Isogeny graphs in cryptography

Luca De Feo

Université Paris Saclay, UVSQ

July 29, 2019
Cryptography meets Graph Theory
Würzburg, Germany

Plan

1. Elliptic curves, isogenies, complex multiplication
2. Isogeny graphs
3. Key exchange

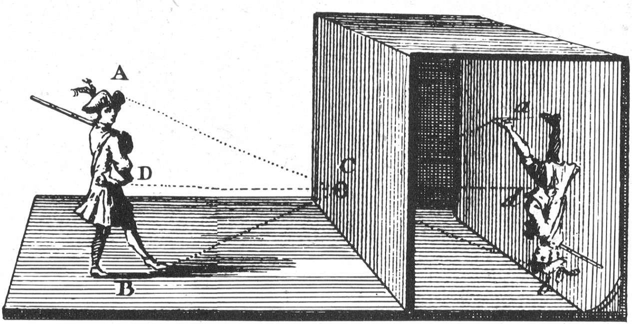
Projective space

Definition (Projective space)

Let $\bar{k}$ an algebraically closed field, the projective space $\mathbb{P}^n(\bar{k})$ is the set of non-null $(n+1)$-tuples $(x_0, \dots, x_n) \in \bar{k}^n$ modulo the equivalence relation

$$(x_0, \dots, x_n) \sim (\lambda x_0, \dots, \lambda x_n) \qquad \text{with } \lambda \in \bar{k} \setminus \{0\}.$$

A class is denoted by $(x_0 : \cdots : x_n)$.

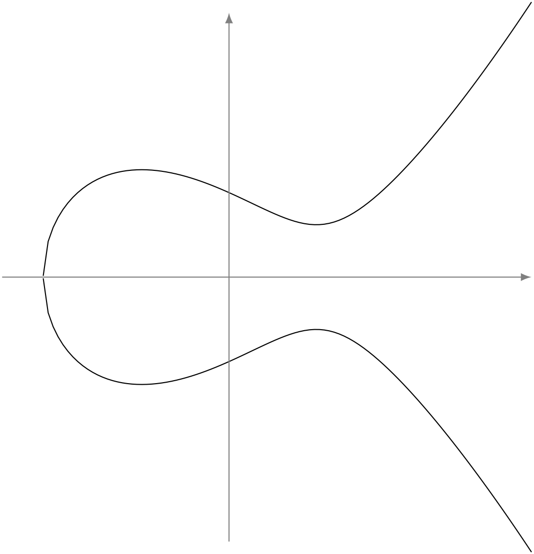


Weierstrass equations

Let k be a field of characteristic $\neq 2, 3$.
An elliptic curve *defined over* k is the locus in $\mathbb{P}^2(\bar{k})$ of an equation

$$Y^2Z = X^3 + aXZ^2 + bZ^3,$$

where $a, b \in k$ and $4a^3 + 27b^2 \neq 0$.



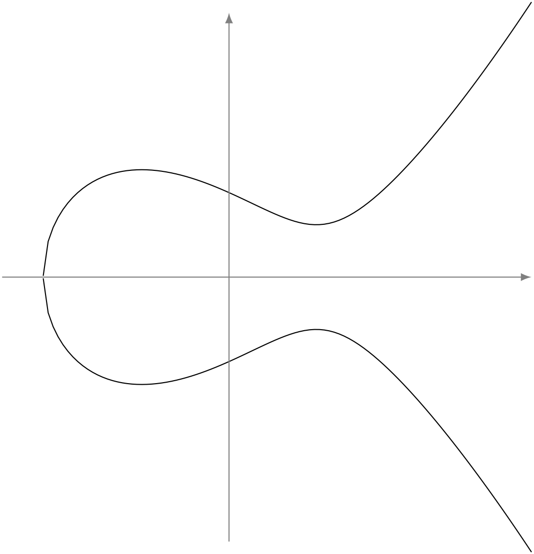
Weierstrass equations

Let k be a field of characteristic $\neq 2, 3$.
An elliptic curve *defined over* k is the locus in $\mathbb{P}^2(\bar{k})$ of an equation

$$Y^2Z = X^3 + aXZ^2 + bZ^3,$$

where $a, b \in k$ and $4a^3 + 27b^2 \neq 0$.

- $\mathcal{O} = (0 : 1 : 0)$ is the point at infinity;



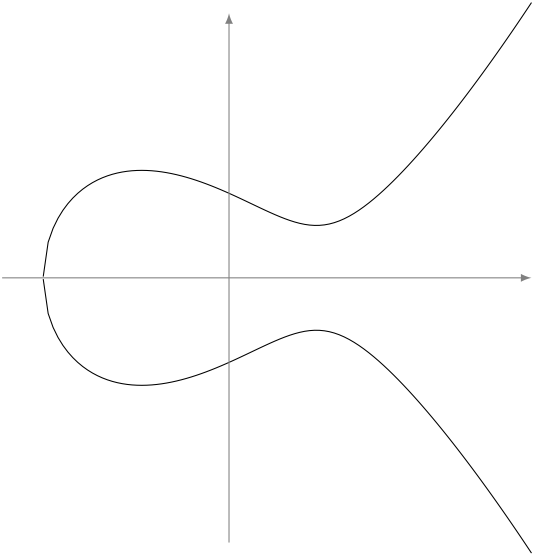
Weierstrass equations

Let k be a field of characteristic $\neq 2, 3$.
An elliptic curve *defined over* k is the locus in $\mathbb{P}^2(\bar{k})$ of an equation

$$Y^2Z = X^3 + aXZ^2 + bZ^3,$$

where $a, b \in k$ and $4a^3 + 27b^2 \neq 0$.

- $\mathcal{O} = (0 : 1 : 0)$ is the point at infinity;
- $y^2 = x^3 + ax + b$ is the affine equation.

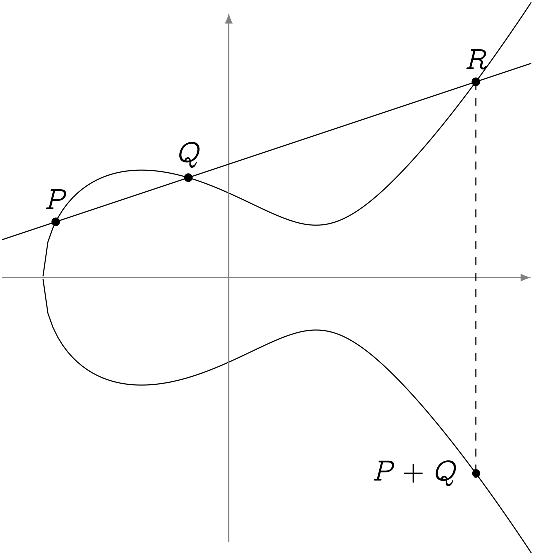


The group law

Bezout's theorem

Every line cuts E in exactly three points (counted with multiplicity).

Define a group law such that any three colinear points add up to zero.



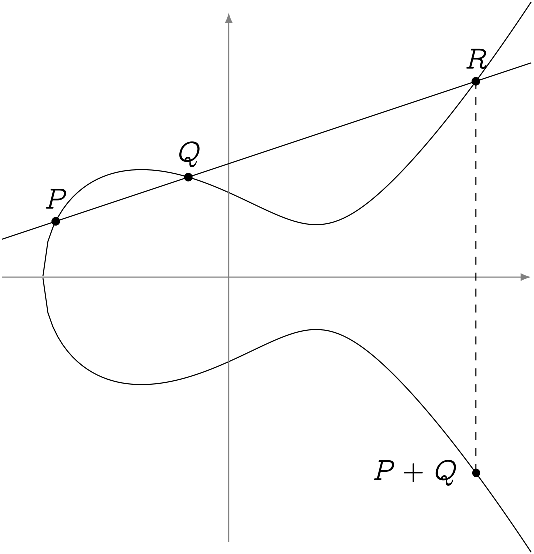
The group law

Bezout's theorem

Every line cuts E in exactly three points (counted with multiplicity).

Define a group law such that any three colinear points add up to zero.

- The law is algebraic (it has *formulas*);



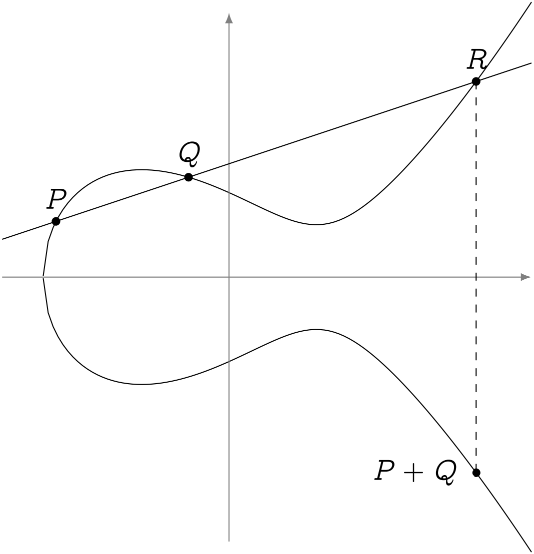
The group law

Bezout's theorem

Every line cuts E in exactly three points (counted with multiplicity).

Define a group law such that any three colinear points add up to zero.

- The law is algebraic (it has *formulas*);
- The law is commutative;
- $\mathcal{O}$ is the group identity;
- Opposite points have the same x-value.



Group structure

Torsion structure

Let E be defined over an algebraically closed field $\bar{k}$ of characteristic p.

$$E[m] \simeq \quad \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \qquad \text{if } p \nmid m,$$

$$E[p^e] \simeq \begin{cases} \mathbb{Z}/p^e\mathbb{Z} & \text{ordinary case,} \\ \{\mathcal{O}\} & \text{supersingular case.} \end{cases}$$

Free part

Let E be defined over a number field k, the group of k-rational points $E(k)$ is finitely generated.

Maps: isomorphisms

Isomorphisms

The only invertible algebraic maps between elliptic curves are of the form

$$(x, y) \mapsto (u^2 x, u^3 y)$$

for some $u \in \bar{k}$.
They are group isomorphisms.

j-Invariant

Let $E : y^2 = x^3 + ax + b$, its j-invariant is

$$j(E) = 1728 \frac{4a^3}{4a^3 + 27b^2}.$$

Two elliptic curves E, E' are isomorphic if and only if $j(E) = j(E')$.

Maps: isogenies

Theorem

Let $\phi : E \to E'$ be a map between elliptic curves. These conditions are equivalent:

- *ϕ is a surjective group morphism,*
- *ϕ is a group morphism with finite kernel,*
- *ϕ is a non-constant algebraic map of projective varieties sending the point at infinity of E onto the point at infinity of E'.*

If they hold ϕ is called an isogeny.

Two curves are called isogenous if there exists an isogeny between them.

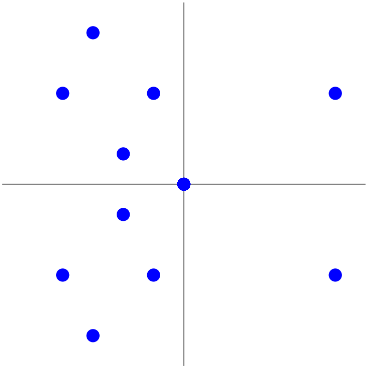
Example: Multiplication-by-m

On any curve, an isogeny from E to itself (i.e., an endomorphism):

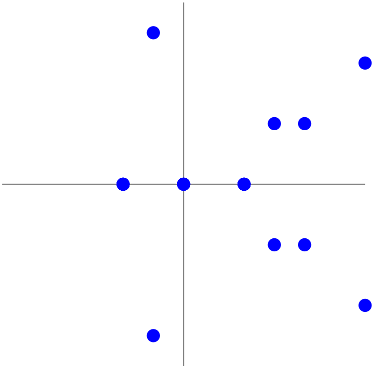
$$\begin{aligned}[m] \;:\; E &\to E,\\ P &\mapsto [m]P.\end{aligned}$$

Isogenies: an example over $\mathbb{F}_{11}$

$E \;:\; y^2 = x^3 + x$

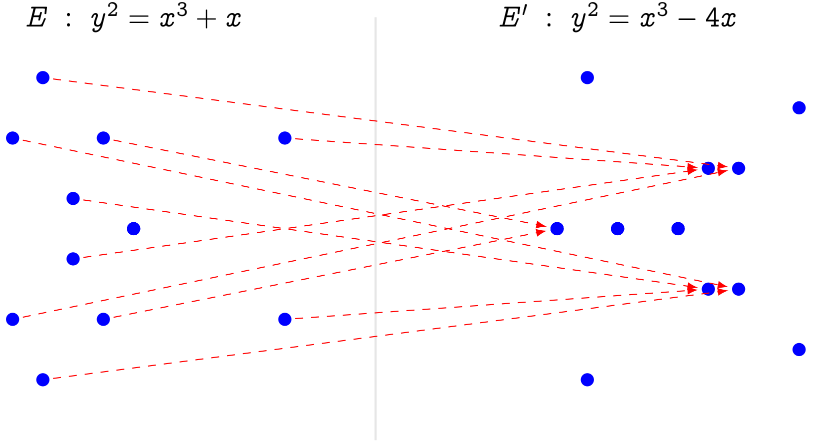


$E' \;:\; y^2 = x^3 - 4x$



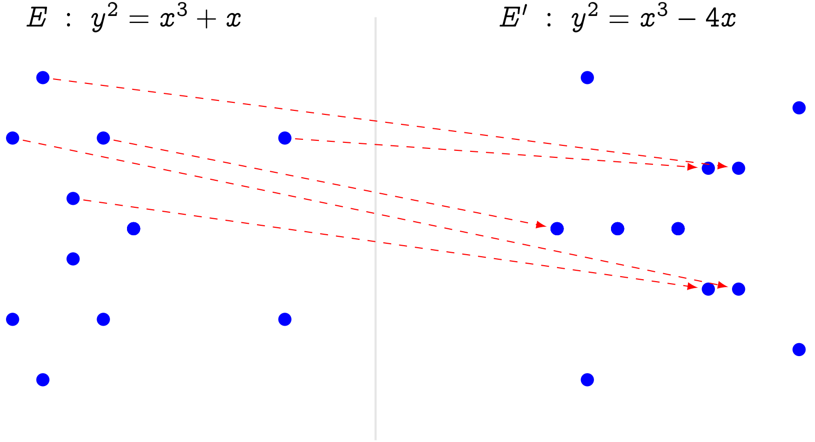
$$\phi(x,y) = \left(\frac{x^2+1}{x},\quad y\frac{x^2-1}{x^2}\right)$$

Isogenies: an example over $\mathbb{F}_{11}$



$$\phi(x, y) = \left(\frac{x^2 + 1}{x}, \quad y\frac{x^2 - 1}{x^2}\right)$$

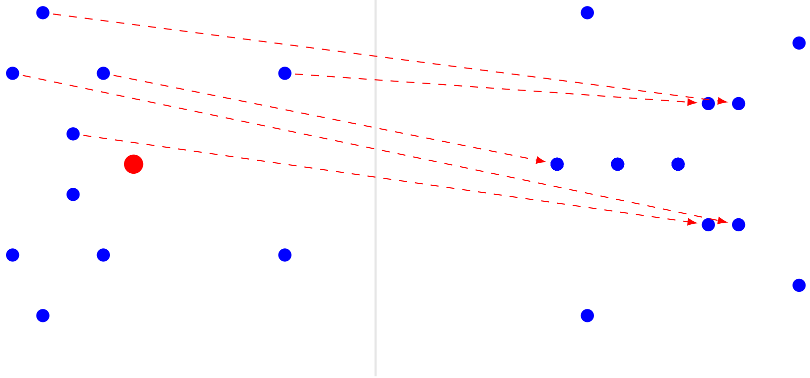
Isogenies: an example over $\mathbb{F}_{11}$



$$\phi(x, y) = \left(\frac{x^2 + 1}{x}, \quad y\frac{x^2 - 1}{x^2} \right)$$

Isogenies: an example over $\mathbb{F}_{11}$

$E\ :\ y^2 = x^3 + x$ $\qquad$ $E'\ :\ y^2 = x^3 - 4x$

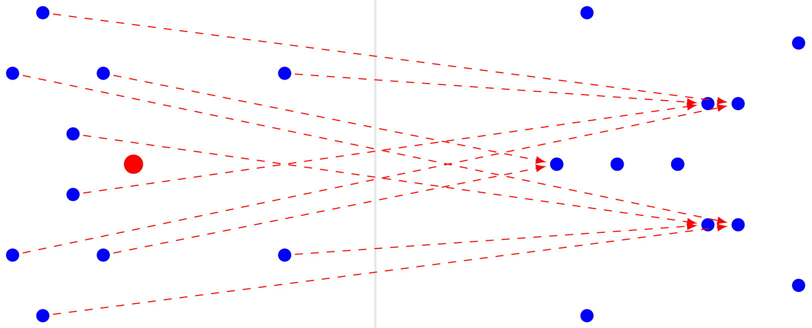


$$\phi(x, y) = \left(\frac{x^2+1}{x},\quad y\frac{x^2-1}{x^2} \right)$$

- Kernel generator in red.

Isogenies: an example over $\mathbb{F}_{11}$

$E : y^2 = x^3 + x$ $\qquad$ $E' : y^2 = x^3 - 4x$

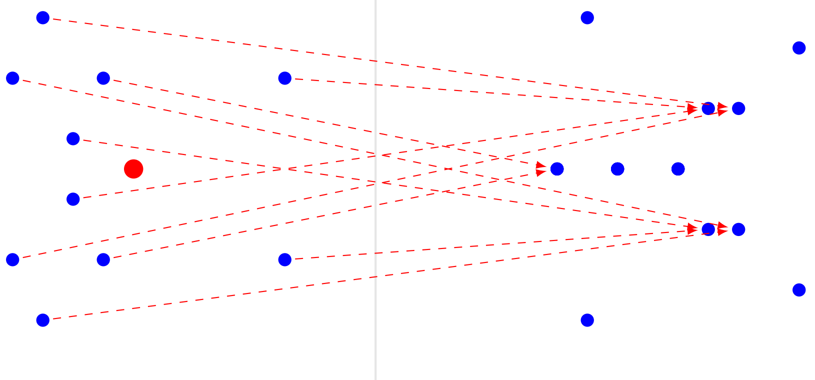


$$\phi(x, y) = \left(\frac{x^2 + 1}{x}, \quad y \frac{x^2 - 1}{x^2} \right)$$

- Kernel generator in red.
- This is a degree 2 map.

Isogenies: an example over $\mathbb{F}_{11}$

$E : y^2 = x^3 + x$ $\qquad$ $E' : y^2 = x^3 - 4x$



$$\phi(x,y) = \left(\frac{x^2+1}{x}, \quad y\frac{x^2-1}{x^2}\right)$$

- Kernel generator in red.
- This is a degree 2 map.
- Analogous to $x \mapsto x^2$ in $\mathbb{F}_q^*$.

Curves over finite fields

Frobenius endomorphism

Let E be defined over $\mathbb{F}_q$. The Frobenius endomorphism of E is the map

$$\pi \;:\; (X : Y : Z) \mapsto (X^q : Y^q : Z^q).$$

Hasse's theorem

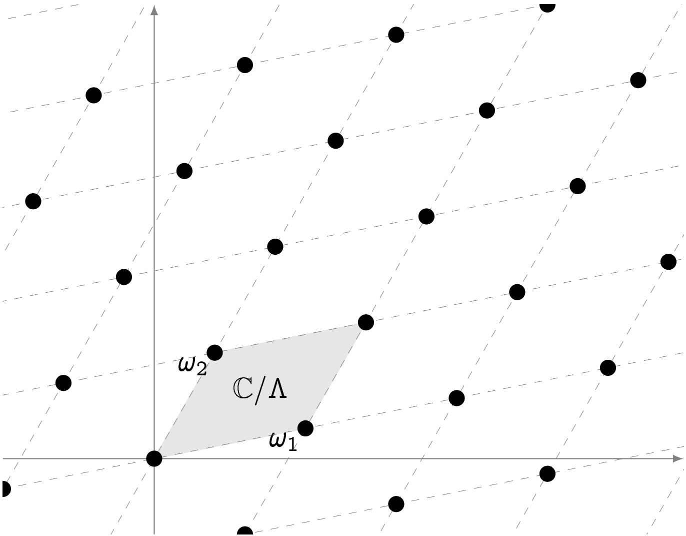
Let E be defined over $\mathbb{F}_q$, then

$$|\#E(k) - q - 1| \leq 2\sqrt{q}.$$

Serre-Tate theorem

Two elliptic curves E, E' defined over a finite field k are isogenous over k if and only if $\#E(k) = \#E'(k)$.

Complex tori

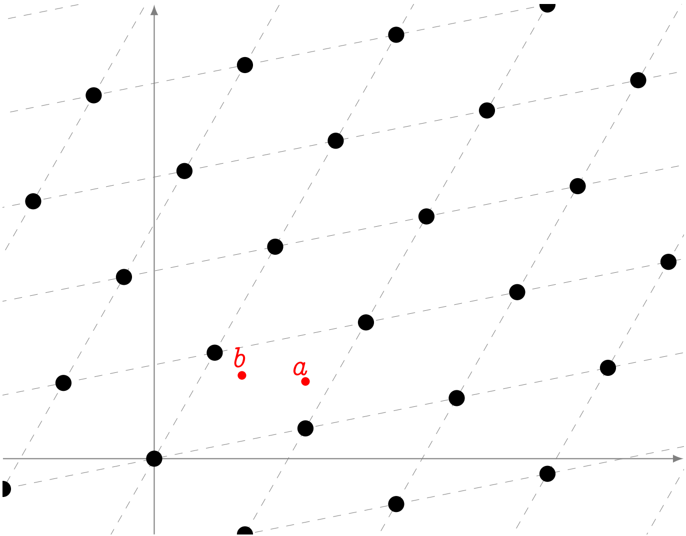


Let $\omega_1, \omega_2 \in \mathbb{C}$ be linearly independent complex numbers. Set

$$\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$$

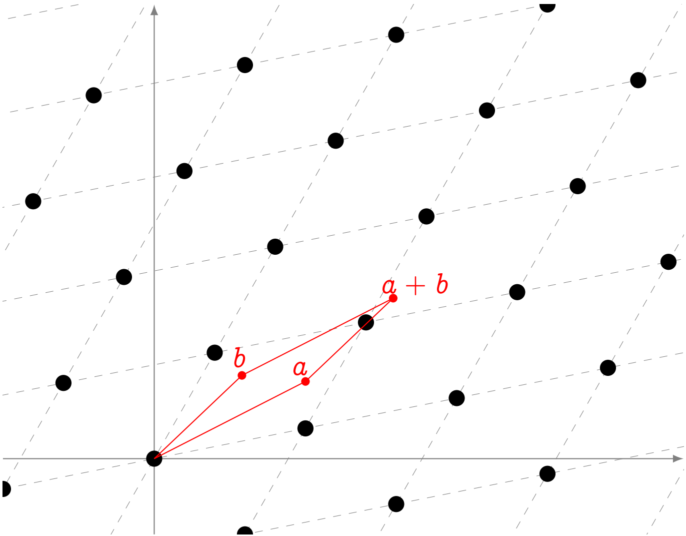
$\mathbb{C}/\Lambda$ is a complex torus.

Complex tori



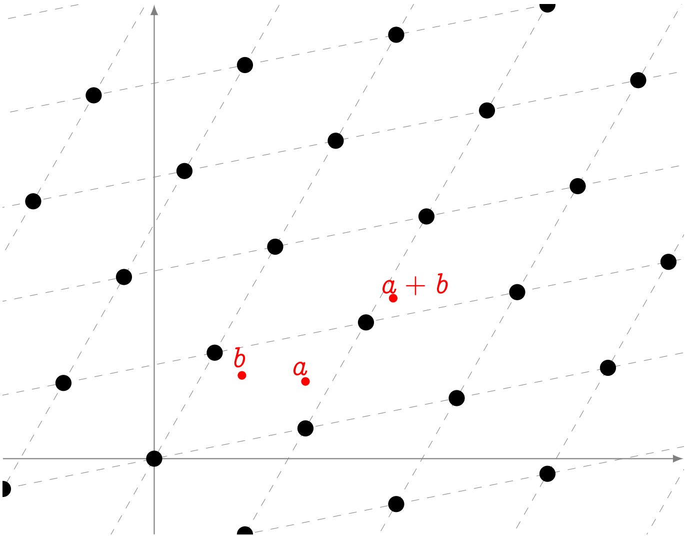
Addition law induced by addition on $\mathbb{C}$.

Complex tori



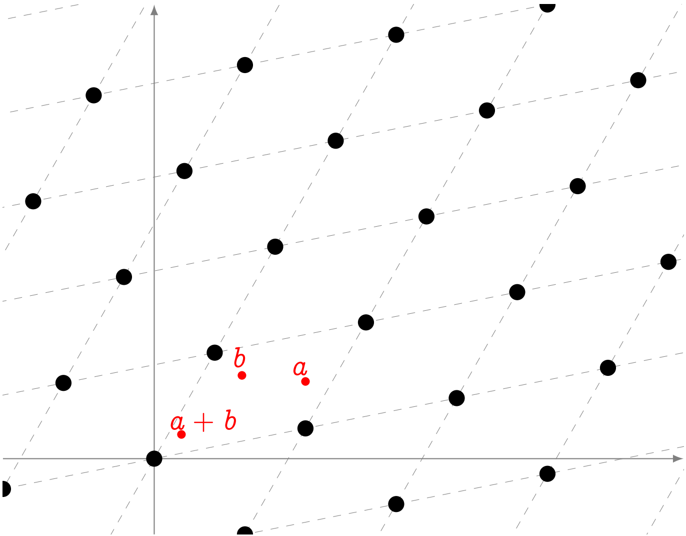
Addition law induced by addition on $\mathbb{C}$.

Complex tori



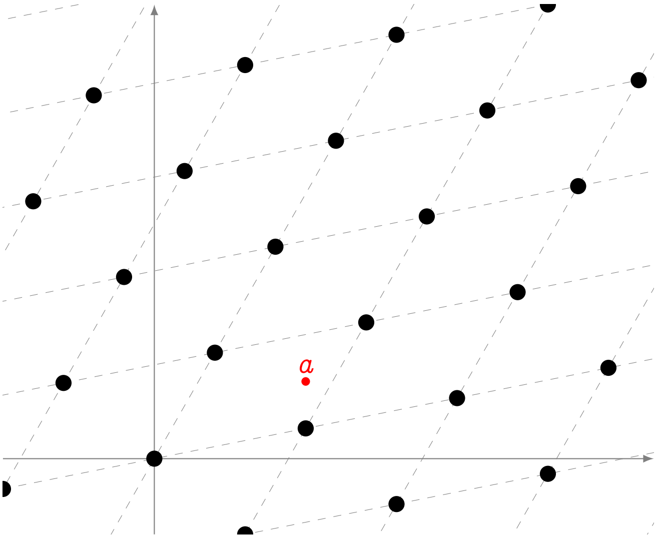
Addition law induced by addition on $\mathbb{C}$.

Complex tori



Addition law induced by addition on $\mathbb{C}$.

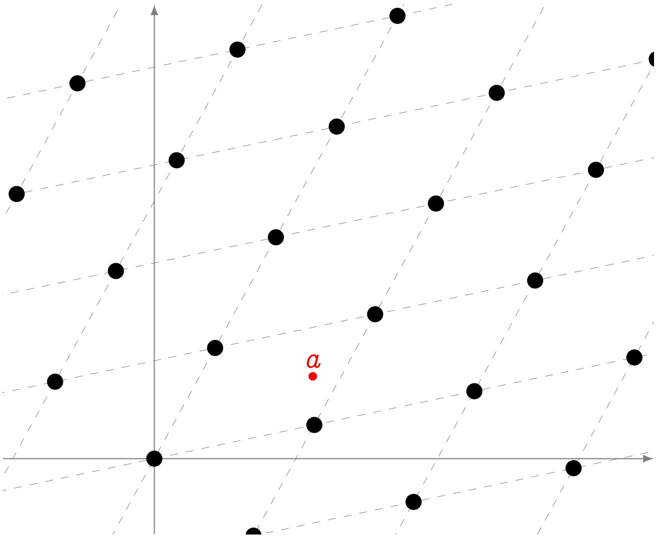
Homotheties



Two lattices are homothetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

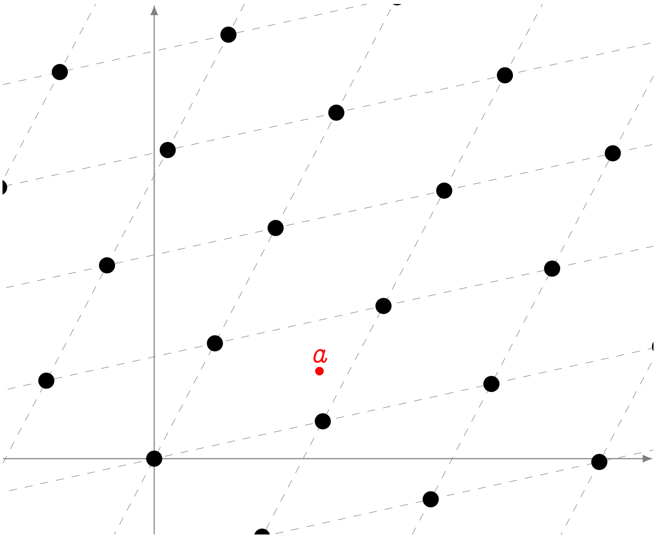
Homotheties



Two lattices are homothetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

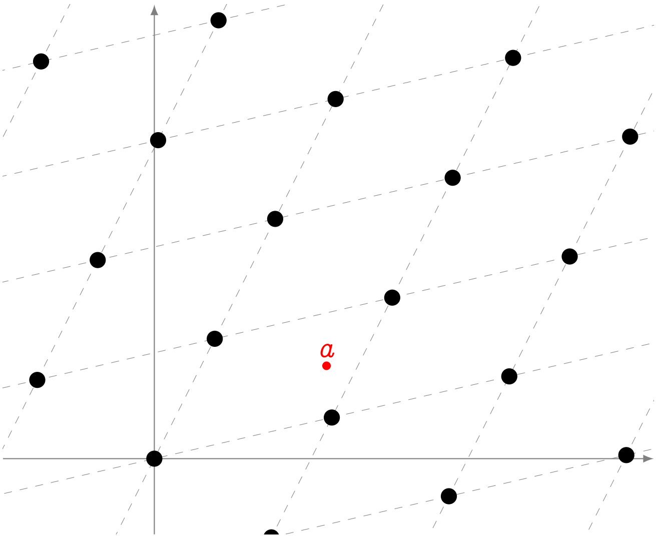
Homotheties



Two lattices are homothetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

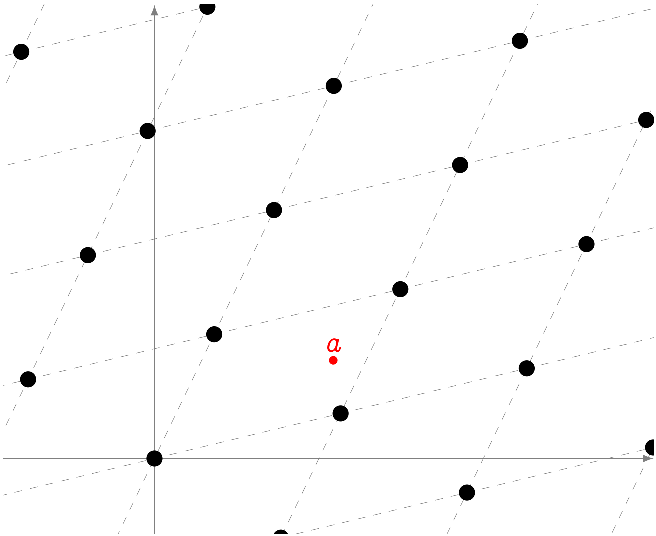
Homotheties



Two lattices are homothetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

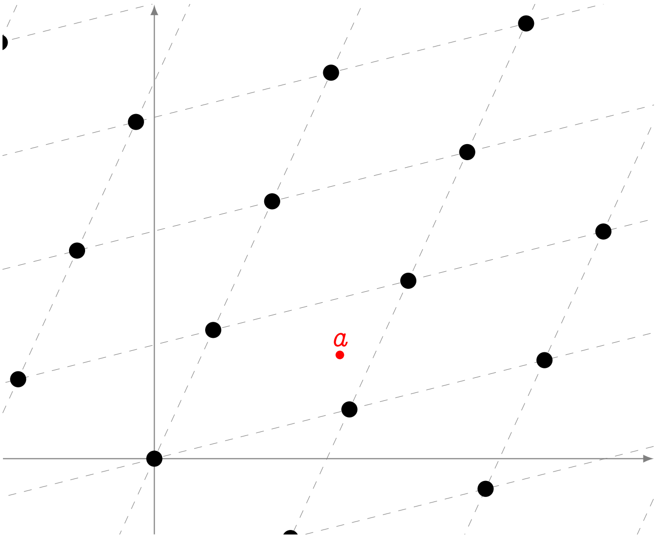
Homotheties



Two lattices are homothetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

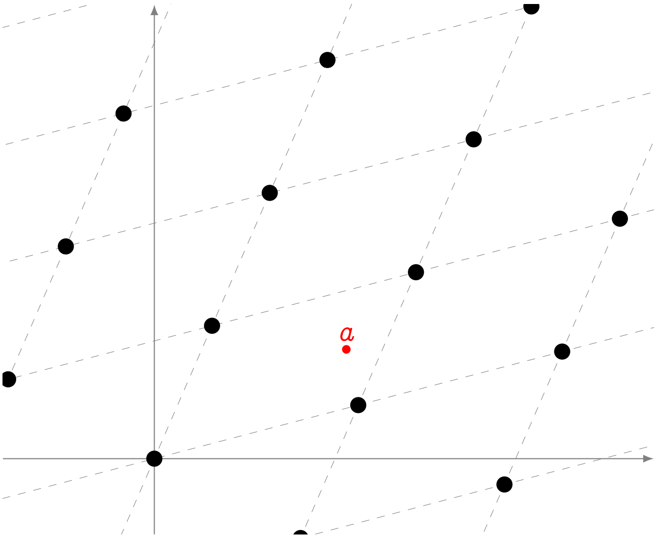
Homotheties



Two lattices are homothetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

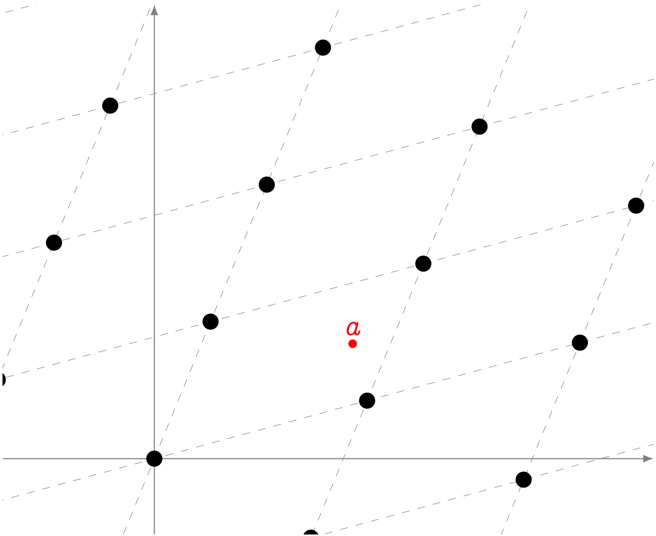
Homotheties



Two lattices are homothetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

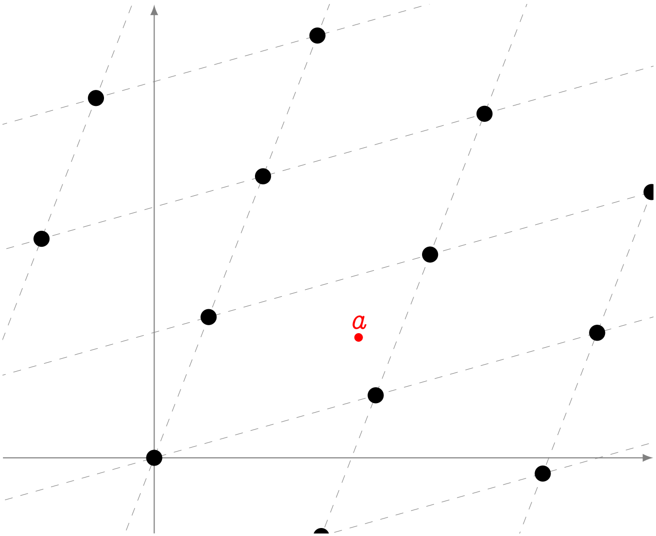
Homotheties



Two lattices are homothetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

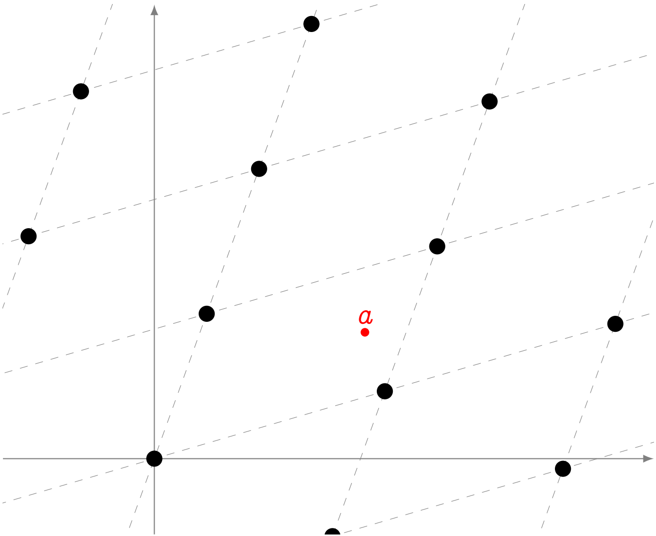
Homotheties



Two lattices are homothetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

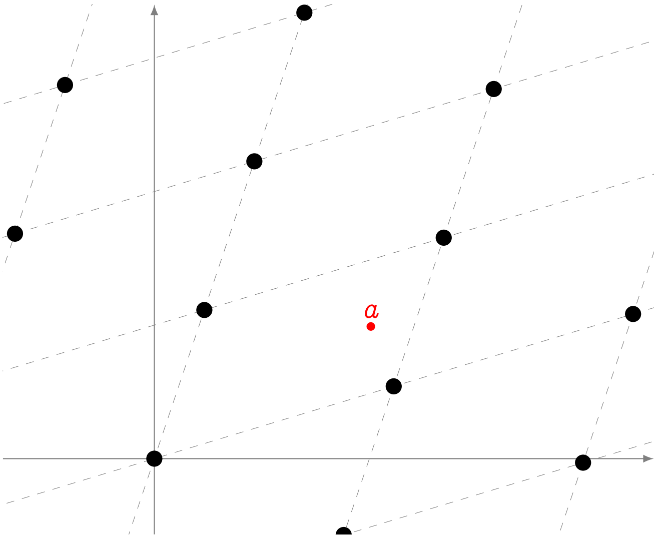
Homotheties



Two lattices are homothetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

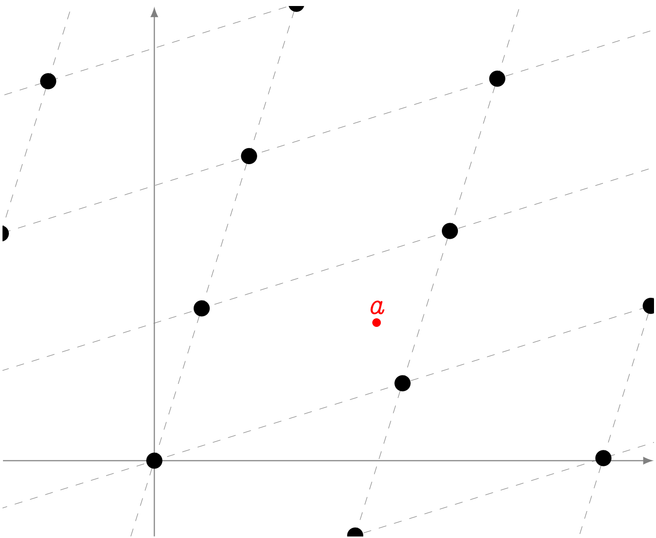
Homotheties



Two lattices are homothetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

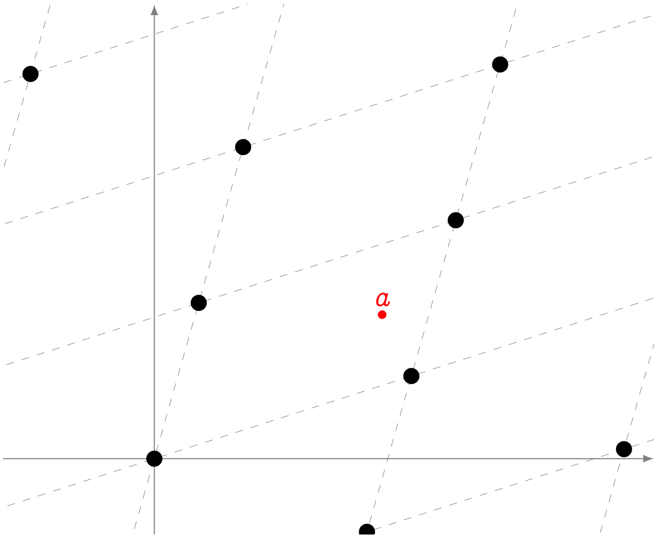
Homotheties



Two lattices are homothetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

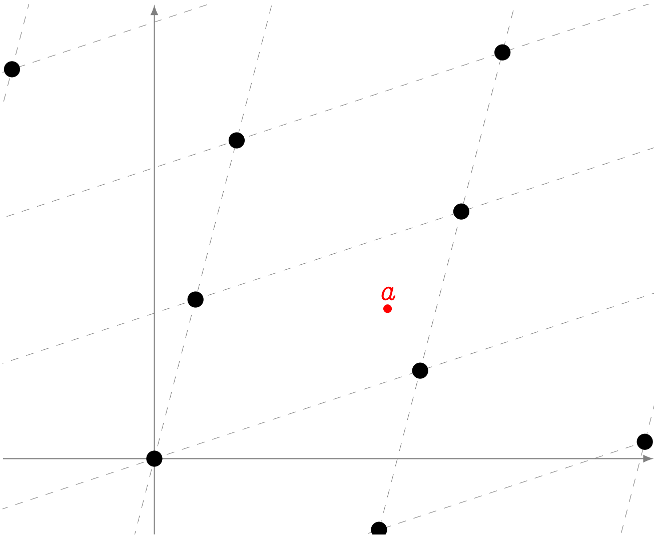
Homotheties



Two lattices are homothetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

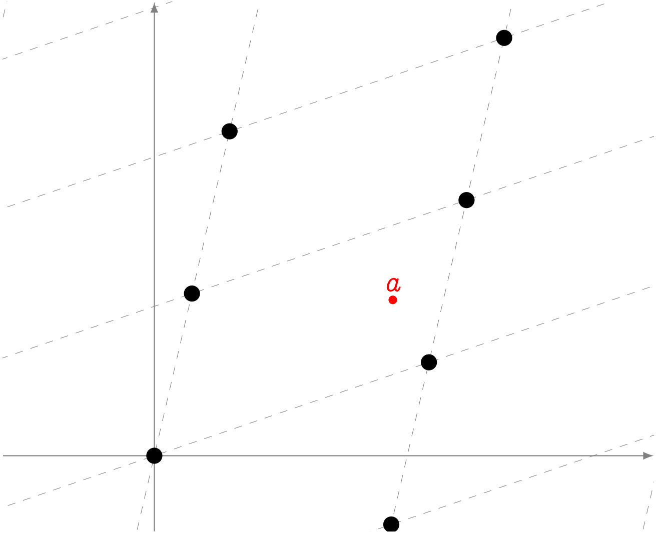
Homotheties



Two lattices are homothetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

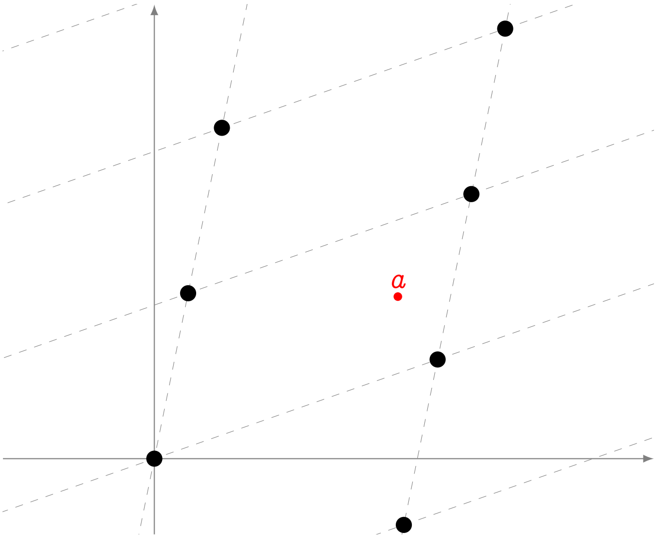
Homotheties



Two lattices are homothetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

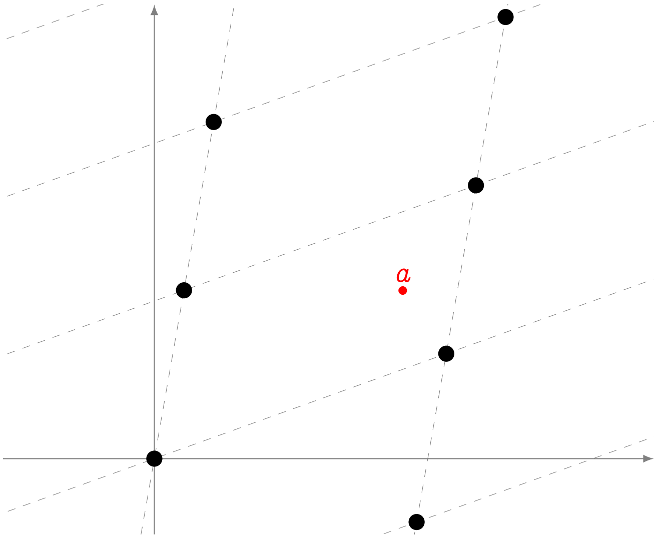
Homotheties



Two lattices are homothetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

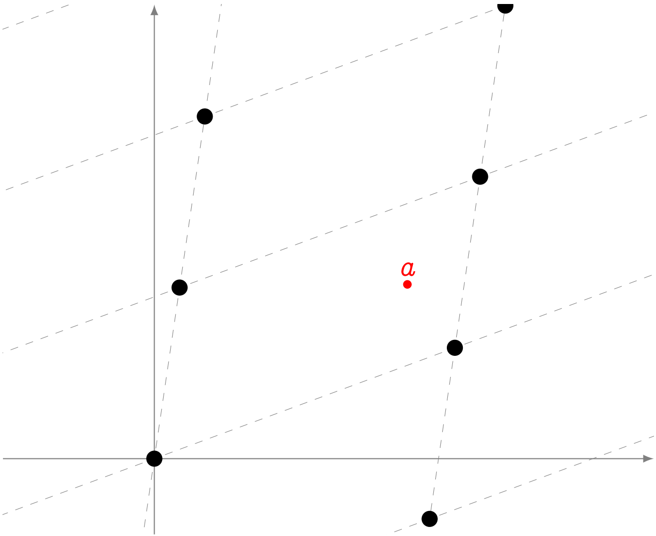
Homotheties



Two lattices are homothetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

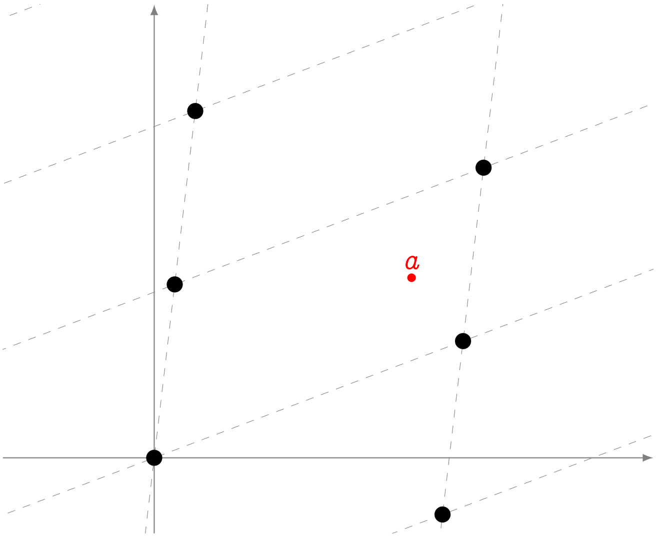
Homotheties



Two lattices are homothetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

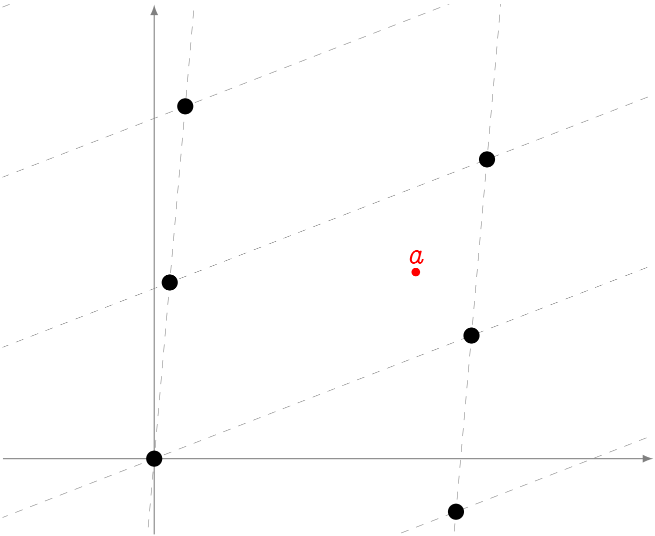
Homotheties



Two lattices are homothetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

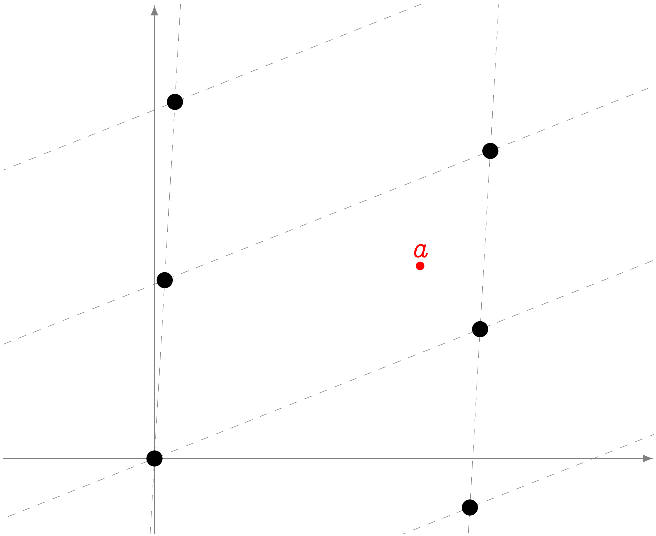
Homotheties



Two lattices are homothetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

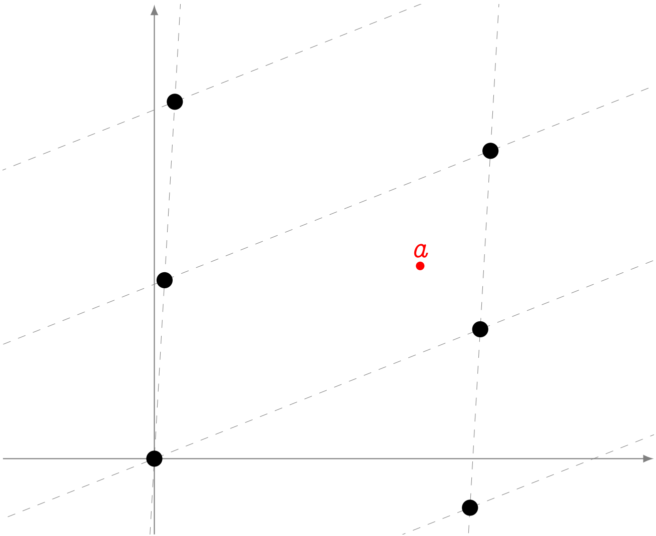
Homotheties



Two lattices are homothetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

Homotheties



Two lattices are homothetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

The j-invariant

We want to classify complex lattices/tori up to homothety.

Eisenstein series

Let Λ be a complex lattice. For any integer $k > 0$ define

$$G_{2k}(\Lambda) = \sum_{\omega \in \Lambda \setminus \{0\}} \omega^{-2k}.$$

Also set

$$g_2(\Lambda) = 60\, G_4(\Lambda), \qquad g_3(\Lambda) = 140\, G_6(\Lambda).$$

Modular j-invariant

Let Λ be a complex lattice, the modular j-invariant is

$$j(\Lambda) = 1728 \frac{g_2(\Lambda)^3}{g_2(\Lambda)^3 - 27 g_3(\Lambda)^2}.$$

Two lattices Λ, Λ' are homothetic if and only if $j(\Lambda) = j(\Lambda')$.

Elliptic curves over $\mathbb{C}$

Weierstrass $\wp$ function

Let Λ be a complex lattice, the Weierstrass $\wp$ function associated to Λ is the series

$$\wp(z;\Lambda) = \frac{1}{z^2} + \sum_{\omega\in\Lambda\setminus\{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right).$$

Fix a lattice Λ, then $\wp$ and its derivative $\wp'$ are elliptic functions:

$$\wp(z+\omega) = \wp(z), \qquad \wp'(z+\omega) = \wp'(z)$$

for all $\omega \in \Lambda$.

Uniformization theorem

Let Λ be a complex lattice. The curve

$$E \ : \ y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$$

is an elliptic curve over $\mathbb{C}$. The map

$$\begin{aligned} \mathbb{C}/\Lambda &\to E(\mathbb{C}), \\ 0 &\mapsto (0 : 1 : 0), \\ z &\mapsto (\wp(z) : \wp'(z) : 1) \end{aligned}$$

is an isomorphism of Riemann surfaces and a group morphism.

Conversely, for any elliptic curve

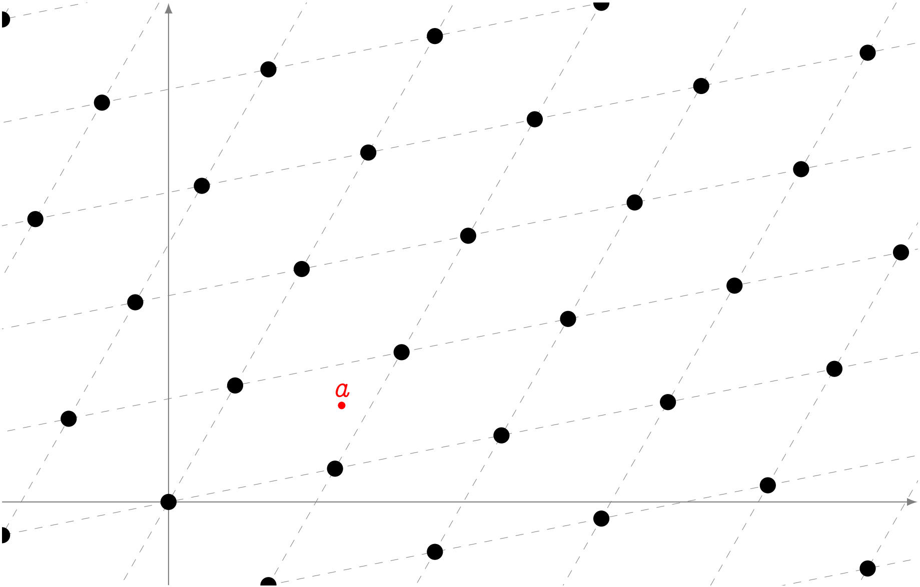
$$E \ : \ y^2 = x^3 + ax + b$$

there is a unique complex lattice Λ such that

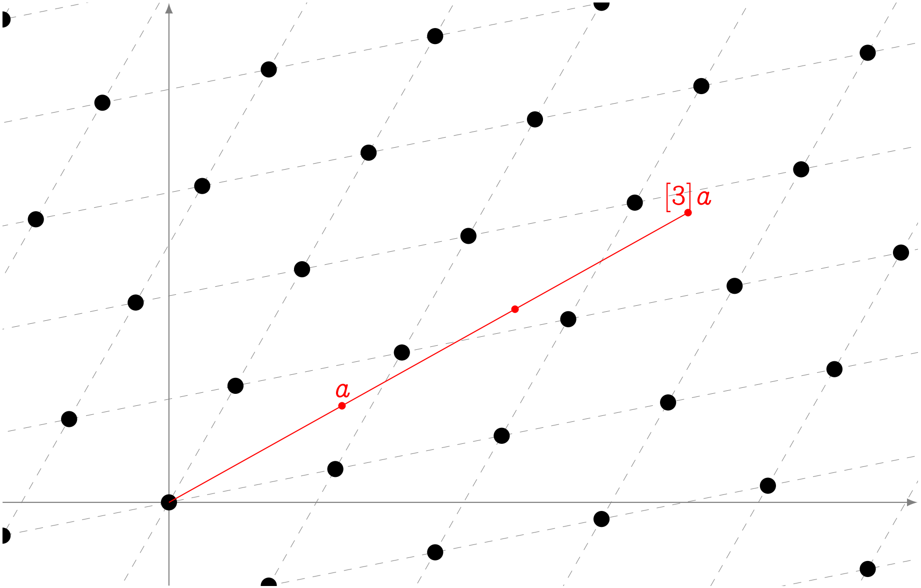
$$g_2(\Lambda) = -4a, \qquad g_3(\Lambda) = -4b.$$

Moreover $j(\Lambda) = j(E)$.

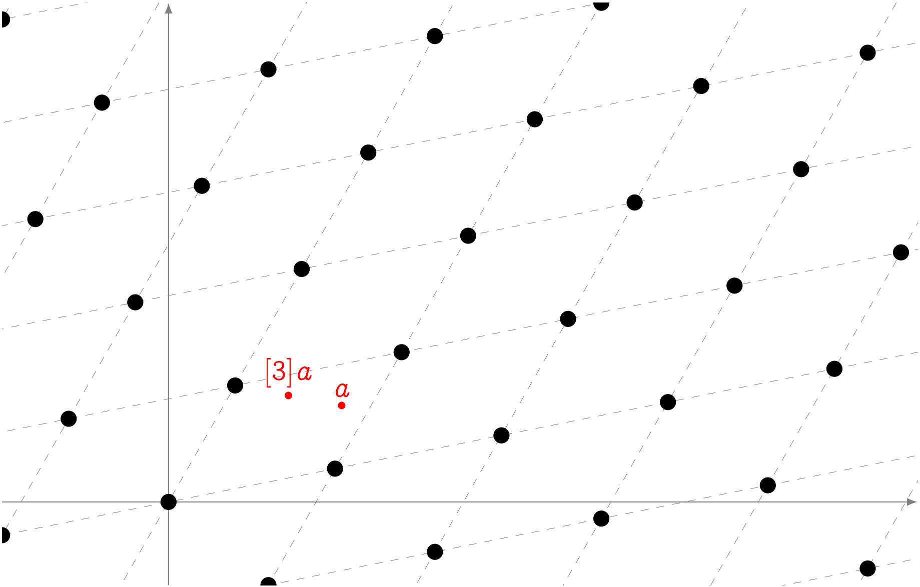
Multiplication



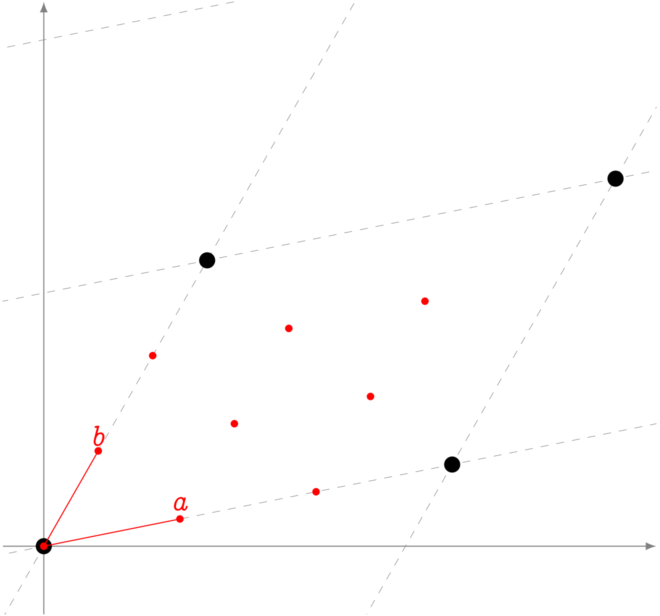
Multiplication



Multiplication



Torsion subgroups



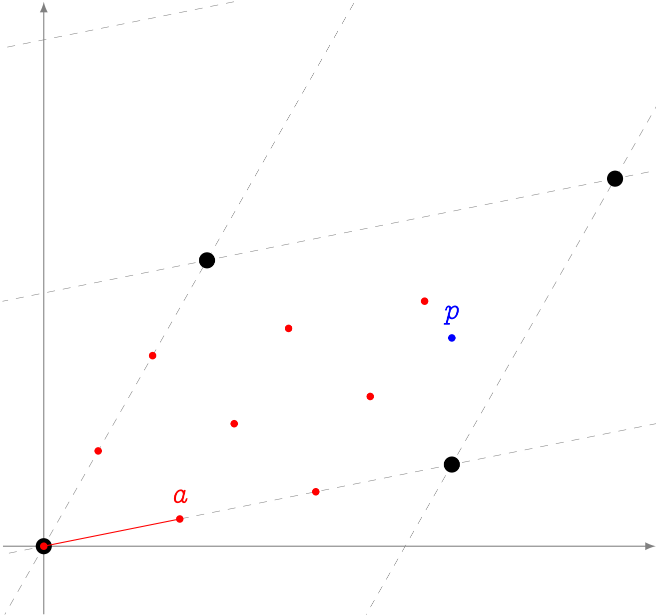
The ℓ-torsion subgroup is made up by the points

$$\left(\frac{i\omega_1}{\ell}, \frac{j\omega_2}{\ell}\right)$$

It is a group of rank two

$$E[\ell] = \langle a, b \rangle \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$$

Isogenies



Let $a \in \mathbb{C}/\Lambda_1$ be an ℓ-torsion point, and let

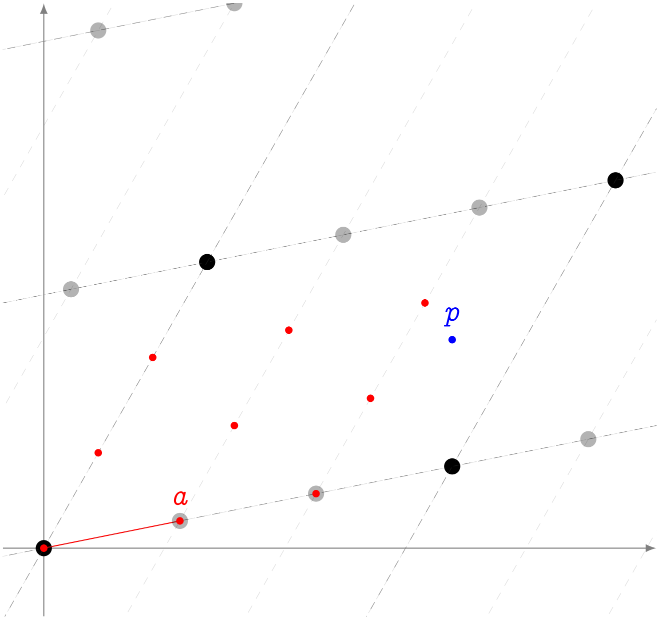
$$\Lambda_2 = a\mathbb{Z} \oplus \Lambda_1$$

Then $\Lambda_1 \subset \Lambda_2$ and we define a degree ℓ cover

$$\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$$

ϕ is a morphism of complex Lie groups and is called an isogeny.

Isogenies



Let $a \in \mathbb{C}/\Lambda_1$ be an ℓ-torsion point, and let

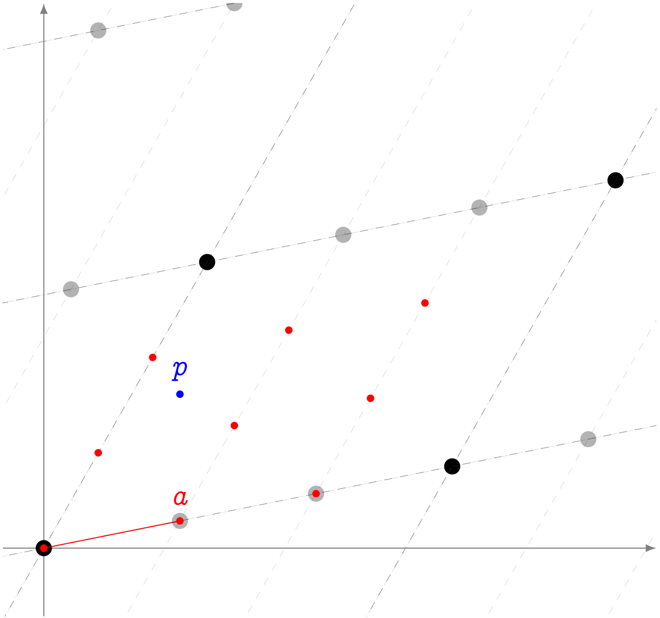
$$\Lambda_2 = a\mathbb{Z} \oplus \Lambda_1$$

Then $\Lambda_1 \subset \Lambda_2$ and we define a degree ℓ cover

$$\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$$

ϕ is a morphism of complex Lie groups and is called an isogeny.

Isogenies



Let $a \in \mathbb{C}/\Lambda_1$ be an ℓ-torsion point, and let

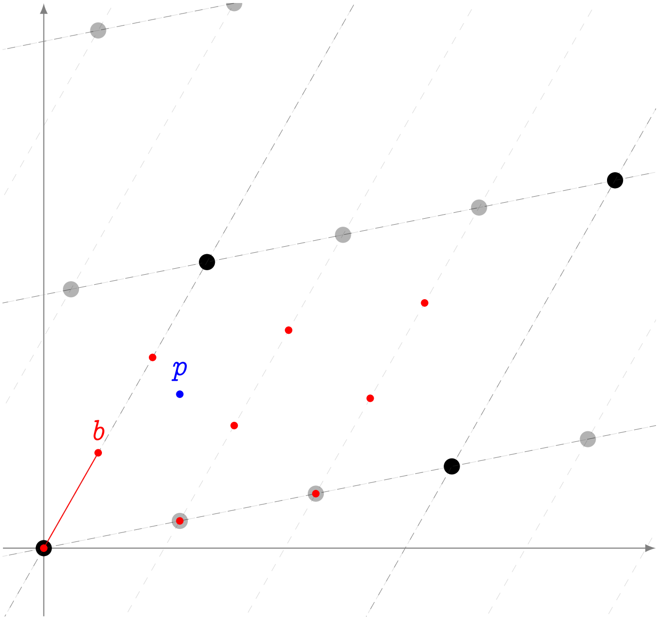
$$\Lambda_2 = a\mathbb{Z} \oplus \Lambda_1$$

Then $\Lambda_1 \subset \Lambda_2$ and we define a degree ℓ cover

$$\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$$

ϕ is a morphism of complex Lie groups and is called an isogeny.

Isogenies



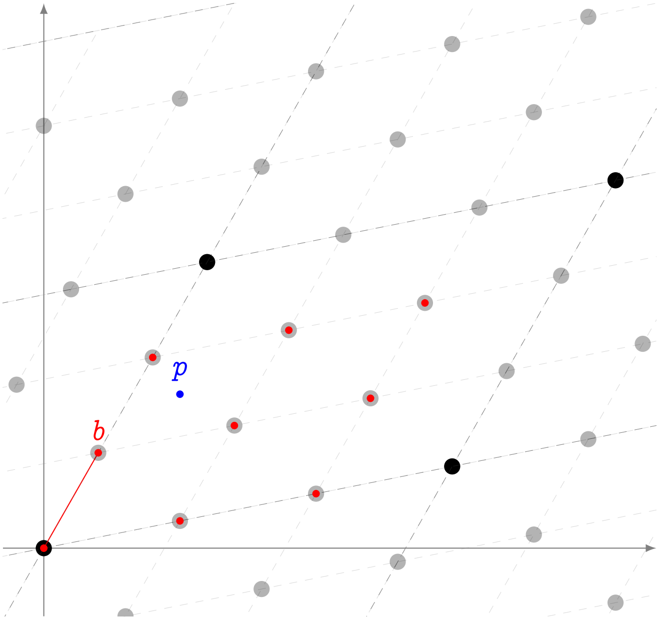
Taking a point b not in the kernel of ϕ, we obtain a new degree ℓ cover

$$\hat{\phi} : \mathbb{C}/\Lambda_2 \to \mathbb{C}/\Lambda_3$$

The composition $\hat{\phi} \circ \phi$ has degree ℓ^2 and is homothetic to the multiplication by ℓ map.

$\hat{\phi}$ is called the dual isogeny of ϕ.

Isogenies



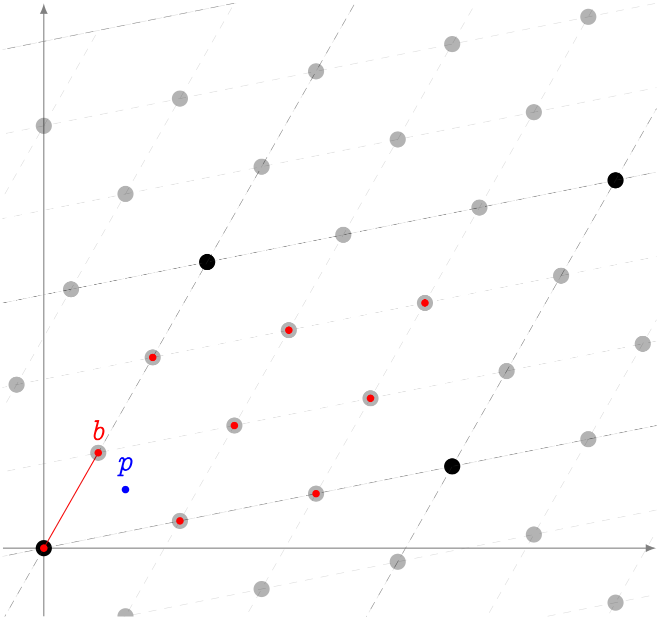
Taking a point b not in the kernel of ϕ, we obtain a new degree ℓ cover

$$\hat{\phi} : \mathbb{C}/\Lambda_2 \to \mathbb{C}/\Lambda_3$$

The composition $\hat{\phi} \circ \phi$ has degree ℓ^2 and is homothetic to the multiplication by ℓ map.

$\hat{\phi}$ is called the dual isogeny of ϕ.

Isogenies



Taking a point b not in the kernel of ϕ, we obtain a new degree ℓ cover

$$\hat{\phi} : \mathbb{C}/\Lambda_2 \to \mathbb{C}/\Lambda_3$$

The composition $\hat{\phi} \circ \phi$ has degree ℓ^2 and is homothetic to the multiplication by ℓ map.

$\hat{\phi}$ is called the dual isogeny of ϕ.

Isogenies: back to algebra

Let $\phi : E \to E'$ be an isogeny defined over a field k of characteristic p.

- $k(E)$ is the field of all rational functions from E to k;
- $\phi^* k(E')$ is the subfield of $k(E)$ defined as

$$\phi^* k(E') = \{f \circ \phi \mid f \in k(E')\}.$$

Degree, separability

1. The degree of ϕ is $\deg \phi = [k(E) : \phi^* k(E')]$. It is always finite.
2. ϕ is said to be separable, inseparable, or purely inseparable if the extension of function fields is.
3. If ϕ is separable, then $\deg \phi = \# \ker \phi$.
4. If ϕ is purely inseparable, then $\ker \phi = \{\mathcal{O}\}$ and $\deg \phi$ is a power of p.
5. Any isogeny can be decomposed as a product of a separable and a purely inseparable isogeny.

Isogenies: back to algebra

Let $\phi : E \to E'$ be an isogeny defined over a field k of characteristic p.

- $k(E)$ is the field of all rational functions from E to k;
- $\phi^* k(E')$ is the subfield of $k(E)$ defined as

$$\phi^* k(E') = \{f \circ \phi \mid f \in k(E')\}.$$

Degree, separability

1. The degree of ϕ is $\deg \phi = [k(E) : \phi^* k(E')]$. It is always finite.
2. ϕ is said to be separable, inseparable, or purely inseparable if the extension of function fields is.
3. If ϕ is separable, then $\deg \phi = \# \ker \phi$.
4. If ϕ is purely inseparable, then $\ker \phi = \{\mathcal{O}\}$ and $\deg \phi$ is a power of p.
5. Any isogeny can be decomposed as a product of a separable and a purely inseparable isogeny.

Isogenies: separable vs inseparable

Purely inseparable isogenies

Examples:

- The Frobenius endomorphism is purely inseparable of degree q.
- All purely inseparable maps in characteristic p are of the form $(X : Y : Z) \mapsto (X^{p^e} : Y^{p^e} : Z^{p^e})$.

Separable isogenies

Let E be an elliptic curve, and let G be a finite subgroup of E. There are a unique elliptic curve E' and a unique separable isogeny ϕ, such that $\ker\phi = G$ and $\phi : E \to E'$.
The curve E' is called the quotient of E by G and is denoted by E/G.

The dual isogeny

Let $\phi : E \to E'$ be an isogeny of degree m. There is a unique isogeny $\hat{\phi} : E' \to E$ such that

$$\hat{\phi} \circ \phi = [m]_E, \quad \phi \circ \hat{\phi} = [m]_{E'}.$$

$\hat{\phi}$ is called the dual isogeny of ϕ; it has the following properties:

1. $\hat{\phi}$ is defined over k if and only if ϕ is;
2. $\widehat{\psi \circ \phi} = \hat{\phi} \circ \hat{\psi}$ for any isogeny $\psi : E' \to E''$;
3. $\widehat{\psi + \phi} = \hat{\psi} + \hat{\phi}$ for any isogeny $\psi : E \to E'$;
4. $\deg \phi = \deg \hat{\phi}$;
5. $\hat{\hat{\phi}} = \phi$.

Algebras, orders

- A quadratic imaginary number field is an extension of $\mathbb{Q}$ of the form $Q[\sqrt{-D}]$ for some non-square $D > 0$.
- A quaternion algebra is an algebra of the form $\mathbb{Q} + \alpha\mathbb{Q} + \beta\mathbb{Q} + \alpha\beta\mathbb{Q}$, where the generators satisfy the relations

$$\alpha^2, \beta^2 \in \mathbb{Q}, \quad \alpha^2 < 0, \quad \beta^2 < 0, \quad \beta\alpha = -\alpha\beta.$$

Orders

Let K be a finitely generated $\mathbb{Q}$-algebra. An order $\mathcal{O} \subset K$ is a subring of K that is a finitely generated $\mathbb{Z}$-module of maximal dimension. An order that is not contained in any other order of K is called a maximal order.

Examples:

- $\mathbb{Z}$ is the only order contained in $\mathbb{Q}$,
- $\mathbb{Z}[i]$ is the only maximal order of $\mathbb{Q}(i)$,
- $\mathbb{Z}[\sqrt{5}]$ is a non-maximal order of $\mathbb{Q}(\sqrt{5})$,
- The ring of integers of a number field is its only maximal order,
- In general, maximal orders in quaternion algebras are not unique.

The endomorphism ring

The endomorphism ring $\mathrm{End}(E)$ of an elliptic curve E is the ring of all isogenies $E \to E$ (plus the null map) with addition and composition.

Theorem (Deuring)

Let E be an elliptic curve defined over a field k of characteristic p.
$\mathrm{End}(E)$ is isomorphic to one of the following:

- $\mathbb{Z}$, only if $p = 0$

  E is ordinary.

- An order $\mathcal{O}$ in a quadratic imaginary field:

  E is ordinary with complex multiplication by $\mathcal{O}$.

- Only if $p > 0$, a maximal order in a quaternion algebra[a]:

  E is supersingular.

[a](ramified at p and ∞)

The finite field case

Theorem (Hasse)

Let E be defined over a finite field. Its Frobenius endomorphism π satisfies a quadratic equation

$$\pi^2 - t\pi + q = 0$$

in $\mathrm{End}(E)$ for some $|t| \leq 2\sqrt{q}$, called the trace of π. The trace t is coprime to q if and only if E is ordinary.

Suppose E is ordinary, then $D_\pi = t^2 - 4q < 0$ is the discriminant of $\mathbb{Z}[\pi]$.

- $K = \mathbb{Q}(\pi) = \mathbb{Q}(\sqrt{D_\pi})$ is the endomorphism algebra of E.
- Denote by $\mathcal{O}_K$ its ring of integers, then

$$\mathbb{Z} \neq \mathbb{Z}[\pi] \subset \mathrm{End}(E) \subset \mathcal{O}_K.$$

In the supersingular case, π may or may not be in $\mathbb{Z}$, depending on q.

Endomorphism rings of ordinary curves

Classifying quadratic orders

Let K be a quadratic number field, and let $\mathcal{O}_K$ be its ring of integers.

- Any order $\mathcal{O} \subset K$ can be written as $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$ for an integer f, called the conductor of $\mathcal{O}$, denoted by $[\mathcal{O}_k : \mathcal{O}]$.
- If d_K is the discriminant of K, the discriminant of $\mathcal{O}$ is $f^2 d_K$.
- If $\mathcal{O}, \mathcal{O}'$ are two orders with discriminants d, d', then $\mathcal{O} \subset \mathcal{O}'$ iff $d' | d$.

$$\begin{tikzcd}
 & \mathcal{O}_K \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Z}+2\mathcal{O}_K \arrow[d, dash] \arrow[dr, dash] & \mathbb{Z}+3\mathcal{O}_K \arrow[dl, dash] \arrow[dr, dash] & \mathbb{Z}+5\mathcal{O}_K \arrow[dl, dash] \arrow[d, dash] \\
\mathbb{Z}+6\mathcal{O}_K \arrow[dr, dash] & \mathbb{Z}+10\mathcal{O}_K \arrow[d, dash] & \mathbb{Z}+15\mathcal{O}_K \arrow[dl, dash] \\
 & \mathbb{Z}[\pi] \simeq \mathbb{Z}+30\mathcal{O}_K &
\end{tikzcd}$$

Ideal lattices

Fractional ideals

Let $\mathcal{O}$ be an order of a number field K. A (fractional) $\mathcal{O}$-ideal $\mathfrak{a}$ is a finitely generated non-zero $\mathcal{O}$-submodule of K.

When K is imaginary quadratic:

- Fractional ideals are complex lattices,
- Any lattice $\Lambda \subset K$ is a fractional ideal,
- The order of a lattice Λ is

$$\mathcal{O}_\Lambda = \{\alpha \in K \mid \alpha\Lambda \subset \Lambda\}$$

Complex multiplication

Let $\Lambda \subset K$, the elliptic curve associated to $\mathbb{C}/\Lambda$ has complex multiplication by $\mathcal{O}_\Lambda$.

The class group

Let $\mathrm{End}(E) = \mathcal{O} \subset \mathbb{Q}(\sqrt{-D})$. Define

- $\mathcal{I}(\mathcal{O})$, the group of invertible fractional ideals,
- $\mathcal{P}(\mathcal{O})$, the group of principal ideals,

The class group

The class group of $\mathcal{O}$ is

$$\mathrm{Cl}(\mathcal{O}) = \mathcal{I}(\mathcal{O})/\mathcal{P}(\mathcal{O}).$$

- It is a finite abelian group.
- Its order $h(\mathcal{O})$ is called the class number of $\mathcal{O}$.
- It arises as the Galois group of an abelian extension of $\mathbb{Q}(\sqrt{-D})$.

Complex multiplication

Fundamental theorem of CM

Let $\mathcal{O}$ be an order of a number field K, and let $\mathfrak{a}_1, \dots, \mathfrak{a}_{h(\mathcal{O})}$ be representatives of $\mathrm{Cl}(\mathcal{O})$. Then:

- $K(j(\mathfrak{a}_i))$ is an Abelian extension of K;
- The $j(\mathfrak{a}_i)$ are all conjugate over K;
- The Galois group of $K(j(\mathfrak{a}_i))$ is isomorphic to $\mathrm{Cl}(\mathcal{O})$;
- $[\mathbb{Q}(j(\mathfrak{a}_i)) : \mathbb{Q}] = [K(j(\mathfrak{a}_i)) : K] = h(\mathcal{O})$;
- The $j(\mathfrak{a}_i)$ are integral, their minimal polynomial is called the Hilbert class polynomial of $\mathcal{O}$.

Lifting

Deuring's lifting theorem

Let E_0 be an elliptic curve in characteristic p, with an endomorphism ω_o which is not trivial. Then there exists an elliptic curve E defined over a number field L, an endomorphism ω of E, and a non-singular reduction of E at a place $\mathfrak{p}$ of L lying above p, such that E_0 is isomorphic to $E(\mathfrak{p})$, and ω_0 corresponds to $\omega(\mathfrak{p})$ under the isomorphism.

Executive summary

- Elliptic curves are algebraic groups;
- Isogenies are the natural notion of morphism for EC: both group and projective variety morphism;
- We can understand most things about isogenies by looking only at endomorphisms;
- Isogenies of curves over $\mathbb{C}$ are especially simple to describe;
- It is easy to construct curves over $\mathbb{C}$ with prescribed complex multiplication;
- Most of what happens in positive characteristic can be understood by:
  - looking at the Frobenius endomorphism, and/or
  - looking at reductions of curves in characteristic 0.

Plan

1. Elliptic curves, isogenies, complex multiplication
2. Isogeny graphs
3. Key exchange

Isogeny graphs

Serre-Tate theorem reloaded

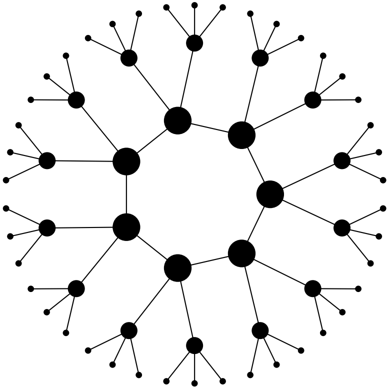
Two elliptic curves E, E' defined over a finite field are isogenous iff their endomorphism algebras $\mathrm{End}(E) \otimes \mathbb{Q}$ and $\mathrm{End}(E') \otimes \mathbb{Q}$ are isomorphic.

Isogeny graphs

- Vertices are curves up to isomorphism,
- Edges are isogenies up to isomorphism.

Isogeny volcanoes

- Curves are ordinary,
- Isogenies all have degree a prime ℓ.



What do isogeny graphs look like?

Torsion subgroups (ℓ prime)

In an algebraically closed field:

$$E[\ell] = \langle P, Q \rangle \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$$

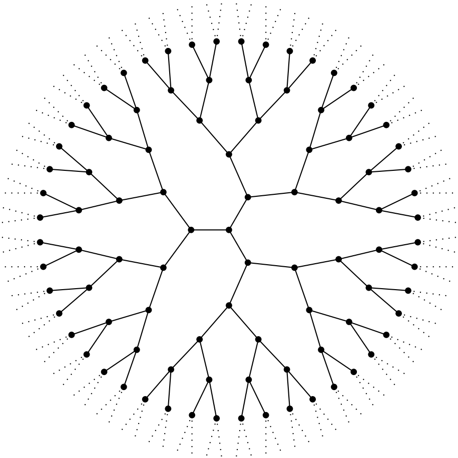
$$\Downarrow$$

There are exactly $\ell + 1$ cyclic subgroups $H \subset E$ of order ℓ:

$$\langle P + Q \rangle, \langle P + 2Q \rangle, \dots, \langle P \rangle, \langle Q \rangle$$

$$\Downarrow$$

There are exactly $\ell + 1$ distinct isogenies of degree ℓ.



(non-CM) 2-isogeny graph over $\mathbb{C}$

What happens over a finite field $\mathbb{F}_p$?

Rational isogenies ($\ell \neq p$)

In the algebraic closure $\bar{\mathbb{F}}_p$

$$E[\ell] = \langle P, Q \rangle \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$$

However, an isogeny is defined over $\mathbb{F}_p$ only if its kernel is Galois invariant.

Enter the Frobenius map

$$\begin{aligned} \pi : E &\longrightarrow E \\ (x, y) &\longmapsto (x^p, y^p) \end{aligned}$$

E is seen here as a curve over $\bar{\mathbb{F}}_p$.

The Frobenius action on $E[\ell]$

$$\begin{aligned} \pi(P) &= \quad aP + bQ \\ \pi(Q) &= \quad cP + dQ \end{aligned}$$

What happens over a finite field $\mathbb{F}_p$?

Rational isogenies ($\ell \neq p$)

In the algebraic closure $\bar{\mathbb{F}}_p$

$$E[\ell] = \langle P, Q\rangle \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$$

However, an isogeny is defined over $\mathbb{F}_p$ only if its kernel is Galois invariant.

Enter the Frobenius map

$$\begin{aligned}\pi : E &\longrightarrow E\\ (x, y) &\longmapsto (x^p, y^p)\end{aligned}$$

E is seen here as a curve over $\bar{\mathbb{F}}_p$.

The Frobenius action on $E[\ell]$

$$aP + bQ$$

$$cP + dQ$$

What happens over a finite field $\mathbb{F}_p$?

Rational isogenies ($\ell \neq p$)

In the algebraic closure $\bar{\mathbb{F}}_p$

$$E[\ell] = \langle P, Q \rangle \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$$

However, an isogeny is defined over $\mathbb{F}_p$ only if its kernel is Galois invariant.

Enter the Frobenius map

$$\begin{aligned} \pi : E &\longrightarrow E \\ (x, y) &\longmapsto (x^p, y^p) \end{aligned}$$

E is seen here as a curve over $\bar{\mathbb{F}}_p$.

The Frobenius action on $E[\ell]$

$$\begin{pmatrix} aP + bQ \\ cP + dQ \end{pmatrix}$$

What happens over a finite field $\mathbb{F}_p$?

Rational isogenies ($\ell \neq p$)

In the algebraic closure $\bar{\mathbb{F}}_p$

$$E[\ell] = \langle P, Q \rangle \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$$

However, an isogeny is defined over $\mathbb{F}_p$ only if its kernel is Galois invariant.

Enter the Frobenius map

$$\begin{aligned} \pi : E &\longrightarrow E \\ (x, y) &\longmapsto (x^p, y^p) \end{aligned}$$

E is seen here as a curve over $\bar{\mathbb{F}}_p$.

The Frobenius action on $E[\ell]$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

What happens over a finite field $\mathbb{F}_p$?

Rational isogenies ($\ell \neq p$)

In the algebraic closure $\bar{\mathbb{F}}_p$

$$E[\ell] = \langle P, Q \rangle \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$$

However, an isogeny is defined over $\mathbb{F}_p$ only if its kernel is Galois invariant.

Enter the Frobenius map

$$\begin{aligned} \pi : E &\longrightarrow E \\ (x, y) &\longmapsto (x^p, y^p) \end{aligned}$$

E is seen here as a curve over $\bar{\mathbb{F}}_p$.

The Frobenius action on $E[\ell]$

$$\pi : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \bmod \ell$$

What happens over a finite field $\mathbb{F}_p$?

Rational isogenies ($\ell \neq p$)

In the algebraic closure $\bar{\mathbb{F}}_p$

$$E[\ell] = \langle P, Q \rangle \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$$

However, an isogeny is defined over $\mathbb{F}_p$ only if its kernel is Galois invariant.

Enter the Frobenius map

$$\begin{aligned} \pi : E &\longrightarrow E \\ (x, y) &\longmapsto (x^p, y^p) \end{aligned}$$

E is seen here as a curve over $\bar{\mathbb{F}}_p$.

The Frobenius action on $E[\ell]$

$$\pi : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \bmod \ell$$

We identify $\pi|E[\ell]$ to a conjugacy class in $\mathrm{GL}(\mathbb{Z}/\ell\mathbb{Z})$.

What happens over a finite field $\mathbb{F}_p$?

Galois invariant subgroups of $E[\ell]$

=

eigenspaces of $\pi \in \mathrm{GL}(\mathbb{Z}/\ell\mathbb{Z})$

=

rational isogenies of degree ℓ

What happens over a finite field $\mathbb{F}_p$?

Galois invariant subgroups of $E[\ell]$

=

eigenspaces of $\pi \in \mathrm{GL}(\mathbb{Z}/\ell\mathbb{Z})$

=

rational isogenies of degree ℓ

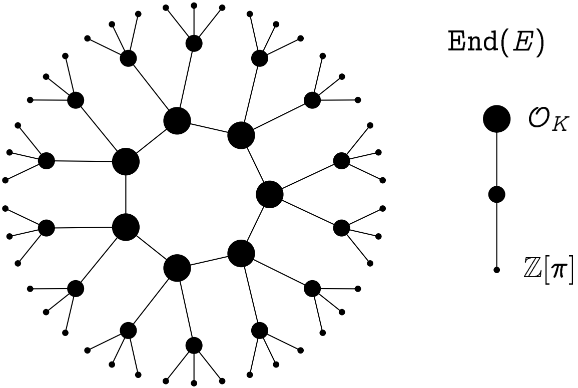
How many Galois invariant subgroups?

- $\pi|E[\ell] \sim \left(\begin{smallmatrix}\lambda & 0\\ 0 & \lambda\end{smallmatrix}\right)$ $\rightarrow$ $\ell + 1$ isogenies
- $\pi|E[\ell] \sim \begin{pmatrix}\lambda & 0\\ 0 & \mu\end{pmatrix}$ with $\lambda \neq \mu$ $\rightarrow$ two isogenies
- $\pi|E[\ell] \sim \left(\begin{smallmatrix}\lambda & *\\ 0 & \lambda\end{smallmatrix}\right)$ $\rightarrow$ one isogeny
- $\pi|E[\ell]$ is not diagonalizable over $\mathbb{Z}/\ell\mathbb{Z}$ $\rightarrow$ no isogeny

Volcanology (Kohel 1996)

Let E, E' be curves with respective endomorphism rings $\mathcal{O}, \mathcal{O}' \subset K$.
Let $\phi : E \to E'$ be an isogeny of prime degree ℓ, then:

if $\mathcal{O} = \mathcal{O}'$, ϕ is horizontal;
if $[\mathcal{O}' : \mathcal{O}] = \ell$, ϕ is ascending;
if $[\mathcal{O} : \mathcal{O}'] = \ell$, ϕ is descending.

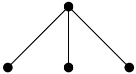


Ordinary isogeny volcano of degree $\ell = 3$.

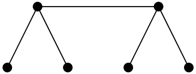
Volcanology (Kohel 1996)

Let E be ordinary,
$\mathrm{End}(E) \subset K$.

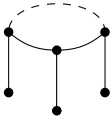
$\mathcal{O}_K$: maximal order of K,
D_K: discriminant of K.



$\left(\frac{D_K}{\ell}\right) = -1$



$\left(\frac{D_K}{\ell}\right) = 0$



$\left(\frac{D_K}{\ell}\right) = +1$

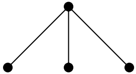
		Horizontal	Ascending	Descending
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$	$1 + \left(\frac{D_K}{\ell}\right)$		
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O} : \mathbb{Z}[\pi]]$	$1 + \left(\frac{D_K}{\ell}\right)$		$\ell - \left(\frac{D_K}{\ell}\right)$
$\ell \mid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O} : \mathbb{Z}[\pi]]$		1	ℓ
$\ell \mid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$		1	

Volcanology (Kohel 1996)

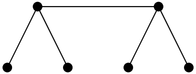
Let E be ordinary,
$\mathtt{End}(E) \subset K$.

$\mathcal{O}_K$: maximal order of K,
D_K: discriminant of K.

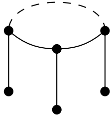
Height $= v_\ell([\mathcal{O}_K : \mathbb{Z}[\pi]])$.



$\left(\frac{D_K}{\ell}\right) = -1$



$\left(\frac{D_K}{\ell}\right) = 0$



$\left(\frac{D_K}{\ell}\right) = +1$

		Horizontal	Ascending	Descending
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$	$1 + \left(\frac{D_K}{\ell}\right)$		
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O} : \mathbb{Z}[\pi]]$	$1 + \left(\frac{D_K}{\ell}\right)$		$\ell - \left(\frac{D_K}{\ell}\right)$
$\ell \mid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O} : \mathbb{Z}[\pi]]$		1	ℓ
$\ell \mid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$		1	

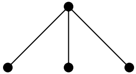
Volcanology (Kohel 1996)

Let E be ordinary,
$\mathrm{End}(E) \subset K$.

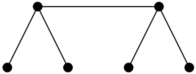
$\mathcal{O}_K$: maximal order of K,
D_K: discriminant of K.

Height $= v_\ell([\mathcal{O}_K : \mathbb{Z}[\pi]])$.

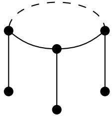
How large is the crater?



$\left(\frac{D_K}{\ell}\right) = -1$



$\left(\frac{D_K}{\ell}\right) = 0$



$\left(\frac{D_K}{\ell}\right) = +1$

		Horizontal	Ascending	Descending
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$	$1 + \left(\frac{D_K}{\ell}\right)$		
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O} : \mathbb{Z}[\pi]]$	$1 + \left(\frac{D_K}{\ell}\right)$		$\ell - \left(\frac{D_K}{\ell}\right)$
$\ell \mid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O} : \mathbb{Z}[\pi]]$		1	ℓ
$\ell \mid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$		1	

How large is the crater of a volcano?

Let $\mathrm{End}(E) = \mathcal{O} \subset \mathbb{Q}(\sqrt{-D})$. Define

- $\mathcal{I}(\mathcal{O})$, the group of invertible fractional ideals,
- $\mathcal{P}(\mathcal{O})$, the group of principal ideals,

The class group

The class group of $\mathcal{O}$ is

$$\mathrm{Cl}(\mathcal{O}) = \mathcal{I}(\mathcal{O})/\mathcal{P}(\mathcal{O}).$$

- It is a finite abelian group.
- Its order $h(\mathcal{O})$ is called the class number of $\mathcal{O}$.
- It arises as the Galois group of an abelian extension of $\mathbb{Q}(\sqrt{-D})$.

Complex multiplication

The $\mathfrak{a}$-torsion

- Let $\mathfrak{a} \subset \mathcal{O}$ be an (integral invertible) ideal of $\mathcal{O}$;
- Let $E[\mathfrak{a}]$ be the subgroup of E annihilated by $\mathfrak{a}$:

$$E[\mathfrak{a}] = \{P \in E \mid \alpha(P) = 0 \text{ for all } \alpha \in \mathfrak{a}\};$$

- Let $\phi : E \to E_{\mathfrak{a}}$, where $E_{\mathfrak{a}} = E/E[\mathfrak{a}]$.

Then $\mathrm{End}(E_{\mathfrak{a}}) = \mathcal{O}$ (i.e., ϕ is horizontal).

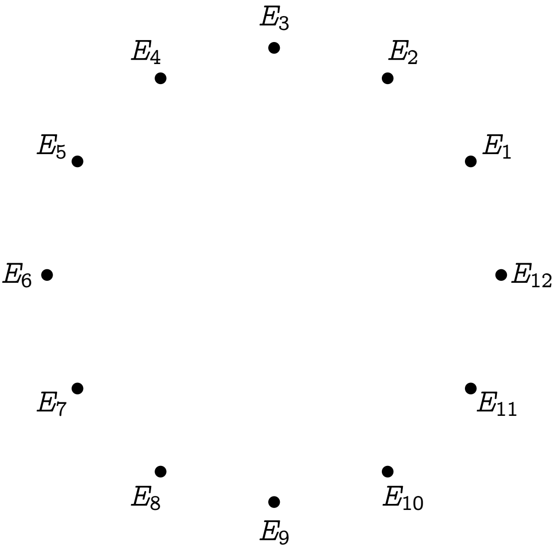
Theorem (Complex multiplication)

The action on the set of elliptic curves with complex multiplication by $\mathcal{O}$ defined by $\mathfrak{a} * j(E) = j(E_{\mathfrak{a}})$ factors through $\mathrm{Cl}(\mathcal{O})$, is faithful and transitive.

Corollary

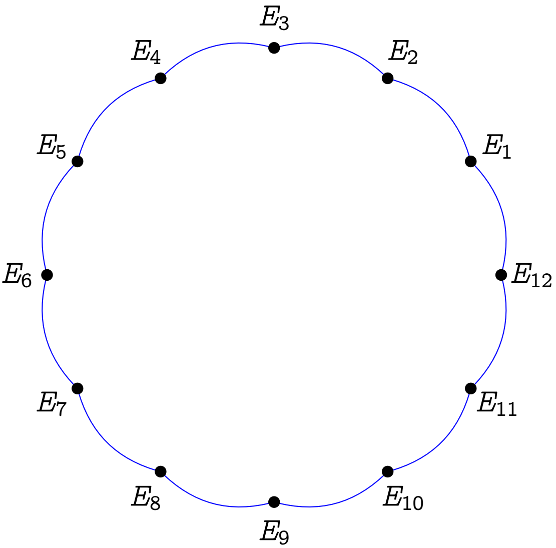
Let $\mathrm{End}(E)$ have discriminant D. Assume that $\left(\frac{D}{\ell}\right) = 1$, then E is on a crater of size N of an ℓ-volcano, and $N | h(\mathrm{End}(E))$

Complex multiplication graphs



Vertices are elliptic curves with complex multiplication by $\mathcal{O}_K$ (i.e., $\mathtt{End}(E) \simeq \mathcal{O}_K \subset \mathbb{Q}(\sqrt{-D})$).

Complex multiplication graphs

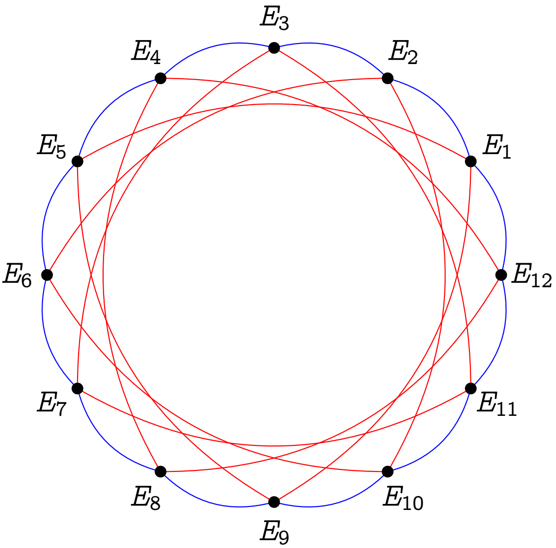


Vertices are elliptic curves with complex multiplication by $\mathcal{O}_K$ (i.e., $\mathrm{End}(E) \simeq \mathcal{O}_K \subset \mathbb{Q}(\sqrt{-D})$).

Edges are horizontal isogenies of bounded prime degree.

— degree 2

Complex multiplication graphs



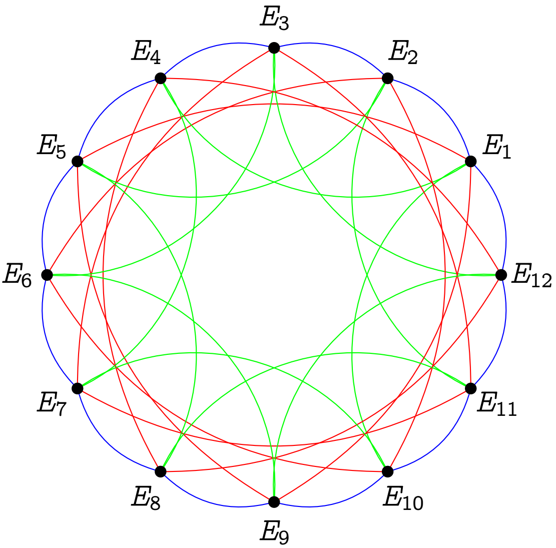
Vertices are elliptic curves with complex multiplication by $\mathcal{O}_K$ (i.e., $\mathrm{End}(E) \simeq \mathcal{O}_K \subset \mathbb{Q}(\sqrt{-D})$).

Edges are horizontal isogenies of bounded prime degree.

— degree 2

— degree 3

Complex multiplication graphs



Vertices are elliptic curves with complex multiplication by $\mathcal{O}_K$ (i.e., $\mathtt{End}(E) \simeq \mathcal{O}_K \subset \mathbb{Q}(\sqrt{-D})$).

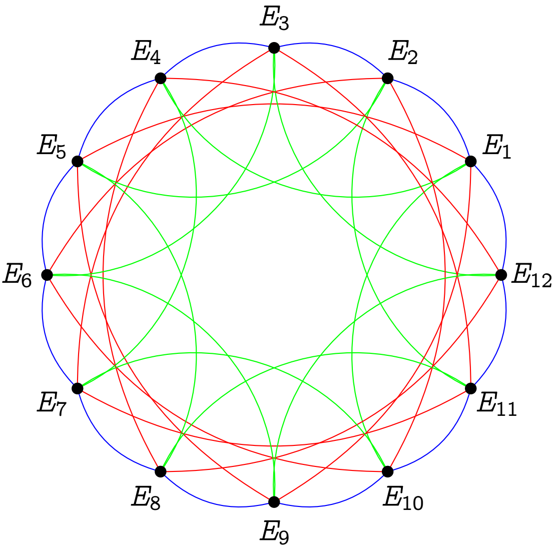
Edges are horizontal isogenies of bounded prime degree.

— degree 2

— degree 3

— degree 5

Complex multiplication graphs



Vertices are elliptic curves with complex multiplication by $\mathcal{O}_K$ (i.e., $\mathtt{End}(E) \simeq \mathcal{O}_K \subset \mathbb{Q}(\sqrt{-D})$).

Edges are horizontal isogenies of bounded prime degree.

— degree 2

— degree 3

— degree 5

Isomorphic to a Cayley graph of $\mathtt{Cl}(\mathcal{O}_K)$.

Supersingular endomorphisms

Recall, a curve E over a field $\mathbb{F}_q$ of characteristic p is supersingular iff

$$\pi^2 - t\pi + q = 0$$

with $t = 0 \mod p$.

Case: $t = 0 \quad \Rightarrow \quad D_\pi = -4q$

- Only possibility for $E/\mathbb{F}_p$,
- $E/\mathbb{F}_p$ has CM by an order of $\mathbb{Q}(\sqrt{-p})$, similar to the ordinary case.

Case: $t = \pm 2\sqrt{q} \quad \Rightarrow \quad D_\pi = 0$

- General case for $E/\mathbb{F}_q$, when q is an even power.
- $\pi = \pm\sqrt{q}$, hence no complex multiplication.

We will ignore marginal cases: $t = \pm\sqrt{q}, \pm\sqrt{2q}, \pm\sqrt{3q}$.

Supersingular complex multiplication

Let $E/\mathbb{F}_p$ be a supersingular curve, then $\pi^2 = -p$, and

$$\pi = \begin{pmatrix} \sqrt{-p} & 0 \\ 0 & -\sqrt{-p} \end{pmatrix} \mod \ell$$

for any ℓ s.t. $\left(\frac{-p}{\ell}\right) = 1$.

Theorem (Delfs and Galbraith 2016)

Let $\mathrm{End}_{\mathbb{F}_p}(E)$ denote the ring of $\mathbb{F}_p$-rational endomorphisms of E. Then

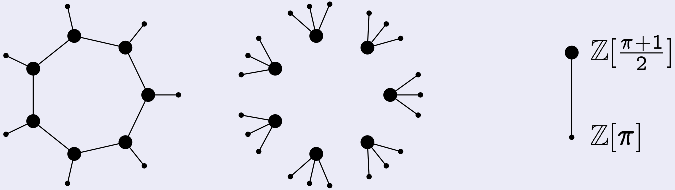
$$\mathbb{Z}[\pi] \subset \mathrm{End}_{\mathbb{F}_p}(E) \subset \mathbb{Q}(\sqrt{-p}).$$

Orders of $\mathbb{Q}(\sqrt{-p})$

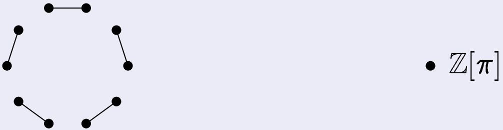
- If $p = 1 \mod 4$, then $\mathbb{Z}[\pi]$ is the maximal order.
- If $p = -1 \mod 4$, then $\mathbb{Z}[\frac{\pi+1}{2}]$ is the maximal order, and $[\mathbb{Z}[\frac{\pi+1}{2}] : \mathbb{Z}[\pi]] = 2$.

Supersingular CM graphs

2-volcanoes, $p = -1 \bmod 4$



2-graphs, $p = 1 \bmod 4$



All other ℓ-graphs are cycles of horizontal isogenies iff $\left(\frac{-p}{\ell}\right) = 1$.

The full endomorphism ring

Theorem (Deuring)

Let E be a supersingular elliptic curve, then

- E is isomorphic to a curve defined over $\mathbb{F}_{p^2}$;
- Every isogeny of E is defined over $\mathbb{F}_{p^2}$;
- Every endomorphism of E is defined over $\mathbb{F}_{p^2}$;
- $\mathrm{End}(E)$ is isomorphic to a maximal order in a quaternion algebra ramified at p and ∞.

In particular:

- If E is defined over $\mathbb{F}_p$, then $\mathrm{End}_{\mathbb{F}_p}(E)$ is strictly contained in $\mathrm{End}(E)$.
- Some endomorphisms do not commute!

An example

The curve of j-invariant 1728

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

is supersingular over $\mathbb{F}_p$ iff $p = -1 \mod 4$.

Endomorphisms

$\mathrm{End}(E) = \mathbb{Z}\langle\iota, \pi\rangle$, with:

- π the Frobenius endomorphism, s.t. $\pi^2 = -p$;
- ι the map

  $$\iota(x, y) = (-x, iy),$$

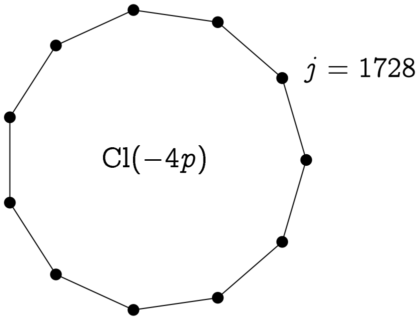
  where $i \in \mathbb{F}_{p^2}$ is a 4-th root of unity. Clearly, $\iota^2 = -1$.

And $\iota\pi = -\pi\iota$.

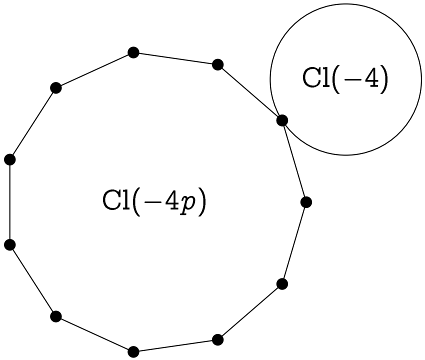
Class group action party

• $j = 1728$

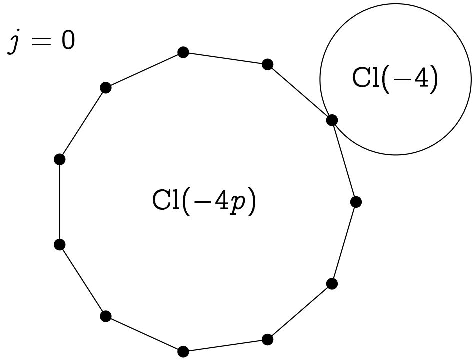
Class group action party



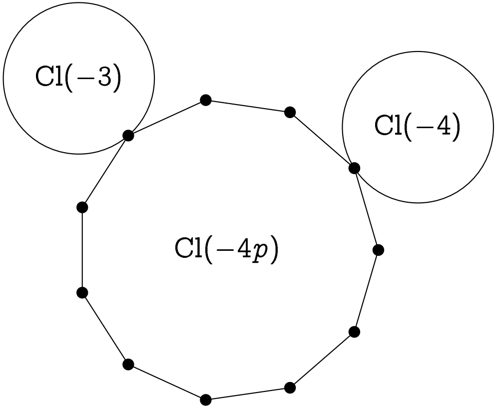
Class group action party



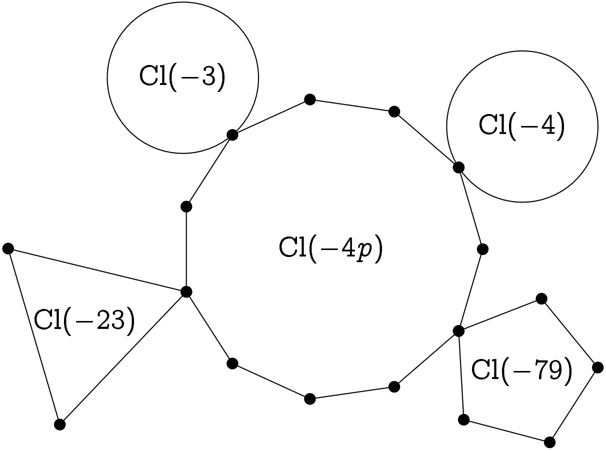
Class group action party



Class group action party



Class group action party



Quaternion algebra?! WTF?[2]

The quaternion algebra $B_{p,\infty}$ is:

- A 4-dimensional $\mathbb{Q}$-vector space with basis $(1, i, j, k)$.
- A non-commutative division algebra[1] $B_{p,\infty} = \mathbb{Q}\langle i, j\rangle$ with the relations:
$$i^2 = a, \quad j^2 = -p, \quad ij = -ji = k,$$
for some $a < 0$ (depending on p).
- All elements of $B_{p,\infty}$ are quadratic algebraic numbers.
- $B_{p,\infty} \otimes \mathbb{Q}_\ell \simeq \mathcal{M}_{2\times 2}(\mathbb{Q}_\ell)$ for all $\ell \neq p$.
I.e., endomorphisms restricted to $E[\ell^e]$ are just 2×2 matrices mod ℓ^e.
- $B_{p,\infty} \otimes \mathbb{R}$ is isomorphic to Hamilton's quaternions.
- $B_{p,\infty} \otimes \mathbb{Q}_p$ is a division algebra.

[1] All elements have inverses.
[2] What The Field?

Supersingular graphs

- Quaternion algebras have many maximal orders.
- For every maximal order type of $B_{p,\infty}$ there are 1 or 2 curves over $\mathbb{F}_{p^2}$ having endomorphism ring isomorphic to it.
- There is a unique isogeny class of supersingular curves over $\bar{\mathbb{F}}_p$ of size $\approx p/12$.
- Left ideals act on the set of maximal orders like isogenies.
- The graph of ℓ-isogenies is $(\ell + 1)$-regular.

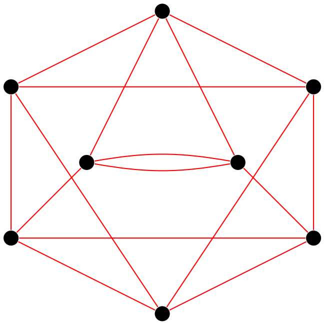


Figure: 3-isogeny graph on $\mathbb{F}_{97^2}$.

Graphs lexicon

Degree: Number of (outgoing/ingoing) edges.

k-regular: All vertices have degree k.

Connected: There is a path between any two vertices.

Distance: The length of the shortest path between two vertices.

Diamater: The longest distance between two vertices.

$\lambda_1 \geq \cdots \geq \lambda_n$: The (ordered) eigenvalues of the adjacency matrix.

Expander graphs

Proposition

If G is a k-regular graph, its largest and smallest eigenvalues satisfy

$$k = \lambda_1 \geq \lambda_n \geq -k.$$

Expander families

An infinite family of connected k-regular graphs on n vertices is an expander family if there exists an $\epsilon > 0$ such that all non-trivial eigenvalues satisfy $|\lambda| \leq (1 - \epsilon)k$ for n large enough.

- Expander graphs have short diameter ($O(\log n)$);
- Random walks mix rapidly (after $O(\log n)$ steps, the induced distribution on the vertices is close to uniform).

Expander graphs from isogenies

Theorem (Pizer 1990, 1998)

Let ℓ be fixed. The family of graphs of supersingular curves over $\mathbb{F}_{p^2}$ with ℓ-isogenies, as $p \to \infty$, is an expander family[a].

[a] Even better, it has the Ramanujan property.

Theorem (Jao, Miller, and Venkatesan 2009)

Let $\mathcal{O} \subset \mathbb{Q}(\sqrt{-D})$ be an order in a quadratic imaginary field. The graphs of all curves over $\mathbb{F}_q$ with complex multiplication by $\mathcal{O}$, with isogenies of prime degree bounded[a] by $(\log q)^{2+\delta}$, are expanders.

[a] May contain traces of GRH.

Executive summary

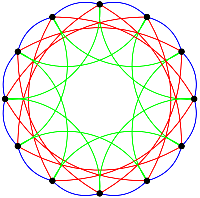
- Separable ℓ-isogeny = finite kernel = subgroup of $E[\ell]$,
  - eigenspace of π iff $\mathbb{F}_q$-rational,
  - distinct eigenvalues $\lambda \neq \mu$ define distinct directions on the crater.
- Isogeny graphs have j-invariants for vertices and “some” isogenies for edges.
- By varying the choices for the vertex and the isogeny set, we obtain graphs with different properties.
- ℓ-isogeny graphs of ordinary curves are volcanoes, (full) ℓ-isogeny graphs of supersingular curves are finite $(\ell + 1)$-regular.
- CM theory naturally leads to define graphs of horizontal isogenies (both in the ordinary and the supersingular case) that are isomorphic to Cayley graphs of class groups.
- CM graphs are expanders. Supseringular full ℓ-isogeny graphs are Ramanujan.

Plan

1. Elliptic curves, isogenies, complex multiplication
2. Isogeny graphs
3. Key exchange

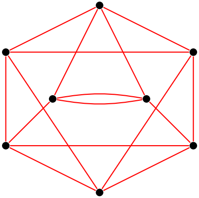
Isogeny graphs taxonomy

Complex Multiplication (CM) graphs



- Ordinary / Supersingular ($\mathbb{F}_p$)
- Superposition of isogeny cycles (one color per degree)
- Isomorphic to Cayley graph of a quadratic class group
- Large automorphism group
- Typical size $O(\sqrt{p})$
- Used in: **CSIDH**

Full **supersingular graphs**



- Supersingular ($\mathbb{F}_{p^2}$)
- One isogeny degree
- $(\ell + 1)$-regular
- Tiny automorphism group
- Size $\approx p/12$
- Used in: **SIDH**

Diffie–Hellman key exchange

Goal: Alice and Bob have never met before. They are chatting over a public channel, and want to agree on a shared secret to start a private conversation.

Setup: They agree on a (large) cyclic group $G = \langle g \rangle$ of order N.

Alice		**Bob**
pick random $a \in \mathbb{Z}/N\mathbb{Z}$		pick random $b \in \mathbb{Z}/N\mathbb{Z}$
compute $A = g^a$		compute $B = g^b$
	$\xrightarrow{\quad A \quad}$	
	$\xleftarrow[\quad B \quad]{}$	

Shared secret is $B^a = g^{ab} = A^b$

Brief history of DH key exchange

1976 Diffie & Hellman publish New directions in cryptography, suggest using $G = \mathbb{F}_p^*$.

1978 Pollard publishes his discrete logarithm algorithm ($O(\sqrt{\#G})$ complexity).

1980 Miller and Koblitz independently suggest using elliptic curves $G = E(\mathbb{F}_p)$.

1994 Shor publishes his quantum discrete logarithm / factoring algorithm.

2005 NSA standardizes elliptic curve key agreement (ECDH) and signatures ECDSA.

2017 $\sim$ 70% of web traffic is secured by ECDH and/or ECDSA.

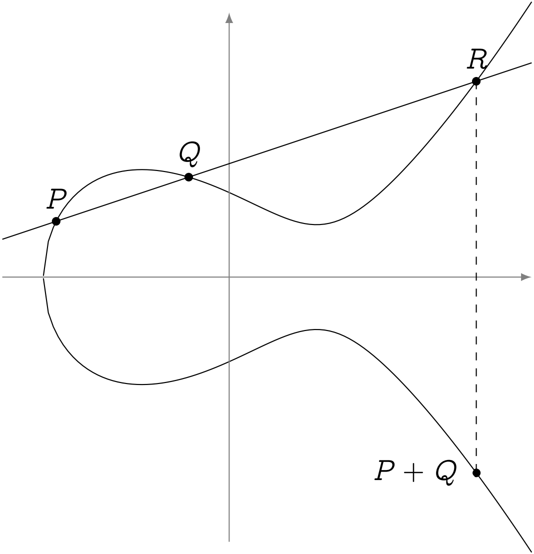
2017 NIST launches post-quantum competition, says “not to bother moving to elliptic curves, if you haven’t yet”.

History of isogeny-based cryptography

- **1996** Couveignes introduces the Hard Homogeneous Spaces. His work stays unpublished for 10 years.
- **2006** Rostovtsev & Stolbunov independently rediscover Couveignes ideas, suggest isogeny-based Diffie–Hellman as a quantum-resistant primitive.
- **2006-2010** Other isogeny-based protocols by Teske and Charles, Goren & Lauter.
- **2011-2012** D., Jao & Plût introduce SIDH, an efficient post-quantum key exchange inspired by Couveignes, Rostovtsev, Stolbunov, Charles, Goren, Lauter.
- **2017** SIDH is submitted to the NIST competition (with the name SIKE, only isogeny-based candidate).
- **2018** D., Kieffer & Smith *resurrect* the Couveignes–Rostovtsev–Stolbunov protocol, Castryck, Lange, Martindale, Panny & Renes publish an efficient variant named CSIDH.

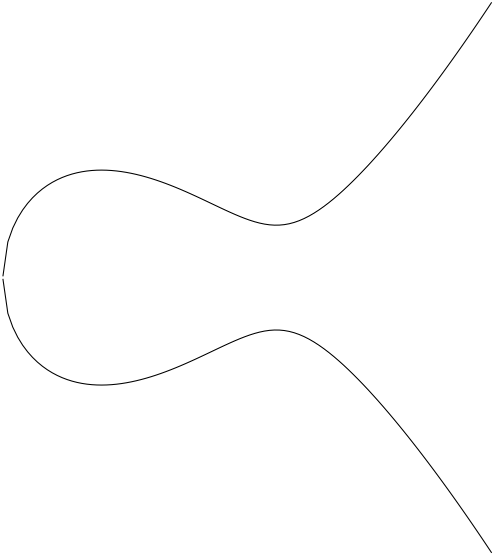
Elliptic curves

Let $E\ :\ y^2 = x^3 + ax + b$ be an elliptic curve...



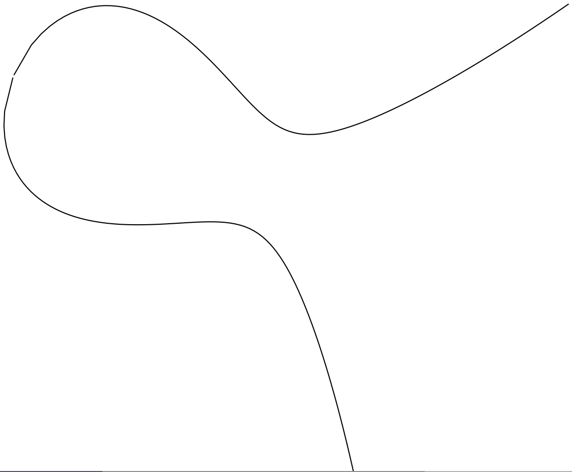
Elliptic curves

Let $E : y^2 = x^3 + ax + b$ be an elliptic curve…



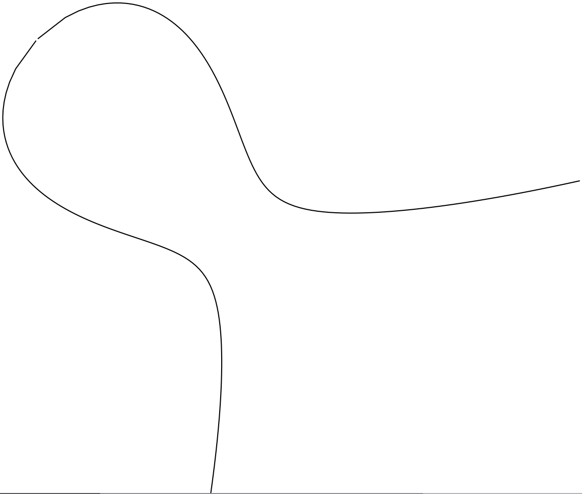
Elliptic curves

Let $E : y^2 = x^3 + ax + b$ be an elliptic curve…



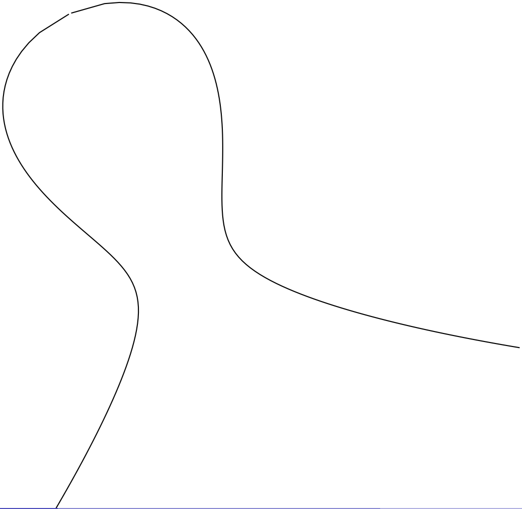
Elliptic curves

Let $E\ :\ y^2 = x^3 + ax + b$ be an elliptic curve…



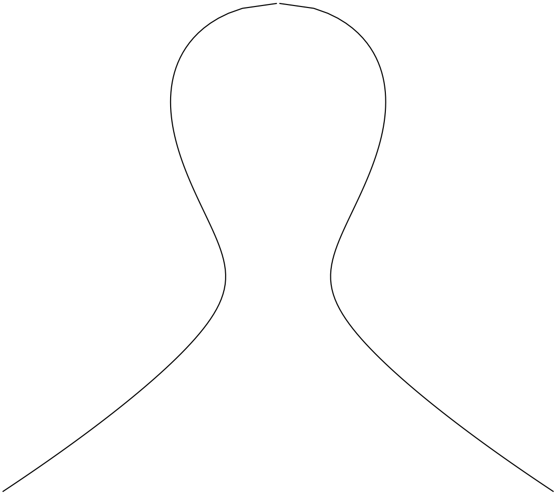
Elliptic curves

Let $E\ :\ y^2 = x^3 + ax + b$ be an elliptic curve…



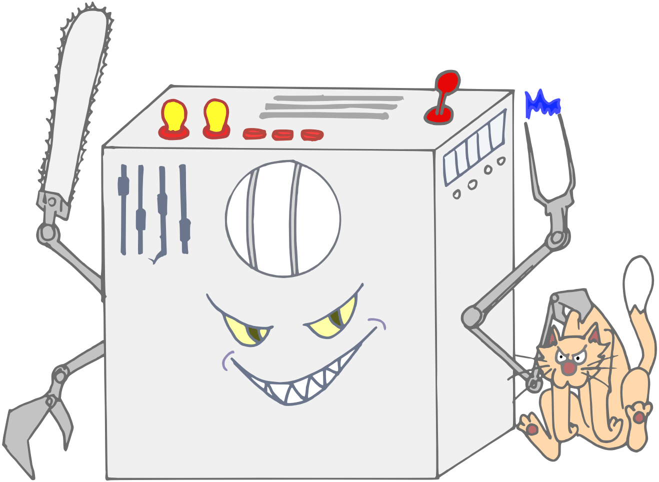
Elliptic curves

Let $E : y^2 = x^3 + ax + b$ be an elliptic curve…

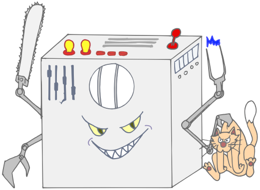


Elliptic curves

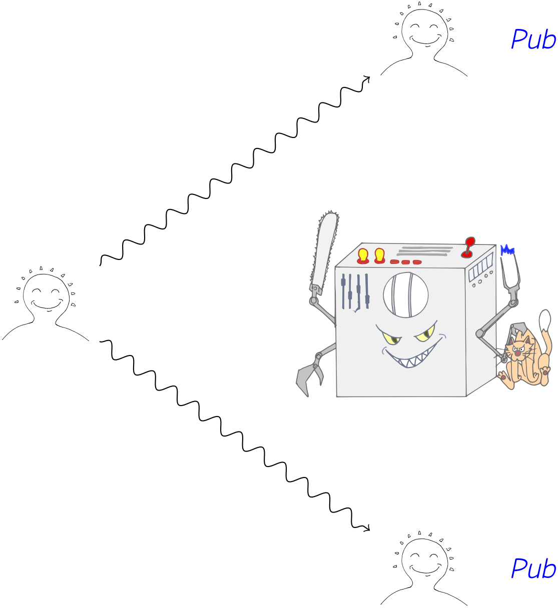
The QUANTHOM Menace



Basically every isogeny-based protocol...



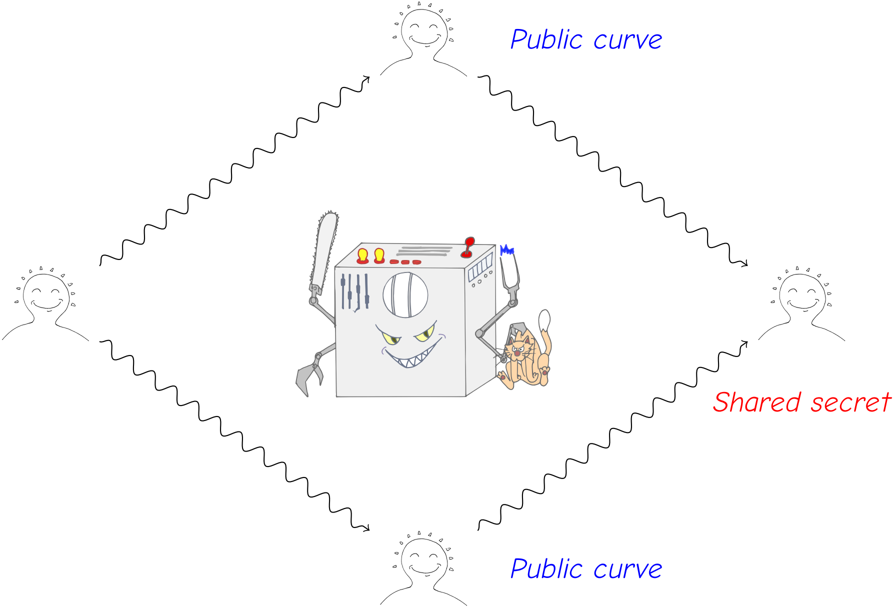
Basically every isogeny-based protocol...



Public curve

Public curve

Basically every isogeny-based protocol...



Computing Isogenies

Vélu's formulas

Input: A subgroup $H \subset E$,

Output: The isogeny $\phi : E \to E/H$.

Complexity: $O(\ell)$ — Vélu 1971, …

Why?
- Evaluate isogeny on points $P \in E$;
- Walk in isogeny graphs.

Computing Isogenies

Vélu's formulas

Input: A subgroup $H \subset E$,

Output: The isogeny $\phi : E \to E/H$.

Complexity: $O(\ell)$ — Vélu 1971, ...

Why?
- Evaluate isogeny on points $P \in E$;
- Walk in isogeny graphs.

Explicit Isogeny Problem

Input: Curve E, (prime) integer ℓ

Output: All subgroups $H \subset E$ of order ℓ.

Complexity: $\tilde{O}(\ell^2)$ — Elkies 1992

Why?
- List all isogenies of given degree;
- Count points of elliptic curves;
- Compute endomorphism rings of elliptic curves;
- Walk in isogeny graphs.

Computing Isogenies

Explicit Isogeny Problem (2)

Input: Curves E, E', isogenous of degree ℓ.

Output: The isogeny $\phi : E \to E'$ of degree ℓ.

Complexity: $O(\ell^2)$ — Elkies 1992; Couveignes 1996; Lercier and Sirvent 2008; De Feo 2011; De Feo, Hugounenq, Plût, and Schost 2016; Lairez and Vaccon 2016, …

Why?

- Count points of elliptic curves.

Computing Isogenies

Explicit Isogeny Problem (2)

Input: Curves E, E', isogenous of degree ℓ.

Output: The isogeny $\phi : E \to E'$ of degree ℓ.

Complexity: $O(\ell^2)$ — Elkies 1992; Couveignes 1996; Lercier and Sirvent 2008; De Feo 2011; De Feo, Hugounenq, Plût, and Schost 2016; Lairez and Vaccon 2016, …

Why?
- Count points of elliptic curves.

Isogeny Walk Problem

Input: Isogenous curves E, E'.

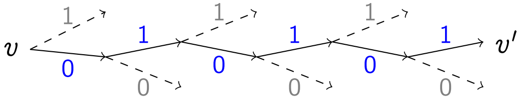
Output: An isogeny $\phi : E \to E'$ of smooth degree.

Complexity: Generically hard — Galbraith, Hess, and Smart 2002, …

Why?
- Cryptanalysis (ECC);
- Foundational problem for isogeny-based cryptography.

Random walks and hash functions (circa 2006)

Any expander graph gives rise to a hash function.



$$H(010101) = v'$$

- Fix a starting vertex v;
- The value to be hashed determines a random path to v';
- v' is the hash.

(Charles, K. E. Lauter, and Goren 2009) hash function (CGL)

- Use the expander graph of supersingular 2-isogenies;
- $\left.\begin{array}{r}\text{Collision resistance}\\ \text{2nd preimage resistance}\end{array}\right\} =$ hardness of finding cycles in the graph;
- Preimage resistance = hardness of finding a path from v to v'.

Hardness of CGL

Finding cycles

- Analogous to finding endomorphisms…
- …very bad idea to start from a curve with known endomorphism ring!
- Translation algortihm: elements of $B_{p,\infty} \leftrightarrow$ isogeny loops
  Doable in $\mathrm{polylog}(p)$.[a]

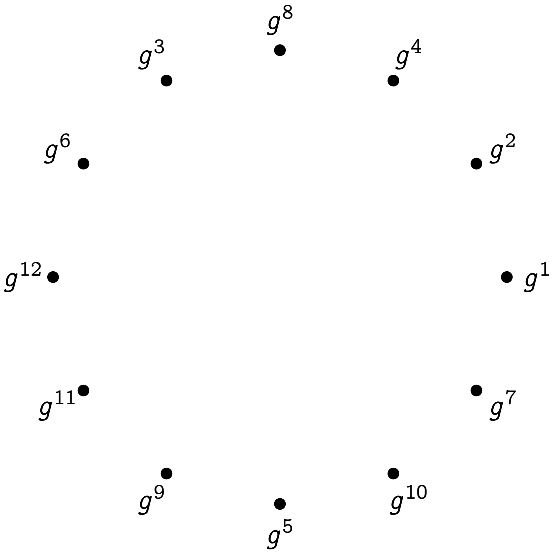
[a] Kohel, K. Lauter, Petit, and Tignol 2014; Eisenträger, Hallgren, K. Lauter, Morrison, and Petit 2018.

Finding paths $E \to E'$

- Analogous to finding connecting ideals between two maximal orders $\mathcal{O}, \mathcal{O}'$ (i.e. a left ideal $I \subset \mathcal{O}$ that is a right ideal of $\mathcal{O}'$).
- Poly-time equivalent to computing $\mathrm{End}(E)$ and $\mathrm{End}(E')$.[a]
- Best known algorithm to compute $\mathrm{End}(E)$ takes $\mathrm{poly}(p)$.[b]

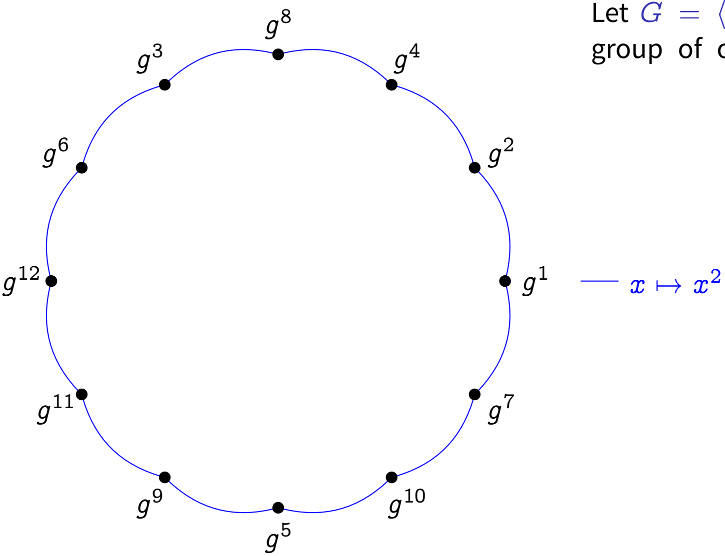
[a] Eisenträger, Hallgren, K. Lauter, Morrison, and Petit 2018.
[b] Kohel 1996; Cerviño 2004.

Expander graphs from groups



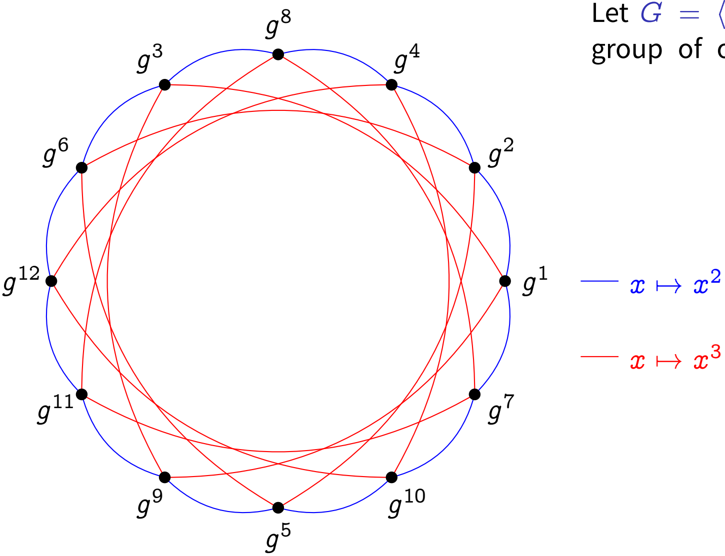
Let $G = \langle g \rangle$ be a cyclic group of order p.

Expander graphs from groups



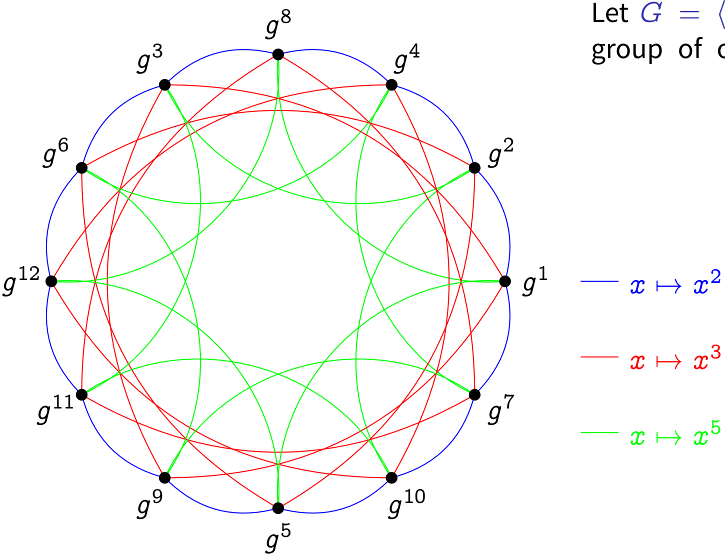
Let $G = \langle g \rangle$ be a cyclic group of order p.

Expander graphs from groups



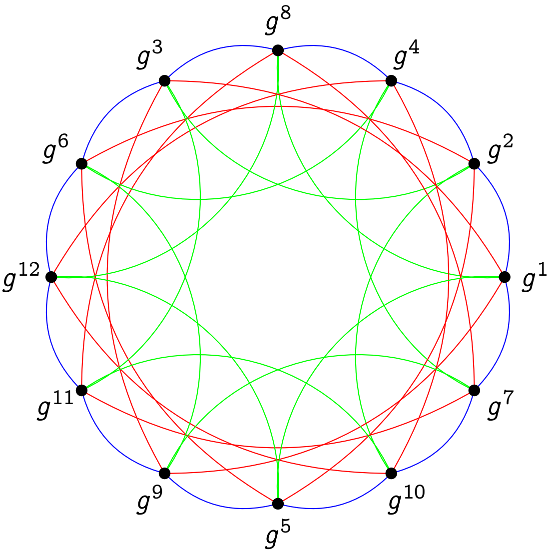
Let $G = \langle g \rangle$ be a cyclic group of order p.

Expander graphs from groups



Let $G = \langle g \rangle$ be a cyclic group of order p.

Expander graphs from groups



Let $G = \langle g \rangle$ be a cyclic group of order p. Let $S \subset (\mathbb{Z}/p\mathbb{Z})^\times$ s.t. $S^{-1} \subset S$.

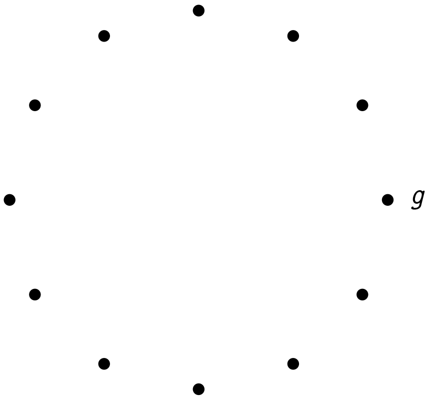
The Schreier graph of $(S, G \setminus \{1\})$ is (usually) an expander.

— $x \mapsto x^2$

— $x \mapsto x^3$

— $x \mapsto x^5$

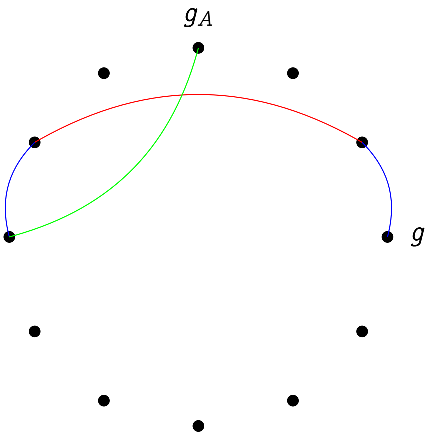
Key exchange from Schreier graphs



Public parameters:

- A group $G = \langle g \rangle$ of order p;
- A subset $S \subset (\mathbb{Z}/p\mathbb{Z})^\times$.

Key exchange from Schreier graphs

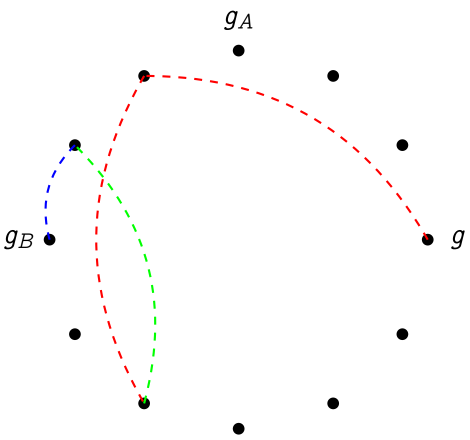


Public parameters:

- A group $G = \langle g \rangle$ of order p;
- A subset $S \subset (\mathbb{Z}/p\mathbb{Z})^\times$.

1. **Alice** takes a secret random walk $s_A : g \to g_A$ of length $O(\log p)$;

Key exchange from Schreier graphs

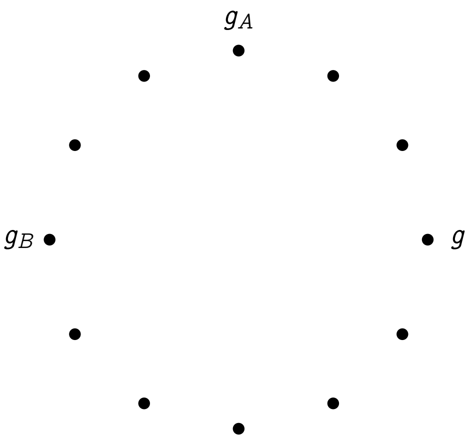


Public parameters:

- A group $G = \langle g \rangle$ of order p;
- A subset $S \subset (\mathbb{Z}/p\mathbb{Z})^\times$.

1. **Alice** takes a secret random walk $s_A : g \to g_A$ of length $O(\log p)$;
2. **Bob** does the same;

Key exchange from Schreier graphs

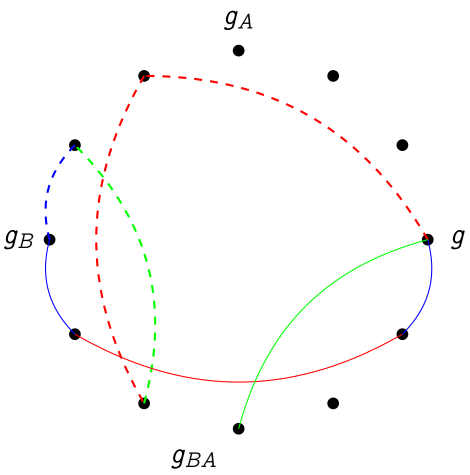


Public parameters:

- A group $G = \langle g \rangle$ of order p;
- A subset $S \subset (\mathbb{Z}/p\mathbb{Z})^\times$.

1. **Alice** takes a secret random walk $s_A : g \to g_A$ of length $O(\log p)$;
2. **Bob** does the same;
3. They publish g_A and g_B;

Key exchange from Schreier graphs

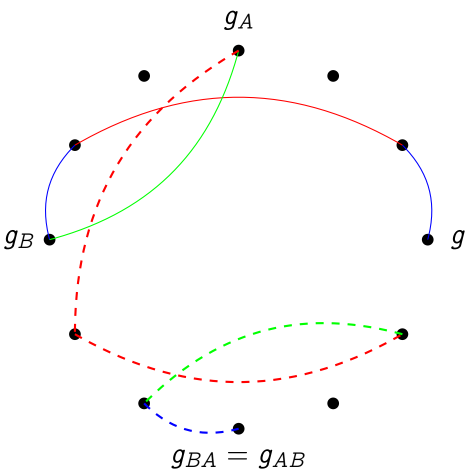


Public parameters:

- A group $G = \langle g \rangle$ of order p;
- A subset $S \subset (\mathbb{Z}/p\mathbb{Z})^\times$.

1. **Alice** takes a secret random walk $s_A : g \to g_A$ of length $O(\log p)$;
2. **Bob** does the same;
3. They publish g_A and g_B;
4. **Alice** repeats her secret walk s_A starting from g_B.

Key exchange from Schreier graphs

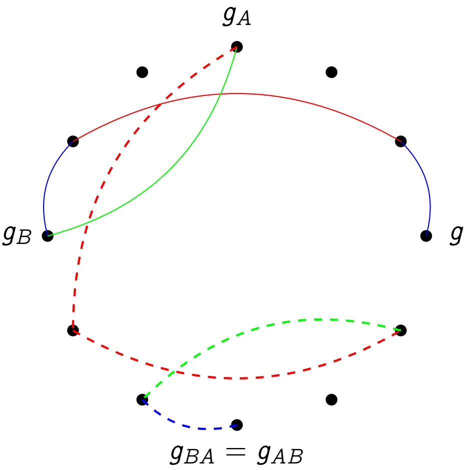


Public parameters:

- A group $G = \langle g \rangle$ of order p;
- A subset $S \subset (\mathbb{Z}/p\mathbb{Z})^\times$.

1. **Alice** takes a secret random walk $s_A : g \to g_A$ of length $O(\log p)$;
2. **Bob** does the same;
3. They publish g_A and g_B;
4. **Alice** repeats her secret walk s_A starting from g_B.
5. **Bob** repeats his secret walk s_B starting from g_A.

Key exchange from Schreier graphs

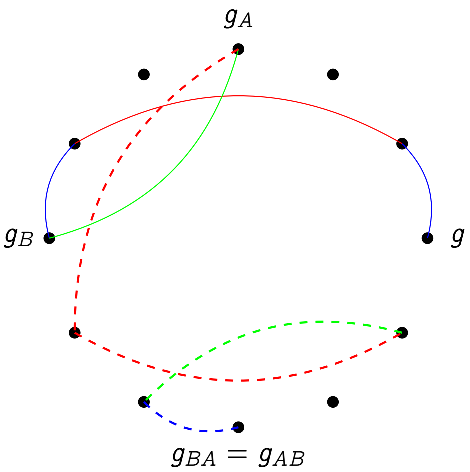


Why does this work?

$$g_A = g^{2\cdot 3\cdot 2\cdot 5},$$
$$g_B = g^{3^2\cdot 5\cdot 2},$$
$$g_{BA} = g_{AB} = g^{2^3\cdot 3^3\cdot 5^2};$$

and g_A, g_B, g_{AB} are uniformly distributed in G…

Key exchange from Schreier graphs



Why does this work?

$$g_A = g^{2\cdot 3\cdot 2\cdot 5},$$

$$g_B = g^{3^2\cdot 5\cdot 2},$$

$$g_{BA} = g_{AB} = g^{2^3\cdot 3^3\cdot 5^2};$$

and g_A, g_B, g_{AB} are uniformly distributed in G…

…Indeed, this is just a twisted presentation of the classical Diffie-Hellman protocol!

Key exchange in graphs of ordinary isogenies[3] (CRS)

Parameters:

- $E/\mathbb{F}_p$ ordinary elliptic curve, with Frobenius endomorphism $\pi \in \mathcal{O}$.
- (small) primes ℓ_1,ℓ_2,…such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.
- elements $\mathfrak{f}_1 = (\ell_1, \pi - \lambda_1)$, $\mathfrak{f}_2 = (\ell_2, \pi - \lambda_2)$,…in $\mathrm{Cl}(\mathcal{O})$.

Secret data: Random walks $\mathfrak{a}, \mathfrak{b} \in \mathrm{Cl}(\mathcal{O})$ in the isogeny graph.

$$\begin{tikzcd}
 & E \arrow[dl, "\mathfrak{f}_1^{a_1}\mathfrak{f}_2^{a_2}\cdots = \mathfrak{a}"'] \arrow[dr, "\mathfrak{b} = \mathfrak{f}_1^{b_1}\mathfrak{f}_2^{b_2}\cdots"] & \\
\mathfrak{a} * E \arrow[dr] & & \mathfrak{b} * E \arrow[dl] \\
 & \mathfrak{a}\mathfrak{b} * E = \mathfrak{b}\mathfrak{a} * E &
\end{tikzcd}$$

[3] Couveignes 2006; Rostovtsev and Stolbunov 2006.

Computing the action of $\mathrm{Cl}(\mathcal{O})$

Input: An ideal class $\mathfrak{a} = \mathfrak{f}_1^{a_1}\mathfrak{f}_2^{a_2}\cdots$.

Output: The elliptic curve $\mathfrak{a} * E$.

Algorithm: Let $\mathfrak{f}^n = (\ell, \pi - \lambda)^n$, repeat n times:

- Use **Elkies' algorithm** to find all (two) curves isogenous to E of degree ℓ,
- Choose the one such that $\ker\phi \subset \ker(\pi - \lambda)$.

Parameters size / performance

Adversary goal: Given E, $\mathfrak{a} * E$, find $\mathfrak{a}$;

Graph size: $\#\,\mathrm{Cl}(\mathcal{O}) \approx \sqrt{p}$;

Best (classical) attack: Meet-in-the-middle / Random-walk in $\sqrt{\#\,\mathrm{Cl}(\mathcal{O})}$;

For 2^{128} security: choose $\log p \sim 512$;

Time to evaluate the isogeny action[a]: Dozens of minutes!

[a] De Feo, Kieffer, and Smith 2018.

Vélu to the rescue?

Input: An ideal class $\mathfrak{a} = \mathfrak{f}_1^{a_1}\mathfrak{f}_2^{a_2}\cdots$.

Output: The elliptic curve $\mathfrak{a} * E$.

Algorithm: Let $\mathfrak{f}^n = (\ell, \pi - \lambda)^n$. Why not:

- *Presciently* find $H = E[\ell] \cap \ker(\pi - \lambda)$,
- Apply Vélu's formulas to H.

Speeding up the class group action

Problem: H must be in $E(\mathbb{F}_p)$ for Vélu's formulas to be efficient.

Idea[a]: Force
$$\begin{cases} p = -1 & \mod \ell, \\ \lambda = 1 & \mod \ell, \end{cases}$$
so that $E[\ell] = H \subset E(\mathbb{F}_p)$.

[a] De Feo, Kieffer, and Smith 2018.

Vélu to the rescue?

Input: An ideal class $\mathfrak{a} = \mathfrak{f}_1^{a_1}\mathfrak{f}_2^{a_2}\cdots$.

Output: The elliptic curve $\mathfrak{a} * E$.

Algorithm: Let $\mathfrak{f}^n = (\ell, \pi - \lambda)^n$. Why not:

- *Presciently* find $H = E[\ell] \cap \ker(\pi - \lambda)$,
- Apply Vélu's formulas to H.

Speeding up the class group action

Problem: H must be in $E(\mathbb{F}_p)$ for Vélu's formulas to be efficient.

Idea[a]**:** Force
$$\begin{cases} p = -1 & \mod \ell, \\ \lambda = 1 & \mod \ell, \end{cases}$$
so that $E[\ell] = H \subset E(\mathbb{F}_p)$.

How to waste an internship: Forcing λ = Forcing $\#E$ = Very hard!

[a] De Feo, Kieffer, and Smith 2018.

Vélu to the rescue?

Input: An ideal class $\mathfrak{a} = \mathfrak{f}_1^{a_1}\mathfrak{f}_2^{a_2}\cdots$.

Output: The elliptic curve $\mathfrak{a} * E$.

Algorithm: Let $\mathfrak{f}^n = (\ell, \pi - \lambda)^n$. Why not:

- *Presciently* find $H = E[\ell] \cap \ker(\pi - \lambda)$,
- Apply Vélu's formulas to H.

Speeding up the class group action

Problem: H must be in $E(\mathbb{F}_p)$ for Vélu's formulas to be efficient.

Idea[a]: Force $\begin{cases} p = -1 & \mod \ell, \\ \lambda = 1 & \mod \ell, \end{cases}$

so that $E[\ell] = H \subset E(\mathbb{F}_p)$.

How to waste an internship: Forcing λ = Forcing $\#E$ = Very hard!

Time to evaluate the isogeny action: Still 5 minutes!

[a] De Feo, Kieffer, and Smith 2018.

Supersingular to the rescue!

For all supersingular curves defined over $\mathbb{F}_p$,

$$\pi = \begin{pmatrix} \sqrt{-p} & 0 \\ 0 & -\sqrt{-p} \end{pmatrix} \mod \ell$$

CSIDH *(pron.: Seaside)*

Choose $p = -1 \mod \ell$ for many primes ℓ;

Hence, $\lambda = 1 \mod \ell$. Win!

Performance: Same security as CRS in less than 50ms![a]

[a] Castryck, Lange, Martindale, Panny, and Renes 2018.

Quantum security

Fact: Shor's algorithm does not apply to Diffie-Hellman protocols from group actions.

Subexponential attack $\exp(\sqrt{\log p \log\log p})$

- Reduction to the hidden shift problem by evaluating the class group action in quantum superspositio[a] (subexpoential cost);
- Well known reduction from the hidden shift to the dihedral (non-abelian) hidden subgroup problem;
- Kuperberg's algorithm[b] solves the dHSP with a subexponential number of class group evaluations.
- Recent work[c] suggests that 2^{64}-qbit security is achieved somewhere in $512 < \log p < 1024$.

[a] Childs, Jao, and Soukharev 2014.

[b] Kuperberg 2005; Regev 2004; Kuperberg 2013.

[c] Bonnetain and Naya-Plasencia 2018; Bonnetain and Schrottenloher 2018; Biasse, Jacobson Jr, and Iezzi 2018; Jao, LeGrow, Leonardi, and Ruiz-Lopez 2018; Bernstein, Lange, Martindale, and Panny 2018.

Key exchange with supersingular curves (2011)

Good news: there is no action of a commutative class group.

Bad news: there is no action of a commutative class group.

Idea: Let Alice and Bob walk in two different isogeny graphs on the same vertex set.

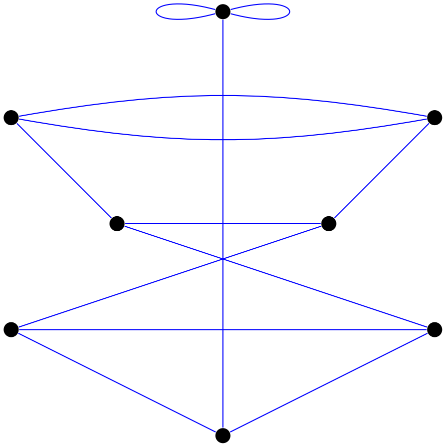


Figure: 2- and 3-isogeny graphs on $\mathbb{F}_{97^2}$.

Key exchange with supersingular curves (2011)

Good news: there is no action of a commutative class group.

Bad news: there is no action of a commutative class group.

Idea: Let Alice and Bob walk in two different isogeny graphs on the same vertex set.

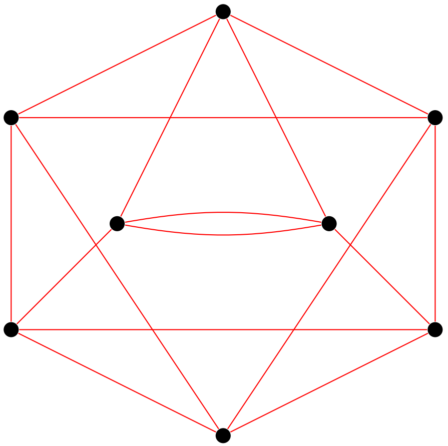


Figure: 2- and 3-isogeny graphs on $\mathbb{F}_{97^2}$.

Key exchange with supersingular curves (2011)

Good news: there is no action of a commutative class group.

Bad news: there is no action of a commutative class group.

Idea: Let Alice and Bob walk in two different isogeny graphs on the same vertex set.

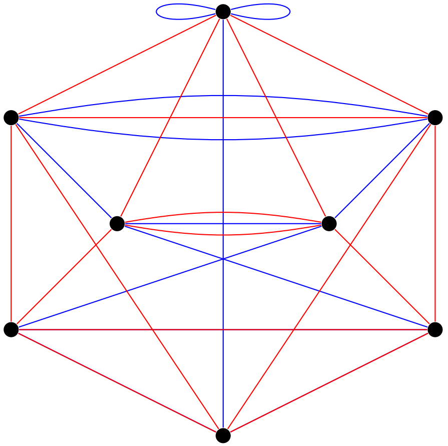


Figure: 2- and 3-isogeny graphs on $\mathbb{F}_{97^2}$.

Key exchange with supersingular curves (2011)

- Fix small primes ℓ_A, ℓ_B;
- No canonical labeling of the ℓ_A- and ℓ_B-isogeny graphs; however…

Walk of length e_A

$$=$$

Isogeny of degree $\ell_A^{e_A}$

$$=$$

Kernel $\langle P\rangle \subset E[\ell_A^{e_A}]$

$$\ker\phi = \langle P\rangle \subset E[\ell_A^{e_A}]$$

$$\ker\psi = \langle Q\rangle \subset E[\ell_B^{e_B}]$$

$$\ker\phi' = \langle \psi(P)\rangle$$

$$\ker\psi' = \langle \phi(Q)\rangle$$

$$\begin{tikzcd}
E \arrow[r, squiggly, "\phi"] \arrow[d, squiggly, "\psi"'] & E/\langle P\rangle \arrow[d, squiggly, "\psi'"] \\
E/\langle Q\rangle \arrow[r, squiggly, "\phi'"'] & E/\langle P, Q\rangle
\end{tikzcd}$$

Supersingular Isogeny Diffie-Hellman[4]

Parameters:

- Prime p such that $p+1 = \ell_A^a \ell_B^b$;
- Supersingular curve $E \simeq (\mathbb{Z}/(p+1)\mathbb{Z})^2$;
- $E[\ell_A^a] = \langle P_A, Q_A \rangle$;
- $E[\ell_B^b] = \langle P_B, Q_B \rangle$.

Secret data:

- $R_A = m_A P_A + n_A Q_A$,
- $R_B = m_B P_B + n_B Q_B$,

$$
\begin{tikzcd}
 & E \arrow[dl, squiggly, "\phi"'] \arrow[dr, squiggly, "\psi"] & \\
E/\langle R_A \rangle \arrow[dr, squiggly, "\psi'"'] & & E/\langle R_B \rangle \arrow[dl, squiggly, "\phi'"] \\
 & E/\langle R_A, R_B \rangle &
\end{tikzcd}
$$

$$\frac{E/\langle R_A \rangle}{\phi(R_B)} \simeq E/\langle R_A, R_B \rangle \simeq \frac{E/\langle R_B \rangle}{\psi(R_A)}$$

[4] Jao and De Feo 2011; De Feo, Jao, and Plût 2014.

Supersingular Isogeny Diffie-Hellman[4]

Parameters:

- Prime p such that $p+1 = \ell_A^a \ell_B^b$;
- Supersingular curve $E \simeq (\mathbb{Z}/(p+1)\mathbb{Z})^2$;
- $E[\ell_A^a] = \langle P_A, Q_A \rangle$;
- $E[\ell_B^b] = \langle P_B, Q_B \rangle$.

Secret data:

- $R_A = m_A P_A + n_A Q_A$,
- $R_B = m_B P_B + n_B Q_B$,

$$
\begin{tikzcd}
 & E \arrow[dl, squiggly, "\phi"'] \arrow[dr, squiggly, "\psi"] & \\
\begin{array}{l} E/\langle R_A \rangle \\ \phi(P_B) \\ \phi(Q_B) \end{array} \arrow[dr, squiggly, "\psi'"'] & & \begin{array}{l} E/\langle R_B \rangle \\ \psi(P_A) \\ \psi(Q_A) \end{array} \arrow[dl, squiggly, "\phi'"] \\
\frac{E/\langle R_A \rangle}{\phi(R_B)} \simeq & E/\langle R_A, R_B \rangle & \simeq \frac{E/\langle R_B \rangle}{\psi(R_A)}
\end{tikzcd}
$$

[4] Jao and De Feo 2011; De Feo, Jao, and Plût 2014.

Supersingular Isogeny Diffie-Hellman[4]

Parameters:

- Prime p such that $p + 1 = \ell_A^a \ell_B^b$;
- Supersingular curve $E \simeq (\mathbb{Z}/(p+1)\mathbb{Z})^2$;
- $E[\ell_A^a] = \langle P_A, Q_A \rangle$;
- $E[\ell_B^b] = \langle P_B, Q_B \rangle$.

Secret data:

- $R_A = m_A P_A + n_A Q_A$,
- $R_B = m_B P_B + n_B Q_B$,

$$\begin{tikzcd}
 & E \arrow[dl, squiggly, "\phi"'] \arrow[dr, squiggly, "\psi"] & \\
E/\langle R_A \rangle \arrow[dr, squiggly, "\psi'"'] & & E/\langle R_B \rangle \arrow[dl, squiggly, "\phi'"] \\
 & E/\langle R_A, R_B \rangle &
\end{tikzcd}$$

$\phi(P_B)$ $\phi(Q_B)$ $\qquad$ $\phi(R_B)$ $\qquad$ $\psi(R_A)$ $\qquad$ $\psi(P_A)$ $\psi(Q_A)$

$$\frac{E/\langle R_A \rangle}{\phi(R_B)} \simeq E/\langle R_A, R_B \rangle \simeq \frac{E/\langle R_B \rangle}{\psi(R_A)}$$

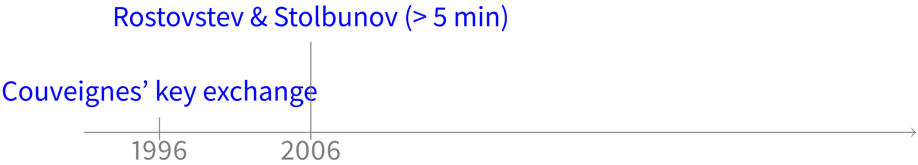
[4] Jao and De Feo 2011; De Feo, Jao, and Plût 2014.

From 10 minutes to 10ms in 20 years

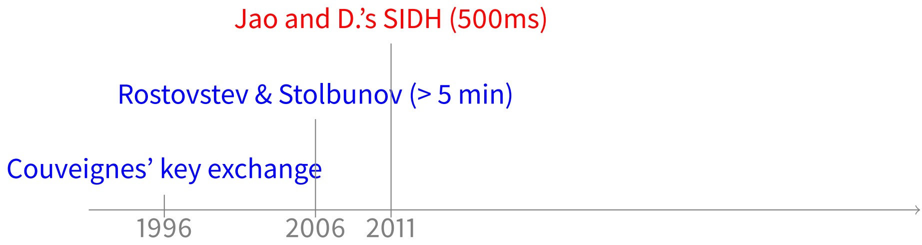
Couveignes’ key exchange

1996

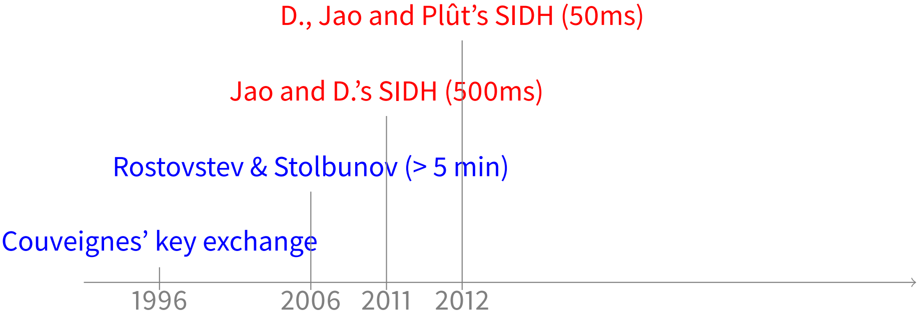
From 10 minutes to 10ms in 20 years



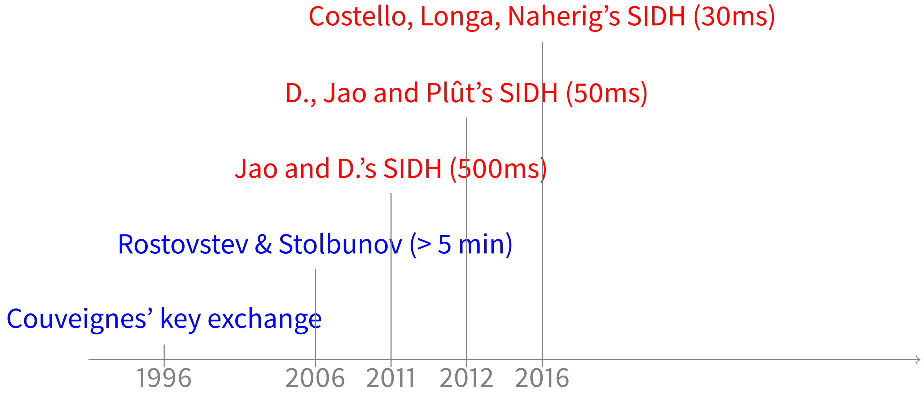
From 10 minutes to 10ms in 20 years



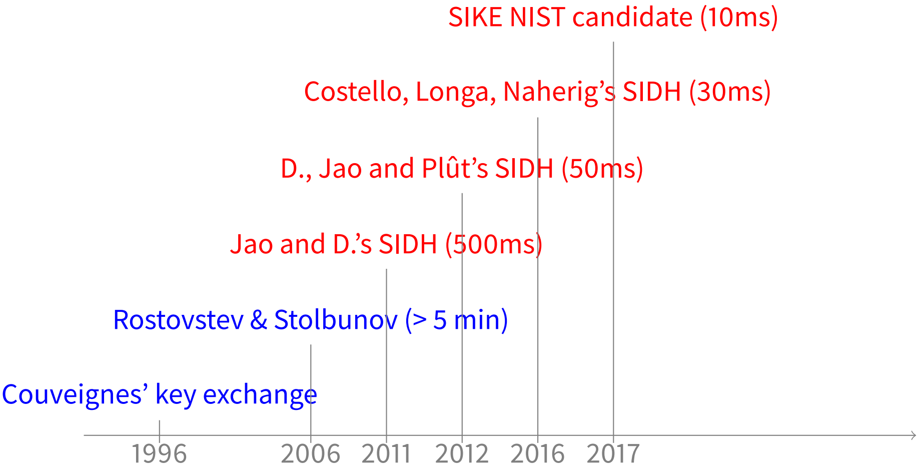
From 10 minutes to 10ms in 20 years



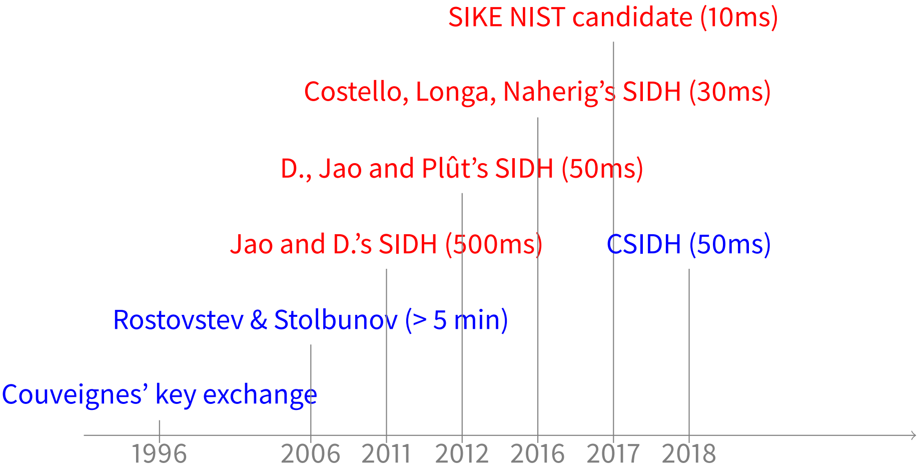
From 10 minutes to 10ms in 20 years



From 10 minutes to 10ms in 20 years

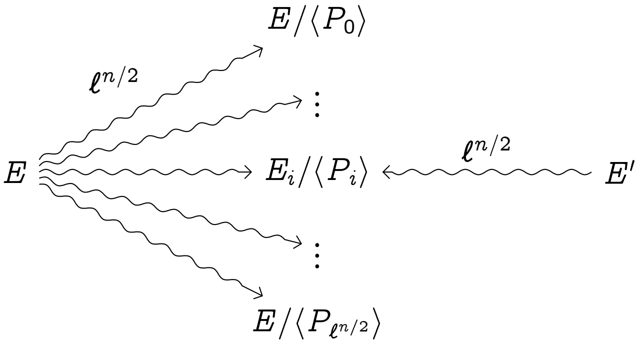


From 10 minutes to 10ms in 20 years



Generic attacks

Problem: Given E, E', isogenous of degree ℓ^n, find $\phi : E \to E'$.



- With high probability ϕ is the unique collision (or *claw*) $O(\ell^{n/2})$.
- A quantum claw finding[5] algorithm solves the problem in $O(\ell^{n/3})$.

[5] Tani 2009.

Security

The SIDH problem

Given E, Alice's public data $E/\langle R_A\rangle, \phi(P_B), \phi(Q_B)$, and Bob's public data $E/\langle R_B\rangle, \psi(P_A), \psi(Q_A)$, find the shared secret $E/\langle R_A, R_B\rangle$.

Under the SIDH assumption:

- The SIDH key exchange protocol is session-key secure.
- The derived El Gamal-type PKE is CPA secure.

Reductions

- SIDH $\to$ Isogeny Walk Problem;
- SIDH $\to$ Computing the endomorphism rings of E and $E/\langle R_A\rangle$.[a]

[a] Kohel, K. Lauter, Petit, and Tignol 2014; Galbraith, Petit, Shani, and Ti 2016.

Chosen ciphertext attack[6]

For simplicity, assume Alice's prime is $\ell = 2$.

Evil Bob

- Alice has a long-term secret $R = mP + nQ \in E[2^e]$;
- Bob produces an ephemeral secret ψ;
- Bob sends to Alice $\psi(P)$, $\psi(Q + 2^{e-1}P)$;
- Alice computes the shared secret correctly iff

$$\begin{aligned} R &= mP + nQ \\ &= mP + nQ + n2^{e-1}P, \end{aligned}$$

  i.e., iff n is even;
- Bob learns one bit of the secret key by checking that Alice gets the right shared secret.

- Bob repeats the queries in a similar fashion, learning one bit per query.
- Detecting Bob's faulty key seems to be as hard as breaking SIDH.

[6] Galbraith, Petit, Shani, and Ti 2016.

CSIDH vs SIDH

	CSIDH	**SIDH**
Speed (NIST 1)	<100ms	$\sim$ 10ms
Public key size (NIST 1)	64B	378B
Key compression[7]		
↳ speed		$\sim$ 15ms[8]
↳ size		222B
Constant time impl.	not yet	yes
Submitted to NIST	no	yes
Best classical attack	$p^{1/4}$	$p^{1/4}$
Best quantum attack	$\tilde{O}\left(3^{\sqrt{\log_3 p}}\right)$	$p^{1/6}$
Key size scales	quadratically	linearly
Security assumption	isogeny walk problem	ad hoc
CPA security	yes	yes
CCA security	yes	Fujisaki-Okamoto
Non-interactive key ex.	yes	no
Signatures	short but slooow!	big and slow

[7] Zanon, Simplicio, Pereira, Doliskani, and Barreto 2018.

[8] https://twitter.com/PatrickLonga/status/1002313366466015232?s=20

SIKE: Supersingular Isogeny Key Encapsulation

- Submission to the NIST PQ competition:

  SIKE.PKE: El Gamal-type system with IND-CPA security proof,
  SIKE.KEM: generically transformed system with IND-CCA security proof.

- Security levels 1, 3 and 5.
- Smallest communication complexity among all proposals in each level.
- Slowest among all benchmarked proposals in each level.
- A team of 14 submitters, from 8 universities and companies.
- Head to `https://sike.org`.

	p	cl. security	q. security	speed	comm.
SIKEp434	$2^{216}3^{137}-1$	NIST-1	NIST-1	–	–
SIKEp503	$2^{250}3^{159}-1$	126 bits	84 bits	10ms	0.4KB
SIKEp751	$2^{372}3^{239}-1$	188 bits	125 bits	30ms	0.6KB

Thank you

http://defeo.lu/

@luca_defeo