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

What's this all about?

- 2011: David Jao & Luca De Feo come up with something now known as "**S**upersingular-**I**sogeny **D**iffie–**H**ellman".

What's this all about?

- 2011: David Jao & Luca De Feo come up with something now known as "**S**upersingular-**I**sogeny **D**iffie–**H**ellman".
- 2020$-\varepsilon$: 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 "**S**upersingular-**I**sogeny **D**iffie–**H**ellman".
- 2020$-\varepsilon$: 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.

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.

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

$$[m]\colon E \to E$$

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

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

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 #2: For any a and b, the map $\iota\colon (x, y) \mapsto (-x, \sqrt{-1} \cdot y)$ 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 $\{\infty\}$.

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

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

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

Isogeny kernels

For any finite subgroup G of E, there exists a unique[1] separable isogeny $\varphi_G \colon E \to E'$ with kernel G.

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

If G is defined over k, then φ_G and E/G are also defined over k.

[1](up to isomorphism of E')

Isogeny kernels

For any finite subgroup G of E, there exists a unique[1] separable isogeny $\varphi_G \colon E \to E'$ with kernel G.

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

If G is defined over k, then φ_G and E/G are also defined over k.

Vélu '71:
Formulas for computing E/G and evaluating φ_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 $\varphi_G \colon E \to E'$ with kernel G.

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

If G is defined over k, then φ_G and E/G are also defined over k.

Vélu '71:
Formulas for computing E/G and evaluating φ_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 (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 $\varphi_G \colon E \to E/G$.

Smooth isogenies

- In SIDH, $\#A = 2^n$ and $\#B = 3^m$ are "crypto-sized". Vélu's formulas take $\Theta(\#G)$ to compute $\varphi_G \colon E \to E/G$.

Smooth isogenies

- In SIDH, $\#A = 2^n$ and $\#B = 3^m$ are "crypto-sized".
  Vélu's formulas take $\Theta(\#G)$ to compute $\varphi_G \colon E \to E/G$.

!! Evaluate φ_G as a chain of small-degree isogenies:
For $G \cong \mathbb{Z}/\ell^k$, set $\ker \psi_i := [\ell^{k-i}](\psi_{i-1} \circ \cdots \circ \psi_1)(G)$.

$$\begin{tikzcd} E \arrow[r, "\psi_1"] \arrow[rrrr, bend right, "\varphi_G"'] & E_1 \arrow[r, "\psi_2"] & \ldots \arrow[r, "\psi_{k-1}"] & E_{k-1} \arrow[r, "\psi_k"] & E/G \end{tikzcd}$$

Smooth isogenies

- In SIDH, $\#A = 2^n$ and $\#B = 3^m$ are "crypto-sized".
  Vélu's formulas take $\Theta(\#G)$ to compute $\varphi_G \colon E \to E/G$.

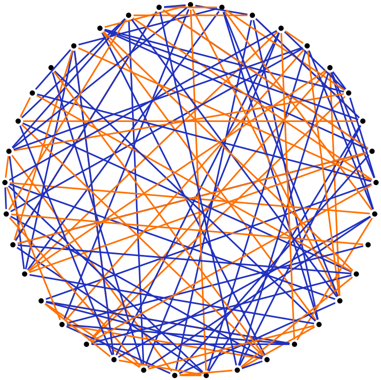
!! Evaluate φ_G as a chain of small-degree isogenies:
For $G \cong \mathbb{Z}/\ell^k$, set $\ker \psi_i := [\ell^{k-i}](\psi_{i-1} \circ \cdots \circ \psi_1)(G)$.

$$\begin{tikzcd} E \arrow[r, "\psi_1"] \arrow[rrrr, bend right, "\varphi_G"'] & E_1 \arrow[r, "\psi_2"] & \dots \arrow[r, "\psi_{k-1}"] & E_{k-1} \arrow[r, "\psi_k"] & E/G \end{tikzcd}$$

$\rightsquigarrow$ Complexity: $O(k^2 \cdot \ell)$. Exponentially smaller than ℓ^k!
"Optimal strategy" improves this to $O(k \log k \cdot \ell)$.

Isogeny graphs

- Graph view: Each ψ_i is a step in the ℓ-isogeny graph.



($q = 431^2$, degrees 2, 3)

Reminder:

SIDH

for those who missed David Jao's ECC talk 8 years ago $\ddot\smile$

SIDH: High-level view

E

SIDH: High-level view

E $\quad$ A

B

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

SIDH: High-level view

$$\begin{tikzcd} E \arrow[r, "\varphi_A"] \arrow[d, "\varphi_B"'] & E/A \\ E/B & \end{tikzcd}$$

- 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

$$\begin{tikzcd} E \arrow[r, "\varphi_A"] \arrow[d, "\varphi_B"'] & E/A \\ E/B & \end{tikzcd}$$

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

SIDH: High-level view

$$
\begin{tikzcd}
E \arrow[r, "\varphi_A"] \arrow[d, "\varphi_B"'] & E/A \arrow[d, phantom, "B'"] \\
E/B \arrow[r, phantom, "A'"'] & {}
\end{tikzcd}
$$

- Alice & Bob pick secret subgroups A and B of E.
- Alice computes $\varphi_A \colon E \to E/A$; Bob computes $\varphi_B \colon E \to E/B$.
  (These isogenies correspond to walking in the isogeny graph.)
- Alice and Bob transmit the values E/A and E/B.
- Alice <u>somehow</u> obtains $A' := \varphi_B(A)$. (Similar for Bob.)

SIDH: High-level view

$$\begin{tikzcd} E \arrow[r, "\varphi_A"] \arrow[d, "\varphi_B"'] & E/A \arrow[d, "\varphi_{B'}"] \\ E/B \arrow[r, "\varphi_{A'}"'] & E/\langle A, B\rangle \end{tikzcd}$$

- Alice & Bob pick secret subgroups A and B of E.
- Alice computes $\varphi_A \colon E \to E/A$; Bob computes $\varphi_B \colon E \to E/B$.
  (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.)
- 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 $A' := \varphi_B(A)$."

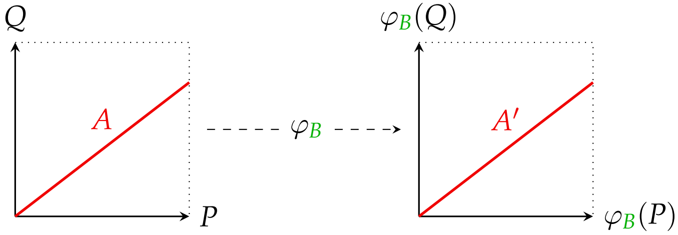
Alice knows only A, Bob knows only φ_B. Hm.

SIDH's auxiliary points

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

Alice knows only A, Bob knows only φ_B. Hm.

Solution: φ_B is a group homomorphism!

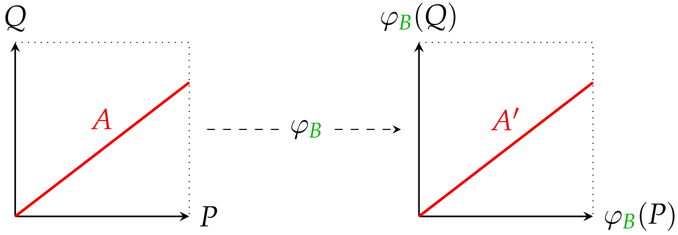


SIDH's auxiliary points

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

Alice knows only A, Bob knows only φ_B. Hm.

Solution: φ_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.

$\Longrightarrow$ Now Alice can compute A' as $\langle \varphi_B(P) + [a]\varphi_B(Q) \rangle$!

SIDH in one slide

Public parameters:

- a large prime $p = 2^n 3^m - 1$ 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	public	Bob
$a \xleftarrow{\text{random}} \{0 \dots 2^n - 1\}$		$b \xleftarrow{\text{random}} \{0 \dots 3^m - 1\}$
$A := \langle P_A + [a]Q_A \rangle$ compute $\varphi_A : E \to E/A$		$B := \langle P_B + [b]Q_B \rangle$ compute $\varphi_B : E \to E/B$
$E/A,\ \varphi_A(P_B),\ \varphi_A(Q_B)$		$E/B,\ \varphi_B(P_A),\ \varphi_B(Q_A)$
$A' := \langle \varphi_B(P_A) + [a]\varphi_B(Q_A) \rangle$ $s := j\big((E/B)/A'\big)$		$B' := \langle \varphi_A(P_B) + [b]\varphi_A(Q_B) \rangle$ $s := j\big((E/A)/B'\big)$

Disclaimer:

All of the following is “obvious” to experts.

Extra points: Information theory

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

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

$\Longrightarrow$ 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.

$\rightsquigarrow$ Rational-function interpolation?

Extra points: Interpolation?

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

$\rightsquigarrow$ Rational-function interpolation?

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

$\rightsquigarrow$ 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.

$\rightsquigarrow$ Rational-function interpolation?

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

$\rightsquigarrow$ 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 φ_A to some $> 3^m$-torsion?

e.g. we win if we get the action of φ_A on the 2^n-torsion.

Extra points: Group theory?

- Can we extrapolate the action of φ_A to some $> 3^m$-torsion?

e.g. we win if we get the action of φ_A on the 2^n-torsion.

$\ddot{\frown}$ There's an isomorphism of groups

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

Extra points: Group theory?

- Can we extrapolate the action of φ_A to some $> 3^m$-torsion?

e.g. we win if we get the action of φ_A on the 2^n-torsion.

$\ddot{\frown}$ There's an isomorphism of groups

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

$\Longrightarrow$ 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 φ_A to some $> 3^m$-torsion?

e.g. we win if we get the action of φ_A on the 2^n-torsion.

☹ There's an isomorphism of groups

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

$\Longrightarrow$ 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 ℓ-torsion, say ℓ^{n+1}?

Extra points: Effective Tate?

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

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

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

Extra points: Effective Tate?

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

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

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

☹ Same problem; group-theoretically there are ℓ^4 ways to lift.

Extra points: Effective Tate?

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

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

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

☹ Same problem; group-theoretically there are ℓ^4 ways to lift.

!! We know more: The degree!

Extra points: Effective Tate?

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

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

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

☹ Same problem; group-theoretically there are ℓ^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 ℓ-torsion, say ℓ^{n+1}?

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

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

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

$\frown$ We know more: The degree! ($\ell \nmid \det$; almost no use.)

- This idea works slightly better for *endo*morphisms (characteristic polynomial constrains to ℓ^2 choices).

Extra points: Petit's endomorphisms (1)

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

Extra points: Petit's endomorphisms (1)

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

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

$$
\begin{tikzcd}
E_0 \arrow[loop left, "\vartheta"] \arrow[r, bend left, "\varphi_A"] & E_A \arrow[l, bend left, "\widehat{\varphi_A}"]
\end{tikzcd}
$$

Extra points: Petit's endomorphisms (1)

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

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

$$\begin{tikzcd} E_0 \arrow[loop left, "\vartheta"] \arrow[rr, bend left, "\varphi_A"] & & E_A \arrow[ll, bend left, "\widehat{\varphi_A}"] \end{tikzcd}$$

$\rightsquigarrow$ We can evaluate endomorphisms of E_A in the subring $R = \left\{ \varphi_A \circ \vartheta \circ \widehat{\varphi_A} \;\middle|\; \vartheta \in \mathrm{End}(E_0) \right\}$ on the 3^m-torsion.

Extra points: Petit's endomorphisms (1)

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

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

$$\begin{tikzcd}
E_0 \arrow[loop left, "\vartheta"] \arrow[rr, bend left, "\varphi_A"] & & E_A \arrow[ll, bend left, "\widehat{\varphi_A}"]
\end{tikzcd}$$

$\rightsquigarrow$ We can evaluate endomorphisms of E_A in the subring $R = \left\{ \varphi_A \circ \vartheta \circ \widehat{\varphi_A} \;\middle|\; \vartheta \in \mathrm{End}(E_0) \right\}$ on the 3^m-torsion.

- Idea: Find $\tau \in R$ of degree $3^m r$; recover 3^m-part from known action; brute-force the $r$emaining part.
  $\Longrightarrow$ (details) $\Longrightarrow$ Recover φ_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 $p = 2^n 3^m - 1$.)

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 $p = 2^n3^m - 1$.)

$\Longrightarrow$ Unless $3^m \gg 2^n$, there is no hope to find τ 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

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

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 $p = 2^n 3^m - 1$.)

$\Longrightarrow$ Unless $3^m \gg 2^n$, there is no hope to find τ with $3^m \mid \deg \tau$ and $\deg \tau / 3^m < 2^n$.

$\Longrightarrow$ 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.

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

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

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

  $\Longrightarrow$ 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.

$\Longrightarrow$ 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.

  $\ddot{\frown}$

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.

  $\ddot\frown$

- Petit's approach cannot be expected to work for "real" (symmetric, two-party) SIDH.

  $\ddot\frown$

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.

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.
  (This "invention" has been filed for patent in Canada...)

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. (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...

...we'll be right back after a short commercial break...

[ˈsiːˌsaɪd]

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

$\rightsquigarrow$ much closer to post-quantum Diffie–Hellman than SIDH $\ddot\smile$.

The pure isogeny problem

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

The pure isogeny problem

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

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 $\varphi\colon E \to E'$.

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 ℓ-isogenous j-invariants.
We are looking for an ℓ^n-isogeny between j_0 and j_n:

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

Equation solving?

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

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

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

Equation solving?

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

$$\begin{aligned}\Phi_\ell(j_0, X_1) = \Phi_\ell(X_1, X_2) = \Phi_\ell(X_2, X_3) = \dots \\ \dots = \Phi_\ell(X_{n-2}, X_{n-1}) = \Phi_\ell(X_{n-1}, j_n) = 0.\end{aligned}$$

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 ℓ-isogenous j-invariants.
We are looking for an ℓ^n-isogeny between j_0 and j_n:

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

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 ¯_(ツ)_/¯, but it works exceptionally badly.

Weil restrictions?

"The Dream"

1. View $E, E'/\mathbb{F}_{p^2}$ as abelian surfaces A, A' over $\mathbb{F}_p$.

Weil restrictions?

"The Dream"

1. View $E, E'/\mathbb{F}_{p^2}$ as abelian surfaces A, A' over $\mathbb{F}_p$.
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.

Weil restrictions?

“The Dream”

1. View $E, E'/\mathbb{F}_{p^2}$ as abelian surfaces A, A' over $\mathbb{F}_p$.
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 ψ between the surfaces.

Weil restrictions?

<u>"The Dream"</u>

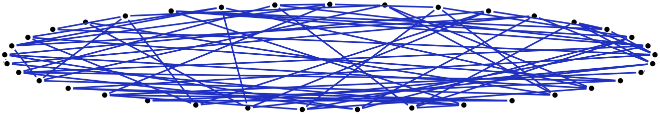
1. View $E, E'/\mathbb{F}_{p^2}$ as abelian surfaces A, A' over $\mathbb{F}_p$.
2. Hope that there is a class-group action of $\mathbb{Q}(\pi)$ on some $\mathbb{F}_p$-isogeny graph containing A, A' (cf. dimension 1).
   - Chloe Martindale's PhD thesis is about the ordinary case; apparently it *should* generalize.
3. Use Kuperberg's subexponential quantum algorithm for the abelian hidden-shift problem to find an isogeny ψ between the surfaces.
4. Hope we can solve the original problem better using ψ.
   - 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 $\widetilde{O}(\sqrt{p})$, so there should be $\approx \sqrt{p}$ orbits.

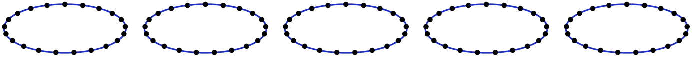
Weil restrictions?

- <u>Educated guess</u>: *If* this works, the orbits are of size $\widetilde{O}(\sqrt{p})$, 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 $\widetilde{O}(\sqrt{p})$, 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 $\widetilde{O}(\sqrt{p})$, 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 $\mathbb{C}$?

<u>"The Dream"</u>

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 $\Phi\colon \mathcal{E} \to \mathcal{E}'$.

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 $\Phi \colon \mathcal{E} \to \mathcal{E}'$.
3. Reduce Φ back modulo p to get $\varphi \colon E \to E'$.

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

[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 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.
- Even given an endomorphism, lifting is prohibitively expensive if its degree is not small.
- Computing an isogeny over $\mathbb{C}$ still seems hard...

[1] Pun intended.

Thank you!