Computing isogenies and endomorphism rings of supersingular elliptic curves

Travis Morrison

University of Waterloo

Elliptic Curve Cryptography 2018
November 19th, 2018

Joint work with Kirsten Eisenträger, Sean Hallgren, Kristin Lauter, Christophe Petit

Elliptic curves and post-quantum cryptography

- A quantum computer could efficiently calculate discrete logs of points on elliptic curves

Elliptic curves and post-quantum cryptography

- A quantum computer could efficiently calculate discrete logs of points on elliptic curves
- Elliptic curve cryptography is insecure in a "post-quantum" world

Elliptic curves and post-quantum cryptography

- A quantum computer could efficiently calculate discrete logs of points on elliptic curves
- Elliptic curve cryptography is insecure in a "post-quantum" world
- There are several proposed isogeny based public key cryptosystems which could remain secure. For example, we are learning about SIDH and CSIDH at this conference

Elliptic curves and post-quantum cryptography

- A quantum computer could efficiently calculate discrete logs of points on elliptic curves
- Elliptic curve cryptography is insecure in a "post-quantum" world
- There are several proposed isogeny based public key cryptosystems which could remain secure. For example, we are learning about SIDH and CSIDH at this conference
- Secret keys are isogenies between elliptic curves defined over finite fields

Elliptic curves and post-quantum cryptography

- A quantum computer could efficiently calculate discrete logs of points on elliptic curves
- Elliptic curve cryptography is insecure in a "post-quantum" world
- There are several proposed isogeny based public key cryptosystems which could remain secure. For example, we are learning about SIDH and CSIDH at this conference
- Secret keys are isogenies between elliptic curves defined over finite fields
- Both protocols mentioned above use supersingular elliptic curves, but the problems considered in this talk pertain to SIDH, or the hash function of Charles-Goren-Lauter, rather than CSIDH

Isogenies

Let k be a finite field of characteristic $p > 3$, and let E, E' be two elliptic curves over k.

- An *isogeny over k* is a surjective morphism

$$\phi : E \to E',$$

  defined over k, which induces a group homomorphism from $E(\bar{k}) \to E'(\bar{k})$.
- Every finite subgroup $K \subseteq E(\bar{k})$ determines a separable isogeny $\phi : E \to E/K$, unique up to isomorphism

The endomorphism ring

- An *endomorphism* of E is an isogeny $\phi : E \to E$, possibly defined over an extension of k.
- Let $\mathrm{End}(E)$ $(= \mathrm{End}_{\overline{k}}(E))$ be the set of endomorphisms of E, together with the zero map on E.
- $\mathrm{End}(E)$ is a ring: addition is defined pointwise, and multiplication is given by composition.
- $\mathrm{End}(E)$ always contains $\mathbb{Z}$: let $n \in \mathbb{Z}$, then the multiplication-by-n map

$$
\begin{aligned}
[n] : E &\to E \\
P &\mapsto \underbrace{P + \cdots + P}_{n \text{ times}}
\end{aligned}
$$

is an endomorphism of E.

Supersingular elliptic curves

Definition

E/k is *supersingular* if its endomorphism algebra

$$B := \mathrm{End}(E) \otimes \mathbb{Q}$$

is a quaternion algebra over $\mathbb{Q}$, i.e. a central simple $\mathbb{Q}$-algebra of dimension 4 over $\mathbb{Q}$.

Supersingular elliptic curves

Definition

E/k is *supersingular* if its endomorphism algebra

$$B := \mathrm{End}(E) \otimes \mathbb{Q}$$

is a quaternion algebra over $\mathbb{Q}$, i.e. a central simple $\mathbb{Q}$-algebra of dimension 4 over $\mathbb{Q}$.

- The j-invariant of a supersingular elliptic curve defined over $\overline{\mathbb{F}_p}$ is in $\mathbb{F}_{p^2}$.
- There are $\lfloor \frac{p-1}{12} \rfloor + \epsilon$ supersingular j-invariants in $\mathbb{F}_{p^2}$, where $\epsilon \in \{0, 1, 2\}$.

SIDH and the CGL hash function

- A private key in SIDH or the CGL hash is an ℓ-power isogeny $\phi : E \to E'$ between two supersingular curves $E, E'/\mathbb{F}_{p^2}$, for distinct primes p, ℓ.

SIDH and the CGL hash function

- A private key in SIDH or the CGL hash is an ℓ-power isogeny $\phi : E \to E'$ between two supersingular curves $E, E'/\mathbb{F}_{p^2}$, for distinct primes p, ℓ.
- Computing such an isogeny amounts to path finding in supersingular isogeny graphs.

Supersingular isogeny graphs

Let $\Phi_\ell(X, Y)$ be the ℓth modular polynomial.

Definition

Let p, ℓ be distinct primes. The graph $G(p, \ell)$ has as its vertices supersingular j-invariants, and the number of edges from j to j' is the multiplicity of j' as a root of $\Phi_\ell(j, Y)$.

Supersingular isogeny graphs

Let $\Phi_\ell(X, Y)$ be the ℓth modular polynomial.

Definition

Let p, ℓ be distinct primes. The graph $G(p, \ell)$ has as its vertices supersingular j-invariants, and the number of edges from j to j' is the multiplicity of j' as a root of $\Phi_\ell(j, Y)$.

Another way to think about $G(p, \ell)$:

- vertices are a complete set of representaives of the isomorphism classes of supersingular elliptic curves,

Supersingular isogeny graphs

Let $\Phi_\ell(X, Y)$ be the ℓth modular polynomial.

Definition

Let p, ℓ be distinct primes. The graph $G(p, \ell)$ has as its vertices supersingular j-invariants, and the number of edges from j to j' is the multiplicity of j' as a root of $\Phi_\ell(j, Y)$.

Another way to think about $G(p, \ell)$:

- vertices are a complete set of representaives of the isomorphism classes of supersingular elliptic curves,
- the edges from E to E' are ℓ-isogenies $\phi : E \to E'$

Supersingular isogeny graphs

Let $\Phi_\ell(X, Y)$ be the ℓth modular polynomial.

Definition

Let p, ℓ be distinct primes. The graph $G(p, \ell)$ has as its vertices supersingular j-invariants, and the number of edges from j to j' is the multiplicity of j' as a root of $\Phi_\ell(j, Y)$.

Another way to think about $G(p, \ell)$:

- vertices are a complete set of representaives of the isomorphism classes of supersingular elliptic curves,
- the edges from E to E' are ℓ-isogenies $\phi : E \to E'$
- (we identify two isogenies ϕ_1, ϕ_2 if $\phi_1 = u \circ \phi_2$ for some $u \in \mathrm{Aut}(E')$.)

Properties of $G(p, \ell)$

- $G(p, \ell)$ has $O(p)$ vertices, and every vertex has out-degree $\ell + 1$

Properties of $G(p, \ell)$

- $G(p, \ell)$ has $O(p)$ vertices, and every vertex has out-degree $\ell + 1$
- $G(p, \ell)$ is connected and its diameter is $O(\log p)$

Properties of $G(p, \ell)$

- $G(p, \ell)$ has $O(p)$ vertices, and every vertex has out-degree $\ell + 1$
- $G(p, \ell)$ is connected and its diameter is $O(\log p)$
- If $p \equiv 1 \pmod{12}$, the graph is an undirected $(\ell + 1)$-regular Ramanujan graph

Properties of $G(p, \ell)$

- $G(p, \ell)$ has $O(p)$ vertices, and every vertex has out-degree $\ell + 1$
- $G(p, \ell)$ is connected and its diameter is $O(\log p)$
- If $p \equiv 1 \pmod{12}$, the graph is an undirected $(\ell + 1)$-regular Ramanujan graph

Pathfinding in $G(p, \ell)$ is equivalent to computing an ℓ-power isogeny between two given supersingular elliptic curves.

The isogeny graph $G(157, 3)$

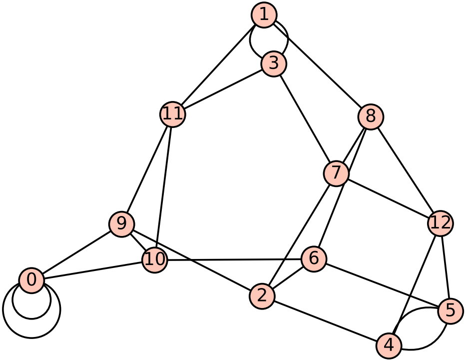


Figure: $G(157, 3)$

Pathfinding in $G(p, \ell)$ and computing endomorphisms

Kohel gave an algorithm which, given a supersingular elliptic curve $E/\mathbb{F}_{p^2}$, computes an order $\Lambda \subseteq \mathrm{End}(E)$.

Pathfinding in $G(p, \ell)$ and computing endomorphisms

Kohel gave an algorithm which, given a supersingular elliptic curve $E/\mathbb{F}_{p^2}$, computes an order $\Lambda \subseteq \mathrm{End}(E)$.

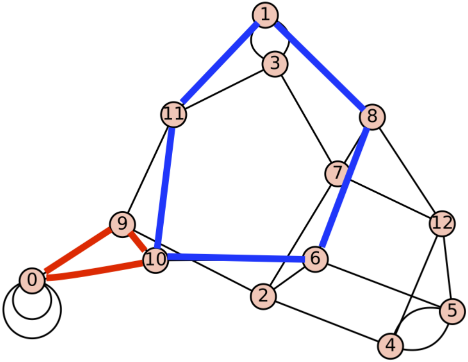


Figure: $\langle 1, \alpha, \beta, \alpha\beta \rangle = \Lambda \subseteq \mathrm{End}(E)$ is an order

Computing isogenies and endomorphism rings

- Pathfinding in $G(p, \ell)$ lets one compute endomorphisms of supersingular elliptic curves.

Computing isogenies and endomorphism rings

- Pathfinding in $G(p, \ell)$ lets one compute endomorphisms of supersingular elliptic curves.
- Conversely, pathfinding in $G(p, \ell)$ reduces to the problem of computing endomorphism rings.

Computing isogenies and endomorphism rings

- Pathfinding in $G(p, \ell)$ lets one compute endomorphisms of supersingular elliptic curves.
- Conversely, pathfinding in $G(p, \ell)$ reduces to the problem of computing endomorphism rings.

Theorem (Eisenträger, Hallgren, Lauter, M-, Petit)

Assume $\ell = O(\log p)$. Then there are polynomial-time (in $\log p$) reductions between the problem of pathfinding in $G(p, \ell)$ and computing endomorphism rings of supersingular elliptic curves, assuming some heuristics.

Quaternion algebras

- Every *quaternion algebra over* $\mathbb{Q}$ is of the form, for some $a, b \in \mathbb{Q}^\times$,

$$H(a, b) := \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}ij$$

where $i^2 = a, j^2 = b$, and $ij = -ji$.

Quaternion algebras

- Every *quaternion algebra over* $\mathbb{Q}$ is of the form, for some $a, b \in \mathbb{Q}^\times$,

$$H(a,b) := \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}ij$$

  where $i^2 = a, j^2 = b$, and $ij = -ji$.
- $H(a,b)$ has an *involution* sending

$$\alpha = w + xi + yj + ziz \mapsto \overline{\alpha} := w - xi - yj - zij.$$

  This lets us define the *reduced norm* and *reduced trace* of an element α:

$$\begin{aligned} \operatorname{nrd}(\alpha) &:= \alpha\overline{\alpha} = w^2 - ax^2 - by^2 + abz^2 \\ \operatorname{trd}(\alpha) &:= \alpha + \overline{\alpha} = 2w. \end{aligned}$$

Let $B/\mathbb{Q}$ be a quaternion algebra and let v be a place of $\mathbb{Q}$. Let H_v be the 4-dimensional division algebra over $\mathbb{Q}_v$.

$$B \otimes \mathbb{Q}_v \simeq \begin{cases} M_2(\mathbb{Q}_v) & \text{we say } B \text{ is } \textit{split} \text{ at } v \\ H_v & \text{we say } B \text{ is } \textit{ramified} \text{ at } v. \end{cases}$$

Let $B/\mathbb{Q}$ be a quaternion algebra and let v be a place of $\mathbb{Q}$. Let H_v be the 4-dimensional division algebra over $\mathbb{Q}_v$.

$$B \otimes \mathbb{Q}_v \simeq \begin{cases} M_2(\mathbb{Q}_v) & \text{we say } B \text{ is } \textit{split} \text{ at } v \\ H_v & \text{we say } B \text{ is } \textit{ramified} \text{ at } v. \end{cases}$$

For example:

- $H(-1,-1)$ is ramified at $\{2,\infty\}$.
- Let $p \equiv 3 \pmod 4$ be a prime. Then $H(-1,-p)$ is ramified at $\{p,\infty\}$.

The endomorphism algebra

Again, let k be a finite field, $\mathrm{char}(K) = p > 3$.

- Assume E/k is supersingular. Then $\mathrm{End}(E) \otimes \mathbb{Q}$ is a quaternion algebra ramified exactly at $\{p, \infty\}$, and the standard involution is given by taking duals, so $\mathrm{nrd} = \deg$.

The endomorphism algebra

Again, let k be a finite field, $\mathrm{char}(K) = p > 3$.

- Assume E/k is supersingular. Then $\mathrm{End}(E) \otimes \mathbb{Q}$ is a quaternion algebra ramified exactly at $\{p, \infty\}$, and the standard involution is given by taking duals, so $\mathrm{nrd} = \deg$.
- We can say more: $\mathrm{End}(E)$ is a maximal order in $\mathrm{End}(E) \otimes \mathbb{Q}$.

The endomorphism algebra

Again, let k be a finite field, $\mathrm{char}(K) = p > 3$.

- Assume E/k is supersingular. Then $\mathrm{End}(E) \otimes \mathbb{Q}$ is a quaternion algebra ramified exactly at $\{p, \infty\}$, and the standard involution is given by taking duals, so $\mathrm{nrd} = \deg$.
- We can say more: $\mathrm{End}(E)$ is a maximal order in $\mathrm{End}(E) \otimes \mathbb{Q}$.
- If E/k is ordinary, $\mathrm{End}(E)$ is a quadratic (but not necessarily maximal) order in its endomorphism algebra, a quadratic imaginary extension of $\mathbb{Q}$

An example

Let $p \equiv 3 \pmod 4$ be a prime. Let $E/\mathbb{F}_p$ be the elliptic curve $E : y^2 = x^3 + x$. We have the endomorphisms

$$\begin{aligned} \phi &: (x, y) \mapsto (-x, \sqrt{-1}y) \\ \pi &: (x, y) \mapsto (x^p, y^p). \end{aligned}$$

- The map $\phi \mapsto i$, $\pi \mapsto j$ extends linearly to an isomorphism of quaternion algebras $\mathrm{End}(E) \otimes \mathbb{Q} \simeq H(-1, -p)$.
- However: $\langle 1, \phi, \pi, \phi\pi \rangle \subsetneq \mathrm{End}(E)$.

Arithmetic of endomorphism rings and isogenies

Work of Waterhouse connects the arithmetic of $\mathrm{End}(E)$ to isogenies $\phi : E \to E'$. Let $E/\mathbb{F}_{p^2}$ be supersingular.

Arithmetic of endomorphism rings and isogenies

Work of Waterhouse connects the arithmetic of $\mathrm{End}(E)$ to isogenies $\phi : E \to E'$. Let $E/\mathbb{F}_{p^2}$ be supersingular.

- Suppose that $\phi : E \to E'$ is an isogeny. Then

$$\begin{aligned} \iota : \mathrm{End}(E') &\hookrightarrow \mathrm{End}(E) \otimes \mathbb{Q} \\ \rho &\mapsto \left(\widehat{\phi} \circ \rho \circ \phi\right) \otimes \frac{1}{\deg \phi} \end{aligned}$$

  embeds $\mathrm{End}(E')$ as a maximal order in $\mathrm{End}(E) \otimes \mathbb{Q}$.

Arithmetic of endomorphism rings and isogenies

Work of Waterhouse connects the arithmetic of $\mathrm{End}(E)$ to isogenies $\phi : E \to E'$. Let $E/\mathbb{F}_{p^2}$ be supersingular.

- Suppose that $\phi : E \to E'$ is an isogeny. Then

$$\begin{aligned}\iota : \mathrm{End}(E') &\hookrightarrow \mathrm{End}(E) \otimes \mathbb{Q} \\ \rho &\mapsto \left(\widehat{\phi} \circ \rho \circ \phi\right) \otimes \frac{1}{\deg \phi}\end{aligned}$$

  embeds $\mathrm{End}(E')$ as a maximal order in $\mathrm{End}(E) \otimes \mathbb{Q}$.
- Set $I := \{\alpha \in \mathrm{End}(E) : \alpha(\ker \phi) = \{0\}\}$. This is a left ideal of $\mathrm{End}(E)$, and $\deg(\phi) = \mathrm{nrd}(I)$.

Arithmetic of endomorphism rings and isogenies

Work of Waterhouse connects the arithmetic of $\mathrm{End}(E)$ to isogenies $\phi : E \to E'$. Let $E/\mathbb{F}_{p^2}$ be supersingular.

- Suppose that $\phi : E \to E'$ is an isogeny. Then

$$\begin{aligned} \iota : \mathrm{End}(E') &\hookrightarrow \mathrm{End}(E) \otimes \mathbb{Q} \\ \rho &\mapsto \left(\widehat{\phi} \circ \rho \circ \phi\right) \otimes \frac{1}{\deg \phi} \end{aligned}$$

  embeds $\mathrm{End}(E')$ as a maximal order in $\mathrm{End}(E) \otimes \mathbb{Q}$.
- Set $I := \{\alpha \in \mathrm{End}(E) : \alpha(\ker \phi) = \{0\}\}$. This is a left ideal of $\mathrm{End}(E)$, and $\deg(\phi) = \mathrm{nrd}(I)$.
- Then $\mathrm{End}(E')$ is isomorphic to the *right order of* I:

$$\mathcal{O}_R(I) := \{\gamma \in \mathrm{End}(E) \otimes \mathbb{Q} : I\gamma \subseteq I\} = \iota(\mathrm{End}(E'))$$

Arithmetic of endomorphism rings and isogenies

- Conversely, given a left ideal $I \subseteq \text{End}(E)$ such that $\text{nrd}(I)$ is coprime to p, define

$$E[I] := \bigcap_{\alpha \in I} \ker \alpha.$$

Arithmetic of endomorphism rings and isogenies

- Conversely, given a left ideal $I \subseteq \mathrm{End}(E)$ such that $\mathrm{nrd}(I)$ is coprime to p, define

$$E[I] := \bigcap_{\alpha \in I} \ker \alpha.$$

- $E[I]$ is a finite subgroup of $E(\overline{\mathbb{F}_{p^2}})$ and thus determines an isogeny

$$\phi_I : E \to E_I := E/E[I].$$

Arithmetic of endomorphism rings and isogenies

- Conversely, given a left ideal $I \subseteq \mathrm{End}(E)$ such that $\mathrm{nrd}(I)$ is coprime to p, define

$$E[I] := \bigcap_{\alpha \in I} \ker \alpha.$$

- $E[I]$ is a finite subgroup of $E(\overline{\mathbb{F}_{p^2}})$ and thus determines an isogeny

$$\phi_I : E \to E_I := E/E[I].$$

- We have $\mathrm{nrd}(I) = |E[I]| = \deg(\phi_I)$.

Computing ℓ-power isogenies

Problem

Given distinct primes p, ℓ and supersingular elliptic curves $E/\mathbb{F}_{p^2}$ and $E'/\mathbb{F}_{p^2}$, compute an isogeny $\phi : E \to E'$ whose degree is ℓ^e for some e.

Computing ℓ-power isogenies

Problem

Given distinct primes p, ℓ and supersingular elliptic curves $E/\mathbb{F}_{p^2}$ and $E'/\mathbb{F}_{p^2}$, compute an isogeny $\phi : E \to E'$ whose degree is ℓ^e for some e.

- This problem can return an isogeny of size polynomial in $\log p$ if $\ell = O(\log p)$: we can represent ϕ by a sequence of ℓ-isogenies, and the diameter of $G(p, \ell)$ is $O(\log p)$.
- This is the problem of pathfinding in $G(p, \ell)$.

Computing endomorphism rings

We can interpret the problem of "computing the endomorphism ring" in different ways: for example, we could ask for the geometric object $\mathrm{End}(E)$. We will simply ask for an order in $B_{p,\infty}$ isomorphic to $\mathrm{End}(E)$. Here $B_{p,\infty}$ denotes the quaternion algebra ramified at $\{p, \infty\}$.

Computing endomorphism rings

We can interpret the problem of "computing the endomorphism ring" in different ways: for example, we could ask for the geometric object $\mathrm{End}(E)$. We will simply ask for an order in $B_{p,\infty}$ isomorphic to $\mathrm{End}(E)$. Here $B_{p,\infty}$ denotes the quaternion algebra ramified at $\{p, \infty\}$.

Problem

Given a supersingular elliptic curve $E/\mathbb{F}_{p^2}$, compute an order $\mathcal{O} \subseteq B_{p,\infty}$ such that $End(E) \simeq \mathcal{O}$.

Computing endomorphism rings

We can interpret the problem of "computing the endomorphism ring" in different ways: for example, we could ask for the geometric object $\mathrm{End}(E)$. We will simply ask for an order in $B_{p,\infty}$ isomorphic to $\mathrm{End}(E)$. Here $B_{p,\infty}$ denotes the quaternion algebra ramified at $\{p, \infty\}$.

Problem

Given a supersingular elliptic curve $E/\mathbb{F}_{p^2}$, compute an order $\mathcal{O} \subseteq B_{p,\infty}$ such that $End(E) \simeq \mathcal{O}$.

For a polynomial-time reduction from computing isogenies to this problem to make sense, we need to know that such an order $\mathcal{O}$ of polynomial size exists.

Endomorphism rings have polynomial size

Theorem (Eisenträger, Hallgren, Lauter, M-, Petit)

Every isomorphism class (i.e. conjugacy class) of maximal orders in $B_{p,\infty}$ contains an order $\mathcal{O}$ of size polynomial in $\log p$.

Endomorphism rings have polynomial size

Theorem (Eisenträger, Hallgren, Lauter, M-, Petit)

Every isomorphism class (i.e. conjugacy class) of maximal orders in $B_{p,\infty}$ contains an order $\mathcal{O}$ of size polynomial in $\log p$.

Sketch of proof:

- Pizer shows $B_{p,\infty}$ and at least one maximal order $\mathcal{O}_0 \subseteq B_{p,\infty}$ have polynomial in $\log p$ size

Endomorphism rings have polynomial size

Theorem (Eisenträger, Hallgren, Lauter, M-, Petit)

Every isomorphism class (i.e. conjugacy class) of maximal orders in $B_{p,\infty}$ contains an order $\mathcal{O}$ of size polynomial in $\log p$.

Sketch of proof:

- Pizer shows $B_{p,\infty}$ and at least one maximal order $\mathcal{O}_0 \subseteq B_{p,\infty}$ have polynomial in $\log p$ size
- The map $[I] \mapsto [\mathcal{O}_R(I)]$ from left ideal classes of $\mathcal{O}$ to isomorphism classes of maximal orders is surjective

Endomorphism rings have polynomial size

Theorem (Eisenträger, Hallgren, Lauter, M-, Petit)

Every isomorphism class (i.e. conjugacy class) of maximal orders in $B_{p,\infty}$ contains an order $\mathcal{O}$ of size polynomial in $\log p$.

Sketch of proof:

- Pizer shows $B_{p,\infty}$ and at least one maximal order $\mathcal{O}_0 \subseteq B_{p,\infty}$ have polynomial in $\log p$ size
- The map $[I] \mapsto [\mathcal{O}_R(I)]$ from left ideal classes of $\mathcal{O}$ to isomorphism classes of maximal orders is surjective
- Every left ideal class contains a representative J such that $\mathrm{nrd}(J) = O(p^2)$

Almost equivalent problems, categorically

Let $B_{p,\infty}$ be the quaternion algebra over $\mathbb{Q}$ ramified at $\{p, \infty\}$.

Problem

Let $\mathcal{O}, \mathcal{O}' \subseteq B_{p,\infty}$ be maximal orders. Let $\ell \neq p$ be a prime. Compute a left ideal $I \subseteq \mathcal{O}$ such that $\mathcal{O}_R(I) \simeq \mathcal{O}'$.

- If $\mathcal{O}, \mathcal{O}'$ have size polynomial in $\log p$, and $\ell = O(\log p)$, then an algorithm of Kohel-Lauter-Petit-Tignol solves this problem in time polynomial in $\log p$
- Why almost? If $E/\overline{\mathbb{F}_p}, E'/\overline{\mathbb{F}_p}$ are supersingular, then $\mathrm{End}(E) \simeq \mathrm{End}(E')$ if and only if $j(E)^p = j(E')$.

Computing isogenies reduces to computing endomorphism rings

Assume we have an oracle which, on input $E/\mathbb{F}_{p^2}$ supersingular, computes a maximal order $\mathcal{O} \subset B_{p,\infty}$ such that $\mathcal{O} \simeq \mathrm{End}(E)$. Suppose we are given two supersingular elliptic curves $E, E'/\mathbb{F}_{p^2}$ and a prime $\ell = O(\log p)$. We sketch an algorithm for computing an ℓ-power isogeny $\phi : E \to E'$.

Computing isogenies reduces to computing endomorphism rings

1. Compute $\mathcal{O} \simeq \mathrm{End}(E), \mathcal{O}' \simeq \mathrm{End}(E')$

Computing isogenies reduces to computing endomorphism rings

1. Compute $\mathcal{O} \simeq \mathrm{End}(E), \mathcal{O}' \simeq \mathrm{End}(E')$
2. Compute a left ideal $I \subseteq \mathcal{O}$ such that $\mathcal{O}_R(I) \simeq \mathcal{O}'$, $\mathrm{nrd}(I) = \ell^e$ using KLPT

Computing isogenies reduces to computing endomorphism rings

1. Compute $\mathcal{O} \simeq \mathrm{End}(E), \mathcal{O}' \simeq \mathrm{End}(E')$
2. Compute a left ideal $I \subseteq \mathcal{O}$ such that $\mathcal{O}_R(I) \simeq \mathcal{O}'$, $\mathrm{nrd}(I) = \ell^e$ using KLPT
3. Compute the ideals $I_k := I + \ell^k \mathcal{O}$; $\mathrm{nrd}(I_k) = \ell^k$.

Computing isogenies reduces to computing endomorphism rings

1. Compute $\mathcal{O} \simeq \mathrm{End}(E), \mathcal{O}' \simeq \mathrm{End}(E')$
2. Compute a left ideal $I \subseteq \mathcal{O}$ such that $\mathcal{O}_R(I) \simeq \mathcal{O}'$, $\mathrm{nrd}(I) = \ell^e$ using KLPT
3. Compute the ideals $I_k := I + \ell^k \mathcal{O}$; $\mathrm{nrd}(I_k) = \ell^k$.
4. Compute the orders $\mathcal{O}_k := \mathcal{O}_R(I_k)$

Computing isogenies reduces to computing endomorphism rings

1. Compute $\mathcal{O} \simeq \mathrm{End}(E), \mathcal{O}' \simeq \mathrm{End}(E')$
2. Compute a left ideal $I \subseteq \mathcal{O}$ such that $\mathcal{O}_R(I) \simeq \mathcal{O}'$, $\mathrm{nrd}(I) = \ell^e$ using KLPT
3. Compute the ideals $I_k := I + \ell^k\mathcal{O}$; $\mathrm{nrd}(I_k) = \ell^k$.
4. Compute the orders $\mathcal{O}_k := \mathcal{O}_R(I_k)$

Computing isogenies reduces to computing endomorphism rings

1. Compute $\mathcal{O} \simeq \mathrm{End}(E), \mathcal{O}' \simeq \mathrm{End}(E')$
2. Compute a left ideal $I \subseteq \mathcal{O}$ such that $\mathcal{O}_R(I) \simeq \mathcal{O}'$, $\mathrm{nrd}(I) = \ell^e$ using KLPT
3. Compute the ideals $I_k := I + \ell^k\mathcal{O}$; $\mathrm{nrd}(I_k) = \ell^k$.
4. Compute the orders $\mathcal{O}_k := \mathcal{O}_R(I_k)$

Now we want to translate the orders $\mathcal{O}_k$ into a sequence of ℓ-isogenies.

Translating $\mathcal{O}_1, \ldots, \mathcal{O}_e$ to isogenies

E $\qquad\qquad\qquad\qquad$ E_I

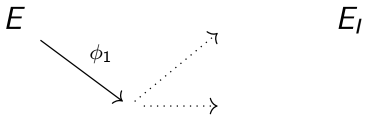
Translating $\mathcal{O}_1, \ldots, \mathcal{O}_e$ to isogenies

- At step k, we compute the neighbors

Translating $\mathcal{O}_1, \ldots, \mathcal{O}_e$ to isogenies

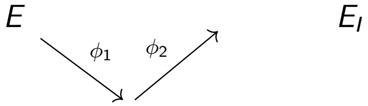
- At step k, we compute the neighbors
- Then we check which neighbor's endomorphism ring is isomorphic to $\mathcal{O}_R(I_k)$

Translating $\mathcal{O}_1, \ldots, \mathcal{O}_e$ to isogenies



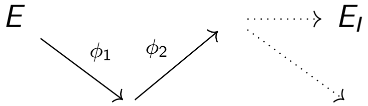
- At step k, we compute the neighbors
- Then we check which neighbor's endomorphism ring is isomorphic to $\mathcal{O}_R(I_k)$

Translating $\mathcal{O}_1, \ldots, \mathcal{O}_e$ to isogenies



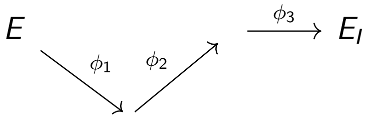
- At step k, we compute the neighbors
- Then we check which neighbor's endomorphism ring is isomorphic to $\mathcal{O}_R(I_k)$

Translating $\mathcal{O}_1, \ldots, \mathcal{O}_e$ to isogenies



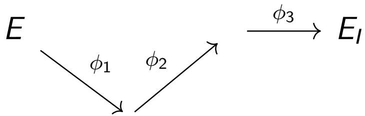
- At step k, we compute the neighbors
- Then we check which neighbor's endomorphism ring is isomorphic to $\mathcal{O}_R(I_k)$

Translating $\mathcal{O}_1, \ldots, \mathcal{O}_e$ to isogenies



- At step k, we compute the neighbors
- Then we check which neighbor's endomorphism ring is isomorphic to $\mathcal{O}_R(I_k)$

Translating $\mathcal{O}_1, \ldots, \mathcal{O}_e$ to isogenies



- At step k, we compute the neighbors
- Then we check which neighbor's endomorphism ring is isomorphic to $\mathcal{O}_R(I_k)$
- Return the sequence of isogenies $\phi_1, \ldots, \phi_e$.

One issue: let $\phi_I : E \to E_I$ be the isogeny corresponding to the path in $G(p, \ell)$ constructed in the reduction. We have $\mathrm{End}(E_I) \simeq \mathrm{End}(E')$, but it could be that $E_I \simeq (E')^{(p)}$ (i.e. $j(E_I)^p = j(E') \neq j(E_I)$).

One issue: let $\phi_I : E \to E_I$ be the isogeny corresponding to the path in $G(p, \ell)$ constructed in the reduction. We have $\mathrm{End}(E_I) \simeq \mathrm{End}(E')$, but it could be that $E_I \simeq (E')^{(p)}$ (i.e. $j(E_I)^p = j(E') \neq j(E_I)$).

- In this case, we replace I with $I \cdot P$, where $P \subseteq \mathcal{O}_R(I)$ is the unique 2-sided ideal of norm p.

One issue: let $\phi_I : E \to E_I$ be the isogeny corresponding to the path in $G(p, \ell)$ constructed in the reduction. We have $\mathrm{End}(E_I) \simeq \mathrm{End}(E')$, but it could be that $E_I \simeq (E')^{(p)}$ (i.e. $j(E_I)^p = j(E') \neq j(E_I)$).

- In this case, we replace I with $I \cdot P$, where $P \subseteq \mathcal{O}_R(I)$ is the unique 2-sided ideal of norm p.
- Compute an ideal of ℓ-power norm equivalent to IP and repeat the algorithm.

Thank you!