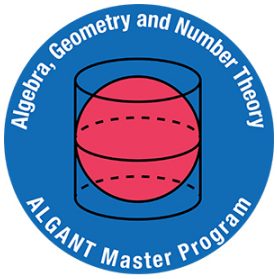


Master thesis

July 2024

On an attack on SIKE using abelian surfaces

Written by
Eva Ragazzini

Supervised by
Prof. Dr. Ulrich Görtz

Università
degli Studi
di Padova

UNIVERSITÄT
DUISBURG
ESSEN
Offen im Denken

Ich erkläre, dass ich die vorliegende Arbeit selbständig verfasst habe und keine anderen als die angegeben Quellen und Hilfsmittel benutzt sowie Zitate kenntlich gemacht habe.

Essen

Contents

Introduction

Cryptography has been used since centuries as a way to ensure secure communications. Since the 1990s, elliptic curves started to play a major role in encryption methods. First, elliptic curve cryptography was based on the discrete logarithm problem for groups coming from elliptic curves over finite fields. Later, other methods based on isogenies between elliptic curves were considered, especially in the search for quantum-computer safe algorithms. In 2016, the National Institute of Standards and Technology (NIST) launched a competition to update their standards to include systems that could resist quantum computers. The standardized version of Supersingular Isogeny Diffie-Hellman (SIDH) proposed by [FJP14] and named Supersingular Isogeny Key Encapsulation (SIKE), was one of the four candidates that made it to the last round of the competition in July 2022. However, in August 2022, Castryck and Décru published the devastating attack [CD22], running in polynomial time when the endomorphism ring of the starting elliptic curve is known. In May 2023, another semi-independent attack [MMP+23] was published, that ameliorates the previous attack by avoiding some iterative decision strategy for computing isogenies. This is the attack we will focus on.

The goal of the thesis is to understand the attack on SIDH, with a particular focus on understanding $(2,2)$-isogenies bewteen abelian surfaces. In Chapter 1, we will first give some preliminary definitions and results we will need throughout the thesis. In Chapter 2, we explain the Supersingular Diffie-Hellmann key-exchange protocol that is the target of the attack, and we construct an explicit example of it for $p = 59$ and for the starting curve $E_0 : y^2 = x^3 + x$ over $\mathbb{F}_{p^2}$. In Chapter 3, we will describe the algorithm used for the attack, as well as the theorem this algorithm relies on. This theorem focuses on understanding a (B, B)-isogeny between product of elliptic curves. In particular, we will conclude the thesis in Chapter 4 by studying $(2,2)$-isogenies between abelian surfaces, and by computing examples of such isogenies.

Acknowledgements

First, I would like to thank my advisor Professor Ulrich Görtz. I am extremely grateful for all his patience during our many meetings, and for all the help he provided throughout this project. A special thanks also goes to all the professors at the University of Luxembourg, who kept in touch and kept supporting me long after I finished my Bachelor studies.

Moreover, I am thankful to all the friends I met through the ALGANT program, mathematicians and non-mathematicians, in Padova and in Essen. I am very grateful for my roommates, who have been a constant source of support during my time in Essen. Thanks to Giacomo for always sharing your enthusiasm whenever you discovered a new French pastry during your time in Bordeaux (it's pain au chocolat, not chocolatine). Thanks to Antonio, Edo and Nicola for all the card games played in your office this past year. Thanks for almost never making me lose first. In particular, thanks to Ben, for all the card games as well, for listening to me complaining probably more than anyone else when things were not working out, and for all the travels already done and the many more to come.

Finally, I would like to thank my family, who has supported me during the entirety of my studies, and has always been here to celebrate with me. Your support has gone a long way, and I wouldn't be here without all your help. Merci, je vous aime.

Chapter 1

Preliminary Notions

In this first chapter, we will recall preliminary notions that will be necessary throughout this thesis. In Section 1.1, we follow [Sil09] and [Was08], as we want to remind some facts on elliptic curves, in particular on isogenies and on endomorphism rings, as well as on elliptic curves over finite fields. The crucial point will be the characterization of supersingular elliptic curves. All these notions will be used in Chapter 2. Then we define in Section 1.2 the notions needed for Chapter 3. We need to study abelian varieties, and in particular abelian surfaces and their dual. For this, we will use [EvdGM21], [GW], as well as [Sil09] again. We also need to review divisors on curves and surfaces so that we can define polarizations and (B, B)-isogenies. Finally, in Section 1.3 we define Jacobians and hyperelliptic curves, and explain how we use the Mumford representation of a divisor, which we will see in Chapter 4. We refer to [Smi05] and [CFA+12].

1.1 Elliptic curves, isogenies and endomorphism ring

In this section, we define elliptic curves and objects related to them, such as isogenies and their dual, torsion subgroups and endomorphism rings. We focus on a particular case of elliptic curves, which are called supersingular. We base this section on [Sil09], and we omit proofs.

We start by defining elliptic curves and the maps between them.

Definition 1.1. *Let K be a field. An **elliptic curve** is a pair (E, O), where E is a smooth, projective curve of genus 1, and $O \in E$ is the point at infinity. We often omit O and say E is an elliptic curve. We say it is **defined over** K, written E/K, if E is defined as a curve over K and $O \in E(K)$. If $\mathrm{char}(K) \neq 2, 3$, E is given up to isomorphism as a plane algebraic curve by a **Weierstrass equation** $E : y^2 = x^3 + Ax + B$, where $A, B \in K$.*

One of the main particularity of elliptic curves is that we can define a composition law, making E an abelian group with identity O.

Construction. *The* ***composition law*** *on elliptic curves is defined as follows. Let E be given by a Weierstrass equation, where E is in the projective plane $\mathbb{P}^2$, so that E consists of the points $P = (x, y)$ satisfying the Weierstrass equation, together with the point at infinity $O = [0 : 1 : 0]$. Let $P, Q \in E$, let L be the line through P and Q (we take the tangent line at P if $P = Q$), and R the third point of intersection between L and E. Let L' be the line through R and O. Then L' intersect E at R, O and a third point $P \oplus Q$.*

We want to focus on maps between curves, and in particular on maps that send the distinguished point of a curve to itself. For the rest of this section, unless said otherwise, let E, E', E'' be elliptic curves defined over K.

Definition 1.2. *An* ***isogeny*** *from E to E' is a morphism $\varphi : E \to E'$ satisfying $\varphi(O) = O$. We say two curves E and E' are* ***isogenous*** *if there exists an isogeny from E to E' such that $\varphi(E) \neq O$. Isogeny is an equivalence relation.*

A natural example of an isogeny is the multiplication by m.

Example 1.3. *For $m \in \mathbb{Z}$, the* ***multiplication by*** *m is given by $[m] : E \to E$, where:*

$$[m](P) = \begin{cases} \underbrace{P + ... + P}_{m-times} & \text{if } m > 0 \\ O & \text{if } m = 0 \end{cases}.$$

We set $[m](P) = [-m](-P)$ if $m < 0$.

Taking the kernel of $[m]$ leads to an important definition.

Definition 1.4. *Let $m \in \mathbb{Z}$ with $m \geq 1$. The* ***m-torsion subgroup of*** *E is the set of points of order m, given by $E[m] = \{P \in E : [m]P = O\}$. The* ***torsion subgroup of*** *E is the set $E_{tors} = \bigcup_{m=1}^{\infty} E[m]$, consisting of all the points of finite order.*

Moreover, since either $\varphi(E) = O$ or $\varphi(E) = E'$, then every isogeny is a finite map of curves (with exception $[0]$), bringing us to the notion of degree.

Definition 1.5. *Let $\varphi : E \to E'$ be a non-zero isogeny. From the injection of function fields $\varphi^* : \bar{K}(E') \to \bar{K}(E)$, we define the* ***degree*** *of φ, denoted by $\deg \varphi$, as the degree of the finite extension $\bar{K}(E)/\varphi^*\bar{K}(E')$. We say the map φ is separable, inseparable or purely inseparable depending on the corresponding property of the field extension. If φ is the zero isogeny, we set $\deg(0) = 0$.*

Example 1.6. *The degree of the multiplication by m isogeny is $\deg[m] = m^2$. Then we have:*

- *If $m \neq 0$ in K (i.e. $char(K) = 0$ or p, where $p \not| \, m$), then $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$;*

- *If* $char(K) = p$, *then* $E[p^e] = \{O\}$ *or* $E[p^e] \cong \mathbb{Z}/p^e\mathbb{Z}$.

Using Definition 1.5, we can define the dual of an isogeny.

Definition 1.7. *Let* $\varphi : E \to E'$ *be an isogeny of degree* m. *The* ***dual*** *of this isogeny is the unique isogeny* $\widehat{\varphi} : E' \to E$ *satisfying* $\widehat{\varphi} \circ \varphi = [m]$. *If* $\varphi = [0]$, *we set* $\widehat{\varphi} = [0]$.

Proposition 1.8. *Let* $\varphi : E \to E'$ *be an isogeny of degree* m.

1. $\widehat{\widehat{\varphi}} = \varphi$.
2. *Let* $\psi : E' \to E''$ *be an isogeny. Then* $\widehat{\psi \circ \varphi} = \widehat{\varphi} \circ \widehat{\psi}$.
3. *Let* $\lambda : E \to E'$ *be an isogeny. Then* $\widehat{\varphi + \lambda} = \widehat{\varphi} + \widehat{\lambda}$.
4. *For all* $m \in \mathbb{Z}$, $\widehat{[m]} = [m]$.

We mention some results we will need later.

Theorem 1.9. *Let* $\varphi : E \to E'$ *be a separable non-zero isogeny. Then* φ *is unramified,* $\#\ker\varphi = \deg\varphi$ *and* $\bar{K}(E)$ *is a Galois extension of* $\varphi^*\bar{K}(E')$.

Theorem 1.10. *Let* Φ *be a finite subgroup of* E. *Then there is a unique elliptic curve* E' *and a separable isogeny* $\varphi : E \to E'$ *satisfying* $\ker\varphi = \Phi$. *We often denote* E' *as* E/Φ.

We now define an invariant of the isomorphism class of the curve, as we will often identify an elliptic curve with this invariant.

Definition 1.11. *The* j***-invariant*** *of a curve in Weierstrass form is* $j = -1728\dfrac{(4A)^3}{\Delta}$, *where* $\Delta = -16(4A^3 + 27B^2)$ *is the discriminant of the curve.*

Let us now discuss the properties of certain sets of isogenies. We denote by $\mathrm{Hom}(E, E')$ the set of isogenies from E to E'. It forms a group, with addition given by $(\varphi + \psi)(P) = \varphi(P) + \psi(P)$, where $\varphi, \psi \in \mathrm{Hom}(E, E')$. More importantly, we want to study the case $E = E'$, i.e. the endomorphism ring.

Definition 1.12. *The* ***endomorphism ring*** *of* E *is* $\mathrm{End}(E) = \mathrm{Hom}(E, E)$, *where the addition law is given as above, and the multiplication law is given by the composition* $(\varphi\psi)(P) = \varphi(\psi(P))$, *for* $\varphi, \psi \in \mathrm{End}(E)$.

This is an important invariant of elliptic curves, and we want to study its structure, in particular in the case of curves defined over finite fields. First, note that $\mathrm{End}(E)$ has characteristic 0, has no zero-divisors and has rank at most four as a $\mathbb{Z}$-module. Let us remind some notions on orders and on quaternion algebras.

Definition 1.13. *Let* $\mathcal{K}$ *be a* $\mathbb{Q}$*-algebra that is finitely generated as a* $\mathbb{Q}$*-vector space. An* ***order*** $\mathcal{R}$ *of* $\mathcal{K}$ *is a subring of* $\mathcal{K}$ *that is finitely generated as a* $\mathbb{Z}$*-module and satisfies* $\mathcal{R} \otimes \mathbb{Q} = \mathcal{K}$.

Definition 1.14. *A **quaternion algebra** is an algebra of the form* $\mathcal{K} = \mathbb{Q}+\mathbb{Q}\alpha+\mathbb{Q}\beta+\mathbb{Q}\alpha\beta$ *whose multiplication satisfies* $\alpha^2, \beta^2 \in \mathbb{Q},\ \alpha^2 < 0,\ \beta^2 < 0,\ \beta\alpha = -\alpha\beta$.

Theorem 1.15. *Let* $\mathcal{R}$ *be a ring of characteristic* 0 *having no zero-divisors, and assume* $\mathcal{R}$ *is such that:*

- $\mathcal{R}$ *has rank at most four as a* $\mathbb{Z}$*-module;*
- $\mathcal{R}$ *has an anti-involution* $\alpha \mapsto \widehat{\alpha}$ *satisfying* $\widehat{\alpha+\beta} = \widehat{\alpha} + \widehat{\beta},\ \widehat{\alpha\beta} = \widehat{\beta}\widehat{\alpha},\ \widehat{\widehat{\alpha}} = \alpha,\ \widehat{a} = a$ *for* $a \in \mathbb{Z} \subset \mathcal{R}$;
- *For* $\alpha \in \mathcal{R}$*, the product* $\alpha\widehat{\alpha}$ *is a non-negative integer, and* $\alpha\widehat{\alpha} = 0$ *if and only if* $\alpha = 0$.

Then $\mathcal{R}$ *is one of the following types of rings:*

1. $\mathcal{R} \cong \mathbb{Z}$;
2. $\mathcal{R}$ *is an order in an imaginary quadratic extension of* $\mathbb{Q}$;
3. $\mathcal{R}$ *is an order in a quaternion algebra over* $\mathbb{Q}$.

Applying this to the endomorphism ring of elliptic curves, we can conclude the following.

Corollary 1.16. *The endomorphism ring* $\mathrm{End}(E)$ *of an elliptic curve* E/K *is either* $\mathbb{Z}$*, an order in an imaginary quadratic field or an order in a quaternion algebra. If* $\mathrm{char}(K) = 0$*, only the first two cases are possible.*

We are particularly interested in the last case of Theorem 1.15 because of its non-commutativity properties.

We now want to study the structure of the endomorphism ring of elliptic curves defined over finite fields. From Example 1.6 we know that in a field of characteristic p, where p is prime, $E[p]$ will be either $\{O\}$ or $\mathbb{Z}/p\mathbb{Z}$, and we know the possibilities for $\mathrm{End}(E)$ from Corollary 1.16. There exists an important relation between the structure of the torsion group $E[p]$ and the endomorphism ring $\mathrm{End}(E)$.

Theorem 1.17. *Let* K *be a field such that* $\mathrm{char}(K) = p > 0$*, let* E/K *be an elliptic curve. For each* $r \in \mathbb{Z}_{\geq 1}$*, let* $\varphi_r : E \to E^{(p^r)}$ *be the* p^r*-power of Frobenius and* $\widehat{\varphi}_r : E^{(p^r)} \to E$ *its dual (note here that* $E^{(p^r)}$ *is obtained by raising the coefficients of the equation of* E *to the* p^r*-th power).*

(a) The following are equivalent:

(i) $E[p^r] = O$ *for one (all)* $r \geq 1$;

(ii) $\widehat{\varphi}_r$ *is (purely) inseparable for one (all)* $r \geq 1$;

(iii) *The map* $[p] : E \to E$ *is purely inseparable and the* j*-invariant* $j(E)$ *of* E *is in* $\mathbb{F}_{p^2}$*;*

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

(b) If the equivalent conditions above do not hold, then $E[p^r] = \mathbb{Z}/p^r\mathbb{Z}$ *for all* $r \geq 1$*. If further* $j(E) \in \bar{F}_p$*, then* $\mathrm{End}(E)$ *is an order of a quadratic imaginary field.*

In particular, this result applies to elliptic curves over finite fields, and helps us characterize two distinguished types of curves.

Definition 1.18. *If* E *satisfies the properties given in Theorem Theorem 1.17(a), we say it is a* ***supersingular elliptic curve****. Otherwise, in the case of Theorem Theorem 1.17(b), we say it is an* ***ordinary elliptic curve****.*

Here, we will mainly use the characterization that supersingular elliptic curves have an endomorphism ring that is an order in a quaternion algebra. But let us nonetheless mention another characterization, using the trace of the Frobenius.

Theorem 1.19. *Let* $E/\mathbb{F}_p$ *be an elliptic curve, let* $\varphi : E \to E,\ (x, y) \mapsto (x^p, y^p)$ *be the* p*-th power Frobenius endomorphism, and let* $a = p + 1 - \#E(\mathbb{F}_p)$ *be the trace of the Frobenius. Let* $\alpha, \beta \in \mathbb{C}$ *be the roots of the polynomial* $T^2 - aT + p$*.*
Then α *and* β *are complex conjugates satisfying* $|\alpha| = |\beta| = \sqrt{p}$*, and for every* $n \geq 1$*, we have*

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

Example 1.20. *Consider an elliptic curve* $E/\mathbb{F}_p^2$*. Then we have* $\#E(\mathbb{F}_{p^2}) = p^2 + 1 \pm 2p = (p \pm 1)^2$*. So* $E(\mathbb{F}_{p^2}) \cong (\mathbb{Z}/(p \pm 1)\mathbb{Z})^2$*.*

Corollary 1.21. *An elliptic curve* $E/\mathbb{F}_p^2$ *is supersingular if and only if* $a \equiv 0 \pmod{p}$*.*

1.2 Abelian varieties, duality and polarizations

In this section, we want to define abelian varieties, with a special focus on abelian surfaces. We also give an overview of the properties defining the dual of an abelian variety, in particular by studying divisors, and seeing the dual as the Picard group of degree 0 of the variety. We end by defining polarizations between a variety and its dual, allowing us to study B-isogenies and (B, B)-isogenies.

We first define algebraic groups and varieties using [CFA+12]. Let us remind that an algebraic variety is a closed set with respect to the Zariski topology that is also irreducible. We want to endow this algebraic variety with a group structure.

Definition 1.22. *An* ***algebraic group*** $\mathcal{G}$ *over a field* K *is an absolutely irreducible variety defined over* K *with the following properties:*

(i) There is a distinguished neutral element $0 \in \mathcal{G}(K)$*;*

(ii) There is an addition map $m : \mathcal{G} \times \mathcal{G} \to \mathcal{G}$*;*

(iii) There is an inversion map $i : \mathcal{G} \to \mathcal{G}$*.*

It must also satisfy the usual group laws:

- $m \circ (\mathrm{Id}_{\mathcal{G}} \times m) = m \circ (m \times \mathrm{Id}_{\mathcal{G}})$ *(associativity);*
- $m_{|\{0\}\times\mathcal{G}} = p_2$*, where* p_2 *is the projection of* $\mathcal{G} \times \mathcal{G}$ *onto the second factor;*
- $m \circ (i \times \mathrm{Id}_{\mathcal{G}}) \circ \delta_{\mathcal{G}} = c_0$ *where* $\delta : \mathcal{G} \to \mathcal{G} \times \mathcal{G}$ *is the diagonal map, and* c_0 *is the map sending* $\mathcal{G}$ *tp 0.*

It is then easy to define our main subject of interest.

Definition 1.23. *An* ***abelian variety*** $\mathcal{A}$ *is a projective algebraic group. When defined over* K*, we note it as* $\mathcal{A}/K$*.*

Example 1.24.
- *Elliptic curves are abelian varieties of dimension 1.*
- *An abelian surface is an abelian variety of dimension 2.*

The group of points is commutative, and similarly to elliptic curves, we can take the n-torsion subgroup of an abelian variety.

Lemma 1.25. *Let* K *be a finite field with* $\mathrm{char}(K) = p$*, and let* $\mathcal{A}$ *be an abelian variety of dimension* g *over* K*. If* $(n, p) = 1$*, then the* n*-torsion subgroup of* $\mathcal{A}$ *is* $\mathcal{A}[n] \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$*.*

We also need to study the dual of an Abelian variety. Formalizing the construction is out of the scope of this thesis, thus we focus on giving its main properties and how to work with it, and we leave [GW] as a reference.

Proposition 1.26. *Let* K *a field. There exists an additive contravariant functor from the category of abelian varieties over* K *to itself, mapping each abelian variety* $\mathcal{A}/K$ *to its* ***dual abelian variety*** $\mathcal{A}^\vee$ *. More explicitly, we have the following:*

1. *For each* $\mathcal{A}/K$ *an abelian variety,* $\mathcal{A}^\vee$ *is the dual abelian variety.* $\mathcal{A}^\vee$ *is an abelian variety defined over* K*, and* $\dim \mathcal{A} = \dim \mathcal{A}^\vee$*.*
2. *For each homomorphism* $f : \mathcal{A} \to \mathcal{B}$ *of abelian varieties* $\mathcal{A}, \mathcal{B}$ *over* K*, there is a* ***dual homomorphism*** $f^\vee : \mathcal{B}^\vee \to \mathcal{A}^\vee$ *such that:*
   - *It preserves the identity morphisms, i.e.* $\mathrm{id}_{\mathcal{A}}^\vee = \mathrm{id}_{\mathcal{A}^\vee}$*;*
   - *It is compatible with the compositions, i.e.* $(f \circ g)^\vee = g^\vee \circ f^\vee$ *for* $g : \mathcal{B} \to \mathcal{A}$ *another homomorphism;*

- *Moreover,* $(f+g)^\vee = f^\vee + g^\vee$ *as homomorphisms* $\mathcal{B}^\vee \to \mathcal{A}^\vee$.

The name is justified given the following result.

Proposition 1.27. *Let* $\mathcal{A}$ *be an abelian variety. There is a natural isomorphism* $\mathcal{A} \to \mathcal{A}^{\vee\vee}$ *between* $\mathcal{A}$ *and its double dual.*

We are now interested in the compatibility of the dual abelian variety with products, as well as in its matrix representation. Let us first remind some results on products of group varieties, working first with products of commutative groups to get a better intuition.

Construction. *Let* $G_1, ..., G_m$ *and* $H_1, ..., H_n$ *be commutative groups written additively, for* $m, n \in \mathbb{Z}$ *some positive integers. Then, every group homomorphism*

$$g : G_1 \times ... \times G_m \to H_1 \times ... \times H_n$$

is of the form

$$(g_1, ..., g_m) \mapsto \sum_{i,j} f_{ij}(g_j) = \sum_j (f_{1j}(g_j), ..., f_{nj}(g_j)),$$

for group homomorphisms $f_{ij} : G_j \to H_i$. *Given* f, *we have that* f_{ij} *is uniquely determined as the composition of*

$$G_j \to G_1 \times ... \times G_m \xrightarrow{f} H_1 \times ... \times H_n \to H_i,$$

where the first map is the inclusion of G_j *into the product* $G_1 \times ... \times G_m$, *and the final map is the projection onto the* i*-th factor. Then* f *is given by the matrix* $(f_{ij})_{i,j}$. *Then, composition of maps is given by multiplication of matrices, using composition of group homomorphism as multiplication for individual entries.*

The same reasoning works for abelian varieties, as they also have a commutative structure. We then have the following result using the fact that the dual is an additive functor.

Proposition 1.28. *Let* $\mathcal{A}$ *and* $\mathcal{B}$ *be abelian varieties defined over* K. *There is a unique isomorphism* $\nu : (\mathcal{A} \times \mathcal{B})^\vee \to \mathcal{A}^\vee \times \mathcal{B}^\vee$ *such that:*

1. *Under this identification, the dual map of the projection* $\mathcal{A} \times \mathcal{B} \to \mathcal{A}$ *is the inclusion* $\mathcal{A}^\vee \to (\mathcal{A} \times \mathcal{B})^\vee = \mathcal{A}^\vee \times \mathcal{B}^\vee$. *Likewise, the dual of the projection* $\mathcal{A} \times \mathcal{B} \to \mathcal{B}$ *is the inclusion* $\mathcal{B}^\vee \to \mathcal{A}^\vee \times \mathcal{B}^\vee$.

2. *The dual map of the inclusion* $\mathcal{A} \to \mathcal{A} \times \mathcal{B}$ *is the projection* $\mathcal{A}^\vee \times \mathcal{B}^\vee \to \mathcal{A}^\vee$. *Likewise, the dual of the inclusion* $\mathcal{B} \to \mathcal{A} \times \mathcal{B}$ *is the projection* $\mathcal{A}^\vee \times \mathcal{B}^\vee \to \mathcal{B}^\vee$.

We now take a look at the matrix form of the dual. Later on, we we will use the product of at most two abelian varieties, so let us simplify the following result by only considering two factors on each side.

Proposition 1.29. *Let $\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}'_1, \mathcal{A}'_2/K$ be abelian varieties. Let $\Phi : \mathcal{A}_1 \times \mathcal{A}_2 \to \mathcal{A}'_1 \times \mathcal{A}'_2$ be a homomorphism of abelian varieties. We take its matrix form to be $(\varphi_{ij})_{i,j}$ with homomorphisms $\varphi_{ij} : \mathcal{A}_j \to \mathcal{A}'_i$. Identifying $(\mathcal{A}_1 \times \mathcal{A}_2)^\vee = \mathcal{A}_1^\vee \times \mathcal{A}_2^\vee$ via ν and $(\mathcal{A}'_1 \times \mathcal{A}'_2)^\vee = \mathcal{A}'^\vee_1 \times \mathcal{A}'^\vee_2$ via ν' (where ν' is defined in the same way as ν in Proposition 1.28), the matrix description of $\nu \circ \Phi^\vee \circ (\nu')^{-1}$ is given by*

$$\nu \circ \Phi^\vee \circ (\nu')^{-1} = (\varphi_{ji}{}^\vee)_{i,j}.$$

Proof. To compute the matrix components of $\Phi^\vee$, we consider the projections $\pi'_i : \mathcal{A}'^\vee_1 \times \mathcal{A}'^\vee_2 \to \mathcal{A}'^\vee_i$ and the inclusions $\iota_j : \mathcal{A}_j^\vee \to \mathcal{A}_1^\vee \times \mathcal{A}_2^\vee$, and then compute the compositions $\pi'_i \circ \Phi \circ \iota_j$. But π'_i is dual to the inclusion $\iota'_i : \mathcal{A}'_i \to \mathcal{A}'_1 \times \mathcal{A}'_2$, and ι_j is dual to the projection $\pi_j : \mathcal{A}_1 \times \mathcal{A}_2 \to \mathcal{A}_j$. So we conclude

$$\pi'_i \circ \Phi^\vee \circ \iota_j = \iota'^\vee_i \circ \Phi^\vee \circ \pi_j^\vee = (\pi_j \circ \Phi \circ \iota'_j)^\vee = \varphi_{ji}^\vee.$$

□

Let us now recall some results on divisors of curves, using [Sil09] as a reference. We will then give some generalizations of these results to divisors over arbitrary varieties.

Definition 1.30. *The **divisor group** $\mathrm{Div}(C)$ of a curve C is the free abelian group generated by the points of C. A **divisor** $D \in \mathrm{Div}(C)$ can be seen as a formal sum $D = \sum_{P \in C} n_P(P)$, where $n_P \in \mathbb{Z}$ is zero almost everywhere.*

We take a look at a particular subgroup of $\mathrm{Div}(C)$.

Definition 1.31. *Let $D \in \mathrm{Div}(C)$. The **degree** of D is defined as $\deg D = \sum_{P \in C} n_P$. The **divisors of degree** 0 is a subgroup of $\mathrm{Div}(C)$, denoted by $\mathrm{Div}^0(C)$. If all n_P's are positive, the divisor is said to be **effective**.*

In some cases, divisors can also be associated to functions.

Definition 1.32. *Assume C is a smooth curve, and let $f \in K(C)^*$. Then we associate to f the divisor $\mathrm{div}(f)$, given by*

$$\mathrm{div}(f) = \sum_{P \in C} \mathrm{ord}_P(f)(P),$$

*where ord_P is the order of f at P. We say that such a divisor is **principal**, and we denote the subgroup of principal divisors by $\mathrm{Prin}(C)$.*

Quotienting the group of divisors by the subgroup of principal divisors, we obtain the following.

Definition 1.33. *The **divisor class group**, also called **Picard group**, is given by*

$$\mathrm{Pic}(C) = \mathrm{Div}(C)/\mathrm{Prin}(C).$$

Two divisors D_1, D_2 are linearly equivalent if $D_1 - D_2$ is principal, and we denote it by $D_1 \sim D_2$.

Since by [Sil09, Chapter II, Remark 3.7] we have $\deg(\mathrm{div}(f)) = 0$, $\mathrm{Prin}(C)$ is a subgroup of $\mathrm{Div}^0(C)$, and the degree-0 part of the Picard group of C is denoted by $\mathrm{Pic}^0(C)$.

Since we only defined divisors on curves, let us see how we can approach divisors on surfaces, and more generally on an abelian variety. Let $\mathcal{A}$ be an abelian variety. We can see a divisor on $\mathcal{A}$ as a finite sum $\sum_i a_i D_i$ where the a_i's are again integers, and the D_i's are codimension-1 subvarieties of $\mathcal{A}$. Then, the rest of the definitions and properties follow in an analogous way as for divisors on curves.

From [GW], we see the Picard group $\mathrm{Pic}^0(\mathcal{A})$ as the group of isomorphism classes of line bundles "algebraically equivalent" to 0 on $\mathcal{A}$. The points of the dual $\mathcal{A}^\vee$ can then be seen as $\mathcal{A}^\vee(K) = \mathrm{Pic}^0(\mathcal{A})$. For an homomorphism, it means the following: take $f : \mathcal{A} \to \mathcal{B}$ to be a homomorphism. Its dual $f^\vee : \mathcal{B}^\vee \to \mathcal{A}^\vee$ can be defined in terms of pullback of line bundles: for a point in $\mathcal{B}^\vee$ viewed as a line bundle $\mathcal{L}$ on $\mathcal{B}$, it is mapped in $\mathcal{A}$ to the line bundle $f^*\mathcal{L}$. If f is surjective, we talk about pullback of divisors, and we can describe $f^\vee$ as given by pullback of divisors. In the case of an isogeny $\mathcal{A} \to \mathcal{A}'$, the homomorphism is surjective and we know $\dim \mathcal{A} = \dim \mathcal{A}'$. Then, by [GW, Prop 27.213], the dual $\mathcal{A}'^\vee \to \mathcal{A}^\vee$ is an isogeny as well. This map can be described by pullback of divisors, and in the case of effective divisors we can take the inverse image along the morphism. Finally, a divisor class D is algebraically equivalent to 0 if and only if it is translation invariant: for every translation isomorphism $t : \mathcal{A} \to \mathcal{A}$, the divisor class is invariant under pullback under t, i.e. t^*D is linearly equivalent to D.

Example 1.34. *Let us study the dual of an elliptic curve E/K. First, note that on curves a line bundle is algebraically equivalent to 0 if and only if it has degree 0. Here, we will work in terms of divisors, so this is equivalent to say that its corresponding divisor class has degree 0. On E, every point $x \in E$ defines a divisor $[x]-[0]$ of degree 0 on the curve. From the Riemann-Roch theorem, that means we have a bijection between $E(K)$ and $\mathrm{Pic}^0(E)$. By [GW, Theorem 26.98], this bijection extends to an isomorphism $\lambda_E : E \to E^\vee$, and this isomorphism $E \cong E^\vee$ explains why we usually don't mention the dual of an elliptic curve. For an isogeny of elliptic curves $\varphi : E \to E'$, the dual isogeny $\widehat{\varphi}$ is given by the composition*

$$E' \xrightarrow{\lambda_{E'}} E'^\vee \xrightarrow{\varphi^\vee} E^\vee \xrightarrow{\lambda_E^{-1}} E.$$

Finally, we are interested in the maps between an abelian variety and its dual.

Definition 1.35. *Let X be an abelian surface and $X^\vee$ its dual. A **polarization** is an isogeny $\lambda_X : X \to X^\vee$. Moreover, we say it is **principal** if it is an isomorphism. In terms of line bundles, referring to [GW, Section 27.52], $\lambda : \mathcal{A} \to \mathcal{A}^\vee$ is a polarization if λ is a symmetric isogeny and the line bundle $(\mathrm{id}, \lambda)^*\mathcal{P}$ on $\mathcal{A}$ is ample, i.e. it has enough sections to give an embedding of $\mathcal{A}$ into a projective space for some positive power. Here, $\mathcal{P}$ denotes the Poincaré bundle on $\mathcal{A} \times \mathcal{A}^\vee$ and is the canonical line bundle on the product of an abelian variety and its dual.*

Definition 1.36. *[EvdGM21, Definition 11.11] Let $f : \mathcal{A} \to \mathcal{B}$ be an isogeny of abelian varieties over a field K. Then,*

$$e_f : \ker(f) \times \ker(f^\vee) \to \mathbb{G}_{m,K}$$

is the perfect bilinear pairing given by $e_f(x, y) = \beta(y)(x)$, where β denotes the isomorphism between $\ker(f^\vee)$ and the Cartier dual $\ker(f)^D$. If $\ker(f)$ is killed by $n \in \mathbb{Z}_{n\geq 1}$, then e_f takes values in $\mu_n \in \mathbb{G}_m$. In particular, for $f = [n]_\mathcal{A}$ the multiplication by n map on $\mathcal{A}$, we get a pairing

$$e_n : \mathcal{A}[n] \times \mathcal{A}^\vee[n] \to \mu_n,$$

*called the **Weil pairing**.*

The notion of polarization allows us to look at some special cases of isogenies between surfaces.

Definition 1.37. *Let B be a positive integer, and let X, Y be two abelian surfaces equipped with polarizations $\lambda_X : X \to X^\vee, \lambda_Y : Y \to Y^\vee$ respectively. A B-**isogeny** of abelian surfaces is an isogeny $\Phi : (X, \lambda_X) \to (Y, \lambda_Y)$ such that*

$$[B] \circ \lambda_X = \Phi^\vee \circ \lambda_Y \circ \Phi,$$

where $\Phi^\vee : Y^\vee \to X^\vee$ is the dual isogeny.

Definition 1.38. *A (B, B)-**isogeny** is a B-isogeny of abelian surfaces such that its kernel is isomorphic to $(\mathbb{Z}/B\mathbb{Z})^2$.*

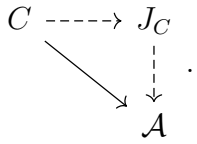
1.3 Jacobians, hyperelliptic curves and Mumford representation of divisors

In this section, we will define the Jacobian of a curve, as we will later need to work with maps between Jacobians of curves. In particular, we will deal with curves of genus 2, which

can be proven to be hyperelliptic. We also want to define the Mumford representation of a reduced divisor, as it will provide a more straightforward way to deal with divisors on Jacobians.

Using the approach of [Smi05], we start by defining the Jacobian of a curve.

Definition 1.39. *Let C be a curve with a fixed base point. The **Jacobian** of C, noted J_C, is a principally polarized abelian variety together with a morphism $C \to J_C$, satisfying the following universal property: any map from C to another abelian variety $\mathcal{A}$ factors uniquely through J_C as in the diagram*



The Jacobian is unique up to isomorphism, and a curve of genus greater than zero can always be embedded in its own Jacobian.

What is interesting about the Jacobian of a curve is its group structure: for a curve C, the Jacobian J_C is an abelian variety, when the curve itself usually isn't one.

Another way to see it is using the Picard group again.

Theorem 1.40. *Let C be a curve, with genus $g_C > 0$. Let J_C be its Jacobian, and let $\alpha : C \hookrightarrow J_C$ an embedding. For each $r \geq 0$, we define $W_r := \underbrace{\alpha(C) + ... + \alpha(C)}_{r\text{-times}} \subset J_C$, and $\Theta := W_{(g_C-1)}$. Then the following statements hold:*

(i) Extending α linearly to a map on divisors, we have $\mathrm{Pic}^0(C) \cong J_C$.

(ii) W_r is a subvariety of J_C of dimension $\dim W_r = \min(r, g_C)$.

(iii) $W_{g_C} = J_C$. We say that C generates J_C.

(iv) $\dim J_C = g_C$.

Example 1.41. *Let E be an elliptic curve, which we know to be of genus 1. By Theorem 1.40, we have that J_E has dimension one. Taking a rational point $x \in E$, the embedding $\alpha_x : E \to J_E, P \mapsto [P - x]$ is an isomorphism. So J_E is isomorphic to the curve of genus 1 with a rational point, i.e. the elliptic curve E itself.*

Corollary 1.42. *Let $\psi : C \to X$ be a morphism of curves. Then the pullback $\psi^* : X \to C$ and the pushforward $\psi_* : C \to X$ induce well-defined homomorphisms of Jacobians*

$$\psi^* : J_X \to J_C \text{ and } \psi_* : J_C \to J_X.$$

In particular, we want to work with Jacobians of curves of genus 2, so that those Jacobians are surfaces. By [GW, Proposition 26.121], all curves of genus 2 are hyperelliptic curves, defined as follows.

Definition 1.43. *A **hyperelliptic curve** C of genus $g > 1$ over a field K is given by the equation*

$$C : y^2 + h(x)y = f(x),$$

*where $f, h \in K[x]$ are such that $2g + 1 \leq \deg(f) \leq 2g + 2$, and $\deg(h) \leq g + 1$. In a more classical way, we also can define a hyperelliptic curve as a curve that admits a covering $h_C : C \to \mathbb{P}^1$ of degree 2. A hyperelliptic curve is equipped with a **hyperelliptic involution** $\iota : C \to C$, given by $(x, y) \mapsto (x, -y - h(x))$.*

Since we will work on $J_C \cong \mathrm{Pic}^0(C)$, we want divisors of degree 0. We need the following type of divisor, which is always of degree 0.

Definition 1.44. *A divisor D on a hyperelliptic curve C of genus g is **reduced** if it can be written as*

$$D = \sum_{i=1}^{m} [P_i] - m[O],$$

where $P_i \neq O$ for all $1 \leq i \leq m$, $m \leq g$ and $P_i \neq \iota(P_j)$ for all $i \neq j$.

Proposition 1.45. *[MoWDoCO+96, Theorem 47] For every divisor $D \in \mathrm{Div}^0(C)$, there is a unique reduced divisor D' such that $D \sim D'$.*

Every degree 0 divisor is equivalent to a unique reduced divisor, so it also admits a unique Mumford representation, which is a representation of divisors on hyperelliptic curves that makes our future work easier.

Definition 1.46. *Let C a hyperelliptic curve of genus g, with affine part given by $y^2 + h(x)y - f(x)$, where $h, f \in K[x]$ and $\deg f = 2g + 1, \deg h \leq g$. Then every non-trivial reduced divisor $D \in \mathrm{Pic}^0(C)$ can be represented by a unique pair of polynomials $u, v \in K[x]$ such that:*

(i) u is monic,

(ii) $\deg v < \deg u \leq g$,

(iii) $u | v^2 + vh - f$.

Take D to be reduced as in Definition 1.44, and let $P_i = (x_i, y_i)$. Then the divisor class of D is given by $u(x) = \prod_{i=1}^{m} (x - x_i)$. In addition, if P_i occurs n_i times, we have $\left(\frac{d}{dx}\right)^j [v(x)^2 + v(x)h(x) - f(x)]_{|x=x_i} = 0$, for $0 \leq j \leq n_i - 1$. By the last condition of Lemma 1.46, we must have $P_i = (x_i, v(x_i))$, with appropriate multiplicity.

Example 1.47. *Let us take a hyperelliptic curve* $C : y^2 = x^5 - 4x^4 - 14x^3 + 36x^2 + 45x = x(x+1)(x-3)(x+3)(x-5)$ *of genus 2 over the real numbers. We have some points* $P = (1, 8), Q = (3, 0), R = (5, 0) \in C$. *Then* $D = [P] + [Q] - 2[O]$ *is a reduced divisor. We want to find its Mumford representation. First, notice that the polynomials* $u, v \in \mathbb{R}[x]$ *are such that* $\deg v < \deg u \leq 2$. *Then, we know that the* x*-coordinates of* P, Q *must be zeroes of* u, *so we have* $u(x) = (x-1)(x-3) = x^2 - 4x + 3$. *Finally, we have* $P = (1, v(1))$ *and* $Q = (3, v(3))$, *so* $v(1) = 8$ *and* $v(3) = 0$. *Since* v *must be of degree one, we conclude that* $v(x) = -4x + 12$. *So* D *can be written as* $[x^2 - 4x + 3, -4x + 12]$. *To go in the opposite direction (i.e. starting from the Mumford representation* $[x^2 + u_1x + u_0, v_1x + v_0]$ *to get back the points), notice first that the factorization of* $x^2 + u_1x + u_0$ *gives the* x *coordinates. Then, it is easy to recover the* y *coordinates from the fact that* $v_1x + v_0$ *is of degree* 1 *and that we must have* $y_i = v(x_i)$.

Let us see what changes if the degree of the hyperelliptic curve is even.

Lemma 1.48. *Let* $C : y^2 = f(x)$ *be a hyperelliptic curve of genus* g *over* K. *Then, for every point* $P \in J_C(K)$, *there is a unique divisor* $D \in \mathrm{Div}(C)$ *of degree* $d = \deg(D) \leq g$ *such that:*

- $P = [D] - d[O]$ *if the degree of* f *is odd, where* O *is the point at infinity of* C,
- $P = [D] - \frac{d}{2}[O_1] - \frac{d}{2}[O_2]$ *if the degree of* f *is even, where* O_1, O_2 *are the two points at infinity of* C.

Now, we will always assume that every genus 2 curve we encounter is of the form $H : y^2 = c_6x^6 + ... + c_0$ with $c_6 \neq 0$, so that all points on its Jacobian J_H are representable as $(\alpha_1, \beta_1) + (\alpha_2, \beta_2) - O_1 - O_2$ with $\alpha_1 \neq \alpha_2$, and have a Mumford representation of the form $[x^2 + u_1x + u_0, v_1x + v_0]$.

Chapter 2

Supersingular Isogeny Diffie-Hellman

The goal of this chapter is to introduce the Supersingular Isogeny Diffie-Hellman problem (SIDH) and provide an example of it. In Section 2.1, we will first remind what is the Diffie-Hellmann key-exchange protocol, and explain how it works on isogeny graphs of supersingular elliptic curves. In Section 2.2, we will see an example of it for supersingular elliptic curves over $\mathbb{F}_{p^2}$ with $p = 59$.

2.1 Key-exchange protocol

Let us first recall the concept of Diffie-Hellman key exchange in general. We have two parties, traditionally named Alice and Bob, who want to establish a secret key k. They start by choosing a public parameter p, and they each choose a private key, that we will denote a and b, for Alice and Bob respectively. After that, they agree on some mathematical method that uses the public parameter and their own private key to each compute a public key, denoted by A for Alice's key, and B for Bob's. Alice sends A to Bob, and Bob sends B to Alice. They use the knowledge of their own private key to compute the private value k (k is computed using either a and B, or b and A). Note that the mathematical method chosen must be difficult to solve without the knowledge of one of the private keys.

Example 2.1. *An example is the discrete logarithm problem. We take g to be a generator of a cyclic group G of order $n \in \mathbb{Z}_{>0}$. Alice and Bob both know g, G and n. Alice chooses $a \in \mathbb{Z}/n\mathbb{Z}$ and computes $A = g^a$, then sends it to Bob. Bob chooses $b \in \mathbb{Z}/n\mathbb{Z}$ and computes $B = g^b$ and sends it to Alice. Alice can then compute $k = B^a = g^{ba}$, and Bob computes $k = A^b = g^{ab}$, which is the secret key.*

Here, the mathematical method we want to use has to do with supersingular elliptic curves, and the difficulty of computing isogenies between them. An aspect distinguishing SIDH from traditional Diffie-Hellman is the non-commutativity. In general, protocols have commutative properties (in Example 2.1, we have $(g^a)^b = (g^b)^a$). But here, we will use the compositions of isogenies with different domains and codomains, so the

computation doesn't work in an arbitrary order. This is why we will introduce the notion of "auxiliary points", allowing us to work with such isogenies anyway. We will refer to the article [FJP14], which was the first to suggest this idea, and we will focus on describing the key-exchange protocol.

We will work with quadratic extension fields of prime fields $\mathbb{F}_p$, where p is a prime of the form $p = \ell_A^a \ell_B^b \cdot f \pm 1$, such that ℓ_A, ℓ_B are both small primes and f is a cofactor chosen to make p prime. Moreover, we choose p such that -1 is not a square in $\mathbb{F}_p$. The extension is formed as $\mathbb{F}_q = \mathbb{F}_{p^2}$, where $\mathbb{F}_{p^2} = \mathbb{F}_p(i)$ with $i^2 + 1 = 0$. For $E_0/\mathbb{F}_q$, using Theorem 1.19, we see $E_0(\mathbb{F}_q)$ is of cardinality $(p \mp 1)^2 = (\ell_A^a \ell_B^b \cdot f)^2$. We are interested in the ℓ_A^a-torsion subgroups. Indeed, $E_0[\ell_A^a] \cong \mathbb{Z}/\ell_A^a\mathbb{Z} \times \mathbb{Z}/\ell_A^a\mathbb{Z}$ by Example 1.6, hence it contains $\ell_A^{a-1}(a+1)$ cyclic subgroups of order ℓ_A^a. Each subgroup Φ of order ℓ_A^a defines a different isogeny $E_0 \to E_0/\Phi$ by Theorem 1.10. Using that reasoning, we have the same result for the ℓ_B^b-torsion subgroup. Each isogeny corresponds to an edge from an elliptic curve to another (or more precisely, from a j-invariant to another, as we will identify the elliptic curves by their j-invariant) in something called an isogeny graph.

Definition 2.2. *An **isogeny graph** is a graph whose nodes are the j-invariant of isogenous curves, and which edges are isogenies between them. We assume those graphs to be undirected, as there always exists a dual isogeny of the same degree.*

The isogeny graphs are (two-sided) expander graphs. Without going into more detail, this is a property we need to make walking along their edges more efficient, as we can see in [FJP14].

Our system is based on the following commutative diagram, which we will explain in the next part:

$$\begin{array}{ccc} E_0 & \xrightarrow{\varphi_A} & E_A = E_0/\langle K_A \rangle \\ \downarrow{\scriptstyle \varphi_B} & & \downarrow{\scriptstyle \varphi'_B} \\ E_B = E_0/\langle K_B \rangle & \xrightarrow[\varphi'_A]{} & E_{AB} = E_0/\langle K_A, K_B \rangle \end{array}$$

Figure 2.1: Commutative diagram of the key-exchange protocol.

Let us fix the public parameters of SIDH. The starting curve is given by $E_0/\mathbb{F}_q$, and the pairs of points $\{P_A, Q_A\}$ and $\{P_B, Q_B\}$ are defined such that

$$\langle P_A, Q_A \rangle = E_0[\ell_A^a], \ \langle P_B, Q_B \rangle = E_0[\ell_B^b].$$

On her side, Alice chooses some private $m_A, n_A \in \mathbb{Z}/\ell_A^a\mathbb{Z}$, not both divisible by ℓ_A. Using

Vélu's formulas from [Vél71], she can then compute an isogeny

$$\varphi_A : E_0 \to E_A = E_0/\langle [m_A]P_A + [n_A]Q_A \rangle$$

with kernel $\langle K_A \rangle = \langle [m_A]P_A + [n_A]Q_A \rangle$ of order ℓ_A^a. This isogeny will be a private parameter. Then she sends the auxiliary points $\varphi_A(P_B), \varphi_A(Q_B)$ to Bob, as well as the curve E_A. Since $K_A \subset E_0[\ell_A^a]$, φ_A can be seen as a composition of ℓ_A-isogenies of smaller degree than $\deg \varphi_A$. Bob does the same, choosing some private $m_B, n_B \in \mathbb{Z}/\ell_B^b\mathbb{Z}$, not both divisible by ℓ_B. He computes an isogeny

$$\varphi_B : E_0 \to E_B = E_0/\langle [m_B]P_B + [n_B]Q_B \rangle$$

with kernel $\langle K_B \rangle = \langle [m_B]P_B + [n_B]Q_B \rangle$, then sends the auxiliary points $\varphi_B(P_A), \varphi_B(Q_A)$ and the curve E_A to Alice. Then, they can compute the following:

- Alice computes $\varphi'_A : E_B \to E_{AB}$ with kernel $\langle [m_A]\varphi_B(P_A) + [n_A]\varphi_B(Q_A) \rangle$;
- Bob computes $\varphi'_B : E_A \to E_{BA}$ with kernel $\langle [m_B]\varphi_A(P_B) + [n_B]\varphi_A(Q_B) \rangle$.

The curves E_{AB} and E_{BA} are not necessarily the same as subvarieties of $\mathbb{P}^2$, but they are always isomorphic, hence we use their j-invariant as our shared secret key. In terms of the isogeny graph, Alice starts at the vertex $j(E_0)$, then moves along the edges to $j(E_A)$ thanks to the knowledge of her private isogeny φ_A. Finally, she uses φ'_B to arrive to the vertex $j(E_{AB})$. Bob proceeds analogously.

To sum up:

Public parameters		Primes a, b and $p = \ell_A^a \ell_B^b \cdot f \pm 1$ $E_0/\mathbb{F}_q$, where $\mathbb{F}_q = \mathbb{F}_{p^2}$ $\{P_A, Q_A\}$ a basis for $E_0[\ell_A^a]$ $\{P_B, Q_B\}$ a basis for $E_0[\ell_B^b]$
	Alice	**Bob**
Private parameters	$m_A, n_A \in \mathbb{Z}/\ell_A^a\mathbb{Z}$ (not both divisible by ℓ_A)	$m_B, n_B \in \mathbb{Z}/\ell_B^b\mathbb{Z}$ (not both divisible by ℓ_B)
Computed secret isogeny	$\varphi_A : E_0 \to E_A$, where $E_A = E_0/\langle [m_A]P_A + [n_A]Q_A \rangle$	$\varphi_B : E_0 \to E_B$, where $E_B = E_0/\langle [m_B]P_B + [n_B]Q_B \rangle$
Computed and exchanged public data	$E_A, \varphi_A(P_B), \varphi_A(Q_B)$	$E_B, \varphi_B(P_A), \varphi_B(Q_A)$
Computed shared secret	$j(E_{AB})$	$j(E_{BA})$

Figure 2.2: SIDH key-exchange protocol.

The difficulty of solving SIDH is called the Supersingular Computational Diffie-Hellman problem (or SSCDH problem). Using the same notation as in Section 2.1, it consists in finding the j-invariant of $E_0/\langle K_A, K_B \rangle$, having access to the same public data. This

problem relies mainly on the Computational Supersingular Isogeny (CSSI) problem, where we have $E_A, \varphi_A(P_B), \varphi_A(Q_B)$, and we need to find a generator K_A for the kernel of φ_A, i.e. we need to find the isogeny. If we knew the isogeny φ_A, we could compute its kernel and then solve $K_A = [m_A]P_A + [n_A]Q_A$ for (m_A, n_A). This turns out to be an easy case of the extended logarithm problem, since E_0 is supersingular, as we can see in [Tes99]. Thus, we could focus our efforts on an attack simply recovering an isogeny. This is easier said than done, as we can see a compilation of all the unsuccessful attempts in [MP19], using techniques such as interpolation, Weil restrictions and graph attacks. The attack we will outline later in the thesis was meant for SIKE (Supersingular Isogeny Key Encapsulation), which is a standardized version of SIDH that was submitted to the NIST (National Institute of Standards of Technology). Contrary to SIDH which is just a key-exchange protocol, SIKE is slightly different as it is a key encapsulation, meaning it has a long term public key.

2.2 Explicit example of key-exchange

Let us compute an explicit example of a Diffie-Hellman key-exchange between Alice and Bob. All computations are done using Sage 10.3 and can be found in Appendix A.1.

Our goal is to have explicit formulas for all maps and curves in the following diagram:

$$\begin{array}{ccc} E_0 & \xrightarrow{\varphi_A} & E_A \\ {\scriptstyle\varphi_B}\downarrow & & \downarrow{\scriptstyle\varphi'_B} \\ E_B & \xrightarrow[\varphi'_A]{} & E_{AB} \end{array}$$

We use the following parameters:

- $\ell_A = 2$ and $\ell_B = 3$;
- $f = 5$;
- $a = 2$ and $b = 1$.

We have $p = 2^2 \cdot 3 \cdot 5 - 1 = 59$[(i)]. We start with the supersingular curve $E_0 : y^2 = x^3 + x$ over $\mathbb{F}_{p^2}$, which has group structure isomorphic to $(\mathbb{Z}/(p+1)\mathbb{Z})^2$. To see this, notice that $q = p^2$, where 2 is even, and that the trace of the Frobenius for $E_0/\mathbb{F}_q$ is $t = -118 = -2p$.

We first want bases $\{P_A, Q_A\}$ and $\{P_B, Q_B\}$ of $E_0[2^2]$ and $E_0[3]$respectively. We get:

$$P_A = (58i + 23, 24i + 37), P_B = (47, 41i).$$

[(i)]This is slightly different from the usual SIKE parameters, which are of the form $p = 2^a 3^b - 1$, but the theory still applies to our example.

As in [FJP14], we use the distortion map $\psi(x, y) = (-x, iy)$ to get Q_A and Q_B:

$$Q_A = \psi(P_A) = (i + 36, 37i + 35), Q_B = \psi(P_B) = (12, 18).$$

A distortion map is an endomorphism ϕ on E such that $\phi(P) \notin \langle P \rangle$. It is known by [GR04] that such map always exists for a supersingular elliptic curve, and that $\langle P, \phi(P) \rangle$ generates $E[r]$ for P a point of order r.
We pick the following secret values:

- $m_A = 3, n_A = 0$;
- $m_B = 2, n_B = 2$.

We compute the isogenies $\varphi_A : E_0 \to E_A$ and $\varphi_B : E_0 \to E_B$, determined by their kernels, i.e. $\langle [m_A]P_A + [n_A]Q_A \rangle$ and $\langle [m_B]P_B + [n_B]Q_B \rangle$ respectively. We get:

- $\langle [m_A]P_A + [n_A]Q_A \rangle = \langle R_A \rangle$, where $R_A = (58i + 23, 35i + 22)$. We then have that φ_A is an isogeny of degree 4 to the curve $E_A : y^2 = x^3 + (23i + 32)x + (10i + 4)$. We can compute it as a rational map explicitly:

$$\varphi_A(x, y) = \left(\frac{x^4 + (3i + 13)x^3 + (-14i - 23)x^2 + (20i - 18)x + 14i + 22}{x^3 + (3i + 13)x^2 + (26i - 5)x + (-3i - 13)}, \right.$$
$$\left. \frac{x^5y + (5i - 10)x^4y + 2x^3y + (2i - 20)x^2y + 5xy + (i + 23)y}{x^5 + (5i - 10)x^4 + (19i - 16)x^3 + (-28i - 12)x^2 + (14i + 23)x + (7i + 3)}\right).$$

- $\langle [m_B]P_B + [n_B]Q_B \rangle = \langle R_B \rangle$, where $R_B = (38i, 49i + 10)$. We then have that φ_B is an isogeny of degree 3 to the curve $E_B : y^2 = x^3 + 5x + 19i$. We can compute it as a rational map explicitly:

$$\varphi_B(x, y) = \left(\frac{x^3 + (-17i)x^2 - 17x + 21i}{x^2 + (-17i)x - 28}, \right.$$
$$\left. \frac{x^3y + (4i)x^2y + 23xy + (14i)y)}{(x^3 + (4i)x^2 - 25x + 2i}\right)$$

Now Alice and Bob can compute the following images:

- $\varphi_A(P_B) = (31i + 13, 46i + 17), \varphi_A(Q_B) = (35i + 12, 11i + 44)$;
- $\varphi_B(P_A) = (27i + 1, 58i + 48), \varphi_B(Q_A) = (18i + 6, 9i + 49)$.

We can now compute φ'_A, φ'_B and E_{AB}, using the kernels $\langle [m_A]\varphi_B(P_A) + [n_A]\varphi_B(Q_A) \rangle$ and $\langle [m_B]\varphi_A(P_B) + [n_B]\varphi_A(Q_B) \rangle$ respectively. We get:

- $\langle [m_A]\varphi_B(P_A) + [n_A]\varphi_B(Q_A) \rangle = \langle K_A \rangle$, where $K_A = (27i + 1, i + 11)$. We then have that φ'_A is an isogeny of degree 4 to the curve $E_{AB} : y^2 = x^3 + (32i + 19)x + 36i$, with $j(E_{AB})$.

- $\langle [m_B]\varphi_A(P_B) + [n_B]\varphi_A(Q_B)\rangle = \langle K_B\rangle$, where $K_B = (20i+50, 16i+54)$. We then have that φ'_B is an isogeny of degree 3 to the curve $E_{AB} : y^2 = x^3 + (32i + 19)x + 36i$.

Chapter 3

Attack of SIDH

The goal of this chapter is to present the attack of SIDH exposed in [MMP+23]. We will first outline the algorithm used to break SIDH as well as the theorem it relies on in Section 3.1. Then, we will prove that theorem in Section 3.2, by splitting the result into four lemmas.

3.1 The algorithm and the main theorem

The attack developed by [MMP+23] consists in solving the Supersingular Isogeny problem with Torsion (SSI-T), described as follows:

Given A, B coprime, $E_0/\mathbb{F}_{p^2}$ and $E_A/\mathbb{F}_{p^2}$ two supersingular elliptic curves connected by a secret isogeny $\varphi_A : E_0 \to E_A$ of degree A, and given the restriction of φ_A to the B-torsion points of E_0 (i.e. $\varphi_A(P_B), \varphi_A(Q_B)$ for $\langle P_B, Q_B \rangle = E_0[B]$), we want to recover φ_A.

The attack relies on the knowledge of some isogeny $\varphi_f : E \to E_0$ of degree $f = B - A$, where we assume without loss of generality that $B > A$. The idea is to construct a (B, B)-isogeny $\Phi : E \times E_A \to X$, where X is an abelian surface, and to recover φ_A from the matrix form of Φ (more precisely, we recover a generator of $\ker(\varphi_A)$, and we can then use Vélu's formulas to recover the isogeny).

The attack developed by [MMP+23] consists in solving the Supersingular Isogeny problem with Torsion (SSI-T), described as follows:

Given A, B coprime, $E_0/\mathbb{F}_{p^2}$ and $E_A/\mathbb{F}_{p^2}$ two supersingular elliptic curves connected by a secret isogeny $\varphi_A : E_0 \to E_A$ of degree A, and given the restriction of φ_A to the B-torsion points of E_0 (i.e. $\varphi_A(P_B), \varphi_A(Q_B)$ for $\langle P_B, Q_B \rangle = E_0[B]$), we want to recover φ_A.

The attack relies on the knowledge of some isogeny $\varphi_f : E \to E_0$ of degree $f = B - A$, where we assume without loss of generality that $B > A$. The idea is to construct a (B, B)-isogeny $\Phi : E \times E_A \to X$, where X is an abelian surface, and to recover φ_A from the matrix

form of Φ (more precisely, we recover a generator of $\ker(\varphi_A)$, and we can then use Vélu's formulas to recover the isogeny).We first consider $g_A : E \to F$ the isogeny with kernel $\widehat{\varphi_f}(\ker(\varphi_A))$, and $g_f : F \to E_A$ the isogeny with kernel $g_A(\ker(\varphi_f))$ such that the following diagram commutes:

$$\begin{array}{ccc} E & \xrightarrow{g_A} & F \\ {\scriptstyle \varphi_f}\downarrow & & \downarrow{\scriptstyle g_f} \\ E_0 & \xrightarrow[\varphi_A]{} & E_A \end{array}.$$

We then consider the isogeny of abelian surfaces defined as

$$\begin{aligned} \Phi : E \times E_A &\to E_0 \times F, \\ (P, Q) &\mapsto (\varphi_f(P) - \widehat{\varphi_A}(Q), g_A(P) + \widehat{g_f}(Q)). \end{aligned}$$

So the isogeny $-\widehat{\varphi_A}$ is the composition of

$$E_A \xrightarrow{0\times \mathrm{id}_A} E \times E_A \xrightarrow{\Phi} E_0 \times F \xrightarrow{\mathrm{pr}_1} E_0,$$

where the first map is the inclusion map with image $\{0\} \times E_A$ and the last is the natural projection map onto the first factor. It is enough to be able to compute each step to be able to evaluate $\widehat{\varphi_A}$, and hence recover $\ker(\varphi_A)$.

Let us now introduce our main theorem, which will allow us to evaluate φ_A and which gives us a description of the kernel of Φ. This theorem was first proved by Kani as Kani's Reducibility Criterion in [Kan97, Theorem 2.6], and was not originally thought for cryptographic purposes.

Theorem 3.1. *Let f, A and B be pairwise coprime integers such that $f = B - A$. Let E, E_A, E_0 and F be elliptic curves connected by isogenies $\varphi_A, \varphi_f, g_A$ and g_f such that the following diagram is commutative:*

$$\begin{array}{ccc} E & \xrightarrow{g_A} & F \\ {\scriptstyle \varphi_f}\downarrow & \searrow^{\varphi} & \downarrow{\scriptstyle g_f} \\ E_0 & \xrightarrow[\varphi_A]{} & E_A \end{array}.$$

In addition, we require that $\deg(\varphi_f) = \deg(g_f)$ and $\deg(\varphi_A) = \deg(g_A)$. Then the isogeny $\Phi \in Hom(E \times E_A, E_0 \times F)$, written as $\begin{pmatrix} \varphi_f & -\widehat{\varphi_A} \\ g_A & \widehat{g_f} \end{pmatrix}$ in its matrix form, is a (B, B)-isogeny with respect to the natural product polarizations on $E \times E_A$ and $E_0 \times F$, and has kernel

$$\ker(\Phi) = \{([A]P, \varphi(P)) | P \in E[B]\}.$$

We will prove this result in Section 3.2.

Finally, we present the algorithm used to recover $\ker(\varphi_A)$, which costs two evaluations of $\widehat{\varphi_f}$ on B-torsion points, an inversion modulo B, and at most two evaluations of a (B, B)-isogeny on A-torsion points.

Algorithm 1 Solving SSI-T, provided an isogeny of degree f

Input: A, B coprime integers, $f = B - A$, supersingular elliptic curves $E_0/\mathbb{F}_{p^2}, E_A/\mathbb{F}_{p^2}$, the existence of a degree-A isogeny $\varphi_A : E_0 \to E_A$ with cyclic kernel, a basis $\{P_B, Q_B\}$ of $E_0[B]$, a basis $\{P_A, Q_A\}$ of $E_0[A]$, auxiliary points $P'_B := \varphi_A(P_B), Q'_B := \varphi_A(Q_B)$, and an isogeny $\varphi_f : E \to E_0$ of degree f.

Output: A generator of $\ker(\varphi_A)$.

1: Let c such that $cf \equiv 1 \pmod{B}$
2: Let $P''_B = [c] \circ \widehat{\varphi_f}(P_B)$ and $Q''_B = [c] \circ \widehat{\varphi_f}(Q_B)$. Using Step 1 and some properties on isogenies, we see that $\varphi_A \circ \varphi_f(P''_B) = P'_B$ and $\varphi_A \circ \varphi_f(Q''_B) = Q'_B$.
3: Let $\Phi : E \times E_A \to E_0 \times F$ be the (B, B)-isogeny with kernel $\ker(\Phi) = \langle([A]P''_B, P'_B), ([A]Q''_B, Q'_B)\rangle$. Indeed, we see that $\langle P''_B, Q''_B\rangle = E[B]$, and $\varphi_A \circ \varphi_f = \varphi$, so this corresponds to the description given in Theorem 3.1.
4: Compute $\Phi(0, P_A) := (P'_A, x)$. Then $P'_A = -\widehat{\varphi_A}(P_A)$.
5: **if** P'_A has order A **then**
6: Return P'_A.
7: **else**
8: Compute $\Phi(0, Q_A) = (Q'_A, y)$, where $Q'_A = -\widehat{\varphi_A}(Q_A)$ and return Q'_A.

In Chapter 4, we will explain how to compute Φ when it is a $(2, 2)$-isogeny.

3.2 Proof of the theorem

We will now prove Theorem 3.1, using four lemmas.

Let us first take a look at the matrix form of the dual of a dimension 2 isogeny. Let E_1, E_2, E'_1, E'_2 be elliptic curves defined over K. For the abelian surface $E_1 \times E_2$, we get an isomorphism

$$\lambda : E_1 \times E_2 \xrightarrow{\begin{pmatrix} \lambda_{E_1} & \\ & \lambda_{E_2} \end{pmatrix}} E_1^\vee \times E_2^\vee \xrightarrow{\nu^{-1}} (E_1 \times E_2)^\vee,$$

using ν as in Proposition 1.28, and the natural polarizations $\lambda_{E_1}, \lambda_{E_2}$. Composing $\begin{pmatrix} \lambda_{E'_1} & \\ & \lambda_{E'_2} \end{pmatrix}$ and $(\nu)^{-1}$, we also have $\lambda' : E'_1 \times E'_2 \xrightarrow{\cong} (E'_1 \times E'_2)^\vee$.

Definition 3.2. *Let $\Phi : E_1 \times E_2 \to E_1' \times E_2'$ be an isogeny represented by the matrix $M = \begin{pmatrix} \varphi_{11} & \varphi_{12} \\ \varphi_{21} & \varphi_{22} \end{pmatrix}$, where $\varphi_{ij} : E_j \to E_i'$. The adjoint of Φ is the isogeny $\tilde{\Phi} : E_1' \times E_2' \to E_1 \times E_2$, represented by the matrix $\tilde{M} = \begin{pmatrix} \widehat{\varphi_{11}} & \widehat{\varphi_{21}} \\ \widehat{\varphi_{12}} & \widehat{\varphi_{22}} \end{pmatrix}$.*

We can then see that the adjoint isogeny is in fact closely related to the dual.

Lemma 3.3. *We have $\tilde{\Phi} = \lambda^{-1} \circ \Phi^\vee \circ \lambda'$, where $\Phi^\vee : (E_1' \times E_2')^\vee \to (E_1 \times E_2)^\vee$ is the dual of Φ.*

Proof. From Proposition 1.29, we know that the matrix description of $\nu \circ \Phi^\vee \circ (\nu')^{-1}$ is given by $\begin{pmatrix} \varphi_{11}^\vee & \varphi_{21}^\vee \\ \varphi_{12}^\vee & \varphi_{22}^\vee \end{pmatrix}$. Using Example 1.34, we have

$$\begin{aligned} \lambda^{-1} \circ \Phi^\vee \circ \lambda' &= \begin{pmatrix} \lambda_{E_1} & \\ & \lambda_{E_2} \end{pmatrix}^{-1} \circ \nu \circ \Phi^\vee \circ (\nu')^{-1} \begin{pmatrix} \lambda_{E_1'} & \\ & \lambda_{E_2'} \end{pmatrix} \\ &= \begin{pmatrix} \lambda_{E_1} & \\ & \lambda_{E_2} \end{pmatrix}^{-1} \circ \begin{pmatrix} \varphi_{11}^\vee & \varphi_{21}^\vee \\ \varphi_{12}^\vee & \varphi_{22}^\vee \end{pmatrix} \circ \begin{pmatrix} \lambda_{E_1'} & \\ & \lambda_{E_2'} \end{pmatrix} \\ &= \tilde{\Phi}. \end{aligned}$$

□

Lemma 3.4. *Let B be a positive integer. An isogeny $\Phi : E_1 \times E_2 \to E_1' \times E_2'$ is a B-isogeny with respect to the product polarizations if and only if $\tilde{\Phi} \circ \Phi = [B]$.*

Proof. Assume Φ is a B-isogeny with respect to the polarizations. By Definition 1.37, Φ is a B-isogeny if and only if $[B] \circ \lambda = \Phi^\vee \circ \lambda' \circ \Phi$. Using Lemma 3.3, we have

$$[B] \circ \lambda = \Phi^\vee \circ \lambda' \circ \Phi \iff [B] = \lambda^{-1} \circ \Phi^\vee \circ \lambda' \circ \Phi = \tilde{\Phi} \circ \Phi.$$

Assume now $\tilde{\Phi} \circ \Phi = [B]$. Then by Lemma 3.3, we have

$$\tilde{\Phi} \circ \Phi = [B] \iff \lambda^{-1} \circ \Phi^\vee \circ \lambda' \circ \Phi = [B] \iff \Phi^\vee \circ \lambda' \circ \Phi = \lambda \circ [B],$$

and $\lambda \circ [B] = [B] \circ \lambda$ since multiplication by B commutes. Thus Φ is a B-isogeny. □

Lemma 3.5. *The map Φ as defined in Theorem 3.1 is a B-isogeny with respect to the product polarizations.*

Proof. The matrix form of Φ is given by $\begin{pmatrix} \varphi_f & -\widehat{\varphi_A} \\ g_A & \widehat{g_f} \end{pmatrix}$, and the matrix of its adjoint is given by $\begin{pmatrix} \widehat{\varphi_f} & \widehat{g_A} \\ -\varphi_A & g_f \end{pmatrix}$. Using Lemma 3.4, as well as the properties of isogenies and of the

commutative diagram:

$$\begin{aligned}\begin{pmatrix}\widehat{\varphi_f} & \widehat{g_A}\\ -\varphi_A & g_f\end{pmatrix}\begin{pmatrix}\varphi_f & -\widehat{\varphi_A}\\ g_A & \widehat{g_f}\end{pmatrix} &= \begin{pmatrix}\widehat{\varphi_f}\circ\varphi_f + \widehat{g_A}\circ g_A & -\widehat{\varphi_f}\circ\widehat{\varphi_A} + \widehat{g_A}\circ\widehat{g_f}\\ -\varphi_A\circ\varphi_f + g_f\circ g_A & \varphi_A\circ\widehat{\varphi_A} + g_f\circ\widehat{g_f}\end{pmatrix}\\ &= \begin{pmatrix}[\deg(\varphi_f)] + [\deg(g_A)] & 0\\ 0 & [\deg(\varphi_A)] + [\deg(g_f)]\end{pmatrix}\\ &= \begin{pmatrix}[B] & 0\\ 0 & [B]\end{pmatrix}.\end{aligned}$$

□

Lemma 3.6. *With Φ as in Theorem 3.1, we have* $\ker(\Phi) = \{([A]P, \varphi(P)) | P \in E[B]\}$.

Proof. Let $K := \{([A]P, \varphi(P)) | P \in E[B]\}$. We want to show $K = \ker(\Phi)$.

- $K \subset \ker(\Phi)$: For any $P \in E[B]$, using the commutative diagram and the commutative properties of the multiplication by A, we have

$$\begin{aligned}\Phi([A]P, \varphi(P)) &= (\varphi_f([A]P) - \widehat{\varphi_A}\circ\varphi(P), g_A([A]P) + \widehat{g_f}\circ\varphi(P))\\ &= ([A]\circ\varphi_f(P) - \widehat{\varphi_A}\circ\varphi_A\circ\varphi_f(P), [A]\circ g_A(P) + \widehat{g_f}\circ g_f\circ g_A(P))\\ &= ([A-A]\circ\varphi_f(P), [A+f]\circ g_A(P))\\ &= (0, [B]\circ g_A(P))\\ &= (0,0)\end{aligned}$$

- $\ker(\Phi) \subset K$: Take $([A]P, Q) \in \ker(\Phi)$. Then, since $\varphi_f([A]P) - \widehat{\varphi_A}(Q) = 0$, we have $\varphi_f([A]P) = \widehat{\varphi_A}(Q)$ and

$$\begin{aligned}[A]\circ\varphi(P) &= \varphi([A]P)\\ &= \varphi_A\circ\varphi_f([A]P)\\ &= \varphi_A\circ\widehat{\varphi_A}(Q)\\ &= [A]Q\end{aligned}$$

Since $P \in E[B]$ by definition and A, B are coprime, then we deduce that $Q = \varphi(P)$. So we have $([A]P, Q) \in K$. □

We then have all the tools to prove the theorem.

Proof of Theorem 3.1. The theorem follows from Lemma 3.5 and Lemma 3.6: Φ is a B-isogeny with respect to the product polarizations. The kernel is isomorphic to $(\mathbb{Z}/B\mathbb{Z})^2$ due to P being in $E[B]$, and that $P \mapsto ([A]P, \varphi(P))$ is injective. Hence it is a (B, B)-isogeny. □

Chapter 4

Computing $(2,2)$-isogenies

In this last chapter, we formalize the notions of quadratic splittings and Richelot isogenies in Section 4.1, so that we are able to describe in Section 4.2 the different types of (B,B)-isogenies we use during the evaluation of the algorithm. Given the current state of research, we only focus on the case $B = 2^a$. Hence we are computing chains of length a of $(2,2)$-isogenies in order to evaluate $\Phi : E \times E_A \to E_0 \times F$. From the Matsusaka-Ran criterion over the complex numbers, proved in [BL04, Corollary 11.8.2], we know that a principally polarized abelian surface is either the Jacobian of a smooth curve of genus 2 or the canonically polarized product of two elliptic curves. This also holds for algebraically closed fields of positive characteristic, and over finite fields, we can have some rare exceptions where this does not hold. They are however so rare that they can be ignored, as we can see in [HNR07, Theorem 1.3]. So we need to be able to compute three types of $(2,2)$-isogenies:

- $(2,2)$-isogenies from a product of two elliptic curves to the Jacobian of a genus 2 curve, as it is required in the first step of Φ;
- $(2,2)$-isogenies between Jacobians of genus 2 curves, as it is required in the $(a-2)$-steps between the first step and the last step of Φ;
- $(2,2)$-isogenies between a Jacobian of a genus 2 curve and the product of two elliptic curves, as it is required in the last step of Φ.

4.1 Quadratic splittings and Richelot isogenies

Continuing with the work of [Smi05, Chapter 8], we assume that for X a hyperelliptic curve of genus 2 over K, with $\mathrm{char}(K) \neq 2$, we have an affine plane model given by $X : y^2 = f_X(x) = \prod_{i=1}^{6}(x - \alpha_i)$, where the α_i's can be in some extension $\bar{K}$. The main aspect we want to notice here is that the hyperelliptic cover $h_X : X \to \mathbb{P}^1$ ramifies in six points, called the Weierstrass points and given by $\omega_i = (\alpha_i, 0) \in X(\bar{K})$. Thanks

to this factorization, we will have a way to represent $(2,2)$-isogenies through something called quadratic splittings. We can find a classical exposition to the theory of quadratic splittings and of Richelot isogenies in [CF96, Chapter 9].

We start by describing Richelot isogenies.

Definition 4.1. *Let $\mathcal{A}$ be a principally polarized abelian surface. Then a* ***Richelot isogeny***

$$\phi : \mathcal{A} \to \mathcal{A}/G$$

is an isogeny for which $G \cong (\mathbb{Z}/2\mathbb{Z})^2$ is a maximal 2-Weil-isotropic subgroup of $\mathcal{A}[2]$. Recall that being a maximal 2-Weil-isotropic subgroup of $\mathcal{A}[2]$ means that the Weil pairing $e_{\mathcal{A},2} : \mathcal{A}[2] \times \mathcal{A}[2] \to \mu_2$ is trivial on G, and G is not properly contained in another subgroup on which the pairing vanishes.

Lemma 4.2. *Let R be a proper, non-trivial subgroup of $J_X[2]$. If R is the kernel of an isogeny of principally polarized abelian surfaces, then R is a maximal 2-Weil-isotropic subgroup of $J_X[2]$.*

Then, by the non-degeneracy of the Weil pairing and since J_X is a principally polarized abelian surface, the maximal 2-Weil-isotropic subgroups of $J_X[2]$ are isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$. By the previous Lemma, if $\mathcal{A}$ is a principally polarized abelian surface and if $\phi : J_X \to \mathcal{A}$ is an isogeny respecting the polarizations such that $\ker \phi$ is a proper, non-trivial subgroup of $J_X[2]$, then ϕ is a $(2,2)$-isogeny. Such kernels are called $(2,2)$-subgroups.

Lemma 4.3. *Each non-zero element of $J_X[2]$ may be uniquely represented by a pair of distinct Weierstrass points of X.*

Proof. Let $P_{i,j} = [(\alpha_i, 0)] - [(\alpha_j, 0)]$, where $(\alpha_i, 0)$ and $(\alpha_j, 0)$ are two Weierstrass points. $P_{i,j}$ is not the divisor of a function on X (by [Sto19, Section 4], if the difference $[P] - [Q]$ of P, Q, two points of a hyperelliptic curve, was a principal divisor, then the hyperelliptic curve would be isomorphic to $\mathbb{P}^1$, which is a contradiction), so its image in J_X is non-zero. We know $2P_{i,j} = \operatorname{div}\left(\frac{(x-\alpha_i)}{(x-\alpha_j)}\right)$, so $2P_{i,j}$ is linearly equivalent to 0 in $\mathrm{Pic}(X)$, and the image of $P_{i,j}$ in J_X is a non-zero element of $J_X[2]$. By definition, $P_{i,j} = -P_{j,i}$, and since $2P_{i,j} = 0$, we also have $[P_{i,j}] = [P_{j,i}]$. So $[P_{i,j}]$ is determined by the unordered pair $\{i, j\}$. We can easily verify that $P_{i,j} + P_{k,l}$ is principal if and only if $\{i, j\} = \{k, l\}$ (indeed, if $\{i, j\} = \{k, l\}$, we know $2P_{i,j}$ is principal, and $P_{i,j} + P_{k,l} = P_{i,j} - P_{l,k}$ can only be principal if $P_{i,j} = P_{l,k}$, i.e. $\{i, j\} = \{l, k\}$), so each pair $\{i, j\}$ uniquely specifies an element of $J_X[2]$. Since $J_X[2] \cong (\mathbb{Z}/2\mathbb{Z})^4$, there are 15 non-zero elements of $J_X[2]$, and since $\binom{6}{2} = 15$, there are 15 distinct pairs of distinct Weierstrass points of X, and we conclude. □

Then, every rational linear factor $a(x - \alpha_i)$ of f_X represents a rational Weierstrass point, and each rational quadratic factor $a(x-\alpha_i)(x-\alpha_j)$ represents a rational pair of Weierstrass

points, hence a rational element $[P_{ij}] \in J_X[2]$. We want to focus only on sets of quadratic factors representing $(2,2)$-subgroups, so we need the following.

Lemma 4.4. *Let P, Q be distinct non-zero elements of $J_X[2]$, represented by quadratic factors G_P, G_Q of f_X. Then the 2-Weil pairing $e_2(P,Q)$ of P and Q is trivial if and only if G_P and G_Q are coprime.*

The $(2,2)$-subgroups of $J_X[2]$ are represented by sets of three pairwise coprime quadratic factors of f_X. This introduces the idea of quadratic splittings, which we will now formalize.

Definition 4.5. *Let $K[x]_{\leq 2}$ be the K-vector space of polynomials of degree at most two, with a Lie algebra structure given by the bracket $[f,g] := \frac{df}{dx} \cdot g - \frac{dg}{dx} \cdot f$, for $f, g \in K[x]_{\leq 2}$. We need to define two important maps:*

- *First, we define a **determinant map***

$$\det : K[x]^3_{\leq 2} \to K.$$

Take $G = (G_1, G_2, G_3) \in K[x]^3_{\leq 2}$, where $G_i = g_{i,3}x^2 + g_{i,2}x + g_{i,1}$ for $1 \leq i \leq 3$. Then, the map is given by

$$\det(G) := \det \begin{pmatrix} g_{1,1} & g_{1,2} & g_{1,3} \\ g_{2,1} & g_{2,2} & g_{2,3} \\ g_{3,1} & g_{3,2} & g_{3,3} \end{pmatrix}.$$

- *We also have the **product map***

$$\prod : K[x]^3_{\leq 2} \to K[x],$$

where

$$\prod(G_1, G_2, G_3) := G_1 G_2 G_3.$$

In general, for each hyperelliptic polynomial f_X, we have a factorization into three polynomials of degree at most two (either three quadratics, or two quadratics and one linear polynomial).

Definition 4.6. *Let $\mathcal{H} = \{f \in K[x] : \deg f \in \{5,6\}, f \text{ square-free}\}$ be the set of all hyperelliptic polynomials of curves of genus 2 over K. The set of **quadratic splittings** is*

$$\mathcal{S} := (\Pi^{-1}(\mathcal{H}))/\sim,$$

*where $\sim$ denotes the equivalence relation defined by $(G_1, G_2, G_3) \sim (G_2, G_3, G_1) \sim (G_3, G_1, G_2)$ and $(G_1, G_2, G_3) \sim (\alpha G_1, \beta G_2, \gamma G_3)$ for all $\alpha, \beta, \gamma \in K^\times$ such that $\alpha\beta\gamma = 1$. We denote the image of G in $\mathcal{S}$ by $[G]$. For an element $f \in \mathcal{H}$, the set of **quadratic splittings of** f is denoted by $\mathcal{S}_f = \Pi^{-1}(f)$.*

We now need to define an involution.

Definition 4.7. *The* ***negation*** $\nu : \mathcal{S} \to \mathcal{S}$ *is given by*

$$\nu([(G_1, G_2, G_3)]) = [(G_1, G_3, G_2)],$$

and $\nu(G)$ *is the* ***negative*** *of* G*.*

It is clear that $\Pi(\nu(G)) = \Pi(G)$, so negation stabilizes each subset $\mathcal{S}_f \subset \mathcal{S}$.

Definition 4.8. *Let* $|\mathcal{S}_f|$ *denote the quotient of* $\mathcal{S}_f$ *by* $\langle\nu\rangle$*. Then, if* G *is a quadratic splitting of* f*, its image in* $|\mathcal{S}_f|$ *is denoted* $|G|$*, and it is the* ***unsigned quadratic splitting of*** f*. Since a quadratic splitting can't be its own negative, every unsigned quadratic splitting corresponds exactly to two quadratic splittings.*

We now have our main result.

Proposition 4.9. *Let* $X : y^2 = f_X(x)$ *be a curve of genus 2. Then, the rational* $(2,2)$*-subgroups of* $J_X[2]$ *are in bijection with the unsigned quadratic splittings of* f_X*.*

Proof. We know already that each $(2,2)$-subgroup R of $J_X[2]$ has three non-zero elements P_1, P_2, P_3, each corresponding to a quadratic factor G_{P_i} of f_X. By Lemma 4.4 and by definition of R, we have that R is 2-Weil-isotropic if and only if the G_{P_i}'s are pairwise coprime, which is equivalent to say that $G_{P_1}G_{P_2}G_{P_3} = cf_X$ for some $c \in K^\times$. Then, without loss of generality we can take $c = 1$ (or divide G_{P_3} by c), and we get a uniquely determined pair $[(G_{P_1}, G_{P_2}, G_{P_3})]$ and $[(G_{P_1}, G_{P_3}, G_{P_2})]$ of quadratic splitting of f_X. Notice that $\nu([(G_{P_1}, G_{P_2}, G_{P_3})]) = [(G_{P_1}, G_{P_3}, G_{P_2})]$ and $\nu([(G_{P_1}, G_{P_3}, G_{P_2})]) = [(G_{P_1}, G_{P_2}, G_{P_3})]$. So we have a uniquely determined unsigned quadratic splitting $|[(G_{P_1}, G_{P_2}, G_{P_3})]|$ and we conclude. □

This is important because we know that $(2,2)$-subgroups are the kernels of $(2,2)$-isogenies. Hence we will study $(2,2)$-isogenies by studying unsigned quadratic splittings. We will see later that we can determine if X is the Jacobian of a genus 2 curve or the product of two elliptic curves by looking at the determinant of the quadratic splitting of its hyperelliptic polynomial.

Definition 4.10. *Let* G *be the quadratic splitting of some hyperelliptic polynomial* f_X*. We say* G *is* ***singular*** *if* $\det(G) = 0$*. Otherwise, we say* G *is* ***non-singular****, and we denote the set of non-singular quadratic splittings by* $\mathcal{S}^{\text{ns}}$*.*

We will first study the case of G singular. Let us first study a particular case, where the polynomial of the hyperelliptic curve has no terms of odd degree. In this case, we can apply a result from [CF96, Chapter 14].

Theorem 4.11. *Let X be a curve of genus 2. We say two curves given by some equation $y^2 = f_X(X)$ are equivalent if they are taken into one another by a fractional linear transformation of x and the related transformation of y. The following properties are then equivalent:*

(1) X is equivalent to a curve $y^2 = c_3x^6 + c_2x^4 + c_1x^2 + c_0$ with no terms of odd degree in X.

(2) X is equivalent to a curve $y^2 = G_1(x)G_2(x)G_3(x)$, where the $G_i(x)$ are linearly dependent quadratics.

If one of those conditions is satisfied, the Jacobian of X is reducible and is isomorphic to the product of two elliptic curves E_1, E_2. The equations of those curves are given by

$$E_1 : y^2 = c_3z^3 + c_2z^2 + c_1z + c_0 \text{ with } z = x^2,$$

and

$$E_2 : v^2 = c_0u^3 + c_1u^2 + c_2u + c_3 \text{ with } y = x^{-2}, v = yx^{-3}.$$

Proof.

- (1) $\implies$ (2): Assume X is equivalent to a curve $y^2 = c_3x^6 + c_2x^4 + c_1x^2 + c_0$. Then we can write it as $y^2 = c_6(x^2 - b_1)(x^2 - b_2)(x^2 - b_3)$ for some $b_1, b_2, b3 \in K$. Then, setting $G_i := (x^2 - b_i)$, we are in case (2) as we have three polynomials with no linear factors.

- (2) $\implies$ (1): Assume X is equivalent to a curve $y^2 = G_1(x)G_2(x)G_3(x)$, where the $G_i(x)$ are linearly dependent quadratics. Since no two of the G_i's have a common root, there are two distinct singular quadratics in the splitting, we call them $(x - \lambda)^2$ and $(x-\nu)^2$. We can then map into a form of equation (1) by substituting $(x-\lambda)/(x-\nu)$ for x.

□

If the hyperelliptic polynomial has terms of odd degrees, we refer to the following construction.

Construction. *Let G be a singular splitting of f_X. Since $\det(G) = 0$, there is a linear dependency between G_1, G_2 and G_3. Since $G_1, G_2 \in K[x]_2$, we can construct a pair of linear polynomials $x_1 = (x - \alpha)$ and $x_2 = (x - \beta)$, together with $a_{11}, a_{12}, a_{21}, a_{22} \in K$ such that $G_1 = a_{11}x_1^2 + a_{12}x_2^2$ and $G_2 = a_{21}x_1^2 + a_{22}x_2^2$. Then G_3 can be expressed as a linear combination of G_1 and G_2, hence in terms of x_1 and x_2, so there exist $a_{31}, a_{32} \in K$ such*

that $G_3 = a_{31}x_1^2 + a_{32}x_2^2$. *To do so, we write:*

$$\begin{aligned} G_1 &= a_{11}x_1^2 + a_{12}x_2^2 \\ &= a_{11}(x-\alpha)^2 + a_{12}(x-\beta)^2 \\ &= a_{11}(x^2 - 2\alpha x + \alpha^2) + a_{12}(x^2 - 2\beta x + \beta^2) \\ &= (a_{11}+a_{12})x^2 - 2(a_{11}\alpha + a_{12}\beta)x + a_{11}\alpha^2 + a_{12}\beta^2, \end{aligned}$$

and similarly, we have

$$G_2 = (a_{21}+a_{22})x^2 - 2(a_{21}\alpha + a_{22}\beta)x + a_{21}\alpha^2 + a_{22}\beta^2.$$

We can then solve the following:

$$\begin{cases} a_{11} + a_{12} = g_{1,3} \\ -2(a_{11}\alpha + a_{12}\beta) = g_{1,2} \\ a_{11}\alpha^2 + a_{12}\beta^2 = g_{1,1} \\ a_{21} + a_{22} = g_{2,3} \\ -2(a_{21}\alpha + a_{22}\beta) = g_{2,2} \\ a_{21}\alpha^2 + a_{22}\beta^2 = g_{2,1} \end{cases},$$

and get the values of a_{31}, a_{32} *from it. Then, we write* X *as*

$$X : y^2 = G_1G_2G_3 = \prod_{i=1}^{3}(a_{i1}x_1^2 + a_{i2}x_2^2).$$

If E_1 *and* E_2 *are the two curves of genus* 1 *defined by*

$$E_1 : y^2 = \prod_{i=1}^{3}(a_{i1}x + a_{i2}),\ \ E_2 : y^2 = \prod_{i=1}^{3}(a_{i1} + a_{i2}x),$$

then there are distinct coverings $\psi_1 : X \to E_1,\ \psi_2 : X \to E_2$ *of degree two given by*

$$\psi_1(x,y) = \left(\left(\frac{x_1}{x_2}\right)^2, \frac{y}{x_2^3}\right),\ \ \psi_2(x,y) = \left(\left(\frac{x_2}{x_1}\right)^2, \frac{y}{x_1^3}\right).$$

Thanks to this construction, we can see more formally what happens when the quadratic splitting of f_X is singular.

Proposition 4.12. *Let* X *be a curve of genus 2. If* f_X *has a singular quadratic splitting* $G = [(G_1, G_2, G_3)]$, *then* J_X *is* $(2,2)$*-isogenous to the product* $E_1 \times E_2$ *of elliptic curves constructed as above.*

Proof. Given the curve X and the singular splitting G, we want to construct the curves E_1, E_2 and their covers $\psi_1 : X \to E_1, \psi_2 : X \to E_2$ as discussed above. Consider J_X an abelian surface. Taking the pullbacks, we see that $\psi_1^*(J_{E_1})$ and $\psi_2^*(J_{E_2})$ are one-dimensional abelian subvarieties of J_X. So J_X is not simple and is isogenous to a product of elliptic curves.

Moreover, taking the pushforwards $\psi_{1*} : J_X \to J_{E_1}, \psi_{2*} : J_X \to J_{E_2}$, which are homomorphisms, we see that the curves J_{E_1} and J_{E_2} are isogeny factors of J_X. We know $G_i = a_{i1}x_1^2 + a_{i2}x_2^2$ and $\psi_1(x,y) = \left(\left(\frac{x_1}{x_2}\right)^2, \frac{y}{x_2^3}\right)$. Then, since every quadratic factor is determined by a pair of Weierstrass points, the 2-torsion subgroup $J_X[2]$ is generated by the difference of the points given by $P_i = \left(-\frac{a_{i,2}}{a_{i,1}}, 0\right)$ for $1 \leq i \leq 3$. So $\psi_1^{-1}(P_i) = \{(r_i, 0), (r_i', 0)\}$, where r_i, r_i' are the roots of G_i. Then $[(r_i, 0) - (r_i', 0)] \in J_X[2]$ maps to $[P_i] - [P_j] \in J_{E_1}[2]$, and this image is zero if and only if $i = j$. We can use the same argument for ψ_2 and $J_{E_2}[2]$. Finally, using Proposition 4.9, we conclude that the kernel of the map $\psi_{1*} \times \psi_{2*} : J_X \to E_1 \times E_2$ is the subgroup specified by the unsigned singular splitting $|G|$. Hence J_X is $(2,2)$-isogenous to the product of elliptic curves $E_1 \times E_2$. □

Let us now see the case of non-singular quadratic splittings, which will be useful to work with $(2,2)$-isogenies between Jacobians of genus 2 curves. We first need a new operator.

Definition 4.13. *The **Richelot operator** is given by*

$$\mathcal{R} : \{G \in K[x]_2^3 : \det(G) \neq 0\} \to K[x]_2^3,$$

$$(G_1, G_2, G_3) \mapsto (\delta[G_2, G_3], \delta[G_3, G_1], \delta[G_1, G_2]),$$

where $\delta = (\det(G))^{-1}$.

Notice first that the Richelot operator induces a well-defined involution $\mathcal{R}(.) : \mathcal{S}^{\text{ns}} \to \mathcal{S}^{\text{ns}}$ on non-singular quadratic splittings. Indeed, taking $G_1, G_2, G_3 \in K[x]_2$ such that $\det(G_1, G_2, G_3) \neq 0$ and $\Pi(G_1, G_2, G_3)$ of degree 5 or 6, then $\Pi(\mathcal{R}(G_1, G_2, G_3))$ is also of degree 5 or 6, and $\mathcal{R}(\mathcal{R}(G)) = G$.

Definition 4.14. *Let $X : y^2 = f_X(x)$ be a curve of genus 2. For each non-singular quadratic splitting G of f_X, we define X_G to be the curve given by*

$$X_G : y^2 = f_{X_G}(x) = \Pi(\mathcal{R}(G)).$$

Then X_G is also a curve of genus 2.

We now need to study some properties of correspondences, so that we are able to properly describe Richelot isogenies. The main idea of correspondences is the following: given two curves X and Y, we want to relate divisors on $X \times Y$ to homomorphisms between

the Jacobians J_X and J_Y. In particular, we will want to work on correspondences $X \times X_G$, as we're interested in homomorphisms from J_X to J_{X_G}.

Definition 4.15. *A **correspondence** on $X \times Y$ is a divisor C on $X \times Y$. We call it **prime** if the divisor is also prime.*

If C is a prime correspondence on $X \times Y$, then the usual projections $\pi_1 : X \times Y \to X$ and $\pi_2 : X \times Y \to Y$ restrict to non-constant morphisms of curves $\pi_1^C : C \to X$ and $\pi_2^C : C \to Y$. So we can see correspondences on $X \times Y$ as formal sums of curves C with morphisms to X and Y.

Definition 4.16. *If C is a prime correspondence on $X \times Y$, then we define the **degrees of** C as*

$$d_1(C) := \deg \pi_1^C,\ d_2(C) := \deg \pi_2^C.$$

*We say C is a (a,b)**-correspondence** if $d_1(C) = a$ and $d_2(C) = b$.*

Then, viewing C as a curve, we have coverings $\pi_1^C : C \to X$, $\pi_2^C : C \to Y$, and we can compose the pullback ${\pi_1^C}^*$ and the pushforward ${\pi_2^C}_*$ to obtain a homomorphism from $\mathrm{Div}(X)$ to $\mathrm{Div}(Y)$. Therefore, there is also an induced homomorphism from J_X to J_Y.

Definition 4.17. *Let $C = \sum_i n_i C_i$ be a correspondence on $X \times Y$, with each of the C_i's being prime. Then, the **induced homomorphism** of C is defined as*

$$\phi_C := \sum_i n_i ({\pi_2^{C_i}}_*) \circ ({\pi_1^{C_i}}^*).$$

By convention, we take ϕ_C to indicate the induced homomorphism of Jacobians.

The map $C \mapsto \phi_C$ gives a homomorphism from $\mathrm{Div}(X \times Y)$ to $\mathrm{Hom}(J_X, J_Y)$.

We can now focus on the case $X \times X_G$. Let (G_1, G_2, G_3) be a representative for G a non-singular quadratic splitting of f_X in $K[x]_2^3$ and let $(H_1, H_2, H_3) = \mathcal{R}((G_1, G_2, G_3))$. Setting $F = G_1(u_1)H_1(u_2) + G_2(u_1)H_2(u_2)$ for some variables u_1, u_2, the fact that $\sum_{i=1}^{3} G_i(u_1)H_i(u_2) + (u_1 - u_2)^2 = 0$ implies

$$f_X(u_1) f_{X_G}(u_2) \equiv G_1(u_1)^2 H_1(u_2)^2 (u_1 - u_2)^2 \pmod{F}.$$

Then, on $X \times X_G$, we have:

$$V(F) = V(F, v_1^2 v_2^2 - f_X(u_1) f_{X_G}(u_2)),$$

for v_1, v_2 some variables.

Definition 4.18. *Let X be a curve of genus 2, and (G_1, G_2, G_3) a representative for G a non-singular quadratic splitting of f_X in $K[x]_2^3$. Let (H_1, H_2, H_3) be defined as before. Then, a correspondence on $X \times X_G$ is given by*

$$C_{(G_1,G_2,G_3)} := V \begin{pmatrix} G_1(u_1)H_1(u_2) + G_2(u_1)H_2(u_2), \\ v_1v_2 - G_1(u_1)H_1(u_2)(u_1 - u_2) \end{pmatrix}.$$

*We call $C_{(G_1,G_2,G_3)}$ a **Richelot correspondence**.*

Since $C_{(G_1,G_2,G_3)} \neq C_{(G_1,G_3,G_2)}$, we can't associate a unique Richelot correspondence to G. Instead, we see that in the non-singular case, all the Richelot correspondences for G are homomorphically equivalent, i.e. all correspondences induce the same homomorphism of Jacobians as in Definition 4.17.

Corollary 4.19. *For every non-singular quadratic splitting G of f_X, there is a well-defined homomorphism $\rho_G : J_X \to J_{X_G}$, given by $\rho_G = \phi_{C_{(G_1,G_3,G_2)}}$. We say ρ_G is the Richelot isogeny of G.*

This brings us to our main result, which describes $(2,2)$-isogenies between Jacobians of genus 2 curves.

Theorem 4.20. *Let $X : y^2 = f_X(x)$ be a curve of genus 2. For G a non-singular quadratic splitting of f_X, then $\rho_G : J_X \to J_{X_G}$ is a $(2,2)$-isogeny and the kernel of ρ_G is the $(2,2)$-subgroup specified by $|G|$. Also, $\rho_G(J_X[2])$ is the $(2,2)$-subgroup specified by $|\mathcal{R}(G)|$.*

Proof. Let us fix some representative (G_1, G_2, G_3) of G in $K[x]_2^3$. Let $i : X_G \to X'_G$ be the isomorphism given by $i(x, y) = (x, \det(G)y)$, where X'_G is some hyperelliptic curve. We know that ρ_G is a Richelot isogeny, which is by definition a $(2,2)$-isogeny, with kernel specified by $|G|$ from Proposition 4.9. Then the composition $i_* \circ \rho_G$ is also a Richelot isogeny, and by Definition 4.14, we see that $\rho_G(J_X[2])$ is the $(2,2)$-subgroup specified by $|\mathcal{R}(G)|$. □

4.2 Explicit constructions of the $(2,2)$-isogenies

4.2.1 $(2,2)$-isogenies between a product of elliptic curves and a Jacobian

First, we want to construct and evaluate a $(2,2)$-isogeny from a product of elliptic curves to a Jacobian of a curve of genus 2. We use the notations of Section 3.1 for the elliptic curves and the points. Using [CD22], we will first describe how to glue the curves E and E_A into the Jacobian of a genus 2 curve H, via the $(2,2)$-subgroup $\langle (2^{a-1}\varphi_f(P_A), 2^{a-1}P), (2^{a-1}\varphi_f(Q_A), 2^{a-1}Q) \rangle$, where $\langle P, Q \rangle = E_A[2^a]$ and $\varphi_A(P_A) = P, \varphi_A(Q_A) = Q$ for $\langle P_A, Q_A \rangle = E_0[2^a]$.

Proposition 4.21. *Let $E/\mathbb{F}_{p^2} : y^2 = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$ and $E_A/\mathbb{F}_{p^2} : y^2 = (x-\beta_1)(x-\beta_2)(x-\beta_3)$ be two elliptic curves. Let Δ_α be the discriminant of $(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$ and Δ_β be the discriminant of $(x-\beta_1)(x-\beta_2)(x-\beta_3)$. We also define the following:*

$$\begin{aligned}
a_1 &= \frac{(\alpha_3-\alpha_2)^2}{\beta_3-\beta_2} + \frac{(\alpha_2-\alpha_1)^2}{\beta_2-\beta_1} + \frac{(\alpha_1-\alpha_3)^2}{\beta_1-\beta_3},\\
b_1 &= \frac{(\beta_3-\beta_2)^2}{\alpha_3-\alpha_2} + \frac{(\beta_2-\beta_1)^2}{\alpha_2-\alpha_1} + \frac{(\beta_1-\beta_3)^2}{\alpha_1-\alpha_3},\\
a_2 &= \alpha_1(\beta_3-\beta_2) + \alpha_2(\beta_1-\beta_3) + \alpha_3(\beta_2-\beta_1),\\
b_2 &= \beta_1(\alpha_3-\alpha_2) + \beta_2(\alpha_1-\alpha_3) + \beta_3(\alpha_2-\alpha_1),\\
A &= \Delta_\beta \frac{a_1}{a_2},\\
B &= \Delta_\alpha \frac{b_1}{b_2},\\
h(x) &= -\left(A(\alpha_2-\alpha_1)(\alpha_1-\alpha_3)x^2 + B(\beta_2-\beta_1)(\beta_1-\beta_3)\right)\\
&\quad \cdot \left(A(\alpha_3-\alpha_2)(\alpha_2-\alpha_1)x^2 + B(\beta_3-\beta_2)(\beta_2-\beta_1)\right)\\
&\quad \cdot \left(A(\alpha_1-\alpha_3)(\alpha_3-\alpha_2)x^2 + B(\beta_1-\beta_3)(\beta_3-\beta_2)\right).
\end{aligned}$$

Then the $(2,2)$-isogeny with domain $E \times E_A$ and kernel $\langle((\alpha_1,0),(\beta_1,0)),((\alpha_2,0),(\beta_2,0))\rangle$ has as codomain the Jacobian of a genus 2 curve H given by $y^2 = h(x)$. Moreover, the degree-2 morphisms are given by

$$\begin{aligned}
&\varphi_1 : H \to E\\
&\quad (x,y) \mapsto \left(\frac{s_1}{x^2} + s_2, (\Delta_\beta/A^3)\frac{y}{x^3}\right),\\
&\varphi_2 : H \to E_A\\
&\quad (x,y) \mapsto (t_1x^2 + t_2, (\Delta_\alpha/B^3)y),
\end{aligned}$$

where

$$\begin{aligned}
s_1 &= -\frac{B}{A}\left(\frac{a_2}{a_1}\right),\\
s_2 &= \frac{1}{a_1}\left(\frac{\alpha_1(\alpha_3-\alpha_2)^2}{\beta_3-\beta_2} + \frac{\alpha_2(\alpha_1-\alpha_3)^2}{\beta_1-\beta_3} + \frac{\alpha_3(\alpha_2-\alpha_1)^2}{\beta_2-\beta_1}\right),\\
t_1 &= -\frac{A}{B}\left(\frac{b_2}{b_1}\right),\\
t_2 &= \frac{1}{b_1}\left(\frac{\beta_1(\beta_3-\beta_2)^2}{\alpha_3-\alpha_2} + \frac{\beta_2(\beta_1-\beta_3)^2}{\alpha_1-\alpha_3} + \frac{\beta_3(\beta_2-\beta_1)^2}{\alpha_2-\alpha_1}\right).
\end{aligned}$$

Then the φ_i's extend to the Jacobian and combine in a $(2,2)$-isogeny $\Psi : J_H \to E \times E_A$ by mapping $[\sum_j P_j] \mapsto \sum_j \varphi(P_j)$.

Here, we are interested in the dual $\widehat{\Psi} : E \times E_A \to J_H$, and we want to evaluate the image of $(\varphi_f(P_A), P) \in E \times E_A$ under $\widehat{\Psi}$. To make things easier, take $[D] \in \Psi^{-1}\{(\varphi_f(P_A), P)\} \subset J_H$ and notice the following property:

$$2[D] = \widehat{\Psi}\Psi([D]) = \widehat{\Psi}(\varphi_f(P_A), P).$$

Thus it is enough to compute some $[D]$ such as above and double it. Let $D = P_H + Q_H - \infty_1 - \infty_2$ be a point on J_H, with Mumford representation $[x^2 + u_1 x + u_0, v_1 x + v_0]$. Our goal is to express $\varphi_i(P_H + Q_H)$ for $i = 1, 2$ in terms of u_0, u_1, v_0, v_1. We focus on $P_H + Q_H$ as the divisor $\infty_1 + \infty_2$ maps to ∞ both under φ_1 and φ_2. Let us start by calculating φ_2. The line connecting $\varphi_2(P_H)$ and $\varphi_2(Q_H)$ has slope

$$\lambda_2 = -\frac{(\Delta_\alpha / B^3) v_1}{t_1 u_1}.$$

Set now $\omega_2 = \lambda_2^2 + \sum_{i=1}^{3} \beta_i - t_1(u_1^2 - 2u_0) - 2t_2$, so then

$$\varphi_2(P_H + Q_H) = \left(\omega_2, -\lambda_2 \left(\omega_2 - t_2 + (u_0 v_1 - u_1 v_0)\frac{t_1}{v_1}\right)\right).$$

The map φ_1 is the same as φ_2 preceded by the transformation $\tilde{\cdot} : (x, y) \mapsto (\frac{1}{x}, \frac{y}{x^3})$. Let $\tilde{u_0}, \tilde{u_1}, \tilde{v_0}, \tilde{v_1}$ be the Mumford coordinates of $\tilde{P_H} + \tilde{Q_H}$. We have:

$$\tilde{u_0} = \frac{1}{u_0}, \quad \tilde{u_1} = \frac{u_1}{u_0}, \quad \tilde{v_0} = \frac{u_1 v_0 - u_0 v_1}{u_0^2}, \quad \tilde{v_1} = \frac{u_1^2 v_0 - u_0 v_0 - u_0 u_1 v_1}{u_0^2}$$

Then, setting $\lambda_1 = -\dfrac{(\Delta_\beta / A^3)\tilde{v_1}}{s_1 \tilde{u_1}}$ and $\omega_1 = \lambda_1^2 + \sum_{i=1}^{3} \alpha_i - s_1({\tilde{u_1}}^2 - 2\tilde{u_0}) - 2s_2$, we get the following:

$$\varphi_1(P_H + Q_H) = \left(\omega_1, -\lambda_1 \left(\omega_1 - s_2 + (\tilde{u_0}\tilde{v_1} - \tilde{u_1}\tilde{v_0})\frac{s_1}{\tilde{v_1}}\right)\right).$$

This gives us four equations in the unknowns u_0, u_1, v_0, v_1:

$$\begin{cases} x(\varphi_1(P_H + Q_H)) = x(\varphi_f(P_A)), \\ y(\varphi_1(P_H + Q_H)) = y(\varphi_f(P_A)), \\ x(\varphi_2(P_H + Q_H)) = x(P), \\ y(\varphi_2(P_H + Q_H)) = y(P). \end{cases}$$

Expressing $[D] \in J_H$ in the equation of H, we also have

$$\begin{aligned} 2v_0^2 - 2v_0v_1u_1 + v_1^2(u_1^2 - 2u_0) =& 2c_0 - u_1c_1 + (u_1^2 - 2u_0)c_2 \\ &+ (u_1^3 + 3u_0u_1)c_3 + (u_1^4 - 4u_1^2u_0 + 2u_0^2)c_4 \\ &+ (-u_1^5 + 5u_1^3u_0 - 5u_1u_0^2)c_5 \\ &+ (u_1^6 - 6u_1^4u_0 + 9u_1^2u_0^2 - 2u_0^3)c_6, \end{aligned}$$

where the c_i's are the coefficients of h. Then, the system has 4 solutions, all defined over $\mathbb{F}_{p^2}$. We can take any of these, and double the corresponding point on J_H to get the image of $(\varphi_f(P_A), P)$.

Example 4.22. *Let us use the example we developed in Section 2.2. The Sage computations are included in Appendix A.2.1. We exchange the notation and we can assume that $A = 3$ and $B = 2^2$, so that we have $f = 1$. We have $E_0/\mathbb{F}_{p^2}$ given by $y^2 = x^3 + x = x(x-i)(x+i)$, and $E_A/\mathbb{F}_{p^2}$ given by $y^2 = x^3 + 5x + 19i = (x+32i)(x+41i)(x+45i)$. For an isogeny $\varphi_f : E \to E_0$ of degree 1, we can pick the isomorphism given by the distortion map $\varphi_f(x,y) = (-x, iy)$, so we have $E/\mathbb{F}_{p^2}$ given by $E : y^2 = x^3 + x$. We can now use the formulas given in Proposition 4.21 to find the codomain of a $(2,2)$-isogeny $\Psi : E \times E_A \to J_H$, where H is a hyperelliptic curve. We get:*

- $\Delta_\alpha = 55, \Delta_\beta = 43$,
- $a_1 = 3i, a_2 = 22$,
- $b_1 = 53i, b_2 = 37$,
- $A = 30i, B = 15i$.

So the equation of H is given by

$$H : y^2 = 29ix^6 + 42ix^4 + 28ix^2 + 44i,$$

and the codomain of Φ is given by its Jacobian J_H.

4.2.2 $(2,2)$-isogenies between two Jacobians

We now describe the $(2,2)$-isogenies between Jacobians of genus 2 curves using Richelot isogenies. Let $H : y^2 = h(x)$ be a hyperelliptic curve, and let $\langle [g_1(x), 0], [g_2(x), 0] \rangle$ be a $(2,2)$-subgroup of its Jacobian, where $g_1(x) = x^2 + g_{11}x + g_{10}, g_2(x) = x^2 + g_{21}x + g_{20}$. Letting $g_3(x) = \frac{h(x)}{g_1(x)g_2(x)} = g_{32}x^2 + g_{31}x + g_{30}$, we see that $G = [(g_1, g_2, g_3)]$ is a quadratic splitting of h. We set $\delta = \det \begin{pmatrix} g_{10} & g_{11} & 1 \\ g_{20} & g_{21} & 1 \\ g_{30} & g_{31} & g_{32} \end{pmatrix}$. If it is non-singular, using the Richelot operator $\mathcal{R}$, we

have that a quadratic splitting of H_G is $[(g_1', g_2', g_3')]$, where $g_i'(x) = \delta^{-1}\left(\frac{dg_j}{dx}g_k - g_j\frac{dg_k}{dx}\right)$ for $(i,j,k) = (1,2,3),(2,3,1),(3,1,2)$. Then, the codomain of our Richelot isogeny is given by $H_G =: H' : \mathtt{y}^2 = h'(\mathtt{x}) = g_1'(\mathtt{x})g_2'(\mathtt{x})g_3'(\mathtt{x})$. We use a different notation for coordinates since we push a point through the $(2,2)$-isogeny via the Richelot correspondence as in Definition 4.18. This correspondence is the curve $X \subset H \times H'$ given by

$$X : g_1(x)g_1'(\mathtt{x}) + g_2(x)g_2'(\mathtt{x}) = y\mathtt{y} - g_1(x)g_1'(\mathtt{x})(x - \mathtt{x}) = 0.$$

Using the natural projection maps $\pi : X \to H, \pi' : X \to H'$, the isogeny is given by the induced homomorphism

$$J_H \to J_{H'}, [D] \mapsto [\pi'_*\pi^* D].$$

So to compute the image of some point $[x^2 + u_1x + u_0, v_1x + v_0] \in J_H$, we need to eliminate the variables x, y from the system

$$\begin{cases} x^2 + u_1x + u_0 = 0, \\ y = v_1x + v_0, \\ y^2 = h(x), \\ g_1(x)g_1'(\mathtt{x}) + g_2(x)g_2'(\mathtt{x}) = 0, \\ y\mathtt{y} = g_1(x)g_1'(\mathtt{x})(x - \mathtt{x}). \end{cases}$$

With respect to the lexicographic order $\mathtt{x} \prec \mathtt{y} \prec y \prec x$, we expect the last two equations of its reduced Gröbner basis to be of the form

$$\mathtt{y} = v_3'\mathtt{x}^3 + v_2'\mathtt{x}^2 + v_1'\mathtt{x} + v_0', \mathtt{x}^4 + u_3'\mathtt{x}^3 + u_2'\mathtt{x}^2 + u_1'\mathtt{x} + u_0' = 0.$$

Finally, $[\mathtt{x}^4 + u_3'\mathtt{x}^3 + u_2'\mathtt{x}^2 + u_1'\mathtt{x} + u_0', v_3'\mathtt{x}^3 + v_2'\mathtt{x}^2 + v_1'\mathtt{x} + v_0']$ are the non-reduced Mumford coordinates for the image on $J_{H'}$.

Example 4.23. *We don't continue Example 4.22 as we will see later in Example 4.24 that it has a singular quadratic splitting and is hence $(2,2)$-isogenous to a product of elliptic curves. Instead, we want an example of a $(2,2)$-isogeny from a Jacobian of a genus 2 curve to another Jacobian of a genus 2 curve. We refer to Appendix A.2.2 for the Sage computations. Let us start from the hyperelliptic curve*

$$\begin{aligned} H : y^2 = h(x) &= x^6 + 54x^5 + 10x^4 + 55x^3 + 37x^2 + 35x + 37, \\ &= (x+1)(x+2)(x+3)(x+27)(x^2 + 21x + 29), \end{aligned}$$

that we define over $\mathbb{F}_{59^2}$*. Let now*

$$\begin{aligned}
g_1 &= x^2 + 21x + 29,\\
g_2 &= (x+1)(x+2) = x^2 + 3x + 2,\\
g_3 &= (x+1)(x+3) = x^2 + 4x + 3,\\
g_4 &= (x+1)(x+27) = x^2 + 28x + 27,\\
g_5 &= (x+2)(x+3) = x^2 + 5x + 6,\\
g_6 &= (x+2)(x+27) = x^2 + 29x + 54,\\
g_7 &= (x+3)(x+27) = x^2 + 30x + 22.
\end{aligned}$$

The set of unsigned quadratic splittings is

$$|\mathcal{S}_h| = \{[(g_1, g_2, g_7)], [(g_1, g_3, g_6)], [(g_1, g_4, g_5)]\},$$

and computing the determinant of each associated matrix, we see that they are all non-singular. So there is a $(2,2)$*-isogeny* $\Delta : J_H \to J_{H'}$*, where* H' *also defines a hyperelliptic curve over* $\mathbb{F}_{59^2}$*. Let us pick the splitting* (g_1, g_2, g_7)*. The matrix* $\delta = \begin{pmatrix} 29 & 21 & 1 \\ 2 & 3 & 1 \\ 22 & 30 & 1 \end{pmatrix}$ *has determinant equal to 15. Then:*

$$\begin{aligned}
h'_1(x) &= 49x^2 + 42x + 24,\\
h'_2(x) &= 23x^2 + 56x + 39,\\
h'_3(x) &= 46x^2 + 20x + 56.
\end{aligned}$$

Finally, the codomain of Δ *is given by* $J_{H'}$*, where*

$$H' : y^2 = 40x^6 + 34x^5 + 23x^4 + 30x^3 + 46x^2 + 39x + 24.$$

4.2.3 $(2,2)$-isogenies between a Jacobian and a product of elliptic curves

We now want to check that the last step takes us back to a product of elliptic curves. For this, we proceed as in Subsection 4.2.2 and do as if we are dealing with a Richelot isogeny again. We just need to check that $\delta = 0$ for the chosen quadratic splitting, so that it is singular.

Example 4.24. *Let us now continue and finish Example 4.22. We can find the Sage code in Appendix A.2.3. We start from*

$$H : y^2 = 29ix^6 + 42ix^4 + 28ix^2 + 44i = 29i(x+3)(x+18)(x+20)(x+39)(x+41)(x+56).$$

It is easy to identify a singular quadratic splitting given by (g_1, g_2, g_3)*, where*

$$\begin{aligned} g_1 &= (x+20)(x+39) = x^2 + 13, \\ g_2 &= 29i(x+3)(x+56) = 29ix^2 + 34i, \\ g_3 &= (x+18)(x+41) = x^2 + 30, \end{aligned}$$

as there are no linear terms to any of the polynomials. Since the hyperelliptic polynomial has no terms of odd degree, we use the formulas given in Theorem 4.11 and we set $c_3 = 29i, c_2 = 42i, c_1 = 28i, c_0 = 44i$*. Then we have explicit formulas for the elliptic curves* E_1 *and* E_2 *given by*

$$E_1 : y^2 = 29ix^3 + 42ix^2 + 28ix + 44i,$$

and

$$E_2 : y^2 = 44ix^3 + 28ix^2 + 42ix + 29i.$$

Changing variables to get the cubic term of the elliptic curve to have a coefficient equal to 1, we have:

$$\begin{aligned} E_1 : y^2 &= x^3 + \frac{42i}{(29i)^2}x^2 + \frac{28i}{(29i)^3}x + \frac{44i}{(29i)^4}, \\ &= x^3 + 9ix^2 + 47x + 55i, \end{aligned}$$

and

$$\begin{aligned} E_2 : y^2 &= x^3 + \frac{28i}{(44i)^2}x^2 + \frac{42i}{(44i)^3}x + \frac{29i}{(44i)^4}, \\ &= x^3 + 24ix^2 + 33x + 49i. \end{aligned}$$

We can then check that E_2 *is isomorphic to* E_0*, as wanted. Moreover,* E_1 *is isomorphic to* E_A*.*

4.3 Checking the kernel of Φ

Finally, we can check that the explicit description of the kernel of Φ that we get from Theorem 3.1 is correct. We should have

$$\ker(\Phi) = \{([3]S, \varphi(S) | S \in E[2^2]\},$$

and using Sage in Appendix A.3 we find

$$\ker(\Phi) = \langle((58i+23, 35i+22), (18i+6, 9i+49)), ((27i+1, i+11), (i+36, 22i+24))\rangle.$$

After working directly with those points, following the method of Subsection 4.2.1, we assume we are in one of the exceptional cases mentioned in [CD22, Section 8.1], and we make a change to the points we work with. Let $P = (18i + 6, 9i + 49) \in E_A, P_c = (58i + 23, 35i+22) \in E, Q = 2(27i+1, i+11) = (27i, 0) \in E_A, Q_c = 2(i+36, 22i+24) = (i, 0) \in E$. We want to evaluate the image of $(P, P_c), (Q, Q_c)$ under Φ, where Φ is the composition $\Psi' \circ \Psi$ as follows:

$$E_A \times E \xrightarrow{\Psi} J_H \xrightarrow{\Psi'} E_1 \times E_2.$$

We use the construction described in Subsection 4.2.1 to compute the image of the points $(P, P_c), (Q, Q_c)$ under $\Psi : E \times E_A \to J_H$, where $H : y^2 = 29ix^6 + 42ix^4 + 28ix^2 + 44i$ as in Example 4.22. We get the following:

- The image of (P, P_c) is the divisor $[x^2 + 57x + 53, y] = [(x + 18)(x + 39), y]$.
- The image of (Q, Q_c) is the divisor $[x^2 + 50, y] = [(x + 3)(x + 56), y]$.
- The image of $(P + Q, P_c + Q_c)$ is the divisor $[x^2 + 2x + 53, y] = [(x + 20)(x + 41), y]$.

We notice the factors are the same as in the singular quadratic splitting of Example 4.24. Computing Ψ', we finally map those divisors onto points of the elliptic curves E_1, E_2, using the maps $\varphi_1 : H \to E_1 \cong F \cong E_A, \varphi_2 : H \to E_2 \cong E_0 \cong E$ (and the appropriate change of variables from E_1 to F, resp. from E_2 to E_0), and mapping divisors $[\sum_i S_i]$ to $\sum_i \varphi_{1/2} S_i$ respectively. We obtain:

- $[(18, 0)] + [(39, 0)]$ is sent to $\varphi_1(18, 0) + \varphi_1(39, 0) = O, \varphi_2(18, 0) + \varphi_2(39, 0) = O$;
- $[(3, 0)] + [(56, 0)]$ is sent to $\varphi_1(3, 0) + \varphi_1(56, 0) = O, \varphi_2(3, 0) + \varphi_2(56, 0) = O$;
- $[(20, 0)] + [(41, 0)]$ is sent to $\varphi_1(20, 0) + \varphi_1(41, 0) = O, \varphi_2(20, 0) + \varphi_2(41, 0) = O$.

All the divisors of the previous step are sent to $(O, O) \in E_1 \times E_2$, so we conclude that the kernel described above generates indeed $\ker(\Phi)$ and we are done.

Appendix A

Sage Code

A.1 Computing the explicit example of key-exchange

[1]:
```
#define our p
p=59
```

[2]:
```
#define the ring we work with
F = GF(p)
R.<x> = PolynomialRing(F)
K.<i> = GF( p^2, modulus=x^2+1 )
```

[3]:
```
#define the starting supersingular elliptic curve
E0 = EllipticCurve(K, [0,0,0,1,0])
E0
```

[3]:
```
Elliptic Curve defined by y^2 = x^3 + x over Finite Field in i of size␣
↪59^2
```

[4]:
```
#determine the torsion basis for E0[2^2]
#warning: this function is not available before Sage 10.2
PA,QA = E0.torsion_basis(2^2)
PA, QA
```

[4]:
```
((58*i + 23 : 24*i + 37 : 1), (i + 36 : 37*i + 35 : 1))
```

[5]:
```
#determine the torsion basis for E0[3]
PB,QB = E0.torsion_basis(3)
PB,QB
```

[5]:
```
((47 : 41*i : 1), (12 : 41 : 1))
```

[6]:
```
#redefine QA, QB using the distorsion map
def psi(P):
    return (-P[0], i*P[1])
```

[7]:
```
QA = psi(PA)
QB = psi(PB)
```

[8]:
```
QA,QB
```

[8]:
```
((i + 36, 37*i + 35), (12, 18))
```

[9]:
```
#define generator of kernel using our chosen secret values
RA=3*E0(PA)+4*E0(QA)
RA
```

[9]:
```
(58*i + 23 : 35*i + 22 : 1)
```

[10]:
```
#check order
RA.order()
```

[10]:
```
4
```

[11]:
```
#create list of points that will help us define the isogeny phiA later
RA_list = [i*RA for i in range(4)]
```

[13]:
```
#create the isogeny phiA
phiA = EllipticCurveIsogeny(E0, RA_list); phiA
```

[13]:
```
Isogeny of degree 4 from Elliptic Curve defined by y^2 = x^3 + x over␣
↪Finite
Field in i of size 59^2 to Elliptic Curve defined by y^2 = x^3 +␣
↪(23*i+32)*x +
(10*i+4) over Finite Field in i of size 59^2
```

[14]:
```
#give the explicit rational maps
phiA.rational_maps()
```

[14]:
```
((x^4 + (3*i + 13)*x^3 + (-14*i - 23)*x^2 + (20*i - 18)*x + (14*i + 22))/
↪(x^3 +
(3*i + 13)*x^2 + (26*i - 5)*x + (-3*i - 13)),
 (x^5*y + (5*i - 10)*x^4*y + 2*x^3*y + (2*i - 20)*x^2*y + 5*x*y + (i +
23)*y)/(x^5 + (5*i - 10)*x^4 + (19*i - 16)*x^3 + (-28*i - 12)*x^2 +␣
↪(14*i +
23)*x + (7*i + 3)))
```

[15]:
```
#do the same for phiB
RB = 2*E0(PB)+2*E0(QB)
RB
```

[15]:
```
(38*i : 49*i + 10 : 1)
```

[16]:
```
RB.order()
```

[16]:
```
3
```

[17]:
```
RB_list = [i*RB for i in range(3)]
```

[18]:
```
phiB = EllipticCurveIsogeny(E0, RB_list); phiB
```

[18]:
```
Isogeny of degree 3 from Elliptic Curve defined by y^2 = x^3 + x over␣
↪Finite
Field in i of size 59^2 to Elliptic Curve defined by y^2 = x^3 + 5*x +␣
↪19*i over
Finite Field in i of size 59^2
```

[19]:
```
phiB.rational_maps()
```

[19]:
```
((x^3 + (-17*i)*x^2 - 17*x + (21*i))/(x^2 + (-17*i)*x - 28),
 (x^3*y + (4*i)*x^2*y + 23*x*y + (14*i)*y)/(x^3 + (4*i)*x^2 - 25*x +␣
↪(2*i)))
```

[25]:
```
#define functions to compute the auxiliary points
def phiAcomp(x,y):
    return ((x^4 + (3*i + 13)*x^3 + (-14*i - 23)*x^2 + (20*i - 18)*x +␣
↪(14*i + 22))/(x^3 + (3*i + 13)*x^2 + (26*i - 5)*x + (-3*i - 13)),
(x^5*y + (5*i - 10)*x^4*y + 2*x^3*y + (2*i - 20)*x^2*y + 5*x*y + (i +␣
↪23)*y)/(x^5 + (5*i - 10)*x^4 + (19*i - 16)*x^3 + (-28*i - 12)*x^2 +␣
↪(14*i + 23)*x + (7*i + 3)))
```

[26]:
```
def phiBcomp(x,y):
    return ((x^3 + (-17*i)*x^2 - 17*x + (21*i))/(x^2 + (-17*i)*x - 28),
(x^3*y + (4*i)*x^2*y + 23*x*y + (14*i)*y)/(x^3 + (4*i)*x^2 - 25*x +␣
↪(2*i)))
```

[27]:
```
phiA_PB = phiAcomp(PB[0],PB[1])
phiA_PB
```

[27]:
```
(31*i + 13, 46*i + 17)
```

[28]:
```
phiA_QB = phiAcomp(QB[0],QB[1])
phiA_QB
```

[28]:
```
(35*i + 12, 11*i + 44)
```

[29]:
```
phiB_PA = phiBcomp(PA[0],PA[1])
phiB_PA
```

[29]:
```
(27*i + 1, 58*i + 48)
```

[30]:
```
phiB_QA = phiBcomp(QA[0],QA[1])
phiB_QA
```

[30]:
```
(18*i + 6, 9*i + 49)
```

[32]:
```
#now compute the isogenies phiA'and phiB' to EAB
#first define EB
EB = EllipticCurve(K, [0,0,0,5,19*i])
EB
```

[32]:
```
Elliptic Curve defined by y^2 = x^3 + 5*x + 19*i over Finite Field in i␣
↪of size
59^2
```

[33]:
```
#compute kernel of phiA'
KA = 3*EB(phiB_PA)+4*EB(phiB_QA)
KA
```

[33]:
```
(27*i + 1 : i + 11 : 1)
```

[34]:
```
KA.order()
```

[34]:
```
4
```

[36]:
```
KA_list = [i*KA for i in range(4)]
```

[37]:
```
phiAprime = EllipticCurveIsogeny(EB, KA_list); phiAprime
```

[37]:
```
Isogeny of degree 4 from Elliptic Curve defined by y^2 = x^3 + 5*x +␣
↪19*i over
Finite Field in i of size 59^2 to Elliptic Curve defined by y^2 = x^3 +
(32*i+19)*x + 36*i over Finite Field in i of size 59^2
```

[38]:
```
#now define EA
EA = EllipticCurve(K, [0,0,0,23*i+32,10*i+4])
EA
```

[38]:
```
Elliptic Curve defined by y^2 = x^3 + (23*i+32)*x + (10*i+4) over Finite␣
↪Field
in i of size 59^2
```

[40]:
```
KB = 2*EA(phiA_PB)+2*EA(phiA_QB)
KB
```

[40]:
```
(20*i + 50 : 16*i + 54 : 1)
```

[32]:
```
KB.order()
```

[32]:
```
3
```

[41]:
```
KB_list = [i*KB for i in range(3)]
```

[42]:
```
phiBprime = EllipticCurveIsogeny(EA, KB_list); phiBprime
```

[42]:
```
Isogeny of degree 3 from Elliptic Curve defined by y^2 = x^3 +␣
↪(23*i+32)*x +
(10*i+4) over Finite Field in i of size 59^2 to Elliptic Curve defined␣
↪by y^2 =
x^3 + (32*i+19)*x + 36*i over Finite Field in i of size 59^2
```

[43]:
```
EAB = EllipticCurve(K, [0,0,0,32*i+19,36*i])
EAB
```

[43]:
```
Elliptic Curve defined by y^2 = x^3 + (32*i+19)*x + 36*i over Finite␣
↪Field in i
of size 59^2
```

[36]:
```
EAB.j_invariant()
```

[36]:
```
15
```

A.2 Computing examples of $(2,2)$-isogenies

A.2.1 $(2,2)$-isogenies between a product of elliptic curves and a Jacobian

[1]:
```
#Define the working parameters and the ring used
p=59
F = GF(p)
R.<x> = PolynomialRing(F)
K.<i> = GF( p^2, modulus=x^2+1 )
```

[2]:
```
#define EA
EA = EllipticCurve(K, [0,0,0,5,19*i])
EA
```

[2]:
```
Elliptic Curve defined by y^2 = x^3 + 5*x + 19*i over Finite Field in i␣
↪of size
59^2
```

[3]:
```
#Define E0
E0 = EllipticCurve(K, [0,0,0,1,0])
E0
```

[3]:
```
Elliptic Curve defined by y^2 = x^3 + x over Finite Field in i of size␣
↪59^2
```

[4]:
```
#we factorize it to be able to determine the values we need to use for␣
↪the gluing step
(x^3 + 5*x + 19*i).factor()
```

[4]:
```
(x + 32*i) * (x + 41*i) * (x + 45*i)
```

[5]:
```
(x^3 + x).factor()
```

[5]:
```
x * (x^2 + 1)
```

[ ]:
```
#we can further factor it as x*(x-i)*(x+i)
```

[6]:
```
#computing the discriminants of the polynomials
(x^3 + 5*x + 19*i).discriminant()
```

[6]:
```
43
```

[7]:
```
(x^3+x).discriminant()
```

[7]:
```
55
```

[8]:
```
#alphas and betas in the thesis
a1 = 0; a2 = -i; a3 = i; b1 = -32*i; b2 = -41*i; b3 = -45*i
```

[9]:
```
#a_i and b_i in the thesis
a_1 = (a3 - a2)^2/(b3-b2) + (a2-a1)^2/(b2-b1) + (a1-a3)^2/(b1-b3)
a_1
```

[9]:
```
3*i
```

[10]:
```
b_1 = (b3-b2)^2/(a3-a2) + (b2-b1)^2/(a2-a1) + (b1-b3)^2/(a1-a3)
b_1
```

[10]: 53*i

[11]:
```
a_2 = a1*(b3-b2) + a2*(b1-b3) + a3*(b2-b1)
a_2
```

[11]: 22

[12]:
```
b_2 = b1*(a3-a2) + b2*(a1-a3) + b3*(a2-a1)
b_2
```

[12]: 37

[13]:
```
#same notation as in the documentation, don't confuse with B of␣
 ↪(B,B)-isogeny
A = 43*((3*i)/22)
A
```

[13]: 30*i

[14]:
```
B = -4 * ((53*i)/37)
B
```

[14]: 15*i

[15]:
```
#equation of the hyperelliptic curve
h = -(A*(a2-a1)*(a1-a3)*x^2 +␣
 ↪B*(b2-b1)*(b1-b3))*(A*(a3-a2)*(a2-a1)*x^2+B*(b3-b2)*(b2-b1))*(A*(a1-a3)*(a3-a2)*x^2
```

[16]:
```
h
```

[16]: 29*i*x^6 + 42*i*x^4 + 28*i*x^2 + 44*i

A.2.2 $(2,2)$-isogenies between two Jacobians

[1]:
```
#Define the working parameters and the ring used
p = 59
F = GF(p)
R.<x> = PolynomialRing(F)
K.<i> = GF( p^2, modulus=x^2+1 )
```

[2]:
```
#Define a polynomial in degree 6
h = x^6 + 54*x^5 + 10*x^4 + 55*x^3 + 37*x^2 + 35*x + 37
```

[3]:
```
#Check its factorization
h.factor()
```

[3]:
```
(x + 1) * (x + 2) * (x + 3) * (x + 27) * (x^2 + 21*x + 29)
```

[4]:
```
(x^2 + 21*x + 29).factor()
```

[4]:
```
x^2 + 21*x + 29
```

[5]:
```
g1 = x^2 + 21*x + 29
g1
```

[5]:
```
x^2 + 21*x + 29
```

[6]:
```
g2 = (x + 1)*(x + 2)
g2
```

[6]:
```
x^2 + 3*x + 2
```

[7]:
```
g3 = (x+1)*(x+3)
g3
```

[7]:
```
x^2 + 4*x + 3
```

[8]:
```
g4 = (x+1)*(x+27)
g4
```

[8]:
```
x^2 + 28*x + 27
```

[9]:
```
g5 = (x+2)*(x+3)
g5
```

[9]:
```
x^2 + 5*x + 6
```

[10]:
```
g6 = (x+2)*(x+27)
g6
```

[10]:
```
x^2 + 29*x + 54
```

[11]:
```
g7 = (x+3)*(x+27)
g7
```

[11]:
```
x^2 + 30*x + 22
```

[12]:
```
A = matrix(K, 3, 3, [1, 21, 29, 1, 3, 2, 1, 30, 22])
A
```

[12]:
```
[ 1 21 29]
[ 1  3  2]
[ 1 30 22]
```

[13]:
```
A.det()
```

[13]:
```
15
```

[14]:
```
B = matrix(K, 3, 3, [1, 21, 29, 1, 4, 3, 1, 29, 54])
B
```

[14]:
```
[ 1 21 29]
[ 1  4  3]
[ 1 29 54]
```

[15]:
```
B.det()
```

[15]:
```
19
```

[16]:
```
C = matrix(K, 3, 3, [1, 21, 29, 1, 28, 27, 1, 5, 6])
C
```

[16]:
```
[ 1 21 29]
[ 1 28 27]
[ 1  5  6]
```

[17]:
```
C.det()
```

[17]:
```
43
```

[18]:
```
#We pick the (g1, g2, g7) splitting:
dg1 = 2*x + 21
dg2 = 2*x + 3
dg7 = 2*x + 30
```

[24]:
```
#Apply the formulas to find the splitting of the equation of the␣
 ↪hyperelliptic curve of the codomain
j1 = K(1/15)*(dg2*g7 - g2*dg7)
j1
```

[24]:
```
49*x^2 + 42*x + 24
```

[27]:
```
j2 = K(1/15)*(dg7*g1 - g7*dg1)
j2
```

[27]:
```
23*x^2 + 56*x + 39
```

[28]:
```
j3 = K(1/15)*(dg1*g2 - g1*dg2)
j3
```

[28]:
```
46*x^2 + 20*x + 56
```

[29]:
```
#Equation of the hyperelliptic curve for the codomain
j1*j2*j3
```

[29]:
```
40*x^6 + 34*x^5 + 23*x^4 + 30*x^3 + 46*x^2 + 39*x + 24
```

A.2.3 $(2,2)$-isogenies between a Jacobian and a product of elliptic curves

[1]:
```
#Define the working parameters and the ring used
p=59
F = GF(p)
R.<x> = PolynomialRing(F)
K.<i> = GF( p^2, modulus=x^2+1 )
```

[2]:
```
#define the polynomials of the splitting
g1 = (x + 20)* (x + 39)
g1
```

[2]:
```
x^2 + 13
```

[3]:
```
g2 = 29*i*(x+3)*(x+56)
g2
```

[3]:
```
29*i*x^2 + 34*i
```

[4]:
```
g3 = (x+18)*(x+41)
g3
```

[4]:
```
x^2 + 30
```

[5]:
```
#check it is indeed a singular splitting
AA = matrix(K, 3, 3, [30, 0, 1, 34*i, 0, 29*i, 13, 0, 1])
AA
```

[5]:
```
[  30    0    1]
[34*i    0 29*i]
[  13    0    1]
```

[6]:
```
AA.det()
```

[6]:
```
0
```

[7]:
```
#Define E0
E0 = EllipticCurve(K, [0,0,0,1,0])
E0
```

[7]:
```
Elliptic Curve defined by y^2 = x^3 + x over Finite Field in i of size␣
↪59^2
```

[8]:
```
#define E1 and E2 with the change of variables
E1 = EllipticCurve(K, [0, (42*i)/(29*i)^2, 0, (28*i)/(29*i)^3, (44*i)/
↪(29*i)^4])
E1
```

[8]:
```
Elliptic Curve defined by y^2 = x^3 + 9*i*x^2 + 47*x + 55*i over Finite␣
↪Field in
i of size 59^2
```

[9]:
```
E2 = EllipticCurve(K, [0, (28*i)/(44*i)^2, 0, (42*i)/(44*i)^3, (29*i)/
↪(44*i)^4])
E2
```

[9]:
```
Elliptic Curve defined by y^2 = x^3 + 24*i*x^2 + 33*x + 49*i over Finite␣
↪Field
in i of size 59^2
```

[10]:
```
#check isomorphism between elliptic curves
E1.is_isomorphic(E0)
```

[10]:
```
False
```

[11]:
```
E2.is_isomorphic(E0)
```

[11]:
```
True
```

A.3 Checking the kernel of Φ

[116]:
```
def phi1(x,y):
    return 2*E0(s1/x^2+s2, (43/A^3)*y/x^3)
```

[128]:
```
phi1(3,0)+phi1(56,0)
```

[128]:
```
(0 : 1 : 0)
```

[126]:
```
phi1(18,0)+phi1(39,0)
```

[126]: (0 : 1 : 0)

[127]:
```
phi1(20,0)+phi1(41,0)
```

[127]: (0 : 1 : 0)

[118]:
```
def phi2(x,y):
    return 2*EA(t1*x^2+t2, (55/B^3)*y)
```

[119]:
```
phi2(3,0)+phi2(56,0)
```

[119]: (0 : 1 : 0)

[122]:
```
phi2(18,0)+phi2(39,0)
```

[122]: (0 : 1 : 0)

[123]:
```
phi2(20,0)+phi2(41,0)
```

[123]: (0 : 1 : 0)

Bibliography

[BL04] Christina Birkenhake and Herbert Lange, *Complex Abelian Varieties*, Springer, Berlin, Germany, 2004.

[CD22] Wouter Castryck and Thomas Decru, *An efficient key recovery attack on sidh*, 2022. https://eprint.iacr.org/2022/975.

[CF96] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus 2*, London Mathematical Society Lecture Note Series, Cambridge University Press, 1996.

[CFA+12] Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Frederik Vercauteren, *Handbook of elliptic and hyperelliptic curve cryptography, second edition*, 2nd ed., Chapman & Hall/CRC, 2012.

[EvdGM21] Bas Edixhoven, Gerard van der Geer, and Ben Moonen, *Abelian varieties (preprint)* (2021).

[FJP14] Luca De Feo, David Jao, and Jérôme Plût, *Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies*, Journal of Mathematical Cryptology **8** (2014), no. 3, 209–247.

[GR04] Steven D Galbraith and Victor Rotger, *Easy decision-diffie-hellman groups*, 2004. https://eprint.iacr.org/2004/070.

[GW] Ulrich Görtz and Torsten Wedhorn, *Algebraic Geometry II: Cohomology of Schemes*, Springer Fachmedien, Wiesbaden, Germany.

[HNR07] Everett W. Howe, Enric Nart, and Christophe Ritzenthaler, *Jacobians in isogeny classes of abelian surfaces over finite fields*, 2007.

[Kan97] Ernst Kani, *The number of curves of genus two with elliptic differentials.*, Journal für die reine und angewandte Mathematik **485** (1997), 93–122.

[MMP+23] Luciano Maino, Chloe Martindale, Lorenz Panny, Giacomo Pope, and Benjamin Wesolowski, *A direct key recovery attack on sidh*, 2023. https://eprint.iacr.org/2023/640.

[MoWDoCO+96] A. Menezes, University of Waterloo. Department of Combinatorics, Optimization, R. Zuccherato, Y.H. Wu, and University of Waterloo. Faculty of Mathematics, *An elementary introduction to hyperelliptic curves*, CORR Report, Faculty of Mathematics, University of Waterloo, 1996.

[MP19] Chloe Martindale and Lorenz Panny, *How to not break sidh*, IACR Cryptol. ePrint Arch. **2019** (2019), 558.

[Sil09] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, New York, NY, USA, 2009.

[Smi05] Benjamin Andrew Smith, *Explicit endomorphisms and correspondences*, Ph.D. Thesis, December 23, 2005.

[Sto19] Michael Stoll, *Arithmetic of hyperelliptic curves*, 2019. University of Bayreuth.

[Tes99] Edlyn Teske, *The Pohlig–Hellman Method Generalized for Group Structure Computation*, J. Symbolic Comput. **27** (June 1999), no. 6, 521–534.

[Vél71] J. Vélu, *Isogénies entre courbes elliptiques*, Comptes-Rendus de l'Académie des Sciences, Série I **273** (1971juillet), 238–241.

[Was08] Lawrence C. Washington, *Elliptic curves: Number theory and cryptography, second edition*, 2nd ed., Chapman & Hall/CRC, 2008.