# Classical and Quantum Algorithms for Isogeny-based Cryptography

by

Anirudh Sankar

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Mathematics
in
Combinatorics and Optimization

Waterloo, Ontario, Canada, 2015

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

## Abstract

Isogeny-based cryptography using supersingular elliptic curves — most prominently, the constructions of De Feo-Jao-Plut — is one of the few practical candidates for post-quantum public key cryptography. Its formidable security claim is earned through the continual exploration of quantum algorithms for 'isogeny problems' and the assessment of the threat they pose to supersingular isogeny-based cryptography. We survey the rich history of classical and quantum algorithms for isogeny problems, and close with an original result — a quantum algorithm for the general supersingular isogeny problem, based on the discovery of Delfs and Galbraith in 2013 — that has exponential-complexity in general and subexponential complexity in an important sub-case. As yet, this algorithm poses a limited threat to the schemes of De Feo-Jao-Plut; however, it is an important algorithm to consider, for it provides insight into the structure of supersingular curves and the isogenies between them, and may lead to newer destructive quantum algorithms.

# Acknowledgements

First and foremost, I would like to thank my supervisor David Jao for introducing me to an exciting field in mathematical cryptography and for mentoring me throughout my Master's program. I would furthermore like to thank my readers Alfred Menezes and Michele Mosca for their constructive input. Lastly, I would like to thank my friends and family for their constant support and encouragement.

## Dedication

This is dedicated to my key inspirations Jeffrey Russo and Jeffrey “Young Thug” Williams.

# Table of Contents

**List of Figures** viii

**1 Introduction** 1

**2 Background on Elliptic Curves** 4

2.1 A Computational Definition . . . . . . . . . . . . . . . . . . . . . . . . . 4

2.2 Weierstrass Equations . . . . . . . . . . . . . . . . . . . . . . . . . . . . 5

2.3 Group Law . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 7

2.4 Finite Field Elliptic Curve groups; $m$-torsion Subgroups; Supersingularity . 8

**3 Background on Isogenies** 10

3.1 Definition, Basic Properties and Important Examples . . . . . . . . . . . . 10

3.2 Separability and Normality . . . . . . . . . . . . . . . . . . . . . . . . . 13

3.3 Isogeny Kernels and Velu's Formula, Representation of Isogenies . . . . . . 15

3.4 Dual Isogenies, Isogeny Classes, Tate's Theorem . . . . . . . . . . . . . . 16

3.5 Elliptic Curves over $\mathbb{C}$ I: An Identification with Lattices and Complex Tori 17

3.6 Elliptic Curves over $\mathbb{C}$ II: Complex Multiplication and Group Actions . . . 21

3.7 Reduction to Ordinary Curves over Finite Fields . . . . . . . . . . . . . . 22

3.7.1 Schoof-Elkies-Atkins (SEA) Technique . . . . . . . . . . . . . . . . 25

**4 Isogeny-based Cryptography 28**

4.1 Cryptography based on Ordinary Curves . . . . . . . . . . . . . . . . . . . . 28

4.1.1 Hard Homogenous Spaces and Some Public-key Protocols . . . . . . 28

4.1.2 The $\mathrm{Cl}(\mathcal{O})$-torsor $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q)$ as a HHS . . . . . . . . . . . . . . . . . 31

4.2 Cryptography based on Supersingular Curves . . . . . . . . . . . . . . . . . 33

4.2.1 Overview . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 33

4.2.2 Parameters . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 34

4.2.3 Protocols . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 35

4.2.4 Performance . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 36

4.2.5 Underlying Computational Problems . . . . . . . . . . . . . . . . . 37

**5 Algorithms for Isogeny Problems and Isogeny Based Cryptography 39**

5.1 Algorithmic Paradigm: Navigating Isogeny Graphs . . . . . . . . . . . . . . 39

5.2 The Ordinary Case . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 40

5.2.1 Levels and Volcanoes . . . . . . . . . . . . . . . . . . . . . . . . 40

5.2.2 Classical Algorithm for the Vectorization Problem: The Algorithm of Galbraith-Hess-Smart . . . . . . . . . . . . . . . . . . . . . . . 44

5.2.3 Subexponential Quantum Algorithm for Vectorization: The Algorithm of Childs-Jao-Soukharev . . . . . . . . . . . . . . . . . . . . 46

5.3 The Supersingular Case . . . . . . . . . . . . . . . . . . . . . . . . . . 47

5.3.1 Expander property; Meet in the Middle Algorithm . . . . . . . . . . 47

5.3.2 Result of Delfs and Galbraith: Partial Reintroduction of ‘Ordinary’ Structure . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 48

5.4 A Quantum Algorithm for the Supersingular Isogeny Problem . . . . . . . 51

5.4.1 Overview . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 51

5.4.2 Quantum Random Walk . . . . . . . . . . . . . . . . . . . . . . . 52

5.4.3 Cryptographic Implications . . . . . . . . . . . . . . . . . . . . . 55

**6 Future Work 56**

**Bibliography 57**

# List of Figures

3.1 A portion of the lattice $L = L_{\langle \omega_1, \omega_2 \rangle}$ in the complex plane and the 'fundamental parallelogram' (shaded) for the torus $\mathbb{C}/L$ . . . . . . . . . . . . . . . . 18

4.1 DH-type key exchange using ordinary curves . . . . . . . . . . . . . . . . . . 31

4.2 Principle behind De Feo-Jao-Plut schemes . . . . . . . . . . . . . . . . . . . 34

4.3 A 'balanced strategy' where $R_0$ has order $l^6$; only the bold edges are computed 37

5.1 Level structure where $[O_K : \mathbb{Z}[\pi]] = 6$ . . . . . . . . . . . . . . . . . . . . . . 41

5.2 Example of a 2-volcano . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 42

5.3 Schematic of quantum algorithm for supersingular isogeny problem . . . . 51

# Chapter 1

# Introduction

Elliptic curve cryptography (ECC) dates back to 1985, when it was realized that it was a promising candidate for public key cryptography based on the intractability of computing discrete logarithms. Indeed, ECC based on discrete logarithms has performed well in practice and still, after decades of research into adversarial attacks, displays strong theoretical resistance to classical attacks.

However, in 1994 Peter Shor [28] described a quantum algorithm for efficiently solving discrete logarithms over finite groups. As yet, a large scale quantum computer that is able to execute such an algorithm for a cryptographically-sized problem has not been built, but it is clear that the landscape of cryptography will be forever changed with the first instance of an adversary with such quantum computing power. This threat has induced the search for *classically* realizable cryptography that is secure in a *post-quantum* world.

One answer comes from ECC itself. In 1997 it was noted by Couveignes [10] that elliptic curves could be used in a fundamentally different way for cryptography than discrete logarithms, by basing the cryptography on the difficulty of computing isogenies, which are maps *between* elliptic curves. Starting from the observation that rational 'horizontal' isogenies can be described by a commutative group action, Couveignes and later, independently, Stolbunov [32] built cryptographic primitives emulating classical ones such as Diffie-Hellman and Elgamal, but with an essentially different underlying problem — that of vectorization for the group action. These constructions were originally thought to display quantum-resistant properties.

However, since Shor's algorithm, theoretical quantum computing research has shown that many more computational problems are subject to improved quantum algorithms, endangering their use as a basis for cryptography in the future. In particular, several black box quantum algorithms tackle entire classes of problems and repeatedly demonstrate the power of quantum computing over classical ones. One of these black box algorithms — the abelian hidden shift problem — was shown by Childs, Jao, and Soukharev [8] to resolve the Vectorization problem with a subexponential quantum algorithm.

However, in 2011 De Feo and Jao, in a work later extended with Plut [12], proposed schemes based on supersingular elliptic curves, which are distinct in their complex multiplication and isogeny behavior from ordinary curves. In particular, at first they do not display the commutativity structure that enables straightforward group action cryptography, but in the actual cryptographic context the authors overcome these 'hurdles' through specific parameter choices and minimal additional auxiliary input; the complexities of supersingular algebraic structure then bolster the security. In particular, they do not succumb to such a sweeping black box algorithm as hidden shift. For an exponentially sized security parameter $p$, the best classical algorithm so far is $O(p^{1/4})$ and this is only improved to $O(p^{1/6})$ with a quantum algorithm.

We investigate the post-quantum security of supersingular cryptography, by considering a more general 'isogeny problem' for supersingular curves. Resolving this problem acquaints us with a major algorithmic paradigm for computing isogenies, which is to find a path in an isogeny graph. The supersingular isogeny graph displays essentially different properties from the ordinary one. However, in 2013, Delfs and Galbraith [13] found that a certain substructure — one where consideration is restricted 'entirely' to the prime subfield $\mathbb{F}_p$ — does display the structure of the ordinary isogeny graph. We describe a new quantum algorithm —from joint work with Biasse and Jao — based on this discovery. The new algorithm runs in exponential time $O(p^{1/4})$ in general but $L_p(1/2, \sqrt{3}/2)$ in the cases where the problem is between curves in the prime subfield substructure. The algorithm has implications for some supersingular cryptography, but not (yet) the schemes of De Feo-Jao-Plut, except possibly to warn against a choice of basepoint over $\mathbb{F}_p$ as a cautionary measure. Nevertheless, it is an important algorithm to consider because it highlights the idiosyncrasies of the supersingular graph, and may serve as a launchpad for future algorithms.

This thesis aims to be as self-contained as possible, and for this reason devotes two chapters to mathematical and computational background for elliptic curves and isogenies. The next two chapters are presented such that they first review the older discoveries for the ordinary case before discussing the supersingular case. We have decided on this presentation because strategies for the supersingular case are frequently informed by ideas from the ordinary case, most prominently the shared commutative square of De Feo-Jao-Plut for supersingular curve cryptographic constructions and the result of Delfs and Galbraith for algorithms for the supersingular isogeny problem.

# Chapter 2

# Background on Elliptic Curves

**Notation 2.0.1.** Throughout these first two chapters, $K$ represents the ground field where a curve is defined and $F$ refers to an intermediate field $K \subseteq F \subseteq \bar{K}$.

Background material in the following two chapters is collected from a variety of sources, including standard sources such as [31, 30, 11, 26, 16, 38], but also various forms of lecture notes and expositions, such as [35, 9].

## 2.1 A Computational Definition

Elliptic curves are objects from algebraic geometry. They have many equivalent definitions in that area. A computational definition that maintains mathematical generality is the following:

**Definition 2.1.1.** An elliptic curve $E$ defined over the *ground field* $K$ (denoted $E/K$) is a smooth, projective plane cubic curve in $\mathbb{P}^2(\bar{K})$

$$E : a_1X^3 + a_2X^2Y + ... + a_{10}Z^3 = 0 : a_1, ..., a_{10} \in K \tag{2.1}$$

together with a distinguished $K$-rational point that is denoted by $\infty$.

Let us elaborate on this definition. A *point* on $E$ is a projective coordinate $P := [P_x : P_y : P_z] \in \mathbb{P}^2(\bar{K})$ such that $X = P_x$, $Y = P_y$ and $Z = P_z$ satisfy the above equation (note that satisfiability is independent of the particular homogenous coordinate representation for $P$). The set of such coordinates constitute the points 'collected' over the algebraic closure, denoted $E(\bar{K})$. For any field $F$ such that $K \subseteq F \subseteq \bar{K}$, we can consider the subset of $F$-rational points, denoted $E(F)$, which are the points $P$ for which there is a homogenous coordinate representation $P := [P_x, P_y, P_z]$ such that $P_x, P_y, P_z \in F$. We are often especially concerned with the points collected over the ground field, the $K$-rational points $E(K)$.

In cryptography, we are interested primarily in the case where $K$ is a finite field $\mathbb{F}_q$ (and call any such $E/K$ an 'elliptic curve over a finite field'). Note that this means we can describe any point in $E(\bar{K})$ exactly, instead of approximating the coordinates.

For theoretical purposes, we are also interested in the case that $K$ is a subfield of $\mathbb{C}$ (and call any such $E/K$ an 'elliptic curve over $\mathbb{C}$' or 'complex elliptic curve'), especially when $K$ is a number field. Where $K$ is not specified in a proposition, it means it applies to both cases: subfield of the complex numbers or a finite field.

Mathematical languages such as SAGE can accept inputs of cubic curve equations with a specified distinguished rational point, but immediately convert it to a standard form such as a Weierstrass form to compute with it. In particular it is in these forms that smoothness — also known as *non-singularity* or *non-degeneracy* — is quickly checked.

## 2.2 Weierstrass Equations

Elliptic curve equations can be transformed by change of variables formulas. Algebro-geometrically these transformations are isomorphisms, and the essential properties of the curve are maintained — the coordinate ring, function fields, etc. In fact, and crucially, more is true — if $\infty$ is preserved, the groups (described in the next section) on the elliptic curve are also isomorphic. This is a consequence of isogeny theory, as will be seen in the next chapter.

We are especially concerned with the useful standard forms known as the *Weierstrass equation* or *form*. Elliptic curves can always be transformed efficiently via a change of variables into a *long Weierstrass form* [31, III.1]:

$$E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{2.2}$$

where $\infty = [0 : 1 : 0]$.

When $K$ has characteristic not equal to $2, 3$ (a situation we'll never have to consider for isogeny cryptography), they can be transformed into the highly compact *short Weierstrass* *form* [31, III.1]:

$$E : Y^2Z = X^3 + aXZ^2 + bZ^3 \tag{2.3}$$

where $\infty = [0 : 1 : 0]$.

For an elliptic curve in Weierstrass form, besides the point $\infty$, all other points on the curve have coordinates $[x : y : 1]$ and correspond to pairs $(x, y)$ that satisfy an affine equation. For example, for an elliptic curve in short Weierstrass form, these pairs $(x, y)$ are the solutions of

$$E : y^2 = x^3 + ax + b. \tag{2.4}$$

Therefore, we can can always restrict our attention to this 'affine model' of the curve for describing points, point computation, and maps between Weierstrass forms.

There are other major advantages of representing an elliptic curve with a Weierstrass form. One of them is that though the forms are not unique for each isomorphism class of curves, the isomorphisms between them are well classified. For example:

**Proposition 2.2.1** ([31, III.1])**.** *Elliptic curves $E/K : y^2 = x^3 + ax + b$ and $E'/K : y^2 = x^3 + a'x + b'$ are isomorphic over $\bar{K}$ iff the coefficients are related by a 'scaling' constant $\mu \in \bar{K}^*$ such that*

$$\begin{aligned} a' &= \mu^2 a \\ b' &= \mu^3 b. \end{aligned} \tag{2.5}$$

*If so, the isomorphism $E \to E'$ is given by $(x, y) \mapsto (\mu x, \mu^{3/2} y)$.*

In the Weierstrass forms it is also easy to collect elementary data about the curve. One of the most important is the *discriminant* $\Delta(E)$ that checks non-degeneracy.

**Definition 2.2.2.** For a curve $E$ in short Weierstrass form (2.4)

$$\Delta(E) = -16(4a^3 + 27b^2). \tag{2.6}$$

$E$ is non-singular (and hence a valid elliptic curve) iff $\Delta(E) \neq 0$.([31, III.1.4]).

Another important quantity is the $j$-invariant, which immediately gives the isomorphism class of the curve.

**Definition 2.2.3.** For $E$ given in short Weierstrass form (2.4)

$$j(E) = -1728(4a)^3/\Delta. \tag{2.7}$$

Two curves $E$ and $E'$ are isomorphic (over $\bar{K}$) iff $j(E) = j(E)$ ([[31, III.1]]).

For curves given in long Weierstrass form, the formulas are a little more elaborate, but not unwieldly from a computational perspective. Thus $j$ and $\Delta$ are always efficiently computable.

Because it is easy to convert plane cubic equations into a Weierstrass form, a form that preserves essential properties of the curve, we may assume our curves are given in these forms to begin with. Note that for cryptography, we only use curves over a field of large characteristic, so we can assume whenever we need to that curves are given in short Weierstrass form (2.4).

## 2.3 Group Law

Elliptic Curves are used in cryptography because they have the additional structure of an *abelian variety*; their points constitute a commutative group whose group operation (denoted $+$) is given by rational functions of their coordinates. In particular, for any elliptic curve $E/K$, and $F$ an algebraic extension of $K$, the points of $E(F)$ forms a group under this operation.

Of the various derivations of this group law, we give the one that in the characteristic 0 case has a visualization as the so-called 'chord-and-tangent' rules. Consider two $F$-rational points $P$ and $Q$. The projective line between (tangent line in the case $P = Q$) them must intersect at a third $F$-rational point, by Bezout's Theorem [14, 5.3]. Call this point $R$. Now consider the line between $R$ and $\infty$. This line must again intersect in a third $F$-rational point, call it $S$. Set $P + Q := S$. Of the group properties, it is easy to establish that $+$ is commutative, that $\infty$ functions as the identity, and that points have inverses. The hardest property to exhibit directly from this description is that $+$ is associative, though the property does hold.

We give explicit formulas for elliptic curves in short Weierstrass form (2.4).

**Proposition 2.3.1** ([38, 2.2])**.** *For a curve $E$ given in short Weierstrass form, the described group law above gives that for $P = (x, y)$, its additive inverse is $-P = (x, -y)$, and the non-trivial 2-torsion points are the points $P = (x, 0)$ on the curve. The remaining formulas for addition of non-trivial affine points are the following. For $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ where $Q \neq -P$, $P + Q = (x_3, y_3)$ where*

$$\begin{aligned} x_3 &= -x_1 - x_2 + \lambda^2 \\ y_3 &= \lambda(x_1 - x_3) - y_1 \end{aligned} \tag{2.8}$$

*where $\lambda$ is the slope of the line through $P$ and $Q$, i.e.*

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & P \neq Q \\ \dfrac{3x_1^2 + a}{2y_1} & P = Q \text{ but } 2P \neq \infty. \end{cases} \tag{2.9}$$

## 2.4 Finite Field Elliptic Curve groups; $m$-torsion Subgroups; Supersingularity

When the ground field $K$ is a number field, the famous Mordell-Weil Theorem says that the group of $K$-rational points $E(K)$ is finitely generated (and thus completely classifiable). But now consider $K = \mathbb{F}_q$ a finite field, and $F/K$ a finite extension (including possibly $F = K$ itself). Then $E(F)$ is finite, while $E(\bar{K})$ is a torsion group of unbounded torsion order.

Central to the theory is the characterization of the $m$-torsion subgroups $E[m] \subseteq E(\bar{K})$.

**Proposition 2.4.1** ([38, 3.1])**.** *Let $p = \text{char}(K)$ and consider $m$ such that $(m, p) = 1$. Then:*

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}. \tag{2.10}$$

*For the remaining case of $m = p^e, e \in \mathbb{Z}^+$, two types of behaviour occur. Either*

$$E[p^e] = \mathbb{Z}/p^e\mathbb{Z} \times \mathbb{Z}/p^e\mathbb{Z}, \qquad e = 1, 2, 3, ... \tag{2.11}$$

*in which case $E$ is said to be* ordinary*, or*

$$E[p^e] = \infty, \qquad e = 1, 2, 3, ... \tag{2.12}$$

*in which case $E$ is said to be* supersingular*.*

These facts are determined by analyzing certain isogenies called ‘multiplication maps’ described in the next chapter. Note that as $m \to \infty$, $E[m]$ is completely invisible over $E(F)$. Nevertheless, using just elementary group theory, Proposition 2.4.1 can establish the following:

**Theorem 2.4.2** ([35, Corollary 7.4])**.** *For $F : K = \mathbb{F}_q$ a finite extension,*

$$E(F) \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \tag{2.13}$$

*for positive integers $m, n$ such that $m|n$ and $p \nmid m$.*

However, describing this isomorphism explicitly is in general infeasible, a fact which drives elliptic curve cryptography. A 'softer' question is the cardinality of $E(F)$. Here the following theorem applies:

**Theorem 2.4.3** ([16, 9.10.3])**.** *Let $E/\mathbb{F}_q$ be an elliptic curve. Then*

$$\#E(\mathbb{F}_q) = q + 1 - t_q \tag{2.14}$$

*where $|t_q| \leq 2\sqrt{q}$.*

The value $t_q$ is known as the trace of the $q$-th Frobenius map $\pi_q$, that we will also see in the next chapter. An important algorithm of Schoof [27] uses isogeny theory and the relationship between $t_q$ and cardinality to efficiently count $\#E(\mathbb{F}_q)$.

The trace of Frobenius tells whether the curve is ordinary or supersingular.

**Proposition 2.4.4** ([16, 9.11.2])**.** *Let $E/\mathbb{F}_q$ be an elliptic curve. Then $E$ is supersingular iff* $\mathrm{char}(\mathbb{F}_q)|t_q$

Thus, Schoof's algorithm also provides an efficient test of whether a curve is supersingular. An important special case is when $E$ is defined over a prime field.

**Corollary 2.4.5.** *Let $E/\mathbb{F}_p$ be an elliptic curve. Then $E$ is supersingular iff $\#E(\mathbb{F}_p) = p + 1$.*

*Proof.* By Theorem 2.4.3, $|t_p| \leq 2\sqrt{p}$. But $p \mid t_p$, so $t_p = 0$. □

# Chapter 3

# Background on Isogenies

## 3.1 Definition, Basic Properties and Important Examples

**Definition 3.1.1.** Let $E_1/K$, $E_2/K$ be elliptic curves. An *isogeny* is a rational map of elliptic curves $\phi : E_1(\bar{K}) \to E_2(\bar{K})$, with coefficients from $\bar{K}$ that preserves the point at infinity, i.e. such that $\phi(\infty) = \infty$.

We can assume $E_1$, and $E_2$ are given as Weierstrass equations. In this case $\phi$ is fully characterized by its action on the affine models for $E_1$ and $E_2$, and in particular can be represented as:

$$\phi(x, y) = \left( \frac{f_1(x, y)}{g_1(x, y)}, \frac{f_2(x, y)}{g_2(x, y)} \right) : f_1, f_2, g_1, g_2 \in \bar{K}[x, y]. \tag{3.1}$$

We allow the coefficients of $\phi$ to come from $\bar{K}$; however, since there are only a finite number of them, they all come from some finite extension of $K$. Let $F$ be a finite dimensional extension of $K$ that contains all the coefficients. Then we say that the isogeny is defined over $F$. When the defining field of an isogeny is known or unimportant, we may simply write $\phi : E_1 \to E_2$.

As rational maps of smooth projective curves, non-trivial isogenies $\phi : E_1 \to E_2$ immediately inherit properties such as:

**Lemma 3.1.2** ([14, Corollary 7.1.1]). *$\phi$ is regular, i.e. it is defined on all of $E_1(\bar{K})$.*

**Lemma 3.1.3** ([14, Problem 8.18])**.** *$\phi$ is surjective on $E_2(\bar{K})$ (also known as geometrically surjective).*

A distinguishing property of isogenies is that they are group homomorphisms.

**Proposition 3.1.4** ([31, III.4.8])**.**

$$\phi(P+Q) = \phi(P) + \phi(Q) \quad \forall P, Q \in E_1(\bar{K}). \tag{3.2}$$

**Definition 3.1.5.** The kernel of $\phi$ is defined by:

$$\ker(\phi) := \{P \mid P \in E_1(\bar{K}) \text{ and } P \in \phi^{-1}(\infty)\}, \tag{3.3}$$

The kernel is exactly what appears to be the pole sets of the affine representation (3.1) of $\phi$ above.

**Lemma 3.1.6.** *For any isogeny $\phi\colon E_1 \to E_2$, $\ker(\phi)$ is finite.*

*Proof.* We prove it in the case $\phi$ is between Weierstrass forms. In this case consider any affine representation (3.1). The kernel $\ker(\phi)$ must be a subset of the intersection of the zero sets of $g_1(x,y)$ and $g_2(x,y)$ on $E_1(\bar{K})$. This has to be finite since $E_1(\bar{K})$ is an irreducible subset of $\mathbb{A}^2(\bar{K})$. □

**Example 3.1.7.** Isomorphisms that preserve $\infty$ (so-called 'pointed isomorphisms', in the language of [16, 9.3]) are perhaps the simplest examples of isogenies. Consider the short Weierstrass form elliptic curves $E : y^2 = x^3 + ax + b$, $a, b \in K$ and $E^{(d)} : y^2 = x^3 + d^2ax + d^3b$ for $d \in \bar{K}^*$. Then $E$ and $E^d$ are isomorphic via the pointed isomorphism

$$\begin{aligned} \phi : E &\rightarrow E^{(d)} \\ \phi(x,y) &= (dx, d^{\frac{3}{2}}x). \end{aligned} \tag{3.4}$$

Note that although $E_1, E_2$ are both defined over $K$, if $d$ is not a square in $\bar{K}$, $\phi$ is not defined over $K$; it is defined over $K(\sqrt{d})$. Thus $E$ and $E^{(d)}$ are isomorphic over $\bar{K}$ but *not* over $K$; in this case $E^{(d)}$ is known as the quadratic twist of $E$ over $K$.

Pointed isomorphisms lead to a natural notion of isomorphism of isogenies.

**Definition 3.1.8.** Isogenies $\phi_1 : E \to E_1$ and $\phi_2 : E \to E_2$ are isomorphic if there is a pointed isomorphism $\mu : E_1 \to E_2$ such that $\phi_2 = \mu \circ \phi_1$.

This definition suggests that the isogeny is essentially characterized by its kernel; we will see how exactly in the next section on quotient isogenies.

We are sometimes interested in where an isomorphism between two isogenies is defined. For example isogenies $\phi : E \to E_1$ and $\phi_d : E \to E_1^{(d)}$, for $E_1^{(d)}$ a quadratic twist of $E_1$, are not isomorphic over $K$.

**Example 3.1.9.** An infinite family of self-isogenies of $E$ (called *endomorphisms* of $E$) is furnished by "multiplication-by-$m$' maps, defined by

$$\begin{aligned} [m] \colon E &\to E \\ P &\mapsto mP. \end{aligned} \tag{3.5}$$

The rational map corresponding to $[m]$ has an affine representation as:

$$[m](x,y) := \left( \frac{\phi_m(x,y)}{\psi_m^2(x,y)}, \frac{\Omega_m(x,y)}{\psi_m(x,y)} \right) \tag{3.6}$$

where $\omega_m, \Omega_m, \psi_m$ are distinguished polynomials that can be computed recursively in $m$. The polynomial family $\psi_m$ are especially important: the roots of these division polynomials on the locus of $E$ are the $m$-torsion points $E[m]$, the kernel of the map $[m]$.

**Example 3.1.10** (Frobenius morphism)**.** These isogenies are central to the theory of elliptic curves defined over finite fields. Consider $E/K$ an elliptic curve, where $K = \mathbb{F}_q$ and $\mathrm{char}(K) = p$, given in short Weierstrass form as $y^2 = x^3 + Ax + B$. It is easily checked ([31, III.4.6]) that $E^{(p)} \colon y^2 = x^3 + A^p x + B^p$ is non-degenerate and that

$$\pi(x,y) := (x^p, y^p) \tag{3.7}$$

is a bijective isogeny $E \to E^{(p)}$. It is known as the Frobenius morphism. Although an inverse map is defined, it is not a rational map, and hence this map is not an isomorphism.

Now if the ground field $K$ has size $q = p^n$ consider $E^{(q)} = E^{(p^n)}$ as well as the $n$-th power of the Frobenius map $\pi_q := \pi^n$. Because this map fixes $K$, $E^{(q)} = E$ and $\pi_q$ (also known as $\pi_E$) is an endomorphism known as the *Frobenius endomorphism.* We will gradually see the importance of $\pi$ and $\pi_q$.

The endomorphisms of a curve $E$ can be pointwise added and composed, and in this way form a ring $\mathrm{End}(E)$. It is easily shown that this ring is torsion free and that $\mathbb{Z} \subseteq \mathrm{End}(E)$ as multiplication maps. For elliptic curves defined over finite fields $\mathrm{End}(E)$ contains more than the multiplication maps, but is still constrained.

**Proposition 3.1.11** ([35, Theorem 13.15])**.** *Let $E/K$ be an elliptic curve over a finite field. Then $E$ is ordinary iff* $\mathrm{End}(E)$ *is an order in an imaginary quadratic field* $\mathbb{Q}(\sqrt{-d})$*. $E$ is supersingular iff* $\mathrm{End}(E)$ *is an order in a imaginary quaternion algebra* $\mathbb{Q}(\alpha, \beta)$ *with* $\alpha, \beta < 0$*.*

The endomorphism ring of a curve $E$ influences the picture of *outgoing* isogenies from the curve. We will see how this is especially useful for ordinary curves in the last section of this chapter.

It can be shown that every endomorphism satisfies a degree 2 monic equation over $\mathbb{Z}$ ([35, Theorem 7.18]); in particular $\pi_q$ satisfies:

$$x^2 - t_q x + q \in \mathbb{Z}[x], \tag{3.8}$$

where $t_q$ is the trace of Frobenius mentioned earlier.

## 3.2 Separability and Normality

Certain results and algorithms only hold for 'separable' and/or 'normalized' isogenies. We thus view (in)separability and (ab)normality as complications to a simpler picture of isogenies, that can nevertheless be easily accounted for and 'corrected'.

An isogeny $\phi : E_1 \to E_2$ induces a monomorphism $\phi^* : \bar{K}(E_2) \to \bar{K}(E_1)$ of function fields defined by $\phi^*(f) = f \circ \phi$. We are interested in the finite extension $\bar{K}(E_1) : \phi^*(\bar{K}(E_2))$.

**Definition 3.2.1.** The *degree* of the isogeny $\phi : E_1 \to E_2$, denoted $\deg(\phi)$, is the dimension:

$$[\bar{K}(E_1) : \phi^*(\bar{K}(E_2))].$$

The separable and inseparable degrees $\deg_i(\phi)$ and $\deg_s(\phi)$ are defined as the dimensions of the corresponding extensions. Note that:

$$\deg(\phi) = \deg_s(\phi)\deg_i(\phi). \tag{3.9}$$

The isogeny is considered *inseparable* whenever there is an inseparable component to the finite extension, i.e. $\deg_i(\phi) > 1$. Otherwise it is separable.

**Proposition 3.2.2** ([31, II.2.6])**.** *Let $\phi : E_1 \to E_2$ be an isogeny. Then* $\deg_s(\phi) = \#\ker(\phi)$*. In particular, when $\phi$ is a separable isogeny* $\deg(\phi) = \#\ker(\phi)$*.*

When $\mathrm{char}(K) = 0$ all isogenies are separable. In the finite field case, the Frobenius map is inseparable.

**Lemma 3.2.3** ([31, II.2.11])**.** *Consider $E/\mathbb{F}_q$ an elliptic curve. Then $\pi_q$ is purely inseparable, i.e.* $\deg_i(\pi_q) = q$ *and* $\deg_s(\pi_q) = 1$.

In fact, all inseparable isogenies arise due to the presence of the Frobenius map.

**Proposition 3.2.4** ([31, II.2.12])**.** *Let $E_1, E_2/\mathbb{F}_q$ be elliptic curves. Then any inseparable isogeny $\psi : E_1 \to E_2$ factors as the composition:*

$$\psi : \psi_{sep} \circ \pi^r \tag{3.10}$$

*where $r$ is a positive integer and $\psi_{sep}$ is a separable isogeny such that* $\deg_s(\psi) = \deg(\psi)$.

Thus, from any inseparable isogeny $\psi$, we can 'get rid of' its Frobenius precomposition $\pi^r$ and 'recover' the separable map $\psi_{sep}$. We do this by just observing the consistent powers of $p$ that arise in the rational map $\psi$ and removing them.

Besides separability, another 'issue' that pertains to isogenies is the question of normalization. Consider again $\phi : E_1/K \to E_2/K$. Just as this rational map induces, functorially, a map $\phi^* : \bar{K}(E_2) \to \bar{K}(E_1)$, it also induces one $\phi^* : \Omega_{E_2} \to \Omega_{E_1}$, where $\Omega_E$ is the 1-dimensional $\bar{K}(E)$-vector space of rational differential forms. Of these forms, a distinguished one is the *invariant differential*:

$$\omega = \frac{dy}{3x^2 + a} = \frac{dx}{2y}$$

**Proposition 3.2.5** ([29, 2.20])**.** *Let $\phi : E_1/K \to E_2/K$ be an isogeny, and $\omega_1, \omega_2$ be the respective invariant differentials. Then*

$$\phi^*(\omega_2) = c\omega_1 \tag{3.11}$$

*For some $c \in \bar{K}(E_1)$. If $c = 1$, $\phi$ is said to be* normalized.

**Proposition 3.2.6.** *Every isogeny $\phi : E_1 \to E_2$ can be postcomposed with a pointed isomorphism $\tau$ such that the composition $\psi = \tau \circ \phi$ is normalized.*

*Proof.* By first applying the appropriate change of variables, we can assume that $E_2$ is in short Weierstrass form. Let $\phi^*(\omega_2) = c\omega_1$. Post-composing with an isomorphism with scaling factor $\mu$ (from 2.2.1) changes the invariant differential $\omega_2' = \frac{1}{\mu}\omega_2$ ([31, III,Table 1.2]. Therefore, choose $\mu = c$ and apply the corresponding isomorphism to $E_2$. □

## 3.3 Isogeny Kernels and Velu's Formula, Representation of Isogenies

Here we explore the question of whether and how an isogeny is characterized by its kernel. In particular, from a finite subgroup $C$ of $E(\bar{K})$, is there a unique curve $E/C$ and an isogeny $\phi_C : E \to E/C$ with kernel $C$ up to isomorphism of curves as well as isogenies? Restricted to the domain of separable isogenies, the answer is yes, and a positive construction of this 'quotient isogeny' is given by Velu's formula [37]. We will detail the construction when $E$ is given in short Weierstrass form.

Let

$$E : y^2 = f(x) = x^3 + ax + b$$

be an elliptic curve. Compute the following quantities.

$$\begin{aligned} v &= \sum_{P \in C - \{0\}} f'(P) \\ w &= \sum_{P \in C - \{0\}} x(P) f'(P). \end{aligned} \tag{3.12}$$

Then $E/C$ is given by:

$$E/C : y^2 = x^3 + Ax + B$$

where

$$\begin{aligned} A &= a - 5v \\ B &= b - 7w. \end{aligned} \tag{3.13}$$

The rational map $\phi_C \colon E \to E_C$ is given by:

$$\phi_C(P) := (x(P) + \sum_{Q \neq \infty \in C} [x(P+Q) - x(Q)], y(P) + \sum_{Q \neq \infty \in C} [y(P+Q) - x(Q)]). \tag{3.14}$$

**Proposition 3.3.1** ([38, Theorem 12.16,12.17])**.** *$E/C$ is an elliptic curve (non-degenerate) and $\phi_C$ is a normalized and separable isogeny $E \to E/C$ with kernel $C$.*

**Proposition 3.3.2** ([29, 3.5])**.** *Suppose $\#C = \ell$. Then the algebraic complexity of computing the codomain $E/C$ and evaluating the rational map $\phi_C$ on a point of $E(K)$ is $O(\ell)$ operations in $\bar{K}$ and $\tilde{O}(\ell M(d))$ operations in $K$, where $d$ is the degree of the minimal ex-*

*tension $F/K$ that contains $C$, and $M\colon \mathbb{N} \to \mathbb{N}$ a function such that multiplying polynomials of degree $n$ costs $M(n)$ base field operations.*

The universal property satisfied by $\phi_C$ is:

**Theorem 3.3.3** ([35, Theorem 6.8]). *Given a separable isogeny $\phi : E_1 \to E_2$ with kernel $C$, there is a pointed isomorphism $\varphi : E_1/C \to E_2$ such that $\phi = \varphi \circ \phi_C$.*

Therefore $\phi_C$ is the unique separable isogeny with kernel $C$ up to isomorphism. Note that for an inseparable isogeny $\phi : E_1 \to E_2$ with kernel $C$, the isogeny $\phi_C$ shares a universal property with $\phi_{\text{sep}}$.

Thus a kernel can represent an isogeny. But now the question arises: given $C$, where is the rational map $\phi_C$ defined? It is not sufficient to consider the field containing the points $C$, just as the multiplication by $[m]$ map is defined over $K$ even though most torsion subgroups $E[m]$ are invisible over $E(K)$. Instead we consider the Galois action on the points.

Given $E/K$, the Galois group $\text{Gal}(\bar{K} : K)$ acts on points of $E$ by acting on their coordinates: it is easy to see that if $P$ is a point of $E$ then so is $\sigma(P)$ for $\sigma \in \text{Gal}(\bar{K} : K)$. Given a subgroup $C$ of $E$, we are interested in where points of $C$ are taken under these Galois actions.

**Proposition 3.3.4** ([3, Theorem III.11]). *Consider a subgroup $C$ of $E(\bar{K})$. Then $C$ is said to be $F$-Galois stable iff for all $P \in C$, and all $\sigma \in \text{Gal}(\bar{K} : F)$, it holds that $\sigma(P) \in C$. The quotient isogeny $\phi_C$ determined by Velu's formula is defined over $F$ if and only if $C$ is $F$-Galois stable.*

When $K = \mathbb{F}_q$, $\text{Gal}(\bar{K} : K)$ is generated by the Frobenius map $x \mapsto x^q$. The Galois action corresponding to this is exactly the Frobenius morphism $\pi_q$.

**Corollary 3.3.5.** *Let $E/\mathbb{F}_q$ be an elliptic curve and $C \subseteq E(\bar{\mathbb{F}}_q)$ be a finite subgroup. Then the quotient isogeny $\phi_C$ determined by Velu's formula is defined over $\mathbb{F}_{q^r}$ if it is the case that for all $P \in C$, $\pi_q^r(P) \in C$.*

## 3.4 Dual Isogenies, Isogeny Classes, Tate's Theorem

For every isogeny $\phi : E_1 \to E_2$ there exists an isogeny $\hat{\phi} : E_2 \to E_1$ known as the *dual isogeny.*

**Proposition 3.4.1** ([31, III.6]). *For every isogeny $\phi : E_1 \to E_2$ there exists a unique isogeny $\hat{\phi} : E_2 \to E_1$ of the same degree* $\deg(\phi)$ *such that* $\phi \circ \hat{\phi} = [\deg(\phi)]$ *and* $\hat{\phi} \circ \phi = [\deg(\phi)]$.

Thus we can define a relation of 'being isogenous': $E_1$ and $E_2$ are $F$- isogenous if there is an isogeny $\phi : E_1 \to E_2$ defined over $F$. Because of the existence of dual isogenies, this relation is symmetric, and hence an equivalence relation, partitioning curves into isogeny classes. Note that changing the field $F$ potentially changes the classes. We can also consider equivalence classes where $F = \bar{K}$, which partitions curves into the most general isogeny classes.

Tate's Theorem says that for elliptic curves over finite fields, there is a simple necessary and sufficient condition for two curves $E, E'$ to be isogenous over a finite field $\mathbb{F}_q$.

**Theorem 3.4.2** ([36, Tate's Theorem]). *Let $E, E'/\mathbb{F}_q$ be elliptic curves. Then $E$ and $E'$ are isogenous over $\mathbb{F}_q$ if and only if $\#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q)$ .*

Because of Schoof's point counting algorithm, it can therefore be efficiently checked whether two curves are isogenous over a particular field. But Tate's theorem is non-constructive, so it does not produce an isogeny where it exists. For a large degree isogeny, constructing the isogeny is a much harder problem — a fact which drives isogeny-based cryptography.

## 3.5 Elliptic Curves over $\mathbb{C}$ I: An Identification with Lattices and Complex Tori

We will appeal heavily to isogeny theory that is developed for complex elliptic curves and then 'reduced' to elliptic curves over finite fields. Over $\mathbb{C}$, elliptic curve theory simplifies because a complex curve can be completely identified with a torus $\mathbb{C}/L$, where $L$ is a lattice in $\mathbb{C}$. Under this identification, isogeny theory in particular simplifies.

**Definition 3.5.1.** A lattice $L := L_{\langle \omega_1, \omega_2 \rangle}$ is the additive subgroup of $\mathbb{C}$ generated by linearly independent element generators $\omega_1, \omega_2 \in \mathbb{C}$:

$$L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2.$$

The numbers $\omega_1, \omega_2$ are known as *periods* of the lattice. We can assume without loss of generality that $\arg(\omega_2) > \arg(\omega_1)$.

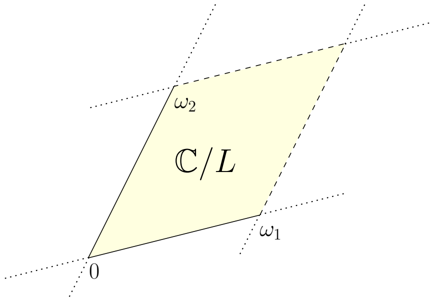

Figure 3.1: A portion of the lattice $L = L_{\langle\omega_1,\omega_2\rangle}$ in the complex plane and the 'fundamental parallelogram' (shaded) for the torus $\mathbb{C}/L$

The quotient structure $\mathbb{C}/L$, which is a torus, has an induced group law as well as an induced topology from the canonical projection map $p : \mathbb{C} \to \mathbb{C}/L$. From this torus we define a special bijection $\Phi_L$ to a complex elliptic curve $E_L$ ([26, Theorem 2.15]). Define

$$E_L : y^2 = x^3 + Ax + B$$

where $A$ and $B$ are the convergent quantities

$$\begin{aligned} A &= 15 \sum_{\omega\in L-\{0\}} \frac{1}{\omega^4} \\ B &= 35 \sum_{\omega\in L-\{0\}} \frac{1}{\omega^6}. \end{aligned} \tag{3.15}$$

The bijection $\Phi_L \colon \mathbb{C}/L \to E_L$ is given by:

$$\Phi_L(z) = \left(\wp(z;L), \frac{\wp'(z;L)}{2}\right) \tag{3.16}$$

where $\wp(z;L)$ is the distinguished *Weierstrass function*, a meromorphic function defined by

$$\wp(z;L) = \frac{1}{z^2} + \sum_{\omega\in L-0} \Big(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\Big).$$

The bijection $\Phi_L$, and in particular the Weierstrass $\wp$-function is extremely well motivated and invokes a rich theory about complex elliptic curves. We just summarize the most relevant facts about the bijection $\Phi_L$ for our purposes.

**Proposition 3.5.2** ([35, Notes 15,16])**.** *$\Phi_L$ is a group isomorphism $\mathbb{C}/L \to E_L(\mathbb{C})$ as well as an isomorphism of complex manifolds.*

The second property implies an isomorphism in the sense of algebraic geometry, so for example $\Phi_L$ induces an isomorphism between the function field $\mathbb{C}(E_L)$ and the field of *elliptic functions* on $\mathbb{C}$ for $L$, $\xi_L$.

The theorem that allows for a full identification of complex elliptic curves with complex tori of the form $\mathbb{C}/L$ is the following.

**Proposition 3.5.3** (Uniformization Theorem [35, Corollary 16.12])**.** *For every complex elliptic curve $E$ in short Weierstrass form, there is a lattice $L$ such that $\mathbb{C}/L$ is isomorphic to $E$ via $\Phi_L$.*

Note that there is nothing special about the short Weierstrass form: indeed, we could rewrite $\phi_L$ to establish a canonical bijection to valid plane cubic curves over $\mathbb{C}$ that define an elliptic curve; we stick to short Weierstrass forms for simplicity.

As a consequence of these two theorems, complex elliptic curves can be fully identified with complex tori. As a notational shorthand, let $\Phi$ refer to this overall correspondence (we can consider $\Phi = \{\Phi_L\}$).

As mentioned earlier, isogeny theory simplifies as a theory for these tori. Let $E = E_{L_1}$ and $E = E_{L_2}$ be two complex elliptic curves. Then an isogeny $\phi : E_{L_1} \to E_{L_2}$ induces a corresponding 'isogeny' $\phi^* : \mathbb{C}/L_1 \to \mathbb{C}/L_2$ of tori:

$$\begin{tikzcd}
\mathbb{C}/L_1 \arrow[r, "\phi^*"] \arrow[d, "\Phi_{L_1}"'] & \mathbb{C}/L_2 \arrow[d, "\Phi_{L_2}"] \\
E_{L_1} \arrow[r, "\phi"] & E_{L_2}
\end{tikzcd} \tag{3.17}$$

i.e. $\phi^* := \Phi_{L_2}^{-1}\phi\Phi_{L_1}$.

It turns out $\phi^*$ is simply a 'multiplication by $\lambda$' for some fixed constant $\lambda \in \mathbb{C}$.

**Lemma 3.5.4** ([26, Theorem 2.38])**.** *Consider $\tilde{\phi} := p^{-1}(\phi^*)$ (i.e. the lift of $\phi^*$). Then $\tilde{\phi}(z) = \lambda z$ for some $\lambda \in \mathbb{C}$ such that $\lambda L_1 \subseteq L_2$. Thus:*

$$\phi^*(z \bmod L_1) = \lambda z \bmod L_2. \tag{3.18}$$

Thus $\phi^*$ can be simply be described as a 'multiplication by $\lambda$' map. Conversely, every $\lambda \in \mathbb{C}$ such that $\lambda L_1 \subseteq L_2$ induces a map $\lambda : \mathbb{C}/L_1 \to \mathbb{C}/L_2$ that comes from an isogeny $\phi$ in (3.17). This result justifies the following notion of isogenies defined strictly in terms of tori:

**Definition 3.5.5.** For two lattices $L, L' \in \mathbb{C}$, consider a $\lambda \in \mathbb{C}$ such that $\lambda L \subset L'$. Then the induced homomorphism:

$$\begin{aligned} \lambda : \mathbb{C}/L &\to \mathbb{C}/L' \\ z \bmod L &\mapsto \lambda z \bmod L' \end{aligned} \tag{3.19}$$

is called an *isogeny*. It has kernel isomorphic to $L'/\lambda L$.

**Definition 3.5.6.** An endomorphism of $\mathbb{C}/L$ is the induced map $\lambda : \mathbb{C}/L \to \mathbb{C}/L$ from a $\lambda \in \mathbb{C}$ such that $\lambda L \subseteq L$.

Note that under the correspondence (3.17), multiplication by $m$ maps $[m]$ correspond to the dilation $\lambda = m$.

**Definition 3.5.7.** An isomorphism from $\mathbb{C}/L_1$ to $\mathbb{C}/L_2$ is the induced map $\lambda : \mathbb{C}/L_1 \to \mathbb{C}/L_2$ where $\lambda L_1 = L_2$.

The complex tori $\mathbb{C}/L_1$ and $\mathbb{C}/L_2$ are isomorphic exactly when one lattice is a scalar multiple of the other. We call this equivalence relation on the lattices *homothety*, and we denote it by $L_1 \sim L_2$.

**Corollary 3.5.8.** $\Phi$ *establishes a bijective correspondence between isomorphism classes of complex elliptic curves (given by $j$-invariant) and complex tori from lattices modulo the relation of homothety.*

Note the following construction of quotient isogenies for a complex tori. Consider a subgroup $C$ of $\mathbb{C}/L$. Now consider $C$ lifted to the complex plane (i.e. under $p^{-1}$); this is a lattice $L_C$ where $L \subseteq L_C$. If we now set $\lambda_C = 1$ we have that $\lambda_C L \subseteq L_C$ and the induced isogeny:

$$\begin{aligned} \lambda_C : \mathbb{C}/L &\to \mathbb{C}/L_C \\ z \bmod L &\mapsto z \bmod L_C \end{aligned} \tag{3.20}$$

has kernel exactly $C$. All isogenies can be described in this way up to homothety of the lattices.

## 3.6 Elliptic Curves over $\mathbb{C}$ II: Complex Multiplication and Group Actions

From this point, we use a 'complex elliptic curve' interchangeably to denote a complex Weierstrass equation $E$ or its torus $\mathbb{C}/L$.

**Definition 3.6.1.** A curve $\mathbb{C}/L$ has complex multiplication if it has an endomorphism $\lambda \notin \mathbb{Z}$.

That is, an elliptic curve has complex multiplication if it has endomorphisms 'beyond' multiplication by $m$ maps. Complex elliptic curves with complex multiplication are strongly characterized.

**Proposition 3.6.2** ([26, Theorem 2.40]). *If a curve $\mathbb{C}/L$ has complex multiplication, where $L = L_{\langle \omega_1, \omega_2 \rangle}$, then $\tau := \frac{\omega_2}{\omega_1}$ is an imaginary quadratic number and* $\mathrm{End}(E)$ *is an order in $K = \mathbb{Q}(\tau)$.*

We are particularly interested, for an order $\mathcal{O}$ in an imaginary quadratic field $K$, in the set of isomorphism classes of complex elliptic curves with endomorphism ring $\mathcal{O}$, denoted $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$. These classes can be classified once it is recognized that $\mathcal{O}$ and its ideals are themselves lattices. The following sets are especially relevant:

$$\begin{aligned} I_{\mathcal{O}} &= \{\text{invertible ideals of } \mathcal{O}\} && (3.21)\\ \mathbb{C}/I_{\mathcal{O}} &:= \{\mathbb{C}/\mathfrak{a} \mid \mathfrak{a} \in I_{\mathcal{O}}\}. && (3.22) \end{aligned}$$

**Lemma 3.6.3** ([35, Section 17.2 + Theorem 18.9]). *For any $E \in \mathbb{C}/I_{\mathcal{O}}$,* $\mathrm{End}(E) = \mathcal{O}$. *Conversely every complex elliptic curve with endomorphism ring $\mathcal{O}$ is isomorphic (through homothety in their lattices) to a member of $\mathbb{C}/I_{\mathcal{O}}$.*

Thus, $\mathbb{C}/I_{\mathcal{O}}$ constitutes a full set of representatives for $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$. However, these representatives are not in general distinct isomorphism classes of curves. In fact

$$\mathbb{C}/\mathfrak{a} \cong \mathbb{C}/\mathfrak{a}' \Leftrightarrow \mathfrak{a} \sim \mathfrak{a}' \Leftrightarrow [\mathfrak{a}] = [\mathfrak{a}'] \text{ in } \mathrm{Cl}(\mathcal{O}).$$

Thus

**Corollary 3.6.4.** $\mathrm{Cl}(\mathcal{O})$ *is bijective with* $\mathrm{Ell}_{O}(\mathbb{C})$*, by:*

$$[\mathfrak{a}] \to \mathbb{C}/\mathfrak{a} \qquad (3.23)$$

*where $\mathfrak{a}$ is a representative for an ideal class such that $\mathfrak{a} \in I_{\mathcal{O}}$. In particular,* $\mathrm{Ell}_O(\mathbb{C})$ *is finite and its size is $h(\mathcal{O})$, the class number of the order.*

However, there is more than just a bijection; $\mathrm{Cl}(\mathcal{O})$ induces, canonically, a free and transitive action on $\mathrm{Ell}_O(\mathbb{C})$. This action derives from a 'parent' action [35, Theorem 18.11] which, importantly, has an interpretation with isogenies:

$$\begin{aligned} \star : I_{\mathcal{O}} \times \mathbb{C}/I_{\mathcal{O}} &\to \mathbb{C}/I_{\mathcal{O}} \\ \mathfrak{a} \star \mathbb{C}/\mathfrak{b} &= \mathbb{C}/\mathfrak{a}^{-1}\mathfrak{b}. \end{aligned} \tag{3.24}$$

Because $\mathfrak{b} \subseteq \mathfrak{a}^{-1}\mathfrak{b}$, this action derives a quotient isogeny

$$\begin{aligned} \phi_{\mathfrak{a}} : \mathbb{C}/\mathfrak{b} &\to \mathbb{C}/\mathfrak{a}^{-1}\mathfrak{b} \\ z \bmod \mathfrak{b} &\mapsto z \bmod \mathfrak{a}^{-1}\mathfrak{b}. \end{aligned} \tag{3.25}$$

The kernel of this map is the set of points annihilated by $\mathfrak{a}$. In particular under the isomorphism $\Phi$, the isogeny is

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

with kernel the "$\mathfrak{a}$"-torsion $E_{\mathfrak{b}}[\mathfrak{a}]$. In particular the kernel has degree $N(\mathfrak{a})$.

This action can be considered modulo relations of isomorphism, both from the acting group and the acting space, where it is well defined. The induced action is

$$\begin{aligned} * : \mathrm{Cl}(\mathcal{O}) \times \mathrm{Ell}_{\mathcal{O}}(\mathbb{C}) &\to \mathrm{Ell}_{\mathcal{O}}(\mathbb{C}) \\ [\mathfrak{a}] * j(\mathbb{C}/\mathfrak{b}) &= j(\mathbb{C}/\mathfrak{a}^{-1}\mathfrak{b}). \end{aligned}$$

This action is free and transitive [30, Proposition 1.2]. Thus $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$ is a *principal homogenous space* for $\mathrm{Cl}(\mathcal{O})$, or a $\mathrm{Cl}(\mathcal{O})$-*torsor*. Note that there is a certain ambiguity in interpreting $*$ with isogenies: if $[\mathfrak{a}] = [\mathfrak{a}']$, whre $\mathfrak{a}, \mathfrak{a}' \in I_{\mathcal{O}}$, and $N(\mathfrak{a}) \neq N(\mathfrak{a}')$, they necessarily derive non-isomorphic isogenies, though they have as codomain the same isomorphism class of curves.

## 3.7 Reduction to Ordinary Curves over Finite Fields

The group action torsor reduces to the finite field setting, in the following sense.

The $j$ invariants of $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$ all lie in a distinguished Galois extension of $K$, called the Hilbert class field $H_{\mathcal{O}}$, with extension degree the class number $h(\mathcal{O})$. Thus we may restrict ourselves to curves defined over $H_{\mathcal{O}}$ and consider $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C}) = \mathrm{Ell}_{\mathcal{O}}(H_{\mathcal{O}})$. Because the curves are defined over a number field, the following two theorems of Deuring, from Kohel's thesis [21], are extremely relevant.

**Theorem 3.7.1.** *Let $\tilde{E}/\bar{\mathbb{Q}}$ be an elliptic curve with endomorphism ring $\mathrm{End}(\tilde{E}) = \mathcal{O}$, where $\mathcal{O}$ is an order in an imaginary quadratic extension $K$ of $\mathbb{Q}$. Let $\mathfrak{P}$ be a prime ideal of $\mathbb{Q}$, over a prime $p$, at which $\bar{E}$ has nondegenerate reduction $E$. The curve $E$ is supersingular if and only if $p$ has only one prime of $K$ above it. If $p$ splits in $K$, then let $m$ be the conductor of $\mathcal{O}$, so that $\mathcal{O} = \mathbb{Z} + m\mathcal{O}_K$. Write $m = p^r m_0$, where $p^r$ is the largest power of $p$ dividing $m$. Then the endomorphism ring of $E$ is as follows.*

1. $\mathrm{End}(E) = \mathbb{Z} + m_0\mathcal{O}_K$ *is the order of $K$ with conductor $m_0$.*

2. *If $(p, m) = 1$ the map $\varphi \to \bar{\varphi}$ is an isomorphism of* $\mathrm{End}(\tilde{E})$ *onto* $\mathrm{End}(E)$.

**Theorem 3.7.2.** *Let $E$ be an elliptic curve over a finite field $k$ of characteristic $p$ and let $\varphi$ be an endomorphism of $E$. Then there exists an elliptic curve $\tilde{E}$ defined over a number field $H$, an endomorphism $\tilde{\varphi}$ of $\tilde{E}$, and a prime $\mathfrak{P}$ over $p$ in $H$ such that $E$ is isomorphic to the reduction of $\tilde{E}$ at $\mathfrak{P}$, and $\varphi$ corresponds to a reduction of $\tilde{\varphi}$ under this isomorphism*

Now consider a prime $p$ that will give such an isomorphism of endomorphism rings between the complex curves and reduced curves (necessarily ordinary), i.e.

1. $p$ splits in the endomorphism algebra $K$.

2. The prime $\mathfrak{P} \in H_{\mathcal{O}}$ over $p$ induces a non-degenerate reduction of Weierstrass forms.

3. $(p, m) = 1$, where $m$ is the conductor of the order $\mathcal{O}$.

Now, for $q = N(\mathfrak{P}) = p^f$, let $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q)$ be the isomorphism classes of *ordinary* curves defined over $\mathbb{F}_q$. Then the reduction map $\mathcal{O}_{H_{\mathcal{O}}} \to \mathcal{O}_{H_{\mathcal{O}}}/\mathfrak{P}$ extends to a reduction

$$g : \mathrm{Ell}_{\mathcal{O}}(H_{\mathcal{O}}) \to \mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q) \tag{3.26}$$

that is typically a bijection [6]. However, this bijection is non-canonical: for example when $p$ splits completely in $H_{\mathcal{O}}$ we have $h(\mathcal{O})$ reductions, under which a given complex curve $\mathbb{C}/\mathfrak{a}$ can reduce to a curve in each one of the classes in $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q)$.

The reduction $g$ preserves the group actions. Consider the set

$$E_{\mathcal{O}}(\mathbb{F}_q) := \{E/\mathbb{F}_q | \, \mathrm{End}(E) \in \mathcal{O}\}. \tag{3.27}$$

Then we have the reduction of the 'parent' action:

$$\begin{array}{rcl} \star : \mathcal{I}_{\mathcal{O}} \times E_{\mathcal{O}}(\mathbb{F}_q) & \to & E_{\mathcal{O}}(\mathbb{F}_q) \\ \mathfrak{a} \star E & = & E/E[\mathfrak{a}] \end{array} \tag{3.28}$$

as well as, modulo isomorphisms, the reduced action known as the *complex multiplication operator*:

$$\begin{aligned} * : \mathrm{Cl}(\mathcal{O}) \times \mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q) \to \mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q) \\ [\mathfrak{a}] * j(E) = j(E/E[\mathfrak{a}]) \end{aligned} \tag{3.29}$$

that makes $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q)$ a $\mathrm{Cl}(\mathcal{O})$-torsor, a fact which originally motivated isogeny based cryptography. Note that the action $\star$ derives an isogeny: $\phi_{\mathfrak{a}} : E \to E/E[\mathfrak{a}]$ of degree $N(\mathfrak{a})$. Indeed, it constitutes a valid representation for this isogeny.

**Lemma 3.7.3.** *The isogeny $\phi_{\mathfrak{a}}$ induced by an ideal $\mathfrak{a} \in I_{\mathcal{O}}$ is $\mathbb{F}_q$-rational.*

*Proof.* For any $P \in E[\mathfrak{a}]$, and for any $a \in \mathfrak{a}$, we have that $a(\pi_E(P)) = \pi_E(a(P)) = \infty$ since $a, \pi_E$ are both in $\mathcal{O}$. Therefore $\pi_E(P) \in E[\mathfrak{a}]$. The claim follows from Corollary 3.3.5. □

Now we consider the computational question of evaluating the action $\star$. Theoretically, this doesn't necessitate the evaluation of an isogeny — one could lift to a complex curve, compute the action there (where we have canonical models $\mathbb{C}/L$), and reduce it, without deriving the isogeny. This method is usually considered totally infeasible for a number of reasons, but especially that the class number $h(\mathcal{O})$ is usually very large, making the Hilbert class field $H_{\mathcal{O}}$ infeasible to build and work with.

Instead, the best known method involves chaining prime degree isogenies. Indeed, consider first the case where $\mathfrak{a}$ decomposes:

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_n^{e_n} \tag{3.30}$$

into split or ramified prime ideals $\mathfrak{p}_i$ of small norm and with small exponents $e_i$. $\phi_{\mathfrak{a}}$ is computed as the composition of the prime degree isogenies $\phi_{\mathfrak{p}_i}$ induced by the prime ideals.

In the case $\mathfrak{a}$ does not satisfy this smoothness property, the best algorithms compute an isogeny induced by an ideal $\mathfrak{a}' \in [\mathfrak{a}]$ that *is* smooth. $\mathfrak{a}'$ and $\mathfrak{a}$ differ by a principal ideal, i.e. $\mathfrak{a} = (\alpha)\mathfrak{a}'$, and there are efficient ways (in the norm of the ideal $\mathfrak{a}$) of computing this principal ideal and evaluating at points the isogeny corresponding to it. If one is only interested in computing the isogeny star operator $*$, this last step can be skipped — in other words, the approach is optimized for evaluating the star operator.

We close by discussing the basic step of this method, which is to evaluate the isogeny $\phi_{\mathfrak{l}}$ induced by a split prime ideal $\mathfrak{l}$ of small prime norm $l$. $\mathfrak{l}$ is generated by $(l, c + d\pi_E)$, where $\pi_E$ is the Frobenius endomorphism and $c, d \in \mathbb{Z}^+$.

A brute force strategy is to compute all $l+1$ cyclic subgroups of $E[l]$; we can then compute the action of $\mathfrak{l}$ on these subgroups. The one entirely annihilated by $\mathfrak{l}$ is exactly the kernel of $\phi_{\mathfrak{l}}$. We can then use Velu's formulas to evaluate $\phi_{\mathfrak{l}}$ as a rational map.

Lemma 3.7.3 suggests we may be able do better: we ought to be able to avoid exploring isogenies that have no chance of being defined over $\mathbb{F}_q$. We include here a discussion of the so-called Schoof-Elkies-Atkins techniques that frequently narrows the ambiguity to just 2 curves and computes the kernels of the isogenies, for it gives a further sense of how complex theory reduces in a useful way in the finite field setting.

### 3.7.1 Schoof-Elkies-Atkins (SEA) Technique

**Algorithm 1** Compute $\phi_{\mathfrak{l}}$ for a split prime ideal $\mathfrak{l}$

```
Input: $E/\mathbb{F}_q$ in Weierstrass form, $\mathfrak{l} = (l, c + d\pi_E)$ a split prime ideal in $I_{\mathcal{O}}$, where $\mathcal{O} \cong \mathrm{End}(E)$ an order in $K$, and $l \nmid [\mathcal{O}_K : \mathbb{Z}[\pi_E]]$
Output: An evaluation of $\phi_{\mathfrak{l}} : E \to E'$
Construct the modular polynomial $\Phi_l(X, Y) \in \mathbb{F}_q$ and find the two roots $j_1$ and $j_2$ of $\Phi_l(j(E), Y)$ over $\mathbb{F}_q$
For each root, use the formulas (3.31) to find target curves $E_1/\mathbb{F}_q$ and $E_2/\mathbb{F}_q$ and a prime degree isogeny algorithm from Proposition 3.7.6 to find points $P_1$ and $P_2$ such that $\langle P_1 \rangle$ and $\langle P_2 \rangle$ are the kernels of the isogenies to $E_1$ and $E_2$ respectively.
Find which point satisfies $[c] + [d]\pi_q(P_i) = \infty$; this point $P_i$ is the kernel of $\phi_{\mathfrak{l}}$
Use Velu's formula for $\langle P_i \rangle$ to evaluate $\phi_{\mathfrak{l}}$
```

**Definition 3.7.4.** The *modular polynomial of degree* $N$ is a symmetric polynomial $\Phi_N(X, Y)$ of degree $2N+1$ in $\mathbb{Z}[X, Y]$ that parameterizes pairs of $j$ invariants over $\mathbb{C}$ that are related by a cyclic $N$-isogeny (for any representative curves).

Consequently, given a curve $E$ and a prime $l$, the roots of $\Phi_l(j(E), X)$ give the $j$-invariants of complex curves $l$-isogenous to $E$. For each root $j'$, we can construct a curve $E'$ as well as a normalized $l$- isogeny $E \to E'$ via the following 'Atkins-Elkies' formulas [27, 6], which has an elegant derivation in the complex setting.

$$\begin{aligned} s &= -\frac{18}{l}\frac{b}{a}\frac{\Phi_X(j(E),j')}{\Phi_Y(j(E),j')}j(E) \\ a' &= -\frac{1}{48}\frac{s^2}{h(h-1728)} \\ b' &= -\frac{1}{864}\frac{s^3}{h^2(h-1728)} \end{aligned} \tag{3.31}$$

**Lemma 3.7.5** ([27, 7])**.** *The curve $E' : y^2 = x^3 + a'x + b'$, where the coefficients are from (3.31), has $j$-invariant $j'$ and establishes the existence of a normalized and separable $l$-isogeny $\phi : E \to E'$.*

Knowledge of $E, E'$ and $l$ establishes a situation converse to the construction using Velu's formula: whereas Velu's formula finds a quotient isogeny and a codomain curve from a kernel, we seek to find the kernel and the corresponding isogeny from knowledge of the codomain curve and the isogeny's degree. For a prime degree $l$, and where the curves are in short Weierstrass form, there are such *isogeny algorithms* and they have their derivation in the complex setting.

**Proposition 3.7.6** ([4])**.** *Let $E, E'$ be two curves of characteristic $0$ in short Weierstrass form, such that there exists a normalized isogeny $\phi : E \to E'$ of known prime degree $l$. Then one can compute the isogeny $\phi$ in $O(M(l)\log l)$ operations.*

The form of the output of the algorithm is typically a *kernel polynomial* — a univariate polynomial whose roots are exactly the $x$-coordinates of the points in $\ker(\phi)$ (this is sufficient for $E$ in short Weierstrass form for each root is the $x$-coordinate of a pair of additive inverses of $E$, both of which are in $\ker(\phi)$). Note that if we take any root $x$ of $f_{E\to E'}$ and find a corresponding point $P = (x, y)$ on $E$, then $\langle P\rangle = \ker(\phi)$.

*Warning* 3.7.7. Although these isogeny algorithms extend *mutatis mutandis* to cyclic $N$-isogenies [4], they do not hold for non-cyclic $N$-isogenies. Therefore, they cannot be naively applied to an isogeny problem underlying isogeny based cryptography.

The reason these facts are helpful is that all these formulas, as well as their properties, hold mod $\mathfrak{P}$ as well; and in this case inspection reveals that it amounts to reducing mod $q$ (note that we must now take $l \neq char(\mathbb{F}_q)$ to ensure separability). In particular, for $E/\mathbb{F}_q$, we only need consider roots of $\Phi_l(j(E), Y)$ that lie over $\mathbb{F}_q$; only these roots produce curves that have a chance of defining an $\mathbb{F}_q$-rational isogeny. As long as $l \nmid [O_k : \mathbb{Z}[\pi_E]]$, $\Phi_l(j(E), Y)$ will have either $0, 1,$ or $2$ roots [34]. When $\mathfrak{l}$ is a split prime over $l$ it will be exactly 2 (when $l$ is ramified there is no ambiguity). Both of these roots are codomains of $\mathbb{F}_q$ rational $l$-isogenies, and thus we only have an ambiguity of at most 2 as opposed to $l+1$ in determining $\phi_{\mathfrak{l}}$. We use the formulas (3.31) to find their kernel polynomials and test it under the action of $\mathfrak{l}$.

# Chapter 4

# Isogeny-based Cryptography

## 4.1 Cryptography based on Ordinary Curves

Isogeny based cryptography was originally based on ordinary curves, and in particular the $\mathrm{Cl}(\mathcal{O})$-torsor $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q)$. It was discovered first by Couveignes [10] in an unpublished article in 1997 and then later independently by Stolbunov [32] in 2008. Both motivate it from the fact that a set with group action that satisfies certain assumptions of 'efficient' and 'hard' problems in the homogenous space generalizes the classical dichotomy of exponentiation vs. discrete logarithm in finite fields, and consequently leads to cryptographic primitives emulating classical ones such as the Diffie-Hellman key exchange and Elgamal encryption, with analogus security reductions.

### 4.1.1 Hard Homogenous Spaces and Some Public-key Protocols

Couveignes gave a succinct descripton of when and how a $G$-torsor $X$, for a commutative group $G$, can lead to public key cryptography.

**Definition 4.1.1.** A $G$-torsor $X$, for a commutative group $G$, based on the group action

$$* : G \times X \to X$$

is a *hard homogenous space* (HHS) if it meets the following general requirements. The following computations should be computationally efficient:

1. (Group computation) Compute for any $g$, $g^{-1}$, or for any two elements $g_1, g_2$, the product $g_1 g_2$.
2. (Random element) Find a random element $g \in G$.
3. (Membership) Test whether a given element $x$ is contained in $X$.
4. (Action) Given $g \in G$ and $x \in X$, compute $g * x$.

The following problems should be computationally hard:

1. (Vectorization) Given $x, y \in X$, find the $g$ such that $g * x = y$.
2. (Parallelization) Given $x$ and $y = g * x$, respond to a challenge $z \in X$, with $g * z$.
3. (Parallel testing) Given a challenge set $x, y, z, z' \in X$, such that $y = g * x$, decide if $z' = g * z$.

'Hard' and 'Easy' are evaluated according to the concrete examples. A basic parameter is $|G| = |X|$. Since the Vectorization problem can be solved in exhaustive search in $O(|X|^{1/2})$ computations of the group action via the birthday paradox, a basic requirement is that $|X|$ must be large (exponential sized).

We give three examples of public key primitives enabled by a HHS: key exchange (emulating Diffie-Hellman), encryption (emulating the Hashed Elgamal scheme), and a zero knowledge identification protocol. We choose these examples in particular for comparison with the supersingular cryptographic schemes of De Feo-Jao-Plut.

### Key Exchange

The Key Exchange protocol generalizes the Diffie-Hellman protocol.

1. Public parameter: a basepoint $x \in X$
2. Alice chooses a random element $a \in G$, and computes $k_a = a * x$, sending this value to Bob
3. Bob chooses a random element $b \in G$, and computes $k_b = b * x$, sending this value to Alice

4. Alice computes $k_{AB} = a * K_b$, while Bob computes the same key $k_{AB} = b * K_A$.

**Proposition 4.1.2.** *The key exchange is* ***KP*** *under an eavesdropping attack with a security reduction to the parallelization problem.*

*Proof.* (Sketch). Consider an algorithm $\mathcal{A}$ that can efficiently solve for the shared key with an eavesdropping attack with sufficiently high probability. Consider also a random instance of the Parallelization problem where we are given $x \in X$ and $y = g * x$ and we are asked to respond to a challenge $z \in X$ with $z' = g * z$. Give $\mathcal{A}$ the inputs $x, k_A := y, k_B := z$. $\mathcal{A}$ outputs a value $k_{AB}$, which is $z'$ with high probability. □

### Public Key Encryption

This protocol generalizes the Hashed Elgamal scheme, and is outlined in Stolbunov's thesis.

1. Public parameters: Hash function $H = \{H_k\} : X \to \{0,1\}^w$, public basepoint $x \in X$.

2. Key Generation: secret key $sk \in G$ randomly chosen and public key $pk = sk * x$, $k \in K$.

3. Encryption: Choose $a \in G$. Then $E(m) = (c, z) := (H_k(a * pk) \oplus m, a * x)$.

4. Decryption: $m = D(c, z) = H_k(sk * z) \oplus c$.

**Proposition 4.1.3** ([32, Theorem 3.2])**.** *The encryption scheme is* ***IND-CPA*** *under the additional assumption that $H$ is entropy smoothing, with a security reduction to the parallel testing problem.*

### Identification Protocol

The protocol is a $\Sigma$-protocol. Peggy proves herself (via her identity $g_p \in G$) to Victor as follows:

1. Public parameters: public basepoint $x \in X$, public-key $pk = g_p * x$.

2. Peggy chooses a random $r \in G$ and computes and transmits $y = r * pk$.

3. Victor chooses a random challenge bit $b \in \{0, 1\}$.

4. If $b = 0$, Peggy reveals $r$ and Victor checks that $r * pk = y$, Else Peggy reveals $g = r * g_p$ and Victor checks that $g * x = y$.

**Proposition 4.1.4.** *[10, 4]The $\Sigma$-protocol is computationally zero knowledge with a security reduction to the parallel testing problem, with soundness error not exceeding* $1/2$. *It can be repeated $t$ times to achieve a soundness error bound of* $1/2^t$.

### 4.1.2 The $\mathrm{Cl}(\mathcal{O})$-torsor $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q)$ as a HHS

$$\begin{tikzcd}
j(E) \arrow[r] \arrow[d] & {[\mathfrak{a}] * j(E)} \arrow[d] \\
{[\mathfrak{b}] * j(E)} \arrow[r] & {[\mathfrak{a}][\mathfrak{b}] * j(E)}
\end{tikzcd}$$

Figure 4.1: DH-type key exchange using ordinary curves

Here we briefly examine the conditions under which $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q)$ can be a HHS. The basic requirement is that $|\,\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q)| = h(\mathcal{O})$ is exponentially large. Writing $h_{\mathcal{O}}$ as $h_{\Delta}$, where $\Delta = disc(\mathcal{O})$, we have

$$h(\Delta) = O(\sqrt{\Delta}\log(\Delta)). \tag{4.1}$$

So $|\Delta|$ needs to be of exponential size. However, even with the best algorithms today, computing the group action — the complex multiplication operator — is subexponential in $\log(|\Delta|)$ (and polynomial in the degree of the acting ideal). Thus encryption in any possibly secure instance of this cryptography has limited performance. We overview a strategy to compute the group action (part of which was discussed in Chapter 1), for it will also have relevance for us later when we discuss destructive algorithms.

#### Computing the Group Action

**Problem 4.1.5.** *Given a $j(E)$ in $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q)$, and $[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O})$, compute $[\mathfrak{a}] * j(E)$.*

As mentioned in Section 2, the strategy for computing this action involves factoring

$$[\mathfrak{a}] = [\mathfrak{p}_1]^{e_1}[\mathfrak{p}_2]^{e_2}...[\mathfrak{p}_n]^{e_n} \tag{4.2}$$

**Algorithm 2** Computing the complex multiplication operator (template)

```
Input: $\Delta, q, [\mathfrak{a}], j(E)$
Output: The element $j(E') \in \mathrm{Ell}_\Delta(\mathbb{F}_q)$ such that $[\mathfrak{a}] * j(E) = j(E')$
1: Compute a factor base $\mathcal{F} = \{\mathfrak{p}_1, \dots, \mathfrak{p}_\mathfrak{n}\}$ of split prime ideals of norm $\leq B$ for some specified $B$
2: Compute a vector $\mathbf{e} = (e_1, \dots, e_n)$ of small $L^1$ norm such that $[\mathfrak{a}] = [\mathfrak{p}_1]^{e_1}[\mathfrak{p}_2]^{e_2} \dots [\mathfrak{p}_n]^{e_n}$
3: Compute a sequence of $(\phi_1, ..., \phi_s)$ of isogenies such that the composition $\phi_c : E \to E_c$ of the sequence has kernel $E[\mathfrak{p_1}^{e_1}...\mathfrak{p_n}^{e_n}]$ using the method of Algorithm 1 in Section 3
4: Return $j(E_c)$
```

where the $\mathfrak{p}_i$ are split prime ideals of small norm and $e_i$ are small exponents, and computing sequentially the action of the split prime ideals. This step (Step 3) is computed in time proportional to $\prod |e_i| N(\mathfrak{p}_i)^2$, so the time taken in this step depends on the 'quality' of the factorization (Steps 1 and 2). Let us briefly discuss this.

The strategy is to compute a finite factor base $\mathcal{F}$ of split primes of bounded norm under which all class group elements can decompose, i.e. for which:

$$\mathrm{Cl}(\mathcal{O}) = \bigotimes_{\mathcal{F}} \mathfrak{p}_i. \tag{4.3}$$

Classical theory (Minkowski's bound) gives the existence of a factor base with norm bound $O(\sqrt{\Delta})$, but under the Generalized Riemann Hypothesis (GRH), a factor base with a much smaller norm bound applies.

**Proposition 4.1.6** (Bach's bound [1]). *Under GRH, there is a factor base for* $\mathrm{Cl}(\mathcal{O}_\Delta)$ *consisting of prime ideals of norm* $< 12\log^2(\Delta)$*.*

However, there is the computational question of actually computing a decomposition 4.3 for an input ideal class $[\mathfrak{a}]$, according to which the entries of vector of exponents $\mathbf{e}$ are small. This requirement can establish a tradeoff with the norm bound $B$ we choose: the more split prime ideals we include, the more relations we can find efficiently, and the easier it is to factor with small exponents.

This particular strategy was described by Broker, Charles, and Lauter [6]. Since then different algorithms for factoring have been described [20, 8, 33] that work better for different parameter choices, and based on different heuristics.

**Proposition 4.1.7.** *The algorithm of Childs, Jao, and Soukharev [8] based on the template in Algorithm 2 has worst case running time of at most* $L_q(\frac{1}{2}, \frac{\sqrt{3}}{2})$*, assuming only GRH.*

#### Parameter Choices

Both Couveignes and Stolbunov proposed that the torsor be based around the maximal order $\mathcal{O} = \mathcal{O}_K$. Couveignes in fact proposes to choose parameters $t, q$ such that the discriminant of $K = \mathbb{Q}(\sqrt{\Delta})$, where $\Delta := t^2 - 4q$ is squarefree, in which case the only possibility for a curve $E/\mathbb{F}_q$ with trace $t$ is $\mathcal{O} = \mathcal{O}_K$. Naively, this stipulation seems unnecessary, especially since the class number increases for suborders

$$h_{\mathcal{O}} = h_K c[\mathcal{O}_K^* : \mathcal{O}^*] \prod_{p|c} (1 - (\frac{K}{p}) p^{-1}).$$

But this increase in cardinality is misleading. The vectorization problem in the suborder $\mathcal{O}$ of $\mathcal{O}_K$ can often easily reduce to a vectorization problem in $\mathcal{O}_K$. This reduction can be viewed as a consequence of the structure of isogeny graphs for ordinary curves, and we'll explore it in the next chapter.

Note that finding the discriminant of the maximal order, which is necessary, e.g. for computing the group action, involves computing and factoring $\Delta$. In a randomized algorithm for choosing a basepoint $E_0/\mathbb{F}_q$, the trace of Frobenius $t_q$ and hence $\Delta$ can be determined efficiently from Schoof's point counting algorithm, but factoring can be hard, especially when $\Delta$ is a product of large primes. The only situation that is reasonable is when $\Delta$ is a product of a large prime and several small ones.

## 4.2 Cryptography based on Supersingular Curves

### 4.2.1 Overview

The supersingular protocols of De Feo-Jao-Plut are inspired by the protocols in the ordinary case in that they are also based on legitimate parties being able to compute a shared commutative diagram with knowledge of a subset of the arrows — isogenies —- that hold the secret kernels $\langle R \rangle$ and $\langle S \rangle$. In the ordinary case it is ideal classes, and their commutativity, that makes this shared construction possible. In this supersingular setting, despite the non-commutativity of the endomorphism ring, legitimate parties can still establish the

$$\begin{tikzcd}
E \arrow[r] \arrow[d] & E/\langle S\rangle \arrow[d] \\
E/\langle R\rangle \arrow[r] & E/\langle S, R\rangle
\end{tikzcd} \tag{4.4}$$

Figure 4.2: Principle behind De Feo-Jao-Plut schemes

square (4.4) by transmitting auxiliary information that is conjectured not to compromise their secrets.

Not only are their schemes a candidate for post-quantum cryptography, it also beats the ordinary protocols from a performance standpoint.

### 4.2.2 Parameters

It is the very particular parameter choices that makes the cryptography possible. The following are computed as setup

1. The characteristic of the prime subfield of the curves $p$ is a large prime of the form $l_A^{e_A} l_B^{e_B} f \pm 1$, where $f$ is a cofactor. These primes are known to be dense [24], so for any choice of $l_A, l_B, e_A, e_B$, a simple trial and error algorithm finds a prime of this form.

2. The base point $E/\mathbb{F}_{p^2}$ is a supersingular curve over $\mathbb{F}_{p^2}$ cardinality $(l_A^{e_A} l_B^{e_B} f)^2$. Such a curve can be computed efficiently via an algorithm of Broker [5].

3. Torsion bases $P_A, Q_A$ of $E[l_A^{e_A}]$ and $P_B, Q_B$ of $E[l_B^{e_B}]$ can be computed efficiently via a simple randomized algorithm that scales random points of $E$, and tests linear independence via the Weil pairing [31, III.8]

The information $p, E, l_A, e_A, l_B, e_B, P_A, P_B, Q_A, Q_B$ are all public parameters of the system. The secrets $\langle S\rangle$ (resp $\langle R\rangle$) are cyclic subgroups of the $l_A^{e_A-1}(l_A+1)$ full cyclic subgroups possible in $E[l_A^{e_A}]$ (resp $l_B^{e_B-1}(l_B+1)$ in $E[l_B^{e_B}]$. The cofactor $f$ has to be sufficiently small that these are large.

### 4.2.3 Protocols

**Key Exchange**

1. Alice randomly chooses two elements $m_A, n_A \in \mathbb{Z}/l_A^{e_A}\mathbb{Z}$, not both divisible by $l_A$, and computes $K_A = \langle [m_A]P_A + [m_B]P_B \rangle$, the kernel of an isogeny $\phi_A : E \to E_A$. She transmits to Bob $E_A$ as well as the auxiliary input $\phi_A(P_B), \phi_A(Q_B)$, the image of the *other* torsion base under the secret isogeny.

2. Bob randomly chooses two elements $m_B, n_B \in \mathbb{Z}/l_B^{e_B}\mathbb{Z}$, not both divisible by $l_B$, and computes $K_B = \langle [m_B]P_B + [n_B]Q_B \rangle$, the kernel of the secret isogeny $\phi_B : E \to E_B$. He transmits to Alice $E_B$ as well as $\phi_B(P_A), \phi_B(Q_A)$.

3. With the auxiliary input, Alice computes an isogeny $\phi'_A : E_B \to E_{AB}$ with kernel $\langle [m_A]\phi_B(P_A) + [n_A]\phi_B(Q_A) \rangle$. Bob proceeds similarly to compute an isogeny $\phi'_B$ with kernel $\langle [m_B]\phi_A(P_B) + [m_B]\phi_A(Q_B) \rangle$.

4. $\phi'_B \circ \phi_A \cong \phi_A \circ \phi_B$, and in particular these compositions have isomorphic codomain

$$E_{AB} = E_0/\langle [m_A]P_A + [n_A]Q_A, [m_B]P_B + [n_B]Q_B \rangle$$

and the $j$-invariant of this curve is the secret key.

The auxiliary input provides an eavesdropper with the ability to evaluate $\phi_A$ on all of $E[l_B^{e_B}]$ (resp $\phi_A$ on $E[l_A^{e_A}]$). This same information is revealed in all the protocols of De Feo-Jao-Plut. However, it is conjectured that this leakage reveals no essential information about $\phi_A$ or $\phi_B$.

**Public Key Encryption**

1. Additional public parameter: a Hash function $H = \{H_k\}_{k \in K} : \mathbb{F}_{p^2} \to \{0,1\}^w$.

2. Key generation: Choose random elements $m_A, n_A \in \mathbb{Z}/l_A^{e_A}\mathbb{Z}$, not both divisible by $l_A$, as well as a random key index $k \in K$. Compute $\phi_A$ as before. The public key is $(E_A, \phi_A(P_B), \phi_A(Q_B), k)$ and the private key is $(m_A, n_A, k)$.

3. Encryption: Randomly choose $m_B, n_B \in \mathbb{Z}/l_B^{e_B}$, and compute $\phi'_B : E_A \to E_{AB}$ as before. Then

$$E(m) = (c := H_k(j(E_{AB}) \oplus m, E_B, \phi_B(P_A), \phi_B(Q_A)). \tag{4.5}$$

4. Decryption: Compute $\phi'_A : E_B \to E_{AB}$ as before. Then recover $m = H_k(j(E_{AB})) \oplus c$.

**Identification Protocol**

In this $\Sigma$-protocol, Peggy wants to prove herself via her identity $S$, a secret $l_A^{e_A}$ torsion point defining an isogeny $\phi : E \to E/\langle S \rangle$.

1. In addition to a torsion base $P, Q$ of $E[l_B^{e_B}]$, their images $\phi(P), \phi(Q)$ become part of the public parameters of the protocol.
2. Peggy chooses a primitive $l_B^{e_B}$ torsion point $R$ and computes a square (4.4). She sends $E/\langle R \rangle$ and $E/\langle S, R \rangle$ as commitment.
3. Victor selects a random bit challenge $b \in \{0, 1\}$.
4. If $b = 0$, Peggy reveals the points $R$ and $\phi(R)$. Victor accepts if they have order $l_B^{e_B}$ and generate the kernels of the isogenies $E \to E/\langle R \rangle$ and $E/\langle S \rangle \to E/\langle S, R \rangle$ respectively.
5. If $b = 1$, Peggy reveals the points $\psi(S)$, where $\psi : E/\langle R \rangle \to E/\langle S, R \rangle$ in the square. Victor accepts if it has order $l_A^{e_A}$ and generates the kernel of the isogeny $E/\langle R \rangle \to E/\langle S, R \rangle$.

### 4.2.4 Performance

These protocols are much faster than the ones proposed for ordinary case. In particular the analagous step to computing the complex multiplication operator is to compute, for a random point $R$ of order $l^e$, the codomain of the isogeny $\phi : E \to E/\langle R \rangle$ as well as evaluate $\phi$ it on auxiliary input points. Naively, applying Velu's formulas to retrieve $\phi$ explicitly is a $O(l_i^{e_i}) = O(\sqrt{p})$ algorithm in time and space, and therefore impractical. However, retrieving $\phi$ 'wholly' is not required. $\phi$ is a composition of $l$-isogenies. Finding such an $e$-length chain and 'pushing' the evaluation of an auxiliary point is simpler, and we can describe it by via an iterative process:

**Lemma 4.2.1.** *Set $E_0 = E$, $R_0 = R$ of order $l^e$, $P_0 = P$ an auxiliary point, and for $0 \leq i < e$, let*

$$E_{i+1} = E_i/\langle [l^{e-i-1}]R_i \rangle, \qquad \phi_i : E_i \to E_{i+1} \qquad R_i = \phi_i(R_i) \qquad P_{i+1} = \phi_i(P_i).$$

*Then $\phi = \phi_{e-1} \circ \cdots \circ \phi_0$, so in particular $E_{e-1} = E/\langle R \rangle$.*

If we have to compute $[l^{e-i-1}]R_i$ from $R_i$ at each stage of the iteration, it results in an algorithm with quadratic complexity in $e$. Although this is already feasible, in practice this can still be improved significantly

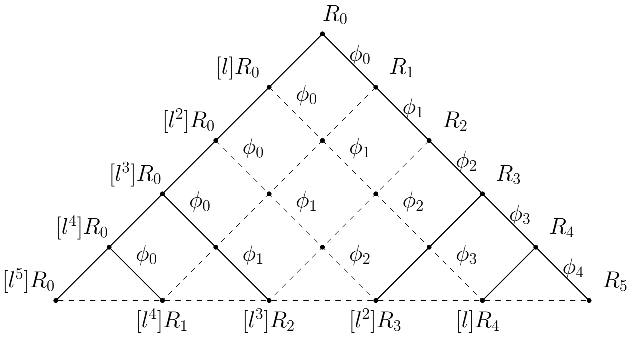

Figure 4.3: A 'balanced strategy' where $R_0$ has order $l^6$; only the bold edges are computed

This diagram represents the iterative process. Each node represents a scalar multiple of $R_i$ that might be explicitly computed. To compute each new rational map $\phi_i$, we have to 'reach' the node $[l^i]R_i$ and apply Velu's formula. Notably, one does not need to compute the values of all the nodes. Consider the subset of the edges in the figure indicative by the bold line, and consider a depth first search through that particular subgraph starting from the top, with a left-first order. In this search, to traverse a positive sloping edge invokes the cost of a scalar multiple of $l$ times a point, and to traverse a downward sloping edge invokes the cost of an evaluation of a rational map at a point. When the bottom row is reached, Velu's formula is applied with the given kernel in order to retrieve the rational map that allows one to move right. Such a 'balanced strategy' (named for the symmetry in the cost tree) has $\frac{1}{2\log 2}n\log(n)$ edges as opposed to $\frac{n(n-1)}{2}$, thus saving heavily in performance cost. One can improve slightly beyond the balanced strategy: the authors of [12] describe an efficient dynamic programming algorithm for the optimal strategy with respect to any measure of cost of, respectively, computing a scalar multiple of a point, and evaluating a degree $l$ map at a point.

### 4.2.5 Underlying Computational Problems

We consider first the problem that, analogous to the vectorization problem, constitutes a total break to all the protocols at once if solved efficiently.

**Problem 4.2.2** (Computational Supersingular Isogeny (CSSI) problem [12])**.** *Let $\phi_A : E_0 \to E_A$ be an isogeny whose kernel is $\langle [m_A]P_A + [n_A]Q_A \rangle$, where $m_A, n_A$ are chosen at* *random from $\mathbb{Z}/l_A^{e_A}\mathbb{Z}$ and not both divisible by $l_A$. Given $E_A$ and the values $\phi_A(P_B), \phi_A(Q_B)$, find a generator $R_A$ of $\langle [m_A]P_A + [n_A]Q_A \rangle$.*

The reason any generator $R_A$ is sufficient is that the extended discrete logarithm problem $R_A = [m_A]P_A + [n_A]Q_A$ is easy for $E_0$, a curve with smooth order.

There is another problem that, for these schemes, is also an 'underlying' problem in that its solution would compromises multiple security objectives and undermine the identification protocol completely.

**Problem 4.2.3** (Decisional Supersingular Isogeny (DSSI) Problem [12])**.** *Let $E_A$ be an another isogenous curve defined over $\mathbb{F}_{p^2}$. Decide whether $E_A$ is $l_A^{e_A}$-isogenous to $E_0$.*

Later we will consider whether algorithms for supersingular elliptic curves help to solve these problems in particular.

# Chapter 5

# Algorithms for Isogeny Problems and Isogeny Based Cryptography

## 5.1 Algorithmic Paradigm: Navigating Isogeny Graphs

Consider the most general isogeny problem:

**Problem 5.1.1.** *Given curves $E_1, E_2$ that are known to be isogenous, compute an isogeny $\phi : E_1 \to E_2$.*

**Lemma 5.1.2** ([35, 6.9])**.** *Any isogeny can be decomposed into a sequence of isogenies of prime degree.*

Because of the above lemma, a major algorithmic strategy for resolving the isogeny problem, in the finite field case, involves computing a sequence of isogenies $\{\phi_i\}_{i=1}^{n}$ of prime degree to intermediate curves such that:

$$\phi_n \circ ... \circ \phi_1 : E_1 \to E_2.$$

For example, a basic walking algorithm 'navigates' the isogeny class of $E_0$ with prime degree isogeny 'steps' until arriving at $E_1$. Such a strategy motivates the usefulness of isogeny graphs: graphs whose vertex sets are curves of an isogeny class (up to a specified isomorphism) and whose edge sets are isogenies (again, up to isomorphism) of degrees from a specified set of primes. The 'isogeny problem' can be recast as a problem of finding a path in the graph. The key question is:

**Question 5.1.3.** *How does an isogeny graph exhibit structure that can be exploited for an algorithm to solve an isogeny problem?*

A second key question is the nature of the solution obtained by an algorithm.

**Question 5.1.4.** *What are the consequences of the algorithms obtained for isogeny based cryptography?*

This chapter addresses both these questions. We separate the discussion of ordinary and supersingular curves, not only because they are always in distinct isogeny classes, but because their isogeny graphs display different structure.

## 5.2 The Ordinary Case

### 5.2.1 Levels and Volcanoes

The material in this subsection is primarily based on [34].

Isogeny graphs of ordinary curves exhibit a highly visual structure that can be exploited for an algorithm. Suppose we are investigating an isogeny problem for curves and isogenies defined over $\mathbb{F}_q$. Then the $\mathbb{F}_q$ isogeny class they belong to is characterized by trace:

$$\mathrm{Ell}_t(\mathbb{F}_q) := \{j(E) : E/\mathbb{F}_q \mid tr(\pi_E) = t\}.$$

$\mathrm{Ell}_t(\mathbb{F}_q)$ will be the vertex set of an isogeny graph. These points can be helpfully placed visually in 'levels' depending on the endomorphism ring. The levels are the sets from the following disjoint union:

$$\mathrm{Ell}_t(\mathbb{F}_q) = \bigsqcup_{\mathbb{Z}[\pi]\subseteq\mathcal{O}\subseteq\mathcal{O}_K} \mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q). \tag{5.1}$$

where the Frobenius element $\pi$ is always the same in the endomorphism algebra $K = \mathbb{Q}(t^2-4q)$. Each endomorphism order $\mathcal{O}$ above is $\mathcal{O} = \mathbb{Z} + c\mathcal{O}_K$ for $c|c_\pi$, where $c_\pi := [\mathcal{O}_K : \mathbb{Z}[\pi]]$. $c$ is the *conductor* for the order $\mathcal{O}$.

Each torsor $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q)$ above constitutes a level and we place a particular torsor $\mathrm{Ell}_{\mathcal{O}_1}(\mathbb{F}_q)$ above $\mathrm{Ell}_{\mathcal{O}_2}(\mathbb{F}_q)$ if the conductor of the former is strictly smaller than the latter.

Separable prime degree isogenies have a visual meaning from this placement of curves.

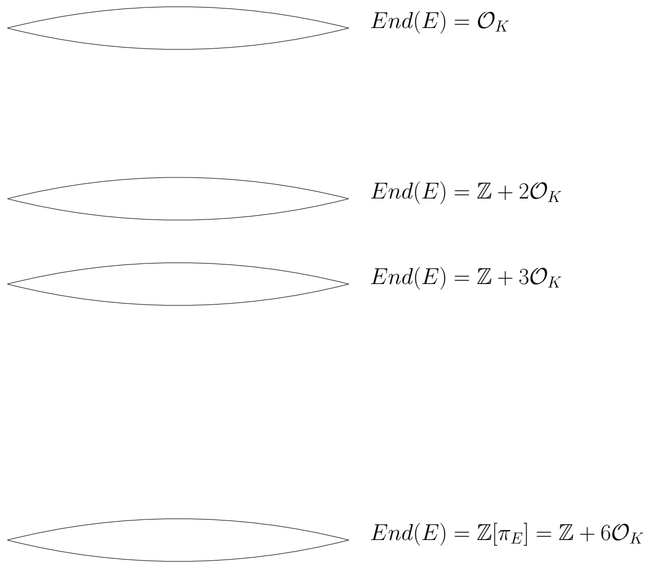
$End(E) = \mathcal{O}_K$
$End(E) = \mathbb{Z} + 2\mathcal{O}_K$
$End(E) = \mathbb{Z} + 3\mathcal{O}_K$
$End(E) = \mathbb{Z}[\pi_E] = \mathbb{Z} + 6\mathcal{O}_K$

Figure 5.1: Level structure where $[O_K : \mathbb{Z}[\pi]] = 6$

**Notation 5.2.1.** For the rest of this section, $l$ will denote a prime such that $l \neq char(\mathbb{F}_q)$.

**Proposition 5.2.2.** *For any $l$-isogeny $\phi : E \to E'$, we have either*

$$\begin{aligned} &\mathrm{End}(E) = \mathrm{End}(E') \\ &[\mathrm{End}(E) : \mathrm{End}(E')] \;=\; l \\ &[\mathrm{End}(E') : \mathrm{End}(E)] \;=\; l. \end{aligned} \tag{5.2}$$

Thus it is meaningful to talk of $\phi$ as horizontal, descending, or ascending (the 1st, 2nd, and 3rd case respectively in (5.2)). Furthermore

**Proposition 5.2.3.** *Every horizontal $l$-isogeny is induced by an ideal $\mathfrak{l}$ over $l$ in the endomorphism ring.*

Now for such a prime $l$, we can consider the vertex set $\mathrm{Ell}_t(\mathbb{F}_q)$ with an edge set of $\mathbb{F}_q$-rational $l$-isogenies, to produce the isogeny graph $G_{l,t}(\mathbb{F}_q)$. This graph can be considered undirected because every $l$-isogeny enables a dual isogeny of the same degree (note that a solution to an isogeny problem is directed, so we may have to take duals when computing an isogeny as a path).

A major theorem is that the ordinary components of $G_{l,t}(\mathbb{F}_q)$ are strongly classified as *volcanoes*:

**Definition 5.2.4.** An $l$-volcano $V$ is a connected undirected graph whose vertices are partitioned into one or more levels $V_0, ..., V_d$ such that:

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 $l + 1$.

For $d = 0$, $V$ is a connected regular graph of degree at most 2.

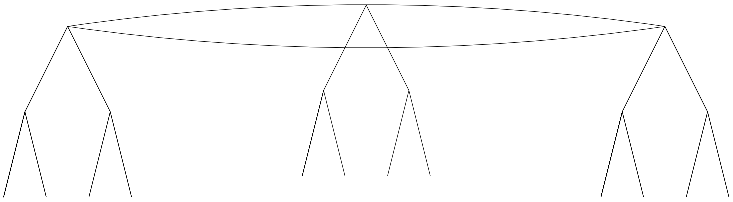

Figure 5.2: Example of a 2-volcano

The fact that the components of the $l$-isogeny graph are volcanoes has major implications on 'travelling' with $l$-isogenies, such as:

1. It is only possible to traverse horizontally on the surface of the volcano.
2. For a curve not on the surface, there is a unique way to ascend.
3. At the floor of the volcano, there is only one way to traverse: ascend.

The precise theorem is as follows.

**Theorem 5.2.5.** *Let $V$ be an ordinary component of $G_{l,t}(\mathbb{F}_q)$ that does not contain 0 or 1728. Then $V$ is an $l$-volcano for which:*

1. *Vertices in $V_i$ have endomorphism ring $O_i$.*
2. *$l \nmid [\mathcal{O}_K : \mathcal{O}_0]$ and $[\mathcal{O}_i : \mathcal{O}_{i+1}] = l$.*
3. *The depth of $V$ is $v_l(c_\pi)$.*

4. *If $l$ is inert in $\mathcal{O}_0$, $|V_0| = 1$. Otherwise $|V_0| = ord([\mathfrak{l}])$, where $\mathfrak{l}$ is a prime ideal in $\mathcal{O}_0$ over $l$.*

5. *Every vertex in $v_i$ has $\frac{h(\mathcal{O}_{i+1})}{h(\mathcal{O}_i)}$ children. Furthermore, by arbitarily identifying a parent-child pair $v_i, v_{i+1}$ with the class group identities $(1_{\mathrm{Cl}(\mathcal{O}_{i+1})}, 1_{\mathrm{Cl}(\mathcal{O}_i)})$, the children of a certain vertex $v_i \in V_i$ are the coset of the kernel of the projection $\rho : \mathrm{Cl}(\mathcal{O}_{i+1}) \to \mathrm{Cl}(\mathcal{O}_i)$. This kernel is generated by an invertible ideal of norm $l^2$.*

Given the volcano structure, the best available algorithm to the general isogeny problem for ordinary curves $E_1$ and $E_2$ has the following outline:

1. Compute an ascending chain of isogenies from $E_1$, $E_2$ to $E_1', E_2'$ respectively, where $E_1'$ and $E_2'$ are curves with maximal order $\mathcal{O}_K$.

2. Solve a vectorization problem for $E_1'$ and $E_2'$ in $\mathcal{O}_K$ and apply it (using e.g. [20], based on the template of algorithm 2).

The algorithm can be considered computing a path in the isogeny graph $G_{\mathcal{L},t}(\mathbb{F}_q)$, with the given vertex set and edge set of isogenies with degrees from $\mathcal{L}$:

$$\mathcal{L} = \mathcal{S} \cup \mathcal{F} \tag{5.3}$$

where $\mathcal{S}$ is the set of primes that divide the conductor $c_\pi$ (some of which are required to ascend) and $\mathcal{F}$ is a factor base of Elkies primes below a certain bound (described in the next section).

Step 1 is based on algorithms of Kohel [21], who was the first to use the volcano structure for algorithms. We will not describe it in detail but remark that it can be totally infeasible if $c_\pi$ contains large prime factors, and constitute the bottleneck of the overall algorithm. However, as Galbraith, Hess, and Smart [17] remark, on average $c_\pi$ is both 'small and smooth', and Kohel's algorithm is typically extremely efficient, so is not included in the runtime of the algorithm.

Note that this level/volcano structure hints that there is no real security advantage, in for example the protocols of Couveignes, to be gained by encrypting in any order than the maximal order $\mathcal{O}_K$. For example, consider encyrpting using the order $\mathcal{O}' = \mathbb{Z} + l\mathbb{O}_{\mathbb{K}}$, for $l$ a small prime. Because the projection homomorphism $\rho : \mathrm{Cl}(\mathcal{O}') \to \mathrm{Cl}(\mathcal{O})$ has a known kernel generated by an ideal of norm $l^2$, and ascending is easy via Kohel's algorithm, the vectorization problem in $\mathcal{O}'$ reduces polynomially to the problem in $\mathcal{O}_K$.

The expected bottleneck of the algorithm is solving the vectorization problem. We will overview the best classical and quantum solutions to this problem.

### 5.2.2 Classical Algorithm for the Vectorization Problem: The Algorithm of Galbraith-Hess-Smart

**Problem 5.2.6.** *Given $E_1, E_2/\mathbb{F}_q$ ordinary elliptic curves satisfying $\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q)$, and $\mathrm{End}(E_1) = \mathrm{End}(E_2) = \mathcal{O}_K$, the maximal order in the endomorphism algebra $K$ of the curves, find an ideal class $[\mathfrak{s}] \in \mathrm{Cl}(\mathcal{O}_K)$ such that $[\mathfrak{s}] * j(E_0) = j(E_1)$*

The state-of-the-art classical algorithm for the vectorization problem is exponential-time, and is due to Galbraith and Stolbunov [15], based on the algorithm of Galbraith, Hess and Smart (GHS) [17]. We recap just a basic version of GHS here, which captures the major idea of the algorithm (and is close to the performance of the best algorithm).

The GHS algorithm is based on a pair of random walks from $j_1 = j(E_1)$ and $j_2 = j(E_2)$ of small prime degree. The walking 'steps' are with isogenies with degrees from a set $\mathcal{F}$ of Elkies primes whose prime ideal factors generate $\mathrm{Cl}(\mathcal{O}_K)$. The intermediate $j$-invariants and isogeny paths leading to them are recorded because a collision of any walk with another's historical 'journey' can resolve the Vectorization problem. The paths to an intermediate $j$-invariant are recorded by an ideal $\mathfrak{a}$. However, a key point that reduces the algorithmic complexity is that $\mathfrak{a}$ does not represent the 'true' path, potentially massive in length, to that $j$-invariant, but an equivalent one, deduced by smoothing out the ideals in the class group at each step of the walk.

**Algorithm 3** GHS algorithm for Vectorization: basic version

```
Input: $j_1$, $j_2$, $\mathbb{F}_q$ and $\Delta_K = disc(K)$, $B < 6\log(|\Delta_K|)^2$
Output: $[\mathfrak{s}] \in \mathrm{Cl}(\mathcal{O}_K)$ such that $[\mathfrak{s}] * j_0 = j_1$
Set $\mathcal{F} = \{$ primes $l < B | (\frac{-p}{l}) = 1\}$
Set $j_1^0 \leftarrow j_1$, $j_2^0 \leftarrow j_2$, $a_1^0 \leftarrow [1]$, $a_2^0 \leftarrow [1]$, $m \leftarrow 0$
while $j_1^m \notin S_2$ and $j_2^m \notin S_1$ do
    Randomly draw $l_1, l_2 \in \mathcal{F}$
    Randomly walk one-step from the latest $j$-invariants with the given degrees , i.e.
    $(j_1^*, \mathfrak{a_1}^*) \leftarrow$ ONE-STEP $(j_1^m, \mathfrak{a}_1^m, l_1)$ and $(j_2^*, \mathfrak{a_2}^*) \leftarrow$ ONE-STEP $(j_2^m, \mathfrak{a}_2^m, l_2)$
    Increment $m$ and set $(j_1^m, \mathfrak{a}_1^m) = (j_1^*, \mathfrak{a}_1^*)$ and $(j_2^m, \mathfrak{a}_2^m) = (j_2^*, \mathfrak{a}_2^*)$
    Append $(j_1^m, \mathfrak{a}_1^m)$ to $S_1$ and $(j_2^m, \mathfrak{a}_2^m)$ to $S_2$
end while
[There must be a collision in the walk]
if $j_1^m \in S_2$ (resp $j_2^m \in S_1$) then
    find index $i$ in $S_2$ where collision occcured (resp $k$ in $S_1$). Then $j_1^m = j_2^i$ (resp
    $j_2^m = j_1^k$). Compute $\mathfrak{s}' = \mathfrak{a}_1^m \mathfrak{a}_2^{-i}$ (resp. $\mathfrak{s}' = \mathfrak{a}_2^{-m} \mathfrak{a}_1^k$)
end if
Solve and return $\mathfrak{s}$, the reduced ideal of $\mathfrak{s}'$
```

**Algorithm 4** ONE-STEP

```
Input: $j, \mathfrak{a}, l, \Delta_K, \mathbb{F}_q$
Output: Random $\mathbb{F}_q$-rational path of degree $l$
Randomly choose $j^*$, a root of $\Phi_l(j, X)$
Find the ideal $\mathfrak{l}$ of norm $l$ inducing an isogeny $j \to j^*$ via the SEA technique (Algorithm
1)
Solve $\mathfrak{a}^*$, the reduced ideal of $\mathfrak{l}\mathfrak{a}$
Output $(j^*, \mathfrak{a}^*)$
```

**Lemma 5.2.7.** *[17, 3.3]Each step of the walk (ONE-STEP) requires at most $O((\log q)\log(|\Delta_K|)^4 = O((\log q)^5)$ field operations.*

**Lemma 5.2.8.** *[17, 3.3] The while loop in Algorithm 3 is expected to terminate after $\sqrt{\pi h_{\Delta_K}/2} = O((\log q)q^{1/4})$ iterations by the birthday paradox.*

**Corollary 5.2.9.** *[17, 3.3]The overall complexity of Algorithm 3 is $O(q^{1/4+\epsilon})$.*

### 5.2.3 Subexponential Quantum Algorithm for Vectorization: The Algorithm of Childs-Jao-Soukharev

**Algorithm 5** Quantum algorithm of Childs-Jao-Soukharev [8]

```
Input: A finite field $\mathbb{F}_q$, a discriminant $\Delta < 0$, and Weierstrass equations of horizontally isogenous elliptic curve $E_1, E_2$
Output: $[\mathfrak{s}] \in \mathrm{Cl}(\Delta)$ such that $[\mathfrak{s}] * j(E_0) = j(E_1)$
Decompose (via a quantum algorithm) $\mathrm{Cl}(\Delta) = \langle[\mathfrak{b}_1]\rangle \oplus ... \oplus \langle[\mathfrak{b}_k]\rangle$, where $|\langle[\mathfrak{b}_j|\rangle| = n_j$
Solve the hidden shift problem defined by the functions $f_0, f_1 : \mathbb{Z}_{n_1} \times ... \times \mathbb{Z}_{n_k} \to \mathrm{Ell}_{q,n}(\mathcal{O}_\Delta)$ satisfying $f_c(x_1, ..., x_k) = ([\mathfrak{b}_1]^{x_1} ... [\mathfrak{b}_k]^{x_k}) * j(E_c)$, giving some $(s_1, ..., s_k) \in \mathbb{Z}_{n_1} \times ... \times \mathbb{Z}_{n_k}$
Output $[\mathfrak{s}] = [\mathfrak{b}_1]^{s_1} ... [\mathfrak{b}_k]^{s_k}$
```

The main idea of this quantum algorithm is to recast the Vectorization problem as an instance of the *abelian hidden shift problem.*

**Problem 5.2.10** (Hidden Abelian Shift Problem). *Given an abelian group $\mathcal{A}$ and a set of $S$ and two injective functions $f, g : \mathcal{A} \to S$ with the property that:*

$$f(a) = g(a + s) \text{ for all } a \in \mathcal{A} \tag{5.4}$$

*for some 'hidden shift' $s$, deduce $s$ given oracle access to $\mathcal{A}$.*

A crucial part of the quantum complexity for this black-box problem is its quantum query complexity, which refers to how many times $f$ and $g$ are (quantumly) queried (this query complexity, as well as quantum time and space complexities, are all formalized in the quantum circuit model of quantum algorithms). A single query has 'unit cost', unlike in the concrete instance of the problem.

Two different quantum solutions to this black box problem have different query and space complexities.

**Proposition 5.2.11** (Kuperberg [23]). *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.*

**Proposition 5.2.12** (Regev [25]). *There is a quantum algorithm that finds $s$ with time and query complexity $L_{|\mathcal{A}|}(\frac{1}{2}, \sqrt{2})$ using space* $\mathrm{poly}(\log |A|)$.

The vectorization problem is framed as hidden shift by setting the following $f, g : \mathrm{Cl}(\mathcal{O}_K) \to \mathrm{Ell}_{\mathcal{O}_K}(\mathbb{F}_q)$

$$f([\mathfrak{b}]) = [\mathfrak{b}] * j(E_1) \tag{5.5}$$
$$g([\mathfrak{b}]) = [\mathfrak{b}] * j(E_0) \tag{5.6}$$

Then the hidden shift $[\mathfrak{s}]$ with the property $f([\mathfrak{a}]) = g([\mathfrak{a}][\mathfrak{s}])$ is evidently the solution to the Vectorization problem $[\mathfrak{s}] * j(E_0) = j(E_1)$.

As a concrete instance of hidden shift, we now have to multiply the query complexity with the time taken to evaluate $f$ and $g$. Each query involves evaluating the complex multiplication operator, which is a subexponential time algorithm. The point is, a subexponential number of queries to a subexponential time algorithm gives an overall subexponential time complexity.

**Proposition 5.2.13.** *Assuming GRH, Algorithm 5 runs in time $L_q(\frac{1}{2}, \frac{\sqrt{3}}{2})$ using a reduction to Kuperberg's Algorithm for Step 2, and time $L_q(\frac{1}{2}, \frac{\sqrt{3}}{2} + \sqrt{2})$, using a reduction to Regev's algorithm.*

This result obviously threatens the post-quantum security of the isogeny-based cryptographic schemes of Couveignes and Stolbunov.

Note that nothing is gained *classically* by recasting the vectorization problem as hidden shift, because the hidden shift problem offers no better classical solution than a generic brute force attack with an exponential number of queries. That the hidden abelian shift offers a subexponential quantum solution is indicative of the power of quantum computers to do something *better* than classical algorithms. Indeed, many computational problems involving periodic properties exhibit, in the quantum setting, an improvement from a classical brute force strategy through such a reduction.

## 5.3 The Supersingular Case

### 5.3.1 Expander property; Meet in the Middle Algorithm

The 'full' supersingular isogeny graph displays very different properties from the ordinary case. Consider $\mathrm{Ell}(\bar{\mathbb{F}}_p)$, the set of supersingular $j$-invariants defined over $\mathbb{F}_p$. We highlight two basic differences to the ordinary case.

**Lemma 5.3.1** ([13]). *The $j$-invariants in* $\mathrm{Ell}(\bar{\mathbb{F}}_p)$ *are all defined over* $\mathbb{F}_{p^2}$. *The size of this set is:*

$$\left\lfloor \frac{p}{12} \right\rfloor + \begin{cases} 0 & : p \equiv 1 \mod 12 \\ 1 & : p \equiv 5, 7 \mod 12 \\ 2 & : p \equiv 11 \mod 12. \end{cases} \tag{5.7}$$

Thus, any supersingular graph over $\bar{\mathbb{F}}_p$ is finite, whereas a 'full' ordinary graph — whose vertices consist of every non-supersingular $j$-invariant in $\bar{\mathbb{F}}_p$ — is infinite. The other major difference is that $\mathrm{Ell}(\bar{\mathbb{F}}_p)$ constitutes a single $\bar{\mathbb{F}}_p$-isogeny class. In fact, more is true. For any prime $l \neq p$, consider the $l$-isogeny graph $G_l(\bar{\mathbb{F}}_p)$ with vertex set $\mathrm{Ell}(\bar{\mathbb{F}}_p)$ and edge set of $l$-isogenies, where the isogenies are defined over $\bar{\mathbb{F}}_p$.

**Proposition 5.3.2.** *[13]* $G_l(\mathbb{F}_p)$ *is a fully connected regular graph of degree* $l + 1$.

Therefore, and very much unlike the ordinary case, an isogeny problem can be resolved by chaining $l$-isogenies for any prime $l \neq p$. $G_l(\mathbb{F}_p)$ has been known to display even more structure as an *expander graph.* This is a 'well connectedness' property that implies the general isogeny problem always has a solution with short paths.

**Definition 5.3.3.** An expander graph with $N$ vertices has expansion constant $c > 0$, if for any subset $U \subseteq V$ of size $|U| \leq \frac{N}{2}$, the boundary $\Gamma(U)$ satisfies $|\Gamma(U)| \geq c|U|$.

**Proposition 5.3.4** ([22, 4.1]). *An expander graph with $N$ vertices has diameter* $O(\log N)$.

Therefore $G_l(\mathbb{F}_p)$ has diameter $O(\log p)$. This motivates Galbraith's 'meet in the middle' algorithm. It is similar to the bidirectional GHS algorithm for Vectorization, but more primitive. For one, we can stick to just moving with isogenies of a fixed prime degree. Secondly, we cannot represent paths by ideals (let alone reduced ideals), so the issue of space is amplified. The resulting algorithm is $O(p^{1/2})$ in time and space, and was the state-of-the-art for the supersingular isogeny problem until the revelation of Delfs and Galbraith [13] in 2013.

### 5.3.2 Result of Delfs and Galbraith: Partial Reintroduction of 'Ordinary' Structure

Although the full supersingular graph displays very different structure to the ordinary case, Delfs and Galbraith noticed that a certain kind of isogeny graph in the supersingular resembles the ordinary case, and can be helpfully exploited for an algorithm. This subsection summarizes their discoveries in [13].

Delfs and Galbraith discovered this structure appears when consideration is entirely restricted to the prime subfield $\mathbb{F}_p$. That is, not only does one only consider curves over $\mathbb{F}_p$, but we also consider exclusively the subset of morphisms — isomorphisms, endomorphisms, and other isogenies — defined over $\mathbb{F}_p$. The relevant vertex set is:

$$\mathrm{Ell}(\mathbb{F}_p) = \{\text{supersingular curves over } \mathbb{F}_p \text{ up to } \mathbb{F}_p \text{ isomorphism}\}. \tag{5.8}$$

In this case, twist classes constitute different vertices.

**Lemma 5.3.5.** *Each supersingular $j$ invariant $\in \mathbb{F}_p$ corresponds to two different twist classes. As a consequence*

$$|\,\mathrm{Ell}(\mathbb{F}_p)| = 2 * \left( \#j_p = \begin{cases} \frac{1}{2}h(-4p) & : p \equiv 1 \mod 4 \\ h(-p) & : p \equiv 7 \mod 8 \\ 2h(-p) & : p \equiv 3 \mod 8 \end{cases} \right) \tag{5.9}$$

Note that this vertex set constitutes an $\mathbb{F}_p$-isogeny class, since every supersingular curve over $\mathbb{F}_p$ has exactly $p+1$ points.

The older number theoretic result that sparks the insight into the structure possible in an isogeny graph for this vertex set is the following. Let $E/\mathbb{F}_p$ a curve. Then although the full endomorphism ring $\mathrm{End}(E)$ is a maximal order in a quaternion algebra, the subring of endomorphisms defined over $\mathbb{F}_p$, denoted $\mathrm{End}_{\mathbb{F}_p}(E)$, resembles the endomorphism ring for ordinary curves

**Theorem 5.3.6.** *Let $E/\mathbb{F}_p$ be a supersingular curve. Then $\mathrm{End}_{\mathbb{F}_p}(E)$ is an order in $\mathbb{Q}(\pi_E) = \mathbb{Q}(\sqrt{-p})$.*

**Corollary 5.3.7.** *Let $E/\mathbb{F}_p$ a supersingular curve. Then*

1. *if $p \equiv 1 \mod 4$, $\mathrm{End}_{\mathbb{F}_p}(E) = \mathbb{Z}[\pi_E] = \mathbb{Z}[\sqrt{-p}] = \mathcal{O}_K$;*

2. *if $p \equiv 3 \mod 4$, $\mathrm{End}_{\mathbb{F}_p}(E) = \mathbb{Z}[\pi_E] = \mathbb{Z}[\sqrt{-p}]$ or $\mathrm{End}_{\mathbb{F}_p}(E) = \mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{-p}}{2}]$, and $c_\pi = 2$.*

Thus, the vertices $\mathrm{Ell}(\mathbb{F}_p)$ can be considered to be in levels as in the ordinary case (admittedly there is no insight to be gained from this alone when $p \equiv 1 \mod 4$, where there is just one level). However, the fact that gives a complete transplanting of the ordinary case is that each level is again a torsor of the relevant class group, and the ordinary 'volcano' picture also transfers completely. This is deduced via the Deuring lifting and reduction to complex curves, and in particular the correspondence

$$\left\{\begin{matrix}\text{supersingular elliptic}\\ \text{curves over } \mathbb{F}_p\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\text{elliptic curves } E \text{ over } \mathbb{C}\\ \text{with } \operatorname{End}(E) \in \{\mathbb{Z}[\sqrt{-p}], \mathcal{O}_K\}\end{matrix}\right\},$$

$$\left\{\begin{matrix}\mathbb{F}_p\text{-rational } \ell\text{-isogenies}\\ \text{between supersingular}\\ \text{elliptic curves over } \mathbb{F}_p\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\ell\text{-isogenies between}\\ \text{elliptic curves } E \text{ over } \mathbb{C}\\ \text{with } \operatorname{End}(E) \in \{\mathbb{Z}[\sqrt{-p}], \mathcal{O}_K\}\end{matrix}\right\}. \tag{5.10}$$

A full description of the structure is given by Delfs and Galbraith as follows.

**Theorem 5.3.8.** *Let $p > 3$ be a prime.*

1. $p \equiv 1 \mod 4$*: There are $h(-4p)$ $\mathbb{F}_p$-isomorphism classes of supersingular curves over $\mathbb{F}_p$, all having the same $\mathbb{F}_p$ endomorphism ring $\mathbb{Z}[\sqrt{-p}]$. From every one there is an outgoing $\mathbb{F}_p$-rational horizontal 2-isogeny as well as two $l$-isogenies for every prime $l > 2$ with $(\frac{-p}{l}) = 1$.*

2. $p \equiv 3 \mod 4$*: There are two levels in the supersingular isogeny graph. From each vertex there are two horizontal $l$-isogenies for every prime $l > 2$ with $(\frac{-p}{l}) = 1$.*

   *(a) If $p \equiv 7 \mod 8$, on each level $h(-p)$ vertices are situated. Surface and floor are connected $1:1$ with 2-isogenies and on the surface we also have two horizontal 2-isogenies from each vertex.*

   *(b) If $p \equiv 3 \mod 8$, we have $h(-p)$ vertices on the surface and $3h(-p)$ on the floor. Surface and floor are connected $1:3$ with 2-isogenies, and there are no horizontal 2-isogenies.*

Following this structure, the following template for an algorithm to the general supersingular isogeny problem for $E_1$ to $E_2$ presents itself:

1. From $E_1$ to $E_2$, possibly defined over $\mathbb{F}_{p^2}$, compute isogenies to $E_1'$ and $E_2'$ defined over $\mathbb{F}_p$.

2. Compute an isogeny between $E_1'$ and $E_2'$ using algorithms from the ordinary case.

The algorithm can be viewed as computing a path in the isogeny graph $\mathcal{X}(\mathbb{F}_p, \mathcal{L})$, with the vertex set $\operatorname{Ell}(\mathbb{F}_p)$ and $\mathcal{L} = 2 \cup \mathcal{F}$ where $\mathcal{F}$ is a set of Elkies primes generating the class group $\operatorname{Cl}(\mathcal{O}_K)$.

Delfs and Galbraith describe a classical algorithm for the supersingular isogeny problem following this template that improves to $O(p^{1/4})$ time complexity if the curves are defined over $\mathbb{F}_p$, and has a $O(p^{1/2})$ time complexity with the bottleneck of Step 1. Nevertheless, it will have better space complexity than the meet in the middle approach.

We discuss a quantum algorithm based on this template. We can avail of quantum components for both Stage 1 and 2.

## 5.4 A Quantum Algorithm for the Supersingular Isogeny Problem

### 5.4.1 Overview

The algorithm is joint work with Biasse and Jao [2]. The algorithm strategy can be understood in terms of the following schematic (Figure 5.3), which represents a path in the isogeny graph.

$$\begin{tikzcd}
E_1 \arrow[d, "\phi_1\text{: quantum random walk}"'] & & E_2 \arrow[d, bend right, "\phi_2\text{: quantum random walk}"'] \\
E_1' \arrow[rr, "\phi_{\mathfrak{a}}\text{: hidden abelian shift problem}"] & & E_2' \arrow[u, dotted, bend right, "\hat{\phi}_2\text{: dual isogeny}"']
\end{tikzcd}$$

Figure 5.3: Schematic of quantum algorithm for supersingular isogeny problem

The only essentially new step in Algorithm 6 is Step 1. Note that that the ascension in Step 2, which is occasionally insurmountable in the ordinary case, is trivial for us: the maximal order is of a known discriminant and it is trivial to take a 2-isogeny to it.

**Algorithm 6** Quantum algorithm to compute isogeny between supersingular curves over a finite field

```
Input: Supersingular curves $E_1, E_2$ defined over some finite field $F_{p^n}$
Output: An isogeny $\psi : E_1 \to E_2$
Compute isogenies $\phi_1 : E_1 \to E_1'$ and $\phi_2 : E_2 \to E_2'$, where $E_1', E_2'$ are defined over $\mathbb{F}_p$, using the quantum random walk algorithm
If $p \equiv 3 \mod 4$, ascend $E_1', E_2'$ to the maximal order in the $\mathbb{F}_p$ endomorphism ring (call the new curves $E_1, E_2$)
Solve the vectorization problem between $E_1', E_2'$ using the Algorithm 5 to find an ideal class $[\mathfrak{a}]$ such that $[\mathfrak{a}] * E_1' = E_2'$
Compute the action $[\mathfrak{a}]$ using an algorithm based on the template of Algorithm 2, e.g. [8], to find an induced isogeny $\phi_{[\mathfrak{a}]}$
Return $\hat{\phi}_2 \circ \phi_{[\mathfrak{a}]} \circ \phi_1$
```

### 5.4.2 Quantum Random Walk

First we discuss a classical random walk. Consider randomly walking from a curve $E/\mathbb{F}_{p^2}$ with $l$-isogenies on the 'full' supersingular graph $G_l(\bar{\mathbb{F}}_p)$. Intuitively, the chances of success of landing in a curve in $E'/\mathbb{F}_p$ depend on the density of the latter set, i.e. the density of the vertices $G_l(\bar{\mathbb{F}}_p) \bigcap \mathbb{F}_p$. Because the isogeny graph $G_l(\bar{\mathbb{F}}_p)$ is an expander, a certain density is guaranteed. The isogeny graph $G_l(\bar{\mathbb{F}}_p)$ is a distinguished type of regular expander graph known as a *Ramanujan* graph. Without going into detail about this property (which is properly defined in spectral graph theory), we quote the standard result about random walks in such a graph.

**Lemma 5.4.1** ([19])**.** *Let $G$ be a Ramanujan graph of degree $k$ on $N$ vertices. Let $S$ be any subset of the vertices of $G$, and $x$ be any vertex of $G$. Then a random walk of length at least*

$$\frac{\log 2N/|S|^{1/2}}{\log k/(2\sqrt{k-1})}$$

*starting from $x$ will land in $S$ with probability at least $\frac{|S|}{2N}$.*

We can apply this lemma to a walk with 3-isogenies, i.e. in the graph $G_3(\bar{\mathbb{F}}_p)$. In this case obviously $k = l + 1 = 4$, $|N| \geq p/12$ by (5.9), and

$$|S| = \#j_p = \begin{cases} \frac{1}{2}h(-4p) & : p \equiv 1 \mod 4 \\ h(-p) & : p \equiv 7 \mod 8 \\ 2h(-p) & : p \equiv 3 \mod 8. \end{cases} \tag{5.11}$$

These numbers can be well approximated. Under the Generalized Riemann Hypothesis, the class number of the maximal order of $\mathbb{Q}(\sqrt{-d})$ satisfies

$$h(d) \geq (1 + o(1)) \frac{\pi}{12e^{\gamma}} \frac{\sqrt{d}}{\log\log(d)}. \tag{5.12}$$

Using direct substitution into (5.4.1), it is easily verified that

**Proposition 5.4.2.** *Under GRH, a random* 3*-isogeny path of length*

$$\lambda \geq \frac{\big(\log(\frac{2}{\sqrt{6e^{\gamma}}}p^{3/4}\big)}{\log(\frac{2}{\sqrt{3}})} \tag{5.13}$$

*passes through a supersingular $j$ invariant over $\mathbb{F}_p$ with probability at least*

$$\tau := \frac{\pi}{12}\frac{1}{p^{1/2}}. \tag{5.14}$$

From this, elementary probability theory establishes that $M$ independent random walks from a curve has success probability $1 - (1 - \tau)^M$. Therefore:

**Lemma 5.4.3.** $M := \log(2)\frac{e^{\gamma}}{\pi}p^{1/2}$ *independent walks of length $\lambda$ will pass through a supersingular curve with probability $\geq \frac{1}{2}$.*

Each walk is of length $O(\log p)$ and computing each 3-isogeny step of the walk takes a constant amount of field operations with the aid of the modular polynomial $\Phi_3(X, Y)$, so each walk has $O(\log p)$ time complexity. Thus the cost of $M = O(p^{1/2})$ classical walks is, suppressing logarithmic factors, $\tilde{O}(p^{1/2})$.

### Using Grover's Search

The classical result is improved quadratically by walking quantumly. The walk is based on the famous Grover's search black-box problem:

**Problem 5.4.4** (Grover's search)**.** *Given a Boolean function on a domain of size $N$*

$$f : [1, ..., N] \to \{0, 1\} \tag{5.15}$$

*and the existence of an index $i$ such that $f(i) = 1$, find such an $i$, given oracle access to $f$.*

This problem formalizes the situation of searching a completely unsorted database of $N$ items for some particular element $i$. Classically, there is no better way to do this search than brute force — the problem is $\Omega(N)$. However,

**Theorem 5.4.5.** *[18] There exists a quantum algorithm that computes a good index $i$ with time and query complexity $O(\sqrt{N})$, with probability $1 - 1/N$.*

We can naturally recast the problem as a Grover's search where the indices are the $M$ walks and a good index is a sucessful walk. Formalizing this search, as a precomputation we generate a random injection

$$g : [1, ..., N] \to \{3 - \text{isogeny paths of length } \lambda \text{ starting from } E\}. \tag{5.16}$$

Each element on the right could be represented by a string of, for example, members of $\{0,1,2\}$, which represent the roots of the modular polynomial $\Phi_3(j, X)$ at each point of the walk. Each such representation will be $O(\log p)$ in length. The search function is then

$$C_f(x) := \begin{cases} 1 & \text{if } f(x) \text{ passes through a supersingular } j - \text{invariant} \in \mathbb{F}_p \\ 0 & \text{otherwise.} \end{cases} \tag{5.17}$$

As part of a Grover's search algorithm, $C_f$ may be called $O(\sqrt{p^{1/2}}) = O(p^{1/4})$ times. Each call involves $O((\log p)^2)$ cost in time. Thus, supressing logarithmic factors, we have:

**Proposition 5.4.6.** *The quantum random walk algorithm runs in time $\tilde{O}(p^{1/4})$, with success probability close to $1/2$ (in particular, certainly greater than $1/4$).*

**Proposition 5.4.7.** *The overall algorithm 6 has quantum complexity $\tilde{O}(p^{1/4})$ and $L_p(\frac{1}{2}, \frac{\sqrt{3}}{2})$ in the case $E_1$ and $E_2$ are defined over $\mathbb{F}_p$.*

*Proof.* When $E_1$ and $E_2$ are defined over $\mathbb{F}_p$, the only step involved is the quantum algorithm of Childs, Jao, and Soukharev. Noting the algorithmic complexity of that algorithm in Proposition 5.2.13, we see that for the relevant torsor here it is $L_p(\frac{1}{2}, \frac{\sqrt{3}}{2})$. When either curve is not defined over $\mathbb{F}_p$, the quantum random walk is the bottleneck, with exponential complexity $\tilde{O}(p^{1/4})$. □

### 5.4.3 Cryptographic Implications

The quantum attack has direct implications for constructions whose security is premised on the difficulty of computing any isogeny between two supersingular elliptic curves, such as the Charles-Goren-Lauter hash function [7].

However, it has little post-quantum implications (as yet) for the De Feo-Jao-Plut schemes, for the algorithm provides no control over the degree. For example, suppose we give to the algorithm the inputs $E$ and $E_A$ from the CSSI problem. The algorithm returns an unspecified isogeny between $E$ and $E_A$, whereas the CSSI problem requires one to retrieve a particular isogeny of degree $l_A^{e_A}$.

The only possibly inescure case for the CSSI problem is where all the following hold simultaenously: The basepoint $E$ is chosen over $\mathbb{F}_p$ and the secret isogeny $\phi_A : E \to E_A$ is 'accidentally' defined $\mathbb{F}_p$, and in addition $\phi_A$ is the induced action by $\mathfrak{a}$ (in the sense of the 'parent' operator $\star$ mentioned in Chapter 3, so $\phi_{\mathfrak{a}} = \phi_A$). Then our algorithm on inputs $E$ and $E_A$ solves a vectorization problem between the two, and it retrieves an ideal $\mathfrak{a}'$. This ideal $\mathfrak{a}'$ may have the 'wrong' norm distinct from $l_i^{e_i}$, but necessarily $\mathfrak{a}' \in [\mathfrak{a}]$, so $\mathfrak{a} = (\alpha)\mathfrak{a}'$. We can then experiment with post-composing $\mathfrak{a}'$ with principal ideals $(\alpha)$ of norm $\frac{l_i^{e_i}}{N(\mathfrak{a}')}$ in order to retrieve $\mathfrak{a}$.

From rudimentary experiments, it is found that even for the basepoint $E$ chosen over $\mathbb{F}_p$ it is rare for $\phi_A$ to be defined over $\mathbb{F}_p$, and even then it is unclear that $\phi_A$ is necessarily induced by an quadratic ideal $\mathfrak{a}$. Regardless, as a precaution, the De Feo-Plut-Jao scheme can simply require one to choose a basepoint curve outside of $\mathbb{F}_p$. In this case, the bottleneck of the random walk makes the overall algorithm run in exponential time $\tilde{O}(p^{1/4})$.

The best algorithm, so far, for the CSSI and DSSI problems, is a meet in the middle attack that takes into account the specific parameters of the schemes. Two trees from $E$ and $E_A$ consisting of all $l_A$ paths from $E$ and $E_A$ of length (degree) $\frac{e_A}{2}$. Since $l_A^{e_A} \sim \sqrt{p}$, these trees have depth $\sim p^{1/4}$). The problems is then to look for a collision in the set of final images (or, for DSSI, to possibly declare that none exists). This problem can be framed as the claw problem in complexity theory.

**Proposition 5.4.8** ([12]). *Framed as the claw problem, the meet in the middle attack runs in time and space $O(p^{1/4})$. By using an improvement for the quantum black box claw problem, the quantum analogue of this attack runs in $O(p^{1/6})$.*

# Chapter 6

# Future Work

In our opinion, it is worthwhile to continue considering the general supersingular isogeny problem and to obtain structural results for the supersingular isogeny graph — even if the algorithms derived do not threaten a particular scheme directly, they may lead to others that do, and otherwise serve to establish general considerations for constructing isogeny-based cryptography using supersingular curves. The approach of Delfs and Galbraith represents an effort to identify structure that is more 'native' to the ordinary case within the supersingular graph. Identifying torsor structures within the supersingular graph, in particular, was shown to be exploitable for significant classical and quantum algorithms for supersingular isogeny problems.

A distinct approach is to better understand and utilize the characterization of the full supersingular isogeny graph with regards to the curves' full endomorphism rings in quaternion algebras, that Kohel established in his thesis [21, Chapter 5]. For supersingular curves it is also true that the (e.g. left) ideals of the endomorphism ring of a curve dictates the picture of outgoing isogenies from a curve. However, from this fact alone we cannot simply derive a group action characterization of isogenies as in the ordinary case, because the left ideal classes of the endomorphism ring do not even form a group. Still, speculatively speaking, understanding and expanding the intricate mathematics in this domain may lead to novel algorithms for the supersingular isogeny problem that more directly contend with the idiosyncrasies of supersingularity.

# Bibliography

[1] Eric Bach. Explicit bounds for primality testing and related problems. *Mathematics of Computation*, 55(191):355–380, 1990.

[2] Jean-François Biasse, David Jao, and Anirudh Sankar. A quantum algorithm for computing isogenies between supersingular elliptic curves. In *Progress in Cryptology–INDOCRYPT 2014*, pages 428–442. Springer, 2014.

[3] Ian F Blake, Gadiel Seroussi, and Nigel Smart. *Elliptic curves in cryptography*, volume 265. Cambridge university press, 1999.

[4] Alin Bostan, François Morain, Bruno Salvy, and Éric Schost. Fast algorithms for computing isogenies between elliptic curves. *Mathematics of Computation*, 77(263):1755–1778, 2008.

[5] Reinier Bröker. Constructing supersingular elliptic curves. *J. Comb. Number Theory*, 1(3):269–273, 2009.

[6] Reinier Bröker, Denis Charles, and Kristin Lauter. Evaluating large degree isogenies and applications to pairing based cryptography. In *Pairing-Based Cryptography–Pairing 2008*, pages 100–112. Springer, 2008.

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

[8] Andrew Childs, David Jao, and Vladimir Soukharev. Constructing elliptic curve isogenies in quantum subexponential time. *Journal of Mathematical Cryptology*, 8(1):1–29, 2014.

[9] Pete L. Clark. Supplementary lecture notes on elliptic curves.

[10] Jean Marc Couveignes. Hard homogeneous spaces. *IACR Cryptology ePrint Archive*, 2006:291, 2006.

[11] David A Cox. *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*, volume 34. John Wiley & Sons, 2011.

[12] Luca De Feo, David Jao, and Jérôme Plût. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *Journal of Mathematical Cryptology*, 8(3):209–247, 2014.

[13] Christina Delfs and Steven D Galbraith. Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$. *Designs, Codes and Cryptography*, pages 1–16.

[14] William Fulton. Algebraic curves: An introduction to algebraic geometry. 2008.

[15] Steven Galbraith and Anton Stolbunov. Improved algorithm for the isogeny problem for ordinary elliptic curves. *Applicable Algebra in Engineering, Communication and Computing*, 24(2):107–131, 2013.

[16] Steven D Galbraith. *Mathematics of public key cryptography.* Cambridge University Press, 2012.

[17] Steven D Galbraith, Florian Hess, and Nigel P Smart. Extending the GHS Weil descent attack. In *Advances in Cryptology—EUROCRYPT 2002*, pages 29–44. Springer, 2002.

[18] Lov K Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 212–219. ACM, 1996.

[19] David Jao, Stephen D Miller, and Ramarathnam Venkatesan. Expander graphs based on GRH with an application to elliptic curve cryptography. *Journal of Number Theory*, 129(6):1491–1504, 2009.

[20] David Jao and Vladimir Soukharev. A subexponential algorithm for evaluating large degree isogenies. In *Algorithmic Number Theory*, pages 219–233. Springer, 2010.

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

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

[23] Greg Kuperberg. A subexponential-time quantum algorithm for the dihedral hidden subgroup problem. *SIAM Journal on Computing*, 35(1):170–188, 2005.

[24] Jeffrey C Lagarias and Andrew M Odlyzko. Effective versions of the Chebotarev density theorem. *Algebraic number fields*, pages 409–464, 1977.

[25] Oded Regev. A subexponential time algorithm for the dihedral hidden subgroup problem with polynomial space. *arXiv preprint quant-ph/0406151*, 2004.

[26] Susanne Schmitt and Horst G Zimmer. *Elliptic Curves: A computational approach*, volume 31. Walter de Gruyter, 2003.

[27] René Schoof. Counting points on elliptic curves over finite fields. *Journal de Théorie des Nombres de Bordeaux*, 7(1):219–254, 1995.

[28] Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997.

[29] Daniel Shumow. Isogenies of elliptic curves: a computational approach. *arXiv preprint arXiv:0910.5370*, 2009.

[30] Joseph H Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151. Springer Science & Business Media, 1994.

[31] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer, 2009.

[32] Anton Stolbunov. *Cryptographic schemes based on isogenies*. PhD thesis, Norwegian University of Science and Technology (NTNU), 2012.

[33] Andrew Sutherland. smoothrelation program.

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

[35] Andrew Sutherland. Lecture notes for elliptic curves 18.783, 2015.

[36] John Tate. Endomorphisms of abelian varieties over finite fields. *Inventiones Mathematicae*, 2(2):134–144, 1966.

[37] Jacques Vélu. Isogénies entre courbes elliptiques. *CR Acad. Sci. Paris Sér. AB*, 273:A238–A241, 1971.

[38] Lawrence C Washington. *Elliptic curves: number theory and cryptography.* CRC press, 2008.