UNIVERSITÀ
DI TRENTO
Department of Mathematics
Laboratory of Industrial Mathematics and Cryptography

Doctoral programme — XXXVI cycle

Graphs and pairings of elliptic curves

Marzio Mula

PhD thesis in Mathematics

Supervised by Nadir Murru
and Federico Pintore

Board:

Wouter Castryck, Dr	COSIC, KU Leuven, Belgium
Luca De Feo, Dr	IBM Research, Switzerland
Roberto La Scala, Prof	Università di Bari, Italy

Abstract

Most isogeny-based cryptosystems ultimately rely, for their security, on ℓ-IsoPath, i.e. the problem of finding a secret ℓ-smooth isogeny between two elliptic curves. As cryptographic applications usually employ weaker variants of ℓ-IsoPath for practical reasons, it is natural to ask whether these variants are equally hard from a computational perspective. For example, what happens if the endomorphism ring of one of the curves is known? Does the existence of suitable pairings affect the hardness of ℓ-IsoPath? What happens if some non-trivial endomorphisms of the domain and codomain curves are known? These kinds of questions lead to different problems, some of which are considered throughout this thesis.

To prevent anyone from knowing the endomorphism ring of a supersingular elliptic curve, we would need a method to hash in the supersingular isogeny graph, i.e. the graph whose vertices are supersingular elliptic curves (up to isomorphism) and whose edges are isogenies of fixed degree. We give examples of cryptographic protocols that could benefit from this and survey some known methods. Since none of them is at the same time efficient and cryptographically secure, we also point out a few alternative approaches.

Later on, we leverage the classic Deuring correspondence between supersingular elliptic curves and quaternion orders to study a weaker version of ℓ-IsoPath, inspired by the study of CM theory from the previous part.

We then focus on the construction of pairings of elliptic curves, showing that, in the general case, finding distinct pairings compatible with a secret isogeny is no easier than retrieving the isogeny itself. In the presence of an orientation, on the other hand, we show that the existence of suitable self-pairings, together with a recent attack on the isogeny-based key-exchange SIDH, does lead to efficiently solving ℓ-IsoPath for some class-group-action-based protocols. In particular, we completely characterize the cases in which these self-pairings exist.

Finally, we introduce a different graph of elliptic curves, which has not been considered before in isogeny-based cryptography and which does not arise, in fact, from isogenies: the *Hessian graph*. We give a (still partial) account of its remarkable regularity and discuss potential cryptographic applications.

Je cessai de me demander ce qu'il fallait faire pour pouvoir faire quelque chose.

À la recherche du temps perdu, Marcel Proust.

Aknowledgements

Ἡ Ἰθάκη σ' ἔδωσε τ' ὡραῖο ταξεῖδι.
Χωρίς αὐτήν δέν θά βγαινες στόν δρόμο.
Ἄλλα δέν ἔχει νά σέ δώσει πιά.

Ἰθάκη, Costantinos Kavafis.

I was not born a traveller. It was only in recent times that I felt the curiosity – and later the desire, if not the urge – to start a journey whose destination seems to be still beyond the horizon. Here I wish to thank at least some of the people who made my travel more meaningful and pleasing.

I express my deepest gratitude to Federico Pintore, who introduced me to isogeny-based cryptography and patiently advised me through my first, uncertain steps into the world of research. I am also very grateful to Lea Terracini, whose enlightening explanations and strive for knowledge allowed me to delve deeper into more and more fascinating aspects of number theory.

Every traveller eventually meets some pirates along the way, and I was lucky enough to encounter Luca De Feo, whose witty advice and amusing company not only broadened my understanding of mathematics, but also gave me enough motivation to face – and survive – three months in Zurich.

I would also like to sincerely thank Wouter Castryck for his welcoming attitude and for the naturalness and modesty with which he brought out amazing mathematical results and ideas that are still fuelling my current research. I am also indebted to Marc Houben and Sam van Buuren for illuminating discussions and good time spent in Leuven.

The price of travelling is that we leave some people behind. I am thankful to those who were not let down by geographical distance: Luca Pezzini, a brother, who keeps supporting me with his wisdom, enduring my rants, and – on occasions – exchanging painfully long mathematical explanations. Filippo Ascolani, Francesca Tozzi, Irene Pezzini, Luca Virano, Tommaso Natta, Umberto Visani and the other friends and family members who make Turin more a home than any other place.

I also thank the people who welcomed me to Trento: Anna Sanfilippo, Chiara Spadafora, Giulia Jannon, Michele Battagliola, and all the people from CryptoLabTN. Andrea Flamini, a welcoming lighthouse in the dark nights of Trento. Giovanni Tognolini, a gold mine of good time, nice chats and adventures, who taught me what travels are really about – and some maths as well. And his friends from the Bronx of Brescia.

Finally, I wish to thank my parents, for their love and for the education they gave me – whose importance I too often underestimate – and my sister, who is the person I miss the most when I am not home.

Contents

Introduction

> *Dicebat Bernardus Carnotensis nos esse quasi nanos gigantium humeris insidentes, ut possimus plura eis et remotiora videre, non utique proprii visus acumine, aut eminentia corporis, sed quia in altum subvehimur et extollimur magnitudine gigantea.*
>
> *Metalogicon*, John of Salisbury.

In the timeline of the study of elliptic curves – which began in the third century AD with the works of Diophantus and continued, in more recent times, with those of Fermat, Jacobi, Weierstrass, Poincaré, Deuring, Mordell, and many others – isogeny-based cryptography occupies no more than a negligible ending segment. Its story begins in the 1990s, when Couveignes [Cou06] and then Rostovstev and Stolbunov [RS06] observed that elliptic curves and the maps between them – called *isogenies* – could be used to construct a Diffie-Hellman-like key-exchange protocol called *CRS*.

There would be no practical reason to prefer CRS to the classical DLog-based Diffie-Hellman, if Shor had not proven, in [Sho97], that the latter could be broken by quantum computers. Shortly after, however, the CRS scheme turned out to be prone to a subexponential quantum attack devised by Childs, Jao, and Soukharev [CJS14], and to be too inefficient to cope with it.

Nevertheless, the shadow of the quantum threat motivated researchers to keep looking for isogeny-based cryptosystems, under the fundamental assumption that finding a secret isogeny between two elliptic curves is computationally hard – even for a quantum computer. This gave birth to two main branches of isogeny-based cryptography, which sprouted from two essentially different key-exchange protocols: the older one, born in 2011, is *SIDH* [DFJP14], which exploited the highly connected and 'unpredictable' structure of the isogeny graph of supersingular elliptic curves. The younger one, born in 2018, is CSIDH [Cas+18a], which is conceptually closer to the original CRS and attempts to overcome its efficiency issues by exploiting, once again, supersingular elliptic curves.

As we said, isogeny-based cryptography sits on top of a mountain of theorems and theoretical results on elliptic curves – and, more generally, abelian varieties. This mountain turned out to be more crumbly than expected, in July 2022, when three attacks [CD23; Mai+23; Rob23], based on results dating back to the 1980s, led to the fall of SIDH. While we write this thesis, rocks are still rolling, and more and more

researchers – including ourselves – feel motivated to dig in the mountain and see how strong the schemes that survived the SIDH attack really are.

This thesis gathers some problems and results, related to isogeny-based cryptography, which represent part of the author's work as a PhD student in Trento. About two-thirds of the materials collected here have already appeared in preprints [MMP22] and publications [Cas+23; MMP]: only minor revisions were made to fit them in a more coherent and up-to-date dissertation. Other sections are instead unpublished, as they have not (yet) reached the maturity necessary to be considered articles in their own right. The following table summarizes the main sources for each part of this thesis.

[MMP22]	I.1-I.6, II.1-II.2
[Cas+23]	I.7-I.8, III.2.2.
[MMP]	Minor insertions
Unpublished	I.9, II.3, III.1, III.2.1, Chap. IV

We detail below the content of each chapter:

- Chapter I serves as a mathematical introduction and gathers some classic results about elliptic curves over perfect fields of characteristic different from $2, 3$.
- Chapter II is devoted to the *full supersingular isogeny graph*, which is the graph used in SIDH. The first problem considered is that of hashing in this graph. We survey various ways to do that, with emphasis on the methods based on the theory of CM curves over $\mathbb{C}$. Finally, we show that the only efficient methods do not result in cryptographically secure hash functions and we propose some possible alternative approaches. The second part of the chapter compares the hardness of the main problem on which most isogeny-based protocols rely – i.e. the problem of finding a secret isogeny of power-smooth degree between two given supersingular elliptic curves (ℓ-IsoPath) – and a decisional problem, which we call IsMSmaller, somehow inspired by the CM methods from the first part of the chapter. In Proposition II.3.2 we use the well-known correspondence between supersingular elliptic curves and quaternion algebras to provide some evidence that, as might be expected, solving the second problem is not enough to solve the first.
- Chapter III is mostly devoted to the existence and construction of 'compatible' pairings on isogenous curves. In Proposition III.2.3, we show that, in the general case, computing 'intrinsically distinct' couples of compatible pairings on two isogenous curves is as hard as solving ℓ-IsoPath. While computing these pairings seems unfeasible in the general case, the situation is radically different if additional information is available. In particular, in the oriented case, compatible self-pairings between oriented curves can be combined with the SIDH attack to break some weak instances of CRS. Propositions III.2.6 and III.2.8 characterize the cases in which such self-pairings exist.
- Chapter IV, which is part of a collaborative work in progress, borrows from classic algebraic geometry the definition of *Hessian* of an elliptic curve and uses it to

define a new type of graphs of elliptic curves, which we call *Hessian graphs*. We state partial results on their structure and suggest some possible cryptographic applications.

Given the heterogeneous composition of this work, it is unsurprising that its chapters – except for Chapter I – can be read in any desired order. Nevertheless, we suggest a chronological order, which, in our opinion, also allows for a pleasing climax from the survey-level results of Chapter II to the more advanced constructions of Chapter III and the bizarre wonders of Chapter IV.

Chapter I

Preliminaries

This chapter gathers some classic results which will be used throughout the remainder of this thesis.

Sections I.1, I.2 and I.3 introduce the core objects of our study, namely elliptic curves and the maps (*isogenies*) between them. Section I.4 gives a brief account of the surprising connection between elliptic curves over $\mathbb{C}$ and those over finite fields, while Sections I.5 and I.6 list various characterizations of supersingular elliptic curves and analyse the peculiar structure of the graphs that arise when their isogenies are considered. These results will be used mainly in Chapter II. In view of Chapter III, in Section I.7 we define orientations for both ordinary and supersingular elliptic curves, following mostly [CK20; Onu21]. In Section I.8 we see how every imaginary quadratic order $\mathcal{O}$ gives rise to a class group action on the set of elliptic curves oriented by $\mathcal{O}$. Finally, in Section I.9, we recall some basic notions about pairings.

I.1 Elliptic curves

Throughout this thesis, we will always use $\Bbbk$ to denote a perfect field with $\operatorname{char}\Bbbk \notin \{2, 3\}$. An *elliptic curve* over $\Bbbk$ is a projective curve that can be written, up to birational equivalence, as an irreducible cubic in $\mathbb{P}^2(\Bbbk)$ in *(short) Weierstrass form*

$$Y^2Z = X^3 + AXZ^2 + BZ^3 \qquad \text{with } A, B \in \Bbbk$$

and such that the *discriminant*, $\Delta(E) = -16(4A^3 + 27B^2)$, is not 0. We will almost always work in the affine chart $X \neq 0$, where the Weierstrass form becomes

$$y^2 = x^3 + Ax + B \qquad \text{with } A, B \in \Bbbk \tag{1}$$

and the only non-affine point, corresponding to $O = [0 : 1 : 0]$, is called the *point at infinity*. The $\Bbbk$-*rational points* of E, denoted by $E(\Bbbk)$, are the solutions in $\Bbbk$ of (1) together with O.
Every elliptic curve E can be endowed with the structure of an abelian group $(E, +)$ whose zero element is O [Sil09, § III.2].

Since elliptic curves are defined up to birational equivalence, there exist various representations other than the Weierstrass model considered above. In Table I.1, we summarize the form of the affine equation and the corresponding definition of the j-invariant (whose definition is recalled in the following Section I.2) for some of these alternative models. We also provide the values of the coefficients A and B of a birationally-equivalent elliptic curve in Weierstrass form.

Table I.1: Other models of elliptic curves

Model	**Affine equation**	**j-invariant**	**Weierstrass form**
Legendre [Sil09, p. 49]	$y^2 = x(x-1)(x-\lambda)$	$2^8\dfrac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}$	$\begin{cases} A = \dfrac{-\lambda^2+\lambda-1}{3} \\ B = \dfrac{-2\lambda^3+3\lambda^2+3\lambda-2}{27} \end{cases}$
Montgomery [CS17, § 2.4]	$B'y^2 = x^3 + A'x^2 + x$	$\dfrac{256(A'^2-3)^3}{A'^2-4}$	$\begin{cases} A = B'^2\left(1-\dfrac{A'^2}{3}\right) \\ B = \dfrac{B'^3A'}{3}\left(\dfrac{2A'^2}{9}-1\right) \end{cases}$
Jacobi [BJ03, § 3]	$y^2 = \epsilon x^4 - 2\delta x^2 + 1$	$64\dfrac{(\delta^2+3\epsilon)^3}{\epsilon(\delta^2-\epsilon)^2}$	$\begin{cases} A = -4\epsilon - \dfrac{4}{3}\delta^2 \\ B = -\dfrac{16}{27}\delta(\delta^2-9\epsilon) \end{cases}$

The singular case The only case in which (1) does not yield an elliptic curve is the singular case, which occurs when $\Delta(E) = 0$. There are then two possibilities, up to birational equivalence: the *cuspidal curve*, of equation $y^2 = x^3$, and the *nodal curve*, of equation $y^2 = x^3 + x^2$.

I.2 Isogenies and isomorphisms

An *isogeny* between two elliptic curves E_1, E_2 over $\Bbbk$ is a morphism

$$\varphi\colon E_1 \to E_2$$

such that $\varphi(O) = O$. We say that φ is a $\Bbbk$-*isogeny*, or that φ is *defined over* $\Bbbk$, if the rational functions defining φ can be chosen with coefficients in $\Bbbk$. We refer to [Sil09, § III.4] for the definition of *degree* – denoted by $\deg(\varphi)$. For our purposes, it is enough to keep in mind the following facts.

Proposition I.2.1. *Let $\varphi\colon E_1 \to E_2$ be an isogeny.*

(i) $\deg(\varphi)$ *is a multiple of* $\#\ker(\varphi)$*, and equality holds if and only if φ is separable.*

(ii) For each finite subgroup G of an elliptic curve E_1 there exists a unique[1] *isogeny with domain E_1 and kernel G.*

Two elliptic curves are called *isogenous* if there exists an isogeny between them. The following celebrated theorem characterizes isogenous curves.

Theorem I.2.2 (Tate)**.** *Let E and E' be two elliptic curves defined over $\Bbbk$. Then E and E' are isogenous if and only if $\#E(\Bbbk) = \#E'(\Bbbk)$.*

An isogeny of degree 1 is an *isomorphism*. Every isomorphism class of elliptic curves over $\overline{\Bbbk}$ can be uniquely identified by an element $j \in \Bbbk$, called the *j-invariant*. The value of j can be easily retrieved from the coefficients of any elliptic curve $E\colon y^2 = x^3+Ax+B$ in the isomorphism class as

$$j(E) = -1728\frac{(4A)^3}{\Delta(E)}.$$

We recall from [Sil09, Prop. III.1.4.b-c] the fundamental properties of j-invariants.

Proposition I.2.3.

(i) Two elliptic curves over $\Bbbk$ are isomorphic if and only if they have the same j-invariant.

(ii) Let $j_0 \in \overline{\Bbbk}$. There exists an elliptic curve over $\Bbbk(j_0)$ whose j-invariant is j_0.

Given an elliptic curve E, for each positive integer m, let $[m]$ denote the 'multiplication-by-m' map which is an isogeny from E to itself such that:

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

The above definition easily extends to negative integers, setting $[-m]P = -([m]P)$. For each $m \in \mathbb{Z}$, the *m-torsion* of E is the subgroup $E[m] = \ker([m])$.

Finally, for each isogeny $\varphi\colon E_1 \to E_2$ of degree m there exists a unique isogeny $\hat{\varphi}\colon E_2 \to E_1$, called the *dual isogeny* of φ, such that $\varphi \circ \hat{\varphi} = \hat{\varphi} \circ \varphi = [m]$.

I.3 Endomorphism rings

Let $\mathrm{End}(E)$ be the set of *endomorphisms* of an elliptic curve E, i.e. the isogenies $E \to E$. In this section, we summarize some fundamental facts about the structure of $\mathrm{End}(E)$.

[1] Up to post-composition with an isomorphism [Sil09, Prop. III.4.12].

Since $\mathrm{End}(E)$ is a torsion-free ring, the map

$$\begin{aligned}[\ ]\colon \mathbb{Z} &\to \mathrm{End}(E)\\ m &\mapsto [m]\end{aligned}$$

is injective. Endomorphisms in the image of the injective map $[\ ]$ are called *trivial* or *scalar*. However, $\mathrm{End}(E)$ may have a richer structure rather than being a simple copy of $\mathbb{Z}$, as we will shortly see.

Characteristic polynomial of an endomorphism A first insight into the structure of $\mathrm{End}(E)$ comes from the observation that every endomorphism satisfies an equation of degree 2.

Lemma I.3.1. *Let φ be an endomorphism of an elliptic curve E over $\Bbbk$, and define*

$$d = \deg(\varphi) \qquad \textit{and} \qquad a = 1 + \deg(\varphi) - \deg(1-\varphi).$$

Then

$$\varphi^2 - [a] \circ \varphi + [d] = [0]. \tag{2}$$

Proof. This can be checked directly using the properties of dual isogenies. □

The integer a from Corollary I.3.1 is called the *trace* of φ and denoted by $\mathrm{tr}(\varphi)$. In particular, when E is over a finite field $\mathbb{F}_q$ of characteristic p, the endomorphism

$$\begin{aligned}\varphi_q\colon E &\to E\\ (x,y) &\mapsto (x^q, y^q)\end{aligned}$$

is called the *q-th power Frobenius endomorphism* of E, and its trace is the *trace of E* over $\mathbb{F}_q$. Moreover, its degree equals q [Sil09, Prop. II.2.11], so that the following yields

$$\left(x^{q^2}, y^{q^2}\right) - [\mathrm{tr}(\varphi_q)](x^q, y^q) + [q](x,y) = O$$

for each $(x,y) \in E(\overline{\mathbb{F}_q})$.

Structure of $\mathrm{End}(E)$ Recall that an algebra B over $\mathbb{Q}$ is a *quaternion algebra* if there exist $i, j \in B$ such that $1, i, j, ij$ form a basis for B as a $\mathbb{Q}$-vector space and

$$i^2 = a, \qquad j^2 = b, \qquad ji = -ij \tag{3}$$

for some $a, b \in \mathbb{Q}^\times$. Moreover, an *order* $\mathcal{O}$ in a quaternion algebra (resp. in a quadratic number field) is a $\mathbb{Z}$-module of rank 4 (resp. 2) which is also a subring.

Remark I.3.2. Let K be a quadratic extension of $\mathbb{Q}$ and denote by $\mathcal{O}_K$ is its ring of integers. Then the orders in K are exactly the rings $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$, where f is a positive integer called the *conductor* of $\mathcal{O}$ [Cox13, Lemma 7.2].

Theorem I.3.3 (Structure of End(E))**.** *Let E be an elliptic curve over $\Bbbk$. Then* End(E) *is either $\mathbb{Z}$, an order in an imaginary quadratic number field, or a maximal order in the quaternion algebra ramified at p and ∞, which we denote by $B_{p,\infty}$.*

Proof. The fact that End(E) is either $\mathbb{Z}$, an imaginary quadratic order or an order in a quaternion algebra follows from Lemma I.3.1 and [Voi21, Thm. 3.1.1]. The remainder of the statement is proven in [Voi21, Thm. 42.1.9].

□

It is natural to ask how frequently these three structures for End(E) can occur. The answer differs depending on the characteristic of $\Bbbk$:

- If $\Bbbk$ has characteristic 0, then 'most' elliptic curves have only trivial endomorphisms. Some elliptic curves, on the other hand, have their endomorphism rings isomorphic to some imaginary quadratic order $\mathcal{O}$. We say that they have *complex multiplication (CM) by $\mathcal{O}$.*
- If $\Bbbk$ has characteristic $p > 0$, then there are about $p/12$ isomorphism classes of elliptic curves whose endomorphism rings are maximal orders in $B_{p,\infty}$. We call these curves *supersingular*. The others are called *ordinary*.

I.4 CM reduction

Isogenies are not the only examples of group homomorphisms between elliptic curves. A relevant family of group homomorphisms between (non-isogenous) elliptic curves are the *reductions modulo primes*, which Deuring proved to be the connecting bridge between elliptic curves over $\overline{\mathbb{Q}}$ and those defined over finite fields.

Let E be an elliptic curve defined over a number field L, and $\mathfrak{P}$ a prime of L. We say that E *has a good reduction* modulo $\mathfrak{P}$ if the $\mathfrak{P}$-adic valuation of $\Delta(E)$ does not equal 0 (see [Sil09, § VII.5] for more details). In particular, this means that the coefficients of E can be regarded as elements of some finite extension of $\mathbb{F}_p$, and they define an elliptic curve $\tilde{E}$ called the *reduction* of E modulo $\mathfrak{P}$. Similarly, every point P of E can be sent to its reduction modulo $\mathfrak{P}$, giving rise to a map

$$\begin{aligned} E &\to \tilde{E} \\ P &\mapsto P \bmod \mathfrak{P}, \end{aligned}$$

called the *reduction map* of E modulo $\mathfrak{P}$, which is a group homomorphism.

Example 1. Let E be the elliptic curve over $\mathbb{Q}$ of equation

$$y^2 = x^3 - \frac{187}{25}x + \frac{991}{125}.$$

Since $\Delta(E) = -2^4 \cdot 23$, E does have good reduction modulo 5. However, the coefficients of E are not readily suitable for being seen as elements of $\mathbb{F}_5$. One needs to consider the isomorphic curve

$$y^2 = x^3 - 187x + 991.$$

whose reduction yields

$$\tilde{E}\colon y^2 = x^3 + 3x + 1.$$

Notice that the reduction map modulo 5 sends the point $(0 : \alpha : 1)$ of E, where $\alpha^2 = 991/125$, into the point at infinity $(0 : 1 : 0)$ of $\tilde{E}$.

Remark I.4.1. In the light of Proposition I.2.1.(ii), the notion of reduction modulo $\mathfrak{P}$ also extends to isogenies: if φ is an isogeny with domain E and kernel coprime with p, then its reduction $\tilde{\varphi}$ is the isogeny with domain $\tilde{E}$ and kernel $\widetilde{\ker}(\varphi)$. If the kernel of φ is generated by a p-torsion point, on the other hand, then its reduction is either the zero map or the Frobenius map over $\mathbb{F}_p$.

Every elliptic curve over $\mathbb{F}_q$ arises as the reduction of some CM curve over $\overline{\mathbb{Q}}$.

Theorem I.4.2 (Deuring)**.** *Let $\mathscr{E}$ be an elliptic curve over a field of characteristic p with a non-trivial endomorphism α_0. Then there exists an elliptic curve E defined over a number field L, an endomorphism α of E and a good reduction $\tilde{E}$ of E at a prime $\mathfrak{P}$ of L over p, such that $\mathscr{E}$ is isomorphic to $\tilde{E}$ and α_0 corresponds to $\tilde{\alpha}$ (the reduction of α at $\mathfrak{P}$) under the isomorphism.*

Proof. See [Deu41; Lan87, Thm. 13.14]. □

From a computational perspective, Deuring's result suggests that, to find an elliptic curve over $\mathbb{F}_q$ with a non-trivial endomorphism of prescribed degree, one might look for a CM curve over $\overline{\mathbb{Q}}$ and check whether it has good reduction modulo p (or some ideal $\mathfrak{P}$ over p).

For a better insight of this approach, which will come in handy in Chapter II, we will now delve deeper into the connection between elliptic curves and lattices over $\mathbb{C}$.

From complex lattices to complex elliptic curves Let x_1 and x_2 be two $\mathbb{R}$-linearly independent vectors in the complex plane $\mathbb{C}$ (viewed as a 2-dimensional $\mathbb{R}$-vector space). The *complex lattice generated by x_1 and x_2* is the set

$$\Lambda = \{z_1 x_1 + z_2 x_2 \mid z_1, z_2 \in \mathbb{Z}\}.$$

Two lattices Λ_1, Λ_2 are *homothetic* if there exists $\beta \in \mathbb{C} \setminus \{0\}$ such that $\Lambda_2 = \beta\Lambda_1$.

We will now recall how an elliptic curve E over $\mathbb{C}$ can be constructed from a complex lattice Λ, and also how $\mathrm{End}(E)$ can be retrieved from Λ. For this part we follow [Cox13, § 10; Sil09, § C.11; Was08, § 9.1-9.3, 10.1] (see also [Gal18, § 16.1] for a general overview on lattices in $\mathbb{R}^n$).

Let Λ be a complex lattice generated by $x_1, x_2 \in \mathbb{C}$. The quotient $\mathbb{C}/\Lambda$ is a *complex torus*. For each integer $k \geq 3$, the *Eisenstein series*

$$G_k(\Lambda) = \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \omega^{-k}$$

converges [Was08, Lem. 9.4]. In order to ease the notation, $60G_4(\Lambda)$ and $140G_6(\Lambda)$ are usually denoted by $g_2(\Lambda)$ and $g_3(\Lambda)$, respectively.

Finally, the *j-invariant* of a complex lattice Λ is defined as

$$j(\Lambda) = 1728 \frac{g_2(\Lambda)^3}{g_2(\Lambda)^3 - 27 g_3(\Lambda)^2}. \tag{4}$$

Theorem I.4.3. *Two complex lattices are homothetic if and only if they have the same j-invariant.*

Proof. See [Cox13, Thm. 10.9] □

As the use of the word 'j-invariant' suggests, complex lattices and elliptic curves (over $\mathbb{C}$) are closely related.

Theorem I.4.4. *Let Λ be a complex lattice, and define the elliptic curve*

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

Then the groups $\mathbb{C}/\Lambda$ and $E(\mathbb{C})$ are isomorphic. Moreover, the map

$$\begin{array}{ccc} \{\text{Homothety classes of complex lattices}\} & \to & \{\text{Isomorphism classes of elliptic curves over } \mathbb{C}\} \\ \Lambda & \mapsto & E_\Lambda \end{array}$$

is well defined, one-to-one and $j(\Lambda) = j(E_\Lambda)$.

Proof. See [Was08, § 9.2 and 9.3]. □

The following proposition clarifies the connection between a complex lattice Λ and the endomorphism ring of E_Λ.

Proposition I.4.5. *Let Λ be a complex lattice, and E_Λ the corresponding elliptic curve as in Theorem I.4.4. Then*

$$\mathrm{End}(E_\Lambda) \cong \{\beta \in \mathbb{C} \mid \beta\Lambda \subseteq \Lambda\}. \tag{5}$$

Proof. See [Was08, Thm 10.1]. □

Therefore, for a complex lattice Λ such that $\mathbb{Z} \subsetneq \{\beta \in \mathbb{C} \mid \beta\Lambda \subseteq \Lambda\}$, the corresponding elliptic curve E_Λ has complex multiplication. In fact, every such Λ is homothetic to a fractional ideal in some imaginary quadratic field, as we are going to prove in Corollary I.4.10.

Proposition I.4.6. *Let $\mathcal{O}$ be an order in an imaginary quadratic field k. Then every non-zero fractional ideal of $\mathcal{O}$ is a complex lattice.*

Proof. See [Cox13, § 10.C]. □

Remark I.4.7. On the other hand, a complex sublattice of an imaginary order $\mathcal{O}$ is not, in general, a fractional ideal, nor even a subring, of $\mathcal{O}$. For example, consider $k = \mathbb{Q}(i)$ and the sublattice Λ generated by 2 and $i = \sqrt{-1}$ in the ring of integers of k. The square of the second generator is -1, which does not lie in Λ. Therefore, Λ is not closed under multiplication.

Let S be the right-hand side of (5), i.e.

$$S = \{\beta \in \mathbb{C} \mid \beta\Lambda \subseteq \Lambda\},$$

and assume that Λ is a fractional ideal of an order $\mathcal{O}$ in a quadratic imaginary field. The inclusion $\mathcal{O} \subset S$ holds trivially. The other inclusion needs not to be true, though (see[Cox13, § 7.A]. When it does (i.e. Λ is *not* a fractional ideal of any order greater than $\mathcal{O}$), Λ is called a *proper* ideal.

Proposition I.4.8. *Let $\mathcal{O}$ be an order in an imaginary quadratic field k, and Λ a proper non-zero fractional ideal in $\mathcal{O}$. Then* $\mathrm{End}(E_\Lambda) \cong \mathcal{O}$.

Proof. It follows immediately from the definition of proper ideal and Proposition I.4.5. □

The above result provides a class of complex elliptic curves whose endomorphism ring is exactly $\mathcal{O}$, that is those of the form E_Λ, where Λ is a proper fractional ideal of $\mathcal{O}$. Actually, up to isomorphism, there are no other complex elliptic curves with endomorphism ring $\mathcal{O}$.

Theorem I.4.9. *Let Λ be a complex lattice, and $\alpha \in \mathbb{C} \setminus \mathbb{Z}$. Then, the inclusion $\alpha\Lambda \subset \Lambda$ holds if and only if there exists an order $\mathcal{O}$ in an imaginary quadratic field k such that $\alpha \in \mathcal{O}$ and Λ is homothetic to a proper fractional ideal of $\mathcal{O}$.*

Proof. See [Cox13, Thm. 10.14]. □

Corollary I.4.10. *Let $\mathcal{O}$ be an imaginary quadratic order and E a complex elliptic curve with* $\mathrm{End}(E) \cong \mathcal{O}$. *Then there exists a proper fractional ideal of $\mathcal{O}$, say Λ, such that $E \cong E_\Lambda$.*

Proof. Theorem I.4.4 ensures that $E \cong E_{\Lambda'}$ for some complex lattice Λ'. Since we are assuming that E is a CM curve, by (5) there exists $\alpha \in \mathbb{C} \setminus \mathbb{Z}$ such that $\alpha\Lambda' \subseteq \Lambda'$. From Theorem I.4.9 we know that there exists an imaginary quadratic order $\mathcal{O}'$ containing α and Λ' is homothetic to a proper fractional ideal of $\mathcal{O}'$, which we denote by Λ. By Proposition I.4.8, $\mathrm{End}(E_\Lambda) = \mathcal{O}'$. Moreover, since Λ and Λ' are homothetic, the curves E_Λ and $E_{\Lambda'}$ are isomorphic. Hence, their endomorphism rings are isomorphic too, i.e. $\mathcal{O} = \mathcal{O}'$. □

Corollary I.4.11. *Let $\mathcal{O}$ be an order in an imaginary quadratic field. Then the map $f\colon \Lambda \mapsto j(E_\Lambda)$ yields a one-to-one correspondence between the ideal class group $\mathrm{Cl}(\mathcal{O})$ and the j-invariants of CM curves with endomorphism ring $\mathcal{O}$.*

Proof. It is easy to prove that two proper fractional ideals of $\mathcal{O}$ determine the same class if and only if they are homothetic as complex lattices. Therefore, f is well-defined on equivalence classes of ideals, and by Theorem I.4.3 it is also injective. Proposition I.4.8 ensures that $f(\Lambda)$ is a CM j-invariant and that the image is a set of j-invariants of CM curves with endomorphism ring $\mathcal{O}$. Finally, surjectivity follows from Corollary I.4.10. □

Hilbert class polynomials Corollary I.4.11 alone does not provide an explicit strategy to compute CM j-invariants. In fact, even though a suitable complex lattice Λ can be easily determined, the infinite sums $g_2(\Lambda)$ and $g_3(\Lambda)$ involved in (4) make any direct computation quite impractical. Furthermore, *a priori* it is not ensured that the CM j-invariants considered in Corollary I.4.11 are algebraic over $\mathbb{Q}$ (f they were not, we would not be able to perform modular reductions of their coefficients). The latter problem is addressed in the following proposition.

Proposition I.4.12. *Let $\mathcal{O}$ be an order in an imaginary quadratic field k, and denote by $\Lambda_1, \Lambda_2, \ldots, \Lambda_h$ a complete set of representatives for the ideal class group $\mathrm{Cl}(\mathcal{O})$. Then the polynomial*

$$P_{\mathcal{O}} = \prod_{i=1}^{h} \big(X - j(E_{\Lambda_i})\big) \tag{6}$$

has integer coefficients. In particular, the CM j-invariants $j(E_{\Lambda_1}), \ldots, j(E_{\Lambda_h})$ are algebraic over $\mathbb{Q}$.

Proof. See [Cox13, Thm. 13.2]. □

The polynomial $P_{\mathcal{O}}$ defined in (6) is called the *Hilbert class polynomial* (or *ring class polynomial*, whenever $\mathcal{O}$ is not maximal) of the imaginary quadratic order $\mathcal{O}$.

There exist several algorithms to compute the Hilbert class polynomial of a given imaginary quadratic order $\mathcal{O}$ in time $\tilde{O}(\mathrm{disc}\,\mathcal{O})$. For the sake of completeness, we sketch below the classical approach from [Coh93, § 7.6.2]:

1) compute a set of representatives $\Lambda_1, \Lambda_2, \ldots, \Lambda_h$ for $\mathrm{Cl}(\mathcal{O})$. Equivalently, following [Coh93, § 5.3.1], enumerate all the positive-definite reduced integral binary quadratic forms $aX^2 + bXY + cY^2$ of discriminant $D = \mathrm{disc}(\mathcal{O})$, i.e. the triples of integers (a, b, c) such that
   - $|b| \leq a \leq c$,
   - if $|b| = a$ or $a = c$, then $b \geq 0$,
   - $b^2 - 4ac = D$.

2) Let (a, b, c) be one of the triples from the previous step. Then the corresponding representative is $\Lambda = \mathbb{Z} + \tau\mathbb{Z}$ with $\tau = \frac{-b+\sqrt{D}}{2a}$, and $j(\Lambda)$ can be approximated via the expansion
$$j(\tau) = 1728 \frac{\left(1 + 240 \sum_{k=1}^{\infty} \frac{k^3 q^k}{1-q^k}\right)^3}{\left(1 + 240 \sum_{k=1}^{\infty} \frac{k^3 q^k}{1-q^k}\right)^3 - \left(1 - 504 \sum_{k=1}^{\infty} \frac{k^5 q^k}{1-q^k}\right)^2}, \tag{7}$$
where $q = e^{2\pi i \tau}$ [Was08, Prop. 9.12].

3) If the approximations $\tilde{j}_1, \ldots, \tilde{j}_h$ from the previous step are 'good enough', thanks to Proposition I.4.12 the exact Hilbert class polynomial of $\mathcal{O}$ can be found by rounding the coefficients of $\prod_{i=1}^{h}(X - \tilde{j}_i)$ to the nearest integers. More precisely, the closeness of $\tilde{j}_i$ to $j(\Lambda_i)$ depends on both the partial sums from (7) considered for the approximation and the precision used for numerical computations. While the impact of the first choice is limited by the rapid convergence of (7), the second one requires a deeper analysis of the coefficients of $P_{\mathcal{O}}$ [Eng06, § 4].

I.5 Supersingular elliptic curves

We will now recall some characterizations of supersingular elliptic curves. Such criteria for supersingularity will be exploited in Section II.2 to generate supersingular curves. In the following, we will use p for a prime number larger than 3 and q for a generic power p^n with $n \in \mathbb{N}$.

Theorem I.5.1 (Definitions of supersingular elliptic curve)**.** *Let $E\colon y^2 = x^3 + Ax + B$ be an elliptic curve over $\mathbb{F}_q$. For each $r \geq 1$ let*
$$\varphi_r\colon E \to E^{(p^r)}$$
be the p^r-th power Frobenius map, where $E^{(p^r)}$ is the elliptic curve of equation $y^2 = x^3 + A^{p^r}x + B^{p^r}$. Then the following are equivalent:

(a1) $E[p^r] = \{O\}$ *for some* $r \geq 1$.

(a2) $E[p^r] = \{O\}$ *for each* $r \geq 1$.

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

[2] We refer to [Sil09, p. 21] for a precise definition of purely inseparable isogenies.

(iii) $\mathrm{End}(E)$ *is an order in a quaternion algebra over* $\mathbb{Q}$.

(iv) $\#E(\mathbb{F}_q) \equiv 1 \mod p$.

If an elliptic curve satisfies one of the above conditions, it is called supersingular. *In particular, the set of* supersingular j-invariants, *i.e.*

$$\{\, j(E) \mid E \text{ is supersingular over } \Bbbk \,\},$$

lies in $\mathbb{F}_{p^2}$.

Proof. See [Sil09, Thm. V.3.1; Was08, Prop. 4.31]. □

Non-supersingular elliptic curves are called *ordinary*.

Corollary I.5.2. *Every supersingular elliptic curve over a field of characteristic p is isomorphic to a supersingular elliptic curve over $\mathbb{F}_{p^2}$.*

Proof. This is an immediate consequence of part (b) of the previous theorem and the properties of j-invariants in Proposition I.2.3. □

I.6 Supersingular isogeny graphs

Supersingular isogeny graphs are a major object of study in isogeny-based cryptography. Their peculiar structure allows 'walking' from a vertex – the isomorphism class of a supersingular elliptic curve – to another in such a way that

- each step can be performed quickly (via Vélu's formulae, see [Gal18, § 25.1.1; Vél71]);
- starting from a given supersingular elliptic curve, every other supersingular elliptic curve can be reached within a 'small' number of steps;
- the endpoints of 'long enough' random walks have an 'almost uniform' distribution (*rapid mixing*).

While the use of supersingular isogeny graphs in cryptography is quite recent [DFJP14], the first results on their structure date back to the works of Eichler [Eic73], Mestre [Mes86], Pizer [Piz98] and Kohel [Koh96].

In this section we provide a general introduction to random walks over graphs, showing the relation between the 'randomness' of a random walk and the structure of the graph. Finally, referring to a famous result due to Pizer [Piz98] (and probably already known to Eichler [Eic73] and Mestre [Mes86]), we show that random walks on suitably-chosen supersingular isogeny graphs end on 'random' vertices.

I.6.1 Random walks

Let G be a graph with set of vertices V and set of edges $\mathcal{E}$. A *random walk* on G is the stochastic process $(X_t)_{t\geq 0}$ defined as follows:

- each state X_t is a vertex of G;
- the starting node X_0 is any vertex of G;
- for each pair of vertices $i, j \in V$,

$$\mathbb{P}_{i\to j} = \begin{cases} \frac{\#\{\text{edges between } i \text{ and } j\}}{\#\{\text{edges starting from } i\}} & \text{if there is an edge between } i \text{ and } j, \\ 0 & \text{otherwise,} \end{cases}$$

  where $\mathbb{P}_{i\to j}$ denotes the probability that, given $X_t = i$ for some $t \geq 0$, the next state X_{t+1} equals j.

The *length* of a random walk is the (possibly infinite) number of its states.

The above definition implies that a random walk is a Markov chain. If G is k-regular, then its transition matrix T is closely related to the adjacency matrix A, namely:

$$T = \frac{1}{k}A.$$

Since the adjacency matrix encloses all information about the structure of G, it is natural to ask which assumptions on G ensure that a sufficiently long random walk on the graph approaches the uniform distribution, no matter how the starting vertex is chosen. To address this question, we call a *probability function* a non-negative map $p\colon V \to \mathbb{R}$ such that $\sum_{x\in V} p(x) = 1$.

Remark I.6.1. Let n be the number of vertices of G, and suppose that we are able to sample a starting node X_0 in G according to a certain probability function $p = (p_1, p_2, \ldots, p_n)$. Then, a random walk from X_0 of length t and transition matrix T on G allows us to sample vertices with probability distribution $T^t p$.

Theorem I.6.2. *Suppose that the graph $G = (V, \mathcal{E})$ is connected, non-bipartite and k-regular with n vertices. Let A be its adjacency matrix and $T = (1/k)A$ the Markov transition matrix. Then, for every probability function p on G we have*

$$\lim_{t\to\infty} T^t p = u$$

where u is the uniform function*, i.e. $u(x) = 1/n$ for each $x \in V$.*

Proof. See [Ter99, Thm. 6.1]. □

Moreover, the convergence of a random walk to the uniform distribution is particularly fast if the eigenvalues of the adjacency matrix are small (in absolute value).

Theorem I.6.3. *Let $G = (V, \mathcal{E})$ be a connected non-bipartite k-regular graph with n vertices. Denote by A its adjacency matrix, and by $T = (1/k)A$ its transition matrix. Define*

$$\mu = \frac{\max(|\lambda_2|, |\lambda_n|)}{k},$$

where $\lambda_1 = k > \lambda_2 \geq \cdots \geq \lambda_n$ are the eigenvalues of A. Then, for every probability function p on G and every positive integer t,

$$\|T^t p - u\|_1 \leq \sqrt{n}\mu^t,$$

where u is the uniform probability function and $\|\cdot\|_1$ is defined as $\|f\|_1 = \sum_{x \in V} |f(x)|$ for each $f : V \to \mathbb{R}$.

Proof. See [Ter99, Thm. 6.2]. □

I.6.2 Ramanujan property

Theorem I.6.3 suggests that the 'speed of expansion' of random walks is related to the absolute value of the eigenvalues of the adjacency matrix of the graph.

A k-regular graph with n vertices is *Ramanujan* if

$$\max(|\lambda_2|, |\lambda_n|) \leq 2\sqrt{k-1},$$

where $\lambda_1 = k > \lambda_2 \geq \cdots \geq \lambda_n$ are the eigenvalues of its adjacency matrix.

Lemma I.6.4 (Rapid mixing on Ramanujan graphs)**.** *Let G be a k-regular Ramanujan graph with n vertices, S be any subset of s vertices, and v be any vertex of G. Then, a random walk of length at least*

$$\frac{\log\left(\frac{n}{\sqrt{s}}\right)}{\log\left(\frac{k}{2\sqrt{k-1}}\right)}$$

starting from v ends in S with probability between $\frac{1}{2}\frac{s}{n}$ and $\frac{3}{2}\frac{s}{n}$.

Proof. See [JMV09, Lem. 2.1]. □

Corollary I.6.5. *Let G be a k-regular Ramanujan graph with n vertices. The diameter of G, i.e. the maximal distance between any pair of its vertices, is $O(\log(n))$.*

Proof. Fix two vertices v and w. Then, setting $S = \{w\}$ in Lemma I.6.4, we can conclude that a random walk of length $\log(n)/\log\big(k/(2\sqrt{k-1})\big)$ starting from v ends in w with non-zero probability. In particular, the distance between v and w is $O(\log(n))$. □

I.6.3 $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$

Let ℓ and p be two distinct primes, $p \geq 5$ and $q = p^r$ for some $r \in \mathbb{N}$. By Tate's theorem [Tat66, § 3], two elliptic curves over $\mathbb{F}_q$ are $\mathbb{F}_q$-isogenous if and only if they have the same trace over $\mathbb{F}_q$. We can thus define the *ℓ-isogeny graph* $\mathcal{G}_\ell(\mathbb{F}_q, a)$ as follows:

- its vertices are the elliptic curves with trace a over $\mathbb{F}_q$ modulo isomorphism over $\mathbb{F}_q$;
- its edges are the isogenies over $\mathbb{F}_q$ of degree ℓ between vertices.

An easy consequence of Tate's theorem is that two curves in the same isogeny graph are either both supersingular or both ordinary, depending on whether their trace over $\mathbb{F}_q$ is a multiple of p. In this chapter, we will focus on supersingular isogeny graphs, while in chapter III we will say more about the ordinary case.

In order to represent the set of supersingular j-invariants in $\mathbb{F}_{p^2}$ (see Theorem I.5.1) in terms of an ℓ-isogeny graph, we wonder if the trace a can be chosen in such a way that the vertices of $\mathcal{G}_\ell(\mathbb{F}_{p^2}, a)$ are in bijection with the supersingular j-invariants. We address this question by rephrasing a result in [AAM19].

Proposition I.6.6. *Let $a \in \{2p, -2p\}$. Then, each supersingular j-invariant $j_0 \in \mathbb{F}_{p^2}$ is represented by exactly one vertex in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, a)$.*

Proof. See [AAM19, pp. 5–6]. □

An alternative supersingular ℓ-isogeny graph, denoted by $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$, can be defined as follows:

- its vertices are the supersingular j-invariants in $\mathbb{F}_{p^2}$;
- its edges are the isogenies of degree ℓ between vertices.

Working with $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$ or with $\mathcal{G}_\ell(\mathbb{F}_{p^2}, \pm 2p)$ is actually the same.

Theorem I.6.7. *$\mathcal{G}_\ell(\overline{\mathbb{F}_p})$ and $\mathcal{G}_\ell(\mathbb{F}_{p^2}, \pm 2p)$ are isomorphic.*

Proof. See [AAM19, Thm. 6]. □

$\mathcal{G}_\ell(\overline{\mathbb{F}_p})$, or equivalently $\mathcal{G}_\ell(\mathbb{F}_{p^2}, \pm 2p)$, enjoys the very properties which ensure 'good mixing' of random walks. First of all, we consider the regularity of the graph.

Proposition I.6.8. *Every vertex of $\mathcal{G}_\ell(\mathbb{F}_{p^2}, \pm 2p)$ has outdegree $\ell + 1$.*

Proof. See [AAM19, §5]. □

Actually, with the possible exception of the vertices 0 and 1728 and their neighbours (see [AAM19, Thm. 7], we can consider $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$ as an undirected $(\ell+1)$-regular graph. In [Piz98], a stronger result is proven.

Theorem I.6.9. *$\mathcal{G}_\ell(\overline{\mathbb{F}_p})$ is Ramanujan.*

Therefore, $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$ enjoys the rapid mixing property stated in Lemma I.6.4. Moreover, since the number of supersingular j-invariants is at most $\lfloor p/12 \rfloor + 2$ (see Corollary II.2.15), from Corollary I.6.5 we conclude that the diameter of $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$ is $O(\log p)$.

I.6.4 The quaternion side

While finding paths between the vertices of $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$ is a computationally hard task, one can construct an alternative version of $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$ by working, as we will say, *on the quaternion side*. Indeed, the link between supersingular j-invariants over $\mathbb{F}_{p^2}$ and maximal orders in $B_{p,\infty}$ is even deeper than one might expect from Theorem I.3.3, because the endomorphism ring of *any* supersingular curve E_0 somehow 'encodes' the whole structure of $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$. We will now give a more precise account of this fact.

Some preliminaries As in the case of number fields, fractional ideals can be defined together with an equivalence relation which makes the set of ideals 'almost' into a group (namely, a *groupoid*: see [Voi21, §19]). The main difference from the number field case is non-commutativity.
The following definitions are drawn from [Voi21, §10, 16].

- The *left order* of a lattice $I \subset B$ is the order
$$\mathcal{O}_\mathsf{L} = \{\alpha \in B \mid \alpha I \subset I\}.$$
- A *left fractional $\mathcal{O}$-ideal* is a lattice $I \subset B$ such that $\mathcal{O} \subseteq \mathcal{O}_\mathsf{L}(I)$.
- The *(reduced) norm* of an ideal I is
$$\mathrm{nrd}(I) = \gcd\{\mathrm{nrd}(\alpha) \mid \alpha \in I\}.$$
- An ideal I is *principal* if $I = \mathcal{O}_\mathsf{L}(I)\alpha$, or, equivalently,[3] if $I = \alpha\mathcal{O}_\mathsf{R}(I)$ for some $\alpha \in B^\times$.
- A lattice I is *invertible* if there exists another lattice I' such that
$$\begin{cases} II' = \mathcal{O}_\mathsf{L}(I) = \mathcal{O}_\mathsf{R}(I'), \\ I'I = \mathcal{O}_\mathsf{L}(I') = \mathcal{O}_\mathsf{R}(I). \end{cases}$$

[3] Voi21, Ex. 16.2.

- An $\mathcal{O}$-left and $\mathcal{O}'$-right ideal I is *invertible* if it is invertible as a lattice and
$$\mathcal{O} = \mathcal{O}_{\mathsf{L}}(I), \qquad \mathcal{O}' = \mathcal{O}_{\mathsf{R}}(I).$$

The class set of an order $\mathcal{O}$ can now be defined, as in [Voi21, §17].

- Define an equivalence relation: two ideals I, J are in the same *right class* if
$$J = \alpha I$$
for some $\alpha \in B^\times$. The equivalence class of I is denoted by $[I]_{\mathsf{R}}$.
- Finally, the set of equivalent classes of ideals is the *right class set* of $\mathcal{O}$:
$$\mathrm{Cls}_{\mathsf{R}}\mathcal{O} = \{[I]_{\mathsf{R}} \colon I \subset B \text{ invertible ideal}\}.$$

Remark I.6.10. The *product* of two ideals I, J is defined only when they are *compatible* in the sense that
$$\mathcal{O}_{\mathsf{R}}(I) = \mathcal{O}_{\mathsf{L}}(J).$$

Deuring's correspondence While the original results date back to Deuring's article [Deu41] in 1941, here we follow [Voi21; Koh96].

Theorem I.6.11. *Let E be a supersingular elliptic curve and $\mathcal{O}$ be the maximal order of $B_{p,\infty}$ such that* $\mathrm{End}(E) \cong \mathcal{O}$. *Then there is a one-to-one correspondence*
$$\{ \textit{ supersingular } j\textit{-invariants in } \mathbb{F}_{p^2} \} \to \mathrm{Cls}_{\mathsf{R}}(\mathcal{O})$$
In particular, each separable isogeny $\varphi \colon E \to E_j$ of degree n corresponds to a left $\mathcal{O}$-ideal of norm n, which is a right $\mathcal{O}_j$-ideal with $\mathcal{O}_j \cong \mathrm{End}(E_j)$.

Proof. See [Voi21, §42; Koh96, §5.3]. □

Even though we omit the complete proof, it is worth recalling the construction used to move back and forth from isogenies to quaternionic ideals. Denote by $\mathcal{O}$ the endomorphism ring of E.

- Let $\varphi \colon E \to E'$ be an isogeny. The corresponding left $\mathcal{O}$-ideal is
$$I_\varphi = \{\alpha \in \mathcal{O} \mid \ker(\varphi) \subseteq \ker(\alpha)\}. \tag{8}$$
- Let I be a proper left $\mathcal{O}$-ideal. The corresponding isogeny is the unique[4] separable isogeny $\varphi_I \colon E \to E_I$ such that
$$\ker(\varphi_I) = \bigcap_{\alpha \in I} \ker \alpha,$$
and $I = I_{\varphi_I}$. See [Wat69, Prop. 3.15].

[4] Up to post-composition with an isomorphism [Sil09, Prop. III.4.12].

- $\deg \varphi_I = \mathrm{nrd}(I)$.
- $\mathcal{O}_{\mathsf{R}}(I) \cong \mathrm{End}\,(E_I)$. More precisely, following [Voi21, Lem 42.2.9], we can define the right action of $\mathrm{End}(E_I)$ on I as

$$\alpha\beta = \frac{\widehat{\varphi_I} \circ \beta \circ \varphi_I \circ \alpha}{\deg \varphi_I}$$

  for each $\alpha \in I$ and $\beta \in \mathrm{End}(E_I)$.

Since we also know $\mathcal{O}_{\mathsf{L}}(I) \cong \mathrm{End}(E)$, we say that I *connects* the endomorphism rings of E and E_I.

Problems that are computationally difficult on $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$ are much easier on the quaternion side. In particular, computing a path between two vertices of $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$ amounts to computing an ideal I of ℓ-powersmooth norm connecting two orders $\mathcal{O}$ and $\mathcal{O}'$. This can be done in polynomial time by means of [KV10, Alg. 3.5] and [DF+20, Alg. 4].

I.7 Orientations

For a given elliptic curve E over $\mathbb{F}_q$, we now focus on the commutative subrings of $\mathrm{End}(E)$ – regardless of whether it is commutative or not, i.e. whether E is ordinary or not. This brings us to the notion of *orientations*.

Let K be an imaginary quadratic field. A *K-orientation* on an elliptic curve E over $\Bbbk$ is an injective ring homomorphism

$$\iota\colon K \hookrightarrow \mathrm{End}^0(E) := \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

The pair (E, ι) is called a *K-oriented elliptic curve*. For an order $\mathcal{O} \subseteq K$, we say that a K-orientation $\iota\colon K \hookrightarrow \mathrm{End}^0(E)$ is an *$\mathcal{O}$-orientation* if $\iota(\mathcal{O}) \subseteq \mathrm{End}(E)$. An $\mathcal{O}$-orientation is called *primitive* if $\iota(\mathcal{O}') \not\subseteq \mathrm{End}(E)$ for every order $\mathcal{O}' \supsetneq \mathcal{O}$ in K. Note that any K-orientation ι is a primitive $\mathcal{O}$-orientation for a unique order $\mathcal{O} \subseteq K$, which is $\iota^{-1}(\mathrm{End}(E))$. We call this order the *primitive order* for the K-orientation.
Finally, an $\mathcal{O}$-orientation on an elliptic curve E over $\Bbbk$ is *locally primitive* at a positive integer m if the index of $\mathcal{O}$ inside the primitive order is coprime to m. The following is a convenient sufficient condition for local primitivity:

Lemma I.7.1. *Let $E/\Bbbk$ be an elliptic curve, let $\sigma \in \mathrm{End}(E)$ and let m be a positive integer such that*

(i) $\mathrm{char}(k) \nmid m$,

(ii) $E[\ell, \sigma] \cong \mathbb{Z}/\ell\mathbb{Z}$ *for every prime divisor* $\ell \mid m$, *where* $E[\ell, \sigma]$ *denotes* $E[\ell] \cap \ker(\sigma)$

Then the natural $\mathbb{Z}[\sigma]$-orientation on E is locally primitive at m. As a partial converse, we have that this orientation is not locally primitive at m as soon as $E[\ell, \sigma] \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ for some prime divisor $\ell \mid m$.

Proof. If the orientation is not locally primitive at m, then we must have $(\sigma - a)/\ell \in \mathrm{End}(E)$ for a prime divisor $\ell \mid m$ and some $a \in \mathbb{Z}$. Thus σ would act as multiplication-by-a on $E[\ell]$. By assumption (ii) we necessarily have $a = 0$, but then $E[\ell, \sigma] = E[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ in view of assumption (i): a contradiction. Conversely, if $E[\ell, \sigma] \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ then by [Sil09, Cor. III.4.11] we know that there exists an $\alpha \in \mathrm{End}(E)$ such that $\alpha \circ [\ell] = \sigma$, so the primitive order must contain σ/ℓ, hence the $\mathbb{Z}[\sigma]$-orientation is not locally primitive at m. □

If $\varphi\colon E \to E'$ is an isogeny and if ι is a K-orientation on E, then we can define an induced K-orientation $\varphi_*(\iota)$ on E' by letting

$$\varphi_*(\iota)(\alpha) = \frac{\varphi \circ \iota(\alpha) \circ \hat{\varphi}}{\deg(\varphi)}, \quad \forall \alpha \in K.$$

Given two K-oriented elliptic curves (E, ι) and (E', ι'), we say that an isogeny $\varphi\colon E \to E'$ is *K-oriented* if $\iota' = \varphi_*(\iota)$. In this case we write $\varphi\colon (E, \iota) \to (E', \iota')$. The dual of a K-oriented isogeny is automatically K-oriented as well. Two K-oriented elliptic curves (E, ι) and (E', ι') are called *isomorphic* if there exists an isomorphism $\varphi\colon E \to E'$ such that $\varphi_*(\iota) = \iota'$.

I.8 Class group actions on oriented elliptic curves

In a similar way as we defined the correspondence between the left class set of a supersingular elliptic curve and the set of all supersingular j-invariants (Theorem I.6.11), for an imaginary quadratic order $\mathcal{O}$ we can now define an action of $\mathcal{C}\ell(\mathcal{O})$ on the set

$$\mathcal{E}\ell\ell^{\mathrm{all}}_{\mathbb{k}}(\mathcal{O}) = \{\, (E, \iota) \mid E \text{ ell. curve over } \overline{\mathbb{k}}, \iota \text{ primitive } \mathcal{O}\text{-orientation on } E \,\}/\cong$$

of primitively $\mathcal{O}$-oriented elliptic curves over $\overline{\mathbb{k}}$ up to K-oriented isomorphisms. The case in which the orientation is by Frobenius is treated in [Sch87; Wat69] and constitutes the main ingredient of CSIDH [Cas+18a]. This group action, which we describe below in more detail, is free, but in general not transitive – see e.g. [Sch87, Thm. 4.5] and [Onu21, Prop. 3.3]. To avoid issues arising from the non-transitivity, we define

$$\mathcal{E}\ell\ell_{\overline{\mathbb{k}}}(\mathcal{O}) \subseteq \mathcal{E}\ell\ell^{\mathrm{all}}_{\overline{\mathbb{k}}}(\mathcal{O})$$

to be a fixed orbit.

The action is defined as follows. Let (E, ι) be a primitively $\mathcal{O}$-oriented elliptic curve and let $[\mathfrak{a}] \in \mathcal{C}\ell(\mathcal{O})$ be an ideal class, which by [Cox13, Cor. 7.17] can be represented by an invertible ideal $\mathfrak{a} \subseteq \mathcal{O}$ of norm coprime to p. One defines the $\mathfrak{a}$-torsion subgroup as

$$E[\mathfrak{a}] = \bigcap_{\alpha \in \mathfrak{a}} \ker(\iota(\alpha)),$$

which is finite of order $N(\mathfrak{a}) = \#(\mathcal{O}/\mathfrak{a})$. Thus there exists a unique[5] separable isogeny $\varphi_\mathfrak{a}\colon E \to E'$ with $\ker(\varphi_\mathfrak{a}) = E[\mathfrak{a}]$. The isomorphism class of $(E', \varphi_{\mathfrak{a}*}(\iota))$ is independent of the choice of the representing ideal $\mathfrak{a}$. By defining $[\mathfrak{a}](E,\iota)$ to be this isomorphism class, one can prove that a free group action is obtained.

The general approach to compute the action of a random element $[\mathfrak{a}] \in \mathcal{C}\ell(\mathcal{O})$ is the following:

- find an ideal $\mathfrak{b} \subset \mathcal{O}$ that can be written as a product of ideals $\prod_i \mathfrak{b}_i^{e_i}$ such that the norm of each $\mathfrak{b}_i$ is at most M and $[\mathfrak{b}] = [\mathfrak{a}]$ (such $\mathfrak{b}$ always exists for $M = O(\log p)$ by [BV07, §9.5]).
- Compute the chain of isogenies

  $$E_0 \xrightarrow{\varphi_{\mathfrak{b}_1}} \ldots \xrightarrow{\varphi_{\mathfrak{b}_n}} E_n$$

  using Vélu's formulas.

With no further assumption on $\mathcal{O}$, however, finding a suitable $\mathfrak{b}$ takes subexponential time. The state-of-the-art algorithm, presented in [BFJ16], also ensures that the exponents e_i are suitably small. Another possible problem is that the kernels of $\mathfrak{b}_1, \ldots, \mathfrak{b}_n$, needed to apply Vélu's formulas, might lie in large extensions of $\mathbb{F}_p$. We will now see, as an example, how CSIDH circumvents these issues by means of an appropriate choice of parameters.

Example 2 (The Frobenius-oriented case, aka CSIDH)**.** The CSIDH scheme sets $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$ for $p = 4\ell_1 \cdot \ldots \cdot \ell_n - 1$. The first advantage of this choice is that $\mathcal{E}\ell\ell^{\mathrm{all}}_{\bar{\mathbb{k}}}(\mathcal{O})$ consists of the ($\mathbb{F}_p$-isomorphism classes of) supersingular elliptic curves defined over $\mathbb{F}_p$, with the orientation given by $\iota\colon \sqrt{-p} \mapsto \pi$. Moreover, by construction, each odd prime ℓ_i dividing $p+1$ *splits* in $\mathcal{O}$, i.e. $\ell_i\mathcal{O}$ can be written as a product of two distinct prime ideals $\mathfrak{l}_i$ and $\bar{\mathfrak{l}_i}$. Precisely (see e.g. [Mil20, Thm. 3.41]), $\mathfrak{l}_i = (\ell_i, \sqrt{-p} - 1)$ and $\bar{\mathfrak{l}_i} = (\ell_i, \sqrt{-p} + 1)$. We stress that $[\bar{\mathfrak{l}_i}] = [\mathfrak{l}_i]^{-1}$ since $\mathfrak{l}_i\bar{\mathfrak{l}_i} = \ell_i\mathcal{O}$, which is principal.

The action of these ideals on $\mathcal{E}\ell\ell^{\mathrm{all}}_{\bar{\mathbb{k}}}(\mathcal{O})$ is transitive and can be efficiently evaluated. In fact, for all $i = 1, \ldots, n$ and $[E] \in \mathcal{E}\ell\ell^{\mathrm{all}}_{\bar{\mathbb{k}}}(\mathcal{O})$, the curves $[\mathfrak{l}_i](E,\iota)$ and $[\bar{\mathfrak{l}_i}](E,\iota)$ are the image curves of the separable isogenies with domain E and kernels

$$E(\mathbb{F}_p) \cap E[\ell_i] \qquad \text{and} \qquad \left\{P \in E(\mathbb{F}_{p^2}) \,\middle|\, \pi(P) = -P\right\} \cap E[\ell_i],$$

respectively.

I.8.1 Oriented isogeny graphs

Isogeny graphs can be also constructed in the context of oriented elliptic curves. In the light of cryptographic applications, we do not limit our construction to isogenies

[5] Up to post-composition with an isomorphism [Sil09, Prop. III.4.12].

of powersmooth degree (as we did for the construction of $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$ in Chapter II), nor to supersingular elliptic curves. We consider instead a finite set of primes $S = \{\ell_1, \dots, \ell_s\}$, and, for an order $\mathcal{O}$ in an imaginary quadratic field K, we define the *oriented graph* $\Gamma_S(\mathcal{O}, p)$ as the graph whose vertices are isomorphism classes of $\mathcal{O}$-oriented elliptic curves defined over $\overline{\mathbb{F}_p}$, and whose edges are K-oriented isogenies of degree ℓ_i for each $i = 1, \dots, s$.

Example 3. The graph $\mathcal{G}_\ell(\mathbb{F}_p)$, defined in Section I.6.3, is a subgraph of $\Gamma_{\{\ell\}}(\mathbb{Z}[\sqrt{-p}], p)$.

When $S = \{\ell\}$, one can prove that the connected components of $\Gamma_S(\mathcal{O}, p)$ contain, as subgraphs, the *ℓ-isogeny volcanoes* introduced by Kohel [Koh96]. They are not the same, though, because each of them has infinitely many levels (and, in particular, infinitely many vertices). We refer to [CK20, Cor. 8] and [Onu21, §4] for a more thorough description of their structure.

For our purposes, however, it is only relevant to remark that every fixed orbit $\mathcal{E}\ell\ell_{\overline{\mathbb{k}}}(\mathcal{O})$ of the action of $\mathcal{C}\ell(\mathcal{O})$ can be seen as a finite subgraph of $\Gamma_S(\mathcal{O}, p)$, where the primes in S split in K and their prime factors generate $\mathcal{C}\ell(\mathcal{O})$.

I.9 Pairings

Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$ of characteristic p, and n be a positive integer coprime with p. We denote by μ_n be the set of n-th roots of unity in $\overline{\mathbb{F}_q}$. As remarked in [Sil10], if we choose a $\mathbb{Z}/n\mathbb{Z}$-basis $\{P, Q\}$ for $E[n]$ and a primitive n-th root of unity ζ_n, then every bilinear pairing $T\colon E[n] \times E[n] \to \mu_n$ corresponds to a 2×2 matrix in $M_2\big(\mathbb{Z}/n\mathbb{Z}\big)$

$$M_T = \begin{pmatrix} x & y \\ w & z \end{pmatrix}$$

whose entries are such that

$$\begin{aligned} T(P,P) &= \zeta_n^x, & T(P,Q) &= \zeta_n^y, \\ T(Q,P) &= \zeta_n^w, & T(Q,Q) &= \zeta_n^z. \end{aligned}$$

We say that T is

- *nondegenerate* if $M_T \in \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ or, equivalently, $R \in E[n] \setminus \{O\}$ implies $T(R, S) \neq 1$ for some $S \in E[n]$.
- *alternating* if M_T is antisymmetric, or, equivalently, $T(R, R) = 0$ for each $R \in E[n]$.

Remark I.9.1. Recall how a basis change on $E[n]$ affects M_T. Let $P' = aP + bQ$ and $Q' = cP + dQ$ be two other generators of $E[n]$. Then the corresponding matrix is $A^t M_T A$, where A is the invertible matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

The map $\tau_A\colon M \mapsto A^t M A$ actually defines an action $\tau\colon A \mapsto \tau_A$ of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ over $M_2(\mathbb{Z}/n\mathbb{Z})$. Thus, the matrices M_T and M'_T representing T w.r.t. different bases lie in the same orbit, i.e. $M'_T = A^t M_T A$ for some $A \in \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. The submodule of anti-symmetric matrices is τ-invariant and consists of the orbit of the matrix W defined in (9). More precisely, $A^t W A = (\det(A))^{-1} W$.
Symmetric matrices are τ-invariant as well.

We are mostly interested in *families* of pairings and their compatibility with isogenies. Given a (possibly inseparable) isogeny $\varphi\colon E \to E'$ and two pairings T, T' on E and E' respectively, we say that T and T' are *compatible with* φ if they satisfy $T'(\varphi(P), \varphi(Q)) = T(P,Q)^{\deg\varphi}$ for every $P, Q \in E[n]$. Expressing this condition in terms of M_T requires some distinctions:

- if $\deg(\varphi)$ is coprime with n, denote by $M_{T'}$ the matrix corresponding to T' with respect to the basis $\{\varphi(P), \varphi(Q)\}$. Then $M_{T'} = \deg(\varphi) M_T$.
- if $\deg(\varphi)$ is not coprime with n, it is not true that the images of P and Q generate all $E'[n]$. Still, we can express the compatibility condition, w.r.t. a given basis $\{P', Q'\}$ of $E'[n]$, as $M_{T'} = \deg(\varphi) B M_T B^t$, where B denotes the coefficients of $\varphi(P)$ and $\varphi(Q)$ in the basis $\{P', Q'\}$. We stress that B is not invertible, in this case.

Remark I.9.2. The set of pairings over $E[n] \times E[n]$ forms a group $(\mathcal{T}, \cdot)$ w.r.t. the point-wise product $(T \cdot U)(P,Q) = T(P,Q) \cdot U(P,Q)$. It is immediate to check that the matrix corresponding to $T \cdot U$ is $M_T + M_U$. This also shows that, if there exist pairings T' and U' on $E'[n] \times E'[n]$, s.t. T, T' and U, U' are compatible with an isogeny $\varphi\colon E \to E'$, then also $T \cdot U$ and $T' \cdot U'$ are compatible with φ.

It is well-known that the Weil pairing on $E[n]$, which we denote by e_n, satisfies all the above properties: see e.g. [BSS05, §IX.6]. In particular, it is compatible with *any* isogeny $\varphi\colon E \to E'$. The corresponding matrix is a scalar multiple of the matrix

$$W = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{9}$$

In fact, whene E is supersingular, every pairing on $E[n]$ arises from 'distorting' e_n by means of some endomorphism (also called *distortion map* in this context).

Proposition I.9.3. *Let E be a supersingular elliptic curve over $\mathbb{F}_q$ and n a positive integer coprime with $p = \mathrm{char}(\mathbb{F}_q)$. Then every bilinear pairing $T(X,Y)$ of $E[n]$ has the form $e_n(X, \omega(Y))$ where e_n is the Weil pairing and ω is a distortion map.*

Proof. Let $M_T \in M_2(\mathbb{Z}/n\mathbb{Z})$ be the matrix corresponding to T, and define W as in (9). We can obviously write $M_T = W\Omega$ with $\Omega = W^{-1} M_T$. To conclude, it is enough to prove that every $\Omega \in M_2(\mathbb{Z}/n\mathbb{Z})$ represents some endomorphism ω. This is a well-known argument [Len96, §3], which we briefly recall. Let K be an extension of $\mathbb{F}_q$ such

that $E[n] \subset E(K)$ and $\mathrm{End}_K(E)$ is the full endomorphism ring of E. Then there is an injective ring homomorphism

$$\mathrm{End}(E) \otimes \mathbb{Z}/n\mathbb{Z} \to \mathrm{End}(E[n]).$$

Since both rings are free $\mathbb{Z}/n\mathbb{Z}$-modules of rank 4, they have both cardinality n^4 and the above map is an isomorphism. □

While Proposition I.9.3 shades light on how all pairings arise from the Weil pairing from a theoretical perspective, it is of little use for actually constructing families of *compatible* pairings on distinct curves: if $\varphi\colon E \to E'$ is an isogeny and ω is an endomorphism of E, computing a compatible pairing on E' would require to know how φ acts on the kernel of ω, which is unlikely to be the case in cryptographic applications. We defer to Section III.2 the introduction of more practical approaches.

Chapter II

Hashing and crawling in the full supersingular isogeny graph

We will now focus on the graph $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$ introduced in I.6, and consider two problems of cryptographic interest: the first arises from the observation that some isogeny-based protocols, such as IS-CUBE [Mor23] and M-SIDH [FMP23], may require a supersingular elliptic curve with unknown endomorphism ring as a starting point. In other words, they may require to *hash* in $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$ in a 'cryptographically secure' way. The best-known algorithm to produce supersingular elliptic curves over a finite field of cryptographic size is only able to 'directly' extract a negligible fraction of all the existing supersingular elliptic curves. The other supersingular elliptic curves can be sampled 'indirectly' as the endpoints of random walks in suitable isogeny graphs. This approach, however, reveals the endomorphism ring of the output curve – unless an oblivious computation is used, which in turn requires a trusted authority or a multiparty protocol. Therefore, a mathematical solution to the problem of sampling supersingular elliptic curves with unknown endomorphism ring, or *cSRS problem*, is yet to be found: we will survey the known approaches and point out some possible research directions.
The latter problem is somehow inspired by the CM methods from the first part of the chapter: to each supersingular elliptic curve we attach an integer, say M, which is the degree of its smallest non-trivial endomorphism, and we ask whether being able to compare different values of M might be enough to break *the* problem on which most isogeny-based protocols rely, i.e. the problem of finding a secret isogeny of power-smooth degree between two given supersingular elliptic curves (ℓ-IsoPath). We will disprove this in Proposition II.3.2, by leveraging the connection between supersingular elliptic curves and quaternion algebras.

The structure of the chapter is as follows: in Section II.1 we motivate and formalize the cSRS problem and ℓ-IsoPath. The former is then discussed in Section II.2, while Section II.3 introduces the problem IsMSmaller and compares it with ℓ-IsoPath.

II.1 Some cryptographic problems

The purpose of this section is to introduce and motivate the remainder of this chapter from a cryptographic perspective.

In Section II.1.1 we present the main hard mathematical problems on which the security of isogeny-based cryptography is based. As we will see, they essentially amount to efficiently finding short paths between given vertices of $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$. Finally, in Section II.1.2, we provide some examples of cryptosystems whose security is affected by the (partial) knowledge of the endomorphism ring of the *starting* supersingular elliptic curve – which will be the motivating problem of Section II.2.

II.1.1 Hard problems on $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$

The following mathematical problems are considered computationally hard [Gal+16, § 2.2].

Problem 1 (ℓ-IsoPath)**.** *Let p and ℓ be distinct primes. Given two uniformly-random supersingular elliptic curves E and E' over $\mathbb{F}_{p^2}$, find an ℓ-isogeny path between them, i.e. a path*

$$E \to E_1 \to \cdots \to E'$$

on $\mathcal{G}_\ell(\mathbb{F}_{p^2}, 2p)$.

Problem 2 (EndRing)**.** *Given a prime p and a uniformly-random supersingular elliptic curve E over $\mathbb{F}_{p^2}$, compute $\mathrm{End}(E)$, i.e. find four endomorphisms that generate $\mathrm{End}(E)$ as a $\mathbb{Z}$-module.*

There exist supersingular elliptic curves whose endomorphism rings can be easily computed – namely, those having non-trivial endomorphisms of small degree. We will discuss this in Section II.2.2.

Solving either ℓ-IsoPath or EndRing turns out to be the same.

Theorem II.1.1. *ℓ-IsoPath and EndRing are computationally equivalent under heuristic assumptions or Generalized Riemann Hypothesis. More precisely:*

- *if two elliptic curves E, E' are given together with their endomorphism rings $\mathrm{End}(E)$ and $\mathrm{End}(E')$, then an ℓ-isogeny $E \to E'$ can be computed in polynomial time;*
- *if an elliptic curve E is given together with an ℓ-isogeny $E' \to E$ and the endomorphism ring $\mathrm{End}(E')$, then $\mathrm{End}(E)$ can be computed in polynomial time.*

Proof. This was proven first under heuristic assumptions in [Eis+20, § 5.5], and later in [Wes21] under the Generalised Riemann Hypothesis. □

However, not all the instances of EndRing need be hard, as we will see in Section II.2.2. Namely, the endomorphism ring of a supersingular elliptic curve with a small non-trivial endomorphism can be computed efficiently (Proposition II.2.6). From this fact stem the two directions of research that we will consider in the rest of this chapter: avoiding these 'weak' curves when choosing the starting parameters of some protocols (Section II.2), and, conversely, trying to reach them to efficiently navigate $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$ (Section II.3).

II.1.2 Cryptographic applications

Hard mathematical problems can often be exploited to construct secure cryptographic protocols, and ℓ-IsoPath and EndRing are no exceptions. Here we focus on examples that highlight the importance of avoiding 'weak curves' in the choice of the starting parameters.

CGL hash function The *CGL function* [CLG09] is a hash function based on the isogeny graph $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$ for some small prime $\ell \neq p$. Such function is outlined in Algorithm 1 for the case $\ell = 2$. Figure II.1 depicts the path in $\mathcal{G}_2(\mathbb{F}_{p^2})$ determined by the computation of the image of the bitstring 101.

Algorithm 1: CGL hash function

Input: A supersingular elliptic curve E_0 over $\mathbb{F}_{p^2}$; a bitstring m of n bits, i.e. $m = b_1 b_2 \cdots b_n$.
Output: $\mathsf{CGL}(m)$.
Choose a 2-torsion point P of E_0;
Compute the isogeny $\varphi_0 \colon E_0 \to E_0/\langle P \rangle$ with kernel $\langle P \rangle$;
Set $E_1 = E_0/\langle P \rangle$;
for $i \in \{1, \ldots, n\}$ **do**
  Find the 2-torsion points of E_i, other than O;
  Rule out the 2-torsion point P such that the map $E_i \to E_i/\langle P \rangle$ with kernel $\langle P \rangle$ is the dual of φ_{i-1};
  Label the remaining 2-torsion points by P_0, P_1 (according to some convention);
  Compute the isogeny $\varphi_i \colon E_i \to E_i/\langle P_{b_i} \rangle$ with kernel $\langle P_{b_i} \rangle$;
  Set $E_{i+1} = E_i/\langle P_{b_i} \rangle$;
end
Set $\mathsf{CGL}(m) = j\,(E_{n+1})$;

In this setting, a collision happens whenever the same curve E_{n+1} can be reached through two distinct ℓ-isogeny paths starting from E_1. Therefore, the hardness of ℓ-IsoPath ensures that the CGL function is, in general, collision-resistant (see [CLG09, § 5]).

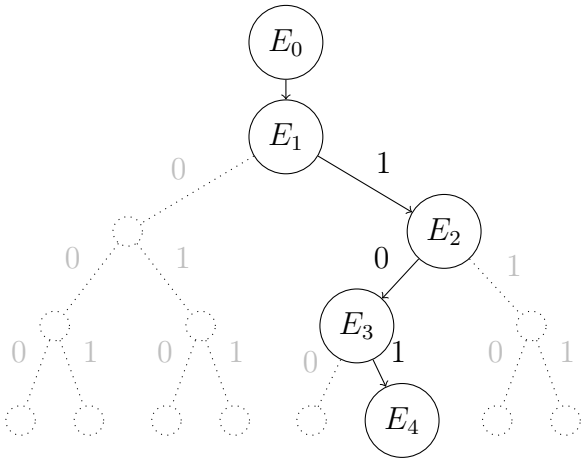

Figure II.1: The path followed by the CGL function within the graph $\mathcal{G}_2(\mathbb{F}_{p^2})$ for the bitstring 101.

However, Theorem II.1.1 suggests that the starting curve E_0 for the CGL hash function should be chosen carefully. Namely, if computing $\mathrm{End}(E_0)$ is by any chance easy, then finding collisions becomes easy as well.

VDF based on isogeny graphs A function is called a *verifiable delay function (VDF)* [Bon+18] if it requires a specified number of sequential steps to be evaluated (independent of the hardware architecture used for the computation) and it is possible to efficiently verify that a value is the correct output of the function. In particular, evaluating a VDF over any input should not be significantly easier if parallel computation is employed.

In [DF+19, §3, §5], De Feo et al. construct a VDF that consists in evaluating at some point $Q \in E'(\mathbb{F}_p)$ a given ℓ^T-degree isogeny $\hat{\varphi}\colon E' \to E$ between two supersingular elliptic curves defined over $\mathbb{F}_p$. Such evaluation requires, in general, polynomial time in T.

However [DF+19, §6.2], if $\mathrm{End}(E)$ is known, an auxiliary isogeny $\psi\colon E \to E'$ of small degree can be precomputed and exploited to speed up the computation of $\hat{\varphi}(Q)$, breaking the sequentiality of the VDF. Therefore, as in the previous example, E should be chosen in such a way that no information about its endomorphisms can be retrieved easily.

Delay encryption The same computational challenge described above – i.e. evaluating at some point $Q \in E'(\mathbb{F}_p)$ a given ℓ^T-degree isogeny $\hat{\varphi}\colon E' \to E$ between two supersingular elliptic curves defined over $\mathbb{F}_p$ – is also exploited in [BDF21] to instantiate a new cryptographic primitive called *delay encryption*, used to produce encrypted messages that can be decrypted (by anyone) only after a given amount of time T. In this case, too, the choice of E is problematic for the same reasons described in the previous paragraph, so that anyone knowing $\mathrm{End}(E)$ would be able to decrypt messages earlier than expected.

Public-key cryptosystems Until July 2022, the key encapsulation mechanism SIKE, based on the public-key cryptosystem SIDH [DFJP14], was one of the flagships of isogeny-based cryptography. Its fall was due to three attacks [CD23; Mai+23; Rob23], the latter of which proved that randomizing the starting curve is not enough to avoid the attack. However, new protocols are still rising from the ashes of SIKE: two examples that require random supersingular elliptic curves among their parameters are IS-CUBE [Mor23] and M-SIDH [FMP23].

Other applications We have already observed that the knowledge of $\mathrm{End}\, E$ can be exploited to speed up the computation of isogenies starting from E. When this fact does not represent a security issue, it provides on the contrary a good motivation for using E instead of some other supersingular elliptic curve with unknown endomorphism ring. This is the case for CSIDH [Cas+18b], SQISign [DF+20], SQISignHD [Dar+23], the VDF in [CSRHT22] and many other isogeny-based protocols. However, we cannot exclude that the discovery/refinement of attacks might eventually force the use of supersingular elliptic curves with unknown endomorphism rings for some of these protocols, too.

II.2 The SRS problem

Section II.1.2 suggests that starting from random supersingular elliptic curves is a good safety practice in a wide variety of protocols. In this section we see to which extent this is feasible in practice.

The first question that needs to be answered is whether sampling *any* supersingular elliptic curve is possible – and this has a positive answer thanks to CM-reduction methods (Section II.2.2). However, there is no cryptographically secure way to randomize the outputs of CM-reductions: this is only possible using trusted setups or multiparty computations [Bas+23]. In the later sections, we will focus instead on alternative ways to sample supersingular elliptic curves in a single-handed and cryptographically secure way.

To this end, we need a more precise formalization of the problem, which comes in two different flavors:

- the first, weaker, version solely focuses on the mathematical problem;
- the second, stronger, version adds some further requirements which take into account the cryptographic applications.

II.2.1 Formalization of the problem

A *supersingular random sampler* is a randomized algorithm A, on input a prime p, that produces a supersingular elliptic curve E over $\mathbb{F}_{p^2}$ in such a way that the output

distribution – for p ranging over the set of all supersingular elliptic curves over $\mathbb{F}_{p^2}$ – is almost uniform, in the sense that it is computationally indistinguishable from the uniform distribution.

Remark II.2.1. Suppose that A' is a deterministic algorithm that, on the input of a prime p, produces a supersingular elliptic curve E over $\mathbb{F}_{p^2}$. Then, A' can be easily turned into a supersingular random sampler A thanks to the rapid mixing property of Lemma I.6.4. Namely, on input p, A simply performs a random walk in $\mathcal{G}_\ell(\overline{\mathbb{F}_{p^2}})$ starting from $E \leftarrow \mathsf{A}'(p)$, and outputs the endpoint of the random walk.

The first problem we define is named the Supersingular Random Sampler (SRS in short) problem:

Supersingular Random Sampling (SRS) problem
Construct a supersingular random sampler whose time complexity is polynomial in $\log p$.

To formulate a stronger version of the SRS problem, for any supersingular random sampler A we define a slight variation of Problem 2, relative to A itself.

Problem 3 ($\textsc{EndRing}_{\mathsf{A}}$)**.** *Given* $E \leftarrow \mathsf{A}(p)$ *and the randomness used by* A *to produce* E*, compute* $\mathrm{End}(E)$*.*

Given a supersingular random sampler A, we say that A is a *supersingular random crypto-sampler* if $\textsc{EndRing}_{\mathsf{A}}$ is computationally hard. This definition motivates the following stronger version of the SRS problem.

Crypto Supersingular Random Sampling (cSRS) problem
Construct a supersingular random crypto-sampler whose time complexity is polynomial in $\log p$.

Remark II.2.2. Let A be a supersingular random sampler consisting of a random walk $E \to E'$ that starts from the output of a deterministic algorithm A', as described in Remark II.2.1. In this case, the randomness used by A is the random walk itself. It is then clear, in the light of Theorem II.1.1, that computing $\mathrm{End}(E')$ using the randomness of A is equivalent to computing $\mathrm{End}(E)$. Therefore, if computing $\mathrm{End}(E)$ is easy, then A' cannot be a supersingular random crypto-sampler.

SRS and cSRS problems over $\mathbb{F}_p$ Our formalization of the SRS and cSRS problems deals with supersingular elliptic curves defined over $\mathbb{F}_{p^2}$, while the majority of applications considered in Section II.1.2 make use of supersingular elliptic curves defined over the subfield $\mathbb{F}_p$. Nothing ensures that an efficient supersingular random (crypto-)sampler can find supersingular elliptic curves over $\mathbb{F}_p$ as efficiently as over $\mathbb{F}_{p^2}$, since the probability that a random supersingular elliptic curve over $\mathbb{F}_{p^2}$ is defined over $\mathbb{F}_p$ is about $1/\sqrt{p}$ [DG16, §4]. However, all the methods considered in this section

can be easily adapted to sample supersingular elliptic curves defined over $\mathbb{F}_p$ (in fact, most of them can be made more efficient in this way). For this reason we will often switch between $\mathbb{F}_{p^2}$ and $\mathbb{F}_p$.

We stress that some extra information about $\mathrm{End}(E)$ is automatically known when E is defined over p, since in this case E is Frobenius-oriented as we have seen in Example 2. Nevertheless, retrieving the full endomorphism ring of E from this information is considered a hard problem. In fact, the security of CSIDH relies (also) on it [Wes22, Cor. 5].

Related work The SRS and cSRS problems are also tackled in an independent work by Booher et al. [Boo+22].

In [Boo+22, §2] the Hasse invariant $H_p(\lambda)$ is considered for elliptic curves in Legendre form, with additional remarks on how some root over $\mathbb{F}_p$ could be found, using an iterative method which also requires an efficient evaluation of the derivative $H'_p(\lambda)$ over $\mathbb{F}_p$. Moreover, some variants of the method that we derive from Proposition II.2.31 are illustrated in [Boo+22, §4].

The following new approaches are also presented in [Boo+22]:

- Computing the roots of $\gcd\left(\Phi_n(x, x^p), \Phi_m(x, x^p)\right)$, where n, m are positive integers coprime with p and Φ_n, Φ_m denote the modular polynomials of levels n and m, respectively [Boo+22, §3]. This amounts to finding j-invariants of elliptic curves having two non-trivial endomorphisms of degrees np and mp, respectively. The roots found have good chances of being supersingular and can be computed in time linear with respect to m, n and $\log(p)$. However, since the output curve has a non-trivial endomorphism of degree nm, either m or n should have the same size as p (otherwise the endomorphism ring can be retrieved [LB20], as we will explain more thoroughly in the proof of Proposition II.2.7).

- Finding supersingular elliptic curves as components of algebraic varieties of higher dimension or higher genus [Boo+22, §5]. One method consists of performing a random walk on the isogeny graph of abelian surfaces, starting from a product of supersingular elliptic curves, until another product of (supersingular) elliptic curves is reached. Another method starts from Kummer surfaces of superspecial abelian surfaces and looks for their supersingular components (if any).

- Using a quantum computer to perform a random chain of ℓ-isogeny paths 'in superposition', for some small primes ℓ [Boo+22, §5]. This method hides most of the information that a classic ℓ-isogeny path would otherwise reveal, but requires a quantum computer to be implemented.

Despite their theoretical interest, none of the methods presented in [Boo+22] result in an efficient supersingular random crypto-sampler.

II.2.2 Known approaches

We now survey some known supersingular random samplers that solve the SRS problem, showing that none of them leads to a supersingular random crypto-sampler.

First, we provide a detailed description of the most efficient, to the best of our knowledge, supersingular random sampler. It consists of the combination of two building blocks: an algorithm due to Bröker and a random walk over $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$. Our goal for this section is to provide a comprehensive explanation of the combination of these blocks.

In Section II.2.2 we will discuss why the resulting algorithm is not a supersingular random crypto-sampler. Finally, in Section II.2.2 we present some cSRS algorithms. They are mainly of theoretical interest, though, since their computational cost is at least sub-exponential in $\log(p)$, and therefore they are not a solution to the cSRS problem.

Bröker's algorithm

For any given prime $p \geq 5$, at least one supersingular j-invariant over $\mathbb{F}_{p^2}$ can be efficiently found thanks to Bröker's algorithm [Brö09], whose core is the reduction of a suitable CM elliptic curve.

Theorem II.2.3 (Deuring)**.** *Fix a prime $p \geq 5$. Let E be an elliptic curve over a number field L, with* $\mathrm{End}(E)$ *isomorphic to an order $\mathcal{O}$ in an imaginary quadratic field k. Let $\mathfrak{P}$ be a prime of L over p, and suppose that E has a good reduction modulo $\mathfrak{P}$, which we denote by $\tilde{E}$. Then $\tilde{E}$ is supersingular if and only if p has only one prime of k above it (that is, p does not split in k).*

Proof. See [Deu41; Lan87, Thm. 13.12]. □

Deuring's theorem provides a criterion for determining whether the reduction modulo a suitable prime ideal $\mathfrak{P}$ of a CM curve is supersingular or not. More precisely, constructing a supersingular elliptic curve over $\overline{\mathbb{F}}_p$ is equivalent to constructing a CM curve E – over some number field – such that p does not split in $\mathrm{End}(E)$. Equivalently, if we denote by k the imaginary quadratic field which $\mathrm{End}(E)$ is an order of, and by D the discriminant of k, p does not split in k if and only if

$$\left(\frac{D}{p}\right) \neq 1, \tag{10}$$

where the left-hand expression denotes the Legendre symbol [Cox13, Prop. 5.16, Cor. 5.17].

Once a quadratic field k satisfying (10) is fixed, the goal is to determine the CM j-invariants whose endomorphism rings lie in k. In Section I.4 we have depicted the following strategy to generate a supersingular j-invariant in $\mathbb{F}_{p^2}$ for a fixed prime $p \geq 5$:

1) Choose an imaginary quadratic field k whose discriminant D satisfies equation (10);

2) Choose an order $\mathcal{O}$ in k;

3) Compute the Hilbert class polynomial $P_{\mathcal{O}}$;

4) Consider the reduction modulo p of $P_{\mathcal{O}}$ and find one of its roots.

Remark II.2.4. This method can be adapted, more generally, to generate elliptic curves of any prescribed order, as shown in [Brö06].

Bröker's algorithm, which is summarized in Algorithm 2, is just a special case of the above strategy. In particular, it performs steps (1) and (2) in such a way that the computation time is polynomial in $\log(p)$, and the j-invariant found lies in $\mathbb{F}_p$. This is achieved by executing the following steps:

- compute the smallest prime $q \equiv 3 \mod 4$ such that $\left(\frac{-q}{p}\right) \neq 1$;
- set $k = \mathbb{Q}(\sqrt{-q})$;
- set $\mathcal{O} = \mathbb{Z}[(1+\sqrt{-q})/2]$, that is the maximal order of $\mathbb{Q}(\sqrt{-q})$.

In particular, the fact that q is the smallest possible ensures that $\mathcal{O}$ is uniquely determined by p, and for this reason we will denote it by $\mathcal{O}_p$ in the following. Thus, the output of Bröker's algorithm depends only on p and the root of $P_{\mathcal{O}}$ chosen at step (4).

Algorithm 2: Bröker's algorithm

Input: A prime $p \geq 5$.
Output: A supersingular j-invariant $j \in \mathbb{F}_p$.
Set $q = 3$;
while $\left(\frac{-q}{p}\right) = 1$ **do**
  Assign q to the next prime equivalent to 3 modulo 4;
end
Compute the Hilbert class polynomial $P_{\mathcal{O}}$ relative to the quadratic order $\mathcal{O}$ of discriminant $-q$;
Find a root $\alpha \in \mathbb{F}_p$ of $P_{\mathcal{O}}$ modulo p;
Set $j = \alpha$.

According to Bröker's analysis in [Brö09, Lem. 2.5], the expected running time of Algorithm 2 is $\tilde{O}\big((\log p)^3\big)$ due to the following reasons:

- heuristically, q is likely to be below 50 for $p \sim 2^{256}$. This fact seems reasonable since half of the elements of $\mathbb{Z}/p\mathbb{Z}$ are quadratic non-residues. In [LO77] it is proven that, under the Generalized Riemann Hypothesis, q has size $O\big((\log p)^2\big)$.

- $P_{\mathcal{O}}$ can be computed in $\tilde{O}(\mathrm{disc}(\mathcal{O})) = \tilde{O}(q) = \tilde{O}\big((\log p)^2\big)$ time, as we have already pointed out in Section I.4.

- a root of $P_{\mathcal{O}}$ in $\mathbb{F}_p$ can be found, as described for example in [GG13, § 14.5], in probabilistic time
$$\tilde{O}\big(\deg(P_{\mathcal{O}})(\log p)^2\big),$$
that is $\tilde{O}\big((\log p)^3\big)$ because $\deg(P_{\mathcal{O}}) = h(\mathcal{O}) = \tilde{O}(\sqrt{q})$. The latter equality is a classical result from [Sie35], where $h(\mathcal{O})$ denotes the class number of the order $\mathcal{O}$).

Extending Bröker's algorithm

The output distribution of Bröker's algorithm is far from being uniform. In fact, for any p, the output belongs to a pre-determined subset of all possible supersingular j-invariants over $\mathbb{F}_{p^2}$, i.e. the roots of $P_{\mathcal{O}}$ in $\mathbb{F}_p$, which are $\tilde{O}(\sqrt{q})$. Following [LB20], we now go back to the general strategy on which Bröker's algorithm is based and see to what extent it can be translated into an efficient SRS algorithm.

Listing imaginary quadratic orders Imaginary quadratic orders can be listed according to their discriminants:

Theorem II.2.5. *Write every integer as f^2D, where D is square-free. There is a bijection*

$$\begin{aligned}
&\{\,\text{Imaginary quadratic orders}\,\} \leftrightarrow \mathbb{Z}_{<0}\\
&\qquad \mathcal{O} \subseteq \mathbb{Q}(\sqrt{D}) \mapsto \begin{cases} \mathrm{disc}\,\mathcal{O} & \text{if } D \equiv 1 \mod 4,\\ \frac{\mathrm{disc}\,\mathcal{O}}{4} & \text{if } D \equiv 2,3 \mod 4 \end{cases}\\
&\text{Order of conductor } f \text{ in } \mathbb{Q}(\sqrt{D}) \hookleftarrow f^2D.
\end{aligned}$$

In particular, if we denote by $\mathcal{D}$ the set

$$\mathcal{D} = \{\mathrm{disc}\,\mathcal{O} \mid \mathcal{O}\,\text{imaginary quadratic order}\,\},$$

we have

$$\mathcal{D} = \left\{ f^2 d \mid f, d \in \mathbb{Z},\, d < 0,\, d \text{ square-free and either } d \equiv 1 \bmod 4 \text{ or } f \text{ is even} \right\}. \quad (11)$$

Proof. We recall from [Cox13, § 5.B] that every imaginary quadratic field can be written as $\mathbb{Q}(\sqrt{D})$ with D negative square-free integer, and its discriminant is

$$d_{\mathbb{Q}(\sqrt{D})} = \begin{cases} D & \text{if } D \equiv 1 \mod 4,\\ 4D & \text{if } D \equiv 2,3 \mod 4. \end{cases}$$

Let $\mathcal{O}_D$ be the ring of integers of $\mathbb{Q}(\sqrt{D})$. Any positive integer f yields a unique order $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_D$ of conductor f, and every imaginary quadratic order can be constructed in this way [Cox13, Lemma 7.2].
Finally, the discriminant of an order of conductor f in $\mathbb{Q}(\sqrt{D})$ is $f^2 d_{\mathbb{Q}(\sqrt{D})}$ (see [Cox13, p. 134]). Therefore, the maps defined above are one inverse to the other. □

Increasing the number of outputs The general strategy on which Bröker's algorithm is based consists of choosing a random imaginary quadratic order $\mathcal{O}$ whose discriminant is not a square modulo p and finding a root of $P_{\mathcal{O}}$ modulo p. Algorithm 3, which we label 'Extended Bröker's algorithm', exactly follows this strategy, setting a lower bound $-4M$ for $\operatorname{disc}\mathcal{O}$.

Algorithm 3: Extended Bröker's algorithm

Input: A prime $p \geq 5$ and a positive integer M.
Output: A supersingular j-invariant $j \in \mathbb{F}_{p^2}$.
Choose a random negative integer $n \in \mathcal{D} \cap [-4M, -3]$, with $\mathcal{D}$ as in (11);
Write $n = f^2 d$ with d square-free;
while $\left(\frac{d}{p}\right) = 1$ **do**
  Choose a new n;
end
Let $\mathcal{O}$ be the imaginary quadratic order of discriminant $f^2 d$;
Compute the Hilbert class polynomial $P_{\mathcal{O}}$;
Compute any root $\alpha \in \mathbb{F}_{p^2}$ of $P_{\mathcal{O}}$ modulo p;
Set $j = \alpha$.

We stress that M should be large enough so that at least one quadratic discriminant $n \in [-4M, -3]$ is not a quadratic residue modulo p (otherwise the algorithm would run endlessly). Under the Generalized Riemann Hypothesis, it is enough to set $M = \tilde{O}\big((\log p)^2\big)$ [LO77].

The analysis of Algorithm 2 can be straightforwardly adapted to show that the expected running time of Algorithm 3 is $\tilde{O}\big(\sqrt{M} \cdot (\log p)^2\big)$:

- $|n|$ is at most $4M$.
- $P_{\mathcal{O}}$ can be computed in $\tilde{O}(\operatorname{disc}(\mathcal{O})) = \tilde{O}(M)$ time.
- a root of $P_{\mathcal{O}}$ in $\mathbb{F}_{p^2}$ can be found in probabilistic time

$$\tilde{O}\big(\deg(P_{\mathcal{O}})(\log p)^2\big) = \tilde{O}\big(\sqrt{M} \cdot (\log p)^2\big).$$

In the light of Theorem II.2.3 and since any supersingular elliptic curve is a CM curve, Algorithm 3 can generate any supersingular j-invariant in $\mathbb{F}_{p^2}$, provided that M is large enough. Therefore, it is natural to ask which is the minimum value of M for

which this holds. A first, rough estimate immediately suggests that M must be quite big (a more precise estimate can be found in [LB20, Prop. A.5]).

Proposition II.2.6. *Let N be the number of possible outputs of Algorithm 3. Then $N = \tilde{O}(M^{3/2})$.*

Proof. Let $\mathcal{O}$ be any quadratic order whose discriminant lies in the range $[-4M, -3]$. We have already observed that the class number $h(\mathcal{O})$, which is equal to the number of distinct roots of $P_{\mathcal{O}}$ modulo p, is $\tilde{O}(M^{1/2})$. If we denote by $h(n)$ the class number of the quadratic order of discriminant n, then

$$N = \sum_{\substack{n \in \mathcal{D} \\ -4M \leq n}} h(n) \leq 4M \cdot \tilde{O}(M^{1/2}) = \tilde{O}(M^{3/2}), \tag{12}$$

where $\mathcal{D}$ is defined as in (11). □

For N to be (close to) the total number of supersingular j-invariants over $\mathbb{F}_{p^2}$, which is about $p/12$ (see Corollary II.2.15 and [Was08, Cor. 4.40]), the previous proposition rules that the value of M must be $\tilde{O}(p^{2/3})$. In that case, though, the running time of Algorithm 3 is exponential, namely, it is $\tilde{O}(p^{1/3})$.

Endomorphisms of small degree On the other hand, for values of M that make Algorithm 3 efficient, the output supersingular elliptic curve is not suitable for cryptographic applications.

Proposition II.2.7. *If E is an output of Algorithm 3 (on input M polynomial in $\log(p)$), then $\mathrm{End}(E)$ can be computed efficiently.*

Proof. The statement is remarked in [LB20, p. 1], but here we provide a more explicit explanation. Following [LB20], we say that a curve is *M-small* if it has a non-trivial endomorphism of degree at most M. Let $\mathcal{O}$ be the quadratic order selected at the end of the while loop in Algorithm 3, and E be an elliptic curve over $\mathbb{F}_{p^2}$ whose j-invariant is the output of the algorithm.

A copy of $\mathcal{O}$ is embedded in $\mathrm{End}(E)$. To prove this, recall from Section I.4 that $j(E)$ is the reduction modulo p of some complex CM j-invariant, say $\tilde{j}$, whose endomorphism ring is isomorphic to $\mathcal{O}$. Let $\tilde{E}$ be a complex CM curve with j-invariant $\tilde{j}$, and suppose that its reduction is E. The reduction map $\mathrm{End}(\tilde{E}) \to \mathrm{End}(E)$ is a degree-preserving injective ring homomorphism [Sil94, Prop. 4.4]. Therefore, $\mathcal{O}$ is embedded in $\mathrm{End}(E)$.

In particular, E is M-small [LB20, Prop. 2.4], i.e. $\mathrm{End}(E)$ contains a non-trivial endomorphism of degree $|\mathrm{disc}\,\mathcal{O}| \leq M$, which can be found applying Vélu's formulae to every subgroup of E having order $|\mathrm{disc}\,\mathcal{O}|$. This can be done efficiently since we are assuming that M is polynomial in the $\log(p)$.

In fact, the whole structure of $\mathrm{End}(E)$ can be computed as follows:

1) Depending on p, consider a 'special' order as in [Eis+18, Prop. 1]. By [Eis+18, Prop. 3], one can compute a j-invariant j_0 whose endomorphism ring is isomorphic to such order. Let E_0 be a curve of j-invariant j_0. By construction, assuming the Generalized Riemann Hypothesis, E_0 is $O(\log^2 p)$-small.

2) [LB20, Thm. 1.3] shows that isogenies of power-smooth degree between M-small curves can be computed in polynomial time in the $\log(p)$. Thus, since $\mathrm{End}(E_0)$ and a power-smooth isogeny $E_0 \to E$ are known, $\mathrm{End}(E)$ can be retrieved by Theorem II.1.1.

□

Bröker's algorithm and random walks

We will now consider the extended Bröker's algorithm (Algorithm 3) under the assumption that M is polynomial in the $\log(p)$ (so that the running time is polynomial, too).

The only known algorithm for (almost) uniformly sampling over the set of all supersingular j-invariants over $\mathbb{F}_{p^2}$ [Vit19, p. 71] is constructed according to the strategy described in Remark II.2.1. In particular, it performs a random walk in $\mathcal{G}_\ell(\overline{\mathbb{F}_{p^2}})$ (for some small prime $\ell \neq p$) starting from an output of Algorithm 3. This algorithm, though, does not solve the cSRS problem, as we are going to show in Section II.2.2.

Almost uniform output Let $n = \#\{\text{Supersingular } j\text{-invariants}\}$ (n is about $p/12$: see Corollary II.2.15 and [Was08, Cor. 4.40]). How long should a random walk be, in order to ensure that every supersingular j-invariant can be reached with probability close to $1/n$? The answer to this question follows from Section I.6.3. Namely, starting from a given supersingular j-invariant in $\mathbb{F}_{p^2}$ (in this case, the output of Algorithm 3), every other supersingular j-invariant in $\mathbb{F}_{p^2}$ can be reached within $O(\log(p))$ steps in $\mathcal{G}_\ell(\overline{\mathbb{F}_{p^2}})$ with probability between $1/2n$ and $3/2n$ (which is indeed close to $1/n$ for large values of p). Thus, the combination of (extended) Bröker's algorithm and random walks solves the SRS problem.

Non-minimal output Unfortunately, combining the (extended) Bröker's algorithm with random walks does not solve the cSRS problem. This is a corollary of Proposition II.2.7.

Corollary II.2.8. *Let* A *be the algorithm that performs random walks starting from an output of Algorithm 3 (on input* M *polynomial in the* $\log(p)$*). Then* $\textsc{EndRing}_{\mathsf{A}}$ *can be solved in polynomial time in the* $\log(p)$*. In particular,* A *is not a supersingular random crypto-sampler.*

Proof. The argument is the same as in Remark II.2.2: once $\mathrm{End}(E)$ and an ℓ-isogeny $E \to E'$ are known, $\mathrm{End}(E')$ can be computed efficiently by Theorem II.1.1. □

Exponential-time algorithms

Here we present two alternative approaches to solve the cSRS problem, based on classic results: exhaustive search via Schoof's algorithm and computation of Hasse invariants. Within this section, we will also explain why the computational cost of these two methods is exponential in $\log(p)$.

Exhaustive search There exist efficient algorithms to check whether a given elliptic curve E over $\mathbb{F}_{p^2}$ is supersingular or not. One of them computes the number of $\mathbb{F}_{p^2}$-rational points of E via Schoof's algorithm [Sch85, § 3] and checks if it equals 1 modulo p (in the light of Theorem I.5.1.d). Therefore, it is natural to ask if an algorithm to solve the cSRS problem might be as simple as an exhaustive search, i.e. sampling random elements in $\mathbb{F}_{p^2}$ until a supersingular j-invariant is found.

Unfortunately, exhaustive search over $\mathbb{F}_{p^2}$ is unfeasible because supersingular j-invariants are 'rare', about 1 out of p elements of $\mathbb{F}_{p^2}$ is a supersingular j-invariant, as we are going to review in Corollary II.2.15.

One might wonder if the probability of finding a supersingular j-invariant increases when the sample space is restricted to the smaller set $\mathbb{F}_p$. The following estimate suggests that this is true, even though the probability of success is still negligible:

Theorem II.2.9. *There are $O(\sqrt{p}\log p)$ supersingular j-invariants over $\mathbb{F}_p$.*

Proof. See [DG16, pp. 2–3]. □

Therefore, a random element in $\mathbb{F}_p$ is a supersingular j-invariant with probability about $\log p/\sqrt{p}$. This rules out exhaustive search over both $\mathbb{F}_{p^2}$ and $\mathbb{F}_p$ as a solution for the cSRS problem.

Hasse invariant Let $\mathbb{F}_q$ be a finite field of odd characteristic p. Hasse [Has35] defines a polynomial $A_q \in \mathbb{F}_q[g_2, g_3]$, such that $A_q(\tilde{g}_2, \tilde{g}_3) = 0$ if and only if the elliptic curve over $\mathbb{F}_q$ of equation

$$y^2 = 4x^3 - \tilde{g}_2 x - \tilde{g}_3$$

is supersingular. Below, we generalize Hasse's characterization of supersingular elliptic curves to other models of elliptic curves.

Consider an elliptic curve E over $\mathbb{F}_q$ given by an equation

$$E\colon y^2 = f(x),$$

where $f(x)$ is a polynomial of degree 3 or 4 as in Table I.1. For any $k > 0$, define

$$A_{p^k} = \text{coefficient of } x^{p^k-1} \text{ in } f(x)^{(p^k-1)/2}.$$

In particular, we call A_p the *Hasse invariant* of E.

The case in which $f(x)$ has degree 3 is considered in [Sil09, Thm. V.4.1.a]. For use in Section II.2.3, we prove here an extension of that case to the polynomials f in Table I.1.

Theorem II.2.10. *Consider a finite field $\mathbb{F}_q$ of odd characteristic p and an elliptic curve E over $\mathbb{F}_q$ given by an equation*

$$E\colon y^2 = f(x),$$

where $f(x)$ is a separable polynomial of degree 3 or 4 as in Table I.1. Then E is supersingular if and only if its Hasse invariant equals 0.

Proof. Since the case $\deg(f) = 3$ is already covered in Silverman's proof, we assume that E is in Jacobi form.
First of all, we count the $\mathbb{F}_q$-rational points of E. [BJ03, § 3] shows that the points of E are in one-to-one correspondence with non-zero triplets $(X : Y : Z)_{[1,2,1]}$ which satisfy

$$Y^2 = \epsilon X^4 - 2\delta X^2 Z^2 + Z^4, \tag{13}$$

where $(X : Y : Z)_{[1,2,1]}$, or simply $(X : Y : Z)$, denotes *weighted projective coordinates* defined by the equivalence relation

$$(X : Y : Z) = (X' : Y' : Z') \quad \Longleftrightarrow \quad \exists\, k \in \overline{\mathbb{F}_p}^{\times} \text{ such that } \begin{cases} X' = kX, \\ Y' = k^2 Y, \\ Z' = kZ. \end{cases} \tag{14}$$

The affine points of E are the image of the bijection

$$\begin{aligned} \{(X : Y : Z)_{[1,2,1]} \mid Z \neq 0\} &\to \mathbb{A}^2(\overline{\mathbb{F}_p}) \\ (X : Y : 1) &\mapsto (X, Y), \end{aligned}$$

that is, they are the solutions of the affine equation $y^2 = \epsilon x^4 - 2\delta x^2 + 1$. In particular, if we let $\chi\colon \mathbb{F}_q^{\times} \to \{-1, 0, 1\}$ be the map such that

$$\chi(z) = \begin{cases} -1 & \text{if } z \text{ is not a square,} \\ 0 & \text{if } z = 0, \\ 1 & \text{if } z \text{ is a non-zero square,} \end{cases}$$

we have

$$\#\big(E(\mathbb{F}_q) \cap \mathbb{A}^2(\mathbb{F}_q)\big) = \sum_{x \in \mathbb{F}_q} \big(1 + \chi\big(f(x)\big)\big) = q + \sum_{x \in \mathbb{F}_q} \chi\big(f(x)\big).$$

The 'points at infinity' of E, on the other hand, are triplets $(X : Y : 0)$ satisfying (13). Notice that X and Y must be non-zero since $\epsilon \neq 0$, so that the equation $Y^2 = \epsilon X^4$ yields two $\mathbb{F}_q$-rational points if ϵ is a square, zero points otherwise. In conclusion,

$$\#\big(E(\mathbb{F}_q)\big) = 1 + \chi(\epsilon) + q + \sum_{x \in \mathbb{F}_q} \chi\big(f(x)\big). \tag{15}$$

Since $\mathbb{F}_q^\times$ is cyclic of order $q-1$, the equality

$$\chi(z) = z^{\frac{q-1}{2}}$$

holds for every $z \in \mathbb{F}_q$. In particular, (15) becomes

$$\#E(\mathbb{F}_q) = 1 + \epsilon^{\frac{q-1}{2}} + q + \sum_{x \in \mathbb{F}_q} \big(f(x)\big)^{\frac{q-1}{2}}.$$

We stress that, if we represent equivalence classes modulo p by integers in $\{-(p-1)/2, \ldots, (p-1)/2\}$, then $\epsilon^{\frac{q-1}{2}}, (f(x))^{\frac{q-1}{2}} \in \{-1, 0, 1\}$ and the latter equation holds in $\mathbb{Z}$.

Furthermore, one can prove the following equality [Was08, Lem. 4.35] for every $i \in \mathbb{N}$:

$$\sum_{x \in \mathbb{F}_q} x^i = \begin{cases} -1 & \text{if } q-1 \mid i, \\ 0 & \text{if } q-1 \nmid i. \end{cases}$$

As a consequence, since $f(x)$ has degree 4, the only non-zero terms in $\sum_{x \in \mathbb{F}_q} f(x)^{(q-1)/2}$ are (up to the sign) the coefficients of x^{q-1} and $x^{2(q-1)}$ in $f(x)^{(q-1)/2}$. Namely, the coefficient of x^{q-1} is A_q by definition, while the coefficient of $x^{2(q-1)}$ is the leading coefficient of $f(x)^{(q-1)/2}$, which is $\epsilon^{\frac{q-1}{2}}$. Then we have

$$\#E(\mathbb{F}_q) \equiv 1 + \epsilon^{\frac{q-1}{2}} - \epsilon^{\frac{q-1}{2}} - A_q \equiv 1 - A_q \mod p.$$

Moreover, from [Sil09, Theorem V.2.3.1] we know that

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

where a is the trace of the q-th power Frobenius endomorphism. By Theorem I.5.1.d we can therefore conclude

$$E \text{ is supersingular} \iff a \equiv 0 \mod p \iff A_q = 0.$$

The implication $A_q = 0 \iff A_p = 0$ follows by induction from the relation

$$A_{p^{r+1}} = A_{p^r} A_p^{p^r},$$

which can be proven exactly as in the cubic case (see [Was08, Lemma 4.36]). □

The explicit formula for the Hasse invariant of a generic elliptic curve in Legendre form is a classical result. Seen as a polynomial in the variable λ, the Hasse invariant can be exploited to find supersingular elliptic curves by determining its roots.

Proposition II.2.11. *Let $y^2 = x(x-1)(x-\lambda)$ be the equation defining an elliptic curve in Legendre form. Then*

$$A_p = (-1)^m \sum_{i=0}^{m} \binom{m}{i}^2 \lambda^i,$$

where $m = (p-1)/2$.

Proof. See [Deu41, p. 201; Was08, Thm. 4.34; Sil09, Thm. V.4.1.b]. □

As a polynomial in the variable λ, A_p has the following coefficients (considered modulo p)[1]

$$c_i = \frac{(m!)^2}{(i!)^2\big((m-i)!\big)^2} \qquad \text{for } i = 0, \ldots, m.$$

It is easy to see that they can be computed recursively, starting from $c_0 = 1$, via the following formula:

$$c_{i+1} = c_i \cdot \frac{(m-i)^2}{(i+1)^2}.$$

In particular, since no coefficient is zero, A_p is far from being sparse and therefore very impractical to store. In terms of computational complexity, computing the zeroes of A_p appears to be worse than an exhaustive search of supersingular j-invariants over $\mathbb{F}_{p^2}$ (described in Section II.2.2). We will say more on this subject in Section II.2.3.

II.2.3 Hasse invariant of other models of elliptic curves

It is natural to wonder whether the Hasse invariant for a generic elliptic curve in a model other than the Legendre one can lead to a sparser polynomial for which computing roots is *efficient*.

In this section, the Hasse invariant A_p (defined in Section II.2.2) is explicitly computed for a generic elliptic curve in Weierstrass, Montgomery, and Jacobi form. Namely, for each model, we construct A_p as a (bivariate or univariate) polynomial whose coefficients lie in $\mathbb{F}_q$, and whose roots are coefficients of supersingular elliptic curves over (some extension of) $\mathbb{F}_q$.

We make use of the same notation as in Section II.2.2, i.e.

$$m = \frac{p-1}{2}$$

where $p \geq 5$ is a prime.

[1] The factor $(-1)^m$ can be neglected since we are interested in the zeroes of A_p.

Weierstrass model

Consider the family of elliptic curves over $\mathbb{F}_q$ in Weierstrass form, i.e. the curves of equation $y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{F}_q$. Thus, the Hasse invariant A_p for a generic curve in this family can be regarded as a polynomial in $\mathbb{F}_q[A, B]$.

Proposition II.2.12. *The Hasse invariant of an elliptic curve $E\colon y^2 = x^3 + Ax + B$, over $\mathbb{F}_q$ and in Weierstrass form, is*

$$A_p = \sum_{i=\lceil \frac{p-1}{4} \rceil}^{\lfloor \frac{p-1}{3} \rfloor} \binom{m}{i} \binom{m-i}{2m-3i} A^{2m-3i} B^{2i-m}. \tag{16}$$

Proof. Write

$$\begin{aligned}(x^3 + Ax + B)^m &= \sum_{i=0}^{m} \binom{m}{i} x^{3i} (Ax + B)^{m-i} \\ &= \sum_{i=0}^{m} \binom{m}{i} x^{3i} \left(\sum_{j=0}^{m-i} \binom{m-i}{j} (Ax)^j B^{m-i-j} \right).\end{aligned}$$

In each term, the degree of x equals $p-1$ if and only if $j = p - 1 - 3i$. Therefore

$$A_p = \sum_{i=\lceil \frac{p-1}{4} \rceil}^{\lfloor \frac{p-1}{3} \rfloor} \binom{m}{i} \binom{m-i}{2m-3i} A^{2m-3i} B^{2i-m}.$$

□

To find supersingular elliptic curves over $\mathbb{F}_{p^2}$, we wonder which values of $A, B \in \mathbb{F}_{p^2}$ are roots of A_p. The cases $A = 0$ or $B = 0$ yield elliptic curves with j-invariant 0 or 1728, for which the following result holds [Sil09, Thm. V.4.1.c; Was08, Prop. 3.37, Cor. 4.40]:

$$\begin{aligned} E \text{ with } j\text{-invariant } 0 \text{ is supersingular} &\iff p \equiv 2 \mod 3, \\ E \text{ with } j\text{-invariant } 1728 \text{ is supersingular} &\iff p \equiv 3 \mod 4. \end{aligned}$$

A and B may therefore be regarded as elements in the multiplicative group $\mathbb{F}_{p^2}^\times$. Namely, we can express A and B as powers of some primitive element $g \in \mathbb{F}_{p^2}^\times$, say

$$A = g^k, \qquad B = g^\ell \qquad \text{with } k, \ell \in \{0, \dots, p^2 - 2\}.$$

Thus we can rewrite A_p as follows:

$$\begin{aligned} A_p &= \sum_{i=\lceil \frac{p-1}{4} \rceil}^{\lfloor \frac{p-1}{3} \rfloor} \binom{m}{i} \binom{m-i}{2m-3i} g^{k(2m-3i)} g^{\ell(2i-m)} \\ &= \sum_{i=\lceil \frac{p-1}{4} \rceil}^{\lfloor \frac{p-1}{3} \rfloor} \binom{m}{i} \binom{m-i}{2m-3i} g^{m(2k-\ell)+i(2\ell-3k)} \end{aligned}$$

To find the coefficients A, B defining supersingular elliptic curves, it is necessary to look for values of k, ℓ such that the latter expression is zero. Moreover, by multiplying the expression by the inverse of $g^{m(2k-\ell)}$, it is enough to consider

$$\sum_{i=\lceil \frac{p-1}{4} \rceil}^{\lfloor \frac{p-1}{3} \rfloor} \binom{m}{i} \binom{m-i}{2m-3i} g^{i(2\ell-3k)}. \tag{17}$$

Notice that (17) can be seen as a polynomial over $\mathbb{F}_p$ in the variable $g^{2\ell-3k}$.

Lemma II.2.13. *Let n be a positive integer and fix $C \in \mathbb{Z}/(p^n-1)\mathbb{Z}$. Then*

$$2L - 3K \equiv C \mod p^n - 1 \tag{18}$$

has $p^n - 1$ solutions in L and K.

Proof. Observe that

- if $k \equiv C \mod 2$, the following pairs
$$\left(k, \frac{3k+C}{2}\right) \qquad \text{and} \qquad \left(k, \frac{3k+C}{2} + \frac{p^n-1}{2}\right)$$
are distinct solutions of (18);
- if $k \not\equiv C \mod 2$, there is no $\ell \in \mathbb{Z}/(p^n-1)\mathbb{Z}$ such that (k, ℓ) satisfies equation (18).

Therefore, equation (18) has
$$2 \cdot \frac{p^n-1}{2} = p^n - 1$$
solutions. □

The zeroes of (17), seen as a polynomial over $\mathbb{F}_p$ in the variable $g^{2\ell-3k}$, correspond to the supersingular j-invariants over $\mathbb{F}_{p^2}$ as detailed in the following results.

Theorem II.2.14. *Let g be a primitive element of $\mathbb{F}_{p^2}$, and fix $C = 2\ell' - 3k'$ such that g^C is a root of*

$$G(X) = \sum_{i=\lceil \frac{p-1}{4} \rceil}^{\lfloor \frac{p-1}{3} \rfloor} \binom{m}{i} \binom{m-i}{2m-3i} X^i \in \mathbb{F}_p[X]. \tag{19}$$

Denote by

$$E' \colon y^2 = x^3 + A'x + B'$$

the corresponding supersingular elliptic curve having

$$A' = g^{k'}, \qquad B' = g^{\ell'}.$$

Then the elliptic curves over $\mathbb{F}_{p^2}$ and isomorphic to E' are exactly the curves of the form $y^2 = x^3 + Ax + B$ where

$$A = g^k, \qquad B = g^\ell$$

with

$$C \equiv 2\ell - 3k \mod p^2 - 1.$$

Proof. Let E be a curve over $\mathbb{F}_{p^2}$ and isomorphic to E' (over $\overline{\mathbb{F}_p}$). Therefore the coefficients of E must satisfy

$$A = u^2 A', \qquad B = u^3 B' \tag{20}$$

for some $u \in \mathbb{F}_{p^2}^\times$ [Sil09, p. 45]. Notice that there are exactly $p^2 - 1$ such curves. In terms of a given generator g of $\mathbb{F}_{p^2}^\times$, we have

$$A = g^k = u^2 g^{k'} = g^{2r+k'} \qquad \text{and} \qquad B = g^\ell = u^3 g^{\ell'} = g^{3r+\ell'}$$

for some $r \in \{0, \dots, p^2 - 2\}$. Then

$$2\ell - 3k \equiv 2(3r + \ell') - 3(2r + k') \equiv 2\ell' - 3k' \equiv C \mod (p^2 - 1).$$

Thus, letting u vary in $\mathbb{F}_{p^2}^\times$, we have $p^2 - 1$ distinct solutions for the equation in L and K

$$2L - 3K \equiv C \mod (p^2 - 1). \tag{21}$$

Lemma II.2.13 ensures that there is no other solution. □

Corollary II.2.15. *Let $G(X)$ be the polynomial defined in* (19)*. The non-zero roots of $G(X)$ are in bijection with the supersingular j-invariants in $\mathbb{F}_{p^2} \setminus \{0, 1728\}$.*

Proof. Let g be a primitive element of $\mathbb{F}_{p^2}$. We have already shown that every non-zero root g^C of $G(X)$ corresponds to some isomorphism class of supersingular elliptic curves. Namely, if

$$E\colon y^2 = x^3 + g^k x + g^\ell$$

is a representative of this class (in particular, $2k - 3\ell \equiv C \mod (p^2 - 1)$), its j-invariant is

$$\begin{aligned} j(E) &= 1728 \cdot \frac{4g^{3k}}{4g^{3k} + 27g^{2\ell}} \\ &= \frac{1728 \cdot 4}{4 + 27g^{2\ell - 3k}}. \end{aligned}$$

Therefore the correspondence

$$\begin{aligned} \{\text{non-zero roots of } G(X)\} &\leftrightarrow \{\text{supersingular } j\text{-invariants in } \mathbb{F}_{p^2} \setminus \{0, 1728\}\} \\ g^C \quad &\mapsto \quad \frac{1728 \cdot 4}{4 + 27g^C} \\ \frac{64 \cdot 4}{j} - \frac{4}{27} &\mapsfrom \quad j \end{aligned} \tag{22}$$

is one-to-one.

□

Let

$$c_i = \binom{m}{i}\binom{m-i}{2m-3i}$$

be the coefficients of $G(X)$ (equation (19)), for $i \in \left\{\lceil \frac{p-1}{4} \rceil, \ldots, \lfloor \frac{p-1}{3} \rfloor\right\}$. We have:

$$\begin{aligned} c_i &= \frac{m!}{i!(m-i)!} \cdot \frac{(m-i)!}{(2m-3i)!(2i-m)!} \\ &= \frac{m!}{i!(2m-3i)!(2i-m)!}. \end{aligned}$$

We can assume that $G(X)$ is normalized with respect to $c_{\lceil \frac{p-1}{4} \rceil}$. Therefore, starting from $c_{\lceil \frac{p-1}{4} \rceil} = 1$, every other coefficient can be computed recursively via the following formula:

$$c_{i+1} = -12 \cdot \frac{(3i+1)(3i+2)}{(4i+3)(4i+5)} \cdot c_i. \tag{23}$$

With the eventual exception of $c_{\lfloor \frac{p-1}{3} \rfloor}$, p does not appear within the factors of any c_i, and hence every coefficient of $G(X)$ is different from 0. This implies that obtaining $G(X)$ requires exponential storage in $\log(p)$.

Montgomery model

Consider the family of elliptic curves over $\mathbb{F}_q$ in Montgomery form, i.e. the curves of equation $y^2 = (x^3 + Ax^2 + x)/B$ with $A, B \in \mathbb{F}_q$, $B \neq 0$ and $A^2 \neq 4$. Thus, the Hasse invariant A_p of a generic curve in this family can be regarded as a polynomial in $\mathbb{F}_q[A, B]$.

We note that the zeroes of A_p do not depend on B, which is in accordance with the fact that j-invariants of Montgomery curves depend only on A (see Table I.1). We can therefore assume $B = 1$ and compute A_p as a polynomial in the only variable A.

Proposition II.2.16. *The Hasse invariant of an elliptic curve $E\colon y^2 = x^3 + Ax^2 + x$, over $\mathbb{F}_q$ and in Montgomery form, is*

$$A_p = \sum_{i=0}^{\lfloor \frac{m}{2} \rfloor} \underbrace{\binom{m}{i}\binom{m-i}{m-2i}}_{c_i} A^{m-2i},$$

and its coefficients can be computed recursively starting from $c_0 = 1$ via the formula

$$c_{i+1} = c_i \cdot \frac{(m-2i)(m-2i-1)}{(i+1)^2}.$$

Proof. We start by observing that

$$\begin{aligned}(x^3+Ax^2+x)^m &= x^m(x^2+Ax+1)^m \\ &= x^m \cdot \sum_{i=0}^{m} \binom{m}{i} x^{2i}(Ax+1)^{m-i} \\ &= x^m \cdot \sum_{i=0}^{m} \binom{m}{i} x^{2i} \left(\sum_{j=0}^{m-i} \binom{m-i}{j} A^j x^j \right).\end{aligned}$$

In each term, the degree of x equals $p-1$ if and only if $m+2i+j = 2m$, or, equivalently, $j = m-2i$. Therefore,

$$A_p = \sum_{i=0}^{\lfloor \frac{m}{2} \rfloor} \underbrace{\binom{m}{i}\binom{m-i}{m-2i}}_{c_i} A^{m-2i}.$$

Notice that $c_0 = 1$ is the coefficient of the leading term; the other coefficients can be computed recursively via the formula

$$c_{i+1} = c_i \cdot \frac{(m-2i)(m-2i-1)}{(i+1)^2}.$$

□

Remark II.2.17. The degrees of the terms in A_p have all the same parity. In particular, if A is a zero of A_p, also $-A$ is. This is, again, in accordance with the fact that j-invariants (and then isomorphism classes) depend only on A^2.

Splitting field of the Hasse invariant Since every supersingular j-invariant lies in $\mathbb{F}_{p^2}$ by Theorem I.5.1.b, the definition of the j-invariant for Montgomery curves (see Table I.1) suggests that the roots of A_p lie in $\mathbb{F}_{p^{12}}$. A stronger result actually holds, as we are going to show in Proposition II.2.21, whose proof requires a few lemmata. The first one is just a special case of [Was08, Ex. 4.10].

Lemma II.2.18. *Let $E\colon y^2 = x^3 + Ax + B$ be an elliptic curve in Weierstrass form over $\mathbb{F}_{p^2}$ with trace a. Then one of its twists has trace $-a$.*

Proof. Let γ be a generator for $\mathbb{F}_{p^4}^{\times}$. Define

$$u = \gamma^{\frac{p^2+1}{2}}$$

and consider the curve

$$E'\colon \quad y^2 = x^3 + u^4 Ax + u^6 B.$$

From [Sil09, p. 45] we know that

$$\begin{aligned}\varphi\colon \quad E &\to E' \\ (x,y) &\mapsto (u^2x, u^3y).\end{aligned}$$

is an isomorphism defined over $\mathbb{F}_{p^4}$ but *not* over $\mathbb{F}_{p^2}$; in other words, E' is a quadratic twist of E.
Let a' be the trace of E'. By [Sil09, Rem. V.2.6] and [Hus87, Prop. 13.1.10] we have

$$\#E(\mathbb{F}_{p^2}) = 1 + p^2 - a, \quad \#E'(\mathbb{F}_{p^2}) = 1 + p^2 - a', \quad \#E(\mathbb{F}_{p^2}) + \#E'(\mathbb{F}_{p^2}) = 2p^2 + 2.$$

The conclusion follows immediately. □

Lemma II.2.19. *Let $E\colon y^2 = x^3 + A'x + B'$ be a supersingular elliptic curve over $\mathbb{F}_{p^2}$ in Weierstrass form with j-invariant different from 0 or 1728, and denote by E' its quadratic twist. Then either $E[4] \subseteq E(\mathbb{F}_{p^2})$ or $E'[4] \subseteq E'(\mathbb{F}_{p^2})$.*

Proof. It is well-known [Sil09, Ex. 3.32, Ex. 5.10] that the number of $\mathbb{F}_{p^2}$-rational points of a supersingular elliptic curve E over $\mathbb{F}_{p^2}$ is $p^2 + 1 - a$, where

$$a \in \{0, \pm p, \pm 2p\}.$$

Furthermore, $a \in \{0, \pm p\}$ if and only if $j(E) \in \{0, 1728\}$ [AAM19, pp. 5–6]. We can therefore assume that E has trace $2p$, while its quadratic twist E' has trace $-2p$ by Lemma II.2.18.

From [Sch87, Lemma 4.8.ii] we know the structure of the $\mathbb{F}_{p^2}$-rational groups of the two curves:

$$E(\mathbb{F}_{p^2}) \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} \quad \text{and} \quad E'(\mathbb{F}_{p^2}) \cong \mathbb{Z}/(p+1)\mathbb{Z} \times \mathbb{Z}/(p+1)\mathbb{Z}.$$

In particular,

- if $p \equiv 1 \mod 4$, then $\mathbb{Z}/(p-1)\mathbb{Z}$ has a subgroup of order 4 and such subgroup must be $\mathbb{Z}/4\mathbb{Z}$. Otherwise, E would have more than 4 points of 2-torsion, contradicting [Sil09, Cor. III.6.4]. Then $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ is a subgroup of $E(\mathbb{F}_{p^2})$ (up to isomorphism). Equivalently, again from [Sil09, Cor. III.6.4], $E[4] \subseteq E(\mathbb{F}_{p^2})$.
- Similarly, if $p \equiv 3 \mod 4$, one can prove $E'[4] \subseteq E'(\mathbb{F}_{p^2})$.

□

Lemma II.2.20. *Let $E'\colon y^2 = x^3 + A'x + B'$ be an elliptic curve over $\mathbb{F}_q$. Then E' is birationally equivalent to a Montgomery curve E over $\mathbb{F}_q$ if and only if*

(i) E' has an $\mathbb{F}_q$-rational 2-torsion point $(\alpha, 0)$,

(ii) $3\alpha^2 + A' = s^2$ *for some* $s \in \mathbb{F}_q^\times$,

and the coefficients of E *are*

$$\begin{cases} A = 3\alpha s^{-1}, \\ B = s^{-1}. \end{cases}$$

Proof. See [OKS00, Prop. 4.1, 7.5]. □

Proposition II.2.21. *The Hasse invariant* A_p *for a generic elliptic curve over* $\mathbb{F}_q$ *in Montgomery form splits completely over* $\mathbb{F}_{p^2}$. *Equivalently, the coefficient* A *of any supersingular Montgomery curve lies in* $\mathbb{F}_{p^2}$.

Proof. First of all, notice that the j-invariant

$$j = \frac{256(A^2-3)^3}{A^2-4}$$

of an elliptic curve in Montgomery form $E\colon By^2 = x^3 + Ax^2 + x$ over $\mathbb{F}_{p^2}$ equals 0 if and only if A is a square root of 3. Similarly, one can check that $j(E) = 1728$ if and only if either $A = 0$ or A is a square root of $2^{-1} \cdot 9$. In both cases, A lies in $\mathbb{F}_{p^2}$.
Let E be an elliptic curve representative of supersingular j-invariant $j' \in \mathbb{F}_{p^2} \setminus \{0, 1728\}$. By Proposition I.2.3, E can be written in Weierstrass form over $\mathbb{F}_{p^2}$:

$$E\colon \quad y^2 = x^3 + A'x + B'.$$

By Lemma II.2.19 we can also assume that the 4-torsion points of E are $\mathbb{F}_{p^2}$-rational. In particular, it has the 2-torsion points $(\alpha_i, 0)$ for $i \in \{1, 2, 3\}$, with $\alpha_i \in \mathbb{F}_{p^2}^\times$ (they are non-zero, otherwise $B' = 0$ and $j = 1728$ which contradicts our assumption). Notice that B' can be written as

$$B' = -\alpha_i^3 - A'\alpha_i \tag{24}$$

for every $i \in \{1, 2, 3\}$. Such relation can be used to factor the fourth division polynomial ψ_4 (see Section II.2.4) as follows:

$$\begin{aligned} \psi_4/2y &= 2x^6 + 10A'x^4 + 40B'x^3 - 10(A')^2x^2 - 8A'B'x - 2(A')^3 - 16(B')^2 \\ &= 2x^6 - 40x^3\alpha_i^3 - 16\alpha_i^6 + 10A'x^4 - 40A'x^3\alpha_i + \\ &\quad + 8A'x\alpha_i^3 - 32A'\alpha_i^4 - 10(A')^2x^2 + 8(A')^2x\alpha_i - 16(A')^2\alpha_i^2 - 2(A')^3 \qquad (25) \\ &= -2(-x^2 + 2x\alpha_i + 2\alpha_i^2 + A')(x^4 + 2x^3\alpha_i + 6x^2\alpha_i^2 - 4x\alpha_i^3 + \\ &\quad + 4\alpha_i^4 + 6A'x^2 - 6A'x\alpha_i + 6A'\alpha_i^2 + (A')^2). \end{aligned}$$

Since ψ_4 vanishes exactly on the x-coordinates of the 4-torsion points (see Proposition II.2.27), for each i there exist two distinct values x_i and x_i' in $\mathbb{F}_{p^2}$ such that the first factor of (25) is zero, i.e.

$$-x^2 + 2x\alpha_i + 2\alpha_i^2 + A',$$

or, equivalently, satisfy

$$A' + 3\alpha_i^2 = (x - \alpha_i)^2. \tag{26}$$

Notice that $x_i - \alpha_i$ is non-zero because $x_i \neq x_i'$. The conditions (a) and (b) from Proposition II.2.20 are therefore verified, and E is birationally equivalent to elliptic curves, over $\mathbb{F}_{p^2}$ and in Montgomery form, with coefficients

$$\begin{cases} A_i = 3\alpha_i(x_i - \alpha_i)^{-1} \\ B_i = (x_i - \alpha_i)^{-1} \end{cases}$$

for every $i \in \{1, 2, 3\}$.
We claim that $A_i^2 \neq A_j^2$ for $i \neq j$. Suppose, by contradiction, $A_i^2 = A_j^2$ for some $i \neq j$. By (26) we can write

$$\begin{aligned} 9\alpha_i^2(3\alpha_i^2 + A')^{-1} &= 9\alpha_j^2(3\alpha_j^2 + A')^{-1} \\ \alpha_i^2(3\alpha_j^2 + A') &= \alpha_j^2(3\alpha_i^2 + A') \\ \alpha_i^2 &= \alpha_j^2, \end{aligned}$$

but this cannot occur. In fact, $\alpha_i \neq \alpha_j$ by construction, and the assumption $B' \neq 0$ together with (24) implies $\alpha_i \neq -\alpha_j$.
To summarize, starting from a suitable supersingular elliptic curve in Weierstrass form with j-invariant $j' \in \mathbb{F}_{p^2} \setminus \{0, 1728\}$, we have found three distinct solutions A_1^2, A_2^2, A_3^2 for the equation

$$j' = \frac{256(X-3)^3}{X-4}.$$

Since there could not be any other solution, the coefficient of x^2 of an elliptic curve in Montgomery form with j-invariant j' must belong to the set $\{\pm A_i \mid i = 1, 2, 3\}$, which is contained in $\mathbb{F}_{p^2}$.

□

Jacobi Consider the family of elliptic curves over $\mathbb{F}_q$ in Jacobi form, i.e. the curves of equation $y^2 = \epsilon x^4 - 2\delta x^2 + 1$ with $\epsilon, \delta \in \mathbb{F}_q$, $\epsilon \neq 0$ and $\delta^2 \neq \epsilon$. Thus, the Hasse invariant A_p of a generic curve in the family can be regarded as a polynomial in $\mathbb{F}_q[\epsilon, \delta]$.

Proposition II.2.22. *The Hasse invariant of an elliptic curve $E\colon y^2 = \epsilon x^4 - 2\delta x^2 + 1$, over $\mathbb{F}_q$ and in Jacobi form, is*

$$A_p = \sum_{i=0}^{\lfloor \frac{m}{2} \rfloor} \underbrace{\binom{m}{i}\binom{m-i}{m-2i}}_{c_i} \epsilon^i (-2\delta)^{m-2i}$$

and its coefficients c_i can be computed recursively starting from $c_0 = 1$ via the formula

$$c_{i+1} = c_i \cdot \frac{(m-2i)(m-2i-1)}{(i+1)^2}.$$

Proof. Similar to the proof of Proposition II.2.16. In particular, notice that the coefficients are the same. □

Efficiency analysis

We have found explicit formulas to construct the Hasse invariant A_p for a generic elliptic curve in different models, in the form of a polynomial. None of them allows for an *efficient* construction of A_p. From a computational point of view, even the storage of A_p becomes problematic when p is of cryptographic size.

However, the combination of (extended) Bröker's algorithm and random walks, as described in Section II.2.2, provides an efficient method to find arbitrarily many roots of A_p. We cannot rule out that this fact, combined with the recursion formulas for the coefficients of A_p, might lead to an efficient algorithm to solve the cSRS problem. We leave the investigation for future work.

II.2.4 Torsion points

In this section, we provide two distinct characterizations of supersingular elliptic curves over finite fields in terms of torsion points.

Division polynomials

Following [Sil09, ex. 3.7; Was08, § 3.2], we introduce division polynomials, which constitute the main tool for the two characterizations. Let

$$E\colon \quad y^2 = x^3 + Ax + B$$

be an elliptic curve over a perfect field $\Bbbk$ with $\operatorname{char}\Bbbk \notin \{2,3\}$. For $m = -1, 0, 1, 2, \ldots$ we define the *division polynomials* $\psi_m \in \Bbbk[x,y]$, relative to E, as

$$\begin{aligned}
\psi_{-1} &= -1,\\
\psi_0 &= 0,\\
\psi_1 &= 1,\\
\psi_2 &= 2y,\\
\psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2,\\
\psi_4 &= 2y(2x^6 + 10Ax^4 + 40Bx^3 - 10A^2x^2 - 8ABx - 2A^3 - 16B^2),
\end{aligned}$$

and then recursively using the following relations:

$$\psi_{2n+1} = \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3 \qquad \text{for } n \geq 2, \tag{27}$$

$$\psi_{2n} = \frac{\psi_{n-1}^2\psi_n\psi_{n+2} - \psi_{n-2}\psi_n\psi_{n+1}^2}{\psi_2} \qquad \text{for } n \geq 3. \tag{28}$$

For ease of notation, for $m \geq 1$ we also define

$$\phi_m = x\psi_m^2 - \psi_{m+1}\psi_{m-1},$$
$$2\psi_2\omega_m = \psi_{m-1}^2\psi_{m+2} - \psi_{m-2}\psi_{m+1}^2$$

for $m \geq 1$.

We now review some well-known results about division polynomials, which can be proven by induction (see [Was08, Lem. 3.3, 3.5]).

Proposition II.2.23. *For each $m > 0$, the polynomial ψ_2 is an even-degree factor of*

$$\begin{cases} \psi_2\psi_m & \text{if } m \text{ is even,} \\ \psi_m & \text{if } m \text{ is odd.} \end{cases}$$

In particular, ψ_m is a polynomial for each m.

Remark II.2.24. If m is odd, ψ_m, ϕ_m and $\psi_2^{-1}\omega_m$ are polynomials in $\Bbbk[x, \psi_2^2]$; the same holds, if m is even, for $\psi_2^{-1}\psi_m$, ϕ_m and ω_m. As a consequence, when evaluating these polynomials at points of E, ψ_2^2 can be substituted with $4(x^3 + Ax + B)$, so that the variable y no longer appears. Therefore, by a slight abuse of notation, we will often identify these polynomials with their representatives in the quotient ring

$$\Bbbk[x, \psi_2^2]/(y^2 - x^3 - Ax - B) \cong \Bbbk[x].$$

Proposition II.2.25. *Consider ϕ_m and ψ_m^2 as elements in $\Bbbk[x]$. Then*

$$\phi_m(x) = x^{m^2} + \text{ terms of lower degree}$$
$$\psi_m^2(x) = m^2x^{m^2-1} + \text{ terms of lower degree.}$$

Theorem II.2.26 (Computation of $[m]P$ via division polynomials)**.** *Consider an elliptic curve $E\colon y^2 = x^3 + Ax + B$ over $\Bbbk$, a point $P = (x_0, y_0) \in E(\overline{\Bbbk}) \setminus \{O\}$ and a positive integer m such that $[m]P \neq O$. Then, the point $[m]P$ can be calculated as follows:*

$$[m]P = \left(\frac{\phi_m}{\psi_m^2}, \frac{\omega_m}{\psi_m^3}\right) \tag{29}$$

or, equivalently,

$$[m]P = \left(x_0 - \frac{\psi_{m-1}\psi_{m+1}}{\psi_m^2}, \frac{\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2}{4y_0\psi_m^3}\right)$$

where we denote by ϕ_m, ψ_m e ω_m the evaluations $\phi_m(x_0, y_0)$, $\psi_m(x_0, y_0)$ and $\omega_m(x_0, y_0)$, respectively.

Proof. See [Was08, §9.5]. □

Proposition II.2.27 (Characterization of $E[m]$ via division polynomials)**.** *Let $E\colon y^2 = x^3 + Ax + B$ be an elliptic curve over $\Bbbk$. Then*

$$E[m] = \{O\} \cup \{(x_0, y_0) \in E(\overline{\Bbbk}) \mid \psi_m(x_0, y_0) = 0\}.$$

Proof. See [CR88, Prop. 9.10]. □

p-torsion points

Theorem I.5.1 ensures that an elliptic curve E over a field of characteristic p is supersingular if and only if $E[p^r] = \{O\}$ for some $r \geq 1$. As in Section II.2.2 and Section II.2.3, in this section we construct a polynomial whose zeroes are exactly the pairs of coefficients A and B defining supersingular elliptic curves in Weierstrass form. In this case, though, the *coefficients* of the considered polynomial lie in a much larger set, namely $\mathbb{F}_p[X]$.

Since any non-constant polynomial over $\mathbb{F}_p$ has its zeroes in $\overline{\mathbb{F}_p}$, Proposition II.2.27 allows us to rephrase the characterization given in Theorem I.5.1.(a1) as follows:

Proposition II.2.28. *Let $E\colon y^2 = x^3 + Ax + B$ be an elliptic curve over a field $\mathbb{F}_q$ of characteristic p. Then E is supersingular if and only if $\psi_{p^r}(x)$ is constant for some $r \geq 1$.*

A refinement of the above result, which we state below in a more general fashion, is given in [Dol18, Lem. 4].

Proposition II.2.29. *Let $E\colon y^2 = x^3 + Ax + B$ be a elliptic curve over $\mathbb{F}_{p^2}$. Then E is supersingular if and only if the polynomial*

$$\psi_{p^r} \quad \textit{with } r = \begin{cases} 1 & \textit{if } \operatorname{tr}(E) = \pm 2p \\ 2 & \textit{if } \operatorname{tr}(E) = 0 \\ 3 & \textit{if } \operatorname{tr}(E) = \pm p \end{cases}$$

is either 1 or -1 in $\mathbb{F}_p[x]$.

Proof. Suppose that E is supersingular (the other implication is a trivial consequence of Proposition II.2.28). Doliskani's proof covers the case $\operatorname{tr}(E) = \pm 2p$, but it can be easily extended to the other cases, as follows. The characteristic polynomial of the Frobenius endomorphism φ_{p^2} of a supersingular elliptic curve E over $\mathbb{F}_{p^2}$ is

$$\begin{cases} X^2 \mp 2pX + p^2 & \text{if } \operatorname{tr}(E) = \pm 2p \\ X^2 + p^2 & \text{if } \operatorname{tr}(E) = 0 \\ X^2 \mp pX + p^2 & \text{if } \operatorname{tr}(E) = \pm p. \end{cases}$$

As a consequence, a suitable r-th power of φ_{p^2} equals $\pm[p^r]$, namely

$$\begin{cases} \varphi_{p^2} = \pm[p] & \text{if } \operatorname{tr}(E) = \pm 2p \\ \varphi_{p^2}^2 = -[p^2] & \text{if } \operatorname{tr}(E) = 0 \\ \varphi_{p^2}^3 = \mp[p^3] & \text{if } \operatorname{tr}(E) = \pm p. \end{cases}$$

Suppose $\mathrm{tr}(E) = -p$. From the latter equations, we can write

$$[p^3](x, y) = \left(x^{p^6}, y^{p^6}\right) \tag{30}$$

for every $(x, y) \in E$, while from equation (29) and Proposition II.2.25 we obtain

$$[p^3](x, y) = \left(\frac{\phi_{p^3}}{\psi_{p^3}^2}, \frac{\omega_{p^3}}{\psi_{p^3}^3}\right) = \left(\frac{x^{p^6} + \text{terms of lower degree}}{p^6 x^{p^6-1} + \text{terms of lower degree}}, \frac{\omega_{p^3}}{\psi_{p^3}^3}\right). \tag{31}$$

Comparing the first coordinates on the right-hand sides of (30) and (31) yields $\psi_{p^3}^2 = 1$. The other cases can be proven similarly. □

Proposition II.2.29 suggests the following strategy to sample supersingular elliptic curves:

- consider ψ_p for a generic elliptic curve over a field of characteristic p, i.e. $\psi_p \in \mathbb{F}_p[A, B, x]$;
- find pairs (A, B) such that $\psi_p^2 - 1$ is zero. Such pairs are coefficients of supersingular elliptic curves.

Some further assumptions can be made to diminish the number of monomials in ψ_p:

- restrict the root finding to $A, B \in \mathbb{F}_p$;
- assume $B = -1 - A$.

Equivalently, we consider $\psi_p^2 - 1$ as an element of the quotient ring $\mathbb{F}_p[A, B, x]/J$, where $J = (A + B + 1, A^{p-1} - 1)$. The second assumption is without loss of generality since every $\mathbb{F}_{p^2}$-isomorphism class of supersingular elliptic curves over $\mathbb{F}_p$ contains at least one curve such that $B = -1 - A$.

Proposition II.2.30. *For each supersingular j-invariant $j \in \mathbb{F}_p$ there is at least one elliptic curve in Weierstrass form that has j-invariant j, is defined over $\mathbb{F}_p$ and passes through $(1, 0)$.*

Proof. If $j = 1728$, the elliptic curve of equation $y^2 = x^3 - x$ has j-invariant 1728 and passes through $(1, 0)$. Assume $j \neq 1728$ and let $E\colon y^2 = x^3 + A'x + B'$ be an elliptic curve, over $\mathbb{F}_p$ and in Weierstrass form, of j-invariant j (it is by Proposition I.2.3.b that we can assume E is defined over $\mathbb{F}_p$). Combining Theorem I.5.1.d and Hasse's inequality

$$|p + 1 - \#E(\mathbb{F}_p)| \leq 2\sqrt{p}$$

(see [Was08, Thm. 4.2]), we know that any supersingular curve over $\mathbb{F}_p$ has exactly $p+1$ rational points; in particular, $\#E(\mathbb{F}_p)$ is even. Therefore, as O is one of the rational points, and every rational point (x, y) yields another point $(x, -y)$, every supersingular

curve over $\mathbb{F}_p$ must intersect the horizontal axis an odd number of times. Let $(x_0, 0)$ be any point in the intersection of the horizontal axis with E. Since $j \neq 1728$, x_0 must be non-zero. Let $u \in \mathbb{F}_{p^2}^{\times}$ be a square root of ${x_0}^{-1}$. Then [Sil09, p. 45] the curve defined by the coefficients

$$A = u^4 A', \qquad B = u^6 B'$$

is isomorphic over $\mathbb{F}_{p^2}$ to E and passes through $(1, 0)$ because we have

$$\begin{aligned} 1 + A + B &= 1 + \frac{A'}{{x_0}^2} + \frac{B'}{{x_0}^3} \\ &= \frac{1}{{x_0}^3}({x_0}^3 + A' x_0 + B') \\ &= 0. \end{aligned}$$

□

Efficiency analysis Even with the addition of extra assumptions on A and B, the computation of $\psi_{p^2} - 1$ remains unfeasible. The main obstacles are the recursive definition of division polynomials and their quickly increasing degrees. Therefore, determining the coefficients of supersingular elliptic curves as roots of $\psi_{p^2} - 1$ seems an impractical method to solve the cSRS problem, despite the theoretical interest of Proposition II.2.29.

Small-torsion points

In this section, we sketch a new method for sampling supersingular elliptic curves over $\mathbb{F}_p$, under the assumption that $p + 1$ has 'many' small factors.

Proposition II.2.31. *Let $p = \prod_{i=1}^{r} \ell_i^{e_i} - 1$ be a prime such that*

$$\prod_{i=1}^{r} \ell_i > 2\sqrt{p}, \tag{32}$$

and denote by r' the minimum integer in $\{1, \ldots, r\}$ satisfying (32). An elliptic curve $E\colon y^2 = x^3 + Ax + B$, over $\mathbb{F}_p$ and in Weierstrass form, is supersingular if and only if the division polynomial $\psi_{\ell_i}(x, y)$ relative to E has a root $(x_i, y_i) \in E(\mathbb{F}_p)$ for each $i \in \{1, \ldots, r'\}$.

Proof. Suppose that E is supersingular. As observed in the proof of Proposition II.2.30, the subgroup $E(\mathbb{F}_p)$ has $p + 1$ elements. In particular, for any prime ℓ_i dividing $p + 1$, Cauchy's theorem ensures that there exists a subgroup of $E(\mathbb{F}_p)$ having order ℓ_i. Equivalently, there exists an $\mathbb{F}_p$-rational ℓ_i-torsion point (x_i, y_i) of E. Such point is a zero for ψ_{ℓ_i} by Proposition II.2.27.

For the converse, the bound (32) is needed. Suppose that there exists an $\mathbb{F}_p$-rational ℓ_i-torsion point of E, and then ℓ_i divides $\#E(\mathbb{F}_p)$, for each $i \in \{1, \dots, r'\}$. Equivalently, by the Chinese Remainder Theorem,

$$\#E(\mathbb{F}_p) \equiv 0 \mod \prod_{i=1}^{r} \ell_i. \tag{33}$$

Moreover, $\#E(\mathbb{F}_p)$ must satisfy Hasse's inequality

$$|p + 1 - \#E(\mathbb{F}_p)| \leq 2\sqrt{p}. \tag{34}$$

Since $\prod_{i=1}^{r'} \ell_i > 2\sqrt{p}$, it is easy to check that the only way for (33) and (34) to both hold is for $\#E(\mathbb{F}_p) = p + 1$. Therefore, E is supersingular by Theorem I.5.1.d. □

Remark II.2.32. Some of the primes used in cryptographic applications do satisfy the hypotheses of Proposition II.2.31. For example, the prime p in CSIDH-512 [Cas+18c, § 8.1] is $p = 4 \cdot 587 \cdot \ell_1 \cdots \ell_{73} - 1$ where $\ell_1, \dots, \ell_{73}$ are the first 73 odd primes.

The characterization of supersingular elliptic curves given by Proposition II.2.31 provides a method to sample supersingular elliptic curves. In particular, given a prime $p = \prod_{i=1}^{r} \ell_i^{e_i} - 1$ such that (32) is satisfied for some (minimal) $r' \leq r$, then any solution of the system of equations

$$\begin{cases} \psi_{\ell_i}(A, B, x_i, y_i) = 0 & \text{for each } i \in \{1, \dots r'\} \\ y_i^2 - x_i^3 - Ax_i - B = 0 & \text{for each } i \in \{1, \dots r'\} \\ x_i^p - x_i = 0 & \text{for each } i \in \{1, \dots r'\} \\ y_i^p - y_i = 0 & \text{for each } i \in \{1, \dots r'\} \\ A^p - A = 0 \\ B^p - B = 0 \end{cases} \tag{35}$$

yields the coefficients A, B of a supersingular elliptic curve $E\colon y^2 = x^3 + Ax + B$ over $\mathbb{F}_p$, together with the coordinates of $\mathbb{F}_p$-rational ℓ_i-torsion points (x_i, y_i) for $i \in \{1, \dots, r'\}$.

Efficiency analysis The polynomials involved in system (35) have either low degree or sparse coefficients. A naive use of Groebner bases or other polynomial-system solvers, though, is far from enough to turn this method into an efficient algorithm to solve the cSRS problem, due to the exponential size of the set of solutions of system (35). We leave any improvement of this technique for future work.

II.3 Comparing M-small supersingular elliptic curves

One of the takeaway messages in this chapter is that supersingular elliptic curves with small non-trivial endomorphisms should be in general avoided when constructing

isogeny-based cryptosystems. In this section, we look at this from a different, cryptanalytic perspective. Namely, we take inspiration from Love and Boneh's work [LB20] and introduce a greedy algorithm – based on 'how small' non-trivial endomorphisms are – to navigate $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$. The algorithm works only 'on the quaternion side', which we have introduced in Section I.6.4. As far as we know, there is no efficient way to implement it on the elliptic-curve side. Its main purpose, rather than solving EndRing, is to provide a heuristic estimate of the complexity of a decisional variant of EndRing, which we will call IsMSmaller.

M-small elliptic curves Given a positive integer M, we say that an elliptic curve E (or, equivalently, its j-invariant) is *M-small* if $\mathrm{End}(E)$ contains a non-trivial endomorphism α of degree at most M. Moreover, to every elliptic curve E we associate the quantity

$$M_E = \min\{\deg(\alpha) \mid \alpha \in \mathrm{End}(E) \setminus \mathbb{Z}\},$$

which is by definition the smallest integer for which E is M-small. Since this quantity is invariant under isomorphisms of E, we may as well write M_j for a given j-invariant.

We can now state more precisely the problem that we are going to consider throughout this section.

Problem 4 (IsMSmaller)**.** *Given two supersingular j-invariants j_0 and j_1, output* 0 *if $M_{j_0} \leq M_{j_1}$, and* 1 *otherwise.*

II.3.1 Distribution of M_j: first heuristics

We will study the distribution of M_j when j ranges in the set of supersingular j-invariants over $\mathbb{F}_{p^2}$.

It is shown in [LB20, Prop. A.5] that $M_j \in \{1, 2, \ldots, \sqrt[3]{p^2}/2 + 1/4\}$. As long as we work on toy examples, we can use the same idea as in Bröker's Algorithm 2 to estimate M_j (faster than the brute-force approach of listing all isogenies of small degree): for each j, one sets $\mathcal{O}$ to be the imaginary quadratic order of smallest absolute discriminant $|-d|$ s.t. j is a root of the Hilbert class polynomial $P_\mathcal{O}$, and sets $\tilde{M}_j$ to be the minimum of the norms in $\mathcal{O}$ (i.e. $(1+d)/4$ if $d \equiv 3 \bmod 4$ and d otherwise). See Algorithm 4.

Remark II.3.1. We stress that, in general, $\tilde{M}_j \neq M_j$. Consider for example $p = 31$: the first iterations of Algorithm 4 yield $\mathcal{O}_1 = \mathbb{Z}[i]$ and $\mathcal{O}_2 = \mathbb{Z}[\sqrt{-2}]$, with Hilbert class polynomials $x - 1728$ and $x - 8000$, respectively. Thus we find that the corresponding j-invariants modulo 31, which are 23 and 2, have an endomorphism of degree 1 and an endomorphism of degree 2, respectively. However, also the remaining supersingular j-invariant, which is 4, has an endomorphism of degree 2 which is not found via the above CM-reductions. The only way to find it via CM reductions, according to [Onu21, Lemma 3.1], is to scan through orders of discriminant $p^r \cdot 2$ for $r > 0$ (in this case $r = 1$ turns out to be enough).

Algorithm 4: Supersingular j-invariants sorted by an upper-bound of M_j

Input: A prime $p \geq 5$.
Output: The list of all supersingular j-invariants, sorted by $\tilde{M}_j$.
Set $i = 1$;
Set $n =$ number of supersingular j-invariants over $\mathbb{F}_{p^2}$;
Set $L = [\,]$;
while $\#L < n$ **do**
  Set $D = i$-th negative fundamental discriminant;
  if $\left(\frac{D}{p}\right) \neq 1$ **then**
    Compute the Hilbert class polynomial $P_{\mathcal{O}}$ relative to the quadratic order $\mathcal{O}$ of discriminant D;
    foreach *root* $\alpha \in \mathbb{F}_{p^2}$ *of* $P_{\mathcal{O}}$ *modulo* p **do**
      if $(\alpha, \_) \notin L$ **then**
        Set $j = \alpha$;
        Set $M_j =$ minimum norm in $\mathcal{O}$;
        Append $(j, \tilde{M}_j)$ to L;
      end
    end
  end
  Set $i = i + 1$;
end

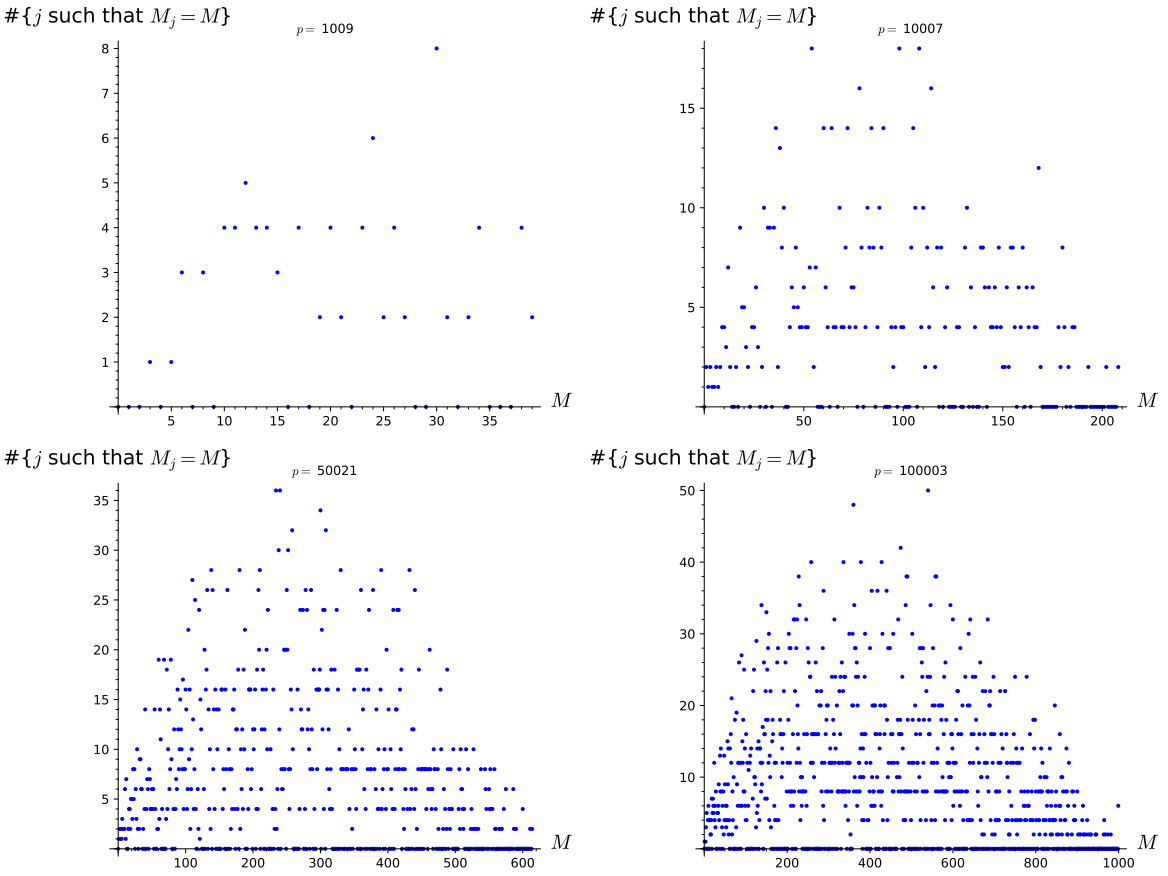

Figure II.2: The j-invariants in $\mathbb{F}_{p^2}$ counted w.r.t. the value of M_j for some small values of p.

In spite of Remark II.3.1, CM reduction still gives an effective intuition of the distribution of M_j: only few small values of M_j can appear, since they are (mostly) the roots of some small-degree Hilbert polynomials, and only few large values of M_j can appear, since the roots of large-degree Hilbert polynomials modulo $\mathfrak{P}$ are likely to be also roots of smaller-degree Hilbert polynomials.

For more precise heuristics, we move to the quaternion side: in this way, computing M_j for a given supersingular j-invariant j amounts to finding a non-trivial element of minimal norm in the maximal order whose class corresponds to j. This allowed us to compute all the values of M_j for some small values of p: see Figure II.2 for some examples.

II.3.2 Greedy algorithm for M_j

If M_j is small, we have already observed in Proposition II.2.6 that the corresponding endomorphism ring can be easily computed. Therefore, solving EndRing amounts to efficiently finding paths in $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$ which lead to small values of M_j. It is then natural to ask whether these paths could be found via a *greedy algorithm* based on the value of

M_j, i.e. an algorithm that, given a supersingular j-invariant in $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$, keeps walking on the graph by choosing the neighbor with smallest M_j at each step. This can be implemented on the quaternion side, as shown in Algorithm 5. To implement this idea on the elliptic-curve side, one would need an efficient oracle for IsMSmaller, telling which of any two elliptic curves has the non-trivial endomorphism of the smallest degree.

Algorithm 5: Greedy algorithm for M_j

Input: A prime $p \geq 5$, a prime $\ell \neq p$ and a maximal order $\mathcal{O} \subseteq B_{p,\infty}$.

Output: A list of ideals $[I_1, \ldots, I_n]$ of norm ℓ and a list of orders $[\mathcal{O}_0 = \mathcal{O}, \mathcal{O}_1, \ldots, \mathcal{O}_n]$ connected by those ideals and s.t. for $i < j$ the minimum norm in $\mathcal{O}_i \setminus \mathbb{Z}$ is smaller or equal than the minimum norm in $\mathcal{O}_j \setminus \mathbb{Z}$.

```
Set M_j = minimum of the norm in O \ Z;
Set connIdeals= [ ];
Set Orders= [O ];
Set flag = 0;
while flag = 0 do
    Enumerate maximal left ideals of norm ℓ of O;
    Set ellNeighbours= list of corresponding right orders;
    if All elements in ellNeighbours belong to Orders then
        Set flag = 1;
    end
    else
        Sort ellNeighbours by the norms of the smallest non-trivial elements;
        Set O = first element in ellNeighbours which is not in Orders;
        Append the corresponding connecting ideal to connIdeals;
        Append O to Orders;
    end
end
```

Toy examples (see Figure II.3) already suggest that optimal paths may not have strictly decreasing values of M_j.

This heuristic intuition is confirmed by the following result, which explicitly provides a large family of starting orders which make Algorithm 5 stop 'too early'.

Proposition II.3.2. *Let j_0 be a supersingular j-invariant s.t. M_{j_0} and $4M_{j_0} - 1$ are both square-free and M_{j_0} is smaller than $\sqrt{p}/(2\ell^2)$. Then none of the elliptic curves listed by (the elliptic-curve version of) Algorithm 5 on input j_0 has $M_j < M_{j_0}$.*

Proof. M_{j_0} is an element of minimal norm in some imaginary order of discriminant d, i.e. it is $(1 + d)/4$ if $d \equiv 3 \bmod 4$ and d otherwise – as already observed at the beginning of II.3.1. Our hypotheses ensure that in both cases d is square-free: in

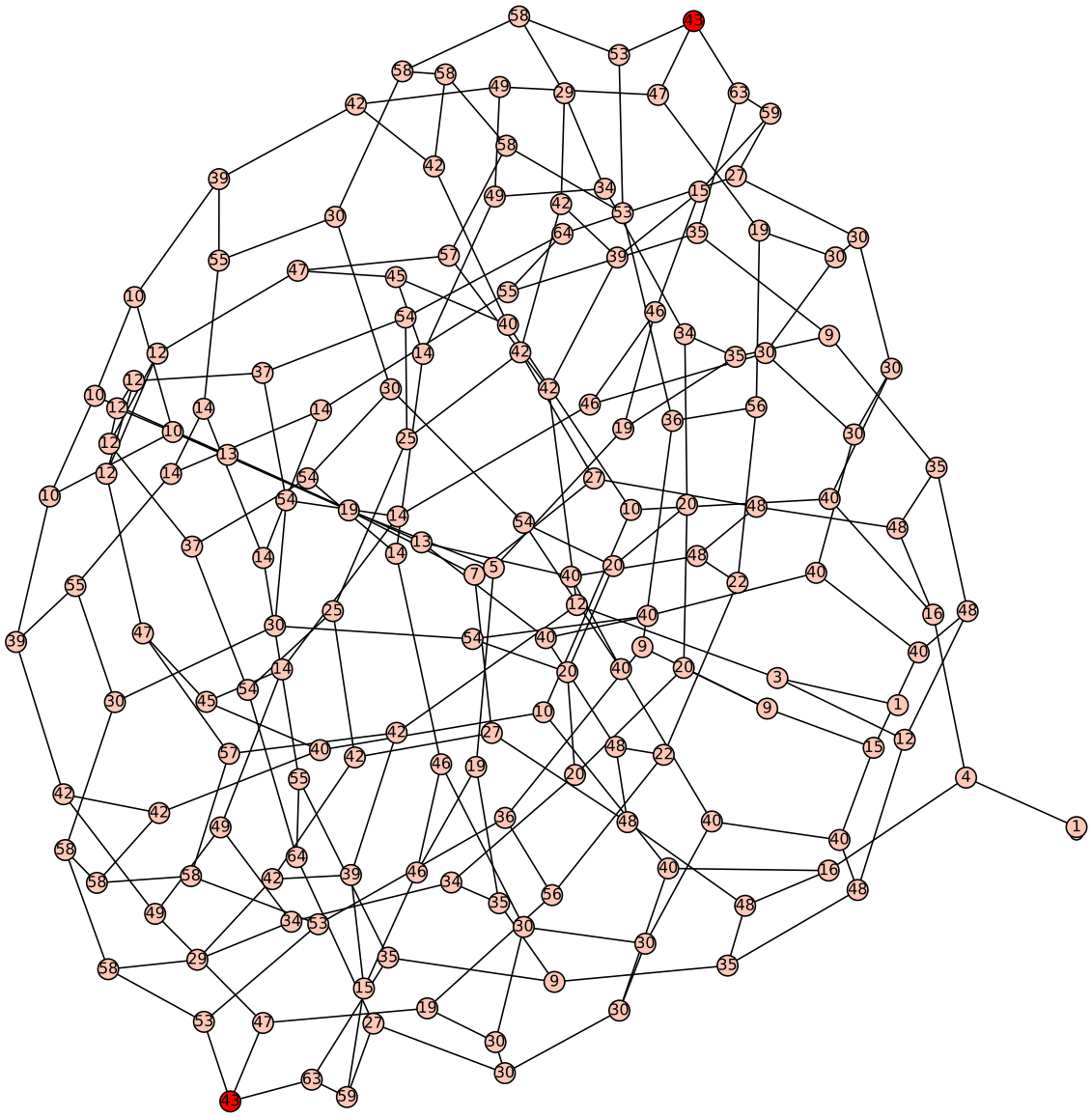

Figure II.3: $\mathcal{G}_2(\mathbb{F}_{2003})$, with vertices labelled by their M_j. The vertices labeled by 43 will cause an M_j-greedy algorithm to stop since their neighbors have $M_j \in \{47, 53, 63\}$. We remark that the symmetry of the graph comes from the Frobenius map sending j to j^p.

particular, it identifies a maximal order in $\mathbb{Q}[\sqrt{d}]$. Suppose by contradiction that there exists an isogeny of degree ℓ connecting j_0 to another supersingular j-invariant j_1 with $M_{j_1} < M_{j_0}$. Therefore, the corresponding order must lie in a different quadratic field than $\mathbb{Q}[\sqrt{d}]$. However, by [LB20, Prop. 4.5], this can only happen if $\ell^4 \geq p/(4M_{j_0}^2)$, which contradicts our assumption on M_{j_0}. □

In light of the above result, we do not expect IsMSmaller to be as hard as EndRing. On the other hand, we conjecture that being able to compute the exact value of M_j might be enough to navigate $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$ efficiently, exploiting the results in [LB20]. We leave this for future work.

Chapter III

Can pairings break CSIDH?

In this chapter we will mostly adopt a cryptanalytic perspective, based on a concern that was raised by the break of SIDH in [CD23; Mai+23; Rob23]: are CSIDH and its variants still secure? Recall that the core of the SIDH attack is as follows:

SIDH attack

Let $\varphi : E \to E'$ be an isogeny between two elliptic curves E, E' over $\mathbb{F}_q$. Suppose that

- the *n-torsion information*, i.e. the action of φ on a basis of $E[n]$, is known for a sufficiently smooth n,
- $\deg(\varphi)$ is known and coprime with n,
- $n^2 > \deg(\varphi)$.

Then φ can be recovered in polynomial time.

Since no n-torsion information is revealed and $\deg(\varphi)$ is unknown in CSIDH, it is not obvious, *a priori*, how it could be affected by the SIDH attack. Nevertheless, some variants of CSIDH do reveal some extra information on the secret isogenies involved: in particular, in Section III.1 we focus on SiGamal, a public-key encryption scheme, and show how its security would be undermined if suitable non-trivial self-pairings existed (and were efficiently computable). While this provides an example of how pairings can be used in the cryptanalysis of isogeny-based protocols (even independently from the SIDH attack), our strategy turns out to be infeasible in the case of SiGamal: the reason is thoroughly explained in Section III.2, where the existence and construction of self-pairings are discussed in a more general framework. On the other hand, we show that the combination of the SIDH attack with the construction of suitable pairings is an effective strategy to target, if not CSIDH, at least some of its variants in which $\deg(\varphi)$ is known and a 'weak' orientation is chosen.

III.1 A motivating example: SiGamal

To acquire a first intuition of how families of compatible pairings, and in particular self-pairings, can be used in cryptanalysis, we consider the SiGamal public-key encryption scheme [MOT20]. In the aftermath of the SIDH attack, SiGamal seemed an easy target since it entails revealing (masked) 2^r-torsion information. However, although the attack idea presented in this section can be seen as a special case of a more general – and in some cases effective – strategy, we anticipate that SiGamal is still unbroken, for reasons that will be made clear in Section III.2. Moreover, we stress that this attack idea does not rely on the SIDH attack.

III.1.1 Structure of the scheme

We briefly recall the structure of SiGamal.

KeyGen: Let p be a prime such that $p+1 = 2^r \ell_1 \cdots \ell_s$, where $\ell_1, \ldots, \ell_s$ are distinct odd primes. Let E_0 be the curve of equation $y^2 = x^3 + x$, and P_0 a random point in $E_0[2^r](\mathbb{F}_p)$.
Alice randomly chooses integers $(\alpha, e_1, \ldots, e_s)$, where $\alpha \in (\mathbb{Z}/2^r\mathbb{Z})^\times$, sets $\mathfrak{a} = (\alpha)\mathfrak{l}^{e_1} \cdots \mathfrak{l}^{e_s}$ and computes $E_1 = [\mathfrak{a}]E_0$ and $P_1 = \mathfrak{a}P_0$. The pairs (E_0, P_0) and (E_1, P_1) are Alice's public key, while $(\alpha, e_1, \ldots, e_s)$ is her secret key.

Enc: Let μ be a plaintext of $r-2$ bits. Bob randomly chooses integers $(\beta, e'_1, \ldots, e'_s)$, where $\beta \in (\mathbb{Z}/2^r\mathbb{Z})^\times$, sets $\mathfrak{b} = (\beta)\mathfrak{l}^{e'_1} \cdots \mathfrak{l}^{e'_s}$ and computes $E_2 = [\mathfrak{b}]E_0$, $P_2 = \mathfrak{b}P_0$, $E_3 = [\mathfrak{b}]E_1$ and $P_3 = \mathfrak{b}(2\mu+1)P_1$. The ciphertext is (E_2, P_2, E_3, P_3).

Dec: Alice computes $P'_3 = \mathfrak{a}P_2$ and solves the discrete logarithm problem over $\mathbb{Z}/2^r\mathbb{Z}$ for P'_3, P_3. The solution is then easily converted to the original plaintext μ.

We stress that the main differences between this scheme, summarized in Figure III.1, and CSIDH are that a large power of 2, namely 2^r, is required to divide $p+1$ and some masked 2^r-torsion information is revealed throughout the protocol.

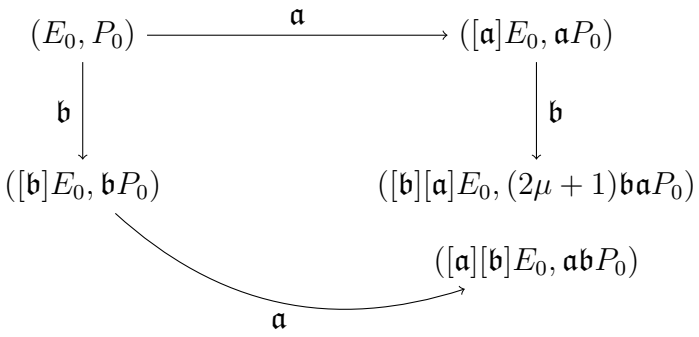

Figure III.1: The SiGamal scheme.

III.1.2 Attack strategy

In SiGamal, the hardness of the IND-CPA game – i.e., given the encryption of one out of two known plaintexts, guessing which one has been encrypted – relies on the following *ad hoc* assumption called the *P-CSSDDH assumption* [MOT20, Thm. 8]: given the curves $E_0, [\mathfrak{a}]E_0, [\mathfrak{b}]E_0, [\mathfrak{ab}]E_0$ and the points $P_0, P_1 = \varphi_{\mathfrak{a}}(P_0)$ and $P_2 = \varphi_{\mathfrak{b}}(P_0)$, no efficient algorithm can distinguish $P_3 = \varphi_{\mathfrak{ab}}(P_0)$ from a uniformly random 2^r-torsion point $P_3' \in [\mathfrak{a}][\mathfrak{b}]E_0(\mathbb{F}_p)$. If there existed non-trivial self-pairings $f_i \colon \langle P_i \rangle \to \mu_{2^s}$ for some $s > 0$, compatible with $\mathbb{F}_p$-rational isogenies of odd degree, then one could compute

$$\begin{aligned} f_1(P_1) &= f_1(\varphi_{\mathfrak{a}}(P_0)) = f_0(P_0)^{N(\mathfrak{a})} \\ f_2(P_2) &= f_2(\varphi_{\mathfrak{b}}(P_0)) = f_0(P_0)^{N(\mathfrak{b})} \\ f_3(P_3) &= f_3(\varphi_{\mathfrak{ab}}(P_0)) = f_0(P_0)^{N(\mathfrak{a})N(\mathfrak{b})}, \end{aligned}$$

where we write $f_i(P_i)$ rather than $f_i(P_i, P_i)$ for brevity. Thus, the P-CSSDDH challenge could be reduced to a decisional Diffie-Hellman problem on μ_{2^s}.

III.1.3 Construction of self-pairings: some attempts

The above attack strategy motivates the search of self-pairings of 2-smooth order. While we defer to Section III.2 a more general framework for the construction of self-pairings, here we focus on how classic pairings fail to provide the non-trivial self-pairings we would need to break SiGamal.

Tate pairings

Since the Weil pairing is alternating, it is always trivial as a self-pairing. A second natural candidate, then, is the Tate pairing. Instead of recalling its construction, we just discuss an often neglected feature, that is its dependence on the finite field considered. To clarify this, we stress that the following tower of fields comes into play when we define a Tate pairing over $E[n]$:

- $\mathbb{F}_q$, the field over which E is defined.
- $\mathbb{F}_{q^s}$, the smallest extension of $\mathbb{F}_q$ containing all n-th roots of unity μ_n (s is the *embedding degree*, i.e. the smallest integer s such that $n \mid q^s - 1$).
- $\mathbb{F}_{q^t}$, the smallest field containing the full n-torsion. One can easily prove that $s \mid t$.

Classically [BSS05, §IX.3], the Tate pairing is defined as

$$\tau_{q,n} \colon E(\mathbb{F}_{q^s})[n] \times E(\mathbb{F}_{q^s})/nE(\mathbb{F}_{q^s}) \to \mu_n$$

and it is π-invariant, where π denotes the Frobenius endomorphism over $\mathbb{F}_q$. In particular, we note that the domain of $\tau_{q,n}$ is *not* $E[n] \times E[n]$. Nevertheless, the definitions

of Section I.9 can be straightforwardly adapted. Since E is defined over any field above $\mathbb{F}_q$, we can replace $\mathbb{F}_q$ by some extension $\mathbb{F}_{q^k}$ and denote by $\tau_{q^k,n}$ the corresponding Tate pairing:

- if k divides s, the tower above $\mathbb{F}_{q^k}$ is the same as the tower above $\mathbb{F}_q$ and $\tau_{q^k,n} = \tau_{q,n}$.
- If $(k,s) = 1$, then $\mathbb{F}_{q^s}$ is replaced by $\mathbb{F}_{q^{ks}}$ in the tower of fields, and thus $\tau_{q^k,n}$ does not have the same domain and codomain as $\tau_{q,n}$. Consider the 'inclusion' map

  $$\iota\colon E(\mathbb{F}_{q^s})/nE(\mathbb{F}_{q^s}) \to E(\mathbb{F}_{q^{ks}})/nE(\mathbb{F}_{q^{ks}})$$

  (we stress that ι is not necessarily injective) and denote by κ the isomorphism from n-th roots of unity in $\mathbb{F}_{q^{ks}}$ to n-th roots of unity in $\mathbb{F}_{q^s}$. Thus we have $\tau_{q,n} = \kappa \circ \tau_{q^k,n} \circ \iota'$, where

  $$\iota'\colon E(\mathbb{F}_{q^s})[n] \times E(\mathbb{F}_{q^s})/nE(\mathbb{F}_{q^s}) \to E(\mathbb{F}_{q^{ks}})[n] \times E(\mathbb{F}_{q^{ks}})/nE(\mathbb{F}_{q^{ks}})$$

  is just the product of the natural inclusion $E(\mathbb{F}_{q^s})[n] \to E(\mathbb{F}_{q^{ks}})[n]$ and ι. Therefore,

  - if ι is injective, then $\tau_{q,n}$ can be simply seen as the restriction of $\tau_{q^k,n}$ to a smaller domain;
  - if ι is not injective, the restriction of $\tau_{q^k,n}$ to the domain of $\tau_{q,n}$ is not as fine as $\tau_{q,n}$ itself: in particular, the two pairings differ on some point in the intersection of their domains.

  The injectivity of ι strictly depends on how many extra n-torsion points E has on $\mathbb{F}_{q^{ks}}$ compared with $\mathbb{F}_{q^s}$. More precisely, we claim that ι is injective if and only if $E(\mathbb{F}_{q^{ks}})[n] = E(\mathbb{F}_{q^k})[n]$. To see that, let P be a point in $\ker(\iota)$. Then $P \in E(\mathbb{F}_{q^k})$ and there exists $Q \in E(\mathbb{F}_{q^{ks}})$ such that $nQ = P$. Therefore $(\pi^s - 1)Q$ is an n-torsion point in $E(\mathbb{F}_{q^{ks}})$. To conclude, we just observe that $(\pi^s - 1)Q$ lies in $E(\mathbb{F}_{q^s})$ if and only if Q does.

Thus we have proven that the number of distinct Tate pairings (i.e. Tate pairings disagreeing on at least one point in the intersection of their domains) on (subgroups of) $E[n]$ is upper-bounded by the number of fields between $\mathbb{F}_{q^s}$ and $\mathbb{F}_{q^t}$.

In SiGamal, the tower of fields considered above is particularly short. Namely, E is defined over $\mathbb{F}_p$ and $n = 2^r$ divides $p+1$. Therefore $E(\mathbb{F}_{p^2}) \cong \mathbb{Z}/(p+1)\mathbb{Z} \times \mathbb{Z}/(p+1)\mathbb{Z}$ [Sch87, Lem. 4.8.ii] and thus $E[n] \subset \mathbb{F}_{p^2}$. The only Tate pairings that need to be considered, then, are $\tau_{p,n}$ and $\tau_{p^2,n}$. Unfortunately, the following result from [Sch07, Thm. 3.4] seems to rule out their effectiveness for our attack.

Theorem III.1.1. *Let E be an elliptic curve defined over $\mathbb{F}_q$ and let n be an integer coprime with q. Assume that $E[n] \subset E(\mathbb{F}_q)$. Then $\tau(P,P) = 1$ for all $P \in E[n]$ if and only if there exists an integer a such that $\pi(R) = aR$ for all $R \in E[n^2]$, where π denotes the Frobenius endomorphism over $\mathbb{F}_q$.*

In SiGamal, since the Frobenius endomorphism over $\mathbb{F}_{p^2}$ satisfies $\pi = -[p]$, we conclude that $\tau_{p^2,n}(P,P)$ is trivial by the above theorem.
Regarding $\tau_{p,n}$, we have shown in the above discussion that it is essentially a restriction of $\tau_{p^2,n}$ to a smaller domain, *unless* $E[n] \subset \mathbb{F}_p$. The full n-torsion is indeed $\mathbb{F}_p$-rational if and only if $r = 1$. In fact, if $r = 1$, $\tau_{p,n}$ can be non-trivial, i.e. we might have $\tau_{p,n}(P_0, P_0) = -1$. However, this is again of no use to break the DDH problem of Section III.1.2, since $\tau_{p,n}(\varphi(P_0), \varphi(P_0))$ consequently equals -1 for any isogeny φ of odd degree starting from E_0. Since every isogeny involved in SiGamal has odd degree, $\tau_{p,n}$ cannot be exploited to distinguish DDH tuples.

Distortion maps

Having ruled out Weil and Tate, in the light of Proposition I.9.3 we might look for pairings arising from suitable distortion maps. More precisely, we are looking for a pairing that is compatible with the (unknown) isogenies $\mathfrak{a}, \mathfrak{b}$ involved in SiGamal.

Proposition III.1.2. *Let $\varphi\colon E \to E'$ be an isogeny of elliptic curves defined over $\mathbb{F}_q$, and n be a positive integer coprime with $p = \mathrm{char}\,(\mathbb{F}_q)$. Suppose that ω and ω' are endomorphisms of E and E' respectively, and assume that ω and φ have degree coprime with n. Then the pairings $T(X,Y) = e_n(X, \omega(Y))$ on $E[n]$ and $T'(X,Y) = e_n(X, \omega'(Y))$ on $E'[n]$ are compatible with φ if and only if*

$$\omega' \equiv \frac{\varphi \circ \omega \circ \hat{\varphi}}{\deg(\varphi)} \mod n. \tag{36}$$

Proof. If (36) holds, then by compatibility of Weil pairing

$$\begin{aligned} T(\varphi(P), \varphi(Q)) &= e_n(\varphi(P), \omega'(\varphi(Q))) \\ &= e_n(\varphi(P), \varphi(\omega(Q))) \\ &= e_n(P, \omega(Q))^{\deg(\varphi)} \\ &= T(P,Q)^{\deg(\varphi)} \end{aligned}$$

for any $P, Q \in E[n]$. Vice versa, if T and T' are compatible with φ then the above equalities hold for any $P, Q \in E[n]$. Therefore $\omega'(\varphi(Q)) = \varphi(\omega(Q))$ for each Q since $\varphi\colon E[n] \to E'[n]$ is by hypothesis an isomorphism and the Weil pairing is nondegenerate. □

In particular, if φ, E and E' are defined over $\mathbb{F}_p$, setting both ω and ω' to be some linear combination of Frobenius endomorphism and identity map trivially satisfies (36). However, this choice automatically results in a trivial self-pairing on $E(\mathbb{F}_p)[n]$ and is therefore not useful for our attack.

The other viable option is starting from some other endomorphism $\omega \in \mathrm{End}(E)$. This is feasible, in SiGamal, since the full endomorphism ring of E_0 is known. However, computing ω' via (36) seems impossible without knowning $\deg(\varphi)$ and, most of all, how φ acts on the full n-torsion.

Pseudo-distortion maps

While finding a suitable distortion map $\omega \in \mathrm{End}(E)$ seems out of reach, we might still settle for a *pseudo-distortion map* of the form $\omega = (\pi + a)/n$, where π denotes the Frobenius endomorphism over $\mathbb{F}_p$ (more generally: the field over which E is defined) and a is an integer. Such ω is not an endomorphism in general: still, $e_n(X, \omega(Y))$ is a well-defined pairing with domain $E(\mathbb{F}_p)[n] \times E(\mathbb{F}_p)/nE(\mathbb{F}_p)$ if and only if ω is well-defined in the sense explained by the following proposition.

Proposition III.1.3. *Let π be the Frobenius endomorphism over $\mathbb{F}_p$, and a, n two integers such that $a \in \{0, \dots, n-1\}$ and $n \mid p+1$. Then*

$$\omega = \frac{\pi + a}{n} : \quad E(\mathbb{F}_p)/nE(\mathbb{F}_p) \to E[n]$$

is well-defined if and only if $a = -1$.
When this is the case, the map $e_n(X, \omega(Y))$ is in fact the Tate pairing $\tau_{p,n}$.

Proof. Let Q be an $\mathbb{F}_p$-rational point. Let P be our 'candidate' for $\omega(Q)$, i.e. a point such that $nP = (\pi + a)(Q)$; since we are requiring that P is of n-torsion, a necessary (and also sufficient) condition for ω to be well-defined is that $\pi + a$ annihilates for any choice of Q. Equivalently,

$$\underbrace{E(\mathbb{F}_p)}_{\ker(\pi - 1)} \subset \ker(\pi + a).$$

One can check that this occurs if and only if $a = -1$ (since $a < p$ by assumption).
The last statement is a well-known fact [Sch07, Thm. 2.5]. □

Therefore, using a pseudo-distortion map of the form $(\pi + a)/n$ works only for $a = -1$, which is the same as using the Tate pairing.

Conclusion

Our so-far failed attempts to construct self-pairings to break SiGamal are an indication – not overwhelming, however – of the fact that these maps might not exist at all. This fact is indeed true, as we will prove in the next section.

III.2 Pairing-based attacks

Before going back to consider the attack on SiGamal, let us see, more generally, how pairings can be used to reconstruct a secret isogeny between two given curves.

III.2.1 Non-oriented case

We start with a remark on the non-oriented, supersingular case. Consider the following problem.

Problem 5 (IsoPairings)**.** *Given a prime p, two coprime integers d and n not divided by p and s.t. $n^2 > d$, and two uniformly-random supersingular elliptic curves E, E' over $\mathbb{F}_{p^2}$ s.t. there exists an isogeny $\varphi\colon E \to E'$ of degree d, compute two non-antisymmetric pairings, say T on $E[n]$ and T' on $E'[n]$, that are compatible with φ.*

We will soon clarify why T and T' are required to be non-antisymmetric – which, incidentally, rules out the Weil pairing.
The question we want to address is whether solving IsoPairings would be enough to recover the action of φ on the n-torsion of E (and possibly φ itself, using the SIDH attack).

To this end, suppose that n is coprime with both p and $\deg(\varphi)$. Some partial n-torsion information can be indeed obtained as follows. Choose two bases $\langle P, Q\rangle = E[n]$ and $\langle P', Q'\rangle = E'[n]$, and let M_T and $M_{T'}$ be the matrices corresponding to T and T' respectively, as in Section I.9. From the very definition of compatibility with φ, we readily deduce that a necessary condition for having $P' = \varphi(P)$ and $Q' = \varphi(Q)$ is $M_{T'} = \deg(\varphi) M_T$. If it is not, Remark I.9.1 ensures that one can perform a change of basis on $E'[n]$ so that this necessary condition is fulfilled. This change of basis does get us closer to finding $\varphi(P)$ and $\varphi(Q)$, but not quite enough: the obvious reason is that different bases might yield the same matrix $M_{T'}$. More formally, studying the number of bases yielding the same $M_{T'}$ amounts to studying the cardinality of the *stabilizer* of $M_{T'}$ w.r.t. the action τ from Remark I.9.1, defined as

$$\mathrm{Stab}(M_{T'}) = \{A \in \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \mid A^t M_{T'} A = M_{T'}\}.$$

It is immediate to see that $\mathrm{Stab}(M_{T'}) \subseteq O(2, \mathbb{Z}/n\mathbb{Z})$, where the latter denotes the orthogonal group of 2 by 2 matrices over $\mathbb{Z}/n\mathbb{Z}$. In particular, as a consequence of Remark I.9.1, equality holds in the case of the Weil pairing, i.e. when $M_{T'} = W$ (defined in (9)). This is the reason why we ruled it out from the definition of IsoPairings.
Thus, a natural question is whether there exist pairings with 'small' stabilizers. The answer is, unfortunately, negative.

Proposition III.2.1. *Let n be an odd integer. Let M be any matrix in $M_2(\mathbb{Z}/n\mathbb{Z})$ and consider the action of $A \in \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ given by $A^t M A$. Then $\#\mathrm{Stab}(M) \geq \phi(n)$, where ϕ is Euler's function.*

Proof. Write

$$M = \begin{pmatrix} x & y \\ w & z \end{pmatrix} \qquad \text{and} \qquad A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Setting $A^tMA = M$ yields a system of four equations which are quadratic in a, b, c, d and linear in x, y, w, z:

$$\begin{cases} xa^2 + (y+w)\,ac + zc^2 - x = 0 \\ xab + yad + wbc + zcd - y = 0 \\ xab + wad + ybc + zcd - w = 0 \\ xb^2 + (y+w)\,bd + zd^2 - z = 0. \end{cases} \tag{37}$$

Write $n = \prod_{j=1}^{e} p_j^{k_j}$, with p_j odd primes. If (a_j, b_j, c_j, d_j) is a solution of (37) modulo $p_j^{k_j}$ for every j, by the Chinese Remainder Theorem such sets of solutions corresponds to a unique solution of (37) modulo n. Since ϕ is multiplicative with respect to its coprime factors, it is enough to prove the statement under the assumption that n is a prime power p^k.
We consider first the case $x = z = 0$, in which (37) becomes

$$\begin{cases} (y+w)\,ac = 0 \\ yad + wbc - y = 0 \\ wad + ybc - w = 0 \\ (y+w)\,bd = 0. \end{cases}$$

It is then immediate to check that, for each $a \in (\mathbb{Z}/p^k\mathbb{Z})^\times$, the matrix

$$A = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$$

trivially belongs to $\mathrm{Stab}(M)$, so that the cardinality of the latter must be at least $\phi(p^k)$. If one among x and z is non-zero, up to applying the action of $J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ (stabilizers of elements in the same orbit have the same cardinality), we may assume that $z \neq 0$ and compute the following Groebner basis for the ideal defined by (37) in the ring of polynomials in a, b, c, d with coefficients in $\mathbb{Q}(x, y, w, z)$ and monomial order $c > d > a > b$:

$$\begin{cases} zc + xb = 0 \\ zd - za + (w+y)\,b = 0 \\ za^2 + (-w-y)\,ab + xb^2 - z \end{cases} \tag{38}$$

To count the solutions of (38) over $\mathbb{Z}/p^k\mathbb{Z}$, we would now like to 'divide by z'. To this end, if z is not a unit, we proceed as follows:

- if x is a unit, replace M with J^tMJ so that x and z are swapped (we stress again that stabilizers of elements in the same orbit have the same cardinality).

- if x is not a unit but $y+w$ is, define $K = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and replace M with $K^t M K$, so that z is replaced by $x+y+w+z$, which is a unit.
- if none among x and $y+w$ is a unit, for each $\alpha \in \mathbb{Z}/p^k\mathbb{Z}$ let $v_p(\alpha)$ denote the maximum k' s.t. $\alpha \equiv 0 \bmod p^{k'}$, with the convention $v_p(0) = \infty$. If $v_p(z) \leq \min\{v_p(x), v_p(y+w)\}$, then we can in fact 'divide by' z the equations in (38). As before, x and z can be swapped replacing M by $J^t M J$, so that the only problematic case is when $v_p(y+w) < \min\{v_p(x), v_p(z)\}$. In this case, one can check that replacing M with $K^t M K$ does the job.
  We stress that, by doing this 'division by a non-unit', we do lose some solutions of (38) (e.g. $3X = 0$ has three solutions in $\mathbb{Z}/9\mathbb{Z}$, while $X = 0$ has only one). However, this is not relevant since we are only looking for a lower bound on the number of solutions.

Thus, (38) can be finally rewritten as

$$\begin{cases} c + \frac{x}{z} b = 0 \\ d - a + \left(\frac{w+y}{z}\right) b = 0 \\ a^2 + \left(\frac{-w-y}{z}\right) ab + \frac{x}{z} b^2 - 1 = 0. \end{cases}$$

In particular, any solution (a, b) of the latter equation uniquely determines c and d. For the sake of notation, set

$$W = \frac{-y-w}{z} \qquad \text{and} \qquad Z = \frac{x}{z},$$

so that the conic we want to study is

$$C\colon \quad a^2 + Wab + Zb^2 - 1 = 0.$$

over $\mathbb{Z}/p^k\mathbb{Z}$, keeping in mind that $\#C \geq \#\mathrm{Stab}(M)$.

- Base case: $n = p$. We adopt a similar counting argument as in the case of elliptic curves [Sil09, Application V.1.3]): a given value of $b \in \mathbb{Z}/p\mathbb{Z}$ yields two (possibly equal) solutions

  $$a = \frac{-bW \pm \sqrt{\Delta(b)}}{2} \qquad \text{where} \qquad \Delta(b) = b^2(W^2 - 4Z) + 4$$

  if and only if $\Delta(b)$ is a square in $\mathbb{Z}/p\mathbb{Z}$. Thus, we can already estimate $\#C \leq 2p$ and, since $(\pm 1, 0)$ is always a point of C, $\#C \geq 2$. In order to refine the lower bound for $\#C$, we exploit the field structure of $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$ and let $\chi\colon \mathbb{F}_p^\times \to \{-1, 0, 1\}$ be the map such that

  $$\chi(z) = \begin{cases} -1 & \text{if } z \text{ is not a square,} \\ 0 & \text{if } z = 0, \\ 1 & \text{if } z \text{ is a non-zero square.} \end{cases}$$

Since $\mathbb{F}_p^\times$ is cyclic of order $p-1$, if we represent the elements of $\mathbb{F}_p$ by $\{-(p-1)/2, \dots, (p-1)/2\}$, the equality

$$\chi(z) = z^{\frac{p-1}{2}}$$

holds for every $z \in \mathbb{F}_p$. Therefore we have

$$\#C = \sum_{b\in\mathbb{F}_p} \big(1 + \chi\big(\Delta(b)\big)\big) = p + \sum_{b\in\mathbb{F}_p} \big(\Delta(b)\big)^{\frac{p-1}{2}}.$$

Moreover, by means of the following equality [Was08, Lem. 4.35]

$$\sum_{b\in\mathbb{F}_p} b^i = \begin{cases} -1 & \text{if } p-1 \mid i, \\ 0 & \text{if } p-1 \nmid i. \end{cases} \qquad \text{for every positive integer } i,$$

the latter sum can be rewritten (modulo p) as follows :

$$\begin{aligned}
\sum_{b\in\mathbb{F}_p} \big(\Delta(b)\big)^{\frac{p-1}{2}} &= \sum_{b\in\mathbb{F}_p} \big(b^2(W^2-4Z)+4\big)^{\frac{p-1}{2}} \\
&= \sum_{b\in\mathbb{F}_p} \sum_{j=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{j} 4^{\frac{p-1}{2}-j} \big(b^2(W^2-4Z)\big)^j \\
&= \sum_{j=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{j} 4^{\frac{p-1}{2}-j} \big(W^2-4Z\big)^j \sum_{b\in\mathbb{F}_p} b^{2j} \\
&= -(W^2-4Z)^{\frac{p-1}{2}}.
\end{aligned}$$

In conclusion, since $2 \le \#C \le 2p$, the only possibilities are

$$\#C = \begin{cases} p-1 \quad \text{or} \quad 2p-1 & \text{if } W^2-4Z \text{ is a quadratic residue modulo } p, \\ p \quad \text{or} \quad 2p & \text{if } W^2-4Z \equiv 0 \mod p, \\ p+1 & \text{if } W^2-4Z \text{ is a quadratic nonresidue modulo } p. \end{cases}$$

In particular, $\#C \ge p-1 = \phi(p)$.

- General case: $n = p^k$ for $k > 1$. As before, a necessary condition for (a, b) to be a point of C is that $\Delta(b)$ be a square. Let us focus on the values of $b \in \{0, \dots, p-1\}$ such that $\Delta(b) \bmod p$ is a quadratic residue, i.e. $\Delta(b)$ is a root of $X^2 - u$ for some $u \in (\mathbb{Z}/p\mathbb{Z})^\times$. For every such b, Hensel's lemma ensures that $\Delta(b) + \ell p$ is a root of u modulo p^k for some unique $\ell \in \{0, \dots, p^{k-1}-1\}$. Since the number of quadratic residues in $(\mathbb{Z}/p^k\mathbb{Z})^\times$ is $\phi(p^k)/2$, a simple counting argument shows that $\Delta(b + \ell p)$ must be a quadratic residue for any $\ell \in \{0, \dots, p^{k-1}-1\}$. In conclusion, for each $b \in \{0, \dots, p-1\}$ s.t. $\Delta(b)$ is a quadratic residue modulo p, the conic C has $2p^{k-1}$ points of the form $(a, b + \ell p)$. Moreover, from the case $n = p$ we readily deduce that there are at least $(p-1)/2$ such values of b. Thus we have found at least $(p-1)p^{k-1} = \phi(p^k)$ points on C.

□

Remark III.2.2. We conjecture that the above proof can be adapted to prove the case of n even. We checked by hand that it holds for $n \in \{2, 4, 8\}$.

Proposition III.2.1 suggests that (at least for n odd) being able to solve IsoPairings is not enough to recover a secret isogeny of known degree between two supersingular elliptic curves. The situation changes, however, if we can compute *two* (suitable) pairs of compatible pairings.

Problem 6 (TwoIsoPairings)**.** *Given a prime p, two coprime integers d and n s.t. $n^2 > d$, and two uniformly-random supersingular elliptic curves E, E' over $\mathbb{F}_{p^2}$ s.t. there exists an isogeny $\varphi\colon E \to E'$ of degree d, compute two pairs of non-antisymmetric pairings, say T, U on $E[n]$ and T', U' on $E'[n]$, s.t.*

- *T and T' (resp. U and U') are compatible with φ.*
- *$\#\left(\mathrm{Stab}(M_T) \cap \mathrm{Stab}(M_U)\right) = O(\log p)$.*

Proposition III.2.3. TwoIsoPairings *and ℓ-*IsoPath *are equivalent.*

Proof (sketch). Consider a prime p, two coprime integers d and n and two uniformly-random supersingular elliptic curves E, E' over $\mathbb{F}_{p^2}$, s.t. there exists an isogeny $\varphi\colon E \to E'$ of degree d. It is not restrictive to assume that d is a power of some prime ℓ.
Suppose first that one can solve ℓ-IsoPath and let $\{P, Q\}$ be a basis of $E[n]$. As shown in Section I.9, the set of pairings over $E[n]$ is in bijection with $M_2(\mathbb{Z}/n\mathbb{Z})$. In particular, one can choose T and U to be the pairings corresponding to

$$M_T = \mathrm{Id} \qquad \text{and} \qquad M_U = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

By choosing $\{\varphi(P), \varphi(Q)\}$ as a basis of $E'[n]$, one can simply set T' and U' to be the pairings corresponding to M_T and M_U. To show that T, T', U, U' are a solution of TwoIsoPairings, we only need to prove that the intersection of their stabilizers contains $O(\log p)$ elements. Indeed, from (38) we readily deduce

$$\mathrm{Stab}(M_T) = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \;\middle|\; a^2 + b^2 - 1 = 0 \right\}$$

and $\mathrm{Stab}(M_T) \cap \mathrm{Stab}(M_U) = \{\pm \mathrm{Id}\}$.
Conversely, suppose that one can solve TwoIsoPairings. Then we proceed as at the beginning of this section: after choosing any basis $\{P, Q\}$ for $E[n]$, we can find a basis $\{P', Q'\}$ for $E'[n]$ such that the matrix corresponding to T' is $\deg(\varphi) M_T$. However, we simultaneously want that the matrix corresponding to U' is $\deg(\varphi) M_U$: this can be achieved by applying changes of bases in $\mathrm{Stab}(M_T)$. Thanks to the assumption on the stabilizers of M_T and M_U having small intersection, there are only $O(\log n)$ bases of

$E'[n]$ for which the matrices corresponding to T' and U' are, respectively, $\deg(\varphi)M_T$ and $\deg(\varphi)M_U$. One of these bases is indeed $\{\varphi(P), \varphi(Q)\}$: then one can resort to the SIDH attack to recover φ. □

However, it is not clear, from a practical perspective, how TwoIsoPairings could be solved without solving ℓ-IsoPath first. In other words, it is not clear how one could force two pairings on $E[n]$ and $E'[n]$ – other than the Weil pairing – to be compatible with $\varphi\colon E \to E'$, *without* knowing φ. The trick is to consider pairings that are compatible with some large family of isogenies to which φ belongs: this turns out to be sometimes feasible, for example, in the presence of an orientation, as we are going to show in the next section.

III.2.2 Oriented case

Let us go back to oriented (not necessarily supersingular) elliptic curves, and see how the knowledge of an orientation can be leveraged, in combination with suitable self-pairings, to attack some class-group-action-based protocols.

Attack strategy

Consider the following problem.

Problem 7 ($\mathcal{O}$-IsoPath)**.** *Let p be a prime, d be a positive integer coprime with p, and let $\mathcal{O}$ be an order in an imaginary quadratic field K. Given d, together with two uniformly random $\mathcal{O}$-oriented elliptic curves (E, ι) and (E', ι') linked by a K-oriented isogeny φ of degree d, find φ.*

We now want to tackle this problem, similarly to what we did for ℓ-IsoPath in Section III.2.1, by combining suitable pairings with the SIDH attack.
To understand the gist of our strategy, let us consider for simplicity the case of CSIDH (see Example 2). Choose $n = \ell^r$ for some small odd prime ℓ which does not divide d and splits in $\mathbb{Q}(\sqrt{-p})$. Then $E[n]$ is spanned by two eigenspaces $\langle P\rangle, \langle Q\rangle$ of the Frobenius endomorphism π_p. Since φ is assumed to be $\mathcal{O}$-oriented, it commutes with π_p. Therefore, $E'[n]$ is also spanned by two eigenspaces $\langle P'\rangle, \langle Q'\rangle$ of π_p on E' corresponding to the same eigenvalues as in $E[n]$. This ensures that $\langle P'\rangle = \langle\varphi(P)\rangle$ and $\langle Q'\rangle = \langle\varphi(Q)\rangle$. In particular, there exist $\lambda, \mu \in (\mathbb{Z}/n\mathbb{Z})^\times$ such that $P' = \lambda\varphi(P)$ and $Q' = \mu\varphi(Q)$. Thus, by compatibility of the classical Weil pairing e_n with isogenies, we obtain

$$e_n(P', Q') = e_n(\lambda\varphi(P), \mu\varphi(Q)) = e_n(P, Q)^{\lambda\mu d}\,.$$

By computing a discrete logarithm, we can therefore eliminate one variable, say μ. In order to determine also λ, we would now need two non-trivial self-pairings f on $\langle P\rangle$ and f' on $\langle P'\rangle$, compatible with every K-oriented isogeny $E \to E'$, to compute

$$f'(P') = f(\lambda\varphi(P)) = f^{\lambda^2 d}\,.$$

This raises again the problem – already encountered in Section III.1.2 – of finding such self-pairings. In the remainder of this chapter, we will see in which cases they exist and how they can be constructed.

Self-pairings

In Section III.1.3 we have seen how self-pairings can be constructed starting from classic bilinear pairings. Here we give a more general framework which, a priori, allows for maps that do *not* come from bilinear pairings. Given a finite subgroup G of an elliptic curve $E/\Bbbk$, we define a *self-pairing* as a homogeneous function

$$f\colon G \to \overline{\Bbbk}^{\times}$$

of degree 2. This means that, for every $P \in G$ and $\lambda \in \mathbb{Z}$,

$$f(\lambda P) = f(P)^{\lambda^2}.$$

Lemma III.2.4. *Self-pairings map points of order n to $\gcd(n,2)n$-th roots of unity.*

Proof. Let $f\colon G \to \overline{\Bbbk}^{\times}$ be a self-pairing on an elliptic curve E. Let $P \in G$ have order n. Then from

$$f(P)^{n^2} = f(nP) = f(O_E) = f(0 \cdot O_E) = f(O_E)^{0^2} = 1$$

and

$$f(P)^{n^2+2n} = \frac{f(P)^{(n+1)^2}}{f(P)} = \frac{f((n+1)P)}{f(P)} = 1$$

it follows that the order of $f(P)$ divides $\gcd(n^2, n^2+2n) = \gcd(n,2)n$. □

Consider two elliptic curves E, E' over $\Bbbk$ equipped with respective self-pairings $f\colon G \to \overline{\Bbbk}^{\times}$, $f'\colon G' \to \overline{\Bbbk}^{\times}$ for finite subgroups $G \subseteq E$, $G' \subseteq E'$. Let $\varphi\colon E \to E'$ be an isogeny. We say that f and f' are *compatible* with φ if

$$\varphi(G) \subseteq G', \qquad f'(\varphi(P)) = f(P)^{\deg(\varphi)}$$

for all $P \in G$.

We are particularly interested in the case in which the domains $G = \langle P \rangle$ and $G' = \langle P' \rangle$ are cyclic: then we know that $\varphi(P) = \lambda P'$ for some $\lambda \in \mathbb{Z}$ and we can conclude

$$f'(P) = f(P)^{\lambda^2 \deg(\varphi)},$$

which (almost) reveals λ if $\deg(\varphi)$ is known and vice versa. We will refer to self-pairings with cyclic domains as *cyclic self-pairings*.

Remark III.2.5. The group structure observed for the set of pairings in Remark I.9.2 also appears in the case of self-pairings. Indeed, given a finite subgroup G of an elliptic curve E over $\Bbbk$, the set of self-pairings for G forms a group $(\mathcal{S}, \cdot)$ w.r.t. the point-wise product $(f \cdot g)(P) = f(P) \cdot g(P)$. In particular, if G is cyclic, $\mathcal{S}$ is cyclic too. Moreover, let $\varphi\colon E \to E'$ be an isogeny and G' be a finite subgroup of E' containing $\varphi(G)$, and suppose that, for some $f \in \mathcal{S}$, there exists a self-pairing f' for G' that is compatible with φ. Then one can easily check that $(f')^i$ is compatible with f^i for every $i > 0$.

Asking for compatibility with K-oriented isogenies imposes severe restrictions.

Proposition III.2.6. *Let $\mathcal{O}$ be an imaginary quadratic order with discriminant $\Delta_\mathcal{O}$ and let (E, ι) be an $\mathcal{O}$-oriented elliptic curve over $\Bbbk$. Assume that there exists a self-pairing*

$$f\colon C \to \overline{\Bbbk}^\times$$

on some finite cyclic subgroup $C \subseteq E$ which is compatible with endomorphisms in $\iota(\mathcal{O})$. In other words, for every $\sigma \in \mathcal{O}$ and every $P \in C$ we have

$$\iota(\sigma)(P) \in C, \qquad f(\iota(\sigma)(P)) = f(P)^{N(\sigma)}.$$

Write $m = \#\langle f(C)\rangle$. Then

(i) $\mathrm{char}(k) \nmid m$,

(ii) $m \mid \Delta_\mathcal{O}$,

(iii) with r the 2-valuation of $\Delta_\mathcal{O}$, we have:

- *if $r = 2$ then $m \mid \Delta_\mathcal{O}/2$,*
- *if $r \geq 3$ then $m \mid \Delta_\mathcal{O}/4$.*

Conversely, if m satisfies these necessary conditions, then we can equip every $\mathcal{O}$-oriented elliptic curve (E, ι) over $\Bbbk$ for which the orientation is locally primitive at m with a cyclic self-pairing

$$f_{(E,\iota)}\colon C_{(E,\iota)} \to \overline{\Bbbk}^\times$$

of order m, such that these self-pairings are compatible with all K-oriented isogenies of degree coprime with m (as usual, K denotes the imaginary quadratic number field containing $\mathcal{O}$).

Remark III.2.7. Note that the image of a self-pairing is not necessarily a group, which is why we write $\langle f(C)\rangle$ rather than $f(C)$.

Proof. Statement *(i)* follows immediately from the fact that $\overline{\Bbbk}^\times$ contains no elements of order $\mathrm{char}(k)$.

As for *(ii)* and *(iii)*, let P be a generator of C. Then $f(P)$ has order m. For any $\sigma \in \mathcal{O}$ we have that $\iota(\sigma)(P) = \lambda_\sigma P$ for some $\lambda_\sigma \in \mathbb{Z}$, and via

$$f(P)^{N(\sigma)} = f(\iota(\sigma)(P)) = f(\lambda_\sigma P) = f(P)^{\lambda_\sigma^2}$$

we see that $N(\sigma) \equiv \lambda_\sigma^2 \bmod m$. Writing s for the 2-valuation of m, we make a case distinction:

- If $s \leq 1$ then from Lemma III.2.4 we see that some multiple R of P must have order m. Let σ be such that $\mathcal{O} = \mathbb{Z}[\sigma]$. From

  $$(\sigma - \hat{\sigma})^2 R = (\sigma^2 + \hat{\sigma}^2 - 2N(\sigma))R = (\lambda_\sigma^2 + \lambda_{\hat{\sigma}}^2 - 2N(\sigma))R = (2N(\sigma) - 2N(\sigma))R = 0$$

  it follows that $m \mid \Delta_\mathcal{O}$ as wanted.

- If $s \geq 2$ then Lemma III.2.4 only shows the existence of a point $R \in C$ of order $m/2$ and we obtain the weaker conclusion $m \mid 2\Delta_\mathcal{O}$. But at least this implies that $\Delta_\mathcal{O}$ is even, so we must have $r \geq 2$. Write $\Delta_\mathcal{O} = -2^r n$ and consider elements in $\mathcal{O}$ of the form

  $$\sigma = \frac{\sqrt{\Delta_\mathcal{O}}}{2} + 2^t a \qquad a, t \in \mathbb{Z}_{\geq 0},$$

  so that $N(\sigma) = 2^{r-2}n + 2^{2t}a^2$ has to be a square modulo 2^s for every choice of a, t. We distinguish further:

  - If r is odd, then also $r - 2$ is odd and taking $a = 0$ immediately shows that $s \leq r - 2$, as wanted.
  - If r is even, then taking $t = (r-2)/2$ yields that $n + a^2$ must be a square modulo 2^{s-r+2} for all a. If $s \geq r$ then this gives a contradiction both in case $n \equiv 1 \bmod 4$ (take $a = 1$) and in case $n \equiv 3 \bmod 4$ (take $a = 0$). So $s \leq r - 1$.

  It remains to show that, if $r \geq 4$ is even, then in fact $s \leq r - 2$. But if $s = r - 1$ then taking $t = (r-4)/2$ yields that $4n + a^2$ must be a square modulo 8 for all a, which gives a contradiction (take $a = 0$).

To prove that the necessary conditions in the first part of the statement are also sufficient, we will construct a family of cyclic self-pairings of order m, one for each $(E, \iota) \in \mathcal{E}\ell\ell_{\bar{\mathbb{k}}}(\mathcal{O})$, which is compatible with all horizontal isogenies. More generally, the construction will apply to all $\mathcal{O}$-oriented elliptic curves (E, ι) for which the orientation is locally primitive at m. Let $m \geq 2$ be any integer in $\mathbb{k}$. Consider an $\mathcal{O}$-oriented elliptic curve (E, ι) and let $\sigma \in \mathcal{O}$ be such that

$$\mathrm{Tr}(\sigma) \equiv 0 \bmod \gcd(m, N(\sigma)). \tag{39}$$

We define

$$T_m^\sigma \colon E[m,\sigma] \times \frac{E[\sigma]}{m(E[\sigma])} \to \mu_m \subseteq \overline{\mathbb{k}}^\times$$
$$(P,Q) \mapsto e_m(P,\sigma(R)),$$

where we denoted $E[m] \cap \ker(\sigma)$ by $E[m,\sigma]$ and for brevity, and $R \in E$ is such that $mR = Q$ and – by a slight abuse of notation – we write σ instead of $\iota(\sigma)$. This is well-defined: indeed,

- we have $(m\sigma)(R) = \sigma(mR) = \sigma(Q) = 0_{E'}$, so $\sigma(R) \in E[m]$,
- making another choice for R amounts to replacing $R \leftarrow R+T$ for some $T \in E[m]$, and
$$e_m(P,\sigma T) = e_m(\hat{\sigma}(P),T) = e_m((\mathrm{Tr}(\sigma)-\sigma)(P),T) = 1$$
where the last equality follows from
$$P \in E[m,\sigma] \subseteq E[m] \cap E[N(\sigma)] = E[\gcd(m,N(\sigma))].$$

We remark that the classic Tate pairing from Section III.1.3 is indeed obtained by applying the above definition to elliptic curves over $\mathbb{F}_q$ equipped with the natural Frobenius orientation and to $\sigma = \pi_q - 1$.

One can check that the pairing T_m^σ is bilinear and non-degenerate and satisfies the following compatibility condition: for any positive integer m and any K-oriented isogeny $\varphi\colon E \to E'$ between $\mathcal{O}$-oriented elliptic curves,

$$T_m^\sigma(\varphi(P),Q) = T_m^\sigma(P,\hat{\varphi}(Q)) \qquad \text{for all } P \in E[m,\sigma],\ Q \in E'[\sigma].$$

Again the proofs are analogue to the corresponding properties of the classic Tate pairing.
Now consider $m \in \mathbb{Z}_{\geq 2}$ such that $m \mid \Delta_\mathcal{O}$, unless m is even in which case we make the stronger assumptions that $2m \mid \Delta_\mathcal{O}$ in case $4 \mid \Delta_\mathcal{O}$, and $4m \mid \Delta_\mathcal{O}$ in case $8 \mid \Delta_\mathcal{O}$. Furthermore, assume that $\mathrm{char}(k) \nmid m$. Pick any generator $\sigma \in \mathcal{O}$ such that

$$m \mid \mathrm{Tr}(\sigma), \tag{40}$$

except in the special case where $v_2(m) = 1$, in which case we want

$$2m \mid \mathrm{Tr}(\sigma) \text{ if } 8 \mid \Delta_\mathcal{O}, \qquad m \mid \mathrm{Tr}(\sigma) \text{ but } 2m \nmid \mathrm{Tr}(\sigma) \text{ if } 8 \nmid \Delta_\mathcal{O}. \tag{41}$$

Such a generator always exists. Indeed, if m is odd then we can choose whatever generator $\sigma \in \mathcal{O}$ and replace it by $\sigma - (\mathrm{Tr}(\sigma))/2 \bmod m$ if needed. If m is even and $8 \mid \Delta_\mathcal{O}$ then we can just take $\sigma = \sqrt{\Delta_\mathcal{O}}/2$, whose trace is exactly zero. If m is even and $8 \nmid \Delta_\mathcal{O}$ then we can take $\sigma = \sqrt{\Delta_\mathcal{O}}/2 + m/2$, with trace m.

Conditions (40–41) trivially imply (39), so from the foregoing it follows that to any elliptic curve E equipped with an $\mathcal{O}$-orientation we can associate the non-degenerate bilinear pairing

$$T_m^\sigma \colon E[m,\sigma] \times \frac{E[\sigma]}{m(E[\sigma])} \to \mu_m \subseteq \overline{\Bbbk}^\times,$$

and we know that this family of pairings is compatible with K-oriented isogenies. We can also view T_m^σ as a left non-degenerate bilinear pairing $E[m,\sigma] \times E[m^\infty,\sigma] \to \mu_m$, where $E[m^\infty,\sigma] = (\bigcup_{k=1}^\infty E[m^j]) \cap \ker(\sigma)$.

Now assume that the orientation is locally primitive at m. Then the group $E[m^\infty,\sigma]$ is cyclic: if it were not cyclic, we would have $E[m'] \subseteq E[m^\infty,\sigma]$ for some positive m' dividing m, but this would mean that $\sigma/m' \in \mathrm{End}(E)$, contradicting that σ is a generator of $\mathcal{O}$ and the orientation is locally primitive. Next, note that our assumptions (40–41) together with

$$\Delta_\mathcal{O} = (\mathrm{Tr}(\sigma))^2 - 4N(\sigma)$$

imply that $m \mid N(\sigma)$. Along with the fact that $E[m^\infty,\sigma]$ is cyclic, this in turn yields that $E[m,\sigma]$ is cyclic of order m. By the left non-degeneracy, we see that T_m^σ is surjective onto μ_m and that it can be converted into a self-pairing

$$\begin{aligned} f_{(E,\iota)} \colon E[m^\infty,\sigma] &\to \mu_m \\ P &\mapsto T_m^\sigma(\tau P, P) \end{aligned}$$

still satisfying $\#\langle \mathrm{im}(f_{(E,\iota))}\rangle = m$; here τ is the index of $E[m,\sigma]$ in $E[m^\infty,\sigma]$. □

We will refer to the quantity $m = \#\langle f(C)\rangle$ as the *order* of the self-pairing f.

To leave room for a few more self-pairings for a given orientation $\mathcal{O}$, one may want to relax the assumptions from Proposition III.2.6 and impose compatibility only with endomorphisms whose norm is coprime to m.

Proposition III.2.8. *We inherit the notation/assumptions from Proposition III.2.6, but now we only require that our cyclic self-pairing*

$$f \colon C \to \overline{\Bbbk}^\times$$

of order m is compatible with endomorphisms $\iota(\sigma)$ for which $\gcd(N(\sigma), m) = 1$. Then $\mathrm{char}(k) \nmid m$, and writing $\Delta_\mathcal{O} = -2^r n$ with n odd, we have:

(a) if $r = 0$ and $n \equiv 3 \bmod 8$ then $m \mid \Delta_\mathcal{O}$,

(b) if $r = 0$ and $n \equiv 7 \bmod 8$ then $m \mid 2\Delta_\mathcal{O}$,

(c) if $r = 2$ and $n \equiv 1 \bmod 4$ then $m \mid \Delta_\mathcal{O}$,

(d) if $r = 2$ and $n \equiv 3 \bmod 4$ then $m \mid \Delta_\mathcal{O}/2$,

(e) if $r = 3, 4$ *then* $m \mid \Delta_{\mathcal{O}}/4$,

(f) if $r \geq 5$ *then* $m \mid \Delta_{\mathcal{O}}/2$.

Conversely, if m *satisfies these necessary conditions, then we can equip every* $\mathcal{O}$*-oriented elliptic curve* (E, ι) *over* $\Bbbk$ *for which the orientation is locally primitive at* m *with a cyclic self-pairing*

$$f_{(E,\iota)} \colon C_{(E,\iota)} \to \overline{\Bbbk}^{\times}$$

of order m*, such that these self-pairings are compatible with all* K*-oriented isogenies of degree coprime with* m *(as usual,* K *denotes the imaginary quadratic number field containing* $\mathcal{O}$*).*

Proof. Write $m = 2^s m'$ with m' odd. Note that the statement $\mathrm{char}(k) \nmid m$ is again immediate.

Too prove the other divisibility conditions, it is easy to see that one can always find a generator $\sigma \in \mathcal{O}$ of norm coprime with m', and by mimicking the proof of Proposition III.2.6 (see the part "If $s \leq 1$ then ...") we find that $m' \mid \Delta_{\mathcal{O}}$. Since the self-pairing

$$\begin{aligned} C &\to \overline{\Bbbk}^{\times} \\ P &\mapsto f(P)^{m'} \end{aligned} \tag{42}$$

has order 2^s, the remaining divisibility conditions just follow from the case $m = 2^s$ which is discussed below. This ignores a subtlety, namely that (42) may be incompatible with endomorphisms σ for which $\gcd(N(\sigma), 2^s m') \neq 1$, rather than just $\gcd(N(\sigma), 2^s) \neq 1$. However, it is easy to check that the proof below does not suffer from this.

As for the converse statement, the cyclic self-pairings

$$f_{(E,\iota),m'} \colon C_{(E,\iota),m'} \to \overline{\Bbbk}^{\times}$$

of order m' that were constructed within the proof of Proposition III.2.6 are compatible with K-oriented isogenies of *any* degree. So, here too, if we manage to find cyclic self-pairings

$$f_{(E,\iota),2^s} \colon C_{(E,\iota),2^s} \to \overline{\Bbbk}^{\times}$$

of order 2^s that are compatible with K-oriented isogenies of odd degree, then

$$\begin{aligned} C_{(E,\iota),2^s} \times C_{(E,\iota),m'} &\to \overline{\Bbbk}^{\times} \\ P &\mapsto f_{(E,\iota),2^s}(P) f_{(E,\iota),m'}(P) \end{aligned}$$

is a family of cyclic self-pairings of the desired kind (we can assume that $C_{(E,\iota),2^s}$ is 2-primary, so that the domain is indeed cyclic).

Therefore, from now on we concentrate on the case $m = 2^s$, i.e. $m' = 1$. We proceed by the case distinction from the proposition statement:

(a) If $s \geq 1$ then by Lemma III.2.4 we know that $C[2] \cong \mathbb{Z}/2\mathbb{Z}$. The generator $\sigma = (1 + \sqrt{\Delta_{\mathcal{O}}})/2$ satisfies $\mathrm{Tr}(\sigma) \equiv N(\sigma) \equiv 1 \bmod 2$, so when acting on $E[2]$ it has characteristic polynomial $x^2 + x + 1$, which is irreducible. By compatibility with σ, however, we know that $C[2]$ is an eigenspace: a contradiction.

(b) If $s \geq 2$ then as in the proof of Proposition III.2.6 we find that $n = N(\sqrt{\Delta_{\mathcal{O}}})$ must be a square modulo 4: a contradiction. If $s = 1$ then we can construct the desired family of self-pairings as follows. Let $C_{(E,\iota)}$ be the subgroup of $E[2]$ that is fixed by $\sigma = (1 + \sqrt{\Delta_{\mathcal{O}}})/2$. This is a cyclic group of order 2 because the characteristic polynomial is $x^2 + x$ in this case. We then simply define

$$\begin{aligned} f_{(E,\iota)} \colon C_{(E,\iota)} &\to \{\pm 1\} \\ P &\mapsto -1, \\ O_E &\mapsto 1 \end{aligned}$$

It is trivial that this family is compatible with K-oriented isogenies of odd degree (but note, as a sanity check for Proposition III.2.6, that it is not compatible with the even-degree endomorphism σ).

We now discuss the cases $r \geq 2$. Note that the existence part is completely covered by the proof of Proposition III.2.6, so it suffices to prove the necessary conditions, except in cases (c) and (f). We will use the notation

$$\sigma_a := a + \sqrt{\Delta_{\mathcal{O}}}/2$$

for any $a \in \mathbb{Z}$. This is an element of $\mathcal{O}$ with norm $a^2 + 2^{r-2}n$.

(c) If $s \geq 3$ then we arrive at a contradiction because $\{n, n+4\} = \{N(\sigma_0), N(\sigma_2)\}$ must both be squares modulo 8.

For existence when $s = 2$, fix an $\mathcal{O}$-oriented elliptic curve (E, ι) and consider the non-zero point $P \in E[2]$ annihilated by σ_1. This point exists because the characteristic polynomial of σ_1 mod 2 is x^2, and it is unique because otherwise $E[2] \subseteq \ker(\sigma_1)$ would imply that 4 divides $1 + n$, a contradiction. Consider the self-pairing

$$\begin{aligned} f_{(E,\iota)} \colon C_{(E,\iota)} &\to \mu_4 \\ P &\mapsto \zeta_4 \\ O_E &\mapsto 1 \end{aligned}$$

where $C_{(E,\iota)} = \langle P \rangle$ and ζ_4 is some fixed primitive 4-th root of unity. This is indeed a self-pairing of order 4: we have

$$f_{(E,\iota)}(\lambda P) = f_{(E,\iota)}(P)^{\lambda^2}$$

for any $\lambda \in \mathbb{Z}$ because odd squares are congruent to 1 modulo 4. It is easy to see that $f_{(E,\iota)}$ is compatible with oriented endomorphisms of odd degree. Indeed, every such endomorphism σ can be written as $a + b\sigma_0$ for some integers a and b, where exactly one among a and b is even since $N(\sigma) = a^2 + b^2 n$ is odd. Thus

$$f_{(E,\iota)}(\sigma(P)) = f_{(E,\iota)}((a+b)P) = f_{(E,\iota)}(P)^{a^2+b^2+2ab} = f_{(E,\iota)}(P)^{N(\sigma)}.$$

To turn this into a family of self-pairings compatible with odd-degree K-oriented isogenies, with every $\mathcal{O}$-oriented elliptic curve (E', ι') that is connected to (E, ι) via a K-oriented isogeny of degree 1 mod 4, we associate a self-pairing as above. If (E', ι') is connected via a K-oriented isogeny of degree 3 mod 4, then we do the same, except we map P to $-\zeta_4$ instead of ζ_4. This is unambiguous because if (E', ι') was connected to (E, ι) via K-oriented isogenies of degrees 1 and 3 mod 4, then (E, ι) would have an oriented endomorphism of degree 3 mod 4: a contradiction since we have shown above that all oriented endomorphisms have norm of the form $a^2 + b^2 n$. By construction, this family of self-pairings is then indeed compatible with K-oriented isogenies of odd degree.[1]

Finally, if $s = 1$, then we can just resort to our family of self-pairings from the proof of Proposition III.2.6.

(d) If $s \geq 2$ then we find that $n = N(\sigma_0)$ must be a square modulo 4: a contradiction.

(e) If $r = 3$ and $s \geq 2$ then $1 + 2n = N(\sigma_1)$ is a square mod 4, while if $r = 4$ and $s \geq 3$ then $1 + 4n = N(\sigma_1)$ is a square mod 8: contradictions.

(f) Assume $s \geq r$. By Lemma III.2.4 we know that $C[2^{s-1}] \cong \mathbb{Z}/2^{s-1}\mathbb{Z}$. Since f is compatible with σ_a for every odd integer a, each of these endomorphisms acts on C by scalar multiplication. But then the same must be true for σ_0: let $\lambda \in \mathbb{Z}$ be a corresponding scalar. Since $\mathrm{Tr}(\sigma_0) = 0$ the eigenvalues of σ_0 acting on $E[2^{s-1}]$ are then given by $\pm\lambda$ and therefore

$$-\lambda^2 \equiv N(\sigma_0) = 2^{r-2} n \bmod 2^{s-1}. \tag{43}$$

On the other hand, the compatibility implies that $N(\sigma_a) \equiv (\lambda + a)^2 \bmod 2^s$ for all odd integers a. Along with the above congruence this yields $a^2 - \lambda^2 \equiv (\lambda + a)^2 \bmod 2^{s-1}$. Plugging in $a = \pm 1$ we find that $(\lambda+1)^2 \equiv (\lambda-1)^2 \bmod 2^{s-1}$, so that $\lambda \equiv 0 \bmod 2^{s-3}$. This means that the left-hand side of (43) vanishes mod 2^{s-1}, leaving us with $2^{r-2} n \equiv 0 \bmod 2^{s-1}$: a contradiction.

For existence when $s < r$, it suffices to assume that $s = r - 1$. Fix an $\mathcal{O}$-oriented elliptic curve (E, ι) such that the orientation is locally primitive at 2. Note that

[1] The construction may not reach every $\mathcal{O}$-oriented elliptic curve (E', ι'), because there may not exist an oriented isogeny to (E, ι), e.g. in view of [Onu21, Prop. 3.3], but we can simply repeat the procedure inside every connected component.

$2^{r-2} \mid N(\sigma_{2^{r-3}})$, so from Lemma I.7.1 we see that $E[2^{r-2}, \sigma_{2^{r-3}}]$ is cyclic of order 2^{r-2}. Fix a generator P and define the self-pairing

$$f_{(E,\iota)} \colon C_{(E,\iota)} \to \mu_{2^{r-1}} \colon \lambda P \mapsto \zeta_{2^{r-1}}^{\lambda^2},$$

where $\zeta_{2^{r-1}}$ is some generator of $\mu_{2^{r-1}}$. As in (c), this is a well-defined self-pairing of order 2^{r-1}. Indeed, for any λ and t we have

$$f_{(E,\iota)}((\lambda + 2^{r-2}t)P) = f_{(E,\iota)}(P)^{\lambda^2 + 2^{r-1}t\lambda + 2^{2(r-2)}t^2} = f_{(E,\iota)}(\lambda P).$$

To see compatibility with odd-degree endomorphisms, similar to in (c), we remark that every oriented endomorphism σ can be written as $a + b\sigma_0$ for some integers a and b. In particular, $N(\sigma) = a^2 + 2^{r-2}b^2$, which is odd if and only if a is. Then

$$f_{(E,\iota)}(\sigma(P)) = f_{(E,\iota)}((a - 2^{r-3}b)P) = f_{(E,\iota)}(P)^{a^2 + 2^{r-2}ab} = f_{(E,\iota)}(P)^{N(\sigma)},$$

where the last equality follows from the fact that $ab \equiv b^2 \bmod 2$ because a is odd, hence $2^{r-2}ab \equiv 2^{r-2}b^2 \bmod 2^{r-1}$. To turn this into a family of self-pairings compatible with odd-degree K-oriented isogenies, we proceed as in (c): if (E', ι') is a primitively $\mathcal{O}$-oriented elliptic curve (locally at 2) connected to (E, ι) via a K-oriented isogeny $\varphi \colon E \to E'$ of odd degree, then we equip (E', ι') with the above self-pairing, except that we use

$$\zeta_{2^{r-1}}^{\deg(\varphi)} \quad \text{instead of} \quad \zeta_{2^{r-1}}$$

as our primitive 2^{r-1}-th root of unity, and we choose the specific generator $P' = \varphi(P)$ of $E'[2^{r-2}, \sigma_{2^{r-3}}]$.[2] To see that this self-pairing is independent of the choice of φ, let

$$\varphi_1, \varphi_2 \colon E \to E'$$

be two K-oriented isogenies of odd degree, and write P'_i for $\varphi_i(P)$. Then $P'_1 = \lambda P'_2$ for some odd λ, and we need to check that $\deg(\varphi_1) \equiv \lambda^2 \deg(\varphi_2) \bmod 2^{r-1}$. Notice that $\hat{\varphi}_2 \circ \varphi_1$ is an oriented endomorphism of E sending P to $\lambda \deg(\varphi_2) P$. By compatibility of $f_{(E,\iota)}$ with oriented endomorphisms of odd degree we have $(\lambda \deg(\varphi_2))^2 \equiv \deg(\varphi_1)\deg(\varphi_2) \bmod 2^{r-1}$. The thesis immediately follows from the fact that $\deg(\varphi_2)$ is a unit modulo 2^{r-1}.

□

Remark III.2.9. The above proof naturally raises the question of whether the self-pairings in the boundary cases

- $s = r = 2$, $n \equiv 1 \bmod 4$,

[2] Here again, as in Footnote 1, the construction may not reach every instance of (E', ι'), but we can repeat the procedure in every connected component.

- $s = r - 1 \geq 4$,

whose existence was shown in a non-effective way, admit a more direct description. Such a description would be needed for these self-pairings to be of any practical use. In the former case, we know that the answer is yes for the Frobenius orientation, thanks to the *semi-reduced Tate pairing* from [CSV20, Rmk. 11]. Namely, let E be an elliptic curve over a finite field $\mathbb{F}_q$ with $q \equiv 1 \bmod 4$ and $\#E(\mathbb{F}_q) \equiv 2 \bmod 4$. Then the semi-reduced Tate pairing, defined as

$$\begin{aligned} E(\mathbb{F}_q)[2] &\to \mu_4 \\ P &\mapsto f_{2,P}(D_R)^{\frac{q^2-1}{4}}, \qquad 2R = P \end{aligned}$$

maps O_E to 1 and it sends the point of order 2 to a primitive 4-th root of unity. Unfortunately, this construction is of Frey–Rück type, i.e. involving Miller functions, and we do not know if/how it generalizes to arbitrary orientations.

Conclusions

Propositions III.2.6 and III.2.8 show that the self-pairings needed to solve $\mathcal{O}$-IsoPath via the strategy sketched in Section III.2 do exist in some cases, depending on $\mathcal{O}$. This fact undermines the security of CRS for some choices of $\mathcal{O}$ – namely, in the Frobenius-oriented case, whenever $\Delta_{\mathcal{O}}$ has a factor ℓ^{2r} for some small prime ℓ. We refer to [Cas+23, §5.3] for an efficient construction of self-pairings needed to attack these weak instances of CRS.

On the other hand, Propositions III.2.6 and III.2.8 also show that self-pairings do *not* exist in some cases. For example, for the parameters of CSIDH (see Example 2), the discriminant of $\mathcal{O}$ is $-4p$, so that the only self-pairings available are for 2-torsion points. This has some (negative) consequences on the possibility of attacking CSIDH and its offspring:

- the attack on SiGamal from Section III.1 cannot work because all isogenies involved have odd degrees by construction.
- even assuming that the degree of the secret key is known in CSIDH (it is in some variants of CSIDH, e.g. [CS+21]), only DDH is broken – which already was in [CSV20], with a slightly different approach – but not the protocol itself.

Chapter IV

A first exploration of Hessian graphs

In this chapter, we construct a family of graphs whose vertices are, once again, (isomorphism classes of) elliptic curves. The edges, however, do *not* represent isogenies. They stem instead from the definition of *Hessian* of an elliptic curve: namely, the determinant of the Hessian matrix of an elliptic curve E with nonzero j-invariant gives rise to another elliptic curve, called the *Hessian of* E and denoted by $\mathrm{Hess}(E)$.

While Hessian varieties are a classic topic in algebraic geometry (see e.g. [Sal79, §5.5]), their possible relevance for isogeny-based cryptography has not been investigated yet. In particular, as in the case of isogeny graphs, we show that one can work directly on isomorphism classes rather than on elliptic curves, and define Hess as a map on $\mathbb{F}_q$ (viewed as a set of j-invariants). This map determines a functional graph which we call a *Hessian graph*. The structure of Hessian graphs seems to be blind to isogenies – in particular, most vertices in the same connected components are non-isogenous – but it has a remarkably regular structure that could be relevant for cryptographic applications.

In Section IV.1 we compute the short Weierstrass form of $\mathrm{Hess}(E)$ for an elliptic curve E over $\Bbbk$, and we show how Hess behaves on $\Bbbk$-isomorphism classes and $\overline{\Bbbk}$-isomorphism classes. This leads us to the definition of *Hessian graphs* in Section IV.2, which is mostly focused on the case $\Bbbk = \mathbb{F}_q$. Here we provide some partial results on the structure of Hessian graphs, with particular emphasis on their *supersingular components*, i.e. the connected components containing at least one supersingular elliptic curve. Finally, in view of a possible application to the SRS problem from Section II.2, we state a necessary condition for a connected component to be supersingular.

IV.1 Hessian of cubic curves

Let $F \in \Bbbk[X, Y, Z]_3$ be a homogeneous cubic. It is well-known that the determinant of the Hessian matrix of F, denoted as $\mathrm{Hess}(F)$, defines another homogeneous cubic, called the *Hessian of* F. In this chapter, we will mostly focus our attention on the

case in which F is irreducible – namely, it defines a non-degenerate projective curve $C \subset \mathbb{P}^2(\Bbbk)$. We refer to Remark IV.1.3 and [CO20, Prop. 4.14] for the remaining cases.

It is well-known [Sil09, §III.1] that in fields of characteristics different from $2, 3$ one can choose F in short Weierstrass form, as

$$F = X^3 + AXZ^2 + BZ^3 - Y^2Z.$$

We will always identify F with the curve C it defines. A straightforward computation shows that its *Hessian curve* $\mathrm{Hess}(C)$ is defined by

$$\mathrm{Hess}(F) = -8(3XY^2 + 3AX^2Z + 9BXZ^2 - A^2Z^3) = 0.$$

Remark IV.1.1. In the remainder of this chapter, we will consider Hessian curves 'up to linear changes of variables' – in particular, we will write every cubic in short Weierstrass form. The reason why this can be done is a classic result: denote by H the Hessian matrix of F, and let $M \in \mathrm{GL}_3(\Bbbk)$ represent a linear change of variables,

$$M \cdot \begin{pmatrix} X \\ Y \\ Z \end{pmatrix} = \begin{pmatrix} X' \\ Y' \\ Z' \end{pmatrix}.$$

Then the hessian matrix of $F(X', Y', Z')$ is $M^t H(X', Y', Z')M$. In particular, the discriminants of the two hessian matrices differ only by a non-zero scalar factor, meaning that $\mathrm{Hess}(F(X, Y, Z))$ and $\mathrm{Hess}(F(X', Y', Z'))$ define the same curve.

We are particularly interested in the case $\Delta(C) \neq 0$, i.e. C is an elliptic curve.

Proposition IV.1.2. *Let E be an elliptic curve over $\mathbb{P}^2(\Bbbk)$ defined by*

$$y^2 = x^3 + Ax + B.$$

If $A = 0$, then $\mathrm{Hess}(E)$ is the union of three independent lines and

$$\mathrm{Hess}(\mathrm{Hess}(E)) = -24 \cdot B \cdot \mathrm{Hess}(E). \tag{44}$$

If $A \neq 0$, then the short Weierstrass form of $\mathrm{Hess}(E)$ is

$$y^2 = x^3 + \frac{-A^3/3 - 3B^2}{A^4}x + \frac{-A^3B/3 - 2B^3}{A^6} \tag{45}$$

and

$$\Delta(\mathrm{Hess}(E)) = -\frac{\Delta(E)}{27A^6}, \tag{46}$$

$$j\big(\mathrm{Hess}(E)\big) = \frac{(6912 - j(E))^3}{27(j(E))^2}. \tag{47}$$

Proof. The case $A = 0$ follows immediately from the equation of $\mathrm{Hess}(E)$: if we dehomogenize it by setting $Y = y/X$ and $Z = z/X$, we obtain the degenerate conic $3Bz^2 + y^2 = 0$, which is the union of two lines (B cannot be 0 since we are assuming $\Delta(E) \neq 0$. The equation $X = 0$ yields an additional line at infinity. These three lines are independent since the matrix of their coefficients,

$$\begin{pmatrix} 0 & 1 & \alpha \\ 0 & 1 & -\alpha \\ 1 & 0 & 0 \end{pmatrix} \qquad \text{with } \alpha^2 = -3B,$$

is invertible (recall that we are assuming the characteristic of $\Bbbk$ to be different from 2). Equation (44) follows from a straightforward computation.
Instead, if $A \neq 0$ then $\mathrm{Hess}(E)$ may be described as the affine component given by $X \neq 0$ together with a unique point at infinity $[0 : 1 : 0]$. To recover its Weierstrass form in the affine chart $X \neq 0$ when $A \neq 0$, we dehomogenize the equation by setting $x = Z/X$ and $y = Y/X$ and obtain

$$\begin{aligned} \mathrm{Hess}(E) &= -6A^2 \left(\left(\frac{2y}{A}\right)^2 + \frac{4}{A}x + \frac{12B}{A^2}x^2 - \frac{4}{3}x^3 \right) \\ &= -216A^2 \left(\left(\frac{y}{3A}\right)^2 + \frac{1}{3A}\left(\frac{x}{3}\right) + \frac{3B}{A^2}\left(\frac{x}{3}\right)^2 - \left(\frac{x}{3}\right)^3 \right). \end{aligned}$$

Finally, the substitution $(x/3, y/(3A)) \mapsto (x, y)$ yields the equation of the Hessian curve

$$y^2 = x^3 - \frac{3B}{A^2}x^2 - \frac{1}{3A}x,$$

and the substitution $x \mapsto x + B/A^2$ yields (45).
Equations (46) and (47) easily follow from (45):

$$\begin{aligned} \Delta(\mathrm{Hess}(E)) &= \frac{(64/27)A^3 + 16B^2}{A^6} = -\frac{\Delta(E)}{27A^6}, \\ j\big(\mathrm{Hess}(E)\big) &= \frac{1728(A^3 + 9B^2)^3}{A^6(A^3 + 27/4B^2)} = j(E)\frac{(A^3 + 9B^2)^3}{A^9} = \frac{(6912 - j(E))^3}{27(j(E))^2}. \end{aligned}$$

□

A consequence of the above Proposition is that the elliptic curves whose Hessian is also an elliptic curve are exactly those with non-zero j-invariant.

Remark IV.1.3. More generally, for a field $\Bbbk$ of characteristic different from 2, the Hessian of three lines of equation

$$\underbrace{(a_{11}X + a_{12}Y + a_{13}Z)(a_{21}X + a_{22}Y + a_{23}Z)(a_{31}X + a_{32}Y + a_{33}Z)}_{F} = 0$$

is equal to $2F \det(M)^2$, where $M = (a_{ij})$. Therefore, Hess sends any three independent lines into themselves, and any non-independent lines into the whole $\mathbb{P}^2(\overline{\Bbbk})$. Similar computations can be performed to check the remaining cases, which were already proven in [CO20, Prop. 4.14]. Namely,

- the Hessian of a nodal cubic is a nodal cubic,
- the Hessian of a cuspidal cubic is a cuspidal cubic,
- the Hessian of a conic plus a line is either a conic plus a line or a single line with multiplicity 3.

Remark IV.1.4. The points in $F \cap \mathrm{Hess}(F)$ are called *flex points* or *inflection points* of F. It is well-known [Dic14; Sil09, Ex. III.3.9; SV21, Lemma 3.7] that, if F is an elliptic curve, its inflection points coincide with its 3-torsion points. Moreover, if we set one of these points to be the identity of $\mathrm{Hess}(F)$ (the natural choice is the identity of F), then $F \cap \mathrm{Hess}(F)$ also coincides with the 3-torsion points of $\mathrm{Hess}(F)$. This can be seen by noticing that, on these 9 points, the addition law of $\mathrm{Hess}(F)$ coincides with the addition law of F.

IV.1.1 Hessian of j-invariants

Equation (47) shows that the j-invariant of the elliptic curve $\mathrm{Hess}(E)$ is invariant under $\overline{\Bbbk}$-isomorphisms of E. This fact suggests that Hess might be seen as a map on $\Bbbk$ sending $j_0 \in \Bbbk$ into the j-invariant of the Hessian of (any) elliptic curve of j-invariant j_0. Consequently, we will write

$$\mathrm{Hess}(j) = \frac{(6912 - j)^3}{27(j)^2}.$$

In this subsection, we investigate how much information is lost when moving to isomorphism classes. In particular, we want to assess the behavior of $\mathrm{Hess}(E)$ with respect to $\Bbbk$-isomorphisms. The most problematic cases are the curves of j-invariants 0 and 1728, as is already evident from the following result.

Lemma IV.1.5. *Assume $p \geq 5$ and, for $j' \in \Bbbk$, define*

$$H_{j'}(j) = j^2(\mathrm{Hess}(j) - j') \in \Bbbk[j].$$

Then

(i) if $j' \notin \{0, 1728\}$, then $H_{j'}$ has only simple roots;

(ii) if $j' = 1728$,

$$H_{1728}(j) = -\frac{1}{27}(j - 1728)(j + 8 \cdot 1728)^2,$$

so that, in particular, $\mathrm{Hess}(1728) = 1728$*;*

(iii) if $j' = 0$,

$$H_0(j) = -\frac{1}{27}(j - 4 \cdot 1728)^3.$$

Proof. This is a straightforward computation using the derivatives

$$H'_{j'} = -\frac{1}{9}3(j^2 + 18jj' - 13824j + 47775744),$$
$$H''_{j'} = -\frac{2}{9}6(j + 9j' - 6912).$$

In fact, $H''_{j'} = 0$ if and only if $j = -9j' + 6912$, in which case $H'_{j'} = 0$ if and only if either $j' = 0$ (in which case also $H_{j'} = 0$, proving (iii)) or $j' = 1536$ (which fails to be a root of $H_{j'}$ since we are assuming that the characteristic of $\Bbbk$ is not 2 or 3).
Double roots are checked similarly: $H'_{j'} = 0$ if and only if

$$j' = \frac{-3j^2 + 41472j - 143327232}{54j},$$

in which case $H_{j'} = 0$ if and only if either $j' = 0$ (which is the case of triple roots) or $j' = 1728$ (which proves (ii)). Then (i) follows from the fact that we have already covered all the possible double and triple roots of $H_{j'}(j)$. □

Given two $\overline{\Bbbk}$-isomorphic elliptic curves E and E' over $\Bbbk$, recall that E' is a *proper twist* of E if there is no $\Bbbk$-isomorphism between E and E'. We denote by $\mathrm{Twist}(E)$ the set of elliptic curves over $\Bbbk$ that are $\overline{\Bbbk}$-isomorphic to E, up to $\Bbbk$-isomorphism. The structure of $\mathrm{Twist}(E)$ is well-known.

Lemma IV.1.6. *Let $E\colon y^2 = x^3 + Ax + B$ be an elliptic curve over $\Bbbk$, and define*

$$n = \begin{cases} 2 & \text{if } j(E) \notin \{0, 1728\}, \\ 4 & \text{if } j(E) = 1728, \\ 6 & \text{if } j(E) = 0. \end{cases} \tag{48}$$

Then $\mathrm{Twist}(E) \cong \Bbbk^\times/(\Bbbk^\times)^n$. Namely, the elements of $\mathrm{Twist}(E)$ can be listed as

(i) $E_D\colon y^2 = x^3 + D^2Ax + D^3B$ *if* $j(E) \notin \{0, 1728\}$,

(ii) $E_D\colon y^2 = x^3 + DAx$ *if* $j(E) = 1728$,

(iii) $E_D\colon y^2 = x^3 + DB$ *if* $j(E) = 0$,

with D ranging in $\Bbbk^\times/(\Bbbk^\times)^n$.

Proof. See [Sil09, Prop. X.5.4]. □

Proposition IV.1.7. *Let $E\colon y^2 = x^3 + Ax + B$ be an elliptic curve defined over $\Bbbk$ and with non-zero j-invariant. Define n as in (48) and, for $D \in \Bbbk^\times$, let E_D be defined as in Lemma IV.1.6. Write $E' = \mathrm{Hess}(E)$ and define n' and E'_D accordingly. Then*

$$\mathrm{Hess}(E_D) = \begin{cases} E'_{D^{-1}} & \text{if } j(E') \notin \{0, 1728\} \text{ or } j(E') = 1728 = j(E), \\ E'_{D^{-2}} & \text{if } j(E') = 1728 \neq j(E), \\ E'_{D^{-3}} & \text{if } j(E') = 0. \end{cases} \tag{49}$$

In particular, Hess *descends to a map* $\mathrm{Twist}(E) \to \mathrm{Twist}(E')$*, which is bijective in the first case of* (49) *and injective in the third.*

Proof. Write $E'\colon y^2 = x^3 + A'x + B'$.
If $j(E) \notin \{0, 1728\}$, then from (45) we get

$$\mathrm{Hess}(E_D)\colon y^2 = x^3 + \frac{1}{D^2}A'x + \frac{1}{D^3}B' = \begin{cases} E'_{D^{-1}} & \text{if } j(E') \notin \{0, 1728\}, \\ E'_{D^{-2}} & \text{if } j(E') = 1728, \\ E'_{D^{-3}} & \text{if } j(E') = 0. \end{cases}$$

Similarly, if $j(E) = 1728$, then by Lemma IV.1.5 we already know that $j(E') = 1728$. More precisely, from (45) we get

$$\mathrm{Hess}(E_D)\colon y^2 = x^3 + \frac{1}{D}A'x,$$

which is exactly $E'_{D^{-1}}$.
From (49), which covers every possible value of $(j(E), j(E'))$, we see that n always divides n' and, therefore, if $D = D'$ in $\Bbbk^\times/(\Bbbk^\times)^n$ then $D^i = (D')^i$ in $\Bbbk^\times/(\Bbbk^\times)^{n'}$ for every i. This proves that Hess is well-defined as a map $\mathrm{Twist}(E) \to \mathrm{Twist}(E')$. The cases in which it is bijective/injective are easily deduced from (49).

□

An immediate consequence of Proposition IV.1.7 is that 'in most cases' proper twists commute with Hess. In particular, when $j(\mathrm{Hess}(E)) \notin \{0, 1728\}$, also the twist of $\mathrm{Hess}(E)$ arises as the Hessian of some elliptic curve (namely, the proper twist of E). The only cases that need special care are those in which extra proper twists might appear.

Proposition IV.1.8. *Let* $E'\colon y^2 = x^3 + A'x + B'$ *be an elliptic curve over* $\Bbbk$.

- *Suppose* $j(E') = 1728$. *Then* $\mathrm{Hess}(E')$ *has* j*-invariant* 1728*, and it is a proper twist of* E' *if and only if* $-3(A')^2 \notin (\Bbbk^\times)^4$. *Moreover, if* $\Bbbk^\times = (\Bbbk^\times)^2$*, then* E' *has no proper twists and it is the Hessian of a curve with* j*-invariant* $-8 \cdot 1728$. *When* $\Bbbk^\times \neq (\Bbbk^\times)^2$*, two cases may occur:*
  - *if* -1 *is not a square in* $\Bbbk$*, then* $\mathrm{Twist}(E')$ *has two elements, and one of them is the Hessian of two curves of* j*-invariant* $-8 \cdot 1728$*, one proper twist of each other.*
  - *if* -1 *is a square in* $\Bbbk$*, then* $\mathrm{Twist}(E')$ *has four elements, two of which are, respectively, the Hessian of an elliptic curve of* j*-invariant* $-8 \cdot 1728$ *and the Hessian of its proper twist.*
- *Suppose* $j(E') = 0$ *and* $\Bbbk^\times = (\Bbbk^\times)^2$. *Then,*

– *if* 1 *has only one cube root in* $\Bbbk$*, then* $\mathrm{Twist}(E')$ *has one element, which is the Hessian of an elliptic curve of* j*-invariant* $4 \cdot 1728$*.*

– *if* 1 *has three cube roots in* $\Bbbk$*, then* $\mathrm{Twist}(E')$ *has three elements, one of which is the Hessian of three* $\Bbbk$*-isomorphic curves of* j*-invariant* $4 \cdot 1728$*.*

If $\Bbbk^\times \neq (\Bbbk^\times)^2$*, the result is analogous, except that* quadratic twists *appear (for example, the quadratic twist of* E' *is obtained replacing* B' *with* D^3B'*, where* D *is a non-square): thus* $\mathrm{Twist}(E')$ *has twice as many elements and, if* $E' = \mathrm{Hess}(E)$*, its quadratic twist equals* $\mathrm{Hess}(E_D)$*, where* D *is a non-square.*

Proof. • Suppose $j(E') = 1728$, i.e. $B' = 0$. It easily follows from (45) that $\mathrm{Hess}(E')$ is the curve of equation $y^2 = x^3 - 1/(3A')x$ and, in turn, E' is the Hessian of this curve. By Lemma IV.1.6, $\mathrm{Hess}(E')$ is a proper twist of E' if and only if there exists $D \in \Bbbk^\times \setminus (\Bbbk^\times)^4$ such that $-1/(3A') = DA'$, which is the same as requiring $-3(A')^2 \notin (\Bbbk^\times)^4$. Moreover, by (45), there exists a curve $E\colon y^2 = x^3 + Ax + B$ s.t. $B \neq 0$ and $\mathrm{Hess}(E) = E'$ if and only if $-A'$ is a square $\alpha^2 \in \Bbbk$, in which case $A = 1/(-6\alpha^2)$ and $B = 1/(36\alpha^3)$. If $\Bbbk^\times = (\Bbbk^\times)^2$, i.e. every element of K is a square, there is nothing left to prove. Otherwise,

– if -1 is not a square, then $(\Bbbk^\times)^4 = (\Bbbk^\times)^2$: indeed, the inclusion $\subseteq$ is always true, and, for each $\alpha \in \Bbbk$, we have that either α or $-\alpha$ is a square, so that polynomial $X^4 - \alpha^2$ has always a root in $\Bbbk$ – which proves the other inclusion. Therefore the cardinality of $\mathrm{Twist}(E')$ is easily deduced from Lemma IV.1.6. Furthermore, by (45), there exists a curve $E\colon y^2 = x^3 + Ax + B$ s.t. $B \neq 0$ and $\mathrm{Hess}(E) = E'$ if and only if $-A'$ is a square $\alpha^2 \in \Bbbk$, in which case $A = 1/(-6\alpha^2)$ and $B = 1/(36\alpha^3)$; in particular, if such E does not exist for E', then it does for its proper twist, and vice versa – since the proper twist of E' is obtained multiplying A' by a non-square. Finally, if $E' = \mathrm{Hess}(E)$ with j-invariant $\neq 1728$, then from (47) follows that $j(E) = -8 \cdot 1728$ and the Hessian of the proper twist of E is $\Bbbk$-isomorphic to E' (otherwise both E' and its proper twist would be Hessians of some curves with j-invariant $\neq 1728$, contradicting what we have already proven).

– if -1 is a square, then $\Bbbk$ contains all the 4-th roots of 1, say ζ^i for $i \in \{0, \dots, 3\}$, which we may choose as representatives of the four elements of $\Bbbk^\times/(\Bbbk^\times)^4$. Therefore the cardinality of $\mathrm{Twist}(E')$ is again deduced from Lemma IV.1.6. The remainder of the proof is an easy adaptation of the case of -1 non-square. In particular, either E' and its quadratic twist, or the other two proper twists, arise as Hessians of some elliptic curve with $B \neq 0$ and its proper twist, respectively.

• Suppose $j(E') = 0$, i.e. $A' = 0$. By (45), E' is the Hessian of $E\colon y^2 = x^3 + Ax + B$ if and only if $A^3 = -9B^2$ and $B = 1/(81B')$. Thus, such an E exists over $\Bbbk$ if

and only if the square of B' – and therefore B' itself – is a cube in $\Bbbk$. In this case, writing $B' = \beta^3 \in \Bbbk$, the equation of E is

$$E\colon y^2 = x^3 - 1/(9\beta^2)x + 1/(81\beta^3). \tag{50}$$

Moreover, one can check from (47) that the j-invariant of E is $4 \cdot 1728$. Suppose $\Bbbk^\times = (\Bbbk^\times)^2$. Then,

- if 1 has only one cube root in $\Bbbk$, then the map $x \mapsto x^3$ is a bijection on $\Bbbk^\times$, i.e. $\Bbbk^\times = (\Bbbk^\times)^3$. In particular, $\Bbbk^\times/(\Bbbk^\times)^6 = \Bbbk^\times/(\Bbbk^\times)^2$, so that, by Lemma IV.1.6, the cardinality of $\mathrm{Twist}(E')$ is 1. Since every element of $\Bbbk$ has a unique cube root, E' arises as the Hessian of some curve E as in (50).
- if 1 has three cube roots in $\Bbbk$, then $\Bbbk^\times/(\Bbbk^\times)^6$ has 3 elements, and so does $\mathrm{Twist}(E')$ by Lemma IV.1.6. One of them arises as the Hessian of some curve E as in (50), and also as the Hessian of the two curves obtained by multiplying β by any primitive cube root of 1.

The case $\Bbbk^\times \neq (\Bbbk^\times)^2$ follows immediately.

□

IV.2 Hessian graphs over finite fields

Let us focus on the case $\Bbbk = \mathbb{F}_q = \mathbb{F}_{p^r}$. As observed in Section IV.1.1, we can view Hess as a map over $\mathbb{F}_q$ (seen as a set of j-invariants) together with a point at infinity ∞ representing the degenerate case Hess(0) (see Proposition IV.1.2). More precisely, we are interested in the *functional graph* of Hess, or *Hessian graph* for short, which is the multigraph with set of vertices $\mathbb{F}_q \cup \{\infty\}$ and n directed edges $x \to y$ iff

$$\mathrm{Hess}(x) - y, \frac{\partial(x^2(\mathrm{Hess}(x) - y))}{\partial x}, \ldots, \frac{\partial^n(x^2(\mathrm{Hess}(x) - y))}{\partial x^n}$$

are all 0.

Remark IV.2.1. We already know, from Lemma IV.1.5, that the only multiple edges are those landing on 0 and 1728.

Remark IV.2.2. For some finer results involving the traces of elliptic curves in the Hessian graph, we will sometimes consider the *Hessian graph with twists*, i.e. we will look at $\mathbb{F}_q$-isomorphism classes rather than $\overline{\mathbb{F}_q}$-isomorphism classes of elliptic curves. Since $\mathbb{F}_q^\times \neq (\mathbb{F}_q^\times)^2$ (we are assuming $2 \nmid q$), by Propositions IV.1.7 and IV.1.8 the resulting graph is essentially a double copy of the Hessian graph, arising from quadratic twists, with the possible appearance of few extra vertices arising from the j-invariants 0 and 1728.

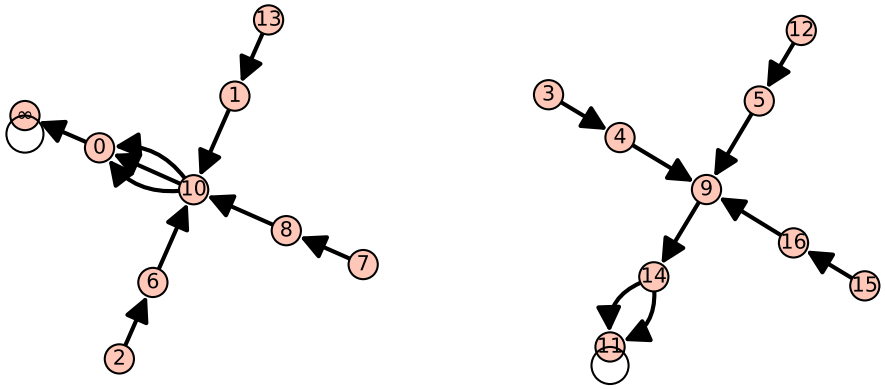

Figure IV.1: Hessian graph on $\mathbb{F}_{17}$.

We may consider a slightly larger family of rational functions, and define, for $k, \ell \in \mathbb{F}_q^*$,

$$F_{k,\ell} : \mathbb{P}^1(\mathbb{F}_q) \to \mathbb{P}^1(\mathbb{F}_q), \quad [x : y] \mapsto [(x + ky)^3 : \ell \cdot x^2 y],$$

which corresponds to the affine map

$$F_{k,\ell}(x) = \frac{(x + k)^3}{\ell \cdot x^2}.$$

Proposition IV.2.3. *The functional graphs corresponding to $F_{1,\ell}, F_{2,\ell}, \ldots$ are isomorphic.*

Proof. One can check that the functional graphs of $F_{k,\ell}$ and $F_{k',\ell}$ are isomorphic via the map

$$x \mapsto k'k^{-1}x.$$

Indeed, one can check that

$$F_{k',\ell}(k'k^{-1}x) = k'k^{-1}F_{k,\ell}(x).$$

□

The link with our previous definition of $\mathrm{Hess}(j)$ is easily seen by observing that

$$\mathrm{Hess}(j) = F_{-6912,-27}(j),$$

so that, in light of Proposition IV.2.3, we may focus on the functional graph of $F_{k,-27}$ for any $k \in \mathbb{F}_q^*$.
A first glance at the Hessian graph over $\mathbb{F}_{17}$ (Figure IV.1) already suggests that, compared with functional graphs arising from other values of ℓ (Figure IV.2), Hessian graphs enjoy a remarkably regular structure.

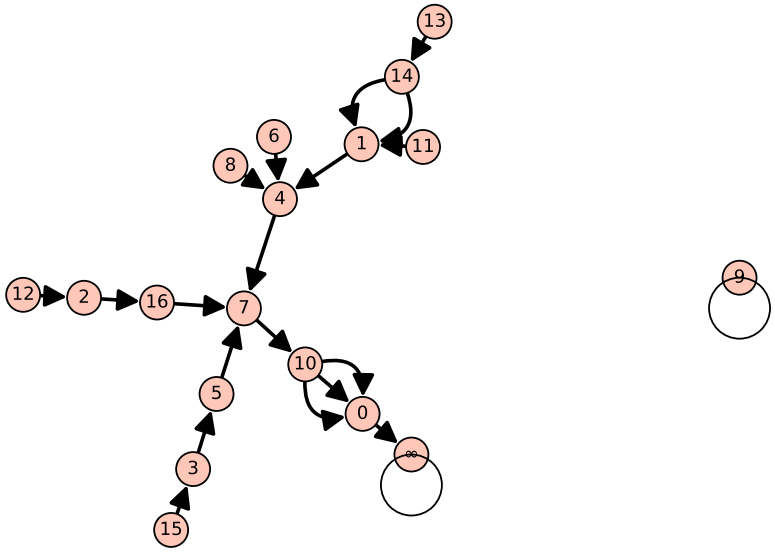

Figure IV.2: Functional graph of $F_{-6912,-8}$ over $\mathbb{F}_{17}$.

IV.2.1 Leaves of the Hessian graph

The *leaves* of the Hessian graph – i.e. the elliptic curves which do not arise as Hessian curves – can be characterized in terms of their traces.

Proposition IV.2.4. *Let E' be an elliptic curve defined over $\mathbb{F}_q$. Then E' has even trace (or, equivalently, order) over $\mathbb{F}_q$ if and only if there exists an elliptic curve E defined over $\mathbb{F}_q$ such that $E' = \mathrm{Hess}(E)$. In particular,*

$$\{\mathrm{Hess}(E) \mid E \text{ is defined over } \mathbb{F}_q\} = \{E \mid \mathrm{tr}(E) \equiv 0 \bmod 2\}.$$

Proof. Since p is odd and $\#E'(\mathbb{F}_q) = q + 1 - \mathrm{tr}(E')$, trace and order of E' have the same parity. If E' has even order, then it has an $\mathbb{F}_q$-rational 2-torsion point P. By writing E in Weierstrass form, we can assume $P = (x', 0)$ for some $x' \in \mathbb{F}_q$, and, up to a change of coordinates $(x, y) \mapsto (x - x', y)$, we can further assume $x' = 0$. Therefore, the equation of E' is

$$y^2 = x^3 + A'x^2 + B'x.$$

From (45) we see that, for

$$A = -\frac{1}{3B'} \qquad \text{and} \qquad B = -\frac{A'}{27(B')^2},$$

the curve $E\colon y^2 = x^3 + Ax + B$ satisfies $\mathrm{Hess}(E) = E'$.
The other implication is trivial since $(0, 0)$ is always an $\mathbb{F}_q$-rational 2-torsion point of the curve defined by (45). □

IV.2.2 Loops

Studying the loops amounts to considering the equation $\mathrm{Hess}^n(j) = j'$ for $n \geq 1$.

Proposition IV.2.5. *If $p \geq 5$, the only loops of length 1 in the Hessian graph start from the vertices $1728, \infty$ and possibly the roots of $7j^2 + 6912j + 47775744$, which exist if and only if -3 is a square in $\mathbb{F}_q$.*

Proof. This follows immediately from the factorization

$$\mathrm{Hess}(j) - j = -\frac{4}{27} \cdot \frac{(j - 1728) \cdot (7j^2 + 6912j + 47775744)}{j^2}$$

and the fact that the discriminant of $7j^2 + 6912j + 47775744$ is $-2^{16}3^9$, which is -3 up to squares. □

Loops of length $n > 1$ can be studied similarly by considering the degree-3^n equation

$$\mathrm{Hess}^n(j) - j = 0, \tag{51}$$

with the caveat that some roots of this equation belong to the loops of length d for $d \mid n$. Some elementary combinatorics allow us to bound the number of loops in a Hessian graph. To understand the idea behind the general formula, let us first consider some simple cases:

- If n is a prime p_1, the only other solutions of (51) are those appearing in loops of length 1, so that we immediately conclude that the loops of length p_1 are $(3^{p_1} - 3)/p_1$. The final division by p_1 comes from the fact that each loop of length p_1 contains p_1 solutions of (51).
- More generally, if n is a prime power $p_1^{e_1}$, we only need to rule out the solutions of (51) which appear in loops of length $1, p_1, p_1^2, \ldots, p_1^{e_1-1}$, i.e. all the roots of $\mathrm{Hess}^{p_1^{e_1-1}}(j) - j$. Therefore, the loops of length n are $\left(3^{p_1^{e_1}} - 3^{p_1^{e_1-1}}\right)/n$.
- If $n = p_1 p_2$, we need to rule out the solutions of (51) which appear in loops of length 1, p_1 or p_2. However, removing the roots of $\mathrm{Hess}^{p_1}(j) - j$ and $\mathrm{Hess}^{p_2}(j) - j$ results in removing twice the roots of $\mathrm{Hess}(j) - j$. Therefore, the loops of length n are $\left(3^{p_1 p_2} - 3^{p_1} - 3^{p_2} + 3\right)/n$.

By combining these ingredients, one can find the following general formula.

Proposition IV.2.6. *Let n be a positive integer and write its factorization $n = \prod_{i=1}^k p_i^{f_i}$. Moreover, define $P = \prod_{i=1}^k p_i^{f_i - 1}$. The number of loops of length n in a Hessian graph over $\mathbb{F}_q$ is at most*

$$\frac{1}{n} \cdot \Big(\sum_{(e_1, \ldots, e_k) \in \{0,1\}^k} (-1)^{k + e_1 + \cdots + e_k} 3^{p_1^{e_1} \cdots p_k^{e_k} P} \Big).$$

Proof. The formula simply condenses a combinatorial argument. Indeed, we have already observed that the j-invariants in a loop of length n are exactly solutions of (51) which are *not* solutions of $\mathrm{Hess}^d(j) - j$ for any proper divisor d of n (since we are only looking for an upper bound, we will always assume that all these solutions lie in $\mathbb{F}_q$ and are distinct). We claim that the number of these solutions is counted by

$$3^n - \sum_{\substack{e_1+\cdots+e_k=k-1 \\ (e_1,\ldots,e_k)\in\{0,1\}^k}} \left(3^{p_1^{e_1}\cdots p_k^{e_k}P}\right) + \sum_{\substack{e_1+\cdots+e_k=k-2 \\ (e_1,\ldots,e_k)\in\{0,1\}^k}} \left(3^{p_1^{e_1}\cdots p_k^{e_k}P}\right) - \cdots + (-1)^k 3^P. \tag{52}$$

To prove our claim, we need to show that each proper divisor d of n appears as $3^{d\cdots}$ in an even number of addends of (52), exactly half of which have a negative sign. This will ensure that the roots of $\mathrm{Hess}^d(j) - j$ are added and subtracted the same number of times by (52) (i.e. they are not counted at the end). Suppose first that d is either P or a divisor of P. This means that every exponent in (52) is a multiple of d. The number of addends in (52), counted with sign, is

$$\sum_{i=0}^{k} (-1)^i \binom{k}{i} = (1 + (-1))^k = 0.$$

If d does not divide P, then (up to reordering $p_1, \ldots, p_k$) it factors as

$$d = p_1^{f_1} \cdots p_\ell^{f_\ell} \cdot [\text{some divisor of } P]$$

for some $\ell > 0$. Therefore, the only exponents of (52) in which d appears are in

$$3^n - \sum_{\substack{e_{\ell+1}+\cdots+e_k=k-\ell-1 \\ (e_{\ell+1},\ldots,e_k)\in\{0,1\}^k}} \left(3^{p_1\cdots p_\ell \cdot p_{\ell+1}^{e_{\ell+1}}\cdots p_k^{e_k}P}\right) + \sum_{\substack{e_{\ell+1}+\cdots+e_k=k-\ell-2 \\ (e_{\ell+1},\ldots,e_k)\in\{0,1\}^k}} \left(3^{p_1\cdots p_\ell \cdot p_{\ell+1}^{e_{\ell+1}}\cdots p_k^{e_k}P}\right) - \cdots + (-1)^{k-\ell} 3^{p_1\cdots p_\ell P}.$$

Counting these addends with sign yields

$$\sum_{i=0}^{k-\ell} (-1)^i \binom{k-\ell}{i} = (1 + (-1))^{k-\ell} = 0.$$

Dividing (52) by n yields the desired formula. □

For example, the first 10 values of the upper bound in Proposition IV.2.6 are

$$3, 3, 8, 18, 48, 116, 312, 810, 2184, 5880.$$

In general, in large extensions of $\mathbb{F}_p$ we expect $\sim 3^n/n$ loops of length n.

IV.2.3 Regularity of the Hessian graph

Lemma IV.2.7. *Let $F_{k,\ell}(x)$ be defined as in Proposition IV.2.3. Then the set of vertices of indegree 1 in the corresponding functional graph is*

$$\{y \in \mathbb{F}_q \mid k(4y\ell - 27k) \text{ is not a square}\} \cup \{\infty\}.$$

In particular, the vertices of indegree 1 in the functional graph of $F_{k,\ell}$ over $\mathbb{F}_q$ are $(q+1)/2$.

Proof. Let y be a vertex in the functional graph of $F_{k,\ell}$. Then y has indegree 1 if and only if the cubic polynomial

$$\tilde{F} = \ell x^2(F_{k,\ell} - y) = x^3 + (3k - \ell y)x^2 + 3k^2x + k^3$$

has exactly one root. By [Dic06, Lem. 2], this occurs if and only if the discriminant of $\tilde{F}$, which is

$$\ell^2 y^2 k^3 (4y\ell - 27k)$$

is not a square.
Finally, the last statement follows immediately from the fact that $y \mapsto k(4y\ell - 27k)$ is a bijection and 0 has indegree 1 by Lemma IV.1.5. □

Proposition IV.2.8. *Let $F = F_{k,-27}$ be defined as in Proposition IV.2.3, and let y be a vertex of indegree 1 (resp. 0 or 3) in the corresponding functional graph over some extension $\mathbb{F}_q$ of $\mathbb{F}_p$. Then the indegree of $F_{k,-27}(y)$ is*

$$\begin{cases} 1 \text{ (resp. } 3) & \text{if either } q \text{ is an even power of } p \text{ or } p \equiv 1 \bmod 3, \\ 3 \text{ (resp. } 1) & \text{otherwise.} \end{cases}$$

Proof. The equality $F(y) = F(y')$ holds for $y' \in \overline{\mathbb{F}_q}$ if and only if either $y' = y$ or y' satisfies

$$y'^2 y^2 + (-3yk^2 - k^3)y' - yk^3 = 0.$$

Then $F(y)$ has indegree 1 if and only if the discriminant of the latter equation, say Δ, is not a square in $\mathbb{F}_q$. We have

$$\Delta = (4y + k)(y + k)^2 k^3.$$

By Lemma IV.2.7, $-3k(4y + k)$ is not (resp. is) a square. Therefore, Δ is not a square in $\mathbb{F}_q$ if and only -3 is (resp. is not) a quadratic residue. One can straightforwardly check by quadratic reciprocity that this happens precisely when q is an even power of p or $p \equiv 1 \bmod 6$ (which is the same as $p \equiv 1 \bmod 3$ since we are assuming that $p \neq 2, 3$). □

Remark IV.2.9. Since Lemma IV.2.7 holds for any ℓ, it is natural to ask whether Proposition IV.2.8 can be generalized to $\ell \neq -27$. Indeed, the first part of the proof carries over for any ℓ, since the equality $F(y) = F(y')$ (and therefore Δ) is independent of ℓ. However, for $\ell \neq -27$ the special link between the quadratic residuosity of Δ and $k(4y\ell - 27k)$ is lost, i.e. it does depend on the value of y (while it does not for $\ell = -27$).

Corollary IV.2.10. *Let $F_{k,-27}(x)$ be defined as in Proposition IV.2.3, and denote by G the corresponding functional graph over $\mathbb{F}_q$. Then*

- *if -3 is a square in $\mathbb{F}_q$, the connected components of G are either pure loops or "totally ramified" trees (in the sense that every vertex, apart from the leaves, has indegree 3).*
- *if -3 is not a square in $\mathbb{F}_q$, a vertex of indegree 1 in G is followed by a vertex with indegree 3, and every vertex with indegree 0 or 3 is followed by a vertex of indegree 1.*

IV.2.4 Supersingular components

Given the Hessian graph over $\mathbb{F}_p$ or $\mathbb{F}_{p^2}$, we are now interested in the *supersingular components* of the graph, i.e. the connected components containing supersingular j-invariants.

Proposition IV.2.11. *Let E be an elliptic curve in short Weierstrass form defined over $\mathbb{F}_q$, and suppose that it has non-zero j-invariant. Then E and* Hess(E) *have the same trace modulo* 3.

Proof. By Remark IV.1.4, E and its Hessian (before rescaling) have the same 3-torsion points. Therefore, their Frobenius endomorphisms coincide over $E[3]$, meaning that they are represented (as automorphisms of $E[3]$) by the same matrix over $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$. In particular, the corresponding characteristic polynomials are equal. This still holds after the scaling needed to write Hess(E) in short Weierstrass form (45), which proves our statement.

□

Corollary IV.2.12. *Let G' be a connected component of the Hessian graph over $\mathbb{F}_q$ with twists (as defined in Remark IV.2.2). Then every curve in G' has the same trace modulo* 3.

Moreover, assume that G' is supersingular:

(i) if $q = p$, then G' contains only curves with traces $0 \bmod 3$*;*

(ii) if $q = p^2$, then G' contains only curves with traces $\pm 1 \bmod 3$, unless it consists of one or two vertices of j-invariant 1728.

Proof. Most of the statement is an immediate consequence of Proposition IV.2.11. As for (ii), recall that supersingular elliptic curves over $\mathbb{F}_{p^2}$ have their traces in $\{\pm 2p, \pm p, 0\}$. Since $p \equiv \pm 1 \bmod 3$, the only case we need to consider is when G' contains a supersingular elliptic curve E of trace 0. It is well-known (see e.g. [AAM19, §4]) that this occurs if and only if $p \equiv 3 \mod 4$ and E has j-invariant 1728. Then, by Proposition IV.1.8, either G' consists of E alone, or it is a loop of length 2 containing E and its quadratic twist. □

Corollary IV.2.12 suggests a simple way to improve the exhaustive-search approach to the cSRS problem from Section II.2.2: rather than sampling random j-invariants in $\mathbb{F}_p$ (resp. $\mathbb{F}_{p^2}$), one can start from a j-invariant corresponding to curves with trace 0 (resp. ± 1) mod 3 and then walk on the corresponding Hessian graph. This, however, does not improve much, heuristically, the efficiency of the algorithm, since supersingular elliptic curves seem to be evenly distributed within the connected components with traces 0 (resp. ± 1) mod 3. Only a better understanding of the structure of the Hessian graph could lead to more significant improvements.

IV.2.5 Open directions

While Corollary IV.2.10 provides a partial explanation of the regular structure of Hessian graphs, we conjecture – based on heuristic observations – that there is still more to be proven.

Define the *depth* of a vertex to be its distance from the loop of its connected component.

Conjecture IV.2.13. *Any two branches starting from vertices of depth $N > 0$ in the same connected component are isomorphic.*

We also define the *depth of a connected component* to be the maximum of the depths of its vertices.

Conjecture IV.2.14. *If $q \equiv 2 \bmod 3$, then each connected component has the same depth.*

See Figure IV.3 for a visual depiction of these conjectures.

From a cryptographic perspective, there are two open directions that we believe might be worth considering: the first one, already pointed out in Section IV.2.4, is to find new approaches to the SRS problem by studying the supersingular connected components of the Hessian graphs over $\mathbb{F}_p$ or $\mathbb{F}_{p^2}$.
The second one concerns 3-isogenies: since, by Remark IV.1.4, 3-torsion points play

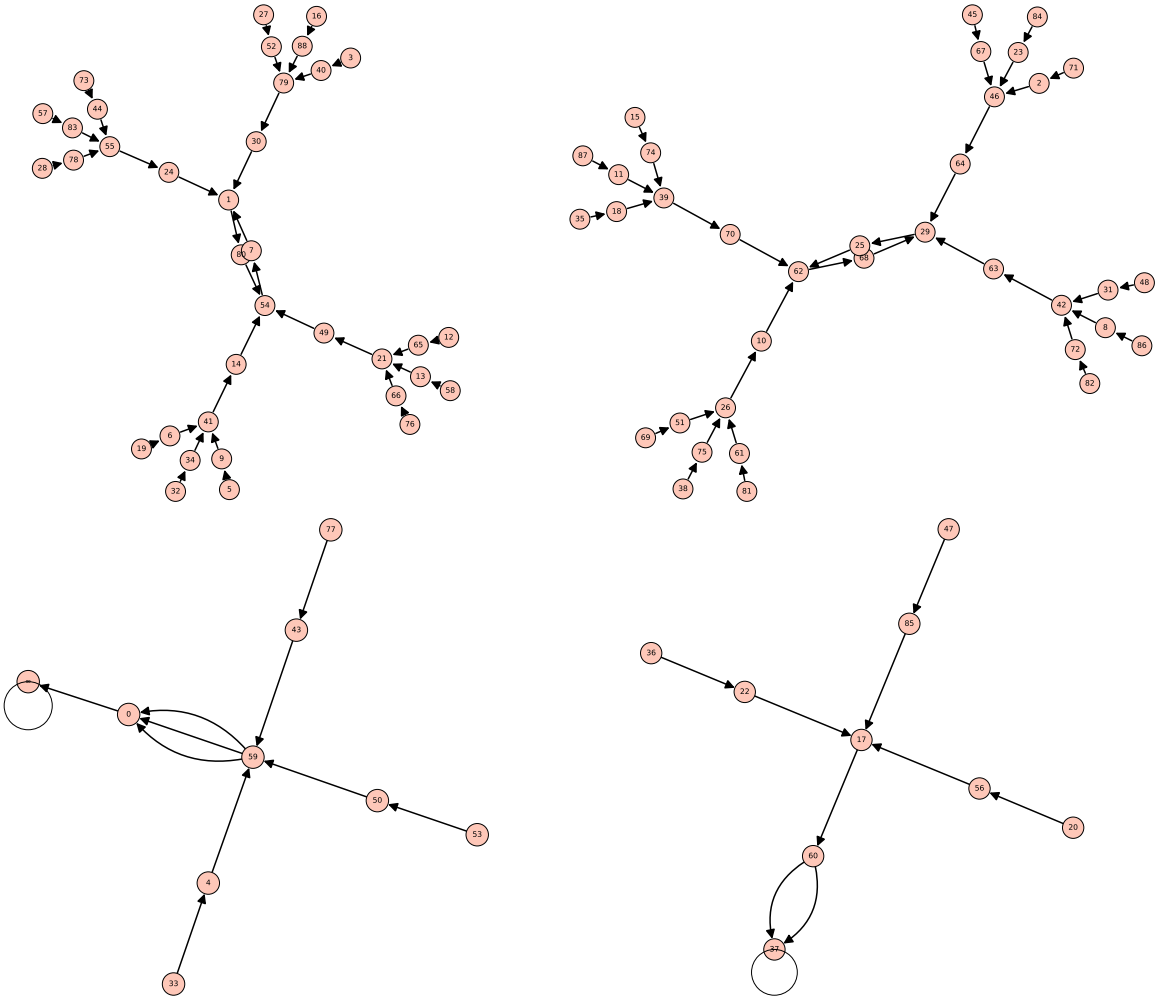

Figure IV.3: Hessian graph on $\mathbb{F}_{89}$. Each connected component has depth 4.

a special role in the construction of Hessian curves, it is reasonable to expect that 3-isogenies can show some regular behavior in the Hessian graph.

Conclusions

...ἃ μὴ οἶδα οὐδὲ οἴομαι εἰδέναι.

Ἀπολογία Σωκράτους, Plato.

Building cryptographic protocols on top of an enormous amount of theory has its advantages, but is prone to the risk that hidden mathematical structures might undermine their security, as it happened to SIDH. Throughout this thesis, we have considered both design problems, such as randomizing the starting supersingular curve, and cryptanalytic problems, such as assessing the hardness of some variants of ℓ-IsoPath and studying the construction of pairings to target, in general, non-oriented elliptic curves and, more specifically, some class-group-action-based protocols.

Some questions were successfully answered: in Proposition II.3.2, we observed that a greedy algorithm based on the 'M-smallness' of supersingular elliptic curves would not be powerful enough to solve ℓ-IsoPath. In Proposition III.2.3, we proved that the knowledge of pairings can be enough to recover a secret isogeny, and showed, in Section III.2.2, that this leads to an effective attack, in some cases, when an orientation is given. Finally, in Chapter IV, we gave a partial account of the remarkable regularity of Hessian graphs, which could have interesting consequences from both a constructive and a cryptanalytic point of view.

On the other hand, we ended up with even more questions than we started with: the problem of hashing in the supersingular isogeny graph is still unsolved, despite the seemingly promising formulas found in Proposition II.2.31. Moreover, an effective construction of some of the self-pairings from Proposition III.2.8 is yet to be found, possibly by mimicking the construction of the *semi-reduced Tate pairing* for the Frobenius-oriented case in [CSV20, Rmk. 11]. Finally, the regularity of Hessian graphs, and even more their possible interconnection with degree-3 isogenies, is not yet fully understood.

Of course, it would be much worse if we had believed that we had solved all the problems of this branch: that would mean either that the branch is not rich enough, or that we are deluded. For now, we just look at the climb ahead, in the hope that it will take us higher.

Other works: p-adic continued fractions

In this appendix, we briefly mention some results from the other main branch of our research, which consists of the study of p-adic continued fractions. We stress that this topic is mostly unrelated to our research in isogeny-based cryptography: the only (and negligible) intersection is the presence of quaternion algebras in [CMT22].

Given an element $\alpha \in \mathbb{R}$, the classical *(Archimedean) continued fraction expansion* (or *CF-expansion* for short) of α is the (possibly infinite) sequence of integers $[c_1, c_2, \dots]$ computed by means of the following algorithm:

$$\begin{cases} \alpha_0 = \alpha \\ c_n = \lfloor \alpha_n \rfloor \\ \alpha_{n+1} = \frac{1}{\alpha_n - c_n} \quad \text{if } \alpha_n - c_n \neq 0, \end{cases} \tag{53}$$

stopping if $\alpha_n = c_n$. It is well known that α is rational if and only if its CF-expansion is finite, and, if α is not rational, then the sequence of *n-th convergents*

$$c_1 + \cfrac{1}{c_2 + \cfrac{1}{\ddots + \cfrac{1}{c_n}}}$$

converges to α.

More generally, let D be a division algebra and $c_1, c_2, \dots$ be a sequence of elements in some subset $R \subseteq D$. One can always define a *continued fraction* $\mathcal{C} = [c_1, c_2, \dots]$ as the formal expression

$$c_1 + \cfrac{1}{c_2 + \cfrac{1}{\ddots}}. \tag{54}$$

The elements $c_1, \dots, c_n$ are called the *partial quotients* of $\mathcal{C}$.

Just as a formal series can converge to some limit, one might ask how $\mathcal{C}$ can 'represent' some value α lying in K.

Two situations can prevent (54) from representing an actual element of K: the appearance of zero denominators and the fact that the sequence $c_1, c_2, \dots$ might be infinite. To deal with these situations, for $n \geq 1$ we consider the *n-th convergent*

$$[c_1, c_2, \dots, c_n] = c_1 + \cfrac{1}{c_2 + \cfrac{1}{\ddots + \cfrac{1}{c_n}}}$$

(which can be seen as a finite continued fraction in its own right). Studying the case in which $\mathcal{C}$ is infinite requires a suitable notion of convergence. Indeed, if D is endowed with a suitable topology (in particular, if it is a metric space), we can consider the convergence of the sequence $\{[c_1, \dots, c_n]\}_{n=1}^{\infty}$: if it converges, we say that $\mathcal{C}$ *converges*.

In this general setting, several problems arise:

- Which continued fractions converge? Or, said otherwise: which elements in the topological completion of D can be represented by continued fractions?
- Can algorithm (53) be adapted to compute these representations?
- Which continued fractions/CF-expansions are finite/periodic?

The questions above have been extensively studied in the 'classical' case, i.e. when $D = \mathbb{Q}$, endowed with the Euclidean topology, and $R = \mathbb{Z}$. The first contributions date back to the works of Wallis, Euler, and Lagrange [Bre12]. More recent works, starting from [Rub70] and [Bro78], deal with the case in which D is a number field endowed with a non-Archimedean absolute value. Our works follow the latter line of research, focusing on non-Archimedean continued fractions:

(i) In [CMT22], we take D to be a quaternion algebra ramified at some odd prime p, R to be the ring

$$R = \{\alpha \in \mathcal{O} \mid v_q(\alpha) \geq 0 \text{ for each place } q \neq p\},$$

where $\mathcal{O}$ is a maximal order in D. We show that the construction of p-adic CF-expansions carries over to this non-commutative setting. In particular, once a suitable *p-adic floor function* is chosen, CF-expansions can be obtained via algorithm (53). We characterize the elements of D having a finite continued fraction expansion and, using a suitable notion of *quaternionic height*, we prove a sufficient condition for a given CF-expansion algorithm (i.e. a given floor function combined with (53)) to provide infinite expansions for every element in D. Further, as an example, we show that a natural generalization of Browkin's algorithm fails to produce finite p-adic CF-expansions for some elements of the quaternion algebra ramified at two distinct rational primes p and q. Finally, we draw some consequences about the solutions of a family of quadratic polynomial equations with quaternionic coefficients.

(ii) In [Cap+23a], we set D to be a number field and we fix a finite subset of *extraneous denominators* $\mathcal{T} \subseteq D$. Defining

$$R' = \{\beta \in \mathcal{O}_D \mid v_q(\alpha) \geq 0 \text{ for each place } q \neq p\},$$

where $\mathcal{O}_D$ is the ring of integers D, we finally take R to be

$$R = \{\alpha \in D \mid \text{there exists } \gamma \in \mathcal{T} \text{ s.t. } \gamma\alpha \in R'\}.$$

We show that, for suitable choices of the set $\mathcal{T}$, for every place p of sufficiently large norm there exists a p-adic CF-expansion algorithm s.t. *every* element of K has a finite CF-expansion. This provides, in particular, a new algorithmic approach to the construction of terminating division chains in number fields.

(iii) In [Cap+23b], we take $D = \mathbb{Q}$ and $R = \mathbb{Z}[1/p]$ for an odd prime p, and study p-adically convergent periodic continued fractions. Unlike the previous works, we do not consider specific CF-expansions algorithms or floor functions: we consider instead every possible eventually periodic sequence of partial quotients in R. To this end, following a previous work by Brock, Elkies, and Jordan [BEJ21], we use the language and techniques of algebraic geometry to study certain algebraic varieties associated with periodic continued fractions with period and preperiod of fixed lengths. In particular, we focus on the *p-adically convergent loci* of these varieties, characterizing the cases in which the variety is a curve.

Bibliography

[AAM19] G. Adj, O. Ahmadi, and A. Menezes. "On Isogeny Graphs of Supersingular Elliptic Curves over Finite Fields". In: *Finite Fields and their Applications* 55 (2019), pp. 268–283.

[Bas+23] A. Basso, G. Codogni, D. Connolly, L. De Feo, T. B. Fouotsa, G. M. Lido, T. Morrison, L. Panny, S. Patranabis, and B. Wesolowski. "Supersingular Curves You Can Trust". In: *Advances in Cryptology – EUROCRYPT 2023: 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23–27, 2023, Proceedings, Part II*. Berlin, Heidelberg: Springer-Verlag, 2023, 405–437. URL: https://doi.org/10.1007/978-3-031-30617-4_14.

[BDF21] J. Burdges and L. De Feo. "Delay Encryption". In: *Advances in Cryptology – EUROCRYPT 2021*. Ed. by A. Canteaut and F.-X. Standaert. Cham: Springer International Publishing, 2021, pp. 302–326.

[BEJ21] B. W. Brock, N. D. Elkies, and B. W. Jordan. "Periodic continued fractions over S-integers in number fields and Skolem's p-adic method". In: *Acta Arith.* 197.4 (2021), pp. 379–420.

[BFJ16] J.-F. Biasse, C. Fieker, and M. J. Jacobson. "Fast heuristic algorithms for computing relations in the class group of a quadratic order, with applications to isogeny evaluation". In: *LMS Journal of Computation and Mathematics* 19.A (2016), 371–390.

[BJ03] O. Billet and M. Joye. "The Jacobi Model of an Elliptic Curve and Side-Channel Analysis". In: *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. AAECC 2003. Lecture Notes in Computer Science*. Vol. 2643. 2003, pp. 34–42.

[Bon+18] D. Boneh, J. Bonneau, B. Bünz, and B. Fisch. "Verifiable Delay Functions". In: *Advances in Cryptology – CRYPTO 2018*. Ed. by H. Shacham and A. Boldyreva. Cham: Springer International Publishing, 2018, pp. 757–788.

[Boo+22] J. Booher et al. *Failing to hash into supersingular isogeny graphs*. Cryptology ePrint Archive, Paper 2022/518. 2022. URL: https://eprint.iacr.org/2022/518.

[Bre12] C. Brezinski. *History of Continued Fractions and Padé Approximants*. Springer Series in Computational Mathematics. Springer Berlin Heidelberg, 2012.

[Brö06] R. Bröker. "Constructing elliptic curves of prescribed order". PhD thesis. Universiteit Leiden, 2006. URL: https://hdl.handle.net/1887/4425.

[Brö09] R. Bröker. "Constructing supersingular elliptic curves". In: *Journal of Combinatorics and Number Theory* 1(3) (2009), pp. 269–273.

[Bro78] J. Browkin. "Continued fractions in local fields I". In: *Demonstratio Mathematica* 11 (1978), pp. 67–82.

[BSS05] I. Blake, G. Seroussi, and N. Smart. *Advances in Elliptic Curve Cryptography*. Vol. 317. London Mathematical Society lecture note series. Cambridge Univ. Press, 2005.

[BV07] J. Buchmann and U. Vollmer. *Binary Quadratic Forms: An Algorithmic Approach*. Vol. 20. Algorithms and Computation in Mathematics. Springer, 2007.

[Cap+23a] L. Capuano, S. Checcoli, M. Mula, and L. Terracini. *On $\mathfrak{P}$-adic continued fractions with extraneous denominators: some explicit finiteness results*. 2023. arXiv: 2311.14034 [math.NT].

[Cap+23b] L. Capuano, M. Mula, L. Terracini, and F. Veneziano. *p-adically convergent loci in varieties arising from periodic continued fractions*. To appear on arXiv. 2023.

[Cas+18a] W. Castryck, T. Lange, C. Martindale, L. Panny, and J. Renes. "CSIDH: An Efficient Post-Quantum Commutative Group Action". In: *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 2018, pp. 395–427.

[Cas+18b] W. Castryck, T. Lange, C. Martindale, L. Panny, and J. Renes. *CSIDH: An Efficient Post-Quantum Commutative Group Action*. Cryptology ePrint Archive, Report 2018/383. https://eprint.iacr.org/2018/383. 2018.

[Cas+18c] W. Castryck, T. Lange, C. Martindale, L. Panny, and J. Renes. "CSIDH: An Efficient Post-Quantum Commutative Group Action". In: *Advances in Cryptology – ASIACRYPT 2018*. Ed. by T. Peyrin and S. Galbraith. Cham: Springer International Publishing, 2018, pp. 395–427.

[Cas+23] W. Castryck, M. Houben, S.-P. Merz, M. Mula, S. van Buuren, and F. Vercauteren. "Weak Instances of Class Group Action Based Cryptography via Self-pairings". In: *Advances in Cryptology – CRYPTO 2023*. Ed. by H. Handschuh and A. Lysyanskaya. Full version on ePrint Archive available at https://eprint.iacr.org/2023/549. Cham: Springer Nature Switzerland, 2023, pp. 762–792.

[CD23] W. Castryck and T. Decru. "An Efficient Key Recovery Attack on SIDH". In: *Advances in Cryptology – EUROCRYPT 2023*. Ed. by C. Hazay and M. Stam. Cham: Springer Nature Switzerland, 2023, pp. 423–447.

[CJS14] A. Childs, D. Jao, and V. Soukharev. "Constructing elliptic curve isogenies in quantum subexponential time". In: *Journal of Mathematical Cryptology* 8.1 (2014), pp. 1–29.

[CK20] L. Colò and D. Kohel. "Orienting supersingular isogeny graphs". In: *Journal of Mathematical Cryptolology* 14.1 (2020), pp. 414–437.

[CLG09] D. X. Charles, K. E. Lauter, and E. Z. Goren. "Cryptographic Hash Functions from Expander Graphs". In: *Journal of Cryptology* 22 (1 2009), pp. 93–113.

[CMT22] L. Capuano, M. Mula, and L. Terracini. *Quaternionic p-adic continued fractions*. 2022. arXiv: 2208.03983 [math.NT].

[CO20] C. Ciliberto and G. Ottaviani. "The Hessian Map". In: *International Mathematics Research Notices* 2022.8 (Dec. 2020), pp. 5781–5817. eprint: https://academic.oup.com/imrn/article-pdf/2022/8/5781/43396011/rnaa288.pdf.

[Coh93] H. Cohen. *A course in computational algebraic number theory*. Vol. 138. Graduate Texts in Mathematics. Berlin: Springer-Verlag, 1993.

[Cou06] J.-M. Couveignes. *Hard homogeneous spaces*. Cryptology ePrint Archive, Report 2006/291. 2006. URL: https://eprint.iacr.org/2006/291.

[Cox13] D. A. Cox. *Primes of the Form $x^2 + ny^2$*. John Wiley & Sons, Ltd, 2013.

[CR88] L. S. Charlap and D. P. Robbins. *An elementary introduction to elliptic curves*. 1988. URL: https://cs.nyu.edu/courses/spring05/G22.3220-001/ec-intro1.pdf.

[CS17] C. Costello and B. Smith. "Montgomery curves and their arithmetic: The case of large characteristic fields". In: *Journal of Cryptographic Engineering* 8 (2017), pp. 227–240.

[CS+21] J. Chávez-Saab, J.-J. Chi-Domínguez, S. Jaques, and F. Rodríguez-Henríquez. "The SQALE of CSIDH: sublinear Vélu quantum-resistant isogeny action with low exponents". In: *Journal of Cryptographic Engineering* 11.4 (2021), pp. 307–319.

[CSRHT22] J. Chavez-Saab, F. Rodríguez-Henríquez, and M. Tibouchi. "Verifiable Isogeny Walks: Towards an Isogeny-Based Postquantum VDF". In: *Selected Areas in Cryptography*. Ed. by R. AlTawy and A. Hülsing. Cham: Springer International Publishing, 2022, pp. 441–460.

[CSV20] W. Castryck, J. Sotáková, and F. Vercauteren. "Breaking the decisional Diffie-Hellman problem for class group actions using genus theory". In: *Crypto 2020 Pt. 2*. Vol. 12171. Lecture Notes in Computer Science. Springer, 2020, pp. 92–120.

[Dar+23] P. Dartois, A. Leroux, D. Robert, and B. Wesolowski. *SQISignHD: New Dimensions in Cryptography*. Cryptology ePrint Archive, Paper 2023/436. 2023. URL: https://eprint.iacr.org/2023/436.

[Deu41] M. Deuring. "Die Typen der Multiplikatorenringe elliptischer Funktionenkörper". In: *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg* 14.1 (1941), pp. 197–272.

[DF+19] L. De Feo, S. Masson, C. Petit, and A. Sanso. "Verifiable Delay Functions from Supersingular Isogenies and Pairings". In: *Advances in Cryptology - ASIACRYPT 2019, 25th International Conference on the Theory and Application of Cryptology and Information Security*. 2019, pp. 248–277.

[DF+20] L. De Feo, D. Kohel, A. Leroux, C. Petit, and B. Wesolowski. *SQISign: compact post-quantum signatures from quaternions and isogenies*. Cryptology ePrint Archive, Report 2020/1240. https://eprint.iacr.org/2020/1240. 2020.

[DFJP14] L. De Feo, D. Jao, and J. Plût. "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies". In: *J. Mathematical Cryptology* 8.3 (2014), pp. 209–247.

[DG16] C. Delfs and S. D. Galbraith. "Computing isogenies between supersingular elliptic curves over F_p". In: *Designs, Codes and Cryptography* 78 (2016), pp. 425–440.

[Dic06] L. E. Dickson. "Criteria for the irreducibility of functions in a finite field". In: *Bulletin of the American Mathematical Society* 13.1 (1906), pp. 1 –8.

[Dic14] L. E. Dickson. "The Points of Inflexion of a Plane Cubic Curve". In: *Annals of Mathematics* 16.1/4 (1914), pp. 50–66. URL: http://www.jstor.org/stable/1968042 (visited on 06/27/2023).

[Dol18] J. Doliskani. "On division polynomial PIT and supersingularity". In: *Appl. Algebra Eng. Commun. Comput.* 29.5 (2018), pp. 393–407.

[Eic73] M. Eichler. "The Basis Problem for Modular Forms and the Traces of the Hecke Operators". In: *Modular Functions of One Variable I*. Ed. by W. Kuijk. Berlin, Heidelberg: Springer Berlin Heidelberg, 1973, pp. 75–152.

[Eis+18] K. Eisenträger, S. Hallgren, K. Lauter, T. Morrison, and C. Petit. "Supersingular Isogeny Graphs and Endomorphism Rings: Reductions and Solutions". In: *Advances in Cryptology – EUROCRYPT 2018*. Ed. by J. B. Nielsen and V. Rijmen. Springer International Publishing, 2018, pp. 329–368.

[Eis+20] K. Eisenträger, S. Hallgren, C. Leonardi, T. Morrison, and J. Park. "Computing endomorphism rings of supersingular elliptic curves and connections to pathfinding in isogeny graphs". In: *Fourteenth Algorithmic Number Theory Symposium*. 2020, pp. 215–232.

[Eng06] A. Enge. "The complexity of class polynomial computation via floating point approximations". In: *Mathematics of Computation* 78 (2006), pp. 1089–1107.

[FMP23] T. Fouotsa, T. Moriya, and C. Petit. "M-SIDH and MD-SIDH: countering SIDH attacks by masking information". In: *Advances in Cryptology – EUROCRYPT 2023*. Ed. by C. Hazay and M. Stam. Lecture Notes in Computer Science. 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2023 ; Conference date: 23-04-2023 Through 27-04-2023. Springer, Apr. 2023, pp. 282–309. DOI: 10.1007/978-3-031-30589-4_10.

[Gal+16] S. D. Galbraith, C. Petit, B. Shani, and Y. B. Ti. "On the Security of Supersingular Isogeny Cryptosystems". In: *Advances in Cryptology – ASIACRYPT 2016*. Ed. by J. H. Cheon and T. Takagi. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016, pp. 63–91.

[Gal18] S. D. Galbraith. *Mathematics of Public Key Cryptography. Version 2.0*. 2018. URL: https://www.math.auckland.ac.nz/~sgal018/crypto-book/main.pdf.

[GG13] J. von zur Gathen and J. Gerhard. *Modern Computer Algebra*. 3rd ed. Cambridge University Press, 2013.

[Has35] H. Hasse. "Existenz separabler zyklischer unverzweigter Erweiterungskörper vom Primzahlgrade p über elliptischen Funktionenkörpern der Charakteristik p." In: *Journal für die reine und angewandte Mathematik* 172 (1935), pp. 77–85.

[Hus87] D. Husemöller. *Elliptic Curves*. 2nd ed. Vol. 111. Graduate Texts in Mathematics. Springer New York, 1987.

[JMV09] D. Jao, S. Miller, and R. Venkatesan. "Expander graphs based on GRH with an application to elliptic curve cryptography". In: *Journal of Number Theory* 129 (June 2009), pp. 1491–1504.

[Koh96] D. Kohel. "Endomorphism rings of elliptic curves over finite fields". Ph.D thesis. 1996. URL: http://iml.univ-mrs.fr/~kohel/pub/thesis.pdf.

[KV10] M. Kirschmer and J. Voight. "Algorithmic enumeration of ideal classes for quaternion orders". In: *SIAM Journal on Computing* 39.5 (2010), pp. 1714–1747.

[Lan87] S. Lang. *Elliptic Functions*. Graduate texts in mathematics. Springer, 1987.

[LB20] J. Love and D. Boneh. "Supersingular Curves With Small Non-integer Endomorphisms". In: *Fourteenth Algorithmic Number Theory Symposium*. 2020, pp. 7–22.

[Len96] H. Lenstra, Jr. "Complex Multiplication Structure of Elliptic Curves". In: *Journal of Number Theory* 56.2 (1996), pp. 227–241. URL: https://www.sciencedirect.com/science/article/pii/S0022314X96900153.

[LO77] J. Lagarias and A. Odlyzko. "Effective Versions of the Chebotarev Density Theorem". In: *Algebraic Number Fields, L-Functions and Galois Properties (A. Fr6hlich, ed.)* Ed. by A. Press. 1977, pp. 409–464.

[Mai+23] L. Maino, C. Martindale, L. Panny, G. Pope, and B. Wesolowski. "A Direct Key Recovery Attack on SIDH". In: *Advances in Cryptology – EUROCRYPT 2023*. Ed. by C. Hazay and M. Stam. Cham: Springer Nature Switzerland, 2023, pp. 448–471.

[Mes86] J.-F. Mestre. "La méthode des graphes. Exemples et applications. [The method of graphs. Examples and applications]". In: *Proceedings of the International Conference on Class Numbers and Fundamental Units of Algebraic Number Fields (Katata, 1986)*. Nagoya University, Department of Mathematics, Nagoya. 1986, pp. 217–242.

[Mil20] J. S. Milne. *Algebraic Number Theory*. 2020. URL: http://www.jmilne.org/math/.

[MMP] L. Maino, M. Mula, and F. Pintore. "A review of mathematical and computational aspects of CSIDH algorithms". In: *Journal of Algebra and Its Applications* (). To appear under "Special Issue on Recent Advances in Coding Theory and Cryptography". eprint: https://doi.org/10.1142/S0219498825300028. URL: https://doi.org/10.1142/S0219498825300028.

[MMP22] M. Mula, N. Murru, and F. Pintore. *On Random Sampling of Supersingular Elliptic Curves*. Cryptology ePrint Archive, Paper 2022/528. 2022. URL: https://eprint.iacr.org/2022/528.

[Mor23] T. Moriya. *IS-CUBE: An isogeny-based compact KEM using a boxed SIDH diagram*. Cryptology ePrint Archive, Paper 2023/1506. 2023. URL: https://eprint.iacr.org/2023/1506.

[MOT20] T. Moriya, H. Onuki, and T. Takagi. "SiGamal: A Supersingular Isogeny-Based PKE and Its Application to a PRF". In: *Advances in Cryptology – ASIACRYPT 2020*. Ed. by S. Moriai and H. Wang. Cham: Springer International Publishing, 2020, pp. 551–580.

[OKS00] K. Okeya, H. Kurumatani, and K. Sakurai. "Elliptic Curves with the Montgomery-Form and Their Cryptographic Applications". In: *Public Key Cryptography*. Ed. by H. Imai and Y. Zheng. Berlin, Heidelberg: Springer Berlin Heidelberg, 2000, pp. 238–257.

[Onu21] H. Onuki. "On oriented supersingular elliptic curves". In: *Finite Fields and Their Applications* 69 (2021), p. 101777.

[Piz98] A. K. Pizer. "Ramanujan graphs". In: *Computational perspectives on number theory (Chicago, IL, 1995)*. Amer. Math. Soc., 1998, 159–178.

[Rob23] D. Robert. "Breaking SIDH in Polynomial Time". In: *Advances in Cryptology – EUROCRYPT 2023*. Ed. by C. Hazay and M. Stam. Cham: Springer Nature Switzerland, 2023, pp. 472–503.

[RS06] A. Rostovtsev and A. Stolbunov. *PUBLIC-KEY CRYPTOSYSTEM BASED ON ISOGENIES*. Cryptology ePrint Archive, Report 2006/145. `https://eprint.iacr.org/2006/145`. 2006.

[Rub70] A. A. Ruban. "Certain metric properties of the p-adic numbers". In: *Sibirsk. Mat. Ž.* 11 (1970), pp. 222–227.

[Sal79] G. Salmon. *A Treatise on the Higher Plane Curves: Intended as a Sequel to a Treatise on Conic Sections*. Hodges, Foster, 1879. URL: `https://archive.org/details/3edtreatiseonhighesalmuoft/mode/2up`.

[Sch07] S. L. Schmoyer. "Triviality and Nontriviality of Tate-Lichtenbaum Self Pairings". PhD thesis. University of Maryland (College Park, Md.), 2007.

[Sch85] R. Schoof. "Elliptic Curves Over Finite Fields and the Computation of Square Roots mod p". In: *Mathematics of Computation* 44.170 (1985), pp. 483–494.

[Sch87] R. Schoof. "Nonsingular plane cubic curves over finite fields". In: *Journal of Combinatorial Theory, Series A* 46.2 (1987), pp. 183 –211.

[Sho97] P. W. Shor. "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". In: *SIAM Journal on Computing* 26.5 (1997), 1484—1509. URL: `https://arxiv.org/abs/quant-ph/9508027`.

[Sie35] C. L. Siegel. "Über die Classenzahl quadratischer Zahlkörper". In: *Acta Arithmetica* 1 (1935), pp. 83–86.

[Sil09] J. H. Silverman. *The Arithmetic of Elliptic Curves*. Vol. 151. Graduate Texts in Mathematics. Springer, 2009.

[Sil10] J. H. Silverman. "A Survey of Local and Global Pairings on Elliptic Curves and Abelian Varieties". In: *Pairing-Based Cryptography - Pairing 2010*. Ed. by M. Joye, A. Miyaji, and A. Otsuka. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 377–396.

[Sil94] J. Silverman. *Advanced topics in the arithmetic of elliptic curves*. Springer-Verlag, 1994.

[SV21] M. Stanojkovski and C. Voll. "Hessian Matrices, Automorphisms of p-Groups, and Torsion Points of Elliptic Curves". In: *Mathematische Annalen* 381.1 (2021), pp. 593–629. URL: https://doi.org/10.1007/s00208-021-02193-8.

[Tat66] J. Tate. "Endomorphisms of abelian varieties over finite fields". In: *Inventiones mathematicae* 2 (1966), pp. 134–144.

[Ter99] A. Terras. *Fourier Analysis on Finite Groups and Applications*. London Mathematical Society Student Texts. Cambridge University Press, 1999.

[Vél71] J. Vélu. "Isogénies entre courbes elliptiques". In: *Comptes Rendus de l'Académie des Sciences de Paris* 273 (1971), pp. 238–241.

[Vit19] V. Vitse. "Simple Oblivious Transfer Protocols Compatible with Supersingular Isogenies". In: *Progress in Cryptology – AFRICACRYPT 2019*. Ed. by J. Buchmann, A. Nitaj, and T. Rachidi. Cham: Springer International Publishing, 2019, pp. 56–78.

[Voi21] J. Voight. *Quaternion Algebras*. Graduate Texts in Mathematics. Springer International Publishing, 2021. URL: https://link.springer.com/book/10.1007/978-3-030-56694-4.

[Was08] L. C. Washington. *Elliptic Curves: Number Theory and Cryptography, Second Edition*. 2nd ed. Chapman & Hall/CRC, 2008.

[Wat69] W. C. Waterhouse. "Abelian varieties over finite fields". In: *Annales scientifiques de l'École Normale Supérieure* Ser. 4, 2.4 (1969), pp. 521–560. URL: http://www.numdam.org/item/ASENS_1969_4_2_4_521_0.

[Wes21] B. Wesolowski. "The supersingular isogeny path and endomorphism ring problems are equivalent". In: *62nd IEEE Annual Symposium on Foundations of Computer Science, FOCS 2021, Denver, CO, USA, February 7-10, 2022*. IEEE, 2021, pp. 1100–1111.

[Wes22] B. Wesolowski. "Orientations and the Supersingular Endomorphism Ring Problem". In: *Advances in Cryptology – EUROCRYPT 2022*. Ed. by O. Dunkelman and S. Dziembowski. Cham: Springer International Publishing, 2022, pp. 345–371.