Elliptic curves, isogenies, and endomorphism rings

Jana Sotáková

QuSoft/University of Amsterdam

July 23, 2020

Abstract

Protocols based on isogenies of elliptic curves are one of the hot topic in post-quantum cryptography, unique in their computational assumptions. This note strives to explain the beauty of the isogeny landscape to students in number theory using three different isogeny graphs - nice cycles and the Schreier graphs of group actions in the commutative isogeny-based cryptography, the beautiful isogeny volcanoes that we can walk up and down, and the Ramanujan graphs of SIDH.

This is a written exposition [1] of the talk I gave at the ANTS summer school 2020, available online at `https://youtu.be/hHD1tqFqjEQ?t=4`.

Contents

[1] Please contact me with any comments or remarks at ja.sotakova@gmail.com.

1 Introduction

There are three different aspects of isogenies in cryptography, roughly corresponding to three different isogeny graphs: unions of cycles as used in CSIDH, isogeny volcanoes as first studied by Kohel, and Ramanujan graphs upon which SIDH and SIKE are built.

We start off with introducting elliptic curves, isogenies of elliptic curves and endomorphisms rings in Section 2. Then we talk about the theory of Complex Multiplication and explain how the commutative isogeny-based protocols (such as CSIDH) work in Section 3. We mention briefly how considering all ℓ-isogenies allows us to build isogeny volcanoes in Section 4. Finally, we move to the case of supersingular elliptic curves and the Ramanujan graphs in Section 5.

2 Background

2.1 Elliptic curves

An elliptic curve E over a finite field $\mathbb{F}_q$ (for $q = p^n$ with $p > 3$) is an algebraic group given by an equation

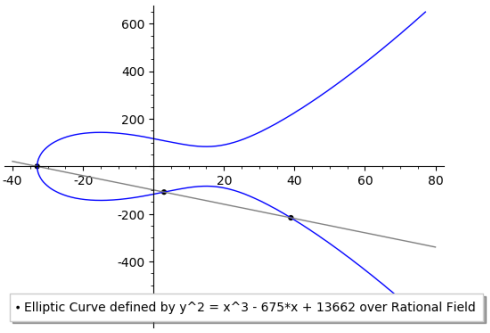
$$E : y^2 = x^3 + ax + b, \quad a, b \in \mathbb{F}_q,\ 4a^3 + 27b^2 \neq 0$$

That is, it is an algebraic variety defied as (the projective closure of) the curve E, which is also a group and the group law is given geometrically.

The points of E are pairs $P = (x_P, y_P) \in (\overline{\mathbb{F}}_q)^2$ satisfying the equation and the point at infinity O_E (with projective coordinates $(0 : 1 : 0)$).

The group law on an elliptic curve is given geometrically:

$$P + Q + R = O_E \quad \longleftrightarrow \quad P, Q, R \text{ lie on a line}$$



and can also be given by algebraic formulae that only depend on the coefficients a, b of E.

Later will label E by the j-invariant

$$j(E) = 1728\frac{4a^3}{4a^3 + 27b^2}.$$

The j-invariant is an $\overline{\mathbb{F}}_q$-isomorphism invariant but not $\mathbb{F}_q$-isomorphism.

The subgroup of rational points $E(\mathbb{F}_q)$ is given by the point at infinity O_E and points (x, y) of E with both coordinates in $\mathbb{F}_q$. Since the group law is given by formulae in $a, b \in \mathbb{F}_q$, this is a subgroup.

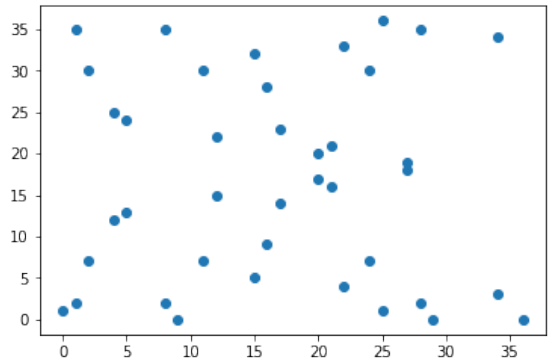


Figure 2.1: *Rational points of $E : y^2 = x^3 + x + 2$ over $\mathbb{F}_{37}$. There are 40 rational points, including O_E.*

Theorem 2.1 (Hasse-Weil)**.** *There are $\#E(\mathbb{F}_q) = q + 1 - t$ points on E where t satisfies $|t| \leq 2\sqrt{q}$.*

Definition 2.2. *Let $E/\mathbb{F}_q$ be an elliptic curve with $q + 1 - t$ points.*

- *If $p \nmid t$ then E is called ordinary,*
- *if $p \mid t$ then E is called supersingular.*

Elliptic curves with the same j-invariant are either all ordinary or all supersingular elliptic curves.

2.2 Isogenies

Definition 2.3. *An isogeny (defined over $\mathbb{F}_q$) between elliptic curves $E, E'/\mathbb{F}_q$ is a rational map*

$$\begin{aligned} \varphi : E &\longrightarrow E' \\ (x, y) &\longmapsto (f(x), y \cdot g(x)) \end{aligned}$$

for some $f, g \in \mathbb{F}_q(x)$, which is also a group homomorphism.

Definition 2.4. *The degree of the isogeny is the degree of φ as a rational map.*

Therefore, the degree is multiplicative. An isogeny of degree ℓ is called an ℓ-isogeny.

Example 2.5. *Multiplication by m for $m \in \mathbb{Z}$: denoted $[m] : E \to E$, sends $P \mapsto [m]P$. This is an isogeny because the group law is defined algebraically. Moreover, it is $\mathbb{F}_q$-rational and has degree $\deg[m] = m^2$.*

- *multiplication by 2: degree 4*

$$[2] : (x, y) \mapsto \left(\frac{x^4 - 2ax^2 - 8bx + a^2}{4(x^3 + ax + b)}, y \cdot g(x) \right)$$

- *multiplication by 3: degree 9*

$$[3] : (x, y) \mapsto \left(\frac{x^9 + lot}{(3x^4 + 6ax^2 + bx - a^2)^2}, y \cdot g(x) \right)$$

Fact 2.6. *Any isogeny has a finite kernel, which can be read off from the denominators. If $p \nmid m$ then* $\deg \varphi = \# \ker \varphi$.

Fact 2.7. *For any isogeny $\varphi : E \to E'$, there exist a dual isogeny $\hat{\varphi} : E' \to E$ with*

$$\hat{\varphi} \circ \varphi = [\deg \varphi].$$

Example 2.8. *A 5-isogeny over $\mathbb{F}_{37}$:*

$$\begin{aligned} E : y^2 = x^3 + x + 2 &\longrightarrow E' : y^2 = x^3 + 31x + 33 \\ (x, y) &\longmapsto \left(\frac{36(x^5 + 8x^4 + 3x^3 + 3x^2 + 3x + 14)}{(x^2 + 4x + 15)^2}, y \cdot g(x) \right) \end{aligned}$$

Has kernel $\{O_E\} \cup \{(x, y) : x^2 + 4x + 15 = 0\} = \{O_E, (8, 2), (8, 35), (25, 1), (25, 36)\}$

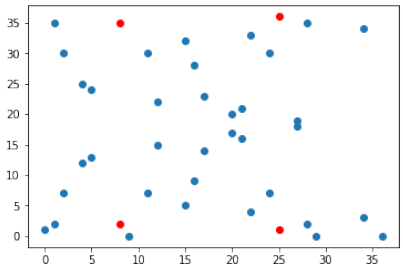


Figure 2.2: *Kernel of the isogeny φ (in red).*

The dual isogeny is

$$\begin{aligned} \hat{\varphi} : y^2 = x^3 + 31x + 33 &\longrightarrow y^2 = x^3 + x + 2 \\ (x, y) &\longmapsto \left(\frac{34x^5 + 28x^4 + 18x^3 + 25x^2 + 5x + 33}{(x^2 + 20x + 34)^2}, y \cdot g(x) \right) \end{aligned}$$

which is again a 5-isogeny.

2.3 Endomorphisms

Let $E/\mathbb{F}_q$ be an elliptic curve. We define the rational endomorphism ring

$$\mathrm{End}_{\mathbb{F}_q}(E) = \{\mathbb{F}_q\text{-isogenies } \varphi : E \to E\} \cup \{0\}.$$

Note that not all endomorphisms of E need to be defined over $\mathbb{F}_q$. It is customary to consider the ring $\mathrm{End}(E)$ of all endomorphims of E but in the following, we will see that studying $\mathrm{End}_{\mathbb{F}_q}(E)$ is easier in the context of isogeny-based cryptography.

Definition 2.9. *The Frobenius endomorphism for $E/\mathbb{F}_q$ is the endomorphism*

$$\begin{aligned} \pi_E : E &\longrightarrow E \\ (x, y) &\longmapsto (x^q, y^q). \end{aligned}$$

The Frobenius endomorphism depends on the field of definition of E and is an isogeny of degree $\deg \pi = q$. It is an important endomorphism because of the following:

Fact 2.10. *For an elliptic curve $E/\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = q + 1 - t$, the Frobenius endomorphims satisfies*

$$\pi^2 - t\pi + q = 0.$$

We call $t = \operatorname{tr} \pi$ the trace of Frobenius.
But from Hasse-Weil's theorem, we know that $|t| \leq 2\sqrt{q}$ so $t^2 - 4q \leq 0$.

Theorem 2.11 (Waterhouse)**.** *For the rational endomorphism ring* $\operatorname{End}_{\mathbb{F}_q}(E)$*, only the following two options are possible:*

1. *If* $t^2 - 4q < 0$ *then* $\mathbb{Q}(\pi)$ *is an imaginary quadratic field and*

$$\operatorname{End}_{\mathbb{F}_q}(E) \hookrightarrow \mathbb{Q}(\pi) = \mathbb{Q}(\sqrt{t^2 - 4q})$$

   as an order $\mathcal{O}$ *containing* $\mathbb{Z}[\pi]$*.*

2. *If* $t^2 - 4q = 0$ *then* $\pi = \pm\sqrt{q} = \pm p^{n/2}$ *and*

$$\operatorname{End}_{\mathbb{F}_q}(E) \hookrightarrow B_{p,\infty}$$

   as a maximal order $\mathcal{O}$ *in a quaternion algebra ramified only at* p *and* ∞*.*

Remark 2.12. *We give a number of references for the above statement.*

1. *The above statement is Theorem 4.1 in Waterhouse's thesis, available at* `https://eudml.org/doc/81852`*.*
2. *For CM theory (orders in imaginary quadratic fields),*
   - *detailed: read Cox's Primes of the form* $x^2 + ny^2$ *(chapter 7 to understand ideals in orders and chapter on EC).*
   - *Sutherland's lectures on elliptic curves give an amazing exposition* `https://ocw.mit.edu/courses/mathematics/18-783-elliptic-curves-spring-2019/lecture-notes/`
3. *For quaternion algebras,*
   - *Kohel's thesis chapter 6-7 is a good resource but it fairly advanced* `http://iml.univ-mrs.fr/~kohel/pub/thesis.pdf`
   - *A more elementary/detailed write-up of the correspondence is chapter 42 of John Voight's book* `https://math.dartmouth.edu/~jvoight/quat.html`
   - *to get comfortable with quaternions you can read Keith Conrad's blurb on quaternions* `https://kconrad.math.uconn.edu/blurbs/ringtheory/quaternionalg.pdf`

Example 2.13 (Examples of endomorphism rings)**.** *We give examples of the above cases.*

1. *The elliptic curve* $E/\mathbb{F}_{31}$ *given by* $E : y^2 = x^3 + x + 4$*:*

$$\#E(\mathbb{F}_{31}) = 26 = 1 - 6 + 31 \quad \longrightarrow t = 6 \quad \text{and } t^2 - 4q = -88 \neq 0.$$

   The Frobenius satisfies

$$\pi^2 - 6\pi + 31 = 0 \quad \longrightarrow \pi = 3 \pm \sqrt{-22}.$$

   So $\operatorname{End}_{\mathbb{F}_{31}}(E)$ *is an order in* $\mathbb{Q}(\pi) = \mathbb{Q}(\sqrt{-22})$ *containing* $\mathbb{Z}[\pi] = \mathbb{Z}[\sqrt{-22}]$*. But* $\mathbb{Z}[\sqrt{-22}]$ *is the maximal order in* $\mathbb{Q}(\pi)$*, so*

$$\operatorname{End}_{\mathbb{F}_{31}}(E) = \mathbb{Z}[\sqrt{-22}].$$

2. *The elliptic curve* $E/\mathbb{F}_{31}$ *given by* $E : y^2 = x^3 - x$*:*

$$\#E(\mathbb{F}_{31}) = 32 = 1 + 0 + 31 \quad \longrightarrow t = 0 \quad \text{and } t^2 - 4q \neq 0.$$

So $\mathrm{End}_{\mathbb{F}_{31}}(E)$ *is an order in* $\mathbb{Q}(\pi) = \mathbb{Q}(\sqrt{-31})$*.*

Exercise: One can show

$$\mathrm{End}_{\mathbb{F}_{31}}(E) \cong \mathbb{Z}\left[\frac{1+\sqrt{-31}}{2}\right].$$

(Hint: Show that it cannot lie on the floor of a 2*-volcano because there are too many* 2*-isogenies. Direct way: show that* $E[2] \subset \ker(\pi + 1)$ *and use the 'factorization property' for isogenies (not covered). This is essentially proof of Theorem 2.7 in [8]* `https://arxiv.org/pdf/1310.7789.pdf`*, works similarly for any* ℓ*.)*

3. *The elliptic curve* $E/\mathbb{F}_{31^2}$ *given by* $E : y^2 = x^3 - x$*:*

$$\#E(\mathbb{F}_{31^2}) = 1024 \quad \longrightarrow t = -62 = -2 \cdot 31 = -2 \cdot \sqrt{q}$$
$$\text{and } t^2 - 4q = 0.$$

So $\mathrm{End}_{\mathbb{F}_{31^2}}(E)$ *is a maximal order in the quaternion algebra* $B_{31,\infty}$*.*
One can show that

$$\mathrm{End}_{\mathbb{F}_{31^2}}(E) \cong \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}\frac{i+j}{2} + \mathbb{Z}\frac{1+ij}{2},$$

with $i^2 = -1$ *and* $j^2 = -31$ *and* $ij = -ji$*.*
Note that this curve is just a base change of the curve above.

Exercise: convince yourself that $\mathbb{Z}\left[\frac{1+\sqrt{-31}}{2}\right]$ *is a subring of* $\mathrm{End}_{\mathbb{F}_{31^2}}(E)$*.*

(Hint: what is $(ij)^2$*?)*

2.4 From ideals to isogenies

For any (nonzero) ideal $\mathfrak{a} \subset \mathcal{O}$ we can produce a finite subgroup

$$E[\mathfrak{a}] = \cap_{\alpha \in \mathfrak{a}} \ker \alpha.$$

Definition 2.14. *Let* $\mathfrak{a}$ *be an ideal of* $\mathcal{O}$*. The isogeny correspodning to* $\mathfrak{a}$*, denoted by* $\varphi_{\mathfrak{a}} : E \to E/E[\mathfrak{a}]$*, is the isogeny with* $\ker(\varphi_{\mathfrak{a}}) = E[\mathfrak{a}]$*.*

The degree of the isogeny is

$$\deg \varphi_{\mathfrak{a}} = \mathrm{N}(\mathfrak{a}).$$

Example 2.15. *Take a prime* ℓ *and* $\mathfrak{l} = (\ell, \pi - 1) \subset \mathcal{O}$*. We want to identify the isogeny correspodning to* $\mathfrak{l}$*. So we need to intersect*

- $\ker[\ell] = E[\ell]$ *is the subgroup of* ℓ*-torsion points,*
- *and* $\ker(\pi - 1) = \{P : \pi(P) = P\} = \{(x, y) : x^q = x \text{ and } y^q = y\} = E(\mathbb{F}_q)$ *the group of rational points.*

So $E[\mathfrak{l}] = E[\ell] \cap E(\mathbb{F}_q) = E(\mathbb{F}_q)[\ell]$*, that is, the points in the* ℓ*-torsion which are defined already over* $\mathbb{F}_q$*. As abelian groups,*

$$E[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}.$$

So the action of $\mathfrak{l} = (\ell, \pi - 1)$ *is given as:*

1. *If* $E(\mathbb{F}_q)[\ell] = E[\ell]$ *then* $\varphi_{\mathfrak{l}}$ *is multiplication by* ℓ*,*
2. *if* $E(\mathbb{F}_q)[\ell] = \langle P \rangle$ *then* $\varphi_{\mathfrak{l}}$ *is the* ℓ*-isogeny with kernel generated by rational* ℓ*-torsion point* P*,*
3. *if* $E(\mathbb{F}_q)[\ell] = \{O_E\}$ *then* $\varphi_{\mathfrak{l}}$ *is the identity.*

3 CM and commutative isogeny-based protocols

3.1 The main theorem of complex multiplication

Let E be an elliptic curve over $\mathbb{F}_q$ with $q+1-t$ points and assume that $t^2-4q \neq 0$. Then $\mathrm{End}_{\mathbb{F}_q}(E) = \mathcal{O}$ is an order in an imaginary quadratic field $\mathbb{Q}(\pi)$ and $\mathcal{O}$ contains $\mathbb{Z}[\pi]$. From any ideal $\mathfrak{a} \subset \mathcal{O}$ we get an isogeny $\varphi_{\mathfrak{a}} : E \to E/E[\mathfrak{a}]$.

Fact 3.1. *If $\mathfrak{a} \subset \mathcal{O}$ is an invertible ideal, then $E/E[\mathfrak{a}]$ has the same endomorphism ring $\mathcal{O}$ and trace t.*

Fact 3.2. *If $\mathfrak{a}$ and $\mathfrak{b}$ are in the same class in $\mathrm{Cl}(\mathcal{O})$, then*

$$E/E[\mathfrak{a}] \cong E/E[\mathfrak{b}] \quad \text{over } \mathbb{F}_q.$$

Denote

$$\mathscr{El}(\mathcal{O}, t) = \{ \text{elliptic curves } E/\mathbb{F}_q : \mathrm{End}_{\mathbb{F}_q}(E) \cong \mathcal{O} \text{ and } \mathrm{tr}(\pi) = t \} / \cong_{\mathbb{F}_q}.$$

Theorem 3.3 (The Main Theorem of Complex Multiplication)**.** *For any $E, E' \in \mathscr{El}(\mathcal{O}, t)$ there exists a unique class $[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O})$ such that*

$$E' = [\mathfrak{a}] \star E.$$

The group $\mathrm{Cl}(\mathcal{O})$ acts on $\mathscr{El}(\mathcal{O}, t)$ freely and transitively by $([\mathfrak{a}], E) \mapsto [\mathfrak{a}] \star E$.

Remark 3.4. *Curves satisfying $\mathrm{End}(E) = \mathcal{O}$ are said to have complex multiplication (CM) by $\mathcal{O}$. The Main Theorem of Complex Multiplication is usually stated about the Galois action on j-invariants of elliptic curves with CM by $\mathcal{O}$.*

Probably the treatment of complex multiplication (over number fields) I liked the best was Lang's Elliptic functions (if you know about modular functions). The rest follows by reducing modulo a prime above p. You can also consult my master's thesis for a concise introduction

***https://jana-sotakova.github.io/masters_thesis_sotakova.pdf*.**

3.2 Diffie-Hellman using groups

Alice and Bob wish to establish a shared secret over an insecure channel. They agree on

- an abelian group G (say $G = (\mathbb{Z}/p\mathbb{Z})^*$ for a large prime p),
- an element $g \in G$ that generates G, known order $N = |G|$.

Alice	insecure channel	Bob
$a \leftarrow \mathbb{Z}/N\mathbb{Z}$	G, g of order N	$b \leftarrow \mathbb{Z}/N\mathbb{Z}$
computes g^a	$\xleftarrow{g^b}$ / $\xrightarrow{g^a}$	computes g^b
receives g^b		receives g^a
computes $(g^b)^a$		computes $(g^a)^b$

So both Alice and Bob share g^{ab}.

The computational assumption is that from g, g^a, g^b one cannot compute g^{ab} (computational Diffie-Hellman assumption). In particular, it is not possible to compute the secret exponent a from seeing only g and g^a (the discrete logarithm problem).

But this protocol is insecure against quantum computers (Shor's algorithm).

3.3 Diffie-Hellman using group actions

Suppose that Alice and Bob also have a free and transitive action of the group G on a set X:

$$G \times X \to X \qquad (g, x) \mapsto g \star x.$$

Choosing $x \in X$ gives a bijection $X \leftrightarrow G$ but the set X hides the structure of G: there is no group law on X that would allow us to take two elements of X and produce their composition in X.

Alice	insecure channel	Bob
$a \leftarrow \mathbb{Z}/N\mathbb{Z}$	G, g of order N, $x \in X$	$b \leftarrow \mathbb{Z}/N\mathbb{Z}$
computes $g^a \star x$	$\xleftarrow[g^a \star x]{g^b \star x}$	computes $g^b \star x$
receives $g^b \star$		receives $g^a \star x$
computes $g^a \star (g^b \star x)$		computes $g^b \star (g^a \star x)$

So both Alice and Bob share $g^{a+b} \star x$.

The computational assumption is that it is not possible to compute $g^{a+b} \star x$ seeing only $g^a \star x$ and $g^b \star x$ (parallelization). In particular, it is not possible to compute g^a from seeing only x and $g^a \star x$, which is called the Group Action Inverse Problem (GAIP) or the vectorization problem, in analogy to finding the vector connecting two points in an affine space.

This protocol is no longer breakable by Shor's algorithm, because an adversary only sees elements in a set, not a group, hence cannot compute with the elements of X.

Remark 3.5. *For more information, read either Couveignes' paper* `https://eprint.iacr.org/2006/291` *or Smith's recent excellent exposition* `https://eprint.iacr.org/2018/882` *for the group action paradigm. Note that you don't need to use the exact DH-protocol with just hiding the group elements using the action, but it is easier to explain the parallel this way.*

3.4 Commutative isogeny-based cryptography

We have a free and transitive group action

$$\mathrm{Cl}(\mathcal{O}) \times \mathscr{El}\ell(\mathcal{O}, t) \to \mathscr{El}\ell(\mathcal{O}, t) \qquad ([\mathfrak{a}], E) \mapsto [\mathfrak{a}] \star E.$$

This is a promising construction (originating in [6] and [14]):

- ✓ we hide* $\mathrm{Cl}(\mathcal{O})$ using the set of elliptic curves $\mathscr{El}\ell(\mathcal{O}, t)$
  (actually, almost always leaks information about 2-torsion, see [5])
- ✓ quantum-safe*
  (subexponential quantum complexity, current research about how safe [2, 12] or `https://csidh.isogeny.org/analysis.html`),
- × we cannot compute $\mathrm{Cl}(\mathcal{O})$ so we cannot get a generator g,
- ✓ we can sample ideals from $\mathrm{Cl}(\mathcal{O})$,
- × we cannot act with all ideals $\mathfrak{a} \subset \mathcal{O}$ because the norms are too big.

But it is enough to choose which ideals we want to act by.

Example 3.6 (Computing the action for some ideals)**.** *Recall the action by ideals* $\mathfrak{l} = (\ell, \pi - 1)$*: if* $E(\mathbb{F}_q)[\ell] = \langle P \rangle$ *is cyclic, then the action is given by the* ℓ*-isogeny*

$$[\mathfrak{l}] \star E = E/\langle P \rangle.$$

So to compute the action of $\mathfrak{l} = (\ell, \pi - 1)$*, we only need to:*

1. *Find a rational point* $P \in E(\mathbb{F}_q)$ *of order* ℓ*,*
   This is easily done by taking a random rational point on E *and mutliplying it by* $(q + 1 + t)/\ell$*. This fails with probability* $\frac{1}{\ell}$ *so we may have to repeat this step.*
2. *Compute the* ℓ*-isogeny* $E \to E/\langle P \rangle$ *using Vélu's formulae [15].*

The modern setup of the group action-based Diffie-Hellman is the following:

- Find elliptic curves E with

$$E(\mathbb{F}_q)[\ell_i] \text{ cyclic for lots of small primes } \ell_i,$$

- Only work with ideals $\mathfrak{l}_i = (\ell, \pi - 1)$ and their products

$$\mathfrak{a} = \prod \mathfrak{l}_i^{e_i} \quad e_i \text{ small.}$$

  We can compute the action of such an ideal $\mathfrak{a}$ by computing a sequence of ℓ_i-isogenies, each performed e_i times, in any order we choose (remember that $\star$ is a group action by an abelian group).

Therefore, the secrets: are now the lists of exponents $(e_1, \ldots, e_r)$. This goes back to [6].
The following are (examples of) the choices of the modern proposals:

- [7] use ordinary elliptic curves over a prime field $\mathbb{F}_p$ with $\#E(\mathbb{F}_p) = q + 1 - t$ divisible by lots of small primes, eg. with points of order ℓ for every

$$\ell \in \{3, 5, 7, 11, 13, 17, 103, 523, 821, 947, 1723\}.$$

- CSIDH [4] uses supersingular elliptic curves ($t = 0$) over $\mathbb{F}_p$ with $p \equiv 3 \mod 8$, the order $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$ and $\#E(\mathbb{F}_p) = p + 1$ divisible by lots of small primes, e.g.

$$p + 1 = 4 \cdot 3 \cdot 5 \cdot \ldots \cdot 373 \cdot 587.$$

- CSURF [3] uses supersingular elliptic curves over $\mathbb{F}_p$ with $p \equiv 7 \mod 8$, the order $\mathcal{O} = \mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$ and $\#E(\mathbb{F}_p) = p + 1$ divisible by lots of small primes, e.g.

$$p + 1 = 8 \cdot 3^2 \cdot \ldots \cdot \widehat{347} \cdot \ldots \cdot \widehat{359} \cdot \ldots \cdot 389.$$

3.5 Isogeny graphs

Recall that $\mathscr{Ell}(\mathcal{O}, t)$ is the set of $\mathbb{F}_q$-isomorphism classes of $E/\mathbb{F}_q$ with $\mathrm{End}_{\mathbb{F}_q}(E) = \mathcal{O}$ and $\operatorname{tr} \pi_E = t$. The class group $\mathrm{Cl}(\mathcal{O})$ acts on $\mathscr{Ell}(\mathcal{O}, t)$. By repeated action of an ideal $\mathfrak{l} = (\ell, \pi - 1)$ on $\mathscr{Ell}(\mathcal{O}, t)$, we obtain a sequences of ℓ-isogenies. If n is the order of $[\mathfrak{l}]$ in $\mathrm{Cl}(\mathcal{O})$, then $[\mathfrak{l}^n] = [\mathcal{O}]$

$$E \xrightarrow{\mathfrak{l}} [\mathfrak{l}] \star E \xrightarrow{\mathfrak{l}} [\mathfrak{l}] \star ([\mathfrak{l}] \star E) = [\mathfrak{l}^2] \star E \xrightarrow{\mathfrak{l}} \cdots \xrightarrow{\mathfrak{l}} [\mathfrak{l}^n] \star E = E,$$

so the repeated action by $\mathfrak{l}$ cycles back to E.

Definition 3.7. *The ℓ-isogeny graph $\mathcal{G}_\ell(\mathbb{F}_q)$ is the graph with*

- *vertices given by the classes in $\mathscr{El}(\mathcal{O}, t)$, labelled by the j-invariants,*
- *there is an undirected edge between $[E_1]$ and $[E_2]$ if there is an isogeny $E_1 \to E_2$.*

Note that this is the same as identifying isogenies if they differ by composition with isomorphisms over $\mathbb{F}_q$ and by identifying dual isogenies.

Note that Alice and Bob's secret key computation can be thought of as taking a walk from the starting vertex E_0 in the ℓ_1-isogeny graph $\mathcal{G}_{\ell_1}(\mathbb{F}_q)$, then jumping to the corresponding vertex in the ℓ_2-isogeny graph and so on. See Figures **??**, **??** and **??**.

On the other hand, the adversary sees these graphs $\mathcal{G}_{\ell_i}(\mathbb{F}_q)$ overlapping: that is, the adversary does not know whether Alice first decided to take an ℓ_i or ℓ_j isogeny or how many steps she took in which graph.

Example 3.8. *Consider $q = 461 = 2 \cdot 3 \cdot 7 \cdot 11 - 1$ and $\mathcal{O} = \mathbb{Z}[\sqrt{-389}]$ and $t = 0$.*

It is easy to follow the walks in each of the graphs $\mathcal{G}_{\ell_i}(\mathbb{F}_q)$.

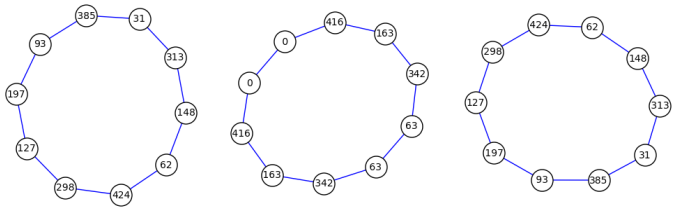
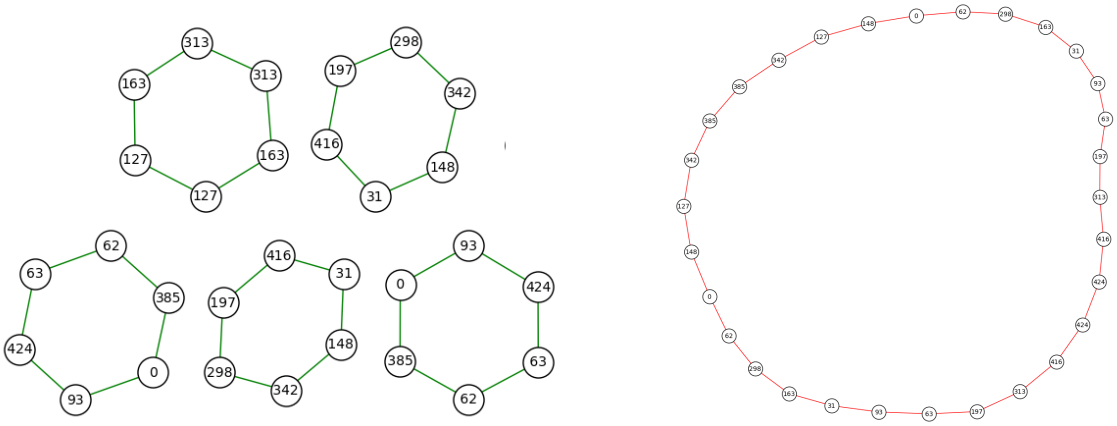


Figure 3.1: *$\mathcal{G}_3(\mathbb{F}_{461})$: the action of $(3, \pi - 1)$*



(a) *$\mathcal{G}_7(\mathbb{F}_{461})$* ***(b)*** *$\mathcal{G}_{11}(\mathbb{F}_{461})$*

But the adversary sees the following entangled graph, and the computational assumptions underlying commutative isogeny-based proposals can be paraphrased as follows: from a given vertex, it is difficult to find a path back to the starting vertex (say top 0).

4 Other ℓ-isogenies

Assume that $\ell \nmid q$. In the complex multiplication story, the rational endomorphism ring of E is an order in an imaginary quadratic field $\mathbb{Q}(\pi)$ and invertible ideals of $\mathcal{O} = \mathrm{End}_{\mathbb{F}_q} E$ correspond to ℓ-isogenies. Moreover, ℓ-isogeny graphs $\mathcal{G}_\ell$ are unions of cycles, so there are two ℓ-isogenies from every $E \in \mathscr{El}(\mathcal{O}, t)$.

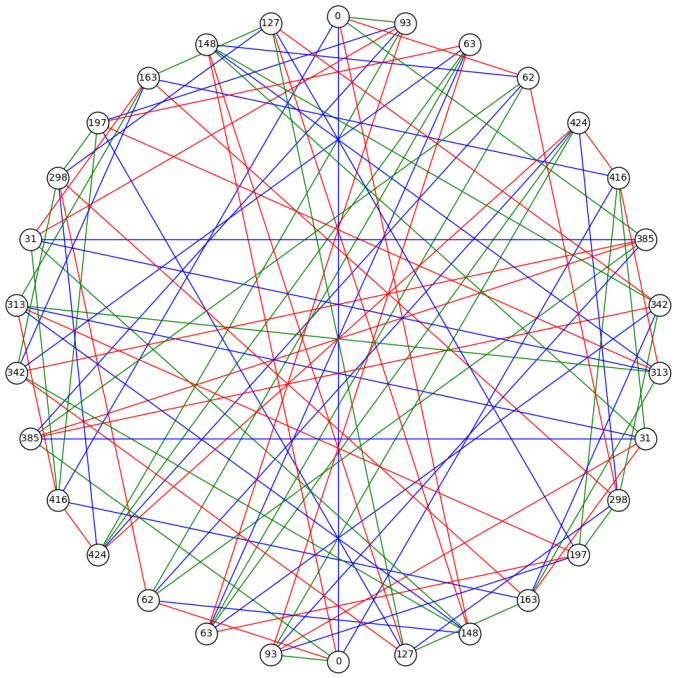


Figure 3.3: *The union of graphs $\mathcal{G}_\ell(\mathbb{F}_{461})$ for $\ell = 3, 7, 11$.*

Recall that an isogeny is given by its kernel and the kernel of an ℓ-isogeny is a subgroup of size ℓ. By looking at the subgroups of size ℓ in

$$E[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z},$$

we see that there are up to $\ell + 1$ isogenies of degree ℓ defined over $\mathbb{F}_q$.

Theorem 4.1 (Tate)**.** *Isogenous curves E and E' over $\mathbb{F}_q$ have the same number of points, i.e.,*

$$\operatorname{tr} \pi_E = t = \operatorname{tr} \pi_{E'}.$$

Because the Frobenius endomorphism of any curve π is a root of $x^2 - tx + q$, if $\operatorname{End}_{\mathbb{F}_q}(E) = \mathcal{O}$ and $\operatorname{End}_{\mathbb{F}_q}(E') = \mathcal{O}'$, then both these orders contain $\mathbb{Z}[\pi]$ and lie in the same quadratic field $\mathbb{Q}(\pi)$.

A more detailed analysis is in David Kohel's thesis.

Theorem 4.2 (Kohel)**.** *If E and E' are ℓ-isogenous by $\varphi : E \to E'$, then*

1. *either $\mathcal{O} = \mathcal{O}'$,* — *$\varphi$ horizontal,*
2. *or $[\mathcal{O} : \mathcal{O}'] = \ell$,* — *$\varphi$ descending,*
3. *or $[\mathcal{O}' : \mathcal{O}] = \ell$.* — *$\varphi$ ascending.*

Therefore, there is a tight connection between ℓ-isogenies of elliptic curves and their endomorphism rings.

Definition 4.3. *Define the component of E as the graph $G = (V, E)$ with*

- *vertices V given by $\mathbb{F}_q$-isomorphism classes of curves which are ℓ^k-isogenous to E,*
- *edges given by ℓ-isogenies, up to $\mathbb{F}_q$ equivalence and dual isogenies (as before).*

This component of E captures all the curves over $\mathbb{F}_q$ that can be reached from E by taking ℓ-isogenies.

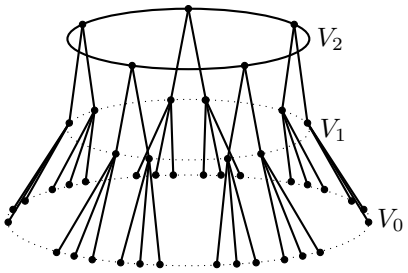


Figure 4.1: *Example of a volcano of height* 2.

Theorem 4.4 (Kohel's theorem)**.** *For any $E/\mathbb{F}_q$, the component of E is an isogeny volcano: There is a partition of the vertices into disjoint sets $V = V_0 \cup V_1 \cup \dots V_h$ such that*

- *the subgraph on V_h is a cycle*
- *the subgraph of V_i for $i \neq h$ has no edges,*
- *isogenies from surface to floor are descending,*
- *isogenies from floor to surface are ascending,*
- *if $i < h$, every $E_i \in V_i$ has exactly one neighbour $E_{i+1} \in V_{i+1}$,*
- *every $E_i \in V_i$ for $i \neq 0$ has $\ell + 1$ neighbours.*

The set V_h is called the surface, the set V_0 is called the floor. Note that some authors flip the labelling so that V_0 is the surface and talk about the depth of the volcano instead.

All curves in V_i have the same endomorphism ring $\mathcal{O}_i$ and the curves on the floor satisfy

$$(\mathcal{O}_0)_\ell = \mathbb{Z}[\pi]_\ell,$$

that is, localizing at ℓ, the endomorphism ring $\mathcal{O}_0$ is as small as possible (the endomorphism ring always contains $\mathbb{Z}[\pi]$). Since the isogenies going towards the surface are ascending and the isogenies going towards the floor are descending, knowing one endomorphism ring allows us to determine the endomorphism rings of all the elliptic curves on this volcano.

Example 4.5. *Assume that one the floor V_0 have $\mathrm{End}_{\mathbb{F}_q}(E) = \mathbb{Z}[\pi]$.*

Going up the volcano we take an ascending isogeny to get an order $\mathcal{O}$ containing $\mathbb{Z}[\pi]$ with index ℓ. Suppose that the volcano is h steps high. Then the levels of volcano correspond to a sequence of orders with successive index ℓ:

$$\mathcal{O}_0 = \mathbb{Z}[\pi] \subset \mathcal{O}_1 \cdots \subset \mathcal{O}_h.$$

Looking at discriminants, we have $\ell^{2h} \mid \Delta_{\mathbb{Z}[\pi]} = t^2 - 4q$.

Therefore, to have a volcano of large height, we need a large power of ℓ to divide $t^2 - 4q$.

Example 4.6 (Supersingular elliptic curves)**.** *For supersingular elliptic curves over $\mathbb{F}_p$ we always have $\Delta_{\mathbb{Z}[\pi]} = -p$ or $-4p$. Therefore, we recover cycles as in Section 3.5 for $\ell \neq 2$ and volcanoes of at most 2 levels for $\ell = 2$.*

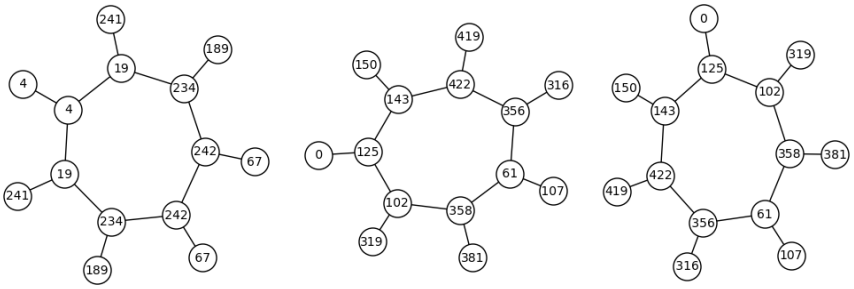


Figure 4.2: *2-isogenies over* $\mathbb{F}_{431}$.

Remark 4.7. *Isogeny volcanoes can be very useful for cryptanalysis.*

5 Supersingular isogeny graphs

In this Section, we will consider the second case from Theorem 2.11, that is, we have an elliptic curve $E/\mathbb{F}_q$ with $q = p^n$ such that its Frobenius endomorphism π satisfies

$$x^2 - tx + q = 0 \quad \text{with } t^2 - 4q = 0, \quad \text{so } t = \pm p^{n/2}.$$

In this case, E is necessarily supersingular (as $p \mid t$) and Theorem 2.11 gives that $\mathrm{End}_{\mathbb{F}_q}(E)$ is a maximal order $\mathcal{O}$ in the quaternion algebra $B_{p,\infty}$.

There are several differences from the commutative case in Section 3:

$-/+$ quaternion algebras are non-commutative,

$+$ we can still construct isogenies from (one-sided) ideals $\mathfrak{a}$ in $\mathcal{O}$,

$-$ even for $\mathfrak{a}$ invertible have $\mathrm{End}_{\mathbb{F}_q}(E) \ncong \mathrm{End}_{\mathbb{F}_q}(E/E[\mathfrak{a}])$,

$-/+$ there is no class group for quaternion algebras that would act on the set of supersingular elliptic curves (considered up to $\overline{\mathbb{F}}_q$-isomorphism),

$+$ all supersingular elliptic curves satisfy $j(E) \in \mathbb{F}_{p^2}$ and so they can already be defined over $\mathbb{F}_{p^2}$, so it is enough to consider the case $t = \pm 2p$,

$+$ every supersingular j-invariant has a representative with $t = -2p$.

5.1 Supersingular curves and isogenies

From now on, we only need[2] to consider the case of supersingular elliptic curves over $\mathbb{F}_{p^2}$ with trace $t = -2p$.

Fact 5.1 (Exercise:)**.**

$$E(\mathbb{F}_{p^2}) \cong \frac{\mathbb{Z}}{(p+1)\mathbb{Z}} \times \frac{\mathbb{Z}}{(p+1)\mathbb{Z}}.$$

Equivalently, for any m*,*

1. *either* $E(\mathbb{F}_{p^2})[m] = \{O_E\}$,
2. *or* $E(\mathbb{F}_{p^2})[m] = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$*, in which case* $m \mid (p+1)^2$.

[2]This is explained well in Adj, Ahmadi, and Menezes `https://eprint.iacr.org/2018/132`

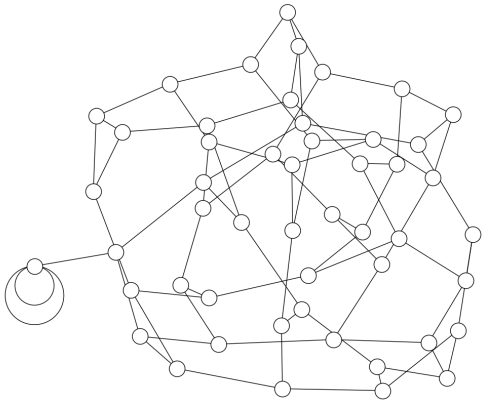


Figure 5.1: *The supersingular isogeny graph* $\mathcal{G}_2(\mathbb{F}_{601})$.

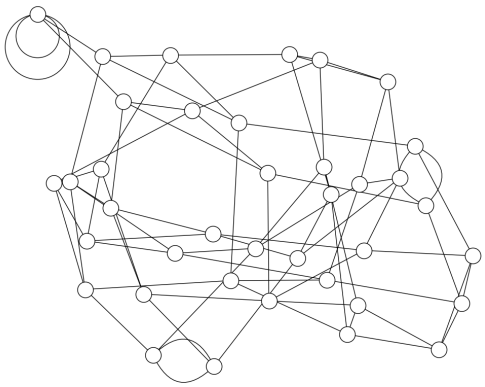


Figure 5.2: *The supersingular isogeny graph* $\mathcal{G}_3(\mathbb{F}_{457})$.

(Hint: Show that the Frobenius acts like a scalar in $\mathrm{End}_{\mathbb{F}_{p^2}}(E)$ *and this means that either all or only trivial* m*-torsion can be defined over* $\mathbb{F}_{p^2}$*.)*

Definition 5.2. *Let* ℓ *be a prime such that* $\ell \mid p+1$*. We define the supersingular* ℓ*-isogeny graph* $\mathcal{G}_\ell(\mathbb{F}_{p^2})$*:*

- *vertices are supersingular* j*-invariants in* $\mathbb{F}_{p^2}$*,*
- *edges are* ℓ*-isogenies, up to equivalence given by identifying isomorphisms and identifying dual isogenies.*

Examples of supersingular isogeny graphs are given in Figure 5.1 and 5.2.
The graph $\mathcal{G}_\ell(\mathbb{F}_{p^2})$ for $\ell \mid p+1$ has the following properties[3]:

1. the graph $\mathcal{G}_\ell(\mathbb{F}_{p^2})$ has $\approx \frac{p}{12}$ vertices,
2. the graph $\mathcal{G}_\ell(\mathbb{F}_{p^2})$ is connected,
3. the graph is $(\ell+1)$-regular with the exception of possibly 2 vertices, corresponding to j-invariants 0 and 1728,
4. the graph $\mathcal{G}_\ell(\mathbb{F}_{p^2})$ has a short diameter: the shortest path between any two vertices has length $\Omega(\log p)$,

[3]For proofs, consult Kohel's thesis `http://iml.univ-mrs.fr/~kohel/pub/thesis.pdf` or Charles, Goren, and Lauter `https://eprint.iacr.org/2006/021`.

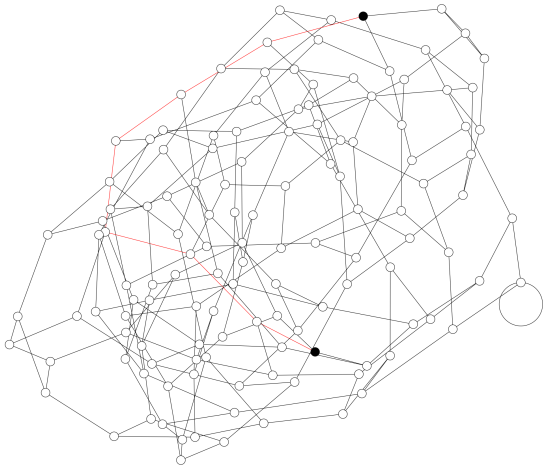


Figure 5.3: *Example of a shortest path between two random vertices in* $\mathcal{G}_2(\mathbb{F}_{1549^2})$.

5. the graph $\mathcal{G}_\ell(\mathbb{F}_{p^2})$ has the rapid mixing property: starting from a vertex v, endpoints of a random walk of length $> \log_\ell p$ are close to uniformly random vertices,

6. (conjecturally: given two arbitrary vertices in $\mathcal{G}_\ell(\mathbb{F}_{p^2})$, it is difficult to find a path between them.

Path finding is currently exponentially hard (in $\log p$), both classically and quantumly.

5.2 SIDH

Supersingular Isogeny Diffie-Hellman is a key exchange protocol from supersingular isogeny curves. We only wish to give a flavor, so we only explain a simplification of Alice's key generation, which relies on the supersingular isogeny graph $\mathcal{G}_\ell(\mathbb{F}_{p^2})$.

From a starting curve $E_0/\mathbb{F}_{p^2}$, Alice chooses a random sequence of ℓ-isogenies, obtaining isogeny

$$\varphi_A : E_0 \to E_A, \quad \deg \varphi_A = \ell^e.$$

Alice's secret is the path in $\mathcal{G}_\ell(\mathbb{F}_{p^2})$ giving the isogeny φ_A and her public key is the curve E_A.

There are many selling points for SIDH:

- fastest attacks on path finding between random vertices are exponential (both quantumly and classically),
- SIDH is easy to instantiate using 2- and 3-isogenies,
- rapid mixing of the graph gives uniformly random* public keys.

The best implementation if SIDH is SIKE [1], which is a candidate proposal in the NIST competition for post-quantum key encapsulation mechanism (tightly related to key exchange).

Taking a second look at the claims above:

1. path finding is not hard for all vertices in $\mathcal{G}_\ell(\mathbb{F}_{p^2})$: it is easier to find paths if
   - the curves are subfield curves, that is, $j(E), j(E') \in \mathbb{F}_p$ [8],
   - both endomorphism rings $\mathrm{End}(E)$ and $\mathrm{End}(E')$ are known [10],
2. Alice needs to publish auxiliary data along with E_A,

- this leads to active attacks (can be remedied at a cost in performance) [9],
- this leads to attacks on unrealistic variants [13], but also on extensions to k-parties,

3. the length of Alice's walk is too short for the rapid mixing property, so there is no guarantee of the randomness of Alice's curve E_A,

4. the subgraph of $\mathcal{G}_\ell(\mathbb{F}_{p^2})$ given by possible secret paths is almost a tree [11], see Figure **??**.

Yet none of this breaks SIKE!

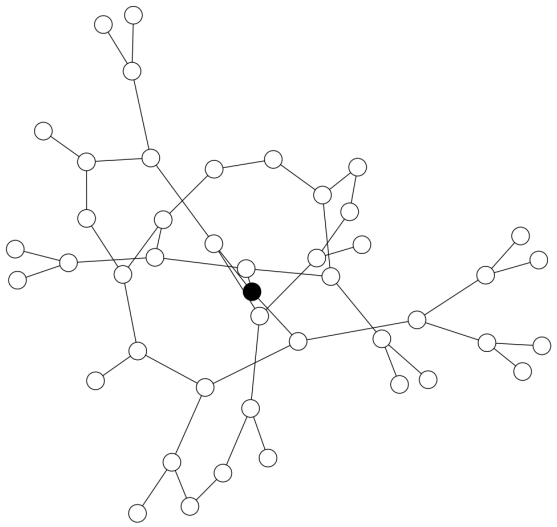


Figure 5.4: *The almost tree of SIKE: the subgraph of $\mathcal{G}_\ell(\mathbb{F}_{p^2})$ which is induced by the paths from the starting curve E_0 to all the possible public keys E_A.*

6 Conclusions

Isogeny-based cryptography is a varied field immensely attractive to number theorists both with its connections to the theory of complex multiplication and to quaternion algebras. There are many unsolved fundamental problems relying the computational assumptions on which the protocols are based.

References

[1] Reza Azarderakhsh, Brian Koziel, Matt Campagna, Brian LaMacchia, Craig Costello, Patrick Longa, Luca De Feo, Michael Naehrig, Basil Hess, Joost Renes, Amir Jalali, Vladimir Soukharev, David Jao, and David Urbanik. Supersingular isogeny key encapsulation, 2017.

[2] Xavier Bonnetain and André Schrottenloher. Quantum security analysis of CSIDH and ordinary isogeny-based schemes. Cryptology ePrint Archive, Report 2018/537, 2018.

[3] Wouter Castryck and Thomas Decru. Csidh on the surface. Cryptology ePrint Archive, Report 2019/1404, 2019.

[4] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: An efficient post-quantum commutative group action. Cryptology ePrint Archive, Report 2018/383, 2018.

[5] Wouter Castryck, Jana Sotáková, and Frederik Vercauteren. Breaking the decisional Diffie-Hellman problem for class group actions using genus theory. Cryptology ePrint Archive, Report 2020/151, 2020.

[6] Jean-Marc Couveignes. Hard homogeneous spaces. Cryptology ePrint Archive, Report 2006/291, 2006.

[7] Luca De Feo, Jean Kieffer, and Benjamin Smith. Towards practical key exchange from ordinary isogeny graphs. Cryptology ePrint Archive, Report 2018/485, 2018.

[8] Christina Delfs and Steven D. Galbraith. Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$. *Designs, Codes and Cryptography*, 78(2):425–440, February 2016.

[9] Steven D. Galbraith, Christophe Petit, Barak Shani, and Yan Bo Ti. On the security of supersingular isogeny cryptosystems. In *Advances in Cryptology–ASIACRYPT 2016: 22nd International Conference on the Theory and Application of Cryptology and Information Security*, pages 63–91. Springer, 2016.

[10] David R. Kohel, Kristin Lauter, Christophe Petit, and Jean-Pierre Tignol. On the quaternion-isogeny path problem. *LMS Journal of Computation and Mathematics*, 17(A):418–432, 2014.

[11] Hiroshi Onuki, Yusuke Aikawa, and Tsuyoshi Takagi. The existence of cycles in the supersingular isogeny graphs used in sike. Cryptology ePrint Archive, Report 2020/439, 2020. `https://eprint.iacr.org/2020/439`.

[12] Chris Peikert. He gives c-sieves on the CSIDH. Cryptology ePrint Archive, Report 2019/725, 2019.

[13] Christophe Petit. Faster algorithms for isogeny problems using torsion point images. In Tsuyoshi Takagi and Thomas Peyrin, editors, *Advances in Cryptology – ASIACRYPT 2017*, pages 330–353. Springer International Publishing, 2017.

[14] Alexander Rostovtsev and Anton Stolbunov. Public-key cryptosystem based on isogenies. Cryptology ePrint Archive, Report 2006/145, April 2006.

[15] Jacques Vélu. Isogénies entre courbes elliptiques. *Comptes Rendus de l'Académie des Sciences de Paris*, 273:238–241, 1971.