How to not break SIDH :(

Chloe Martindale[1] Lorenz Panny[2]

[1]University of Bristol [2]TU/e

Royal Holloway, 29th April 2021

CFAIL

Conference for Failed Attempts and Insightful Losses

Submission deadline 2021: 1st May (3-page abstract)

What is this all about?

Diffie–Hellman key exchange '76

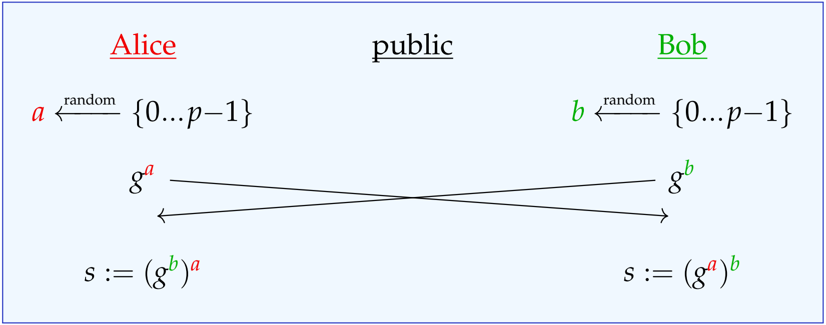
Public parameters:

- 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



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

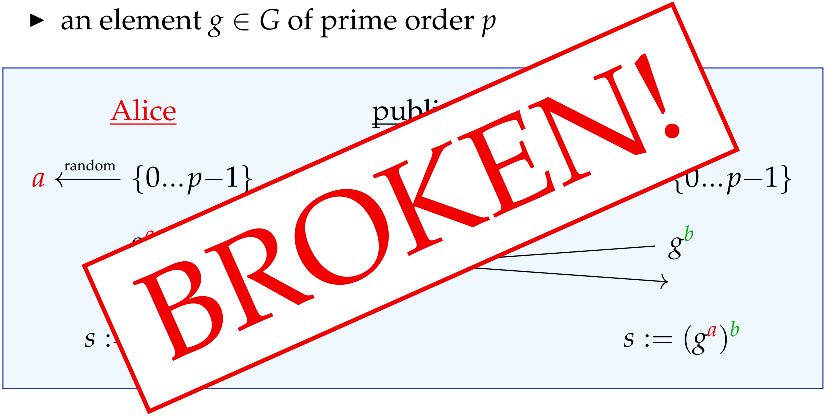
Alice	public	Bob
$a \xleftarrow{\text{random}} \{0 \ldots p-1\}$		$b \xleftarrow{\text{random}} \{0 \ldots p-1\}$
g^a	$\longrightarrow$	g^b
	$\longleftarrow$	
$s := (g^b)^a$		$s := (g^a)^b$

Fundamental reason this works: $\cdot^a$ and $\cdot^b$ are commutative!

Diffie–Hellman key exchange ’76

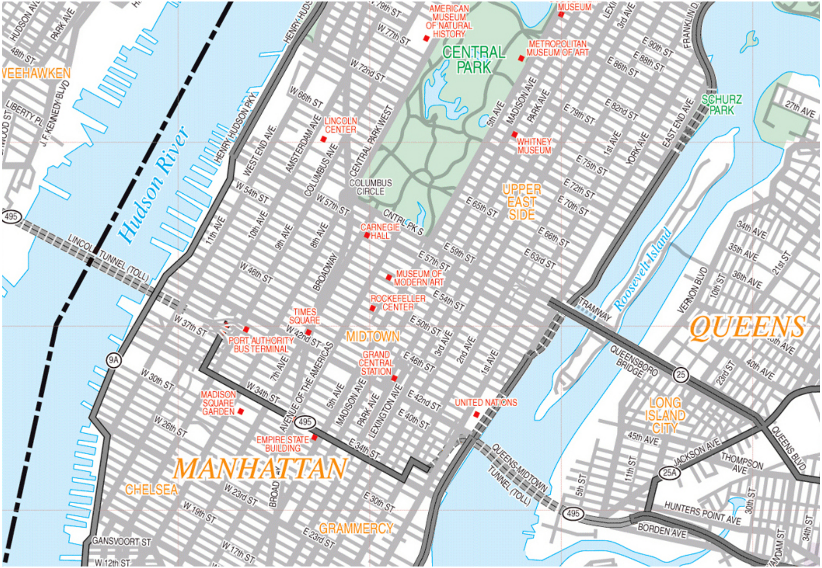
Public parameters:

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

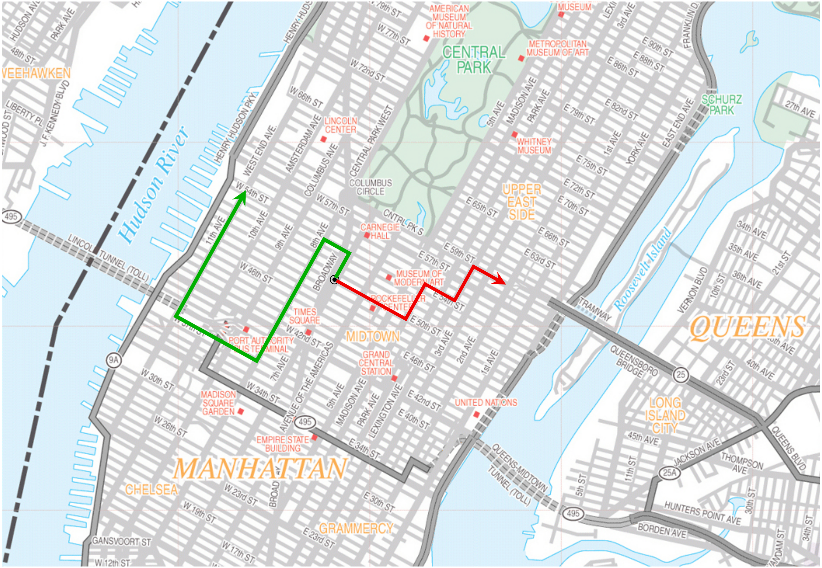


Fundamental reason this works: $\cdot^a$ and $\cdot^b$ are commutative!

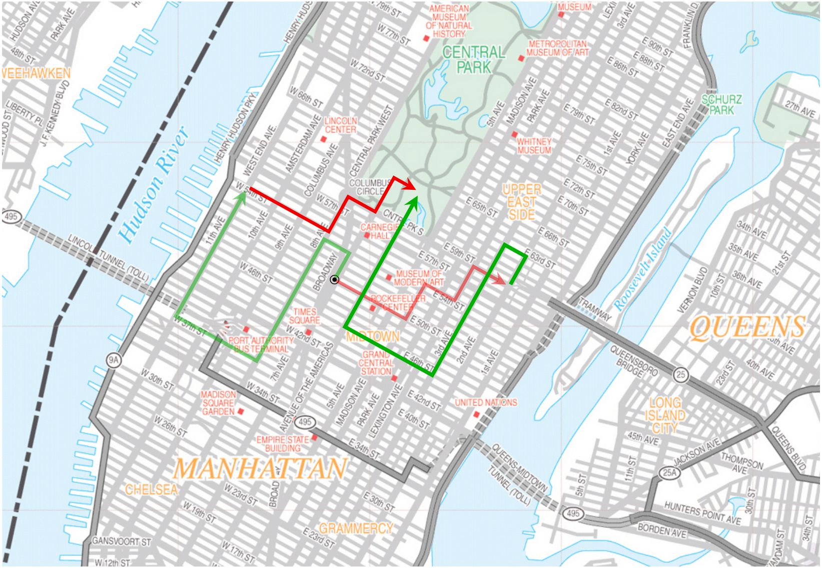
Graph walking Diffie–Hellman?



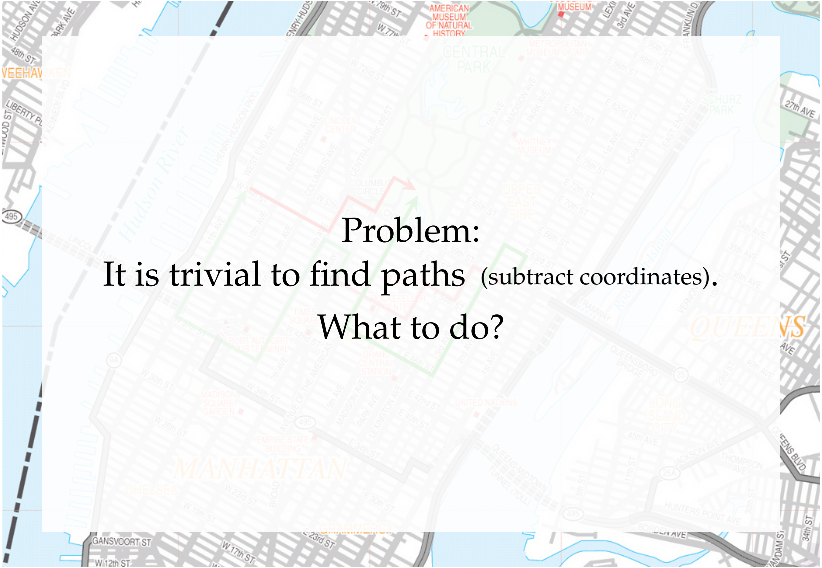
Graph walking Diffie–Hellman?



Graph walking Diffie–Hellman?



Graph walking Diffie–Hellman?



Problem:

It is trivial to find paths (subtract coordinates).

What to 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.

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 maths.

Maths slide 1/5: Elliptic curves *(nodes)*

An elliptic curve (modulo details) is given by an equation

$$E\colon\ y^2 = x^3 + ax + b.$$

A point on E is a solution to this equation *or* the 'fake' point ∞.

Maths slide 1/5: Elliptic curves *(nodes)*

An elliptic curve (modulo details) is given by an equation

$$E\colon\ y^2 = x^3 + ax + b.$$

A point on E is a solution to this equation *or* the 'fake' point ∞.

E is an abelian group: we can 'add' points.

- The neutral element is ∞.
- The inverse of (x, y) is $(x, -y)$.
- The sum of (x_1, y_1) and (x_2, y_2) is

$$\left(\lambda^2 - x_1 - x_2,\ \lambda(2x_1 + x_2 - \lambda^2) - y_1\right)$$

do **not** remember these formulas!

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.

Maths slide 2/5: 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.

Maths slide 2/5: 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.

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

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

Maths slide 2/5: 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.

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 $\{\infty\}$.

Maths slide 2/5: 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.

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 $\{(2, 9), (2, -9), \infty\}$.

Maths slide 2/5: 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 $\mathrm{End}(E)$.

Maths slide 2/5: 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 $\mathrm{End}(E)$.

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

Maths slide 3/5: Isogenies and 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')

Maths slide 3/5: Isogenies and 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')

Maths slide 3/5: Isogenies and 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 why we use supersingular curves!

[1](up to isomorphism of E')

Maths slide 4/5: Endomorphisms and torsion points

An endomorphism of an elliptic curve E is an isogeny $E \to E$, or the zero map.

Maths slide 4/5: Endomorphisms and torsion points

An endomorphism of an elliptic curve E is an isogeny $E \to E$, or the zero map.

Example: The multiplication-by-m map

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

is an endomorphism.

Maths slide 4/5: Endomorphisms and torsion points

An endomorphism of an elliptic curve E is an isogeny $E \to E$, or the zero map.

Example: The multiplication-by-m map

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

is an endomorphism. If $m \neq 0$ in the base field, its kernel is

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

Maths slide 4/5: Endomorphisms and torsion points

An endomorphism of an elliptic curve E is an isogeny $E \to E$, or the zero map.

Example: The multiplication-by-m map

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

is an endomorphism. If $m \neq 0$ in the base field, its kernel is

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

- A point $P \in E[m]$ is called an m-torsion point.

Maths slide 4/5: Endomorphisms and torsion points

An endomorphism of an elliptic curve E is an isogeny $E \to E$, or the zero map.

Example: The multiplication-by-m map

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

is an endomorphism. If $m \neq 0$ in the base field, its kernel is

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

- A point $P \in E[m]$ is called an m-torsion point.
- The group $G = \langle P \rangle$ generated by an m-torsion point $P \in E[m]$ is the kernel of an m-isogeny written

$$f : E \to E/G.$$

Maths slide 5/5: Supersingular isogeny graphs

$E/\overline{\mathbb{F}_p}$ is *supersingular* if it has no points of order p.

Maths slide 5/5: Supersingular isogeny graphs

$E/\overline{\mathbb{F}_p}$ is *supersingular* if it has no points of order p.

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

For this talk: the supersingular S-isogeny graph consists of:

- vertices given by isomorphism classes of supersingular elliptic curves,
- edges $E — E'$ that represent an ℓ-isogeny $E \to E'$ and its dual $E' \to E$, where $\ell \in S$ (up to isomorphism)

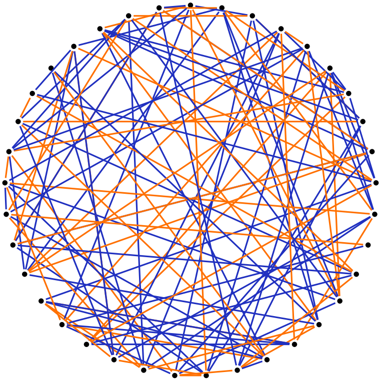
both defined over $\overline{\mathbb{F}_p}$.

SIDH as an isogeny graph

- **Vertices**: isomorphism classes of elliptic curves defined over $\overline{\mathbb{F}_p}$.
- **Edges**: 2- and 3-isogenies of elliptic curves (up to some equivalence).

SIDH as an isogeny graph

- **Vertices**: isomorphism classes of elliptic curves defined over $\overline{\mathbb{F}_p}$.
- **Edges**: 2- and 3-isogenies of elliptic curves (up to some equivalence).



2 and 3-isogenies of elliptic curves over $\mathbb{F}_{431^2}$

Now:

SIDH

SIDH: the dirty details

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 $E[3^m]$

SIDH: the dirty details

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
$a \xleftarrow{\text{random}} \{0 \ldots 2^n - 1\}$		$b \xleftarrow{\text{random}} \{0 \ldots 3^m - 1\}$

SIDH: the dirty details

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
$a \xleftarrow{\text{random}} \{0 \dots 2^n - 1\}$		$b \xleftarrow{\text{random}} \{0 \dots 3^m - 1\}$
$A := \langle P_A + [a]Q_A \rangle$		$B := \langle P_B + [b]Q_B \rangle$

SIDH: the dirty details

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
$a \xleftarrow{\text{random}} \{0 \ldots 2^n - 1\}$		$b \xleftarrow{\text{random}} \{0 \ldots 3^m - 1\}$
$A := \langle P_A + [a]Q_A \rangle$		$B := \langle P_B + [b]Q_B \rangle$
compute $\varphi_A : E \to E/A$		compute $\varphi_B : E \to E/B$

SIDH: the dirty details

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
$a \xleftarrow{\text{random}} \{0 \ldots 2^n - 1\}$		$b \xleftarrow{\text{random}} \{0 \ldots 3^m - 1\}$
$A := \langle P_A + [a]Q_A \rangle$		$B := \langle P_B + [b]Q_B \rangle$
compute $\varphi_A : E \to E/A$		compute $\varphi_B : E \to E/B$
$E/A,\ \varphi_A(P_B),\ \varphi_A(Q_B)$		$E/B,\ \varphi_B(P_A),\ \varphi_B(Q_A)$

SIDH: the dirty details

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
$a \xleftarrow{\text{random}} \{0 \ldots 2^n - 1\}$		$b \xleftarrow{\text{random}} \{0 \ldots 3^m - 1\}$
$A := \langle P_A + [a]Q_A \rangle$		$B := \langle P_B + [b]Q_B \rangle$
compute $\varphi_A : E \to E/A$		compute $\varphi_B : E \to E/B$
$E/A,\ \varphi_A(P_B),\ \varphi_A(Q_B)$	$\longleftrightarrow$	$E/B,\ \varphi_B(P_A),\ \varphi_B(Q_A)$
$A' := \langle \varphi_B(P_A) + [a]\varphi_B(Q_A) \rangle$		$B' := \langle \varphi_A(P_B) + [b]\varphi_A(Q_B) \rangle$

SIDH: the dirty details

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

SIDH: the dirty details

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

Break it by: given public info, find secret key: φ_A (or just A).

Here's some things that don't break it...

Extra points

Aim: given points P_B, Q_B on E, the image E/A of the secret isogeny $\varphi_A : E \to E/A$, and the images $\varphi_A(P_B)$ and $\varphi_B(Q_B)$, find φ_A.

Fact: with the parameters used in SIDH, the images $\varphi_A(P_B)$ and $\varphi_B(Q_B)$ uniquely determine the secret isogeny φ_A.

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.

$\rightsquigarrow$ 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.

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.

Extra points: Group theory?

- Recall: we know the image under φ_A of 3^m-torsion points P_B and Q_B.

Extra points: Group theory?

- Recall: we know the image under φ_A of 3^m-torsion points P_B and Q_B.
- Can we extrapolate the image under φ_A of some other (coprime) ℓ^n-torsion points and exploit it?

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

Extra points: Group theory?

- Recall: we know the image under φ_A of 3^m-torsion points P_B and Q_B.
- Can we extrapolate the image under φ_A of some other (coprime) ℓ^n-torsion points and exploit it?

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

$\frown$ 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?

- Recall: we know the image under φ_A of 3^m-torsion points P_B and Q_B.
- Can we extrapolate the image under φ_A of some other (coprime) ℓ^n-torsion points and exploit it?

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

☹ There's an isomorphism of groups

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

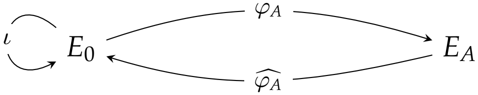
$\Longrightarrow$ can't learn anything about 2^n from 3^m using groups alone.
(Annoying: This shows up in many disguises.)

Extra points: Petit's endomorphisms

- For typical SIDH parameters, we know the endomorphism ring $\mathrm{End}(E_0)$.

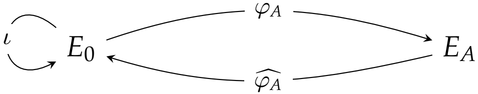
Extra points: Petit's endomorphisms

- For typical SIDH parameters, we know the endomorphism ring $\mathrm{End}(E_0)$.
- Going back and forth to E_0 yields endomorphisms of E_A:



Extra points: Petit's endomorphisms

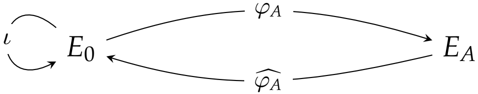
- For typical SIDH parameters, we know the endomorphism ring $\mathrm{End}(E_0)$.
- Going back and forth to E_0 yields endomorphisms of E_A:



$\rightsquigarrow$ We can compute the image of our 3^m-torsion points on E_A under these endomorphisms.

Extra points: Petit's endomorphisms

- For typical SIDH parameters, we know the endomorphism ring $\mathrm{End}(E_0)$.
- Going back and forth to E_0 yields endomorphisms of E_A:



$\rightsquigarrow$ We can compute the image of our 3^m-torsion points on E_A under these endomorphisms.

- Idea: Find an appropriate endomorphism τ of degree $3^m r$; recover 3^m-part as above; brute-force the $r$emaining part.
  $\rightsquigarrow$ image of r-torsion point under φ_A
  $\Longrightarrow$ (details) $\Longrightarrow$ Recover the secret φ_A.

$\frown$ To get r small enough to be an attack, we have to change the SIDH parameters so that Alice's isogeny has a much higher degree than Bob's.

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.

  $\ddot\frown$

[1]Check `eprint.iacr.org/2020/633` Section 8 for a generalised approach that has more of a chance...

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.[1]

  ☹

[1] Check `eprint.iacr.org/2020/633` Section 8 for a generalised approach that has more of a chance...

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.[1]

  $\ddot\frown$

- Life sucks.

[1] Check `eprint.iacr.org/2020/633` Section 8 for a generalised approach that has more of a chance...

The pure isogeny problem

Fundamental problem: given supersingular E and $E'/\mathbb{F}_{p^2}$ that are ℓ^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 $P \in E(\overline{\mathbb{F}_p})$ 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 $f : E \to E'$.

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.
- 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 $P \in E(\overline{\mathbb{F}_p})$ 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.

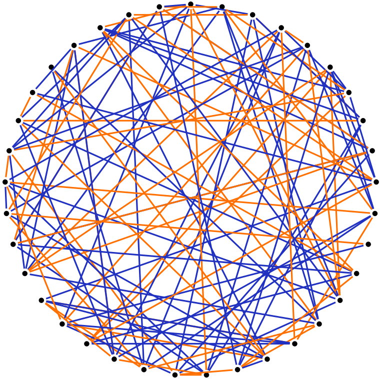
Solution (b) is meet-in-the-middle: complexity $\tilde{O}(p^{1/4})$.

Exploiting subgraphs

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

Exploiting subgraphs

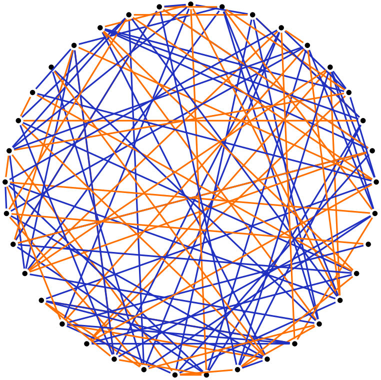
The SIDH graph has a $\mathbb{F}_p$-subgraph:



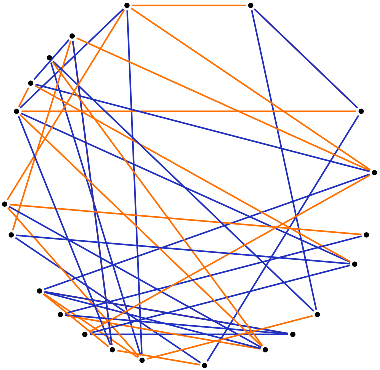
2, 3-isogenies
over $\mathbb{F}_{431^2}$

Exploiting subgraphs

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

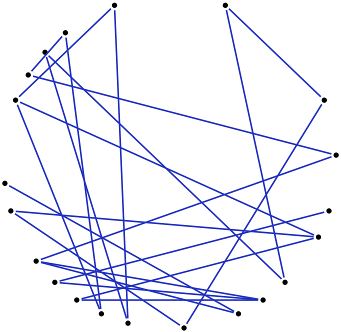


2, 3-isogenies
over $\mathbb{F}_{431^2}$



2, 3-isogenies
over $\mathbb{F}_{431}$

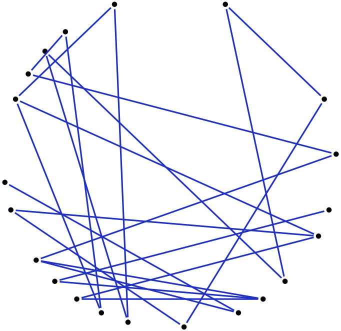
Exploiting subgraphs?



3-isogenies

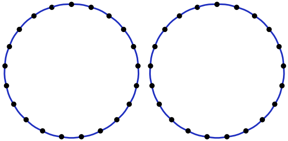
nodes up to $\overline{\mathbb{F}_{431}}$-isomorphism

Exploiting subgraphs?



3-isogenies

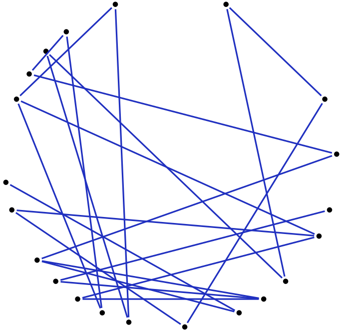
nodes up to $\overline{\mathbb{F}_{431}}$-isomorphism



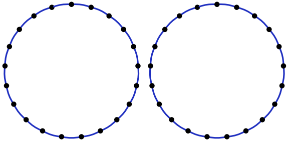
3-isogenies

nodes up to $\mathbb{F}_{431}$-isomorphism

Exploiting subgraphs?



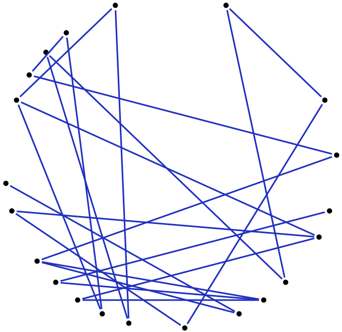
3-isogenies
nodes up to $\overline{\mathbb{F}_{431}}$-isomorphism



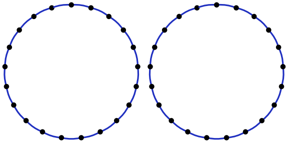
3-isogenies
nodes up to $\mathbb{F}_{431}$-isomorphism

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

Exploiting subgraphs?



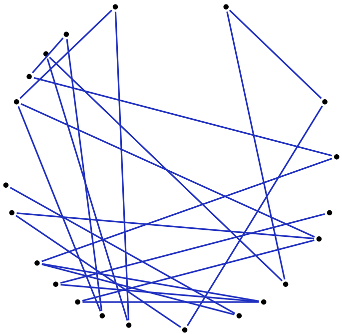
3-isogenies
nodes up to $\overline{\mathbb{F}_{431}}$-isomorphism



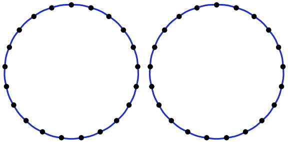
3-isogenies
nodes up to $\mathbb{F}_{431}$-isomorphism

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?



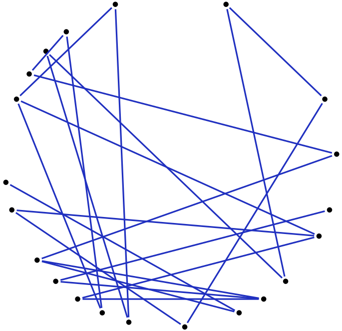
3-isogenies
nodes up to $\overline{\mathbb{F}_{431}}$-isomorphism



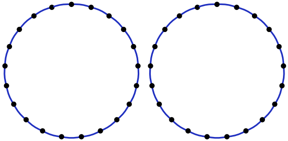
3-isogenies
nodes up to $\mathbb{F}_{431}$-isomorphism

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?



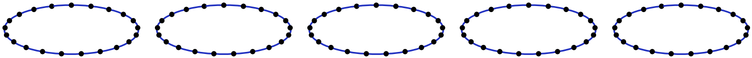
3-isogenies
nodes up to $\overline{\mathbb{F}_{431}}$-isomorphism



3-isogenies
nodes up to $\mathbb{F}_{431}$-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)

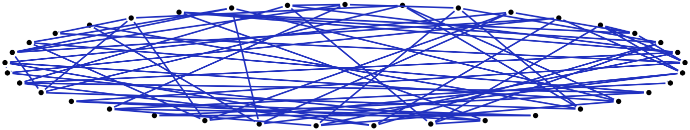
More graphs defined over $\mathbb{F}_p$



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: $O(1/\sqrt{p})$. $\ddot\frown$

More equivalent categories: lifting to $\mathbb{C}$

$$\left\{ \begin{array}{c} \text{Elliptic curves } E \text{ defined over } \mathbb{C} \\ \text{with } \operatorname{End}(E) = R \end{array} \right\}$$

Here computing isogenies is easy!

$$\updownarrow$$

$$\left\{ \begin{array}{c} \text{Non-supersingular elliptic curves defined over } \mathbb{F}_q \\ \text{with } \operatorname{End}(E) = R \end{array} \right\}$$

Here computing isogenies is harder.

More equivalent categories: lifting to $\mathbb{C}$

A well-chosen subset of

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

Here computing isogenies is easy!

$$\updownarrow$$

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

Here computing isogenies is harder.

More equivalent categories: lifting to $\mathbb{C}$

A well-chosen subset of

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

Here computing isogenies is easy!

$$\updownarrow$$

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

Here computing isogenies is harder.

- Computing the equivalence is slow.

More equivalent categories: lifting to $\mathbb{C}$

A well-chosen subset of

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

Here computing isogenies is easy!

$$\updownarrow$$

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

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

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

Here computing isogenies is easy!

$$\updownarrow$$

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

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!