Isogenies: The basics, some applications, and not~~hing~~ much in between

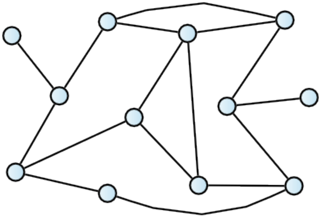
Lorenz Panny

Technische Universität München

5 December 2023

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.

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

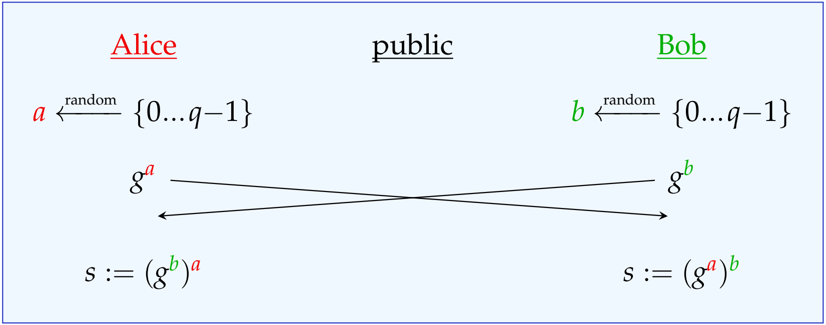
Public parameters:

- 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



Alice

public

Bob

$a \xleftarrow{\text{random}} \{0 \ldots q-1\}$

$b \xleftarrow{\text{random}} \{0 \ldots q-1\}$

g^a

g^b

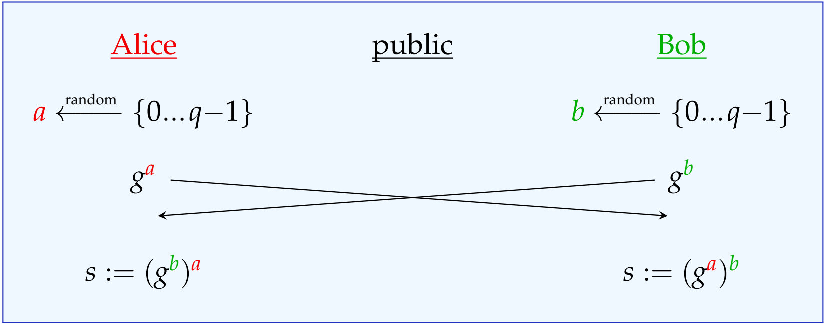
$s := (g^b)^a$

$s := (g^a)^b$

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



Alice

public

Bob

$a \xleftarrow{\text{random}} \{0 \ldots q-1\}$

$b \xleftarrow{\text{random}} \{0 \ldots q-1\}$

g^a

g^b

$s := (g^b)^a$

$s := (g^a)^b$

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

Diffie–Hellman: Bob vs. Eve

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 $B \leftarrow t \cdot g$.

Diffie–Hellman: Bob vs. Eve

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?

Diffie–Hellman: Bob vs. Eve

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 $B \leftarrow t \cdot g$.

Attacker Eve

1. Set $t \leftarrow g$. If $t = B$ return 1.
2. Set $t \leftarrow t \cdot g$. If $t = B$ return 2.
3. Set $t \leftarrow t \cdot g$. If $t = B$ return 3.
4. Set $t \leftarrow t \cdot g$. If $t = B$ return 3.

...

$b-2$. Set $t \leftarrow t \cdot g$. If $t = B$ return $b-2$.
$b-1$. Set $t \leftarrow t \cdot g$. If $t = B$ return $b-1$.
b. Set $t \leftarrow t \cdot g$. If $t = B$ return b.
$b+1$. Set $t \leftarrow t \cdot g$. If $t = B$ return $b + 1$.
$b+2$. Set $t \leftarrow t \cdot g$. If $t = B$ return $b + 2$.

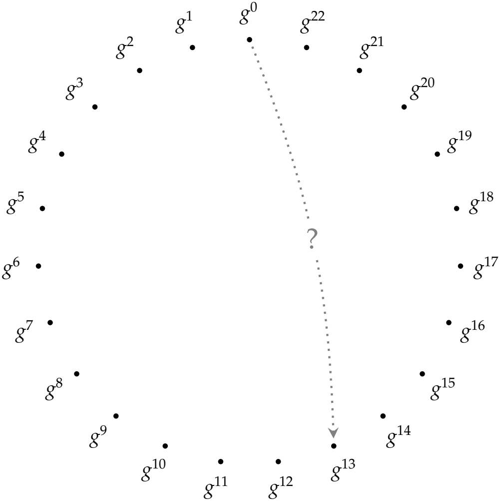
...

Diffie–Hellman: Bob vs. Eve

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 $b-1$.
b. Publish $B \leftarrow t \cdot g$.	b. Set $t \leftarrow t \cdot g$. If $t = B$ return b.
	$b+1$. Set $t \leftarrow t \cdot g$. If $t = B$ return $b+1$.
	$b+2$. Set $t \leftarrow t \cdot g$. If $t = B$ return $b+2$.
	...

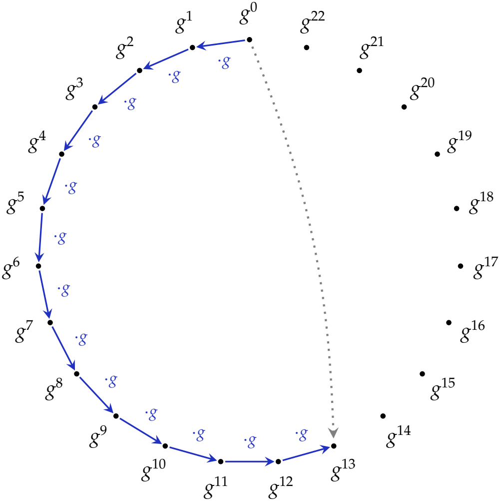
Effort for both: $O(\#G)$. Bob needs to be smarter.

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



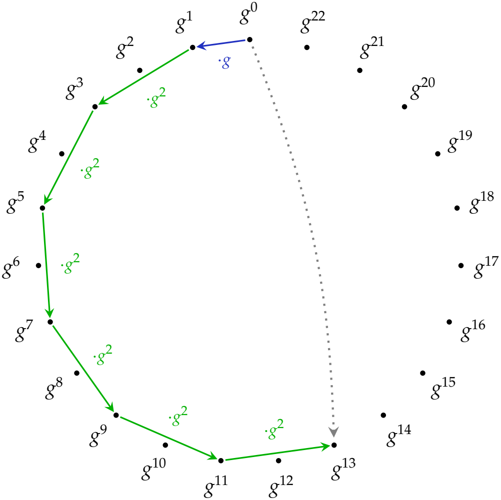
Bob computes his public key g^{13} from g.

multiply



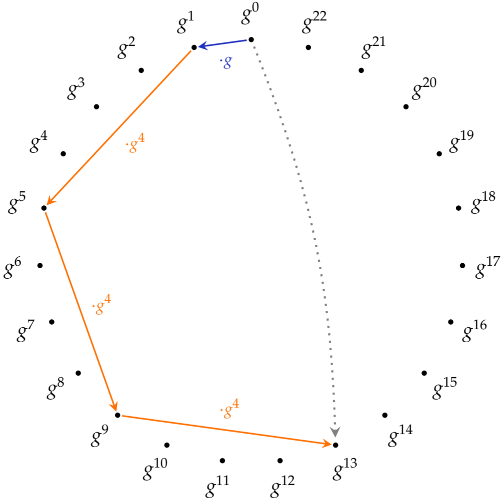
Bob computes his public key g^{13} from g.

Square-and-multiply



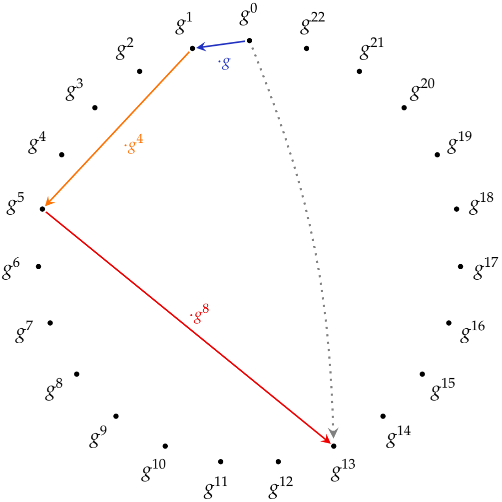
Bob computes his public key g^{13} from g.

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



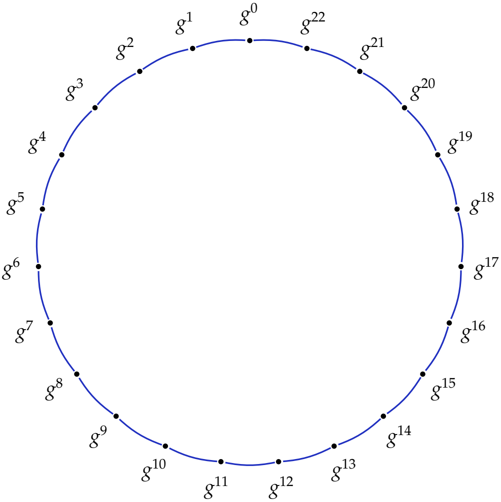
Bob computes his public key g^{13} from g.

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

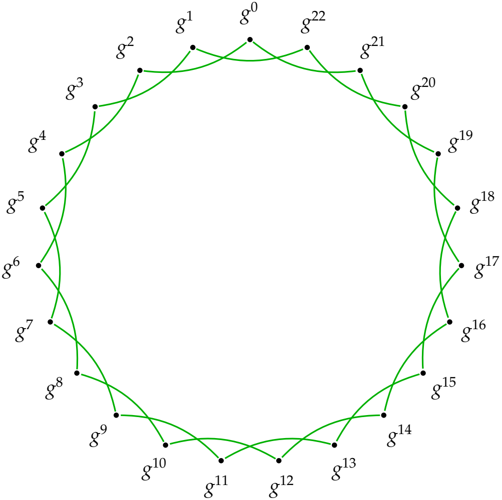


Bob computes his public key g^{13} from g.

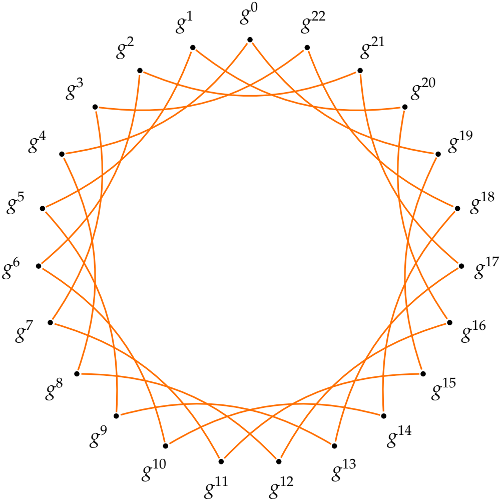
Square-and-multiply as graphs



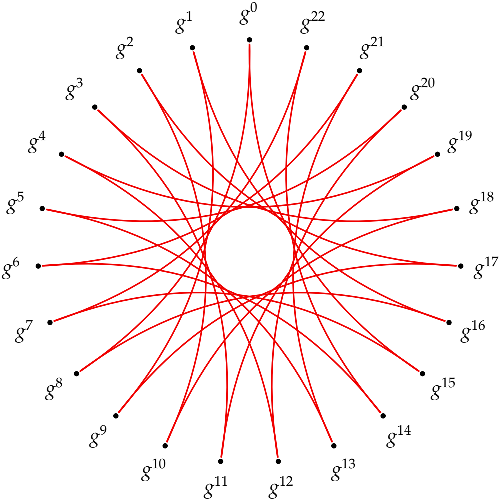
Square-and-multiply as graphs



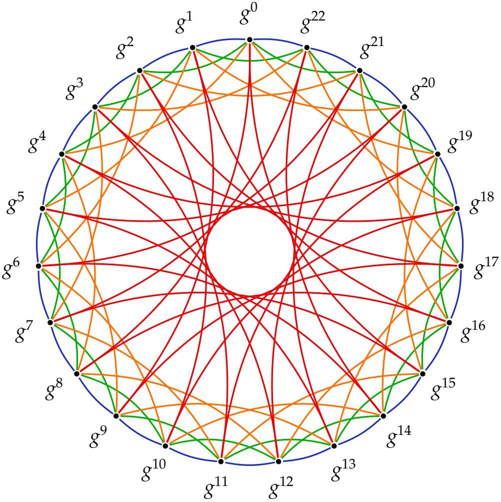
Square-and-multiply as graphs



Square-and-multiply as graphs



Square-and-multiply as a graph



Crypto on graphs?

We’ve been doing it all the time!

The fast mixing requirement

Fast mixing: paths of length log(# nodes) to everywhere.

The fast mixing requirement

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

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

The fast mixing requirement

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 $\Theta(\sqrt{\#G})$.

The fast mixing requirement

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 $\Theta(\sqrt{\#G})$.

$\rightsquigarrow$ Exponential separation!

The fast mixing requirement

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 $\Theta(\sqrt{\#G})$.

$\rightsquigarrow$ Exponential separation!

...and they lived happily ever after**?**

The fast mixing requirement

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 $\Theta(\sqrt{\#G})$.

$\rightsquigarrow$ 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.

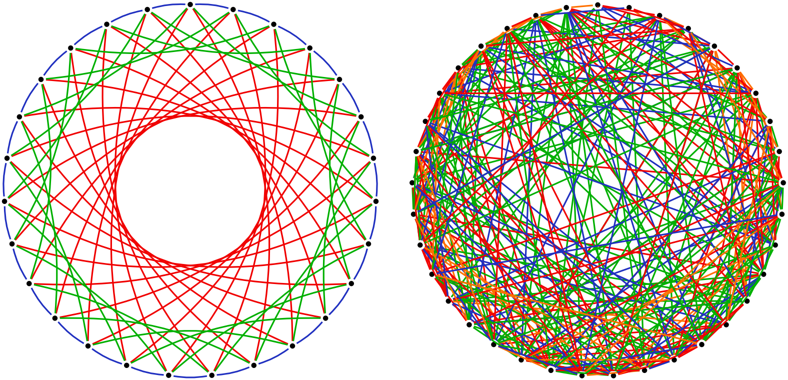
In some cases,

isogeny graphs

can replace $\underset{\textit{some}}{\curlywedge}$ DLP-based constructions post-quantumly.

The beauty and the beast

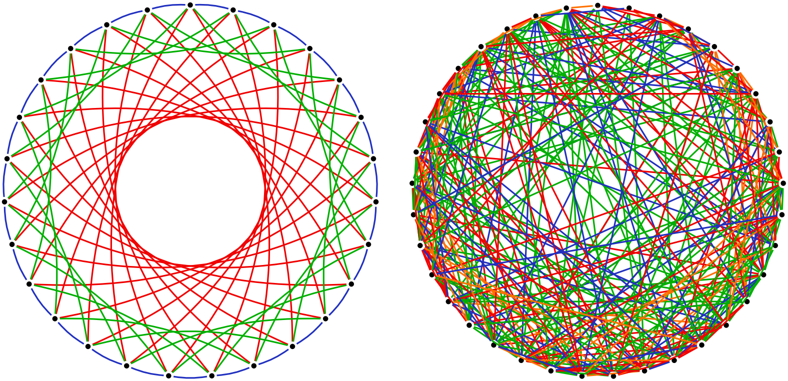
Components of particular isogeny graphs look like this:



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. ✓
- 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.

Elliptic curves

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

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

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

Elliptic curves

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

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

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 ∞.

Elliptic curves

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

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

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.

Elliptic curves

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

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

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.

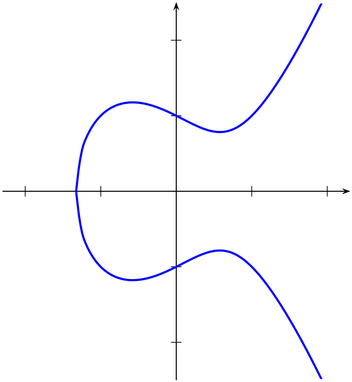
- The neutral element is ∞.
- The inverse of (x, y) is $(x, -y)$.
- The sum of (x_1, y_1) and (x_2, y_2) is

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

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.

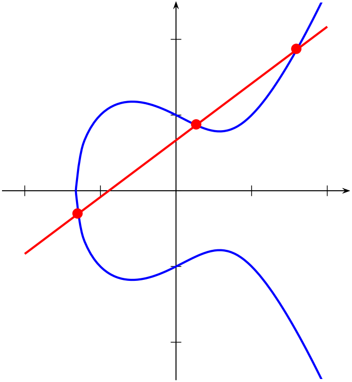
do **not** remember these formulas!

Elliptic curves (picture over $\mathbb{R}$)



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

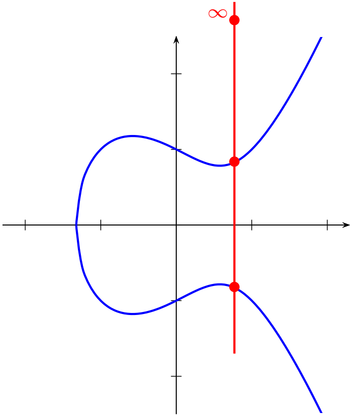
Elliptic curves (picture over $\mathbb{R}$)



Addition law:

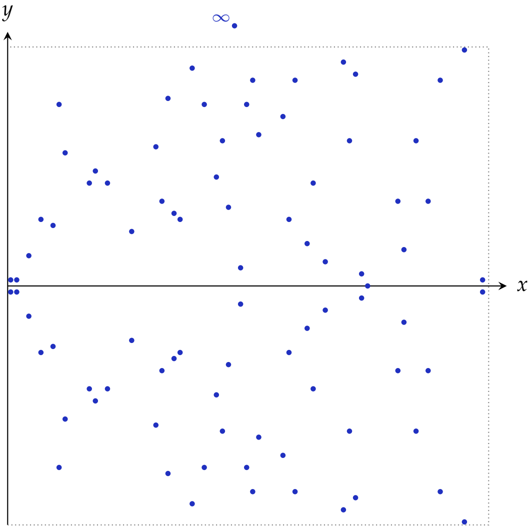
$$P + Q + R = \infty \quad \Longleftrightarrow \quad \{P, Q, R\} \text{ on a straight line.}$$

Elliptic curves (picture over $\mathbb{R}$)



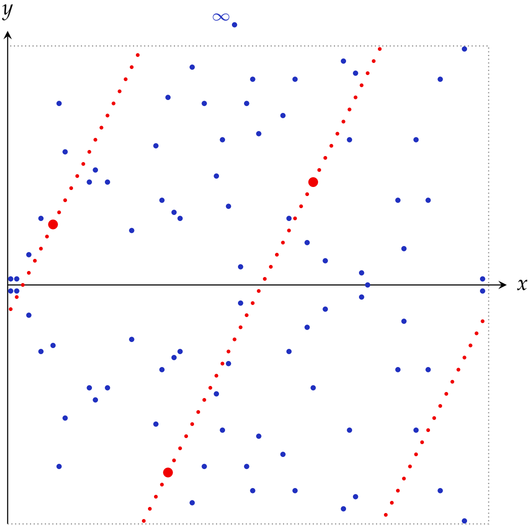
The *point at infinity* ∞ lies on every vertical line.

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

Isogenies

Isogenies

...are just fancily-named

nice maps

between elliptic curves.

Isogenies

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

Isogenies

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

- given by rational functions.

Isogenies

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

- given by rational functions.
- a group homomorphism.

Isogenies

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

- given by rational functions.
- a group homomorphism.

<u>Reminder</u>:

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

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

Isogenies

An isogeny of elliptic curves is a non-zero map $E \to E'$ 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 $\varphi\colon E \to E'$ is $\{P \in E \ : \ \varphi(P) = \infty\}$.
The degree of a separable* isogeny is the size of its kernel.

Isogenies (examples)

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

- given by rational functions.
- a group homomorphism.

Isogenies (examples)

An isogeny of elliptic curves is a non-zero map $E \to E'$ 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 $\{(2, 9), (2, -9), \infty\}$.

Isogenies (examples)

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

- given by rational functions.
- a group homomorphism.

Example #2: For any a and b, the map $\iota \colon (x, y) \mapsto (-x, \sqrt{-1} \cdot y)$ defines a degree-1 isogeny of the elliptic curves

$$\{y^2 = x^3 + ax + b\} \longrightarrow \{y^2 = x^3 + ax - b\}\,.$$

It is an *isomorphism*; its kernel is $\{\infty\}$.

Isogenies (examples)

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

- given by rational functions.
- a group homomorphism.

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

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

Isogenies (examples)

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

- given by rational functions.
- a group homomorphism.

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

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

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

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

Isogenies (examples)

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

- given by rational functions.
- a group homomorphism.

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

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

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

Isogenies (examples)

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

- given by rational functions.
- a group homomorphism.

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

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

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

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

Isogenies (examples)

An isogeny of elliptic curves is a non-zero map $E \to E'$ 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 $\pi - 1$ is precisely the set of rational points $E(\mathbb{F}_q)$.
Important <u>fact</u>: An isogeny φ is $\mathbb{F}_q$-rational iff $\pi \circ \varphi = \varphi \circ \pi$.

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.

---

[1] (up to isomorphism of E')

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)

---

[1] (up to isomorphism of E')

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')

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.

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

---

[1] (up to isomorphism of E')

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.

$\rightsquigarrow$ 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!)

---

[1] (up to isomorphism of E')

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.

$\rightsquigarrow$ 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!)

$\rightsquigarrow$ Decompose large-degree isogenies into prime steps.
That is: Walk in an isogeny graph.

---

[1] (up to isomorphism of E')

Isogeny graphs

Consider a field k and let $S \not\ni \mathrm{char}(k)$ be a set of primes.

The S-isogeny graph over k consists of

Isogeny graphs

Consider a field k and let $S \not\ni \mathrm{char}(k)$ be a set of primes.

The S-isogeny graph over k consists of

- vertices given by elliptic curves over k;

Isogeny graphs

Consider a field k and let $S \not\ni \mathrm{char}(k)$ 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;

Isogeny graphs

Consider a field k and let $S \not\ni \mathrm{char}(k)$ 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

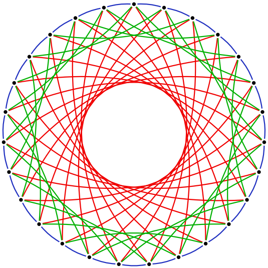
Consider a field k and let $S \not\ni \mathrm{char}(k)$ be a set of primes.

The S-isogeny graph over k consists of

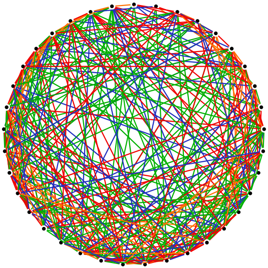
- vertices given by elliptic curves over k;
- edges given by ℓ-isogenies, $\ell \in S$, over k;

up to k-isomorphism.

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



$k = \mathbb{F}_{419},\ S = \{3, 5, 7\}$



$k = \mathbb{F}_{431^2},\ S = \{2, 3, 5, 7\}$.

Predictable groups

Elliptic curves in general can be very annoying

Predictable groups

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

Predictable groups

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

Solution:

Let $p \geq 5$ be prime.

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

Predictable groups

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

Solution:

Let $p \geq 5$ be prime.

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

$\rightsquigarrow$ Easy method to control the group structure by choosing p!

$\rightsquigarrow$ Cryptography works well using supersingular curves.

Predictable groups

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

<u>Solution:</u>

Let $p \geq 5$ be prime.

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

$\rightsquigarrow$ Easy method to control the group structure by choosing p!

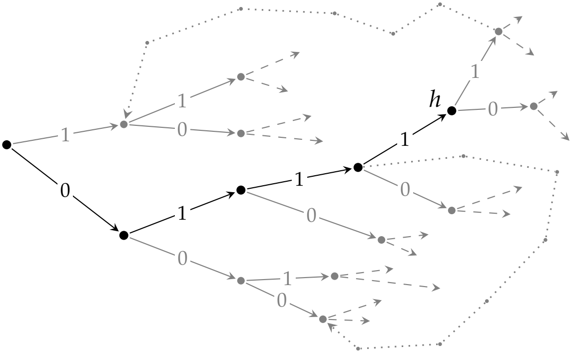
$\rightsquigarrow$ Cryptography works well using supersingular curves.

(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 $H \leq E$, compute $\varphi_H \colon E \to E'$, and set $E \leftarrow E'$.
- 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 [ˈsiːˌsaɪd]

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

Isogeny-based key exchange: High-level view

E

Isogeny-based key exchange: High-level view

$$\begin{tikzcd}
E \arrow[r, "\varphi_A"] \arrow[d, "\varphi_B"'] & E_A \\
E_B &
\end{tikzcd}$$

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

Isogeny-based key exchange: High-level view

$$\begin{tikzcd}
E \arrow[r, "\varphi_A"] \arrow[d, "\varphi_B"'] & E_A \arrow[dl, dashed, shift left] \\
E_B \arrow[ur, dashed, shift left] &
\end{tikzcd}$$

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

Isogeny-based key exchange: High-level view

$$\begin{tikzcd}
E \arrow[rr, "\varphi_A", red] \arrow[dd, "\varphi_B"', green] & & E_A \arrow[d, "\varphi'_B", green] \arrow[ddll, dashed, red] \\
 & & E_{AB} \\
E_B \arrow[r, "\varphi'_A"', red] \arrow[uurr, dashed, green] & E_{BA} &
\end{tikzcd}$$

- Alice & Bob pick secret $\varphi_A : E \to E_A$ and $\varphi_B : E \to E_B$.
  (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 $\varphi_{B'} : E_A \to E_{AB}$,

Isogeny-based key exchange: High-level view

$$\begin{tikzcd}
E \arrow[rr, "\varphi_A"] \arrow[dd, "\varphi_B"'] & & E_A \arrow[d, "\varphi'_B"] \arrow[ddll, dashed] \\
 & & E_{AB} \\
E_B \arrow[r, "\varphi'_A"'] \arrow[uurr, dashed] & E_{BA} \arrow[ur, equal] &
\end{tikzcd}$$

- Alice & Bob pick secret $\varphi_A : E \to E_A$ and $\varphi_B : E \to E_B$.
  (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?

$$\begin{tikzcd}
E \arrow[rr, "\varphi_A"] \arrow[dd, "\varphi_B"'] & & E_A \arrow[d, thick, "\varphi'_B"] \\
& & E_{AB} \\
E_B \arrow[r, thick, "\varphi'_A"'] & E_{BA} \arrow[ur, equal] &
\end{tikzcd}$$

How to find “parallel” isogenies?

$$\begin{tikzcd}
E \arrow[rr, "\varphi_A"] \arrow[dd, "\varphi_B"'] & & E_A \arrow[d, "\varphi'_B"] \\
& & E_{AB} \\
E_B \arrow[r, "\varphi'_A"'] & E_{BA} \arrow[ur, equal] &
\end{tikzcd}$$

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.

“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.

$\rightsquigarrow$ For all such E can canonically find an isogeny $\varphi_\ell \colon E \to E'$.

“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.

$\rightsquigarrow$ 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.

Cycles from “special” isogenies

What happens when we iterate such a “special” isogeny?

Cycles from “special” isogenies

What happens when we iterate such a “special” isogeny?

$$\begin{tikzcd}
 & & & E_{\ell^{r-1}} \arrow[dl] & \cdots \arrow[l] & E_{\ell^6} \arrow[l] \\
 & & E_{\ell^r} \arrow[ddr] & & & E_{\ell^5} \arrow[u] \\
 & & & & E_{\ell^4} \arrow[ur] & \\
E \arrow[r] & E_\ell \arrow[r] & E_{\ell^2} \arrow[r] & E_{\ell^3} \arrow[ur] & &
\end{tikzcd}$$

Cycles from "special" isogenies

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

$$\begin{tikzcd}
 & & & & & & \cdots \arrow[dll] & E_{\ell^6} \arrow[l] \\
 & & & & E_{\ell^{r-1}} \arrow[dl] & & & \\
 & & & E_{\ell^r} \arrow[dd] & & & & E_{\ell^5} \arrow[uu] \\
 & & & & & E_{\ell^4} \arrow[urr] & & \\
E \arrow[r] & E_\ell \arrow[r] & E_{\ell^2} \arrow[r] & E_{\ell^3} \arrow[urr] & & & &
\end{tikzcd}$$

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

Cycles from “special” isogenies

What happens when we iterate such a “special” isogeny?

$$\begin{tikzcd}
 & & & & \cdots \arrow[dl] & E_{\ell^6} \arrow[l] \\
 & & & E_{\ell^{r-1}} \arrow[d] & & \\
 & & & E_{\ell^r} \arrow[dd] & & E_{\ell^5} \arrow[uu] \\
 & & & & E_{\ell^4} \arrow[ur] & \\
E \arrow[r] & E_\ell \arrow[r] & E_{\ell^2} \arrow[r] & E_{\ell^3} \arrow[ur] & &
\end{tikzcd}$$

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

$\Longrightarrow$ The “special” isogenies φ_ℓ form isogeny cycles!

Compatible cycles from “special” isogenies

What happens when we compose those “special” isogenies?

Compatible cycles from “special” isogenies

What happens when we compose those “special” isogenies?

$$\begin{tikzcd}
 & & E_{m\ell} & E_{\ell m} \\
 & E_m \arrow[ur, "\varphi'_\ell"] & & \\
 & & E_\ell \arrow[uur, "\varphi_m"] & \\
E \arrow[uur, "\varphi'_m"] \arrow[urr, "\varphi_\ell"] & & &
\end{tikzcd}$$

Compatible cycles from “special” isogenies

What happens when we compose those “special” isogenies?

$$\begin{tikzcd}
 & & E_{m\ell} & E_{\ell m} \\
E_m \arrow[urr, "\varphi'_\ell"] & & & \\
 & & E_\ell \arrow[uur, "\varphi_m"] & \\
E \arrow[uu, "\varphi'_m"] \arrow[urr, "\varphi_\ell"] & & &
\end{tikzcd}$$

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

Compatible cycles from “special” isogenies

What happens when we compose those “special” isogenies?

$$\begin{tikzcd}
E_m \arrow[r, "\varphi'_\ell"] & E_{\ell m} \\
E \arrow[u, "\varphi'_m"] \arrow[r, "\varphi_\ell"] & E_\ell \arrow[u, "\varphi_m"']
\end{tikzcd}$$

- 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.

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

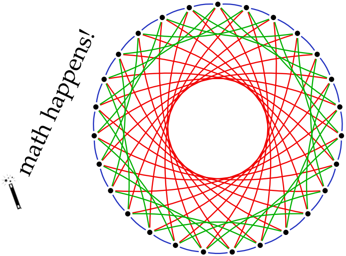
- Choose some small odd primes $\ell_1, ..., \ell_n$.
- Make sure $p = 4 \cdot \ell_1 \cdots \ell_n - 1$ is prime.
- Let $X = \{y^2 = x^3 + Ax^2 + x$ supersingular with $A \in \mathbb{F}_p\}$.

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 "special" ℓ_i-isogenies 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 "special" ℓ_i-isogenies within X.



$p = 419$

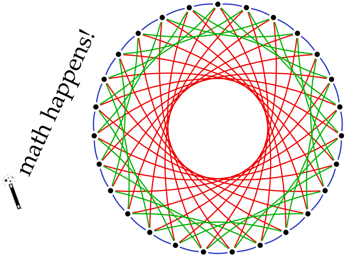
$\ell_1 = 3$

$\ell_2 = 5$

$\ell_3 = 7$

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 "special" ℓ_i-isogenies within X.



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

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

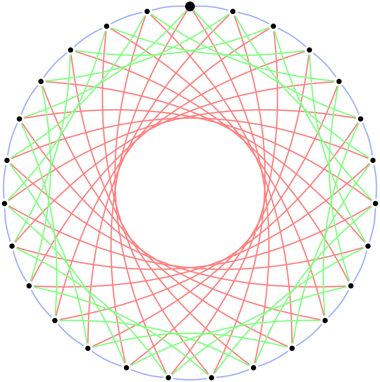
CSIDH key exchange

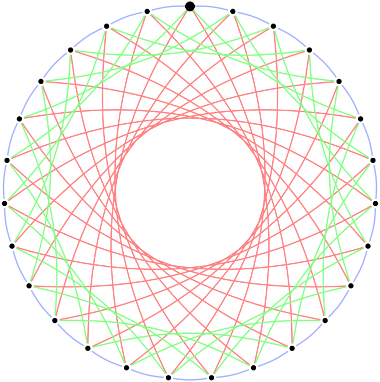
Alice

[+, +, −, −]

Bob

[−, +, −, −]





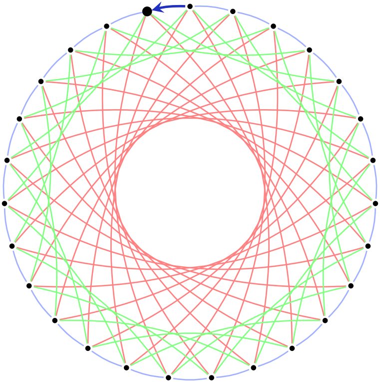
CSIDH key exchange

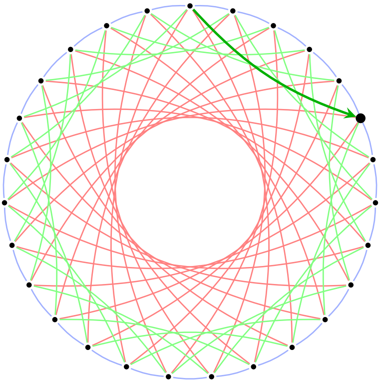
Alice

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

Bob

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

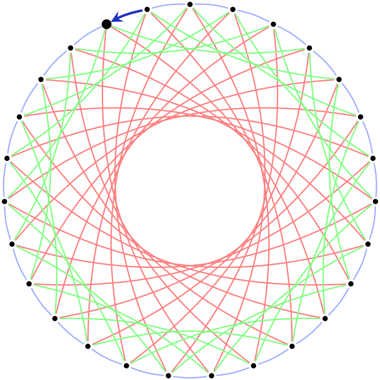




CSIDH key exchange

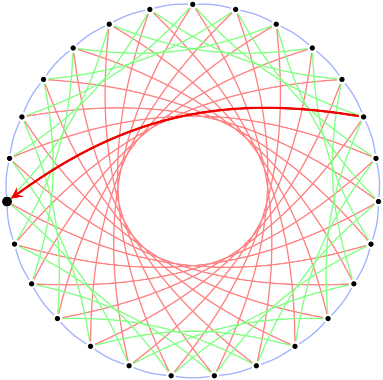
Alice

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



Bob

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



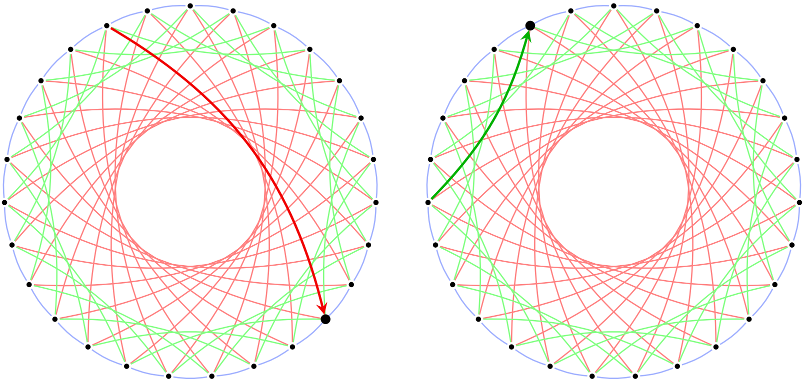
CSIDH key exchange

Alice

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

Bob

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

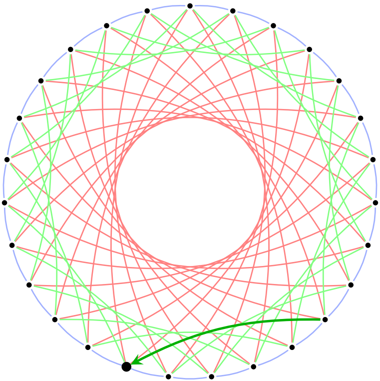


CSIDH key exchange

Alice

[+, +, −, −]

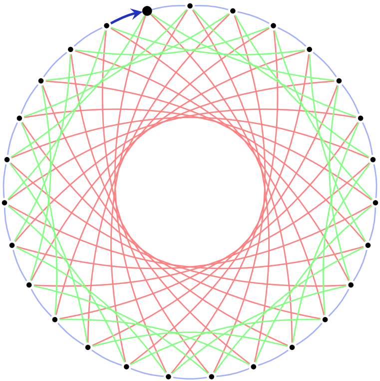
↑



Bob

[−, +, −, −]

↑



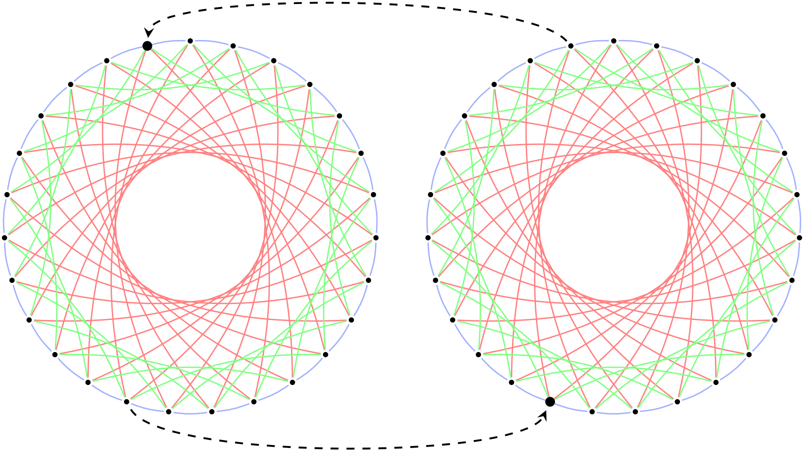
CSIDH key exchange

Alice

[**+**, **+**, **−**, **−**]

Bob

[**−**, **+**, **−**, **−**]



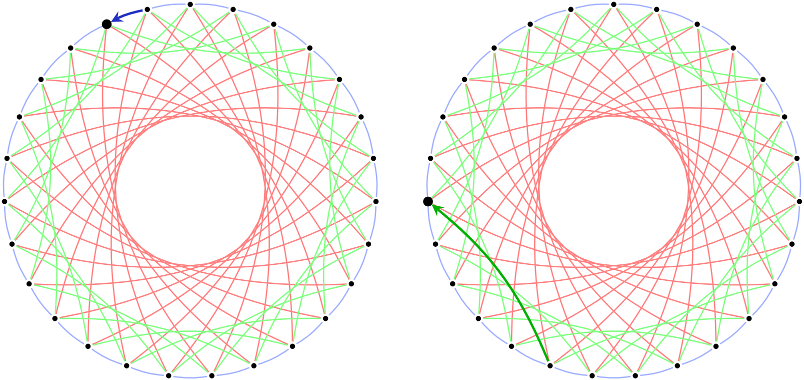
CSIDH key exchange

Alice

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

Bob

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



CSIDH key exchange

Alice

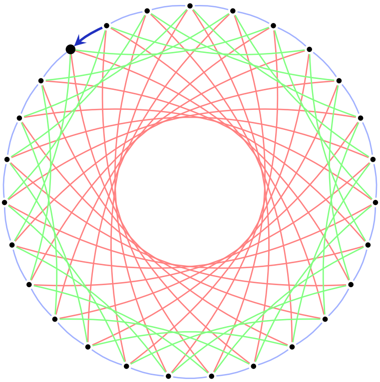
[+, +, −, −]

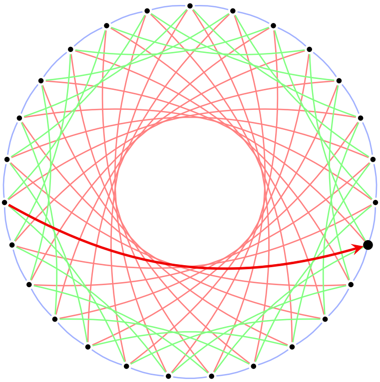
↑

Bob

[−, +, −, −]

↑

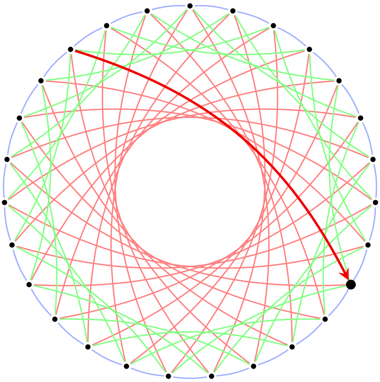




CSIDH key exchange

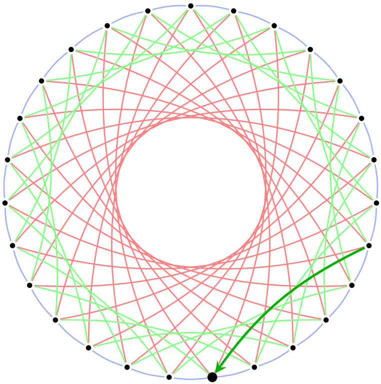
Alice

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



Bob

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



CSIDH key exchange

Alice

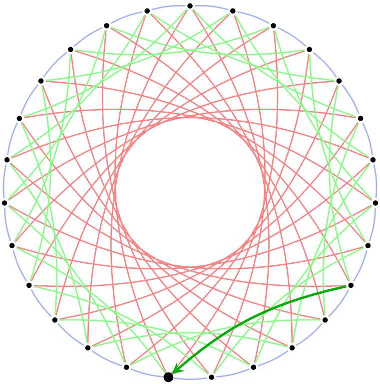
[+, +, −, −]

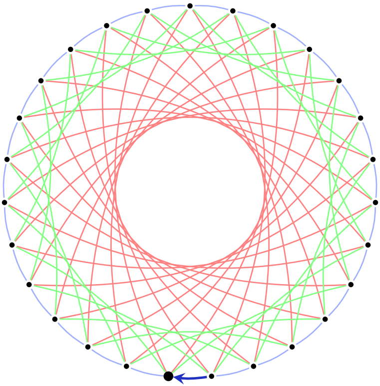
↑

Bob

[−, +, −, −]

↑

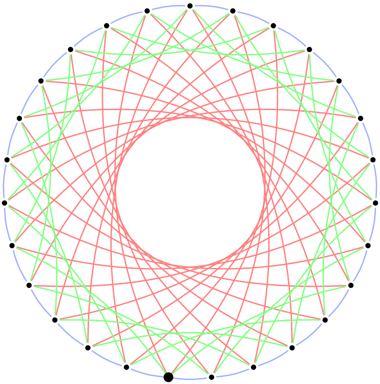




CSIDH key exchange

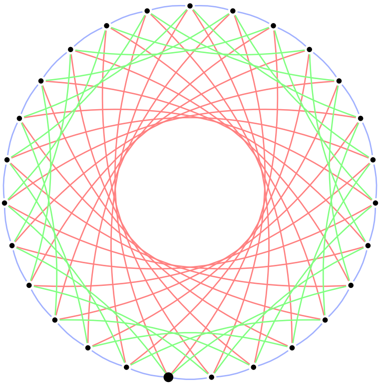
Alice

$[+, +, -, -]$



Bob

$[-, +, -, -]$



And... action!

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

And... 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 $(+1, \quad 0, -3) \in \mathbb{Z}^3$.

And... 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: $[\mathbf{+},\mathbf{+},\mathbf{-},\mathbf{-},\mathbf{-},\mathbf{+},\mathbf{-},\mathbf{-}]$ 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!

The class group

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

The class group

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

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

The class group

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

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

The class group

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

!! The set X is **finite** $\Longrightarrow$ 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 $\mathbb{Z}^n/\Lambda$ is the ideal-class group $\mathrm{cl}(\mathbb{Z}[\sqrt{-p}])$.

The class group

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

!! The set X is **finite** $\Longrightarrow$ The action is **not free**.
There exist vectors $\underline{v} \in \mathbb{Z}^n \backslash \{0\}$ 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 $\mathbb{Z}^n / \Lambda$ is the ideal-class group $\mathrm{cl}(\mathbb{Z}[\sqrt{-p}])$.

!! 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

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

Why no Shor?

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

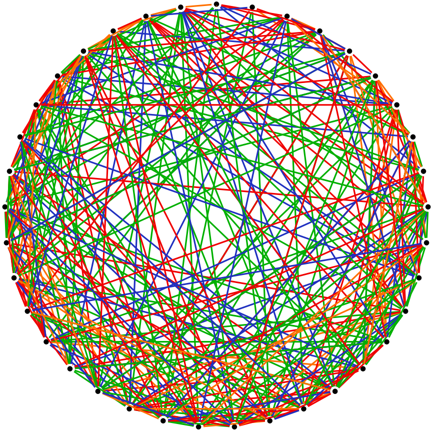
Shor computes α from $h = g^\alpha$ by finding the kernel of the map

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

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

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

More “special” isogenies

- Earlier: “Special” isogenies φ_ℓ with rational kernel points.

More “special” isogenies

- Earlier: “Special” isogenies φ_ℓ with rational kernel points.
- In other words: $\ker \varphi_\ell = \ker[\ell] \cap \ker(\pi - 1)$.
  (Recall the Frobenius endomorphism $\pi\colon\ (x, y) \mapsto (x^p, y^p)$.)

More “special” isogenies

- Earlier: “Special” isogenies φ_ℓ with rational kernel points.
- In other words: $\ker\varphi_\ell = \ker[\ell] \cap \ker(\pi - 1)$.
  (Recall the Frobenius endomorphism $\pi\colon (x,y) \mapsto (x^p, y^p)$.)

!! Over $\mathbb{F}_{p^2}$, we can have more endomorphisms.
Example: $y^2 = x^3 + x$ has $\iota\colon (x,y) \mapsto (-x, \sqrt{-1}\cdot y)$.

More “special” isogenies

- Earlier: “Special” isogenies φ_ℓ with rational kernel points.
- In other words: $\ker \varphi_\ell = \ker[\ell] \cap \ker(\pi - 1)$.
  (Recall the Frobenius endomorphism $\pi\colon\ (x, y) \mapsto (x^p, y^p)$.)

!! Over $\mathbb{F}_{p^2}$, we can have more endomorphisms.
Example: $y^2 = x^3 + x$ has $\iota\colon\ (x, y) \mapsto (-x, \sqrt{-1} \cdot y)$.

- Extremely non-obvious fact in this setting:

Every isogeny $\varphi\colon E \to E'$ comes from a subset $I_\varphi \subseteq \mathrm{End}(E)$.

More “special” isogenies

- Earlier: “Special” isogenies φ_ℓ with rational kernel points.
- In other words: $\ker \varphi_\ell = \ker[\ell] \cap \ker(\pi - 1)$.
  (Recall the Frobenius endomorphism $\pi\colon\ (x, y) \mapsto (x^p, y^p)$.)

!! Over $\mathbb{F}_{p^2}$, we can have more endomorphisms.
Example: $y^2 = x^3 + x$ has $\iota\colon\ (x, y) \mapsto (-x, \sqrt{-1} \cdot y)$.

- Extremely non-obvious fact in this setting:

Every isogeny $\varphi\colon E \to E'$ comes from a subset $I_\varphi \subseteq \mathrm{End}(E)$.

☺ We understand the structure of $\mathrm{End}(E)$.

More “special” isogenies

- Earlier: “Special” isogenies φ_ℓ with rational kernel points.
- In other words: $\ker\varphi_\ell = \ker[\ell] \cap \ker(\pi - 1)$.
  (Recall the Frobenius endomorphism $\pi\colon\ (x,y) \mapsto (x^p, y^p)$.)

!! Over $\mathbb{F}_{p^2}$, we can have more endomorphisms.
Example: $y^2 = x^3 + x$ has $\iota\colon\ (x,y) \mapsto (-x, \sqrt{-1}\cdot y)$.

- Extremely non-obvious fact in this setting:

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

:) We understand the structure of $\operatorname{End}(E)$.

:) We understand how I_φ, I_ψ relate for isogenies $\varphi, \psi\colon E \to E'$.
(NB: Same E'.)

The Deuring correspondence

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

The Deuring correspondence

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

...is a strong connection between two $\overset{\textit{a priori}}{\curlyvee}$ very different worlds:

The Deuring correspondence

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

...is a strong connection between two$\overset{\textit{a priori}}{\curlyvee}$very different worlds:

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

The Deuring correspondence

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

...is a strong connection between two $\overset{\textit{a priori}}{\curlyvee}$ very different worlds:

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

The Deuring correspondence

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

...is a strong connection between two$\overset{\textit{a priori}}{\curlyvee}$very different worlds:

- 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.

The Deuring correspondence

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

...is a strong connection between two $\overset{\textit{a priori}}{\curlyvee}$ very different worlds:

- 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 $\mathbf{i}, \mathbf{j}$ satisfy $\mathbf{i}^2 = -1,\ \mathbf{j}^2 = -p,\ \mathbf{ji} = -\mathbf{ij}$.

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

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 $E_1\colon\ y^2 = x^3 + 1$.

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

Signing with isogenies

$$\begin{tikzcd} E_0 \arrow[r, dashed, "\textit{secret}"] & E_A \end{tikzcd}$$

Signing with isogenies

$$\begin{tikzcd}
E_0 \arrow[rr, dashed, "\mathit{secret}"] \arrow[d, "\mathit{commitment}"'] & & E_A \\
E_1
\end{tikzcd}$$

Signing with isogenies

$$\begin{tikzcd}
E_0 \arrow[r, dashed, "secret"] \arrow[d, "commitment"'] & E_A \\
E_1 \arrow[r, "challenge"'] & E_2
\end{tikzcd}$$

Signing with isogenies

$$\begin{tikzcd}
E_0 \arrow[r, dashed, "\textit{secret}"] \arrow[d, "\textit{commitment}"'] & E_A \arrow[d, thick, "\textit{signature}"] \\
E_1 \arrow[r, "\textit{challenge}"'] & E_2
\end{tikzcd}$$

Signing with isogenies

$$\begin{tikzcd}
E_0 \arrow[r, dashed, "\textit{secret}"] \arrow[d, "\textit{commitment}"'] & E_A \arrow[d, line width=1.5pt, "\textit{signature}"] \\
E_1 \arrow[r, "\textit{challenge}"'] & E_2
\end{tikzcd}$$

- Fiat–Shamir: signature scheme from identification scheme.

Signing with isogenies

$$\begin{tikzcd}
E_0 \arrow[r, dashed, "\textit{secret}"] \arrow[d, "\textit{commitment}"'] & E_A \arrow[d, thick, "\textit{signature}"] \\
E_1 \arrow[r, "\textit{challenge}"'] & E_2
\end{tikzcd}$$

- Fiat–Shamir: signature scheme from identification scheme.
- Easy response: $E_A \to E_0 \to E_1 \to E_2$. *Obviously broken.*

Signing with isogenies

$$\begin{tikzcd}
E_0 \arrow[r, dashed, "\textit{secret}"] \arrow[d, "\textit{commitment}"'] & E_A \arrow[d, thick, "\textit{signature}"] \\
E_1 \arrow[r, "\textit{challenge}"'] & E_2
\end{tikzcd}$$

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

SQIsign

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.

SQIsign

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 $\mathrm{End}(E), \mathrm{End}(E')$, can find *smooth* isogeny $E \to E'$.
- From $\mathrm{End}(E), \mathrm{End}(E')$, can randomize within $\mathrm{Hom}(E, E')$.

SQIsign

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 $\mathrm{End}(E), \mathrm{End}(E')$, can find *smooth* isogeny $E \to E'$.
- From $\mathrm{End}(E), \mathrm{End}(E')$, can randomize within $\mathrm{Hom}(E, E')$.

$\rightsquigarrow$ SQIsign takes the “broken” signature $E_A \to E_0 \to E_1 \to E_2$ and rewrites it into a random isogeny $E_A \to E_2$.

SQIsign

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.

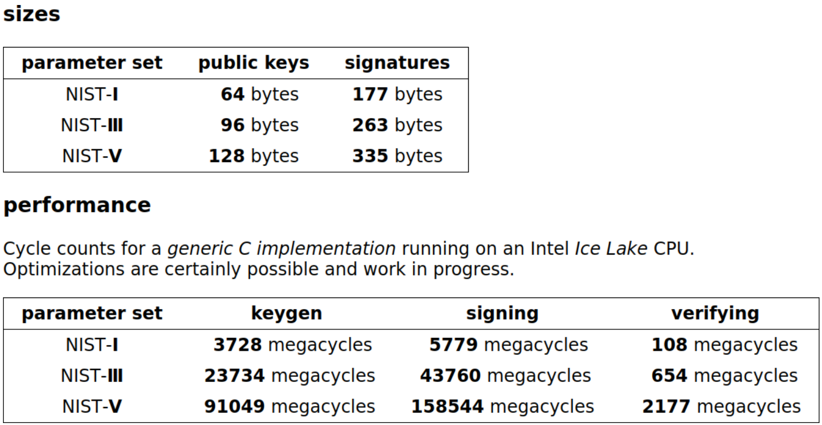
Main technical tool: The KLPT algorithm.

- From $\mathrm{End}(E), \mathrm{End}(E')$, can find *smooth* isogeny $E \to E'$.
- From $\mathrm{End}(E), \mathrm{End}(E')$, can randomize within $\mathrm{Hom}(E, E')$.

$\rightsquigarrow$ SQIsign takes the “broken” signature $E_A \to E_0 \to E_1 \to E_2$ and rewrites it into a random isogeny $E_A \to E_2$.

> *“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

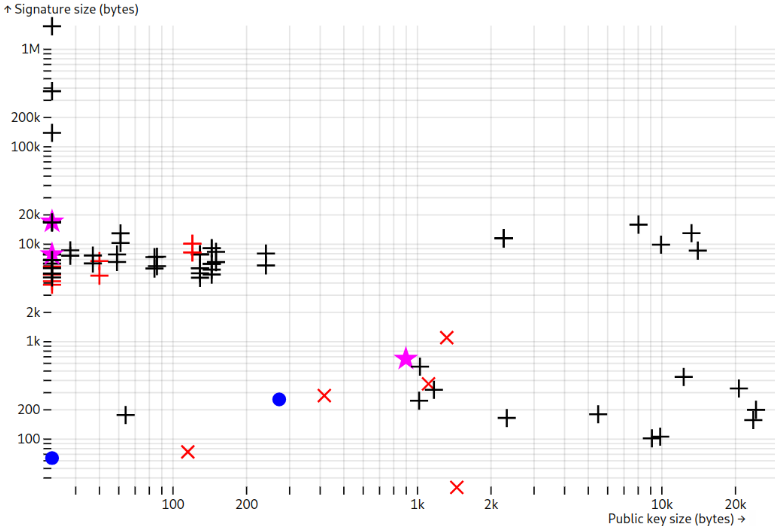
performance

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. ✓

Summary

Summary

CSIDH...

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

Summary

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).

Summary

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.

Summary

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.

Summary

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.

Summary

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.

Summary

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.

Summary

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?