $F_2$, we have two options, corresponding to the $j$-invariants 47 and 28. Depending on how we chose $\mathfrak{p}_7$ (i.e. whether it is principal here or not), we will go along to either one of the two $j$-invariants. Suppose that we chose $\mathfrak{p}_7$ such that $F_2 = 47$. Solving the subsequent systems of equations, we obtain the following ladder

$$\begin{array}{ccccccccc} 0 & \longrightarrow & 15 & \longrightarrow & 28 & \longrightarrow & 48 & \longrightarrow & 17 \\ \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & 15 & \longrightarrow & 47 & \longrightarrow & 47 & \longrightarrow & 15. \end{array}$$

## 7.2 Oriented Supersingular Isogeny Diffie-Hellman (OSIDH)

Oriented Supersingular Isogeny Diffie-Hellman, abbreviated as OSIDH, is a key exchange protocol that uses oriented supersingular elliptic curves. This protocol uses $\ell$-isogeny ladders, as were defined in the previous section. We will first look at an obvious, but insecure, way to construct a key exchange protocol using oriented supersingular elliptic curves. After this we will look at the actual OSIDH protocol.

### 7.2.1 Preliminaries

We will first try to construct a key exchange protocol using orientations in a simple manner.

The setup is as follows: Alice and Bob choose a descending $\ell$-isogeny chain

$$E_0 \to E_1 \to \cdots \to E_n,$$

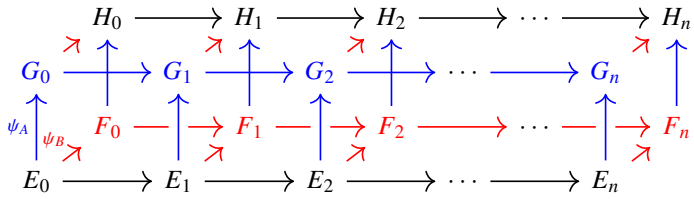
where $E_0$ has an $\mathcal{O}_K$-orientation. This information is public. Additionally they both choose a secret endomorphism of smooth degree of $E_0$, denoted by $\psi_A$ for Alice and $\psi_B$ for Bob.
In the protocol they will both build a ladder on the given $\ell$-isogeny chain using the secret isogeny $\psi_A$ and $\psi_B$. Therefore Alice obtains

$$\begin{array}{ccccccccc} E_0 & \xrightarrow{\phi_0} & E_1 & \xrightarrow{\phi_1} & E_2 & \xrightarrow{\phi_2} & \cdots & \xrightarrow{\phi_{n-1}} & E_n \\ \downarrow{\scriptstyle \psi_A} & & \downarrow & & \downarrow & & & & \downarrow \\ F_0 & \xrightarrow{\phi_{A,0}} & F_1 & \xrightarrow{\phi_{A,1}} & F_2 & \xrightarrow{\phi_{A,2}} & \cdots & \xrightarrow{\phi_{A,n-1}} & F_n, \end{array}$$

in this ladder everything that is colored red is known only to Alice. Bob obtains

$$\begin{array}{ccccccccc} E_0 & \xrightarrow{\phi_0} & E_1 & \xrightarrow{\phi_1} & E_2 & \xrightarrow{\phi_2} & \cdots & \xrightarrow{\phi_{n-1}} & E_n \\ \downarrow{\scriptstyle \psi_A} & & \downarrow & & \downarrow & & & & \downarrow \\ G_0 & \xrightarrow{\phi_{B,0}} & G_1 & \xrightarrow{\phi_{B,1}} & G_2 & \xrightarrow{\phi_{A,2}} & \cdots & \xrightarrow{\phi_{A,n-1}} & G_n, \end{array}$$

in this ladder everything that is colored blue is known only to Bob. Now they will exchange their complete $\ell$-isogeny chain, i.e. Alice sends $(F_i, \phi_{A,i})$ to Bob and Bob sends $(G_i, \phi_{B,i})$ to Alice. After the exchange they will both apply their own secret isogeny, $\psi_A$ and $\psi_B$, to the ladder they obtained. That will give them both a new $\ell$-isogeny chain and the chains they obtain will be the same since the class group of an order in an imaginary quadratic field is commutative. Denoting the final $\ell$-isogeny chain by $(H_i)$ we can illustrate the protocol in a diagram as follows:




Here the red colours still denote the isogenies that belong to Alice and the blue ones the ones that belong to Bob. It is clear that Alice and Bob will share a (secret) curve $H_n$ in the end. However, in this protocol they share a lot of information, namely their constructed ladders. It is shown in [31, Section 5.1] that this is too much information as it renders the protocol insecure. Note that if the isogeny, denote it by $\psi$, between $E_n$ and $F_n$ is known to some adversary, then the adversary can compute $G_n/\ker(\psi)$ to obtain $H_n$, since the class group is commutative. This would leak the secret key.

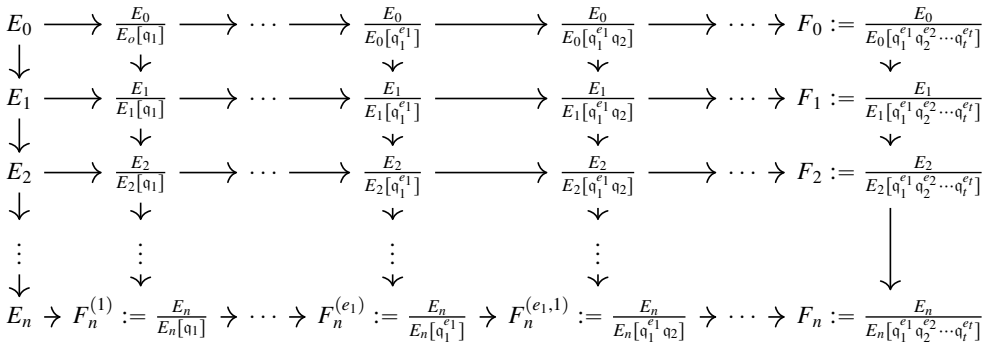
The authors show that it is feasible for an adversary to compute such an isogeny between $E_n$ and $F_n$. For the details we refer to [31, Section 5.1], but the idea is as follows; by sharing the full isogeny chains $(E_i)$ and $(F_i)$, it is possible to compute the endomorphism rings $\mathrm{End}(E_n)$ and $\mathrm{End}(F_n)$. It is believed that computing an isogeny between supersingular elliptic curves $E_n \to F_n$ while knowing $\mathrm{End}(E_n)$ is broadly equivalent to computing $\mathrm{End}(F_n)$. This is the case since, as described in Section 5.3.1, we can identify supersingular elliptic curves and isogenies between them with left $\mathrm{End}(F_n)$-ideals. Therefore, the protocol as described in this section gives away too much information. In the next section we will see how to construct a protocol where Alice and Bob don't have to share their full isogeny chains.

### 7.2.2 The protocol

We will now introduce the actual OSIDH protocol. As mentioned, the problem with the previous protocol lies in the fact that Alice and Bob both share their full $\ell$-isogeny chains. If we make some adjustments to the set-up, it turns out that they can use a similar method where they do not have to share the full chains and can securely arrive at the same secret curve/key.

The set-up is as follows: Alice and Bob agree on an imaginary quadratic field $K$ and on a descending $\ell$-isogeny chain $E_0 \to E_1 \to E_2 \to \cdots \to E_n$ where $E_0$ has an $\mathcal{O}_K$-orientation. They also agree on prime ideals $\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_t$ in $\mathrm{End}(E_n) \cap K$

that split in $\mathcal{O}_K$ and lie over primes $q_1, q_2, \ldots, q_t$, respectively. Then Alice picks a secret key $(e_1, e_2, \ldots, e_t)$ where $e_i \in [-r, r]$ for some $r$ that is known to both. Bob picks a secret key $(d_1, d_2, \ldots, d_t)$ with $d_i \in [-r, r]$. They both construct a ladder, this time the ladder is a lot bigger than in the previous section. For Alice, the ladder looks as follows:



We can view the isogeny from $E_0$ to $F_0$, denoted by $\psi_{A,0}$, as the analogue of the secret isogeny $\psi_A$ in the previous protocol, since the $e_i$ are secret. Note that we choose $\mathfrak{q}_i$ to be in $\mathrm{End}(E_n) \cap K =: \mathcal{O}_n$ and that $\mathcal{O}_i \supsetneq \mathcal{O}_{i+1}$ since we have a descending chain. Therefore all $\psi \in \mathfrak{q}_i$ are endomorphisms of all $E_j$, for all $i$ and for all $j$. Bob constructs a similar ladder using his secret key $(d_1, \ldots, d_t)$, arriving at some curve $G_n := \frac{E_n}{E_n[\mathfrak{q}_1^{d_1} \cdots \mathfrak{q}_t^{d_t}]}$. Alice and Bob will share their final curves $F_n$ and $G_n$, *without* orientation. They will build another ladder on top of this curve using their own secret keys again. However, since they haven't shared their full ladder this time, they do not know with which isogeny to build the ladder (there are $q_i + i$ isogenies of degree $q_i$). This happens since they don't know the chosen orientation on the final curve $F_n$ and $G_n$. Of course both Alice and Bob know the orientation $\iota_0$ on $E_0$, but Alice chooses some secret isogeny $\psi_{A,0} : E_0 \to F_0$ and Bob chooses some secret isogeny $\psi_{B,0} : E_0 \to G_0$. This makes that every isogeny $\psi_{A,i} : E_i \to F_i$ and $\psi_{B,i} : E_i \to G_i$ is secret. The orientation on $F_n$ is given by

$$\frac{1}{\deg(\psi_{A,n})} \psi_{A,n} \circ \iota_n \circ \widehat{\psi_{A,n}},$$

where $\iota_n$ is the induced orientation, by $\iota_0$ on $E_0$, on $E_n$. Hence the orientation on the final curves is secret and Alice and Bob need to share some more information

to get to the same curve in the end, however they should not share the full ladder as we have seen in the previous section.

Theoretically, there is not really a difference between computing all the intermediate steps/ladders and computing just the final ladder $(F_i)$. However, in [32, Assumption 5.1] and [32, Theorem 6.2] it is shown that to construct a ladder $((E_i,\ \phi_i),\ \psi_i,\ (F_i, \phi_i'))$ we can compute

$$\gcd(\Phi_\ell(X, j(E_{i+1})), \Phi_q(X, j(F_i))) = 0$$

for all $i$. For this we assume that $q$ is a prime, but if we would want to compute the final ladder at once we would have a power of $q$, which is not prime. Moreover, the larger $q$ becomes, the more difficult the modular polynomial $\Phi_q$ will be to calculate.

Note that to construct the ladder, Alice chose some $\psi_{A,0} : E_0 \to F_0$. However, she does not share this isogeny with Bob. Similarly, Bob chose some isogeny to push forward his ladder and did not share this isogeny with Alice. They also shouldn't share these isogenies since that would reveal the ladder. However, it is secure for Alice and Bob to share the following information: using the isogeny they used to push forward their own ladder, they can continue to compute

$$F_{n,i}^{(j)} := \frac{E_n}{E_n[\mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_i^{e_i+j} \cdots \mathfrak{q}_t^{e_t}]} \quad \text{and} \quad G_{n,i}^{(j)} := \frac{E_n}{E_n[\mathfrak{q}_1^{d_1} \cdots \mathfrak{q}_i^{d_i+j} \cdots \mathfrak{q}_t^{d_t}]}.$$

They will compute these values for all $i \in \{1, \ldots, t\}$ and for all $j \in [-r, r]$. Then they will send these to the other party. Now Alice can use her secret key to take the correct amount of steps in the direction of each $\mathfrak{q}_i$, as illustrated in Figure 7. In this figure $e_1 < 0$ and $e_2 > 0$.

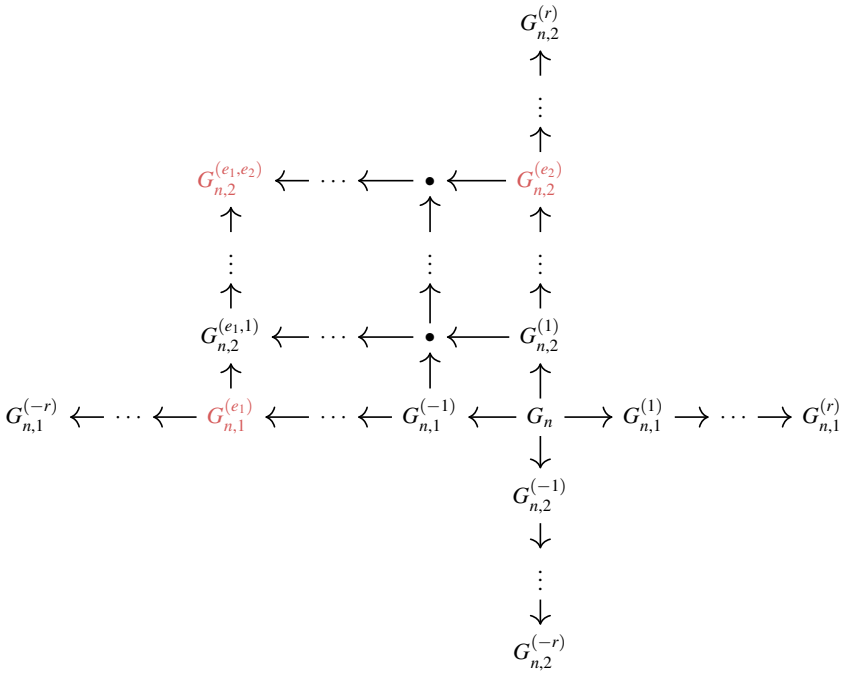



Figure 7: How Alice finds $G_{n,2}^{(e_1,e_2)}$

Continuing like this, Alice will end up with the following curve

$$\frac{G_n}{G_n[\mathfrak{q}_1^{e_1}\cdots\mathfrak{q}_t^{e_t}]} = \frac{E_n}{E_n[\mathfrak{q}_1^{e_1+d_1}\cdots\mathfrak{q}_t^{e_t+d_t}]} =: H_n.$$

Bob will do the same thing with his own secret key and the directions that he got from Alice. In the end he will also end up with the curve

$$\frac{F_n}{F_n[\mathfrak{q}_1^{d_1}\cdots\mathfrak{q}_t^{d_t}]} = \frac{E_n}{E_n[\mathfrak{q}_1^{e_1+d_1}\cdots\mathfrak{q}_t^{e_t+d_t}]} = H_n.$$

Therefore, after carrying out the protocol, Alice and Bob end up with the same (secret) curve $H_n$. We can summarize these steps in the following protocol:
For a discussion of the parameters and security considerations of OSIDH, we refer to [31].

Oriented Supersingular Isogeny Diffie-Hellman (OSIDH)

**Public parameters** : A descending $\ell-$isogeny chain :
$E_0 \to E_1 \to \cdots \to E_n$.
A set of splitting primes :
$\mathfrak{q}_1, \mathfrak{q}_2 \cdots \mathfrak{q}_t \subseteq \text{End}(E_n) \cap K$.

| **Alice** | | **Bob** |
|---|---|---|
| $(e_1, \ldots, e_t)$ | | $(d_1, \ldots, d_t)$ |
| $F_n := \dfrac{E_n}{E_n[\mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_t^{e_t}]}$ | | $G_n := \dfrac{E_n}{E_n[\mathfrak{q}_1^{d_1} \cdots \mathfrak{q}_t^{d_t}]}$ |
| $F_n \to F_{n,i}^{(1)} \to \cdots \to F_{n,i}^{(r)}$ | | $G_n \to G_{n,i}^{(1)} \to \cdots \to G_{n,i}^{(r)}$ |
| $F_n \to F_{n,i}^{(-1)} \to \cdots \to F_{n,i}^{(-r)}$ | | $G_n \to G_{n,i}^{(-1)} \to \cdots \to G_{n,i}^{(-r)}$ |
| | $\xrightarrow{F_n - \text{directions}}$ | |
| | $\xleftarrow{G_n - \text{directions}}$ | |
| Take $e_i$ steps in $\mathfrak{q}_i-$isogeny chain and push forward information $\forall j > i$ | | Take $d_i$ steps in $\mathfrak{q}_i-$isogeny chain and push forward information $\forall j > i$ |
| **Output** : $\dfrac{G_n}{G_n[\mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_t^{e_t}]} = H_n$ | | **Output** : $\dfrac{F_n}{F_n[\mathfrak{q}_1^{d_1} \cdots \mathfrak{q}_t^{d_t}]} = H_n$ |

Figure 8: An illustration of OSIDH

### 7.2.3 Relation to SIDH

OSIDH is based loosely on SIDH. Recall that in SIDH, Alice and Bob perform (roughly) the three following steps

- They construct secret isogenies to curves $E_A$ (for Alice) and $E_B$ (for Bob).
- They exchange the curves $E_A$ and $E_B$ plus some additional information (i.e. the secret isogenies applied on a generator of the basis of the $\ell_1$ and $\ell_2$ torsion points).
- Using the exchanged information, Alice and Bob are able to apply their own secret isogeny and arrive at the same (secret) curve.

Looking at OSIDH in the same way, we see a lot of similarities in the protocol. We can roughly distinguish the following three steps in OSIDH:

- Alice and Bob choose secret isogenies ($\psi_{A,0}$ and $\psi_{B,0}$) and using a ladder

construction they end up at the (oriented) curves $F_n$ (for Alice) and $G_n$ (for Bob).

- They exchange the (unoriented) curve $F_n$ and $G_n$ plus some additional information (i.e., the $F_n$-directions and $G_n$-directions).
- Using the exchanged information, Alice and Bob are able to apply their own secret keys to get to the same (secret) curve.

The methods look quite similar; the curves $E_A$ and $F_n$ and the isogenies to them, are both obtained by choosing some secret kernel. However, there is some extra structure in OSIDH due to the composition of isogenies and the orientations on the curves. In OSIDH, we do not have to rely on a basis for certain torsion groups and therefore also not on computations on the basis. Another difference is that since we consider imaginary quadratic fields, the class groups we consider in OSIDH are commutative, whereas the ones in SIDH are not.

Overall, SIDH and OSIDH are quite similar, this fact gives rise to the question if we could do something similar for SQISign, i.e., can we build a $\Sigma$-protocol (based on SQISign) that uses orientations? We will look at this in the next section.

## 7.3 Orientations and Σ-protocols

### 7.3.1 Σ-protocol in SQISign

In this section we will try to construct a Σ-protocol that looks like SQISign and uses orientations. Recall the Σ-protocol for SQISign from Section 6.5.

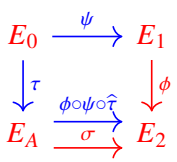
**Parameters:** The setup of the scheme is as follows. A prime $p$ is chosen and then a supersingular elliptic curve $E_0$ over $\mathbb{F}_p$ with special extremal endomorphism ring $\mathcal{O}_0$ is chosen. We choose $D_c$ to be an odd smooth number of $\lambda$ bits and $D = 2^e$ where $e$ is above the diameter of the supersingular 2-isogeny graph. The prover wants to prove knowledge of a secret $\tau$.

**Key generation:** The key pair, consisting of a public key and a secret key, is generated as follows. A random isogeny walk starting at $E_0$ is chosen. This isogeny walk is denoted by $\tau$ and ends at some vertex corresponding to an elliptic curve $E_A$. The public key is the curve $E_A$ and the secret key is the isogeny $\tau$, i.e. the key pair is $(\mathsf{pk}, \mathsf{sk}) = (E_A, \tau)$.

**The protocol:**

- First the Prover $P$ picks a random (secret) $\psi : E_0 \to E_1$. It sends $E_1$ to the Verifier $V$.
- The Verifier $V$ picks a cyclic isogeny $\phi : E_1 \to E_2$ of degree $D_c$ and sends a description of $\phi$ to $P$.
- The prover $P$ constructs from $\phi \circ \psi \circ \widehat{\tau} : E_A \to E_2$ some new isogeny $\sigma : E_A \to E_2$ of degree $D$ such that $\widehat{\phi} \circ \sigma$ is cyclic.
- The Verifier $V$ accepts when $\sigma$ is an isogeny from $E_A \to E_2$ of degree $D$ and $\widehat{\phi} \circ \sigma$ is cyclic.

The protocol can be illustrated as the diagram below. Here the red parts denote public information and the blue ones secret information. Note that $\sigma \neq \phi \circ \psi \circ \widehat{\tau}$.



### 7.3.2 New 3-move protocol using orientations

**Remark 7.20.** Note that we know that a curve $E_0$, as in the $\Sigma$-protocol for SQISign, has an element $\pi$ in its endomorphism ring such that $\pi^2 = -p$, i.e. there is an element that acts as the square root of $-p$. In particular this implies that there is an embedding

$$\mathbb{Q}(\sqrt{-p}) \hookrightarrow \mathrm{End}^0(E_0)$$

and

$$\mathbb{Z}[\sqrt{-p}] \hookrightarrow \mathrm{End}(E_0).$$

Therefore $E_0$ has a $\mathbb{Q}(\sqrt{-p})$-orientation and a $\mathbb{Z}[\sqrt{-p}]$-orientation.

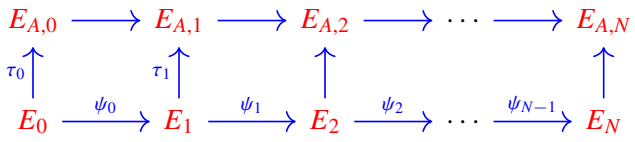
The fact that there is such an orientation allows us to construct $\ell$-isogeny chains and ladders starting at $E_0$.

We will now illustrate an attempt at a $\Sigma$-protocol. The setup is as follows: Let $E_0$ be a supersingular elliptic curve with special extremal endormorphism ring, then by Remark 7.20 we know that $E_0$ has a $\mathbb{Z}[\sqrt{-p}]$-orientation. The key generation algorithm outputs a (secret) isogeny $\tau_0 : E_0 \to E_{A,0}$, where $E_{A,0}$ is public, so the public key is $E_{A,0}$ and the secret key is $\tau_0$. The 3-step protocol looks as follows:

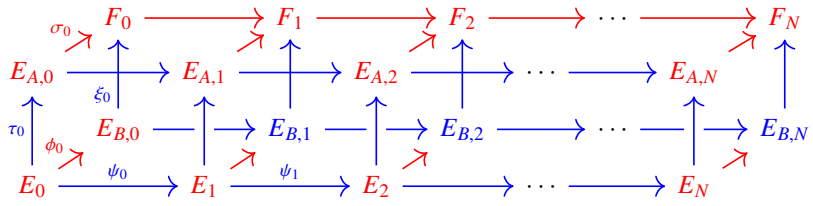
- The prover constructs an $\ell$-isogeny chain starting at $E_0$

  $$E_0 \xrightarrow{\psi_0} E_1 \xrightarrow{\psi_1} E_2 \xrightarrow{\psi_2} \cdots \xrightarrow{\psi_{N-1}} E_N.$$

  The prover constructs a ladder on this chain, using the secret isogeny $\tau_0$. It will send $E_{A,i}$ and $E_i$ for all $i$ to the verifier.




- The verifier will output a random isogeny $\phi_0 : E_0 \to E_{B,0}$, where $E_{B,0}$ is some supersingular elliptic curve. It will send both $\phi_0$ and $E_{B,0}$ to the prover.
- The prover can construct a ladder on the chain $(E_i, \psi_i)$ using the isogeny $\phi_0$ from the verifier. It can build isogenies $\xi_i : E_{B,i} \to F_i$ and $\sigma_i : E_{A,0} \to F_i$ using the given information, in such a way that we obtain a commutative diagram as below.




Note that the choice for $F_i$ and $\xi_i$ and $\sigma_i$ is unique, since we can view the diagram below as a ladder of length 2 that comes from the isogeny chain $E_i \rightarrow E_{B,i}$ and the isogeny $\tau_i$. The prover sends the $F_i$, all isogenies between the $F_i$ and $F_{i+1}$ and the isogenies $\sigma_i$ for all $i$ to the verifier.

$$\begin{array}{ccc} E_i & \xrightarrow{\phi_i} & E_{B,i} \\ \downarrow{\scriptstyle \tau_i} & & \downarrow{\scriptstyle \xi_i} \\ E_{A,i} & \xrightarrow{\sigma_i} & F_i, \end{array}$$

The verifier checks whether all $\sigma_i$ are indeed maps from $E_{A,i}$ of $\deg(\sigma_i) = \deg(\phi_i) = \deg(\phi_0)$. In the diagrams all red colored symbols are public/shared and the blue ones are secret.

**Remark 7.21.** First note that the protocol satisfies correctness, since the verifier will always accept when the prover indeed knows $\tau_0$, since it will be able to construct proper $\sigma_i$.
Note that if we don't require the isogenies between the $F_i$ to be sent, a malicious prover could compute a subgroup of $E_{A,i}$ with $\deg(\phi_i)$ elements and then use Vélu to construct an isogeny starting at $E_{A,0}$ with proper degree. This isogeny probably doesn't give the commutative diagram, hence we need a means for the verifier to be able to check the commutativity.

But, if we require the prover to send the full $\ell$-isogeny chain $(F_i)$ (as we did in the protocol) to the verifier, the prover doesn't get away with the method from Remark 7.21, since he will also have to find degree $\ell$ isogenies between all $F_i$ and $F_{i+1}$, which is generally not easy.

This method looks a lot like SQISign, but here the prover doesn't need an algorithm to mask $\xi_i \circ \phi_i \circ \widehat{\tau}_i$, since we simply don't need to share $\xi_i$. That is solved by sending the $\ell$-isogeny chain $F_i$, which seems difficult to construct for anyone that doesn't actually know $\tau_0$. Also, we do not require the cyclicity conditions anymore. This is possible because of the commutativity of the diagram constructed in the protocol.

**Remark 7.22.** Note that in this protocol we do not actually need to have a supersingular elliptic curve with a special extremal endomorphism ring. In fact, it suffices to choose $E_0$ to be any supersingular elliptic curve that has an $\mathcal{O}$-orientation on it. For example, we could choose $E/\mathbb{F}_{p^2}$ with $j(E) = 0$ and $p \equiv 2 \bmod 3$, this has a (primitive) $\mathbb{Z}[\zeta_3]$-orientation or we could choose $E/\mathbb{F}_{p^2}$ with $j(E) = 1728$ and $p \equiv 3 \bmod 4$, which has a (primitive) $\mathbb{Z}[i]$-orientation. Generally, this is also how the initial curves in OSIDH are chosen. This makes the suggested protocol generally more applicable.

### 7.3.3 Properties of Σ-protocols

The described protocol satisfies the basic properties of a Σ-protocol, however, for it to actually be a Σ-protocol it needs to satisfy *correctness, special soundness* and *special honest verifier zero-knowledge* as described in Definition 6.4. Up to now, we know that it satisfies correctness, but special soundness and special honest verifier zero-knowledge remain to be proven.

The *correctness* of the described protocol follows in the same way that Alice and Bob arrive at the same curve in the section "First naive protocol" in [31], which is described in subsection 7.2.1. The idea is as follows: if the prover actually knows $\tau_0$, it can use it to push it forward on some ladder and he will obtain isogenies $\tau_i$'s to curves $E_{A,i}$'s. Subsequently, using $\phi_0$ on the same ladder, he obtains another ladder: $(E_{B,i})$. By the commutativity of the class group, using $\tau_0$ on $E_{B,0}$ and $\phi_0$ on $E_{A,0}$, he will get a unique curve $F_0$. The same holds for the other $F_i$. The maps $\sigma_i : E_{B,i} \to F_i$ will have $\deg(\sigma_i) = \deg(\phi_0)$ by construction and the constructed ladder $(F_i)$ with isogenies $\rho_i$ will satisfy $\deg(\rho_i) = \ell$ by construction as well. Therefore the verfier will output *accept* everytime the prover follows the protocol and actually knows $\tau_0$.

The other two properties are *special soundness* and *special honest verifier zero-knowledge*. Recall the definitions:

- *Special soundness:* There exists a polynomial time algorithm $\mathcal{E}$ (also called the *extractor*) such that on input of two accepting transcripts $(a, c, z)$ and $(a, c', z')$ for $x$ with $c \neq c'$, outputs a witness $\tilde{w}$ such that $(x, \tilde{w}) \in R$.

- *Special honest verifier zero-knowledge:* There exists a PPT algorithm Sim such that on input of $x$, Sim outputs a transcript $(\tilde{a}, \tilde{c}, \tilde{z})$ such that the transcript has the same probability distribution as the honest protocol transcript $\Pi(x; w)$.

*Special soundness* for the SQISign Σ-protocol was proven using the relation:

$$R = \{(E_A, \alpha) \ : \ \text{where } \alpha \text{ is a cyclic endomorphism of smooth degree}\}$$

and it basically relies on the assumption that the Supersingular Smooth Endomorphism Problem is hard. This problem is stated as follows:

**Problem.** (Supersingular Smooth Endomorphism Problem)
Given a prime $p$ and a supersingular elliptic curve $E/\mathbb{F}_{p^2}$, find a (non-trivial) cyclic endomorphism of $E$ of smooth degree.

However, in our protocol, the signature does not only consist of an isogeny like $\alpha$, but it consists of several isogenies $\sigma_i$ together with their target curves $F_i$ and a full description of the ladder $(F_i, \rho_i)$. Therefore we would have to define a relation of the sort

$$R = \{(E_{A,i}, \sigma_i, (F_i, \rho_i)) \ : \ \sigma_i : E_{A,i} \to F_i \text{ and } \rho_i : F_i \to F_{i+1} \text{ for } i \in \{1, \dots N\}\}.$$

This relation is quite different from the relation that is used for the SQISign Σ-protocol. Therefore we cannot simply use the method and assumption used in SQISign, but it is possible that we can use properties of isogeny ladders to prove the special soundness property.

We have not yet considered the *honest verifier zero-knowledge* property of the protocol, hence this part still needs to be researched.

### 7.3.4 Security considerations

The secret information in this protocol is the secret key: $\tau_0$. This is the information that should not be given away or leaked via the protocol. Therefore when considering the security of the protocol, we need to consider attacks that try to gain information on $\tau_0$. When considering the first attempt at a key exchange protocol using orientations, we saw that the $\ell$-isogeny chains gave away too much information, in particular they could be used to compute endomorphism rings and those could in turn be used to compute isogenies between the final curves $E$ and $F$. In the case of the protocol described above, we have

information on the endomorphism ring of $E_0$, since the orientation is known. However, an adversary will not know the endomorphism ring of $F_0$ a priori, or via isogeny chains. Therefore, the same type of attack would not work on this protocol.

This is only one of the possible attacks on the scheme. More (possible) attacks need to be considered before being able to say anything about the security.

# Appendix

## A Magma code

This is a function for finding supersingular $j$-invariants over a field with $N$ elements:

```
> J := function(N)
function> jSuperInvs := [];
function> for x in GF(N) do
function|for> if IsSupersingular(EllipticCurveFromjInvariant(x)) then
function|for|if> Include(~jSuperInvs,x);
function|for|if> end if;
function|for> end for;
function> return jSuperInvs;
function> end function;
```

Given a field with $N$ elements and an element $Y$ corresponding to the $j$-invariant of a supersingular elliptic curve over this field, this code determines which $j$-invariants it is $L$-isogenous to:

```
> R<x,y> := PolynomialRing(GF(N),2);
> PL := R!ClassicalModularPolynomial(L);
> for x in J(N) do
for> if Evaluate((Evaluate(PL, 1, GF(N)!Y)), 2, x) eq 0 then
for|if> x;
for|if> end if;
for> end for;
```

# References

[1] Denis X Charles, Kristin E Lauter, and Eyal Z Goren. *Cryptographic hash functions from expander graphs*. *Journal of CRYPTOLOGY*, 22(1):93–113, 2009.

[2] Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, and Benjamin Wesolowski. *SQISign: compact post-quantum signatures from quaternions and isogenies*. Cryptology ePrint Archive, Report 2020/1240, 2020. `https://ia.cr/2020/1240`.

[3] David Jao and Luca De Feo. *Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies*. In *Post-Quantum Cryptography*, pages 19–34. Springer Berlin Heidelberg, 2011.

[4] Sukhpal Singh Gill, Adarsh Kumar, Harvinder Singh, Manmeet Singh, Kamalpreet Kaur, Muhammad Usman, and Rajkumar Buyya. *Quantum computing: A taxonomy, systematic review and future directions*. *Software: Practice and Experience*, 52(1):66–114, 2022. `https://onlinelibrary.wiley.com/doi/abs/10.1002/spe.3039`.

[5] J.H. Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer New York, 2010.

[6] Hartshorne R. *Algebraic Geometry*. Number 52 in Graduate Texts in Mathematics. Springer New York, 1977.

[7] Jean Vélu. *Isogénies entre courbes elliptiques*. *Comptes Rendus de l'Académie des Sciences de Paris*, 273:238–241, 1971.

[8] J. Voight. *Quaternion Algebras*. Graduate Texts in Mathematics. Springer New York, 2021.

[9] William C. Waterhouse. *Abelian varieties over finite fields*. *Annales scientifiques de l'É.N.S.*, 2(4):521–560, 1969.

[10] Mike Krebs and Anthony Shaheen. *Expander Families and Cayley Graphs. A Beginner's Guide.* Oxford University Press, 2011.

[11] Schlomo Hoory, Nathan Linial, and Avi Wigderson. *Expander graphs and their applications*. *Bulletin of the American Mathematical Society*, 43(4):439–561, August 2006.

[12] Luca Trevisan. *Lecture 20: Quasirandomness of Expander Graphs*. U.C. Berkeley, April 2016. https://lucatrevisan.github.io/expanders2016/lecture20.pdf.

[13] Luca de Feo. *Mathematics of Isogeny Based Cryprography*. Université Paris Saclay, November 2017. https://arxiv.org/abs/1711.04062.

[14] Luca de Feo. *Isogeny graphs in Cryptography*. Graph Theory Meets Cryptography. Université Paris Saclay, August 2019. http://defeo.lu/wurzburg/wurzburg.pdf.

[15] Alexander Rostovtsev and Anton Stolbunov. *Public-key cryptosystem based on isogenies*. Cryptology ePrint Archive, Report 2006/145, 2006. https://ia.cr/2006/145.

[16] M. Childs, David Jao, and Vladimir Soukharev. *Constructing elliptic curve isogenies in quantum subexponential time*. *J. Mathematical Cryptology*, 8(1):1–29, 2014. https://arxiv.org/abs/1012.4019.

[17] Andrew Sutherland. *Isogeny volcanoes*. *The Open Book Series*, 1(1):507–530, nov 2013.

[18] Gora Adj, Omran Ahmadi, and Alfred Menezes. *On the isogeny graphs of supersingular elliptic curves over finite fields*. *Finite Fields and their Applications*, 55:268–283, 2019. https://doi.org/10.1016/j.ffa.2018.10.002.

[19] Sarah Arpin, Catalina Camacho-Navarro, Kristin Lauter, Joelle Lim, Kristina Nelson, Travis Scholl, and Jana Sotáková. *Adventures in Supersingularland*, September 2019. https://arxiv.org/abs/1909.07779.

[20] A.K. Pizer. *Theta series and modular forms of level $p^2M$*. *Compositio Mathematica*, 40(2):177–241, 1980.

[21] B Gross. Heights and the special values of l-series. In *Conference Proceedings of the CMS*, volume 7, 1987.

[22] A.K. Pizer. *Ramanujan Graphs and Hecke Operators*. *Bulletin of the American Mathematical Society*, 23(1):127–137, 1990.

[23] Lisa Kohl. Lecture notes: *Introduction to cryptography*, September 2021.

[24] D. Kohel, K. Lauter, C. Petit, and J. Tignol. On the quaternion $\ell$-isogeny path problem. *LMS Journal of Computation and Mathematics*, 17(Spec. Issue A):418–432, 2014. https://doi.org/10.1112/S1461157014000151.

[25] Carmit Hazay and Yehuda Lindell. *Sigma protocols and Efficient Zero-knowledge*. Springer Berlin Heidelberg, 2010.

[26] Ivan Damgård. *On Σ-protocols*, 2010. https://cs.au.dk/~ivan/Sigma.pdf.

[27] Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography*. Chapman and Hall/CRC Press, 2007.

[28] Amos Fiat and Adi Shamir. *How to prove yourself: practical solutions to identification and signature problems*. In *Advances in Cryptology - CRYPTO 86'*, Lecture Notes in Computer Science. Springer Berlin Heidelberg.

[29] M. Abdalla, J.H. An, M. Bellare, and C. Namprempre. *From identification to signatures via the Fiat-Shamir transform: Minimizing assumptions for security and forward-security.* International Conference on the Theory and Applications of Cryptographic Techniques, 2002.

[30] David R. Kohel. *Endomorphism rings of elliptic curves over finite fields*. PhD thesis, University of California. Berkeley, 1996.

[31] Leonardo Colò and David Kohel. *Orienting supersingular isogeny graphs*. Cryptology ePrint Archive, Report 2020/985, 2020. https://ia.cr/2020/985.

[32] Hiroshi Onuki. *On oriented supersingular elliptic curves*, 2020. https://arxiv.org/abs/2002.09894.

[33] J.H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer New York, 1994.

[34] Ken McMurdy. *Explicit generators for endomorphism rings of supersingular elliptic curves*, 2014. https://phobos.ramapo.edu/~kmcmurdy/research/McMurdy-ssEndoRings.pdf.