Technische Universität Kaiserslautern
Fachbereich Mathematik

Endomorphism Rings of Ordinary Abelian Varieties

Sogo Pierre Sanon

Vom Fachbereich Mathematik
der Technischen Universität Kaiserslautern
zur Verleihung des akademischen Grades

Doktor der Naturwissenschaften
(Doctor rerum naturalium, Dr. rer. nat.)

genehmigte Dissertation

1. Gutachter: Prof. Dr. Claus Fieker
2. Gutachter: Prof. Renate Scheidler

Tag der Disputation: 31.03.2022

D 386

"Impossible is just an opinion."

Paulo Coelho

Abstract

The main objects of study in this thesis are abelian varieties and their endomorphism rings. Abelian varieties are not just interesting in their own right, they also have numerous applications in various areas such as in algebraic geometry, number theory and information security. In fact, they make up one of the best choices in public key cryptography and more recently in post-quantum cryptography. Endomorphism rings are objects attached to abelian varieties. Their computation plays an important role in explicit class field theory and in the security of some post-quantum cryptosystems.

There are subexponential algorithms to compute the endomorphism rings of abelian varieties of dimension one and two. Prior to this work, all these subexponential algorithms came with a probability of failure and additional steps were required to unconditionally prove the output. In addition, these methods do not cover all abelian varieties of dimension two. The objective of this thesis is to analyse the subexponential methods and develop ways to deal with the exceptional cases.

We improve the existing methods by developing algorithms that always output the correct endomorphism ring. In addition to that, we develop a novel approach to compute endomorphism rings of some abelian varieties that could not be handled before. We also prove that the subexponential approaches are simply not good enough to cover all the cases. We use some of our results to construct a family of abelian surfaces with which we build post-quantum cryptosystems that are believed to resist subexponential quantum attacks - a desirable property for cryptosystems. This has the potential of providing an efficient non interactive isogeny based key exchange protocol, which is also capable of resisting subexponential quantum attacks and will be the first of its kind. Some of these results have already been published in [53].

Zusammenfassung

Die Hauptgegenstände dieser Arbeit sind abelsche Varietäten und ihre Endomorphismenringe. Abelsche Varietäten sind nicht nur an sich interessant, sie haben auch zahlreiche Anwendungen in verschiedenen Bereichen wie der algebraischen Geometrie, der Zahlentheorie und der Informationssicherheit. Tatsächlich stellen abelsche Varietäten ein vielversprechendes Werkzeug in der Public-Key-Kryptografie und neuerdings auch in der Post-Quantum-Kryptografie dar. Endomorphismenringe sind Objekte, die mit abelschen Varietäten verknüpft sind. Ihre Berechnung spielt eine wichtige Rolle in der expliziten Klassenkörpertheorie und in der Sicherheit einiger Post-Quantum-Verschlüsselungssysteme.

Es gibt subexponentielle Algorithmen, um die Endomorphismenringe von abelschen Varietäten der Dimension eins und zwei zu berechnen. Der Stand der Dinge vor dieser Arbeit war, dass all diese subexponentiellen Algorithmen eine Ausfallwahrscheinlichkeit hatten und weitergehende, zusätzliche Schritte erforderlich waren, um das Ergebnis der Ausgabe zweifelslos auf seine Richtigkeit zu überprüfen. Außerdem deckten diese Methoden nicht alle abelschen Varietäten von Dimension zwei ab. Das ursprüngliche Ziel dieser Arbeit bestand darin, diese subexponentiellen Algorithmen zu analysieren und Wege zu entwickeln, um die Ausfälle zu beheben.

Nun präsentieren wir hiermit Algorithmen, welche die bestehenden Methoden weitreichend verbessern, da sie immer den korrekten Endomorphismenring liefern. Darüber hinaus haben wir einen neuartigen Ansatz entwickelt, um Endomorphismenringe gewisser abelscher Varietäten zu berechnen, was zuvor unmöglich war. Wir beweisen auch, dass der subexponentielle Ansatz vorausgehender Methoden nicht ausreichend ist, um alle Fälle abzudecken. Ferner verwenden wir einige unserer Ergebnisse für die Konstruktion abelscher Flächen, mit denen wir Post-Quantum-Verschlüsselungssysteme definieren, von denen angenommen wird, dass sie subexponentiellen Quantenangriffen widerstehen – eine wünschenswerte Eigenschaft für Verschlüsselungssysteme. Diese Verschlüsselungssysteme haben das Potenzial, ein effizientes, nicht interaktives, auf Isogenien basiertes Schlüsselaustauschprotokoll zu definieren, das auch subexponentiellen Quantenangriffen widersteht, was als solches das erste seiner Art sein wird. Einige dieser Ergebnisse wurden bereits in [53] veröffentlicht.

Acknowledgements

Foremost, I wish to thank my supervisor Prof. Dr. Claus Fieker for his constructive criticism and insightful feedback that pushed me to sharpen my thinking and brought my work to a higher level. I wish to extend my special gratitude to Professor Renate Scheidler for accepting to review my thesis. I would like to thank the German Academic Exchange Service (DAAD) and SFB-TRR 195 'Symbolic Tools in Mathematics and their Application' of the German Research Foundation (DFG) for financial assistance.

I wish to show my appreciation to Dr. Tommy Hofmann and Dr. Carlo Sircana for our wonderful collaboration and the helpful discussions we had during my time as a PhD candidate. I am thankful to Yvonne Weber for her help in writing the German abstract of this thesis.

I also wish to extend my special thanks to Dr. Aslam Ali and Dr. Jayantha Suranimalee with whom I shared the office space and often had stimulating discussions about academics as well as life.

Finally, I could not have completed this dissertation without the support of my family and my love Josephine Tetteh, who provided enjoyable discussions as well as happy distractions to rest my mind outside of my research. Thank you all for making this PhD possible.

Contents

List of Algorithms

To my family

Chapter 1

Introduction

Abelian varieties are mathematical objects that are as interesting to mathematicians as they are to cryptographers. In fact, they are one of the most studied objects in algebraic geometry, number theory and arithmetic geometry, to mention a few. They play a significant role in the proof of Fermat's last theorem, one of the biggest mathematical achievements in the 20th century. In cryptography, abelian varieties, especially elliptic curves (abelian varieties of dimension one) and abelian surfaces (abelian varieties of dimension two) have been used and are continued to be used to produce some of the best cryptographic schemes that are utilized in everyday life to secure data and communications. Some of these applications include the Bitcoin digital currency system [92, 116], WhatsApp messaging app [116], national ID cards [100], and transport layer security (TLS) [85, 99, 116], just to name a few.

Endomorphism rings of abelian surfaces are also relevant security parameters in certain cryptographic applications like Supersingular Isogeny Diffie-Hellman key exchange (SIDH), [48]. SIDH is one of the most promising post-quantum cryptographic schemes. These are cryptosystems that can withstand attacks by quantum computers. The computation of endomorphism rings of abelian varieties is not only an important problem in cryptography but also in computational number theory. For instance, it is important in the computation of class polynomials, which play a role in explicit class field theory [113]. It is also used in the construction of abelian varieties with prescribed number of points, in the so-called Complex Multiplication (CM) method, [49], which has application in elliptic curve cryptography. It is therefore important to study the computation of endomorphism rings of abelian varieties.

Endomorphism rings computation

The main objectives of this thesis are to study the computation of the endomorphism rings of abelian varieties, more specifically in dimension one and two, and to investigate their applications in cryptography. We focus on ordinary abelian varieties defined over finite fields, the largest group of abelian varieties defined over finite field. Abelian varieties are roughly algebraic varieties that are also abelian groups. The endomorphism ring of an abelian variety is the set of endomorphisms together with pointwise addition and composition.

Kohel in [72], was the first to investigate the computation of endomorphism rings of abelian varieties. Given an ordinary elliptic curve defined over a finite field, he developed a method that computes its endomorphism ring in deterministic exponential time in the size of the base field. Other exponential methods in higher dimension, like in [49], were also developed. The first subexponential method is due to Bisson and Sutherland in [17], where under some assumptions, they computed endomorphism rings of ordinary elliptic curves. This was generalized by Bisson in [12], only assuming the Generalized Riemann Hypothesis (GRH). He extended his method to compute the endomorphism ring of principally polarized, absolutely simple, ordinary abelian surfaces in subexponential time [14]. However, he discarded two families of abelian surfaces for his approach to work. In [110], Springer developed a method similar to the one in [17] to compute endomorphism rings of ordinary abelian surfaces but does not also work for the two families excluded in [14].

Lattice Method

There is a general approach behind all the subexponential methods that we are going to call the "lattice method". It is based on the theory of complex multiplication and consists of exploiting the action of the class group or polarized class group in higher dimensions (complex multiplication action) on some set of abelian varieties. The subexponential complexity comes from the fact that class groups can be computed in subexponential time or more precisely, relations can be computed in subexponential time. There is a way to get a set-theoretic lattice that contains candidates of endomorphism ring and the role of the complex multiplication action is to identify the endomorphism ring among those candidates.

While using the lattice method, we are faced with two main problems. The first problem is that the complex multiplication action fails to tell apart some candidates from the true endomorphism ring in subexponential time. The second problem is that the computation of these candidates is expensive. For elliptic curves, we can work around these obstacles but in higher dimensions there are no known ways to handle all the cases. Another issue with the lattice method is that the algorithms can fail to give correct output and additional steps are needed to confirm or reject the result. This is solved in this thesis for both elliptic curves and abelian surfaces.

The lack of subexponential algorithms to compute the endomorphism rings of some abelian varieties can have interesting applications in post-quantum cryptography. In fact, it gives the opportunity to build a system whose security will be based on the difficulty of computing the endomorphism ring, leading to a system that can resist subexponential attacks.

Post-Quantum Cryptography

Post-quantum cryptography is the branch of cryptography that constructs and studies cryptosystems that are safe even under quantum attacks. It became an active field of research with the discovery of Shor's algorithm in 1994. Shor's algorithm is the first quantum algorithm that can effectively attack systems that are currently in use, such as Rivest–Shamir–Adleman (RSA) cryptosystem and Elliptic Curve Diffie-Hellman (ECDH), [100, 108]. With the progress made in quantum computers in recent years, current cryptographic systems stand a risk to be broken, thereby prompting the need to develop post-quantum cryptographic schemes which can better withstand quantum attacks.

The key exchange protocols are the most affected by quantum computers. Many systems conjectured to resist quantum attacks have been proposed for the replacement of current protocols. Among these are isogeny-graph based cryptosystems. Isognies are maps between two not necessarily identical abelian varieties. Isogeny based cryptosystems were first proposed by Couveignes, [38], and use ordinary elliptic curves. They were independently rediscovered by Rostovtsev and Stolbunov in [101]. We refer to the system introduced by Couveignes, Rostovtsev and Stolbunov as CRS cryptosystem. Due to its poor performance and the discovery of a subexponential attack by Childs, Jao and Soukharev in [34], CRS became less attractive even with the improvement of performance in [43]. The focus then shifted to supersingular elliptic curves which turned out to perform better. The first idea of using supersingular isogeny graphs for cryptography was

proposed by Charles, Goren and Lauter for use in a hash function, [32]. The Supersingular Isogeny Diffie-Hellman key exchange was developed by Jao and De Feo in [42] and more recently the Commutative Supersingular Isogeny Diffie-Hellman key exchange (CSIDH) in [30] by Castryck, Lange, Martindale, Renes, Panny. The CSIDH is similar to CRS but uses supersingular elliptic curves, it has many interesting features such as fast implementation and it is non interactive and a key can be reused for a certain number of times without compromising the security of the system. CRS and CSIDH are both affected by the subexponential attack in [34].

Overview

Chapter 2 introduces the different concepts that are used throughout the thesis. It gives a brief overview of global class field theory and the general theory of abelian varieties. It also introduces the theory of complex multiplication.

Chapter 3 studies in depth the computation of the endomorphism rings of ordinary elliptic curves defined over finite fields. We present the exponential method by Kohel, [72] and the the subexponential method by Bisson [12], which was the state of the art algorithm before our work. However, as mentioned earlier, it comes with a probability of failure. We develop a new approach that always outputs the correct endomorphism rings. This new method is also faster in practice compared to the previous ones and we illustrate that by an example.

Chapter 4 focuses on abelian varieties in higher dimension and investigates the generalization of the lattice method in dimension 2. We give some backgrounds and present already known algorithms which are not able to compute the endomorphism rings of all ordinary abelian surfaces. We extend the method to compute the endomorphism rings of abelian surfaces that could not be handled by previous algorithms. We also show the limitation of the lattice method by constructing families of two dimensional abelian varieties whose endomorphism rings are not computable in subexponential time by the lattice method, which means that the approach is just inefficient to cover all the cases. These results can be found in [53]. We prove a similar result as in Chapter 3 by providing a new algorithm which works without failure and is also faster in practice.

Chapter 5 uses the families of abelian surfaces constructed in Chapter 4 to build a post-quantum cryptosystem that is the first non-interactive isogeny based cryptosystem conjectured to resist subexponential attacks. It also provides a good overview of isogeny

based cryptography in the post-quantum setting. We believe this has a lot of potential to provide the first efficient non-interactive isogeny based cryptosystem that resists subexponential attacks.

Chapter 2

Preliminaries

In this chapter, we introduce the different notions that occur in the rest of this thesis. We give a brief overview of global class field theory and the general theory of abelian varieties. We also give an introduction to the theory of complex multiplication.

2.1 Global class field theory

We follow references [79, 93] and refer to them for the proofs.

Let L/K be a Galois extension of number fields with Galois group G. Given an unramified prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, all ideals here are nonzero, and a prime $\mathfrak{P}$ of $\mathcal{O}_L$ lying above $\mathfrak{p}$, there exists a unique automorphism $\sigma_{\mathfrak{P}} \in G$ satisfying

$$\sigma_{\mathfrak{P}}(x) \equiv x^q \mod \mathfrak{P} \text{ for all } x \in \mathcal{O}_L,$$

where $q = \mathrm{norm}_{K/\mathbb{Q}}(\mathfrak{p})$.

The automorphism $\sigma_{\mathfrak{P}}$ is called the Frobenius automorphism of $\mathfrak{P}$ and is denoted by

$$\sigma_{\mathfrak{P}} = \left(\frac{L/K}{\mathfrak{P}}\right).$$

Now let L/K be an unramified abelian extension of number fields and $\mathfrak{P}$ a finite prime of L lying above a prime $\mathfrak{p}$ of K. For any $\tau \in G$ we have

$$\left(\frac{L/K}{\tau(\mathfrak{P})}\right) = \tau \left(\frac{L/K}{\mathfrak{P}}\right) \tau^{-1} = \left(\frac{L/K}{\mathfrak{P}}\right).$$

Hence if G is abelian, the Frobenius automorphisms $\sigma_{\tau\mathfrak{P}}$ of the primes $\tau\mathfrak{P}$ are all the same. The Frobenius automorphisms in G then depends only on $\mathfrak{p} = \mathfrak{P} \cap K$ not $\mathfrak{P}$ itself.

For abelian extensions we use the notation $\left(\frac{L/K}{\mathfrak{p}}\right)$ for $\left(\frac{L/K}{\mathfrak{P}}\right)$ and call this the Frobenius automorphism of $\mathfrak{p}$.

We define the group of fractional ideals of $\mathcal{O}_K$ to be the free abelian group generated by the prime ideals of $\mathcal{O}_K$, and denote it by I_K. Then any element of I_K is of the form $\prod_{\mathfrak{p}} \mathfrak{p}^{v(\mathfrak{p})}$ and we define

$$\left(\frac{L/K}{\prod_{\mathfrak{p}} \mathfrak{p}^{v(\mathfrak{p})}}\right) = \prod_{\mathfrak{p}} \left(\frac{L/K}{\mathfrak{p}}\right)^{v(\mathfrak{p})}.$$

Theorem 2.1.1. *The map defined by*

$$\begin{aligned} I_K &\to \mathrm{Gal}(L/K) \\ \mathfrak{a} &\mapsto \left(\frac{L/K}{\mathfrak{a}}\right) \end{aligned}$$

for unramified abelian extension L/K is a group homomorphism and it is surjective . It is called the Artin map.

Let P_K be the group of principal ideals of K. P_K is a subgroup of I_K and the quotient group I_K/P_K is finite and it is called the class group of K. We denote it by Cl_K or $\mathrm{Cl}(\mathcal{O}_K)$.

Theorem 2.1.2. *Given a number field K, there is an unramified finite abelian extension $\mathcal{H}_K$ of K, called the Hilbert class field, such that the Artin map induces an isomorphism*

$$\mathrm{Cl}_K \xrightarrow{\sim} \mathrm{Gal}(\mathcal{H}_K/K).$$

The field $\mathcal{H}_K$ is the maximal abelian unramified extension of K.

For a number field K, a finite prime is simply a prime ideal of K and an infinite prime is an embedding of K into $\mathbb{C}$. We define a modulus $\mathfrak{m}$ as a formal product of primes in K, finite or infinite. We denote by $\mathfrak{m}_0$ the finite part of $\mathfrak{m}$ and by $\mathfrak{m}_\infty$ the infinite part,

a subset of real embeddings. Let $I_{\mathfrak{m},K}$ be the subset of I_K generated by ideals coprime to $\mathfrak{m}_0$ and $P_{\mathfrak{m},K}$ be the subgroup of $I_{\mathfrak{m},K}$ generated by principal ideals of the form $\alpha\mathcal{O}_K$, with $\alpha \equiv 1 \mod \mathfrak{m}_0$ and $i(\alpha) > 0$ for all embeddings $i \in \mathfrak{m}_\infty$

The quotient $I_{\mathfrak{m},K}/P_{\mathfrak{m},K}$ is called the ray class group of K modulo $\mathfrak{m}$ and we denote it by $\mathrm{Cl}_{\mathfrak{m},K}$. If $\mathfrak{m}$ contains all the real embeddings, $\mathrm{Cl}_{\mathfrak{m},K}$ is called the narrow ray class group modulo $\mathfrak{m}_0$.

Example 2.1.3. *If $\mathfrak{m} = \mathfrak{m}_0 = \mathcal{O}_K$ then the ray class group $\mathrm{Cl}_{\mathfrak{m},K}$ is just the usual class group $\mathrm{Cl}(\mathcal{O}_K)$ and narrow ray class group modulo $\mathfrak{m}_0$ (i.e. $\mathfrak{m}_\infty$ contains all the real embeddings) is the usual narrow class group, which is defined as the set of invertible fractional ideals modulo the subgroup of principal ideals generated by totally positive elements.*

We define an order $\mathcal{O}$ in a number field K to be a lattice that is also a unitary subring of full rank of $\mathcal{O}_K$. The conductor of $\mathcal{O}$ is defined as $\mathfrak{f}_\mathcal{O} = \{x \in K : x\mathcal{O}_K \subset \mathcal{O}\}$. It is an invariant of the order and is the largest subset of K that is an ideal of $\mathcal{O}$ and $\mathcal{O}_K$.

If $\mathcal{O}$ is an order in K, we define the Picard group, $\mathrm{Pic}(\mathcal{O})$, to be the set of invertible fractional ideals of $\mathcal{O}$, modulo the subgroup of principal ideals.

Theorem 2.1.4. *The map*

$$\begin{aligned} I_{\mathfrak{f}_\mathcal{O},K} &\to \mathrm{Pic}(\mathcal{O}) \\ \mathfrak{a} &\mapsto [\mathfrak{a} \cap \mathcal{O}] \end{aligned}$$

is a surjective homomorphism with kernel $P_{\mathfrak{f}_\mathcal{O}} = \{\alpha\mathcal{O}_K : \alpha \in \mathcal{O}, \alpha\mathcal{O} + \mathfrak{f}_\mathcal{O} = \mathcal{O}\}$.

Theorem 2.1.5. *There is a unique abelian extension $\mathcal{H}_\mathcal{O}$ of K called the ring class field of $\mathcal{O}$, such that all primes of K ramified in $\mathcal{H}_\mathcal{O}$ divide the conductor $\mathfrak{f}_\mathcal{O}$ of $\mathcal{O}$ and the map*

$$\begin{aligned} I_{\mathfrak{f}_\mathcal{O},K} &\to \mathrm{Gal}(\mathcal{H}_\mathcal{O}/K) \\ \mathfrak{a} &\mapsto \left(\frac{\mathcal{H}_{\mathcal{O}/K}}{\mathfrak{a}}\right) \end{aligned}$$

given by the Artin symbol is surjective with kernel $P_{\mathfrak{f}_\mathcal{O}}$.

The map in Theorem 2.1.5 induces an ismomorphism $\mathrm{Pic}(\mathcal{O}) \cong \mathrm{Gal}(\mathcal{H}_\mathcal{O}/K)$.

2.2 Abelian varieties

The main objects of study in this thesis are abelian varieties and their endomorphism rings. In this section we review some basics of abelian varieties that are relevant throughout the thesis. We follow classical references such as [11, 75, 82, 83, 91] and we refer to them for proofs.

2.2.1 Abelian varieties

Definition 2.2.1.1. A group variety over a field k is a variety V together with the morphisms

$$m : V \times V \to V \text{ and } i : V \to V$$

and a point $\varepsilon \in V(k)$ such that the structure on $V(\overline{k})$ defined by m and i is that of a group with multiplication induced m, inverse by i and identity element ε.

We fix a perfect field k as the base field of varieties and curves in this section.

Definition 2.2.1.2. A connected and complete group variety is called an abelian variety.

We denote the group operations of abelian varieties additively.

Definition 2.2.1.3. A homorphism of abelian varieties is a morphism of the underlying algebraic varieties that preserves the group structure.

Proposition 2.2.1.4. *Let $\mathcal{A}$ be an abelian variety. Then*

- *every morphism $f : \mathcal{A} \to \mathcal{B}$ of abelian varieties is the composite of a homomorphism $h : \mathcal{A} \to \mathcal{B}$ with a translation t_b, where $b = -f(0) \in \mathcal{B}(k)$;*
- *the group law on $\mathcal{A}$ is commutative.*

Proposition 2.2.1.5 (Rigidity theorem)**.** *A group variety is an abelian variety if and only if it is projective.*

Example 2.2.1.6. *Elliptic curves, which are smooth, projective, algebraic curves of genus one with a specified point, are abelian varieties of dimension* 1*. If the characteristic of the base field is different from* 2 *and* 3*, they can also be defined as a plane algebraic curve*

$\mathcal{E} : y^2 = x^3 + ax + b$, with $a, b \in k$ and $4a^3 + 37b^2 \neq 0$. The specified point serves as the identity element of the group. In higher dimension, it is in general hard to find equations describing abelian varieties, the theory is much more abstract.

The quotient of any abelian variety by any closed subgroup is an abelian variety. In particular the quotient of an abelian variety by any finite subgroup is an abelian variety and they have the same dimension.

Definition 2.2.1.7. We say that an abelian variety is simple if it has no non-proper abelian subvarieties defined over k and that it is absolutely simple if it has no non-proper abelian subvarieties over the algebraic closure $\overline{k}$.

2.2.2 Isogeny

Let $\mathcal{A}, \mathcal{B}$ be abelian varieties. A homomorphism $f : \mathcal{A} \to \mathcal{B}$ is an isogeny if it is surjective and the abelian varieties have the same dimension. The kernel of an isogeny is finite. The degree of an isogeny is the degree of the function field extension $[k(\mathcal{B}) : k(\mathcal{A})]$. An isogeny is separable if the function field extension is separable. When the isogeny is separable, its degree is equal to the size of its kernel. When there is an isogeny from $\mathcal{A}$ to $\mathcal{B}$, we say $\mathcal{A}$ is isogenous to $\mathcal{B}$.

Example 2.2.2.1.

- *Let $\mathcal{E}_1$ and $\mathcal{E}_2$ be elliptic curves given by equations $y^2 = x^3 + x$ and $y^2 = x^3 - 3x + 3$ defined over $\mathbb{F}_{71}$, respectively. The map from $\mathcal{E}_1$ to $\mathcal{E}_2$ defined by*

$$(x, y) \mapsto \left(\frac{x^3 - 4x^2 + 30x - 12}{(x-2)^2}, \frac{x^3 - 6x^2 - 14x + 35}{(x-2)^3} \cdot y \right)$$

  is a isogeny and its kernel is given by $\{(2, 9), (2, -9), \infty\}$, where ∞ is the point at infinity.

- *For any abelian variety $\mathcal{A}$, the homormorphism multipication by n, denoted by $[n]_{\mathcal{A}}$, is an isogeny and we write its kernel as $\mathcal{A}[n]$.*

- *The compositon of two isogenies is also an isogny and the degree of the composite is the product of the degree of the two isogenies.*

Theorem 2.2.2.2. *If* $\dim(\mathcal{A}) = g$ *and* $\operatorname{char} k = p$*, then the map* $[n]_{\mathcal{A}}$ *is separable when* n *is coprime to* p *and in that case* $\mathcal{A}[n] \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$*. When* n *is a power of* p*, then* $\mathcal{A}[n] \cong \mathbb{Z}/n^r\mathbb{Z}$*, where* $r \leq g$ *and it is called the* p*-rank of* $\mathcal{A}$*.*

Definition 2.2.2.3. Assume k has characteristic $p \neq 0$. Then the abelian variety $\mathcal{A}$ of dimension g is called ordinary if the p-rank is equal to g. If $g = 1$ and $\mathcal{A}$ is not ordinary, $\mathcal{A}$ is said to be supersingular.

Proposition 2.2.2.4. *If* $f : \mathcal{A} \to \mathcal{B}$ *is an isogeny of degree* d*, then there exists an isogeny* $\hat{f} : \mathcal{B} \to \mathcal{A}$*, called the dual of* f*, such that* $\hat{f} \circ f = [d]_{\mathcal{A}}$ *and* $f \circ \hat{f} = [d]_{\mathcal{B}}$*.*

Corollary 2.2.2.5. *Being isogenous is an equivalence relation.*

Definition 2.2.2.6. An abelian variety is said to be supersingular if it is isogenous to a product of supersingular elliptic curves and it is said to be superspecial if it isomorphic to a product of supersingular elliptic curves.

Proposition 2.2.2.7. *Every nonzero abelian variety* $\mathcal{A}$ *defined over* k *is isogenous to a product of power of non-isogenous simple abelian varieties over* k*.*

2.2.3 Dual abelian varieties and polarizations

Let $\mathcal{A}$ be an abelian variety defined over k. We define the Picard group of $\mathcal{A}$ as the group $\operatorname{Pic}(\mathcal{A})$ of isomorphism classes of line bundles on $\mathcal{A}_{\overline{k}}$. Let $\mathcal{L}$ be a line bundle on $\mathcal{A}_{\overline{k}}$ and $\phi_{\mathcal{L}}$ be the map defined by

$$\begin{aligned} \phi_{\mathcal{L}} : \mathcal{A}(\overline{k}) &\to \operatorname{Pic}(\mathcal{A}) \\ x &\mapsto [T_x^*\mathcal{L} \otimes \mathcal{L}^{-1}] \end{aligned}$$

where $[\mathcal{L}]$ is the isomorphism class of $\mathcal{L}$ and T_x is the translation by x on $\mathcal{A}(\overline{k})$, see [91, Section 2.6].

Theorem 2.2.3.1. *The map* $\phi_{\mathcal{L}}$ *is a homomorphism.*

Let $\operatorname{Pic}^0(\mathcal{A}) = \{[\mathcal{L}] \in \operatorname{Pic}(\mathcal{A}) : [T_x^*\mathcal{L}] = [\mathcal{L}], \text{ for all } x \in \mathcal{A}(\overline{k})\}$. $\operatorname{Pic}^0(\mathcal{A})$ is a subgroup of $\operatorname{Pic}(\mathcal{A})$ and it can also be defined as the isomorphism classes of line bundles $[\mathcal{L}]$ such that the map $\phi_{\mathcal{L}}$ is the zero homomorphism.

Theorem 2.2.3.2. $\operatorname{Pic}^0(\mathcal{A})$ *is the group of* $\overline{k}$*-points of an abelian variety over* k*.*

Definition 2.2.3.3. The abelian variety in Theorem 2.2.3.2 is called the dual of $\mathcal{A}$ and we denote as $\hat{\mathcal{A}}$.

Every homomorphism $f : \mathcal{A} \to \mathcal{B}$ of abelian varieties gives rise to a homomorphism $\hat{f} : \hat{\mathcal{B}} \to \hat{\mathcal{A}}$, by just sending $[\mathcal{L}]$ to $[f^*\mathcal{L}]$.

Definition 2.2.3.4. A polarization $\lambda_{\mathcal{A}}$ on an abelian variety $\mathcal{A}$ is an isogeny $\lambda_{\mathcal{A}} : \mathcal{A} \to \hat{\mathcal{A}}$ such that $\lambda_{\mathcal{A}} = \phi_{\mathcal{L}}$, where $\mathcal{L}$ is an ample line bundle on $\mathcal{A}(\overline{k})$. The degree of a polarization is the degree of the isogeny. It is called principal if it is an isomorphism, i.e. it has degree one.

A polarized abelian variety is an abelian variety together with a polarization. We say that a polarized abelian variety $(\mathcal{A}, \lambda_{\mathcal{A}})$ is defined over k if both $\mathcal{A}$ and $\lambda_{\mathcal{A}}$ are defined over k. Two polarized abelian varieties $(\mathcal{A}, \lambda_{\mathcal{A}})$ and $(\mathcal{B}, \lambda_{\mathcal{B}})$ are isogenous if there is an isogeny of abelian varieties, $f : \mathcal{A} \to \mathcal{B}$, that is compatible with the polarizations, i.e, the following diagram commutes:

$$\begin{array}{ccc} \mathcal{A} & \xrightarrow{f} & \mathcal{B} \\ \downarrow{\scriptstyle \lambda_{\mathcal{A}}} & & \downarrow{\scriptstyle \lambda_{\mathcal{B}}} \\ \hat{\mathcal{A}} & \xleftarrow[\hat{f}]{} & \hat{\mathcal{B}} \end{array}$$

2.2.4 Endomorphism rings

Let $\mathcal{A}$ and $\mathcal{B}$ be abelian varieties over a field k and f, g two homomorphisms from $\mathcal{A}$ to $\mathcal{B}$. We define a morphism $f + g : \mathcal{A} \to \mathcal{B}$ as follows:

$$(f + g)(x) = f(x) + g(x),$$

It then follows that $\mathrm{Hom}_k(\mathcal{A}, \mathcal{B})$, the set of all homorphisms from $\mathcal{A}$ to $\mathcal{B}$ defined over k, has the structure of an abelian group. Hence $\mathrm{End}_k(\mathcal{A}) := \mathrm{Hom}_k(\mathcal{A}, \mathcal{A})$ has a ring structure with composition as multiplication.

The group $\mathrm{Hom}_k(\mathcal{A}, \mathcal{B})$ is torsion free. In fact, we have for $n \in \mathbb{Z} \setminus \{0\}$ and $f \in \mathrm{Hom}_k(\mathcal{A}, \mathcal{B})$, then $n \circ f = [n]_{\mathcal{B}} \circ f = f \circ [n]_{\mathcal{A}}$ and since the kernels of $[n]_{\mathcal{A}}$ and $[n]_{\mathcal{B}}$ are finite, we have that $n \circ f$ is not the zero homomorphism if f is not the zero homomorphism. We call $\mathrm{End}_k(\mathcal{A}) \otimes_{\mathbb{Z}} \mathbb{Q}$ the endomorphism algebra of $\mathcal{A}$. If $f \in \mathrm{Hom}_k(\mathcal{A}, \mathcal{B})$ is an isogeny, it is invertible in $\mathrm{Hom}_k(\mathcal{A}, \mathcal{B}) \otimes_{\mathbb{Z}} \mathbb{Q}$.

Proposition 2.2.4.1. *Let $f : \mathcal{A} \to \mathcal{B}$ be a homomorphism between abelian varieties. If $\mathcal{A}$ and $\mathcal{B}$ are simple then f is either zero or an isogeny.*

For a simple abelian variety $\mathcal{A}$, all nonzero elements of $\mathrm{End}_k(\mathcal{A})$ are isogenies.

2.2.5 The Rosati involution

Let $(\mathcal{A}, \lambda_{\mathcal{A}})$ be a polarized abelian variety. The isogeny $\lambda_{\mathcal{A}}$ is invertible in $\mathrm{Hom}_k(\mathcal{A}, \hat{\mathcal{A}}) \otimes_{\mathbb{Z}} \mathbb{Q}$. We define the Rosati involution as follows:

Definition 2.2.5.1. The Rosati involution on the endomorphism algebra, $\mathrm{End}_k(\mathcal{A}) \otimes_{\mathbb{Z}} \mathbb{Q}$, corresponding to $\lambda_{\mathcal{A}}$ is defined by the map

$$\begin{aligned}(\cdot)^\dagger : \mathrm{End}_k(\mathcal{A}) \otimes_{\mathbb{Z}} \mathbb{Q} &\to \mathrm{End}_k(\mathcal{A}) \otimes_{\mathbb{Z}} \mathbb{Q} \\ \alpha &\mapsto \alpha^\dagger := \lambda_{\mathcal{A}}^{-1} \circ \hat{\alpha} \circ \lambda_{\mathcal{A}}.\end{aligned}$$

Theorem 2.2.5.2. *The bilinear form*

$$\begin{aligned}\mathrm{End}_k(\mathcal{A}) \otimes_{\mathbb{Z}} \mathbb{Q} \times \mathrm{End}_k(\mathcal{A}) \otimes_{\mathbb{Z}} \mathbb{Q} &\to \mathbb{Q} \\ (\alpha, \beta) &\mapsto \mathrm{Tr}(\alpha \circ \beta^\dagger)\end{aligned}$$

is positive definite.

From the previous theorem we have:

Proposition 2.2.5.3. *The automorphism group of $(\mathcal{A}, \lambda_{\mathcal{A}})$ is finite.*

2.2.6 Jacobian varieties

Throughout the thesis, by a curve C of genus g defined over k, we mean a smooth, projective, geometrically irreducible curve over k of genus g.

The Jacobian of C denoted by $\mathrm{Jac}(C)$ is a certain principally polarized abelian variety of dimension g such that $\mathrm{Jac}(C)(\overline{k}) = \mathrm{Pic}^0(C(\overline{k}))$, where $\mathrm{Pic}^0(C)$ is the group of degree-0 divisors on C modulo the group of principal divisors. If C is an elliptic curve then we have $\mathrm{Jac}(C) \cong C$.

Given a point $P \in C(\overline{k})$, the Abel-Jacobi map with base point P is defined by

$$\begin{aligned} \alpha : C &\to \mathrm{Jac}(C) \\ Q &\mapsto [Q - P]. \end{aligned}$$

It is a morphism of varieties over $\overline{k}$ and can be extended additively to divisors.

Every morphism of curves $\varphi : C \to C'$ induces a homomorphism $\varphi_* : \mathrm{Div}(C) \to \mathrm{Div}(C')$ given by $[P] \mapsto [\varphi(P)]$. The homomorphism φ_* maps degree-0 divisors to degree-0 divisors and principal divisors to principal divisors and so induces a homomorphism $\varphi_* : \mathrm{Jac}(C) \to \mathrm{Jac}(C')$. If α, α' are Abel-Jacobi maps with base point $P \in C$ and $\varphi(P) \in C'$ respectively, the diagram

$$\begin{array}{ccc} C & \xrightarrow{\varphi} & C' \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \alpha'} \\ \mathrm{Jac}(C) & \xrightarrow{\varphi_*} & \mathrm{Jac}(C') \end{array}$$

commutes.

Theorem 2.2.6.1. *[83, Section 12] Let C and C' be curves defined over an algebraically closed field k, and α, α' the Abel-Jacobi maps with base point $P \in C$, $\varphi(P) \in C'$ respectively. Let $\varphi : \mathrm{Jac}(C) \to \mathrm{Jac}(C')$ be an isomorphism of principally polarized abelian varieties.*

1. *There exists an isomorphism $\rho : C \to C'$ that satisfies $\varphi = \pm\rho_*$.*
2. *Assume that the curves have genus ≥ 2. If C is not hyperelliptic, then the sign can be chosen arbitrarily, and ρ is uniquely determined by φ and $\pm$.*

From Theorem 2.2.6.1, two curves defined over $\overline{k}$ are isomorphic if and only if their Jacobians are isomorphic as polarized abelian varieties.

Definition 2.2.6.2. Hyperelliptic curves of genus g are curves of the form $y^2 = f(x)$, for some squarefree polynomial of degree $2g + 1$ or $2g + 2$.

Proposition 2.2.6.3. *[118] Abelian varieties of dimension one or two are Jacobian varieties of hyperelliptic curves. In dimension three, an abelian variety is the Jacobian of either a genus 3 plane quartic or a hyperelliptic curve.*

2.3 Complex abelian varieties

The theorems and their proofs in this section can be found in [75].

Definition 2.3.1. A complex torus is a quotient V/Λ, where V is a complex vector space and Λ a lattice in V, i.e, a discrete subgroup of full rank.

Definition 2.3.2. Let V/Λ be a complex torus. A Riemann form on V/Λ is an anti-symmetric form $E : V \times V \to \mathbb{R}$ that is $\mathbb{R}$-bilinear, satisfies $E(\Lambda, \Lambda) \subseteq \mathbb{Z}$, such that for $u, v \in V$ we have $E(iu, v) = E(iv, u)$ and such that the associated Hermitian form $H(u, v) = E(iu, v) + iE(u, v)$ is positive definite.

We say that a complex torus is polarizable if it admits a Riemann form.

Let $\mathcal{A}$ be an abelian variety defined over $\mathbb{C}$. Then $\mathcal{A}$ is complex manifold and it has the analytic structure of a complex torus. If the dimension of $\mathcal{A}$ is g, then the tangent space to the identity of $\mathcal{A}$ is isomorphic to $\mathbb{C}^g$.

The exponential map, $\exp_{\mathcal{A}} : \mathbb{C}^g \to \mathcal{A}$ is surjective and $\Lambda := \ker \exp_{\mathcal{A}}$ is a lattice of $\mathbb{C}^g$ and we have $\mathbb{C}^g/\Lambda \cong \mathcal{A}$.

Not all complex tori correspond to some abelian variety.

Theorem 2.3.3. *A complex torus is an abelian variety if and only if it is polarizable.*

A polarization of a complex abelian variety determines a Riemann form and it is principal if and only if the determinant of the corresponding Riemann form is 1.

Definition 2.3.4. The Siegel upper half-space $\mathcal{H}_g$ is the set of $g \times g$ symmetric matrices over $\mathbb{C}$ with positive definite imaginary part.

Theorem 2.3.5. *Complex tori $\mathbb{C}^g/\Lambda$ corresponding to abelian varieties are exactly those whose lattice Λ can be put under the form $\mathbb{Z}^g + \Omega\mathbb{Z}^g$ for some matrix Ω in $\mathcal{H}_g$.*

For an abelian variety $\mathcal{A} := \mathbb{C}^g/\left(\mathbb{Z}^g + \Omega\mathbb{Z}^g\right)$, the matrix Ω is called the period matrix of $\mathcal{A}$.

We define the symplectic group $\mathrm{Sp}_{2g}(\mathbb{Z})$ as the group of $2g \times 2g$ matrices M with coefficients in $\mathbb{Z}$ satisfying

$$ {}^tM \begin{pmatrix} 0 & \mathbf{1}_g \\ -\mathbf{1}_g & 0 \end{pmatrix} M = \begin{pmatrix} 0 & \mathbf{1}_g \\ -\mathbf{1}_g & 0 \end{pmatrix}. $$

Theorem 2.3.6. *Two complex abelian varieties $\mathcal{A}$ and $\mathcal{A}'$ with period matrices Ω and Ω' are isomorphic if and only if there is a matrix $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{Sp}_{2g}(\mathbb{Z})$ such that $\Omega = (A\Omega' + B)(C\Omega' + D)^{-1}$.*

It follows that the symplectic group $\mathrm{Sp}_{2g}(\mathbb{Z})$ acts on $\mathcal{H}_g$ and equivalence classes correspond to the isomorphism classes of complex abelian varieties of dimension g.

Let $T = V/\Lambda$ be a complex torus and E a Riemann form on T. The dual $\hat{T}$ is given by $\hat{T} = V^*/\Lambda^*$, with V^* the complex vector space of the antilinear functionals $V \to \mathbb{C}$ and $\Lambda^* = \{f \in V^* : \mathrm{Im}(f) \subseteq \mathbb{Z}\}$.

If a complex abelian variety $\mathcal{A}$ corresponds to the complex torus T, then its dual $\hat{\mathcal{A}}$ corresponds to $\hat{T}$. The isogeny corresponding to E is defined from $\mathcal{A}$ to $\hat{\mathcal{A}}$ as follows: $\lambda_{\mathcal{A}} : \mathcal{A} \to \hat{\mathcal{A}}$, $\lambda_{\mathcal{A}}(v) = H(v, \cdot)$, where H is the Hermitian form associated to E.

2.4 Complex multiplication

We refer to [107] and [112] for more details on this section.

2.4.1 CM-fields and CM-types

Definition 2.4.1.1. A CM-field is a number field K that is a totally imaginary quadratic extension of a totally real number field K_0.

Lemma 2.4.1.2. *[107, Section 8.1, Lemma 3] Let K be a number field. The following are equivalent.*

1. *The field K is totally real or a CM-field.*
2. *There exists an automorphism $\bar{\cdot} : x \mapsto \overline{x}$ of K such that for every embedding $\sigma : K \to \mathbb{C}$, the automorphism $\bar{\cdot}$ is the restriction of complex conjugation on $\mathbb{C}$ to K via σ, i.e, we have $\bar{\cdot} \circ \sigma = \sigma \circ \bar{\cdot}$.*

Moreover, the following holds:

- *any composite of finitely many CM-fields and totally real fields containing at least one CM-field is a CM-field,*
- *the normal closure of CM-field is a CM-field,*
- *if ϕ is an embedding of CM-fields $K_1 \to K_2$, then we have $\bar{\cdot} \circ \phi = \phi \circ \bar{\cdot}$.*
- *any subfield of a CM-field is totally real or a CM-field.*

Let K be a CM-field of degree $2n$. There are then $2n$ embeddings of K into the normal closure K^c and since K is totally complex, each embedding has a complex conjugate.

Definition 2.4.1.3. A CM-type, Φ, of K is a collection of n embeddings such that an embedding and its complex conjugate are not in Φ at the same time. Two CM-type Φ, Φ' are equivalent if there is an automorphism σ of K such that $\sigma\Phi = \Phi'$.

Let $K_1 \subseteq K_2$ be CM-fields and Φ a CM-type of K_1. There is a CM-type of K_2

$$\Phi_{K_2} = \{\phi \in \mathrm{Hom}(K_2, L) : \phi|_{K_1} \in \Phi\},$$

with L normal over $\mathbb{Q}$ and contains subfields isomorphic to K_1 and K_2. We say that the CM-type Φ_{K_2} is induced by Φ or that Φ induces Φ_{K_2}.

Definition 2.4.1.4. A CM-type is said to be primitive if it is not induced from a CM-type of a strict CM-subfield.

Proposition 2.4.1.5. *[84, Proposition 1.9] Let K be a CM-field and Φ a CM-type of K with values in $L \supseteq K^c$. There is a unique subfield $K_1 \subset K$ and a unique CM-type Φ_1 of K_1 with values in L such that Φ_1 is primitive and Φ is induced from Φ_1. Also we have*

$$\mathrm{Gal}(K^c/K_1) = \{\sigma \in \mathrm{Gal}(K^c/\mathbb{Q}) : \Phi_{K^c}\sigma = \Phi_{K^c}\}.$$

For quartic CM-fields we have the following.

Example 2.4.1.6. *[107, Example 8.4(2)] A quartic CM-field K is either Galois cyclic, biquadratic, or non-normal with Galois group D_4 (of order 8).*

- *If K is biquadratic, there is only one equivalence class of CM-types and the field is not primitive. It has an imaginary quadratic subfield whose CM-type induces the CM-type of K.*

- *If K is cyclic, there is also only one CM-type up to equivalence. However the field together with the CM-type is primitive.*
- *In general if the CM-field is abelian, it has a unique equivalence class of CM-types.*
- *In the non-Galois case, there are two equivalence classes of CM-types (since the only non trivial automorphism is the complex conjugate).*

For any pair (K, Φ) of CM-field and CM-type, there exists another pair (K^r, Φ^r) associated to it called the reflex of (K, Φ) and it is defined as follows.

Considering the CM-type Φ as having value in K^c, the induced CM-type Φ_{K^c} with values in K^c is a collection of automorphisms and we can take the inverse $\Phi_{K^c}^{-1} := \{\phi^{-1} | \phi \in \Phi_{K^c}\}$. $\Phi_{K^c}^{-1}$ is also a CM-type of K^c. The pair (K^r, Φ^r) are the CM-field and the primitive CM-type that induces Φ_L^{-1}, see Proposition 2.4.1.5.

Definition 2.4.1.7. The field K^r is called the reflex field of (K, Φ), the CM-type Φ^r is called the reflex type of (K, Φ) and (K^r, Φ^r) the reflex of (K, Φ).

If (K, Φ) is primitive, then we have $K^{rr} = K$ and $\Phi^{rr} = \Phi$, see [107, Section 8.3 Proposition 29].

Lemma 2.4.1.8. *[84, Example 1.28] Let (K, Φ) be a pair of CM-field and CM-type. We have:*

1. $\mathrm{Gal}(K^c/K^r) = \{\sigma \in \mathrm{Gal}(K^c/\mathbb{Q}) : \sigma\Phi = \Phi\}$
2. *The field K^r is generated over $\mathbb{Q}$ in K^c by an element of the form $\sum_{\phi\in\Phi} \phi(x)$ for $x \in K$.*

Example 2.4.1.9. *[107, Example 8.4(2)(C)] Let K be a non-Galois quartic CM-field. Its normal closure K^c has Galois group $D_4 = \langle r, s\rangle$ with $r^4 = s^2 = (rs)^2 = e$. The complex conjugation automorphism $\bar{\cdot}$ equals r^2 in this notation. We assume that $\mathrm{Gal}(K^c/K) = \langle s\rangle$. The CM-types of K up to equivalence are $\Phi = \{\mathrm{id}, r_{|K}\}$ and $\Phi' = \{\mathrm{id}, r^3_{|K}\}$.*

The CM-type induced by Φ on the normal closure of K is $\Phi_{K^c} = \{e, r, s, rs\}$ and we have $\Phi_{K^c}^{-1} = \{e, r^3, s, rs\} = \{e, r^3\}\langle rs\rangle$. We then obtain the reflex field K^r of Φ as the fixed field of $\langle rs\rangle$. K^r is also a quartic CM-field but is not isomorphic to K. The reflex type of Φ is the CM-type $\{\mathrm{id}, r^3_{|K^r}\}$.

Let (K, Φ) be a pair of CM-field K and CM-type of Φ.

Definition 2.4.1.10. The type norm of Φ is defined as

$$\begin{aligned} N_\Phi : K &\to K^r \\ x &\mapsto \prod_{\phi\in\Phi} \phi(x). \end{aligned}$$

We can also define the reflex type norm which is the type norm of Φ^r. If (K,Φ) is primitive, N_{Φ^r} is defined from K^r to K.

The type norm map can be extended to ideals and ideal class groups.

Lemma 2.4.1.11. *[107, Section 8.3, Proposition 29] The map N_Φ induces homomorphisms*

$$\begin{aligned} N_\Phi : I_K &\to I_{K^r} \\ \mathfrak{a} &\mapsto \mathfrak{a}', \end{aligned}$$

where $\mathfrak{a}'\mathcal{O}_{K^c} = \prod_{\phi\in\Phi} \phi(\mathfrak{a})\mathcal{O}_{K^c}$,

and

$$N_\Phi : \mathrm{Cl}_K \to \mathrm{Cl}_{K^r}\,.$$

2.4.2 Complex multiplication on complex abelian varieties

Definition 2.4.2.1. An abelian variety $\mathcal{A}$ defined over k of dimension g is said to have complex multiplication or CM by a CM-field K, if K has degree $2g$ and there is an embedding $i : K \to \mathrm{End}(\mathcal{A}) \otimes \mathbb{Q}$, $\mathrm{End}(\mathcal{A}) := \mathrm{End}_{\overline{k}}(\mathcal{A})$. We say that $\mathcal{A}$ has CM by an order $\mathcal{O}$ of K if $i^{-1}(\mathrm{End}(\mathcal{A})) = \mathcal{O}$. We say that $(\mathcal{A}, i)$ is defined over k if $\mathcal{A}$ is defined over k as well as every element of $i(\mathcal{O})$.

Let $\mathcal{A}$ be a complex abelian variety of dimension g with complex multiplication by K and a fixed $i : K \to \mathrm{End}(\mathcal{A}) \otimes \mathbb{Q}$. There is a ring homomorphism $D : \mathrm{End}(\mathcal{A}) \to \mathrm{End}(\mathbb{C}^g)$ called the analytic representation of $\mathrm{End}(\mathcal{A})$. Let ρ be the composition $\rho := D \circ i : K \to \mathrm{End}(\mathbb{C}^g)$.

Lemma 2.4.2.2. *[107, Section 5.2] There exists a unique CM-type Φ of K such that the representation ρ is equivalent over $\mathbb{C}$ to the direct sum representation $\oplus_{\phi\in\Phi}\phi$.*

We say that $(\mathcal{A}, i)$ has CM-type (K,Φ).

Proposition 2.4.2.3. *[107, Section 8.2] A polarized abelian variety with CM-type (K, Φ) is absolutely simple if and only if Φ is primitive.*

Proposition 2.4.2.4. *There is a bijection between the set of isogeny classes of simple ordinary pairs $(\mathcal{A}, i)$ and the set of isomorphism classes of primitive types (K, Φ)*

Definition 2.4.2.5. Let $(\mathcal{A}, i)$ and $(\mathcal{A}', i')$ be abelian varieties of type (K, Φ). A homomorphism f from $\mathcal{A}$ to $\mathcal{A}'$ is called a homomorphism from $(\mathcal{A}, i)$ to $(\mathcal{A}', i')$ if it satisfies

$$f \circ i(\alpha) = i'(\alpha) \circ f$$

for every $\alpha \in K$.

Proposition 2.4.2.6. *[107, Section 14, Proposition 1] Let (K, Φ) be a primitive CM-type and let $(\mathcal{A}, i)$ and $(\mathcal{A}', i')$ be varieties of type (K, Φ). Then every homomorphism of $\mathcal{A}$ into $\mathcal{A}'$ is a homomorphism of $(\mathcal{A}, i)$ into $(\mathcal{A}', i')$.*

Proposition 2.4.2.7. *[107, Section 8.5, Proposition 30] Let $\mathcal{A}$ be a simple abelian variety over a field $k \subset \mathbb{C}$ with CM by (K, Φ) and $i : K \hookrightarrow \mathrm{End}(\mathcal{A}) \otimes \mathbb{Q}$. Then $\mathcal{A}$ is defined over k if and only if the reflex field K^r of (K, Φ) is contained in k.*

We define a lattice in an algebraic number field K as a finitely generated $\mathbb{Z}$-submodule of K that spans K over $\mathbb{Q}$.

Let K be a CM-field of degree $2g$ and $\Phi = \{\phi_1, \ldots, \phi_g\}$ be a CM-type of K with values in $\mathbb{C}$. We consider Φ as a map from K to $\mathbb{C}^g$ by $\Phi(x) = (\phi_1(x), \ldots, \phi_g(x))$ for all $x \in K$. For any lattice $\mathfrak{a}$ of K, the image $\Phi(\mathfrak{a})$ is a lattice of rank $2g$ inside $\mathbb{C}^g$ and hence $\mathbb{C}^g/\Phi(\mathfrak{a})$ is a complex torus.

Theorem 2.4.2.8. *[107, Section 7] Any complex abelian variety $\mathcal{A}$ with CM by (K, Φ) with $i^{-1}(\mathrm{End}(\mathcal{A})) = \mathcal{O}$ is analytically ismomorphic to $\mathbb{C}^g/\Phi(\mathfrak{a})$, for some lattice $\mathfrak{a}$ in $\mathcal{O}$. Furthermore*

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

For an inveritble ideal $\mathfrak{m}$ in $\mathcal{O}$, the variety $\mathbb{C}^g/\Phi(\mathfrak{m}^{-1}\mathfrak{a})$ is isogenous to $\mathbb{C}^g/\Phi(\mathfrak{a})$, and its endomorphism ring is also $\mathcal{O}$. The varieties are isomorphic if and only if $\mathfrak{m}$ is principal. It then follows that:

Proposition 2.4.2.9. *[107, Section 7] The Picard group $\mathrm{Pic}(\mathcal{O})$ acts freely on the set of isomorphism classses of abelian varieties of CM-type (K, Φ) with endomorphim ring $\mathcal{O}$.*

Let $(\mathcal{A}, i)$ be a complex abelian variety with primitive CM-type (K, Φ) and $\mathcal{O} = i^{-1}(\mathrm{End}(\mathcal{A}))$. A polarization on $\mathcal{A}$ can be described in terms of the arithmetic of K.

We assume that $\mathcal{A}$ admits a polarization and is of dimension g. $\mathcal{A}$ is isomorphic to $\mathbb{C}^g/\Phi(\mathfrak{a})$, with $\mathfrak{a}$ some lattice of K. The dual of the variety $\mathbb{C}^g/\Phi(\mathfrak{a})$ is given by $\mathbb{C}^g/\Phi(\mathfrak{a}^*)$ where

$$\mathfrak{a}^* = \{\beta : \mathrm{Tr}_{K/\mathbb{Q}}(\beta\overline{\mathfrak{a}}) \subset \mathbb{Z}\}.$$

A polarization $\lambda_{\mathcal{A}} : \mathbb{C}^g/\Phi(\mathfrak{a}) \to \mathbb{C}^g/\Phi(\mathfrak{a}^*)$ is given by $x \mapsto \Phi(\xi) \cdot x$ for some purely imaginary element $\xi \in K$ i.e $\overline{\xi} = -\xi$, such that $\mathrm{Im}(\phi_i(\xi)) > 0$, for every $i \in \{1, \ldots, g\}$.

The corresponding Riemann form of this polarization is given by $E_{\Phi,\xi}(\Phi(x), \Phi(y)) = \mathrm{Tr}(\xi\overline{x}y)$, for $x, y \in K$ and the polarization is principal if and only if $\lambda_{\mathcal{A}}(\Phi(\mathfrak{a})) = \Phi(\mathfrak{a}^*)$ i.e., if and only if $\xi\mathfrak{a} = \mathfrak{a}^*$.

Let $\mathcal{A}$ be a principally polarized abelian variety with CM by (K, Φ). If we fix a CM-type (K, Φ), the principally polarized abelian variety $\mathcal{A}$ is determined by the pair $(\mathfrak{a}, \xi)$ and the Shimura class group or polarized class group of $\mathcal{O}$, acts on such pairs.

Definition 2.4.2.10. For any order $\mathcal{O}$ in a CM-field K, denote by $I_{\mathcal{O}}$ the group consisting of all pairs $(\mathfrak{m}, \rho)$ satisfying $\mathfrak{m}\overline{\mathfrak{m}} = \rho\mathcal{O}$ where $\mathfrak{m}$ is an invertible fractional ideal of $\mathcal{O}$ and ρ a totally positive element of K_0, endowed with component-wise multiplication. Let $P_{\mathcal{O}}$ be its subgroup formed by pairs of the form $(\mu\mathcal{O}, \mu\bar{\mu})$ for $\mu \in K$. The quotient $I_{\mathcal{O}}/P_{\mathcal{O}}$ is called the polarized class group of $\mathcal{O}$. We denote it by $\mathfrak{C}(\mathcal{O})$.

For $(\mathfrak{m}, \rho) \in \mathfrak{C}(\mathcal{O})$ the pair $(\mathfrak{m}^{-1}\mathfrak{a}, \rho\xi)$ corresponds to a principally polarized abelian variety isogenous to $\mathcal{A}$.

Proposition 2.4.2.11. *[107, Section 17] The group $\mathfrak{C}(\mathcal{O})$ acts freely on the set of isomorphism classes of principally polarized abelian varieties having complex multiplication by $\mathcal{O}$ with type Φ.*

When $\mathcal{O} = \mathcal{O}_K$, the action is also transitive, Theorem 2.4.2.13.

The polarized class group $\mathfrak{C}(\mathcal{O})$ is related to $\mathrm{Pic}(\mathcal{O})$ via the following exact sequence

$$1 \to \mathcal{O}_0^+/\,\mathrm{norm}_{K/K_0}(\mathcal{O}^*) \xrightarrow{\mu\mapsto(\mathcal{O},\mu)} \mathfrak{C}(\mathcal{O}) \xrightarrow{(\mathfrak{m},\rho)\mapsto\mathfrak{m}} \mathrm{Pic}(\mathcal{O}) \xrightarrow{\mathrm{norm}_{K/K_0}} \mathrm{Cl}^+(\mathcal{O}_0)$$

with $\mathcal{O}_0^+ = \mathcal{O} \cap \mathcal{O}_{K_0}^+$ the group of totally positive units in $\mathcal{O}_0 = \mathcal{O} \cap \mathcal{O}_{K_0}$ and $\mathrm{Cl}^+(\mathcal{O}_0)$ the narrow class group *i.e* the group of fractional ideals modulo the group of principal ideals with totally positive generators.

We now focus on complex abelian varieties with CM by the maximal order $\mathcal{O}_K$ of a CM-field K. We denote by $\mathcal{A}(\Phi, \mathfrak{a}, \xi)$ the abelian variety corresponding to the triple $(\Phi, \mathfrak{a}, \xi)$.

Theorem 2.4.2.12. *[107] Suppose Φ is a CM-type of some CM-field K of degree $2g$. Then the following hold.*

1. *For any triple $(\Phi, \mathfrak{a}, \xi)$ as above, the pair $(\mathbb{C}^g/\Phi(\mathfrak{a}), E_{\Phi,\xi})$ defines a principally polarized abelian variety $\mathcal{A}(\Phi, \mathfrak{a}, \xi)$ with CM by $\mathcal{O}_K$ of type Φ.*
2. *Every principally polarized abelian variety over $\mathbb{C}$ with CM by $\mathcal{O}_K$ of type Φ is isomorphic to $\mathcal{A}(\Phi, \mathfrak{a}, \xi)$, for some triple $(\Phi, \mathfrak{a}, \xi)$.*
3. *The abelian variety $\mathcal{A}(\Phi, \mathfrak{a}, \xi)$ is simple if and only if Φ is primitive. If this is the case, then the embedding $i : K \to \mathrm{End}(\mathcal{A}) \otimes \mathbb{Q}$ is an isomorphism.*
4. *For every pair of triples $(\Phi, \mathfrak{a}, \xi)$ and $(\Phi, \mathfrak{a}', \xi')$ with the same CM-type Φ, the principally polarized abelian varietis $\mathcal{A}(\Phi, \mathfrak{a}, \xi)$ and $\mathcal{A}(\Phi, \mathfrak{a}', \xi')$ are isomorphic if there exists $\gamma \in K^*$ such that*
   - *$\mathfrak{a}' = \gamma\mathfrak{a}$ and*
   - *$\xi' = (\gamma\overline{\gamma})^{-1}\xi$.*

   If Φ is primitive, then the converse holds.

Theorem 2.4.2.13. *[107, Section 14] Let K be a CM-field with CM-type Φ. The polarized class group $\mathfrak{C}(\mathcal{O}_K)$ acts freely and transitively on the set of isomorphism classes of principally polarized complex abelian varieties having complex multiplication by $\mathcal{O}_K$ with type Φ.*

In the case of an elliptic curve, the endomorphism ring does not need to be maximal for the action to be transitive.

Theorem 2.4.2.14. *[28, Chapter 13] Let $\mathcal{O}$ be an imaginary quadratic order in a number field K and Φ a CM-type. The Picard group $\mathrm{Pic}(\mathcal{O})$ acts freely and transitively on the set of isomorphism classes of complex elliptic curves with complex multiplication by $\mathcal{O}$ with type Φ.*

We finish this section by stating the main theorem of complex multiplication.

Let $\mathcal{A}$ be a complex principally polarized abelian variety with CM by $\mathcal{O}_K$ with CM-type Φ. The abelian variety can be defined over the Hilbert class field $\mathcal{H}_{K^r}$ of the reflex field K^r of K.

Theorem 2.4.2.15. *[107, Sections 15.3 and 16.3] Invertible ideals of K^r act on polarized complex abelian varieties with complex multiplication by $\mathcal{O}_K$ via*

$$\mathfrak{m} \in I_K^r : \mathcal{A}(\Phi, \mathfrak{a}, \xi) \mapsto \mathcal{A}(\Phi, N_{\Phi^r}(\mathfrak{m})^{-1}\mathfrak{a}, \mathrm{norm}_{K^r/\mathbb{Q}}(\mathfrak{m})\xi).$$

An ideal $\mathfrak{m}$ acts trivially when its reflex type norm $N_{\Phi^r}(\mathfrak{m})$ is a principal ideal of $\mathcal{O}_K$ and is generated by a nonzero element μ which satisfies $\mu\overline{\mu} = \mathrm{norm}_{K^r/\mathbb{Q}}(\mathfrak{m})$.

The action can be seen as of the action Galois group of $\mathcal{H}_{K^r}$ via the Artin map and it can be used to describe abelian extensions of K^r, see [112, Chapter 1, Section 9 and 10].

2.5 Abelian varieties over finite fields

Our primary interest in this thesis are abelian varieties defined over finite fields. The results we state in this section can be found in [45, 105, 117, 122, 123].

Let $\mathcal{A}$ be an abelian variety defined over $\mathbb{F}_q$. We define the Frobenius endomorphism $\pi_{\mathcal{A}}$ of $\mathcal{A}$ as the map that raises coordinates of points of $\mathcal{A}(\overline{\mathbb{F}}_q)$ to the q^{th} power.

Definition 2.5.1. Let q be a prime power. A q-Weil number π is an algebraic integer such that for every embedding $\phi : \mathbb{Q}(\pi) \to \mathbb{C}$, we have $|\phi(\pi)| = \sqrt{q}$. We say that two q-Weil numbers π and π' are conjugate if the minimal polynomials of π and π' are the same. A polynomial that is the characteristic polynomial of a q-Weil number is called a q-Weil polynomial.

Theorem 2.5.2. *If $\mathcal{A}$ is a simple abelian variety over $\mathbb{F}_q$, then the Frobenius endomorphism $\pi_{\mathcal{A}}$ is a q-Weil number.*

Let $\mathcal{A}$ be an abelian variety over $\mathbb{F}_q$. The zeta function of $\mathcal{A}$ is defined as

$$\zeta_{\mathcal{A}}(t) = \exp\left(\sum_{m\geq 1} \#\mathcal{A}\left(\mathbb{F}_{q^m}\right)\frac{t^m}{m}\right)$$

The following was proved by Weil in [124]:

Theorem 2.5.3. *The zeta function of a g-dimensional abelian variety $\mathcal{A}$ can be written as*

$$\zeta_{\mathcal{A}}(t) = \frac{P_1(t)P_3(t)\cdots P_{2g-1}(t)}{P_0(t)P_2(t)\cdots P_{2g}(t)}$$

for some $P_i(t) \in \mathbb{Z}[t]$ whose complex zeros have absolute value $q^{-i/2}$.

The Frobenius endomorphism $\pi_{\mathcal{A}}$ of a g-dimensional abelian variety admits a characteristic polynomial $\chi_{\mathcal{A}}$ that we call the characteristic polynomial of $\pi_{\mathcal{A}}$ or simply the characteristic polynomial of $\mathcal{A}$. $\chi_{\mathcal{A}}(t) \in \mathbb{Z}[t]$ and it has degree $2g$.

Corollary 2.5.4. *The complex roots of $\chi_{\mathcal{A}}$ all have absolute value $\sqrt{q}$ and the polynomial P_{2g} in the zeta function is $\prod(1-\alpha t)$ where α ranges over of $2g$ distinct such roots.*

From Honda-Tate theory we have the following:

Theorem 2.5.5. *[117, Theorem 1] Let $\mathcal{A}$ and $\mathcal{B}$ be two abelain varieties over $\mathbb{F}_q$, with characteristic polynomials $\chi_{\mathcal{A}}$ and $\chi_{\mathcal{B}}$, respectively. The following are equivalent:*

- *$\mathcal{A}$ is $\mathbb{F}_q$-isogenous to $\mathcal{B}$*
- *$\chi_{\mathcal{A}} = \chi_{\mathcal{B}}$*
- *$\mathcal{A}$ and $\mathcal{B}$ have the same number of points over $\mathbb{F}_{q^m}$, for every $m > 0$.*

In addition, $\mathcal{B}$ is $\mathbb{F}_q$ isogenous to a subvariety of $\mathcal{A}$ if and only if $\chi_{\mathcal{B}}$ divides $\chi_{\mathcal{A}}$.

From Theorem 2.5.5 we can see that if $\mathcal{A}$ is simple then its characteristic polynomial $\chi_{\mathcal{A}}$ is irreducible. We can define the following map

$$\{\text{Isogeny classes of simple AV over } \mathbb{F}_q\} \to \{\text{Conjugacy classes of } q\text{-Weil numbers}\}$$
$$\mathcal{A} \mapsto \pi_{\mathcal{A}}$$

Theorem 2.5.6. *(Honda-Tate) The map defined above is a bijection between the isogeny classes of simple abelian varieties over $\mathbb{F}_q$ and conjugacy classes of q-Weil numbers.*

Theorem 2.5.7. *If $\mathcal{A}$ is a simple abelian variety of dimension g, the characteristic polynomial of its Frobenius endomorphism π is some power m^e of its minimal polynomial, where $\mathbb{Q} \otimes \mathrm{End}(\mathcal{A})$ is a division algebra of dimension $2eg$, and its center K is the field $\mathbb{Q}(\pi) \cong \mathbb{Q}[x]/(m(x))$ of degree $2g/e$.*

Theorem 2.5.8. *A simple abelian variety $\mathcal{A}$ defined over a finite field $\mathbb{F}_q$ is ordinary if* $\mathrm{End}(\mathcal{A})$ *is an order in a CM-field K of degree $2g$, with g the dimension of $\mathcal{A}$.*

If an elliptic curve over $\mathbb{F}_q$ is not ordinary, it is supersingular and its endomorphism ring is not commutative, it is an order in a quanternion algebra of dimension 4.

Unlike abelian varieties defined over number fields for which complex multiplication is a rare situation, abelian varieties over finite fields always have complex multiplication. Most of the theory discussed in Section 2.4.2 descends to abelian varieties over finite fields.

Let $\mathcal{A}$ be an ordinary abelian variety defined over $\mathbb{F}_q$. From the theory of Serre and Tate [105], $\mathcal{A}$ lifts to a complex abelian variety $\tilde{\mathcal{A}}$ with the same endomorphism ring as $\mathcal{A}$. Moreover, from [45, Section 3], the polarizations also lift properly, and in particular $\mathcal{A}$ is principally polarizable if and only if $\tilde{\mathcal{A}}$ is.

Theorem 2.5.9. *Let $\mathcal{O}$ be an imaginary quadratic order. For elliptic curves defined over a finite field $\mathbb{F}_q$, the Picard group* $\mathrm{Pic}(\mathcal{O})$ *acts freely and transitively on the set of isomorphism classes of elliptic curves defined over $\mathbb{F}_q$ with endomorphism ring $\mathcal{O}$.*

For simple and ordinary abelian varieties we have:

Theorem 2.5.10. *Let $\mathcal{A}$ be a simple ordinary abelian variety defined over a finite field $\mathbb{F}_q$, let π be its Frobenius endomorphism, let $K = \mathbb{Q}(\pi)$, and let $\mathcal{O} \subset K$ be its endomorphism ring. The invertible ideals $\mathfrak{a}$ of norm coprime to the discriminant of $\mathbb{Z}[\pi, \overline{\pi}]$ act on the set of isomorphism classes of abelian varieties isogenous to $\mathcal{A}$ with endomorphism ring $\mathcal{O}$ as isogenies of degree their norm, and this defines a free action of* $\mathrm{Pic}(\mathcal{O})$ *on the set of isomorphism classes of abelian varieties isogenous to $\mathcal{A}$ with endomorphism ring $\mathcal{O}$.*

When polarization is considered, we have:

Theorem 2.5.11. *Let $\mathcal{A}$ be a principally polarized, absolutely simple and ordinary abelian variety defined over a finite field $\mathbb{F}_q$, let π be its Frobenius endomorphism, let $K = \mathbb{Q}(\pi)$, and let $\mathcal{O} \subset K$ be its endomorphism ring. The polarized class group $\mathfrak{C}(\mathcal{O})$ acts freely on the set of isomorphism classes of abelian varieties isogenous to $\mathcal{A}$ (as principally polarized abelian varieties) with endomorphism ring $\mathcal{O}$.*

We end this chapter with some important results of Waterhouse, [122].

Proposition 2.5.12. *Endomorphism rings of ordinary abelian varieties defined over finite base fields are unaffected by base field extensions.*

Proposition 2.5.13. *Let K be the CM-field of some ordinary abelian variety $\mathcal{A}$ defined over $\mathbb{F}_q$. The orders of K containing $\mathbb{Z}[\pi_{\mathcal{A}}, \overline{\pi}_{\mathcal{A}}]$ are exactly those that arise as endomorphism rings of abelian varieties defined over $\mathbb{F}_q$ with complex multiplication by K.*

Proposition 2.5.14. *Let K be the CM-field of some principally polarized ordinary abelian variety $\mathcal{A}$ defined over $\mathbb{F}_q$. The orders of K containing $\mathbb{Z}[\pi_{\mathcal{A}}, \overline{\pi}_{\mathcal{A}}]$ that are stable under complex conjugation are exactly those that arise as endomorphism rings of principally polarized abelian varieties defined over $\mathbb{F}_q$ with complex multiplication by K.*

Chapter 3

Computation of Endomorphism Rings of Elliptic Curves

In this chapter we study the computation of endomorphism rings of ordinary elliptic curves defined over finite fields. We describe the exponential method developed by Kohel [72] and subexponential methods by Bisson and Sutherland [12, 17]. We present a novel approach which improves existing subexponential methods and it is also fast in practice.

3.1 Background

The computation of endomorphism rings of elliptic curves over finite fields started with the work of Kohel, [72]. Since then, it gained popularity and is now a fundamental problem in computational number theory and in cryptography. The computation of the endomorphism rings of supersingular elliptic curves play a central role in Post-Quantum cryptography via the Supersingular Isogeny Diffie–Hellman key exchange (SIDH), [47, 48]. Computation of endomorphism rings of ordinary elliptic curves also has many applications including in explicit class field theory and pairing-based cryptosystems [4] as well as in Elliptic-Curve Diffie–Hellman Key exchange (ECDH), [102].

For a supersingular elliptic curve $\mathcal{E}/\mathbb{F}_q$, the best known algorithm to compute its endomorphism ring has an exponential runtime in $\log q$, [48]. When $\mathcal{E}$ is ordinary, subexponential methods have been developed. They first appeared in the work of Bisson and Sutherland, [17] and it was achieved by making some assumptions including the Generalized Riemann Hypothesis (GRH). The method was improved in [12], in which all the

assumptions except for the Generalized Riemann Hypothesis were removed and it also has a better asymptotic complexity. Both methods output an order that is isomorphic to the endomorphism ring but with a known probability of failure. To unconditionally verify the output, a certification method is used. The subexponential methods have been extended to ordinary abelian surfaces (abelian varieties of dimension two) [14, 53, 110]. We present an improvement of the method in [12] for which the output is unconditionally correct and so the certification is not needed. The method is also faster in practice.

3.2 Exponential method

In this section we give an overview of the exponential method of Kohel to compute the endomorphism rings of ordinary elliptic curves defined over finite fields.

3.2.1 Isogeny volcanoes

Isogenies play a central role in the algorithm of Kohel via the now known isogeny volcanoes. Before delving into isogeny volcanoes, we introduce the more general notion of ℓ-volcano.

Definition 3.2.1.1. Let ℓ be a prime number. An ℓ-volcano V is a connected undirected graph whose vertices are partitioned into one or more levels $V_0, \ldots, V_d$ such that the following hold:

1. The subgraph on V_0 (the surface) is a regular graph of degree at most 2.
2. For $i > 0$, each vertex in V_i has exactly one neighbor in level V_{i-1}, and this accounts for every edge not on the surface.
3. For $i < d$, each vertex in V_i has degree $\ell + 1$.

We call the integer d the depth of the volcano. Figure 3.1 is the picture of an 3-volcano of depth 2.

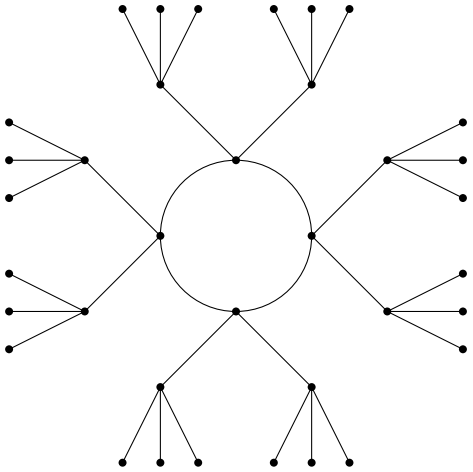

FIGURE 3.1: A 3-volcano of depth 2

ℓ-volcanoes arise naturally in the context of graphs of isogenies between ordinary elliptic curves over finite fields.

Definition 3.2.1.2. Let ℓ be a prime number and $\varphi : \mathcal{E} \to \mathcal{E}'$ be isogenous elliptic curves. We say that $\mathcal{E}$ and $\mathcal{E}'$ are ℓ-isogenous or that φ is an ℓ-isogeny if the degree of φ is ℓ.

Let $\mathcal{E}$ be an elliptic curve defined over some field k and ℓ a prime number. If ℓ is different from the characteristic of k, then by Theorem 2.2.2.2, $\mathcal{E}[\ell]$ is isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^2$. Thus, there are $\ell+1$ subgroups of order ℓ in $\mathcal{E}[\ell]$. Since each finite subgroup of $\mathcal{E}(\overline{k})$ is the kernel of a uniquely determined separable isogeny (up to isomorphism) [109, Prop. III.4.12], the $\ell + 1$ subgroups correspond to separable ℓ-isogenies. As stated in Proposition 2.2.2.4, any ℓ-isogeny φ has a dual $\hat{\varphi}$ and $\varphi \circ \hat{\varphi} = [\ell]$, and so the kernel of φ is a subgroup of $\ker[\ell] = \mathcal{E}[\ell]$. This shows that any ℓ-isogeny from $\mathcal{E}$ arises from one of the $\ell+1$ subgroups of $\mathcal{E}[\ell]$.

It is worth mentioning that not all of the $\ell + 1$ isogenies from $\mathcal{E}$ are necessarily defined over k. The Galois group $G := \mathrm{Gal}(k(\mathcal{E}[\ell])/k)$, where $k(\mathcal{E}[\ell])$ is the finite field extension of k which contains the coordinates of elements of $\mathcal{E}[\ell]$, acts linearly on $\mathcal{E}[\ell]$. An ℓ-isogeny φ is defined over k if the kernel is invariant under the action of G. If G fixes more than two subgroups of order ℓ in $\mathcal{E}[\ell]$, then it fixes all of the $\ell+1$ subgroups. This leads to the following:

Lemma 3.2.1.3. *Let $\mathcal{E}/k$ be an elliptic curve with $j(E) \neq 0, 1728$ and let ℓ be a prime different from the characteristic of k. Up to isomorphism, the number of k-rational ℓ-isogenies from $\mathcal{E}$ is $0, 1, 2,$ or $\ell + 1$.*

Definition 3.2.1.4. An isogeny f between abelian varieties $\mathcal{A}$ and $\mathcal{B}$ is said to be horizontal if $\mathrm{End}(\mathcal{A})$ is isomorphic to $\mathrm{End}(\mathcal{B})$. In that case we say that $\mathcal{B}$ is horizontally isogenous to $\mathcal{A}$. If it is not horizontal, it is called vertical.

Theorem 3.2.1.5. *[13, Corollary V.1.1] The possible degrees of vertical isogenies of prime degree in a given isogeny class of ordinary elliptic curves are the prime divisors of the index $[\mathcal{O}_K : \mathbb{Z}[\pi]]$.*

Definition 3.2.1.6. For a field k and a prime ℓ different from the characteristic of k, the k-rational ℓ-isogeny graph $G_\ell(k)$, is defined as having all isomorphism classes of the elliptic curves defined over k as its vertices, and having a directed edge $(\mathcal{E}_1, \mathcal{E}_2)$ for each k-rational ℓ-isogeny from $\mathcal{E}_1$ to $\mathcal{E}_2$.

The graph $G_\ell(k)$ is a directed graph and if two elliptic curves $\mathcal{E}_1$ and $\mathcal{E}_2$ have their j-invariant different from 0 and 1728, there are exactly as many edges $(\mathcal{E}_1, \mathcal{E}_2)$ as $(\mathcal{E}_2, \mathcal{E}_1)$, by taking the dual. However for $j = 0$ and $j = 1728$ that is not the case.

If $k = \mathbb{F}_q$ is a finite field, then $G_\ell(k)$ is a finite graph that is the disjoint union of ordinary connected components and one supersingular connected component. For the ordinary components we have the following:

Theorem 3.2.1.7. *Let V be an ordinary component of $G_\ell(\mathbb{F}_q)$ that does not contain 0 or 1728. Then V is an ℓ-volcano for which the following hold:*

1. *The vertices in level V_i all have the same endomorphism ring $\mathcal{O}_i$.*
2. *The subgraph on V_0 has degree $1 + \left(\frac{D_0}{\ell}\right)$, where D_0 is the discriminant of $\mathcal{O}_0$.*
3. *If $\left(\frac{D_0}{\ell}\right) \geq 0$, then $|V_0|$ is the order $[\mathfrak{l}]$ in $\mathrm{Pic}(\mathcal{O}_0)$; otherwise $|V_0| = 1$.*
4. *The depth of V is $d = \mathrm{val}_\ell\left(\left(t^2 - 4q\right)/D_0\right)/2$, where t it the trace of any $\mathcal{E}$, with $j(\mathcal{E}) \in V$.*
5. *$\ell \nmid [\mathcal{O}_K : \mathcal{O}_0]$ and $[\mathcal{O}_i : \mathcal{O}_{i+1}] = \ell$ for $0 \leq i < d$.*

Proof. Follows from [72, Proposition 23]. □

Definition 3.2.1.8. For an integer a, we define and denote the valuation of a at a prime number p by

$$v_p(a) = \max\{e \in \mathbb{Z} \mid p^e \text{ divides } a\}.$$

If we restrict the set of vertices to elliptic curves with complex multiplication by a given imaginary quadratic field we obtain the following result.

Theorem 3.2.1.9. *[72, Proposition 23] Consider the graph of isogenies of prime degree ℓ between isomorphism classes of elliptic curves defined over a finite field with complex multiplication by the imaginary quadratic field $K = \mathbb{Q}(\sqrt{D})$ of discriminant D, and denote by v the valuation of $[\mathcal{O}_K : \mathbb{Z}[\pi]]$ at ℓ. The following exhaustively describe all edges of this graph.*

1. *From a curve $\mathcal{E}$ at depth $u > 0$, i.e. the valuation of $[\mathcal{O}_K : \mathrm{End}(\mathcal{E})]$ at ℓ is u, there is one isogeny going up to a curve at depth $u - 1$.*
2. *From a curve at depth $u < v$, there are ℓ isogenies going down to ℓ curves at depth $u + 1$, unless $u = 0$ in which case there are $\ell - 1$, ℓ or $\ell + 1$ when $D$is respectively a square, zero, or a non-square modulo ℓ.*
3. *From a curve at depth 0, there are two isogenies going to curves at depth 0 when D is a square modulo ℓ, and one when D is divisible by ℓ.*

This theorem is central in the algorithm of Kohel.

3.2.2 Kohel's Algorithm

The result above can be used to determine the endomorphism of ordinary elliptic curves defined over finite fields. Let $\mathcal{E}/\mathbb{F}_q$ be an ordinary elliptic curve with Frobenius endomorphism π. The trace of π can be efficiently computed, using the Schoof-Elkies-Atkin algorithm, [33, 61, 104]. Let $\chi_{\mathcal{E}}$ be the characteristic polynomial of π. If we fix an isomorphism between the endomorphism algebra $\mathbb{Q}(\pi)$ and the number field $K := \mathbb{Q}[x]/(\chi_{\mathcal{E}})$, it is a classical result that the endomorphism ring of $\mathcal{E}$ contains the order $\mathbb{Z}[\pi]$. Since we are working with imaginary quadratic number fields, orders are uniquely identified by their indices in the maximal order, those indices are also known as conductors. So, computing the endomorphism ring of an ordinary elliptic curve amounts to finding its index in the maximal order $\mathcal{O}_K$. The index of $\mathbb{Z}[\pi]$ in $\mathcal{O}_K$, except for possible factors of 2, is the square part of $4q - t_\pi$, where t_π is the trace of π.

Let $v = [\mathcal{O}_K : \mathbb{Z}[\pi]]$ with $v = \ell_1^{e_1} \dots \ell_r^{e_r}$ where the $\ell_i' s$ are prime numbers. The endomorphism ring has a conductor of the form $u = \ell_1^{d_1} \dots \ell_r^{d_r}$ with $e_i - d_i \geq 0$. The main idea of the exponential method in [72] is to determine the exponent d_i using the ℓ_i-isogeny graph and it works as follows:

We compute three different chains of degree ℓ_i-isogenies starting form $\mathcal{E}$ so that at least one chain descends to a higher level. This idea is due to Mireille Fouquet, [56, 57]. We eventually get to the floor i.e. a curve whose depth is the depth of the volcano. We then obtain chains of isogenies, and the chain that first hits the floor has length $f_i = e_i - d_i$, from which the exponent d_i can be deduced. In the next section, we will explain how to navigate the isogeny graph. We have the following algorithm:

Algorithm 1 `Endomorphism ring computation` [72]

Input: An elliptic curve $\mathcal{E}/\mathbb{F}_q$.

Output: The conductor of its endomorphism ring.

1: Count the points of $\mathcal{E}$ and deduce its complex multiplication field K.
2: For each prime ℓ dividing $[\mathcal{O}_K : \mathbb{Z}[\pi]]$:
3: Compute three curves ℓ-isogenous to $\mathcal{E}$.
4: Keep walking a chain with no back-tracking of ℓ-isogenies from each and denote by u_ℓ the length of the chain that ends first.
5: Return $[\mathcal{O}_K : \mathbb{Z}[\pi]] / \prod \ell^{u_\ell}$.

In Step 4, non-tracking means that the chain does not contain the duals of the isogenies already in the chain. Assuming GRH, Algorithm 1 can be improved. It relies on the complex multiplication theory. Let $\mathcal{E}/\mathbb{F}_q$ be an ordinary elliptic curve with endomorphism ring isomorphic to some order $\mathcal{O}$. From Theorem 2.5.9 there are exactly $|\operatorname{Pic}(\mathcal{O})|$ isomorphism classes of elliptic curves defined over $\mathbb{F}_q$ isogenous to $\mathcal{E}$ with endomorphism ring $\mathcal{O}$. Kohel used that fact to produce the following algorithm:

Algorithm 2 `Endomorphism ring computation` [72]

Input: An elliptic curve $\mathcal{E}/\mathbb{F}_q$.

Output: The conductor of its endomorphism ring.

1: Count the points of $\mathcal{E}$ and deduce its complex multiplication field K.
2: For each prime power factor $\ell^v \leq q^{1/6}$ of $[\mathcal{O}_K : \mathbb{Z}[\pi]]$:
3: Apply Algorithm 1
4: For each prime power factor $\ell^v \geq q^{1/6}$ of $[\mathcal{O}_K : \mathbb{Z}[\pi]]$:
5: Count the number n of curves having horizontal isogenies to $\mathcal{E}$.
6: Determine the order with class number n.

The GRH is assumed so that the Bach bound, Theorem 3.3.5.3, can be used in Step 5 and Step 6. The first step of Algorithm 1 and Algorithm 2 can be performed in polynomial time in $\log q$ by using the Schoof–Elkies–Atkin (SEA) algorithm. The main bottleneck in the two algorithms above is the computation of vertical ℓ-isogenies. We have the following:

Lemma 3.2.2.1. *[13, Lemma III.2.5] Let π be a q-Weil number with minimal polynomial of degree $2g$. The index $[\mathcal{O}_K : \mathbb{Z}[\pi, \overline{\pi}]]$ is bounded above by $2^{g(g-1)}q^{g^2/2}$ and $|\operatorname{disc}(\mathbb{Z}[\pi, \overline{\pi}])| < 4^{g(2g-1)}q^{g^2}$.*

If $\mathcal{E}/\mathbb{F}_q$ is an ordinary elliptic curve with Frobenius endomorphism π and CM by K, by Lemma 3.2.2.1, $[\mathcal{O}_K : \mathbb{Z}[\pi]]$ is bounded by $\sqrt{q}$ and so the prime divisors of $[\mathcal{O}_K : \mathbb{Z}[\pi]]$ can be exponential in $\log q$. This implies that in general, the exponential complexity in $\log q$ cannot be avoided in Algorithms 1 and 2. In fact, there are no known algorithms that compute vertical ℓ-isogenies with complexity not at least linear but in general quadratic in ℓ, [23, 35, 51]. The runtime of Algorithm 1 is bounded by $q^{1+o(1)}$.

In Algorithm 2, the runtime of all computations in Step 2 and 3 is at most $q^{1/3+o(1)}$. If GRH is assumed, the runtime of all steps after Step 3 is bounded by $q^{1/3+o(1)}$.

Theorem 3.2.2.2. *[72, Theorem 1] Under GRH, Algorithm 2 computes the endomorphism rings of ordinary elliptic curves in deterministic time $q^{1/3+o(1)}$.*

We now focus on the subexponential methods.

3.3 Subexponential methods

As mentioned earlier, the first subexponential algorithm for computing the endomorphism rings of ordinary elliptic curves defined over finite fields was developed by Bisson and Sutherland in [17]. This was achieved by assuming many heuristics, including, but not limited to the Generalized Riemann Hypothesis (GRH). Bisson subsequently improved the method in [12] by obtaining a better asymptotic complexity and removing all heuristics except GRH. In this section we present the approach in [12]; which we are going to refer to as the "Lattice Method". Our improvement in Section 3.4 is based on it. It can also be extended to abelian surfaces which we will study in Chapter 4.

3.3.1 Overview of the method

We give an overview of the lattice method for ordinary elliptic curves.

Let $\mathcal{E}/\mathbb{F}_q$ be an ordinary elliptic curve with π its Frobenius endomorphism and $\chi_\mathcal{E}$ the characteristic polynomial of π. The characteristic polynomial $\chi_\mathcal{E}$ is of the form $\chi_\mathcal{E} = x^2 - tx + q$, where t is the trace of π. By Theorem 2.5.8, the endomorphism algebra $\mathbb{Q} \otimes \mathrm{End}(\mathcal{E})$ is isomorphic to the imaginary quadratic number field $K = \mathbb{Q}[x]/(\chi_\mathcal{E}(x))$. We fix an isomorphism and consider $\mathrm{End}(\mathcal{E})$ as an order in $\mathcal{O}_K$, the maximal order of K. From Proposition 2.5.14, the endomorphism ring always contains the order $\mathbb{Z}[\pi, \overline{\pi}] = \mathbb{Z}[\pi]$ and any order $\mathcal{O}$ satisfying $\mathbb{Z}[\pi] \subseteq \mathcal{O} \subseteq \mathcal{O}_K$ is the endomorphism ring of an elliptic curve isogenous to $\mathcal{E}$. Hence the endomorphism ring satisfies $\mathbb{Z}[\pi] \subseteq \mathrm{End}(\mathcal{E}) \subseteq \mathcal{O}_K$.

The general approach to computing endomorphism ring in subexponential is to use the theory of complex multiplication to identify which order $\mathcal{O}$, satisfying $\mathbb{Z}[\pi] \subseteq \mathcal{O} \subseteq \mathcal{O}_K$, corresponds to the endomorphism ring. One way to identify the endomorphism ring would be to check each order until we get the endomorphism ring. This would lead to an exponential runtime since in general, we have an exponential number of such orders (exponential in $\log q$). To effectively identify the endomorphism ring, it can be observed that the set of all those orders, under subset inclusion, form a lattice and this gives rise to an efficient way to find $\mathrm{End}(\mathcal{E})$. This lattice has a mininal order which is $\mathbb{Z}[\pi]$ and a maximal one, $\mathcal{O}_K$.

The method works as follows: we start with the order $\mathbb{Z}[\pi]$ and check whether it contains a minimal overorder, see Definition 3.3.1.1, which is contained in the endomorphism ring.

If such order exists, the order $\mathbb{Z}[\pi]$ is replaced by that order and the process is reiterated until we get an order $\mathcal{O}$ that is not contained in any order which is contained in the endomorphism ring.

The following figure, taken from [13, Figure 5], shows how we can compute the endomorphism ring using the lattice method.

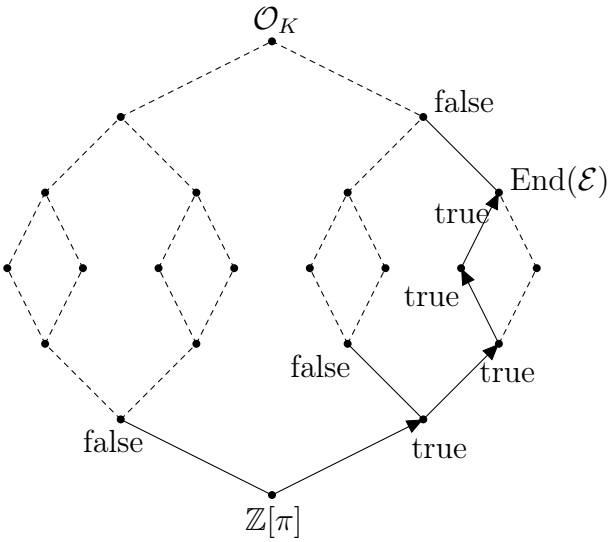

FIGURE 3.2: Lattice method.

The following algorithm tests at most polynomially many orders before finding End($\mathcal{E}$).

Algorithm 3 `Computation of endomorphism ring [12, Algorithm 5.1]`

Input: An elliptic curve $\mathcal{E}/\mathbb{F}_q$.

Output: An order isomorphic to the endomorphism ring of $\mathcal{E}$.

1: Compute the Frobenius polynomial $\chi_{\mathcal{E}}$ of $\mathcal{E}$ and construct the order $\mathcal{O}' = \mathbb{Z}[\pi]$.

2: For minimal overorders $\mathcal{O}$ of $\mathcal{O}'$:

3: If $\mathcal{O} \subset \text{End}(\mathcal{E})$, set $\mathcal{O}' \leftarrow \mathcal{O}$ and go to Step 2.

4: Return $\mathcal{O}'$

Definition 3.3.1.1. Let K be a number field and $\mathcal{O}, \mathcal{O}'$ be orders in K. The order $\mathcal{O}$ is said to be an overorder of $\mathcal{O}'$ if $\mathcal{O}' \subsetneq \mathcal{O}$. It is a minimal overorder if it is an overorder and there is no $\mathcal{O}'' \subset \mathcal{O}_K$ such that $\mathcal{O}' \subsetneq \mathcal{O}'' \subsetneq \mathcal{O}$.

Assuming GRH, Algorithm 3 returns the structure of the endomorphism ring of an elliptic curve defined over $\mathbb{F}_q$ in probabilistic time $L(q)^{1+o(1)} + L(q)^{1/\sqrt{2}+o(1)}$, where $L(x) = e^{\sqrt{\log(x)\log\log(x)}}$. We provide a detailed analysis of the algorithm in Section 3.3.5.

3.3.2 Complex multiplication action

In Algorithm 3, Step 3 is important and checking whether an order $\mathcal{O}$ is contained in $\mathrm{End}(\mathcal{E})$ is not straightforward; we do not even know $\mathrm{End}(\mathcal{E})$. In order to achieve this; we rely on the theory of complex multiplication, which gives us a link between isogenies and endomorphism rings that we can exploit.

Let $\mathcal{E}/\mathbb{F}_q$ be an ordinary elliptic curve with Frobenius endomorphism π. Theorem 3.3.2.1 below is the result from complex multiplication that is relevant in computing $\mathrm{End}(\mathcal{E})$.

Theorem 3.3.2.1. *[28, Chapter 13] For any ideal $\mathfrak{a}$ of $\mathrm{End}(\mathcal{E})$, denote by $\varphi_\mathfrak{a}$ the isogeny with kernel $\cap_{\alpha\in\mathfrak{a}} \ker\alpha$. The Picard group $\mathrm{Pic}(\mathrm{End}(\mathcal{E}))$ acts faithfully and transitively on the set of isomorphism classes of elliptic curves horizontally isogenous to $\mathcal{E}$ by $\mathfrak{a} : \mathcal{E} \mapsto \varphi_\mathfrak{a}(\mathcal{E})$.*

We use relations to check containment between two orders.

Definition 3.3.2.2. We define relations as multisets of ideals of $\mathbb{Z}[\pi]$. We say that a relation R holds in an order $\mathcal{O}$ (or that it is a relation of $\mathcal{O}$) if the product $\prod_{\mathfrak{a}\in R} \mathfrak{a}\mathcal{O}$ is trivial in $\mathrm{Pic}(\mathcal{O})$.

By Theorem 3.3.2.1, a relation R holds in $\mathrm{End}\,(\mathcal{E})$ if and only if the image of the composition of the isogenies $\varphi_{\mathfrak{a}\,\mathrm{End}(\mathcal{E})}$, for $\mathfrak{a} \in R$, is isomorphic to $\mathcal{E}$. Isogenies corresponding to ideals of the form $\mathfrak{a}\,\mathrm{End}(\mathcal{E})$, $\mathfrak{a} \in R$, can be computed with Algorithm 7 and the isogenies are used to check if R holds in $\mathrm{End}(\mathcal{E})$ or not. We denote by $\Lambda_\mathcal{O}$ all relations holding in an order $\mathcal{O} \supseteq \mathbb{Z}[\pi]$.

Lemma 3.3.2.3. *[40, Chapter 7] If a relation holds in some order, it holds in all orders containing it.*

The converse of Lemma 3.3.2.3 is not always true. In fact, we can have two orders $\mathcal{O}$ and $\mathcal{O}'$ such that all relations in $\mathcal{O}$ also hold in $\mathcal{O}'$ but $\mathcal{O}$ is not contained in $\mathcal{O}'$. However we know exactly when that happens.

Proposition 3.3.2.4. *[12, Proposition 7.2] Let $\mathcal{O}$ and $\mathcal{O}'$ be orders in an imaginary quadratic field K. The lattice $\Lambda_{\mathcal{O}'}$ contains $\Lambda_{\mathcal{O}}$ if the order $\mathcal{O}'$ contains $\mathcal{O}$ or:*

1. *$K = \mathbb{Q}(\sqrt{-4})$ and $\mathcal{O}'$ has conductor 2;*
2. *$K = \mathbb{Q}(\sqrt{-3})$ and $\mathcal{O}'$ has conductor 2 or 3;*
3. *The prime 2 splits in K and $\mathcal{O}'$ has index 2 in some order above $\mathcal{O}$ of odd conductor.*

By Proposition 3.3.2.4, after checking that all relations in $\mathcal{O}$ are also relations in $\mathcal{O}'$, we need to check whether $\mathcal{O} \subseteq \mathcal{O}'$ locally at 2 and 3 before concluding that $\mathcal{O}$ is contained in $\mathcal{O}'$ or not. By check whether $\mathcal{O} \subseteq \mathcal{O}'$ locally at 2 and 3, we mean to check whether $\mathrm{val}_2([\mathcal{O}_K : \mathcal{O}'])$ less than $\mathrm{val}_2([\mathcal{O}_K : \mathcal{O}])$ and $\mathrm{val}_3[(\mathcal{O}_K : \mathcal{O}'])$ less than $\mathrm{val}_3([\mathcal{O}_K : \mathcal{O}])$.

In checking whether a relation holds in $\mathrm{End}\,(\mathcal{E})$, we have to be able to compute the corresponding isogenies efficiently. We need relations for which the cost of computing the isogenies is not too expensive.

3.3.3 Finding relations

By finding a relation we mean finding prime ideals and exponents such that their product is a principal ideal. Finding relations is an important task in the computation of the class group. We start this subsection by giving an outline of the class group computation and then we will present algorithms that compute relations for which computing the corresponding isogenies is efficient.

By Theorem 3.3.5.3, under GRH, for any imaginary quadratic order $\mathcal{O}$ of discriminant D, the Picard group $\mathrm{Pic}(\mathcal{O})$ can be generated by classes of ideals of prime norm and norm less than $N \geq 6\log^2|D|$. Let $\mathfrak{B}$ be a generating set of $\mathrm{Pic}(\mathcal{O})$. Then the map

$$\begin{aligned} \sigma_{\mathcal{O}} : \mathbb{Z}^{|\mathfrak{B}|} &\to \mathrm{Pic}(\mathcal{O}) \\ x &\mapsto \prod_{\mathfrak{p}\in\mathfrak{B}} [\mathfrak{p}]^{x_{\mathfrak{p}}}, \end{aligned}$$

where $[\mathfrak{p}]$ represents the class of $\mathfrak{p}$, is surjective and its kernel corresponds to the set of relations formed by prime ideals in $\mathfrak{B}$. We have that $\ker \sigma_{\mathcal{O}} = \Lambda_{\mathcal{O}}$ and

$$\mathrm{Pic}(\mathcal{O}) \cong \mathbb{Z}^{|\mathfrak{B}|}/\Lambda_{\mathcal{O}}.$$

We identify the ideal class $\sigma_{\mathcal{O}}(x) = \prod_{\mathfrak{p}\in\mathfrak{B}}[\mathfrak{p}]^{x_\mathfrak{p}}$ with the ideal $\prod_{\mathfrak{p}\in\mathfrak{B}}\mathfrak{p}^{x_\mathfrak{p}}$.

Once we have a set $\mathfrak{B}$, commonly called the factor base, computing the structure of the Picard group of $\mathcal{O}$ is essentially equivalent to computing enough elements in the kernel $\Lambda_{\mathcal{O}}$.

There are many ways to compute relations. An easy way would be to use a baby-step giant-step or Pollard's rho method, which would have exponential runtime. Subexponential algorithms for computing relations also exits and we are interested in those.

The subexponential method for computing relations for imaginary quadratic orders was first developed by Seysen in [106]. This led to a subexponential algorithm for computing the structure of Picard group of quadratic number fields in [64]. In both cases, the GRH had to be assumed to achieve subexponential complexity. A generalization to high degree number fields was done by Buchmann, [25], however more heuristics had to be assumed in addition to GRH. There have been many theoretical and practical improvements to Buchmann's algorithm; all of them rely on an index calculus strategy (i.e. make use of a factor base and relations between elements in the factor base) and have subexponential complexity.

The following algorithm returns a relation of an imaginary quadratic order in subexponential time, given a factor base.

Algorithm 4 `Finding relation [13, Algorithm VI.2.3]`

Input: An order imaginary order $\mathcal{O}$ and a factor base $\mathfrak{B}$.

Output: A relation i.e an element in $\ker \sigma_{\mathcal{O}}$.

1: Take a random element $x \in \mathfrak{B}$ and compute $\mathfrak{a} = \sigma_{\mathcal{O}}(x)$.
2: Reduce $\mathfrak{a}$ to an equivalent but smaller ideal $\mathfrak{b}$.
3: If possible, find a preimage $y \in \sigma_{\mathcal{O}}^{-1}(\mathfrak{b})$ and return $x - y$.
4: Return to Step 1.

The relations obtained from Algorithm 4 are formed by prime ideals of bounded norms. However their exponents are not bounded. In the context of endomorphism ring computation, we want to be able to compute isogenies corresponding to those relations. In fact if $n \in \Lambda_{\mathcal{O}}$, the associated isogeny chain contains at most $\|n\|_1 = \sum |n_p|$ isogenies of degree at most N, the bound on the size of the factor base $\mathfrak{B}$. In order to control the cost of isogeny computation, we need relations whose exponents are small. Hence the relations we are interested in should be formed by prime ideals of bounded norms and their exponents should also be bounded.

In addition to relations with small norms and small exponents, the relations had to behave as random relations for Bisson's method to work. However, we do not need that condition in the appraoch presented in Section 3.4.

We present results that show that for imaginary quadratic orders, all those conditions above are satisfied provided that we assume GRH.

Theorem 3.3.1. *[34, Theorem 5] Under GRH, for all $\varepsilon > 0$ there exists some $c > 1$ such that the following holds. Let $\mathcal{O}$ be an imaginary quadratic order. Denote by D its discriminant, and let N and l be integers verifying*

$$N \geq \log^{2+\varepsilon} |D| \quad \text{and} \quad l \geq c\frac{\log |D|}{\log\log |D|}.$$

If n is drawn uniformly at random from the set of vectors of $\mathbb{Z}^{|\mathfrak{B}|}$ with norm $\|n\|_1 = l$, the probability that the ideal $\sigma_{\mathcal{O}}(n)$ falls in any subset S of $\mathrm{Pic}(\mathcal{O})$ is at least $\frac{|S|}{2 \times |\mathrm{Pic}(\mathcal{O})|}$, where $|S|$ and $|\mathrm{Pic}(\mathcal{O})|$ represent the cardinality of S and $\mathrm{Pic}(\mathcal{O})$ respectively.

As a corollary we have:

Corollary 3.3.2. *[12, Corollary 6.2] Under GRH, for $N = log^{2+\varepsilon}|D|$ the diameter of $\Lambda_{\mathcal{O}}$ is $o(\log^{4+\varepsilon} |D|)$*

The following algorithm computes relations whose associated isogeny can be efficiently computed.

Algorithm 5 `Finding relation [12, Algorithm 6.3]`

Input: An imaginary quadratic order $\mathcal{O}$ of discriminant D and some $\gamma > 0$.

Output: A quasi-random relation $n \in \Lambda_{\mathcal{O}}$ with $\|n\|_1 = o(\log^{6+\varepsilon} |D|)$.

1: Form the set $\mathfrak{B}$ of primes $\mathfrak{p}$ of $\mathcal{O}$ with norm less than $N = L(q)^{\gamma}$.
2: Draw uniform at random a vector $x \in \mathbb{Z}^{|\mathfrak{B}|}$ with coordinates $|x_{\mathfrak{p}}| < \log^{4+\varepsilon} |D|$ if $\mathrm{norm}(\mathfrak{p}) < \log^{2+\varepsilon} |D|$, else $x_{\mathfrak{p}} = 0$.
3: Compute the reduced ideal representative $\mathfrak{a}$ of $\sigma_{\mathcal{O}}(x)$.
4: If $\mathfrak{a}$ factors over $\mathfrak{B}$ as $\prod \mathfrak{p}^{y_{\mathfrak{p}}}$ then return the vector $z = x - y$, otherwise, go back to Step 2.

The reason why random relations are needed is because the relations are used to characterize the orders and in case they are not random, the probability of failure in [12, Theorem 5.3] is higher. We have

Lemma 3.3.3. *[12, Lemma 6.5] Under GRH, take any two orders $\mathcal{O}$ and $\mathcal{O}'$; a relation of $\mathcal{O}$ generated by Algorithm 5 has a probability $[\Lambda_{\mathcal{O}} : \Lambda_{\mathcal{O}} \cap \Lambda_{\mathcal{O}'}]^{-1} + o(1)$ of holding in $\mathcal{O}'$.*

The relations output by Algorithm 5 are of the form $\prod \mathfrak{p}^{z_{\mathfrak{p}}}$, with $\|z\|_1$ less than $O(\log |D|)$ and we call them short relations. There is another algorithm, [34, Algorithm 1], that also computes short relations. It can be considered as a generalization of Algorithm 5. This will be particularly important in our alternative method in Section 3.4.

The following algorithm computes a smooth representative of an ideal class $[\mathfrak{b}]$.

Algorithm 6 `Finding relation [34, Algorithm 1]`

Input: An imaginary order $\mathcal{O}$ of discriminant D, $\gamma > 0$, $[\mathfrak{b}]$ an ideal class and an integer t satisfying $C\dfrac{\log h_D}{\log(\log(|D|))} < t < C\log(|D|)$

Output: A relation vector $z \in \mathbb{Z}^{|\mathfrak{B}|}$ such that $[\mathfrak{b}] = \prod_{\mathfrak{p}\in\mathfrak{B}} [\mathfrak{p}]^{z_{\mathfrak{p}}}$ or nil.

1: Compute a factor base consisting of split primes to obtain a factor base $\mathfrak{B}$ of primes with norm less than $N = L(q)^{\gamma}$.
2: Set $\mathcal{S} \leftarrow \emptyset$, $\mathcal{P} \leftarrow \{\text{norm}(\mathfrak{p}) : \mathfrak{p} \in \mathfrak{B}\}$.
3: Set $\ell \leftarrow L(\frac{1}{4\gamma})$.
4: For $i = 0$ to ℓ do
5: Select $v \in \mathbb{Z}^{|\mathfrak{B}|}_{0\ldots|D|-1}$ uniformly at random subject to the condition that $\|v\|_1 = t$.
6: Calculate the reduced ideal $\mathfrak{a}_v$ in the ideal class $[\mathfrak{b}] \cdot \left[\prod_{\mathfrak{p}\in\mathfrak{B}} \mathfrak{p}^{v_{\mathfrak{p}}}\right]$
7: Set $\mathcal{S} \leftarrow \mathcal{S} \cup \text{norm}(\mathfrak{a}_v)$.
8: Using Bernstein's algorithm [5], find a $\mathcal{P}$-smooth element such that $\text{norm}(\mathfrak{a}_v) \in \mathcal{S}$ (if one exists), or else return nil.
9: Find the prime factorization of the integer $\text{norm}(\mathfrak{a}_v)$.
10: Using Theorem 3.1 of Seysen [106] on the prime factorization of $\text{norm}(\mathfrak{a}_v)$, factor the ideal $\mathfrak{a}_v$ over $\mathfrak{B}$ to obtain $\mathfrak{a}_v = \prod_{\mathfrak{p}\in\mathfrak{B}} \mathfrak{p}^{a_{\mathfrak{p}}}$, for some $a \in \mathbb{Z}^{|\mathfrak{B}|}$.
11: Return $z = a - v$.

As we mentioned above, we are interested in short relations in order to control the cost of the computation of the associated isogenies. We only consider imaginary quadratic orders $\mathcal{O}$ that contain $\mathbb{Z}[\pi]$ where π is the Frobenius endomorphism of some elliptic curve $\mathcal{E}/\mathbb{F}_q$. In choosing prime ideals in the factor base $\mathfrak{B}$ in the algorithms above, we restrict to prime ideals that are coprime to $[\mathcal{O}_K : \mathbb{Z}[\pi]]$ and this does not affect the computation.

We will see in the next section how to compute isogenies associated to the image of such prime ideals in $\mathrm{End}(\mathcal{E})$.

3.3.4 Isogeny computation

We now explain how we can compute an isogeny corresponding to an ideal of $\mathrm{End}(\mathcal{E})$, for an ordinary elliptic curve $\mathcal{E}/\mathbb{F}_q$, without knowing $\mathrm{End}(\mathcal{E})$. We begin with the following proposition, which can be used to identify the kernel of an isogeny associated to some prime ideal in $\mathrm{End}(\mathcal{E})$.

Proposition 3.3.4.1. *[59, Stage 3] Let $\mathfrak{a}$ be an ideal of $\mathrm{End}(\mathcal{E})$ of prime norm ℓ; write it as $\ell\,\mathrm{End}(\mathcal{E}) + u(\pi)\,\mathrm{End}(\mathcal{E})$, where the polynomial u is an irreducible factor of $\chi_{\mathcal{E}} \mod \ell$. The kernel of the corresponding isogeny $\phi_{\mathfrak{a}\,\mathrm{End}(\mathcal{E})}$ is an eigenspace of the Frobenius endomorphism, and we have $u = \chi_{\mathcal{E}}|_{\ker \phi_{\mathfrak{a}}}$.*

The map $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}$ preserves the norm ℓ and the polynomial u of ideals $\mathfrak{a}$ in $\mathbb{Z}[\pi]$. Because the $\mathrm{norm}(\mathfrak{a}) = \ell$, the kernel of the isogeny is a subgroup of order ℓ in the ℓ-torsion subgroup $\mathcal{E}[\ell]$.

The following algorithm computes isogenies corresponding to prime ideals appearing in the relations defined in Definition 3.3.2.2.

Algorithm 7 `Computation of the endomorphism ring [12, Algorithm 4.1]`

Input: An elliptic curve $\mathcal{E}/\mathbb{F}_q$ and a prime ideal $\mathfrak{a}$ in $\mathbb{Z}[\pi]$ with norm ℓ.

Output: The isogenous elliptic curve $\phi_{\mathfrak{a}\,\mathrm{End}(\mathcal{E})}(\mathcal{E})$.

1: Find a basis (P_i) of the ℓ-torsion of $\mathcal{E}$ over $\mathbb{F}_{q^{\ell-1}}$ using Algorithm 8.
2: Write the matrix M of the Frobenius endomorphism on (P_i).
3: Compute the eigenspaces of $M \in \mathrm{Mat}_2(\mathbb{Z}/\ell\mathbb{Z})$.
4: Determine which is the kernel of the isogeny $\phi_{\mathfrak{a}\,\mathrm{End}(\mathcal{E})}$.
5: Compute this isogeny using Velu's formula, [120].

Since the polynomial u is the same for the ideals $\mathfrak{a}$ and $\mathfrak{a}\,\mathrm{End}(\mathcal{E})$, it can be used in Step 4 to determine which one of the eigenspaces is the kernel of the isogeny corresponding to $\mathfrak{a}\,\mathrm{End}(\mathcal{E})$.

We present an algorithm that computes a basis of the ℓ-torsion subgroup $\mathcal{E}[\ell]$, for a prime ℓ and an elliptic curve $\mathcal{E}/\mathbb{F}_q$.

Algorithm 8 `[12, Algorithm 4.3]`

Input: An elliptic curve $\mathcal{E}/\mathbb{F}_q$ with Frobenius polynomial $\chi_\mathcal{E}$ and a prime ℓ.

Output: A basis of the ℓ-torsion $\mathcal{E}[\ell]$ over $\mathbb{F}_{q^{\ell-1}}$.

1: Decompose $|\mathcal{E}(\mathbb{F}_{q^{\ell-1}}|$ as $m\ell^k$ where $\ell \nmid m$.
2: Let P and Q be m times random points of $\mathcal{E}(\mathbb{F}_{q^{\ell-1}})$.
3: Compute the order ℓ^{k_P} of P and ℓ^{k_Q} of O and assume $k_P \geq k_Q$.
4: Precompute the table $(i, i\ell^{k_P-1}P)$ for $i \in \mathbb{Z}/\ell\mathbb{Z}$.
5: For j from $k_Q - 1$ down to 1:
6: If $\ell^j Q = i\ell^{k_P-1}P$ for some i, set $Q \leftarrow Q - i\ell^{k_P-j-1}P$.
7: If $Q = 0_\mathcal{E}$ then go back to Step 2.
8: Return $(\ell^{k_P-1}P, \ell^{k_Q-1}Q)$.

Proposition 3.3.4. *Algorithm 7 has a probabilistic runtime of* $O(\ell^{2+o(1)} \log^{2+o(1)} q)$, *with* $\mathrm{norm}(\mathfrak{a}) = \ell$.

Proof. See [12, Section 4]. □

With Algorithm 7, we can check whether a relation holds in $\mathrm{End}(\mathcal{E})$ or not, without having $\mathrm{End}(\mathcal{E})$. The following algorithm checks whether an order is contained in the endomorphism ring.

Algorithm 9 `Checking whether` $\mathcal{O} \subseteq \mathrm{End}(\mathcal{E})$ `[12, Algorithm 7.1]`

Input: An elliptic curve $\mathcal{E}/\mathbb{F}_q$ and an order $\mathcal{O} \supseteq \mathbb{Z}[\pi]$.

Output: Whether $\mathcal{O} \subseteq \mathrm{End}(\mathcal{E})$, with failure probability $o(1/\log^2 q)$.

1: Generate a set of $3 \log\log q$ relations of $\mathcal{O}$ with Algorithm 5.
2: If one does not hold in $\mathrm{End}(\mathcal{E})$, return false.
3: Check whether $\mathcal{O} \subseteq \mathrm{End}(\mathcal{E})$ locally at 2 and 3, if not, return false.
4: Return true.

Since we cannot test all relations, in Step 1, only $3 \log\log q$ random relations of $\mathcal{O}$ are generated and tested and this leads to the possibility of a wrong output. This is the reason why it was important that the short relations from Algorithm 5 had to be proven to be random to minimize the probability of failure. The probability of failure captures the scenarios where relations that do not hold in $\mathrm{End}\,(\mathcal{E})$ were not tested in Algorithm 9 and in that case, the algorithm can return true, but $\mathcal{O}$ is not contained in $\mathrm{End}\,(\mathcal{E})$.

This subsequently affects the output of Algorithm 3, which can fail to produce the correct endomorphism ring. To circumvent this and unconditionally check the output, a certification method of [17, Section 3.2] is used. Let $\mathcal{E}/\mathbb{F}_q$ be an ordinary elliptic curve with Frobenius endomorphism π.

Definition 3.3.5. A certificate for an order $\mathcal{O} \supset \mathbb{Z}[\pi]$ consists of :

- a family of orders $\mathcal{O}_i$ and relations r_i that hold in $\mathcal{O}_i$ but not in $\mathcal{O}$,
- a family of orders $\mathcal{O}_j$ and relations r_j that hold in $\mathcal{O}$ but not in $\mathcal{O}_j$,

such that $\mathcal{O}$ is the only order containing $\mathbb{Z}[\pi]$ satisfying $\mathcal{O}_i \not\subset \mathcal{O}$ and $\mathcal{O}_j \not\supset \mathcal{O}$ for all i and j.

Algorithms to compute certificates and verifying whether the output of Algorithm 3 is indeed the endomorphism ring are given in [17, Algorithm Certify and Algorithm Verify]. Since we do not need that in the alternative method, we do not go more into details. We refer to [113, Section 3.2] for a more detailed presentation.

In Section 3.4 we show how to overcome this obstacle by providing a way to get relations that characterizes orders and we produce an algorithm that always outputs the correct endomorphism ring.

3.3.5 Complexity analysis

We now give more details regarding the complexity of the algorithm that computes the endomorphism rings in [12]. We prove the following:

Theorem 3.3.5.1. *[12, Theorem 5.3] Under GRH, Algorithm 3 computes the endomorphism ring of an ordinary elliptic curve $\mathcal{E}/\mathbb{F}_q$, with failure probability $o(1)$, in probabilistic time $L(q)^{1+o(1)} + L(q)^{1/\sqrt{2}+o(1)}$, where the first term only accounts for the complexity of factoring the discriminant $D = O(q)$.*

The first step of the algorithm computes the Frobenius polynomial $\chi_{\mathcal{E}}$ of the Frobenius endomorphism π of $\mathcal{E}$. Computing $\chi_{\mathcal{E}}$ is essentially equivalent to counting the number of $\mathbb{F}_q$-rational points on $\mathcal{E}$. This is known to be fast via the Schoof-Ekies-Atkin algorithm, [57], which is polynomial in $\log q$.

For the factorization, which is needed for overorders computation, the method of Lenstra and Pomerance, [77], unconditionally factors the discriminant D and has a runtime of $L(|D|)^{1+o(1)}$. The discriminant D satisfies $|D| \leq 4q$. Hence the complexity of factoring D is at most $L(q)^{1+o(1)}$. Other factoring methods exist, with better asymptomatic complexity but they rely on unproven hypothesis, see [86] for instance.

In the rest of the algorithm, the main task is checking whether an order $\mathcal{O}$ is in the endomorphism ring via Algorithm 9. Let $\mathcal{O}$ be an order in a quadratic number field. We discuss the complexity of Algorithms 5 and 6 which are the important steps of Algorithm 9.

In the discussion above we only considered prime ideals that are elements of the factor base. We now prove, as a consequence of the Cebotarev density theorem, [119], that it is actually enough to consider prime ideals as a generating set of the Picard group.

Theorem 3.3.5.2. *Let L/K be a finite normal extension of number fields, and denote by $\pi(\mathfrak{p})$ the Frobenius element in $\mathrm{Gal}(L/K)$ which corresponds to a given prime $\mathfrak{p}$ of K. Such Frobenius elements are asymptotically uniformly distributed in the sense that for any conjugacy class $\mathcal{C}$ of the Galois group*

$$|\{\mathfrak{p} : \pi(\mathfrak{p}) \in \mathcal{C}, \mathrm{norm}(\mathfrak{p}) < x\}| \sim \frac{|\mathcal{C}|}{|\operatorname{Gal}(L/K)|} \operatorname{Li}(x)$$

as $x \to \infty$, where $\operatorname{Li}(x) = \int_2^x \frac{dt}{\log t}$ is asymptotically equal to the number of rational primes less than x.

This theorem has many applications and one of the consequences that plays a role in our context is that for an order $\mathcal{O}$, the density of prime ideals which belong to a prescribed ideal class in $\operatorname{Pic}(\mathcal{O})$ is $1/\operatorname{Pic}(\mathcal{O})$, which means that each ideal class can be represented by a prime ideal. Hence it is enough to only consider prime ideals as elements in the generating set.

The generating set or factor base $\mathfrak{B}$ in the algorithms above contains prime ideals of norm less than some bound N. If $n = |\operatorname{Pic}(\mathcal{O})|$, the current best unconditional bound is exponential in $\log n$, [26]. However, assuming GRH leads to a better bound, polynomial in $\log n$ [2].

Theorem 3.3.5.3. *[2, Theorem 4] Assuming GRH, for an order $\mathcal{O}$ with discriminant D in a number field, the prime ideals of norm less than $12 \log^2 |D|$ generate the Picard group of $\operatorname{Pic}(\mathcal{O})$. If $\mathcal{O}$ is an order in a quadratic number field, then this bound can be reduced to $6 \log^2 |D|$.*

For the computation of Picard groups, it is enough to generate relations that contain ideals of small norms. For our application, we need short relations i.e. the exponent should also be small and this is due to isogeny computation. In fact, to compute an isogeny associated to an ideal of the form $\mathfrak{p}^{n_\mathfrak{p}}$, we compute $n_\mathfrak{p}$ isogenies (starting with possibly a different elliptic curve each time). Under GRH, Bisson proved, Corollary 3.3.2, as a consequence of the result of Jao, Miller and Venkatesan, Theorem 3.3.1, that relations formed by primes with exponent $o(\log^{4+\varepsilon}|D|)$ generate the Picard group of an order $\mathcal{O}$ with discriminant D.

Algorithms 4, 5 and 6 all have a step where it is checked whether an ideal is only divisible by prime ideals in the factor base. In order to study the complexity the algorithms, it is crucial to know how this divisibility works or behaves. This is related to the smoothness properties of integers.

Definition 3.3.5.4. Any integer x is said to be y-smooth if it has no prime factor larger than y. We denote the number of y-smooth integers less than x by $\Psi(x, y)$.

If we take $y = x^{1/u}$, for some $u \geq 3$ we obtain the following result of Canfield, Erdös and Pomerance, [27]:

Theorem 3.3.5.5. *For $u \geq 3$ we have*

$$\Psi(x, x^{1/u}) \geq x \exp(-u(\log u + \log\log u - 1 + o(1)))$$

This result is at the center of most subexponential algorithms in computational number theory. We have:

Theorem 3.3.5.6. *The probability for a random number of $\{1, \ldots, x\}$ to be $L(x)^\gamma$-smooth is equivalent to $L(x)^{-1/2\gamma + o(1)}$ as $x \to \infty$.*

Proof. See [62, Section 1]. □

In our context, we work with ideals and the theorem above has to be adapted. We say that an ideal is smooth if its norm is also smooth. An important step of Algorithms 5 and 6 is the factorization of reduced ideals over some factor base. A theorem similar to the one above but for reduced ideals rather than integers can be used to estimate the probability of obtaining smooth representative and also to set an appropriate bound to increase that probability. In order to use Theorem 3.3.5.6, it is important that reduced ideals of ideal

classes behave like random integers in a certain interval. This was proved to hold for ideals in imaginary quadratic orders using the correspondence between reduced binary quadratic forms and reduced ideals in imaginary quadratic orders, [106]. The method does not extend to higher degree number fields and it is usually used as heuristic in the proof of the complexity of most subexponential algorithms, for instance, the class group computation for general number fields, [25].

We have the following result of Seysen [106]:

Proposition 3.3.5.7. *Let $\mathcal{O}$ be an imaginary quadratic order with discriminant D. The number of reduced ideals whose norm is $L(|D|)^{\gamma}$-smooth is at least $n/L(|D|)^{-1/2\gamma+o(1)}$, where n is the cardinality of* $\mathrm{Pic}(\mathcal{O})$.

The reduced ideals we are interested in are reduced ideals of ideals of the form $\sigma_{\mathcal{O}}(x)$, with x drawn uniformly at random in the box $\{0,\ldots,\log^{4+\varepsilon}|D|\}^{|\mathfrak{B}|}$. For Proposition 3.3.5.7 to be useful, we have to make sure that the ideals we generate are uniformly distributed in $\mathrm{Pic}(\mathcal{O})$. We need to avoid situations where only certain ideal classes are obtained. In the proposition below, by quasi-uniformly distributed we mean that the probability for $\sigma_{\mathcal{O}}(x)$ to be in a subset S of $\mathrm{Pic}(\mathcal{O})$ is $(1+o(1))\frac{|S|}{|\mathrm{Pic}(\mathcal{O})|}$.

Proposition 3.3.5.8. *[106] For an imaginary quadratic order $\mathcal{O}$ with discriminant D, ideal classes $\sigma_{\mathcal{O}}(x)$ of random selected vectors $x \in \{0,\ldots,\log^{4+\varepsilon}|D|\}^{|\mathfrak{B}|}$ are quasi-uniformly distributed in the Picard group of $\mathcal{O}$.*

Proposition 3.3.5.7 does not extend to general number fields. However the same behaviour is observed to hold and as we said above, it is usually considered as a heuristic in many computational number theoretic problems.

Theorem 3.3.5.9. *Under GRH, Algorithm 5 and 6 require each*

$$L(|D|)^{\gamma+o(1)} + L(|D|)^{1/(4\gamma)+o(1)}$$

operations to find a relation of $\mathcal{O}$.

Proof. See [34, Corollary 4.7] and [12, Propostion 6.4]. □

Theorem 3.3.5.10. *Let $\mathcal{E}/\mathbb{F}_q$ be an ordinary elliptic curve with Frobenius endomorphism π. The isogeny associated to a relation from Algorithm 5 or 6 can be computed by Algorithm 7 in $L(q)^{1/\sqrt{2}+o(1)}$.*

Proof. Let D be the discriminant of $\mathbb{Z}[\pi]$. We have $D = O(q)$. Algorithm 7 computes the isogeny corresponding to a prime ideal of norm ℓ n $O(\ell^{2+o(1)} \log^{2+o(1)} q)$. The relations output by Algorithm 5 and Algorithm 6 are formed by prime ideals of norms at most $L(q)^{\gamma}$ and exponents less than $\log^{4+\varepsilon} q$. The associated isogeny to a relation can then be computed in $L(q)^{2\gamma+o(1)}$. To balance the cost, the optimal choice of γ is $\frac{1}{2\sqrt{2}}$. Hence the complexity is $L(q)^{1/\sqrt{2}+o(1)}$. □

The two theorems above give rise to the complexity of computing a relation and the associated isogeny. Since random relations are used to tell orders apart, it is important that the output relations of the algorithms are uniformly distributed in the set of all relations. The lack of uniform distribution could lead to a higher probability of being in the situation where Algorithm 9 returns true while the output should have been false. But by Lemma 3.3.3 if $\mathcal{O}$ and $\mathcal{O}'$ are imaginary quadratic orders with $\mathcal{O}'$ is an order contained in $\mathcal{O}$, relations found by Algorithm 5 are quasi-uniformly distributed in $\Lambda_O/\Lambda_{\mathcal{O}'}$.

With this result, we can estimate the number of relations in a given order that are needed to obtain a satisfactory probability of a correct output of Algorithm 9. In [13, Chapter 7], Bisson showed that it is sufficient to only generate polynomially many relations in an order $\mathcal{O}$ with discriminant D, polynomial in $\log\log D$, to ensure that the relations characterize $\Lambda_{\mathcal{O}}$ i.e if all those relations are also relations in $\mathrm{End}(\mathcal{E})$, then $\mathcal{O} \subseteq \mathrm{End}(\mathcal{E})$ with probability $1 - o(1)$.

We conclude with the following:

Theorem 3.3.5.11. *Let $\mathcal{E}/\mathbb{F}_q$ be a simple ordinary elliptic curve. Under GRH, the endomorphism ring $\mathrm{End}(\mathcal{E})$ can be computed in $L(q)^{1+o(1)} + L(q)^{1/\sqrt{2}+o(1)}$, with failure probability $o(1)$.*

Proof. Let π be the Frobenius endomorphism of $\mathcal{E}$. The number of orders containing $\mathbb{Z}[\pi]$, to distinguish from is polynomial in $\log q$. For each order we compute a polynomial (polynomial in $\log\log q$) number of relations and compute their associated isogenies in time $L(q)^{1/\sqrt{2}+o(1)}$. Since the complexity of the certification procedure is at most $L(q)^{1/\sqrt{2}+o(1)}$, the overall complexity of computing the endomorphism ring is $L(q)^{1+o(1)} + L(q)^{1/\sqrt{2}+o(1)}$, where $L(q)^{1+o(1)}$ is the complexity of factoring the discriminant of $\mathbb{Z}[\pi]$. □

3.4 Improvements

In the method we presented above, in order to check whether an order $\mathcal{O}$ is in the endomorphism ring $\mathcal{E}$, we check if all relations of $\mathcal{O}$ hold in the endomorphism ring. But if we consider $\mathcal{O}' \subseteq \mathrm{End}(\mathcal{E})$, with $\mathbb{Z}[\pi] \subseteq \mathcal{O}' \subseteq \mathcal{O}$, all relations of $\mathcal{O}'$ hold in $\mathcal{O}$ by Lemma 3.3.2.3 and we do not need to check relations that hold in $\mathcal{O}'$ while verifying if $\mathcal{O} \subseteq \mathrm{End}\,(\mathcal{E})$.

We now provide a different approach that excludes those relations and only takes into account relations that need to be checked. We start with the following result which is a generalization of [70, Theorem 5.6], it can also be found in [111, Section 6].

Theorem 3.4.1. *Let $\mathcal{O}_1 \subseteq \mathcal{O}_2$ be orders in a number field K with relative conductor $\mathfrak{f}_{2,1} := (\mathcal{O}_1 : \mathcal{O}_2) = \{x \in K | x\mathcal{O}_2 \subseteq \mathcal{O}_1\}$. Then we have the following exact sequence:*

$$1 \longrightarrow \mathcal{O}_1^* \longrightarrow \mathcal{O}_2^* \longrightarrow (\mathcal{O}_2/\mathfrak{f}_{2,1})^* \,/\, (\mathcal{O}_1/\mathfrak{f}_{2,1})^* \longrightarrow \mathrm{Pic}(\mathcal{O}_1) \longrightarrow \mathrm{Pic}(\mathcal{O}_2) \longrightarrow 1.$$

Proof. We have the following diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K^*/\mathcal{O}_1^* & \longrightarrow & \bigoplus_{\mathfrak{p}} K^*/\mathcal{O}_{1\mathfrak{p}}^* & \longrightarrow & \mathrm{Pic}(\mathcal{O}_1) & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \eta} & & \\ 1 & \longrightarrow & K^*/\mathcal{O}_2^* & \longrightarrow & \bigoplus_{\mathfrak{p}} K^*/\mathcal{O}_{2\mathfrak{p}}^* & \longrightarrow & \mathrm{Pic}(\mathcal{O}_2) & \longrightarrow & 1 \end{array}$$

with exact rows, where β is induced by the embedding $\mathcal{O}_{1\mathfrak{p}}, \hookrightarrow \mathcal{O}_{2\mathfrak{p}}$ for primes $\mathfrak{p}$ in $\mathcal{O}_1$, $\mathcal{O}_{2\mathfrak{p}}$ the localization of $\mathcal{O}_2$ by $\mathcal{O}_1 \setminus \mathfrak{p}$ ($\mathcal{O}_{2\mathfrak{p}} \cong \bigoplus_{\mathfrak{q} \supseteq \mathfrak{p}} \mathcal{O}_{2\mathfrak{q}}$, where the $\mathfrak{q}$ runs over the prime ideals of $\mathcal{O}_2$ that contain $\mathfrak{p}$) and α, η are the natural surjections. By applying the Snake Lemma we obtain

$$1 \to \mathcal{O}_1^* \to \mathcal{O}_2^* \to \ker \beta \to \mathrm{Pic}(\mathcal{O}_1) \to \mathrm{Pic}(\mathcal{O}_2) \to 1.$$

We show that $\ker \beta \cong (\mathcal{O}_2/\mathfrak{f}_{2,1})^* \,/\, (\mathcal{O}_1/\mathfrak{f}_{2,1})^*$. We have $\ker \beta \cong \bigoplus_{\mathfrak{p}} \mathcal{O}_{2\mathfrak{p}}^*/\mathcal{O}_{1\mathfrak{p}}^*$. The rings $\mathcal{O}_{1\mathfrak{p}}$ and $\mathcal{O}_{2\mathfrak{p}}$ are equal for all $\mathfrak{p}$ not dividing the conductor $\mathfrak{f}_{2,1}$ of $\mathcal{O}_1$ in $\mathcal{O}_2$. We then have $\bigoplus_{\mathfrak{p} \supseteq \mathfrak{f}_{2,1}} \mathcal{O}_{2\mathfrak{p}}^*/\mathcal{O}_{1\mathfrak{p}}^* \cong \ker \beta$. From the proof of [111, 6.7. Theorem] we can deduce that

$$\mathcal{O}_{2\mathfrak{p}}^*/\mathcal{O}_{1\mathfrak{p}}^* \cong (\mathcal{O}_{2\mathfrak{p}}/\mathfrak{f}_{2,1}\mathcal{O}_{2\mathfrak{p}})^* \,/\, (\mathcal{O}_{1\mathfrak{p}}/\mathfrak{f}_{2,1}\mathcal{O}_{1\mathfrak{p}})^*.$$

It follows that

$$\bigoplus_{\mathfrak{p}\supseteq\mathfrak{f}_{2,1}} \mathcal{O}_{2\mathfrak{p}}^*/\mathcal{O}_{1\mathfrak{p}}^* \cong \bigoplus_{\mathfrak{p}\supseteq\mathfrak{f}_{2,1}} (\mathcal{O}_{2\mathfrak{p}}/\mathfrak{f}_{2,1}\mathcal{O}_{2\mathfrak{p}})^* / (\mathcal{O}_{1\mathfrak{p}}/\mathfrak{f}_{2,1}\mathcal{O}_{1\mathfrak{p}})^* \cong (\mathcal{O}_2/\mathfrak{f}_{2,1})^* / (\mathcal{O}_1/\mathfrak{f}_{2,1})^*,$$

by [70, Theorem 4.1]. Thus $\ker\beta \cong (\mathcal{O}_2/\mathfrak{f}_{2,1})^* / (\mathcal{O}_1/\mathfrak{f}_{2,1})^*$. □

The non-trivial elements of $\ker\beta/(\mathcal{O}_2^*/\mathcal{O}_1^*)$ correspond to relations that hold in $\mathcal{O}_2$ but not in $\mathcal{O}_1$. In other words, they represent ideals that are not principal in $\mathcal{O}_1$ but their embedding in $\mathcal{O}_2$ is principal. We denote $\ker\beta/(\mathcal{O}_2^*/\mathcal{O}_1^*)$ by $R_{\mathcal{O}_2,\mathcal{O}_1}$. We have the following:

Proposition 3.4.2. *Let $\mathcal{O}_1 \subseteq \mathcal{O}_2$ be orders in a number field K. The relations of $\mathcal{O}_2$ are either relations of $\mathcal{O}_1$ or relations formed by elements coming from the group $R_{\mathcal{O}_2,\mathcal{O}_1}$ and relations of $\mathcal{O}_1$.*

Proof. Let R be a relation that holds in $\mathcal{O}_2$ but not in $\mathcal{O}_1$. Then from the exact sequence

$$1 \to R_{\mathcal{O}_2,\mathcal{O}_1} \xrightarrow{f} \mathrm{Pic}(\mathcal{O}_1) \to \mathrm{Pic}(\mathcal{O}_2) \to 1,$$

we have that there exists an element $[\alpha] \in R_{\mathcal{O}_2,\mathcal{O}_1}$, with $\alpha \notin \mathfrak{f}_{2,1}$, and I a principal ideal in $\mathcal{O}_1$ such that $(\alpha\mathcal{O}_2) \cap \mathcal{O}_1 = I\prod_{\mathfrak{a}\in R}\mathfrak{a}\mathcal{O}_1$. It follows that $\alpha\mathcal{O}_2 = I\prod_{\mathfrak{a}\in R}\mathfrak{a}\mathcal{O}_2$. Hence $\prod_{\mathfrak{a}\in R}\mathfrak{a}\mathcal{O}_2 = (\alpha\mathcal{O}_2)I^{-1}$. □

Remark 3.4.3. From Proposition 3.4.2, in order to check if all relations of $\mathcal{O}_2$ hold in some other order for which we know that all relations of $\mathcal{O}_1$ hold, it is sufficient to only check relations from $R_{\mathcal{O}_2,\mathcal{O}_1}$. We will see later that only one relation suffices.

3.4.1 Imaginary quadratic orders

We now focus on imaginary quadratic orders.

Proposition 3.4.1.1. *[65, Proposition 5.2] Let $\mathcal{O}_1, \mathcal{O}_2$ be orders in an imaginary number field K with $\mathcal{O}_2$ a minimal overorder of $\mathcal{O}_1$. We have the following:*

- *The conductor $\mathfrak{f}_{2,1}$ of $\mathcal{O}_1$ in $\mathcal{O}_2$ is a prime ideal of $\mathcal{O}$.*
- *If $\mathfrak{f}_{2,1} \cap \mathbb{Z} = (p)$, then $p = [\mathcal{O}_2 : \mathcal{O}_1]$.*

Proposition 3.4.1.2. *Let $\mathcal{O}_1, \mathcal{O}_2$ be orders in an imaginary quadratic field K. If $\mathcal{O}_2$ is a minimal overorder of $\mathcal{O}_1$, then the group $(\mathcal{O}_2/\mathfrak{f}_{2,1})^* / (\mathcal{O}_1/\mathfrak{f}_{2,1})^*$ is cyclic.*

Proof. Let $p = [\mathcal{O}_2 : \mathcal{O}_1]$. If p does not divide $[\mathcal{O}_K : \mathcal{O}_2]$ and p is unramified, then from [23, Lemma 3.1], the quotient $(\mathcal{O}_2/\mathfrak{f}_{2,1})^* / (\mathcal{O}_1/\mathfrak{f}_{2,1})^*$ is cyclic.

We now look at the other cases. We have from [40, Theorem 7.24] that

$$h(\mathcal{O}_1) = \frac{h(\mathcal{O}_K) f_1}{[\mathcal{O}_K^* : \mathcal{O}_1^*]} \prod_{q|f_1} \left(1 - \left(\frac{d_K}{q}\right)\frac{1}{q}\right)$$
$$h(\mathcal{O}_2) = \frac{h(\mathcal{O}_K) f_2}{[\mathcal{O}_K^* : \mathcal{O}_2^*]} \prod_{q|f_2} \left(1 - \left(\frac{d_K}{q}\right)\frac{1}{q}\right)$$

where $f_1 := [\mathcal{O}_K : \mathcal{O}_1]$ and $f_2 = [\mathcal{O}_K : \mathcal{O}_2]$ and $h(\mathcal{O}_1)$, $h(\mathcal{O}_2)$ are the cardinality of $\mathrm{Pic}(\mathcal{O}_1)$ and $\mathrm{Pic}(\mathcal{O}_2)$ respectively. We have $f_1 = pf_2$ and the cardinality of the group $(\mathcal{O}_2/\mathfrak{f}_{2,1})^* / (\mathcal{O}_1/\mathfrak{f}_{2,1})^*$ is given by

$$\frac{f_1}{f_2} \left(\prod_{q|f_1} \left(1 - \left(\frac{d_K}{q}\right)\frac{1}{q}\right)\right) \left(\prod_{q|f_2} \left(1 - \left(\frac{d_K}{q}\right)\frac{1}{q}\right)\right)^{-1}$$

If p is ramified then the size of the group $(\mathcal{O}_2/\mathfrak{f}_{2,1})^* / (\mathcal{O}_1/\mathfrak{f}_{2,1})^*$ is p. This is because $\left(\frac{d_K}{p}\right) = 0$ in that case.

In the case p divides $[\mathcal{O}_K : \mathcal{O}_2]$, the order of the group $(\mathcal{O}_2/\mathfrak{f}_{2,1})^* / (\mathcal{O}_1/\mathfrak{f}_{2,1})^*$ is also p since in that case

$$\prod_{q|f_1} \left(1 - \left(\frac{d_K}{q}\right)\frac{1}{q}\right) = \prod_{q|f_2} \left(1 - \left(\frac{d_K}{q}\right)\frac{1}{q}\right)$$

Thus in both cases, the group has a prime order and so it is cyclic. □

Corollary 3.4.1.3. *Let $\mathcal{O}_1, \mathcal{O}_2$ be imaginary quadratic orders with $\mathcal{O}_2$ a minimal overorder of $\mathcal{O}_1$ and p such that $(p) = \mathbb{Z} \cap \mathfrak{f}_{2,1}$. The group $R_{\mathcal{O}_2,\mathcal{O}_1}$ is cyclic. If $\mathrm{val}_p([\mathcal{O}_K : \mathcal{O}_2]) = 0$ and p is unramified, the cardinality of the group $(\mathcal{O}_2/\mathfrak{f}_{2,1})^* / (\mathcal{O}_1/\mathfrak{f}_{2,1})^*$ is either $p+1$ or $p-1$. If $\mathrm{val}_p([\mathcal{O}_K : \mathcal{O}_2]) > 0$ or if p is ramified, the cardinality is p.*

The unit group of any imaginary quadratic order is $\{1, -1\}$, except for orders in $\mathbb{Q}(i)$ and $\mathbb{Q}(\zeta_3)$. For orders in $\mathbb{Q}(i)$, only the ring of integers has four units, $\{1, -1, i, -i\}$, for any other suborder, the unit group is $\{1, -1\}$. Similarly for $\mathbb{Q}(\zeta_3)$, any order other than the ring of integers has unit group $\{1, -1\}$. The unit groups of $\mathcal{O}_1$ and $\mathcal{O}_2$ in the diagram in Theorem 3.4.1 are both equal to $\{\pm 1\}$ except when $\mathcal{O}_2$ is the ring of integers of $\mathbb{Q}(i)$ and $\mathbb{Q}(\zeta_3)$.

We can use the group $R_{\mathcal{O}_2,\mathcal{O}_1}$ to improve the computation of endomorphism rings of ordinary elliptic curves.

Proposition 3.4.1.4. *Let $\mathcal{E}/\mathbb{F}_q$ be an ordinary elliptic curve with Frobenius endomorphism π. Let $\mathcal{O}_1, \mathcal{O}_2$ be orders in $\mathbb{Q}(\pi)$ such that $\mathbb{Z}[\pi] \subseteq \mathcal{O}_1 \subseteq \mathcal{O}_2$, $\mathcal{O}_1 \subseteq \mathrm{End}(\mathcal{E})$ and $\mathcal{O}_2$ a minimal orverorder of $\mathcal{O}_1$. To check whether $\mathcal{O}_2$ is contained in $\mathrm{End}(\mathcal{E})$, it is enough to check if the relation coming from a generator of $R_{\mathcal{O}_2,\mathcal{O}_1}$ holds in $\mathrm{End}(\mathcal{E})$.*

Proof. Since relations in $\mathcal{O}_1$ already hold in $\mathrm{End}(\mathcal{E})$, we only have to check relations of $\mathcal{O}_2$ that are not relations in $\mathcal{O}_1$. By Proposition 3.4.2, it suffices to check relations from $R_{\mathcal{O}_2,\mathcal{O}_1}$ and since $R_{\mathcal{O}_2,\mathcal{O}_1}$ is cyclic, we only need to consider a generator. □

If the cardinality of the group $R_{\mathcal{O}_2,\mathcal{O}_1}$ is p, any non-trivial element is a generator and it can be used to check whether $\mathcal{O}_2 \subseteq \mathrm{End}(\mathcal{E})$. We now show that even in the other cases in Corollary 3.4.1.3, it is enough to check for a random nonzero element.

Theorem 3.4.1.5. *Let $\mathcal{E}/\mathbb{F}_q$ be an ordinary elliptic curve with Frobenius endomorphism π and $\mathcal{O}_1, \mathcal{O}_2$ be orders in the CM-field K containing $\mathbb{Z}[\pi]$. Let R be a relation of $\mathcal{O}_1$ that is not a relation in any proper suborder of $\mathcal{O}_1$. Then, R is a relation of $\mathcal{O}_2$ if and only if $\mathcal{O}_1 \subseteq \mathcal{O}_2$ or we are in one of the cases of Proposition 3.3.2.4.*

Proof. The cases in Proposition 3.3.2.4 are the only ones where $\Lambda_{\mathcal{O}_1} = \Lambda_{\mathcal{O}_2}$ with $\mathcal{O}_1$ and $\mathcal{O}_2$ not contained in each other. We assume that we are not in those situations.

If $\mathcal{O}_1 \subseteq \mathcal{O}_2$, then all relations of $\mathcal{O}_1$ are relations of $\mathcal{O}_2$ by Lemma 3.3.2.3. Now assume that R is a relation of $\mathcal{O}_2$ and that $\mathcal{O}_1$ is not a suborder of $\mathcal{O}_2$. We show that R has to be a relation in $\mathcal{O} := \mathcal{O}_1 \cap \mathcal{O}_2$ and that will be a contradiction since $\mathcal{O} \subsetneq \mathcal{O}_1$

Let $\mathcal{O}' = \mathcal{O}_1 + \mathcal{O}_2$, $\mathfrak{f}_1 = (\mathcal{O} : \mathcal{O}_1)$, $\mathfrak{f}_2 = (\mathcal{O} : \mathcal{O}_2)$. Unless $\mathcal{O}_1 = \mathcal{O}_2 = \mathcal{O}_K$, either $\mathcal{O}_1^*/\mathcal{O}^*$ or $\mathcal{O}_2^*/\mathcal{O}^*$ is trivial. But we cannot have $\mathcal{O}_1 = \mathcal{O}_2 = \mathcal{O}_K$, since R is not a relation in $\mathcal{O}$. We then focus on the groups $(\mathcal{O}_1/\mathfrak{f}_1)^* / (\mathcal{O}/\mathfrak{f}_1)^*$ and $(\mathcal{O}_2/\mathfrak{f}_2)^* / (\mathcal{O}/\mathfrak{f}_2)^*$. We have that $\mathfrak{f}_1$ and $\mathfrak{f}_2$ are coprime and

$$(\mathcal{O}_1/\mathfrak{f}_1)^* / (\mathcal{O}/\mathfrak{f}_1)^* \cong (\mathcal{O}_1/\mathfrak{f}_1\mathfrak{f}_2)^* / (\mathcal{O}/\mathfrak{f}_1\mathfrak{f}_2)^*$$
$$(\mathcal{O}_2/\mathfrak{f}_2)^* / (\mathcal{O}/\mathfrak{f}_2)^* \cong (\mathcal{O}_2/\mathfrak{f}_2\mathfrak{f}_1)^* / (\mathcal{O}/\mathfrak{f}_2\mathfrak{f}_1)^*.$$

Hence R is a relation in $\mathcal{O}_1$ and $\mathcal{O}_2$ implies that there is $x \in \mathcal{O}'$ such that the class of x satisfies $[x] \in (\mathcal{O}_1/\mathfrak{f}_1\mathfrak{f}_2)^*$ and $[x] \in (\mathcal{O}_2/\mathfrak{f}_1\mathfrak{f}_2)^*$. This implies that $[x] \in (\mathcal{O}/\mathfrak{f}_2\mathfrak{f}_1)^*$. It follows that R is then a relation in $\mathcal{O}$ which is a contradiction. □

The computation of $R_{\mathcal{O}_2,\mathcal{O}_1}$ can be reduced to the computation of the multiplicative group of residue class rings $\mathcal{O}/\mathfrak{a}$, for an order $\mathcal{O}$ and a prime ideal $\mathfrak{a}$ of $\mathcal{O}$, which can be computed using [70, Algorithm 4.5] or [97, Section 2.5].

For our application, we do not need to compute the group $R_{\mathcal{O}_2,\mathcal{O}_1}$, we just need to find a relation in $\mathcal{O}_2$ that correspond to a nonzero element of $R_{\mathcal{O}_2,\mathcal{O}_1}$.

Corollary 3.4.1.6. *Let $\mathcal{E}/\mathbb{F}_q$ be an ordinary elliptic curve with Frobenius endomorphism π. Let $\mathcal{O}_1, \mathcal{O}_2$ be orders in $\mathbb{Q}(\pi)$ such that $\mathbb{Z}[\pi] \subseteq \mathcal{O}_1 \subseteq \mathcal{O}_2$, $\mathcal{O}_1 \subseteq \mathrm{End}(\mathcal{E})$ and $\mathcal{O}_2$ a minimal orverorder of $\mathcal{O}_1$. To check whether $\mathcal{O}_2$ is contained in $\mathrm{End}(\mathcal{E})$, it is enough to check if a relation corresponding to any nonzero element of $R_{\mathcal{O}_2,\mathcal{O}_1}$ holds in $\mathrm{End}\,(\mathcal{E})$.*

A relation coming from a nonzero element of $R_{\mathcal{O}_2,\mathcal{O}_1}$ is relation formed by prime ideals whose products equals $\alpha\mathcal{O}_2$, with $[\alpha]$ a nonzero element in $R_{\mathcal{O}_2,\mathcal{O}_1}$. We then have that $(\alpha\mathcal{O}_2) \cap \mathcal{O}_1$ is not principal. In practice, to check whether $\mathcal{O}_2 \subseteq \mathrm{End}\,(\mathcal{E})$, we compute the isogeny corresponding to the relation from a non-zero element of $R_{\mathcal{O}_2,\mathcal{O}_1}$. To control the cost of isogeny computation, we look for smooth relations and for that we use Algorithm 6, which takes as input an ideal and returns a smooth representative. We have the following:

Algorithm 10 `Checking whether` $\mathcal{O} \subseteq \mathrm{End}(\mathcal{E})$

Input: An elliptic curve $\mathcal{E}/\mathbb{F}_q$ and orders $\mathcal{O}_2 \supseteq \mathcal{O}_1 \supseteq \mathbb{Z}[\pi]$ with $\mathcal{O}_1 \subseteq \mathrm{End}(\mathcal{E})$ and $\mathcal{O}_2$ a minimal overorder of $\mathcal{O}_1$.

Output: Whether $\mathcal{O}_2 \subseteq \mathrm{End}(\mathcal{E})$.

1: Get an ideal $(\alpha\mathcal{O}_2) \cap \mathcal{O}_1$ in $\mathcal{O}_1$ corresponding to a nonzero element $[\alpha]$ of $R_{\mathcal{O}_2,\mathcal{O}_1}$.
2: Use Algorithm 6 to get a smooth representative of the ideal class in $\mathrm{Pic}(\mathcal{O}_1)$ and the corresponding smooth relation, R, in $\mathcal{O}_2$.
3: If R does not hold in $\mathrm{End}(\mathcal{E})$, return false.
4: Check whether $\mathcal{O}_2 \subseteq \mathrm{End}(\mathcal{E})$ locally at 2 and 3, if not, return false.
5: Return true.

In Step 2, we first look for smooth representative of the ideal in $\mathrm{Pic}(\mathcal{O}_1)$ instead of $\mathrm{Pic}(\mathcal{O}_2)$ because using Algorithm 6 directly with a relation in $\mathcal{O}_2$ may give a relation that could hold in $\mathcal{O}_1$. Also for the factor base in Algorithm 6, we choose primes that are coprime to

the index $[\mathcal{O}_K : \mathbb{Z}[\pi]]$. That way, we can map ideals to $\mathcal{O}_2$ and so norms and exponents will be preserved and we can use Algorithm 7. Algorithm 9 also checks whether $\mathcal{O}_2 \subseteq \mathrm{End}(\mathcal{E})$ with failure probability of $o(1/\log^2 q)$.

Proposition 3.4.1.7. *The output of Algorithm 10 is always correct.*

Proof. If the relation generated in Algorithm 10 holds in $\mathrm{End}(\mathcal{E})$, any relation of $\mathcal{O}_2$ holds in $\mathrm{End}(\mathcal{E})$ by Proposition 3.4.2. After checking whether $\mathcal{O}_2$ is contained in $\mathrm{End}(\mathcal{E})$ locally at 2 and 3, the output is correct. □

One of the main advantages of using Algorithm 10 instead of Algorithm 9 as a subroutine in the computation of the endomorphism rings of ordinary elliptic curves is that it gives the endomorphism ring directly, there is no need to use a certificate like in [12].

3.4.2 Complexity analysis

As mentioned above, we can use Algorithm 10 instead of Algorithm 9 to compute endomorphism rings of ordinary elliptic curves over finite fields.

Proposition 3.4.2.1. *(GRH) Let $\mathcal{E}/\mathbb{F}_q$ be an ordinary elliptic curve with Frobenius endomorphism π and let $\mathbb{Z}[\pi] \subseteq \mathcal{O}_1 \subseteq \mathcal{O}_2$ be orders with $\mathcal{O}_1 \subseteq \mathrm{End}(\mathcal{E})$ and $\mathcal{O}_2$ a minimal overorder of $\mathcal{O}_1$. Algorithm 10 checks whether $\mathcal{O}_2 \subseteq \mathrm{End}(\mathcal{E})$ in probabilistic time $L(q)^{1/\sqrt{2}+o(1)}$.*

Proof. The cost of obtaining a random non-trivial element in the group $R_{\mathcal{O}_2,\mathcal{O}_1}$ in Step 1 is negligible compared to the overall complexity. Using Algorithm 6 and Algorithm 7, we can check if the relation generated in Step 1 holds in $\mathrm{End}(\mathcal{E})$ in probabilistic time $L(q)^{1/\sqrt{2}+o(1)}$. Step 4 has a negligible complexity. The overall complexity is then $L(q)^{1/\sqrt{2}+o(1)}$. □

To sum up, we have the following algorithm:

Algorithm 11 `Computation of endomorphism ring`

Input: An elliptic curve $\mathcal{E}/\mathbb{F}_q$.

Output: An order isomorphic to the endomorphism ring of $\mathcal{E}$.

1: Compute the Frobenius polynomial $\chi_{\mathcal{E}}$ of $\mathcal{E}$ and construct the order $\mathcal{O}' = \mathbb{Z}[\pi]$.
2: For minimal overorders $\mathcal{O}$ of $\mathcal{O}'$:
3: Use Algorithm 10 with input $\mathcal{O}$, $\mathcal{O}'$, $\mathcal{E}$ to check whether $\mathcal{O}$ is contained in $\mathrm{End}(\mathcal{E})$.
4: If $\mathcal{O} \subseteq \mathrm{End}(\mathcal{E})$, set $\mathcal{O}' \leftarrow \mathcal{O}$ and go to Step 2.
5: Return $\mathcal{O}'$.

Theorem 3.4.2.2. *(GRH) Algorithm 11 computes the endomorphism ring of an ordinary elliptic curve $\mathcal{E}/\mathbb{F}_q$ in probabilistic time $L(q)^{1+o(1)} + L(q)^{1/\sqrt{2}+o(1)}$.*

Proof. Step 1 takes at most polynomial time. The cost of factoring the discriminant D of the equation order $\mathbb{Z}[\pi]$, which satisfies $|D| < 4q$, is $L(q)^{1+o(1)}$. The number of orders tested in Step 3 is at most $\log_2[\mathcal{O}_K : \mathbb{Z}[\pi]]$. The quantity $[\mathcal{O}_K : \mathbb{Z}[\pi]]$ is bounded by $2\sqrt{q}$ by [13, Lemma III.2.5]. It follows that the total complexity is $L(q)^{1/\sqrt{2}+o(1)} + L(q)^{1+o(1)}$. □

Remark 3.4.2.3.

- Our method and the method in [12] have the same asymptotic complexity. However, Algorithm 11 always outputs the endomorphism ring without a failure probability. We do not make use of a certificate to unconditionally verify the output unlike in [12] and also performs well in practice. A the complexity of a certification is $L(q)^{1/\sqrt{2}+o(1)}$, [12, Section 5],
- Also, instead of generating $3 \log \log q$ relations each time we want to check whether an order $\mathcal{O}$ is contained in the endomorphism ring, we only use one relation with our technique. The cost of generating a relation and computing the corresponding isogenies is $L(q)^{1/\sqrt{2}+o(1)}$.

3.4.3 Examples

We use the first example in [17] and show that our method is much more efficient. We mainly focus on steps that could be removed if we use our method. We use the algorithm FindRelation in [17] to compute our relations. The rest of the computation is done using Magma [19].

Let $\mathcal{E}/\mathbb{F}_q$ be an elliptic curve with

$$q = 160693804425899027555081234320605007554655094341590901447829 9$$

and the Weierstrass equation of $\mathcal{E}$, $y^2 = x^3 - 3x^2 + c_{\mathcal{E}}$, with

$$c_{\mathcal{E}} = 660897170071025494489036936911196131075522079970680898049528.$$

The trace of $\mathcal{E}$ is $t = 212$ and as indicated in [17], it takes only few seconds to compute it with the Schoof-Elkies-Atkin Algorithm. Let K be the CM-field and π the Frobenius endomorphism of $\mathcal{E}$. It also takes few seconds to compute

$$[\mathcal{O}_K : \mathbb{Z}[\pi]] = 2 \cdot 127 \cdot 524287 \cdot 7195777666870732918103$$

and the discriminant $d_K = -7$.

Computing the endomorphism ring locally at 2 and 127 can be achieved in seconds and the endomorphism ring is maximal at 2 and 127, i.e, 2 and 127 do not divide the index $[\mathcal{O}_K : \mathrm{End}(\mathcal{E})]$.

Let $p_1 := 524287$, $p_2 := 7195777666870732918103$, $\mathcal{O}$ the order in $\mathcal{O}_K$ with $[\mathcal{O}_K : \mathcal{O}] = p_1 p_2$, $\mathcal{O}_1$ the order with $[\mathcal{O}_K : \mathcal{O}_1] = p_1$ and $\mathcal{O}_2$ with $[\mathcal{O}_K : \mathcal{O}_2] = p_2$. We obtain in seconds the relation

$$R = \mathfrak{p}_1^{23}\mathfrak{p}_2^5\mathfrak{p}_3\mathfrak{p}_4^2,$$

that holds in $\mathcal{O}_1$, but not in $\mathcal{O}$, with $\mathfrak{p}_1$ a prime ideal above 2 in $\mathcal{O}_1$, $\mathfrak{p}_2$ a prime above 11 in $\mathcal{O}_1$, $\mathfrak{p}_3$ a prime ideal above 43 in $\mathcal{O}_1$ and $\mathfrak{p}_4$ a prime ideal above 71 in $\mathcal{O}_1$. We check whether this relation holds in $\mathrm{End}\,(\mathcal{E})$ via isogenies and we found that it does hold in few seconds. This implies that p_1 divides $[\mathcal{O}_K : \mathrm{End}(\mathcal{E})]$.

We now have to check if the endomorphism ring is $\mathcal{O}_K$ or not. We find almost instantly that $\mathfrak{p}$, a prime above 11 in $\mathcal{O}_1$, is a relation in $\mathcal{O}_K$ but it is not a relation in $\mathcal{O}_1$. To check whether $\mathrm{End}\,(\mathcal{E}) = \mathcal{O}_K$ we check if the isogeny corresponding to $\mathfrak{p}$ is an endomorphism. We find that it is not and we conclude that $\mathrm{End}(\mathcal{E}) = \mathcal{O}_1$.

In [17], the same example is computed in about 10 minutes. In our case, the total time spent to compute the endomorphism ring is proportional to that in [17] without the

step that checks whether p_1 divides the conductor of $\mathrm{End}(\mathcal{E})$. This step takes about eight minutes. So we have an eight minutes gain with a total time of 10 minutes. With the exact setting as in [17], we would be able to compute the endomorphism ring $\mathrm{End}(\mathcal{E})$ in less than two minutes with our method.

Chapter 4

Computation of Endomorphism Rings of Abelian Surfaces

In this chapter, we study the computation of the endomorphism rings of abelian varieties in high dimensions. We essentially focus on abelian surfaces i.e. abelian varieties of dimension two. However, some of the results apply to abelian varieties of dimension greater than two. We provide an extension of the previous methods which can be used to compute the endomorphism rings of principally polarized, absolutely simple, and ordinary abelian surfaces defined over finite fields in subexponential time in the size of the base field that could not be handled by previous methods. In addition, we show that the endomorphism rings of certain principally polarized, absolutely simple, and ordinary abelian surfaces are not computable in subexponential time with current methods, including ours. These results can be found in [53]. Finally, we show how the output of some algorithms in [14] can be made unconditionally correct.

4.1 Background

The exponential algorithm by Kohel we studied in the previous chapter cannot be extended to ordinary abelian varieties in general. However, other exponential methods in higher dimensions, like the one by Eisenträger and Lauter in [49], exist. The first subexponential method to compute endomorphism rings of ordinary abelian surfaces, i.e. abelian varieties of dimension two, was developed by Bisson in [14], which is a generalization of the approach we presented for ordinary elliptic curves in the previous chapter. However, as we will see, it is not suited for all abelian surfaces. In [110], a method by Springer,

similar to the one in [17] is used to compute the endomorphism rings of ordinary abelian surfaces satisfying certain conditions.

In [53], an extension of the method in [14], by Fieker, Hofmann and Sanon, is provided and allowed the computation of the endomorphism rings of some of the abelian surfaces that were excluded in [14], in subexponential time. Also in [53], a family of abelian surfaces, whose endomorphism rings are not computable in subexponential time with current methods, were constructed.

As in the previous chapter we start with the exponential method.

4.2 Exponential method

The method developed by Kohel using isogeny volcanoes does not extend to abelian varieties of higher dimensions as explained in [13, Section V.2]. However, there are other exponential methods that work in any dimension such as the method in [49] by Eisenträger and Lauter and that of Wagner in [121].

Eisenträger and Lauter developed an exponential method to check whether an endomorphism ring of an abelian variety is maximal. This also works for other orders and it is based on the following result:

Proposition 4.2.1. *[49, Corollary 9] Let $\mathcal{A}$ be an abelian variety over an algebraically closed field. If α is an endomorphism of $\mathcal{A}$ and n is coprime to the ambient characteristic, then $\mathcal{A}[n] \subseteq \ker \alpha$ if and only if $\alpha/n \in \mathrm{End}(\mathcal{A})$, that is, if there exits an endomorphism β such that $\alpha = n \circ \beta = \beta \circ n$.*

If $\mathcal{A}$ is defined over a finite field and is ordinary, Proposition 4.2.1 remains true since from Proposition 2.5.12, the endomorphism ring $\mathrm{End}(\mathcal{A})$ is unaffected by base field extensions.

Let $\mathcal{A}/\mathbb{F}_q$ be an ordinary abelian variety with Frobenius endomorphism π and $\mathcal{O}$ an order in the complex multiplication field K of $\mathcal{A}$. To test whether $\mathcal{O}$ is contained in $\mathrm{End}(\mathcal{A})$, we first compute a generating set S of $\mathcal{O}$, as a $\mathbb{Z}$-module. The elements of S can be written as $\frac{1}{n}\sum_i \alpha_i \pi^i$, with n and the $\alpha_i's$ integers. The order $\mathcal{O}$ is a subset of $\mathrm{End}\,\mathcal{A}$ if each generator satisfies $\mathcal{A}[n] \subseteq \ker(\sum_i \alpha_i \pi^i)$.

The complexity is exponential in $\log q$ because in general, n is exponential in $\log q$ and to check whether $\mathcal{A}[n] \subseteq \ker(\sum_i \alpha_i \pi^i)$, we compute n-torsion points which takes polynomial time in n. To compute the torsion subgroups, we use Algorithm 8 which extends nicely to Jacobian varieties, [39, Section 8].

This approach is used in the subexponential method we describe in the next section. More specifically, it computes the endomorphism ring locally at small primes and those primes are much less than the characteristic of the base field and they will satisfy the condition in Proposition 4.2.1.

As mentioned before, there is also an exponential method due to Wagner [121]. It can be interpreted as a Chinese Remainder Theorem variant of the one we just described. We do not use it in this thesis and we refer the reader to [121] or [13, Section V.3].

4.3 Subexponential methods

We present an extension of the lattice method from Chapter 3 to principally polarized, absolutely simple and ordinary abelian surfaces.

Let $\mathcal{A}/\mathbb{F}_q$ be a principally polarized, absolutely simple and ordinary abelian surface, with π its Frobenius endomorphism and $\chi_{\mathcal{A}}$ the characteristic polynomial of π. The characteristic polynomial $\chi_{\mathcal{A}}$ is a q-Weil polynomial of degree 4. The endomorphism algebra $\mathbb{Q} \otimes \mathrm{End}(\mathcal{A})$ is isomorphic to the field $K = \mathbb{Q}[x]/(\chi_{\mathcal{A}}(x))$, which is a quartic CM-field. We fix an isomorphism between $\mathbb{Q} \otimes \mathrm{End}(\mathcal{A})$ and $K = \mathbb{Q}[x]/(\chi_{\mathcal{A}}(x))$, which by Proposition 2.4.2.4, is equivalent to choosing a CM-type Φ of K. In addition since $\mathcal{A}$ is absolutely simple, by Proposition 2.4.2.3, Φ is primitive. By Proposition 2.5.14, the endomorphism ring always contains the order $\mathbb{Z}[\pi, \overline{\pi}]$ and is stable under complex conjugation. Also any order $\mathcal{O}$ satisfying $\mathbb{Z}[\pi, \overline{\pi}] \subseteq \mathcal{O} \subseteq \mathcal{O}_K$ that is stable under complex conjugation is the endomorphism ring of a principally polarized abelian variety isogenous to $\mathcal{A}$.

The algorithm in [14] that computes the endomorphism rings of abelian surfaces is very similar to that of elliptic curves. It is as follows:

Algorithm 12 `Computation of endomorphism ring [13, Algorithm VIII.1.2]`

Input: A simple ordinary abelian variety $\mathcal{A}/\mathbb{F}_q$.

Output: An order isomorphic to the endomorphism ring of $\mathcal{A}$.

1: Compute the Frobenius polynomial $\chi_{\mathcal{A}}$ of $\mathcal{A}$ and construct the order $\mathcal{O}' = \mathbb{Z}[\pi, \overline{\pi}]$.
2: For minimal overorders $\mathcal{O}$ of $\mathcal{O}'$:
3: If $\mathcal{O} \subset \mathrm{End}(\mathcal{A})$ set $\mathcal{O}' \leftarrow \mathcal{O}$ and go to Step 3.
4: Return $\mathcal{O}'$.

The algorithm is similar to Algorithm 3, although there are lots of differences when it comes to individual steps. We detail those differences below. As before, relations play an important role in the computation of endomorphism rings of abelian surfaces.

We recall the definition of the polarized class group of an order in a CM-field.

Definition 4.3.1. For any order $\mathcal{O}$ in a CM-field K, the polarized class group $\mathfrak{C}(\mathcal{O})$ of $\mathcal{O}$ is defined to be the quotient of the group $I_{\mathcal{O}}$ consisting of all pairs $(\mathfrak{a}, \rho)$ satisfying $\mathfrak{a}\bar{\mathfrak{a}} = \rho\mathcal{O}$ where $\mathfrak{a}$ is an invertible fractional ideal of $\mathcal{O}$ and ρ a totally positive element of K_0, endowed with component-wise multiplication, modulo $P_{\mathcal{O}}$, its subgroup formed by pairs of the form $(\mu\mathcal{O}, \mu\bar{\mu})$ for $\mu \in K$.

Definition 4.3.2. Let $\mathcal{A}/\mathbb{F}_q$ be a principally polarized absolutely simple and ordinary abelian surface with Frobenius endomorphism π. A relation is any tuple $(\alpha_1, \ldots, \alpha_k)$ of elements of $\mathfrak{C}(\mathbb{Z}[\pi, \overline{\pi}])$. We say that a relation holds in an order $\mathcal{O} \supset \mathbb{Z}[\pi, \overline{\pi}]$ if the product $\alpha_1 \cdots \alpha_k$ is trivial in $\mathfrak{C}(\mathcal{O})$ through the map of Lemma 4.3.3, and that it holds in $\mathrm{End}(\mathcal{A})$ if the corresponding isogeny chain $\phi_{\alpha_1} \cdots \phi_{\alpha_k}$ maps $\mathcal{A}$ to an isomorphic abelian variety.

We denote the set of all relations of an order $\mathcal{O}$ by $\Lambda_{\mathcal{O}}$. A subset of $\Lambda_{\mathcal{O}}$, formed by relations containing ideals of the form $N_{\Phi^r} \circ N_{\Phi}(\mathfrak{p})$, where $\mathfrak{p}$ is a prime ideal in $\mathfrak{C}(\mathcal{O})$, is used in [14] rather than the full lattice of relations, because it leads to an efficient isogeny computation. We denote the set by $\Lambda_{\Phi}(\mathcal{O})$ and we will we come back to it in the subsequent sections.

Lemma 4.3.3. *[14, Lemma 4.1] For a Weil number π and for any two orders $\mathcal{O} \subset \mathcal{O}'$ containing $\mathbb{Z}[\pi, \overline{\pi}]$, the map $(\mathfrak{a}, \rho) \in I_{\mathcal{O}} \to (\mathfrak{a}\mathcal{O}', \rho) \in I_{\mathcal{O}'}$ induces a natural morphism of polarized class groups $\mathfrak{C}(\mathcal{O}) \to \mathfrak{C}(\mathcal{O}')$; this morphism is surjective when restricted and co-restricted to elements satisfying $\rho \in \mathbb{Q}$.*

To determine whether a specific order $\mathcal{O}$ is contained in the endomorphism ring of $\mathcal{A}$, we select relations and check whether these relations hold in $\mathcal{A}$. And to check whether a relation holds in $\mathcal{A}$, we need to compute isogenies.

At the time of the writing of [14], the isogenies that could be computed efficiently were (ℓ, ℓ)-isogenies. An (ℓ, ℓ)-isogeny is a separable isogeny whose kernel is isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^2$. The relations that correspond to such isogenies are obtained through the reflex field and reflex type norm. This is why the subset $\Lambda_\Phi(\mathcal{O})$ of relations of $\mathcal{O}$ is used instead of the full lattice of relations. Since the CM-type Φ is primitive, we have the following diagram which can found in [14, Figure 2]:

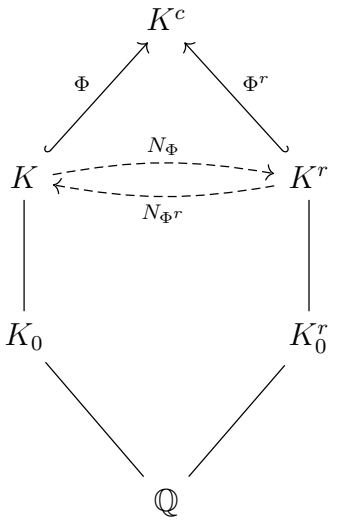

FIGURE 4.1: The complex multiplication field, its reflex field, and type norm maps.

From the figure above, we can indeed see that if the CM-type is primitive, which is always the case since we we work with absolutely simple varieties, the image of the map $N_{\Phi^r} \circ N_\Phi$ goes back to the CM-field K.

The rest of this section is devoted to detailing the different steps of Algorithm 12 as well as providing a succinct complexity analysis.

4.3.1 Difference between the computation of endomorphism rings of elliptic curves and abelian surfaces

We have already mentioned some differences above. Here we discuss them in more detail. A major difference is the appearance of polarization. In the elliptic curve case, we use the

action of the Picard group via Theorem 3.3.2.1, for principally polarized abelian varieties, we need the action to preserve polarization, and for that reason the polarized class group is used instead, Theorem 2.5.11. This means that all relations we use in dimension two are relations in the polarized class group instead of the Picard group.

Another major difference is the structure of the lattice of orders itself. For imaginary quadratic fields, the structure is quite simple and overorders can be computed efficiently. This changes when we consider quartic CM-fields or any higher degree CM-fields. Computing overorders becomes challenging and as a matter of fact, Bisson excluded some abelian surfaces because of that. We denote the set of those abelian surfaces by $\mathcal{A}_1$.

Apart from the computation of overorders, there is another aspect that prevents the method from computing the endomorphism rings of some abelian surfaces. This is when two orders have the same set of relations but they are distant from each other (see Definition 4.3.1.2 for the definition of distance between orders). In that case, relations cannot tell the orders apart. It also happens that two imaginary quadratic orders have the same set of relations, but this only happens locally at 2 and 3 by Proposition 3.3.2.4 and we use the exponential methods to handle those cases and determine the correct endomorphism rings.

For abelian surfaces, we might have to compute the endomorphism rings locally at primes that are exponential in $\log q$, where q is the cardinality of the base field. Using an exponential method to handle those cases is not an option if we want to achieve subexponential complexity. Bisson proved that this situation does not happen too often by showing that those cases constitute a zero density subset of the total cases.

Theorem 4.3.1.1. *[14, Theorem 7.1] Let $(\mathcal{A}_i/\mathbb{F}_{q_i})_{i\in\mathbb{N}}$ be a sequence of ordinary abelian surfaces defined over fields of monotonously increasing cardinality $q_i \to \infty$. Denote by $v_i = [\mathcal{O}_{\mathbb{Q}(\pi_i)} : \mathbb{Z}[\pi_i, \overline{\pi}_i]]$ their conductor gaps, and by $n_i = \mathrm{norm}_{K_0/\mathbb{Q}}(D_{K/K_0})$ the norm of the relative discriminant of their CM-fields $K = \mathbb{Q}(\pi_i)$. Assume that there exists a constant C such that, for all positive integers u and m :*

- *the probability of indices $i < m$ for which $u|v_i$ is at most C/u;*
- *the proportion of indices $i < m$ for which $u|v_i$ and $u|n_i$ is at most C/u^2.*

For any $\tau > 0$, the density of indices i for which there exists two orders $\mathcal{O}$ and $\mathcal{O}'$ containing $\mathbb{Z}[\pi_i, \overline{\pi}_i]$, stable under complex conjugation, satisfying $\Lambda_\Phi(\mathcal{O}) = \Lambda_\Phi(\mathcal{O}')$, and such that $\ell^{\mathrm{val}_\ell v_i} > L(q_i)^\tau$ for some prime factor ℓ of index $[\mathcal{O} + \mathcal{O}' : \mathcal{O} \cap \mathcal{O}']$, is zero.

This theorem says that apart from a zero density set of abelian surfaces defined over finite fields, the lattice $\Lambda_\Phi(\mathcal{O})$ uniquely characterizes $\mathcal{O}$ from other orders containing $\mathbb{Z}[\pi, \overline{\pi}]$, except locally at small primes and so an exponential method can handle those. We denote the zero density set by $\mathcal{A}_2$.

Definition 4.3.1.2. Let $\mathcal{O}$ and $\mathcal{O}'$ be orders in a number field K. We define the distance between $\mathcal{O}$ and $\mathcal{O}'$ as the index $[\mathcal{O} + \mathcal{O}' : \mathcal{O} \cap \mathcal{O}']$.

There are other differences related to the computation of short relations. In fact, in addition to the GRH, it is assumed that the norm of reduced ideals are as smooth as random integers (this was proven in the quadratic case [106]). This assumption is important in studying the complexity of generating relations in orders in quartic CM-fields. In class group computation algorithms using the index calculus method, it is assumed for any number field of degree greater than two [25].

4.3.2 Isogeny computation and short relations

The isogeny computation for abelian surfaces is more complicated than that of elliptic curves. There is no easy way to represent abelian varieties in higher dimensions like the Weierstrass equation for elliptic curves. Also, the quotient $\mathcal{A}/G$ of a principally polarized abelian variety by a finite subgroup does not necessarily admit or preserve principal polarization. Methods to compute isogenies in higher dimensions were developed in [24, 36, 46]. In our context, we are not just interested in computing isogenies from given subgroups, but we also need to find subgroups corresponding to prime ideals in the polarized class group. We start by discussing ways to obtain subgroups that correspond to a separable isogeny associated to ideals in the polarized group of the endomorphism ring of a simple ordinary abelian variety.

Proposition 4.3.2.1. *[59, Stage 3] Let $\mathcal{A}/\mathbb{F}_q$ be a simple ordinary abelian variety, $\mathcal{O}$ its endomorphism ring and $\pi \in \mathcal{O}$ the element corresponding to its Frobenius endomorphism. Let $\mathfrak{a}$ be an invertible prime ideal of $\mathcal{O}$, written as $\ell\mathcal{O} + u(\pi)\mathcal{O}$, where ℓ is its norm and u is an irreducible factor modulo ℓ of the characteristic polynomial $\chi_\mathcal{A}$ of the primitive element π. Assume that ℓ is prime to the discriminant of $\mathbb{Z}[\pi, \overline{\pi}]$. Then the characteristic polynomial of the Frobenius endomorphism acting on $\ker(\phi_\mathfrak{a})$ is u.*

With this proposition, the kernel of the isogenies corresponding to ideals from the polarized class group can be computed without knowing the endomorphism ring. As in the

elliptic curve case, an algorithm similar to Algorithm 8 can be used to compute the basis of the torsion group $\mathcal{A}[\ell]$, for some prime ℓ. The main difference from elliptic curves is the possibility to draw points uniformly at random. It is not known how to do this efficiently for all abelian varieties, but it can be done for Jacobian varieties by using their underlying curve [39]. Once we obtain a basis of the ℓ-torsion subgroup, an algorithm similar to Algorithm 7 can be used to determine the subgroup corresponding to the isogeny we wish to compute.

The challenging part of the computation comes after obtaining the subgroup corresponding to the kernel of the isogeny. For elliptic curves, we can use Velu's formula as we have already seen. In higher dimensions, Lubicz and Robert [78] and later Cossset and Robert, [36] gave a generalization of Velu's formula. Given an abelian surface $\mathcal{A}$, their method takes a subgroup G that is isotropic with respect to the Weil pairing and isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^2$ and the algorithm outputs the isogeny $\mathcal{A} \to \mathcal{A}/G$. The condition on the subgroup, namely isotropic and isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^2$ is mainly to handle polarization [14, Section 4] and those subgroups correspond to ideals in $\Lambda_\Phi(\mathcal{O})$.

We have the following:

Proposition 4.3.2.2. *[36, Theorem 1.2] Let $\mathcal{A}/\mathbb{F}_q$ be a principally polarized, absolutely simple and ordinary abelian surface and let G be a rational isotropic subgroup, with respect to the Weil pairing, isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^2$, of $\mathcal{A}$ with ℓ a prime different from the characteristic of $\mathbb{F}_q$. There is an algorithm that evaluates the separable isogeny with kernel G with a worst-case complexity of $\ell^{6+o(1)}$ operations in the base field.*

The output of the algorithm in Proposition 4.3.2.2 is a representative of the isomorphism class $\mathcal{A}/G$ defined over the field of definition of the individual points of G, and this happens even if the subgroup G and $\mathcal{A}/G$ are rational. It is important to be able to obtain a representative of the variety over $\mathbb{F}_q$. The method of Mestre in [81] can be used for principally polarized, absolutely simple and ordinary abelian surfaces to get a representative of the isomorphism class $\mathcal{A}/G$ defined over the minimal field. Since we compute isogeny chains (corresponding to relations), after each isogeny evaluation step, the representative of the image defined over the base field is needed in order to perform the next isogeny computation.

Since the work of Cosset and Robert [36], some progress has been made in isogeny computation and it is now possible to compute cyclic separable isogenies, i.e. isogenies whose kernels are cyclic groups.

As stated before, some abelian varieties of the form $\mathcal{A}/G$ do not admit polarization. In [46], there is a characterisation that can be used to determine if the abelian variety $\mathcal{A}/G$ admits a principal polarization and if so, compute it and the corresponding isogeny by using theta functions. For more details on Mumford's theory of theta function see [87–90].

Theorem 4.3.2.3. *[46, Theorem 1.1] Let $\mathcal{L}_0$ be a principal polarization on $\mathcal{A}$. The a priori non-polarized abelian variety $\mathcal{A}/G$ admits a polarization $\mathcal{M}_0$ if and only if there is a totally positive real endomorphism β in $\mathrm{End}(\mathcal{A})$ such that $G \subset \ker(\beta)$ and G is a maximal isotropic subgroup for the commutator pairing $e_{\mathcal{L}_0^\beta}$.*

For the precise definition of the commutator pairing, see Section 3.1.2 in [46].

Theorem 4.3.2.4. *[46, Theorem 1.3] Let ℓ be an odd prime different from the characteristic of $\mathbb{F}_q$, the base field of $\mathcal{A}$, $\mathcal{L}_0$ a principal polarization on $\mathcal{A}$ and $G \subset \mathcal{A}(\overline{\mathbb{F}_q})$ be a π-stable cyclic subgroup of order ℓ, with π the Frobenius endomorphism. Under the following hypotheses:*

- *H.1 ℓ is either split or ramified in $\mathcal{O}_{K_0}$ and one of the prime ideals of $\mathcal{O}_{K_0}$ above ℓ is principal and generated by a totally positive element $\beta \in \mathcal{O}_{K_0}$ of norm ℓ such that $G \subset \mathcal{A}[\beta]$.*
- *H.2 The abelian variety has maximal local real endomorphism ring at ℓ.*
- *H.3 The conductor gap $[\mathcal{O}_{K_0} : \mathbb{Z}[\pi + \bar{\pi}]]$ is coprime to 2ℓ, where $\bar{\pi}$ is the image of the Frobenius endomorphism under complex conjugation.*
- *H.4 There is an algorithm $RM(\alpha, y)$ that computes the action of a real multiplication endomorphism α in $\mathrm{End}(\mathcal{A})_0$ on a 4-torsion point $y \in \mathcal{A}[4]$,*

the abelian variety $\mathcal{A}/G$ admits a principal polarization and there is an algorithm that computes its theta null point in polynomial time in $\log q$ and ℓ.

The theta null point determines the principally polarized abelian surfaces. We are interested in principally polarized abelian surfaces, not the explicit isogeny, and having the theta null point is enough to determine the equation of the underlying curve C of $\mathcal{A}/G$, [36].

Theorem 4.3.2.5. *Suppose $\mathcal{A}$ is a principally polarized, absolutely simple, and ordinary abelian surface. The algorithm of Theorem 4.3.2.4 can compute all isogenies corresponding to prime ideals of prime norms and coprime to $2 \times [\mathcal{O}_K : \mathbb{Z}[\pi, \bar{\pi}]]$ from the polarized class group $\mathfrak{C}(\mathrm{End}(\mathcal{A}))$.*

Proof. Let $\mathfrak{p}$ be a prime ideal from $\mathfrak{C}(\mathrm{End}(\mathcal{A}))$ of prime norm. From the complex multiplication action we know that the subgroup G corresponding to $\mathfrak{p}$ is π-stable. Also, since $\mathfrak{p}$ is an element of the polarized class group, we have $\mathfrak{p}\overline{\mathfrak{p}} = \alpha\,\mathrm{End}(\mathcal{A})$ with α a totally positive element in K_0 with $\mathrm{norm}(\alpha)$ in $\mathcal{O}_{K_0}$ prime. It then follows that $\alpha\mathcal{O}_{K_0}$ is a prime ideal in $\mathcal{O}_{K_0}$. Hypothesis $H.4$ is satisfied for principally polarized, absolutely simple, ordinary abelian surfaces, see [46, Remark 3]. Since the ideals are coprime to $2 \times [\mathcal{O}_K : \mathbb{Z}[\pi, \bar{\pi}]]$, Hypothesis $H.2$ and $H.3$ are satisfied. □

We discuss the computation of short relations in the polarized class group of an order in a CM-field with primitive CM-type. There are quite a number of similarities with the relation computation in the previous chapter and so we give a brief description.

Let $\mathcal{A}/\mathbb{F}_q$ be a principally polarized, absolutely simple and ordinary abelian surface with Frobenius endomorphism π and CM-field and CM-type (K, Φ). Let $\mathcal{O} \supset \mathbb{Z}[\pi, \overline{\pi}]$ be an order in K. The following algorithm computes a short relation that holds in $\mathcal{O}$.

Algorithm 13 `Generating short relations [14, Algorithm 4.3]`

Input: $\mathcal{O}$ and a parameter $\gamma > 0$.

Output: A relation holding in $\mathcal{O}$ for which the corresponding isogeny can be computed efficiently.

1: Form a set $\mathfrak{B}$ of prime ideals $\mathfrak{p}$ of $\mathcal{O}$ with norm less than $L(|\operatorname{disc}(\mathcal{O})|)^{\gamma}$.
2: Draw a vector $x \in \mathbb{Z}^{|\mathfrak{B}|}$ uniformly at random with coordinates $|x_{\mathfrak{p}}| < \log(|\operatorname{disc}(\mathcal{O})|)^{4+\epsilon}$ when $\mathrm{norm}_{K/\mathbb{Q}}(\mathfrak{p}) < \log(|\operatorname{disc}(\mathcal{O})|)^{2+\epsilon}$ and $x_{\mathfrak{p}} = 0$ otherwise.
3: Compute a reduced ideal representative $\mathfrak{a}$ of $\prod \mathfrak{p}^{x_{\mathfrak{p}}}$
4: If $\mathfrak{a}$ factors over $\mathfrak{B}$ as $\prod \mathfrak{p}^{y_{\mathfrak{p}}}$:
5: Return the relation containing $N_{\Phi^r}(N_{\Phi}(\mathfrak{p}))$ with multiplicity $x_{\mathfrak{p}} - y_{\mathfrak{p}}$ for $\mathfrak{p} \in \mathfrak{B}$.
6: Go back to Step 2.

As explained through Figure 4.1, the image in Step 5 is indeed an element of the polarized class group. The different bounds on the exponents of the prime ideals remain valid for orders in CM-fields of arbitrarily degree as pointed out by Bisson in [14, Section 4].

After presenting the relation computation algorithm, the natural next step is to use those relations to check whether the lattice of relations $\Lambda_{\Phi}(\mathcal{O})$, for some order $\mathcal{O}$, is contained in the set of relations $\Lambda_{\Phi}(\mathrm{End}(\mathcal{A}))$ of the endomorphism ring. We have the following algorithm:

Algorithm 14 `Checking whether` $\Lambda_\Phi(\mathcal{O}) \subseteq \Lambda_\Phi(\mathrm{End}(\mathcal{A}))$ `[14, Algorithm 5.1]`

Input: An absolutely simple, ordinary and principally polarized abelian surface $\mathcal{A}/\mathbb{F}_q$ and an integer m.

Output: Whether $\Lambda_\Phi(\mathcal{O}) \subseteq \Lambda_\Phi(\mathrm{End}(\mathcal{A}))$, with failure probability at most q^{-m}.

1: Repeat $m \log_2 q$ times:
2: Find relation $(\alpha_1, \ldots, \alpha_k)$ of $\mathfrak{C}(\mathcal{O})$ with Algorithm 13.
3: If the corresponding isogeny $\phi_{\alpha_1} \circ \cdots \circ \phi_{\alpha_k}$ does not map $\mathcal{A}$ to an isomorphic variety (by comparing their Igusa invariants), return false.
4: Return true.

We now study the complexity of the computation of the endomorphism ring of abelian surfaces and then show an alternative method to Algorithm 14 that produces the same result but without a probability of failure.

4.3.3 Complexity analysis

We gave a quite detailed complexity analysis in the previous chapter. Some of the techniques and results are still satisfied in dimension two.

The relations we are looking for are from orders of a quartic CM-field and the smoothness property of reduced ideals is essential to analyse Algorithm 13. For number fields of degree greater that two, it is not proven that reduced ideals have the smoothness properties of integers. We then assume the following:

Hypothesis 4.3.3.1. *Reduced ideals have the smoothness properties of integers in Theorem 3.3.5.6 of comparable size*

Proposition 4.3.3.2. *[14, Proposition 4.4] Under GRH and Hypothesis 4.3.3.1, Algorithm 13 generates a relation with total norm* $L(|\operatorname{disc}(\mathcal{O})|)^{4\gamma+o(1)}$ *in an order* $\mathcal{O}$ *in expected time* $L(|\operatorname{disc}(\mathcal{O})|)^{\gamma+o(1)} + L(|\operatorname{disc}(\mathcal{O})|)^{1/(4\gamma)+o(1)}$.

To balance the cost of generating relations with that of evaluating the associated isogenies, the choice of $\gamma = 1/(4\sqrt{3})$ is made.

Proposition 4.3.3.3. *[14, Proposition 5.2] Under GRH and Hypothesis 4.3.3.1, Algorithm 14 determines whether the relation lattice* $\Lambda_\Phi(\mathrm{End}(\mathcal{A}))$ *contains that of a prescribed order* $\mathcal{O}$ *with error probability using an expected* $L(|\operatorname{disc}(\mathcal{O})|)^{\sqrt{3}+o(1)}$ *operations in the base field.*

By using Lemma 3.2.2.1 we have $|\operatorname{disc}(\mathcal{O})| < 4^6 q^4$ and so the complexity of Algorithm 14 is $L(q)^{2\sqrt{3}+o(1)}$.

Theorem 4.3.3.4. *[14, Theorem 7.2] Under GRH and Hypothesis 4.3.3.1 the endomorphism ring of an absolutely simple, principally polarized and ordinary abelian surface not in $\mathcal{A}_1$ or in $\mathcal{A}_2$ defined over $\mathbb{F}_q$ may be computed in average probabilistic time $L(q)^{2\sqrt{3}+o(1)}$ with error probability less than $1/q^4$.*

Proof. The bottleneck of Algorithm 12 is Step 3. After getting the order with the right lattice of relations, the exponential algorithm of Eisenträger and Lauter is used to compute the endomorphism ring locally at small primes, which has negligible complexity since we excluded the set $\mathcal{A}_2$. Also, since the set $\mathcal{A}_1$ is excluded, all overorders can be obtained in subexponential time. □

To unconditionally certify the result like in the elliptic curve case, a certificate is used to check whether the lattice of relations is really that of the endomorphism ring. The complexity of generating a certificate and that of the verification is subexponential in $\log q$. In case the output of Algorithm 12 is wrong, we have to redo the computation until the correct order is obtained.

In [110], a different approach of computing endomorphism rings of abelian surfaces is presented. It is the generalization of the first subexponential method of Bisson and Sutherland for elliptic curves, [17], and is restricted to abelian surfaces satisfying certain conditions. Under those conditions, we can compute $\mathfrak{l}$-isogenies, where $\mathfrak{l}$ is an ideal in the ring of integers of the maximal totally real subfield of the CM-field. The Picard group action also preserves polarization under those conditions. We do not go further into details since our work is not based on it and we also note that the approach does not extend the method of Bisson, [14]. Interested readers can see [110] for more details.

In the rest of this chapter we present an approach that outputs the endomorphism ring without a probability of failure. We also focus on the sets $\mathcal{A}_1$ and $\mathcal{A}_2$ by showing how the endomorphism rings of some abelian surfaces in $\mathcal{A}_1$ can still be computed in subexponential time. We also discuss the limitation of lattice methods in computing the endomorphism rings of some abelian surfaces.

4.4 Extension and improvement of the lattice method

This section is taken from our paper [53]. We start by extending the result of Bisson, [14] by computing the endomorphism rings of some abelian surfaces in the set $\mathcal{A}_1$ in subexponential time. We note that the cases we cover were not computable with previous methods, [14, 110].

4.4.1 Computation of overorders

The computation of overorders of an order $\mathcal{O}$ in an étale $\mathbb{Q}$-algebra has been studied in [80]. The algorithm computes all subgroups of $\mathcal{O}_K/\mathcal{O}$ and finds the subgroups that correspond to overorders. The same technique is used in [14]. When the size of the group is "large", this method becomes infeasible, since the number of subgroups becomes too large. We present the method of [65] which is an improvement of that in [80].

4.4.1.1 Minimal overorders

The method in [65] can be applied to any semisimple algebra over a number field, but since our main interest is the computation of minimal overorders of a given order in a number field, we focus on number fields.

Definition 4.4.1.1. Let K be a number field.

- For any two subsets X, Y of K, we denote by $(X : Y)$ the set $\{x \in K | xY \subseteq X\}$. For orders $\mathcal{O}_1 \subseteq \mathcal{O}_2$ of K, we define the conductor of $\mathcal{O}_1$ in $\mathcal{O}_2$ as the set $(\mathcal{O}_1 : \mathcal{O}_2)$. The conductor $(\mathcal{O}_1 : \mathcal{O}_2)$ is the largest ideal of $\mathcal{O}_2$ contained in $\mathcal{O}_1$.
- An order $\mathcal{O}_2$ is said to be an p-overorder of $\mathcal{O}_1$, p a prime number, if the index $[\mathcal{O}_2 : \mathcal{O}_1]$ is a power of p.

We have the following:

Proposition 4.4.1.2. *[65, Propsition 5.2] Let $\mathcal{O}_2$ be a minimal overorder of $\mathcal{O}_1$. Then the following hold:*

- *The conductor $(\mathcal{O}_1 : \mathcal{O}_2)$ is a prime ideal $\mathfrak{P}$ of $\mathcal{O}_1$.*

- *We have* $\mathcal{O}_2 \subseteq (\mathfrak{P} : \mathfrak{P})$.
- *If* $\mathfrak{P} \cap \mathbb{Z} = (p)$, *then* p *is the unique prime divisor of* $[\mathcal{O}_2 : \mathcal{O}_1]$, *the index of* $\mathcal{O}_1$ *in* $\mathcal{O}_2$.

Proposition 4.4.1.3. *[65, Proposition 5.3] Let* $\mathcal{O}_2$ *be minimal overorder of* $\mathcal{O}_1$ *with conductor* $\mathfrak{P}$. *Then* $\mathcal{O}_2/\mathfrak{P}$ *is a two-dimensional* $\mathcal{O}_1/\mathfrak{P}$*-subspace of* $(\mathfrak{P} : \mathfrak{P})/\mathfrak{P}$ *or* $\mathcal{O}_1/\mathfrak{P} \subseteq \mathcal{O}_2/\mathfrak{P}$ *is an extension of finite fields of prime degree. Moreover, there are at most two prime ideals of* $\mathcal{O}_2$ *lying over* $\mathfrak{P}$.

In [65], Proposition 4.4.1.3 was used to compute minimal overorders. We do not describe it in details here and we refer the reader to the original paper. We are interested in the case where the order $\mathcal{O}$ is Gorenstein or Bass at prime $\mathfrak{P}$, in which case minimal overorders can be efficiently computed, Section 4.4.1.2. We apply this to the endomorphism ring computation and extend the method in [14], Section 4.4.

4.4.1.2 Gorenstein and Bass orders

Definition 4.4.1.4. [65, Section 5]

- An order $\mathcal{O}$ is Gorenstein at a prime ideal $\mathfrak{P} \subseteq \mathcal{O}$ if $\mathcal{O}/\mathfrak{P} \cong (\mathcal{O} : \mathfrak{P})/\mathcal{O}$ as $\mathcal{O}/\mathfrak{P}$-modules. The order $\mathcal{O}$ is said to be Gorenstein if it is Gorenstein at all of its prime ideals.
- An order $\mathcal{O}$ is Bass at a prime ideal $\mathfrak{P} \subseteq \mathcal{O}$ if $\mathcal{O}_K/\mathfrak{P}\mathcal{O}_K$ has $\mathcal{O}/\mathfrak{P}$-dimension at most 2. The order $\mathcal{O}$ is said to be Bass if it is Bass at all of its prime ideals.

The importance of Gorenstein orders comes from the following proposition.

Proposition 4.4.1.5. *[65, Section 5] If* $\mathcal{O}$ *is Gorenstein at* $\mathfrak{P}$ *and* $\mathcal{O} \neq (\mathfrak{P} : \mathfrak{P})$, *then* $(\mathfrak{P} : \mathfrak{P})$ *is the unique minimal overorder of* $\mathcal{O}$ *with conductor* $\mathfrak{P}$.

Remark 4.4.1.6.

- The definitions of Gorenstein rings and Bass rings are equivalent to the standard definitions, see [3, Theorem 6.3] and [63, 2.3 Theorem].

- If $\mathcal{O}$ is Bass, all its overorders are Gorenstein, [63, 2.3 Theorem]. This implies that each minimal overorder $\mathcal{O}'$ of $\mathcal{O}$ is of the form $(\mathfrak{P} : \mathfrak{P})$, for some prime $\mathfrak{P}$ of $\mathcal{O}$, [65, Proposition 5.21].

Proposition 4.4.1.7.

1. *The cost of checking whether an order is Gorenstein or Bass at a prime $\mathfrak{P}$ is at most polynomial in* $\log p$, $(p) = \mathfrak{P} \cap \mathbb{Z}$.

2. *The cost of computing the minimal overorder of a Gorenstein order $\mathcal{O}$ with conductor $\mathfrak{P}$ is at most polynomial in* $\log p$, $(p) = \mathfrak{P} \cap \mathbb{Z}$.

Proof. The operations that have to be performed, computing quotients of free $\mathbb{Z}$-modules, quotient ideals and dimensions of vector spaces, have at most polynomial time complexity as described in [76, Section 2]. □

Algorithm 15 `Computation of minimal overorders with conductor` $\mathfrak{P}$

Input: An order $\mathcal{O}$ in a number field K and a prime ideal $\mathfrak{P}$ in $\mathcal{O}$.

Output: Minimal overorders of $\mathcal{O}$ with conductor $\mathfrak{P}$

1: If $\mathcal{O}$ is Gorenstein at $\mathfrak{P}$ and $\mathcal{O} \neq (\mathfrak{P} : \mathfrak{P})$
2: $S_{\mathfrak{P}} \leftarrow \{(\mathfrak{P} : \mathfrak{P})\}$.
3: Return $S_{\mathfrak{P}}$
4: Else
5: Use [65, Algorithm 5.7-(ii)-(b)] to compute $S_{\mathfrak{P}}$, the set of minimal overorders of $\mathcal{O}$ with conductor $\mathfrak{P}$.
6: Return $S_{\mathfrak{P}}$.

We now apply these ideas to the computation of endomorphism of ordinary abelian varieties and extend the main result in [14].

4.4.1.3 Gorenstein and Bass orders in number fields

For the application to the computation of endomorphism rings of ordinary abelian surfaces, the number field is a primitive quartic CM-field K and the minimal order is $\mathbb{Z}[\pi, \bar{\pi}]$. We have the following:

Theorem 4.4.1.8. *The order $\mathbb{Z}[\pi, \bar{\pi}]$ is always Gorenstein.*

Proof. See [31, Theorem 11]. □

Theorem 4.4.1.8 shows that if the factorisation of $[\mathcal{O}_K : \mathbb{Z}[\pi, \bar{\pi}]]$ is known, the minimal overorders of $\mathbb{Z}[\pi, \bar{\pi}]$ can be computed in polynomial time in the logarithm of the largest prime factor dividing $v := [\mathcal{O}_K : \mathbb{Z}[\pi, \bar{\pi}]]$. We now show that the minimal order $\mathbb{Z}[\pi, \bar{\pi}]$ is Bass at any prime $\mathfrak{P}$, with $p = \mathfrak{P} \cap \mathbb{Z}$ and $\mathrm{val}_p(v) \leq 2$.

Proposition 4.4.1.9. *Let $\mathcal{O}$ be an order in a number field K and p a prime number such that the valuation of $[\mathcal{O}_K : \mathcal{O}]$ at p is 1. Then $\mathcal{O}$ is Bass at primes $\mathfrak{P}$, with $\mathfrak{P} \cap \mathbb{Z} = (p)$.*

Proof. The order $\mathcal{O}$ is Bass at $\mathfrak{P}$ if $\mathcal{O}_K/\mathfrak{P}\mathcal{O}_K$ has $\mathcal{O}/\mathfrak{P}$-dimension at most 2. As groups, we have $\mathcal{O}_K/\mathcal{O} \cong (\mathcal{O}_K/\mathfrak{P})/(\mathcal{O}/\mathfrak{P})$. We then have $|(\mathcal{O}_K/\mathfrak{P})| = wp|(\mathcal{O}/\mathfrak{P})|$, with $[\mathcal{O}_K : \mathcal{O}] = wp$, $(w, p) = 1$. We know that $|(\mathcal{O}/\mathfrak{P})| = p^\alpha$ for some $\alpha \geq 1$. It follows that $|\mathcal{O}_K/\mathfrak{P}\mathcal{O}_K| \leq p|\mathcal{O}/\mathfrak{P}| \leq |\mathcal{O}/\mathfrak{P}|^2$. Hence, the dimension of $\mathcal{O}_K/\mathfrak{P}$ as a $\mathcal{O}/\mathfrak{P}$-vector space is at most 2. □

Corollary 4.4.1.10. *The order $\mathbb{Z}[\pi, \bar{\pi}]$ is Bass at a prime $\mathfrak{P}$ if the valuation of $[\mathcal{O}_K : \mathbb{Z}[\pi, \bar{\pi}]]$ at p is at most 2, where $(p) = \mathbb{Z} \cap \mathfrak{P}$.*

Proof. From Theorem 4.4.1.8 we know that the minimal order $\mathbb{Z}[\pi, \bar{\pi}]$ is Gorenstein and the overorder $\mathcal{O}$ with conductor $\mathfrak{P}$ will be Bass since $[\mathcal{O}_K : \mathcal{O}]$ will have valuation at most 1 at $\mathbb{Z} \cap \mathfrak{P}$. □

We give some example showing that this is not a sufficient condition.

Example 4.4.1.11.

- *Let K be the CM-field with the defining polynomial, the Weil polynomail, $f = x^4 - 300x^3 + 38042x^2 - 2348700x + 61293241$ over $\mathbb{Q}$, with π a root of f and $\bar{\pi}$ its complex conjugate. Then we have $[\mathcal{O}_K : \mathbb{Z}[\pi, \bar{\pi}]] = 2^4 \cdot 5^3$. Consider the ideal $5\mathcal{O}_K = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3\mathfrak{P}_4$ and $2\mathcal{O}_K = \mathfrak{P}^2$. Let $\mathfrak{Q}_1 = \mathfrak{P}_1 \cap \mathbb{Z}[\pi, \bar{\pi}]$ and $\mathfrak{Q} = \mathfrak{P} \cap \mathbb{Z}[\pi, \bar{\pi}]$. We have $|\mathbb{Z}[\pi, \bar{\pi}]/\mathfrak{Q}| = 2$, $|\mathcal{O}_K/\mathfrak{Q}\mathcal{O}_K| = 4$, $|\mathbb{Z}[\pi, \bar{\pi}]/\mathfrak{Q}_1| = 5$ and $|\mathcal{O}_K/\mathfrak{Q}_1\mathcal{O}_K| = 25$. We see that even though the valuation of the index $[\mathcal{O}_K : \mathbb{Z}[\pi, \bar{\pi}]]$ at 2 and 5 is greater than 2, the order $\mathbb{Z}[\pi, \bar{\pi}]$ is still Bass at $\mathfrak{Q}$ and $\mathfrak{Q}_1$.*

- *Let K be the number field with defining polynomial $g = x^4 - 10x^3 - 9750x^2 - 56830x + 32296489$ over $\mathbb{Q}$ with π a root of g and $\bar{\pi}$ its complex conjugate. We have $[\mathcal{O}_K : \mathbb{Z}[\pi, \bar{\pi}]] = 2^2 \cdot 3^8$. Consider the ideal $3\mathcal{O}_K = \mathfrak{P}^2$, with $\mathfrak{P}$ a prime ideal. Let $\mathfrak{Q} = \mathfrak{P} \cap \mathbb{Z}[\pi, \bar{\pi}]$. We get $|\mathbb{Z}[\pi, \bar{\pi}]/\mathfrak{Q}| = 3$ and $|\mathcal{O}_K/\mathfrak{Q}\mathcal{O}_K| = 81$, which implies that the order $\mathbb{Z}[\pi, \bar{\pi}]$ is not Bass at $\mathfrak{Q}$.*

Theorem 4.4.1.12. *Let $\mathcal{A}/\mathbb{F}_q$ be an absolutely simple, principally polarized, and ordinary abelian surface with Frobenius endomorphism π and complex multiplication field K and $\tau > 0$. If the valuation of primes dividing $[\mathcal{O}_K : \mathbb{Z}[\pi, \overline{\pi}]]$ and greater than $L(q)^\tau$ is at most 2 then the endomorphism ring of $\mathcal{A}$ can be computed in subexponential time in q.*

Proof. Follow from Corollary 4.4.1.10. □

4.4.2 Computation of the endomorphism rings of some abelian surfaces in $\mathcal{A}_1$

We show how to extend the result in [14] by computing the endomorphism rings of some ordinary abelian surfaces belonging to the set $\mathcal{A}_1$ of abelian varieties that have been excluded in [14] and [110]. The set $\mathcal{A}_1$ is the set of ordinary abelian surfaces defined over finite fields such that $[\mathcal{O}_K : \mathbb{Z}[\pi, \bar{\pi}]]$ has valuation greater than 1 at prime numbers $p > L(q)^\tau$ for some $\tau > 0$, where K is the CM-field of the Abelian variety, π the Frobenius element and q the cardinality of their base field. This set was discarded because the computation of overorders locally at those primes can be exponential in $\log(q)$.

With our method, when an order is Bass or Gorenstein at primes above p, the complexity of computing the minimal overorders locally at p is at most polynomial in $\log p$. In fact, the p-minimal overorders are of the form $(\mathfrak{P} : \mathfrak{P})$, for each $\mathfrak{P}$ above p, which are at most four. Computing those overorders uses at most polynomial time in $\log p$. Hence any abelian variety with $[\mathcal{O}_K : \mathbb{Z}[\pi, \bar{\pi}]]$ having valuation 2 at large primes can be handled with the method. Those are not the only cases that our method covers. As mentioned in Example 4.4.1.11 the valuation of the index at a prime number can be greater than 2 and the order will still be Bass at prime ideals above that prime number.

We can then add a step in the algorithm that checks whether the order is Bass or Gorenstein at a prime ideal and if that the case the overorders can be computed efficiently.

Here is the algorithm:

Algorithm 16 `Computation of endomorphism ring`

Input: An absolutely simple, ordinary, principally polarized abelian variety $\mathcal{A}$ of dimension 2 defined over a field with q elements, $\tau > 0$.

Output: Order isomorphic to the endomorphism ring of $\mathcal{A}$.

1: Compute the Frobenius polynomial $\chi_{\mathcal{A}}$ of $\mathcal{A}$.
2: Factor the discriminant D of $\chi_{\mathcal{A}}$ and construct the order $\mathcal{O}' = \mathbb{Z}[\pi, \bar{\pi}]$.
3: For $\mathfrak{P}$ a prime ideal of $\mathcal{O}'$, $(p) = \mathfrak{P} \cap \mathbb{Z}$, with p divisor of $[\mathcal{O}_K : \mathcal{O}']$:
4: If $\mathcal{O}'$ is not Gorenstein at $\mathfrak{P}$ and $p > L(q)^{\tau}$, STOP.
5: Else
6: Compute the set $S_{\mathfrak{P}}$ of minimal overorders of $\mathcal{O}'$ with conductor $\mathfrak{P}$ using Algorithm 15.
7: For $\mathcal{O}$ in $S_{\mathfrak{P}}$:
8: If $\mathcal{O} \subseteq \mathrm{End}(\mathcal{A})$ set $\mathcal{O}' \leftarrow \mathcal{O}$ and go to Step 3.
9: Compute $\mathrm{End}(\mathcal{A})$ locally at "small" prime as described in [14, Section 7].

Algorithm 16 does not cover all cases and for some abelian varieties, even if all the overorders can be computed efficiently, the lattice method (method used in [12, 14]) cannot compute all endomorphism rings in subexponential time. We discuss that in Section 4.5.

4.4.2.1 Practical computations

We used the library AVIsogenies, [15], to compute isogenies and the package Nemo/Hecke, [52], for overorders computations.

We consider the Jacobian variety $\mathcal{A}$ of the hyperelliptic curve with equation

$$y^2 = x^5 + 5x^4 + 6x^2 + 1$$

over the field $\mathbb{F}_q$, $q = 7^{11}$. The characteristic polynomial of its Frobenius endomorphism is given by $x^4 + 2465522390x^2 + q^2$ and the index $[\mathcal{O}_K : \mathbb{Z}[\pi, \bar{\pi}]] = 2^3 \cdot 7877^2 \cdot 40063^2$.

There are 24 overorders of $\mathbb{Z}[\pi, \bar{\pi}]$ in $\mathcal{O}_K$. It takes only few seconds to compute them. In fact, as proved in Theorem 4.4.1.10 the ring $\mathbb{Z}[\pi, \bar{\pi}]$ is Bass at 7877 and 40063. There are three 7877-overorders and only one 40063-overorder. The exponential method in [49] to compute the endomorphism rings can be used to compute $\mathrm{End}(\mathcal{A})$ locally at 2. It turns out that the endomorphism ring is locally minimal at 2. We have $3\mathcal{O}_K = \mathfrak{p}^2$, with $\mathfrak{p}$

principal. However, the image of the 3-isogeny is found not to be isomorphic to $\mathcal{A}$. It then follows that $\mathrm{End}\,\mathcal{A}$ is not $\mathcal{O}_K$. The ideal $5\mathbb{Z}[\pi,\bar{\pi}] = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$ with $\mathfrak{p}_1\mathfrak{p}_2$ being a relation in $\mathrm{End}(\mathcal{A})$ but not for $\mathbb{Z}[\pi,\bar{\pi}]$ and all orders locally minimal at 40063. This implies that $\mathrm{End}\,\mathcal{A}$ is locally maximal at 40063. Finally the ideal $31\mathcal{O}_K = \mathfrak{q}_1\mathfrak{q}_2$, and both ideals $\mathfrak{q}_1, \mathfrak{q}_2$ are principal in the endomorphism ring (they are both relations in the isogeny graph). They are not principal in the orders not maximal at 7877. We the conclude that the endomorphism ring of $\mathcal{A}$ is the overorder of $\mathbb{Z}[\pi,\bar{\pi}]$ with index 2^3 in the maximal order $\mathcal{O}_K$. We have

$$\mathrm{End}\,(\mathcal{A}) = \mathbb{Z}\left[1, \pi, \frac{\pi^2 + 601608693}{7877 \cdot 40063}, \frac{\pi^2 + q\pi + 1411816807777155131 + 1232761195 \cdot \overline{\pi}}{7877 \cdot 40063 \cdot \overline{\pi}}\right].$$

The narrow class number of the ring of integers of the totally real subfield is 2 which implies that the method in [110] cannot be used, since it only works when the the narrow class number of the ring of integers of the totally real subfield is 1.

Algorithm 14 checks whether the set of relations of a given order $\mathcal{O}$ is contained in the endomorphism ring of some abelian surface with a failure probability. We show how to avoid this failure probability and also make the algorithm fast.

4.4.3 Improvement of computation of endomorphism rings

We show that in the computation of endomorphism rings of abelian surfaces, we do not need to compute many relations and that only one relation is enough to check whether the relation lattice of an order is contained in that of another order. With that relation, Algorithm 14 always returns the correct output. We also show how this particular relation can be computed.

Let $\mathcal{A}/\mathbb{F}_q$ be a principally polarized, absolutely simple and ordinary abelian surface with Frobenius endomorphism π and CM-field and CM-type (K, Φ).

We focus on quartic non-biquadratic CM-fields, as they correspond to the CM-fields of principally polarized, absolutely simple and ordinary abelian surfaces. We let K be a quartic non-biquadratic CM-field.

Lemma 4.4.3.1. *[16, Lemma 7] Let $\mathcal{O} \subset \mathcal{O}'$ be orders in K. Denote by ϕ the natural morphism $\mathfrak{C}(\mathcal{O}) \to \mathfrak{C}(\mathcal{O}')$ as defined in Lemma 4.3.3 and consider the relative norm*

$$\psi : \frac{(\mathcal{O}'/f\mathcal{O}_K)^\times}{(\mathcal{O}/f\mathcal{O}_K)^\times \mu_{\mathcal{O}'}} \to \frac{(\mathcal{O}'_0/f\mathcal{O}_{K_0})^\times}{(\mathcal{O}_0/f\mathcal{O}_{K_0})^\times},$$

where $f = [\mathcal{O}_K : \mathcal{O}]$ *and* $\mu_{\mathcal{O}'}$ *the group of roots of unity. We have* $\ker\phi = \ker\psi$ *and* $\operatorname{coker}\phi \subset \operatorname{coker}\psi$.

We have $\mu_{\mathcal{O}'} = \{\pm 1\}$, unless $\mathcal{O} = \mathbb{Z}[\zeta_5]$ in which case $\mu_{\mathbb{Z}[\zeta_5]}$ has 10 elements.

The relations that hold in $\mathfrak{C}(\mathcal{O}')$ but not in $\mathfrak{C}(\mathcal{O})$ are given by elements in the kernel of ϕ.

Theorem 4.4.3.2. *Let* $\mathcal{O}$ *and* $\mathcal{O}'$ *be orders in* K *and the map* $\phi_1 : \mathfrak{C}(\mathcal{O}\cap\mathcal{O}') \to \mathfrak{C}(\mathcal{O})$ *and* $\phi_2 : \mathfrak{C}(\mathcal{O}\cap\mathcal{O}') \to \mathfrak{C}(\mathcal{O}')$ *be the natural morphisms. Then we have* $\ker\phi_1 \cap \ker\phi_2$ *is the trivial group.*

Proof. Let $\mathcal{O}_1 = \mathcal{O}\cap\mathcal{O}'$. We show that

$$\frac{(\mathcal{O}/f\mathcal{O}_K)^\times}{(\mathcal{O}_1/f\mathcal{O}_K)^\times\mu_{\mathcal{O}}} \cap \frac{(\mathcal{O}'/f\mathcal{O}_K)^\times}{(\mathcal{O}_1/f\mathcal{O}_K)^\times\mu_{\mathcal{O}'}}$$

is the trivial group. The natural maps

$$i_{\mathcal{O}} : \frac{((\mathcal{O}/f\mathcal{O}_K)^\times}{(\mathcal{O}_1/f\mathcal{O}_K)^\times\mu_{\mathcal{O}}} \to \frac{(\mathcal{O}_K/f\mathcal{O}_K)^\times}{(\mathcal{O}_1/f\mathcal{O}_K)^\times\mu_{(\mathcal{O}_K}}$$
$$i_{\mathcal{O}'} : \frac{((\mathcal{O}'/f\mathcal{O}_K)^\times}{(\mathcal{O}_1/f\mathcal{O}_K)^\times\mu_{\mathcal{O}'}} \to \frac{(\mathcal{O}_K/f\mathcal{O}_K)^\times}{(\mathcal{O}_1/f\mathcal{O}_K)^\times\mu_{(\mathcal{O}_K}}$$

are injective by the proof of [16, Proposition 9]. In the same proof it is shown that $\operatorname{Im}(i_{\mathcal{O}'}) \cap \operatorname{Im}(i_{\mathcal{O}})$ is the trivial group. From Lemma 4.4.3.1, we have that $\ker\phi_1$ is a subgoup of $\dfrac{(\mathcal{O}/f\mathcal{O}_K)^\times}{(\mathcal{O}_1/f\mathcal{O}_K)^\times\mu_{\mathcal{O}}}$ and $\ker\phi_2$ is a subgroup of $\dfrac{(\mathcal{O}'/f\mathcal{O}_K)^\times}{(\mathcal{O}_1/f\mathcal{O}_K)^\times\mu_{\mathcal{O}'}}$ and this proves the claim that $\ker\phi_1 \cap \ker\phi_2$ is the trivial group. □

From this theorem we prove the following:

Theorem 4.4.3.3. *Let* $\mathcal{A}/\mathbb{F}_q$ *be a principally polarized, absolutely simple and ordinary abelian variety with Frobenius endomorphism* π. *Let* $\mathcal{O} \supset \mathbb{Z}[\pi,\overline{\pi}]$ *be an order and* R *a relation in* $\mathcal{O}$ *which does not hold in any order strictly contained in* $\mathcal{O}$ *and contained in* $\operatorname{End}(\mathcal{A})$. R *holds in* $\operatorname{End}(\mathcal{A})$ *if and only if the set of relations of* $\mathcal{O}$ *is contained in the set of relations of* $\operatorname{End}(\mathcal{A})$.

Proof. If the set of relations of $\mathcal{O}$ is contained in the set of relations of $\operatorname{End}(\mathcal{A})$, then R holds in $\operatorname{End}(\mathcal{A})$. Now assume that R holds in $\operatorname{End}(\mathcal{A})$ and let $\phi_1 : \mathfrak{C}(\mathcal{O}\cap\operatorname{End}(\mathcal{A})) \to \mathfrak{C}(\mathcal{O})$ and $\phi_2 : \mathfrak{C}(\mathcal{O}\cap\operatorname{End}(\mathcal{A})) \to \mathfrak{C}(\operatorname{End}(\mathcal{A}))$. We know from Theorem 4.4.3.2 that $\ker\phi_1\cap\ker\phi_2$

is the trivial group. If we assume that there is a relation R' that is a relation of $\mathcal{O}$ but not in $\mathrm{End}(\mathcal{A})$ then we have that R' is not a relation of $\mathcal{O} \cap \mathrm{End}(\mathcal{A})$. It follows that R' is a nontrivial element in $\ker \phi_1$ and that $\mathrm{End}(\mathcal{A}) \cap \mathcal{O} \subsetneq \mathcal{O}$. Hence R is a nontrivial element of $\ker \phi_1$ and also of $\ker \phi_2$. This is a contradiction because $\ker \phi_1 \cap \ker \phi_2$ is the trivial group. □

Corollary 4.4.3.4. *Let $\mathcal{A}/\mathbb{F}_q$ be a principally polarized, absolutely simple and ordinary abelian surface with Frobenius endomorphism π and $\mathcal{O}$ an order in K, $\mathcal{O}'$ a minimal overorder of $\mathcal{O}$ with $\mathcal{O} \subset \mathrm{End}(\mathcal{A})$. Then $\Lambda_{\mathcal{O}'} \subset \Lambda_{\mathrm{End}(\mathcal{A})}$ if and only if $\Lambda_{\mathcal{O}'} = \Lambda_{\mathcal{O}}$ or a relation of $\mathcal{O}'$ that is not a relation in $\mathcal{O}$ is a relation of $\mathrm{End}(\mathcal{A})$.*

Proof. We know that $\Lambda_{\mathcal{O}} \subset \Lambda_{\mathcal{O}'}$ by Lemma 4.3.3. If $\Lambda_{\mathcal{O}'} \subset \Lambda_{\mathrm{End}(\mathcal{A})}$, then either $\Lambda_{\mathcal{O}'} = \Lambda_{\mathcal{O}}$ or a relation of $\mathcal{O}'$ that is not a relation in $\mathcal{O}$ is a relation of $\mathrm{End}(\mathcal{A})$. If $\Lambda_{\mathcal{O}'} = \Lambda_{\mathcal{O}}$, then $\Lambda_{\mathcal{O}'} \subset \Lambda_{\mathrm{End}(\mathcal{A})}$. Now assume that $\Lambda_{\mathcal{O}'} \supsetneq \Lambda_{\mathcal{O}}$ and let R be a relation of $\mathcal{O}'$ that is not a relation in $\mathcal{O}$. Then by Theorem 4.4.3.3, if R is a relation of $\mathrm{End}(\mathcal{A})$ then $\Lambda_{\mathcal{O}'} \subset \Lambda_{\mathrm{End}(\mathcal{A})}$. □

Now we show how we can find a relation of $\mathcal{O}$ that is not a relation in any other suborder of $\mathcal{O}$.

Let $\mathcal{O}'$ be a minimal overorder of $\mathcal{O}$. Then there is a prime number p such that $[\mathcal{O}' : \mathcal{O}] = p^\alpha$ for some $\alpha > 0$ and

$$\frac{(\mathcal{O}'/f\mathcal{O}_K)^\times}{(\mathcal{O}/f\mathcal{O}_K)^\times \mu_{\mathcal{O}'}} \cong \frac{(\mathcal{O}'/p^\alpha\mathcal{O}')^\times}{(\mathcal{O}/p^\alpha\mathcal{O})^\times \mu_{\mathcal{O}'}}.$$

The computation of the multiplicative group of residue class rings of orders was studied by Klüners and Pauli in [70].

Let $\mathcal{A}/\mathbb{F}_q$ be a principally polarized, absolutely simple and ordinary abelian surface with Frobenius endomorphism π. In order to compute $\mathrm{End}(\mathcal{A})$, we start by computing the minimal overorders of $\mathbb{Z}[\pi, \overline{\pi}]$ that are stable under complex conjugation and check if one of them is contained in the endomorphism ring by using relations. If we find one, we repeat the process starting with that order. It is worth noting that all relations in $\mathbb{Z}[\pi, \overline{\pi}]$ are relations of $\mathrm{End}(\mathcal{A})$, since $\mathbb{Z}[\pi, \overline{\pi}] \subset \mathrm{End}(\mathcal{A})$ and we do not need to check whether they hold in the endomorphism ring. In Algorithm 14, the $20 \log q$ relations are random relations and they do not exclude the already known cases. By Corollary 4.4.3.4, only

one relation is enough for each order. For $\mathcal{O}'$ a minimal overorder of an order $\mathcal{O}$ with $\mathcal{O} \subset \mathrm{End}(\mathcal{A})$, any non trivial element of the kernel of ψ,

$$\psi : \frac{(\mathcal{O}'/f\mathcal{O}_K)^\times}{(\mathcal{O}/f\mathcal{O}_K)^\times \mu_{\mathcal{O}'}} \to \frac{(\mathcal{O}'_0/f\mathcal{O}_{K_0})^\times}{(\mathcal{O}_0/f\mathcal{O}_{K_0})^\times},$$

gives rise to a relation of $\mathcal{O}'$ that is not a relation of $\mathcal{O}$. If the kernel itself is trivial, then we can conclude that $\mathcal{O}$ and $\mathcal{O}'$ have the same set of relations.

Suppose that $\ker\psi$ is nontrivial and let $\alpha \in \ker\psi$ be a non trivial element. Then the element $(\alpha\mathcal{O}', \alpha\overline{\alpha})$ is trivial in $\mathfrak{C}(\mathcal{O}')$ but we have $(\alpha\mathcal{O}')\cap\mathcal{O}$ is not principal. The computation of a short relation equivalent to $(\alpha\mathcal{O}', \alpha\overline{\alpha})$ can be obtained by adapting Algorithm [34, Algorithm 1] and the corresponding isogeny is easily computed. We obtain the following algorithm:

Algorithm 17 `Checking whether` $\Lambda_\Phi(\mathcal{O}') \subseteq \Lambda_\Phi(\mathrm{End}(\mathcal{A}))$

Input: A principally polarized, absolutely simple and ordinary abelian variety $\mathcal{A}/\mathbb{F}_q$ with CM-pair (K, Φ) and orders $\mathcal{O}, \mathcal{O}'$ with $\mathcal{O} \subset \mathrm{End}(\mathcal{A})$ and $\mathcal{O}'$ a minimal overorder of $\mathcal{O}$.

Output: Whether $\Lambda_\Phi(\mathcal{O}') \subseteq \Lambda_\Phi(\mathrm{End}(\mathcal{A}))$.

1: If $\ker\psi$ is trivial or of exponent 2.
2: Return true.
3: Else:
4: Get a relation R of $\mathcal{O}'$ that is not a relation of $\mathcal{O}$, from an element $a \in \ker\psi$ with a^2 not trivial.
5: Get a smooth representative of $R \cap \mathcal{O}$ in $\mathfrak{C}(\mathcal{O})$ and the corresponding smooth relation, R', in $\mathfrak{C}(\mathcal{O}')$.
6: If $N_{\Phi^r}(N_\Phi(R'))$ does not hold in $\mathrm{End}(\mathcal{A})$, return false.
7: Return true.

Theorem 4.4.3.5. *The output of Algorithm 17 is always correct.*

Proof. By [16, Lemma 6], for an order $\mathcal{O}$, all squares of elements of $\mathfrak{C}(\mathcal{O})$ are images of the map $N_{\Phi^r} \circ N_\Phi$. This means that if $\ker\psi$ has exponent at most 2, relations of $\mathcal{O}'$ are either relations of $\mathcal{O}$ or their images under $N_{\Phi^r} \circ N_\Phi$ are relations in $\mathcal{O}$. Hence if $\ker\psi$ has exponent at most 2 we have $\Lambda_\Phi(\mathcal{O}') = \Lambda_\Phi(\mathcal{O}) \subseteq \Lambda_\Phi(\mathrm{End}(\mathcal{A}))$. If the exponent of $\ker\psi$ is greater than 2, we can find an element, say a, whose square is nontrivial. The relation $N_{\Phi^r}(N_\Phi(R))$ associated to a^2 will be a relation in $\mathcal{O}'$ that is not a relation in

$\mathcal{O}$. From Corollary 4.4.3.4 we know that using that relation is enough to check whether $\Lambda_\Phi(\mathcal{O}') \subseteq \Lambda_\Phi(\mathrm{End}(\mathcal{A}))$ and all the isogenies in the isogeny chain are (ℓ, ℓ)-isogenies. □

Algorithm 17 can replace Algorithm 14 in the computation of endomorphism rings of abelian surfaces. The latter algorithm performs similar computation but does not always output the correct result. It comes with a probability of failure. Algorithm 17 generates only one relation and Algorithm 14 polynomially many relations (polynomial in $\log q$) and that makes Algorithm 17 faster in practice.

Theorem 4.4.3.6. *Let $\mathcal{A}/\mathbb{F}_q$ be a principally polarized, absolutely simple and ordinary abelian surface. Under the same assumption as in Theorem 4.3.3.4, if Algorithm 17 is used in Algorithm 12, the output of Algorithm 12 is always correct.*

Proof. Once Algorithm 17 is unconditionally correct, Algorithm 12 will also be correct. □

Theorem 4.4.3.7. *Under the same assumption as in Theorem 4.3.3.4, Algorithm 17 determines whether the lattice of relations of* $\mathrm{End}(\mathcal{A})$ *contains that of an order $\mathcal{O}$ using $L(q)^{2\sqrt{3}+o(1)}$ operations in the base field.*

Proof. It takes $L(q)^{2\sqrt{3}+o(1)}$ operations in the base field to obtain a relation and compute the associated isogeny and those are the dominant steps in the algorithm. Hence the complexity of the algorithm is $L(q)^{2\sqrt{3}+o(1)}$. □

Although we were able to remove the probability of failure in the main algorithm in [14], in the next subsequent sections, we present some limitation of the lattice method by providing families of varieties whose endomorphism rings cannot be computed in subexponential time with current methods.

4.5 Limitation of current methods

This section is dedicated to the limitation of current methods. We show that unless new approaches are developed, the endomorphism rings of some abelian surfaces will not be computable in subexponential time.

4.5.1 Exponentially many minimal overorders

The result presented in this section are published in [53].

Even under the assumption that orders can be distinguished using their polarized class group, current methods for computing endomorphism rings due to [14] are subexponential only by restricting to varieties, where the computation of overorders of $\mathbb{Z}[\pi.\bar{\pi}]$ locally can be performed in subexponential time. In [14] this is achieved by restricting to varieties with $[\mathcal{O}_K : \mathbb{Z}[\pi, \bar{\pi}]]$ not divisible by squares of large primes. In this section we show that given a CM-field K of degree ≥ 4 and prime power $q = p^m$, $m > 4$, there exists an order with $\Omega(p)$ many minimal p-overorders which are invariant under complex conjugation. Using Honda–Tate theory we obtain families of absolutely simple, principally polarized, ordinary abelian varieties over finite fields $\mathbb{F}_q$, for which current lattice based methods for computing the endomorphism ring have exponential complexity.

Let K be a CM-field of degree n with complex conjugation $\sigma : K \to K$. We first show that for every odd prime p, there is a σ-invariant order $\mathcal{O}$ that has $\Omega(p)$ many σ-invariant minimal p-overorders.

Lemma 4.5.1. *[20, Lemma 1.4] Let $\mathcal{O}$ be an order of K. Every additive subgroup G of $\mathcal{O}$ that satisfies $\mathbb{Z} + m^2\mathcal{O} \subseteq G \subseteq \mathbb{Z} + m\mathcal{O}$ for some integer $m \in \mathbb{Z}$ is an order.*

Corollary 4.5.2. *The order $\mathbb{Z} + p^2\mathcal{O}$ has $(p^{n-1} - 1)/(p - 1) = \Omega(p^{n-2})$ many minimal p-overorders contained in $\mathbb{Z} + p\mathcal{O}$.*

Proof. Lemma 4.5.1 implies that all subspaces of $(\mathbb{Z} + p\mathcal{O})/(\mathbb{Z} + p^2\mathcal{O})$ yield overorders of $\mathbb{Z} + p\mathcal{O}$ and it is clear that the minimal overorders of $\mathbb{Z} + p^2\mathcal{O}$ contained in $\mathbb{Z} + p\mathcal{O}$ correspond to the one-dimensional $\mathbb{F}_p$-subspaces of $(\mathbb{Z} + p\mathcal{O})/(\mathbb{Z} + p^2\mathcal{O})$. □

Note that as $n \geq 4$, this implies that $\mathbb{Z} + p^2\mathcal{O}$ has at least $\Omega(p^2)$ minimal p-overorders. However, in the context of computing the endomorphism rings of principally polarized abelian varieties, we are only interested in orders that are invariant under σ. It could be the cases, that the number of σ-invariant minimal overorders is much smaller than $\Omega(p)$. We show that for $n \geq 4$, the number of σ-invariant minimal overorders is $\Omega(p)$.

Lemma 4.5.3. *Assume that $\mathcal{O}$ is a σ-invariant order of K. The order $\mathbb{Z} + p^2\mathcal{O}$ has at least $\Omega(p^{\lceil (n-1)/2 \rceil - 1})$ many σ-invariant minimal p-overorders contained in $\mathbb{Z} + p\mathcal{O}$.*

Proof. First note that both $\mathbb{Z} + p\mathcal{O}$ and $\mathbb{Z} + p^2\mathcal{O}$ are σ-invariant. The orders under consideration correspond to σ-invariant $\mathbb{F}_p$-subspaces of $(\mathbb{Z} + p\mathcal{O})/(\mathbb{Z} + p^2\mathcal{O})$, that is, to $\mathbb{F}_p[G]$-submodules of $(\mathbb{Z}+p\mathcal{O})/(\mathbb{Z}+p^2\mathcal{O})$, where $G = \langle\sigma\rangle = \{1, \sigma\}$. Here $\mathbb{F}_p[G]$ denotes the group algebra of G over $\mathbb{F}_p$. As $\gcd(p, |G|) = 1$, Maschke's theorem, [74, Chapter $XVIII$, Theorem 1.2], asserts that the group algebra $\mathbb{F}_p[G]$ is semisimple. Now $\mathbb{F}_p[G]$ has exactly two (absolutely) irreducible modules V^+, V^-, which are both of $\mathbb{F}_p$-dimension 1. Hence as an $\mathbb{F}_p[G]$-module we have $(\mathbb{Z} + p\mathcal{O})/(\mathbb{Z} + p^2\mathcal{O}) \cong V_+^{n_+} \bigoplus V_-^{n_-}$ with $n_+, n_- \in \mathbb{Z}_{\geq 0}$ and $n_+ + n_- = n - 1$. In particular we have either $n_+ \geq \lceil (n-1)/2 \rceil$ or $n_- \geq \lceil (n-1)/2 \rceil$. Now $V_+^{n_+}$ has $(p^{n_+} - 1)/(p - 1) = \Omega(p^{n_+ - 1})$ many one-dimensional $\mathbb{F}_p[G]$-submodules, and similar for V_-^{n-1}. Hence $(\mathbb{Z} + p\mathcal{O})/(\mathbb{Z} + p^2\mathcal{O})$ has at least $\Omega(p^{\lceil (n-1)/2) \rceil - 1})$ many one-dimensional $\mathbb{F}_p[G]$-submodules. □

We note that as $n \geq 4$, this implies that $\mathbb{Z} + p^2\mathcal{O}$ has at least $\Omega(p)$ minimal p-overorders which are σ-invariant. We now show that orders of the type $\mathbb{Z} + p^2\mathcal{O}$ can be the endomorphism ring of a principally polarized abelian variety.

Theorem 4.5.4. *Let K be a CM-field of degree ≥ 4 and p an odd prime. There is a q-Weil number π, where $q = p^m$, $m > 4$, is a prime power and an order $\mathcal{O} \supseteq \mathbb{Z}[\pi, \bar{\pi}]$, stable under complex conjugation, such that $\mathcal{O}$ has at least $\Omega(p)$ many minimal p-overorders invariant under complex conjugation.*

Proof. Let K be a CM-field of degree $n = 4$ and let τ be any q-Weil number, where $q = p^{m_1}$ is a prime power. We choose $R = \mathbb{Z}[\tau, \bar{\tau}]$. The order R is invariant under complex conjugation and thus $\mathbb{Z} + p^2\mathbb{Z}[\tau, \bar{\tau}]$ has at least $\Omega(p^{\lceil (n-1)/2 \rceil - 1}) = \Omega(p)$ many minimal p-overorders by Lemma 4.5.3. Now let $\mathcal{O} = \mathbb{Z} + p^2\mathbb{Z}[\tau, \bar{\tau}]$. We note that $p^2\mathbb{Z}[\tau, \bar{\tau}] \subseteq \mathcal{O}$, which implies, $\pi, \bar{\pi} \subseteq \mathcal{O}$, where $\pi = p^2\tau$. But π is also a Weil number, more precisely, π is a p^{4+m_1}-Weil number. Thus $\mathcal{O}$ is an order, which is invariant under complex conjugation and which contains $\mathbb{Z}[\pi, \bar{\pi}]$ for some Weil number π. □

Corollary 4.5.5. *For each odd prime power $q = p^m$, $m > 4$ and quartic CM-field K, there exists a principally polarized, absolutely simple abelian surface $\mathcal{A}$ with Frobenius endomorphism $\pi \in K$, such that there exists an order $\mathbb{Z}[\pi, \bar{\pi}] \subseteq \mathcal{O}$ with the following properties:*

1. *$\mathcal{O}$ is the endomorphism ring of $\mathcal{A}$,*

2. *The order $\mathcal{O}$ has $\Omega(p)$ many minimal p-overorders invariant under complex conjugation.*

Proof. From Honda–Tate theory we know that the orders containing the minimal order $\mathbb{Z}[\pi, \bar{\pi}]$ are the endomorphism rings of some abelian varieties. Those that contain $\mathbb{Z}[\pi, \bar{\pi}]$ and are invariant under complex conjugation correspond to the endomorphism rings of principally polarized abelian varieties. So there is a principally polarized, absolutely simple abelian variety with endomorphism ring isomorphic to $\mathcal{O}$. The claim follows. □

Assume that $q = p^5$ is an odd prime power, K a quartic CM-field, and $\mathcal{O}$ the order and $\mathcal{A}$ the abelian surface with Frobenius endomorphism π as in Corollary 4.5.5. We claim that any lattice method for computing $\mathrm{End}(A)$ that works by computing overorders starting at $\mathbb{Z}[\pi, \bar{\pi}]$ has exponential complexity in $\log(q)$. Indeed, once the order $\mathcal{O}$ is found, to verify that $\mathcal{O}$ is indeed the endomorphism ring, we have to verify that locally at p, the endomorphism ring is not contained in any of the p-overorders of $\mathcal{O}$. As there are $\Omega(p)$ minimal p-overorders of $\mathcal{O}$ which are invariant under complex conjugation, and p is exponential in $\log(q)$ considering all relevant minimal p-overorders of $\mathcal{O}$ is thus exponential in $\log(q)$.

We want to mention that the method in [110] is not applicable to abelian surfaces provided by Corollary 4.5.5. The assumptions in [110] include that the endomorphism ring contains the maximal order of the totally real subfield of the CM-field. This implies that the endomorphism ring cannot have an exponential number of overorders locally at a prime, which follows from the following observations.

Proposition 4.5.6. *Let K be a CM-field of degree n with maximal real subfield K_0 and $\mathcal{O}$ an order of K.*

1. *If $\mathcal{O}$ is a Gorenstein order and p a prime divisors of $[\mathcal{O}_K : \mathcal{O}]$, then $\mathcal{O}$ has at most n minimal p-overorders.*

2. *If $\mathcal{O}$ contains $\mathcal{O}_{K_0}$, then $\mathcal{O}$ is Gorenstein.*

Proof.

1. Since the order is Gorenstein, the minimal overorders correspond to $(\mathfrak{P} : \mathfrak{P})$, where the $\mathfrak{P}$'s are prime ideals above primes dividing $[\mathcal{O}_K : \mathcal{O}]$. We have at most n of such prime ideals for each prime dividing $[\mathcal{O}_K : \mathcal{O}]$.

2. Follows from [24, Lemma 4.4].

□

Thus we immediately obtain:

Corollary 4.5.7. *If $\mathcal{A}$ is an abelian surface from Corollary 4.5.5 with Frobenius endomorphism $\pi \in K$, then* $\mathrm{End}(A)$ *does not contain $\mathcal{O}_{K_0}$. In particular, the algorithm of [110] is not applicable to $\mathcal{A}$.*

To the best of our knowledge, these are the two subexponential methods that compute endomorphism rings of principally polarized, absolutely simple, and ordinary abelian surfaces. It is worth noting that this limitation is not only restricted to abelian surfaces (as Theorem 4.5.4 is not restricted to quartic fields). In fact, in higher dimensions, any method that is based on the lattice method like in [14] will not be able to cover all cases. This doesn't happen for elliptic curves because imaginary quadratic orders are uniquely determined by their conductors and so we cannot have many minimal overorders locally at a prime. In higher dimensions this is not the case.

With recent developments in isogeny computation, any isogeny corresponding to an element of the polarized class group can be computed. However, we show in Section 4.5.2 that this does really not affect or improve the subexponential algorithms. In fact, we use the work of Bisson and Streng, [16], to indicate that even if we can compute all relations and their associated isogenies, instead of relations coming from the reflex type norm, there will still be an infinite number of cases where orders cannot be separated by the use of relations in subexponential time.

4.5.2 Indistinguishable orders

We show that if we assume that all isogenies can be efficiently computed, the set $\mathcal{A}_2$ will still have to be excluded and so the restriction was not due to lack of isogeny computation techniques.

We recall that in the work of Bisson, [14], the isogenies used in the algorithm were the (ℓ, ℓ)-isogenies and this led him to consider specific types of relations, namely those coming from the reflex type norm. In [16], he and Streng studied the extend to which

these relations can efficiently tell orders apart in a quartic CM-field and they derived Theorem 4.3.1.1.

We first check to what extend the full set of relations can tell orders apart.

Let $\mathcal{O}$ and $\mathcal{O}'$ be orders in a non-biquadratic CM-field K and let $\mathcal{O}'' = \mathcal{O} \cap \mathcal{O}'$. Assume that $\Lambda_{\mathcal{O}} \subset \Lambda_{\mathcal{O}'}$ and let $\phi : \mathfrak{C}(\mathcal{O}'') \to \mathfrak{C}(\mathcal{O})$.

Proposition 4.5.2.1. *We have* $\ker \phi$ *is trivial.*

Proof. We have $\ker \phi \subset \ker(\mathfrak{C}(\mathcal{O}'') \to \mathfrak{C}(\mathcal{O})) \cap \ker(\mathfrak{C}(\mathcal{O}'') \to \mathfrak{C}(\mathcal{O}'))$, because $\Lambda_{\mathcal{O}} \subset \Lambda_{\mathcal{O}'}$. But we have seen in Theorem 4.4.3.2 that $\ker(\mathfrak{C}(\mathcal{O}'') \to \mathfrak{C}(\mathcal{O})) \cap \ker(\mathfrak{C}(\mathcal{O}'') \to \mathfrak{C}(\mathcal{O}'))$ is trivial. □

Lemma 4.5.2.2. *Let* $v = \mathrm{val}_p([\mathcal{O} : \mathcal{O}'']/[\mathcal{O}_0 : \mathcal{O}''_0])$. *Then we have* $p^{v-6}(p-1)^6 \leq 2^{-1}|\mu_{\mathcal{O}}|$. *If* $\mathcal{O} \neq \mathbb{Z}[\zeta_5]$, *then if* $p = 2$, $v \leq 6$ *and if* $p = 3$, $v \leq 2$. *Otherwise if* $\mathcal{O} = \mathbb{Z}[\zeta_5]$, *then for* $p = 2$, $v \leq 8$, *for* $p = 3$, $v \leq 3$, *for* $p = 5$, $v \leq 1$, *and for* $p = 7$, $v \leq 1$.

In general if $v \geq 1$, *then* $p \leq 7$.

Proof. Using [16, Proposition 10], we establish that the order of the kernel is greater than $p^v(1-1/p)^6/(|\mu_{\mathcal{O}}/\{\pm 1\}|)$, (also see proof of [16, Lemma 11]). Since the kernel is trivial we obtain

$$p^{v-6}(p-1)^6 \leq 2^{-1}|\mu_{\mathcal{O}}|,$$

and the rest of the results follows. □

Theorem 4.5.2.3. *If* $\Lambda_{\mathcal{O}} \subset \Lambda_{\mathcal{O}'}$ *with* $\mathcal{O} \neq \mathbb{Z}[\zeta_5]$, *then the quotient* $[\mathcal{O} : \mathcal{O}'']/[\mathcal{O}_0 : \mathcal{O}''_0]$ *is an integer dividing* $2^6 \times 3^2$ *and if* $\mathcal{O} = \mathbb{Z}[\zeta_5]$, *then* $[\mathcal{O} : \mathcal{O}'']/[\mathcal{O}_0 : \mathcal{O}''_0]$ *divides* $2^8 \times 3^3 \times 5 \times 7$.

Proof. Follows from Lemma 4.5.2.2. □

Corollary 4.5.2.4. *The indices* $[\mathcal{O} : \mathcal{O}'']$ *and* $[\mathcal{O}_0 : \mathcal{O}''_0]$ *have the same valuation at all prime* $\ell > 7$.

A similar result appeared in [16, Corollary 22], where $\ell > 41$. This is understandable since using the full set of relation, like in our case, should reduce the number of cases where orders that are different have the same set of relations.

We might think that using the full set of relations would change the result in Theorem 4.3.1.1. However, a close look at the proof shows that although some more orders will

be able to be told apart, the restriction remains and we will still have orders which are distant from each other and have the same set of relations. We have

Theorem 4.5.2.5. *Let $(\mathcal{A}_i/\mathbb{F}_{q_i})_{i\in\mathbb{N}}$ be a sequence of ordinary abelian varieties defined over fields of monotonously increasing cardinality $q_i \to \infty$. Denote by $v_i = [\mathcal{O}_{\mathbb{Q}(\pi_i)} : \mathbb{Z}[\pi_i, \overline{\pi}_i]]$ their conductor gaps, and by $n_i = \mathrm{norm}(D_{K/K_0})$ the norm of the relative discriminant of their CM-fields $K = \mathbb{Q}(\pi_i)$. Assume that there exists a constant C such that, for all positive integers u and m :*

- *the probability of indices $i < m$ for which $u|v_i$ is at most C/u;*
- *the proportion of indices $i < m$ for which $u|v_i$ and $u|n_i$ is at most C/u^2.*

For any $\tau > 0$, the density of indices i for which there exists two orders $\mathcal{O}$ and $\mathcal{O}'$ containing $\mathbb{Z}[\pi_i, \overline{\pi}_i]$, stable under complex conjugation, satisfying $\Lambda_{\mathcal{O}} = \Lambda_{\mathcal{O}'}$, and such that $\ell^{\mathrm{val}_\ell\, v_i} > L(q_i)^\tau$ for some prime factor ℓ of index $[\mathcal{O} + \mathcal{O}' : \mathcal{O} \cap \mathcal{O}']$, is zero.

Proof. It follows the proof of Theorem [16, Propositon 23] but we take $M \geq 7$ instead of $M \geq 41$, which reduces the number of indices i satisfying the condition. □

Using [16, Expample 15], we can see that there are infinitely many such orders. In fact, some orders $\mathcal{O} \subset \mathcal{O}'$ with $\Lambda_\Phi(\mathcal{O}) = \Lambda_\Phi(\mathcal{O}')$ are given with $[\mathcal{O}' : \mathcal{O}]$ arbitrary large. For those orders the kernel of the corresponding map ψ is trivial which means that, in addition to $\Lambda_\Phi(\mathcal{O})$ being equal to $\Lambda_\Phi(\mathcal{O}')$, we also have $\Lambda_{\mathcal{O}} = \Lambda_{\mathcal{O}'}$.

Example 4.5.2.6. *We consider the family of orders in [16, Example 15]. Let K be a primitive CM-field with β a square root of a totally negative number in K_0 such that $\mathcal{O}_K = \mathbb{Z}[\beta]$. Let F be a positive integer and*

$$\begin{aligned}
\mathcal{O} &= \mathbb{Z} + F^2\beta\mathbb{Z} + F^2\beta^2\mathbb{Z} + F^2\beta^3\mathbb{Z},\\
\mathcal{O}' &= \mathbb{Z} + F^2\beta\mathbb{Z} + F\beta^2\mathbb{Z} + F^2\beta^3\mathbb{Z},\\
\mathcal{O}_0 &= \mathbb{Z} + F^2\beta^2\mathbb{Z},\\
\mathcal{O}'_0 &= \mathbb{Z} + F\beta^2\mathbb{Z}.
\end{aligned}$$

We have $\mathcal{O} \subset \mathcal{O}'$ and $[\mathcal{O}_K : \mathcal{O}] = F^2$.

For

$$\psi : \frac{(\mathcal{O}'/F^2\mathcal{O}_K)^\times}{(\mathcal{O}/F^2\mathcal{O}_K)^\times \mu_{\mathcal{O}'}} \to \frac{(\mathcal{O}'_0/F^2\mathcal{O}_{K_0})^\times}{(\mathcal{O}_0/F^2\mathcal{O}_{K_0})^\times},$$

if F is odd, the kernel of ψ is trivial and so we have $\Lambda_{\mathcal{O}} = \Lambda_{\mathcal{O}'}$.

In conclusion, we see that any improvement in isogeny computation will not really have an impact on the endomorphism ring computation and and will not help remove the restriction related to relations being able to tell orders apart.

It should be noted that the other method in [110] cannot handle elements in $\mathcal{A}_2$. In fact, it only considers orders that contains the maximal order of the maximal totally real subfield of the CM-field of interest. It is a classical result [24, Theorem 2.1] that such orders can be identified by ideals in the maximal order of the maximal totally real subfield. Those orders can be told apart using relations in subexponential time.

There has been no attempt to extend the lattice method to principally polarized abelian varieties of dimension 3. One reason is that abelian varieties of dimension greater than 2 are less interest for application in cryptography. Other reasons include the lack of algorithms that will perform similar task as Mestre's algorithm and the fact that isogeny computation becomes more and more expensive as the dimension gets higher. Also, the approach involves drawing points at random, which is computationally very expensive in higher dimensions. The sets $\mathcal{A}_1$ and $\mathcal{A}_2$ will contain more varieties as well, making the lattice method less efficient and less attractive in higher dimensions.

Chapter 5

Genus Two Isogeny Cryptography

In this last chapter, we propose a key exchange protocol in a post-quantum setting. It is similar to the isogeny-graph based cryptosystems of Couveignes and Rostovtsev–Stolbunov [38, 101] but instead of ordinary elliptic curves, we use a certain class of ordinary abelian surfaces. We prove that unlike the Couveignes-Rostovtsev-Stolbunov key exchange protocol, we do not have subexponential quantum attacks. We also provide some conditions for its efficient implementation.

5.1 Background

Elliptic curves and Jacobians of hyperellitptic curves of genus 2 have been considered for cryptography since the 1980's and the cryptosystems built on them are among the best public-key cryptosystems in use nowadays. The elliptic curve cryptography (ECC) allows smaller keys compared to the other public-key encryption schemes, nevertheless, there is a risk that it becomes insecure in the coming years, together with most of public-key cryptosystems that are in use.

In 1994, Shor [108], developed a quantum algorithm that can efficiently solve problems known to be difficult to solve with classical methods. The impact of that finding is that any cryptosystem whose security is based on the difficulty of factoring integers or solving the discrete logarithm problem can succumb quantum attacks. With the progress made in quantum computers in recent years, current public-key cryptographic systems then stand a risk of being compromised, thereby prompting the need to develop post-quantum cryptographic schemes which can better withstand quantum attacks, [100]. It is important

to note that asymmetric or public-key cryptography is more affected than its symmetric counterpart at the moment [6]. Many systems have been proposed as a replacement of current public-key encryption schemes. Examples include lattice based cryptosystems, code based cryptosystems and isogeny based cryptosystems. In this chapter, we focus on isogeny based cryptosystems which are among the latest ones to be proposed and probably the least-explored family. They present some interesting features that we will present in the subsequent sections.

Couveignes, [38], was the first to propose an isogeny based cryptosystem in 1997. His manuscript went unpublished for about 10 years and the method was eventually rediscovered by Rostovtsev and Stolbunov in [101]. The resulting system is often called the CRS cryptosystem. The CRS cryptosystem is a key exchange protocol that unlike the RSA or ECC is believed to resist polynomial quantum attacks. It can be put in a general framework of Hard Homogeneous Space (HHS) developed by Couveignes in his paper. An HHS is, roughly, a free and transitive action of a finite commutative group G on some set X with some extra conditions.

The CRS cryptosystem is based on ordinary elliptic curves and exploits the complex multiplication action to obtain an isogeny graph which is then used to build the system. The computation of isogenies between ordinary abelian varieties can be expensive and hence makes CRS impractical. In [43], De Feo, Kieffer and Smith provided a method of generating a suitable system of parameters that accelerate the key exchange protocol. This method, however, remains inefficient for practical use.

Another aspect that makes CRS less attractive is the development of a subexpoenential attack by Childs, Jao and Soukharev in [34]. This led Jao and De Feo to consider supersingular elliptic curves with which they constructed the Supersingular Isogeny Diffie-Hellman key exchange (SIDH). SIDH allows fast isogeny computation and is quite different from CRS. For instance, SIDH is interactive and its keys succumb active attacks, while CRS is non-interactive and a key can be used a couple of times before making the system vulnerable to attacks. On the other hand, SIDH is not affected by the subexponential quantum attacks in [34].

An approach similar to the one in [43] was used to build an efficient system, the Commutative Supersingular Isogeny Diffie-Hellman key exchange (CSIDH), [30], which is also an HHS but with different group G and set X from the CRS. It uses supersingular elliptic curves and the group G is the Picard group of a suborder of the endomorphism ring of

some supersingular elliptic curve. CSIDH benefits from both worlds, ordinary and supersingular, the commutative group action and the efficient isogeny computation. It is a secure non-interactive key exchange with tiny public keys and practical performance, [30, Section 7 and 8]. The subexponential attack in [9] works on CSIDH. However, it remains a serious candidate for post-quantum cryptography. The fact that there are subexponential algorithms for integer factorization did not stop the use of RSA worldwide.

Jacobians of hyperelliptic curves of dimension two have not really been investigated in the setting of post-quantum cryptography. In [55], a genus two analogue of SIDH was studied. We investigate the analogue of CRS in genus two and use the fact that some abelian surfaces are beyond the reach of current methods of computing their endomorphism rings, to construct systems that we believe can resist subexponential quantum attacks.

5.2 Hard Homogeneous Spaces

In this section, we present the concept of Hard Homogeneous Spaces (HHS) and give two instances, CRS and CSIDH.

Definition 5.2.1. A hard homogeneous space consists of a finite commutative group G acting freely and transitively on some set X. The following tasks are required to be easy (e.g., polynomial):

1. Compute the group operations in G.
2. Sample randomly from G with close to uniform distribution.
3. Decide validity and equality of a representation of elements of X.
4. Compute the action of a group element $g \in G$ on some $x \in X$.

The following problems are required to be hard (e.g, not polynomial):

(A) Given $x, x' \in X$, find $g \in G$ such that $g \cdot x = x'$.

(B) Given $x, x', y \in X$ such that $x' = g \cdot x$, find $y' = g \cdot y$

In other words, a Hard Homogenous Space is a Principal Homogenous Space such that the action of G on X can be efficiently computed, but inversion is computationally hard.

A cryptosystem can be built from an HHS, which resembles Diffie-Hellman key exchange:

The private keys of Alice and Bob are random elements $a, b \in G$ and they publish their public keys, $a \cdot x_0$ and $b \cdot x_0$ respectively, with $x_0 \in X$ a public fixed element. They both end up with the shared secret $b \cdot (a \cdot x_0) = a \cdot (b \cdot x_0)$. The system is secure since the first hard problem above protects the private keys and the shared secret is protected by the second problem.

In order to obtain the traditional Diffie-Hellman, we take X to be a cyclic group of order p a prime, with x a generator and $G = (\mathbb{Z}/p\mathbb{Z})^*$, the multiplicative group. We define the action of G on $X \setminus \{1\}$ by $g \cdot x = x^g$ and we obtain the traditional discrete logarithm problem (DLP).

Not all systems built on an HHS are related to the DLP. Some are even believed to resist attacks based on Shor's algorithm. The Couveignes-Rostovtsev-Stolbunov key exchange protocol (CRS) and the Commutative Supersingular Isogeny Diffie-Hellman (CSIDH) are instances of such systems. They are built on two different HHSs.

5.2.1 Couveignes-Rostovtsev-Stolbunov key exchange protocol

In the case of CRS, the HHS has the following parameters:

- $X = \mathrm{Ell}_q(\mathcal{O})$, the set isomorphism classes over $\overline{\mathbb{F}}_q$ of ordinary elliptic curves defined over $\mathbb{F}_q$, with complex multiplication by $\mathcal{O}$, for some well-chosen q and $\mathcal{O}$ an imaginary quadratic order.
- $G = \mathrm{Pic}(\mathcal{O})$, the Picard group of $\mathcal{O}$.

The action of G on X is the complex multiplication action, Theorem 3.3.2.1.

If we take a generic element of the Picard group G, there is no known algorithm that computes the action in polynomial time (in $\log q$) - the best algorithm has a subexponential runtime [68]. However, to have an HHS, the group action should be efficiently computable. A way to make the action efficient is to consider a subset S of small prime ideals in $\mathcal{O}$ such that their images in the Picard group generate the whole Picard group. The computation of the action of an arbitrary element is then the composition of small elements of S.

The action of the Picard group G on X can also be viewed as walks in an isogeny graph.

5.2.1.1 Isogeny graphs of ordinary elliptic curves over finite fields

Let $\mathcal{E}/\mathbb{F}_q$ be an ordinary elliptic curve and ℓ a prime different from the characteristic of $\mathbb{F}_q$. The ℓ-isogeny graph is an ℓ-volcano graph, [115]. Although such graphs have important applications such as in computing modular polynomials and Hilbert class polynomials, they are not a good candidate for isogeny based cryptography because of the lack of mixing property. On the other hand, horizontal isogeny graphs are more suited to build key exchange protocols.

Horizontal isogeny graphs are graphs whose vertices are isomorphism classes of elliptic curves with CM by a given imaginary quadratic order $\mathcal{O}$ and whose edges are equivalence classes of isogenies belonging to some particular family, two isogenies being equivalent if they share a kernel. They can be used to transfer the discrete logarithm problem from an ordinary elliptic curve to another [66]. A property that is often used while working with isogeny graphs is the expander property. Expander graphs have strong connectivity properties.

Let $\mathcal{G}$ be an undirected graph with n vertices, $\{v_1, v_2, \ldots, v_n\}$. The adjacency matrix of $\mathcal{G}$ is a square $n \times n$ matrix A such that its entry A_{ij} is one when there is an edge from vertex v_i to vertex v_j, and zero when there is no edge. The matrix A is real and symmetric and by the spectral theorem it has n real eigenvalues. If we suppose that the graph $\mathcal{G}$ is k-regular with A having eigenvalues $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$, then $\lambda_1 = k$ and is called the trivial eigenvalue.

Definition 5.2.1.1. Let $\delta > 0$. The k-regular graph $\mathcal{G}$ is (one-sided) δ-expander if $\lambda_2 \leq (1-\delta)k$. It is a two-sided δ-expander if the stronger bound $|\lambda_2| \leq (1-\delta)k$ is satisfied.

Lemma 5.2.1.2. *(Mixing theorem) Let $\mathcal{G}$ be a finite k-regular graph for which the non-trivial eigenvalues λ of the adjacency matrix A satisfy the bound $|\lambda| \leq c$, for some $c < k$. Let S be a subset of the set of vertices of $\mathcal{G}$ and v a vertex of $\mathcal{G}$. Then any random walk in the length at least $\frac{\log(2|\mathcal{G}|/\sqrt{|S|})}{\log(k/c)}$ will end in S with probability between $\frac{|S|}{2|\mathcal{G}|}$ and $\frac{3|S|}{2|\mathcal{G}|}$.*

Proof. [67] □

Expander families of graphs have many applications in cryptography. Horizontal isogeny graphs are expander graphs.

Theorem 5.2.1.3. *Let $\mathbb{F}_q$ be a finite field and let $\mathcal{O} \subset \mathbb{Q}[\sqrt{-D}]$ be an order in a quadratic imaginary field. Let $\mathcal{G}$ be the graph whose vertices are elliptic curves over $\mathbb{F}_q$ with complex multiplication by $\mathcal{O}$, and whose edges are horizontal isogenies of prime degree bounded by $(\log q)^{2+\delta}$ for some fixed $\delta > 0$. Assume that $\mathcal{G}$ is non-empty. Then, under GRH, $\mathcal{G}$ is a regular graph and there exists an ε, independent of $\mathcal{O}$ and q, such that $\mathcal{G}$ is a one-sided ε-expander.*

Proof. [67]. □

As we mentioned before, the action of G on X in the case of CRS can be viewed as walks on the corresponding horizontal isogeny graphs. An element $g \in G$ is of the form $g = s_i^{\alpha_1} \cdots s_n^{\alpha_n}$, with $s_1, \ldots, s_n \in S$, S a generating set of G, and the action $g \cdot x$ corresponds to an isogeny walk starting from x and the edges are isogenies corresponding to the ideals s_i. By Lemma 5.2.1.2, an action of a random element of G on an element $x \in X$ can be obtained by taking a random walk from x that is long enough. Elements of X are represented by their j-invariant and the equality of a representation of elements of X can be efficiently checked.

The horizontal isogeny graph is a special case of a more general type of graph namely Schreier graphs.

Definition 5.2.1.4. Let $\mathcal{G}$ be a group acting freely on a set X, in the sense that there is a map

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

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

Schreier graphs are undirected graphs and regular because of the constraints on the set S. Horizontal isogeny graphs are Schreier graphs with the set S formed by the images of the prime ideals bounded by $(\log q)^{2+\delta}$ as in Theorem 5.2.1.3.

Let $\mathcal{E}/\mathbb{F}_q$ be an ordinary elliptic curve with endomorphism ring isomorphic to $\mathcal{O}$. By Theorem 3.3.4, the action of an ideal $\mathfrak{a}$ of $\mathcal{O}$ of norm polynomial in $\log q$ can be computed

in polynomial time. Using a subset S of ideals of small norm makes it possible to compute actions of random elements in polynomial time. We also do not have to compute the Picard group $\mathrm{Pic}(\mathcal{O})$ as well as the set $\mathrm{Ell}_q(\mathcal{O})$, for which the best known algorithm is subexponential. We can also avoid explicit ideal class arithmetic. In fact, only isogenies are computed and to compute an isogeny walk, we successively compute the corresponding isogeny for each prime until we get the j-invariant of the last curve of the chain.

With what we have presented above, we can see that points 1 to 4 in the definition of HHS are satisfied. The fact that the horizontal isogeny graph is an expander graph is important in proving that problem (A) and (B) are indeed hard as we will see in Section 5.2.1.3.

5.2.1.2 Construction of CRS

Concretely, the key exchange is as follows:

We have the following public parameters: An elliptic curve $\mathcal{E}_0/\mathbb{F}_q$ with Frobenius endomorphism π, a set $L = \{\ell_1, \ldots, \ell_m\}$ of different prime numbers and an element λ_i for each ℓ_i with

- q large enough,
- the discriminant D of $\mathbb{Z}[\pi]$ containing a large prime factor (for security reason),
- the set $L = \{\ell_1, \ldots, \ell_m\}$ satisfying $\left(\frac{D}{\ell_i}\right) = 1$, *i.e* primes that split in $\mathbb{Z}[\pi]$, (which correspond to the prime ideals in Theorem 5.2.1.3),
- and λ_i satisfying $\pi^2 - t\pi + q = (\pi - \lambda_i)(\pi - \mu_i) \mod \ell_i$.

The $\mu_i's$ are not included in the public data because they represent a backward walk (the dual of the isogenies associated to $\lambda_i's$) and would shorten the length of the isogeny walks. The kernel of the isogeny corresponding to (ℓ_i, λ_i) is $\mathcal{E}[\ell_i] \cap \ker(\pi - \lambda_i)$.

We summarized the key exchange protocol between two parties in a table as in [41, Section 14]:

Public Parameters	An elliptic curve $\mathcal{E}_0/\mathbb{F}_q$, a set of primes $L = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D}{\ell_i}\right) = 1$, A Frobenius eigenvalue λ_i for each ℓ_i.	
	Alice	Bob
Pick random secret	ρ_A a random walk from $\mathcal{E}_0$	ρ_B a random walk from $\mathcal{E}_0$
Compute public data	$j(\mathcal{E}_A)$ with $\mathcal{E}_A = \rho_A(\mathcal{E}_0)$	$j(\mathcal{E}_B)$ with $\mathcal{E}_B = \rho_B(\mathcal{E}_0)$
Exchange data	sends $j(\mathcal{E}_A)$ to Bob	sends $j(\mathcal{E}_B)$ to Alice
Compute shared keys	$j(\mathcal{E}_{AB})$, with $\mathcal{E}_{AB} = \rho_A(\mathcal{E}_B)$	$j(\mathcal{E}_{AB})$, with $\mathcal{E}_{AB} = \rho_B(\mathcal{E}_A)$

TABLE 5.1: CRS key exchange

Since by Theorem 5.2.1.3, the primes used in the exchange are all polynomial in $\log q$, each isogeny computation has polynomial complexity. Thus, the overall cost of implementing the protocol is polynomial in $\log q$. We note that the knowledge of the endomorphism ring of $\mathcal{E}_0$ is not required in the implementation of the protocol.

5.2.1.3 Security of CRS

The security of the system relies on Problems (A) and (B). However, a solution to Problem (A) will also solve Problem (B). All the protocol's security rests on the following isogeny path problem:

Problem 5.2.1.5. *Given two ordinary elliptic curves $\mathcal{E}$ and $\mathcal{E}'$ defined over a finite field $\mathbb{F}_q$, with $|\mathcal{E}(\mathbb{F}_q)| = |\mathcal{E}'(\mathbb{F}_q)|$, having the same endomorphism ring, find an isogeny walk from $\mathcal{E}$ to $\mathcal{E}'$. In order words, given two horizontally isogenous elliptic curves $\mathcal{E}$ and $\mathcal{E}'$, find an isogeny $\varphi : \mathcal{E} \to \mathcal{E}'$ of smooth order.*

We present the best classical and quantum algorithm to solve Problem 5.2.1.5.

The best known classical algorithm was developed by Galbraith, Hess and Smart in [59]. The method is known as the meet-in-the-middle key search and it works as follows:

Algorithm 18 `Meet-in-the-middle` [59]

Input: Horizontally isogenous ordinary elliptic curves $\mathcal{E}/\mathbb{F}_q$ and $\mathcal{E}'/\mathbb{F}_q$.

Output: An isogeny from $\mathcal{E}$ to $\mathcal{E}'$ with smooth order.

1: Start with two random walks of horizontal isogenies from $\mathcal{E}$ and $\mathcal{E}'$ and detect the moment when they collide.
2: Reduce the size of the obtained walk using index-calculus techniques like Algorithm 6.
3: Return the corresponding isogeny.

Step 1 is a version of Pollard's rho method. Since the size of the $\mathrm{Ell}_q(\mathcal{O})$ is the same as $|\operatorname{Pic}(\mathcal{O})|$ and since $|\operatorname{Pic}(\mathcal{O})| \sim \sqrt{|D|}$, where D is the discriminant of $\mathcal{O}$, by the birthday paradox, the complexity of the algorithm is $O(\sqrt[4]{|D|})$. Finally, we have that $D \sim q$ and so the complexity of the attack is $O(\sqrt[4]{q})$. Hence, the complexity of the best known classical attacks is exponential in $\log q$.

There is a subexponential quantum attack first developed by Childs, Jao and Soukharev in [34]. They observed that the problem of finding an isogeny between two ordinary curves $\mathcal{E}/\mathbb{F}_q$ and $\mathcal{E}'/\mathbb{F}_q$ having the same endomorphism ring could be reduced to the abelian hidden shift problem which can be solved in subexponential quantum time.

This problem is defined as follows:

Let H be a known finite abelian group and $f_0, f_1 : H \to S$ be functions, with S a known finite set. The functions f_0, f_1 are said to hide a shift $s \in H$ if f_0 is injective and $f_1(x) = f_0(xs)$, for all $x \in H$. The solution of the hidden shift problem consists of determining s.

In our context, Problem 5.2.1.5 can be reduced to the hidden shift problem. For two curves $\mathcal{E}$ and $\mathcal{E}'$, horizontally isogenous, with endomorphism ring $\mathcal{O}$ with discriminant D, we let $[\mathfrak{s}] \in \operatorname{Pic}(\mathcal{O})$ such that $[\mathfrak{s}] \cdot j(\mathcal{E}) = j(\mathcal{E}')$.

We define functions $f_0, f_1 : \operatorname{Pic}(\mathcal{O}) \to \mathrm{Ell}_q(\mathcal{O})$ with

$$\begin{aligned} f_0 : \operatorname{Pic}(\mathcal{O}) &\to \mathrm{Ell}_q(\mathcal{O}) \\ [\mathfrak{b}] &\mapsto [\mathfrak{b}] \cdot j(\mathcal{E}) \\ f_1 : \operatorname{Pic}(\mathcal{O}) &\to \mathrm{Ell}_q(\mathcal{O}) \\ [\mathfrak{b}] &\mapsto [\mathfrak{b}] \cdot j(\mathcal{E}'). \end{aligned}$$

We can see that f_0, f_1 hide $[\mathfrak{s}]$ and by [34, Lemma 5.1] f_0 is injective.

There are two quantum algorithms that solve the hidden shift problem, Kuperberg's algorithm, [73] and Regev's algorithm, [98].

Theorem 5.2.1.6. *[73, Theorem 7.1] (Kuperberg's algorithm) The abelian hidden shift problem has a quantum algorithm with time and query complexity $2^{O(\sqrt{n})}$, where n is the length of the output, uniformly for all finitely generated abelian groups.*

Theorem 5.2.1.7. *[34, Theorem 5.2](Regev's algorithm) Let A be a finite abelian group and let the functions f_0 and f_1 hide some unknown $s \in A$. Then there is a quantum algorithm that finds s with time and query complexity $L(|A|)^{\sqrt{2}+o(1)}$ with polynomial space complexity in $\log |A|$.*

The following algorithm solves the isogeny construction problem (Problem 5.2.1.5).

Algorithm 19 `Hidden shift problem [34, Algorithm 3]`

Input: A finite field $\mathbb{F}_q$, discriminant D of $\mathrm{End}(\mathcal{E})$, and horizontally isogenous ordinary elliptic curves $\mathcal{E}/\mathbb{F}_q$ and $\mathcal{E}'/\mathbb{F}_q$.

Output: An isogeny from $\mathcal{E}$ to $\mathcal{E}'$ with smooth order.

1: Decompose $\mathrm{Pic}(\mathcal{O}) = \langle [\mathfrak{b}_1] \rangle \oplus \cdots \oplus \langle [\mathfrak{b}_k] \rangle$, with $|\langle [\mathfrak{b}_i] \rangle| = n_i$.

2: Solve the hidden shift problem defined by the functions $f_0, f_1 : \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_n \to \mathrm{Ell}_q(\mathcal{O})$ satisfying $f_c(x_1, \ldots, x_k) = ([\mathfrak{b}_1]^{x_1} \cdots [\mathfrak{b}_k]^{x_k}) \cdot j(\mathcal{E}_c)$, $c \in \{1, 2\}$, giving some $(s_1, \ldots, s_k) \in \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$

3: Return $[\mathfrak{s}] = [\mathfrak{b}_1]^{s_1} \cdots [\mathfrak{b}_k]^{s_k}$.

Theorem 5.2.1.8. *[34, Theorem 5.4 and Remark 5.5] Under GRH, Algorithm 19 runs in time $L(q)^{1/\sqrt{2}+o(1)}$ (respectively, $L(q)^{3/\sqrt{2}+o(1)}$) using Kuperberg's algorithm (respectively, Regev's algorithm) to solve the hidden shift problem.*

In [8], Biasse, Iezzi and Jacobson gave an improvement of the attack by using efficient evaluation of the complex multiplication action from [10]. We have:

Theorem 5.2.1.9. *[8, Corollary 1] Let $\mathcal{E}$ and $\mathcal{E}'$ be two elliptic curves and $\mathcal{O}$ be an imaginary quadratic order of discriminant D such that $\mathrm{End}(\mathcal{E}) \cong \mathrm{End}(\mathcal{E}') \cong \mathcal{O}$. Then assuming [8, Hypothesis 1] for some constant $c > 0$, there is a quantum algorithm for computing $[\mathfrak{s}]$ such that $[\mathfrak{s}] \cdot j(\mathcal{E}) = j(\mathcal{E}')$ with:*

- *heuristic time complexity $e^{O(\sqrt{\log |D|})}$, polynomial quantum memory and $e^{O(\sqrt{\log |D|})}$ classical memory.*

- *heuristic time complexity* $L(|D|)^{1/\sqrt{2}+o(1)}$ *with polynomial memory (both classical and quantum).*

The first case is with Kuperberg's algorithm which is faster but requires more memory in the classical setting, subexponential. The second case is with Regev's algorithm and has the advantage of only requiring polynomial classical memory.

5.2.1.4 Public key selection

The CRS protocol was proposed as potential post-quantum candidate but its performance is poor compared to other quantum resistant systems. The development of the subexponential quantum attack we discussed above made the system even less attractive. In order to improve its performance, De Feo, Kieffer and Smith in [43] proposed a method to construct ordinary elliptic curves for which the complex multiplication action is more efficient to compute.

The cryptosystem is slow because of the computation of isogenies corresponding to ideals. In fact, for an elliptic curve $\mathcal{E}/\mathbb{F}_q$, although the isogenies are defined over $\mathbb{F}_q$, the points of their kernels may be defined over an extension of $\mathbb{F}_q$, in which case, computation has to be done over extensions of $\mathbb{F}_q$, making it expensive. A sufficient condition for the kernel of an ℓ-isogeny to be defined over $\mathbb{F}_q$ is to have ℓ divides $|\mathcal{E}(\mathbb{F}_q)|$. The method in [43] consists of constructing ordinary elliptic curves in such a way that most of the isogenies that are involved in the implementation of the protocol have their kernel defined over the based field.

There is an algorithm that computes the ordinary elliptic curves with a given number of rational points, known as the CM-method, [1, 114], however, it has an exponential complexity in $\log q$. The approach in [43] constructs an elliptic curve $\mathcal{E}$ over a prime field $\mathbb{F}_p$ with polynomial complexity. We have:

Algorithm 20 `Construction of elliptic curves [43, Section 4]`

Input: A prime p.

Output: A promising elliptic curve for CRS.

1: Choose a smoothness bound B.
2: Pick elliptic curves $\mathcal{E}$ in $\mathbb{F}_p$ at random, and use SEA algorithm to check whether for any $\ell \leq B$, $|\mathcal{E}(\mathbb{F}_p)| \equiv 0 \mod \ell$ and abort if this is not satisfied.
3: For each $\mathcal{E}$ which passed the tests above, compute $|\mathcal{E}(\mathbb{F}_p)|$ and estimate the key exchange running time.
4: Return the fastest curve.

When a prime ℓ divides $|\mathcal{E}(\mathbb{F}_p)|$, the ℓ-torsion points are all defined over $\mathbb{F}_p$ and so the points of the kernel of any ℓ-isogeny are defined on $\mathbb{F}_p$. For a well chosen bound B, the algorithm has a polynomial runtime. Unfortunately, even with this construction, CRS remains slow to implement. In practice, the algorithm is only efficient for small bounds B (in [43], $B = 13$). For more on the construction see [43, Section 4].

In the quest for constructing a system similar to CRS that also performs well, supersingular elliptic curves have been considered in such a way that the commutative complex multiplication action can still be exploited. The advantage is that, for supersingular elliptic curves, Algorithm 20 is much more effective.

5.2.2 Commutative Supersingular Isogeny Diffie-Hellman

In [30], Castryck, Lange, Martindale, Renes, Panny used a different HHS to build a more efficient system. Instead of ordinary elliptic curves, they used supersingular ones. We present their method in this section and throughout the section, $\mathcal{E}$ is defined over $\mathbb{F}_q$ and we assume that p, the characteristic of $\mathbb{F}_q$, is greater than 3.

5.2.2.1 Isogeny graphs of supersingular elliptic curves over finite fields

We recall the definition of supersingular elliptic curves.

Definition 5.2.2.1. An elliptic curve $\mathcal{E}/\mathbb{F}_q$ is said to be supersingular if the p-torsion subgroup is the trivial subgroup.

We have the following:

Theorem 5.2.2.2. *[109, Theorem V.3.1] Let $\mathcal{E}/\mathbb{F}_q$ be an elliptic curve and π its Frobenius endomorphism. The following are equivalent:*

1. *$\mathcal{E}[p^r] = \{0\}$, for all $r \geq 1$.*
2. *The map $[p] : \mathcal{E} \to \mathcal{E}$ is purely inseparable and $j(\mathcal{E}) \in \mathbb{F}_{p^2}$.*
3. *$\mathrm{End}(\mathcal{E})$ is an order in a quaternion algebra.*
4. *$\mathcal{E}$ is supersingular.*

Supersingular elliptic curves have many features that make them nice to work with.

Theorem 5.2.2.3. *Let p, ℓ be distinct primes, then*

- *all supersingular j-invariants of curves in $\overline{\mathbb{F}}_p$ are defined over $\mathbb{F}_{p^2}$;*
- *there are*

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

  isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$;

- *the graph of supersingular curves over $\overline{\mathbb{F}}_p$ with ℓ-isogenies is connected, $(\ell+1)$-regular, and has the Ramanujan property. In particular it is an expander graph.*

Proof. See [109, Theorem V.4.1], [95, 96]. □

Unlike ordinary elliptic curves whose ℓ-isogeny graphs are volcanoes, the ℓ-isogeny graphs of supersingular curves have the mixing property. This is the basis of SIDH. We can develop a similar setting as in the ordinary case by considering supersingular elliptic curves defined of $\mathbb{F}_p$ and endomorphisms that are defined over $\mathbb{F}_p$.

Theorem 5.2.2.4. *[44, Theorem 2.1] Let $\mathcal{E}/\mathbb{F}_q$, be a supersingular elliptic curve with $q = p^n$ and $|\mathcal{E}(\mathbb{F}_q)| = q + 1 - t$, where $|t| \leq 2\sqrt{q}$ and π its Frobenius endomorphism. Then one of the following cases must be true:*

1. *n is even and $t = \pm 2\sqrt{q}$,*

2. *n is even, $p \not\equiv 1 \mod 3$ and $t = \pm\sqrt{q}$,*

3. *n is even and $p \not\equiv 1 \mod 4$ and $t = 0$,*

4. *n is odd and $t = 0$,*

The division algebra $\mathrm{End}_{\mathbb{F}_q}(\mathcal{E}) \otimes \mathbb{Q}$ is determined by the different cases. In the first case, it is a quaternion algebra over $\mathbb{Q}$, π is a rational integer and $\mathrm{End}_{\mathbb{F}_q}(\mathcal{E})$ is a maximal order in $\mathrm{End}_{\mathbb{F}_q}(\mathcal{E}) \otimes \mathbb{Q}$. In the other three cases, $\mathrm{End}_{\mathbb{F}_q}(\mathcal{E}) \otimes \mathbb{Q} = \mathbb{Q}(\pi)$, an imaginary quadratic field over $\mathbb{Q}$ and $\mathrm{End}_{\mathbb{F}_q}(\mathcal{E})$ is an order in $\mathrm{End}_{\mathbb{F}_q}(\mathcal{E}) \otimes \mathbb{Q}$ with conductor prime to p.

If $\mathcal{E}/\mathbb{F}_p$ is a supersingular elliptic curve, then its Frobenius endomorphism π satisfies $\pi^2 - t\pi + p$ in $\mathrm{End}_{\mathbb{F}_p}(\mathcal{E})$, where t is the trace of π. From the Theorem above we have that $t = 0$ and that $\mathrm{End}_{\mathbb{F}_p}(\mathcal{E})$ is an order in an imaginary quadratic field K. As in the ordinary case, $\mathrm{End}_{\mathbb{F}_p}(\mathcal{E})$ always contains $\mathbb{Z}[\pi]$.

Proposition 5.2.2.5. *Let $\mathcal{E}/\mathbb{F}_p$ be a supersingular elliptic curve and G a finite $\mathbb{F}_p$-rational subgroup of $\mathcal{E}$. Then there is a supersingular elliptic curve $\mathcal{E}'/\mathbb{F}_p$ and a separable isogeny $\varphi : \mathcal{E} \to \mathcal{E}'$ defined over $\mathbb{F}_p$ with kernel G. The codomain $\mathcal{E}'$ and the isogeny φ are unique up to $\mathbb{F}_p$-isomorphism.*

Proof. See [109, Proposition III.4.12, Remark III.4.13.2, Exercise III.3.13*e*]. □

Considering a supersingular elliptic curve $\mathcal{E}/\mathbb{F}_p$, ideals of $\mathrm{End}_{\mathbb{F}_p}(\mathcal{E})$ corresponds to separable isogenies much like for ordinary elliptic curves. In fact, for an invertible ideal $\mathfrak{a}$ in $\mathrm{End}_{\mathbb{F}_p}(\mathcal{E})$, by Proposition 5.2.2.5, the corresponding isogeny is the isogeny (up to $\mathbb{F}_p$-isomorphism) $\varphi_{\mathfrak{a}}$ with kernel $\cap_{\alpha \in \mathfrak{a}} \ker \alpha$. We denote the codomain by $\mathcal{E}/\mathfrak{a}$. This leads to an action of the Picard group of $\mathrm{End}_{\mathbb{F}_p}(\mathcal{E})$ on the set of elliptic curves defined over $\mathbb{F}_p$ that are isogenous to $\mathcal{E}$

Theorem 5.2.2.6. *[103, Theorem 4.5] Let $\mathcal{O}$ be an order in an imaginary quadratic field and $\pi \in \mathcal{O}$ such that $\mathrm{Ell}_{\mathbb{F}_p}(\mathcal{O}, \pi)$, the set of $\mathbb{F}_p$-isomorphism classes of elliptic curves $\mathcal{E}$ defined over $\mathbb{F}_p$ with $\mathrm{End}_{\mathbb{F}_p}(\mathcal{E}) \cong \mathcal{O}$ such that π corresponds to the $\mathbb{F}_p$-Frobenius endomorphism of $\mathcal{E}$, is nonempty. Then the Picard group $\mathrm{Pic}(\mathcal{O})$ acts freely and transitively on the set $\mathrm{Ell}_{\mathbb{F}_p}(\mathcal{O}, \pi)$ via the map*

$$\begin{aligned} \mathrm{Pic}(\mathcal{O}) \times \mathrm{Ell}_{\mathbb{F}_p}(\mathcal{O}, \pi) &\to \mathrm{Ell}_{\mathbb{F}_p}(\mathcal{O}, \pi) \\ ([\mathfrak{a}], \mathcal{E}) &\mapsto \mathcal{E}/\mathfrak{a} \end{aligned}$$

in which $\mathfrak{a}$ is chosen to be an integral representative.

We already discussed this for ordinary elliptic curves. For ordinary elliptic curves, the endomorphism rings are unaffected by base field extension as seen in Proposition 2.5.12 and so the above theorem is the same as Theorem 3.3.2.1 in the ordinary case. It remains true for supersingular elliptic curves if the conditions in the theorem are satisfied. As it can be expected, the ℓ-isogeny graphs of supersingular elliptic curves defined over $\mathbb{F}_p$ have an ℓ-volcano structure.

Theorem 5.2.2.7. *[44, Theorem 2.7] Let p, ℓ be distinct and $\mathcal{G}_{\mathbb{F}_p,\ell}$ be a connected component of the $\mathbb{F}_p$-rational ℓ-isogeny graph with vertices all supersingular elliptic curves defined over $\mathbb{F}_p$. Assume that $p \equiv 11 \mod 12$ or that $\mathcal{G}_{\mathbb{F}_p,\ell}$ contains no curve with j-invariant 0 or 1728. If ℓ does not divide $t^2 - 4p$, with t the trace of the Frobenius endomorphism of any curve in $\mathcal{G}_{\mathbb{F}_p,\ell}$, then all the elliptic curves in $\mathcal{G}_{\mathbb{F}_p,\ell}$ have the same $\mathbb{F}_p$-rational endomorphism ring $\mathcal{O} \subset K$, and $\mathcal{O}$ is locally maximal at ℓ. Moreover if t^2 is a nonzero square modulo ℓ, then $\mathcal{G}_{\mathbb{F}_p,\ell}$ is a cycle whose length equals the order of $[\mathfrak{l}]$ in $\mathrm{Pic}(\mathcal{O})$, where $\mathfrak{l}$ is a prime ideal dividing $\ell\mathcal{O}$. If not, then $\mathcal{G}_{\mathbb{F}_p,\ell}$ is a single vertex and no edges.*

The HHS for CSIDH consists of X, the set of $\mathbb{F}_p$-isomorphism classes of supersingular elliptic curves $\mathcal{E}$ defined over $\mathbb{F}_p$ with $\mathrm{End}_{\mathbb{F}_p}(\mathcal{E})$ isomorphic to a given imaginary quadratic order $\mathcal{O}$ and $G = \mathrm{Pic}(\mathcal{O})$.

The action of the HHS can be interpreted as walk in some isogeny graph that is an expander. We cannot compute the action of a random ideal in polynomial time and the same strategy is used as before, i.e, considering prime ideals that generate the Picard group.

The expander gaph is obtained by selecting some primes $\ell_1, \ldots, \ell_m$ such that $\mathcal{G}_{\mathbb{F}_p,\ell_i}$ is a cycle and taking the union of the cycles on the same set of vertices. By taking enough primes, we obtain an expander graph as in Theorem 5.2.1.3. The key exchange protocol and the attacks on CSIDH are the same as CRS, see [7–9, 18] for more on the attacks. The main difference is the ability to construct supersingular elliptic curves for which the protocol is fast to implement.

5.2.2.2 Construction of CSIDH

Let $\mathcal{E}/\mathbb{F}_p$ be a supersingular elliptic curve. By Theorem 5.2.2.4, $|\mathcal{E}(\mathbb{F}_p)| = p+1$. In order to obtain a supersingular elliptic curve $\mathcal{E}/\mathbb{F}_p$ with $|\mathcal{E}(\mathbb{F}_p)|$ divisible by small primes, we

take $p = 4 \cdot \ell_1 \cdots \ell_m - 1$ prime with the $\ell_i' s$ prime and consider the curve $\mathcal{E}_0 : y^2 = x^3 + x$ which turns out to be supersingular due to the fact that $p \equiv 3 \mod 4$. It suffices to check that the trace is zero. We then obtain $|\mathcal{E}(\mathbb{F}_p)| = p + 1 = 4 \cdot \ell_1 \cdots \ell_m$.

If the primes $\ell_1, \ldots, \ell_m$ are the primes involved in the implementation of the key exchange, then all computations are performed over $\mathbb{F}_p$ and this makes the implementation CSIDH very fast.

5.2.2.3 Comparison between CRS, CSIDH and SIDH

The main difference between CRS and CSIDH is the disparity in the efficiency of implementing both protocols; apart from that, both share similar properties. They offer public key validation, are non-interactive key exchange systems and their keys can be reused for certain number of times without compromising the security. This represents one of the differences with SIDH which is interactive, [60]. CRS and CSIDH also differ from SIDH by the data that is used as the public key. For the former two systems, only the elliptic curves (or their j-invariants) are used as public keys. For SIDH, in addition to the elliptic curves, two other points are published. The publication of those extra points can weaken the system in some cases, [94], although this seems not to be the case in general. The main advantage of SIDH over CRS and CSIDH is the fact that no subexponential attack on SIDH is known in general.

We present a non-interactive system that is conjectured to resist subexponential quantum attacks.

5.3 Post-Quantum Cryptography in genus 2

Abelian surfaces have been considered in cryptography since the $1980's$ by Koblitz in [71], as finite abelian groups for cryptosystems whose security is based on the difficulty of DLP. In the post-quantum setting, to best of our knowledge, only principally polarised supersingular abelian surfaces have been investigated in attempts to develop an analog of the SIDH in genus 2 [29, 37, 54, 55].

There is no stated reason why ordinary abelian surfaces have not been considered in isogeny based cryptography but a reason for this lack of interest could be that if the CRS is impractical, a similar system in genus 2 will be worse since isogeny computation is more

expensive in higher dimensions. Also, abelian surfaces are more difficult to manipulate. For instance finding an ordinary abelian surface with a given number of rational points is far more difficult than it is for elliptic curves.

However, as often, considering higher dimensional abelian varieties presents some advantages. For instance in [55], it is proved that the genus two isogeny Diffie-Hellman protocol achieves the same level of security as SIDH but uses a prime with a third of the bit length. We use some ordinary abelian surfaces to build a genus 2 analog of CRS to obtain an isogeny based cryptosystem that we believe resists subexponential attacks. We remark that the initial reason for Jao and De Feo to consider supersingular elliptic curves was to obtain an isogeny based cryptosystem that can resist subexponential quantum attacks. All previous isogeny based cryptosystems built on an HHS failed to address this.

5.3.1 Horizontal isogeny graphs of ordinary abelian surfaces

For the rest of this chapter, we let $\mathcal{A}/\mathbb{F}_q$ be a principally polarized, absolute simple, ordinary abelian variety, with CM by $\mathcal{O}$, an order in a CM-field K with K_0 the maximal totally real subfield of K and $\mathrm{End}(\mathcal{A})_0 = \mathrm{End}(\mathcal{A}) \cap K_0$. We also let π be the Frobenius endomorphism of $\mathcal{A}$ and $\chi_{\mathcal{A}}$ its characteristic. We fix an isomorphism between $\mathbb{Q}\otimes\mathrm{End}(\mathcal{A})$ and $K = \mathbb{Q}[x]/(\chi_{\mathcal{A}}(x))$.

From Theorem 2.5.11, the polarized class group acts freely on the set of isomorphism classes of abelian varieties isogenous to $\mathcal{A}$ (as principally polarized abelian varieties) with endomorphism ring $\mathcal{O}$. We have seen in Chapter 2 that the polarized class group satisfies the following:

$$1 \to \mathcal{O}_0^+ / \operatorname{norm}_{K/K_0}(\mathcal{O}^*) \xrightarrow{\mu \mapsto (\mathcal{O},\mu)} \mathfrak{C}(\mathcal{O}) \xrightarrow{(\mathfrak{m},\rho)\mapsto \mathfrak{m}} \mathrm{Pic}(\mathcal{O}) \xrightarrow{\operatorname{norm}_{K/K_0}} \mathrm{Cl}^+(\mathcal{O}_0)$$

with $\mathcal{O}_0^+ = \mathcal{O} \cap \mathcal{O}_{K_0}^+$, the group of totally positive units in $\mathcal{O}_0 = \mathcal{O} \cap \mathcal{O}_{K_0}$ and $\mathrm{Cl}^+(\mathcal{O}_0)$ the narrow class group *i.e* the group of fractional ideals modulo the group of principal ideals with totally positive generators.

The polarized class group can then be viewed as a subgroup H of $\mathrm{Pic}(\mathrm{End}(\mathcal{A}))$ under the map defined in the exact sequence. However, some information will be lost. The elements of the quotient $\mathcal{O}_0^+ / \operatorname{norm}_{K/K_0}(\mathcal{O}^*)$ are trivial in H. They represent the different polarizations on the abelian varieties in the orbits of the action. The subgroup H does not act on the set of principally polarized abelian varieties; but on the set of principally

polarizable abelian varieties. When $|\mathcal{O}_0^+/\operatorname{norm}_{K/K_0}(\mathcal{O}^*)| = 1$, the group H and the polarized class group are isomorphic and all polarizable abelian varieties admit a unique polarization. If $\mathcal{A}$ is an abelian surface, we have $|\mathcal{O}_0^+/\operatorname{norm}_{K/K_0}(\mathcal{O}^*)| \in \{1, 2\}$.

Let $\mathcal{V}_{\mathbb{F}_q,\mathcal{O}}$ be the set of isomorphism classes of principally polarizable abelian varieties defined over $\mathbb{F}_q$ isogenous to $\mathcal{A}$ with endomorphism ring isomorphic to $\mathcal{O}$. Let $\mathfrak{f}$ be the conductor of $\mathcal{O}$ in $\mathcal{O}_K$.

We use the complex multiplication action to define a graph as follows:

Let $H(\mathcal{A})$ be the set of varieties on the orbits of the action of H on $\mathcal{V}_{\mathbb{F}_q,\mathcal{O}}$ and $\mathcal{S}$ a set of invertible ideals in $\mathcal{O}$ that generates H. We define $\mathcal{G}_\mathcal{S}$ to be the graph, whose vertices are elements of $H(\mathcal{A})$ and there is an edge between two vertices if there is an isogeny between them corresponding to an ideal in $\mathcal{S}$. The graph $\mathcal{G}_S$ is a multigraph, since two elements in $\mathcal{S}$ can represent the same element in H. Let $\mathfrak{m}$ be an ideal of $\mathcal{O}$, $B > 0$ and

$$\mathcal{S}_B = \{\text{ideals of } \mathcal{O} \text{ of prime norm bounded by } B \text{ and coprime to } \mathfrak{fm}\}.$$

Then we have:

Theorem 5.3.1.1. *[69, Theorem 1.1](GRH) Assuming the Generalized Riemann Hypothesis, for any $\varepsilon > 0$, there exists a bound*

$$B = O\left((g[\mathrm{Pic}(\mathcal{O}) : H] \ln(d_K N(\mathfrak{fm})))^{2+\varepsilon}\right), \ d_K \text{ the discriminant of } K,$$

such that the graph $\mathcal{G}_{\mathcal{S}_B}$ is an expander graph. In particular, for any subset W of $H(\mathcal{A})$, any walk of length at least $\log(2|H|/\sqrt{|W|})$ starting from a given vertex will end in W with a probability between $\frac{|W|}{2|H|}$ and $\frac{3|W|}{2|H|}$. The graph $\mathcal{G}_{\mathcal{S}_B}$ is connected and rapidly mixes random walks.

This graph was used in [69] to prove random self-reducibility of the discrete logarithm problem in genus 2 and explicitly compute isogenies between Jacobians of genus 2 hyperelliptic curves.

From here, we can see that we are in the genus two analog of the CRS. In fact, $(H, H(\mathcal{A}))$ is an HHS with the complex multiplication action. As before, it is useful to use a graph and use a generating set of the group H for the group action so that the system can be implemented in polynomial time in $\log q$.

From now on we focus on a primitive CM-field K of degree 4 and we have $|\mathcal{O}_0^+/\operatorname{norm}_{K/K_0}(\mathcal{O}^*)| \in \{1,2\}$. We let

$$\mathcal{S}_B = \{\text{ideals of } \mathcal{O} \text{ of prime norm bounded by } B \text{ and coprime to } 2 \times [\mathcal{O}_K : \mathbb{Z}[\pi, \bar{\pi}]]\}.$$

In this case, by Theorem 4.3.2.5, we can compute all the isogenies corresponding to elements in $\mathcal{S}_B$. If $|\mathcal{O}_0^+/\operatorname{norm}_{K/K_0}(\mathcal{O}^*)|$ is one, navigating the isogeny graph is easy and each vertex can be represented by the absolute Igusa invariants of the corresponding abelian surface. Igusa invariants are the anolog of the j-invariant for abelian surfaces, see [112]. However, when it is two, each vertex corresponds to a pair of polarizable abelian varieties, see [69, Section 4.2] for more detail for that case.

By [69, Lemma 2.1] the index $[\mathrm{Pic}(\mathcal{O}) : H]$ is either the cardinality or half the cardinality of the narrow class class group of $\mathcal{O}_0 := \mathcal{O} \cap K_0$ and for a proper choice of K, it can be polynomial in $\log q$. The index $[\mathcal{O}_K : \mathbb{Z}[\pi, \overline{\pi}]]$ is less than $4q^2$, by [13, Lemma III.2.5]. The bound B in Theorem 5.3.1.1 is then polynomial in $\log q$ for a proper choice of parameters..

If K is chosen so that $h^+_{\mathcal{O}_0} := |\mathrm{Cl}^+(\mathcal{O}_0)|$ is polynomial in $\log q$, we only need to consider separable isogenies of degree polynomial in $\log q$ (up to the bound B) to obtain an expander graph. Also any path of length at least $\log(2|H|) \leq \log(2|\operatorname{Pic}(\mathcal{O})|)$ from any vertex will end in a subset W with the probability between $\frac{|W|}{2|H|}$ and $\frac{3|W|}{2|H|}$. Since the size of the Picard group $\mathrm{Pic}(\mathcal{O})$ is polynomial in q, [13, 69], $\log(2|H|)$ is polynomial in $\log q$. The cost of computing an isogeny path of length $\log(2|H|)$ is at most polynomial. It follows that the implementation of the system is at most polynomial in $\log q$.

5.3.2 Key exchange protocol

We describe a public key exchange protocol with ordinary, principally polarized, absolutely simple abelian surfaces much like in Section 5.2.1.2.

We start with a principally polarized, absolutely simple, ordinary abelian surface $\mathcal{A}_0/\mathbb{F}_q$, whose endomorphism ring is not computable in subexponential time with current methods, see Section 4.5.1. Let $\mathcal{O}$ be its endomorphism ring in a quartic CM-field K and we let $|\mathcal{O}_0^+/\operatorname{norm}_{K/K_0}(\mathcal{O}^*)| = 1$, for simplicity. The protocol uses elements in the set $V_{\mathbb{F}_q}(\mathcal{O})$, the set of isomorphism classes of principally polarized, absolutely simple, and ordinary abelian varieties isogenous to $\mathcal{A}_0$ and with the same endomorphism ring, without explicitly computing $\mathcal{O}$.

Let $\{\ell_1, \ldots, \ell_m\}$ be the set of prime numbers corresponding to the norm of ideals in the set $\mathcal{S}_B$ (Theorem 5.3.1.1). For each prime ℓ_i, $\chi_{\mathcal{A}_0} \mod \ell_i$ either has four roots $\lambda_{i,1}, \overline{\lambda}_{i,1}, \lambda_{i,2}, \overline{\lambda}_{i,2}$ or two roots $\lambda_{i,1}, \overline{\lambda}_{i,1}$, where $\chi_{\mathcal{A}_0}$ is the characteristic polynomial of the Frobenius endomorphism of $\mathcal{A}_0$. Let $L_i = \{(\ell_i, \lambda_{i,j}) : j = 1 \text{ or } j \in \{1, 2\}\}$ and $L = \cup L_i$.

The parameters of the protocols are:

- The abelian variety $\mathcal{A}_0/\mathbb{F}_q$,
- The set L.

An element $(\ell_i, \lambda_{i,j})$ corresponds to the isogeny associated to the prime ideal generated by ℓ_i and $\pi - \lambda_{i,j}$, which corresponds to the isogeny with kernel $\mathcal{A}_0[\ell_i] \cap \ker(\pi - \lambda_{i,j})$. The elements $\overline{\lambda}_{i,j}$ are not included in the set L, they are considered as backward walk. Two parties, Alice and Bob can exchange a secret key as follows:

- Alice chooses a walk of length at least the bound in Theorem 5.3.1.1 to ensure random mixing and shares the variety $\mathcal{A}_A$ or the absolute Igusa invariants of $\mathcal{A}_A$.
- Bob does the same and shares $\mathcal{A}_B$ or the absolute Igusa invariants of $\mathcal{A}_B$.
- After exchanging both varieties, Alice takes the same walk but starting from $\mathcal{A}_B$ and obtains $\mathcal{A}_{BA}$.
- Bob also takes the same walk as before but starting from $\mathcal{A}_A$ and obtains $\mathcal{A}_{AB}$.

Both parties get the same variety as shared key. This is the same procedure as the Rostovtsev-Stolbunov key exchange protocol, however, the technique used to solve the Rostovtsev-Stolbunov key exchange protocol in quantum subexponential time does not work in our case. In fact the main obstacle is the computation of the endomorphism rings.

5.3.3 Cryptosystem security

We choose $\mathcal{A}$ in such a way that computing the endomorphism ring can only be achieved in exponential time with current methods.

In order to attack the system, the following problem has to be solved:

Problem 5.3.3.1. *Given two isogenous principally polarized, absolutely simple and ordinary abelian surfaces $\mathcal{A}$ and $\mathcal{B}$ defined over a finite field $\mathbb{F}_q$, find an isogeny walk from $\mathcal{A}$ to $\mathcal{B}$.*

5.3.3.1 Classical security

The current best classical method for solving Problem 5.3.3.1 is found in [69, Section 5]. It is a generalization of the method of Galbraith [58] and works as follows:

Algorithm 21 `Isogeny path problem in genus 2 [69]`

Input: Horizontally isogenous ordinary abelian varieties $\mathcal{A}/\mathbb{F}_q$ and $\mathcal{B}/\mathbb{F}_q$.

Output: An isogeny from $\mathcal{A}$ to $\mathcal{B}$ with smooth order.

1: Build independent random paths in $\mathcal{G}_{\mathcal{S}_B}$ of length $O(\log q)$ from $\mathcal{A}$ until $O(q)$ vertices are reached.
2: Build independent random paths of length $O(\log q)$ from $\mathcal{B}$ until a collision occurs with one of the paths generated in Step 1.
3: Compute a short path between $\mathcal{A}$ and $\mathcal{B}$.
4: Return the corresponding isogeny.

In the algorithm we compute $O(q)$ isogenies of degrees at most $\log(q)$. So the complexity of all the computations is exponential in $\log q$. This is the currently known best classical attack on the cryptosystem.

5.3.3.2 Quantum security

The best known quantum algorithm that solves the isogeny path problem uses algorithms that solve the hidden shift problem. It is the only subexponential method that we know of. In order to use the hidden shift algorithm to attack the system, we need to know the Picard group of the endomorphism ring. The endomorphism ring is not part of the public parameters that are used to implement the protocol and can be kept secret.

The orders that we constructed in Chapter 4 are of the form $\mathbb{Z} + p^2\mathbb{Z}[\tau, \overline{\tau}]$, for τ a p-Weil number, with p a prime number. There are methods to compute abelian surfaces defined over finite fields with a given endomorphism ring $\mathcal{O}$. For the CM method for example, we first compute the Igusa class polynomials corresponding to the order $\mathcal{O}$, which have their coefficients in $\mathbb{Q}$, and then take them modulo q, a power of some prime p_1 and

get the roots corresponding to the absolute Igusa invariants of the some abelian surface defined over $\mathbb{F}_q$. We then construct the corresponding abelian surface $\mathcal{A}$ defined over $\mathbb{F}_q$ with $\mathrm{End}(\mathcal{A})$ isomorphic to $\mathcal{O}$. Although we use orders of the form $\mathbb{Z} + p^2\mathbb{Z}[\tau, \overline{\tau}]$, the Frobenius endomorphism of the abelian surface we obtain is not necessarily $p^2\tau$ and the variety is not necessarily defined over a field of characteristic p. Hence, even though we use orders of the form $\mathbb{Z} + p^2\mathbb{Z}[\tau, \overline{\tau}]$, to the best of our knowledge, this fact does not introduce any weaknesses or help an attacker.

The best known algorithm that can compute the endomorphism ring of abelian surfaces used in our protocol is the one from Eisenträger and Lauter, [49], and it has exponential complexity in $\log q$. We know of no quantum algorithm that solves the endomorphism ring computation with complexity better than the current classical ones. For elliptic curves, even if the endomorphism ring is not given, there are subexponential algorithms that compute endomorphism rings of any ordinary elliptic curves, as discussed in Chapter 3.

In order to use algorithms that solve the hidden shift problem, we need to first compute the endomorphism ring of $\mathcal{A}$ and so cannot be achieve subexponential complexity.

5.3.4 Public key selection

For an efficient implementation of the system, it is important that the majority of the primes in L from Section 5.3.2 divide $|\mathcal{A}_0(\mathbb{F}_q)|$. For abelian surfaces this is difficult to achieve. The main task is to construct an abelian surface satisfying that property and whose endomorphism ring cannot be computed by current subexponential algorithms.

We first describe a method that produces q-Weil numbers, q a power of a prime p, in a quartic CM-field field K.

5.3.4.1 Construction of Weil numbers

We recall that a q-Weil number π in K is an algebraic integer in K such that for all embeddings $\sigma : K \to \mathbb{C}$, we have $|\sigma(\pi)| = \sqrt{q}$.

Let p be a prime. We start by decomposing the ideal $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$. Let $\mathcal{P}$ be the subgroup of $\mathcal{I}_K$ generated by $\mathfrak{p}_1, \ldots, \mathfrak{p}_4$. Let

$$\begin{aligned} f : \mathcal{P} &\to \mathrm{Cl}_K \\ \mathfrak{p}_i &\mapsto [\mathfrak{p}_i]. \end{aligned}$$

The elements in the subgroup $F = \ker f$ are principal ideals. If we take the cone C inside F, consisting of integral ideals in F, then it is generated by ideals that are generated by Weil numbers.

Algorithm 22 *q-Weil numbers*

Input: A CM-field K and a prime number p.

Output: A cone containing q-Weil numbers for different powers q of p.

1: Factor $p\mathcal{O}_K$, and let $\mathfrak{p}_1 \ldots, \mathfrak{p}_r$.
2: Compute $\ker f$.
3: Construct C, subgroup generated by the integral elements I in $\ker f$ i.e $I \cap \mathcal{O}_K = I$.
4: Return a set S consisting of generators of ideals in C.

Proposition 5.3.4.1. *Any principal ideal in the generating set S in Algorithm 22 is generated by some q-Weil number.*

Proof. Let $I = \langle \alpha \rangle \in S$. Then $|\operatorname{norm}_{K/K_0}(\alpha)| = |\alpha\overline{\alpha}| = q$, with q some power of p. Let σ be an embedding from K to $\mathbb{C}$. Since K is a CM-field, by Lemma 2.4.1.2, σ commutes with the complex conjugate map. Hence $|\sigma(\alpha\overline{\alpha})| = |\sigma(\alpha)\overline{\sigma(\alpha)}| = |\sigma(\alpha)|^2 = q$. Hence α is a q-Weil number. □

The complexity of the algorithm is at most subexponential in the discriminant of K.

5.3.4.2 Abelian surfaces with given properties

For an order $\mathcal{O}$ in a quartic CM-field, we define $\mathcal{A}_\mathcal{O}$ to be the set of isomorphic classes of principally polarized and simple complex abelian surfaces with endomorphism ring isomorphism to $\mathcal{O}$. The set $\mathcal{A}_\mathcal{O}$ is known to be finite. The Igusa class polynomials H_1, H_2, H_3 are defined as follows:

$$H_j = \prod_{\mathcal{A} \in \mathcal{A}_\mathcal{O}} (x - i_j(\mathcal{A})), \quad j \in \{1, 2, 3\},$$

where the $i'_j s$ are the absolute Igusa invariants.

The following algorithm, known as the CM-method, constructs an abelian surface over some finite field with given endomorphism ring:

Algorithm 23 `Computation of abelian surfaces [22, 49]`

Input: A large prime p_1 and a p-Weil number τ.

Output: An ordinary abelian surface $\mathcal{A}$ defined over $\mathbb{F}_{p_1}$ with endomorphism ring isomorphic to $\mathcal{O} := \mathbb{Z} + p^2\mathbb{Z}[\tau, \overline{\tau}]$.

1: Compute the Igusa class polynomials H_1, H_2, H_3 of $\mathbb{Z} + p^2\mathbb{Z}[\tau, \overline{\tau}]$

2: From a triple of roots modulo p_1 of H_1, H_2, H_3, construct a genus 2 curve C over $\mathbb{F}_{p_1}$ using Mestre's algorithm.

3: Return the Jacobian $J(C)$

This algorithm has an exponential routine in the logarithm of the discriminant of the order $\mathcal{O}$, [49].

To obtain an abelian surface with a given order and with a given number of rational points, an early abort method that we presented in Algorithm 20 can provide abelian surfaces whose number of rational points is divisible by some primes. Unfortunately, the best way to generate good abelian surfaces which can make our system efficient has an exponential runtime. We are not interested in practical performance using ordinary abelian surfaces, but rather introduce the idea of subexponential quantum resistant non-interactive isogeny based cryptosystem. Our aim is to use supersingular or superspecial abelian surfaces to produce a genus 2 analog of CSIDH.

5.3.5 Potential applications

We do not provide a practical example since we are aware that it will be slow anyway. We rather discuss some interesting potential applications.

The CRS cryptosystem is inefficient but led to the construction of CSIDH which is fast to implement. Our method has the potential of leading to the first efficient non-interactive isogeny based key exchange protocol that can resist subexponential quantum attacks, a genus 2 CSIDH.

The idea is to use either supersingular abelian surfaces or superspecial abelian surfaces. An abelian variety is said to be supersingular if it is isogenous to a product of supersingular

elliptic curves over the algebraic closure of the base field. It is said to be superspecial if it is isomorphic to a product of supersingular elliptic curves over the algebraic closure of the base field. The two notions coincide with supersingularity in dimension one. More background on this can be found in [21].

It has already been established in [50] that over a field of characteristic p, superspecial curves, curves with Jacobian superspecial, can be written over $\mathbb{F}_{p^2}$, each having either the least or the most number of rational points allowed by the Weil conjectures and that for fixed p the number of superspecial curves of arbitrary genus is finite. This is similar to Theorem 5.2.2.3 for supersingular elliptic curves. However, some results, such as the commutative CM action on superisngular or supersingular abelian surfaces, like Theorem 5.2.2.5, need to be established before we are able to produce a genus 2 CSIDH.

This is beyond the scope of this thesis, and we leave that as an open problem which we will consider for future work.

Index

Bibliography

[1] Arthur Oliver Lonsdale Atkin and François Morain. Elliptic curves and primality proving. *Math. Comp.*, 61(203):29–68, 1993. [Cited on page 97.]

[2] Eric Bach. Explicit bounds for primality testing and related problems. *Math. Comp.*, 55(191):355–380, 1990. [Cited on page 44.]

[3] Hyman Bass. On the ubiquity of Gorenstein rings. *Math. Z.*, 82:8–28, 1963. [Cited on page 70.]

[4] Juliana Belding, Reinier Bröker, Andreas Enge, and Kristin Lauter. Computing Hilbert class polynomials. In *Algorithmic Number Theory Symposium*, volume 5011 of *Lecture Notes in Comput. Sci.*, pages 282–295. Springer, Berlin, 2008. [Cited on page 27.]

[5] Daniel J. Bernstein. How to find smooth parts of integers. *URL: http://cr. yp. to/papers. html# smoothparts. ID 201a045d5bb24f43f0bd0d97fcf5355a*, 20, 2004. [Cited on page 40.]

[6] Daniel J. Bernstein and Tanja Lange. Post-quantum cryptography. *Nature*, 549(7671):188–194, 2017. [Cited on page 88.]

[7] Daniel J. Bernstein, Tanja Lange, Chloe Martindale, and Lorenz Panny. Quantum circuits for the CSIDH: optimizing quantum evaluation of isogenies. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 409–441. Springer, 2019. [Cited on page 101.]

[8] Jean-François Biasse, Annamaria Iezzi, and Michael J. Jacobson, Jr. A note on the security of CSIDH. In *Progress in cryptology—INDOCRYPT 2018*, volume 11356 of *Lecture Notes in Comput. Sci.*, pages 153–168. Springer, Cham, 2018. [Cited on page 96.]

[9] Jean-François Biasse, David Jao, and Anirudh Sankar. A quantum algorithm for computing isogenies between supersingular elliptic curves. In *Progress in cryptology—INDOCRYPT 2014*, volume 8885 of *Lecture Notes in Comput. Sci.*, pages 428–442. Springer, Cham, 2014. [Cited on pages 89 and 101.]

[10] Jean-François Biasse, Claus Fieker, and Michael J. Jacobson, Jr. Fast heuristic algorithms for computing relations in the class group of a quadratic order, with applications to isogeny evaluation. *LMS Journal of Computation and Mathematics*, 19(A):371–390, 2016. [Cited on page 96.]

[11] Christina Birkenhake and Herbert Lange. *Complex abelian varieties*, volume 302 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2004. [Cited on page 9.]

[12] Gaetan Bisson. Computing endomorphism rings of elliptic curves under the GRH. *J. Math. Cryptol.*, 5(2):101–113, 2011. [Cited on pages viii, 2, 4, 27, 28, 34, 35, 37, 39, 40, 41, 42, 43, 46, 53, 54, and 74.]

[13] Gaetan Bisson. *Endomorphism Rings in Cryptography*. Theses (PhD), Institut National Polytechnique de Lorraine - INPL ; Technische Universiteit Eindhoven, July 2011. [Cited on pages viii, 30, 33, 35, 38, 47, 54, 58, 59, 60, and 105.]

[14] Gaetan Bisson. Computing endomorphism rings of abelian varieties of dimension two. *Math. Comp.*, 84(294):1977–1989, 2015. [Cited on pages viii, 2, 28, 57, 58, 59, 60, 61, 62, 64, 66, 67, 68, 69, 70, 71, 73, 74, 79, 80, and 83.]

[15] Gaetan Bisson, Robert Cosset, Damien Robert, et al. Avisogenies (abelian varieties and isogenies). *Magma package for explicit isogenies between abelian varieties*, 2010. [Cited on page 74.]

[16] Gaetan Bisson and Marco Streng. On polarised class groups of orders in quartic CM-fields. *Math. Res. Lett.*, 24(2):247–270, 2017. [Cited on pages 75, 76, 78, 83, 84, and 85.]

[17] Gaetan Bisson and Andrew V. Sutherland. Computing the endomorphism ring of an ordinary elliptic curve over a finite field. *J. Number Theory*, 131(5):815–831, 2011. [Cited on pages 2, 27, 34, 43, 54, 55, 56, 58, and 68.]

[18] Xavier Bonnetain and André Schrottenloher. Quantum security analysis of csidh and ordinary isogeny-based schemes. *IACR Cryptol. ePrint Arch.*, 2018:537, 2018. [Cited on page 101.]

[19] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system i: The user language. *Journal of Symbolic Computation*, 24(3-4):235–265, 1997. [Cited on page 54.]

[20] Johannes Franciscus Brakenhoff. *Counting problems for number rings*. PhD thesis, Leiden University, 2009. [Cited on page 80.]

[21] Bradley Wayne Brock. *Superspecial curves of genera two and three*. ProQuest LLC, Ann Arbor, MI, 1993. Thesis (Ph.D.)–Princeton University. [Cited on page 111.]

[22] Reinier Bröker, Kristin Lauter, and Marco Streng. Abelian surfaces admitting an (l, l)-endomorphism. *J. Algebra*, 394:374–396, 2013. [Cited on pages viii and 110.]

[23] Reinier Bröker, Kristin Lauter, and Andrew V. Sutherland. Modular polynomials via isogeny volcanoes. *Math. Comp.*, 81(278):1201–1231, 2012. [Cited on pages 33 and 50.]

[24] Ernest Hunter Brooks, Dimitar Jetchev, and Benjamin Wesolowski. Isogeny graphs of ordinary abelian varieties. *Res. Number Theory*, 3:Paper No. 28, 38, 2017. [Cited on pages 63, 83, and 86.]

[25] Johannes Buchmann. A subexponential algorithm for the determination of class groups and regulators of algebraic number fields. In *Séminaire de Théorie des Nombres, Paris 1988–1989*, volume 91 of *Progr. Math.*, pages 27–41. Birkhäuser Boston, Boston, MA, 1990. [Cited on pages 38, 46, and 63.]

[26] David A. Burgess. The distribution of quadratic residues and non-residues. *Mathematika*, 4:106–112, 1957. [Cited on page 44.]

[27] Rodney Canfield, Paul Erdős, and Carl Pomerance. On a problem of Oppenheim concerning "factorisatio numerorum". *J. Number Theory*, 17(1):1–28, 1983. [Cited on page 45.]

[28] John William Scott Cassels and A. Fröhlich, editors. *Algebraic number theory*. Academic Press, Inc. [Harcourt Brace Jovanovich, Publishers], London, 1986. Reprint of the 1967 original. [Cited on pages 22 and 36.]

[29] Wouter Castryck, Thomas Decru, and Benjamin Smith. Hash functions from superspecial genus-2 curves using Richelot isogenies. *J. Math. Cryptol.*, 14(1):268–292, 2020. [Cited on page 102.]

[30] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: an efficient post-quantum commutative group action. In *Advances in*

cryptology—ASIACRYPT 2018. Part III, volume 11274 of *Lecture Notes in Comput. Sci.*, pages 395–427. Springer, Cham, 2018. [Cited on pages 4, 88, 89, and 98.]

[31] Tommaso Giorgio Centeleghe and Jakob Stix. Categories of abelian varieties over finite fields, I: Abelian varieties over $\mathbb{F}_p$. *Algebra Number Theory*, 9(1):225–265, 2015. [Cited on page 72.]

[32] Denis X. Charles, Kristin E. Lauter, and Eyal Z. Goren. Cryptographic hash functions from expander graphs. *J. Cryptology*, 22(1):93–113, 2009. [Cited on page 4.]

[33] Rong-Jaye Chen. Schoof-Elkies-Atkin algorithm. *PhD thesis, Department of Computer Science, National Chiao Tung University*, pages 1–17, 2008. [Cited on page 31.]

[34] Andrew Childs, David Jao, and Vladimir Soukharev. Constructing elliptic curve isogenies in quantum subexponential time. *J. Math. Cryptol.*, 8(1):1–29, 2014. [Cited on pages viii, 3, 4, 39, 40, 46, 78, 88, 95, and 96.]

[35] Paula Cohen. On the coefficients of the transformation polynomials for the elliptic modular function. *Math. Proc. Cambridge Philos. Soc.*, 95(3):389–402, 1984. [Cited on page 33.]

[36] Romain Cosset and Damien Robert. Computing (ℓ, ℓ)-isogenies in polynomial time on Jacobians of genus 2 curves. *Math. Comp.*, 84(294):1953–1975, 2015. [Cited on pages 63, 64, and 65.]

[37] Craig Costello and Benjamin Smith. The supersingular isogeny problem in genus 2 and beyond. In *Post-quantum cryptography*, volume 12100 of *Lecture Notes in Comput. Sci.*, pages 151–168. Springer, Cham, [2020] ©2020. [Cited on page 102.]

[38] Jean-Marc Couveignes. Hard homogeneous spaces. *IACR Cryptol. ePrint Arch.*, 2006:291, 2006. https://ia.cr/2006/291. [Cited on pages 3, 87, and 88.]

[39] Jean-Marc Couveignes. Linearizing torsion classes in the Picard group of algebraic curves over finite fields. *J. Algebra*, 321(8):2085–2118, 2009. [Cited on pages 59 and 64.]

[40] David A. Cox. *Primes of the form $x^2 + ny^2$*. Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, second edition, 2013. Fermat, class field theory, and complex multiplication. [Cited on pages 36 and 50.]

[41] Luca De Feo. Mathematics of isogeny based cryptography. *arXiv preprint arXiv:1711.04062*, 12, 2017. [Cited on page 93.]

[42] Luca De Feo, David Jao, and Jérôme Plût. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *J. Math. Cryptol.*, 8(3):209–247, 2014. [Cited on page 4.]

[43] Luca De Feo, Jean Kieffer, and Benjamin Smith. Towards practical key exchange from ordinary isogeny graphs. In *Advances in cryptology—ASIACRYPT 2018. Part III*, volume 11274 of *Lecture Notes in Comput. Sci.*, pages 365–394. Springer, Cham, 2018. [Cited on pages viii, 3, 88, 97, and 98.]

[44] Christina Delfs and Steven D. Galbraith. Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$. *Des. Codes Cryptogr.*, 78(2):425–440, 2016. [Cited on pages 99 and 101.]

[45] Pierre Deligne. Variétés abéliennes ordinaires sur un corps fini. *Invent. Math.*, 8:238–243, 1969. [Cited on pages 23 and 25.]

[46] Alina Dudeanu, Dimitar Jetchev, Damien Robert, and Marius Vuille. Cyclic isogenies for abelian varieties with real multiplication. *arXiv: Number Theory*, 2017. [Cited on pages 63, 65, and 66.]

[47] Kirsten Eisenträger, Sean Hallgren, Kristin Lauter, Travis Morrison, and Christophe Petit. Supersingular isogeny graphs and endomorphism rings: reductions and solutions. In *Advances in cryptology—EUROCRYPT 2018. Part III*, volume 10822 of *Lecture Notes in Comput. Sci.*, pages 329–368. Springer, Cham, 2018. [Cited on page 27.]

[48] Kirsten Eisenträger, Sean Hallgren, Chris Leonardi, Travis Morrison, and Jennifer Park. Computing endomorphism rings of supersingular elliptic curves and connections to path-finding in isogeny graphs. *Open Book Series*, 4(1):215–232, 2020. [Cited on pages 1 and 27.]

[49] Kirsten Eisenträger and Kristin Lauter. A CRT algorithm for constructing genus 2 curves over finite fields. In *Arithmetics, geometry, and coding theory (AGCT 2005)*, volume 21 of *Sémin. Congr.*, pages 161–176. Soc. Math. France, Paris, 2010. [Cited on pages viii, 1, 2, 57, 58, 74, 108, and 110.]

[50] Torsten Ekedahl. On supersingular curves and abelian varieties. *Math. Scand.*, 60(2):151–178, 1987. [Cited on page 111.]

[51] Andreas Enge. Computing modular polynomials in quasi-linear time. *Math. Comp.*, 78(267):1809–1824, 2009. [Cited on page 33.]

[52] Claus Fieker, William Hart, Tommy Hofmann, and Fredrik Johansson. Nemo/Hecke: Computer algebra and number theory packages for the julia programming language. In *Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation*, ISSAC '17, pages 157–164, New York, NY, USA, 2017. ACM. [Cited on page 74.]

[53] Claus Fieker, Tommy Hofmann, and Sogo Pierre Sanon. On the computation of the endomorphism rings of abelian surfaces. *J. Number Theory*, 229:39–52, 2021. [Cited on pages ii, iii, 4, 28, 57, 58, 69, and 80.]

[54] Enric Florit and Benjamin Smith. Automorphisms and isogeny graphs of abelian varieties, with applications to the superspecial richelot isogeny graph. *arXiv preprint arXiv:2101.00919*, 2021. [Cited on page 102.]

[55] Victor E. Flynn and Yan Bo Ti. Genus two isogeny cryptography. In *Post-quantum cryptography*, volume 11505 of *Lecture Notes in Comput. Sci.*, pages 286–306. Springer, Cham, 2019. [Cited on pages 89, 102, and 103.]

[56] Mireille Fouquet. *Anneau d'endomorphismes et cardinalité des couples elliptiques: aspects algorithmiques*. PhD thesis, Palaiseau, Ecole polytechnique, 2001. [Cited on page 32.]

[57] Mireille Fouquet and François Morain. Isogeny volcanoes and the SEA algorithm. In *Algorithmic Number Theory Symposium (Sydney, 2002)*, volume 2369 of *Lecture Notes in Comput. Sci.*, pages 276–291. Springer, Berlin, 2002. [Cited on pages 32 and 43.]

[58] Steven D. Galbraith. Constructing isogenies between elliptic curves over finite fields. *LMS Journal of Computation and Mathematics*, 2:118–138, 1999. [Cited on page 107.]

[59] Steven D. Galbraith, Florian Hess, and Nigel P. Smart. Extending the GHS Weil descent attack. In *Advances in cryptology—EUROCRYPT 2002 (Amsterdam)*, volume 2332 of *Lecture Notes in Comput. Sci.*, pages 29–44. Springer, Berlin, 2002. [Cited on pages viii, 41, 63, 94, and 95.]

[60] Steven D. Galbraith, Christophe Petit, Barak Shani, and Yan Bo Ti. On the security of supersingular isogeny cryptosystems. In *Advances in cryptology—ASIACRYPT 2016. Part I*, volume 10031 of *Lecture Notes in Comput. Sci.*, pages 63–91. Springer, Berlin, 2016. [Cited on page 102.]

[61] Ben Galin. Schoof-Elkies-Atkin algorithm. *Senior thesis, Department of Mathematics, Stanford University, USA*, 2007. [Cited on page 31.]

[62] Andrew Granville. Smooth numbers: computational number theory and beyond. In *Algorithmic number theory: lattices, number fields, curves and cryptography*, volume 44 of *Math. Sci. Res. Inst. Publ.*, pages 267–323. Cambridge Univ. Press, Cambridge, 2008. [Cited on page 45.]

[63] Cornelius Greither. On the two generator problem for the ideals of a one-dimensional ring. *J. Pure Appl. Algebra*, 24(3):265–276, 1982. [Cited on pages 70 and 71.]

[64] James L. Hafner and Kevin S. McCurley. A rigorous subexponential algorithm for computation of class groups. *Journal of the American Mathematical Society*, 2(4):837–850, 1989. [Cited on page 38.]

[65] Tommy Hofmann and Carlo Sircana. On the computation of overorders. *Int. J. Number Theory*, 16(4):857–879, 2020. [Cited on pages 49, 69, 70, and 71.]

[66] David Jao, Stephen D. Miller, and Ramarathnam Venkatesan. Do all elliptic curves of the same order have the same difficulty of discrete log? In *Advances in cryptology—ASIACRYPT 2005*, volume 3788 of *Lecture Notes in Comput. Sci.*, pages 21–40. Springer, Berlin, 2005. [Cited on page 91.]

[67] David Jao, Stephen D. Miller, and Ramarathnam Venkatesan. Expander graphs based on GRH with an application to elliptic curve cryptography. *J. Number Theory*, 129(6):1491–1504, 2009. [Cited on pages 91 and 92.]

[68] David Jao and Vladimir Soukharev. A subexponential algorithm for evaluating large degree isogenies. In *Algorithmic Number Theory Symposium*, volume 6197 of *Lecture Notes in Comput. Sci.*, pages 219–233. Springer, Berlin, 2010. [Cited on page 90.]

[69] Dimitar Jetchev and Benjamin Wesolowski. Horizontal isogeny graphs of ordinary abelian varieties and the discrete logarithm problem. *Acta Arith.*, 187(4):381–404, 2019. [Cited on pages viii, 104, 105, and 107.]

[70] Jürgen Klüners and Sebastian Pauli. Computing residue class rings and Picard groups of orders. *J. Algebra*, 292(1):47–64, 2005. [Cited on pages 48, 49, 52, and 77.]

[71] Neal Koblitz. Hyperelliptic cryptosystems. *J. Cryptology*, 1(3):139–150, 1989. [Cited on page 102.]

[72] David Russell Kohel. *Endomorphism rings of elliptic curves over finite fields*. ProQuest LLC, Ann Arbor, MI, 1996. Thesis (Ph.D.)–University of California, Berkeley. [Cited on pages viii, 2, 4, 27, 30, 31, 32, and 33.]

[73] Greg Kuperberg. A subexponential-time quantum algorithm for the dihedral hidden subgroup problem. *SIAM J. Comput.*, 35(1):170–188, 2005. [Cited on page 96.]

[74] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002. [Cited on page 81.]

[75] Serge Lang. *Complex multiplication*, volume 255. Springer Science & Business Media, 2012. [Cited on pages 9 and 15.]

[76] Hendrik Willem Lenstra, Jr. Algorithms in algebraic number theory. *Bull. Amer. Math. Soc. (N.S.)*, 26(2):211–244, 1992. [Cited on page 71.]

[77] Hendrik Willem Lenstra, Jr. and Carl Pomerance. A rigorous time bound for factoring integers. *J. Amer. Math. Soc.*, 5(3):483–516, 1992. [Cited on page 44.]

[78] David Lubicz and Damien Robert. Computing isogenies between abelian varieties. *Compositio Mathematica*, 148(5):1483–1515, 2012. [Cited on page 64.]

[79] Chang Lv and YingPu Deng. On orders in number fields: Picard groups, ring class fields and applications. *Sci. China Math.*, 58(8):1627–1638, 2015. [Cited on page 6.]

[80] Stefano Marseglia. Computing the ideal class monoid of an order. *J. Lond. Math. Soc. (2)*, 101(3):984–1007, 2020. [Cited on page 69.]

[81] Jean-François Mestre. Construction de courbes de genre 2 à partir de leurs modules. In *Effective methods in algebraic geometry (Castiglioncello, 1990)*, volume 94 of *Progr. Math.*, pages 313–334. Birkhäuser Boston, Boston, MA, 1991. [Cited on page 64.]

[82] James S. Milne. Abelian varieties. *Arithmetic geometry*, pages 103–150, 1986. [Cited on page 9.]

[83] James S. Milne. Jacobian varieties. In *Arithmetic geometry*, pages 167–212. Springer, 1986. [Cited on pages 9 and 14.]

[84] James S. Milne. Complex multiplication. *Lecture notes available at http://www.jmilne.org/math/*, 2006. [Cited on pages 17 and 18.]

[85] Bodo Moeller, Nelson Bolyard, Vipul Gupta, Simon Blake-Wilson, and Chris Hawk. Elliptic curve cryptography (ECC) cipher suites for transport layer security (TLS). RFC 4492, May 2006. https://www.rfc-editor.org/info/rfc4492. [Cited on page 1.]

[86] Peter L. Montgomery. A survey of modern integer factorization algorithms. *CWI Quarterly*, 7(4):337–366, 1994. [Cited on page 44.]

[87] David Mumford. On the equations defining abelian varieties. I. *Invent. Math.*, 1:287–354, 1966. [Cited on page 65.]

[88] David Mumford. On the equations defining abelian varieties. II. *Invent. Math.*, 3:75–135, 1967. [Same as above.]

[89] David Mumford. On the equations defining abelian varieties. III. *Invent. Math.*, 3:215–244, 1967. [Same as above.]

[90] David Mumford. *Tata lectures on theta. II*, volume 43 of *Progress in Mathematics*. Birkhäuser Boston, Inc., Boston, MA, 1984. Jacobian theta functions and differential equations, With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman and H. Umemura. [Cited on page 65.]

[91] David Mumford. *Abelian varieties*. Studies in mathematics. Hindustan Book Agency, 2008. [Cited on pages 9 and 11.]

[92] Satoshi Nakamoto and A. Bitcoin. A peer-to-peer electronic cash system. *Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf*, 4, 2008. [Cited on page 1.]

[93] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. [Cited on page 6.]

[94] Christophe Petit. Faster algorithms for isogeny problems using torsion point images. In *Advances in cryptology—ASIACRYPT 2017. Part II*, volume 10625 of *Lecture Notes in Comput. Sci.*, pages 330–353. Springer, Cham, 2017. [Cited on page 102.]

[95] Arnold K. Pizer. Ramanujan graphs and Hecke operators. *Bull. Amer. Math. Soc. (N.S.)*, 23(1):127–137, 1990. [Cited on page 99.]

[96] Arnold K. Pizer. Ramanujan graphs. In *Computational perspectives on number theory (Chicago, IL, 1995)*, volume 7 of *AMS/IP Stud. Adv. Math.*, pages 159–178. Amer. Math. Soc., Providence, RI, 1998. [Cited on page 99.]

[97] Michael Pohst and Hans Zassenhaus. *Algorithmic algebraic number theory*, volume 30 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 1997. Revised reprint of the 1989 original. [Cited on page 52.]

[98] Oded Regev. A subexponential time algorithm for the dihedral hidden subgroup problem with polynomial space. *arXiv preprint quant-ph/0406151*, 2004. [Cited on page 96.]

[99] Eric Rescorla and Tim Dierks. The Transport Layer Security (TLS) Protocol Version 1.2. RFC 5246, August 2008. https://www.rfc-editor.org/info/rfc5246. [Cited on page 1.]

[100] Martin Roetteler, Michael Naehrig, Krysta M Svore, and Kristin Lauter. Quantum resource estimates for computing elliptic curve discrete logarithms. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 241–270. Springer, 2017. [Cited on pages 1, 3, and 87.]

[101] Alexander Rostovtsev and Anton Stolbunov. Public-key cryptosystem based on isogenies. Cryptology ePrint Archive, Report 2006/145, 2006. https://eprint.iacr.org/2006/145. [Cited on pages 3, 87, and 88.]

[102] Asep Saepulrohman, Asep Denih, and A Talib Bon. Elliptic curve diffie-hellman cryptosystem for public exchange process. In *The 5th NA International Conference on Industrial Engineering and Operations Management*, pages 1–6, 2020. [Cited on page 27.]

[103] René Schoof. Nonsingular plane cubic curves over finite fields. *J. Combin. Theory Ser. A*, 46(2):183–211, 1987. [Cited on page 100.]

[104] René Schoof. Counting points on elliptic curves over finite fields. *Journal de Théorie des Nombres de Bordeaux*, 7(1):219–254, 1995. [Cited on page 31.]

[105] Jean-Pierre Serre and John Tate. Good reduction of abelian varieties. *Ann. of Math. (2)*, 88:492–517, 1968. [Cited on pages 23 and 25.]

[106] Martin Seysen. A probabilistic factorization algorithm with quadratic forms of negative discriminant. *Math. Comp.*, 48(178):757–780, 1987. [Cited on pages 38, 40, 46, and 63.]

[107] Goro Shimura. Complex multiplication of abelian varieties and its application to number theory. *Publ. Math. Soc. Japan*, 6, 1961. [Cited on pages 16, 17, 18, 19, 20, 21, 22, and 23.]

[108] Peter W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *35th Annual Symposium on Foundations of Computer Science (Santa Fe, NM, 1994)*, pages 124–134. IEEE Comput. Soc. Press, Los Alamitos, CA, 1994. [Cited on pages 3 and 87.]

[109] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986. [Cited on pages 29, 99, and 100.]

[110] Caleb Springer. Computing the endomorphism ring of an ordinary abelian surface over a finite field. *J. Number Theory*, 202:430–457, 2019. [Cited on pages 2, 28, 57, 68, 69, 73, 75, 82, 83, and 86.]

[111] Peter Stevenhagen. The arithmetic of number rings. In *Algorithmic number theory: lattices, number fields, curves and cryptography*, volume 44 of *Math. Sci. Res. Inst. Publ.*, pages 209–266. Cambridge Univ. Press, Cambridge, 2008. [Cited on page 48.]

[112] Marco Streng. *Complex multiplication of abelian surfaces*. Mathematical Institute, Faculty of Science, Leiden University, 2010. [Cited on pages 16, 23, and 105.]

[113] Andrew V. Sutherland. Computing Hilbert class polynomials with the Chinese Remainder Theorem. *Mathematics of Computation*, 80(273):501–538, 2011. [Cited on pages 1 and 43.]

[114] Andrew V. Sutherland. Accelerating the CM method. *LMS J. Comput. Math.*, 15:172–204, 2012. [Cited on page 97.]

[115] Andrew V. Sutherland. Isogeny volcanoes. In *Proceedings of the Tenth Algorithmic Number Theory Symposium*, volume 1 of *Open Book Ser.*, pages 507–530. Math. Sci. Publ., Berkeley, CA, 2013. [Cited on page 91.]

[116] Halil Kemal Taşkın and Murat Cenk. Tmvp-friendly primes for efficient elliptic curve cryptography. In *2020 International Conference on Information Security and Cryptology (ISCTURKEY)*, pages 80–87. IEEE, 2020. [Cited on page 1.]

[117] John Tate. Endomorphisms of abelian varieties over finite fields. *Invent. Math.*, 2:134–144, 1966. [Cited on pages 23 and 24.]

[118] Ruggiero Torelli. Sulle varietà di jacobi. *Rendiconti della Reale Accademia Nazionale dei Lincei*, 22.5:98–103, 1913. [Cited on page 14.]

[119] Nikolaj Tschebotareff. Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören. *Mathematische Annalen*, 95(1):191–228, 1926. [Cited on page 44.]

[120] Jacques Vélu. Isogénies entre courbes elliptiques. *CR Acad. Sci. Paris, Séries A*, 273:305–347, 1971. [Cited on page 41.]

[121] Markus Wagner. Über Korrespondenzen zwischen algebraischen Funktionenkörpern. *Ph.D. thesis, Technische Universität Berlin*, 2009. http://www.math.tu-berlin.de/ ẅagner/Diss.pdf. [Cited on pages 58 and 59.]

[122] William C. Waterhouse. Abelian varieties over finite fields. In *Annales scientifiques de l'École Normale Supérieure*, volume 2, pages 521–560, 1969. [Cited on pages 23 and 25.]

[123] William. C. Waterhouse and James S. Milne. Abelian varieties over finite fields. In *1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969)*, pages 53–64, 1971. [Cited on page 23.]

[124] André Weil. *Sur les courbes algébriques et les variétés qui s'en déduisent*, volume 7 of *Publ. Inst. Math. Univ. Strasbourg*. Hermann et Cie., Paris, 1948. [Cited on page 23.]

Curriculum Vitae

Technische Universitat Kaiserslautern	Kaiserslautern, Germany
Ph.D. in Mathematics.	2018–Current
Stellenbosch University	Stellenbosch, South Africa
M.Sc. in Mathematics.	2016–2017
African Institute of Mathematical Sciences	Cape Town, South Africa
Structured master's degree in Mathematics	2015–2016
Université Polytechnique de Bobo-Dioulasso	Bobo-Dioulasso, Burkina Faso
Maîtrise en mathématiques appliquées	2013–2014
Université Polytechnique de Bobo-Dioulasso	Bobo-Dioulasso, Burkina Faso
Licence en mathématiques appliquées	2010–2013

Wissenschaftlicher Werdegang

Technische Universitat Kaiserslautern	Kaiserslautern, Deutschland
Doktor der Naturwissenschaften	2018–Current
Stellenbosch University	Stellenbosch, Süd Afrika
M.Sc. in Mathematics.	2016–2017
African Institute of Mathematical Sciences	Kapstadt, Süd Afrika
Structured master's degree in Mathematics	2015–2016
Université Polytechnique de Bobo-Dioulasso	Bobo-Dioulasso, Burkina Faso
Maîtrise en mathématiques appliquées	2013–2014
Université Polytechnique de Bobo-Dioulasso	Bobo-Dioulasso, Burkina Faso
Licence en mathématiques appliquées	2010–2013

List of Publications

- Claus Fieker, Tommy Hofmann, and Sogo Pierre Sanon. On the computation of the endomorphism rings of abelian surfaces. J. Number Theory, 229:39–52, 2021.