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!)
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?
Square-and-multiply

\[ g \cdot g \cdot g \cdot g \cdot g \cdot g \cdot g \cdot g \cdot g \cdot g \cdot g \cdot g \cdot g \cdot g \cdot g \cdot g \cdot g \cdot g \cdot g \cdot g \cdot g \cdot g^0 \cdot g^1 \cdot g^2 \cdot g^3 \cdot g^4 \cdot g^5 \cdot g^6 \cdot g^7 \cdot g^8 \cdot g^9 \cdot g^{10} \cdot g^{11} \cdot g^{12} \cdot g^{13} \cdot g^{14} \cdot g^{15} \cdot g^{16} \cdot g^{17} \cdot g^{18} \cdot g^{19} \cdot g^{20} \cdot g^{21} \cdot g^{22} \]
multiply
Square-and-multiply
Square-and-multiply-and-square-and-multiply
Square-and-multiply-and-square-and-multiply-and-square-and-multiply-and-square-and-multiply

\[ g \cdot g \cdot g \cdot g \cdot g \cdot g \cdot g \cdot g \cdot g \cdot g \cdot g \cdot g \cdot g \cdot g \cdot g \cdot g \cdot g \cdot g ^ {2} \cdot g ^ {2} \cdot g ^ {2} \cdot g ^ {2} \cdot g ^ {2} \cdot g ^ {2} \cdot g \cdot g ^ {4} \cdot g ^ {4} \cdot g ^ {4} \cdot g \cdot g ^ {4} \cdot g ^ {8} \cdot g ^ {0} \cdot g ^ {22} \cdot g ^ {21} \cdot g ^ {20} \cdot g ^ {19} \cdot g ^ {18} \cdot g ^ {17} \cdot g ^ {16} \cdot g ^ {15} \cdot g ^ {14} \cdot g ^ {13} \]
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** ['síːˌsaɪd]

https://csidh.isogeny.org

\[ \mathbb{F}_{p^2} \]

**SIDH**

https://sike.org
Stand back!

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

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

A point on $E$ is a solution $(x, y)$ or the “fake” point $\infty$. 
An elliptic curve (modulo details) is given by an equation

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

A point on \( E \) is a solution \((x, y)\) or the “fake” point \( \infty \).

\( E \) is an abelian group: we can “add” points.

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

\[
(\lambda^2 - x_1 - x_2, \lambda(2x_1 + x_2 - \lambda^2) - y_1)
\]

where \( \lambda = \frac{y_2-y_1}{x_2-x_1} \) if \( x_1 \neq x_2 \) and \( \lambda = \frac{3x_1^2+a}{2y_1} \) otherwise.
An isogeny of elliptic curves is a non-zero map \( E \rightarrow E' \) that is:
- given by rational functions.
- a group homomorphism.

The degree of a separable* isogeny is the size of its kernel.
An isogeny of elliptic curves is a non-zero map $E \rightarrow E'$ that is:
- given by rational functions.
- a group homomorphism.

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

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

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 $\iota : (x, y) \mapsto (-x, \sqrt{-1} \cdot y)$ 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 $\{\infty\}$. 

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

\*Separability ensures the isogeny is well-defined over the base field.
An isogeny of elliptic curves is a non-zero map $E \rightarrow E'$ that is:
- given by rational functions.
- a group homomorphism.

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

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

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

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

*Note: The word “separable” is used here to indicate that the isogeny is separable. This is a common convention in the field of cryptography and algebraic geometry, but it is not explicitly defined in the text. The full explanation of separability would involve more advanced mathematics beyond the scope of this document.
An isogeny of elliptic curves is a non-zero map \( E \rightarrow E' \) that is:

- given by rational functions.
- a group homomorphism.

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

An endomorphism of \( E \) is an isogeny \( E \rightarrow E \), or the zero map. The ring of endomorphisms of \( E \) is denoted by \( \text{End}(E) \).
An **isogeny** of elliptic curves is a non-zero map $E \to E'$ that is:

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

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

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

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

---

Tate's theorem: $E, E'/\mathbb{F}_q$ are isogenous over $\mathbb{F}_q$ if and only if $\# E(\mathbb{F}_q) = \# E'(\mathbb{F}_q)$.
An isogeny of elliptic curves is a non-zero map $E \rightarrow E'$ that is:
- given by rational functions.
- a group homomorphism.

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

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

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

Tate’s theorem:
$E, E'/\mathbb{F}_q$ are isogenous over $\mathbb{F}_q$ if and only if $\#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q)$. 
For any finite subgroup $G$ of $E$, there exists a unique\(^1\) separable* isogeny $\varphi_G : E \to E'$ with kernel $G$.

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

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

\(^1\)(up to isomorphism of $E'$)
Math slide #3: Isogenies and kernels

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

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

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

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

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

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

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

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

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

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

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!

\textsuperscript{1}(up to isomorphism of $E'$)
Let $p$ be a prime and $q$ a power of $p$.

An elliptic curve $E/\mathbb{F}_q$ is \textit{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 \textit{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 $\#E(\mathbb{F}_{p^2}) = (p + 1)^2$.

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

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

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

- vertices given by isomorphism classes of supersingular elliptic curves,
- edges given by equivalence classes\(^1\) of $\ell$-isogenies ($\ell \in S$), both defined over $\mathbb{F}_q$.

---

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

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

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

[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 $\Rightarrow$ “practical” performance.
Choose some small odd primes $\ell_1, \ldots, \ell_n$.

Make sure $p = 4 \cdot \ell_1 \cdots \ell_n - 1$ is prime.

Let $X = \{ y^2 = x^3 + Ax^2 + x \text{ supersingular with } A \in \mathbb{F}_p \}$.

Look at the $\ell_i$-isogenies defined over $\mathbb{F}_p$ within $X$.

Walking “left” and “right” on any $\ell_i$-subgraph is efficient.

$p = 419$

$\ell_1 = 3$

$\ell_2 = 5$

$\ell_3 = 7$
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.
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 $X = \{y^2 = x^3 + Ax^2 + x \text{ supersingular with } A \in \mathbb{F}_p\}$.
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 $X = \{ y^2 = x^3 + Ax^2 + x \text{ supersingular with } A \in \mathbb{F}_p \}$.
- Look at the $\ell_i$-isogenies defined over $\mathbb{F}_p$ within $X$. 
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 $\ell_i$-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 $X = \{y^2 = x^3 + Ax^2 + x \text{ supersingular with } A \in \mathbb{F}_p\}$.
- Look at the $\ell_i$-isogenies defined over $\mathbb{F}_p$ within $X$.

$\begin{align*}
p &= 419 \\
\ell_1 &= 3 \\
\ell_2 &= 5 \\
\ell_3 &= 7
\end{align*}$

- Walking “left” and “right” on any $\ell_i$-subgraph is **efficient**.
CSIDH key exchange

Alice

\[ +, +, -, - \]

Bob

\[ -, +, -, - \]
CSIDH key exchange

Alice

\[ [+ , \pm , - , - ] \]

Bob

\[ [ - , \pm , - , - ] \]
CSIDH key exchange

Alice
\[ [+., +., -., -.] \]

Bob
\[ [\text{-}, +., \text{-}, \text{-}]. \]
CSIDH key exchange

Alice
[\(+, +, -,-\)]

Bob
[-, +, -,-]
CSIDH key exchange

Alice
\[ [+ , + , - , - ] \]

Bob
\[ [ - , + , - , - ] \]
CSIDH key exchange

Alice
[+, +, -, -]

Bob
[+, - , - , - ]
CSIDH key exchange

Alice
\[
[+, +, -, -]
\]

Bob
\[
[-, +, -, -]
\]
CSIDH key exchange

Alice

\[
\{+, +, -, -\}
\]

Bob

\[
\{-, +, -, -\}
\]
CSIDH key exchange

Alice

\[ [+ , + , - , - ] \]

Bob

\[ [ - , + , - , - ] \]
CSIDH key exchange

Alice

[+, +, −, −]

Bob

[−, +, −, −]
CSIDH key exchange

Alice

\[ +, +, -, - \]

Bob

\[ -, +, -, - \]
Where’s the group action?

Cycles are compatible: \([\text{right then left}] = [\text{left then right}]\)

\(\leadsto\) only need to keep track of total step counts for each \(\ell_i\).

Example: \([+ , + , - , - , - , + , - , -]\) just becomes \((+1, 0, -3) \in \mathbb{Z}^3\).
Where’s the group action?

Cycles are compatible: \([\text{right then left}] = [\text{left then right}]\)  
\[\mapsto\] only need to keep track of total step counts for each \(\ell_i\).
Example: \([+, +, -, -, -, +, -, -]\) just becomes \((+1, 0, -3) \in \mathbb{Z}^3\).

There is a group action of \((\mathbb{Z}^n, +)\) on our set of curves \(X\)!
Where’s the group action?

Cycles are compatible: \([\text{right then left}] = [\text{left then right}]\)

\(\sim\) only need to keep track of total step counts for each \(\ell_i\).

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

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 \(\text{cl}(\mathbb{Z}[\sqrt{-p}])\).
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 $\ell_i$ 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 \( p + 1 = 4 \cdot \ell_1 \cdots \ell_n \implies \text{very smooth order!} \)

- “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 \( \ell_i \) 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 \( \ell_i \) with \( x \in \mathbb{F}_p \) 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 $\ell_i$ 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 $\ell_i$ with $x \in \mathbb{F}_p$ 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 $\alpha$ from $g^\alpha$ in any group in polynomial time.
Why no Shor?

Shor’s algorithm quantumly computes $\alpha$ from $g^{\alpha}$ in any group in polynomial time.

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

$$f : \mathbb{Z}^2 \rightarrow G, \ (x, y) \mapsto g^x \cdot h^y.$$
Why no Shor?

Shor’s algorithm quantumly computes $\alpha$ from $g^\alpha$ in any group in polynomial time.

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

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

For group actions, we simply cannot compose $a \ast s$ and $b \ast s$!
Security of CSIDH

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

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

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

Fully exponential: Complexity $\exp\left(\log p^{1/10 + o(1)}\right)$.

Solving abelian hidden shift breaks CSIDH.

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

Subexponential: Complexity $\exp\left(\log p^{1/2 + o(1)}\right)$.
Core problem:
Given $E, E' \in X$, find a smooth-degree isogeny $E \rightarrow E'$.

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

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

Fully exponential: Complexity $\exp\left((\log p)^{1+o(1)}\right)$. 
Security of CSIDH

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

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

$\Rightarrow$ best known classical attack: meet-in-the-middle, $\tilde{O}(p^{1/4})$.
Fully exponential: Complexity $\exp((\log p)^{1+o(1)})$.

Solving abelian hidden shift breaks CSIDH.

$\Rightarrow$ non-devastating quantum attack (Kuperberg’s algorithm).
Subexponential: Complexity $\exp((\log p)^{1/2+o(1)})$. 
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

\[ E \]
Alice & Bob pick secret subgroups $A$ and $B$ of $E$. 
SIDH: High-level view

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

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

$$
\begin{align*}
E & \xrightarrow{\varphi_A} E/A \\
& \downarrow \varphi_B \\
E/B & 
\end{align*}
$$
SIDH: High-level view

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

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

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

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

- Alice & Bob pick secret subgroups $A$ and $B$ of $E$.
- Alice computes $\varphi_A : E \to E/A$; Bob computes $\varphi_B : E \to E/B$. (These isogenies correspond to walking on the isogeny graph.)
- Alice and Bob transmit the values $E/A$ and $E/B$.
- Alice somehow obtains $A' := \varphi_B(A)$. (Similar for Bob.)
- They both compute the shared secret
  $$\frac{E/B}{A'} \cong E/\langle A, B \rangle \cong \frac{E/A}{B'}.$$
SIDH’s auxiliary points

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

...but Alice knows only $A$, Bob knows only $\varphi_B$. 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 \( \varphi_B \). Hm.

**CSIDH’s solution: use distinguished subgroups.**

**SIDH’s solution: \( \varphi_B \) is a group homomorphism!**
SIDH’s auxiliary points

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

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

**SIDH’s solution: use distinguished subgroups.**

**SIDH’s solution:** $\varphi_B$ 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.

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

\[ Q \quad A \quad \cdots \quad \varphi_B \quad \cdots \quad \varphi_B(P) \]

\[ P \quad \rightarrow \quad A' \quad \rightarrow \quad \varphi_B(P) \]
Decomposing smooth isogenies

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

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

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

\[
E \xrightarrow{\psi_1} E_1 \xrightarrow{\psi_2} \cdots \xrightarrow{\psi_{k-1}} E_{k-1} \xrightarrow{\psi_k} E/G \]

\( \varphi_G \)
Decomposing smooth isogenies

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

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

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

Complexity: \( O(k^2 \cdot \ell) \). Exponentially smaller than \( \ell^k \! \). “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 $\varphi_G : E \to E/G$.

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

$$E \xrightarrow{\psi_1} E_1 \xrightarrow{\psi_2} \cdots \xrightarrow{\psi_{k-1}} E_{k-1} \xrightarrow{\psi_k} E/G$$

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

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

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

Public parameters:

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

<table>
<thead>
<tr>
<th>Alice</th>
<th>public</th>
<th>Bob</th>
</tr>
</thead>
<tbody>
<tr>
<td>( a ) (\xleftarrow{\text{random}}) {0...(2^n - 1})</td>
<td></td>
<td>( b ) (\xleftarrow{\text{random}}) {0...(3^m - 1})</td>
</tr>
<tr>
<td>( A := \langle P + [a]Q \rangle )</td>
<td></td>
<td>( B := \langle R + [b]S \rangle )</td>
</tr>
<tr>
<td>compute ( \varphi_A : E \rightarrow E/A )</td>
<td></td>
<td>compute ( \varphi_B : E \rightarrow E/B )</td>
</tr>
<tr>
<td>( E/A, \varphi_A(R), \varphi_A(S) )</td>
<td></td>
<td>( E/B, \varphi_B(P), \varphi_B(Q) )</td>
</tr>
<tr>
<td>( A' := \langle \varphi_B(P) + [a]\varphi_B(Q) \rangle )</td>
<td>( B' := \langle \varphi_A(R) + [b]\varphi_A(S) \rangle )</td>
<td>( s := j((E/B)/A') )</td>
</tr>
</tbody>
</table>
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 $\left\lfloor \frac{p}{12} \right\rfloor + \varepsilon$. Alice & Bob can choose from about $\sqrt{p}$ secret keys each.

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

[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: $\tilde{O}(p^{1/4})$ time & space (!).
- Collision finding: $\tilde{O}(p^{3/8}/\sqrt{\text{memory}/\text{cores}})$.

Quantum attacks:
- Claw finding: claimed $\tilde{O}(p^{1/6})$.
  [JS19] says this is more expensive than classical attacks.
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: $\tilde{O}(p^{1/4})$ time & space (!).
- Collision finding: $\tilde{O}(p^{3/8}/\sqrt{\text{memory}/\text{cores}})$.

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

Bottom line: Fully exponential. Complexity $\exp((\log p)^{1+o(1)})$. 
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. ✓
- Overview of SIDH key exchange. ✓
- 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.
}

¹Needless 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 $\varphi_A$ acts on the entire $3^m$-torsion.
- Note $3^m$ is smooth $\Rightarrow$ can evaluate $\varphi_A$ 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 $\varphi_A$ acts on the entire $3^m$-torsion.
- Note $3^m$ is smooth $\Rightarrow$ can evaluate $\varphi_A$ on any $R \in E_0[3^m]$.

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

$\Rightarrow$ 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 $\varphi_A$.

$\Rightarrow$ Rational function interpolation?
Auxiliary points: Interpolation?

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

$\Rightarrow$ Rational function interpolation?

$\therefore$ ...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 $\varphi_A$.

$\leadsto$ Rational function interpolation?

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

$\leadsto$ 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 $\varphi_A$.

$\Rightarrow$ Rational function interpolation?

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

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

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

ˎ There’s an isomorphism of groups

$$E(\mathbb{F}_{p^2}) \cong E[2^n] \times E[3^m].$$
Can we extrapolate the action of $\varphi_A$ to some $\geq 3^m$-torsion? e.g. we win if we get the action of $\varphi_A$ on the $2^n$-torsion.

There's an isomorphism of groups

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

\[\Rightarrow\] can't learn anything about $2^n$ from $3^m$ using groups alone.
Auxiliary points: Group theory?

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

- There’s an isomorphism of groups

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

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

There's an isomorphism of groups

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

$\implies$ 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.)
For typical SIDH parameters, we know endomorphisms $\iota, \pi$ of $E_0$ such that $\text{End}(E_0) = \langle 1, \iota, \frac{\iota + \pi}{2}, \frac{1 + \iota \pi}{2} \rangle$. 
Auxiliary points: Petit’s endomorphisms (1)

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

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

\[
E_0 \xrightarrow{\iota} E_0 \xleftarrow{\varphi_A} E_A
\]

\[
E_0 \xrightarrow{\varphi_A} E_A
\]
Auxiliary points: Petit’s endomorphisms (1)

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

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

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

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

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

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

  \[ \iota \quad \text{E}_0 \quad \varphi_A \quad \text{E}_A \]

  \[ \widehat{\varphi}_A \]

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

- Idea: Find $\tau \in R$ of degree $3^m r$; recover $3^m$-part from known action; brute-force the remaining $r$-part.
  \[ \rightarrow \text{(details)} \rightarrow \text{recover } \varphi_A. \]
Petit uses endomorphisms $\tau \in R$ of the form

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

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

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

(Recall $p = 2^n3^m - 1$.)
Petit uses endomorphisms $\tau \in R$ of the form

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

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

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

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

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