What are isogenies and why do we care?

Lorenz Panny

Technische Universiteit Eindhoven

Amsterdam, Netherlands, 4 October 2019

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 efficient* algorithms to recover paths from endpoints.
  (*Both* classical and quantum!)

Big picture

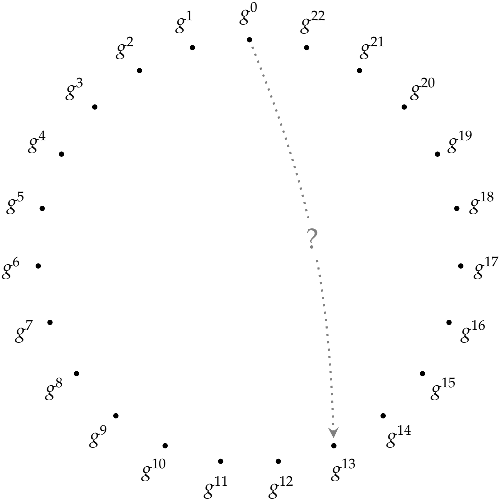
- Isogenies are a source of exponentially-sized graphs.
- We can walk efficiently on these graphs.
- Fast mixing: short paths to (almost) all nodes.
- No efficient* algorithms to recover paths from endpoints.
  (*Both* classical and quantum!)
- Enough structure to navigate the graph meaningfully.
  That is: some *well-behaved* “directions” to describe paths.

Big picture

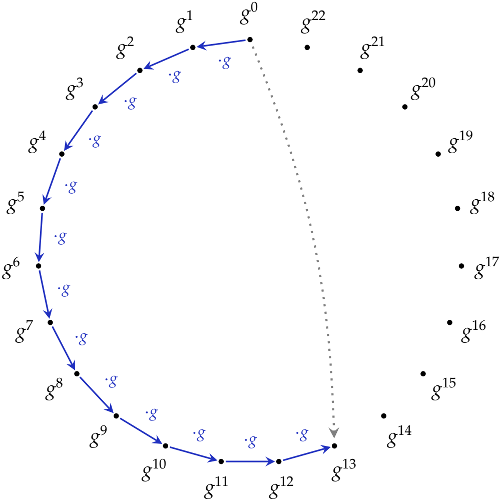
- Isogenies are a source of exponentially-sized graphs.
- We can walk efficiently on these graphs.
- Fast mixing: short paths to (almost) all nodes.
- No efficient* algorithms to recover paths from endpoints.
  (*Both* classical and quantum!)
- Enough structure to navigate the graph meaningfully.
  That is: some *well-behaved* “directions” to describe paths.

It is easy to construct graphs that satisfy *almost* all of these —
but getting all at once seems rare. Isogenies!

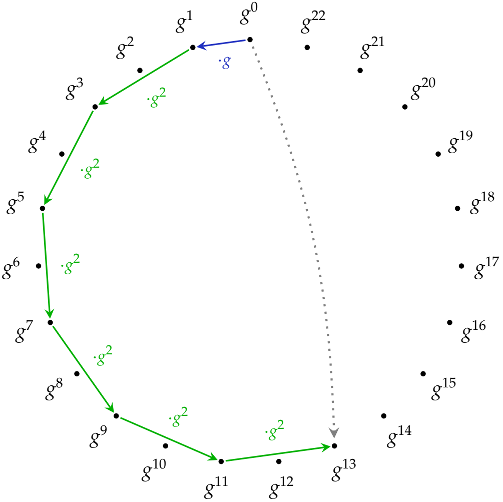
Crypto on graphs?


g^0
g^1
g^2
g^3
g^4
g^5
g^6
g^7
g^8
g^9
g^{10}
g^{11}
g^{12}
g^{13}
g^{14}
g^{15}
g^{16}
g^{17}
g^{18}
g^{19}
g^{20}
g^{21}
g^{22}
?

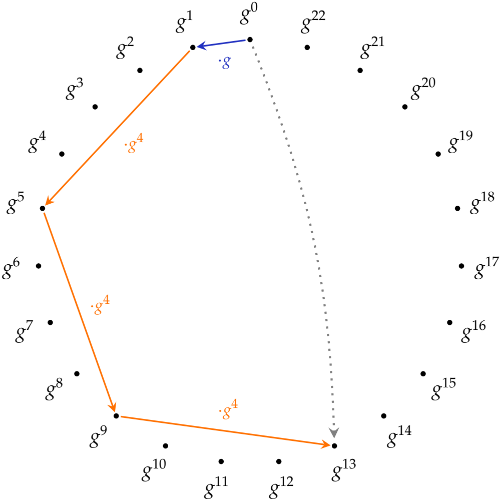
multiply


g^0
g^1
g^2
g^3
g^4
g^5
g^6
g^7
g^8
g^9
g^{10}
g^{11}
g^{12}
g^{13}
g^{14}
g^{15}
g^{16}
g^{17}
g^{18}
g^{19}
g^{20}
g^{21}
g^{22}
$\cdot g$
$\cdot g$
$\cdot g$
$\cdot g$
$\cdot g$
$\cdot g$
$\cdot g$
$\cdot g$
$\cdot g$
$\cdot g$
$\cdot g$
$\cdot g$
$\cdot g$

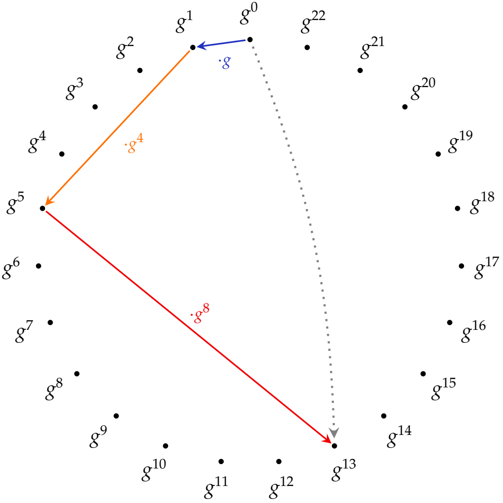
Square-and-multiply



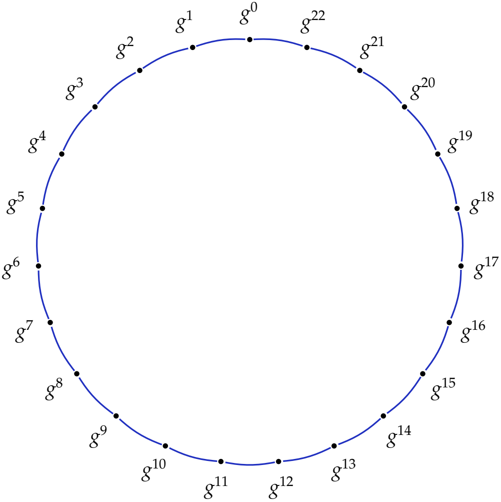
Square-and-multiply-and-square-and-multiply



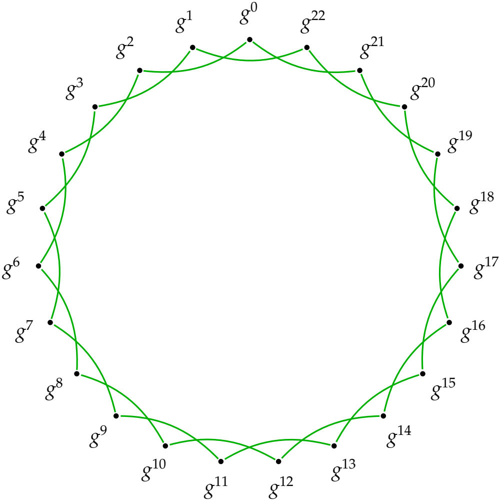
Square-and-multiply-and-square-and-multiply-and-squ



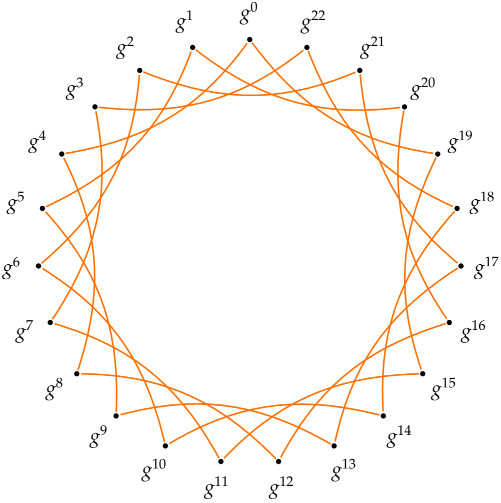
Square-and-multiply as graphs



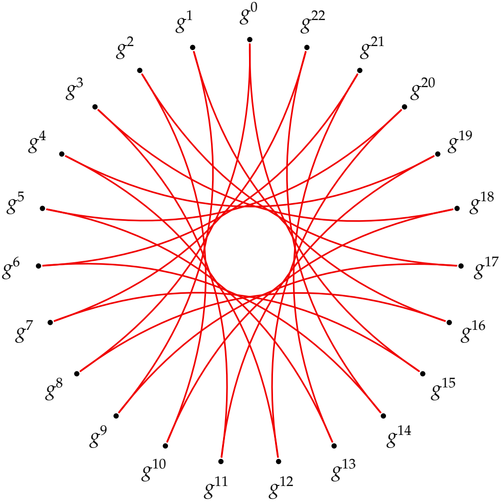
Square-and-multiply as graphs



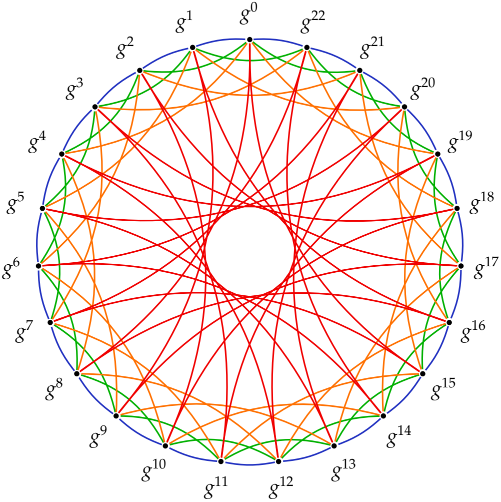
Square-and-multiply as graphs



Square-and-multiply as graphs



Square-and-multiply as a graph

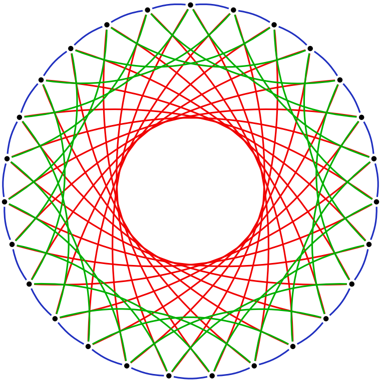


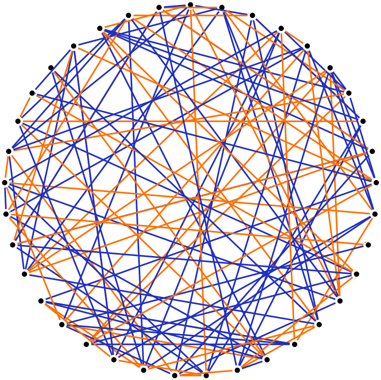
Crypto on graphs?

We’ve been doing it all along!

The beauty and the beast

Components of particular isogeny graphs look like this:

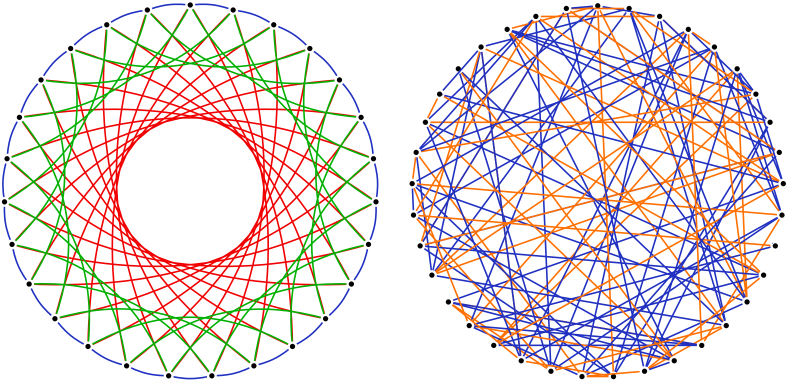




Which of these is good for crypto?

The beauty and the beast

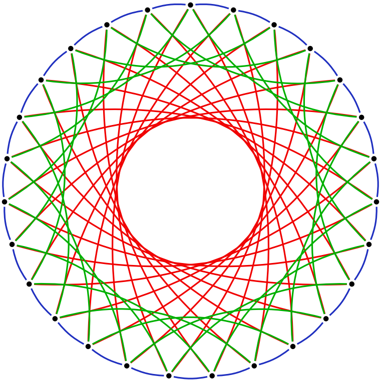
Components of particular isogeny graphs look like this:



Which of these is good for crypto? **Both.**

The beauty and the beast

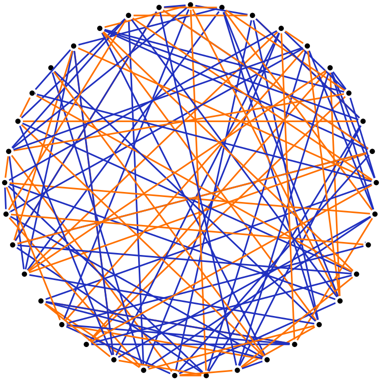
At this time, there are two distinct families of systems:



$\mathbb{F}_p$

CSIDH [ˈsiːˌsaɪd]

https://csidh.isogeny.org



$\mathbb{F}_{p^2}$

SIDH

https://sike.org

Stand back!

We’re going to do math.

Math slide #1: 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 (x, y) *or* the “fake” point ∞.

Math slide #1: 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 (x, y) *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

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

where $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ if $x_1 \neq x_2$ and $\lambda = \frac{3x_1^2 + a}{2y_1}$ otherwise.

do **not** remember these formulas!

Math slide #2: Isogenies *(edges)*

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

- given by rational functions.
- a group homomorphism.

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

Math slide #2: Isogenies *(edges)*

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

- given by rational functions.
- a group homomorphism.

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

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

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

Math slide #2: Isogenies *(edges)*

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

- given by rational functions.
- a group homomorphism.

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

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 $\{\infty\}$.

Math slide #2: Isogenies *(edges)*

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

- given by rational functions.
- a group homomorphism.

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

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

Math slide #2: Isogenies *(edges)*

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

- given by rational functions.
- a group homomorphism.

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

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

Math slide #2: Isogenies *(edges)*

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

- given by rational functions.
- a group homomorphism.

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

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

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

Math slide #2: Isogenies *(edges)*

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

- given by rational functions.
- a group homomorphism.

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

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

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

Tate's theorem:
$E, E'/\mathbb{F}_q$ are isogenous over $\mathbb{F}_q$ if and only if $\#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q)$.

Math slide #3: 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')

Math slide #3: 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')

Math slide #3: 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: $\Theta(\#G)$ ⇝ only suitable for small degrees.

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

[1] (up to isomorphism of E')

Math slide #4: Supersingular isogeny graphs

Let p be a prime and q a power of p.

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

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

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

Math slide #4: Supersingular isogeny graphs

Let p be a prime and q a power of p.

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

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

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

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

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

- vertices given by isomorphism classes of supersingular elliptic curves,
- edges given by equivalence classes[1] of ℓ-isogenies ($\ell \in S$),

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

[1] Two isogenies $\varphi\colon E \to E'$ and $\psi\colon E \to E''$ are identified if $\psi = \iota \circ \varphi$ for some isomorphism $\iota\colon E' \to E''$.

CSIDH [ˈsiːˌsaɪd]

A brief history of CSIDH

Sometimes, there is a (free & transitive) group action of $\mathrm{cl}(\mathcal{O})$ on the set of curves with endomorphism ring $\mathcal{O}$.

A brief history of CSIDH

Sometimes, there is a (free & transitive) group action of $\mathrm{cl}(\mathcal{O})$ on the set of curves with endomorphism ring $\mathcal{O}$.

[Couveignes '97/'06], independently [Rostovtsev–Stolbunov '06]:

Use this group action on ordinary curves for Diffie–Hellman.

A brief history of CSIDH

Sometimes, there is a (free & transitive) group action of $\mathrm{cl}(\mathcal{O})$ on the set of curves with endomorphism ring $\mathcal{O}$.

[Couveignes '97/'06], independently [Rostovtsev–Stolbunov '06]:

Use this group action on ordinary curves for Diffie–Hellman.

[De Feo–Kieffer–Smith '18]:

Massive speedups, but still unbearably slow.

A brief history of CSIDH

Sometimes, there is a (free & transitive) group action of $\mathrm{cl}(\mathcal{O})$ on the set of curves with endomorphism ring $\mathcal{O}$.

[Couveignes '97/'06], independently [Rostovtsev–Stolbunov '06]:

Use this group action on ordinary curves for Diffie–Hellman.

[De Feo–Kieffer–Smith '18]:

Massive speedups, but still unbearably slow.

[Castryck–Lange–Martindale–Panny–Renes '18]:

Switch to supersingular curves $\Longrightarrow$ "practical" performance.

CSIDH in one slide

CSIDH in one slide

- Choose some small odd primes $\ell_1, ..., \ell_n$.
- Make sure $p = 4 \cdot \ell_1 \cdots \ell_n - 1$ is prime.

CSIDH in one slide

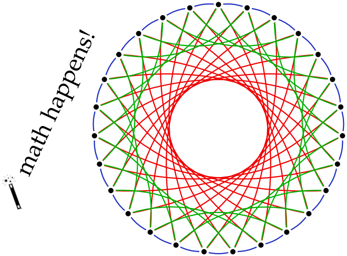
- Choose some small odd primes $\ell_1, ..., \ell_n$.
- Make sure $p = 4 \cdot \ell_1 \cdots \ell_n - 1$ is prime.
- Let $X = \{y^2 = x^3 + Ax^2 + x$ supersingular with $A \in \mathbb{F}_p\}$.

CSIDH in one slide

- Choose some small odd primes $\ell_1, ..., \ell_n$.
- Make sure $p = 4 \cdot \ell_1 \cdots \ell_n - 1$ is prime.
- Let $X = \{y^2 = x^3 + Ax^2 + x$ supersingular with $A \in \mathbb{F}_p\}$.
- Look at the ℓ_i-isogenies defined over $\mathbb{F}_p$ within X.

CSIDH in one slide

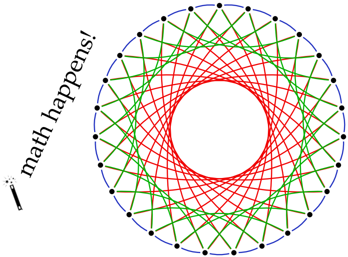
- Choose some small odd primes $\ell_1, ..., \ell_n$.
- Make sure $p = 4 \cdot \ell_1 \cdots \ell_n - 1$ is prime.
- Let $X = \{y^2 = x^3 + Ax^2 + x$ supersingular with $A \in \mathbb{F}_p\}$.
- Look at the ℓ_i-isogenies defined over $\mathbb{F}_p$ within X.



$p = 419$
$\ell_1 = 3$
$\ell_2 = 5$
$\ell_3 = 7$

CSIDH in one slide

- Choose some small odd primes $\ell_1, \ldots, \ell_n$.
- Make sure $p = 4 \cdot \ell_1 \cdots \ell_n - 1$ is prime.
- Let $X = \{y^2 = x^3 + Ax^2 + x$ supersingular with $A \in \mathbb{F}_p\}$.
- Look at the ℓ_i-isogenies defined over $\mathbb{F}_p$ within X.



$p = 419$

$\ell_1 = 3$

$\ell_2 = 5$

$\ell_3 = 7$

- Walking "left" and "right" on any ℓ_i-subgraph is efficient.

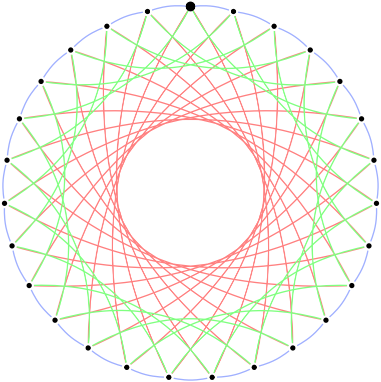
CSIDH key exchange

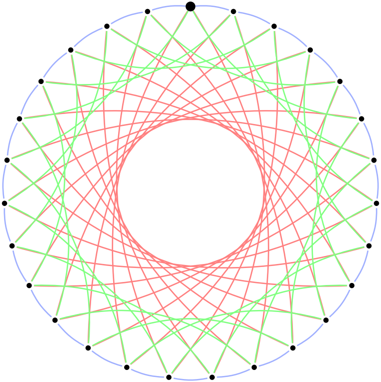
Alice

[+, +, −, −]

Bob

[−, +, −, −]

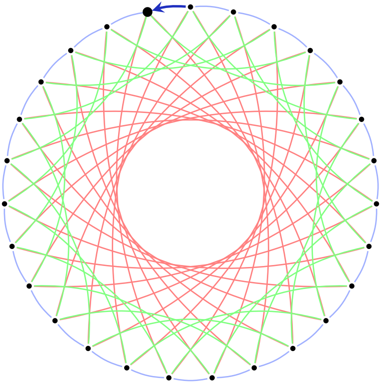




CSIDH key exchange

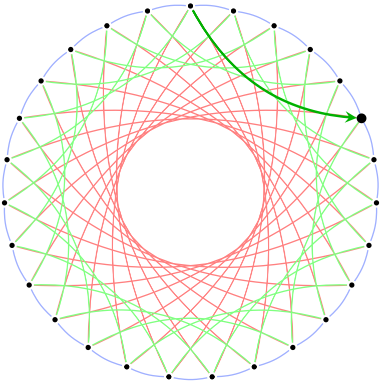
Alice

[+, +, −, −]
↑



Bob

[−, +, −, −]
↑

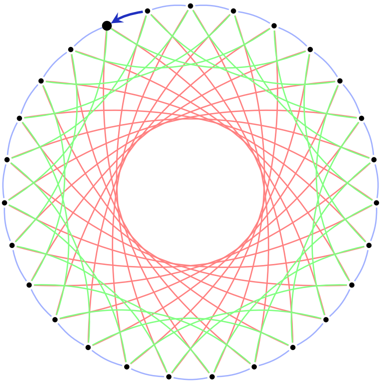


CSIDH key exchange

Alice

[+, +, −, −]

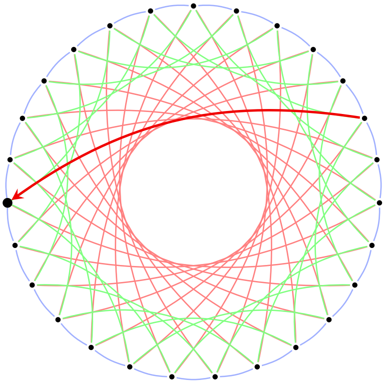
↑



Bob

[−, +, −, −]

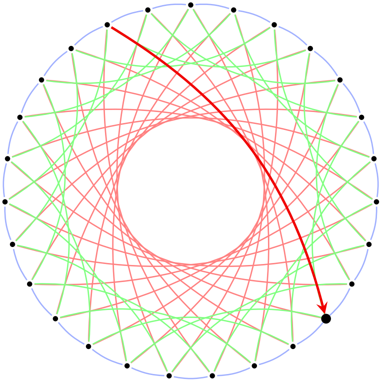
↑



CSIDH key exchange

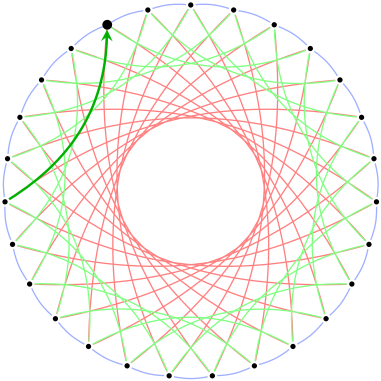
Alice

$[+, +, \underset{\uparrow}{-}, -]$



Bob

$[-, +, \underset{\uparrow}{-}, -]$



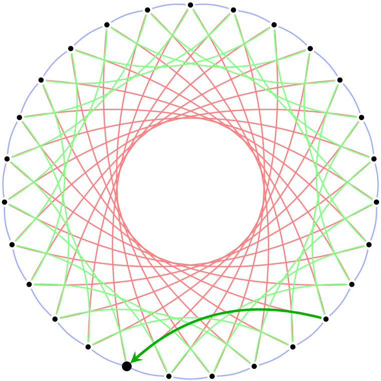
CSIDH key exchange

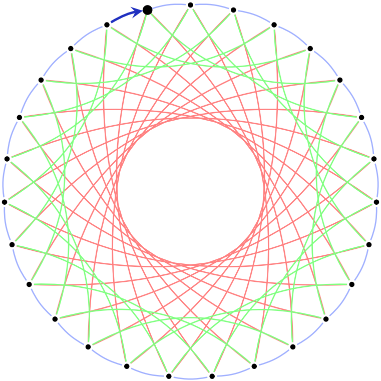
Alice

[+, +, −, −]
↑

Bob

[−, +, −, −]
↑





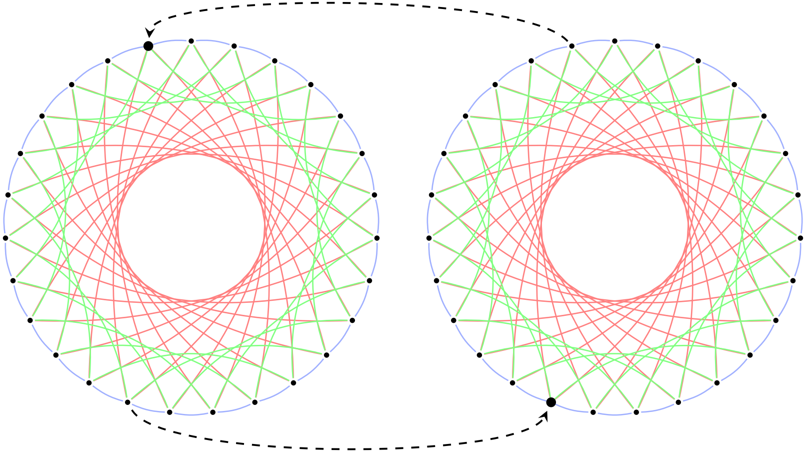
CSIDH key exchange

Alice

[+, +, −, −]

Bob

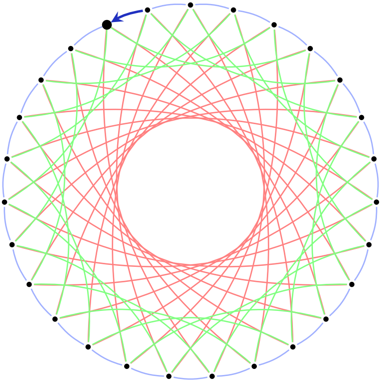
[−, +, −, −]



CSIDH key exchange

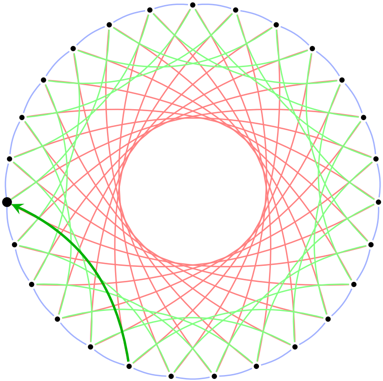
Alice

[+, +, −, −]
↑



Bob

[−, +, −, −]
↑



CSIDH key exchange

Alice

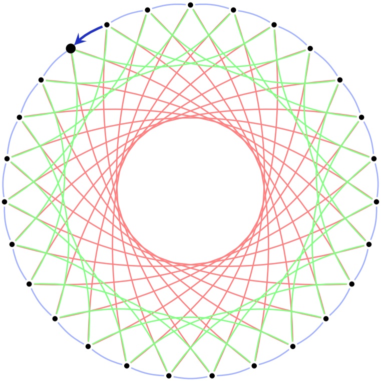
[+, +, −, −]

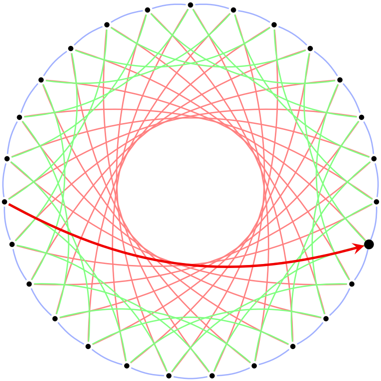
↑

Bob

[−, +, −, −]

↑





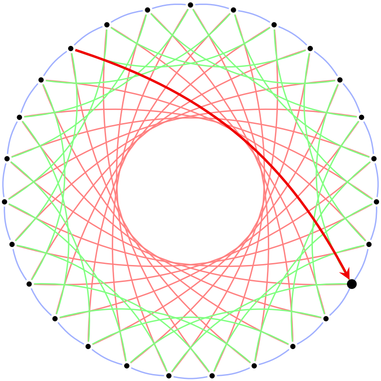
CSIDH key exchange

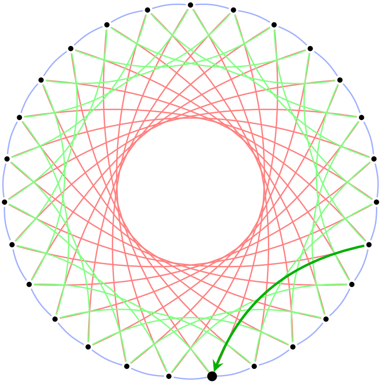
Alice

$[+, +, \underset{\uparrow}{-}, -]$

Bob

$[-, +, \underset{\uparrow}{-}, -]$

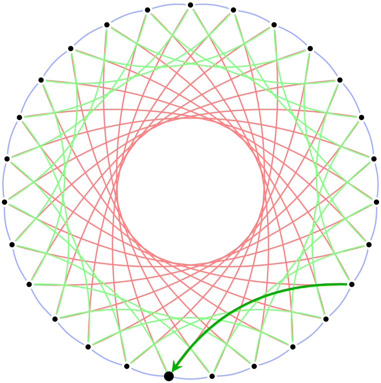




CSIDH key exchange

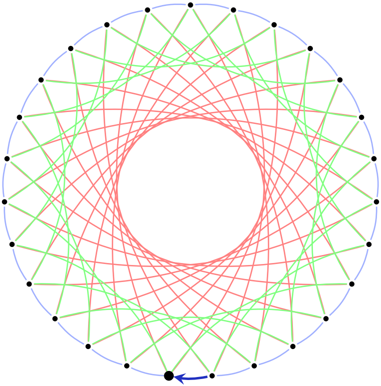
Alice

$[+, +, -, \underset{\uparrow}{-}]$



Bob

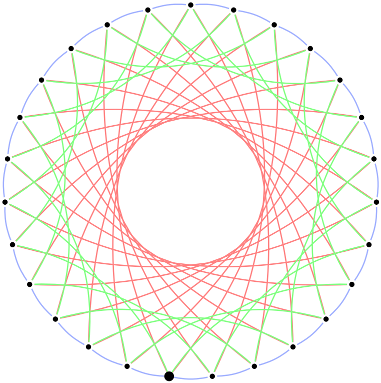
$[-, +, -, \underset{\uparrow}{-}]$



CSIDH key exchange

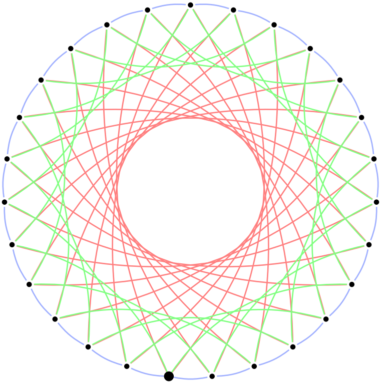
Alice

[+, +, −, −]



Bob

[−, +, −, −]



Where's the group action?

Cycles are compatible: [right then left] = [left then right]
$\rightsquigarrow$ only need to keep track of total step counts for each ℓ_i.

Example: $[+, +, -, -, -, +, -, -]$ just becomes $(+1, \quad 0, -3) \in \mathbb{Z}^3$.

Where's the group action?

Cycles are compatible: [right then left] = [left then right]
$\rightsquigarrow$ only need to keep track of total step counts for each ℓ_i.

Example: [**+**, **+**, **−**, **−**, **−**, **+**, **−**, **−**] just becomes $(+1, \quad 0, -3) \in \mathbb{Z}^3$.

There is a group action of $(\mathbb{Z}^n, +)$ on our set of curves X!

Where's the group action?

Cycles are compatible: [right then left] = [left then right]
$\rightsquigarrow$ only need to keep track of total step counts for each ℓ_i.

Example: $[+,+,-,-,-,+,-,-]$ just becomes $(+1,\quad 0,-3)\in\mathbb{Z}^3$.

There is a group action of $(\mathbb{Z}^n,+)$ on our set of curves X!

By complex-multiplication theory, the quotient of $\mathbb{Z}^n$ by the subgroup acting trivially is the ideal-class group $\mathrm{cl}(\mathbb{Z}[\sqrt{-p}])$.

Walking in the CSIDH graph

- Our curves in the graph have $E(\mathbb{F}_{p^2}) \cong \mathbb{Z}/(p{+}1) \times \mathbb{Z}/(p{+}1)$. Recall $p + 1 = 4 \cdot \ell_1 \cdots \ell_n \implies$ very smooth order!
- "Left" and "right" steps correspond to quotienting out distinguished subgroups of $E[\ell_i] \cong \mathbb{Z}/\ell_i \times \mathbb{Z}/\ell_i$.

Walking in the CSIDH graph

- Our curves in the graph have $E(\mathbb{F}_{p^2}) \cong \mathbb{Z}/(p+1) \times \mathbb{Z}/(p+1)$. Recall $p+1 = 4 \cdot \ell_1 \cdots \ell_n \implies$ very smooth order!
- "Left" and "right" steps correspond to quotienting out distinguished subgroups of $E[\ell_i] \cong \mathbb{Z}/\ell_i \times \mathbb{Z}/\ell_i$.

Computing a "left" step:

1. Find a point $(x, y) \in E$ of order ℓ_i with $x, y \in \mathbb{F}_p$.
2. Compute the isogeny with kernel $\langle (x, y) \rangle$.

Walking in the CSIDH graph

- Our curves in the graph have $E(\mathbb{F}_{p^2}) \cong \mathbb{Z}/(p+1) \times \mathbb{Z}/(p+1)$. Recall $p + 1 = 4 \cdot \ell_1 \cdots \ell_n \implies$ very smooth order!
- "Left" and "right" steps correspond to quotienting out distinguished subgroups of $E[\ell_i] \cong \mathbb{Z}/\ell_i \times \mathbb{Z}/\ell_i$.

Computing a "left" step:

1. Find a point $(x, y) \in E$ of order ℓ_i with $x, y \in \mathbb{F}_p$.
2. Compute the isogeny with kernel $\langle (x, y) \rangle$.

Computing a "right" step:

1. Find a point $(x, y) \in E$ of order ℓ_i with $x \in \mathbb{F}_p$ $\underline{\text{but } y \notin \mathbb{F}_p}$.
2. Compute the isogeny with kernel $\langle (x, y) \rangle$.

Walking in the CSIDH graph

- Our curves in the graph have $E(\mathbb{F}_{p^2}) \cong \mathbb{Z}/(p+1) \times \mathbb{Z}/(p+1)$. Recall $p+1 = 4 \cdot \ell_1 \cdots \ell_n \implies$ very smooth order!
- "Left" and "right" steps correspond to quotienting out distinguished subgroups of $E[\ell_i] \cong \mathbb{Z}/\ell_i \times \mathbb{Z}/\ell_i$.

Computing a "left" step:

1. Find a point $(x, y) \in E$ of order ℓ_i with $x, y \in \mathbb{F}_p$.
2. Compute the isogeny with kernel $\langle (x, y) \rangle$.

Computing a "right" step:

1. Find a point $(x, y) \in E$ of order ℓ_i with $x \in \mathbb{F}_p$ $\underline{\text{but } y \notin \mathbb{F}_p}$.
2. Compute the isogeny with kernel $\langle (x, y) \rangle$.

Net result: With x-only arithmetic everything happens over $\mathbb{F}_p$.
$\implies$ Efficient to implement!

Why no Shor?

Shor's algorithm quantumly computes α from g^α in any group in polynomial time.

Why no Shor?

Shor's algorithm quantumly computes α from g^α in any group in polynomial time.

Shor computes α from $h = g^\alpha$ by finding the kernel of the map

$$f\colon\ \mathbb{Z}^2 \to G,\ (x, y) \mapsto g^x \cdot h^y\,.$$

Why no Shor?

Shor's algorithm quantumly computes α from g^α in any group in polynomial time.

Shor computes α from $h = g^\alpha$ by finding the kernel of the map

$$f\colon\ \mathbb{Z}^2 \to G,\ (x, y) \mapsto g^x \underset{\uparrow}{\cdot} h^y\,.$$

For group actions, we simply cannot compose $a * s$ and $b * s$!

Security of CSIDH

Core problem:
Given $E, E' \in X$, find a smooth-degree isogeny $E \to E'$.

Security of CSIDH

Core problem:
Given $E, E' \in X$, find a smooth-degree isogeny $E \to E'$.

The size of X is $\#\mathrm{cl}(\mathbb{Z}[\sqrt{-p}]) = 3 \cdot h(-p) \approx \sqrt{p}$.

$\rightsquigarrow$ best known classical attack: meet-in-the-middle, $\tilde{\mathcal{O}}(p^{1/4})$.

Fully exponential: Complexity $\exp\big((\log p)^{1+o(1)}\big)$.

Security of CSIDH

Core problem:
Given $E, E' \in X$, find a smooth-degree isogeny $E \to E'$.

The size of X is $\#\mathrm{cl}(\mathbb{Z}[\sqrt{-p}]) = 3 \cdot h(-p) \approx \sqrt{p}$.

$\rightsquigarrow$ best known classical attack: meet-in-the-middle, $\tilde{\mathcal{O}}(p^{1/4})$.

Fully exponential: Complexity $\exp\big((\log p)^{1+o(1)}\big)$.

Solving abelian hidden shift breaks CSIDH.

$\rightsquigarrow$ non-devastating quantum attack (Kuperberg's algorithm).

Subexponential: Complexity $\exp\big((\log p)^{1/2+o(1)}\big)$.

Can we avoid Kuperberg's algorithm?

The supersingular isogeny graph over $\mathbb{F}_{p^2}$ has less structure.

- **SIDH** uses the full $\mathbb{F}_{p^2}$-isogeny graph. No group action!

Can we avoid Kuperberg's algorithm?

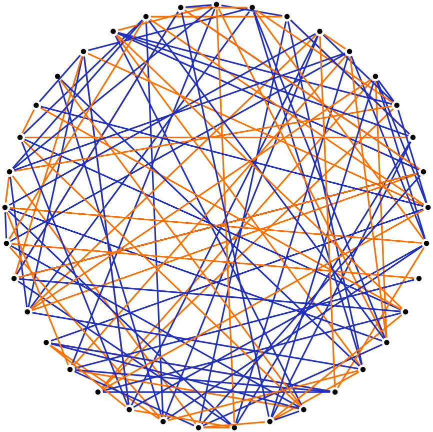
The supersingular isogeny graph over $\mathbb{F}_{p^2}$ has less structure.

- **SIDH** uses the full $\mathbb{F}_{p^2}$-isogeny graph. No group action!

- Problem: also no more intrinsic sense of direction.

$\rightsquigarrow$ need extra information to let Alice & Bob's walks commute.

"It all bloody looks the same!" — a famous isogeny cryptographer



Now: SIDH (Jao, De Feo; 2011)

SIDH: High-level view

E

SIDH: High-level view

- 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 $\varphi_A \colon E \to E/A$; Bob computes $\varphi_B \colon E \to E/B$.
  (These isogenies correspond to walking on 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 on 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 on 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 on the isogeny graph.)
- Alice and Bob transmit the values E/A and E/B.
- Alice somehow obtains $A' := \varphi_B(A)$. (Similar for Bob.)
- They both compute the shared secret

$$(E/B)/A' \cong E/\langle A, B\rangle \cong (E/A)/B'.$$

SIDH's auxiliary points

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

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

CSIDH's solution: use distinguished subgroups.

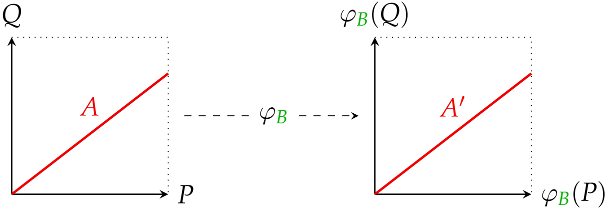
SIDH's auxiliary points

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

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

CSIDH's solution: use distinguished subgroups.

SIDH's solution: φ_B is a group homomorphism!



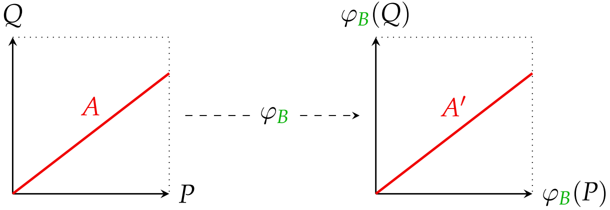
SIDH's auxiliary points

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

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

CSIDH's solution: use distinguished subgroups.

SIDH's solution: φ_B is a group homomorphism! (and $A \cap B = \{\infty\}$)



- 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 $\langle \varphi_B(P) + [a]\varphi_B(Q) \rangle$.

Decomposing smooth isogenies

- In SIDH, $\#A$ and $\#B$ are “crypto-sized”.
  Vélu’s formulas take $\Theta(\#G)$ to compute $\varphi_G\colon E \to E/G$.

Decomposing 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 $\ker \psi_i := [\ell^{k-i}](\psi_{i-1} \circ \cdots \circ \psi_1)(G)$.

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

Decomposing 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 $\ker \psi_i := [\ell^{k-i}](\psi_{i-1} \circ \cdots \circ \psi_1)(G)$.

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

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

Decomposing 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 $\ker \psi_i := [\ell^{k-i}](\psi_{i-1} \circ \cdots \circ \psi_1)(G)$.

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

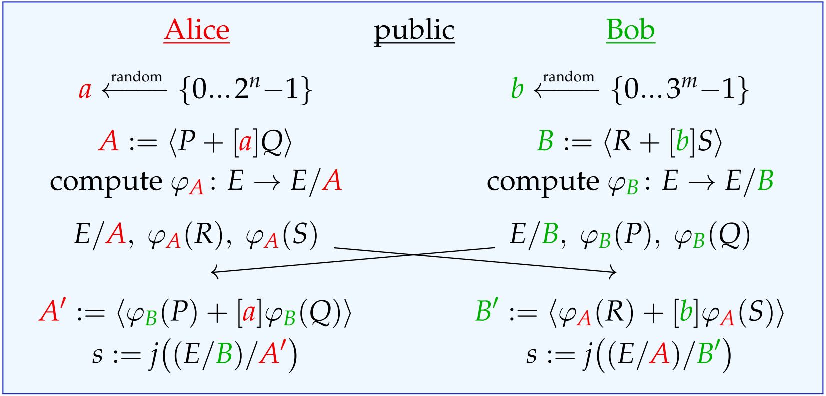
⇝ Complexity: $O(k^2 \cdot \ell)$. Exponentially smaller than ℓ^k!
"Optimal strategy" improves this to $O(k \log k \cdot \ell)$.

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

SIDH in one slide

Public parameters:

- a large prime $p = 2^n 3^m - 1$ and a supersingular $E/\mathbb{F}_p$
- bases (P, Q) of $E[2^n]$ and (R, S) of $E[3^m]$ (recall $E[k] \cong \mathbb{Z}/k \times \mathbb{Z}/k$)



Alice | public | Bob

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

$A := \langle P + [a]Q \rangle$ | $B := \langle R + [b]S \rangle$

compute $\varphi_A : E \to E/A$ | compute $\varphi_B : E \to E/B$

$E/A,\ \varphi_A(R),\ \varphi_A(S)$ | $E/B,\ \varphi_B(P),\ \varphi_B(Q)$

$A' := \langle \varphi_B(P) + [a]\varphi_B(Q) \rangle$ | $B' := \langle \varphi_A(R) + [b]\varphi_A(S) \rangle$

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

Security of SIDH

The SIDH graph has size $\lfloor p/12 \rfloor + \varepsilon$.
Alice & Bob can choose from about $\sqrt{p}$ secret keys each.

Security of SIDH

The SIDH graph has size $\lfloor p/12 \rfloor + \varepsilon$.
Alice & Bob can choose from about $\sqrt{p}$ secret keys each.

Classical attacks:

- Meet-in-the-middle: $\tilde{\mathcal{O}}(p^{1/4})$ time *& space (!)*.
- Collision finding: $\tilde{\mathcal{O}}(p^{3/8}/\sqrt{\mathit{memory}}/\mathit{cores})$.

Security of SIDH

The SIDH graph has size $\lfloor p/12 \rfloor + \varepsilon$.
Alice & Bob can choose from about $\sqrt{p}$ secret keys each.

Classical attacks:

- Meet-in-the-middle: $\tilde{\mathcal{O}}(p^{1/4})$ time *& space (!)*.
- Collision finding: $\tilde{\mathcal{O}}(p^{3/8}/\sqrt{memory}/cores)$.

Quantum attacks:

- Claw finding: claimed $\tilde{\mathcal{O}}(p^{1/6})$.
  [JS19] says this is *more expensive than classical attacks*.

Security of SIDH

The SIDH graph has size $\lfloor p/12 \rfloor + \varepsilon$.
Alice & Bob can choose from about $\sqrt{p}$ secret keys each.

Classical attacks:

- Meet-in-the-middle: $\tilde{\mathcal{O}}(p^{1/4})$ time *& space (!)*.
- Collision finding: $\tilde{\mathcal{O}}(p^{3/8}/\sqrt{\mathit{memory}}/\mathit{cores})$.

Quantum attacks:

- Claw finding: claimed $\tilde{\mathcal{O}}(p^{1/6})$.
  [JS19] says this is *more expensive than classical attacks*.

Bottom line: Fully exponential. Complexity $\exp\big((\log p)^{1+o(1)}\big)$.

That’s nice and all, but... so what?

That’s nice and all, but... so what?

CSIDH...

- is a drop-in post-quantum replacement for (EC)DH.

That’s nice and all, but... so what?

CSIDH...

- is a drop-in post-quantum replacement for (EC)DH.
- is the only known somewhat efficient post-quantum non-interactive key exchange (full public-key validation).

That's nice and all, but... so what?

CSIDH...

- is a drop-in post-quantum replacement for (EC)DH.
- is the only known somewhat efficient post-quantum non-interactive key exchange (full public-key validation).
- has a clean mathematical structure: a true group action.

That’s nice and all, but... so what?

CSIDH...

- is a drop-in post-quantum replacement for (EC)DH.
- is the only known somewhat efficient post-quantum non-interactive key exchange (full public-key validation).
- has a clean mathematical structure: a true group action.

SIDH...

- may get standardized in NIST’s not-a-competition.

That’s nice and all, but... so what?

CSIDH...

- is a drop-in post-quantum replacement for (EC)DH.
- is the only known somewhat efficient post-quantum non-interactive key exchange (full public-key validation).
- has a clean mathematical structure: a true group action.

SIDH...

- may get standardized in NIST’s not-a-competition.
- has exponential attack cost as far as we know.

That’s nice and all, but… so what?

CSIDH…

- is a drop-in post-quantum replacement for (EC)DH.
- is the only known somewhat efficient post-quantum non-interactive key exchange (full public-key validation).
- has a clean mathematical structure: a true group action.

SIDH…

- may get standardized in NIST’s not-a-competition.
- has exponential attack cost as far as we know.

Both…

- have tiny keys compared to other post-quantum schemes.

That's nice and all, but... so what?

CSIDH...

- is a drop-in post-quantum replacement for (EC)DH.
- is the only known somewhat efficient post-quantum non-interactive key exchange (full public-key validation).
- has a clean mathematical structure: a true group action.

SIDH...

- may get standardized in NIST's not-a-competition.
- has exponential attack cost as far as we know.

Both...

- have tiny keys compared to other post-quantum schemes.
- are quite slow compared to other post-quantum schemes.

State of this talk

- Crash course on elliptic-curve isogenies. ✓
- Overview of CSIDH key exchange.[1] ✓
- Overview of SIDH key exchange.[1] ✓
- Sales pitch why any of this might matter. ✓

[1] Needless to say, isogenies also give rise to other primitives.
(Check out ePrint 2019/166 for a cool out-of-the-box idea with isogenies *and* pairings.)

State of this talk

- Crash course on elliptic-curve isogenies. ✓
- Overview of CSIDH key exchange.[1] ✓
- Overview of SIDH key exchange.[1] ✓
- Sales pitch why any of this might matter. ✓

- Now:

```
if (not yet out of time) {
    Explore some easy ways to not break SIDH.
}
```

[1] Needless to say, isogenies also give rise to other primitives.
(Check out ePrint 2019/166 for a cool out-of-the-box idea with isogenies *and* pairings.)

How to not break SIDH

A short beginner's guide

Chloe Martindale   Lorenz Panny

Technische Universiteit Eindhoven

Amsterdam, Netherlands, 4 October 2019

Auxiliary points: Information theory

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

Auxiliary points: Information theory

- By linearity, the two points $\varphi_A(R), \varphi_A(S)$ encode how φ_A acts on the entire 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 k-torsion and $k^2 > 4d$, then $\phi = \psi$.

$\Longrightarrow$ Except for very unbalanced parameters,
the public points uniquely determine the secret isogenies.

Auxiliary points: Interpolation?

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

$\rightsquigarrow$ Rational function interpolation?

Auxiliary points: Interpolation?

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

$\rightsquigarrow$ Rational function interpolation?

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

Auxiliary points: Interpolation?

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

$\rightsquigarrow$ 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.

Auxiliary points: Interpolation?

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

$\rightsquigarrow$ 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.

- No known algorithms for interpolating and decomposing at the same time.

Auxiliary points: Group theory?

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

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

Auxiliary points: Group theory?

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

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

☹ There's an isomorphism of groups

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

Auxiliary points: Group theory?

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

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

☹ There's an isomorphism of groups

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

$\implies$ can't learn anything about 2^n from 3^m using groups alone.

Auxiliary points: Group theory?

- Can we extrapolate the action of φ_A to some $\geq 3^m$-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

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

$\Longrightarrow$ can't learn anything about 2^n from 3^m using groups alone.

> "[...] elliptic curves are as close to generic groups as it gets."
>
> —me, all the time

Auxiliary points: Group theory?

- Can we extrapolate the action of φ_A to some $\geq 3^m$-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

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

$\implies$ can't learn anything about 2^n from 3^m using groups alone.

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

—me, all the time

(Exception: pairings, but those are also just bilinear maps.)

Auxiliary points: Petit's endomorphisms (1)

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

Auxiliary 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:

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

Auxiliary points: Petit's endomorphisms (1)

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

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

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

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

Auxiliary 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:

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

$\rightsquigarrow$ 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 remaining r-part.
  $\Longrightarrow$ (details) $\Longrightarrow$ recover φ_A.

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

Auxiliary 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 $\deg\tau/3^m < 2^n$.

Questions?