university of groningen / faculty of science and engineering / mathematics and applied mathematics

TNO

Design choices in CSIDH

Master's Project Mathematics

July 2025

Student: Anna W.A. de Bruijn

First supervisor: Ekin Özman

Second assessor: Jaap Top

Supervisor TNO Groningen: Sven E. Bootsma

Supervisor TNO Den Haag: Thomas Attema

Acknowledgements

This master thesis was written during an internship at TNO, made possible by Sven Bootsma. Many thanks to the lovely people at TNO, there are too many of you to mention you all here. In particular, I would like to thank my supervisors Sven and Thomas for their support and helpful feedback. I would also like to thank Ekin, my first supervisor at the university, for her feedback and encouragement in times when writing things down was difficult. Also, thank you Jaap, not only for setting up the internship together with Sven, but also for the many inspiring algebra courses during my time as a mathematics student at the University of Groningen.

Abstract

The Commutative Supersingular Isogeny Diffie-Hellman (CSIDH) protocol uses commutative group actions based on the theory of complex multiplication. It is constructed from the Couveignes-Rostovtsev-Stolbunov scheme by design choices that speed up the group action computations significantly. We discuss the mathematics behind the choices for Vélu's equations and supersingular Montgomery curves.

Contents

1 Introduction

Research into quantum computing is progressing fast if we may believe the many press releases on the website of Science Daily. It seems, therefore, that the invention of a stable large-scale quantum computer is only a matter of time. On the one hand, many cryptographic applications can benefit from their use, since they speed up calculations dramatically. On the other hand, however, many cryptographic protocols in current digital infrastructure do not withstand attacks by large-scale quantum computers. In order to combat this looming threat, the National Institute of Standards and Technology[1] (NIST) has funded research of global experts into finding cryptographic algorithms based on intractable problems for both classical and quantum computers, called *post-quantum cryptography* (PQC). One of the proposals in the domain of isogeny-based PQC that came about too late to be submitted for the first round, is *Commutative Supersingular Isogeny Diffie-Hellman* (CSIDH). It was first introduced in 2018 by Wouter Castryck, Tanja Lange, Chloe Martindale, Joost Renes and Lorenz Panny in the eponymous paper [Cas+18]. The intractability of isogeny-based PQC remains to date.

CSIDH is a proposal for a post-quantum-secure key exchange protocol using the hardness of recovering isogenies from the elliptic curves in their (co-)domain. Based on the Couveignes-Rostovtsev-Stolbunov scheme, it is made substantially more efficient by a clever choice of parameters. With this master thesis, we inform the reader of the reasons behind some design choices and discuss their mathematical foundation.

Let us outline the structure from beginning to end. We start by introducing the reader to cryptographic group actions, the complex multiplication (CM) group action on elliptic curves that give rise to isogenies and the resulting isogeny graphs. This introduction establishes the mathematics of the CRS scheme, introduced by Couveignes [Cou06] and independently rediscovered by Rostovtsev, Stolbunov [RS06]. From that foundation we introduce the design choices that CSIDH is built on. In the next two chapters, we highlight two of these design choices. We address the use of supersingular elliptic curves, and introduce the reader to the properties of Montgomery curves: elliptic curves that can be defined by an equation of the form $By^2 = x^3 + Ax^2 + x$ over a finite field. Throughout the text, we assume prior knowledge about class group theory, commutative algebra and elliptic curves.

1.1 Contributions

This thesis is meant to be an overview of and introduction to the intricacies of CSIDH. It does therefore not contain many new results. Contributions consist of enlightening Examples (e.g. Examples 2.6, 2.17, 3.2, 3.7) and the proof of Theorem 4.5 in [DG16, Equation (1) on page 426]. Moreover, we also include improved versions of the proofs to Theorem 3.5 in [DG16, Theorem 2.7] and Proposition 3.6 in [Cas+18, Proposition 8].

[1] NIST is an agency within the U.S. Department of Commerce.

1.2 Notation

k: a perfect field.

$\mathbb{F}_q$: the finite field of characteristic p such that $q = p^r$ for some $r \in \mathbb{Z}_{>0}$.

K: a number field.

$\mathcal{O}$: an order of a number field K.

$\mathcal{O}_K$: the ring of integers of the number field K and the maximal order.

$\mathrm{Ell}(\mathcal{O})$: the set of isomorphism classes of ordinary elliptic curves defined over $\mathbb{C}$ with complex multiplication by fractional $\mathcal{O}$-ideals in an order $\mathcal{O}$ of a quadratic imaginary number field K.

$\mathrm{Ell}_{\overline{\mathbb{F}}_q}(\mathcal{O})$: the set of $\overline{\mathbb{F}}_q$-rational isomorphism classes of ordinary elliptic curves defined over $\mathbb{F}_q$ with complex multiplication by fractional $\mathcal{O}$-ideals in an order $\mathcal{O}$ in a quadratic imaginary number field K.

$\mathrm{Ell}_{\mathbb{F}_q}(\mathcal{O})$: the set of $\mathbb{F}_q$-rational isomorphism classes of elliptic curves defined over $\mathbb{F}_q$ with complex multiplication by fractional $\mathcal{O}$-ideals in an order $\mathcal{O}$ in a quadratic imaginary number field K.

$h(\mathcal{O})$: the order of the class group $\mathrm{Cl}(\mathcal{O})$.

$\mathrm{End}_p(E)$: the $\mathbb{F}_p$-rational endomorphism ring of an elliptic curve E over the prime field $\mathbb{F}_p$. It is a subring of the full endomorphism ring $\mathrm{End}(E)$.

$G_{k,L}$: the isogeny graph consisting of k-rational equivalence classes of ℓ-isogenies as edges, where $\ell \in L$, and k-isomorphism classes of supersingular elliptic curves with complex multiplication defined over k.

$\cong$: isomorphism of [*specified algebraic structure*].

$\approx$: approximation of a real number in decimal places.

$\simeq$: asymptotically equal, meaning equal in the limit.

L_q: logarithmic notation, or L-notation, see Definition C.7.

$\tilde{O}$: read: 'soft O', see Definition C.2.

2 Preliminaries

2.1 Diffie-Hellman key exchange and cryptographic group actions

Consider the scenario in which two parties, commonly called Alice and Bob, would like to send each other messages over an insecure channel. One of the methods they could use in order to keep the contents of the messages secret, is to construct a common key to encrypt and decrypt the message in a symmetrical process. The Diffie-Hellman key exchange [DH22] is a protocol to establish such a common key over an insecure channel. This protocol uses *abelian group actions*, which is a group action where the group in question is abelian.

Definition 2.1 (Group action)**.** Let G be a group and X a nonempty set. A group action of $(G, X, \star)$ is a map $\star\colon G \times X \to X$ which we write as $(g, x) \mapsto g \star x$, satisfying

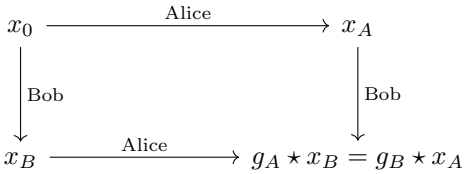
1. $e \star x = x$ for every $x \in X$ (here $e \in G$ is the unit element);
2. $(gh) \star x = g \star (h \star x)$ for all $g, h \in G$ and all $x \in X$.

The Diffie-Hellman key exchange protocol is then defined as follows.

Setup of public parameters: an abelian group action $(G, X, \star)$ and fixed base point $x_0 \in X$.

Key generation: the secret key g_C randomly sampled from G. The public key $x_C := g_C \star x_0$.

Key exchange: Alice and Bob have key pairs (g_A, x_A) and (g_B, x_B) respectively. Upon the publication of x_B, Alice computes $g_A \star x_B$. Similarly for Bob. They recover a shared secret key.



In terms of practicality, x_A and x_B must be computationally easy to compute while recovering g_A and g_B must be hard. The following conditions aim to provide these characteristics.

A *Principal Homogeneous Space* (PHS) for a group G is a set X with an action $(G, X, \star)$ such that for any $x_1, x_2 \in X$ there exists a unique g in G such that $g \star x_1 = x_2$. In other words, the map $\varphi_x\colon G \to X$ defined by $g \mapsto g \star x$ is a bijection for any x. A *Hard Homogeneous Space* (HHS) is a PHS where the group action $(G, X, \star)$ is computationally efficient, but inverting φ_x is difficult for any x. It was first introduced in a seminal work by Couveignes in 1997, see [Cou06]. An example of an (assumed and classical) HHS is the group $G = (\mathbb{Z}/p\mathbb{Z})^*$ together with the set $X = \langle x_0 \rangle - \{1\}$ where x_0 generates a group of order p, a prime. The map φ_x sends each g to $g \star x = x^g$. Inverting φ_x is the Discrete Logarithm Problem (DLP).

In order for the group action to be suitable for implementation in a computer algorithm, we would like for the group action to be *effective* according to the following definition, taken from [NP20, Definition 2]. This requires the representation of group- and set elements as bit strings, on which we perform computations.

Definition 2.2 ([NP20], Definition 2)**.** A group action $(G, X, \star)$ is effective if the following properties are satisfied:

1. The group G is finite and there exist efficient probabilistic polynomial time (PPT) algorithms for:
   (a) Membership testing, i.e., to decide if a given bit string represents a valid group element in G.
   (b) Equality testing, i.e., to decide if two bit strings represent the same group element in G.
   (c) Sampling, i.e., to sample an element g from a distribution $\mathcal{D}_G$ on G. We consider distributions that are statistically close to uniform[2].

[2]For the complex multiplication group action, this implies we assume that the distribution of small normed ideals in the class group of an order are uniformly distributed.

(d) Operation, i.e., to compute gh for any $g, h \in G$.

(e) Inversion, i.e., to compute g^{-1} for any $g \in G$.

2. The set X is finite and there exist efficient algorithms for:

   (a) Membership testing, i.e., to decide if a bit string represents a valid set element.

   (b) Unique representation, i.e., given any arbitrary set element $x \in X$, compute a string $\hat{x}$ that canonically represents x.

3. There exists a distinguished element $x_0 \in X$, called the origin, such that its bit-string representation is known.

4. There exists an efficient algorithm that given (some bit-string representations of) any $g \in G$ and any $x \in X$, outputs $g \star x$.

A group action is called *cryptographic* if it is effective and defines a HHS. We recall an example of such a cryptographic group action, where $g \star x = x^g$ with $g \in G = (\mathbb{Z}/p\mathbb{Z})^*$ for p a prime and $x \in X = \langle x_0 \rangle - \{1\}$. The algorithms for computing discrete logarithms for a generic group G and set $X = \langle x_0 \rangle - \{1\}$ require $O(\sqrt{q})$ computations[3], see [Jou09], and are optimal for generic groups G [Sho97]. This does not exclude the existence of better attacks for specific group actions. However, no better classical algorithms are known to exist when G is a subgroup of $E(\mathbb{F}_p)$, where E is an elliptic curve defined over $\mathbb{F}_p$. This fact establishes the robustness of[4] the Elliptic Curve Diffie-Hellman (ECDH) protocol. In ECDH $X = \langle P \rangle - \{O\}$ where P is a $\mathbb{F}_p$-rational point of order ℓ, where ℓ divides $\#E(\mathbb{F}_p)$, on an elliptic curve E defined over $\mathbb{F}_p$, and $G = (\mathbb{Z}/\ell\mathbb{Z})^*$. The maps $\phi_Q \colon (\mathbb{Z}/\ell\mathbb{Z})^* \to \langle P \rangle - \{1\}$ are defined by $n \star Q = [n]Q$, where $[n]$ denotes the multiply-by-n isogeny. The elliptic curve DLP is a computationally hard problem for classical computers because of the unpredictability of scalar multiplication on an elliptic curve.

However, Shor's quantum algorithm is expected to solve DLPs in polynomial time on a quantum computer [Sho94]. Hence, Diffie-Hellman key exchange protocols based on the DLP, such as ECDH, are unsafe against quantum adversaries. Since we expect quantum computers to become operable in the near future, this motivates the search for new abelian group actions that withstand quantum attacks. In the seminal work [Cou06], Couveignes introduces a specific HHS based on complex multiplication of elliptic curves that is conjecturally post-quantum secure. This master thesis explores the mathematics behind the protocol it inspired.

2.2 Elliptic curves with complex multiplication

For the theory on elliptic curves we refer the reader to Silverman's *The Arithmetic of Elliptic Curves*, see [Sil86]. We are specifically interested in elliptic curves E that have *complex multiplication* (CM). In short, this means the endomorphism ring $\mathrm{End}(E)$ of E contains strictly more endomorphisms than the multiplication-by-m endomorphisms. The following theorem fully characterizes the endomorphism ring of E.

Theorem 2.3 (Deuring, [Sil86] Corollary III.9.4, [Koh96] and [Feo17] Theorem 53.)**.** *Let E be an elliptic curve defined over a field k of characteristic p. The endomorphism ring* $\mathrm{End}(E)$ *is isomorphic to one of the following:*

- $\mathbb{Z}$*;*
- *An order $\mathcal{O}$ in a quadratic imaginary field; in this case we say that E has complex multiplication by $\mathcal{O}$;*
- *Only if $p > 0$, a maximal order $\mathcal{O}$ in the quaternion algebra $B_{p,\infty}$; in this case we say that E has quaternionic multiplication by $\mathcal{O}$. This happens if and only if E is supersingular.*

The theory of complex multiplication is an involved topic within mathematics. Some of its characteristics yield a structure that turns out to be a possible candidate for cryptographic group actions. In order to discern this structure, we first consider ordinary elliptic curves with CM defined over a number field.

[3] Here q is the largest prime divisor of $p - 1$. For e.g. 256-bit security, we choose G such that $\log_2(q) \approx 256$.

[4] In the 1980's suggested by Miller [Mil85] and Koblitz [Kob87].

2.2.1 Elliptic curves with complex multiplication over a number field

Let us consider an ordinary elliptic curve $E/\mathbb{C}$ with complex multiplication by a maximal order $\mathcal{O}_K$, the ring of integers of a quadratic imaginary number field K. We recall the uniformization theorem [Sil86, Theorem VI.5.1] proving that for any such $E/\mathbb{C}$ there exists a full lattice $\Lambda \subset \mathbb{C}$ and an isomorphism

$$f\colon \mathbb{C}/\Lambda \xrightarrow{\sim} E(\mathbb{C}).$$

Let us therefore denote the elliptic curve corresponding to a lattice Λ by E_Λ. We also recall from [Sil86, p. VI.5.3] that

$$\mathrm{End}(E_\Lambda) \cong \{\alpha \in \mathbb{C}\colon \alpha\Lambda \subset \Lambda\}$$

as a ring. Indeed, each α satisfying $\alpha\Lambda \subset \Lambda$ yields an endomorphism $[\alpha]$ due to the commutativity of the following diagram [Sil94, Page 97].

$$\begin{array}{ccc} \mathbb{C}/\Lambda & \xrightarrow{z\mapsto\alpha\cdot z} & \mathbb{C}/\Lambda \\ \Big\downarrow{\scriptstyle f} & & \Big\downarrow{\scriptstyle f} \\ E_\Lambda & \xrightarrow{[\alpha]} & E_\Lambda \end{array}$$

We notice, see [Sil94, Chapter II], that a non-zero fractional $\mathcal{O}_K$-ideal[5] $\mathfrak{a}$ in a quadratic imaginary number field K is a full lattice in $\mathbb{C}$. Hence,

$$\begin{aligned} \mathrm{End}(E_\mathfrak{a}) &\cong \{\alpha \in \mathbb{C}\colon \alpha\mathfrak{a} \subset \mathfrak{a}\} \\ &= \{\alpha \in K\colon \alpha\mathfrak{a} \subset \mathfrak{a}\} \quad \text{since } \mathfrak{a} \subset K \\ &= \mathcal{O}_K. \end{aligned}$$

Therefore, any non-zero fractional $\mathcal{O}_K$-ideal $\mathfrak{a}$ yields an elliptic curve $E_\mathfrak{a}$ with complex multiplication by $\mathcal{O}_K$. Moreover, since *homothetic* lattices[6] yield isomorphic elliptic curves, we find that $\mathfrak{a}$ and $c\mathfrak{a}$ give rise to isomorphic elliptic curves $E_\mathfrak{a} \cong E_{c\mathfrak{a}}$ with complex multiplication by $\mathcal{O}_K$, see [Sil86, Corollary VI.4.1.1]. Therefore, there must exist a direct link between isomorphism classes of ordinary elliptic curves with CM by $\mathcal{O}_K$ and ideal classes in the ideal class group $\mathrm{Cl}(\mathcal{O}_K)$.

Definition 2.4 (Ideal class group)**.** Let $\mathcal{O}_K$ be the ring of integers of a number field K. Let $\mathcal{I}(\mathcal{O}_K)$ be the group of invertible[7] fractional $\mathcal{O}_K$-ideals, and let $\mathcal{P}(\mathcal{O}_K)$ be the group of principal ideals.

The ideal *class group* of $\mathcal{O}_K$ is the quotient group

$$\mathrm{Cl}(\mathcal{O}_K) = \mathcal{I}(\mathcal{O}_K)/\mathcal{P}(\mathcal{O}_K).$$

It is a finite abelian group; its order is called the class number of $\mathcal{O}_K$, and denoted by $h(\mathcal{O}_K)$.

For a non-zero fractional $\mathcal{O}_K$-ideal $\mathfrak{a}$, let $\overline{\mathfrak{a}}$ denote its ideal class in $\mathrm{Cl}(\mathcal{O}_K)$. Let $\mathrm{Ell}(\mathcal{O}_K)$ be the set of isomorphism classes of elliptic curves with CM by $\mathcal{O}_K$. We know that there is a map $\mathrm{Cl}(\mathcal{O}_K) \to \mathrm{Ell}(\mathcal{O}_K)$ given by $\overline{\mathfrak{a}} \mapsto E_\mathfrak{a}$ as above. Moreover, by [Sil94, Proposition II.1.2] there is a well-defined group action of $\mathrm{Cl}(\mathcal{O}_K)$ on $\mathrm{Ell}(\mathcal{O}_K)$ determined by $\overline{\mathfrak{a}} \star E_\Lambda = E_{\mathfrak{a}^{-1}\Lambda}$.

Suppose $\mathfrak{a}$ is an integral $\mathcal{O}_K$-ideal. We define the $\mathfrak{a}$-torsion subgroup $E_\Lambda[\mathfrak{a}]$ of $E_\Lambda/\mathbb{C}$ by

$$\begin{aligned} E_\Lambda[\mathfrak{a}] &= \{P \in E_\Lambda(\mathbb{C})\colon [\alpha]P = O \text{ for all } \alpha \in \mathfrak{a}\} \\ &\cong \{z \in \mathbb{C}/\Lambda\colon \alpha z = 0 \text{ for all } \alpha \in \mathfrak{a}\} \\ &= \{z \in \mathbb{C}\colon \alpha z \in \Lambda \text{ for all } \alpha \in \mathfrak{a}\}/\Lambda \\ &= \{z \in \mathbb{C}\colon z\mathfrak{a} \subset \Lambda\}/\Lambda \\ &= \mathfrak{a}^{-1}\Lambda/\Lambda \\ &= \ker(\mathbb{C}/\Lambda \to \mathbb{C}/\mathfrak{a}^{-1}\Lambda) \\ &= \ker(E \to \overline{\mathfrak{a}} \star E), \end{aligned}$$

[5] Where $\mathcal{O}_K$ denotes the ring of integers of K.

[6] We know Λ_1 and Λ_2 are homothetic if there exists $c \in \mathbb{C}$ such that $c\Lambda_1 = \Lambda_2$.

[7] Recall that non-zero fractional ideals of a Dedekind ring are invertible. The ring of integers of a number field is a Dedekind ring.

where $E \to \mathfrak{a} \star E$ defines an isogeny. So if $\mathfrak{a} = m\mathcal{O}_K$ for an integer m, then $E[\mathfrak{a}]$ is just $E[m]$. We notice that the endomorphisms, such as the multiplication-by-m isogeny, must be defined by the non-zero fractional principal $\mathcal{O}_K$-ideals.

The modular j-invariant of the lattice $\mathfrak{a}$ is an algebraic integer $j(\mathfrak{a})$ such that $K(j(\mathfrak{a}))$ is the ring class field of the order $\mathcal{O}_K$, see [Cox22, Theorem 11.1]. For a fixed order $\mathcal{O}_K$, all the $j(\mathfrak{a})$ are conjugate and give rise to the splitting field $K(j(\mathfrak{a}))$, a ramified abelian[8] extension of K. The following result highlights the remarkable connection between the class group and the modular j-invariant, and thus also to elliptic curves with complex multiplication.

Theorem 2.5 ([Sil94], Theorem II.4.3 and Proposition II.2.4)**.** *Let $\mathcal{O}_K$ be the maximal order of an imaginary quadratic number field $K/\mathbb{Q}$, and let $\mathfrak{a}_1, \ldots, \mathfrak{a}_{h(\mathcal{O}_K)}$ be representatives of $\mathrm{Cl}(\mathcal{O}_K)$. Then:*

(1) $K\left(j\left(\mathfrak{a}_i\right)\right)$ is an abelian extension of K;

(2) The $j\left(\mathfrak{a}_i\right)$ are all conjugate over K;

(3) The Galois group of $K\left(j\left(\mathfrak{a}_i\right)\right)$ is isomorphic to $\mathrm{Cl}(\mathcal{O}_K)$ via

$$F\colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{Cl}(\mathcal{O}_K),$$

uniquely characterized by the condition $E^\sigma = F(\sigma)\star E$ for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$ and all $E \in \mathrm{Ell}_{\overline{\mathbb{F}}_q}(\mathcal{O}_K)$;

(4) $[\mathbb{Q}\left(j\left(\mathfrak{a}_i\right)\right) : \mathbb{Q}] = [K\left(j\left(\mathfrak{a}_i\right)\right) : K] = h(\mathcal{O}_K)$;

(5) The $j\left(\mathfrak{a}_i\right)$ are integral, their minimal polynomial is called the Hilbert class polynomial *of $\mathcal{O}_K$;*

(6) $\mathrm{Cl}(\mathcal{O}_K)$ acts freely and transitively on $\mathrm{Ell}_{\overline{\mathbb{F}}_q}(\mathcal{O}_K)$, in particular $\#\,\mathrm{Ell}_{\overline{\mathbb{F}}_q}(\mathcal{O}_K) = h(\mathcal{O}_K)$.

Example 2.6. In this example we compute the group action of ideal classes on elliptic curves. However, rather than choosing a starting curve, we start with the ring of integers of the number field $\mathbb{Q}(\sqrt{-5})$. Using Theorem 2.5, compute the elliptic curves defined by the invertible ideals that generate $\mathrm{Cl}(\mathcal{O}_{\mathbb{Q}(\sqrt{-5})})$.

Let us consider the imaginary quadratic number field $K = \mathbb{Q}(\sqrt{-5})$. Notice $-5 \equiv 3 \bmod 4$ and so $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. Since $\Delta(\mathbb{Z}[\sqrt{-5}]) = -20$, we find that $\mathrm{Cl}(\mathbb{Z}[\sqrt{-5}])$ is generated by ideal classes of the primes of norm at most $\left(\frac{2}{\pi}\right)\sqrt{20} < 3$ due to Minkowski's theorem. Then the unique prime $\mathfrak{p}_2 = (2, 1+\sqrt{-5})$ of norm 2 is non-principal and its square is generated by 2. Thus, $\mathrm{Cl}(\mathbb{Z}[\sqrt{-5}]) \cong \mathbb{Z}/2\mathbb{Z}$ meaning $h_K = 2$. Therefore, the Hilbert class polynomial must be quadratic. We compute it using `Magma`, see Appendix A.1, where the ideal $\mathfrak{p}_2$ is the complex lattice $2\mathbb{Z} + (1+\sqrt{-5})\mathbb{Z}$, meaning $\tau = \frac{1+\sqrt{-5}}{2}$. It defines the number field $K = \mathbb{Q}(\sqrt{-5})$ and so $\Delta_K = -20$. Next, we use a functionality in `Magma` that takes the discriminant Δ_K as input and yields the Hilbert class polynomial $H(x)$ as output, see line 6 in Appendix A.1.

We find that the roots of H lie in the field extension $L = \mathbb{Q}(\sqrt{5})$. One of the roots of H we denote $a = 320(1975 - 884\sqrt{5}) \in L$, the roots are given by a and $-a + 1264000$. They are the j-invariants of two elliptic curves,

$$E_1\colon y^2 = x^3 - x^2 + \frac{1}{2176}(-121a - 182435008)x + \frac{1}{2176}(7139a + 41742920512)$$
$$E_2\colon y^2 = x^3 - x^2 + \frac{1}{2176}(121a - 335379008)x + \frac{1}{2176}(-7139a + 50766616512)$$

defined over L. According to Theorem 2.5 (3), the class group $\mathrm{Cl}(\mathcal{O}_K)$ is isomorphic to $\mathrm{Gal}(K(\sqrt{5})/K)$. The latter contains the identity automorphism and the non-trivial action $\sigma \in \mathrm{Gal}(K(\sqrt{5})/K)$ defined by $\sigma(\sqrt{5}) = -\sqrt{5}$ and $\sigma(\sqrt{-5}) = \sqrt{-5}$ meaning $\sigma(i) = -i$. We use it to compute the complex multiplication action via the map $F\colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{Cl}(\mathcal{O}_K)$. We know

$$E_1^\sigma\colon y^2 = x^3 - x^2 + \frac{1}{2176}(-121\sigma(a) - 182435008)x + \frac{1}{2176}(7139\sigma(a) + 41742920512)$$
$$E_2^\sigma\colon y^2 = x^3 - x^2 + \frac{1}{2176}(121\sigma(a) - 335379008)x + \frac{1}{2176}(-7139\sigma(a) + 50766616512)$$

and since $\sigma(a) = 320(1975 + 884\sqrt{5}) = -a + 1264000$, we find $E_1^\sigma = E_2$ and $E_2^\sigma = E_1$. Thus, $E_2 = \overline{\mathfrak{p}}_2 \star E_1$ and $E_1 = \overline{\mathfrak{p}}_2 \star E_2$. ♙

[8] Such that its Galois group is abelian.

So far we only defined complex multiplication by a maximal order $\mathcal{O}_K$. However, curves with CM by a maximal order also have CM by suborders using the fact that $\mathcal{O}$ has conductor[9] f with respect to $\mathcal{O}$.

Proposition 2.7 ([Cox22], Proposition 7.20)**.** *Let $\mathcal{O}$ be an order of conductor f in an imaginary quadratic field K and $\mathcal{O}_K$ its ring of integers.*

(i) If $\mathfrak{a}$ is an $\mathcal{O}_K$-ideal prime[10] *to f, then $\mathfrak{a} \cap \mathcal{O}$ is an $\mathcal{O}$-ideal prime to f of the same norm.*

(ii) If $\mathfrak{a}$ is an $\mathcal{O}$-ideal prime to f, then $\mathfrak{a}\mathcal{O}_K$ is an $\mathcal{O}_K$-ideal prime to f of the same norm.

(iii) The map $\mathfrak{a} \mapsto \mathfrak{a} \cap \mathcal{O}$ induces an isomorphism

$$I_K(f) = \{\mathcal{O}_K\text{-ideals prime to } f\} \xrightarrow{\sim} \{\mathcal{O}\text{-ideals prime to } f\} = I(\mathcal{O}, f),$$

and the inverse of this map is given by $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_K$.

We can therefore define $\mathrm{Cl}(\mathcal{O})$, with $\mathcal{O}$ not necessarily maximal, as follows.

Proposition 2.8 ([Cox22], Proposition 7.19 and Proposition 7.22)**.** *Let $\mathcal{O}$ be an order of conductor f in an imaginary quadratic field K. Then there are natural isomorphisms*

$$\mathrm{Cl}(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O}) \cong I(\mathcal{O}, f)/P(\mathcal{O}, f) \cong I_K(f)/P_{K,\mathbb{Z}}(f),$$

where $I(\mathcal{O})$ is the set of proper fractional $\mathcal{O}$-ideals and $P_{K,\mathbb{Z}}(f)$ is the subgroup of $I_K(f)$ generated by principal ideals of the form $\alpha\mathcal{O}_K$, where $\alpha \in \mathcal{O}_K$ satisfies $\alpha \equiv a \bmod f\mathcal{O}_K$ for some integer a relatively prime to f.

In the context of a cryptographic protocol, we do not care much for elliptic curves defined over number fields. Rather, we want the elliptic curves to be defined over finite fields $\mathbb{F}_q$ where $q = p^n$ is a prime power, because as a result the isogeny graph (see Chapter 2.3) is of finite size. In other words, the set and group G, X we want to compute group actions on, are of finite size in this context. In the next section we explore which properties of complex multiplication remain true when we shift our focus to elliptic curves with CM defined over a finite field $\mathbb{F}_q$.

2.2.2 Elliptic curves with complex multiplication over a finite field

The following result from [Feo17, Theorem 74] based on [Lan87, Chapter 10 §4] relates elliptic curves with CM by an order $\mathcal{O} \subset K$ defined over a number field, to their reductions with CM by the same order defined over a finite field. Moreover, depending on the splitting behavior of primes in K, it also tells us whether the reduction is ordinary or supersingular.

Theorem 2.9 (Deuring, [Lan87] Chapter 10 §4)**.** *Let E be an elliptic curve over a number field L, with complex multiplication by an order $\mathcal{O} \subset K$. Let $\mathfrak{p}$ be a place of L over p, and assume that E has non-singular reduction modulo $\mathfrak{p}$, denoted by $E(\mathfrak{p})$. The curve $E(\mathfrak{p})$ is supersingular if and only if p has only one prime of K above it (p fully ramifies or remains prime in K).*

Suppose that p splits completely in K. Let f be the conductor of $\mathcal{O}$, and write $f = p^r f_0$, where $p \nmid f_0$. Then:

- *$E(\mathfrak{p})$ has complex multiplication by the order in K with conductor f_0.*
- *If $p \nmid f$, then the map $\omega \mapsto \omega(\mathfrak{p})$ defines an isomorphism of* $\mathrm{End}(E)$ *and* $\mathrm{End}(E(\mathfrak{p}))$.

Example 2.10 ([Feo17], Examples 73,75)**.** Let us consider the order $\mathbb{Z}[i] \subset \mathbb{Q}(i)$. We know $\mathbb{Z}[i]$ is a PID and thus the class group $\mathrm{Cl}(\mathcal{O})$ is trivial. We compute $j(\mathbb{Z}[i]) = 1728$ viewing $\mathbb{Z}[i]$ as a lattice, see [Sil86, Exercise 6.6]. From this j-invariant and the formula for the discriminant[11] of an elliptic curve, we derive that the elliptic curve is defined by a short Weierstrass equation where $A = 1$ and $B = 0$. Thus, the only elliptic curve with complex multiplication by $\mathbb{Z}[i]$ is $E/\mathbb{Q}\colon y^2 = x^3 + x$.

[9] An order $\mathcal{O}$ has conductor f with respect to $\mathcal{O}_K$ if f is the smallest integer for which $f\mathcal{O}_K \subset \mathcal{O}$.
[10] We say an $\mathcal{O}$-ideal $\mathfrak{a}$ is prime to an integer f if the norm $N(\mathfrak{a})$ of the ideal and f are coprime.
[11] See page 45 in [Sil86].

Let us consider the reduction of $E/\mathbb{Q}$ at the places $p \equiv 3 \bmod 4$ where $p \geq 5$. We know that p remains prime in $\mathbb{Z}[i]$ and so by Theorem 2.12 the reduction $E(p)$ must be supersingular. Next we consider the reduction at a prime $p \equiv 1 \bmod 4$, let us fix $p = 5$. To determine whether E has non-singular reduction modulo 5, we first determine $\Delta(E)$. Namely, we know from [Sil86, Pages 55, 56] that $E(5)$ has non-singular reduction if 5 does not divide Δ. Using the formula for Δ in [Sil86, Page 45], we compute $\Delta = -64$ and so $E(5)$ is non-singular. Note $E(5)$ has complex multiplication by $\mathbb{Z}[i]$, the maximal order of $\mathbb{Q}(i)$ and so it has conductor equal to 1. We know $5 = (2+i)(2-i)$ in $\mathbb{Z}[i]$, meaning 5 completely splits. Then $E(5)$ is ordinary. Since $p = 5$ does not divide the conductor, the map $\omega \mapsto \omega(5)$ defines an isomorphism $\mathrm{End}(E) \cong \mathrm{End}(E(5))$. It can be understood as reducing the coefficients of the coordinate functions modulo 5. ♙

Theorem 2.11 (Complex multiplication, [Feo17] Theorem 77)**.** *Let $\mathbb{F}_q$ be a finite field, $\mathcal{O} \subset K$ an order in a quadratic imaginary field, and $\mathrm{Ell}_{\overline{\mathbb{F}}_q}(\mathcal{O})$ the set of $\overline{\mathbb{F}}_q$-isomorphism classes of ordinary elliptic curves with complex multiplication by $\mathcal{O}$.*

Assume $\mathrm{Ell}_{\overline{\mathbb{F}}_q}(\mathcal{O})$ is non-empty, then it is a principal homogeneous space for the class group $\mathrm{Cl}(\mathcal{O})$, under the action

$$\begin{aligned} \mathrm{Cl}(\mathcal{O}) \times \mathrm{Ell}_{\overline{\mathbb{F}}_q}(\mathcal{O}) &\longrightarrow \mathrm{Ell}_{\overline{\mathbb{F}}_q}(\mathcal{O}) \\ (\overline{\mathfrak{a}}, E) &\longmapsto \overline{\mathfrak{a}} \star E \end{aligned}$$

defined above.

Proof. See Theorem 2.5 for $\mathcal{O} = \mathcal{O}_K$. Moreover, in combination with Proposition 2.8, we find that Theorem 2.5 also holds for non-maximal orders $\mathcal{O}$. Indeed, let $\mathfrak{a}_1, \ldots, \mathfrak{a}_{h(\mathcal{O})}$ be representatives of $\mathrm{Cl}(O)$. We know from [Cox22, Theorem 11.1 and Chapter 13] that the $j(\mathfrak{a}_i)$ are conjugate algebraic integers with a minimal polynomial of degree $h(\mathcal{O})$ called the class 'equation'. Since the class equation is defined over a field of characteristic 0, we notice that the $j(\mathfrak{a}_\mathfrak{i})$ are pairwise distinct. Therefore, they gives rise distinct $\overline{\mathbb{F}}_q$-isomorphism classes of elliptic curves with CM by $\mathcal{O}$. ♘

Moreover, we can relate an elliptic curve E defined over $\mathbb{F}_q$ where $q = p^n$ a prime power back to a curve over $\mathbb{C}$, as long as its endomorphism ring is non-trivial[12].

Theorem 2.12 (Deuring's lifting theorem, [Lan87] Chapter 10 §4)**.** *Let E_0 be an elliptic curve in characteristic p, with an endomorphism ω_o which is not trivial. Then there exists an elliptic curve E defined over a number field L, an endomorphism ω of E, and a non-singular reduction of E at a place $\mathfrak{p}$ of L lying above p, such that E_0 is isomorphic to $E(\mathfrak{p})$, and ω_0 corresponds to $\omega(\mathfrak{p})$ under the isomorphism.*

In fact, we know that $\mathrm{End}(E)$ is never trivial whenever E is defined over a finite field $\mathbb{F}_q$. The finite field $\mathbb{F}_q$ is uniquely defined by the q-th power Frobenius automorphism, and the latter can be extended to an endomorphism π of the elliptic curve E.

Definition 2.13 (Frobenius endomorphism)**.** Let E be an elliptic curve defined over $\mathbb{F}_q$ in Weierstrass form. Its *q-th power Frobenius endomorphism* $\pi \colon E \to E$ is the map that sends

$$(x, y) \mapsto (x^q, y^q)$$

and $O \mapsto O$.

We use the Frobenius endomorphism to identify the rational points in $E(\overline{\mathbb{F}}_q)$. For example, we know $\#E(\mathbb{F}_q) = \#\ker(1 - \pi)$ because the q-th power Frobenius π coincides with the identity on $\mathbb{F}_q$-rational points exactly. This fact can also be used in the proof of the following result.

Theorem 2.14 ([Sil86], Theorem V.2.3.1)**.** *Let $E/\mathbb{F}_q$ be an elliptic curve, π the q-th power Frobenius endomorphism and*

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

called the trace of the Frobenius. Then π satisfies $\pi^2 - t\pi + q = 0$ in $\mathrm{End}(E)$.

The above Equation 1 is often used to determine whether the curve E is ordinary/supersingular and to determine the amount of $\mathbb{F}_q$-rational points. Indeed, we know E is supersingular if and only if the trace

[12] Non-trivial meaning, strictly larger than $\mathbb{Z}$.

is 0 modulo q, see [Sil86, Exercise V.5.10]. We call $X^2 - tX + q$ the *characteristic polynomial* of π and Δ_π the corresponding *discriminant*.

As was hinted at in Chapter 2.2.1, we know that the complex multiplication action on elliptic curves defined over a number field yields isogenies of elliptic curves $E \to \overline{\mathfrak{a}} \star E$. Due to Theorem 2.12, complex multiplication is then also defined for the reductions that are defined over a finite field. We aim to characterize the resulting isogenies more carefully, because they provide the hardness to the isogeny-based Diffie-Hellman protocol. Recall that an elliptic curve is a smooth genus 1 curve.

Definition 2.15 ([Sil86], Definition on page 21)**.** Let $\phi : C_1 \to C_2$ be a map of curves defined over L. If ϕ is constant, we define the *degree* of ϕ to be 0. Otherwise we say that ϕ is a finite map and we define its degree to be

$$\deg \phi = [L(C_1) : \phi^* L(C_2)].$$

We say that ϕ is *separable*, *inseparable*, or *purely inseparable* if the field extension $L(C_1)/\phi^* L(C_2)$ has the corresponding property, and we denote the separable and inseparable degrees of the extension by $\deg_s \phi$ and $\deg_i \phi$, respectively.

We know from [Sil86, Theorem III.4.10] that the separable degree of an isogeny ϕ is equal to the number of points in its kernel, i.e.

$$\deg_s \phi = \#\ker(\phi).$$

Thus, if an isogeny is separable, then its degree is equal to the number of points in its kernel. Note that the q-th Frobenius endomorphism is purely inseparable for elliptic curves E defined over $\mathbb{F}_q$, because $a^q = a$ for all $a \in \mathbb{F}_q(E)$ and so the polynomial[13] $X^q - u$ has only one root. Luckily, we can restrict our attention to separable isogenies by factoring out π using the following result.

Corollary 2.16 ([Sil86], Corollary II.2.12)**.** *Every map $\psi : C_1 \to C_2$ of (smooth) curves over a field of characteristic $p > 0$ factors as*

$$C_1 \xrightarrow{\pi} C_1^{(q)} \xrightarrow{\lambda} C_2,$$

where $q = \deg_i(\psi)$, the map π is the q-th power Frobenius map, and the map λ is separable.

Due to Corollary 2.16, we are able to assume an isogeny ϕ is separable if and only if its degree is not congruent to 0 modulo p. Since the degree of a separable isogeny is given by the order of its kernel, we say two isogenies are equivalent if they have the same kernel. Unless the coordinate functions of the map are specified, we take an isogeny to mean an equivalence class of isogenies in the remainder of this thesis.

We restrict our attention to separable isogenies φ of degree ℓ, a prime different from p. The kernel of such an ℓ-isogeny φ is a cyclic subgroup of $E[\ell]$. We call an isogeny with a cyclic kernel a *cyclic isogeny*. We know from [Sil86, Corollary III.6.4(b)] that $E[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$. The latter contains $\ell + 1$ cyclic subgroups. We say that an ℓ-isogeny φ is $\mathbb{F}_q$-rational if $\pi(\ker(\varphi)) = \ker(\varphi)$. This suggests that we look at the restriction of π to $E[\ell]$ if we only want to work with $\mathbb{F}_q$-rational isogenies. As the characteristic polynomial and trace suggest, we know from [Sil86, Chapter III.7 The Tate Module] that π acts on $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ as an element in $\mathrm{GL}_2(\mathbb{F}_\ell)$, up to conjugation. Therefore, π must have 0 to 2 $\mathbb{F}_\ell$-rational eigenvalues, i.e. elements λ in $\mathbb{F}_\ell$ for which $\pi(P) = \lambda P$ where P generates a subgroup[14] of order ℓ. This yields the following possibilities, where $K = \mathbb{Q}(\pi) := \mathbb{Q}(\sqrt{\Delta_\pi})$ is a quadratic number field.

Atkin: π has no eigenvalues in $\mathbb{F}_\ell$, i.e. $X^2 - tX + q$ is irreducible modulo ℓ; then E has no $\mathbb{F}_q$-rational ℓ-isogenies. Therefore, $\left(\frac{\Delta_K}{\ell}\right) = -1$ (using the Legendre symbol).

ramified: π has one eigenvalue of (geometric) multiplicity one in $\mathbb{F}_\ell$, i.e. it is conjugate to a non-diagonal matrix

$$\begin{pmatrix} \lambda & * \\ 0 & \lambda \end{pmatrix},$$

then there is one $\mathbb{F}_q$-rational ℓ-isogeny from E. Moreover, $\left(\frac{\Delta_K}{\ell}\right) = 0$.

[13] Where $u \in \mathbb{F}_q(E)$ is a uniformizer at some nonsingular point $P \in E(\mathbb{F}_q)$, see [Sil86, Proposition II.1.4].
[14] This subgroup defines the kernel of an ℓ-isogeny.

ramified: π has one eigenvalue of multiplicity two in $\mathbb{F}_\ell$, i.e. it acts like a scalar matrix

$$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix},$$

then there are $\ell + 1$ $\mathbb{F}_q$-rational ℓ-isogenies from E. Moreover, $\left(\frac{\Delta_K}{\ell}\right) = 0$.

Elkies: π has two distinct eigenvalues in $\mathbb{F}_\ell$, i.e. it is conjugate to a diagonal matrix

$$\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$$

with $\lambda \neq \mu$; then there are two $\mathbb{F}_q$-rational ℓ-isogenies from E. Then $\left(\frac{\Delta_K}{\ell}\right) = 1$.

Example 2.17. We try to discern the different cases using small prime (i.e. for both p and ℓ small) examples.

Let us start with the supersingular elliptic curve model $E\colon y^2 = x^3 + x$ defined over $\mathbb{F}_{11}$. We know from [Sil86, Corollary III.6.4] that $E[3] \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, and so we look for a finite extension of $\mathbb{F}_{11}$ where all these 3-torsion points are defined, using the code in Appendix A.6.

It turns out an extension of degree 2 does the trick, meaning $E[3] \subseteq E(\mathbb{F}_{121})$. We find that $\pi_{11}(P) = P$ and $\pi_{11}(Q) = P + 2Q$. Therefore, if we assign the basis $P \to (1,0)^T$ and $Q \to (0,1)^T$ we find that π_{11} is conjugate to the matrix

$$\begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}$$

in $\mathrm{GL}_2(\mathbb{F}_3)$. This checks out with the fact that π_{11} sends $2P$ to $2P$ and $P+Q$ to $2P+2Q$. Note that this matrix is conjugate to a diagonal matrix with eigenvalues 1 and 2 in $\mathbb{F}_3$. We check if this corresponds to the splitting behavior of the characteristic polynomial modulo 3. To this end, we determine the trace of the Frobenius endomorphism π_{11} with respect to $E/\mathbb{F}_{11}$ using `Trace(E,1)`. The trace $t = 0$ because E is supersingular, see Example 2.10. We note that $X^2 + 11 \bmod 3 \equiv X^2 + 2 \equiv (X+1)(X-1)$ and so we are in the Elkies case, such that E has two 3-isogenies defined over $\mathbb{F}_{11}$. Using the above information (and some further `Magma` calculations), we understand that the isogenies are defined by the cyclic subgroups of $E[3]$ generated by P and $P+Q$ with eigenvalues 1 and 2 in $\mathbb{F}_3$ respectively. Lastly, we compute $\Delta_K = -11$ since $11 \equiv 3 \bmod 4$. Thus,

$$\left(\frac{\Delta_K}{\ell}\right) = \left(\frac{-11}{3}\right) = \left(\frac{-1}{3}\right)\left(\frac{11}{3}\right) = 1$$

because 11 is a non-square residue modulo 3.

Next we explore the Atkin case, where we need the characteristic polynomial $X^2 - tX + q$ to be irreducible modulo ℓ. By trial and error, we are able to select an irreducible polynomial $X^2 + 7 \equiv X^2 + 1 \bmod 3$, meaning we want to work with an elliptic curve $E/\mathbb{F}_7$ with trace $t = 0$ such that $E[3]$ is contained in a small extension of $\mathbb{F}_7$. Since $7 \equiv 3 \bmod 4$, we know $E\colon y^2 = x^3 + x$ has trace $t = 0$ over $\mathbb{F}_7$ because it is supersingular, see Example 2.10. We derive from the code in Appendix A.7 that $E[3] \subset E[\mathbb{F}_{7^4}]$.

We compute $\pi_7(P) = P + 2Q$, $\pi_7(Q) = 2P + 2Q$. Therefore, if we assign the basis $P \to (1,0)^T$ and $Q \to (0,1)^T$ we find that π_7 is conjugate to the matrix

$$\begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}$$

in $\mathrm{GL}_2(\mathbb{F}_3)$. It is clear from the characteristic polynomial that π_7 has no eigenvalues over $\mathbb{F}_3$. Lastly, we know $\Delta_K = -7$ since $7 \equiv 3 \bmod 4$. Therefore,

$$\left(\frac{\Delta_K}{\ell}\right) = \left(\frac{-7}{3}\right) = \left(\frac{-1}{3}\right)\left(\frac{7}{3}\right) = -1$$

because 7 is a non-square residue modulo 3. ♙

We are interested in the so-called Elkies primes ℓ, i.e. the primes ℓ for which $X^2 - tX + q$ completely splits. Indeed, if ℓ is Elkies, then there exist two $\mathbb{F}_p$-rational ℓ-isogenies per elliptic curve E, which is the maximal amount. This yields isogeny graphs, see the next chapter, in which any two nodes are connected by a very short path. Such graphs are useful in cryptography because the probability distribution of taking a walk (i.e. an isogeny) converges rapidly to the uniform distribution as the length of the walk increases. Since recovering isogenies, and thus walks, provide the hardness factor to the scheme we aim to study, it is essential that walks through isogeny graphs are sufficiently difficult to recover. For the definition and basic properties of isogeny graphs, we start a new chapter.

2.3 Isogeny graphs

An isogeny graph is a graph in which the vertices are represented by isomorphism classes of elliptic curves and the edges by the isogenies. In this chapter, we focus in particular on ordinary elliptic curves with CM by orders in a number field K defined over a finite field $\mathbb{F}_q$, and on $\mathbb{F}_q$-rational ℓ-isogenies.

First of all, we can divide the graph up into segments by distinguishing vertices through their endomorphism rings $\mathrm{End}(E)$, i.e. the orders that they have complex multiplication by. Indeed, we know all such orders $\mathcal{O}$ contain the multiplication-by-m map, i.e. all of $\mathbb{Z}$, and the q-th power Frobenius endomorphism π. Therefore, they must all contain $\mathbb{Z}[\pi] := \mathbb{Z}[\sqrt{\Delta_\pi}]$ and have the same field of fractions $K = \mathbb{Q}(\pi)$. Thus, $\mathbb{Z}[\pi] \subset \mathcal{O} \subset \mathcal{O}_K$ and

$$\Delta_\pi = [\mathcal{O} \colon \mathbb{Z}[\pi]]^2 [\mathcal{O}_K \colon \mathcal{O}]^2 \Delta_K.$$

Hence, we know that an order is maximal if its discriminant is square-free. Moreover, there can exist only finitely many orders with field of fractions K. The following result from [Koh96, Proposition 21] sheds more light on our approach.

Proposition 2.18 ([Koh96], Proposition 21)**.** *Let E, E' be elliptic curves defined over a finite field. Suppose that there exists an isogeny $\phi : E \to E'$ of prime degree ℓ, then* $\mathrm{End}(E)$ *contains* $\mathrm{End}(E')$ *or* $\mathrm{End}(E')$ *contains* $\mathrm{End}(E)$*, and the index of one in the other divides ℓ.*

Using terminology from [Koh96], we fix a prime ℓ and say an elliptic curve E lies on the *surface* if $v_\ell([\mathcal{O}_K \colon \mathrm{End}(E)]) = 0$, where v_ℓ is the ℓ-adic valuation. We say E is at *depth* d if $d = v_\ell([\mathcal{O}_K \colon \mathrm{End}(E)])$. The *maximal depth* is $v_\ell([\mathcal{O}_K \colon \mathbb{Z}[\pi]])$ and curves at that depth are said to lie on the *floor* of the graph. Kohel calls an ℓ-isogeny *horizontal* if its codomain is an elliptic curve at the same depth. It is called *descending* if its codomain lies at greater depth, *ascending* if its codomain lies at lesser depth. The following result gives us the number of isogenies on each level of the graph.

Theorem 2.19 ([Koh96], Proposition 23)**.** *Let $E/\mathbb{F}_q$ be an ordinary elliptic curve, π its Frobenius endomorphism, and Δ_K the fundamental discriminant of $K = \mathbb{Q}(\pi)$.*

1. *If E is not at the floor, there are $\ell + 1$-many $\mathbb{F}_q$-rational isogenies of degree ℓ from E, in total.*
2. *If E is at the floor, there are no descending $\mathbb{F}_q$-rational ℓ-isogenies from E.*
3. *If E is at the surface, then there are $\left(\frac{\Delta_K}{\ell}\right) + 1$-many $\mathbb{F}_q$-rational horizontal ℓ-isogenies from E (and no ascending $\mathbb{F}_q$-rational ℓ-isogenies).*
4. *If E is not at the surface, there are no horizontal $\mathbb{F}_q$-rational ℓ-isogenies from E, and one ascending $\mathbb{F}_q$-rational ℓ-isoqeny.*

Note that the isogeny graphs in Figure 1 resemble a volcano. Therefore, we call each such graph an *isogeny volcano*, following the example of [FM02]. To continue this analogy, we call the surface of an Elkies isogeny volcano the *crater*. Next, we focus specifically on the horizontal ℓ-isogenies at the surface (or crater) of an isogeny volcano. The horizontal ℓ-isogenies correspond directly to prime ideal classes in $\mathrm{Cl}(\mathcal{O})$ via complex multiplication. The vertices on the surface are given by $\mathrm{Ell}_{\overline{\mathbb{F}}_q}(\mathcal{O})$, the $\overline{\mathbb{F}}_q$-isomorphism classes of ordinary elliptic curves $E/\mathbb{F}_q$ with complex multiplication by fractional $\mathcal{O}$-ideals prime to the conductor of $\mathcal{O}$. We fix a prime ℓ and depending on the cases from before, we obtain the following surfaces of ℓ-isogeny volcanoes.

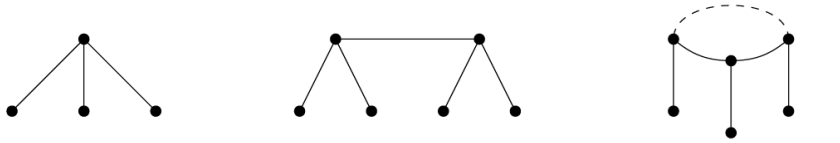


Figure 1: Isogeny volcano types of 2-isogenies depending on $\left(\frac{\Delta_K}{\ell}\right)$. In the Atkin case, no $\mathbb{F}_q$-rational horizontal isogenies exist at the surface. In the ramified case only one such isogeny exists per vertex at the surface. In the Elkies case, two $\mathbb{F}_q$-rational isogenies per vertex at the surface exist. Taken from the third version of [Feo17, Page 29].

Corollary 2.20. *Let $\mathcal{O}$ be a quadratic imaginary order, and assume that $\mathrm{Ell}_{\overline{\mathbb{F}}_q}(\mathcal{O})$ is non-empty. Let ℓ be a prime such that $\mathcal{O}$ is ℓ-maximal, i.e. such that ℓ does not divide the conductor of $\mathcal{O}$. All ℓ-isogeny volcanoes of curves in $\mathrm{Ell}_{\overline{\mathbb{F}}_q}(\mathcal{O})$ are isomorphic as graphs. Furthermore, one of the following is true.*

(0) If the ideal (ℓ) is prime in $\mathcal{O}$, then there are $h(\mathcal{O})$ distinct ℓ-isogeny volcanoes of Atkin type, with surface in $\mathrm{Ell}_{\overline{\mathbb{F}}_q}(\mathcal{O})$.

(1) If (ℓ) is ramified in $\mathcal{O}$, i.e., if it decomposes as a square $\mathfrak{l}^2$, then there are $h(\mathcal{O})/2$ distinct ℓ-isogeny volcanoes of ramified type, with surface in $\mathrm{Ell}_{\overline{\mathbb{F}}_q}(\mathcal{O})$.

(2) If (ℓ) splits as a product $\mathfrak{l} \cdot \mathfrak{l}'$ of two distinct prime ideals, then there are $h(\mathcal{O})/n$ distinct ℓ-isogeny volcanoes of Elkies type, with craters in $\mathrm{Ell}_{\overline{\mathbb{F}}_q}(\mathcal{O})$ of size n, where n is the order of $\bar{\mathfrak{l}}$ in $\mathrm{Cl}(\mathcal{O})$.

Let us focus on the crater of the graph in the Elkies case. This subgraph is generated by the isogenies on the surface is 2-regular and finite, i.e. a cycle. We recall that the Frobenius endomorphism splits modulo ℓ, meaning

$$0 \equiv \pi^2 - t\pi + q \equiv (\pi - \lambda)(\pi - \mu) \bmod \ell$$

where $\lambda, \mu \in \mathbb{F}_\ell$ are distinct eigenvalues associated to the action of π on $E[\ell]$. They correspond to the ideal $\mathfrak{l} = (\ell, \pi - \lambda)$ and its inverse $\mathfrak{l}' = (\ell, \pi - \mu)$, that are both of norm ℓ. Then $E[\mathfrak{l}] \cup E[\mathfrak{l}'] = E[\ell]$ and $[\mathfrak{l}']$ is the dual of $[\mathfrak{l}]$ because $[\ell] = [\mathfrak{l}] \circ [\mathfrak{l}'] = [\mathfrak{l}'] \circ [\mathfrak{l}]$. In the crater, the isogenies $[\mathfrak{l}]$ and $[\mathfrak{l}']$ yield opposite directions as can be seen from Figure 2 underneath.

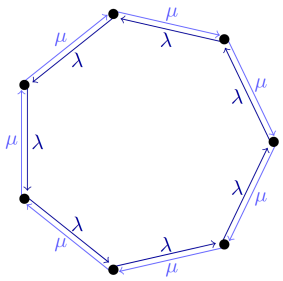


Figure 2: Isogeny cycle of arbitrary length for an Elkies prime ℓ, the edge directions associated with the Frobenius eigenvalues λ and μ. Taken from the third version of [Feo17, Figure 9].

The set $\mathrm{Ell}_{\overline{\mathbb{F}}_q}(\mathcal{O})$ is partitioned into craters of size equal to the order of the ideal class of $\mathfrak{l} = (\ell, \pi - \lambda)$ in $\mathrm{Cl}(\mathcal{O})$. This is a basic instance of a Caley graph of the class group $\mathrm{Cl}(\mathcal{O})$ with edge set $S = \{\mathfrak{l}, \mathfrak{l}'\}$. Notice that we can enlarge S by adding the prime ideals belonging to different Elkies primes $\ell' \neq \ell$. The union of different craters yields the end product and is used in the Couveignes-Rostovtsev-Stolbunov (CRS) scheme. We introduce the latter in the next chapter.

3 The origins of CSIDH

3.1 Couveignes-Rostovtsev-Stolbunov (CRS) scheme

?? The CRS scheme uses the correspondence between isogenies of ordinary elliptic curves with complex multiplication by an imaginary quadratic order $\mathcal{O}$, and ideals in the class group $\mathrm{Cl}(\mathcal{O})$. Since $\mathrm{Cl}(\mathcal{O})$ is commutative, there exists an abelian group action of ideal classes in $\mathrm{Cl}(\mathcal{O})$ on elliptic curves over $\mathbb{F}_q$ with CM by $\mathcal{O}$ that we can use to instantiate the DH protocol. This group action is a HHS due to the use of modular equations $\Phi_\ell(X, Y) = 0$, see [Cox22, Chapter 11.C], in the group action computations.

In this chapter we first explain the CRS scheme for a Diffie-Hellman protocol using the modular equation. Next, we compare it to computing the group action using Vélu's equations, see Theorem 3.3.

Setup of public parameters: an ordinary elliptic curve $E_0/\mathbb{F}_q$ with $\mathrm{End}(E_0) = \mathcal{O}$ and set of Elkies primes $\{\ell_1, \ldots, \ell_n\}$.

Key generation: the secret key $(e_1, \ldots, e_n)$ where each e_i is sampled randomly from $\{-m, \ldots, m\}$ representing $\mathfrak{a} = \mathfrak{l}_1^{e_1} \ldots \mathfrak{l}_\mathfrak{n}^{e_n} \in \mathrm{Cl}(\mathcal{O})$, where $\mathfrak{l}_i = (\ell_i, \pi - \lambda)$. The public key $j(E_A)$, where $E_A := E_0/E_0[\mathfrak{a}]$.

Key exchange: Alice and Bob have key pairs $(\mathfrak{a}, j(E_A))$ and $(\mathfrak{b}, j(E_B))$. Upon the publication of $j(E_B)$, Alice finds the chain of $\mathbb{F}_q$-rational roots of the modular equation corresponding to each factor of her secret key $\mathfrak{a}$. Similarly for Bob. They both recover the same j-invariant as the last links of their chains, their shared secret key.

The security of this protocol stems from the hardness of recovering isogenies, an intractable problem. For the origins of the CRS scheme, we quote from [Cas+18, Page 2].

"*The first proposal of an isogeny-based cryptosystem was made by Couveignes in 1997* [Cou06]. *It described a non-interactive key exchange protocol where the space of public keys equals the set of $\mathbb{F}_q$-isomorphism classes of ordinary elliptic curves over $\mathbb{F}_q$ whose endomorphism ring is a given order $\mathcal{O}$ in an imaginary quadratic field and whose trace of Frobenius has a prescribed value. .... His work was only circulated privately and thus not picked up by the community; the corresponding paper* [Cou06] *was never formally published and posted on ePrint only in 2006. The method was eventually independently rediscovered by Rostovtsev and Stolbunov in 2004 (in Stolbunov's master's thesis, which was initially written in Russian and later published on ePrint as* [RS06] in 2006)."

This led to the abbreviation by which we know the CRS scheme.

3.1.1 Computing a group action using the modular equations

Let us first establish the mathematical foundations of the CRS scheme. We work in the context of an order $\mathcal{O}$ such that its field of fractions K is an imaginary quadratic number field. If we consider the Frobenius endomorphism π of $\mathbb{F}_q$ modulo ℓ, it has at most two roots $\lambda, \mu \in \mathbb{Z}/\ell\mathbb{Z}$, where ℓ is any prime integer $\ell \neq p$. We are interested in the Elkies case, where $\lambda \neq \mu$ exist such that $(\ell)\mathcal{O} = \mathfrak{l}\mathfrak{l}'$ with $\mathfrak{l} = (\ell, \pi - \lambda)$ and $\mathfrak{l}' = (\ell, \pi - \mu)$. The isogenies we are interested in are defined by the ideals $\mathfrak{l}$ and their inverses $\mathfrak{l}'$, which yields $\mathbb{F}_q$-rational isogenies $[\mathfrak{l}]$ and their duals $[\mathfrak{l}']$ on any ordinary elliptic curve over $\mathbb{F}_q$ with complex multiplication by $\mathcal{O}$.

These ideals are sampled from $\mathrm{Cl}(\mathcal{O})$ under the assumption that small[15] Elkies prime ideals $\mathfrak{l}_i$ have large order and that their ideal classes are evenly distributed in $\mathrm{Cl}(\mathcal{O})$. Under these assumptions, we expect that ideals of the form $\mathfrak{l}_1^{e_1} \ldots \mathfrak{l}_n^{e_n}$, where $e_i \in \mathbb{Z}_{>0}$, rarely lie in the same ideal class. Since the $\mathfrak{l}_\mathfrak{i}$ are global parameters, the costly process of selecting Elkies primes ℓ_i does not greatly affect the efficiency of the protocol.

Next we would like to evaluate the group action of an ideal $\mathfrak{l} = (\ell, \pi - \lambda)$ in $\mathrm{Cl}(\mathcal{O})$ on an ordinary elliptic

[15] In terms of their norm.

curve $E_0/\mathbb{F}_q$ with CM by $\mathcal{O}$. This amounts to finding the elliptic curve in the codomain of an isogeny. Couveignes proposed the use of the modular equation $\Phi_\ell(X, Y) = 0$, where elliptic curves are represented by their j-invariant.

If we compute the $\mathbb{F}_q$-rational roots Y_i of the modular polynomial $\Phi_\ell(j(E_0), Y)$, they correspond to the j-invariants of the two neighboring curves[16] of E_0 in the ℓ-isogeny graph. In the first step from the starting curve E_0, we choose the neighbor corresponding to the action of $\mathfrak{l} = (\ell, \pi - \lambda)$. We can check this by taking any non-zero point (x, y) satisfying the kernel polynomial[17], and checking if $\pi(x, y) = [\lambda](x, y)$ modulo the kernel polynomial and on the curve. If the equality holds, the right choice was made. In any consequent steps, we want to avoid backtracking. To this end it suffices to choose the j-invariant that was not chosen in the previous step.

The output of this scheme is a j-invariant which corresponds to multiple elliptic curve Weierstrass models and in particular at least two models that are both defined over $\mathbb{F}_q$. They form a set $\mathrm{Twist}((E_0, O)/\mathbb{F}_q)$ called the twists of the elliptic curve E_0. If we work with ordinary elliptic curves, the twists can be distinguished by their trace. Thus, in that case we are able to recover an elliptic curve $E/\mathbb{F}_q$. For more information about this algorithm, see [FKS18, Pages 9, 10, 11]. This method is based on [Cox22, Proposition 14.11], which reads as follows.

Proposition 3.1 ([Cox22], Proposition 14.11)**.** *Let E and E' be elliptic curves over $\mathbb{C}$. Then there is a cyclic isogeny α from E to E' of degree ℓ if and only if $\Phi_\ell(j(E), j(E')) = 0$.*

Note that Elkies primes $\mathfrak{l} = (\ell, \pi - \lambda)$ and $\mathfrak{l}' = (\ell, \pi - \mu)$ define dual isogenies, since $(\ell) = \mathfrak{l}\mathfrak{l}'$. Moreover, since $\deg([\ell]) = \ell^2$, we know that $\mathfrak{l}$ and $\mathfrak{l}'$ must be separable because $p \nmid \ell$. Thus, we know that $\deg(\mathfrak{l}) = \deg(\overline{\mathfrak{l}}) = \#\ker(\mathfrak{l})$. Therefore, $\ell = \#\ker(\mathfrak{l})$, meaning $\mathfrak{l}$ is a cyclic isogeny. Thus, $\mathfrak{l}\colon E_0 \to E_1$ if and only if $\Phi_\ell(j(E_0), j(E_1)) = 0$ when we consider E_0, E_1 to be elliptic curves over $\mathbb{C}$. Similarly for $\mathfrak{l}'$. This proves the mathematical principals of the protocol.

An initial advantage of this method is that the degree of the field extension $r = [\mathbb{F}_{q^r} : \mathbb{F}_q]$ such that $\ker(\mathfrak{l}_i) \subseteq E_j(\mathbb{F}_{q^r})$ does not influence the computation. We see this clearly demonstrated in the following toy example.

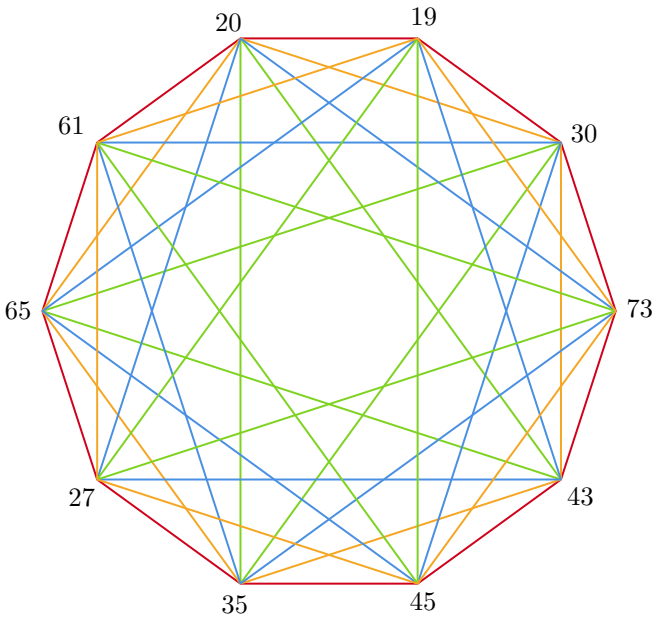
Example 3.2. Consider the ordinary elliptic curve $E_0/\mathbb{F}_{83}\colon y^2 = x^3 + x + 1$, we aim to find its horizontal neighbors in the ℓ-isogeny graphs using the modular equation $\Phi_\ell(X, j(E)) \in \mathbb{F}_{83}[X]$ and for as many different ℓ as we can. To this end, we need to find primes ℓ that are Elkies, because they define the edges of the isogeny graph. We find them using the `Magma` code in Appendix A.2. We know that the classical database of `Magma` only contains modular equations for the primes up to and including 41. Therefore, we only need to check whether the first 40 primes are Elkies. Using `Magma`, we compute that the trace of $E/\mathbb{F}_{83}$ is $t = -6$. Thus, the characteristic polynomial of the Frobenius endomorphism is $x^2 + 6x + 83$. If this polynomial splits into distinct linear factors modulo a prime, then the primes is Elkies. This yields the Elkies primes $\{3, 5, 11, 13, 23, 29, 31, 41\}$ that satisfy this condition. We compute that $j_0 := j(E_0) = 65 \bmod 83$ is the j-invariant of E_0.

Let us start with the prime $\ell = 3$. Consider the classical modular equation $\Phi_3(X, j(E_0))$ over $\mathbb{F}_{83}$ and look at its linear factors to derive the next j-invariant. In the first step, we find that $\Phi_3(X, j_0)$ has two linear factors $X + 63$ and $X + 48$ modulo 83, see Appendix A.3 for the relevant code. Therefore, the neighboring $\overline{\mathbb{F}}_{83}$-isomorphism classes must have j-invariants $-63 \equiv 20 \bmod 83$ and $-48 \equiv 35 \bmod 83$. We choose $j_2 \equiv 20 \bmod 83$ for our first step. In the second step, we try to find the linear factors of $\Phi_3(X, 35 \bmod 83)$. This yields the original j-invariant $j_0 \equiv 65 \bmod 83$ and a new j-invariant $j_4 \equiv 30 \bmod 83$, so it only makes sense to continue evaluating $\Phi_3(X, 30 \bmod 83)$. In the fourth step we find $j_8 \equiv 35 \bmod 83$ again, we are able to conclude $\Phi_3(X, Y)$ generates a cyclic graph with 5 vertices.

Repeating this process for each $\ell \in \{3, 5, 11, 13, 23, 29, 31, 41\}$ and j_i, we obtain the following union of graphs, in which each vertex corresponds to the j-invariant obtained through evaluating the modular equations. Hereby, the following colors correspond to the following subgraphs. Red corresponds to $\ell = 5, 31, 41$, orange corresponds to $\ell = 3$, green corresponds to $\ell = 11$ and blue corresponds to $\ell = 13, 23, 29$.

[16] See the Elkies case in Chapter 2.2.2.

[17] As described in the PhD thesis of Kohel, see [Koh96, Chapter 2.4]. If the kernel is viewed as a finite subgroup scheme of the elliptic curve as a group scheme, it can be described by a polynomial in the coordinate x of the Weierstrass equation. For multiplication-by-m endomorphisms, these are the m-th division polynomials, see [Sil86, Exercise 3.7].



Next we look at an example of the CRS scheme with the modular equation $\Phi(X, Y) = 0$ in the Diffie-Hellman protocol that we started this chapter with.

Setup of public parameters: consider the ordinary elliptic curve

$$E_0/\mathbb{F}_{83} \colon y^2 = x^3 + x + 1$$

with j-invariant $j(E_0/\mathbb{F}_{83}) = 65$ and set of Elkies primes $\{3, 5, 11, 13\}$.

Key exchange: Let $\mathfrak{p}_\ell = (\ell, \pi - \lambda_\ell)$ whose action works in the clockwise direction in above graph, and where $(\pi - \lambda_\ell)(\pi - \mu_\ell) \equiv 0 \bmod \ell$. Alice picks the secret key $(1, -2, 3, 0)$ representing the ideal $\mathfrak{a} = \mathfrak{p}_3\mathfrak{p}_5^{-2}\mathfrak{p}_{11}^3 \in \mathrm{Cl}(\mathcal{O})$. Similarly, Bob picks the secret key $(0, -1, 1, 2)$ representing the ideal $\mathfrak{b} = \mathfrak{p}_5^{-1}\mathfrak{p}_{11}\mathfrak{p}_{13}^3$.

Alice computes her public key $j(E_A)$ as follows. She first determines the roots of $\Phi_3(X, 65 \bmod 83)$ in $\mathbb{F}_{83}$ belonging to the first prime in the ideal factorization of $\mathfrak{a}$. We observe from the graph above that this yields $j_2 = 20$. Next, she determines the roots of $\Phi_5(X, 20 \bmod 83)$ in $\mathbb{F}_{83}$. This corresponds to walking along the red edge out of 20, but rather in anti-clockwise direction because the exponent is negative. Thus, we obtain $j_1 = 61$. However, we need to compute this step twice and so we end up in $j_0 = 65$. Computing these steps for every factor yields her public key $j_2 = 20$. In literature, her walk is sometimes denoted by[a] $(+, -, -, +, +, +)$. We notice that the order of steps does not matter.

Similarly, Bob computes the roots of $\Phi_5(X, 65 \bmod 83)$ in $\mathbb{F}_{83}$ for the first (non-zero) factor of $\mathfrak{a}$. This corresponds to walking along the red edge out of 65 mod 83 in anti-clockwise direction. At the final step, one can check that he obtains the public key $j_5 = 73$. His walk is sometimes denoted by $(-, +, +, +)$.

Key exchange: Both Alice and Bob publish $j(E_A) = 20$ and $j(E_B) = 73$. They repeat the same computations, but instead they take $j(E_B), j(E_A)$ as their first inputs into $\Phi_\ell(X, Y)$ respectively. We check that they both obtain $j_4 = 30$.

[a] This walk contains a loop due to the scale of the example, meaning $(1, -2, 3, 0) = (0, 0, 3, 0)$. Similarly for Bob's walk: $(0, -1, 1, 2) = (0, -1, 0, 0)$.

This concludes the example. ♙

The most computationally expensive part of this scheme is to find the two linear factors of each modular equation $\Phi_\ell(X, j(E_i)) \in \mathbb{F}_q[X]$. According to [FKS18], the fastest algorithm for finding these roots uses principles from the Cantor-Zassenhaus algorithm which costs $\tilde{O}(\ell \log q)$ operations[18] in $\mathbb{F}_q$. Therefore, the algorithm executing this scheme costs $\tilde{O}(\ell \log q)$ operations in $\mathbb{F}_q$.

[18] We use the tilde to indicate certain logarithmic factors are ignored, see Definition C.2.

3.1.2 Vélu's equations

There exists another method for computing isogenies where we do not need modular polynomials and thus avoid a costly root-finding process. It uses Vélu's equations, see Theorem 3.3 underneath. They are a simple and effective tool in computing isogenies [ı], because we only need an ℓ-cyclic subgroup of $E(\overline{\mathbb{F}}_q)$, i.e. a subgroup of order ℓ consisting of $\overline{\mathbb{F}}_q$-rational points on the elliptic curve E. This method is based on the following theorem in [Was08, Theorem 12.16].

Theorem 3.3 ([Was08], Theorem 12.16)**.** *Let E be an elliptic curve given by the generalized Weierstrass equation*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with all a_i in some field K. Let C be a finite subgroup of $E(\overline{K})$. Then there exists an elliptic curve E' and a separable isogeny α from E to E' such that $C = \operatorname{Ker}\alpha$.

For a point $Q = (x_Q, y_Q) \in C$ with $Q \neq \infty$, define

$$\begin{aligned} g_Q^x &= 3x_Q^2 + 2a_2x_Q + a_4 - a_1y_Q \\ g_Q^y &= -2y_Q - a_1x_Q - a_3 \\ v_Q &= \begin{cases} g_Q^x & (\text{ if } 2Q = \infty) \\ 2g_Q^x - a_1g_Q^y & (\text{ if } 2Q \neq \infty) \end{cases} \\ u_Q &= \left(g_Q^y\right)^2. \end{aligned}$$

Let C_2 be the points of order 2 in C. Choose $R \subset C$ such that we have a disjoint union

$$C = \{\infty\} \cup C_2 \cup R \cup (-R)$$

(in other words, for each pair of non-2-torsion points $P, -P \in C$, put exactly one of them in R). Let $S = R \cup C_2$. Set

$$v = \sum_{Q \in S} v_Q, \quad w = \sum_{Q \in S} (u_Q + x_Q v_Q)$$

Then E' has the equation

$$Y^2 + A_1XY + A_3Y = X^3 + A_2X^2 + A_4X + A_6$$

where

$$\begin{aligned} A_1 = a_1, \quad A_2 = a_2, \quad A_3 = a_3, \\ A_4 = a_4 - 5v, \quad A_6 = a_6 - \left(a_1^2 + 4a_2\right)v - 7w. \end{aligned}$$

The isogeny is given by

$$X = x + \sum_{Q \in S} \left(\frac{v_Q}{x - x_Q} + \frac{u_Q}{(x - x_Q)^2} \right),$$

$$Y = y - \sum_{Q \in S} \left(u_Q \frac{2y + a_1x + a_3}{(x - x_Q)^3} + v_Q \frac{a_1(x - x_Q) + y - y_Q}{(x - x_Q)^2} + \frac{a_1u_Q - g_Q^xq_Q^y}{(x - x_Q)^2} \right).$$

Example 3.4. Let us apply Vélu's equations to the example from before, the ordinary elliptic curve $E\colon y^2 = x^3 + x + 1$ over the finite field $\mathbb{F}_{83}$. Using the following code

```
L<a>:=GF(83,1);
E:=EllipticCurve([L|1,1]);
T:=TorsionSubgroupScheme(E,3);
Points(T);
```

we find the 3-torsion points $P = (3, 60)$ and $-P = (3, 23)$ giving rise to a 3-isogeny with kernel $\langle P \rangle$. Filling out the formulas for $C_2 = \emptyset$ and $S = \{P\}$, we end up with the following elliptic curve in the codomain:

$$E'/\mathbb{F}_{83}\colon y^2 = x^3 - 279x - 101975$$

which has j-invariant 20. This checks out with the graph of 3-isogenies in Example 3.2. ♙

We are able to construct $\ker[\mathfrak{l}] = \langle P \rangle$ where $\mathfrak{l} = (\ell, \pi - \lambda)$ according to [FKS18, Page 11], by finding a non-trivial ℓ-torsion point $P \in E(\mathbb{F}_{q^r})$, where $r = \text{order}(\lambda \bmod \ell)$. Indeed, let us first consider any point Q in $\ker[\mathfrak{l}]$. Therefore, $\ell Q = O$ and $\pi Q = \lambda Q$. We find that

$$\pi^r Q = \lambda^r Q \equiv Q \bmod \ell.$$

Since $\ell Q = O$, this implies $\pi^r Q = Q$ and so we find $\ker[\mathfrak{l}] \subseteq E(\mathbb{F}_{q^r})$, where π is the q-th power Frobenius endomorphism. Next, we note $0 = \pi^2 - t\pi + q \equiv (\pi - \lambda)(\pi - \mu) \bmod \ell$, and so any $Q \in E[\ell](\mathbb{F}_{q^r})$ is in the kernel of $[\mathfrak{l}]$ or $[\mathfrak{l}']$ where $\mathfrak{l}' = (\ell, \pi - \mu)$. Thus, if $\text{order}(\mu \bmod \ell)$ does not divide r, we find that necessarily $E[\ell](\mathbb{F}_{q^r}) = \ker[\mathfrak{l}]$. For this reason we select the eigenvalue λ such that $\text{order}(\lambda \bmod \ell) < \text{order}(\mu \bmod \ell)$. Finding a non-trivial ℓ-torsion point P can then be done as follows. We multiply a random point R in $E(\mathbb{F}_{q^r})$ by $\#E(\mathbb{F}_{q^r})/\ell$ and check if this yields a non-trivial ℓ-torsion point $P := \#E(\mathbb{F}_{q^r})/\ell \cdot R$. If we do not succeed, we repeat the process by choosing another point R in $E(\mathbb{F}_{q^r})$. This of course requires $\ell \mid \#E(\mathbb{F}_{q^r})$, and so for a start we need to compute the order of $E(\mathbb{F}_{q^r})$.

Note that $\#E(\mathbb{F}_{q^r})$ can be computed from the trace t of π: we know $\#E(\mathbb{F}_q) = q + 1 - t$ and so the trace t is derived from the characteristic polynomial $x^2 - tx + q$ of π. By fixing the roots $\alpha, \overline{\alpha} \in \mathbb{C}$ we find $t = \alpha + \overline{\alpha}$. If we denote $\pi = \pi_q$ the q-th power Frobenius endomorphism, we know $\pi_q^r = \pi_{q^r}$ and so since $\alpha, \overline{\alpha}$ are eigenvalues of π, then $\#E(\mathbb{F}_{q^r}) = q^r + 1 - t_r$ with $t_r = \alpha^r + \overline{\alpha}^r$. The recurrence relation $t_0 = \alpha^0 + \overline{\alpha}^0 = 2$, $t_1 = t$ and $t_{n+1} = t \cdot t_n - q \cdot t_{n-1}$ is then proved by induction[19]. In this way $\#E(\mathbb{F}_{q^r}) = q^r + 1 - t_r$ can be computed much faster depending on how large r is. Assuming $\log \#E(\mathbb{F}_{q^r}) \simeq r \log q$ provided $\ell = O(\log q)$, the costliest step in this algorithm is multiplication of a point Q by $\#E(\mathbb{F}_{q^r})/\ell$, which costs $\tilde{O}(r^2 \log q)$ $\mathbb{F}_q$-operations.

Comparing the two methods, we find that the modular method costs $\tilde{O}(\ell \log q)$-many $\mathbb{F}_q$-operations while Vélu's method costs $\tilde{O}(r^2 \log q)$. Therefore, if we can force $r = 1$, this saves a factor ℓ when we use Vélu's method. This is exactly what is done in CSIDH, a scheme based on the method we established in this chapter.

3.2 The design choices of CSIDH

In this chapter we introduce CSIDH, the Commutative Supersingular Isogeny Diffie-Hellman characterized by the following protocol.

Setup of public parameters: a supersingular elliptic curve $E_0/\mathbb{F}_p \colon y^2 = x^3 + x$ with $\text{End}_p(E_0) = \mathbb{Z}[\sqrt{-p}]$ and set of Elkies primes $\{\ell_1, \ldots, \ell_n\}$ such that $p = 4 \prod_{i=1}^n \ell_i - 1 \equiv 3 \bmod 8$.

Key generation: the secret key $(e_1, \ldots, e_n)$ where each e_i is sampled randomly from $\{-m, \ldots, m\}$ representing $\mathfrak{a} = \mathfrak{l}_1^{e_1} \ldots \mathfrak{l}_\mathfrak{n}^{e_n} \in \text{Cl}(\mathbb{Z}[\sqrt{-p}])$, where $\mathfrak{l}_i = (\ell_i, \pi - 1)$. The public key A, where $E_A := E/E[\mathfrak{a}] \colon y^2 = x^3 + Ax^2 + x$.

Key exchange: Alice and Bob have key pairs $(\mathfrak{a}, A)$ and $(\mathfrak{b}, B)$. Upon the publication of B, Alice computes the chain of $\mathbb{F}_p$-rational Montgomery coefficients corresponding to Vélu's equations applied to the kernel of each factor of her secret key $\mathfrak{a}$. Similarly for Bob. They both recover the same Montgomery coefficient at the end of this chain, their shared secret key.

The protocol contains specific design choices that are explained in this chapter, where we regard CRS as our point of departure.

The major drawback of CRS using Vélu's equations by De Feo, Kieffer and Smith [FKS18] if we require $r = 1$, is its inefficiency largely caused by the following selection process. They aim to find an ordinary

[19] Note that since $\alpha\overline{\alpha} = q$,

$$\begin{aligned} t t_n - q t_{n-1} &= (\alpha + \overline{\alpha})(\alpha^n + \overline{\alpha}^n) - q(\alpha^{n-1} + \overline{\alpha}^{n-1}) \\ &= \alpha^{n+1} + \overline{\alpha}^{n+1} + \alpha\overline{\alpha}^n + \overline{\alpha}\alpha^n - q\alpha^{n-1} - q\overline{\alpha}^{n-1} \\ &= \alpha^{n+1} + \overline{\alpha}^{n+1} \\ &= t_{n+1}. \end{aligned}$$

elliptic curve E defined over $\mathbb{F}_q$ with $\mathbb{F}_q$-rational points P_i of order ℓ_i for many different small primes ℓ_i. We know that this is true if and only if $\#E(\mathbb{F}_q)$ is congruent to 0 modulo ℓ_i for all i. Each non-trivial point P_i yields a $\mathbb{F}_q$-rational ℓ-isogeny, φ_i, with cyclic kernel $\langle P_i \rangle$ via Vélu's equations.

Moreover, as described in [Cas+18, page], Childs, Jao and Soukharev [CJS14] showed in 2010 that the CRS scheme could be broken with quantum algorithms that have a time complexity of $L_q[1/2]$, i.e. in subexponential time. This would be acceptable if it were not also true that CRS is incredibly slow: it takes minutes to compute a single isogeny. One of the vulnerabilities the attack exploits is the commutativity of the class group of the endomorphism ring of an ordinary elliptic curve, which is an order in an imaginary quadratic number field. Therefore, supersingular elliptic curves were considered because their endomorphism ring was a maximal order in a quaternion algebra and therefore not commutative. This consideration resulted in the *Supersingular Isogeny Diffie-Hellman*, which was broken in 2022 in two independent efforts using a theorem by Kani, see [CD23] and [MM22]. We note that this scheme does not use the CRS scheme in which ordinary elliptic curves are substituted for supersingular ones. However, this idea did inspire Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny and Joost Renes to develop a scheme known as *Commutative Supersingular Isogeny Diffie-Hellman*. In this chapter we introduce this scheme to the reader.

First of all, the choice for supersingular curves means that $\#E(\mathbb{F}_q) = q+1$, see [Sil86, Theorem V.4.1(a)], guaranteeing the existence of an ℓ-cyclic subgroup in $E(\mathbb{F}_q)$ whenever $\ell \mid (q+1)$. Next, we address the other inefficiencies in the design of this scheme, by lowering the computation cost $\tilde{O}(r^2 \log(q))$ as follows. We require $q = p$ to be prime and $r = 1$ in order to reduce the cost. Thus, if $\lambda \equiv 1 \bmod \ell$, then[20] $\mathfrak{l} = (\ell, \pi - 1)$ and we know that $\ker(\pi - 1) \subseteq E(\mathbb{F}_p)$ because the p-th power Frobenius π coincides with the identity morphism exactly on $\mathbb{F}_p$. Moreover, since we work with supersingular curves, we know that the trace is always 0 and so the characteristic polynomial of the (p-th power) Frobenius morphism is[21] $x^2 + p$. Therefore, $\lambda + \mu \equiv 0 \bmod \ell$ and so $\mu \equiv -1 \bmod \ell$. Note that then $\mathfrak{l}' = (\ell, \pi + 1)$ and the points in $\ker(\pi + 1)$ are exactly those that satisfy $\pi(x, y) = (x, -y)$, i.e. with $x \in \mathbb{F}_p$ and $y \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$. This all checks out, since $p = \lambda \cdot \mu \equiv -1 \bmod \ell$ holds true for any $\ell \mid (p+1)$. Thus, if we can find a non-trivial point P with $x(P) \in \mathbb{F}_p$ and $y(P) \in \mathbb{F}_{p^2}$ of order ℓ, we have found the kernel $\langle P \rangle$ of a $\mathbb{F}_p$-rational ℓ-isogeny $[\mathfrak{l}]$ or $[\mathfrak{l}']$ and we can use Vélu's equations, see Theorem 3.3, to compute the group action.

Finding a point P of order ℓ is a computationally costly process because it involves many and potentially large elliptic curve point multiplications, see [Cas+18] and [Sil86, Chapter XI.1]. Therefore, we prefer to work with many small primes[22] ℓ_i to lower the running time. For instance, in order to guarantee a key space of 256 bits, the designers of CSIDH fix

$$p = 4 \prod_{i=1}^{74} \ell_i - 1, \tag{2}$$

where $\ell_1 = 3, \ell_2 = 5 \ldots, \ell_{73} = 373$ are the smallest 73 odd primes, and $\ell_{74} = 587$ in order to ensure p is a prime itself. The exponents of these ideals are taken in a range $\{-5, \ldots, 5\}$ which indeed results in a key-space size of

$$\log_2((2 \cdot 5 + 1)^{74}) \approx 255.9979$$

bits. The amount of bits can be chosen smaller or larger by decreasing or increasing the prime p, respectively.

The ℓ-isogenies we are interested in are $\mathbb{F}_p$-rational if and only if the Frobenius endomorphism of the field of definition stabilizes the respective kernels. This allows us to regard the vertices in the isogeny graph of a supersingular elliptic curve as $\mathbb{F}_p$-isomorphism classes. However, so far we have only determined the structure of an isogeny volcano for ordinary elliptic curves. A similar structure also exists for supersingular elliptic curves and it depends on the characteristic p of the prime field $\mathbb{F}_p$ as we can see from the following result. Recall $p \equiv 3 \bmod 4$, which can be seen from Equation (2).

Theorem 3.5 ([DG16],Theorem 2.7)**.** *Let $p > 3$ be a prime and $K = \mathbb{Q}(\sqrt{-p})$ with ring of integers $\mathcal{O}_K$.*

(1) $p \equiv 1 \bmod 4$: There are $h(\mathcal{O}_K)$-many $\mathbb{F}_p$-isomorphism classes of supersingular elliptic curves over $\mathbb{F}_p$, all having the same endomorphism ring $\mathcal{O}_K = \mathbb{Z}[\sqrt{-p}]$. From every class, i.e. vertex, there is

[20] Recall, $(\ell)\mathcal{O} = \mathfrak{l}\mathfrak{l}'$ as fractional $\mathcal{O}$-ideals.
[21] Hence, $\pi = [\sqrt{-p}]$.
[22] In stark contrast with ECC.

one outgoing $\mathbb{F}_p$-rational horizontal 2-isogeny as well as two horizontal ℓ-isogenies for every prime $\ell > 2$ with $\left(\frac{-p}{\ell}\right) = 1$.

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

(a) If $p \equiv 7 \bmod 8$, on each level $h(\mathcal{O}_K)$-many vertices are situated. Surface and floor are connected 1 to 1 with 2-isogenies and on the surface we also have two horizontal 2-isogenies from each vertex.

(b) If $p \equiv 3 \bmod 8$, we have $h(\mathcal{O}_K)$-many vertices on the surface and $3h(\mathcal{O}_K)$-many on the floor. Surface and floor are connected 1 to 3 with 2-isogenies, and there are no horizontal 2-isogenies.

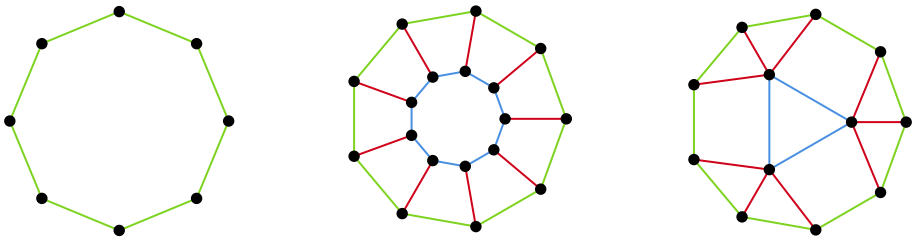


Figure 3: Examples of $\mathbb{F}_p$-volcanoes belonging to the cases 1, 2(a) and 2(b) (from left to right). The vertical 2-isogenies are red, the horizontal isogenies on the floor are green and the horizontal isogenies on the surface are blue.

Proof. See Chapter 4.4. ∎

In contrast to the CRS scheme where we look at the whole endomorphism ring $\mathrm{End}(E)$, in CSIDH we only look at the $\mathbb{F}_p$-rational endomorphisms for a supersingular elliptic curve E defined over the prime field $\mathbb{F}_p$. Denoted $\mathrm{End}_p(E)$, the $\mathbb{F}_p$-rational subring is an order in an imaginary quadratic number field, see [Wat69, Theorem 4.1 and Theorem 6.1]. It contains the p-th power Frobenius endomorphism $\pi = [\sqrt{-p}]$ and therefore $\mathbb{Z}[\pi] := \mathbb{Z}[\sqrt{-p}] \subseteq \mathrm{End}_p(E)$. Since $p \equiv 3 \bmod 4$, we know from Theorem 3.5 that the floor of the isogeny graph corresponding to $\mathbb{Z}[\sqrt{-p}]$ contains the most vertices out of all levels. Therefore, we prefer to work with $\mathbb{F}_p$-isomorphism classes of elliptic curves situated on the floor of a volcano. We thus only consider horizontal isogenies and $\mathbb{F}_p$-isomorphism classes of elliptic curves with the same endomorphism ring.

In the context of the Diffie-Hellman protocol, CSIDH has starting curve $E_0 \colon y^2 = x^3 + x$, which defines a supersingular elliptic curve over $\mathbb{F}_p$ whenever $p \equiv 3 \bmod 4$, see Example 2.10. We also know $x^3 + x$ can only have one $\mathbb{F}_p$-rational root because $\sqrt{-1} \notin \mathbb{F}_p$ if $p \equiv 3 \bmod 4$. Therefore, only one subgroup of order 2 exists in $E(\mathbb{F}_p)$. By Theorem 3.5 this implies E_0 must lie on the floor of the isogeny volcano. Therefore, $\mathrm{End}_p(E) = \mathbb{Z}[\sqrt{-p}]$. Although this does no longer address the vulnerability from the $L_q[1/2]$ quantum attack due to Childs, Jao and Soukharev[23], the resulting scheme proves to be much more efficient. It was first published in 2018 [Cas+18].

Distinguishing vertices using the j-invariant is not possible in this scheme. We need another method to identify the $\mathbb{F}_p$-isomorphism classes. Namely, even though two elliptic curves are not isomorphic over $\mathbb{F}_p$, they might have the same j-invariant if they are isomorphic over $\overline{\mathbb{F}}_p$. In that case, they are each other's quadratic twist[24]. We can efficiently denote and distinguish $\mathbb{F}_p$-isomorphism classes if we require $p \equiv 3 \bmod 8$ and $\mathrm{End}_p(E) = \mathbb{Z}[\sqrt{-p}]$ using the following proposition from [Cas+18].

Proposition 3.6 ([Cas+18], Proposition 8)**.** *Let $p \geq 5$ be a prime such that $p \equiv 3 \bmod 8$, and let $E/\mathbb{F}_p$ be a supersingular elliptic curve. Then $\mathrm{End}_p(E) = \mathbb{Z}[\sqrt{-p}]$ if and only if there exists $A \in \mathbb{F}_p$ such that E is $\mathbb{F}_p$-isomorphic to the curve $E_A : y^2 = x^3 + Ax^2 + x$. Moreover, if such a A exists then it is unique.*

Proof. See the end of Chapter 5.4. ∎

[23] The endomorphism ring we work with is a commutative ring, meaning the attack remains viable.
[24] This is not true if $j = 0$ or $j = 1728$.

We explore the details and other perks of the Montgomery form $By^2 = x^3 + Ax^2 + x$ for elliptic curves in Chapter 5.

Example 3.7. We aim to find all the vertices at the floor level of the isogeny volcano of the curve $E_0/\mathbb{F}_{419}\colon y^2 = x^3 + x$, with $419 = 4(3 \cdot 5 \cdot 7) - 1$ and so $419 \equiv 3 \bmod 4$. To this end we want to determine the class group actions of $\mathfrak{p}_3 = (3, \pi - 1), \mathfrak{p}_5 = (5, \pi - 1)$ and $\mathfrak{p}_7 = (7, \pi - 1)$ giving rise to the isogenies making up the horizontal isogeny graph with E_0. We find for $i \in \{3, 5, 7\}$ that

$$\begin{aligned} E_0[\mathfrak{p}_i] &= \left\{P \in E_0(\overline{\mathbb{F}}_{419})\colon \alpha(P) = 0 \text{ for all } \alpha \in \mathfrak{p}_i\right\} \\ &= E_0[N(\mathfrak{p}_i)] \cap E_0(\mathbb{F}_{419}) \end{aligned}$$

and next we randomly choose a $\mathbb{F}_{419}$-rational point P in the kernel of $[N(\mathfrak{p}_i)]$ and check whether $(420/N(\mathfrak{p}_i))\,P$ has order $N(\mathfrak{p}_i)$. If it has, then $\langle P\rangle$ gives rise to a kernel of an $N(\mathfrak{p}_i)$-isogeny which we can compute using Vélu's equations. We determine[25] $N((3, \pi - 1)) = 3$, $N((5, \pi - 1)) = 5$ and $N((7, \pi - 1)) = 7$. Using the functionalities `.isogeny()` and `.montgomery_model()` in `Sage`, we can compute all the vertices of the isogeny volcano belonging to the order $\mathbb{Z}[\pi]$ and starting curve E_0. For the relevant code, we refer to Appendix B.1.

From here we can already construct the isogeny volcano(es), using [Feo17, Corollary 78], see Corollary 2.20. In the context of this example, $\mathcal{O} = \mathbb{Z}[\sqrt{-419}]$ with conductor 2. The prime ℓ is one of $\{3, 5, 7\}$ and does therefore not divide the conductor. Hence, ℓ splits as a product of two distinct prime ideals, $(\ell, \pi - 1)$ and $(\ell, \pi + 1)$ and so there are $h(\mathbb{Z}[\sqrt{-419}])/n$ distinct ℓ-isogeny volcanoes of Elkies type, with craters in $\mathrm{Ell}_{\mathbb{F}_q}(\mathbb{Z}[\sqrt{-419}])$ of size n, where n is the order of $(\ell, \pi - 1)$ in $\mathrm{Cl}(\mathbb{Z}[\sqrt{-419}])$. We know from Theorem 2.5 that $h(\mathcal{O})$ is given by degree of the Hilbert class polynomial of $\mathbb{Z}[\pi] = \mathbb{Z}[\sqrt{-419}]$. Using the `Magma` code in Appendix A.4, we find that $h(\mathbb{Z}[\sqrt{-419}]) = 27$. Moreover, using the functionality `RingClassGroup()` in `Magma` it is possible to determine $\mathrm{Cl}(\mathcal{O})$, which appears to be cyclic of order 27.

The generator of $\mathrm{Cl}(\mathcal{O})$ is the ideal class $[(3\pi, 1 + \pi)] = [(3, \pi + 1)] = [\mathfrak{p}_3^{-1}]$, so using the basis $\{1, \pi\}$ and the inverse of the map `m`: $\mathrm{Cl}(\mathcal{O}) \to \{\text{ideals in } \mathcal{O}\}$, we compute the relations $[\mathfrak{p}_5] = 12[\mathfrak{p}_3]$ and $[\mathfrak{p}_7] = 5[\mathfrak{p}_3]$. Therefore, $n = 27$ for $\ell = 3, 7$ and $n = 9$ for $\ell = 5$ so we obtain one isogeny graph with 27 vertices for the order $\mathbb{Z}[\sqrt{-419}]$. Note that the action of $\mathfrak{p}_5$ generates three disjoint cycles of each nine isogeny classes.

Using all of the information from above, we are able to construct the isogeny volcano of the order $\mathbb{Z}[\sqrt{-419}]$ with starting curve belonging to the Montgomery coefficient 0, see Figure 4. Since the Montgomery coefficients are unique ($419 \equiv 3 \bmod 8$), we denote each $\mathbb{F}_{419}$-isomorphism class of elliptic curves by its Montgomery coefficient. See Appendix B.1 for the code.

[25] Since the extension of residue fields is of degree $[\mathbb{Z}[\pi]/(i, \pi - 1) : \mathbb{F}_i] = 1$ for each $i \in \{3, 5, 7\}$.

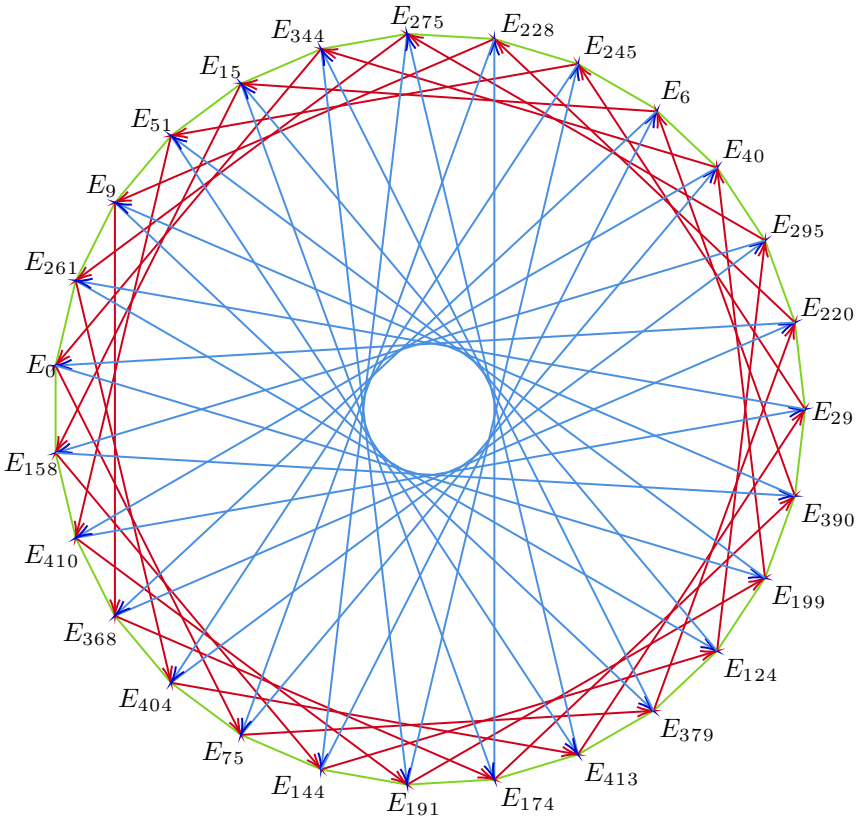


Figure 4: The union of horizontal isogeny graphs $G_{\mathbb{F}_{419},3}$ in green, $G_{\mathbb{F}_{419},5}$ in blue and $G_{\mathbb{F}_{419},7}$ in red. The Montgomery coefficients uniquely define the $\mathbb{F}_{419}$-isomorphism classes of elliptic curves.

It is also possible to generate such an isogeny graph for the order $\mathbb{Z}[(\sqrt{-419}+1)/2]$ of $\mathbb{Q}(\sqrt{-419})$ using Proposition 2.7 taken from [Cox22, Proposition 7.20]. Note that $-419 \equiv 1 \bmod 4$ and thus $\mathbb{Z}[\sqrt{-419}]$ is not a maximal order because $\mathbb{Z}[\sqrt{-419}] \subsetneq \mathbb{Z}[(\sqrt{-419}+1)/2]$ as orders of $\mathbb{Q}(\sqrt{-419})$. However, $\mathbb{Z}[(\sqrt{-419}+1)/2]$ is maximal[26] and thus the conductor[27] $f = 2$. Notice that the prime ideals $\mathfrak{p}_i$ are coprime to (2) in $\mathbb{Z}[\sqrt{-419}]$. Thus, they remain prime in $\mathbb{Z}[(\sqrt{-419}+1)/2]$. We compute their orders and thus the isogeny graph `Magma` using the code in Appendix A.5.

We notice that `m(G.1)`$= \mathfrak{p}_3^{-1}$ because $\{1, (\pi+1)/2\}$ is the basis of `S`$= \mathbb{Z}[(\sqrt{-419}+1)/2]$. Therefore, $[\mathfrak{p}_3]$ generates $\mathrm{Cl}(\mathbb{Q}(\sqrt{-419}))$, and therefore also $[\mathfrak{p}_5]$ and $[\mathfrak{p}_7]$. Using the inverse of the map `m`: $\mathrm{Cl}(\mathcal{O}_K) \to \{\text{ideals in } \mathcal{O}_K\}$, we obtain the relations $[\mathfrak{p}_5] = 3\,[\mathfrak{p}_3]$ and $[\mathfrak{p}_7] = 5\,[\mathfrak{p}_3]$. Hence, $n = 9$ for $\ell = 3, 7$, and $n = 3$ for $\ell = 5$. ♙

[26] Because

$$\Delta\left(\mathbb{Z}[\frac{\sqrt{-419}+1)}{2}]\right) = \Delta\left(f_{\mathbb{Q}}^{(\sqrt{-419}+1)/2}\right) = \Delta\left(x^2 - x + 105\right) = -419$$

is square-free.

[27] Note $[\mathbb{Z}[(\sqrt{-419}+1)/2] : \mathbb{Z}[\sqrt{-419}]] = 2$ because $n = 2$ is the smallest positive integer satisfying $n\mathbb{Z}[(\sqrt{-419}+1)/2] \subseteq \mathbb{Z}[\sqrt{-419}]$.

4 Supersingular isogeny graphs

In Chapter 2.3 of the preliminaries we introduce the reader to isogeny graphs of ordinary elliptic curves. However, in CSIDH exclusively supersingular elliptic curves are considered for a set of Elkies primes. This yields isogeny graphs that admit structure as described in Theorem 3.5, see also the example in Figure 3. Using the theory of (supersingular) elliptic curves, this chapter is a collection of important results that help us in proving said theorem at the end of this chapter.

Let E be a supersingular elliptic curve defined over the finite field $\mathbb{F}_q$ where $q = p^n$ is a prime power and $p \geq 5$. Recall that $\#E(\mathbb{F}_q) = q + 1$ if the curve E is supersingular, see [Sil86, Theorem V.4.1(a)]. By combining this fact with the following result, we are able to generate an isogeny graph consisting exclusively of (isomorphism classes of) supersingular curves and $\mathbb{F}_p$-rational isogenies (up to equivalence[28]).

Proposition 4.1 ([Sil86], Exercise 5.4)**.** *Two elliptic curves E, E' defined over a finite field $\mathbb{F}_q$ are isogenous over $\mathbb{F}_q$ if and only if $\#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q)$.*

Proof. From left to right, we notice $E(\mathbb{F}_q) = \ker(1 - \pi_E)$ where π_E is the q-th power Frobenius endomorphism of E, an elliptic curve. By assumption there exists an $\mathbb{F}_q$-rational isogeny $f\colon E \to E'$. We know that an isogeny $f\colon E \to E'$ is defined over $\mathbb{F}_q$ if $f \circ \pi_E = \pi_{E'} \circ f$, because the latter implies its kernel is invariant under the action of the Frobenius. On that note, we may assume that f is separable, because we can always factor the Frobenius endomorphism out. Note that the degree of a composition of isogenies is equal to the product of the degrees. Moreover, $1 - \pi_E$ is a separable isogeny for any E and so $\#\ker(1 - \pi_E) = \deg(1 - \pi_E)$. This concludes the proof since $f \circ \pi_E = \pi_{E'} \circ f$ implies $f \circ (1 - \pi_E) = (1 - \pi_{E'}) \circ f$ and so

$$\begin{aligned} \deg(f) \cdot \deg(1 - \pi_E) &= \deg(1 - \pi_{E'}) \cdot \deg(f) \\ \deg(1 - \pi_E) &= \deg(1 - \pi_{E'}) \\ \#\ker(1 - \pi_E) &= \#\ker(1 - \pi_{E'}) \\ \#E(\mathbb{F}_q) &= \#E'(\mathbb{F}_q). \end{aligned}$$

For the direction from right to left, we notice that if $\#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q)$, then they must have the same Frobenius endomorphism, because they have the same trace. We know from [Tat66, Theorem 1] that this implies E, E' are $\mathbb{F}_q$-isogenous. In order to not leave the reader empty handed, we hint on this connection. Waterhouse shows underneath Tate's theorem in [Wat69, Chapter 2] that the algebra $\mathrm{End}_{\mathbb{F}_q(E)} \otimes \mathbb{Q}_\ell$ of the elliptic curve $E/\mathbb{F}_q$ is completely determined by π. Moreover, it determines E up to $\mathbb{F}_q$-isogeny. ⌂

As a consequence, all elliptic curves in an isogeny graph must have the same trace. We fix the trace $t = 0$ and count the number of $\mathbb{F}_p$-isomorphism classes with supersingular elliptic curves in order to determine the structure of the $\mathbb{F}_p$-isogeny graph, denoted $G_{\mathbb{F}_p}$. Instead of doing this directly using the results in [Sch87] for example, we follow the structure in [DG16] which starts by looking at the full supersingular isogeny graph $G_{\overline{\mathbb{F}}_p} \supset G_{\mathbb{F}_p}$.

4.1 The number of j-invariants in a supersingular isogeny graph

Let $G_{\overline{\mathbb{F}}_p,\ell}$ denote the full supersingular isogeny graph for a fixed Elkies prime ℓ. It is a directed irregular graph in which the vertices are $\overline{\mathbb{F}}_p$-isomorphism classes of supersingular elliptic curves and the edges are equivalence classes of ℓ-isogenies defined over $\overline{\mathbb{F}}_p$. The vertices are uniquely represented by the j-invariants of the isomorphism classes, because $\overline{\mathbb{F}}_p$ is algebraically closed by definition. Note that we may regard any supersingular elliptic curve over $\mathbb{F}_{p^2}$, because the j-invariant of a supersingular elliptic curve always lies in $\mathbb{F}_{p^2}$, see [Sil86, Theorem V.3.1(a)(iii)]. Let S_{p^2} denote the set of all supersingular j-invariants in $\mathbb{F}_{p^2}$.

Proposition 4.2 ([Sil86], Theorem V.4.1(c))**.** *There is one supersingular curve in characteristic 3, and for $p \geq 5$, the number of supersingular elliptic curves (up to $\overline{\mathbb{F}}_p$-isomorphism) is*

[28] Two isogenies are equivalent if they have the same kernel.

$$\#S_{p^2} = \left\lfloor \frac{p}{12} \right\rfloor + \begin{cases} 0 & \text{if } p \equiv 1 \bmod 12 \\ 1 & \text{if } p \equiv 5 \bmod 12 \\ 1 & \text{if } p \equiv 7 \bmod 12 \\ 2 & \text{if } p \equiv 11 \bmod 12 \end{cases}$$

Next we focus on the graph $G_{\mathbb{F}_p,\ell}$ where the vertices are $\mathbb{F}_p$-isomorphism classes of elliptic curves and the edges are $\mathbb{F}_p$-rational ℓ-isogenies for a given prime ℓ. It is not a subgraph of the full supersingular isogeny graph, because each vertex in the full supersingular isogeny graph may contain multiple $\mathbb{F}_p$-isomorphism classes. We note that $G_{\mathbb{F}_p,L}$ is not necessarily connected, since we ignore j-invariants that are contained in $\mathbb{F}_{p^2} \setminus \mathbb{F}_p$. In order to obtain a connected graph, we need to find a set $L = \{\ell_1, \dots \ell_n\}$ such that the union[29]

$$G_{\mathbb{F}_p,L} = \bigcup_{\ell \in L} G_{\mathbb{F}_p,\ell}$$

is connected.

Next, we aim to determine the number of vertices in a connected graph $G_{\mathbb{F}_p,L}$, i.e. for sufficiently large L. To this end, we fix the number of $\mathbb{F}_p$-rational points on an elliptic curve. This is equivalent to fixing the trace of the elliptic curves by Theorem 2.14. The following result from [Cox22, Theorem 14.18] helps us determine the number of j-invariants in $\mathbb{F}_p$. In order to understand it, we first introduce the Hurwitz class number. Given an order $\mathcal{O}$ in an imaginary quadratic number field K, the Hurwitz class number[30] is defined as

$$H(\mathcal{O}) = \sum_{\mathcal{O} \subseteq \mathcal{O}' \subseteq \mathcal{O}_K} \frac{2}{|\mathcal{O}'^*|} h(\mathcal{O}').$$

We denote $H(\mathcal{O}) =: H(\Delta_{\mathcal{O}})$.

Theorem 4.3 (Deuring, see [Cox22] Theorem 14.18)**.** *Let $p \geq 5$ be prime. Then the number of elliptic curves E over $\mathbb{F}_p$ which have $\#E(\mathbb{F}_p) = p + 1 - t$ is*

$$\frac{p-1}{2} H\left(t^2 - 4p\right),$$

where H is the Hurwitz class number.

In the context of supersingular curves, we know that $t = 0$ and thus $-4p = \Delta_\pi$ the discriminant of the order $\mathbb{Z}[\pi]$ in the number field $K = \mathbb{Q}(\pi) = \mathbb{Q}(\sqrt{-p})$. The order $\mathbb{Z}[\pi]$ plays an important role due to the following result.

Theorem 4.4 ([Sch87], Theorem 4.3)**.** *Let E be a supersingular elliptic curve over $\mathbb{F}_p$, where $p \geq 5$. The $\mathbb{F}_p$-endomorphism ring of a supersingular elliptic curve is a complex quadratic order $\mathcal{O}$ of a number field $K = \mathbb{Q}(\sqrt{-p})$ with*

$$\mathbb{Z}[\sqrt{-p}] \subset \mathcal{O} \quad \text{and} \quad p \nmid [\mathcal{O}_K : \mathcal{O}].$$

Depending on $p \bmod 4$, we can further characterize the number of supersingular elliptic curves over $\mathbb{F}_p$, up to $\mathbb{F}_p$-isomorphism. To this end, we count the number of supersingular j-invariants in $\mathbb{F}_p$ and the number of quadratic twists of an elliptic curve in this and the next two sub-chapters. The following result is the first step in this process. It appears in [DG16] without proof, and we provide a proof in this thesis that leans on the result and proof of Theorem 4.3 and in [Cox22, Theorem 14.18] respectively.

Theorem 4.5 ([DG16], Page 426)**.** *Let $p \geq 5$ be prime. Then the number of supersingular j-invariants in $\mathbb{F}_p$ is*

$$\begin{aligned} h(\mathcal{O}_K)/2 &\text{ if } p \equiv 1 \bmod 4 \\ h(\mathcal{O}_K) &\text{ if } p \equiv 7 \bmod 8 \\ 2h(\mathcal{O}_K) &\text{ if } p \equiv 3 \bmod 8, \end{aligned}$$

where $h(\mathcal{O})$ is the ideal class number of the order $\mathcal{O}$.

[29] Not disjoint, but defined by taking the union of the respective vertex and edge sets.
[30] Taken from [Cox22, Page 319].

Before we prove this theorem, let us consider the following results.

Lemma 4.6. *The rational prime 2 splits in $\mathbb{Z}[(\sqrt{-p}+1)/2]$ for $p \equiv 7 \bmod 8$ and remains inert in $\mathbb{Z}[(\sqrt{-p}+1)/2]$ for $p \equiv 3 \bmod 8$.*

Proof. Let us first consider $p \equiv 7 \bmod 8$. We note that $\frac{p+1}{4}$ must be even as a consequence. Therefore,

$$(2) = \left(2, \frac{\sqrt{-p}+1}{2}\right)\left(2, \frac{\sqrt{-p}-1}{2}\right)$$

into distinct prime ideals because

$$\frac{\sqrt{-p}+1}{2} \cdot \frac{\sqrt{-p}-1}{2} = \frac{-p-1}{4}$$

is even. Next, consider $p \equiv 3 \bmod 8$. The minimal polynomial defining $\mathbb{Z}[(\sqrt{-p}+1)/2]$ is given by $X^2 - X + (p+1)/4$. We find that $X^2 + X + (p+1)/4$ is irreducible modulo 2 because $(p+1)/4$ is odd. By the Kummer-Dedekind Theorem, this implies 2 is inert in $\mathbb{Z}[(\sqrt{-p}+1)/2]$, meaning (2) is prime in the ring of integers. ∎

Lemma 4.7 ([Cox22], Theorem 7.24)**.** *Let $\mathcal{O}$ be the order of conductor f in an imaginary quadratic field K. Then*

$$h(\mathcal{O}) = \frac{h(\mathcal{O}_K)\, f}{[\mathcal{O}_K^* : \mathcal{O}^*]} \prod_{q \mid f} \left(1 - \left(\frac{\Delta_K}{q}\right)\frac{1}{q}\right).$$

Furthermore, $h(\mathcal{O})$ is always an integer multiple of $h(\mathcal{O}_K)$.

Proof of Theorem 4.5. Let us first address the number of supersingular j-invariants in $\mathbb{F}_p$ regardless of $p \bmod 4, 8$. We know by Deuring's Lifting Theorem, see Theorem 2.12, that any elliptic curve E defined over $\mathbb{F}_p$ is the (good) reduction at p of an elliptic curve over a number field. We are interested in the primes p at which the latter has supersingular reduction. As is done in the proof of Theorem 4.3, we consider to this end an order $\mathcal{O}$ in the imaginary quadratic number field $K = \mathbb{Q}(\pi)$, where π is the Frobenius endomorphism for an ordinary elliptic curve, containing $\mathbb{Z}[\pi]$. We also consider a proper $\mathcal{O}$-ideal $\mathfrak{a}$. Let $L = K(j(\mathfrak{a}))$ such that p splits completely in L by [Cox22, Theorem 9.4]. If $\mathfrak{p}$ is a prime of L dividing p, then $\mathcal{O}_L/\mathfrak{p} \cong \mathbb{F}_p$.

For $j(\mathfrak{a}) \neq 0, 1728$ we let

$$k = \frac{27 j(\mathfrak{a})}{j(\mathfrak{a} - 1728)}.$$

We can then define a collection of elliptic curves by

$$E_c \colon y^2 = 4x^3 - kc^2 x - kc^3$$

for arbitrary $c \in \mathcal{O}_L \setminus \mathfrak{p}$. Reducing E_c at a prime p implies we take c in $\mathbb{F}_p \setminus \{0\}$ instead. This yields $p-1$ distinct reductions of E_c with the same j-invariant, because in the proof of [Cox22, Theorem 14.18] it is shown that E_c has good reduction modulo p due to the fact that we take $c \in \mathcal{O}_L \setminus \mathfrak{p}$. A different definition of k and E_c in the cases $j(\mathfrak{a}) = 0, 1728$ yields the same result.

We know that there exist exactly $p(p-1)$ distinct elliptic curves over $\mathbb{F}_p$. Suppose $a \in \mathbb{Z}_{\geq 0}$ distinct ordinary j-invariants occur, where $a \leq p$. Then, the number of supersingular elliptic curves over $\mathbb{F}_p$ is equal to $p(p-1) - a(p-1) = (p-a)(p-1)$. Moreover, we know from [Sil86, Proposition III.1.4(c)] that for any $j_0 \in \mathbb{F}_p$ there exists an elliptic curve over $\mathbb{F}_p$ with $j(E) = j_0$. Thus, there exist $p-a$ supersingular j-invariants and exactly $p-1$ distinct supersingular elliptic curves per j-invariant. Therefore, the number of distinct j-invariants belonging elliptic curves E over $\mathbb{F}_p$ which have $\#E(\mathbb{F}_p) = p+1$ (i.e. the supersingular elliptic curves) is

$$\frac{1}{2} H(-4p).$$

Next, suppose the Frobenius endomorphism π has trace $t = 0$ and $p \geq 5$, so we focus on the supersingular case. If $p \equiv 1 \bmod 4$, then $\mathbb{Z}[\pi] = \mathcal{O}_K$ is maximal and so

$$H(\mathbb{Z}[\pi]) = \frac{2}{|\mathbb{Z}[\pi]^*|} h(\mathbb{Z}[\pi]).$$

Note that π has characteristic polynomial $X^2 + p$ and so the number field $\mathbb{Q}(\alpha) := \mathbb{Q}[x]/(x^2 + p)$ has one complex embedding $\alpha \mapsto \pm\sqrt{-p}$. Therefore, we know from Dirichlet's unit theorem that no fundamental unit exists in $\mathbb{Z}[\pi]$. Moreover, since the extension $K/\mathbb{Q}$ is quadratic, the unit group $\mathbb{Z}[\pi]^* = \{\pm 1\}$. Indeed, we know that if $\mathbb{Z}[\pi]^* = \langle \zeta_m \rangle$ with m the largest integer for which $\mathbb{Q}(\zeta_m) \subset K$, then $[\mathbb{Q}(\zeta_m) \colon \mathbb{Q}]$ should divide $[K \colon \mathbb{Q}] = 2$ and any odd prime factor of m should divide Δ_K. We know $\Delta_K = -4p$ if $p \equiv 1 \bmod 4$, and so this only allows for the second, fourth and sixth roots of unity because they are the only ones that give rise to an at most quadratic field extension. However, since $\zeta_6 = (1 \pm i\sqrt{3})/2$, we can discard the sixth roots of unity because $p \neq 3$. Similarly, we find that $\zeta_4 \notin \mathbb{Z}[\pi]^*$ because $\zeta_4 = \pm i \notin K = \mathbb{Q}(\sqrt{-p})$. Thus, $|\mathbb{Z}[\pi]^*| = 2$ and so

$$H(\mathbb{Z}[\pi]) = h(\mathbb{Z}[\pi]) \text{ if } p \equiv 1 \bmod 4.$$

In the case $p \equiv 3 \bmod 4$, we know $\mathbb{Z}[\pi] \subsetneq \mathcal{O}_K = \mathbb{Z}\left[\frac{\pi+1}{2}\right] \subset K$. If $p \geq 5$, we find that similarly as before $|\mathbb{Z}[\pi]^*| = 2$ and $|\mathbb{Z}[(\pi + 2)/2]^*| = 2$ since they have the same field of fractions. Therefore,

$$H(\mathbb{Z}[\pi]) = h(\mathbb{Z}[\pi]) + h(\mathcal{O}_K).$$

We aim to further simplify this expression by finding a relation between the ideal class groups of $\mathbb{Z}[\pi]$ and $\mathcal{O}_K = \mathbb{Z}[(\pi + 1)/2]$. To this end we use the results in Lemma 4.6 and Lemma 4.7. In the equation of Lemma 4.7,

$$\left(\frac{\Delta_K}{q}\right)$$

denotes the Kronecker symbol, also called the Legendre symbol if the prime q is odd.

Since $p \geq 5$, we immediately know that $[\mathcal{O}_K^* \colon \mathbb{Z}[\pi]^*] = 1$ from the arguments above. Next, we know that $f = 2$ if $p \equiv 3 \bmod 4$. The only prime divisor of the conductor is therefore $q = 2$. Also, we know that $\Delta_K = -p$. It remains to determine the Kronecker symbol, which is tied to the question whether 2 splits or remains inert in $\mathcal{O}_K$.

If $p \equiv 3 \bmod 8$, then we know from Lemma 4.6 that 2 stays inert in $\mathcal{O}_K$, and so

$$\left(\frac{-p}{2}\right) = -1,$$

which is in agreement with the definition given in [Cox22, Page 146]. We compute

$$h(\mathbb{Z}[\pi]) = 2h(\mathcal{O}_K) \cdot \left(1 + \frac{1}{2}\right) = 3h(\mathcal{O}_K).$$

If $p \equiv 7 \bmod 8$, then by Lemma 4.6 we find that 2 splits in $\mathcal{O}_K$ and so

$$\left(\frac{-p}{2}\right) = 1,$$

again in accordance with the definition of the Kronecker symbol. Therefore,

$$h(\mathbb{Z}[\pi]) = 2h(\mathcal{O}_K) \cdot \left(1 - \frac{1}{2}\right) = h(\mathcal{O}_K).$$

From this proof, we derive two facts that help us determine the structure of $\mathbb{F}_p$-rational supersingular isogeny graphs in Chapter 4.4.

Corollary 4.8. *If $p \equiv 3 \bmod 8$, then $h(\mathbb{Z}[\pi]) = 3h(\mathcal{O}_K)$ and if $p \equiv 7 \bmod 8$, then $h(\mathbb{Z}[\pi]) = h(\mathcal{O}_K)$.*

4.2 The (quadratic) twist of an elliptic curve

An elliptic curve and its non-trivial[31] (quadratic) twists give rise to distinct $\mathbb{F}_p$-isomorphism classes. To understand how many $\mathbb{F}_p$-isomorphism classes exist, we consider the concept of a (quadratic) twist of an elliptic curve over a perfect field k, taken from [Sil86, Proposition X.5.4]. Let $\mathrm{Twist}((E,O)/k)$ denote the isomorphisms of the elliptic curve E in Weierstrass form defined over k.

Proposition 4.9 ([Sil86], Proposition X.5.4)**.** *Assume that* $\mathrm{Char}(k) \neq 2,3$*, and let*

$$n = \begin{cases} 2 & \text{if } j(E) \neq 0, 1728, \\ 4 & \text{if } j(E) = 1728, \\ 6 & \text{if } j(E) = 0 \end{cases}$$

Then $\mathrm{Twist}((E,O)/k)$ *is canonically isomorphic to* $k^*/(k^*)^n$*. More precisely, choose a Weierstrass equation*

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

for E/k*, and let* $D \in k^*$*. Then the elliptic curve* $E_D \in \mathrm{Twist}((E,O)/k)$ *corresponding to* $D \bmod (k^*)^n$ *has Weierstrass equation*

(i) $E_D : y^2 = x^3 + D^2Ax + D^3B$ *if* $j(E) \neq 0, 1728$*,*

(ii) $E_D : y^2 = x^3 + DAx$ *if* $j(E) = 1728$ *(so* $B = 0$*),*

(iii) $E_D : y^2 = x^3 + DB$ *if* $j(E) = 0$ *(so* $A = 0$*).*

Using this proposition and given the number of $\mathbb{F}_p$-rational points on an elliptic curve, we can determine the number of $\mathbb{F}_p$-rational points on the quadratic twist corresponding to $D = -1$ if $p \equiv 3 \bmod 4$ and on the condition that $j \neq 0, 1728$.

In the remainder of Chapter 4.2 we assume $p \equiv 3 \bmod 4$ and $j \neq 0, 1728$.

Note $\mathbb{F}_p^*/(\mathbb{F}_p^*)^2$ is generated by[32] -1 and thus $D = -1$ yields the unique non-trivial quadratic twist of E. This inspires the following result.

Proposition 4.10. *Assume* $p \equiv 3 \bmod 4$ *and consider an elliptic curve* $E\colon y^2 = x^3 + Ax + B$ *with* $j(E) \neq 0, 1728$ *defined over* $\mathbb{F}_p$ *such that* $\#E(\mathbb{F}_p) = p+1-t$*. Then the elliptic curve* $E_{-1} \in \mathrm{Twist}((E,O)/k)$ *satisfies* $\#E_{-1}(\mathbb{F}_p) = p + 1 + t$*.*

Proof. We work in the context of a finite prime field $k = \mathbb{F}_p$ where $p \equiv 3 \bmod 4$ and aim to use Proposition 4.9. We know -1 is a non-quadratic residue modulo p and so $D = -1$ defines a non-trivial twist if $A, B \neq 0$. Then the map $\varphi\colon E \to E_{-1}$ is be defined by[33] $(x,y) \mapsto (-x, iy)$ such that

$$E_{-1}\colon y^2 = x^3 + Ax - B.$$

Note that the latter is $\mathbb{F}_p$-isomorphic to

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

via $[-1]\colon E_{-1} \to E'$ where $(x,y) \mapsto (-x,y)$. Since -1 is a non-quadratic residue in $\mathbb{F}_p$, we know that for any $x \in \mathbb{F}_p$, if $x^3 + Ax + B$ is a non-quadratic residue modulo p, then $-x^3 - Ax - B$ must be a quadratic residue. Thus, for any $x \in \mathbb{F}_p$ we find that if $x^3 + Ax + B \neq 0$, then $(x, x^3 + Ax + B)$ must be a point in $E(\mathbb{F}_p)$ or $E'(\mathbb{F}_p)$ exclusively. Note that each $x \in \mathbb{F}_p$ for which $x^3 + Ax + B = 0$ appears exactly once in both $E(\mathbb{F}_p)$ and $E'(\mathbb{F}_p)$. Counting the point at infinity for both curves, this implies $\#E(\mathbb{F}_p) + \#E'(\mathbb{F}_p) = 2(p+1)$. Since $E' \cong E_{-1}$ over $\mathbb{F}_p$, we know that $\#E' = \#E_{-1}$ by Proposition (4.1), which yields $\#E_{-1}(\mathbb{F}_p) = p + 1 + t$. ∎

[31] A twist is trivial if it is $\mathbb{F}_p$-isomorphic to the original curve.

[32] We know that an element $a \in \mathbb{F}_p^*$ is a square if and only if $a^{\frac{p-1}{2}} = 1$. Note $(-1)^{\frac{p-1}{2}} = -1$ since $p \equiv 3 \bmod 4$. Therefore, a is a square if and only if $-a$ is a non-square in $\mathbb{F}_p^*$.

[33] Therefore, $\varphi = [i]$.

Thus, an ordinary elliptic curve E defined over $\mathbb{F}_p$ where $p \equiv 3 \bmod 4$ and $j(E) \neq 0, 1728$ is never $\mathbb{F}_p$-isogenous to E_{-1} by Proposition 4.1, because $p \nmid t$. However, when E is supersingular then $p \mid t$ and we recall the bound on the trace $|t| \leq 2p$ from [Sil86, Theorem V.1.1]. If $p \geq 5$, this implies $t = 0$. Therefore, E and E_{-1} are $\mathbb{F}_p$-isogenous in the supersingular case. They have the same j-invariant because they are isomorphic via the multiplication-by-i map, an isomorphism. In Example (3.7), each j-invariant appears at most twice on the floor of the supersingular graph $G_{\mathbb{F}_{419},L}$ where $L = \{3, 5, 7\}$. Even for the curves with j-invariants $0, 1728$ in $\mathbb{F}_{419}$. We prove in Chapter 4.3 that this is no coincidence.

In the Diffie-Hellman protocol introduced in Chapter 3.2, it is no longer practical to use just the j-invariant to uniquely represent vertices in the isogeny graph, because multiple vertices can have the same j-invariant. Although one could additionally communicate the coefficients of the Weierstrass model to resolve this issue, in practice there exists a more efficient and elegant solution using the Montgomery form. For the details surrounding its use, we refer to Chapter 5. Importantly, it grants us a new method by which we can efficiently denote $\mathbb{F}_p$-isomorphism classes if $p \equiv 3 \bmod 8$. To determine the number of vertices in a supersingular isogeny graph, we take a closer look at the amount of $\mathbb{F}_p$-isomorphism classes per j-invariant.

4.3 The number of $\mathbb{F}_p$-isomorphism classes for a given j-invariant

The following theorem tells us the number of $\mathbb{F}_p$-isomorphism classes of elliptic curves per supersingular j-invariant in $\mathbb{F}_p$. It displays commonalities with Proposition 4.9, which is not a coincidence. Indeed, all elliptic curves that have the same j-invariant, are twists of one another. Note that the number of $\mathbb{F}_p$-isomorphism classes is equal to the number of non-trivial twists, i.e. the number of elements in $\mathbb{F}_p^*/(\mathbb{F}_p^*)^n$ where $n \in \{2, 4, 6\}$ depending on the j-invariant. We can use this fact to prove the following result.

Theorem 4.11 ([BS07], Theorem 2.2)**.** *Let $p \geq 5$ and let $j \in \mathbb{F}_p$. The number of elliptic curves (up to $\mathbb{F}_p$-isomorphism) with j-invariant j is:*

(i) 4 if $j = 1728$ and $p \equiv 1 \bmod 4$;

(ii) 6 if $j = 0$ and $p \equiv 1 \bmod 3$;

(iii) 2 otherwise.

Proof. If $j \neq 0, 1728$, suppose using the notation from Proposition 4.9 that there are two elliptic curves, denoted E and E_D where D is in $\mathbb{F}_p^*$, with $j = j(E) = j(E_D)$. If $E\colon y^2 = x^3 + Ax + B$, then we know that E, E_D are $\mathbb{F}_p$-isomorphic if there exist $a, b \in \mathbb{F}_p^*$ such that

$$a^4 A = D^2 A \quad \text{and} \quad b^6 B = D^3 B.$$

Since $A, B \neq 0$, this can only be true if D is a square in $\mathbb{F}_p^*$. The number of $\mathbb{F}_p$-isomorphism classes with fixed j-invariant $j \neq 0, 1728$ must then be equal to $\#\mathbb{F}_p^*/(\mathbb{F}_p^*)^2$. Notice that the map $\varphi_2\colon \mathbb{F}_p^* \to \mathbb{F}_p^*$ defined by $x \mapsto x^2$ has kernel $\ker(\varphi_2) = \{\pm 1\}$. Since $\#\ker(\varphi_2) = \#\mathbb{F}_p^*/(\mathbb{F}_p^*)^2$, where $\mathrm{im}(\varphi_2) = (\mathbb{F}_p^*)^2$, we can conclude.

If $j = 1728$, we claim that the number of $\mathbb{F}_p$-isomorphism classes equals the number of elements in $\mathbb{F}_p^*/(\mathbb{F}_p^*)^4$. Indeed, elliptic curves with this j-invariant are of the form $E\colon y^2 = x^3 + Ax$ and for any $D \bmod (\mathbb{F}_p^*)^4$ we have $E_D\colon y^2 = x^3 + DAx$ by Proposition 4.9. We know that E, E_D are isomorphic over $\mathbb{F}_p$ if and only if there exists $a \in \mathbb{F}_p^*$ with

$$DA = a^4 A.$$

Thus, it suffices to determine $\#\mathbb{F}_p^*/(\mathbb{F}_p^*)^4$. First, consider $p \equiv 1 \bmod 4$. Since the map $\varphi_4\colon \mathbb{F}_p^* \to \mathbb{F}_p^*$ defined by $x \mapsto x^4$ has $\ker(\varphi_4) = \{\pm i, \pm 1\} \subset \mathbb{F}_p^*$, we find that $\#\mathbb{F}_p^*/(\mathbb{F}_p^*)^4 = 4$. However, if $p \equiv 3 \bmod 4$, then $\ker(\varphi_4) = \{\pm 1\}$ and so $\#\mathbb{F}_p^*/(\mathbb{F}_p^*)^4 = 2$.

If $j = 0$, we find analogously that the number of $\mathbb{F}_p$-isomorphism classes equals the number of elements in $\mathbb{F}_p^*/(\mathbb{F}_p^*)^6$. Indeed, elliptic curves with this j-invariant are of the form $E\colon y^2 = x^3 + B$ and for any

$D \bmod (\mathbb{F}_p^*)^6$ we have $E_D\colon y^2 = x^3 + DB$ by Proposition 4.9. We know that E, E_D are isomorphic over $\mathbb{F}_p$ if and only if there exists $b \in \mathbb{F}_p^*$ with

$$DB = b^6 B.$$

Thus, it suffices to determine $\#\mathbb{F}_p^*/(\mathbb{F}_p^*)^6$. First, consider $p \equiv 1 \bmod 3$. Since the map $\varphi_6\colon \mathbb{F}_p^* \to \mathbb{F}_p^*$ defined by $x \mapsto x^6$ has $\ker(\varphi_6) = \{(\pm 1 \pm \sqrt{-3})/2, \pm 1\} \subset \mathbb{F}_p^*$, we find that $\#\mathbb{F}_p^*/(\mathbb{F}_p^*)^6 = 6$. However, if $p \equiv 2 \bmod 3$, then $\ker(\varphi_6) = \{\pm 1\}$ and so $\#\mathbb{F}_p^*/(\mathbb{F}_p^*)^6 = 2$. ↰

Proposition 4.12. *Consider $p \geq 5$ and let E be an elliptic curve over $\mathbb{F}_p$. If $j(E) = 1728$, then E is supersingular if and only if $p \equiv 3 \bmod 4$. If $j(E) = 0$, then E is supersingular if and only if $p \equiv 2 \bmod 3$.*

In order to prove this result, we need a criterion by which we can check if an elliptic curve is supersingular. To this end, we use the first part of [Sil86, Theorem V.4.1] as a lemma in our proof.

Lemma 4.13 ([Sil86], Theorem V.4.1)**.** *Let $\mathbb{F}_q$ be a finite field of characteristic $p \geq 3$. Let $E/\mathbb{F}_q$ be an elliptic curve given by a Weierstrass equation*

$$E : y^2 = f(x)$$

where $f(x) \in \mathbb{F}_q[x]$ is a cubic polynomial with distinct roots in $\overline{\mathbb{F}}_q$. Then E is supersingular if and only if the coefficient of x^{p-1} in $f(x)^{(p-1)/2}$ is zero.

Proof of Proposition 4.12. If $j(E) = 1728$, this means $E\colon y^2 = x^3 + x$, because E can be defined by a short Weierstrass equation[34] where $A = 1$ and $B = 0$. We claim that the coefficient of x^{p-1} in $(x^3 + x)^{(p-1)/2}$ is equal to zero if and only if $p \equiv 3 \bmod 4$. Notice $(p-1)/2$ is an odd integer, so choosing $(p-1)/2$ factors from $\{x^3, x\}$ never yields x^{p-1}. On the other hand, if $p \equiv 1 \bmod 4$, then $(p-1)/2$ is even and so we can pick x^3 and x an equal number of times, giving rise to x^{p-1}.

If $j(E) = 0$, this means $E\colon y^2 = x^3 + 1$ by analogous reasoning. We claim that the coefficient of x^{p-1} in $(x^3 + 1)^{(p-1)/2}$ is equal to zero if and only if $p \equiv 2 \bmod 3$. Notice $(p-1)/2 \equiv 2 \bmod 3$, so there exists $k \in \mathbb{Z}_{\geq 0}$ such that choosing $(p-1)/2 = 3k + 2$ factors from $\{x^3, 1\}$ never yields $x^{p-1} = x^{6k+4}$, because this would imply there exists $n \in \mathbb{Z}_{\geq} 0$ such that

$$\begin{aligned} 6k + 4 &= 3(3k + 2 - n) \\ 3n &= 3k + 2. \end{aligned}$$

Since famously $3 \nmid 2$, we conclude choosing $(p-1)/2$ factors from $\{x^3, 1\}$ never yields x^{p-1}. On the other hand, if $p \equiv 1 \bmod 3$, then $p - 1$ is divisible by 3. Choosing x^3 a number of $(p-1)/3$ times yields x^{p-1}. ↰

4.4 The supersingular $\mathbb{F}_p$-isogeny graph

Next, we determine the structure of $G_{\mathbb{F}_p, L}$ depending on p and such that L contains a sufficient number of[35] Elkies primes and 2. We need the following results in order to prove Theorem 3.5, which completely determines the structure of $G_{\mathbb{F}_p, L}$.

Lemma 4.14. *Let $p \geq 5$. The number of $\mathbb{F}_p$-isomorphism classes of supersingular curves over $\mathbb{F}_p$ is*

$$\begin{aligned} h(\mathcal{O}_K) &\text{ if } p \equiv 1 \bmod 4 \\ 2h(\mathcal{O}_K) &\text{ if } p \equiv 7 \bmod 8 \\ 4h(\mathcal{O}_K) &\text{ if } p \equiv 3 \bmod 8, \end{aligned}$$

where $h(\mathcal{O})$ is the ideal class number of the order $\mathcal{O}$.

[34] A short Weierstrass equation is of the form $y^2 = x^3 + Ax + B$ where $j = 1728\frac{4A^3}{4A^3 + 27B^2}$, see page 45 in [Sil86].

[35] Sufficient in the sense that the resulting graph is connected, and such that the CSIDH protocol generates a key with the desired number of bits.

Proof. We notice from Theorem 4.11 and Proposition 4.12 that for any supersingular j-invariant in $\mathbb{F}_p$ there exist exactly two $\mathbb{F}_p$-isomorphism classes of elliptic curves. We combine this observation with the results of Theorem 4.5 to finish the proof. ↰

Lemma 4.15 ([DG16], page 432)**.** *Let $p \equiv 3 \bmod 4$ where $p \geq 5$, and let E be a supersingular elliptic curve defined over $\mathbb{F}_p$. Then*

$$\mathrm{End}_p(E) = \mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right] \text{ if and only if } E[2] \subset E(\mathbb{F}_p).$$

Proof. See the excellent proof of the ePrint [Arp+21, Lemma 3.4]. ↰

Proof of Theorem 3.5. Due to Theorem 4.4, we notice that for any supersingular elliptic curve E in $G_{\mathbb{F}_p,L}$ either $\mathrm{End}_p(E) = \mathbb{Z}[\sqrt{-p}]$ or $\mathrm{End}_p(E) = \mathcal{O}_K$. If $p \equiv 1 \bmod 4$ then $\mathbb{Z}[\sqrt{-p}] = \mathcal{O}_K$ and if $p \equiv 3 \bmod 4$ they are distinct. Thus, the $\mathbb{F}_p$-rational supersingular isogeny graph $G_{\mathbb{F}_p,L}$ has at most two layers. Vertical isogenies can only occur if $p \equiv 3 \bmod 4$.

Next, we determine the occurrence of edges, i.e. $\mathbb{F}_p$-rational isogenies of degree $\ell \in L$, in $G_{\mathbb{F},L}$ such that $\ell \mid (p+1)$. Since $E[\ell](\overline{\mathbb{F}}_p) \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ for any prime ℓ, we know that every elliptic curve E gives rise to $(\ell+1)$-many ℓ-isogenies. We are interested in the isogenies that are $\mathbb{F}_p$-rational. We know that an isogeny is $\mathbb{F}_p$-rational if its kernel is invariant under $G(\overline{\mathbb{F}}_p/\mathbb{F}_p)$. In the context of a finite field this is equivalent to invariance under the action of the corresponding Frobenius. Thus, the occurrence of an $\mathbb{F}_p$-rational ℓ-isogeny between two vertices depends on the splitting behavior of the characteristic polynomial $X^2 + p$ modulo ℓ. For odd ℓ, we refer back to the Atkin, ramified and Elkies case just above Example 2.17.

Case 1 ($p \equiv 1 \bmod 4$): Let us first consider odd ℓ. In CSIDH, only primes ℓ that split in $\mathbb{Q}(\sqrt{-p})$ (Elkies case) are selected such that $\ell \in L$. This yields two $\mathbb{F}_p$-rational horizontal ℓ-isogenies. We know $\ell = 2$ ramifies in $\mathbb{Q}(\sqrt{-p})$ and so only one $\mathbb{F}_p$-rational horizontal 2-isogeny exists. The graph is a cycle of length $h(\mathcal{O}_K)$ by Lemma 4.14.

Case 2 ($p \equiv 7 \bmod 8$): Similarly to the previous case, if ℓ is odd then selecting only Elkies primes ℓ results in two $\mathbb{F}_p$-rational horizontal ℓ-isogenies. No vertical $\mathbb{F}_p$-rational ℓ-isogenies can occur due to Proposition 2.18.

Note from Lemma 4.6 that 2 splits, and so this yields at most two $\mathbb{F}_p$-rational horizontal 2-isogenies. We know from 4.15 that $E[2] \subset E(\mathbb{F}_p)$ if E lies on the surface and so each elliptic curve isomorphism on the surface has exactly one vertical $\mathbb{F}_p$-rational 2-isogeny.

Thus, the surface is a cycle of length $h(\mathcal{O}_K)$ connected one to one with the floor, which is also a cycle of length $h(\mathcal{O}_K)$ by Lemma 4.14 and Corollary 4.8.

Case 3 ($p \equiv 3 \bmod 8$): Similarly to the previous case, if ℓ is odd then selecting only Elkies primes ℓ results in two $\mathbb{F}_p$-rational horizontal ℓ-isogenies. No vertical $\mathbb{F}_p$-rational ℓ-isogenies can occur due to Proposition 2.18.

Note from Lemma 4.6 that 2 is inert, and so this yields no horizontal 2-isogenies. We know from 4.15 that $E[2] \subset E(\mathbb{F}_p)$ if E lies on the surface and so each elliptic curve isomorphism on the surface has exactly three outgoing $\mathbb{F}_p$-rational 2-isogenies.

Thus, the surface is a cycle of length $h(\mathcal{O}_K)$ connected one to three with the floor, which is also a cycle of length $3h(\mathcal{O}_K) = h(\mathbb{Z}[\pi])$ by Lemma 4.14 and Corollary 4.8.

This concludes the proof.

↰

5 Montgomery curves

Montgomery curves and their arithmetic were introduced in 1987 by Peter L. Montgomery in *Speeding the Pollard and elliptic curve methods of factorization*, see [Mon87]. It is an important paper, not only for its original improvements to Lenstra's ECM factorization methods, but for its wider use in cryptographic applications concerning scalar multiplication on elliptic curves.

Montgomery curves are specific instances of elliptic curves that can be defined by an equation of the form $By^2 = x^3 + Ax^2 + x$. The scalar multiplication on a Montgomery curve is optimized to an efficient x-only arithmetic. We only briefly address this important aspect of Montgomery curves in this chapter. Rather, we establish the definition of Montgomery curves and describe which elliptic curves are Montgomery with the help of a survey in tribute to Montgomery, *Montgomery curves and their arithmetic*, see [CS18]. Moreover, we prove Proposition 3.6, following the proof of [Cas+18, Proposition 8] with details added where necessary. Last but not least, we discuss the role of Montgomery curves in public key validation.

5.1 Montgomery curves

An elliptic curve over a finite field $\mathbb{F}_q$ where $q \geq 5$ is Montgomery if we can define it by an equation of the form

$$E_{A,B} \colon By^2 = x^3 + Ax^2 + x. \tag{3}$$

Notice that its projective equation with coordinates $(X \colon Y \colon Z)$ where $x = X/Z$ and $y = Y/Z$ has the same unique point $O = (0 \colon 1 \colon 0)$ where $Z = 0$ as elliptic curves in Weierstrass form. Moreover, we immediately notice that $B \neq 0$, otherwise the equation describes three lines in $\overline{\mathbb{F}}_q$ defined by the equation $0 = x(x^2 + Ax + 1)$. Similarly, $A \neq \pm 2$ because if $B < 0$ and $A = 2$ or $B > 0$ and $A = -2$, then the equation $By^2 = x(x \pm 1)^2$ has a node.

Since Montgomery curves are elliptic curves, there exists a group law $\oplus$ on its rational points $E_{A,B}(\mathbb{F}_q)$. One can find the equations that describe the group law in [CS18, Chapter 2.2]. We include them in this chapter for the sake of readability.

Analogously to the equations for the Weierstrass form, the point O acts as the zero element and the negation map $\ominus(x, y) = (x - y)$ on all points on the affine plane $Z \neq 0$ and $\ominus(O) = O$. If $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ are points in $E_{A,B}(\mathbb{F}_q)$, then $P \oplus Q = (x_\oplus, y_\oplus)$ where

$$\begin{aligned} x_\oplus &= B\lambda^2 - (x_P + x_Q) - A \\ y_\oplus &= \lambda(x_P - x_\oplus) - y_P \end{aligned}$$

and

$$\lambda = \begin{cases} (y_Q - y_P)/(x_Q - xP) & \text{if } P \neq Q \text{ or } P \neq \ominus Q, \\ (3x_P^2 + 2Ax_P + 1)/(2By_P) & \text{if } P = Q. \end{cases}$$

It is not yet the x-only arithmetic that spark cryptographic interest in Montgomery curves. This x-line arithmetic follows optimized equations in terms of the projective coordinates and can be found in [CS18, Chapter 3]. We address how we can use this x-only arithmetic in CSIDH to reduce the computation time in Chapter 5.5.

Every Montgomery curve is an elliptic curve, but not necessarily vice versa. We explore this relation in terms of the coefficients of the Weierstrass and Montgomery form in the next chapter.

5.2 Relation between Weierstrass and Montgomery form

We limit ourselves to the prime field $\mathbb{F}_p$. In this chapter we study which elliptic curves in Weierstrass form are Montgomery. One of the sufficient conditions is a specified j-invariant. To this end, let us compute the j-invariant of Equation 3.

In order to get Equation (3) into Weierstrass form, we apply the transformation $(x, y) \mapsto (u, v) = (x, 2\sqrt{B}y)$. This yields the Weierstrass form $v^2 = 4u^3 + 4Au^2 + 4u$. Using the equations on page of [Sil86], we compute that

$$j(E_{A,B}) = 256\frac{(A-3)^3}{A^2-4}. \tag{4}$$

Any elliptic curve with a j-invariant of this form is Montgomery. This does not give us a clear relation in terms of the Weierstrass coefficients of an elliptic curve, and so we first discuss properties of Montgomery curves that help us find such a relation.

Proposition 5.1 ([OKS00], Proposition 1)**.** *Let $p \geq 5$. A Weierstrass-form elliptic curve $E : v^2 = u^3 + au + b$ is transformable to the Montgomery-form if there exist α, β in $\mathbb{F}_p$ such that*

1. $\alpha^3 + a\alpha + b = 0$,
2. $3\alpha^2 + a = \beta^2$.

Proof, following the proof of Proposition 1 in [OKS00]. Let us try to determine for which short Weierstrass equations $v^2 = u^3 + au + b$ there exists a transformation $(u, v) \mapsto (x, y) = (s(u - \alpha'), t(v - \beta'))$ to Montgomery form. We observe that elliptic curves in Montgomery form must all contain the point $T = (0, 0)$. Therefore, any Montgomery curve defined by a short Weierstrass equation $v^2 = u^3 + au + b$ must have a $\mathbb{F}_p$-rational point $(\alpha, 0)$ of order two on it that is sent to T under the transformation. Thus, $\alpha' = \alpha$ and $\beta' = 0$, where $\alpha^3 + a\alpha + b = 0$.

The transformation $(u, v) \mapsto (x, y) = (s(u - \alpha), tv)$ to $By^2 = x^3 + Ax^2 + x$ implies

$$Bt^2v^2 = s^3(u-\alpha)^3 + As^2(u-\alpha)^2 + s(u-\alpha).$$

Substituting $v^2 = u^3 + au + b$ yields

$$Bt^2(u^3 + au + b) = s^3(u-\alpha)^3 + As^2(u-\alpha)^2 + s(u-\alpha),$$

and so comparing the coefficients of the u^3-term yields $Bt^2 = s^3$. Substituting the latter and dividing by s results in the equation

$$s^2(u^3 + au + b) = s^2(u-\alpha)^3 + As(u-\alpha)^2 + (u-\alpha).$$

Next, we compute the derivative with respect to u and consequently assign $u = \alpha$. Then

$$s^2(3\alpha^2 + a) = 1.$$

Therefore, in order for this transformation to exist, we need some $\beta = 1/s$ in $\mathbb{F}_p$ such that $3\alpha^2 + a = \beta^2$. ⏢

Let $B = 1/\beta$ and $t = 1/\beta$ such that $Bt^2 = s^3$. Then the transformation is defined by

$$(u, v) \mapsto (x, y) = ((u - \alpha)/\beta, v/\beta). \tag{5}$$

It maps the Weierstrass equation $v^2 = u^3 + au + b$ to the Montgomery equation $By^2 = x^3 + Ax^2 + x$ where $A = 3\alpha/\beta$ and $B = 1/\beta$. With this information, we can rewrite the transformation in Equation (5) in terms of A, B and compute its inverse. This results in the transformation[36] $(x, y) \mapsto (u, v) = ((x + A/3)/B, y/B)$. It maps the Montgomery equation $By^2 = x^3 + Ax^2 + x$ to a short Weierstrass equation

$$v^2 = u^3 + \frac{(3 - A^2)}{3B^2}u + \frac{A(2A^2 - 9)}{27B^3}.$$

Applying the inverse map defined by $(u, v) \mapsto (x, y) = (Bu - A/3, Bv)$ to elliptic curves satisfying Proposition 5.1 yields the Montgomery form $By^2 = x^3 + Ax^2 + x$.

[36] It differs to the transformation in [CS18] by a sixth power of B.

5.3 The group structure of $E_{A,B}(\mathbb{F}_p)$

We notice that Equation (3) admits at least one $\mathbb{F}_q$-rational point of order 2, i.e. $T = (0,0) \in E_{A,B}[2](\mathbb{F}_q)$. Thus, we can conclude $E_{A,B}[2] \subset E_{A,B}(\mathbb{F}_q)$ if and only if $A^2 - 4$ is a quadratic residue in $\mathbb{F}_p$. It turns out that we can say more about the structure of $E_{A,B}(\mathbb{F}_p)$ depending on the coefficients A, B.

To this end, we observe that the j-invariant, see Equation (4), does not depend on B. Taking a closer look explains this property. Indeed, an isogeny $\varphi_{B'} \colon E_{A,B} \to E_{A,B'}$ defined by taking $(x,y) \mapsto (x, \sqrt{B/B'}y)$ is defined over $\mathbb{F}_p$ exactly when B/B' is a quadratic residue in $\mathbb{F}_p$. We call $E_{A,B'}$ a quadratic twist of $E_{A,B}$. The map $\varphi_{B'}$ defines an isomorphism over $\mathbb{F}_{p^2}$ for any $B' \neq 0$. Note that all non-trivial quadratic twists of $E_{A,B}$ for fixed B are $\mathbb{F}_p$-isomorphic. Indeed, if both B/B' and B/B'' are non-quadratic residues belonging to the non-trivial quadratic twists $E_{A,B'}$ and $E_{A,B''}$ respectively, then B'/B'' must be a quadratic residue in $\mathbb{F}_p$.

Proposition 5.2. *Let $E_{A,B}$ be a Montgomery curve defined over the prime field $\mathbb{F}_p$ where $p \geq 5$. Then $4 \mid \#E_{A,B}(\mathbb{F}_p)$.*

Proof. Recall $A^2 - 4 \neq 0$ and $B \neq 0$ such that $E_{A,B}$ describes an elliptic curve.

Case 1: (both $A \pm 2$ are (non-)quadratic residues) In this case $A^2 - 4$ is a quadratic residue, so $x^2 + Ax + 1$ splits completely in $\mathbb{F}_p$. Therefore,

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong E_{A,B}[2] \subseteq E_{A,B}(\mathbb{F}_p).$$

Since $E_{A,B}(\mathbb{F}_p)$ has a subgroup of order 4, this implies the group order must be divisible by 4 and so we conclude.

Case 2: ($A + 2$ is quadratic residue, $A - 2$ is not) Since $T = (0,0)$ is the only $\mathbb{F}_p$-rational point of order 2, we aim to prove that there exists $P = (\alpha, \beta) \in E_{A,B}(\mathbb{F}_p)$ such that $2P = T$. Using the group law, this means the equations

$$\begin{aligned} \lambda &= \frac{3\alpha^2 + 2A\alpha + 1}{2B\beta} \\ 0 &= B\lambda^2 - 2\alpha - A \\ 0 &= \lambda\alpha - \beta \end{aligned}$$

must have $\mathbb{F}_p$-rational solutions for α, β. Since $\lambda^2 = (A + 2\alpha)/B$, this means there needs to exist $\alpha \in \mathbb{F}_p$ such that $(A + 2\alpha)/B$ is a quadratic residue, which also depends on B. If B is quadratic residue, we check that $\alpha = 1$ defines the $\mathbb{F}_p$-rational points

$$P_\pm = (1, \pm\sqrt{(A+2)/B}) \in E_{A,B}(\mathbb{F}_p)$$

of order 4. If B is a non-quadratic residue, we check that $\alpha = -1$ defines the $\mathbb{F}_p$-rational points $P_\pm = (-1, \mp\sqrt{(A-2)/B}) \in E_{A,B}(\mathbb{F}_p)$. Therefore, $E_{A,B}(\mathbb{F}_p)$ has a subgroup of order 4 such that its order must be divisible by 4.

Note that the non-trivial quadratic twist $E_{A,B'}$ contains both $P_\pm$ of order 4 in the cases where 'B a quadratic residue and $\alpha = -1$' and 'B a non-quadratic residue and $\alpha = 1$', because B' is a quadratic residue when B is not and vice versa.

Case 3: ($A - 2$ is a quadratic residue, $A + 2$ is not) Analogous to the previous case, except if B is a quadratic residue then $\alpha = -1$ defines the points of order 4, and if B is a non-quadratic residue then $\alpha = 1$ does. ∎

5.4 Supersingular Montgomery curves

Suppose $E_{A,B}$ is supersingular, so $\#E_{A,B}(\mathbb{F}_p) = p + 1$. By Proposition 5.2, this implies $p \equiv 3 \bmod 4$. As we have seen before, this means -1 is a non-quadratic residue in $\mathbb{F}_p^*$. Consequently, we observe from our

discussion of the quadratic twist of a Montgomery curve that we may take $B = 1$ and $B' = -1$ such that $E_{A,1}$ has non-trivial quadratic twist $E_{A,-1}$. They define distinct $\mathbb{F}_p$-isomorphism classes. Moreover, we know from Theorem 4.11 and Proposition 4.12 that they are the only two such classes that have the same j-invariant. We write $E_A := E_{A,1}$.

Moreover, we notice $E_{A,-1}\colon -y^2 = x^3 + Ax^2 + x$ is $\mathbb{F}_p$-isomorphic to the Montgomery curve $E_{-A}\colon y^2 = x^3 + Ax^2 + x$ via the isomorphism $(x, y) \mapsto (-x, y)$. Thus, every supersingular Montgomery curve is of the form[37] E_A and has non-trivial quadratic twist E_{-A}. Next, we take a closer look at the group structure depending on $A \pm 2$.

Case 1: (both $A \pm 2$ are (non-)quadratic residues) As we saw in the proof of Proposition 5.2, if both $A \pm 2$ are (non-)quadratic residues, then $E_A(\mathbb{F}_p)$ and $E_{-A}(\mathbb{F}_p)$ contain the full 2-torsion subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

If $A \pm 2$ are both square residues, this implies $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \subseteq E_A(\mathbb{F}_p)$. We list the elements in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \leftrightarrow$ (i.e. corresponding to) the points in $E_A(\mathbb{F}_p)$ of order at most 4.

$$
\begin{aligned}
&(0,0) \leftrightarrow O, && (0,2) \leftrightarrow T = (0,0),\\
&(1,0) \leftrightarrow S = \left((-A + \sqrt{A^2-4})/2, 0\right), && (1,2) \leftrightarrow R = \left((-A - \sqrt{A^2-4})/2, 0\right),\\
&(0,1) \leftrightarrow P = (1, \sqrt{A+2}), && (1,1) \leftrightarrow Q = (-1, \sqrt{A-2}),\\
&(0,3) \leftrightarrow 3P = (1, -\sqrt{A+2}), && (1,3) \leftrightarrow 3Q = (-1, -\sqrt{A-2}).
\end{aligned}
$$

If $A \pm 2$ are both non-quadratic residues, then $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \subseteq E_{-A}(\mathbb{F}_p)$ instead since $-1(A \pm 2) = -A \mp 2$ must be square residues.

Case 2: ($A + 2$ is a quadratic residue, $A - 2$ is not) First of all, $A^2 - 4 = (-A)^2 - 4$ is non-quadratic and so both $E_A(\mathbb{F}_p)$ and $E_{-A}(\mathbb{F}_p)$ contain at most one point of order 2, namely $T = (0, 0)$. However, $\mathbb{Z}/4\mathbb{Z} \subseteq E_A(\mathbb{F}_p)$ since the points $P = (1, \sqrt{A+2})$ and $3P = (1, -\sqrt{A+2})$ are of order 4 in $E_A(\mathbb{F}_p)$. Since $-1(A-2) = -A+2$ is square, also $\mathbb{Z}/4\mathbb{Z} \subseteq E_{-A}(\mathbb{F}_p)$ because $P' = (1, \sqrt{-A+2})$ and $3P' = (1, -\sqrt{-A+2})$ are of order 4 in $E_{-A}(\mathbb{F}_p)$.

Case 3: ($A - 2$ is a quadratic residue, $A + 2$ is not) Analogously to the previous case both $E_A(\mathbb{F}_p)$ and $E_{-A}(\mathbb{F}_p)$ contain at most point of order 2. However, $E_A(\mathbb{F}_p)$ contains the points $Q = (-1, \sqrt{A-2})$ and $3Q = (-1, -\sqrt{A-2})$ of order 4. Note $E_{-A}(\mathbb{F}_p)$ must then contain the points $Q' = (-1, \sqrt{-A-2})$ and $3Q' = (-1, -\sqrt{-A-2})$ of order 4.

The results are summarized in [CS18, Table 1]. From them, we are able to determine which case(s) we work with depending on $p \bmod 8$. Indeed, if $p \equiv 3 \bmod 8$, then neither $\#E_A(\mathbb{F}_p)$ nor $\#E_{-A}(\mathbb{F}_p)$ can contain $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Thus, $A^2 - 4$ cannot be a quadratic residue and at most one $\mathbb{F}_p$-rational point T of order 2 exists in both Mordell-Weil groups. Therefore, we find by Theorem 3.5 or Lemma 4.15 that if $p \equiv 3 \bmod 8$ and E_A a Montgomery curve, then $\mathrm{End}_p(E_A) = \mathbb{Z}[\pi]$. This proves one direction in the result of Proposition 3.6, because $\mathbb{F}_p$-isomorphic curves have the same $\mathbb{F}_p$-rational endomorphism ring.

The proof of Proposition 3.6 can also be found in [Cas+18, Chapter 5] in less detail. We explore the latter in the proof underneath.

Proof of Proposition 3.6. We already proved that an elliptic curve E that is $\mathbb{F}_p$-isomorphic to a Montgomery curve $E_A\colon y^2 = x^3 + Ax^2 + x$ must have $\mathrm{End}_p(E) = \mathbb{Z}[\pi]$. Therefore, suppose $\mathrm{End}_p(E) = \mathbb{Z}[\pi]$ where E is a supersingular elliptic curve defined over $\mathbb{F}_p$.

We know from [Cas+18, Theorem 7], that the class group $\mathrm{Cl}(\mathbb{Z}[\pi])$ acts freely and transitively on the set $\mathrm{Ell}_{\mathbb{F}_p}(\mathbb{Z}[\pi])$. This set is non-empty because it contains $E_0\colon y^2 = x^3 + x$ if $p \equiv 3 \bmod 8$. Indeed, we notice that the only point of order 2 on E_0 is $T = (0, 0)$, because $x^2 + 1 = 0$ is irreducible in $\mathbb{F}_p[x]$. Therefore, there exists $\overline{\mathfrak{a}} \in \mathrm{Cl}(\mathbb{Z}[\pi])$ such that $\overline{\mathfrak{a}} \star E_0 = E$.

Since we take $L = \{\ell_1, \ldots, \ell_n\}$ large enough such that $G_{\mathbb{F}_p,L}$ is connected and $\ell_i < p$ because $p = 4\prod_{i=1}^{n} \ell_i - 1$, there exists an ideal class $\overline{\mathfrak{a}}$, with the desired properties, containing an integral representative

[37] Ironically, we work with Weierstrass form again, albeit not short Weierstrass form.

of norm coprime to p. Therefore, the action of $\overline{\mathfrak{a}}$ defines a separable $\mathbb{F}_p$-rational isogeny $\varphi_{\mathfrak{a}}\colon E_0 \to E$. Moreover, it must have odd degree if $p \equiv 3 \bmod 8$, because both E_0 and E have $\mathbb{F}_p$-rational endomorphism ring $\mathbb{Z}[\pi]$. Thus, we find from Theorem 3.5 $G_{\mathbb{F}_p,L}$ does not contain horizontal isogenies with even degree.

As a result, the kernel $\ker(\varphi_{\mathfrak{a}})$ does not contain $T = (0, 0,)$, the 2-torsion point in $E_0(\mathbb{F}_p)$. By [Ren18, Proposition 1], there exists $A \in \mathbb{F}_p$ such that $\ker(\varphi_{\mathfrak{a}})$ gives rise to an isogeny $\psi\colon E_0 \to E_A$. We know from [Sil86, Exercise III.3.13(e)] that $\mathbb{F}_p$-rational isogenies with a given kernel are unique up to post-composition with $\mathbb{F}_p$-isomorphisms. Therefore, E is $\mathbb{F}_p$-isomorphic to E_A.

Next, we aim to prove that if $\mathrm{End}_p(E) = \mathbb{Z}[\pi]$ such that $E \cong_{\mathbb{F}_p} E_A$, then A is unique. To this end, consider any $B \in \mathbb{F}_p$ such that $E_A \cong_{\mathbb{F}_p} E_B$. Note that both E_A, E_B are in Weierstrass form. We know from [Sil86, Proposition III.3.1(b)] that there exists a linear change of variables

$$x = u^2X + r, \quad y = u^3Y + su^2X + t \tag{6}$$

where $u \in \mathbb{F}_p^*$, $s, t, r \in \mathbb{F}_p$ and the Montgomery curves

$$E_A\colon y^2 = x^3 + Ax^2 + x, \quad E_B\colon Y^2 = X^3 + BX^2 + X.$$

Let $f(x, y) = x^3 + Ax^2 + x - y^2 = 0$ and $F(X, Y) = X^3 + BX^2 + X - Y^2 = 0$. We know from the proof of [Sil86, Proposition III.3.1(a)] that x, X have a pole of order 2 and y, Y have a pole of order 3 at $O = (0\colon 1\colon 0)$. The elliptic curve equations $f(x, y) = 0$ and $F(X, Y) = 0$ are the linear relations of the spanning sets $\{1, x, y, x^2, xy, y^2, x^3\}$ and $\{1, X, Y, X^2, XY, Y^2, X^3\}$ respectively, that keep them from being bases of the vector space $\mathcal{L}(6O)$ over $\mathbb{F}_p$, which is of dimension $\ell(6O) = 6$.

We are able to exclusively use the functions $\{1, X, Y, X^2, XY, Y^2, X^3\}$ due to the linear transformations in Equation (6). We obtain another redundancy by computing $f(u^2X+r, u^3Y+su^2+su^2X+t)-u^6F(X, Y) = 0$ in the function field $\mathbb{F}_p(E_B)$. This yields the linear relation,

$$\begin{aligned}(u^2X + r)^3 + A(u^2X + r)^2 + u^2X + r - (u^3Y + su^2X + t)^2 \\ -u^6X^3 - u^6BX^2 - u^6X + u^6Y^2 = 0 \\ \Rightarrow (2su^5)XY + (3ru^4 - u^6B + u^4A - s^2u^4)X^2 + (2tu^3)Y \\ +(3r^2u^2 + u^2 - u^6 + 2Aru^2 - 2stu^2)X + (r^3 + Ar^2 + r - t^2)1 = 0,\end{aligned}$$

rewritten in terms of the functions $\{1, X, Y, X^2, XY\}$ over $\mathbb{F}_p$. We know that they span $\mathcal{L}(5O)$ over $\mathbb{F}_p$, see the definition in [Sil86, Page 34]. We claim that they are a basis for $\mathcal{L}(5O)$.

To this end, we know E_B has genus $g = 1$ because it is an elliptic curve. By [Sil86, Corollary II.5.5(b)] this implies $\deg(K_{E_B}) = 0$. Thus, $\deg(K_{E_B} - 5O) < 0$ and so $\ell(K_{E_B} - 5O) = 0$ by [Sil86, Proposition II.5.2(a)]. Therefore, $\ell(5O) = \deg(5O) - 1 + 1 = 5$ by Riemann-Roch, see [Sil86, Theorem II.5.4]. Therefore, $\mathcal{L}(5O)$ must be of dimension 5. This proves the claim, and so the coefficient of each function must be zero in $\mathbb{F}_p$. This yields the equations

$$\begin{aligned}XY\colon &\quad 0 = 2su^5 \\ X^2\colon &\quad 0 = (3r + A - s^2 - Bu^2)u^4 \\ Y\colon &\quad 0 = 2tu^3 \\ X\colon &\quad 0 = (3r^2 + 1 - u^4 + 2Ar - 2st)u^2 \\ 1\colon &\quad 0 = r^3 + Ar^2 + r - t^2.\end{aligned}$$

We find from the coefficients of XY and Y that $s = t = 0$ since $u \in \mathbb{F}_p^*$. This simplifies the constant term to $r^3 + Ar^2 + r = 0$, a familiar expression. Since $\mathrm{End}_p(E_A) = \mathbb{Z}[\pi]$, we know from Lemma 4.15 that E_A has only one $\mathbb{F}_p$-rational root of order 2, namely $T = (0, 0)$. Therefore, $r = 0$ is the only solution. Then from the coefficient of X we have $u^4 = 1$. By assumption $p \equiv 3 \bmod 8$ and so $u = \pm 1$ are the only solutions. Therefore, $u^2 = 1$. Substitution in the coefficient of X^2 yields $A = B$. ⌂

5.5 Key validation and x-only arithmetic

Let us first briefly address the x-only arithmetic Montgomery curves are famous for. As is described in [Cas+18, Page 26] and [CS18], we can simplify the group action computation using Vélu's equations if we

work with Montgomery curves by ignoring the y-coordinate of points in a cyclic subgroup $\langle P \rangle$ or order ℓ, where $P = (x, y)$ such that $x \in \mathbb{F}_p$ with $\ell \neq p$ an odd prime. This reduces the computation time by about half according to [Cas+18]]. However, in order to determine which kernel, $\ker([\mathfrak{l}])$ or $\ker([\mathfrak{l}'])$, an ℓ-torsion point P generates, we need some information about the y-coordinate. This requires an extra step in computing the class-group action; checking whether $x^3 + Ax^2 + x$ is a quadratic residue in $\mathbb{F}_p$. If it is, then $y \in \mathbb{F}_p$ and so $\langle P \rangle = \ker([\mathfrak{l}])$ where $\mathfrak{l} = (\ell, \pi - 1)$. Since ℓ is odd, $y \neq 0$ and so if $x^3 + Ax^2 + x$ is a non-quadratic residue in $\mathbb{F}_p$, then $y \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ meaning $\langle P \rangle = \ker([\mathfrak{l}'])$ where $\mathfrak{l}' = (\ell, \pi + 1)$.

Next, we address the *key validation* in the CSIDH protocol. However, rather than working with a naïve Diffie-Hellman protocol, we extend it to an Elgamal encryption scheme such that the latter includes the encryption and decryption of the plain- and ciphertext respectively, see [PPG24, Chapter 8.5]. It reduces the number of total messages by one[38] and it reveals the need for key validation.

Key validation is an extra step in Elgamal based on CSIDH that Alice takes before computing the shared secret key (or masking key) in order to make sure that the published public key B is of the right format. In the context of CSIDH, the expected format is a Montgomery coefficient B that defines a supersingular elliptic curve E_B with $\mathrm{End}_p(E_B) = \mathbb{Z}[\pi]$, conform Proposition 3.6. Upon taking note of B, Alice counts the number of points in $E_B(\mathbb{F}_p)$, where $p \equiv 3 \bmod 8$, as is done in [Cas+18, Algorithm 1]. If this amount is $p + 1$, then B defines a supersingular elliptic curve and so the public key B is of the right format. This extra step serves a specific purpose.

We assume under Kerckhoff's principle, see [PPG24, Definition 1.3.1], that adversaries know all the details about a cryptosystem such as the encryption and decryption algorithms, except for the secret key(s). Thus, key validation does not protect an Elgamal based on CSIDH protocol from a man-in-the-middle attack, in which e.g. an adversary Eve poses as Bob to obtain the plaintext. Rather, it is a safety measure for a *chosen cipher attack* (CCA), where adversaries posing as Bob choose a public key in the wrong format such that it reveals the private key chosen by Alice if she computes the shared secret key with it.

This concludes the many purposes Montgomery curves serve in the CSIDH protocol.

[38] Relative to a naïve Diffie-Hellman and encryption+decryption approach.

6 Future research

The CSIDH protocol, although mathematically interesting, cannot compete with lattice-based PQCDH in terms of running time. Indeed, a study from 2024 into optimizations and practical use [Cam+24] concludes that with a running time of tens of seconds, CSIDH is only practical in cases that require very small key-sizes. Choosing a 512-bit prime p the public keys have size 64 bytes and private keys can be stored in 32 bytes, see [Cas+18, Chapter 8.1]. However, only in this year, a hybrid post-quantum key exchange (HPQKE) paper was published proposing a protocol in which CSIDH and ECDH are combined, see [QC25].

One of the author's recommendations for future research is the choice of Elkies primes ℓ_i in constructing

$$p = 4\prod_{i=1}^{n} \ell_i - 1.$$

On the one hand, small ℓ_i reduce the computation time spent on elliptic curve scalar multiplication. On the other hand, for a supersingular E with $\mathrm{End}_p(E) = \mathbb{Z}[\pi]$, we know from Appendix D that $E(\mathbb{F}_p)$ is cyclic and so choosing a random point $P \in E(\mathbb{F}_p)$ such that $(p + 1/\ell_i)P$ has order ℓ has a chance of succeeding equal to $1 - 1/\ell_i$. Thus, in constructing a prime p the choice for the first $n - 1$ odd primes $\ell_1 = 3, \ell_2 = 5, \ldots$ is not necessarily straightforward. This requires programming since it is heavily focused on implementation.

We conclude that the CSIDH protocol is a grateful subject for future work.

A Magma code

A.1 Complex multiplication over a number field

```
Q:=RationalField();
P<x>:=PolynomialRing(Q);
K:=NumberField(2*x^2-2*x+3);
R:=RingOfIntegers(K);
D:=Discriminant(R);
H<x>:=HilbertClassPolynomial(D);
L<a>,Roots:=SplittingField(H);
Roots;
E1:=MinimalModel(EllipticCurveWithjInvariant(Roots[1]));
E2:=MinimalModel(EllipticCurveWithjInvariant(Roots[2]));
```

A.2 Finding Elkies primes

```
ElkiesPrimes:=[];
for i:=1 to 50 do
    p:=NthPrime(i);
    R<x>:=PolynomialRing(GF(p));
    f:=x^2+6*x+83;
    //If both the multiplicity and degree of the first factor is 1, we know f splits
    completely modulo p
    if Factorization(f)[1][2] ne 2 and Degree(Factorization(f)[1][1]) ne 2 then
        ElkiesPrimes:=Append(ElkiesPrimes,p);
    end if;
end for;
ElkiesPrimes;
```

A.3 Modular polynomial group action

```
l:=3;
R<x,y>:=PolynomialRing(GF(83),2);
//We define the elliptic curve E:y^2=x^3+x+1 over the finite field F_83
E0:=EllipticCurve([GF(83)!1,GF(83)!1]);
//The j-invariant of E denotes the vertex in the graph from which we start
j0:=jInvariant(E0);
A:=R!ClassicalModularPolynomial(l);
//Factorizing B=Phi_3(X,j_0) modulo 83 yields two linear factors and their zeroes are
    the j-invariants of the neighboring curves
B:=Evaluate(A,[x,j0]);
C:=Evaluate(A,[x,GF(83)!(-63)]);
D:=Evaluate(A,[x,GF(83)!(-53)]);
E:=Evaluate(A,[x,GF(83)!(-40)]);
j0; Factorization(B); Factorization(C); Factorization(D); Factorization(E);
```

A.4 Class group of $\mathbb{Z}[\sqrt{-419}]$

```
Q:=RationalField();
P<x>:=PolynomialRing(Q);
//Define the order Z[pi]
R:=EquationOrder(x^2+419);
//m is a map from the ring class group to a representative small normed ideal
G,m:=RingClassGroup(R);
G;
//G is cyclic with generator G.1, and m(G.1)=(pi+1,3pi)=(3,pi+1)
m(G.1);
//The basis R.1=1 and R.2=pi
Basis(R);
I:=ideal<R|3,R.2-1>;
```

```
Inverse(m)(I);
J:=ideal<R|5,R.2-1>;
Inverse(m)(J);
M:=ideal<R|7,R.2-1>;
Inverse(m)(M);
```

A.5 Class group of $\mathbb{Z}[(1+\sqrt{-419})/2]$

```
Q:=RationalField();
P<x>:=PolynomialRing(Q);
S:=MaximalOrder(x^2+419);
G,m:=ClassGroup(S:Proof:="Full");
G;
m(G.1);
Basis(S);
I:=ideal<S|5,2*S.2+3>;
Inverse(m)(I);
J:=ideal<S|7,2*S.2+5>;
Inverse(m)(J);
```

A.6 Splitting behavior Elkies case

```
F:=GF(11);
L<a>:=GF(11,2);
P<x>:=PolynomialRing(F);
f:=MinimalPolynomial(a,F);
f;
Roots(f,L);
E:=EllipticCurve([L|1,0]);
G,m:=pPowerTorsion(E,3);
G;
P:=m(G.1);
Q:=m(G.2);
P;
Q;
2*P;
2*Q;
2*P+2*Q;
P+2*Q;
2*P+Q;
FrobeniusMap(E,1)(P);
```

A.7 Splitting behavior Atkin case

```
F:=GF(7);
//F_{7^4} is the smallest finite field for which the full 3-torsion group is contained
    in E(F_{7^4})
L<a>:=GF(7,4);
P<x>:=PolynomialRing(F);
f:=MinimalPolynomial(a,F);
f;
Roots(f,L);
E:=EllipticCurve([L|1,0]);
//Compute the abstract group G of 3-torsion points that are defined over L, where m is a
     map from G to the group of L-rational points on E
G,m:=pPowerTorsion(E,3);
G;
P:=m(G.1);
Q:=m(G.2);
P;
Q;
2*P;
2*Q;
```

```
2*P+2*Q;
P+2*Q;
2*P+Q;
//Using the Frobenius map of L on the set of 3-torsion points, we determine the
    subspaces of the corresponding matrix
FrobeniusMap(E,1)(P);
```

B Sage code

B.1 Isogeny steps

The following code needs (at least) `Sage 10.3`.

```
def phi(E,l):
    p=E.base_field().characteristic()
    assert E.order() == p+1 and mod(p,4) == 3
    D=divisors((p+1)/4)
    assert l in D
    P=((p+1)//l)*E.gens()[0]
    assert P.order() == l
    Ephi=E.isogeny(P).codomain().montgomery_model()
    return Ephi

p=419

#Compute the 3-isogeny steps
E=EllipticCurve(GF(p),[0,418,0,102,275]).montgomery_model()
print(E,'\n','with j-invariant',E.j_invariant(),'and Montgomery coefficient',E.a2())
for i in range(27):
    E=phi(E,3)
    print(E,'\n','with j-invariant', E.j_invariant(),'and Montgomery coefficient',E.a2()
    )
print()

#Compute the 5-isogeny steps
E=EllipticCurve(GF(p),[0,418,0,102,275]).montgomery_model()
print(E,'\n','with j-invariant',E.j_invariant(),'and Montgomery coefficient',E.a2())
for i in range(9):
    E=phi(E,5)
    print(E,'\n','with j-invariant', E.j_invariant(),'and Montgomery coefficient',E.a2()
    )
print()

#Compute the 7-isogeny steps
E=EllipticCurve(GF(p),[0,418,0,102,275]).montgomery_model()
print(E,'\n','with j-invariant',\
E.j_invariant(),'and Montgomery coefficient',E.a2())
for i in range(27):
    E=phi(E,7)
    print(E,'\n','with j-invariant', E.j_invariant(),'and Montgomery coefficient',E.a2()
    )
print()
```

C Bachmann-Landau notation

In order to objectively measure the amount of time[39] $f(n)$ an algorithm takes to compute on a given input n, Bachmann-Landau notation was designed. It is used to study the asymptotic efficiency of algorithms, i.e. how fast $f(n)$ grows with n in the limit[40]. The information in this appendix is mainly taken from Chapter I.3 in [Cor+22]. We start by giving an example in pseudo-code.

[39] Note that $f(n)$ actually denotes the number of bit operations depending on the input n, because external factors determine the amount of time each such operation takes.

[40] Meaning, as $n \to \infty$.

```
SumOfSquares(n)
1 s=0               //c_1
2 i=1               //c_2a
3 while(i \leq n)   //c_2b
4   j=i*i           //c_3
5   s=s+j           //c_4
6   i=i+1           //c_2c
7 return s          //c_5
```

We label each operation in order to do the following computation:

$$\begin{aligned} f(n) &= c_1 + c_{2a} + c_5 + (n+1)c_{2b} + n(c_3 + c_4 + c_{2c}) \\ &= (c_{2b} + c_{2c} + c_3 + c_4)n + c_1 + c_{2a} + c_{2b} + c_5 \\ &= An + B, \end{aligned}$$

i.e. $f(n)$ grows linearly with the input n. Therefore, there exists a linear function $g(n)$ and an input n_0 such that for any n greater than n_0 there is an non-strict upper bound $cg(n)$ for $f(n)$, where c is some fixed constant. More formally,

$$\limsup_{n\to\infty} \frac{f(n)}{n} < \infty.$$

We denote this by $f(n) = O(n)$.

Definition C.1.

$$O(g(n)) = \{f(n) \colon \exists c > 0 \text{ and } \exists n_0 \text{ such that } \forall n > n_0 \text{ we have } |f(n)| \leq c \cdot g(n)\},$$

see graph (a) in Figure 5.

By convention, all constants and lower order terms of $g(n)$ are ignored when we write $O(g(n))$ (read 'big O'). For example if $g(n) = 2n^2 + 3n$, then $O(2n^2 + 3n) = O(n^2)$. Also, if $f(n)$ is constant then $f(n) = O(1)$. It is particularly useful as a worst-case scenario estimate for the running time of protocols and their respective attacks in order to guarantee security.

In some papers $\tilde{O}$ is meant to denote O-notation in which certain logarithmic factors are ignored [Cor+22, Page 63].

Definition C.2.

$$\tilde{O}(g(n)) = \left\{f(n) \colon \exists\ c, k, n_0 > 0 \text{ such that } 0 \leq f(n) \leq cg(n)\log^k(n) \text{ for all } n \geq n_0\right\}.$$

In other cases, one might rather want to know the shortest running time of a piece of code.

Definition C.3.

$$\Omega(g(n)) = \{f(n) \colon \exists c > 0 \text{ and } \exists n_0 \text{ such that } \forall n > n_0 \text{ we have } |f(n)| \geq c \cdot g(n)\},$$

see graph (b) in Figure 5.

Last but not least, if $f(n)$ is in both $O(g(n))$ and $\Omega(g(n))$, we say that it is also in $\Theta(g(n))$.

Definition C.4.

$$\Theta(g(n)) = \{f(n) \colon \exists c_1 > 0,\ \exists c_2 > 0 \text{ and } \exists n_0 \text{ such that } \forall n > n_0 \text{ we have } c_1 g(n) \leq f(n) \leq c_2 g(n)\},$$

see graph (c) in Figure 5.

Note that all these notations yield non-strict (asymptotic) bounds on the elements in their respective sets. The next definitions give similar sets of functions, however the bounds that the relations impose are strict this time. In other words: $g(n)$ grows faster than the functions $f(n)$ in the set after a certain n_0.

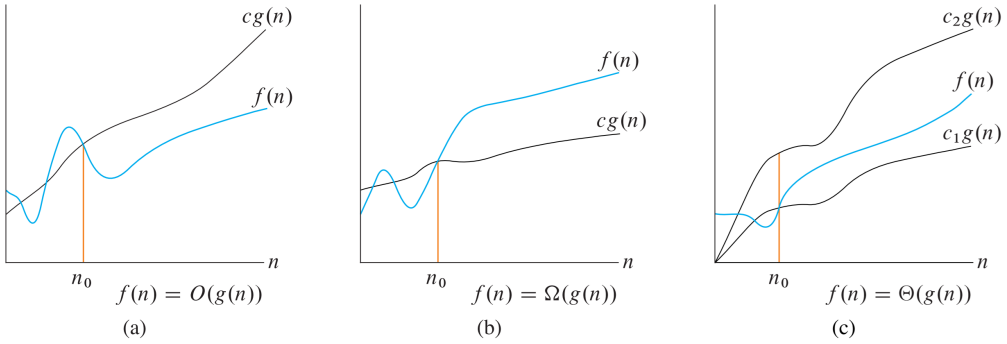


Figure 5: Where n_0 denotes the minimal possible input value. Taken from [Cor+22, Chapter I.3].

Definition C.5.

$$o(g(n)) = \{f(n) \colon \forall c > 0,\ \exists n_0 \text{ such that } 0 \leq f(n) < c \cdot g(n) \forall n \geq n_0\}$$

yields a strict upper bound on the $f(n)$.

On the other hand, there exists the set of functions respecting a strict (asymptotic) lower bound of $g(n)$.

Definition C.6.

$$\omega(g(n)) = \{f(n) \colon \forall c > 0,\ \exists n_0 \text{ such that } 0 \leq c \cdot g(n) < f(n) \forall n \geq n_0\}.$$

In general, we know that logarithmic $<$ polynomial $<$ exponential. In the context of the thesis, we are most interested in so called 'L-notation'. The next definitions are taken from a section written by Arjen K. Lenstra in the Encyclopedia [TJ14, Pages 709 and 710].

Definition C.7. For $t, \gamma \in \mathbb{R}$ with $0 \leq t \leq 1$, we use $L_x[t, \gamma]$ to describe any function of x equal to

$$e^{(\gamma + o(1))(\log(x))^t (\log(\log(x)))^{1-t}} \text{ for } x \to \infty$$

with natural logarithms and $o(1)$ denoting any function of x that goes to 0 as $x \to \infty$.

The L-notation function has the following properties:

1. $L_x[t, \gamma] + L_x[t, \delta] = L_x[t, \max(\gamma, \delta)]$,
2. $L_x[t, \gamma] \cdot L_x[t, \delta] = L_x[t, \gamma + \delta]$,
3. $L_x[t, \gamma] \cdot L_x[s, \delta] = L_x[t, \gamma]$ if $t > s$,
4. For any fixed k:
   (a) $L_x[t, \gamma]^k = L_x[t, k\gamma]$,
   (b) $\gamma > 0$ then $(\log x)^k L_x[t, \gamma] = L_x[t, \gamma]$,
5. $\pi\left(L_x[t, \gamma]\right) = L_x[t, \gamma]$ where $\pi(y)$ is the number of primes $\leq y$.

If $L_x[t, \gamma]$ is used to indicate running times for fixed γ, we notice that if $t = 0$ it describes a polynomial time function in $\log(x)$, if $0 < t < 1$ it describes a sub-exponential time function in $\log(x)$ and if $t = 1$ it describes an exponential time function in $\log(x)$.

D Extra results

There exists an important relationship between the $\mathbb{F}_p$-rational endomorphism ring $\mathrm{End}_p(E)$ and the group structures $E(\mathbb{F}_p)$ and $E(\mathbb{F}_{p^2})$ of a supersingular elliptic curve E. Suppose $\mathrm{End}_p(E) = \mathcal{O}$ is an order containing $\mathbb{Z}[\pi]$. Hendrik W. Lenstra Jr. has shown that the group structure of $E(\mathbb{F}_p)$ is isomorphic to $\mathcal{O}/(\pi - 1)$, see [Len96, Theorem 1(a)]. Using this fact, we are able to prove the following result.

Proposition D.1. *If $E/\mathbb{F}_p$ is a supersingular elliptic curve such that $\mathrm{End}_{\mathbb{F}_p}(E) = \mathbb{Z}[\pi]$, then*

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

Proof. Using [Len96, Theorem 1(a)], let us first consider $E(\mathbb{F}_p) \cong \mathbb{Z}[\pi]/(\pi - 1)$. Since E is supersingular, $\pi = \sqrt{-p}$ and so

$$\begin{aligned}
\mathbb{Z}[\pi]/(\pi - 1) &\cong (\mathbb{Z}[X]/(X^2 + p))/((X - 1, X^2 + p)/(X^2 + p)) \\
&\cong (\mathbb{Z}[X]/(X^2 + p))/((X - 1, p + 1)/(X^2 + p)) \\
&\cong \mathbb{Z}/(p+1)\mathbb{Z}[X]/(X - 1) \\
&\cong \mathbb{Z}/(p+1)\mathbb{Z}.
\end{aligned}$$

Similarly,

$$\begin{aligned}
\mathbb{Z}[\pi]/(\pi^2 - 1) &\cong (\mathbb{Z}[X]/(X^2 + p))/((X^2 - 1, X^2 + p)/(X^2 + p)) \\
&\cong (\mathbb{Z}[X]/(X^2 + p))/((X^2 - 1, p + 1)/(X^2 + p)) \\
&\cong \mathbb{Z}/(p+1)\mathbb{Z}[X]/(X^2 - 1) \\
&\cong \mathbb{Z}/(p+1)\mathbb{Z}[X]/(X + 1) \times \mathbb{Z}/(p+1)\mathbb{Z}[X]/(X - 1) \\
&\cong \mathbb{Z}/(p+1)\mathbb{Z} \times \mathbb{Z}/(p+1)\mathbb{Z}.
\end{aligned}$$

Let ℓ be a prime dividing $p + 1$. Note that this implies that there exists exactly $\ell + 1$ cyclic subgroups of order ℓ in $E(\mathbb{F}_{p^2})$ if E is supersingular and $\mathrm{End}_{\mathbb{F}_p}(E) = \mathbb{Z}[\pi]$. Indeed, the generators of these subgroups correspond directly with points in $\mathbb{P}^1(\mathbb{F}_\ell)$, via the map

$$\begin{aligned}
\{\text{elements of order } \ell \text{ in } \mathbb{Z}/(p+1)\mathbb{Z} \times \mathbb{Z}/(p+1)\mathbb{Z}\} &\to \mathbb{P}^1(\mathbb{F}_\ell) \\
(a, b) &\mapsto \frac{\ell}{p+1}(a, b).
\end{aligned}$$

These subgroups give rise to cyclic ℓ-isogenies defined over $\mathbb{F}_{p^2}$. Whether they also are defined over the prime field $\mathbb{F}_p$ depends on the splitting behavior of the Frobenius modulo ℓ, as we have seen in the preliminaries.

References

[Arp+21] Sarah Arpin et al. "Adventures in Supersingularland". In: *Experimental Mathematics* 32.2 (Oct. 2021), pp. 241–268. ISSN: 1944-950X. DOI: 10.1080/10586458.2021.1926009. URL: http://dx.doi.org/10.1080/10586458.2021.1926009.

[BS07] Reinier Bröker and Peter Stevenhagen. "Constructing elliptic curves of prime order". PhD thesis. Universiteit Leiden, 2007.

[Cam+24] Fabio Campos et al. "Optimizations and Practicality of High-Security CSIDH". In: *IACR Communications in Cryptology* 1.1 (Apr. 9, 2024). ISSN: 3006-5496. DOI: 10.62056/anjbksdja.

[Cas+18] Wouter Castryck et al. "CSIDH: An Efficient Post-Quantum Commutative Group Action". In: *Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2-6, 2018, Proceedings, Part III*. Ed. by Thomas Peyrin and Steven D. Galbraith. Vol. 11274. Lecture Notes in Computer Science. Springer, 2018, pp. 395–427. DOI: 10.1007/978-3-030-03332-3_15. URL: https://doi.org/10.1007/978-3-030-03332-3%5C_15.

[CD23] Wouter Castryck and Thomas Decru. "An Efficient Key Recovery Attack on SIDH". 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 V*. Ed. by Carmit Hazay and Martijn Stam. Vol. 14008. Lecture Notes in Computer Science. Springer, 2023, pp. 423–447. DOI: 10.1007/978-3-031-30589-4_15. URL: https://doi.org/10.1007/978-3-031-30589-4%5C_15.

[CJS14] Andrew M. Childs, David Jao, and Vladimir Soukharev. "Constructing elliptic curve isogenies in quantum subexponential time". In: *J. Math. Cryptol.* 8.1 (2014), pp. 1–29. DOI: 10.1515/JMC-2012-0016. URL: https://doi.org/10.1515/jmc-2012-0016.

[Cor+22] Thomas H. Cormen et al. *Introduction to algorithms*. MIT press, 2022.

[Cou06] Jean Marc Couveignes. "Hard Homogeneous Spaces". In: *IACR Cryptol. ePrint Arch.* (2006), p. 291. URL: http://eprint.iacr.org/2006/291.

[Cox22] David A. Cox. *Primes of the Form x2+ ny2: Fermat, Class Field Theory, and Complex Multiplication. with Solutions*. Vol. 387. American Mathematical Soc., 2022.

[CS18] Craig Costello and Benjamin Smith. "Montgomery curves and their arithmetic - The case of large characteristic fields". In: *J. Cryptogr. Eng.* 8.3 (2018), pp. 227–240. DOI: 10.1007/S13389-017-0157-6. URL: https://doi.org/10.1007/s13389-017-0157-6.

[DG16] Christina Delfs and Steven D. Galbraith. "Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$". In: *Des. Codes Cryptogr.* 78.2 (2016), pp. 425–440. DOI: 10.1007/S10623-014-0010-1. URL: https://doi.org/10.1007/s10623-014-0010-1.

[DH22] Whitfield Diffie and Martin E. Hellman. "New Directions in Cryptography". In: *Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman*. Ed. by Rebecca Slayton. Vol. 42. ACM Books. ACM, 2022, pp. 365–390. DOI: 10.1145/3549993.3550007. URL: https://doi.org/10.1145/3549993.3550007.

[Feo17] Luca De Feo. "Mathematics of Isogeny Based Cryptography". In: *CoRR* abs/1711.04062 (2017). arXiv: 1711.04062. URL: http://arxiv.org/abs/1711.04062.

[FKS18] Luca De Feo, Jean Kieffer, and Benjamin Smith. "Towards Practical Key Exchange from Ordinary Isogeny Graphs". In: *Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2-6, 2018, Proceedings, Part III*. Ed. by Thomas Peyrin and Steven D. Galbraith. Vol. 11274. Lecture Notes in Computer Science. Springer, 2018, pp. 365–394. DOI: 10.1007/978-3-030-03332-3_14. URL: https://doi.org/10.1007/978-3-030-03332-3%5C_14.

[FM02] Mireille Fouquet and François Morain. "Isogeny Volcanoes and the SEA Algorithm". In: *Algorithmic Number Theory, 5th International Symposium, ANTS-V, Sydney, Australia, July 7-12, 2002, Proceedings*. Ed. by Claus Fieker and David R. Kohel. Vol. 2369. Lecture Notes in Computer Science. Springer, 2002, pp. 276–291. DOI: 10.1007/3-540-45455-1_23. URL: https://doi.org/10.1007/3-540-45455-1%5C_23.

[Jou09] Antoine Joux. *Algorithmic cryptanalysis*. Chapman and Hall/CRC, 2009.

[Kob87] Neal Koblitz. “Elliptic curve cryptosystems”. In: *Mathematics of computation* 48.177 (1987), pp. 203–209.

[Koh96] David Russell Kohel. *Endomorphism rings of elliptic curves over finite fields*. University of California, Berkeley, 1996. URL: https://www.i2m.univ-amu.fr/perso/david.kohel/pub/thesis.pdf.

[Lan87] Serge Lang. *Elliptic Functions*. Springer-Verlag, 1987.

[Len96] H.W. Lenstra, Jr. “Complex Multiplication Structure of Elliptic Curves”. In: *Journal of Number Theory* 56.2 (1996), pp. 227–241. ISSN: 0022-314X. DOI: https://doi.org/10.1006/jnth.1996.0015. URL: https://www.sciencedirect.com/science/article/pii/S0022314X96900153.

[Mil85] Victor S. Miller. “Use of Elliptic Curves in Cryptography”. In: *Advances in Cryptology - CRYPTO ’85, Santa Barbara, California, USA, August 18-22, 1985, Proceedings*. Ed. by Hugh C. Williams. Vol. 218. Lecture Notes in Computer Science. Springer, 1985, pp. 417–426. DOI: 10.1007/3-540-39799-X_31. URL: https://doi.org/10.1007/3-540-39799-X%5C_31.

[MM22] Luciano Maino and Chloe Martindale. *An attack on SIDH with arbitrary starting curve*. Cryptology ePrint Archive, Paper 2022/1026. 2022. URL: https://eprint.iacr.org/2022/1026.

[Mon87] Peter L. Montgomery. “Speeding the Pollard and elliptic curve methods of factorization”. In: *Mathematics of computation* 48.177 (1987), pp. 243–264.

[NP20] Hart Montgomery Navid Alamati Luca De Feo and Sikhar Patranabis. “Cryptographic group actions and applications”. In: *Advances in Cryptology–ASIACRYPT 2020: 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7–11, 2020, Proceedings, Part II 26*. Ed. by Shiho Moriai and Huaxiong Wang. Springer. 2020, pp. 411–439. ISBN: 978-3-030-64834-3.

[OKS00] Katsuyuki Okeya, Hiroyuki Kurumatani, and Kouichi Sakurai. “Elliptic Curves with the Montgomery-Form and Their Cryptographic Applications”. In: *Public Key Cryptography*. Ed. by Hideki Imai and Yuliang Zheng. Berlin, Heidelberg: Springer Berlin Heidelberg, 2000, pp. 238–257. ISBN: 978-3-540-46588-1.

[PPG24] Christof Paar, Jan Pelzl, and Tim Güneysu. *Understanding Cryptography - From Established Symmetric and Asymmetric Ciphers to Post-Quantum Algorithms, Second Edition*. Springer, 2024. ISBN: 978-3-662-69006-2. DOI: 10.1007/978-3-662-69007-9. URL: https://doi.org/10.1007/978-3-662-69007-9.

[QC25] Mingping Qi and Chi Chen. “HPQKE: Hybrid Post-Quantum Key Exchange Protocol for SSH Transport Layer From CSIDH”. In: *IEEE Transactions on Information Forensics and Security* 20 (2025), pp. 2122–2131. DOI: 10.1109/TIFS.2025.3539943.

[Ren18] Joost Renes. “Computing Isogenies Between Montgomery Curves Using the Action of (0, 0)”. In: *Post-Quantum Cryptography*. Ed. by Tanja Lange and Rainer Steinwandt. Cham: Springer International Publishing, 2018, pp. 229–247. ISBN: 978-3-319-79063-3.

[RS06] Alexander Rostovtsev and Anton Stolbunov. “Public-Key Cryptosystem Based on Isogenies”. In: *IACR Cryptol. ePrint Arch.* (2006), p. 145. URL: http://eprint.iacr.org/2006/145.

[Sch87] René Schoof. “Nonsingular plane cubic curves over finite fields”. In: *Journal of Combinatorial Theory, Series A* 46.2 (1987), pp. 183–211. ISSN: 0097-3165. DOI: https://doi.org/10.1016/0097-3165(87)90003-3. URL: https://www.sciencedirect.com/science/article/pii/0097316587900033.

[Sho94] Peter W. Shor. “Algorithms for Quantum Computation: Discrete Logarithms and Factoring”. In: *35th Annual Symposium on Foundations of Computer Science, Santa Fe, New Mexico, USA, 20-22 November 1994*. IEEE Computer Society, 1994, pp. 124–134. DOI: 10.1109/SFCS.1994.365700. URL: https://doi.org/10.1109/SFCS.1994.365700.

[Sho97] Victor Shoup. “Lower Bounds for Discrete Logarithms and Related Problems”. In: *Advances in Cryptology - EUROCRYPT ’97, International Conference on the Theory and Application of Cryptographic Techniques, Konstanz, Germany, May 11-15, 1997, Proceeding*. Ed. by Walter Fumy. Vol. 1233. Lecture Notes in Computer Science. Springer, 1997, pp. 256–266. DOI: 10.1007/3-540-69053-0_18. URL: https://doi.org/10.1007/3-540-69053-0%5C_18.

[Sil86] Joseph H. Silverman. *The arithmetic of elliptic curves*. Vol. 106. Graduate texts in mathematics. Springer, 1986. ISBN: 978-3-540-96203-8.

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*. Vol. 151. Springer Science & Business Media, 1994.

[Tat66] John Tate. "Endomorphisms of abelian varieties over finite fields". In: *Inventiones mathematicae* 2 (1966), pp. 134–144. URL: https://pazuki.perso.math.cnrs.fr/index_fichiers/Tate66.pdf.

[TJ14] Henk C. A. van Tilborg and Sushil Jajodia. *Encyclopedia of cryptography and security*. Springer Science & Business Media, 2014.

[Was08] Lawrence C. Washington. *Elliptic curves: number theory and cryptography*. Chapman and Hall/CRC, 2008.

[Wat69] William C Waterhouse. "Abelian varieties over finite fields". In: *Annales scientifiques de l'École normale supérieure*. Vol. 2. 4. 1969, pp. 521–560. URL: https://www.numdam.org/item/10.24033/asens.1183.pdf.