Computing isogenies and endomorphism rings of supersingular elliptic curves

Travis Morrison

University of Waterloo

AMS Special Session on the Mathematics of Cryptography
March 23rd, 2019
Elliptic Curve Diffie-Hellman

- Alice and Bob want to compute a shared secret.

They agree on a public elliptic curve $E/F_p$ and a point $P \in E(F_p)$.

Alice chooses an integer $A$ as her private key, and Bob chooses $B$ as his private key.

$[A]P \cdot P \cdot [AB]P = [BA]P \cdot [B]P$
Elliptic Curve Diffie-Hellman

- Alice and Bob want to compute a shared secret.
- They agree on a public elliptic curve $E / \mathbb{F}_p$ and a point $P \in E(\mathbb{F}_p)$.

$[A]P \cdot [AB]P = [BA]P \cdot [B]P$
Elliptic Curve Diffie-Hellman

- Alice and Bob want to compute a shared secret.
- They agree on a public elliptic curve $E/\mathbb{F}_p$ and a point $P \in E(\mathbb{F}_p)$.
- Alice chooses an integer $A$ as her private key, and Bob chooses $B$ as his private key.

\[
\begin{align*}
[A]P = [A]P \\
[B]P \\
[A]P \quad [AB]P = [BA]P \\
[B]P \\
P
\end{align*}
\]
ECDH vs a quantum computer


- Shor's algorithm is a quantum algorithm which efficiently solves this problem!

- Elliptic curve cryptography is insecure in a "post-quantum" world
ECDH vs a quantum computer

- Shor’s algorithm is a quantum algorithm which efficiently solves this problem!
ECDH vs a quantum computer

- Shor’s algorithm is a quantum algorithm which efficiently solves this problem!
- Elliptic curve cryptography is insecure in a “post-quantum” world
(Supersingular) Isogeny Diffie-Hellman

- Alice and Bob want to compute a shared secret. They agree on a public (supersingular) elliptic curve $E/\mathbb{F}_{p^2}$. 

Alice and Bob want to compute a shared secret. They agree on a public (supersingular) elliptic curve $E/F_{p^2}$. Alice chooses a cyclic subgroup $A \subseteq E(F_{p^2})$ as her private key, and Bob chooses $B \subseteq E(F_{p^2})$ as his private key.
(Supersingular) Isogeny Diffie-Hellman

- Alice and Bob want to compute a shared secret. They agree on a public (supersingular) elliptic curve $E/\mathbb{F}_{p^2}$.
- Alice chooses a cyclic subgroup $A \subseteq E(\mathbb{F}_{p^2})$ as her private key, and Bob chooses $B \subseteq E(\mathbb{F}_{p^2})$ as his private key.
A private key in SIDH or the CGL hash is an $\ell$-power isogeny $\phi : E \rightarrow E'$ between two supersingular curves $E, E'/\mathbb{F}_{p^2}$, for distinct primes $p, \ell$. 
SIDH and the CGL hash function

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

**Definition**

$E/k$ is *supersingular* if its endomorphism algebra

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

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 $\mathbb{F}_p$ is in $\mathbb{F}_p^2$. 

▶ There are $\lfloor \frac{p-1}{12} \rfloor + \epsilon$ supersingular $j$-invariants in $\mathbb{F}_p^2$, where $\epsilon \in \{0, 1, 2\}$. 


Supersingular elliptic curves

**Definition**

$E/k$ is *supersingular* if its endomorphism algebra

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

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 $\mathbb{F}_p$ is in $\mathbb{F}_{p^2}$.
Supersingular elliptic curves

**Definition**

\( E/k \) is *supersingular* if its endomorphism algebra

\[ B := \text{End}(E) \otimes \mathbb{Q} \]

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 \( \left\lfloor \frac{p-1}{12} \right\rfloor + \epsilon \) supersingular \( j \)-invariants in \( \mathbb{F}_{p^2} \), where \( \epsilon \in \{0, 1, 2\} \).
Supersingular isogeny graphs

Let $\Phi_\ell(X, Y)$ be the $\ell$th modular polynomial.
Supersingular isogeny graphs

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

**Definition**

Let $p, \ell$ 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 $\ell$th modular polynomial.

**Definition**

Let $p, \ell$ 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 $\Phi_\ell(j, Y)$.

How to think about $G(p, \ell)$:
Supersingular isogeny graphs

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

**Definition**

Let $p, \ell$ 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 $\Phi_\ell(j, Y)$.

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

- vertices are a complete set of representatives of the isomorphism classes of supersingular elliptic curves,
Supersingular isogeny graphs

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

**Definition**

Let $p, \ell$ 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 $\Phi_\ell(j, Y)$.

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

- vertices are a complete set of representatives of the isomorphism classes of supersingular elliptic curves,
- the edges from $E$ to $E'$ are $\ell$-isogenies $\phi : E \to E'$
Supersingular isogeny graphs

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

**Definition**

Let $p, \ell$ 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 $\Phi_\ell(j, Y)$.

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

- vertices are a complete set of representatives of the isomorphism classes of supersingular elliptic curves,
- the edges from $E$ to $E'$ are $\ell$-isogenies $\phi: E \to E'$
- (we identify two isogenies $\phi_1, \phi_2$ if $\phi_1 = u \circ \phi_2$ for some $u \in \text{Aut}(E')$. )
The isogeny graph $G(157, 3)$

Figure: $G(157, 3)$
Computing isogenies and endomorphism rings

- Computing cycles in $G(p, \ell)$ yield endomorphisms of supersingular elliptic curves.
Computing isogenies and endomorphism rings

- Computing cycles in $G(p, \ell)$ yield 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.
Computing isogenies and endomorphism rings

- Computing cycles in $G(p, \ell)$ yield 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.
An example

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

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

The map $\phi \mapsto i, \pi \mapsto j$ extends linearly to an isomorphism of quaternion algebras

$$\text{End}(E) \otimes \mathbb{Q} \simeq H(-1, -p).$$

However: $\langle 1, \phi, \pi, \phi \pi \rangle \subset \text{End}(E)$. 
Computing $\ell$-power isogenies

**Problem**

Given distinct primes $p, \ell$ 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 $\ell^e$ for some $e$. 

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

This is the problem of pathfinding in $G(p, \ell)$. 

Computing $\ell$-power isogenies

Problem

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

- This problem can return an isogeny of size polynomial in $\log p$ if $\ell = O(\log p)$: we can represent $\phi$ by a sequence of $\ell$-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:

- We could ask for the geometric object, i.e. given by actual endomorphisms $\text{End}(E)$. 

Computing endomorphism rings

We can interpret the problem of “computing the endomorphism ring” in different ways:

- We could ask for the geometric object, i.e. given by actual endomorphisms $\text{End}(E)$.
- Or the algebraic object: an order in $B_{p,\infty}$ isomorphic to $\text{End}(E)$. 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 $O \subseteq B_{p,\infty}$ such that $\text{End}(E) \cong O$. 

Computing endomorphism rings

We can interpret the problem of “computing the endomorphism ring” in different ways:

- We could ask for the geometric object, i.e. given by actual endomorphisms $\text{End}(E)$.
- Or the algebraic object: an order in $B_{p,\infty}$ isomorphic to $\text{End}(E)$. 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 $\text{End}(E) \simeq \mathcal{O}$.***
Endomorphism rings have polynomial size

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

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.

**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 $\log p$.***
Arithmetic of endomorphism rings and isogenies

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

- Suppose that $\phi : E \to E'$ is an isogeny.
Arithmetic of endomorphism rings and isogenies

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

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

  \[ \iota : \text{End}(E') \hookrightarrow \text{End}(E) \otimes \mathbb{Q} \]

  \[ \rho \mapsto \left( \hat{\phi} \circ \rho \circ \phi \right) \otimes \frac{1}{\deg \phi} \]

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

\[ \text{Set} \quad I := \{ \alpha \in \text{End}(E') : \alpha(\ker \phi) = \{0\} \}. \] This is a left ideal of $\text{End}(E')$, and $\deg(\phi) = \text{nrd}(I)$. 

\[ \text{Then} \quad \text{End}(E') \text{ is isomorphic to the right order of } I : \quad \text{OR}(I) := \{ \gamma \in \text{End}(E') \otimes \mathbb{Q} : I \gamma \subseteq I \} = \iota(\text{End}(E')) \]
Arithmetic of endomorphism rings and isogenies

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

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

\[
\iota : \text{End}(E') \hookrightarrow \text{End}(E) \otimes \mathbb{Q}
\]

\[
\rho \mapsto \left( \hat{\phi} \circ \rho \circ \phi \right) \otimes \frac{1}{\deg \phi}
\]

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

- Set \( I := \{ \alpha \in \text{End}(E) : \alpha(\ker \phi) = \{0\} \} \). This is a left ideal of \( \text{End}(E) \), and \( \deg(\phi) = \text{nrd}(I) \).
Arithmetic of endomorphism rings and isogenies

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

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

$$\iota : \text{End}(E') \hookrightarrow \text{End}(E) \otimes \mathbb{Q}$$

$$\rho \mapsto \left( \hat{\phi} \circ \rho \circ \phi \right) \otimes \frac{1}{\deg(\phi)}$$

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

- Set $I := \{ \alpha \in \text{End}(E) : \alpha(\ker \phi) = \{0\} \}$. This is a left ideal of $\text{End}(E)$, and $\deg(\phi) = \text{nrd}(I)$.

- Then $\text{End}(E')$ is isomorphic to the right order of $I$:

$$\mathcal{O}_R(I) := \{ \gamma \in \text{End}(E) \otimes \mathbb{Q} : I \gamma \subseteq I \} = \iota(\text{End}(E'))$$
Arithmetic of endomorphism rings and isogenies

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

\[
E[I] := \bigcap_{\alpha \in I} \ker \alpha.
\]
Conversely, given a left ideal $I \subseteq \text{End}(E)$ such that $\text{nrd}(I)$ is coprime to $p$, define

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

$E[I]$ 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 $I \subseteq \text{End}(E)$ such that $\text{nrd}(I)$ 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 $\text{nrd}(I) = |E[I]| = \deg(\phi_I)$. 
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 $\mathcal{O} \simeq \text{End}(E)$. 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 $\ell$-power isogeny $\phi : E \to E'$. 
Computing isogenies reduces to computing endomorphism rings

Given $E, E'$:

1. Call oracle for $\mathcal{O} \simeq \text{End}(E), \mathcal{O}' \simeq \text{End}(E')$
Computing isogenies reduces to computing endomorphism rings

Given $E, E'$:

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

3. Compute the ideals $I_k := I + \ell^k \mathcal{O}$ for $k = 1, \ldots, e - 1$; $\text{nrd}(I_k) = \ell^k$.

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 $\ell$-isogenies.
Computing isogenies reduces to computing endomorphism rings

Given $E, E'$:

1. Call oracle for $\mathcal{O} \simeq \text{End}(E), \mathcal{O}' \simeq \text{End}(E')$
2. Compute a left ideal $I \subseteq \mathcal{O}$ such that $\mathcal{O}_R(I) \simeq \mathcal{O}'$, $\text{nrd}(I) = \ell^e$ using KLPT
3. Compute the ideals $I_k := I + \ell^k \mathcal{O}$ for $k = 1, \ldots, e - 1$; $\text{nrd}(I_k) = \ell^k$. 
Computing isogenies reduces to computing endomorphism rings

Given $E, E'$:
1. Call oracle for $\mathcal{O} \cong \text{End}(E), \mathcal{O}' \cong \text{End}(E')$
2. Compute a left ideal $I \subseteq \mathcal{O}$ such that $\mathcal{O}_R(I) \cong \mathcal{O}'$, $\text{nrd}(I) = \ell^e$ using KLPT
3. Compute the ideals $I_k := I + \ell^k \mathcal{O}$ for $k = 1, \ldots, e - 1; \text{nrd}(I_k) = \ell^k$.
4. Compute the orders $\mathcal{O}_k := \mathcal{O}_R(I_k)$
Computing isogenies reduces to computing endomorphism rings

Given \( E, E' \):

1. Call oracle for \( O \simeq \text{End}(E), O' \simeq \text{End}(E') \)
2. Compute a left ideal \( I \subseteq O \) such that \( O_R(I) \simeq O' \), \( \text{nrd}(I) = \ell^e \) using KLPT
3. Compute the ideals \( I_k := I + \ell^k O \) for \( k = 1, \ldots, e - 1 \); \( \text{nrd}(I_k) = \ell^k \).
4. Compute the orders \( O_k := O_R(I_k) \).
Computing isogenies reduces to computing endomorphism rings

Given $E, E'$:

1. Call oracle for $\mathcal{O} \simeq \text{End}(E), \mathcal{O}' \simeq \text{End}(E')$
2. Compute a left ideal $I \subseteq \mathcal{O}$ such that $\mathcal{O}_R(I) \simeq \mathcal{O}'$, $\text{nrd}(I) = \ell^e$ using KLPT
3. Compute the ideals $I_k := I + \ell^k \mathcal{O}$ for $k = 1, \ldots, e - 1$; $\text{nrd}(I_k) = \ell^k$.
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 $\ell$-isogenies.
Translating $\mathcal{O}_1, \ldots, \mathcal{O}_e$ to isogenies

\[ E \quad \quad \quad \quad E_i \]
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 $O_1, \ldots, O_e$ to isogenies

At step $k$, we compute the neighbors

Then we check which neighbor’s endomorphism ring is isomorphic to $O_R(I_k)$
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 $O_1, \ldots, O_e$ to isogenies

At step $k$, we compute the neighbors

Then we check which neighbor's endomorphism ring is isomorphic to $O_R(I_k)$
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 $\phi_1, \ldots, \phi_e$. 

$E \xrightarrow{\phi_1} \xrightarrow{\phi_2} E_1 \xrightarrow{\phi_3}$
Thank you!
One issue with the reduction: let $\phi_I : E \to E_I$ be the isogeny corresponding to the path in $G(p, \ell)$ constructed in the reduction. We have $\operatorname{End}(E_I) \simeq \operatorname{End}(E')$, 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 $I'$ of $\ell$-power norm equivalent to $IP$ and repeat the algorithm with $I'$ in place of $I$. 
One issue with the reduction: let $\phi_I : E \to E_I$ be the isogeny corresponding to the path in $G(p, \ell)$ constructed in the reduction. We have $\text{End}(E_I) \cong \text{End}(E')$, but it could be that $E_I \cong (E')^{(p)}$ (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 with the reduction: let $\phi_I : E \to E_I$ be the isogeny corresponding to the path in $\mathbb{G}(p, \ell)$ constructed in the reduction. We have $\operatorname{End}(E_I) \simeq \operatorname{End}(E')$, 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 $I'$ of $\ell$-power norm equivalent to $IP$ and repeat the algorithm with $I'$ in place of $I$. 
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

$$\phi : E \rightarrow E',$$

defined over $k$, which induces a group homomorphism from $E(k) \rightarrow E'(k)$.

- Every finite subgroup $K \subseteq E(k)$ determines a separable isogeny $\phi : E \rightarrow E/K$, unique up to isomorphism
The endomorphism ring

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

$$[n] : E \to E$$

$$P \mapsto P + \cdots + P$$

$n$ times

is an endomorphism of $E$. 
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

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

This lets us define the reduced norm and reduced trace of an element $\alpha$:

$$\text{nrd}(\alpha) := \alpha \overline{\alpha} = w^2 - ax^2 - by^2 + abz^2$$
$$\text{trd}(\alpha) := \alpha + \overline{\alpha} = 2w.$$
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 $\mathbb{Q}_v$.

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

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 $\{p, \infty\}$.


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 $\mathbb{Q}_v$.

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

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 $\{p, \infty\}$. 
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 $\ell$-power isogeny between two given supersingular elliptic curves.
Let $k$ be a finite field, $\text{char}(k) = p > 3$.

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

- In fact, $\text{End}(E)$ is a maximal order in $\text{End}(E) \otimes \mathbb{Q}$. 

- If $E/k$ is ordinary, $\text{End}(E)$ is a quadratic (but not necessarily maximal) order in its endomorphism algebra, a quadratic imaginary extension of $\mathbb{Q}$. 

The endomorphism algebra
The endomorphism algebra

Let $k$ be a finite field, $\text{char}(k) = p > 3$.

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

- In fact, $\text{End}(E)$ is a maximal order in $\text{End}(E) \otimes \mathbb{Q}$. 
The endomorphism algebra

Let $k$ be a finite field, $\text{char}(k) = p > 3$. 

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

In fact, $\text{End}(E)$ is a maximal order in $\text{End}(E) \otimes \mathbb{Q}$.

If $E/k$ is ordinary, $\text{End}(E)$ is a quadratic (but not necessarily maximal) order in its endomorphism algebra, a quadratic imaginary extension of $\mathbb{Q}$.
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 $\Lambda \subseteq \text{End}(E)$. 
Pathfinding in $G(p, \ell)$ and computing endomorphisms

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

Figure: $\langle 1, \alpha, \beta, \alpha\beta \rangle = \Lambda \subseteq \text{End}(E)$ is an order
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 \( \mathcal{O}_R(I) \simeq \mathcal{O}' \) and \( \text{nrd}(I) = \ell^e \) for some \( e \).

- 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 \( \text{End}(E) \simeq \text{End}(E') \) if and only if \( j(E)^p = j(E') \).
Sketch of proof:

Pizer shows $B_p, \infty$ and at least one maximal order $O_0 \subseteq B_p, \infty$ have polynomial in log $p$ size.

The map $[I] \mapsto [O_R(I)]$ from left ideal classes of $O$ to isomorphism classes of maximal orders is surjective.

Every left ideal class contains a representative $J$ such that $\text{nrd}(J) = O(p^2)$. 
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
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.
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 $\text{nrd}(J) = O(p^2)$.