Introduction to Isogeny-based Cryptography

Chloe Martindale Lorenz Panny

Technische Universiteit Eindhoven

SIAM-AG, Bern, Switzerland, 10 July 2019

Why Isogeny-Based Crypto?

The discrete logarithm problem (DLP) is a fundamental building block in crypto:

The DLP:

Let G be a group. For $g \in G$ and $n \in \mathbb{Z}$, given g and g^n, find n.

Why Isogeny-Based Crypto?

The discrete logarithm problem (DLP) is a fundamental building block in crypto:

The DLP:

Let G be a group. For $g \in G$ and $n \in \mathbb{Z}$, given g and g^n, find n.

- In crypto, we use G where the DLP is (sub-)exponentially harder than computing g^n.

Why Isogeny-Based Crypto?

The discrete logarithm problem (DLP) is a fundamental building block in crypto:

The DLP:

Let G be a group. For $g \in G$ and $n \in \mathbb{Z}$, given g and g^n, find n.

- In crypto, we use G where the DLP is (sub-)exponentially harder than computing g^n.
- Shor's algorithm makes the DLP only polynomially harder than computing g^n for any group G – with a quantum computer.

Why Isogeny-Based Crypto?

The discrete logarithm problem (DLP) is a fundamental building block in crypto:

The DLP:
Let G be a group. For $g \in G$ and $n \in \mathbb{Z}$, given g and g^n, find n.

- In crypto, we use G where the DLP is (sub-)exponentially harder than computing g^n.
- Shor's algorithm makes the DLP only polynomially harder than computing g^n for any group G – with a quantum computer.

One solution: Isogeny-based cryptography.

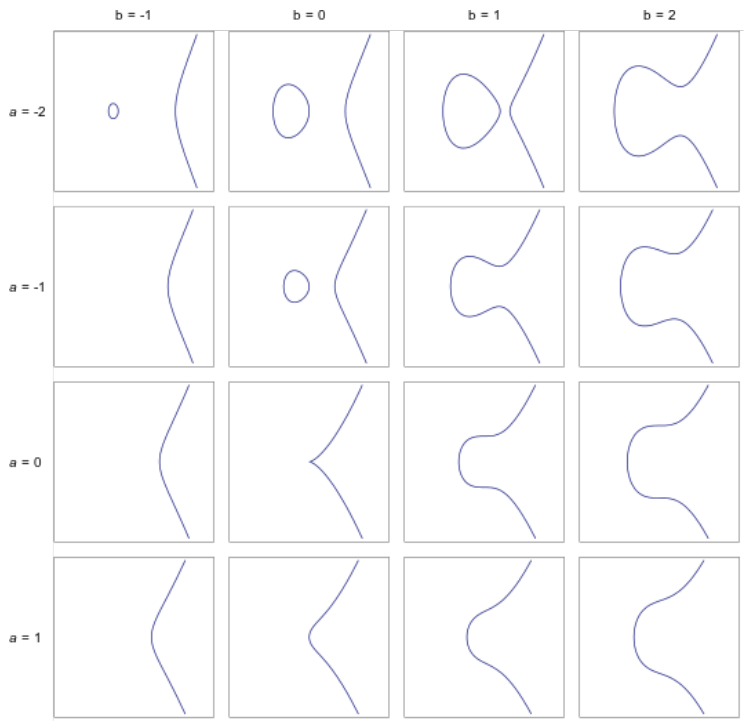
Fundamentals: elliptic curves

Definition

Let k be a field of characteristic $\neq 2$. An elliptic curve over k is a smooth[1] curve

$$E/k : y^2 = f(x),$$

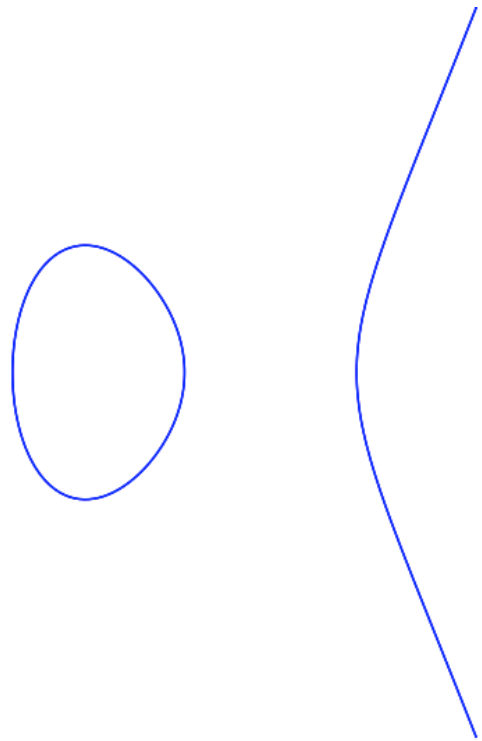
where $f(x) \in k[x]$ is of degree 3.



[1] No self-intersections or cusps.

Fundamentals: the group law on elliptic curves

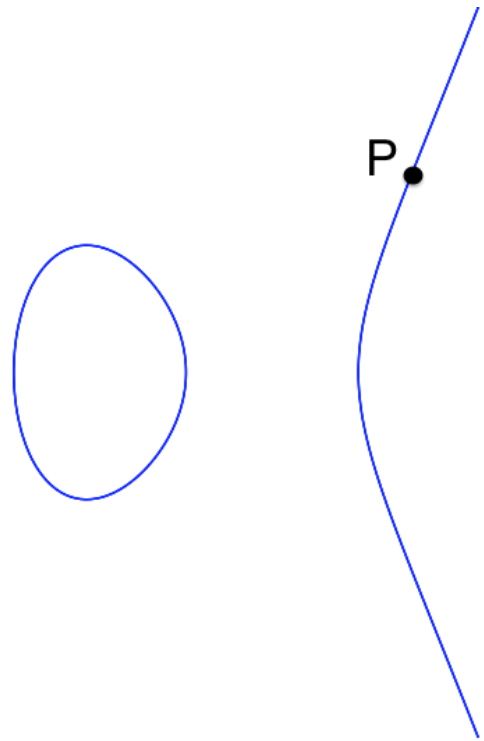
- For any field k, the k-rational points[2] of E form a group, written $E(k)$.



[2] solutions to the equation $y^2 = f(x)$, or the 'point at infinity' P_∞

Fundamentals: the group law on elliptic curves

- For any field k, the k-rational points[2] of E form a group, written $E(k)$.

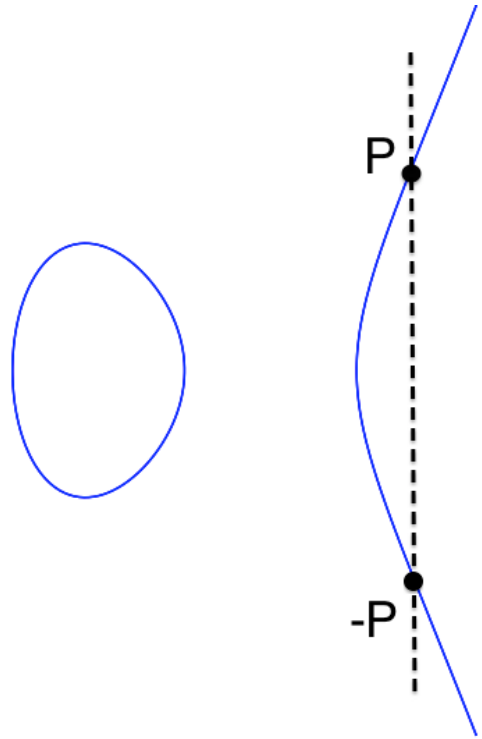


The group identity P_∞, the 'point at infinity', lies on every vertical line.

[2] solutions to the equation $y^2 = f(x)$, or the 'point at infinity' P_∞

Fundamentals: the group law on elliptic curves

- For any field k, the k-rational points[2] of E form a group, written $E(k)$.

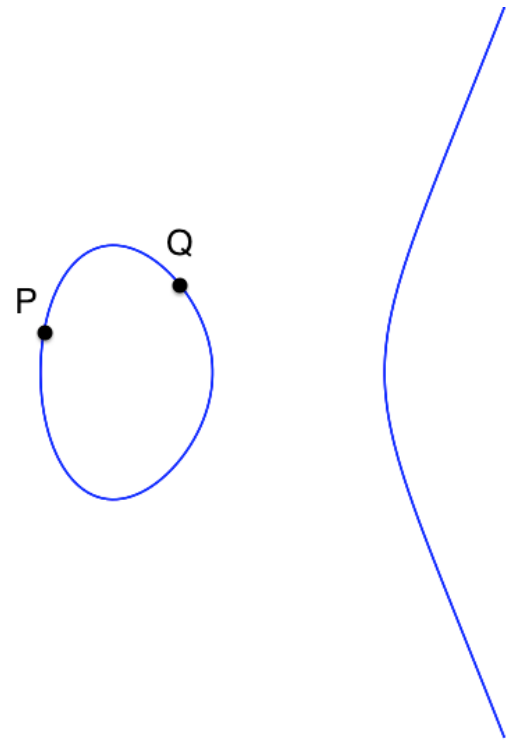


The group identity P_∞, the 'point at infinity', lies on every vertical line.

[2] solutions to the equation $y^2 = f(x)$, or the 'point at infinity' P_∞

Fundamentals: the group law on elliptic curves

- For any field k, the k-rational points[2] of E form a group, written $E(k)$.

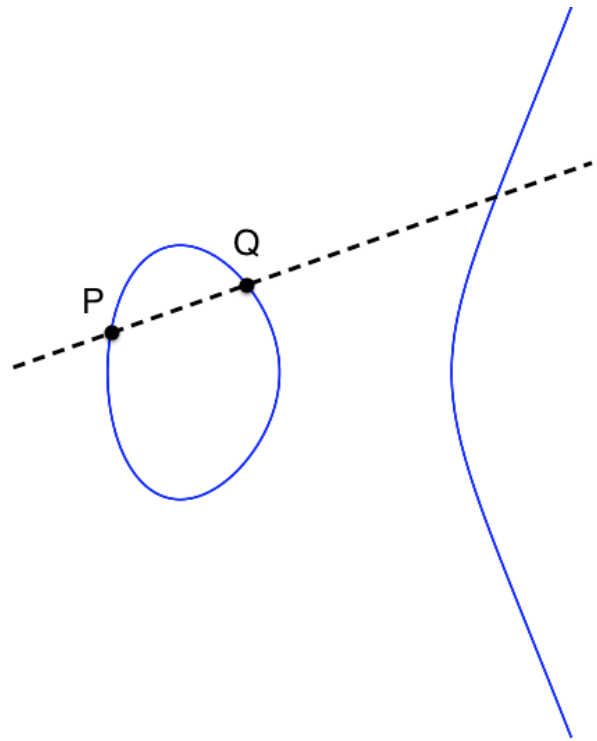


The group identity P_∞, the 'point at infinity', lies on every vertical line.

[2] solutions to the equation $y^2 = f(x)$, or the 'point at infinity' P_∞

Fundamentals: the group law on elliptic curves

- For any field k, the k-rational points[2] of E form a group, written $E(k)$.

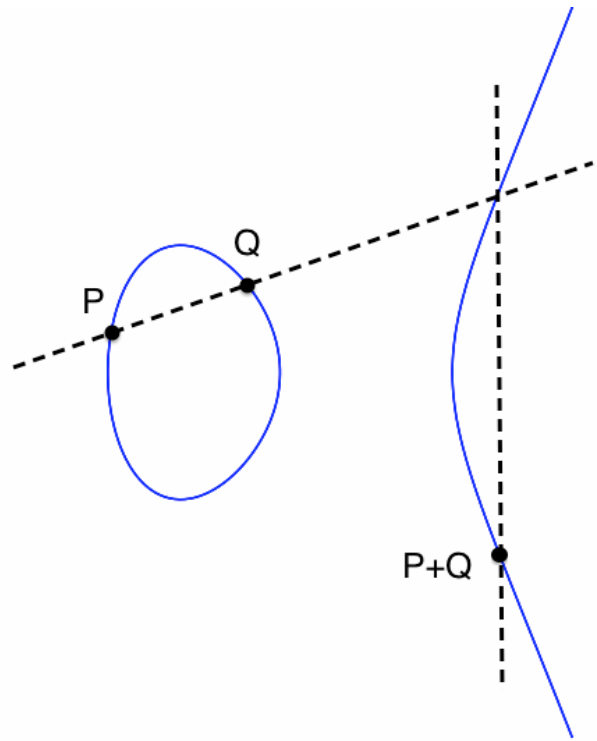


The group identity P_∞, the 'point at infinity', lies on every vertical line.

[2] solutions to the equation $y^2 = f(x)$, or the 'point at infinity' P_∞

Fundamentals: the group law on elliptic curves

- For any field k, the k-rational points[2] of E form a group, written $E(k)$.



The group identity P_∞, the 'point at infinity', lies on every vertical line.

[2] solutions to the equation $y^2 = f(x)$, or the 'point at infinity' P_∞

Fundamentals: Elliptic curves

Especially important for isogeny-based crypto:

Definition

Let $E/\mathbb{F}_q$ be an elliptic curve, with $q = p^n$.
E is supersingular if $p \mid (q + 1 - \#E(\mathbb{F}_q))$.
Otherwise E is ordinary.

Fundamentals: Elliptic curves

Especially important for isogeny-based crypto:

Definition

Let $E/\mathbb{F}_q$ be an elliptic curve, with $q = p^n$.
E is supersingular if $p \mid (q + 1 - \#E(\mathbb{F}_q))$.
Otherwise E is ordinary.

Important special cases:

- When $E/\mathbb{F}_p$ supersingular and $\#E(\mathbb{F}_p) = p + 1$.
- When $E/\mathbb{F}_{p^2}$ supersingular and $\#E(\mathbb{F}_{p^2}) = (p + 1)^2$.

Fundamentals: Elliptic curves

Especially important for isogeny-based crypto:

Definition

Let $E/\mathbb{F}_q$ be an elliptic curve, with $q = p^n$.
E is supersingular if $p \mid (q + 1 - \#E(\mathbb{F}_q))$.
Otherwise E is ordinary.

Important special cases:

- When $E/\mathbb{F}_p$ supersingular and $\#E(\mathbb{F}_p) = p + 1$.
- When $E/\mathbb{F}_{p^2}$ supersingular and $\#E(\mathbb{F}_{p^2}) = (p + 1)^2$.

Example

Define $E/\mathbb{F}_5 : y^2 = x^3 + 1$. Then

$$E(\mathbb{F}_5) = \{(0, 1), (0, -1), (2, 3), (2, -3), (-1, 0), P_\infty\},$$

so $E/\mathbb{F}_5$ is supersingular.

Fundamentals: Isogenies of elliptic curves

Definition

An isogeny of elliptic curves over k is a non-zero morphism $E \to E'$ with finite kernel. It is given by rational maps.

Fundamentals: Isogenies of elliptic curves

Definition

An isogeny of elliptic curves over k is a non-zero morphism $E \to E'$ with finite kernel. It is given by rational maps.

Example

Define $E_{51}/\mathbb{F}_{419} : y^2 = x^3 + 51x^2 + x$

$$\begin{array}{rccc} [2]: & E_{51} & \to & E_{51} \\ & (x,y) & \mapsto & 2\cdot(x,y) := (x,y)+(x,y) \end{array}$$

Fundamentals: Isogenies of elliptic curves

Definition

An isogeny of elliptic curves over k is a non-zero morphism $E \to E'$ with finite kernel. It is given by rational maps.

Example

Define $E_{51}/\mathbb{F}_{419} : y^2 = x^3 + 51x^2 + x$

$$\begin{array}{rccc} [2] : & E_{51} & \to & E_{51} \\ & (x,y) & \mapsto & 2 \cdot (x,y) := (x,y) + (x,y) \end{array}$$

- Composing-an-element-with-itself is a morphism for any abelian variety. Also: it induces a morphism of groups.

Fundamentals: Isogenies of elliptic curves

Definition

An isogeny of elliptic curves over k is a non-zero morphism $E \to E'$ with finite kernel. It is given by rational maps.

Example

Define $E_{51}/\mathbb{F}_{419} : y^2 = x^3 + 51x^2 + x$

$$\begin{array}{rccc} [2]: & E_{51} & \to & E_{51} \\ & (x,y) & \mapsto & 2\cdot(x,y) := (x,y)+(x,y) \end{array}$$

- Composing-an-element-with-itself is a morphism for any abelian variety. Also: it induces a morphism of groups.
- Explicit calculations show that:

$$\begin{array}{rccc} [2]: & E_{51} & \to & E_{51} \\ & (x,y) & \mapsto & \left(\frac{\frac{1}{2}x^4-18x^3-163x^2-18x+\frac{1}{2}}{8x(x^2+9x+1)}, \frac{y(x^6+18x^5+5x^4-5x^2-18x-1)}{(8x(x^2+9x+1))^2}\right). \end{array}$$

Fundamentals: Isogenies of elliptic curves

Definition

An isogeny of elliptic curves over k is a non-zero morphism $E \to E'$ with finite kernel. It is given by rational maps.

Fundamentals: Isogenies of elliptic curves

Definition

An isogeny of elliptic curves over k is a non-zero morphism $E \to E'$ with finite kernel. It is given by rational maps.

Example

Define $E_A/\mathbb{F}_{419} : y^2 = x^3 + Ax^2 + x$

Fundamentals: Isogenies of elliptic curves

Definition

An isogeny of elliptic curves over k is a non-zero morphism $E \to E'$ with finite kernel. It is given by rational maps.

Example

Define $E_A/\mathbb{F}_{419} : y^2 = x^3 + Ax^2 + x$

- A less obvious isogeny:

$$\begin{array}{rccc} f: & E_{51} & \to & E_9 \\ & (x,y) & \mapsto & \left(\frac{x^3-183x^2+73x+30}{(x+118)^2}, y\frac{x^3-65x^2-104x+174}{(x+118)^3}\right). \end{array}$$

Fundamentals: Isogenies of elliptic curves

Definition

An isogeny of elliptic curves over k is a non-zero morphism $E \to E'$ with finite kernel. It is given by rational maps.

Example

Define $E_A/\mathbb{F}_{419} : y^2 = x^3 + Ax^2 + x$

- A less obvious isogeny:

$$\begin{array}{rccc} f: & E_{51} & \to & E_9 \\ & (x,y) & \mapsto & \left(\frac{x^3-183x^2+73x+30}{(x+118)^2}, y\frac{x^3-65x^2-104x+174}{(x+118)^3}\right). \end{array}$$

- $\ker(f) = \{(-118, 51), (-118, -51), P_\infty\}$

Fundamentals: Isogenies of elliptic curves

Definition

Let $E, E'/\mathbb{F}_q$ be elliptic curves and let $\ell \in \mathbb{Z}_{>0}$ be coprime to q.
An ℓ-isogeny $f : E \to E'$ is an isogeny with $\#\ker(f) = \ell$.

Fundamentals: Isogenies of elliptic curves

Definition

Let $E, E'/\mathbb{F}_q$ be elliptic curves and let $\ell \in \mathbb{Z}_{>0}$ be coprime to q.
An ℓ-isogeny $f : E \to E'$ is an isogeny with $\#\ker(f) = \ell$.

- Our example $f : E_{51} \to E_9$ over $\mathbb{F}_{419}$ was a 3-isogeny.

Fundamentals: Isogenies of elliptic curves

Definition

Let $E, E'/\mathbb{F}_q$ be elliptic curves and let $\ell \in \mathbb{Z}_{>0}$ be coprime to q.
An ℓ-isogeny $f : E \to E'$ is an isogeny with $\#\ker(f) = \ell$.

- Our example $f : E_{51} \to E_9$ over $\mathbb{F}_{419}$ was a 3-isogeny.
- Fact: an isogeny is uniquely determined by its kernel (up to isomorphism).

Fundamentals: Isogenies of elliptic curves

Definition

Let $E, E'/\mathbb{F}_q$ be elliptic curves and let $\ell \in \mathbb{Z}_{>0}$ be coprime to q.
An ℓ-isogeny $f : E \to E'$ is an isogeny with $\#\ker(f) = \ell$.

- Our example $f : E_{51} \to E_9$ over $\mathbb{F}_{419}$ was a 3-isogeny.
- Fact: an isogeny is uniquely determined by its kernel (up to isomorphism).
- Write $\varphi_G : E \to E/G$ for the isogeny from E with kernel G.

Fundamentals: Isogenies of elliptic curves

Definition

Let $E, E'/\mathbb{F}_q$ be elliptic curves and let $\ell \in \mathbb{Z}_{>0}$ be coprime to q.
An ℓ-isogeny $f : E \to E'$ is an isogeny with $\#\ker(f) = \ell$.

- Our example $f : E_{51} \to E_9$ over $\mathbb{F}_{419}$ was a 3-isogeny.
- Fact: an isogeny is uniquely determined by its kernel (up to isomorphism).
- Write $\varphi_G : E \to E/G$ for the isogeny from E with kernel G.
- Vélu's formulas compute the ℓ-isogeny from its kernel in time $\Theta(\ell)$.

Fundamentals: Isogenies of elliptic curves

Of special interest in crypto:

- We call an isogeny cyclic if its kernel is cyclic.

Fundamentals: Isogenies of elliptic curves

Of special interest in crypto:

- We call an isogeny cyclic if its kernel is cyclic.
- The kernel of a cyclic ℓ-isogeny is generated by an ℓ-torsion point (in particular: a point of order ℓ).

Fundamentals: Isogenies of elliptic curves

Of special interest in crypto:

- We call an isogeny cyclic if its kernel is cyclic.
- The kernel of a cyclic ℓ-isogeny is generated by an ℓ-torsion point (in particular: a point of order ℓ).
- An ℓ-torsion point is a point $P \in E(k)$ such that

$$[\ell]P = \underbrace{P + \cdots + P}_{\ell \text{ times}} = P_\infty.$$

Fundamentals: Isogenies of elliptic curves

Of special interest in crypto:

- We call an isogeny cyclic if its kernel is cyclic.
- The kernel of a cyclic ℓ-isogeny is generated by an ℓ-torsion point (in particular: a point of order ℓ).
- An ℓ-torsion point is a point $P \in E(k)$ such that

$$[\ell]P = \underbrace{P + \cdots + P}_{\ell \text{ times}} = P_\infty.$$

Our example $f : E_{51} \to E_9$ was a cyclic 3-isogeny:

$$\begin{aligned}\ker(f) &= \{(-118, 51), (-118, -51), P_\infty\} \\ &= \{(-118, 51), [2](-118, 51), [3](-118, 51)\}.\end{aligned}$$

Fundamentals: Isogenies of elliptic curves

Of special interest in crypto:

- We call an isogeny cyclic if its kernel is cyclic.
- The kernel of a cyclic ℓ-isogeny is generated by an ℓ-torsion point (in particular: a point of order ℓ).
- An ℓ-torsion point is a point $P \in E(k)$ such that

$$[\ell]P = \underbrace{P + \cdots + P}_{\ell \text{ times}} = P_\infty.$$

Our example $f : E_{51} \to E_9$ was a cyclic 3-isogeny:

$$\begin{aligned}\ker(f) &= \{(-118, 51), (-118, -51), P_\infty\} \\ &= \{(-118, 51), [2](-118, 51), [3](-118, 51)\}.\end{aligned}$$

$\rightsquigarrow$ we could also write

$$f = \varphi_{\langle(-118,51)\rangle} : E_{51} \to E_{51}/\langle(-118, 51)\rangle.$$

Decomposing smooth isogenies

- We will use isogenies with 'crypto-sized' (*big*) kernels.
  Vélu's formulas take $\Theta(\#G)$ to compute $\varphi_G \colon E \to E/G$.

Decomposing smooth isogenies

- We will use isogenies with 'crypto-sized' (*big*) kernels.
  Vélu's formulas take $\Theta(\#G)$ to compute $\varphi_G \colon E \to E/G$.

!! Make sure G has smooth order.

Decomposing smooth isogenies

- We will use isogenies with 'crypto-sized' (*big*) kernels.
  Vélu's formulas take $\Theta(\#G)$ to compute $\varphi_G \colon E \to E/G$.

!! Make sure G has smooth order.

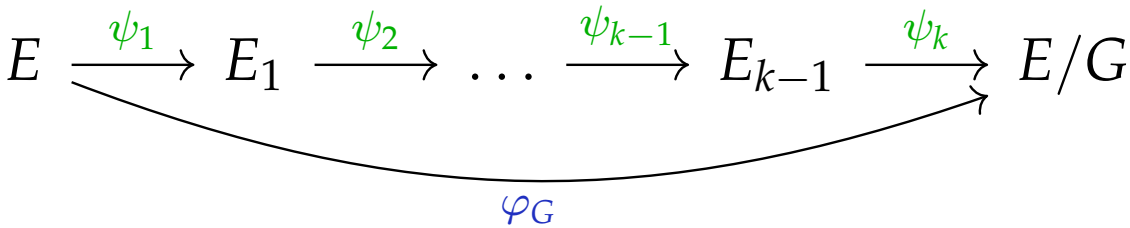
!! Evaluate φ_G as a chain of small-degree isogenies:

Decomposing smooth isogenies

- We will use isogenies with 'crypto-sized' (*big*) kernels.
  Vélu's formulas take $\Theta(\#G)$ to compute $\varphi_G \colon E \to E/G$.

!! Make sure G has smooth order.

!! Evaluate φ_G as a chain of small-degree isogenies:
  For $G \cong \mathbb{Z}/\ell^k$, we can decompose φ_G into ℓ-isogenies $\psi_1, \ldots, \psi_k$:

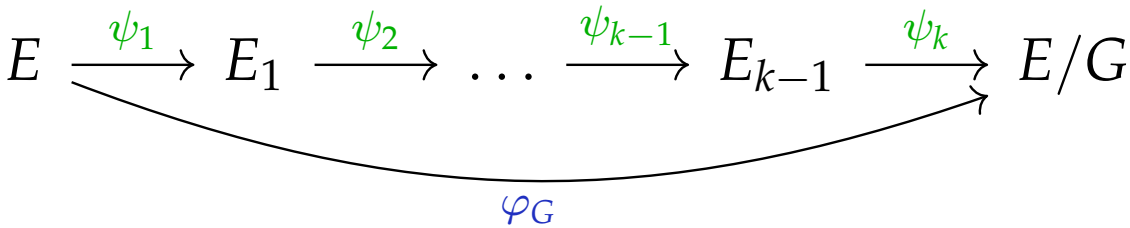


Decomposing smooth isogenies

- We will use isogenies with 'crypto-sized' (*big*) kernels.
  Vélu's formulas take $\Theta(\#G)$ to compute $\varphi_G \colon E \to E/G$.

!! Make sure G has smooth order.

!! Evaluate φ_G as a chain of small-degree isogenies:
  For $G \cong \mathbb{Z}/\ell^k$, we can decompose φ_G into ℓ-isogenies $\psi_1, \ldots, \psi_k$:



$\rightsquigarrow$ Complexity: $O(k^2 \cdot \ell)$. *Exponentially smaller* than $\#G = \ell^k$!
'Optimal strategy' improves this to $O(k \log k \cdot \ell)$.

Elliptic curves and isogenies

Definition

Let $E/\mathbb{F}_q$ be an elliptic curve and let $\ell \in \mathbb{Z}_{>0}$. Let $f : E \to E'$ be an ℓ-isogeny.

Elliptic curves and isogenies

Definition

Let $E/\mathbb{F}_q$ be an elliptic curve and let $\ell \in \mathbb{Z}_{>0}$. Let $f : E \to E'$ be an ℓ-isogeny.
Then there exists a unique (up to isomorphism) ℓ-isogeny

$$f^\vee : E' \to E$$

such that

$$f^\vee \circ f = [\ell].$$

Elliptic curves and isogenies

Definition

Let $E/\mathbb{F}_q$ be an elliptic curve and let $\ell \in \mathbb{Z}_{>0}$. Let $f : E \to E'$ be an ℓ-isogeny.
Then there exists a unique (up to isomorphism) ℓ-isogeny

$$f^\vee : E' \to E$$

such that

$$f^\vee \circ f = [\ell].$$

This is called the dual isogeny.

Elliptic curves and isogenies

Definition

Let $E/\mathbb{F}_q$ be an elliptic curve and let $\ell \in \mathbb{Z}_{>0}$. Let $f : E \to E'$ be an ℓ-isogeny.
Then there exists a unique (up to isomorphism) ℓ-isogeny

$$f^\vee : E' \to E$$

such that

$$f^\vee \circ f = [\ell].$$

This is called the dual isogeny.

(As before $[\ell]$ denotes the multiplication-by-ℓ map.)

Fundamentals: Isogeny graphs

Definition

Let q be a prime power and ℓ be a prime not dividing q. The isogeny graph $G_{\ell,n}$ over $\mathbb{F}_q$ has

Fundamentals: Isogeny graphs

Definition

Let q be a prime power and ℓ be a prime not dividing q. The isogeny graph $G_{\ell,n}$ over $\mathbb{F}_q$ has

- Nodes: elliptic curves defined over $\mathbb{F}_q$ with n points (up to $\mathbb{F}_q$-isomorphism).

Fundamentals: Isogeny graphs

Definition

Let q be a prime power and ℓ be a prime not dividing q. The isogeny graph $G_{\ell,n}$ over $\mathbb{F}_q$ has

- Nodes: elliptic curves defined over $\mathbb{F}_q$ with n points (up to $\mathbb{F}_q$-isomorphism).
- Edges: an edge $E - E'$ represents an ℓ-isogeny $E \to E'$ defined over $\mathbb{F}_q$ together with its dual isogeny. (up to post-composition with isomorphisms).

Isogeny graphs

Example

Replace eg. 

by

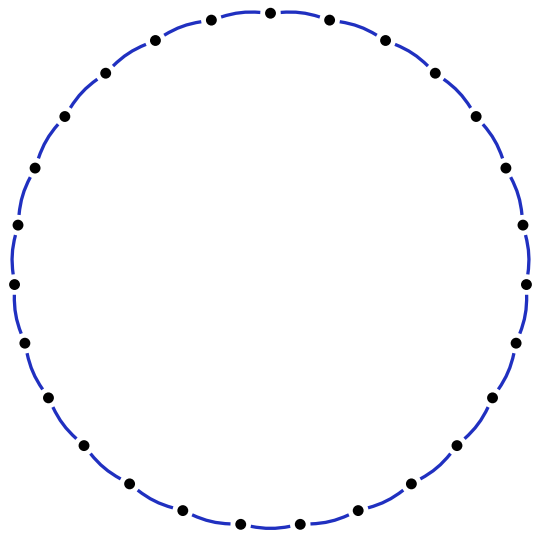
Isogeny graphs

Example

Replace eg. 

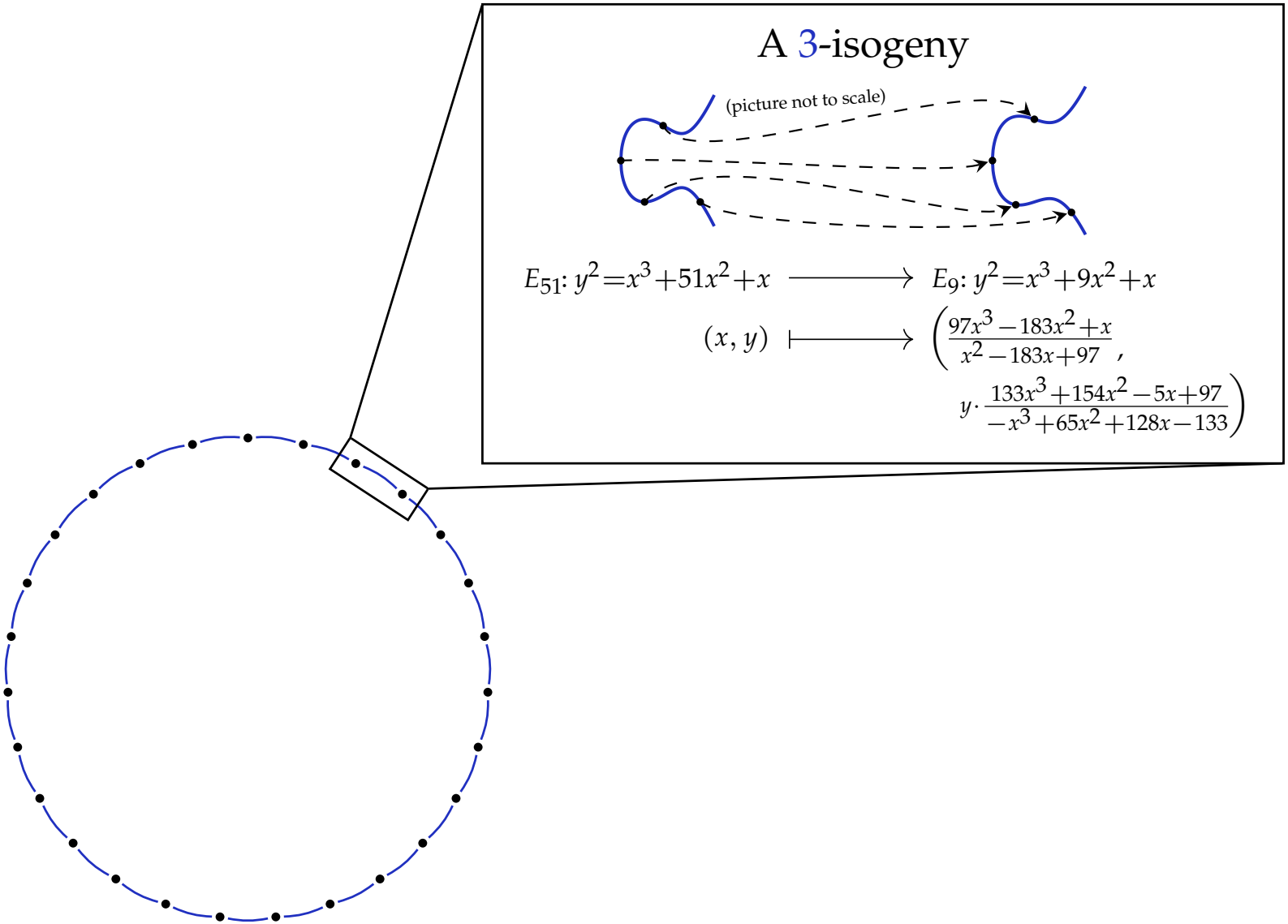
by

Then the graph $G_{3,420}$ over $\mathbb{F}_{419}$ looks like:



[NB: the nodes with $p + 1 = 420$ points are the supersingular nodes].

Isogeny graphs



Fragen?

Questions?

Domande?

Dumondas?

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. More later.

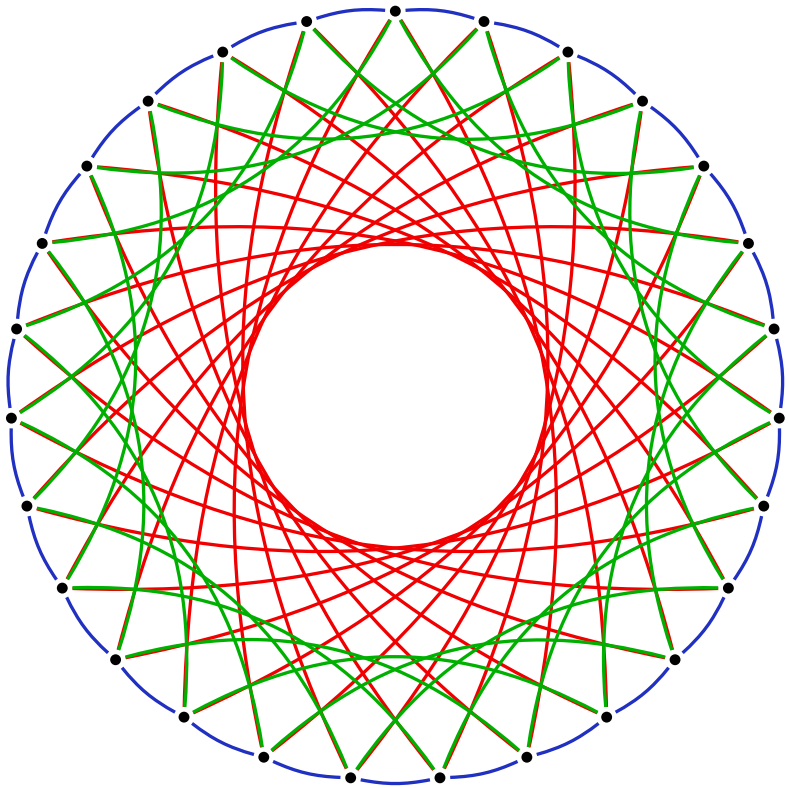
Big picture 🔎🔎

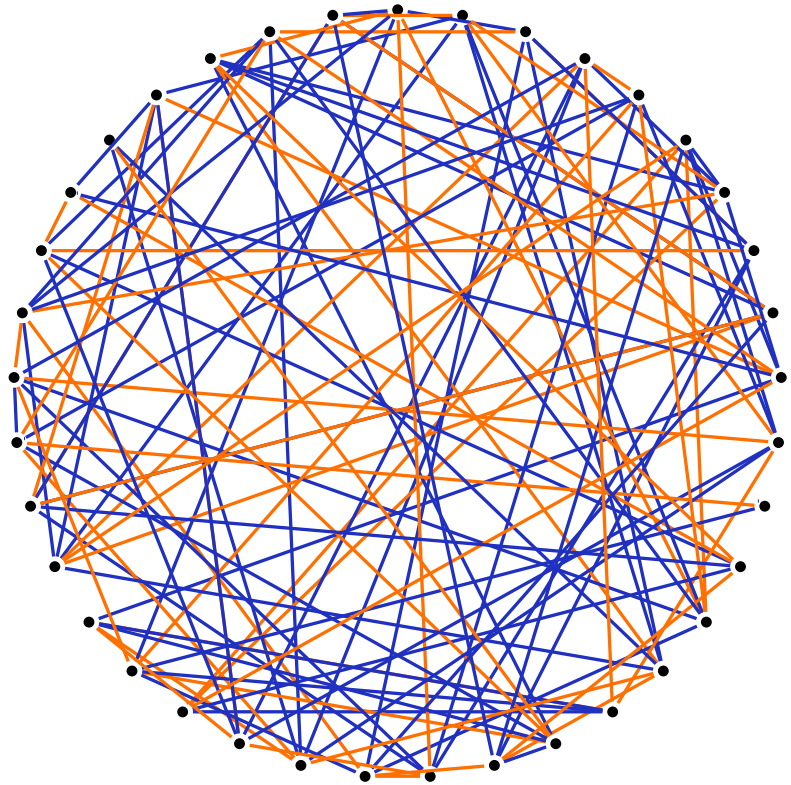
- Isogenies are a source of exponentially-sized graphs.
- We can walk efficiently on these graphs.
- Fast mixing: short paths to (almost) all nodes.
- No efficient* algorithms to recover paths from endpoints.
  (*Both* classical and quantum!)
- Enough structure to navigate the graph meaningfully.
  That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

It is easy to construct graphs that satisfy *almost* all of these —
not enough for crypto!

The beauty and the beast

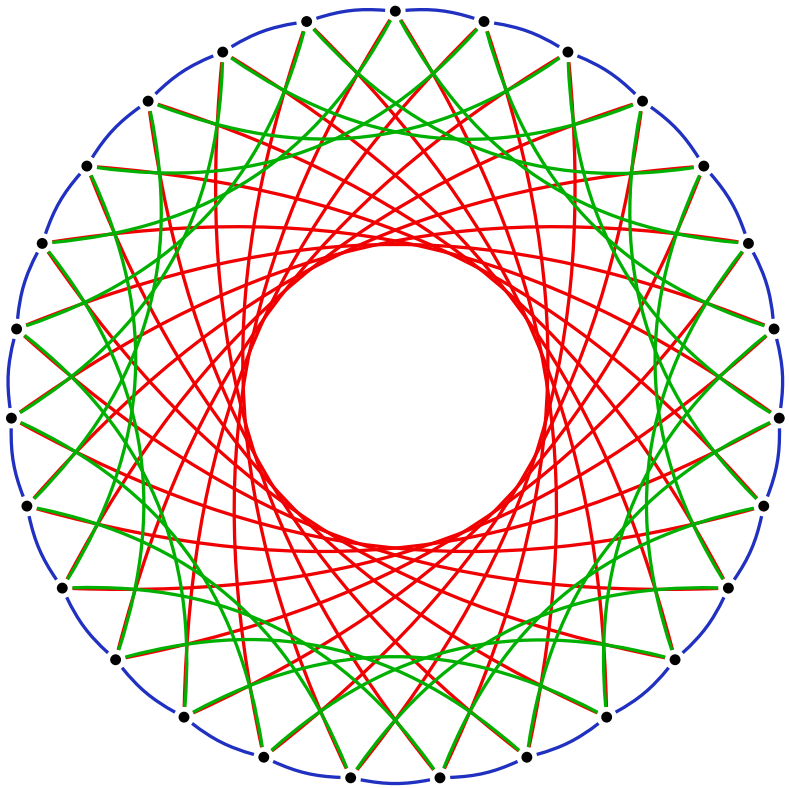
Components of well-chosen isogeny graphs look like this:

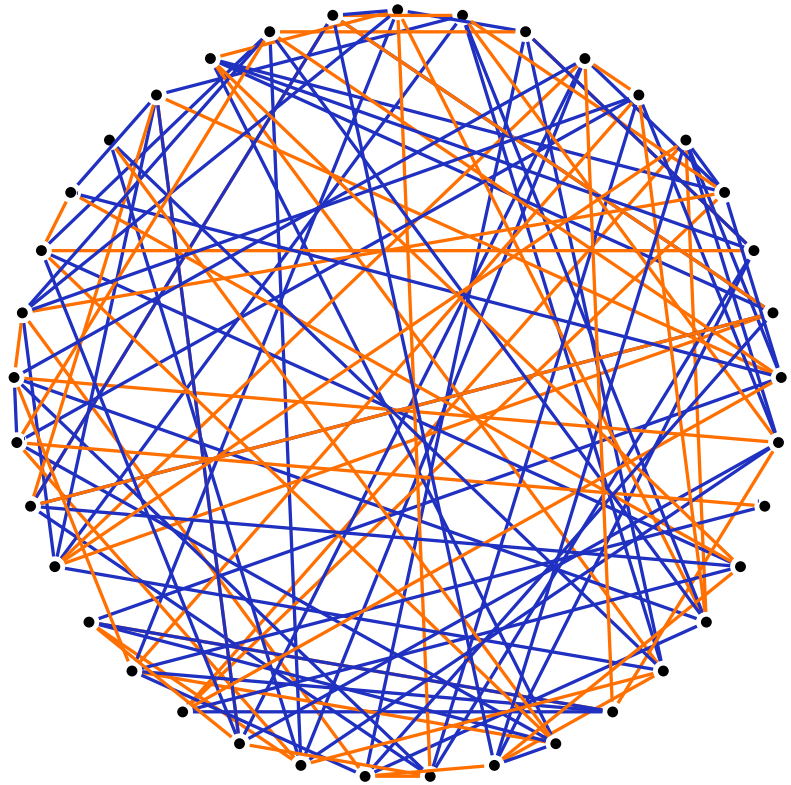




The beauty and the beast

Components of well-chosen isogeny graphs look like this:

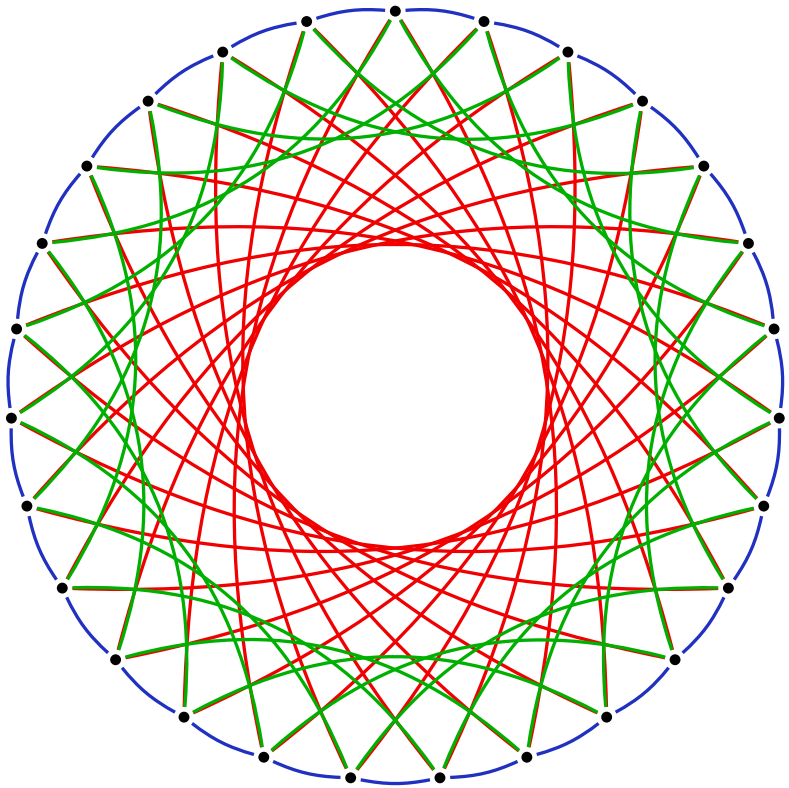


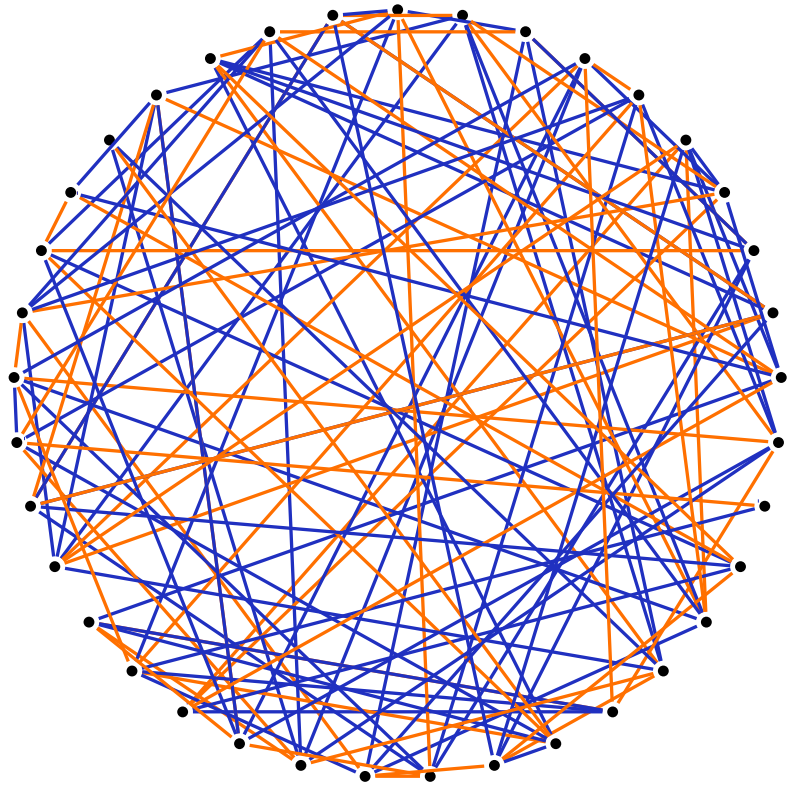


Which of these is good for crypto?

The beauty and the beast

Components of well-chosen isogeny graphs look like this:

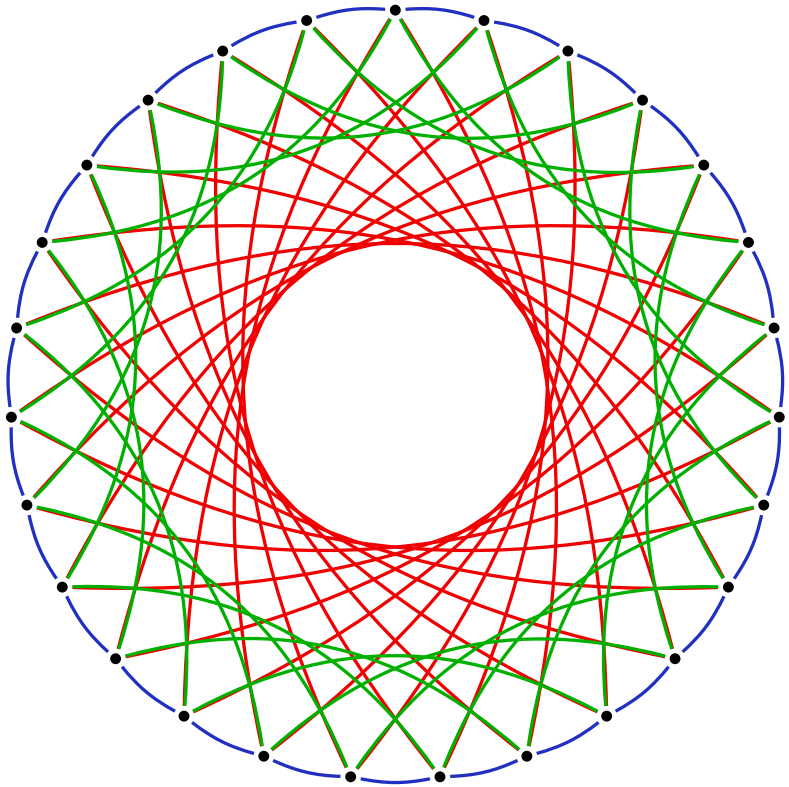




Which of these is good for crypto? **Both.**

The beauty and the beast

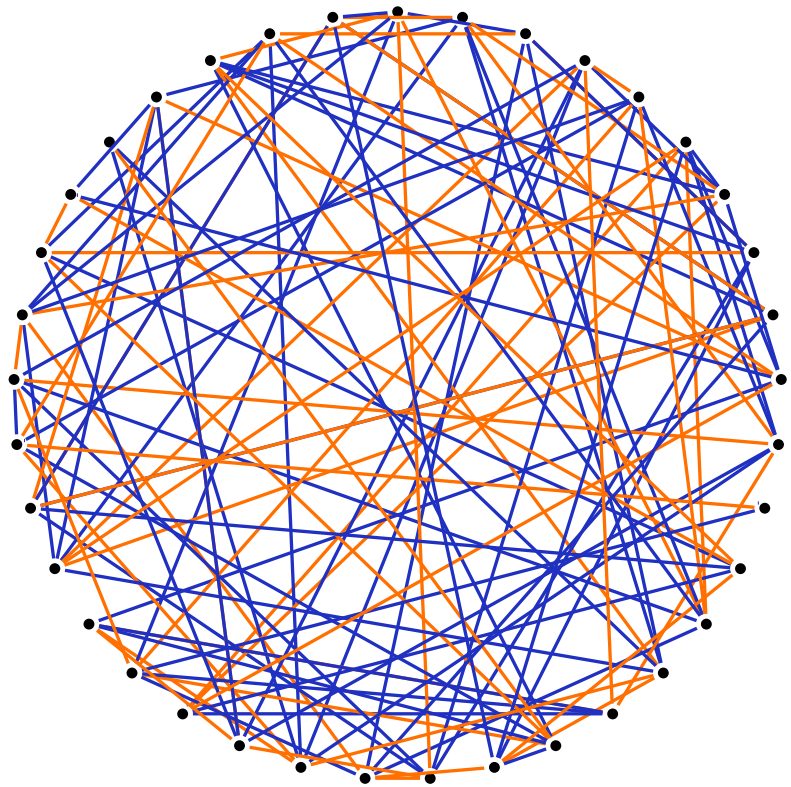
At this time, there are two distinct families of systems:



$q = p$

CSIDH ['siːˌsaɪd]

`https://csidh.isogeny.org`



$q = p^2$

SIDH

`https://sike.org`


CSIDH ['si:ˌsaɪd]
(Castryck, Lange, Martindale, Panny, Renes; 2018)

CSIDH in one slide

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

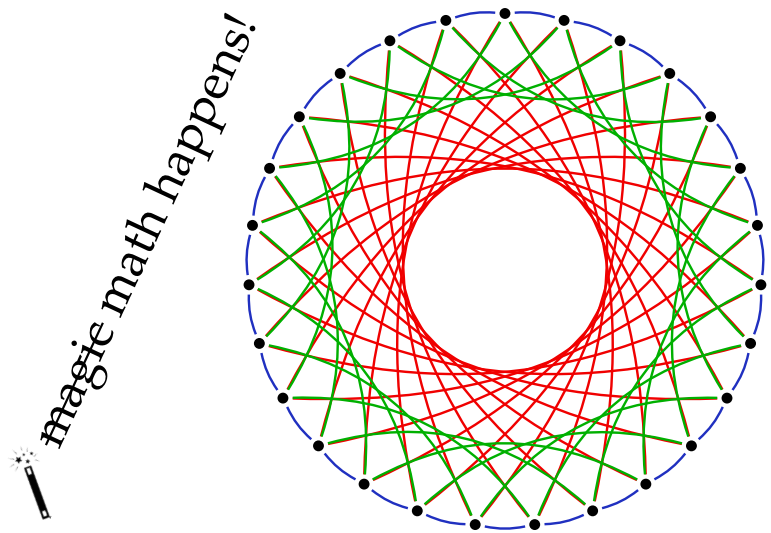
- Choose some small odd primes $\ell_1, \ldots, \ell_n$.
- Make sure $p = 4 \cdot \ell_1 \cdots \ell_n - 1$ is prime.
- Let $X = \{y^2 = x^3 + Ax^2 + x$ over $\mathbb{F}_p$ with $p+1$ points$\}$.

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 $X = \{y^2 = x^3 + Ax^2 + x$ over $\mathbb{F}_p$ with $p+1$ points$\}$.
- Look at the ℓ_i-isogenies defined over $\mathbb{F}_p$ within X.

CSIDH in one slide

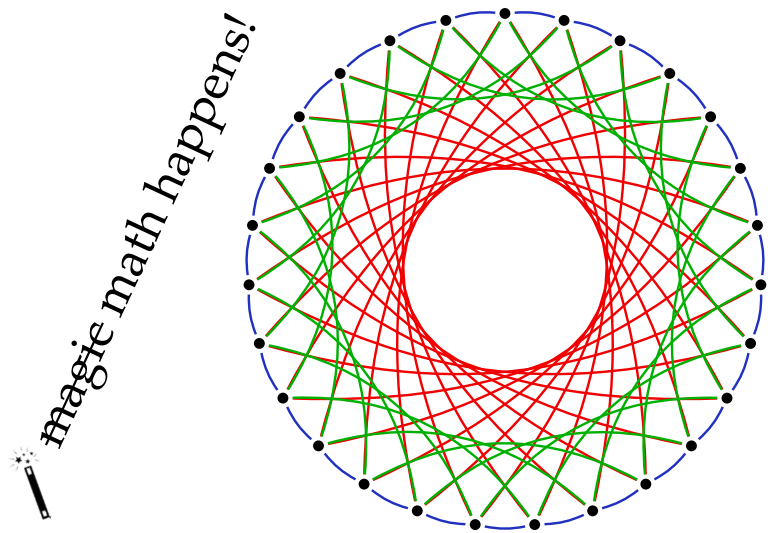
- Choose some small odd primes $\ell_1, \ldots, \ell_n$.
- Make sure $p = 4 \cdot \ell_1 \cdots \ell_n - 1$ is prime.
- Let $X = \{y^2 = x^3 + Ax^2 + x$ over $\mathbb{F}_p$ with $p+1$ points$\}$.
- Look at the ℓ_i-isogenies defined over $\mathbb{F}_p$ within X.



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

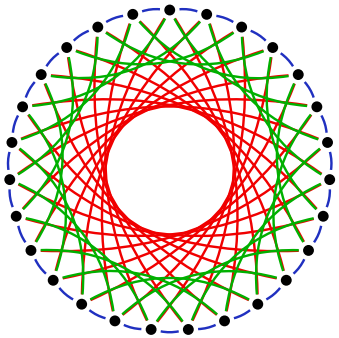
CSIDH in one slide

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

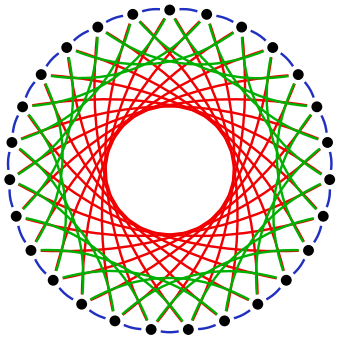


$p = 419$
$\ell_1 = 3$
$\ell_2 = 5$
$\ell_3 = 7$

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



Elliptic-curve people may know this graph:
It is the union of depth-0 isogeny volcanoes.



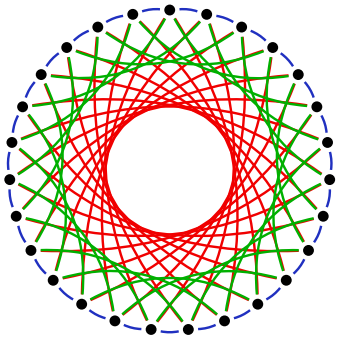
Elliptic-curve people may know this graph:
It is the union of depth-0 isogeny volcanoes.

Typical formulation:

Theorem. Let $\mathcal{O}$ be an imaginary quadratic order and k a field. If the set

$$\mathcal{E}\ell\ell_{\mathcal{O}}(k) = \{\, j(E) \mid E/k \text{ ordinary}, \ \mathrm{End}(E) \cong \mathcal{O} \,\}$$

is non-empty, then the ideal-class group $\mathrm{cl}(\mathcal{O})$ acts freely and transitively on $\mathcal{E}\ell\ell_{\mathcal{O}}(k)$.



Elliptic-curve people may know this graph:
It is the union of depth-0 isogeny volcanoes.

Typical formulation:

Theorem. Let $\mathcal{O}$ be an imaginary quadratic order and k a field. If the set

$$\mathcal{E}\ell\ell_{\mathcal{O}}(k) = \{\, j(E) \mid E/k \text{ ordinary}, \ \mathrm{End}(E) \cong \mathcal{O} \,\}$$

is non-empty, then the ideal-class group $\mathrm{cl}(\mathcal{O})$ acts freely and transitively on $\mathcal{E}\ell\ell_{\mathcal{O}}(k)$.

Less well-known:

This *also* works for supersingular elliptic curves if one restricts to $k = \mathbb{F}_p$, $\cong_{\mathbb{F}_p}$, and $\mathrm{End}_{\mathbb{F}_p}$.

Walking in the CSIDH graph

Supersingular curves have computational benefits:
By taking special p, it is easy to control the group structure!
(Not easy for ordinary curves in 'interesting' cases.)

Walking in the CSIDH graph

Supersingular curves have computational benefits:
By taking special p, it is easy to control the group structure!
(Not easy for ordinary curves in 'interesting' cases.)

Taking a 'positive' step on the ℓ_i-subgraph:

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

Walking in the CSIDH graph

Supersingular curves have computational benefits:
By taking special p, it is easy to control the group structure!
(Not easy for ordinary curves in 'interesting' cases.)

Taking a 'positive' step on the ℓ_i-subgraph:

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

Taking a 'negative' step on the ℓ_i-subgraph:

1. Find a point $(x, y) \in E$ of order ℓ_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

Supersingular curves have computational benefits:
By taking special p, it is easy to control the group structure!
(Not easy for ordinary curves in 'interesting' cases.)

Taking a 'positive' step on the ℓ_i-subgraph:

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

Taking a 'negative' step on the ℓ_i-subgraph:

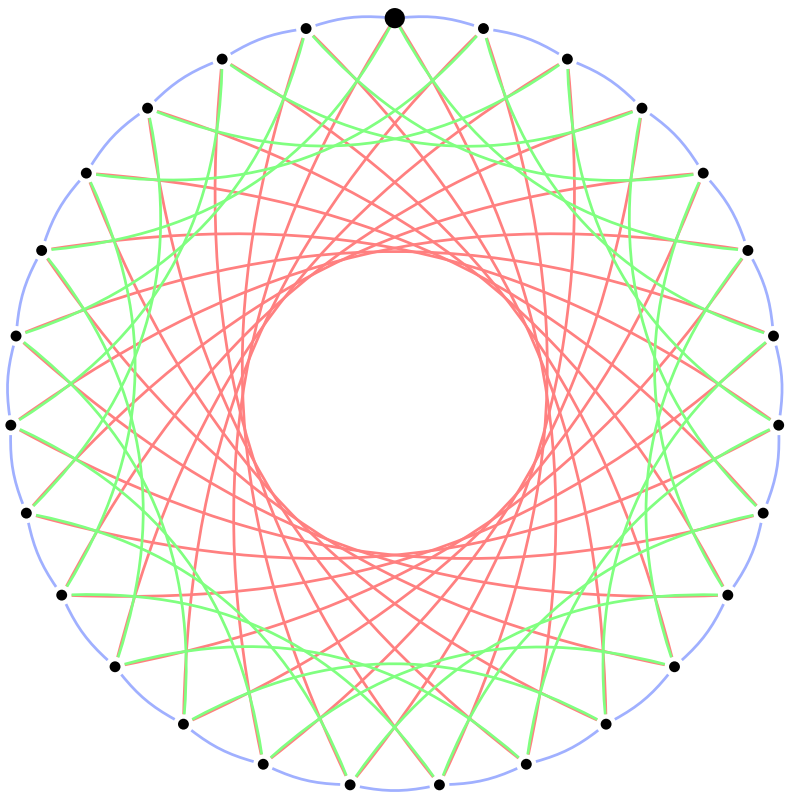
1. Find a point $(x, y) \in E$ of order ℓ_i with $x \in \mathbb{F}_p$ but $y \notin \mathbb{F}_p$.
2. Compute the isogeny with kernel $\langle (x, y) \rangle$.

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

CSIDH key exchange

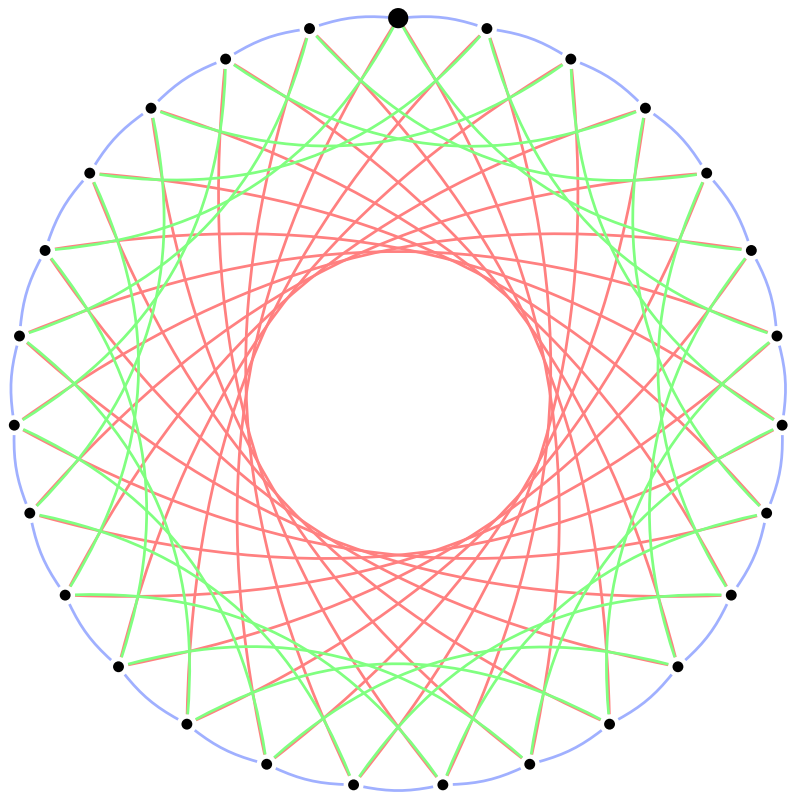
Alice

$[+, +, -, -]$



Bob

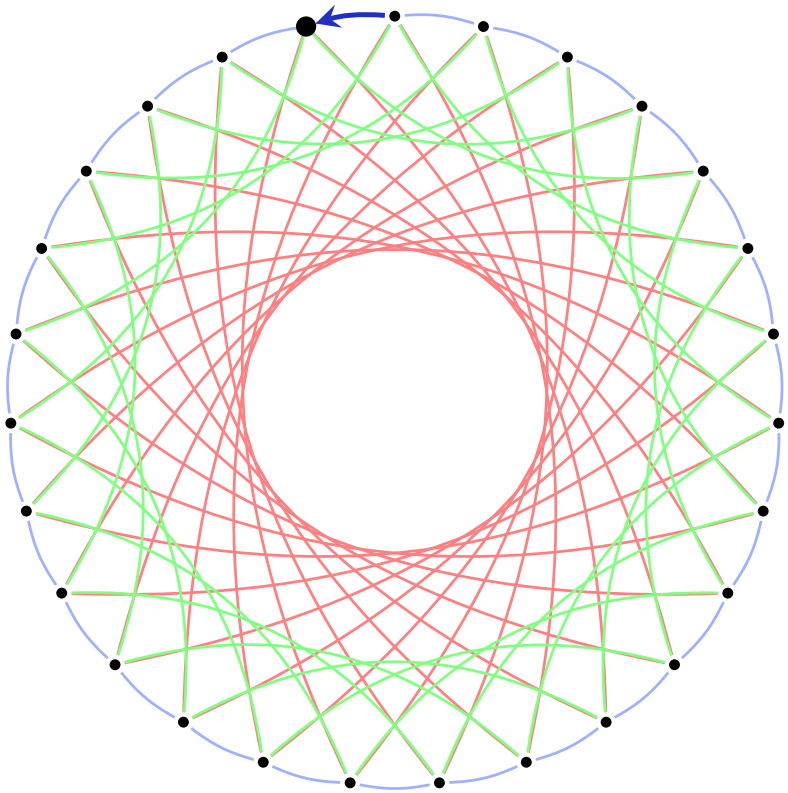
$[-, +, -, -]$



CSIDH key exchange

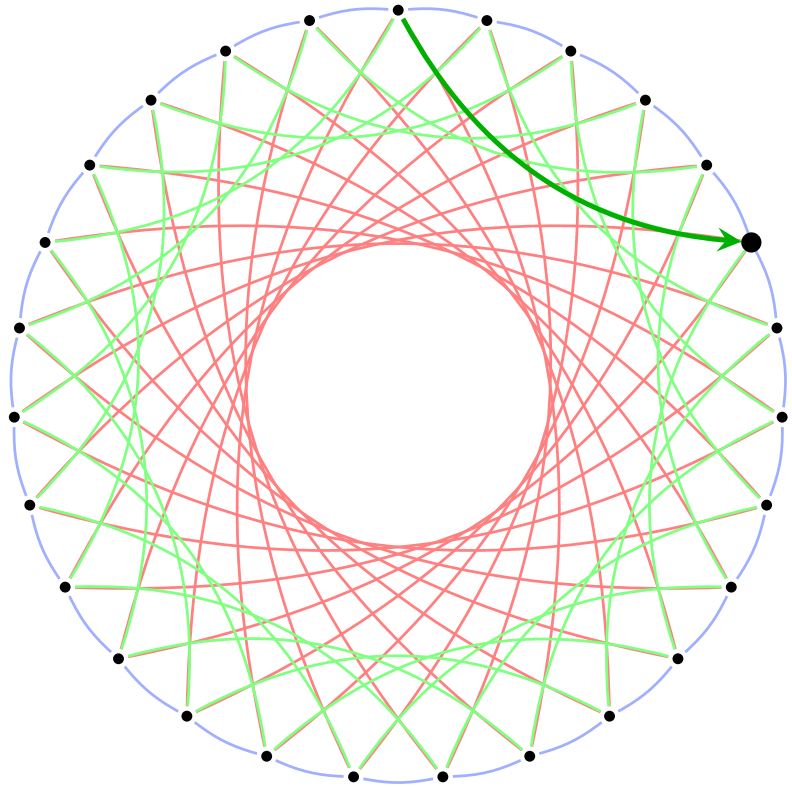
Alice

$[+, +, -, -]$



Bob

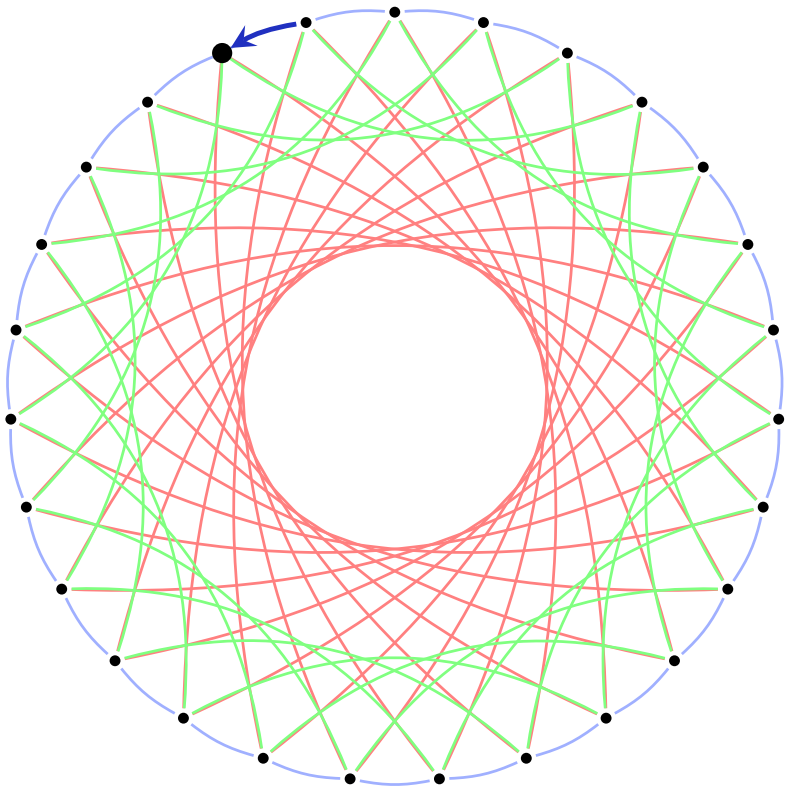
$[-, +, -, -]$



CSIDH key exchange

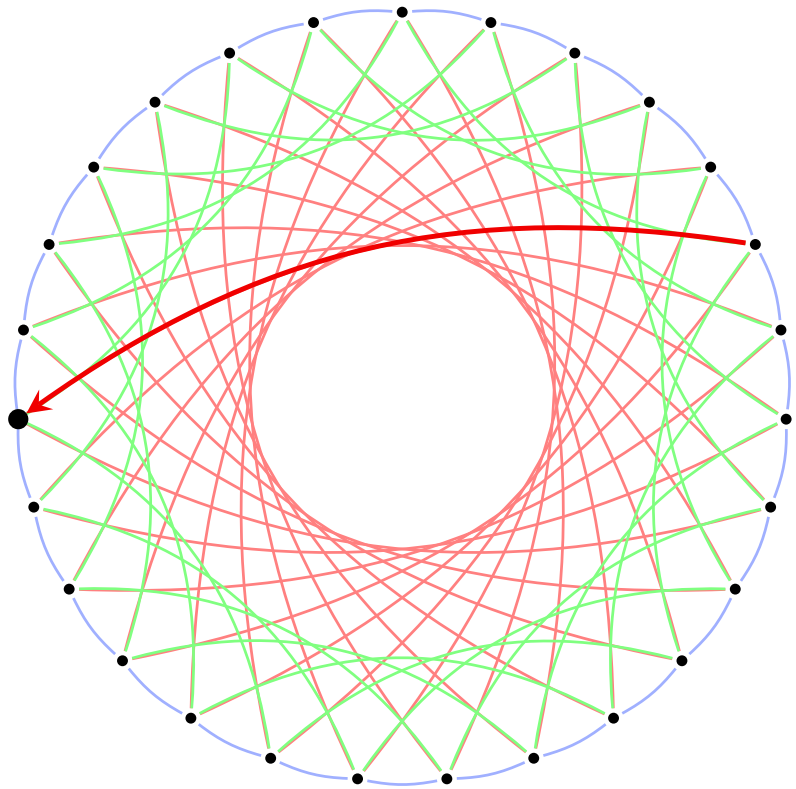
Alice

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



Bob

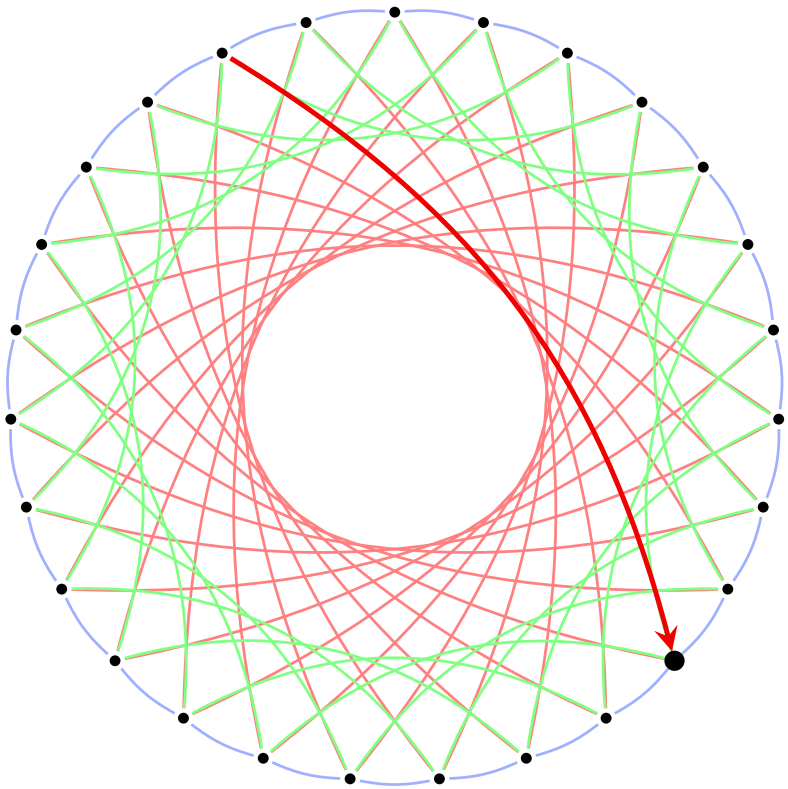
$[-, \underset{\uparrow}{+}, -, -]$



CSIDH key exchange

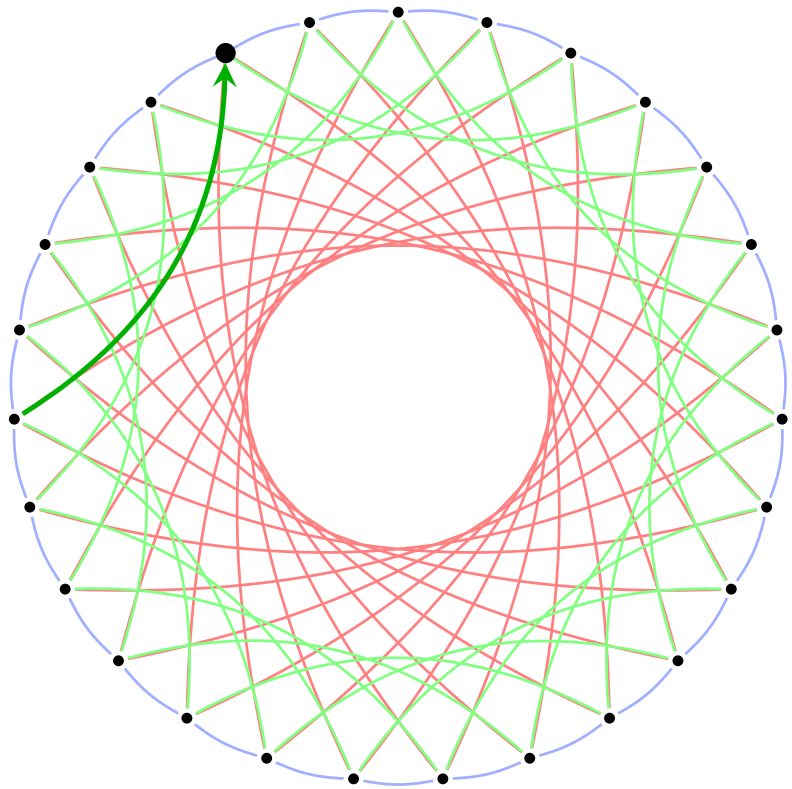
Alice

$[+, +, -, -]$



Bob

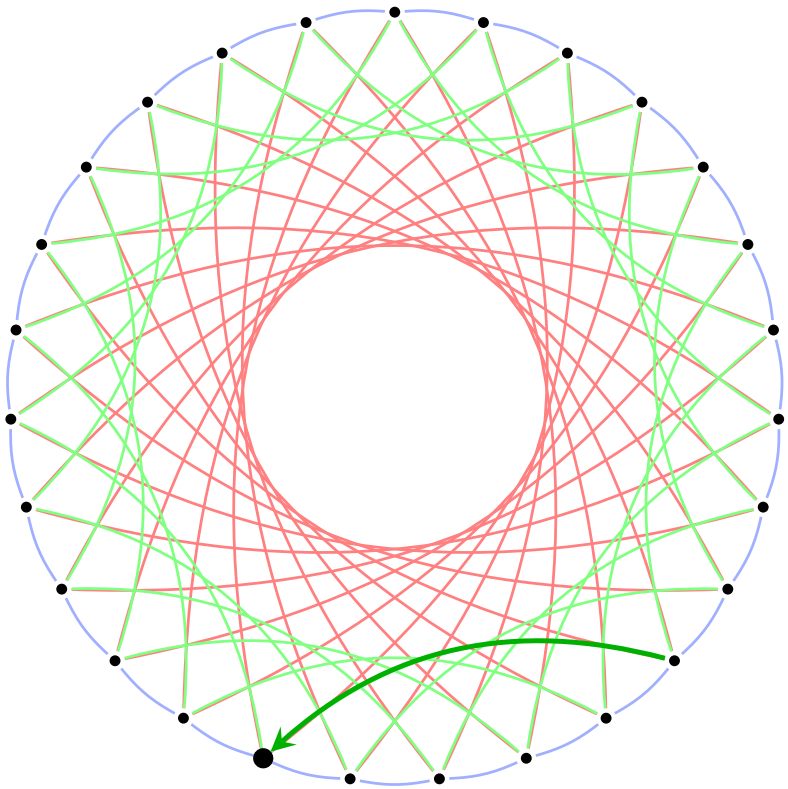
$[-, +, -, -]$



CSIDH key exchange

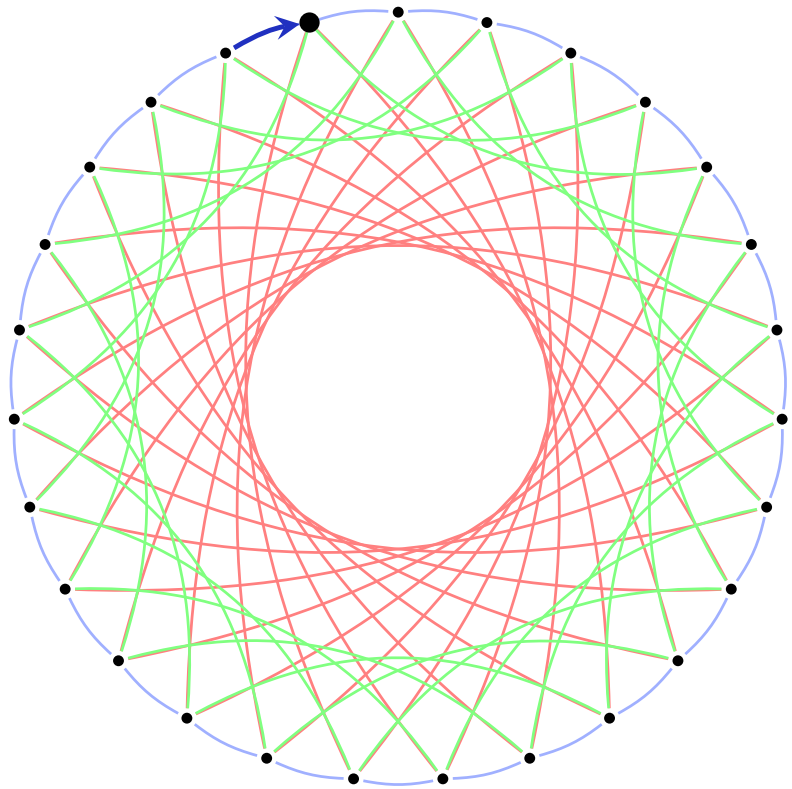
Alice

$[+, +, -, -]$



Bob

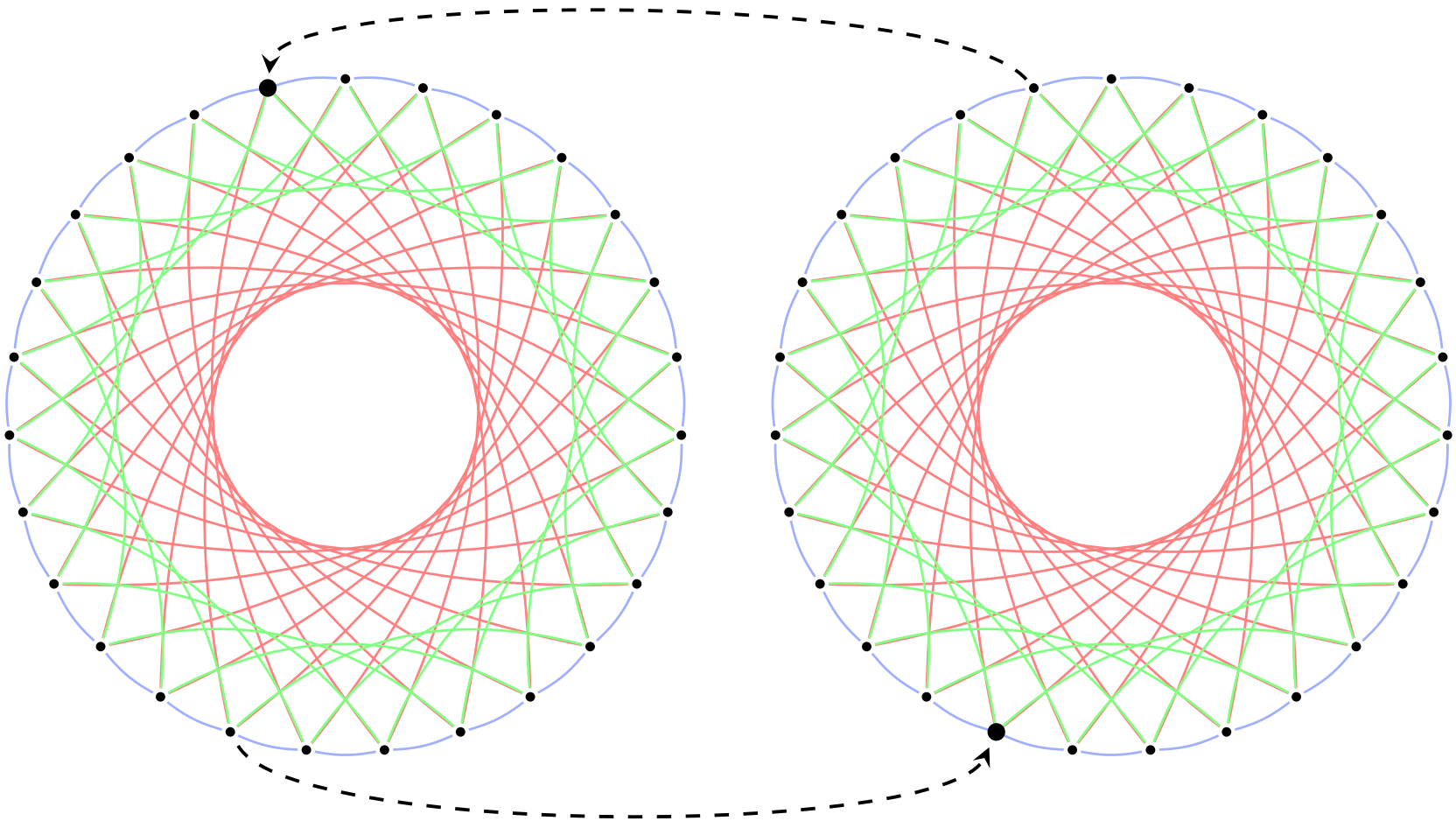
$[-, +, -, -]$



CSIDH key exchange

Alice
$[+, +, -, -]$

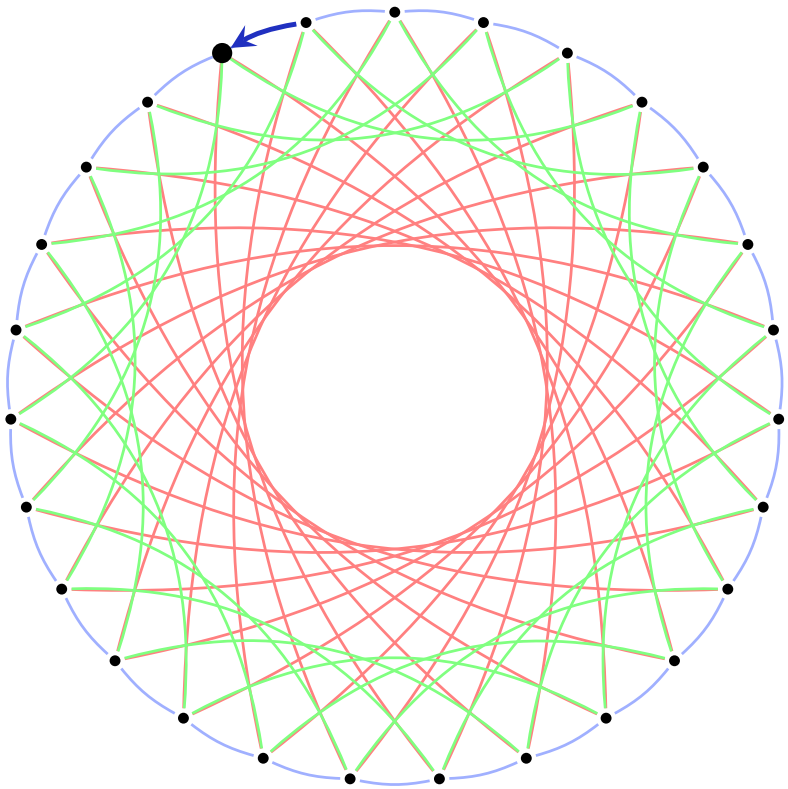
Bob
$[-, +, -, -]$



CSIDH key exchange

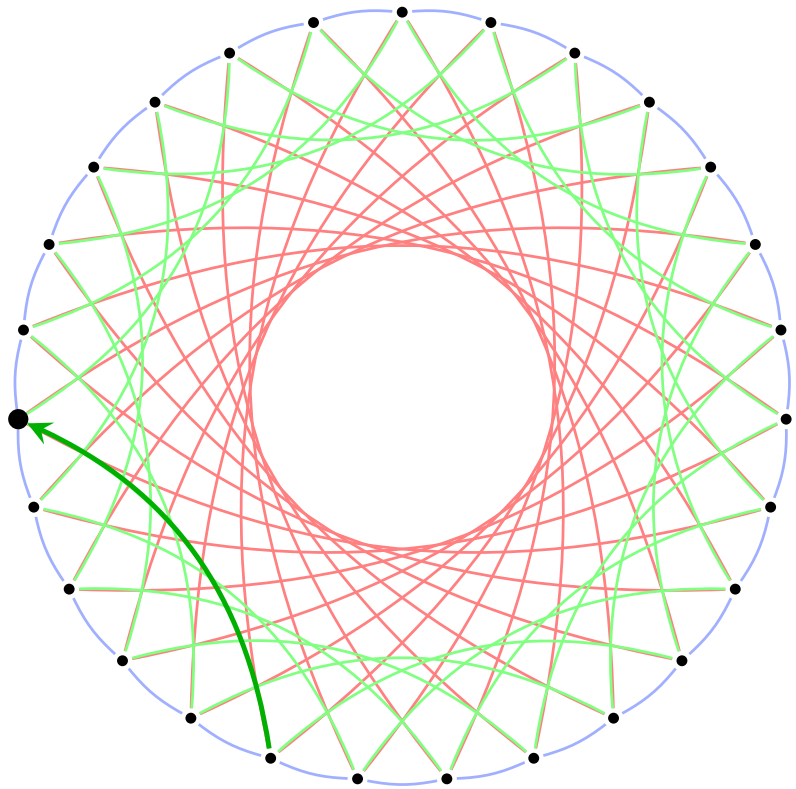
Alice

$[+, +, -, -]$



Bob

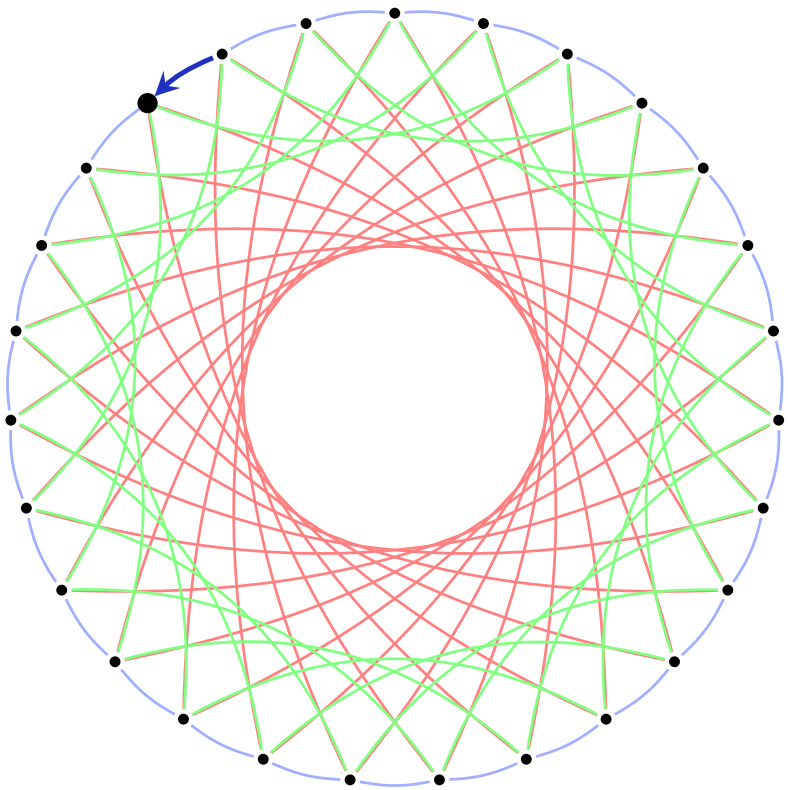
$[-, +, -, -]$



CSIDH key exchange

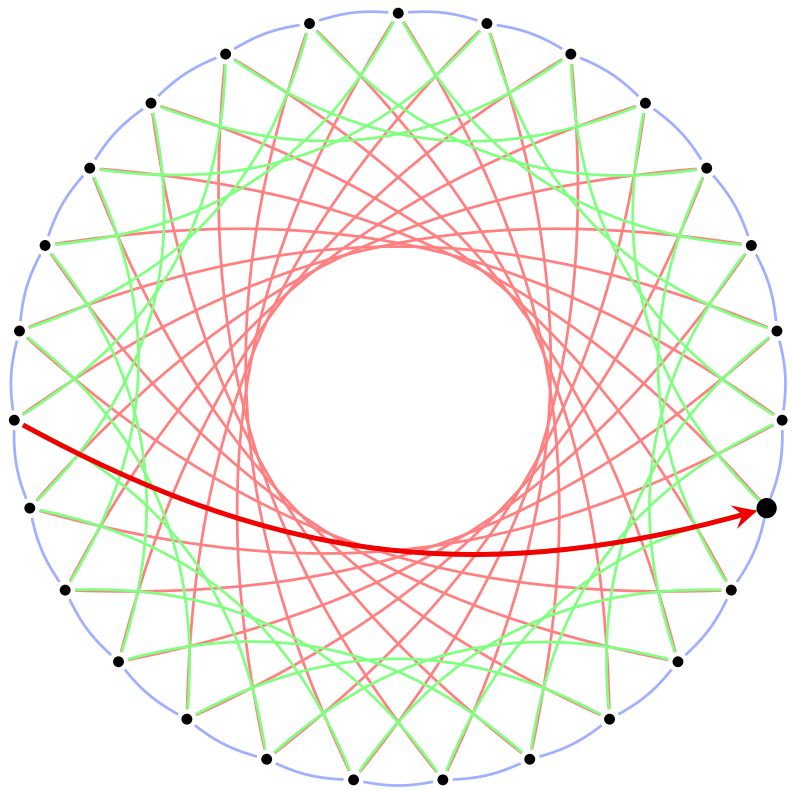
Alice

$[+, +, -, -]$



Bob

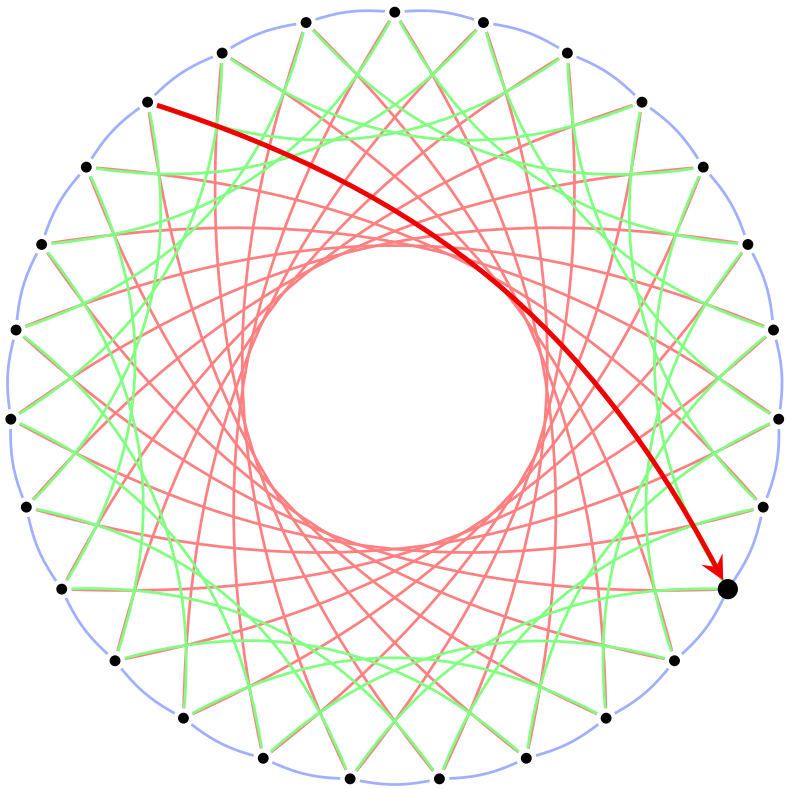
$[-, +, -, -]$



CSIDH key exchange

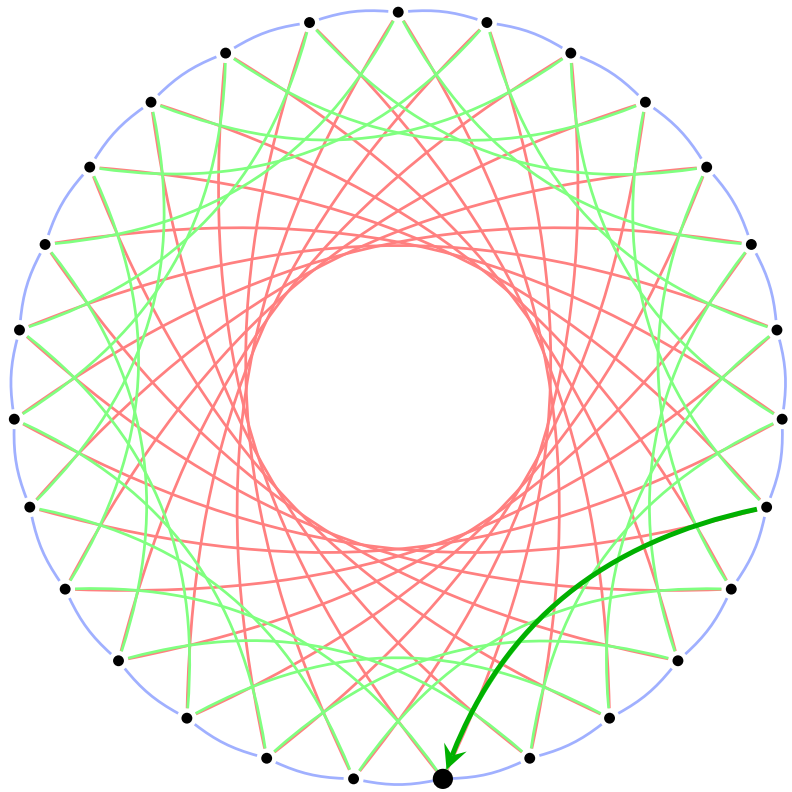
Alice

$[+, +, -, -]$



Bob

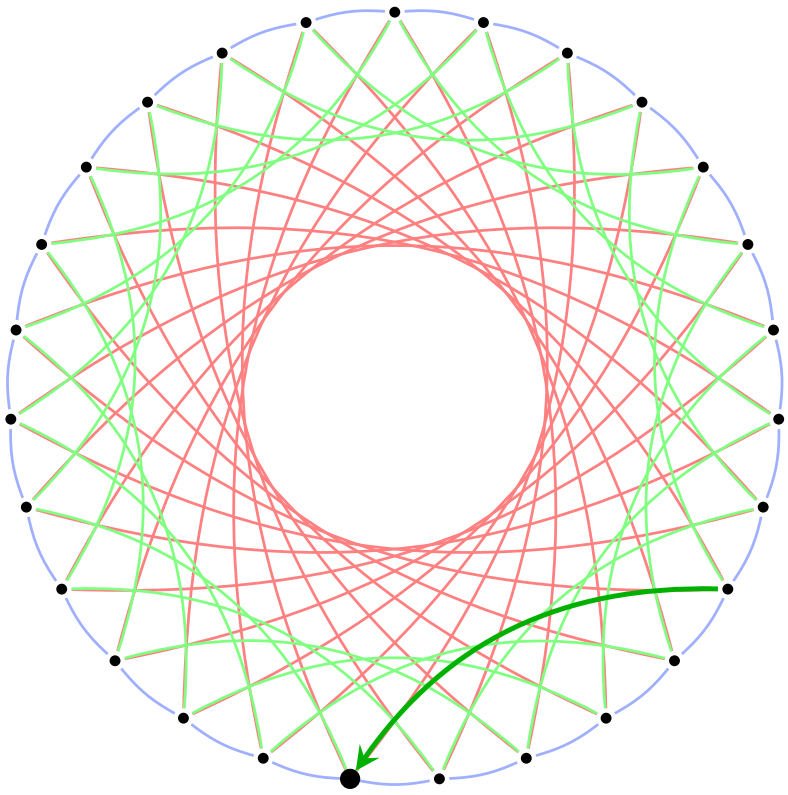
$[-, +, -, -]$



CSIDH key exchange

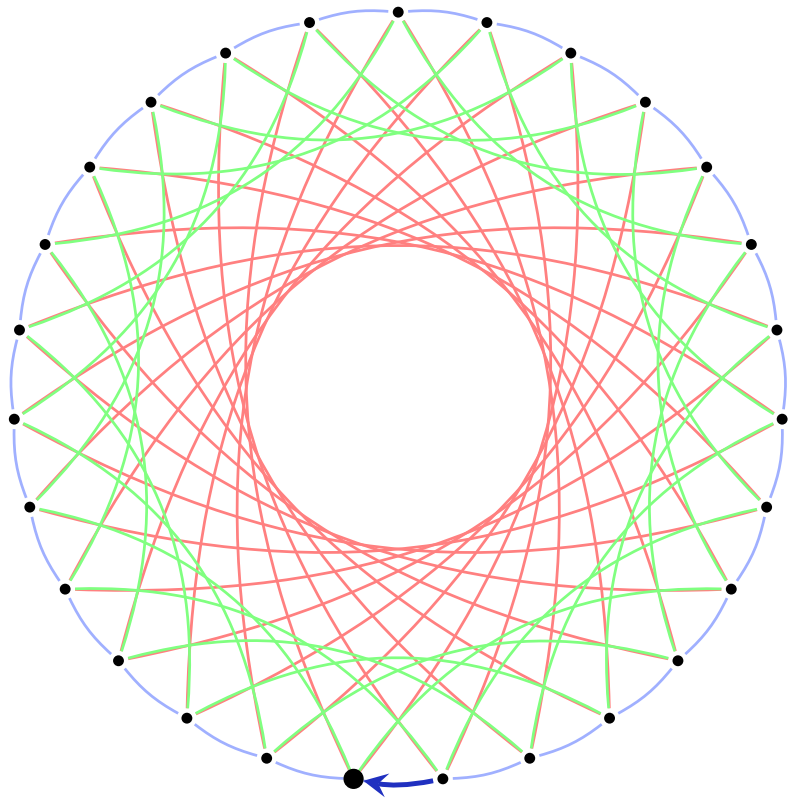
Alice

$[+, +, -, -]$



Bob

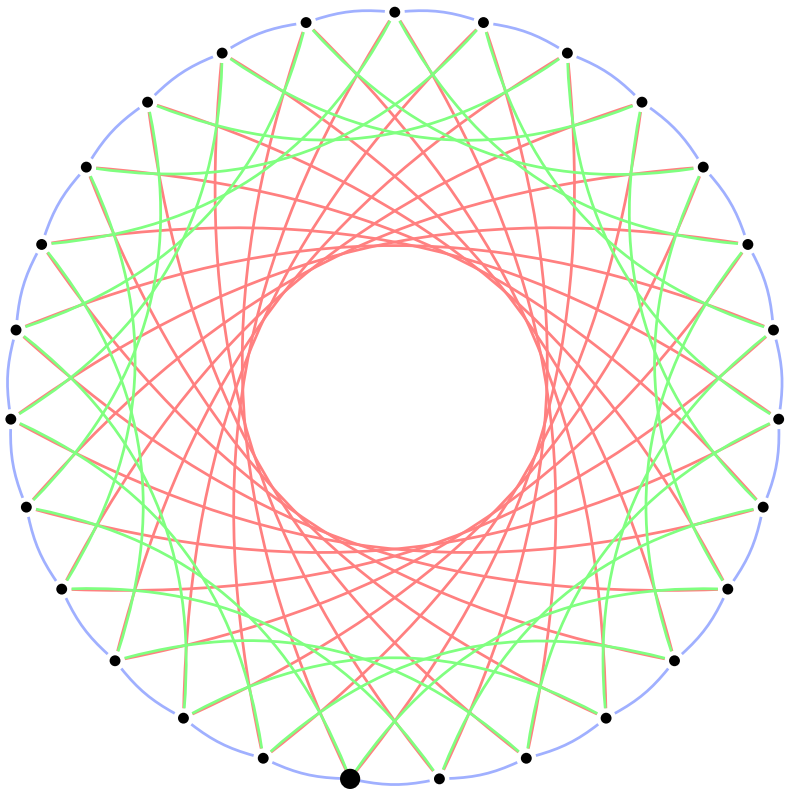
$[-, +, -, -]$



CSIDH key exchange

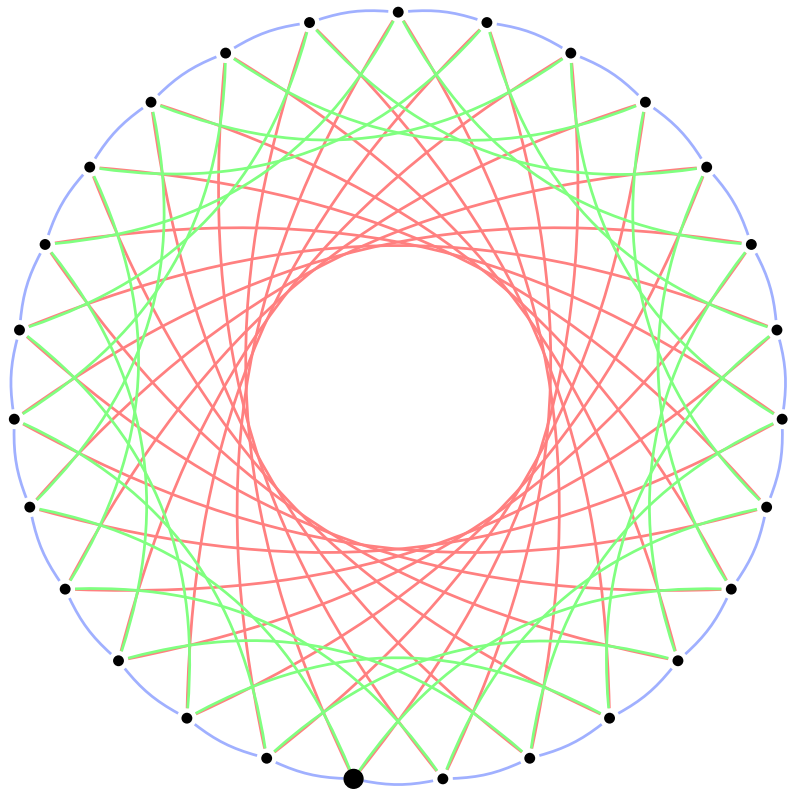
Alice

$[+, +, -, -]$



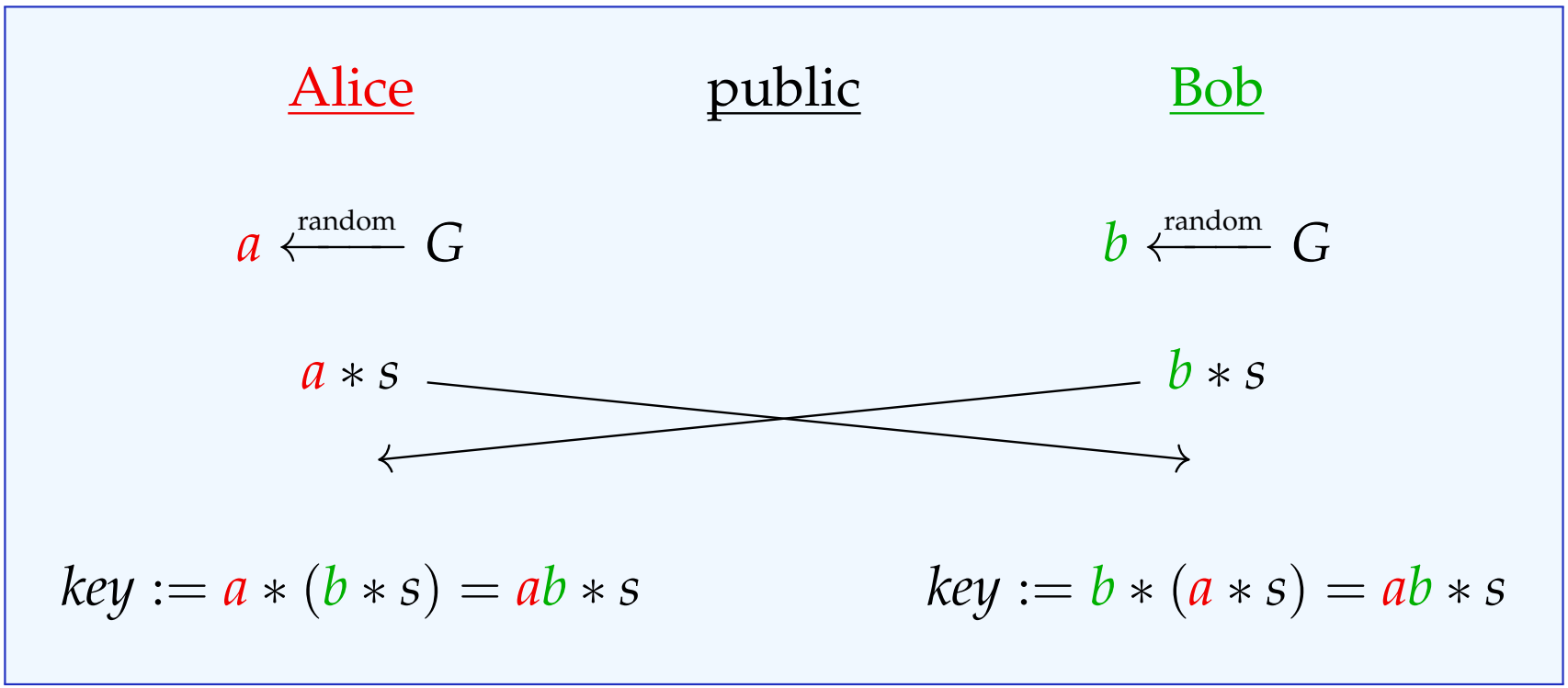
Bob

$[-, +, -, -]$



Group=action-based key exchange

Like in the CSIDH example, we *generally* get a key exchange from a commutative group action $G \times S \to S$:



Why no Shor?

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 generally cannot compose $a * s$ and $b * s$!

Security of CSIDH

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

Security of CSIDH

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

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

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

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

Security of CSIDH

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

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

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

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

Solving abelian hidden shift breaks CSIDH.

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

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

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?

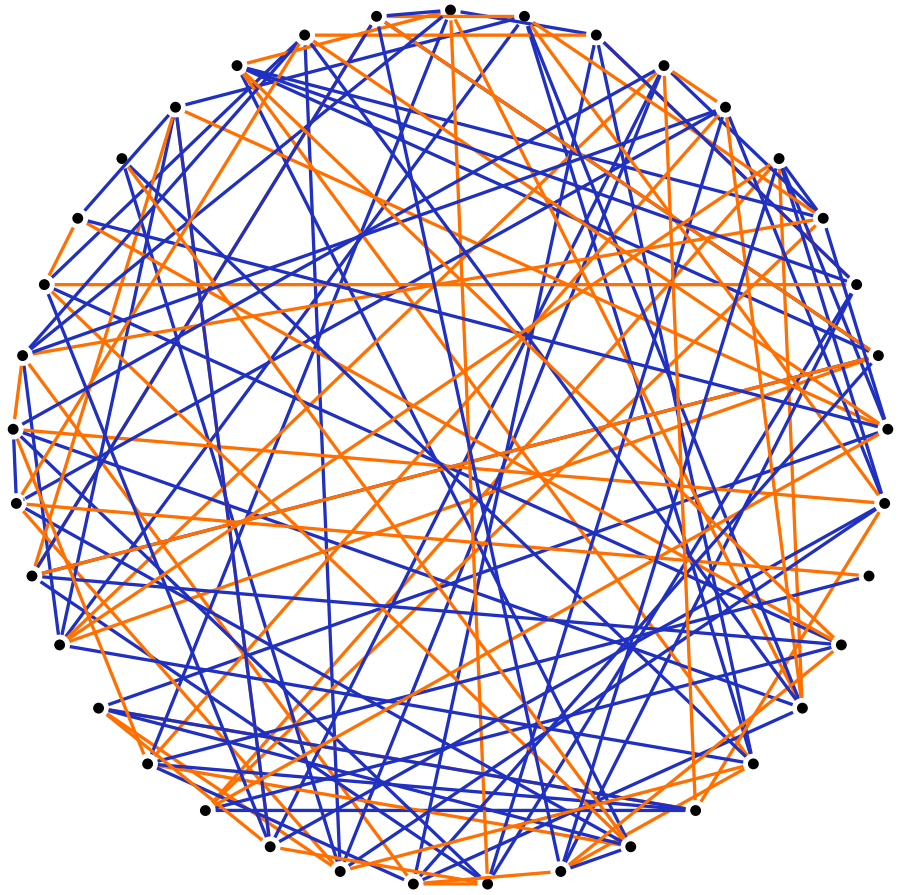
The supersingular isogeny graph over $\mathbb{F}_{p^2}$ has less structure.

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

- Problem: also no more intrinsic sense of direction.

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

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



Now: SIDH (Jao, De Feo; 2011)

(...whose name doesn't allow for nice pictures of beaches...)

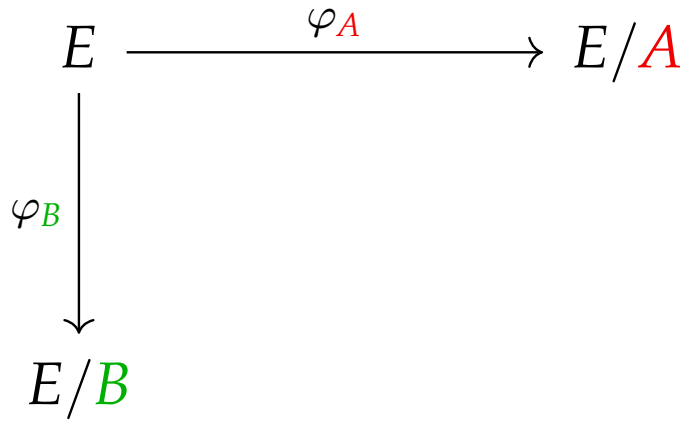
SIDH: High-level view

E

SIDH: High-level view

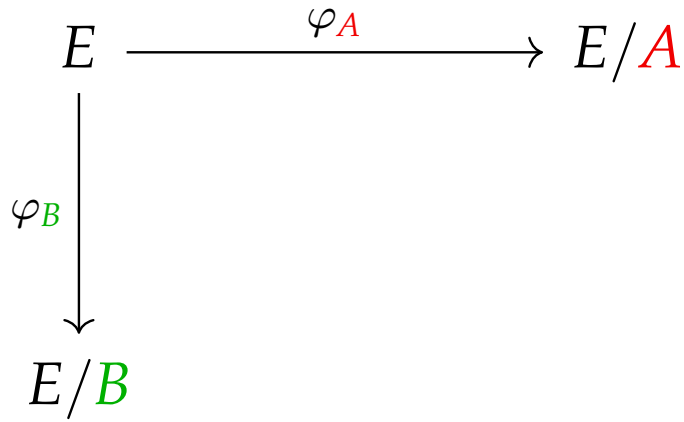
- Alice & Bob pick secret subgroups A and B of E.

SIDH: High-level view



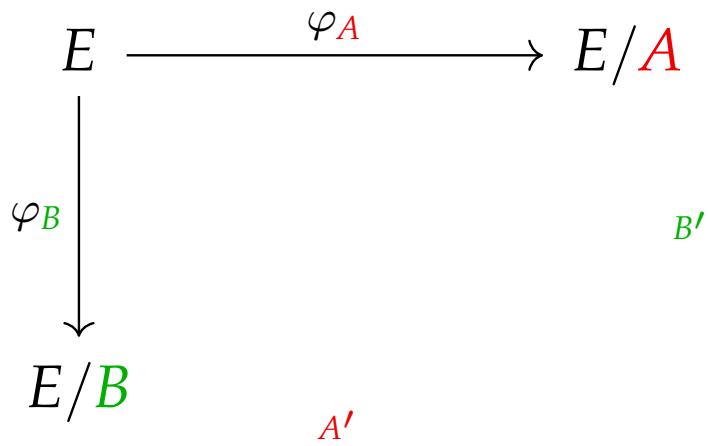
- Alice & Bob pick secret subgroups A and B of E.
- Alice computes $\varphi_A : E \to E/A$; Bob computes $\varphi_B : E \to E/B$.
  (These isogenies correspond to walking on the isogeny graph.)

SIDH: High-level view



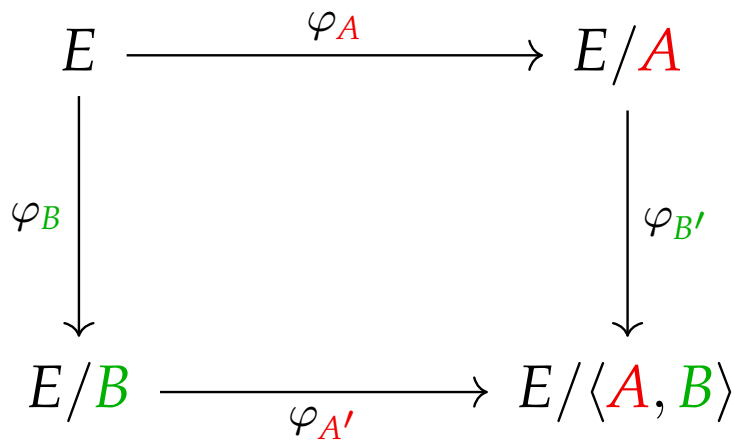
- Alice & Bob pick secret subgroups A and B of E.
- Alice computes $\varphi_A : E \to E/A$; Bob computes $\varphi_B : E \to E/B$.
  (These isogenies correspond to walking on the isogeny graph.)
- Alice and Bob transmit the values E/A and E/B.

SIDH: High-level view



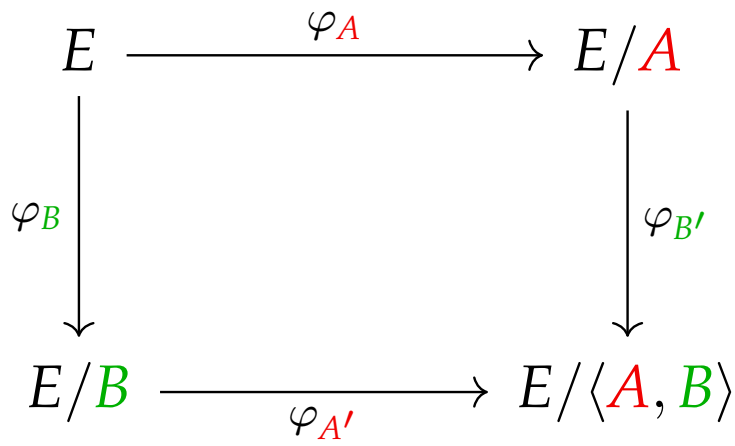
- Alice & Bob pick secret subgroups A and B of E.
- Alice computes $\varphi_A : E \to E/A$; Bob computes $\varphi_B : E \to E/B$.
  (These isogenies correspond to walking on the isogeny graph.)
- Alice and Bob transmit the values E/A and E/B.
- Alice somehow obtains $A' := \varphi_B(A)$. (Similar for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

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

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

By the way: This is *also* the high-level view for CSIDH... 🙃

SIDH's auxiliary points

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

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

SIDH's auxiliary points

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

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

Solution: φ_B is a group homomorphism!

- 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.

SIDH's auxiliary points

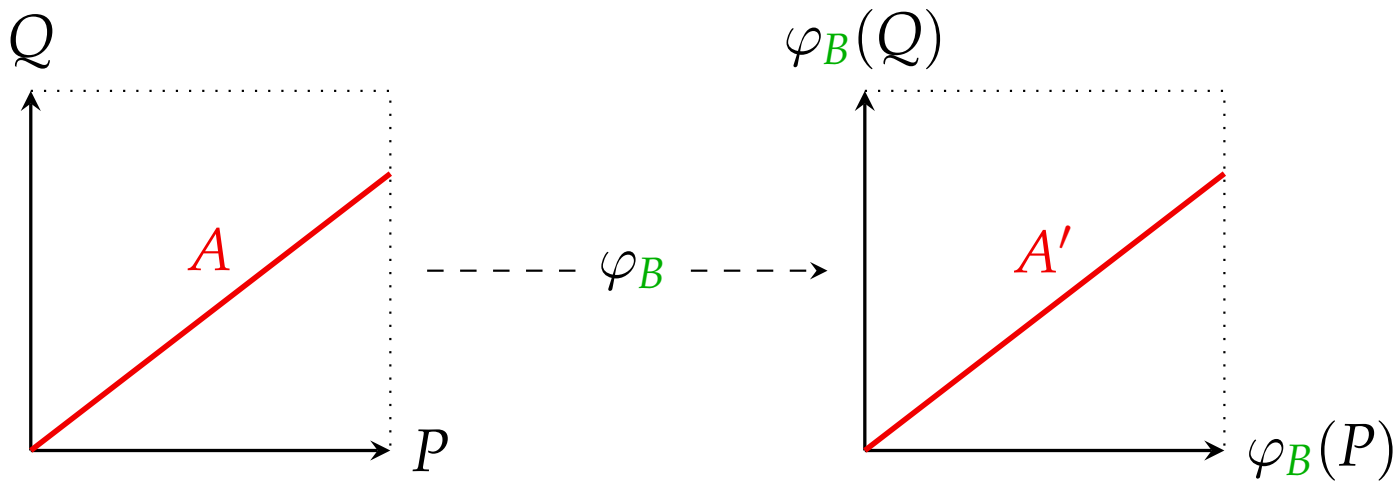
Previous slide: "Alice somehow obtains $A' := \varphi_B(A)$."

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

Solution: φ_B is a group homomorphism!

- Alice picks A as $\langle P + [a]Q \rangle$ for fixed public $P, Q \in E$.
- Bob includes $\varphi_B(P)$ and $\varphi_B(Q)$ in his public key.

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



SIDH in one slide

Public parameters:

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

Alice	public	Bob
$a \xleftarrow{\text{random}} \{0 \dots 2^n - 1\}$		$b \xleftarrow{\text{random}} \{0 \dots 3^m - 1\}$
$A := \langle P + [a]Q \rangle$		$B := \langle R + [b]S \rangle$
compute $\varphi_A : E \to E/A$		compute $\varphi_B : E \to E/B$
$E/A,\ \varphi_A(R),\ \varphi_A(S)$	$\longrightarrow$	
	$\longleftarrow$	$E/B,\ \varphi_B(P),\ \varphi_B(Q)$
$A' := \langle \varphi_B(P) + [a]\varphi_B(Q) \rangle$		$B' := \langle \varphi_A(R) + [b]\varphi_A(S) \rangle$
$s := j\big((E/B)/A'\big)$		$s := j\big((E/A)/B'\big)$

Security of SIDH

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

Security of SIDH

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

Classical attacks:

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

Security of SIDH

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

Classical attacks:

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

Quantum attacks:

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

Security of SIDH

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

Classical attacks:

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

Quantum attacks:

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

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

Fragen?

Questions?

Domande?

Dumondas?