How to not break SIDH  🙁

Chloe Martindale        Lorenz Panny

Technische Universiteit Eindhoven

New York, 1 June 2019
What is this all about?
Diffie–Hellman key exchange ’76

Public parameters:
- a finite group $G$ (traditionally $\mathbb{F}_p^*$, today also elliptic curves)
- an element $g \in G$ of prime order $p$
Diffie–Hellman key exchange ’76

Public parameters:

- a finite group $G$ (traditionally $\mathbb{F}_p^*$, today also elliptic curves)
- an element $g \in G$ of prime order $p$

**Diagram:**

<table>
<thead>
<tr>
<th><strong>Alice</strong></th>
<th>public</th>
<th><strong>Bob</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>$a \xleftarrow{} \text{random} {0...p-1}$</td>
<td></td>
<td>$b \xleftarrow{} \text{random} {0...p-1}$</td>
</tr>
<tr>
<td>$g^a$</td>
<td></td>
<td>$g^b$</td>
</tr>
<tr>
<td>$s := (g^b)^a$</td>
<td></td>
<td>$s := (g^a)^b$</td>
</tr>
</tbody>
</table>
Diffie–Hellman key exchange ’76

Public parameters:

- a finite group $G$ (traditionally $\mathbb{F}_p^*$, today also elliptic curves)
- an element $g \in G$ of prime order $p$

```
Alice

$\overset{\text{random}}{\leftarrow} \{0\ldots p-1\}$

$g^a$

$s := (g^b)^a$

Bob


$\overset{\text{random}}{\leftarrow} \{0\ldots p-1\}$

$g^b$

$s := (g^a)^b$
```

Fundamental reason this works: $\cdot^a$ and $\cdot^b$ are commutative!
Diffie–Hellman key exchange ‘76

Public parameters:

- a finite group $G$ (traditionally $\mathbb{F}_p^*$, today also elliptic curves)
- an element $g \in G$ of prime order $p$

Fundamental reason this works: $\cdot^a$ and $\cdot^b$ are commutative!
Graph walking Diffie–Hellman?

Problem:
It is trivial to find paths (subtract coordinates).
What do?
Graph walking Diffie–Hellman?

Problem:
It is trivial to find paths (subtract coordinates).
What do?
Graph walking Diffie–Hellman?

Problem:
It is trivial to find paths (subtract coordinates). What do?
Graph walking Diffie–Hellman?

Problem:
It is trivial to find paths (subtract coordinates).
What do?
Big picture

- Isogenies are a source of exponentially-sized graphs.
Big picture 🕵️

- Isogenies are a source of exponentially-sized graphs.
- We can walk efficiently on these graphs.

It is easy to construct graphs that satisfy almost all of these — not enough for crypto!
Big picture

- Isogenies are a source of exponentially-sized graphs.
- We can walk efficiently on these graphs.
- Fast mixing: short paths to (almost) all nodes.
Big picture 🤔

- **Isogenies** are a source of exponentially-sized graphs.
- We can walk efficiently on these graphs.
- Fast mixing: short paths to (almost) all nodes.
- No known efficient algorithms to recover paths from endpoints.
Big picture

- **Isogenies** are a source of *exponentially-sized graphs*.
- We can **walk efficiently** on these graphs.
- **Fast mixing**: short paths to (almost) all nodes.
- **No known efficient algorithms to recover paths from endpoints**.
- **Enough structure to navigate** the graph meaningfully.
  That is: some *well-behaved* ‘directions’ to describe paths. More later.
Big picture

- Isogenies are a source of exponentially-sized graphs.
- We can walk efficiently on these graphs.
- Fast mixing: short paths to (almost) all nodes.
- No known efficient algorithms to recover paths from endpoints.
- Enough structure to navigate the graph meaningfully. That is: some well-behaved ‘directions’ to describe paths. More later.

It is easy to construct graphs that satisfy almost all of these — not enough for crypto!
Stand back!

We’re going to do math.
An elliptic curve (modulo details) is given by an equation

\[ E: y^2 = x^3 + ax + b. \]

A point on \( E \) is a solution to this equation or the ‘fake’ point \( \infty \).
An elliptic curve (modulo details) is given by an equation

\[ E: \quad y^2 = x^3 + ax + b. \]

A point on \( E \) is a solution to this equation or the ‘fake’ point \( \infty \).

\( E \) is an abelian group: we can ‘add’ points.

- The neutral element is \( \infty \).
- The inverse of \((x, y)\) is \((x, -y)\).
- The sum of \((x_1, y_1)\) and \((x_2, y_2)\) is
  \[
  (\lambda^2 - x_1 - x_2, \lambda(2x_1 + x_2 - \lambda^2) - y_1)
  \]
  where \( \lambda = \frac{y_2 - y_1}{x_2 - x_1} \) if \( x_1 \neq x_2 \) and \( \lambda = \frac{3x_1^2 + a}{2y_1} \) otherwise.

*do not remember these formulas!*
An isogeny of elliptic curves is a non-zero map $E \to E'$ that is:

- given by rational functions.
- a group homomorphism.

The degree of a separable* isogeny is the size of its kernel.
An isogeny of elliptic curves is a non-zero map $E \to E'$ that is:

- given by rational functions.
- a group homomorphism.

The degree of a separable* isogeny is the size of its kernel.

Example #1: For each $m \neq 0$, the multiplication-by-$m$ map 

$$[m] : E \to E$$

is a degree-$m^2$ isogeny. If $m \neq 0$ in the base field, its kernel is 

$$E[m] \cong \mathbb{Z}/m \times \mathbb{Z}/m.$$
An isogeny of elliptic curves is a non-zero map \( E \to E' \) that is:

- given by rational functions.
- a group homomorphism.

The degree of a separable* isogeny is the size of its kernel.

Example #2: For any \( a \) and \( b \), the map \( \iota: (x, y) \mapsto (-x, \sqrt{-1} \cdot y) \) defines a degree-1 isogeny of the elliptic curves

\[
\{ y^2 = x^3 + ax + b \} \longrightarrow \{ y^2 = x^3 + ax - b \}.
\]

It is an isomorphism; its kernel is \( \{ \infty \} \).
An isogeny of elliptic curves is a non-zero map $E \rightarrow E'$ that is:

- given by rational functions.
- a group homomorphism.

The degree of a separable* isogeny is the size of its kernel.

Example #3: $(x, y) \mapsto \left( \frac{x^3-4x^2+30x-12}{(x-2)^2}, \frac{x^3-6x^2-14x+35}{(x-2)^3} \cdot y \right)$
defines a degree-3 isogeny of the elliptic curves

$$\{y^2 = x^3 + x\} \rightarrow \{y^2 = x^3 - 3x + 3\}$$

over $\mathbb{F}_{71}$. Its kernel is $\{(2, 9), (2, -9), \infty\}$. 
An **isogeny** of elliptic curves is a non-zero map $E \to E'$ that is:
- given by **rational functions**.
- a **group homomorphism**.

The **degree** of a separable* isogeny is the size of its **kernel**.

An **endomorphism** of $E$ is an isogeny $E \to E$, or the zero map. The **ring** of endomorphisms of $E$ is denoted by $\text{End}(E)$. 

---

*Separable isogenies are those that are not ramified, meaning they do not introduce new points of order dividing the characteristic of the base field.
Math slide #2: Isogenies (edges)

An **isogeny** of elliptic curves is a non-zero map $E \to E'$ that is:

- given by **rational functions**.
- a **group homomorphism**.

The **degree** of a separable* isogeny is the size of its **kernel**.

An **endomorphism** of $E$ is an isogeny $E \to E$, or the zero map. The **ring** of endomorphisms of $E$ is denoted by $\text{End}(E)$.

Each isogeny $\varphi : E \to E'$ has a unique **dual isogeny** $\hat{\varphi} : E' \to E$ characterized by $\hat{\varphi} \circ \varphi = \varphi \circ \hat{\varphi} = [\deg \varphi]$. 

---

*Separable isogenies are those for which the kernel is a finite subgroup of $E$. This condition ensures that the isogeny respects the group structure in a way that is analogous to the linear independence of polynomials in field extensions.**
Until now: Everything over the algebraic closure.
For arithmetic, we need to know which fields objects live in.
Math slide #3: Fields of definition

Until now: Everything over the algebraic closure.
For arithmetic, we need to know which fields objects live in.

An elliptic curve/point/isogeny is defined over $k$ if the coefficients of its equation/formula lie in $k$. 
Math slide #3: Fields of definition

Until now: Everything over the algebraic closure.
For arithmetic, we need to know which fields objects live in.

An elliptic curve/point/isogeny is defined over $k$ if the coefficients of its equation/formula lie in $k$.

For $E$ defined over $k$, let $E(k)$ be the points of $E$ defined over $k$. 
For any finite subgroup $G$ of $E$, there exists a unique\(^1\) separable isogeny $\varphi_G : E \to E'$ with kernel $G$.

The curve $E'$ is denoted by $E/G$. (cf. quotient groups)

If $G$ is defined over $k$, then $\varphi_G$ and $E/G$ are also defined over $k$.

\(^1\)(up to isomorphism of $E'$)
For any finite subgroup $G$ of $E$, there exists a unique\(^1\) separable isogeny $\varphi_G : E \to E'$ with kernel $G$.

The curve $E'$ is denoted by $E/G$. (cf. quotient groups)

If $G$ is defined over $k$, then $\varphi_G$ and $E/G$ are also defined over $k$.

Vélu '71:
Formulas for computing $E/G$ and evaluating $\varphi_G$ at a point.
Complexity: $\Theta(#G) \rightsquigarrow$ only suitable for small degrees.

\(^1\)(up to isomorphism of $E'$)
For any finite subgroup $G$ of $E$, there exists a unique\(^1\) separable isogeny $\varphi_G : E \rightarrow E'$ with kernel $G$.

The curve $E'$ is denoted by $E/G$. (cf. quotient groups)

If $G$ is defined over $k$, then $\varphi_G$ and $E/G$ are also defined over $k$.

Vélu '71:
Formulas for computing $E/G$ and evaluating $\varphi_G$ at a point.

Complexity: $\Theta(\#G)$ $\rightsquigarrow$ only suitable for small degrees.

Vélu operates in the field where the points in $G$ live.
$\rightsquigarrow$ need to make sure extensions stay small for desired $\#G$
$\rightsquigarrow$ this is why we use supersingular curves!

\(^{1}\)(up to isomorphism of $E'$)
Let $p$ be a prime, $q$ a power of $p$, and $\ell$ a positive integer $\notin p\mathbb{Z}$.

An elliptic curve $E/\mathbb{F}_q$ is **supersingular** if $p \mid (q + 1 - \#E(\mathbb{F}_q))$.

We care about the cases $\#E(\mathbb{F}_p) = p + 1$ and $\#E(\mathbb{F}_{p^2}) = (p + 1)^2$.

$\rightsquigarrow$ easy way to control the group structure by choosing $p$!
Math slide #5: Supersingular isogeny graphs

Let $p$ be a prime, $q$ a power of $p$, and $\ell$ a positive integer $\notin p\mathbb{Z}$.

An elliptic curve $E/\mathbb{F}_q$ is **supersingular** if $p \mid (q + 1 - \#E(\mathbb{F}_q))$.

We care about the cases $\#E(\mathbb{F}_p) = p + 1$ and $\#E(\mathbb{F}_{p^2}) = (p + 1)^2$.

→ easy way to control the group structure by choosing $p$!

Let $S \not\ni p$ denote a set of prime numbers.

The **supersingular $S$-isogeny graph** over $\mathbb{F}_q$ consists of:

▶ vertices given by isomorphism classes of supersingular elliptic curves,

▶ edges given by equivalence classes\(^1\) of $\ell$-isogenies ($\ell \in S$),

both defined over $\mathbb{F}_q$.

\(^1\)Two isogenies $\varphi: E \to E'$ and $\psi: E \to E''$ are identified if $\psi = \iota \circ \varphi$ for some isomorphism $\iota: E' \to E''$. 

The beauty and the beast

Components of the isogeny graphs look like this:
The beauty and the beast

Components of the isogeny graphs look like this:

\[ S = \{3, 5, 7\}, \quad q = 419 \]
The beauty and the beast

Components of the isogeny graphs look like this:

\[ S = \{3, 5, 7\}, \quad q = 419 \]

\[ S = \{2, 3\}, \quad q = 431^2 \]
The beauty and the beast

At this time, there are **two** distinct families of systems:

\[ q = p \]

**CSIDH** [ˈsiːˌsaɪd]
https://csidh.isogeny.org

\[ q = p^2 \]

**SIDH**
https://sike.org
...we’ll be right back after a short commercial break...

[ˈsɪːˌsɛɪd]

Life’s good at the CSIDH!

→ essentially post-quantum Diffie–Hellman.
...is an efficient commutative group action on an isogeny graph. 
\[ \mapsto \text{essentially post-quantum Diffie–Hellman.} \]
...we’ll be right back after a short commercial break...

Life’s good at the CSIDH!

[ˈsiːˌsaɪd]

...is an efficient commutative group action on an isogeny graph.

⇝ essentially post-quantum Diffie–Hellman.
Now:
SIDH

(...whose name doesn’t allow for nice pictures of beaches...)
With great commutative group action comes great subexponential attack.
With great commutative group action comes great subexponential attack.

- SIDH uses the full $\mathbb{F}_{p^2}$-isogeny graph. No group action!
With great commutative group action comes great subexponential attack.

- SIDH uses the full $\mathbb{F}_{p^2}$-isogeny graph. No group action!
- Problem: also no intrinsic sense of direction.
  
  “It all bloody looks the same!” — a famous isogeny cryptographer

$\leadsto$ need extra information to let Alice & Bob’s walks commute.
SIDH: High-level view

Alice & Bob pick secret subgroups $A$ and $B$ of $E$.

Alice computes $\varphi_A: E \rightarrow E/A$; Bob computes $\varphi_B: E \rightarrow E/B$.

These isogenies correspond to walking on the isogeny graph.

Alice and Bob transmit the values $E/A$ and $E/B$.

Alice somehow obtains $A':=\varphi_B(A)$.

(Similar for Bob.)

They both compute the shared secret $(E/B)/A' \sim = E/\langle A, B \rangle \sim (E/A)/B'$.
SIDH: High-level view

- Alice & Bob pick secret subgroups $A$ and $B$ of $E$.

\[
\begin{array}{c}
E \xrightarrow{\varphi_A} E/A \\
\downarrow \varphi_B \downarrow \varphi_{B'} \\
E/B \xrightarrow{\varphi_{A'}} E/\langle A, B \rangle
\end{array}
\]
SIDH: High-level view

- Alice & Bob pick secret subgroups $A$ and $B$ of $E$.
- Alice computes $\varphi_A : E \to E/A$; Bob computes $\varphi_B : E \to E/B$.
  (These isogenies correspond to walking on the isogeny graph.)
SIDH: High-level view

- Alice & Bob pick secret subgroups $A$ and $B$ of $E$.
- Alice computes $\varphi_A : E \to E/A$; Bob computes $\varphi_B : E \to E/B$.
  (These isogenies correspond to walking on the isogeny graph.)
- Alice and Bob transmit the values $E/A$ and $E/B$. 
SIDH: High-level view

Alice & Bob pick secret subgroups \( A \) and \( B \) of \( E \).

Alice computes \( \varphi_A : E \to E/A \); Bob computes \( \varphi_B : E \to E/B \).
(These isogenies correspond to walking on the isogeny graph.)

Alice and Bob transmit the values \( E/A \) and \( E/B \).

Alice somehow obtains \( A' := \varphi_B(A) \). (Similar for Bob.)
SIDH: High-level view

Alice & Bob pick secret subgroups $A$ and $B$ of $E$.

Alice computes $\varphi_A : E \to E/A$; Bob computes $\varphi_B : E \to E/B$.
(Theses isogenies correspond to walking on the isogeny graph.)

Alice and Bob transmit the values $E/A$ and $E/B$.

Alice somehow obtains $A' := \varphi_B(A)$. (Similar for Bob.)

They both compute the shared secret

$$(E/B)/A' \cong E/\langle A, B \rangle \cong (E/A)/B'.$$
SIDH’s auxiliary points

Previous slide: “Alice somehow obtains $A' := \varphi_B(A)$.”

Alice knows only $A$, Bob knows only $\varphi_B$. Hm.
SIDH’s auxiliary points

Previous slide: “Alice somehow obtains $A' := \varphi_B(A)$.”

Alice knows only $A$, Bob knows only $\varphi_B$. Hm.

Solution: $\varphi_B$ is a group homomorphism!

$Q$  $\varphi_B(Q)$

$A$  $\varphi_B(P)$

$A'$

$P$
SIDH’s auxiliary points

Previous slide: “Alice somehow obtains $A' := \varphi_B(A)$.”

Alice knows only $A$, Bob knows only $\varphi_B$. Hm.

Solution: $\varphi_B$ is a group homomorphism!

- Alice picks $A$ as $\langle P + [a]Q \rangle$ for fixed public $P, Q \in E$.
- Bob includes $\varphi_B(P)$ and $\varphi_B(Q)$ in his public key.

$\implies$ Now Alice can compute $A'$ as $\langle \varphi_B(P) + [a]\varphi_B(Q) \rangle$!
SIDH in one slide

Public parameters:
- a large prime $p = 2^n3^m - 1$ and a supersingular $E / \mathbb{F}_p$
- bases $(P_A, Q_A)$ and $(P_B, Q_B)$ of $E[2^n]$ and $E[3^m]$

**Alice**

$\begin{align*}
a & \overset{\text{random}}{\leftarrow} \{0 \ldots 2^n - 1\} \\
A & := \langle P_A + [a]Q_A \rangle \\
\text{compute } \varphi_A : E \to E / A
\end{align*}$

$E / A, \varphi_A(P_B), \varphi_A(Q_B)$

$A' := \langle \varphi_B(P_A) + [a]\varphi_B(Q_A) \rangle$

$s := j((E / B) / A')$

**Bob**

$\begin{align*}
b & \overset{\text{random}}{\leftarrow} \{0 \ldots 3^m - 1\} \\
B & := \langle P_B + [b]Q_B \rangle \\
\text{compute } \varphi_B : E \to E / B
\end{align*}$

$E / B, \varphi_B(P_A), \varphi_B(Q_A)$

$B' := \langle \varphi_A(P_B) + [b]\varphi_A(Q_B) \rangle$

$s := j((E / A) / B')$
All of the following is ‘obvious’ to the experts.

We often observe smart people rediscovering and wasting time on these ideas.
Extra points: Information theory

- By linearity, the two points $\varphi_A(P_B), \varphi_A(Q_B)$ encode how $\varphi_A$ acts on the whole $3^m$-torsion.
- Note $3^m$ is smooth $\Rightarrow$ can evaluate $\varphi_A$ on any $R \in E_0[3^m]$. 
Extra points: Information theory

- By linearity, the two points $\varphi_A(P_B), \varphi_A(Q_B)$ encode how $\varphi_A$ acts on the whole $3^m$-torsion.
- Note $3^m$ is smooth $\Rightarrow$ can evaluate $\varphi_A$ on any $R \in E_0[3^m]$.

**Lemma.** If two $d$-isogenies $\phi, \psi$ act the same on the $m$-torsion and $m^2 > 4d$, then $\phi = \psi$.

$\Rightarrow$ Except for very imbalanced parameters, the public points uniquely determine the secret isogenies.
Extra points: Interpolation?

- Recall: Isogenies are rational maps. We know enough input-output pairs to determine the map.

Rational function interpolation?
Extra points: Interpolation?

- Recall: Isogenies are rational maps. We know enough input-output pairs to determine the map.

- Rational function interpolation?

- ...the polynomials are of exponential degree $\approx \sqrt{p}$.

- can’t even write down the result without decomposing into a sequence of smaller-degree maps.
Extra points: Interpolation?

- Recall: Isogenies are rational maps. We know enough input-output pairs to determine the map.

\[ \Rightarrow \text{Rational function interpolation?} \]

\[ \sim \text{...the polynomials are of exponential degree } \approx \sqrt{p}. \]

\[ \sim \text{can’t even write down the result without decomposing into a sequence of smaller-degree maps.} \]

- No known algorithms for interpolating and decomposing at the same time.
Extra points: Group theory?

- Can we extrapolate the action of $\varphi_A$ to some $\geq 3^m$-torsion?
  e.g. we win if we get the action of $\varphi_A$ on the $2^n$-torsion.
Extra points: Group theory?

- Can we extrapolate the action of $\varphi_A$ to some $\geq 3^m$-torsion? e.g. we win if we get the action of $\varphi_A$ on the $2^n$-torsion.

- There’s an isomorphism of groups

$$E(F_{p^2}) \cong (\mathbb{Z}/2^n)^2 \times (\mathbb{Z}/3^m)^2.$$
Can we extrapolate the action of $\varphi_A$ to some $\geq 3^m$-torsion?

\[ \text{e.g. we win if we get the action of } \varphi_A \text{ on the } 2^n\text{-torsion.} \]

There’s an isomorphism of groups

\[ E(\mathbb{F}_{p^2}) \cong (\mathbb{Z}/2^n)^2 \times (\mathbb{Z}/3^m)^2. \]

\[ \implies \text{can’t learn anything about } 2^n \text{ from } 3^m \text{ using groups alone.} \]

(Annoying: This shows up in many disguises.)
Extra points: Group theory?

- Can we extrapolate the action of $\varphi_A$ to some $\geq 3^m$-torsion? e.g. we win if we get the action of $\varphi_A$ on the $2^n$-torsion.

- There’s an isomorphism of groups

\[ E(\mathbb{F}_{p^2}) \cong (\mathbb{Z}/2^n)^2 \times (\mathbb{Z}/3^m)^2. \]

\[ \implies \text{can’t learn anything about } 2^n \text{ from } 3^m \text{ using groups alone.} \]

(Annoying: This shows up in many disguises.)

“[...] elliptic curves are as close to generic groups as it gets.”

—me, 2018

(Exception: pairings, but those are also just bilinear maps.)
Extra points: Effective Tate?

Previous slide: Little hope for coprime extrapolation. What about higher \( \ell \)-torsion, say \( \ell^{n+1} \)?
Extra points: Effective Tate?

Previous slide: Little hope for coprime extrapolation. What about higher $\ell$-torsion, say $\ell^{n+1}$?

**Theorem.** For ell. curves $E, E'/\mathbb{F}_q$ and a prime $\ell \neq p$, the map $\text{Hom}_{\mathbb{F}_q}(E, E') \otimes \mathbb{Z}_\ell \longrightarrow \text{Hom}_{\mathbb{F}_q}(E[\ell^{\infty}], E'[\ell^{\infty}])$ is bijective.

Read: An isogeny is uniquely defined by how it acts on sufficiently high $\ell^k$-torsion.
Extra points: Effective Tate?

Previous slide: Little hope for coprime extrapolation. What about higher $\ell$-torsion, say $\ell^{n+1}$?

**Theorem.** For ell. curves $E, E'/\mathbb{F}_q$ and a prime $\ell \neq p$, the map

$$\text{Hom}_{\mathbb{F}_q}(E, E') \otimes \mathbb{Z}_\ell \rightarrow \text{Hom}_{\mathbb{F}_q}(E[\ell^\infty], E'[\ell^\infty])$$

is bijective.

Read: An isogeny is uniquely defined by how it acts on sufficiently high $\ell^k$-torsion.

⇝ Same problem; group-theoretically there are $\ell^4$ ways to lift.
Extra points: Effective Tate?

Previous slide: Little hope for coprime extrapolation. What about higher $\ell$-torsion, say $\ell^{n+1}$?

**Theorem.** For elliptic curves $E, E'/\mathbb{F}_q$ and a prime $\ell \neq p$, the map $\text{Hom}_{\mathbb{F}_q}(E, E') \otimes \mathbb{Z}_\ell \longrightarrow \text{Hom}_{\mathbb{F}_q}(E[\ell^\infty], E'[\ell^\infty])$ is bijective.

Read: An isogeny is uniquely defined by how it acts on sufficiently high $\ell^k$-torsion.

いますが Same problem; group-theoretically there are $\ell^4$ ways to lift.

!! We know more: The degree!
Extra points: Effective Tate?

Previous slide: Little hope for coprime extrapolation. What about higher $\ell$-torsion, say $\ell^{n+1}$?

**Theorem.** For ell. curves $E, E'/\mathbb{F}_q$ and a prime $\ell \neq p$, the map $\text{Hom}_{\mathbb{F}_q}(E, E') \otimes \mathbb{Z}_\ell \rightarrow \text{Hom}_{\mathbb{F}_q}(E[\ell^\infty], E'[\ell^\infty])$ is bijective.

Read: An isogeny is uniquely defined by how it acts on sufficiently high $\ell^k$-torsion.

- Same problem; group-theoretically there are $\ell^4$ ways to lift.

- We know more: The degree! ($\ell \nmid \det$; almost no use.)
Extra points: Effective Tate?

Previous slide: Little hope for coprime extrapolation. What about higher $\ell$-torsion, say $\ell^{n+1}$?

**Theorem.** For ell. curves $E, E'/\mathbb{F}_q$ and a prime $\ell \neq p$, the map $\text{Hom}_{\mathbb{F}_q}(E, E') \otimes \mathbb{Z}_\ell \rightarrow \text{Hom}_{\mathbb{F}_q}(E[\ell^\infty], E'[\ell^\infty])$ is bijective.

Read: An isogeny is uniquely defined by how it acts on sufficiently high $\ell^k$-torsion.

- Same problem; group-theoretically there are $\ell^4$ ways to lift.

- We know more: The degree! ($\ell \nmid \text{det};$ almost no use.)

- This idea works slightly better for endomorphisms (characteristic polynomial constrains to $\ell^2$ choices).
For typical SIDH parameters, we know endomorphisms $\iota, \pi$ of $E_0$ such that $\text{End}(E_0) = \langle 1, \iota, \frac{\iota + \pi}{2}, \frac{1 + \iota \pi}{2} \rangle$. 
Extra points: Petit’s endomorphisms (1)

- For typical SIDH parameters, we know endomorphisms $\iota, \pi$ of $E_0$ such that $\text{End}(E_0) = \langle 1, \iota, \frac{\iota + \pi}{2}, \frac{1 + \iota \pi}{2} \rangle$.

- Going back and forth to $E_0$ yields endomorphisms of $E_A$:

$$E_0 \xrightarrow{\iota} \xleftarrow{\hat{\varphi}_A} E_A \xrightarrow{\varphi_A}$$

We can evaluate endomorphisms of $E_A$ in the subring $R = \{ \varphi_A \circ \vartheta \circ \hat{\varphi}_A \mid \vartheta \in \text{End}(E_0) \}$ on the $3m$-torsion.

Idea: Find $\tau \in R$ of degree $3m$; recover $3m$-part from known action; brute-force the remaining part. $\Rightarrow (\text{details}) \Rightarrow \text{Recover } \varphi_A$. 

23 / 33
Extra points: Petit’s endomorphisms (1)

- For typical SIDH parameters, we know endomorphisms $\iota, \pi$ of $E_0$ such that $\text{End}(E_0) = \langle 1, \iota, \frac{\iota + \pi}{2}, \frac{1 + \iota \pi}{2} \rangle$.

- Going back and forth to $E_0$ yields endomorphisms of $E_A$:

$$\iota \quad E_0 \quad \varphi_A \quad E_A \quad \tilde{\varphi}_A$$

\[\Rightarrow\] We can evaluate endomorphisms of $E_A$ in the subring $R = \{ \varphi_A \circ \vartheta \circ \tilde{\varphi}_A \mid \vartheta \in \text{End}(E_0) \}$ on the $3^m$-torsion.
Extra points: Petit’s endomorphisms (1)

- For typical SIDH parameters, we know endomorphisms $\iota, \pi$ of $E_0$ such that $\text{End}(E_0) = \langle 1, \iota, \frac{\iota + \pi}{2}, \frac{1 + \iota \pi}{2} \rangle$.

- Going back and forth to $E_0$ yields endomorphisms of $E_A$:

\[
\begin{array}{ccc}
E_0 & \xrightarrow{\iota} & E_0 \\
\downarrow \varphi_A & & \uparrow \hat{\varphi}_A \\
E_A & \xleftarrow{\hat{\varphi}_A} & E_A
\end{array}
\]

\[\rightsquigarrow\text{ We can evaluate endomorphisms of } E_A \text{ in the subring } R = \{ \varphi_A \circ \vartheta \circ \hat{\varphi}_A \mid \vartheta \in \text{End}(E_0) \} \text{ on the } 3^m-\text{torsion}.\]

- Idea: Find $\tau \in R$ of degree $3^m r$; recover $3^m$-part from known action; brute-force the remaining part.  
  \[\implies (\text{details}) \implies \text{Recover } \varphi_A.\]
Extra points: Petit’s endomorphisms (2)

Petit uses endomorphisms $\tau \in R$ of the form

$$\tau = a + \varphi_A (b \nu + c \pi + d \nu \pi) \widehat{\varphi_A},$$

where $\deg \nu = 1$ and $\deg \pi = \deg \nu \pi = p$. Hence

$$\deg \tau = a^2 + 2^{2n}b^2 + 2^{2n}pc^2 + 2^{2n}pd^2.$$ 

(Recall $p = 2^n3^m - 1$.)
Extra points: Petit’s endomorphisms (2)

- Petit uses endomorphisms $\tau \in R$ of the form
  \[ \tau = a + \varphi_A(b\nu + c\pi + d\nu\pi)\hat{\varphi}_A, \]
  where $\deg \nu = 1$ and $\deg \pi = \deg \nu\pi = p$. Hence
  \[ \deg \tau = a^2 + 2^{2n}b^2 + 2^{2n}pc^2 + 2^{2n}pd^2. \]
  (Recall $p = 2^n3^m - 1$.)

$\implies$ Unless $3^m \gg 2^n$, there is no hope to find $\tau$ with $3^m \mid \deg \tau$ and $\deg \tau/3^m < 2^n$. 
Extra points: Summary

- Same problem all over the place:
  There seems to be no way to obtain anything from the given action-on-$3^m$-torsion except what's given.
  😞
Extra points: Summary

▶ Same problem all over the place:
There seems to be no way to obtain anything from the
given action-on-$3^m$-torsion except what’s given.

コミュニケーションアイコン

▶ Petit’s approach cannot be expected to work for ‘real’
(symmetric, two-party) SIDH.

コミュニケーションアイコン
Extra points: Summary

▶ Same problem all over the place:
There seems to be no way to obtain anything from the given action-on-$3^m$-torsion except what’s given.

 :

▶ Petit’s approach cannot be expected to work for ‘real’ (symmetric, two-party) SIDH.

 :

▶ Life sucks.

\_\_\_(ツ)_/\_\_
The pure isogeny problem

Fundamental problem: given supersingular $E$ and $E'/\mathbb{F}_{p^2}$ that are $\ell^n$-isogeneous, compute an isogeny $\phi : E \to E'$. 
The pure isogeny problem

Example

Choose

\[ E/\mathbb{F}_{431} : y^2 = x^3 + 1 \quad \text{and} \quad E'/\mathbb{F}_{431} : y^2 = x^3 + 291x + 298. \]
The pure isogeny problem

Example
Choose

\[ E/\mathbb{F}_{431} : y^2 = x^3 + 1 \quad \text{and} \quad E'/\mathbb{F}_{431} : y^2 = x^3 + 291x + 298. \]

These elliptic curves are \( 2^2 = 4 \)-isogenous. Problem: compute an isogeny \( f : E \to E' \).

The kernel of \( f : E \to E' \) is generated by a point \( P \in E(\mathbb{F}_p) \) of order 4.
The pure isogeny problem

Example

Choose

\[ E/\mathbb{F}_{431} : y^2 = x^3 + 1 \quad \text{and} \quad E'/\mathbb{F}_{431} : y^2 = x^3 + 291x + 298. \]

These elliptic curves are \(2^2 = 4\)-isogenous. Problem: compute an isogeny \(f : E \to E'\).

The kernel of \(f : E \to E'\) is generated by a point \(P \in E(\overline{\mathbb{F}_p})\) of order 4.

- Solution (a): try all nine possible order 4 kernels and use Vélu’s formulas to find \(f\).
The pure isogeny problem

Example
Choose

\[ E / \mathbb{F}_{431} : y^2 = x^3 + 1 \quad \text{and} \quad E' / \mathbb{F}_{431} : y^2 = x^3 + 291x + 298. \]

These elliptic curves are \(2^2 = 4\)-isogenous. Problem: compute an isogeny \(f : E \rightarrow E'\).

The kernel of \(f : E \rightarrow E'\) is generated by a point \(P \in E(\overline{\mathbb{F}_p})\) of order 4.

- Solution (a): try all nine possible order 4 kernels and use Vélu’s formulas to find \(f\).
- Solution (b): try all three possible order 2 kernels from both \(E\) and \(E'\) and check when the codomain is the same.
The pure isogeny problem

Example

Choose

\[ E/\mathbb{F}_{431} : y^2 = x^3 + 1 \quad \text{and} \quad E'/\mathbb{F}_{431} : y^2 = x^3 + 291x + 298. \]

These elliptic curves are \( 2^2 = 4 \)-isogenous. Problem: compute an isogeny \( f : E \to E' \).

The kernel of \( f : E \to E' \) is generated by a point \( P \in E(\mathbb{F}_p) \) of order 4.

- Solution (a): try all nine possible order 4 kernels and use Vélu’s formulas to find \( f \).
- Solution (b): try all three possible order 2 kernels from both \( E \) and \( E' \) and check when the codomain is the same. Solution (b) is meet-in-the-middle: complexity \( \tilde{O}(p^{1/4}) \).
Exploiting subgraphs

The SIDH graph has a $\mathbb{F}_p$-subgraph:
Exploiting subgraphs

The SIDH graph has a $\mathbb{F}_p$-subgraph:

\[ S = \{2, 3\}, \quad q = 431^2 \]
Exploiting subgraphs

The SIDH graph has a $\mathbb{F}_p$-subgraph:

$$S = \{2, 3\}, \; q = 431^2$$

$$S = \{2, 3\}, \; p = 431$$
Exploiting subgraphs?

\[ S = \{3\}, \ p = 431, \]

nodes up to \( \mathbb{F}_p \)-isomorphism
Exploiting subgraphs?

\[ S = \{3\}, \quad p = 431, \]

nodes up to \( \mathbb{F}_p \)-isomorphism

\[ S = \{3\}, \quad p = 431, \]

nodes up to \( \mathbb{F}_p \)-isomorphism
Exploiting subgraphs?

$S = \{3\}, \ p = 431,$
nodes up to $\overline{F}_p$-isomorphism

Kuperberg’s subexponential quantum algorithm to compute a hidden shift applies to this! Complexity: $L_p[1/2]$. 
Exploiting subgraphs?

$S = \{3\}, \ p = 431,$

nodes up to $\mathbb{F}_p$-isomorphism

$S = \{3\}, \ p = 431,$

nodes up to $\mathbb{F}_p$-isomorphism

Kuperberg’s subexponential quantum algorithm to compute a hidden shift applies to this! Complexity: $L_p[1/2]$. Finding nearest node in subgraph costs...
Exploiting subgraphs?

$S = \{3\}, \ p = 431,
\text{nodes up to } \mathbb{F}_p\text{-isomorphism}$

$S = \{3\}, \ p = 431,
\text{nodes up to } \mathbb{F}_p\text{-isomorphism}$

Kuperberg’s subexponential quantum algorithm to compute a hidden shift applies to this! Complexity: $L_p[1/2]$. Finding nearest node in subgraph costs... $\tilde{O}(p^{1/2})$. 
Exploiting subgraphs?

\[ S = \{3\}, \ p = 431, \]

nodes up to $\mathbb{F}_p$-isomorphism

Kuperberg’s subexponential quantum algorithm to compute a hidden shift applies to this! Complexity: $L_p[1/2]$. Finding nearest node in subgraph costs... $\tilde{O}(p^{1/2})$. 

(Delfs-Galbraith, Biasse-Jao-Sankar)
More graphs defined over $\mathbb{F}_p$

From 1-dimensional $E/\mathbb{F}_{p^2}$,

construct 2-dimensional $W(E)/\mathbb{F}_p$

‘Weil restriction’

This picture is very unlikely to be accurate.
More graphs defined over $\mathbb{F}_p$

- The associated graph of 2-dimensional objects is (heuristically) $O(\sqrt{p})$ cycles of length $O(\sqrt{p})$.
  (Superspecial principally polarized abelian surfaces if you care)
More graphs defined over $\mathbb{F}_p$

- The associated graph of 2-dimensional objects is (heuristically) $O(\sqrt{p})$ cycles of length $O(\sqrt{p})$.
  (Superspecial principally polarized abelian surfaces if you care)
- If your two elliptic curves are in the same cycle, Kuperberg’s algorithm can find the isogeny in subexponential time.
More graphs defined over $\mathbb{F}_p$

- The associated graph of **2-dimensional** objects is (heuristically) $O(\sqrt{p})$ cycles of length $O(\sqrt{p})$.
  (Superspecial principally polarized abelian surfaces if you care)

- If your two elliptic curves are in the same cycle, Kuperberg’s algorithm can find the isogeny in subexponential time.

- Probability of being in the same cycle: $O(1/\sqrt{p})$. 
More graphs defined over $\mathbb{F}_p$

- The associated graph of 2-dimensional objects is (heuristically) $O(\sqrt{p})$ cycles of length $O(\sqrt{p})$.
  (Superspecial principally polarized abelian surfaces if you care)
- If your two elliptic curves are in the same cycle, Kuperberg’s algorithm can find the isogeny in subexponential time.
- Probability of being in the same cycle: $O(1/\sqrt{p})$. ☺️
More equivalent categories: lifting to $\mathbb{C}$

\[
\begin{align*}
\{ & \text{Elliptic curves } E \text{ defined over } \mathbb{C} \\
& \text{with } \text{End}(E) = R \}
\end{align*}
\]

Here computing isogenies is easy!

\[
\begin{align*}
\{ & \text{Non-supersingular elliptic curves defined over } \mathbb{F}_q \\
& \text{with } \text{End}(E) = R \}
\end{align*}
\]

Here computing isogenies is harder.
More equivalent categories: lifting to $\mathbb{C}$

A well-chosen subset of

$$\left\{ \begin{array}{l} \text{Elliptic curves } E \text{ defined over } \mathbb{C} \\ \text{with } \phi \in \text{End}(E) \end{array} \right\}$$

Here computing isogenies is easy!

$$\uparrow \Downarrow$$

$$\left\{ \begin{array}{l} \text{Supersingular elliptic curves defined over } \mathbb{F}_q \\ \text{with non-scalar } \phi \in \text{End}(E) \end{array} \right\}$$

Here computing isogenies is harder.
More equivalent categories: lifting to $\mathbb{C}$

A well-chosen subset of

\[
\left\{ \begin{array}{l}
\text{Elliptic curves } E \text{ defined over } \mathbb{C} \\
\text{with } \phi \in \text{End}(E)
\end{array} \right\}
\]

Here computing isogenies is easy!

\[
\uparrow
\]

\[
\downarrow
\]

\[
\left\{ \begin{array}{l}
\text{Supersingular elliptic curves defined over } \mathbb{F}_q \\
\text{with non-scalar } \phi \in \text{End}(E)
\end{array} \right\}
\]

Here computing isogenies is harder.

- Computing the equivalence is slow.
More equivalent categories: lifting to $\mathbb{C}$

A well-chosen subset of

\[
\begin{cases}
\text{Elliptic curves } E \text{ defined over } \mathbb{C} \\
\text{with } \phi \in \text{End}(E)
\end{cases}
\]

Here computing isogenies is easy!

\[
\begin{array}{c}
\uparrow \\
\downarrow
\end{array}
\]

\[
\begin{cases}
\text{Supersingular elliptic curves defined over } \mathbb{F}_q \\
\text{with non-scalar } \phi \in \text{End}(E)
\end{cases}
\]

Here computing isogenies is harder.

- Computing the equivalence is slow.
- Finding a non-scalar endomorphism is hard.
More equivalent categories: lifting to $\mathbb{C}$

A well-chosen subset of

\[
\left\{ \begin{array}{l}
\text{Elliptic curves } E \text{ defined over } \mathbb{C} \\
\text{with } \phi \in \text{End}(E)
\end{array} \right. 
\]

Here computing isogenies is easy!

\[
\left\{ \begin{array}{l}
\text{Supersingular elliptic curves defined over } \mathbb{F}_q \\
\text{with non-scalar } \phi \in \text{End}(E)
\end{array} \right. 
\]

Here computing isogenies is harder.

- Computing the equivalence is slow.
- Finding a non-scalar endomorphism is hard.
- If you can find non-scalar endomorphisms, SIDH is probably already broken by earlier work (Kohel-Lauter-Petit-Tignol and Galbraith-Petit-Shani-Ti).
Thank you!