Attacks and non-attacks on SIDH

Lorenz Panny

Technische Universiteit Eindhoven

Bochum, 2 December 2019

Largely based on “How to not break SIDH”, which is joint work with Chloe Martindale.
What’s this all about?

David Jao & Luca De Feo
What’s this all about?

- 2011: David Jao & Luca De Feo come up with something now known as “supersingular-isogeny Diffie–Hellman.”

- 2020 - ε: Semi-surprisingly, this stuff is still not broken. Question for the next few dozens of minutes: Why?
What’s this all about?

- 2011: David Jao & Luca De Feo come up with something now known as “Supersingular-Isogeny Diffie–Hellman”.

2020−ε: Semi-surprisingly, this stuff is still not broken.

Question for the next few dozens of minutes: Why?
What’s this all about?

- 2011: David Jao & Luca De Feo come up with something now known as “Supersingular-Isogeny Diffie–Hellman”.

- 2020–ε: Semi-surprisingly, this stuff is still not broken.
What’s this all about?

- 2011: David Jao & Luca De Feo come up with something now known as “Supersingular-Isogeny Diffie–Hellman”.

- 2020−ε: Semi-surprisingly, this stuff is still not broken. Question for the next few dozens of minutes: Why?
Stand back!

We’re going to do math.
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.
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 \( E \rightarrow E' \) 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

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

It is an isomorphism; its kernel is \( \{\infty\} \).
Isogenies

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 #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

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

over $\mathbb{F}_{71}$. Its kernel is $\{(2, 9), (2, -9), \infty\}$. 

* A separable isogeny is one that is not ramified at any point.
Isogeny kernels

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 $E'$)
Isogeny kernels

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

Vélu operates in the field where the points in $G$ live.

$\leadsto$ need to make sure extensions stay small for desired $\#G$

$\leadsto$ this is (one reason) why we use supersingular curves!

\(^1\)(up to isomorphism of $E'$)
Smooth isogenies

- In SIDH, $\#A$ and $\#B$ are “crypto-sized”.

  Vélu’s formulas take $\Theta(\#G)$ to compute $\varphi_G : E \to E/G$. 

- Evaluate $\varphi_G$ as a chain of small-degree isogenies:

  For $G \sim = \mathbb{Z}/\ell^k$, set $\ker \psi_i = (\psi_i - 1 \circ \cdots \circ \psi_1)(G)$.

  $E \xrightarrow{\psi_1} \cdots \xrightarrow{\psi_{k-1}} E/\psi_k \xrightarrow{\psi_k} E/G$.

  Complexity: $O(k^2 \cdot \ell^k)$. Exponentially smaller than $\ell^{k^2}$.

  "Optimal strategy" improves this to $O(k \log k \cdot \ell^k)$. 


Smooth isogenies

- In SIDH, \( \#A = 2^n \) and \( \#B = 3^m \) are “crypto-sized”.
  Vélu’s formulas take \( \Theta(\#G) \) to compute \( \varphi_G : E \to E/G \).
Smooth isogenies

- In SIDH, \( \#A = 2^n \) and \( \#B = 3^m \) are “crypto-sized”.

Vélu’s formulas take \( \Theta(\#G) \) to compute \( \varphi_G : E \to E/G \).

!! Evaluate \( \varphi_G \) as a chain of small-degree isogenies:

For \( G \cong \mathbb{Z}/\ell^k \), set \( \ker \psi_i := [\ell^{k-i}](\psi_{i-1} \circ \cdots \circ \psi_1)(G) \).

\[
\begin{array}{ccccccc}
E & \xrightarrow{\psi_1} & E_1 & \xrightarrow{\psi_2} & \cdots & \xrightarrow{\psi_{k-1}} & E_{k-1} & \xrightarrow{\psi_k} & E/G \\
& & & & \Downarrow \varphi_G & & & &
\end{array}
\]

Complexity: \( O(k^2 \cdot \ell^k) \). Exponentially smaller than \( \ell^{k^2} \).

"Optimal strategy" improves this to \( O(k \log k \cdot \ell^k) \).
Smooth isogenies

► In SIDH, \( \#A = 2^n \) and \( \#B = 3^m \) are “crypto-sized”.

Vélu’s formulas take \( \Theta(\#G) \) to compute \( \varphi_G : E \to E/G \).

!! Evaluate \( \varphi_G \) as a chain of small-degree isogenies:

For \( G \cong \mathbb{Z}/\ell^k \), set \( \ker \psi_i := [\ell^{k-i}](\psi_{i-1} \circ \cdots \circ \psi_1)(G) \).

\[
\begin{array}{cccccc}
E & \xrightarrow{\psi_1} & E_1 & \xrightarrow{\psi_2} & \cdots & \xrightarrow{\psi_{k-1}} & E_{k-1} & \xrightarrow{\psi_k} & E/G \\
\varphi_G
\end{array}
\]

\( \sim \) Complexity: \( O(k^2 \cdot \ell) \). Exponentially smaller than \( \ell^k \! \)!

“Optimal strategy” improves this to \( O(k \log k \cdot \ell) \).
Isogeny graphs

- Graph view: Each $\psi_i$ is a step in the $\ell$-isogeny graph.

\[(q = 431^2, \text{degrees } 2, 3)\]
Reminder:

SIDH

for those who missed David Jao’s ECC talk 8 years ago 😊
SIDH: High-level view

$E$
SIDH: High-level view

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

$\varphi_B$ is a group homomorphism!
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 \( E/F_p \)
- bases \((P_A, Q_A)\) and \((P_B, Q_B)\) of \(E[2^n]\) and \(E[3^m]\)

<table>
<thead>
<tr>
<th>Alice</th>
<th>public</th>
<th>Bob</th>
</tr>
</thead>
<tbody>
<tr>
<td>( a ) ( \xleftarrow{\text{random}} ) {0…2^n−1}</td>
<td>( b ) ( \xleftarrow{\text{random}} ) {0…3^m−1}</td>
<td></td>
</tr>
<tr>
<td>( A := \langle P_A + [a]Q_A \rangle )</td>
<td>( B := \langle P_B + [b]Q_B \rangle )</td>
<td></td>
</tr>
<tr>
<td>compute ( \varphi_A : E \rightarrow E/A )</td>
<td>compute ( \varphi_B : E \rightarrow E/B )</td>
<td></td>
</tr>
<tr>
<td>( E/A, \varphi_A(P_B), \varphi_A(Q_B) )</td>
<td>( E/B, \varphi_B(P_A), \varphi_B(Q_A) )</td>
<td></td>
</tr>
<tr>
<td>( A' := \langle \varphi_B(P_A) + [a]\varphi_B(Q_A) \rangle )</td>
<td>( B' := \langle \varphi_A(P_B) + [b]\varphi_A(Q_B) \rangle )</td>
<td></td>
</tr>
<tr>
<td>( s := j(\langle E/B \rangle/A') )</td>
<td>( s := j(\langle E/A \rangle/B') )</td>
<td></td>
</tr>
</tbody>
</table>
Disclaimer:
All of the following is “obvious” to experts.
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 $\rightsquigarrow$ can evaluate $\varphi_A$ on any $R \in E_0[3^m]$. 

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

Except for very unbalanced parameters, the public points uniquely determine the secret isogenies.
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 $\leadsto$ 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 $\phi = \psi$.

$\implies$ Except for very unbalanced 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.

  ⇞ 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.

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

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

 değerlendirme There’s an isomorphism of groups

\[
E(F_{p^2}) \cong (\mathbb{Z}/2^n)^2 \times (\mathbb{Z}/3^m)^2.
\]
Extra points: Group theory?

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

- There’s an isomorphism of groups

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

$\implies$ can’t learn anything about $2^n$ from $3^m$ using groups alone.
(Annoying: This shows up in many disguises.)
Extra points: Group theory?

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

- There's an isomorphism of groups

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

$$\implies$$ can't learn anything about $2^n$ from $3^m$ 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 “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 $\text{Hom}_{\mathbb{F}_q}(E, E') \otimes \mathbb{Z}_\ell \rightarrow \text{Hom}_{\mathbb{F}_q}(E[\ell^\infty], E'[\ell^\infty])$ is bijective.

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

● 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 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.

Choose 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.

\[ \rightsquigarrow \text{Same problem; group-theoretically there are } \ell^4 \text{ ways to lift.} \]

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

- This idea works slightly better for endomorphisms (characteristic polynomial constrains to \( \ell^2 \) choices).
Extra points: Petit’s endomorphisms (1)

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

\[
\begin{array}{ccc}
\vartheta & \circlearrowleft & E_0 \\
\psi & \longrightarrow & \varphi_A \\
\widehat{\varphi}_A & \longrightarrow & E_A
\end{array}
\]

\( \Rightarrow \) We can evaluate endomorphisms of \( E_A \) in the subring \( R = \{ \varphi_A \circ \vartheta \circ \widehat{\varphi}_A \mid \vartheta \in \text{End}(E_0) \} \) 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 $E_A$:

\[
\begin{array}{ccc}
\vartheta & \circlearrowleft & \iota & \circlearrowleft & E_0 & \circlearrowright & \varphi_A & \circlearrowleft & E_A & \varphi_A
\end{array}
\]

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

- Idea: Find $\tau \in R$ of degree $3^mr$; recover $3^m$-part from known action; brute-force the remaining part.

$\Rightarrow$ (details) $\Rightarrow$ Recover $\varphi_A$. 
Extra points: Petit’s endomorphisms (2)

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

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

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

where $\deg \iota = 1$ and $\deg \pi = \deg \iota\pi = p$. 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: Petit’s endomorphisms (2)

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

$$\tau = a + \varphi_A (b\iota + c\pi + d\iota\pi)\hat{\varphi}_A,$$

where $\deg \iota = 1$ and $\deg \pi = \deg \iota\pi = p$. 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 $\deg \tau/3^m < 2^n$.

$\implies$ Petit’s endomorphisms are not sufficiently petit-degree ☹️.
Auxiliary-points active attack  [Galbraith–Petit–Shani–Ti]

- Recall: Bob sends $P' := \varphi_B(P)$ and $Q' := \varphi_B(Q)$ to Alice. She computes $A' = \langle P' + [a]Q' \rangle$ and, from that, obtains $s$. 

Validating that Bob is honest is as hard as breaking SIDH. Only usable with ephemeral keys or as a KEM "SIKE."
Auxiliary-points active attack  [Galbraith–Petit–Shani–Ti]

- Recall: Bob sends $P' := \varphi_B(P)$ and $Q' := \varphi_B(Q)$ to Alice. She computes $A' = \langle P' + [a]Q' \rangle$ and, from that, obtains $s$.

- Bob cheats and sends $Q'' := Q' + [2^{n-1}]P'$ instead of $Q'$. Alice computes $A'' = \langle P' + [a]Q'' \rangle$.
Auxiliary-points active attack [Galbraith–Petit–Shani–Ti]

- Recall: Bob sends $P' := \varphi_B(P)$ and $Q' := \varphi_B(Q)$ to Alice. She computes $A' = \langle P' + [a]Q' \rangle$ and, from that, obtains $s$.

- Bob cheats and sends $Q'' := Q' + [2^{n-1}]P'$ instead of $Q'$. Alice computes $A'' = \langle P' + [a]Q'' \rangle$.

If $a = 2u$ : $[a]Q'' = [a]Q' + [u][2^n]P' = [a]Q'$.

If $a = 2u+1$ : $[a]Q'' = [a]Q' + [u][2^n]P' + [2^{n-1}]P' = [a]Q' + [2^{n-1}]P'$.
Auxiliary-points active attack  [Galbraith–Petit–Shani–Ti]

► Recall: Bob sends $P' := \varphi_B(P)$ and $Q' := \varphi_B(Q)$ to Alice. She computes $A' = \langle P' + [a]Q' \rangle$ and, from that, obtains $s$.

► Bob cheats and sends $Q'' := Q' + [2^{n-1}]P'$ instead of $Q'$. Alice computes $A'' = \langle P' + [a]Q'' \rangle$.

If $a = 2u$ : $[a]Q'' = [a]Q' + [u][2^n]P' = [a]Q'$.

If $a = 2u+1$: $[a]Q'' = [a]Q' + [u][2^n]P' + [2^{n-1}]P' = [a]Q' + [2^{n-1}]P'$.

$\implies$ Bob learns the parity of $a$. 

|
Auxiliary-points active attack  [Galbraith–Petit–Shani–Ti]

- Recall: Bob sends $P' := \varphi_B(P)$ and $Q' := \varphi_B(Q)$ to Alice. She computes $A' = \langle P' + [a]Q' \rangle$ and, from that, obtains s.

- Bob cheats and sends $Q'' := Q' + [2^{n-1}]P'$ instead of $Q'$. Alice computes $A'' = \langle P' + [a]Q'' \rangle$.

  - If $a = 2u$ : $[a]Q'' = [a]Q' + [u][2^n]P' = [a]Q'$.

  $\implies$ Bob learns the parity of $a$.

  Similarly, he can completely recover $a$ in $O(n)$ queries.
Auxiliary-points active attack [Galbraith–Petit–Shani–Ti]

- Recall: Bob sends $P' := \varphi_B(P)$ and $Q' := \varphi_B(Q)$ to Alice. She computes $A' = \langle P' + [a]Q' \rangle$ and, from that, obtains $s$.

- Bob cheats and sends $Q'' := Q' + [2^{n-1}]P'$ instead of $Q'$. Alice computes $A'' = \langle P' + [a]Q'' \rangle$.
  
  If $a = 2u$ : $[a]Q'' = [a]Q' + [u][2^n]P' = [a]Q'$.
  If $a = 2u+1$: $[a]Q'' = [a]Q' + [u][2^n]P' + [2^{n-1}]P' = [a]Q' + [2^{n-1}]P'$.

$\implies$ Bob learns the parity of $a$.
  
  Similarly, he can completely recover $a$ in $O(n)$ queries.

Validating that Bob is honest is $\approx$ as hard as breaking SIDH.

$\implies$ only usable with ephemeral keys or as a KEM “SIKE”.
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.

😞

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

😞
Interlude: How DH is SIDH?

Observation: SIDH has sometimes been marketed as “post-quantum Diffie–Hellman”.

Is this accurate?
Interlude: How DH is SIDH?

Observation: SIDH has sometimes been marketed as “post-quantum Diffie–Hellman”.

Is this accurate?

- **Not symmetric**: Easily fixable, simply run two SIDH instances with opposite roles simultaneously.
Observation: SIDH has sometimes been marketed as “post-quantum Diffie–Hellman”.

Is this accurate?

- **Not symmetric**: Easily fixable, simply run two SIDH instances with opposite roles simultaneously.
  (This “invention” has been filed for patent in Canada...)
Observation: SIDH has sometimes been marketed as “post-quantum Diffie–Hellman”.

Is this accurate?

- **Not symmetric**: Easily fixable, simply run two SIDH instances with opposite roles simultaneously. (This “invention” has been filed for patent in Canada...)

- **Active attack**: Not easily fixable; implies a significant lack of DH-ness!
...we’ll be right back after a short commercial break...

[ˈsiːˌsɛid]
...is an efficient commutative group action on an isogeny graph.
\( \rightsquigarrow \) much closer to post-quantum Diffie–Hellman than SIDH \( \rightsquigarrow \).
The pure isogeny problem

Fundamental problem: Given supersingular elliptic curves $E, E'/\mathbb{F}_{p^2}$, compute an isogeny $\varphi : E \to E'$. 
The pure isogeny problem

Fundamental problem: Given supersingular elliptic curves $E, E'/\mathbb{F}_{p^2}$, compute an isogeny $\varphi: E \to E'$.

Galbraith–Petit–Shani–Ti: Any isogeny works to break SIDH.
The pure isogeny problem

Fundamental problem: Given supersingular elliptic curves $E, E'/\mathbb{F}_{p^2}$, compute an isogeny $\varphi: E \to E'$.

Galbraith–Petit–Shani–Ti: *Any* isogeny works to break SIDH.

Known solutions are generic: Graph walking, claw finding, ... (These are all exponential-time, even quantumly.)
Equation solving?

Modular polynomials parameterize $\ell$-isogenous $j$-invariants. We are looking for an $\ell^n$-isogeny between $j_0$ and $j_n$:

$$\Phi_\ell(j_0, X_1) = \Phi_\ell(X_1, X_2) = \Phi_\ell(X_2, X_3) = \ldots$$

$$\ldots = \Phi_\ell(X_{n-2}, X_{n-1}) = \Phi_\ell(X_{n-1}, j_n) = 0.$$
Equation solving?

Modular polynomials parameterize $\ell$-isogenous $j$-invariants. We are looking for an $\ell^n$-isogeny between $j_0$ and $j_n$:

$$
\Phi_\ell(j_0, X_1) = \Phi_\ell(X_1, X_2) = \Phi_\ell(X_2, X_3) = \ldots
$$

$$
\ldots = \Phi_\ell(X_{n-2}, X_{n-1}) = \Phi_\ell(X_{n-1}, j_n) = 0.
$$

Throw this system into a Gröbner basis algorithm and pray.
Equation solving?

**Modular polynomials** parameterize \( \ell \)-isogenous \( j \)-invariants. We are looking for an \( \ell^n \)-isogeny between \( j_0 \) and \( j_n \):

\[
\Phi_\ell(j_0, X_1) = \Phi_\ell(X_1, X_2) = \Phi_\ell(X_2, X_3) = \ldots \\
\ldots = \Phi_\ell(X_{n-2}, X_{n-1}) = \Phi_\ell(X_{n-1}, j_n) = 0.
\]

Takahashi–Kudo–Ikematsu–Yasuda–Yokoyama (MathCrypt 2019): Throw this system into a **Gröbner basis algorithm** and pray.

Same paper:
Plug start and end *curves* into *Vélu’s formulas* and solve for the kernel point.
Equation solving?

**Modular polynomials** parameterize \( \ell \)-isogenous \( j \)-invariants. We are looking for an \( \ell^n \)-isogeny between \( j_0 \) and \( j_n \):

\[
\Phi_\ell(j_0, X_1) = \Phi_\ell(X_1, X_2) = \Phi_\ell(X_2, X_3) = \ldots \\
\ldots = \Phi_\ell(X_{n-2}, X_{n-1}) = \Phi_\ell(X_{n-1}, j_n) = 0.
\]

Takahashi–Kudo–Ikematsu–Yasuda–Yokoyama (MathCrypt 2019): Throw this system into a **Gröbner basis algorithm** and pray.

Same paper: Plug start and end *curves* into Vélu’s formulas and solve for the kernel point.

Paper is still not online \( \sim \), but it works **exceptionally badly**.
Weil restrictions?

“The Dream”

"The Dream"


2. Hope that there is a class-group action of $\mathbb{Q}(\pi)$ on some $\mathbb{F}_p$-isogeny graph containing $A, A'$ (cf. dimension 1).
   - Chloe Martindale’s PhD thesis is about the ordinary case; apparently it should generalize.

3. Use Kuperberg’s subexponential quantum algorithm for the abelian hidden-shift problem to find an isogeny $\psi$ between the surfaces.

4. Hope we can solve the original problem better using $\psi$.

▶ Can we always “unrestrict” back to $\mathbb{F}_p^2$ somehow?

▶ Endomorphism-ring black magic?
Weil restrictions?

“The Dream”


2. Hope that there is a class-group action of $\mathbb{Q}(\pi)$ on some $\mathbb{F}_p$-isogeny graph containing $A, A'$ (cf. dimension 1).
   ▶ Chloe Martindale’s PhD thesis is about the ordinary case; apparently it should generalize.

3. Use Kuperberg’s subexponential quantum algorithm for the abelian hidden-shift problem to find an isogeny $\psi$ between the surfaces.

▶ Can we always “unrestrict” back to $\mathbb{F}_p^2$ somehow?
▶ Endomorphism-ring black magic?
“The Dream”


2. Hope that there is a class-group action of $\mathbb{Q}(\pi)$ on some $\mathbb{F}_p$-isogeny graph containing $A, A'$ (cf. dimension 1).
   - Chloe Martindale’s PhD thesis is about the ordinary case; apparently it should generalize.

3. Use Kuperberg’s subexponential quantum algorithm for the abelian hidden-shift problem to find an isogeny $\psi$ between the surfaces.

4. Hope we can solve the original problem better using $\psi$.
   - Can we always “unrestrict” back to $\mathbb{F}_p^2$ somehow?
   - Endomorphism-ring black magic?
Weil restrictions?

- **Educated guess:** If this works, the orbits are of size $\tilde{O}(\sqrt{p})$, so there should be $\approx \sqrt{p}$ orbits.
Weil restrictions?

- **Educated guess:** If this works, the orbits are of size $\tilde{O}(\sqrt{p})$, so there should be $\approx \sqrt{p}$ orbits.

From a supersingular elliptic curve $E/\mathbb{F}_{p^2}$, construct a superspecial abelian surface $A/\mathbb{F}_p$. 

(Picture not to scale.)
Weil restrictions?

- **Educated guess:** If this works, the orbits are of size $\tilde{O}(\sqrt{p})$, so there should be $\approx \sqrt{p}$ orbits.

- Kuperberg can only work if the two abelian surfaces are in the same orbit... which is exponentially unlikely.
Weil restrictions?

- **Educated guess**: If this works, the orbits are of size $\tilde{O}(\sqrt{p})$, so there should be $\approx \sqrt{p}$ orbits.

- Kuperberg can only work if the two abelian surfaces are in the same orbit... which is exponentially unlikely.

- There are more problems...
  - How to **compute the group action** in dimension 2?
  - Can we always **lift back** isogenies?
Lifting to $\mathbb{C}$?

“The Dream”

1. **Lift** $E, E'/\mathbb{F}_{p^2}$ to elliptic curves $\mathcal{E}, \mathcal{E}'$ defined over $\mathbb{C}$. 
Lifting to $\mathbb{C}$?

"The Dream"

1. Lift $E, E'/\mathbb{F}_p$ to elliptic curves $\mathcal{E}, \mathcal{E}'$ defined over $\mathbb{C}$.
2. Hope we can compute an isogeny $\Phi: \mathcal{E} \rightarrow \mathcal{E}'$. 
Lifting to \( \mathbb{C} \)?

"The Dream"

1. Lift \( E, E'/\mathbb{F}_p^2 \) to elliptic curves \( \mathcal{E}, \mathcal{E}' \) defined over \( \mathbb{C} \).
2. Hope we can compute an isogeny \( \Phi: \mathcal{E} \rightarrow \mathcal{E}' \).
3. Reduce \( \Phi \) back modulo \( p \) to get \( \varphi: E \rightarrow E' \).
Lifting to $\mathbb{C}$?

Well, none of this really seems to work:

- For the lifts to have a chance at being isogenous, we need to lift together \textbf{with an endomorphism} (cf. ordinary canonical lifts).
Lifting to \( \mathbb{C} \)?

Well, none of this really seems to work:

- For the lifts to have a chance at being isogenous, we need to lift together **with an endomorphism** (cf. ordinary canonical lifts).

- Thus, we need to **find** an endomorphism. If we can do this, we can already break SIDH without the added complexity\(^1\) of lifting.

\(^1\)Pun intended.
Lifting to $\mathbb{C}$?

Well, none of this really seems to work:

- For the lifts to have a chance at being isogenous, we need to lift together \textbf{with an endomorphism} (cf. ordinary canonical lifts).

- Thus, we need to \textbf{find} an endomorphism. If we can do this, we can already break SIDH without the added complexity\textsuperscript{1} of lifting.

- Even given an endomorphism, lifting is \textbf{prohibitively expensive} if its degree is not small.

\textsuperscript{1}Pun intended.
Lifting to $\mathbb{C}$?

Well, none of this really seems to work:

- For the lifts to have a chance at being isogenous, we need to lift together \textit{with an endomorphism} (cf. ordinary canonical lifts).

- Thus, we need to \textbf{find} an endomorphism. If we can do this, we can already break SIDH without the added complexity$^1$ of lifting.

- Even given an endomorphism, lifting is \textbf{prohibitively expensive} if its degree is not small.

- Computing an isogeny over $\mathbb{C}$ still \textit{seems hard}...

---

$^1$Pun intended.
Thank you!