Isogenies: The basics, some applications, and nothing much in between

Lorenz Panny

Technische Universität München

5 December 2023

• <u>Isogenies</u> are a source of exponentially-sized graphs.



Big picture $\rho \rho$

- ► <u>Isogenies</u> are a source of exponentially-sized graphs.
- We can walk efficiently on these graphs.

- ► <u>Isogenies</u> are a source of exponentially-sized graphs.
- We can walk efficiently on these graphs.
- Fast mixing: short paths to (almost) all nodes.

- ► <u>Isogenies</u> 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!)

- ► <u>Isogenies</u> 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.

- ► <u>Isogenies</u> 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.

Finding graphs with *almost* all of these properties is easy — but getting all at once seems rare.

Crypto on graphs?

Diffie-Hellman key exchange 1976

Public parameters:

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

Diffie-Hellman key exchange 1976

Public parameters:

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



Diffie-Hellman key exchange 1976

Public parameters:

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



Fundamental reason this works: ^{*a*} and ^{*b*} are commutative!

Bob

- 1. Set $t \leftarrow g$.
- 2. Set $t \leftarrow t \cdot g$.
- 3. Set $t \leftarrow t \cdot g$.
- 4. Set $t \leftarrow t \cdot g$.

•••

- b-2. Set $t \leftarrow t \cdot g$.
- b-1. Set $t \leftarrow t \cdot g$.
 - *b*. Publish $B \leftarrow t \cdot g$.



Is this a good idea?

Bob	Attacker Eve
1. Set $t \leftarrow g$.	1. Set $t \leftarrow g$. If $t = B$ return 1.
2. Set $t \leftarrow t \cdot g$.	2. Set $t \leftarrow t \cdot g$. If $t = B$ return 2.
3. Set $t \leftarrow t \cdot g$.	3. Set $t \leftarrow t \cdot g$. If $t = B$ return 3.
4. Set $t \leftarrow t \cdot g$.	4. Set $t \leftarrow t \cdot g$. If $t = B$ return 3.
$b-2$. Set $t \leftarrow t \cdot g$.	$b-2$. Set $t \leftarrow t \cdot g$. If $t = B$ return $b-2$.
$b-1$. Set $t \leftarrow t \cdot g$.	$b-1$. Set $t \leftarrow t \cdot g$. If $t = B$ return $b-1$.
<i>b</i> . Publish $B \leftarrow t \cdot g$.	<i>b</i> . Set $t \leftarrow t \cdot g$. If $t = B$ return <i>b</i> .
	$b+1$. Set $t \leftarrow t \cdot g$. If $t = B$ return $b+1$.
	$b+2$. Set $t \leftarrow t \cdot g$. If $t = B$ return $b+2$.

•••

Bob	<u>Attacker Eve</u>
1. Set $t \leftarrow g$.	1. Set $t \leftarrow g$. If $t = B$ return 1.
2. Set $t \leftarrow t \cdot g$.	2. Set $t \leftarrow t \cdot g$. If $t = B$ return 2.
3. Set $t \leftarrow t \cdot g$.	3. Set $t \leftarrow t \cdot g$. If $t = B$ return 3.
4. Set $t \leftarrow t \cdot g$.	4. Set $t \leftarrow t \cdot g$. If $t = B$ return 3.
$b-2$. Set $t \leftarrow t \cdot g$.	$b-2$. Set $t \leftarrow t \cdot g$. If $t = B$ return $b-2$.
$b-1$. Set $t \leftarrow t \cdot g$.	$b-1$. Set $t \leftarrow t \cdot g$. If $t = B$ return $b-1$.
<i>b</i> . Publish $B \leftarrow t \cdot g$.	<i>b</i> . Set $t \leftarrow t \cdot g$. If $t = B$ return <i>b</i> .
	$b+1$. Set $t \leftarrow t \cdot g$. If $t = B$ return $b+1$.
	$b+2$. Set $t \leftarrow t \cdot g$. If $t = B$ return $b + 2$.

Effort for both: O(#G). Bob needs to be smarter.

(This attacker is also kind of dumb, but that doesn't matter for my point here.)



Bob computes his public key g^{13} from g.

multiply



Square-and-multiply



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



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













Crypto on graphs? We've been doing it all the time!

Fast mixing: paths of length $\log(\# \text{ nodes})$ to everywhere.

Fast mixing: paths of length $\log(\# \text{ nodes})$ to everywhere.

With square-and-multiply, computing $\alpha \mapsto g^{\alpha}$ takes $\Theta(\log \alpha)$.

Fast mixing: paths of length $\log(\# \text{ nodes})$ to everywhere.

With square-and-multiply, computing $\alpha \mapsto g^{\alpha}$ takes $\Theta(\log \alpha)$. For well-chosen groups, computing $g^{\alpha} \mapsto \alpha$ takes $\Theta(\sqrt{\#G})$.

7/44

Fast mixing: paths of length $\log(\# \text{ nodes})$ to everywhere.

With square-and-multiply, computing $\alpha \mapsto g^{\alpha}$ takes $\Theta(\log \alpha)$. For well-chosen groups, computing $g^{\alpha} \mapsto \alpha$ takes $\Theta(\sqrt{\#G})$.

→ Exponential separation!

Fast mixing: paths of length $\log(\# \text{ nodes})$ to everywhere.

With square-and-multiply, computing $\alpha \mapsto g^{\alpha}$ takes $\Theta(\log \alpha)$. For well-chosen groups, computing $g^{\alpha} \mapsto \alpha$ takes $\Theta(\sqrt{\#G})$.

→ Exponential separation!

...and they lived happily ever after?

Fast mixing: paths of length $\log(\# \text{ nodes})$ to everywhere.

With square-and-multiply, computing $\alpha \mapsto g^{\alpha}$ takes $\Theta(\log \alpha)$. For well-chosen groups, computing $g^{\alpha} \mapsto \alpha$ takes $\Theta(\sqrt{\#G})$.

→ Exponential separation!

...and they lived happily ever after?

Shor's quantum algorithm computes α from g^{α} in any group in polynomial time.

In some cases, isogeny graphs

can replace DLP-based constructions post-quantumly.

In some cases, isogeny graphs

can replace DLP-based constructions post-quantumly. s_{some}

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. ::
Plan for this talk

- ► High-level overview for intuition.
- \checkmark

- ► Elliptic curves & isogenies.
- The CGL hash function.
- The CSIDH non-interactive key exchange.
- The SQIsign signature scheme.

Stand back!



We're going to do math.

An elliptic curve over a field *F* of characteristic $\notin \{2,3\}$ is^{*} an equation of the form

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

with $a, b \in F$ such that $4a^3 + 27b^2 \neq 0$.

An elliptic curve over a field *F* of characteristic $\notin \{2,3\}$ is^{*} an equation of the form

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

with $a, b \in F$ such that $4a^3 + 27b^2 \neq 0$.

A point on *E* is a solution (x, y), <u>or</u> the "fake" point ∞ .

An elliptic curve over a field *F* of characteristic $\notin \{2,3\}$ is^{*} an equation of the form

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

with $a, b \in F$ such that $4a^3 + 27b^2 \neq 0$.

A point on *E* is a solution (x, y), <u>or</u> the "fake" point ∞ .

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

An elliptic curve over a field *F* of characteristic $\notin \{2,3\}$ is^{*} an equation of the form

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

with $a, b \in F$ such that $4a^3 + 27b^2 \neq 0$. 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

e of
$$(x, y)$$
 is $(x, -y)$.
 $f(x_1, y_1)$ and (x_2, y_2) is
$$\begin{pmatrix} a_0 & \mathbf{n}_{ot} \\ \delta h_{e_{S_e}} & \mathbf{n}_{ot} \\ \delta h_{e_{S_e}} & \delta h_{e_{T_e}} \\ \delta h_{e_{T_e}} & \mathbf{n}_{ot} \\ \delta h_{e_{S_e}} & \mathbf{n}_{o_{T_e}} \\ \delta h_{e_{T_e}} & \mathbf{n}_{o_{$$

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.

Elliptic curves (picture over \mathbb{R})



The elliptic curve $y^2 = x^3 - x + 1$ over \mathbb{R} .

Elliptic curves (picture over \mathbb{R})



Addition law: $P + Q + R = \infty \iff \{P, Q, R\}$ on a straight line.

Elliptic curves (picture over \mathbb{R})



The *point at infinity* ∞ lies on every vertical line.

Elliptic curves (picture over \mathbb{F}_p)



The same curve $y^2 = x^3 - x + 1$ over the finite field \mathbb{F}_{79} .

Elliptic curves (picture over \mathbb{F}_p)



The <u>addition law</u> of $y^2 = x^3 - x + 1$ over the finite field \mathbb{F}_{79} .



... are just fancily-named

nice maps

between elliptic curves.



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

An isogeny of elliptic curves is a non-zero map *E* → *E*' that is:
given by rational functions.

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

- given by rational functions.
- a group homomorphism.

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

- given by rational functions.
- a group homomorphism.

Reminder:

A rational function is f(x, y)/g(x, y) where f, g are polynomials.

A group homomorphism φ satisfies $\varphi(P + Q) = \varphi(P) + \varphi(Q)$.

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

- given by rational functions.
- a group homomorphism.

Reminder:

A rational function is f(x, y)/g(x, y) where f, g are polynomials. A group homomorphism φ satisfies $\varphi(P + Q) = \varphi(P) + \varphi(Q)$.

The kernel of an isogeny $\varphi : E \to E'$ is $\{P \in E : \varphi(P) = \infty\}$. 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.

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

- given by rational functions.
- a group homomorphism.

Example #1:
$$(x, y) \mapsto \left(\frac{x^3 - 4x^2 + 30x - 12}{(x-2)^2}, \frac{x^3 - 6x^2 - 14x + 35}{(x-2)^3} \cdot y\right)$$

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

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

- given by rational functions.
- a group homomorphism.

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 $\{\infty\}$.

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

- given by rational functions.
- a group homomorphism.

Example #3: For each $m \neq 0$, the multiplication-by-*m* map

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

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

- given by rational functions.
- a group homomorphism.

Example #3: For each $m \neq 0$, the multiplication-by-*m* map

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

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

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

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

- given by rational functions.
- a group homomorphism.

Example #4: For E/\mathbb{F}_q , the map

$$\pi\colon (x,y)\mapsto (x^q,y^q)$$

is a degree-*q* isogeny, the *Frobenius endomorphism*.

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

- given by rational functions.
- a group homomorphism.

Example #4: For E/\mathbb{F}_q , the map

$$\pi\colon (x,y)\mapsto (x^q,y^q)$$

is a degree-q isogeny, the *Frobenius endomorphism*.

The kernel of π –1 is precisely the set of rational points $E(\mathbb{F}_q)$.

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

- given by rational functions.
- a group homomorphism.

Example #4: For E/\mathbb{F}_q , the map

$$\pi\colon (x,y)\mapsto (x^q,y^q)$$

is a degree-*q* isogeny, the *Frobenius endomorphism*.

The kernel of π -1 is precisely the set of rational points $E(\mathbb{F}_q)$. Important <u>fact</u>: An isogeny φ is \mathbb{F}_q -rational iff $\pi \circ \varphi = \varphi \circ \pi$.

For any finite subgroup *G* of *E*, there exists a unique¹ separable^{*} isogeny $\varphi_G \colon E \to E'$ with kernel *G*.

¹(up to isomorphism of E')

For any finite subgroup *G* of *E*, there exists a unique¹ separable^{*} isogeny $\varphi_G \colon E \to E'$ with kernel *G*.

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

¹(up to isomorphism of E')

For any finite subgroup *G* of *E*, there exists a unique¹ 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')

For any finite subgroup *G* of *E*, there exists a unique¹ 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*.

 \rightsquigarrow To choose an isogeny, simply choose a finite subgroup.

¹(up to isomorphism of E')

For any finite subgroup *G* of *E*, there exists a unique¹ 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*.

- → To choose an isogeny, simply choose a finite subgroup.
 - We have formulas to compute and evaluate isogenies.
 (...but they are only efficient for "small" degrees!)

¹(up to isomorphism of E')

For any finite subgroup *G* of *E*, there exists a unique¹ 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*.

- \rightsquigarrow To choose an isogeny, simply choose a finite subgroup.
 - We have formulas to compute and evaluate isogenies.
 (...but they are only efficient for "small" degrees!)
- → Decompose large-degree isogenies into prime steps. That is: Walk in an isogeny graph.

¹(up to isomorphism of E')

Consider a field *k* and let $S \not\supseteq char(k)$ be a set of primes.

The *S*-isogeny graph over *k* consists of

Consider a field *k* and let $S \not\supseteq char(k)$ be a set of primes.

The *S*-isogeny graph over *k* consists of

vertices given by elliptic curves over k;

Consider a field *k* and let $S \not\supseteq char(k)$ be a set of primes.

The *S*-isogeny graph over *k* consists of

- vertices given by elliptic curves over k;
- edges given by ℓ -isogenies, $\ell \in S$, over k;

Consider a field *k* and let $S \not\supseteq char(k)$ be a set of primes.

The *S*-isogeny graph over *k* consists of

- vertices given by elliptic curves over k;
- edges given by ℓ -isogenies, $\ell \in S$, over k;

up to *k*-isomorphism.
Isogeny graphs

Consider a field *k* and let $S \not\supseteq char(k)$ be a set of primes.

The *S*-isogeny graph over *k* consists of

- vertices given by elliptic curves over k;
- edges given by ℓ -isogenies, $\ell \in S$, over k;

up to *k*-isomorphism.

Example components containing $E: y^2 = x^3 + x$:





Elliptic curves in general can be very annoying

Elliptic curves in general can be very annoying *computationally*: Points in $E[\ell]$ have a tendency to live in large extension fields.

Elliptic curves in general can be very annoying *computationally*: Points in $E[\ell]$ have a tendency to live in large extension fields.

Solution:

Let $p \ge 5$ be prime.

- E/\mathbb{F}_p is *supersingular* if and only if $\#E(\mathbb{F}_p) = p+1$.
- ▶ In that case, $E(\mathbb{F}_p) \cong \mathbb{Z}/(p+1)$ or $E(\mathbb{F}_p) \cong \mathbb{Z}/\frac{p+1}{2} \times \mathbb{Z}/2$, and $E(\mathbb{F}_{p^2}) \cong \mathbb{Z}/(p+1) \times \mathbb{Z}/(p+1)$.

Elliptic curves in general can be very annoying *computationally*: Points in $E[\ell]$ have a tendency to live in large extension fields.

Solution:

Let $p \ge 5$ be prime.

- E/\mathbb{F}_p is *supersingular* if and only if $\#E(\mathbb{F}_p) = p+1$.
- ▶ In that case, $E(\mathbb{F}_p) \cong \mathbb{Z}/(p+1)$ or $E(\mathbb{F}_p) \cong \mathbb{Z}/\frac{p+1}{2} \times \mathbb{Z}/2$, and $E(\mathbb{F}_{p^2}) \cong \mathbb{Z}/(p+1) \times \mathbb{Z}/(p+1)$.

→ Easy method to control the group structure by choosing *p*!
→ Cryptography works well using supersingular curves.

Elliptic curves in general can be very annoying *computationally*: Points in $E[\ell]$ have a tendency to live in large extension fields.

Solution:

Let $p \ge 5$ be prime.

- E/\mathbb{F}_p is *supersingular* if and only if $\#E(\mathbb{F}_p) = p+1$.
- ▶ In that case, $E(\mathbb{F}_p) \cong \mathbb{Z}/(p+1)$ or $E(\mathbb{F}_p) \cong \mathbb{Z}/\frac{p+1}{2} \times \mathbb{Z}/2$, and $E(\mathbb{F}_{p^2}) \cong \mathbb{Z}/(p+1) \times \mathbb{Z}/(p+1)$.

→ Easy method to control the group structure by choosing *p*!
→ Cryptography works well using supersingular curves.

(All curves are supersingular until lunch time.)

Plan for this talk

- ► High-level overview for intuition.
- ► Elliptic curves & isogenies.
- The CGL hash function.
- The CSIDH non-interactive key exchange.
- The SQIsign signature scheme.

The Charles–Goren–Lauter hash function



- ► Start at some curve *E*.
- For each input digit b: Map the pair (E, b) to a finite subgroup H ≤ E, compute φ_H: E → E', and set E ← E'.
- ► Finally return *E*.

Plan for this talk

- ► High-level overview for intuition.
- Elliptic curves & isogenies.
- ► The CGL hash function.
- The CSIDH non-interactive key exchange.
- The SQIsign signature scheme.

CSIDH ['sir,said]

A REAL PROPERTY &

[Castryck–Lange–Martindale–Panny–Renes 2018]

Ε



► Alice & Bob pick secret \(\varphi_A: E \rightarrow E_A\) and \(\varphi_B: E \rightarrow E_B\). (These isogenies correspond to walking on the isogeny graph.)



- ► Alice & Bob pick secret \(\varphi_A: E \rightarrow E_A\) and \(\varphi_B: E \rightarrow E_B\). (These isogenies correspond to walking on the isogeny graph.)
- Alice and Bob transmit the end curves E_A and E_B .



- ► Alice & Bob pick secret \(\varphi_A: E \rightarrow E_A\) and \(\varphi_B: E \rightarrow E_B\). (These isogenies correspond to walking on the isogeny graph.)
- Alice and Bob transmit the end curves E_A and E_B .
- Alice <u>somehow</u> finds a "parallel" $\varphi_{A'} : E_B \to E_{BA}$, and Bob <u>somehow</u> finds $\varphi_{B'} : E_A \to E_{AB}$,



- ► Alice & Bob pick secret \(\varphi_A: E \rightarrow E_A\) and \(\varphi_B: E \rightarrow E_B\). (These isogenies correspond to walking on the isogeny graph.)
- Alice and Bob transmit the end curves E_A and E_B .
- ► Alice <u>somehow</u> finds a "parallel" $\varphi_{A'}$: $E_B \to E_{BA}$, and Bob <u>somehow</u> finds $\varphi_{B'}$: $E_A \to E_{AB}$, such that $E_{AB} \cong E_{BA}$.

How to find "parallel" isogenies?



How to find "parallel" isogenies?



CSIDH's solution:

Use special isogenies φ_A which can be transported to the curve E_B totally independently of the secret isogeny φ_B . (Similarly with reversed roles, of course.)

"Special" isogenies

Let E/\mathbb{F}_p be supersingular and recall $E(\mathbb{F}_p) \cong \mathbb{Z}/(p+1)$.

"Special" isogenies

Let E/\mathbb{F}_p be supersingular and recall $E(\mathbb{F}_p) \cong \mathbb{Z}/(p+1)$.

 \Rightarrow For every $\ell \mid (p+1)$ exists a unique order- ℓ subgroup H_{ℓ} .

Let E/\mathbb{F}_p be supersingular and recall $E(\mathbb{F}_p) \cong \mathbb{Z}/(p+1)$.

- \Rightarrow For every $\ell \mid (p+1)$ exists a unique order- ℓ subgroup H_{ℓ} .
- \rightsquigarrow For all such *E* can canonically find an isogeny $\varphi_{\ell} \colon E \to E'$.

Let E/\mathbb{F}_p be supersingular and recall $E(\mathbb{F}_p) \cong \mathbb{Z}/(p+1)$.

- \Rightarrow For every $\ell \mid (p+1)$ exists a unique order- ℓ subgroup H_{ℓ} .
- \rightsquigarrow For all such *E* can canonically find an isogeny $\varphi_{\ell} \colon E \to E'$.

We consider prime ℓ and refer to φ_{ℓ} as a "special" isogeny.

What happens when we iterate such a "special" isogeny?

What happens when we iterate such a "special" isogeny?



What happens when we iterate such a "special" isogeny?



!! The "tail" $E \to E_{\ell^3}$ can't exist: Backwards arrow is unique.

What happens when we iterate such a "special" isogeny?



!! The "tail" $E \to E_{\ell^3}$ can't exist: Backwards arrow is unique. \implies The "special" isogenies φ_{ℓ} form isogeny cycles!

What happens when we compose those "special" isogenies?

What happens when we compose those "special" isogenies?



What happens when we compose those "special" isogenies?



• Exercise: $\ker(\varphi'_{\ell} \circ \varphi'_m) = \ker(\varphi_m \circ \varphi_{\ell}) = \langle \ker \varphi_{\ell}, \ker \varphi'_m \rangle.$

What happens when we compose those "special" isogenies?



► Exercise: $\ker(\varphi'_{\ell} \circ \varphi'_m) = \ker(\varphi_m \circ \varphi_{\ell}) = \langle \ker \varphi_{\ell}, \ker \varphi'_m \rangle$. !! The order cannot matter \implies cycles must be compatible.

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

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

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

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



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



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

CSIDH key exchange
























Cycles are compatible: [right then left] = [left then right]



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



Cycles are compatible: [right then left] = [left then right] \rightarrow only need to keep track of total step counts for each ℓ_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*!

<u>**Recall</u>:** Group action of $(\mathbb{Z}^n, +)$ on set of curves *X*.</u>

<u>**Recall</u>:** Group action of $(\mathbb{Z}^n, +)$ on set of curves *X*.</u>

!! The set *X* is **finite** \implies The action is **not free**. There exist vectors $\underline{v} \in \mathbb{Z}^n \setminus \{0\}$ which act trivially.

<u>**Recall</u>:** Group action of $(\mathbb{Z}^n, +)$ on set of curves *X*.</u>

!! The set *X* is **finite** \implies The action is **not free**. There exist vectors $\underline{v} \in \mathbb{Z}^n \setminus \{0\}$ which act trivially. Such \underline{v} form a full-rank subgroup $\Lambda \subseteq \mathbb{Z}^n$.

<u>**Recall</u>**: Group action of $(\mathbb{Z}^n, +)$ on set of curves *X*.</u>

!! The set *X* is **finite** \implies The action is **not free**. There exist vectors $\underline{v} \in \mathbb{Z}^n \setminus \{0\}$ which act trivially. Such \underline{v} form a full-rank subgroup $\Lambda \subseteq \mathbb{Z}^n$.

We understand the structure: By complex-multiplication theory, the quotient \mathbb{Z}^n/Λ is the ideal-class group $cl(\mathbb{Z}[\sqrt{-p}])$.

<u>**Recall</u>**: Group action of $(\mathbb{Z}^n, +)$ on set of curves *X*.</u>

!! The set *X* is **finite** \implies The action is **not free**. There exist vectors $\underline{v} \in \mathbb{Z}^n \setminus \{0\}$ which act trivially. Such \underline{v} form a full-rank subgroup $\Lambda \subseteq \mathbb{Z}^n$.

We understand the structure: By complex-multiplication theory, the quotient \mathbb{Z}^n/Λ is the ideal-class group $\operatorname{cl}(\mathbb{Z}[\sqrt{-p}])$.

!! This group characterizes *when two paths lead to the same curve*.

Why no Shor?

Shor's quantum algorithm computes α from g^{α} in any group in polynomial time.

Why no Shor?

Shor's quantum algorithm 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

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

Why no Shor?

Shor's quantum algorithm 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

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

For group <u>actions</u>, we simply cannot compose a * s and b * s!

Plan for this talk

- ► High-level overview for intuition.
- Elliptic curves & isogenies.
- ► The CGL hash function.
- The CSIDH non-interactive key exchange.
- The SQIsign signature scheme.



Now: Supersingular isogeny graphs <u>over \mathbb{F}_{p^2} </u>.

• Earlier: "Special" isogenies φ_{ℓ} with rational kernel points.

- Earlier: "Special" isogenies φ_{ℓ} with rational kernel points.
- ► In other words: ker $\varphi_{\ell} = \text{ker}[\ell] \cap \text{ker}(\pi 1)$. (Recall the Frobenius endomorphism $\pi: (x, y) \mapsto (x^p, y^p)$.)

- Earlier: "Special" isogenies φ_{ℓ} with rational kernel points.
- ► In other words: ker $\varphi_{\ell} = \text{ker}[\ell] \cap \text{ker}(\pi 1)$. (Recall the Frobenius endomorphism $\pi: (x, y) \mapsto (x^p, y^p)$.)
- **!!** Over \mathbb{F}_{p^2} , we can have more endomorphisms. Example: $y^2 = x^3 + x$ has $\iota: (x, y) \mapsto (-x, \sqrt{-1} \cdot y)$.

- Earlier: "Special" isogenies φ_{ℓ} with rational kernel points.
- ► In other words: ker $\varphi_{\ell} = \text{ker}[\ell] \cap \text{ker}(\pi 1)$. (Recall the Frobenius endomorphism $\pi : (x, y) \mapsto (x^p, y^p)$.)
- **!!** Over \mathbb{F}_{p^2} , we can have more endomorphisms. Example: $y^2 = x^3 + x$ has $\iota: (x, y) \mapsto (-x, \sqrt{-1} \cdot y)$.
- Extremely non-obvious fact in this setting:

<u>Every</u> isogeny $\varphi \colon E \to E'$ comes from a subset $I_{\varphi} \subseteq \operatorname{End}(E)$.

- Earlier: "Special" isogenies φ_{ℓ} with rational kernel points.
- ► In other words: ker $\varphi_{\ell} = \text{ker}[\ell] \cap \text{ker}(\pi 1)$. (Recall the Frobenius endomorphism $\pi: (x, y) \mapsto (x^p, y^p)$.)
- **!!** Over \mathbb{F}_{p^2} , we can have more endomorphisms. Example: $y^2 = x^3 + x$ has $\iota: (x, y) \mapsto (-x, \sqrt{-1} \cdot y)$.
- Extremely non-obvious fact in this setting:

<u>Every</u> isogeny $\varphi \colon E \to E'$ comes from a subset $I_{\varphi} \subseteq \operatorname{End}(E)$.

 \because We understand the structure of End(E).

- Earlier: "Special" isogenies φ_{ℓ} with rational kernel points.
- ► In other words: ker $\varphi_{\ell} = \text{ker}[\ell] \cap \text{ker}(\pi 1)$. (Recall the Frobenius endomorphism $\pi: (x, y) \mapsto (x^p, y^p)$.)
- **!!** Over \mathbb{F}_{p^2} , we can have more endomorphisms. Example: $y^2 = x^3 + x$ has $\iota: (x, y) \mapsto (-x, \sqrt{-1} \cdot y)$.
- Extremely non-obvious fact in this setting:

<u>Every</u> isogeny $\varphi \colon E \to E'$ comes from a subset $I_{\varphi} \subseteq \operatorname{End}(E)$.

- \because We understand the structure of End(*E*).
- \because We understand how I_{φ}, I_{ψ} relate for isogenies $\varphi, \psi \colon E \to E'$. (NB: Same E'.)

... is the formal version of what I just said.

... is the formal version of what I just said.

a priori ... is a strong connection between two^Yvery different worlds:

... is the formal version of what I just said.

... is a strong connection between two $\dot{\gamma}$ very different worlds:

a priori

• Supersingular elliptic curves defined over \mathbb{F}_{p^2} .

... is the formal version of what I just said.

a priori

- Supersingular elliptic curves defined over \mathbb{F}_{p^2} .
- Quaternions: Maximal orders in a certain algebra $B_{p,\infty}$.

... is the formal version of what I just said.

...is a strong connection between two^Yvery different worlds:

a priori

- Supersingular elliptic curves defined over \mathbb{F}_{p^2} .
- Quaternions: Maximal orders in a certain algebra $B_{p,\infty}$.

Isogenies become "connecting ideals" in quaternion land.

... is the formal version of what I just said.

a priori

- Supersingular elliptic curves defined over \mathbb{F}_{p^2} .
- Quaternions: Maximal orders in a certain algebra $B_{p,\infty}$.

Isogenies become "connecting ideals" in quaternion land.

∵ One direction is easy, the other seems hard! ~→ *Cryptography*!

The Deuring correspondence (examples)

Let p = 7799999 and let **i**, **j** satisfy $i^2 = -1$, $j^2 = -p$, ji = -ij.

The ring $\mathcal{O}_0 = \mathbb{Z} \oplus \mathbb{Z} \mathbf{i} \oplus \mathbb{Z} \frac{\mathbf{i}+\mathbf{j}}{2} \oplus \mathbb{Z} \frac{1+\mathbf{i}\mathbf{j}}{2}$ corresponds to the curve $E_0: y^2 = x^3 + x$.

The ring $\mathcal{O}_1 = \mathbb{Z} \oplus \mathbb{Z} 4947\mathbf{i} \oplus \mathbb{Z} \frac{4947\mathbf{i}+\mathbf{j}}{2} \oplus \mathbb{Z} \frac{4947+32631010\mathbf{i}+\mathbf{ij}}{9894}$ corresponds to the curve $E_1: y^2 = x^3 + 1$.

The ideal $I = \mathbb{Z} 4947 \oplus \mathbb{Z} 4947\mathbf{i} \oplus \mathbb{Z} \frac{598+4947\mathbf{i}+\mathbf{j}}{2} \oplus \mathbb{Z} \frac{4947+598\mathbf{i}+\mathbf{i}\mathbf{j}}{2}$ defines an isogeny $E_0 \to E_1$ of degree $4947 = 3 \cdot 17 \cdot 97$.
$E_0 \xrightarrow{secret} E_A$









► <u>Fiat-Shamir</u>: signature scheme from identification scheme.



- ► <u>Fiat–Shamir</u>: signature scheme from identification scheme.
- Easy response: $E_A \rightarrow E_0 \rightarrow E_1 \rightarrow E_2$. *Obviously broken*.



- ► <u>Fiat–Shamir</u>: signature scheme from identification scheme.
- Easy response: $E_A \rightarrow E_0 \rightarrow E_1 \rightarrow E_2$. *Obviously broken*.
- **<u>SQIsign's solution</u>**: Construct new path $E_A \rightarrow E_2$ (using secret).

<u>Main idea:</u>

- Construct the "signature square" in quaternion land.
- Project the whole situation down to the curve world.
- The verifier can check on curves that everything is correct.

Main idea:

- Construct the "signature square" in quaternion land.
- Project the whole situation down to the curve world.
- The verifier can check on curves that everything is correct.

Main technical tool: The KLPT algorithm.

- ▶ From End(E), End(E'), can find *smooth* isogeny $E \rightarrow E'$.
- ▶ From End(E), End(E'), can randomize within Hom(E, E').

Main idea:

- ► Construct the "signature square" in quaternion land.
- Project the whole situation down to the curve world.
- The verifier can check on curves that everything is correct.

Main technical tool: The KLPT algorithm.

- ▶ From End(E), End(E'), can find *smooth* isogeny $E \rightarrow E'$.
- ▶ From End(E), End(E'), can randomize within Hom(E, E').
- → SQIsign takes the "broken" signature $E_A \rightarrow E_0 \rightarrow E_1 \rightarrow E_2$ and rewrites it into a random isogeny $E_A \rightarrow E_2$.

Main idea:

- ► Construct the "signature square" in quaternion land.
- Project the whole situation down to the curve world.
- The verifier can check on curves that everything is correct.

Main technical tool: The KLPT algorithm.

- ▶ From End(E), End(E'), can find *smooth* isogeny $E \rightarrow E'$.
- ▶ From End(E), End(E'), can randomize within Hom(E, E').
- → SQIsign takes the "broken" signature $E_A \rightarrow E_0 \rightarrow E_1 \rightarrow E_2$ and rewrites it into a random isogeny $E_A \rightarrow E_2$.

"If you have KLPT implemented very nicely as a black box, then anyone can implement SQIsign." — Yan Bo Ti

SQIsign: Numbers

sizes

parameter set	public keys	signatures
NIST-I	64 bytes	177 bytes
NIST-III	96 bytes	263 bytes
NIST-V	128 bytes	335 bytes

performance

Cycle counts for a *generic C implementation* running on an Intel *Ice Lake* CPU. Optimizations are certainly possible and work in progress.

parameter set	keygen	signing	verifying
NIST-I	3728 megacycles	5779 megacycles	108 megacycles
NIST-III	23734 megacycles	43760 megacycles	654 megacycles
NIST-V	91049 megacycles	158544 megacycles	2177 megacycles

Source: https://sqisign.org

SQIsign: Comparison



Source: https://pqshield.github.io/nist-sigs-zoo

Plan for this talk

- ► High-level overview for intuition.
- ► Elliptic curves & isogenies.
- ► The CGL hash function.
- The CSIDH non-interactive key exchange.
- ► The SQIsign signature scheme.





CSIDH...

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

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).

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.

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.

SQIsign...

► has remarkably tiny keys and signatures, post-quantumly.

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.

SQIsign...

- ► has remarkably tiny keys and signatures, post-quantumly.
- ► rests on the assumed hardness of finding endomorphisms.

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.

SQIsign...

- ► has remarkably tiny keys and signatures, post-quantumly.
- ► rests on the assumed hardness of finding endomorphisms.

Both...

► have tiny sizes compared to other post-quantum schemes.

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.

SQIsign...

- ► has remarkably tiny keys and signatures, post-quantumly.
- ► rests on the assumed hardness of finding endomorphisms.

Both...

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

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.

SQIsign...

- ► has remarkably tiny keys and signatures, post-quantumly.
- ► rests on the assumed hardness of finding endomorphisms.

Both...

- ► have tiny sizes compared to other post-quantum schemes.
- ► are quite slow compared to other post-quantum schemes.
- ► are really cool!

Questions?