# Isogeny graphs in cryptography


**Luca De Feo**

**Université Paris Saclay, UVSQ & Inria**


**March 19–23, 2018, Post-Scryptum Spring School, Les 7 Laux**

Slides online at http://defeo.lu/docet/

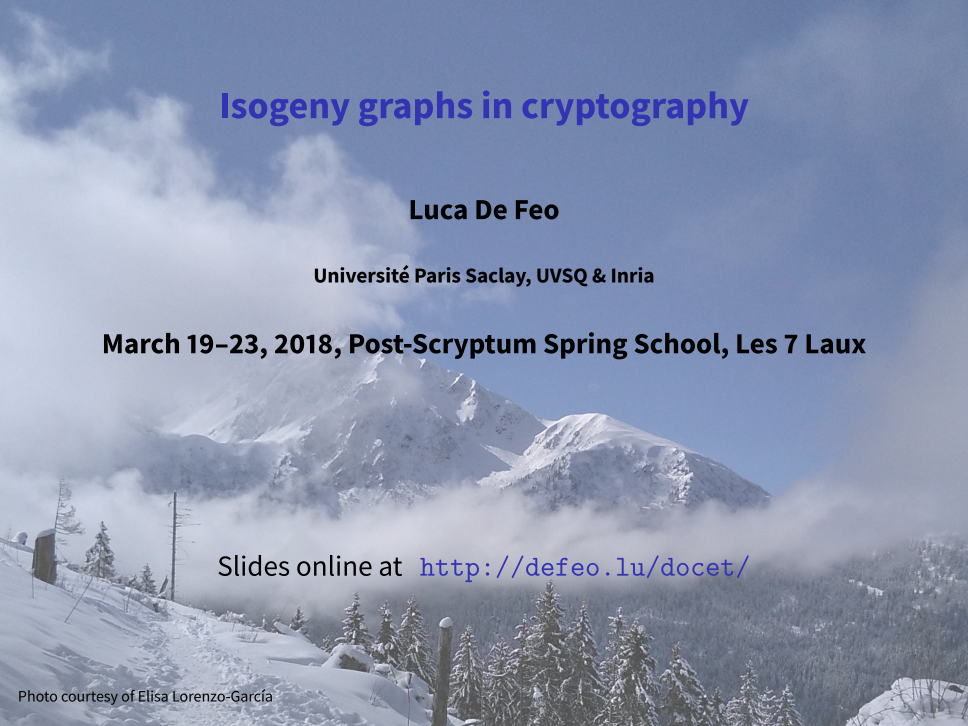


Photo courtesy of Elisa Lorenzo-García

# Overview

1. Foundations
   - Elliptic curves
   - Isogenies
   - Complex multiplication
2. Isogeny-based cryptography
   - Isogeny walks
   - Key exchange from ordinary graphs
   - Key exchange from supersingular graphs
   - The SIKE submission

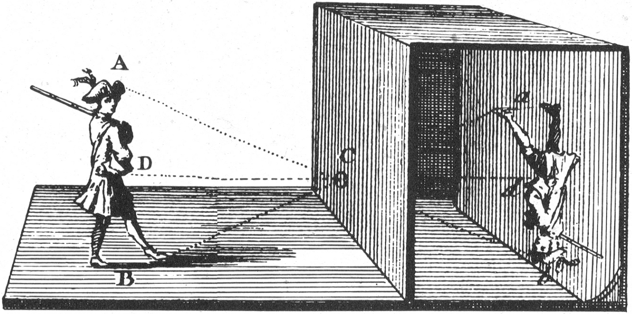
# Projective space

## 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 $(x_0 : \dots : x_n)$.

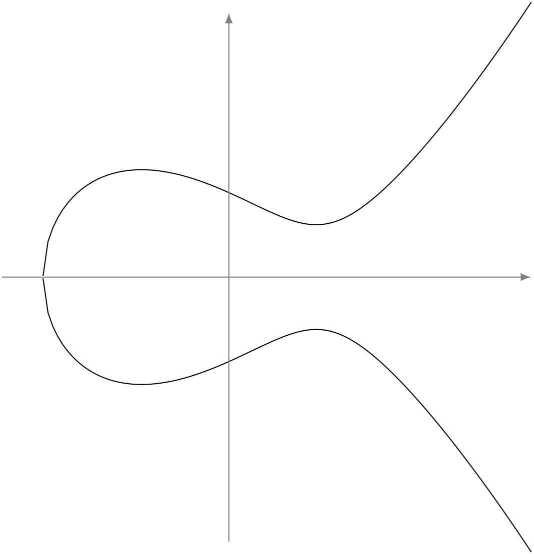


# Weierstrass equations

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 $4a^3 + 27b^2 \neq 0$.



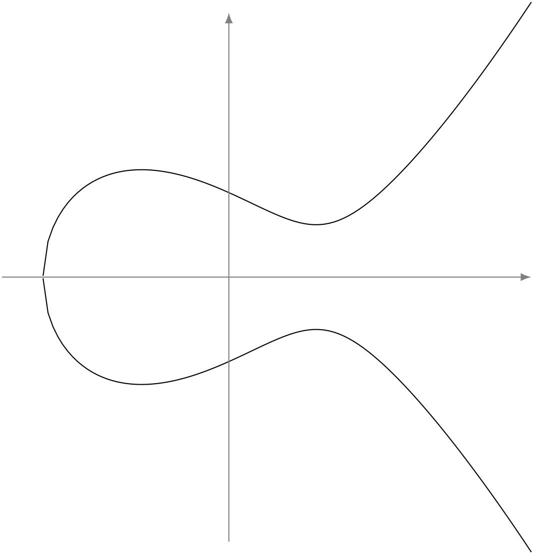
# Weierstrass equations

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

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

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

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



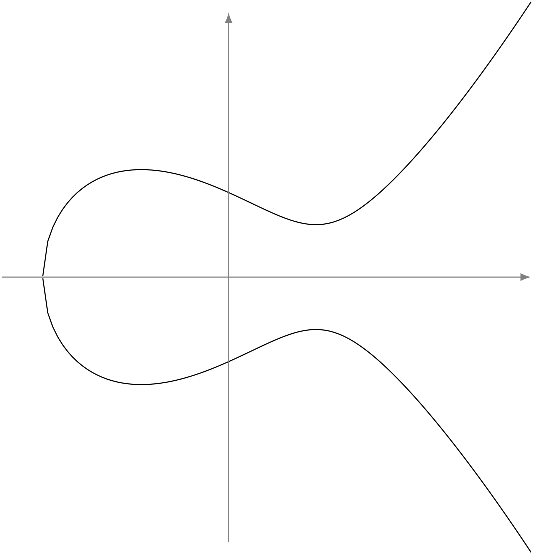
# Weierstrass equations

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.

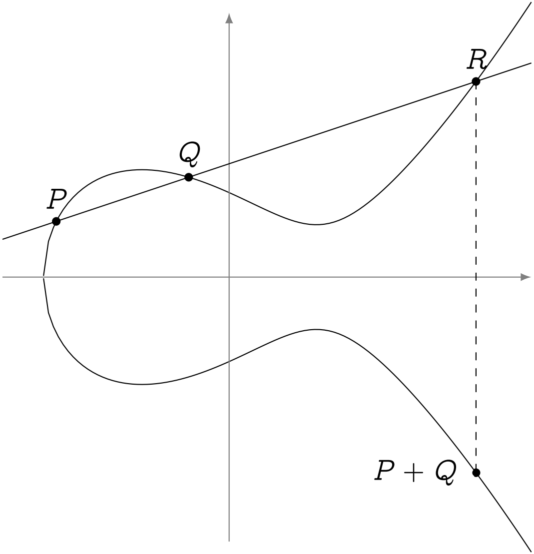


# The group law

## 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.



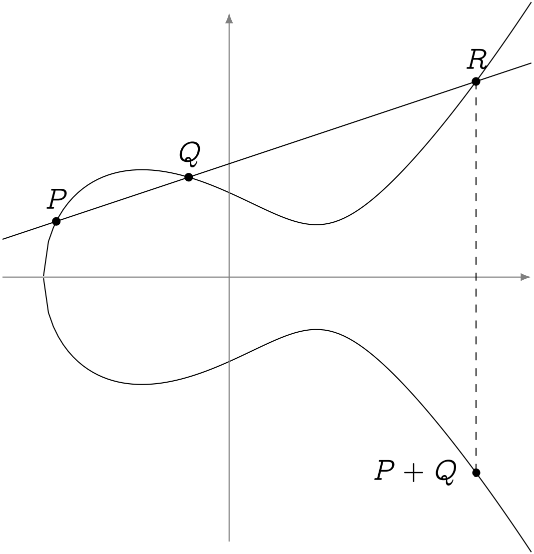
# The group law

**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*);



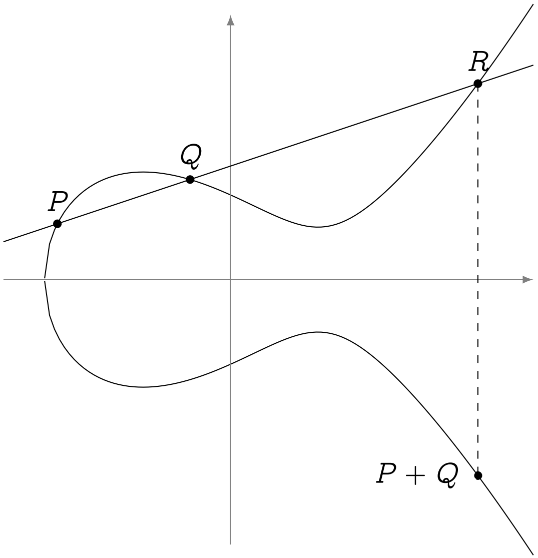
# The group law

**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:*

- *$\phi$ is a surjective group morphism,*
- *$\phi$ is a group morphism with finite kernel,*
- *$\phi$ 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 $\phi$ is called an isogeny.*

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

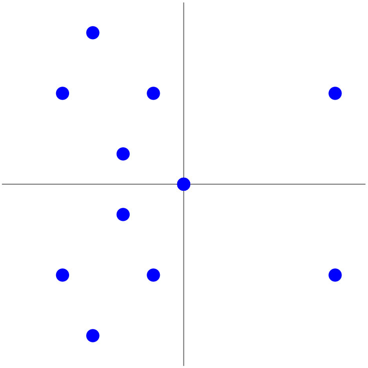
## Example: Multiplication-by-$m$

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

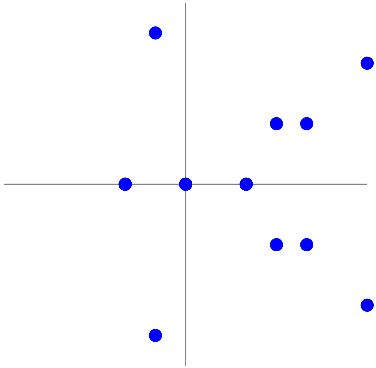
$$\begin{aligned}[m] \ : \ E &\to E, \\ P &\mapsto [m]P.\end{aligned}$$

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

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



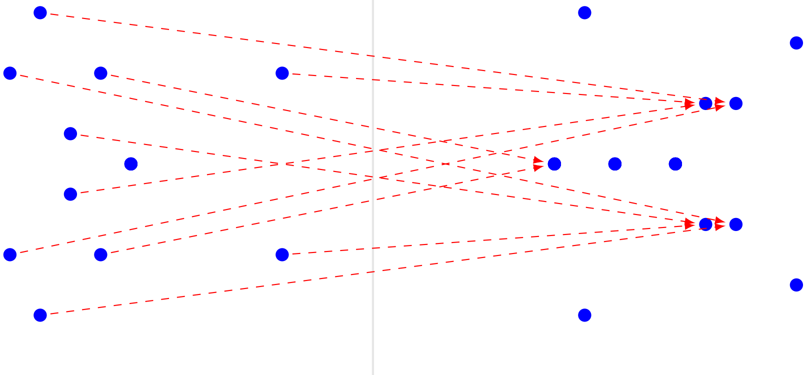
$$E' \;:\; y^2 = x^3 - 4x$$



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

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

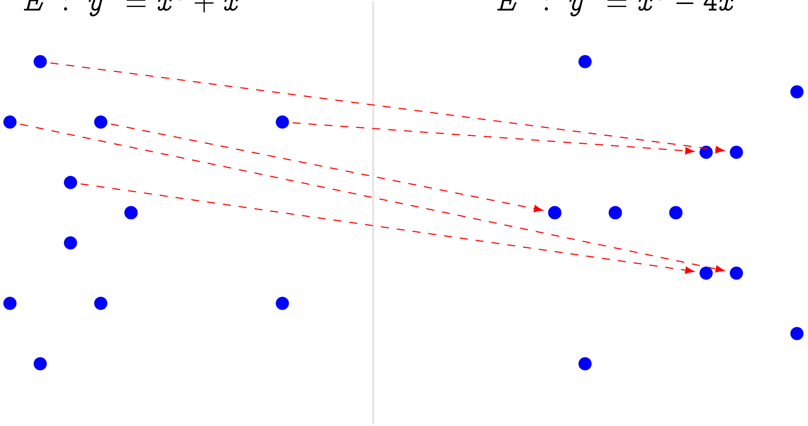
$E : y^2 = x^3 + x$ $\qquad$ $E' : y^2 = x^3 - 4x$



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

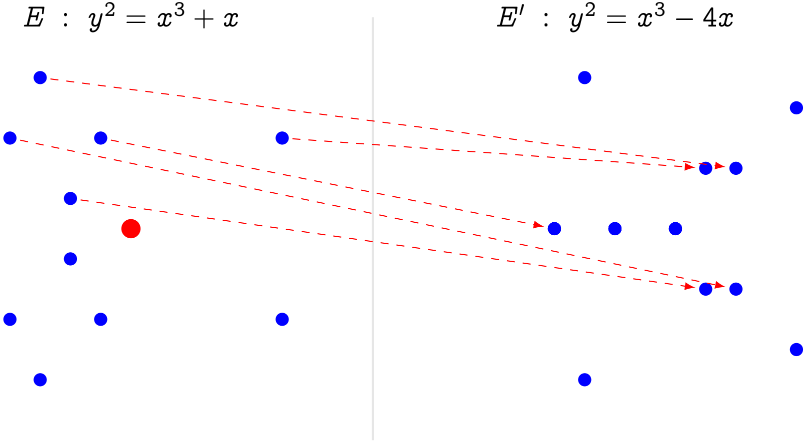
# Isogenies: an example over $\mathbb{F}_{11}$

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



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

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

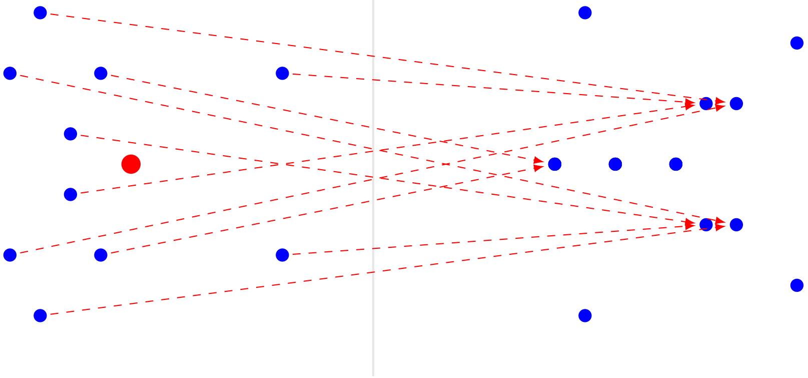



$$\phi(x, y) = \left( \frac{x^2 + 1}{x}, \quad y \frac{x^2 - 1}{x^2} \right)$$

- Kernel generator in red.

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

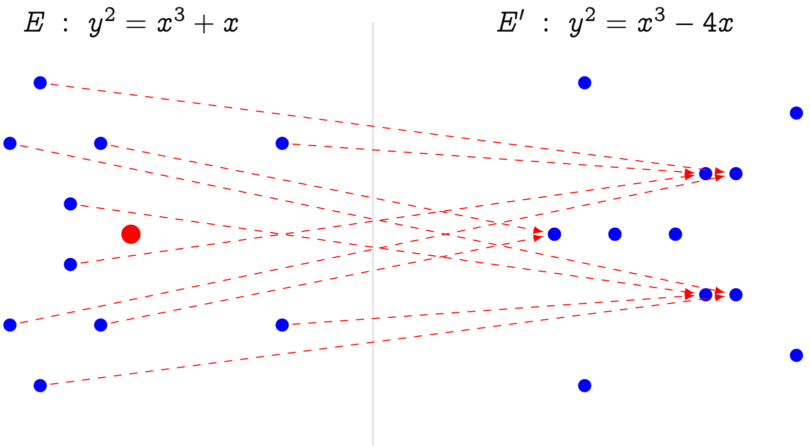
$E \; : \; y^2 = x^3 + x$ $\qquad$ $E' \; : \; y^2 = x^3 - 4x$



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

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

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




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

- 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

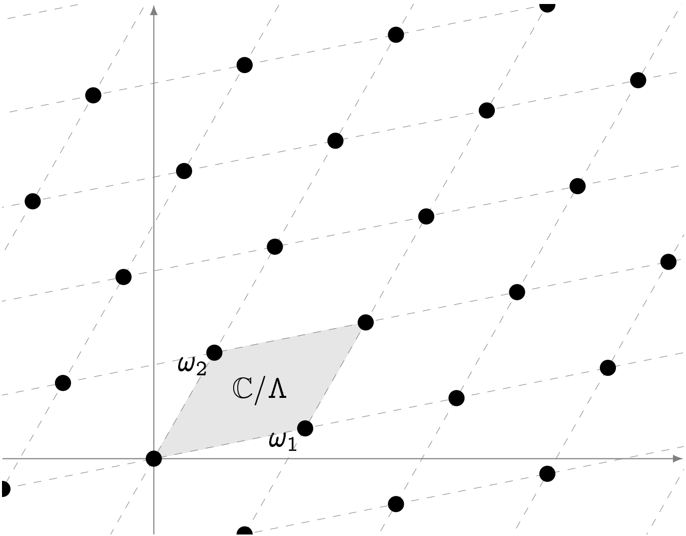
Let $E$ be defined over $\mathbb{F}_q$, then

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

## 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

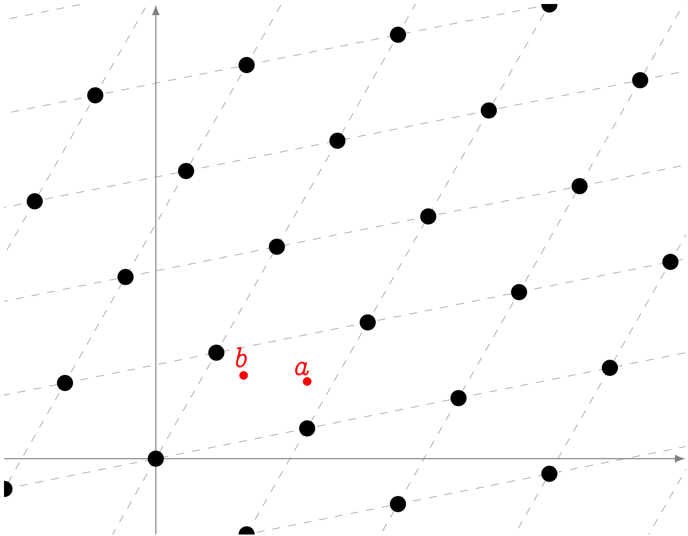



Let $\omega_1, \omega_2 \in \mathbb{C}$ be linearly independent complex numbers. Set

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

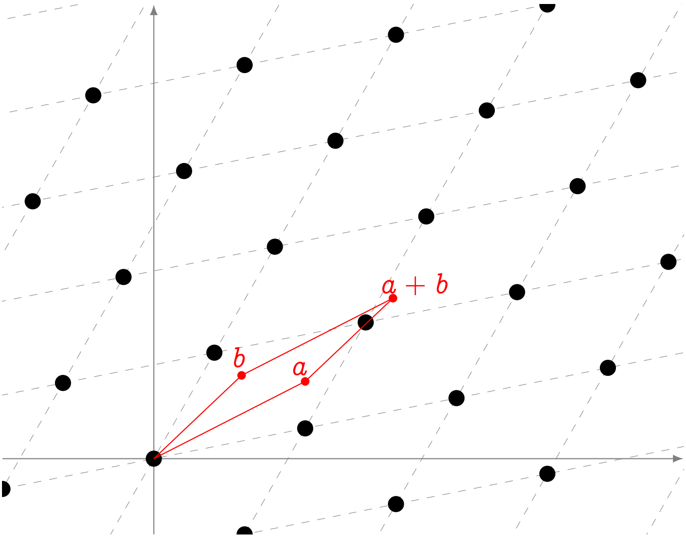
$\mathbb{C}/\Lambda$ is a complex torus.

# Complex tori



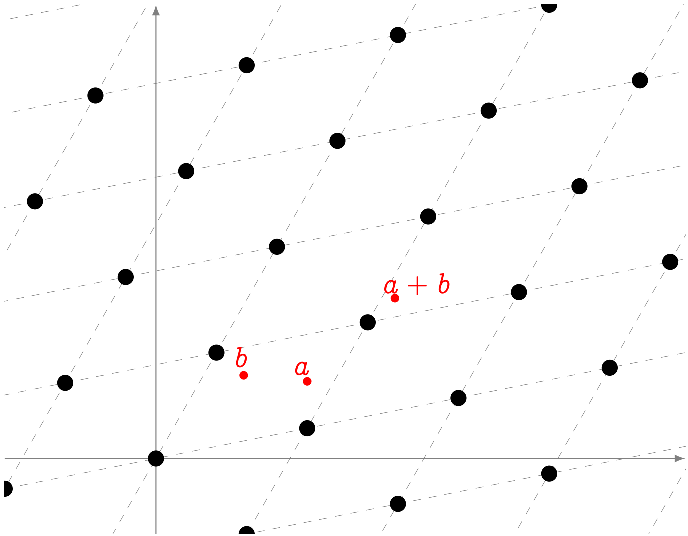

Addition law induced by addition on $\mathbb{C}$.

# Complex tori



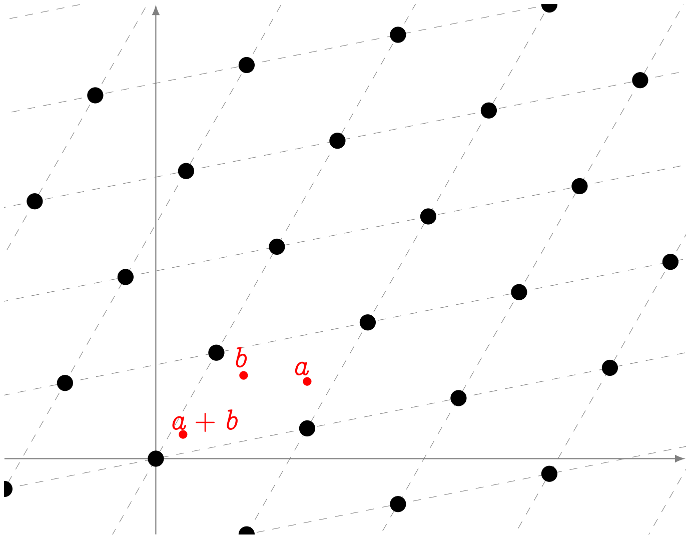

Addition law induced by addition on $\mathbb{C}$.

# Complex tori



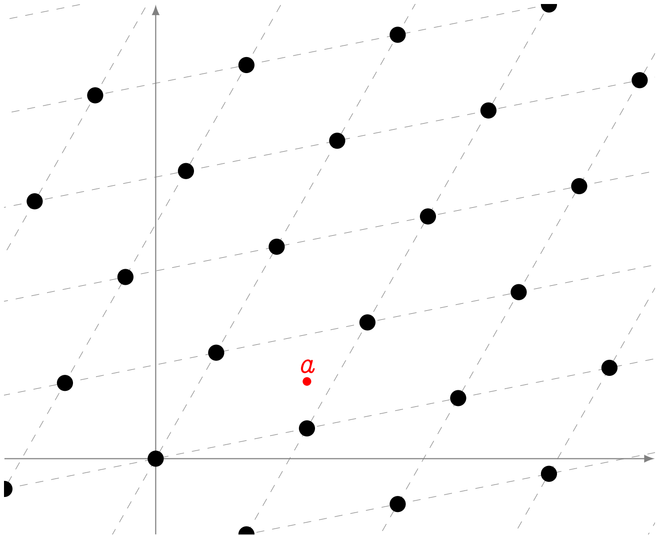

Addition law induced by addition on $\mathbb{C}$.

# Complex tori




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

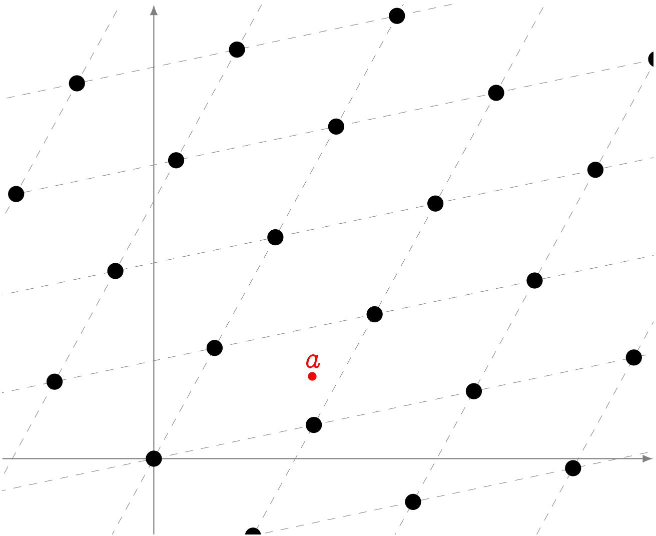
# Homotheties




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

$$\alpha\Lambda_1 = \Lambda_2$$

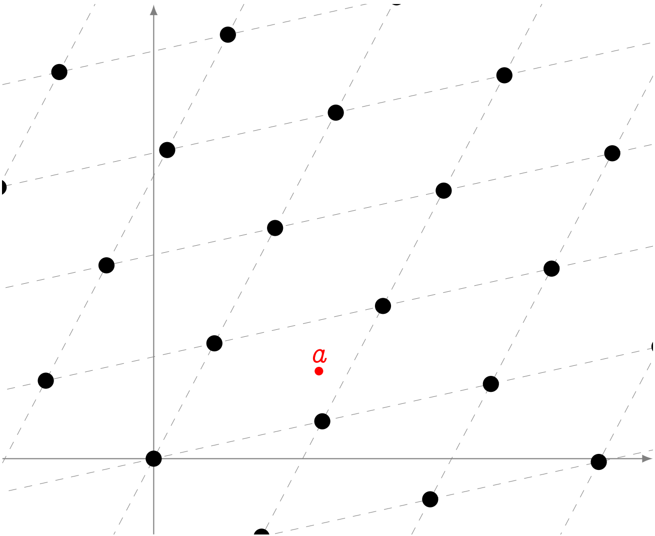
# Homotheties




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

$$\alpha\Lambda_1 = \Lambda_2$$

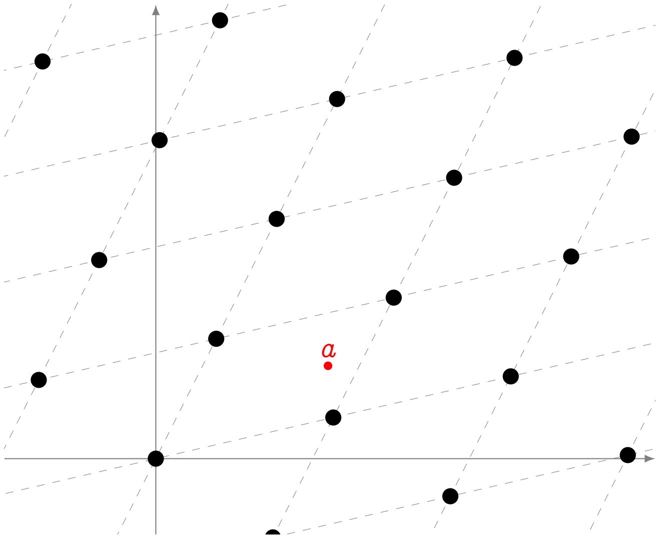
# Homotheties




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

$$\alpha\Lambda_1 = \Lambda_2$$

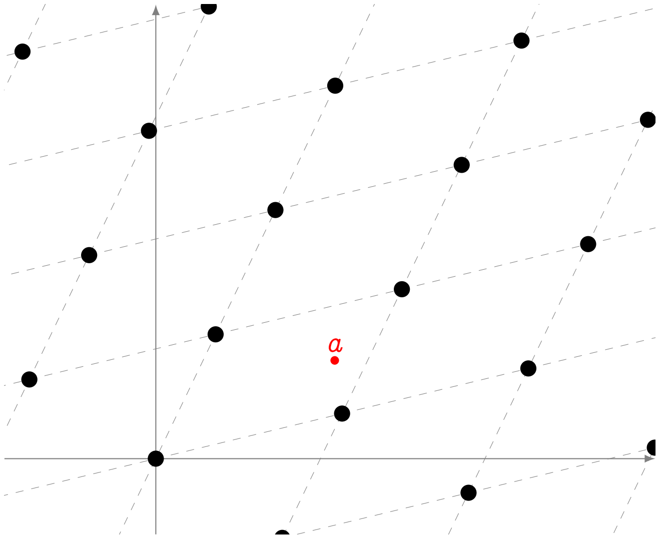
# Homotheties




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

$$\alpha\Lambda_1 = \Lambda_2$$

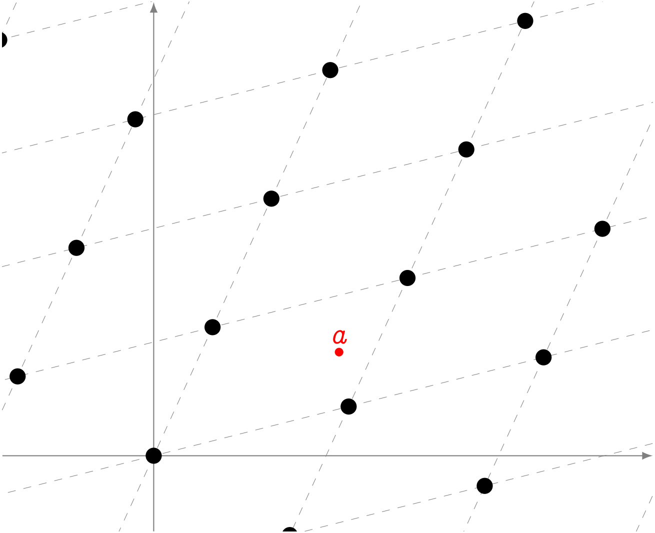
# Homotheties




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

$$\alpha\Lambda_1 = \Lambda_2$$

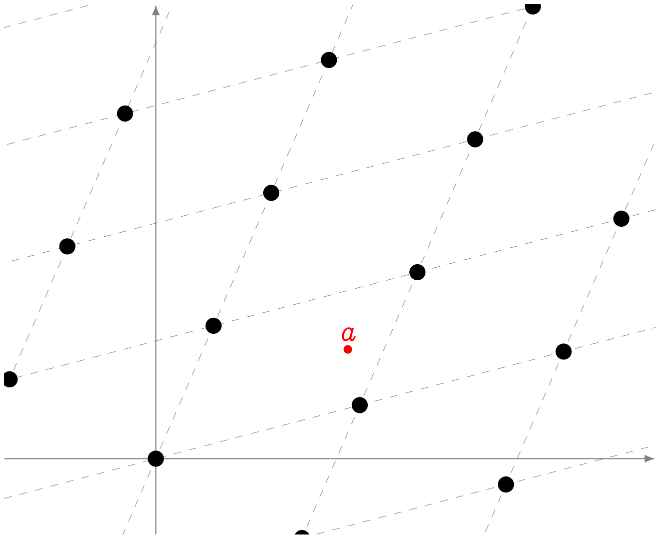
# Homotheties




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

$$\alpha \Lambda_1 = \Lambda_2$$

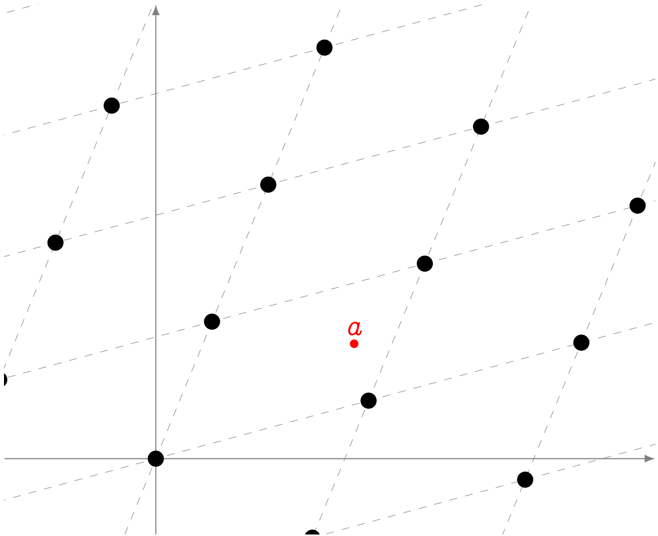
# Homotheties




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

$$\alpha\Lambda_1 = \Lambda_2$$

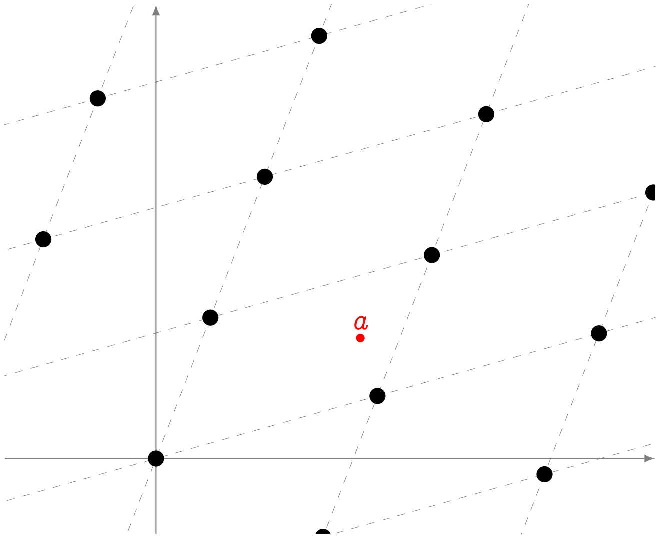
# Homotheties




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

$$\alpha\Lambda_1 = \Lambda_2$$

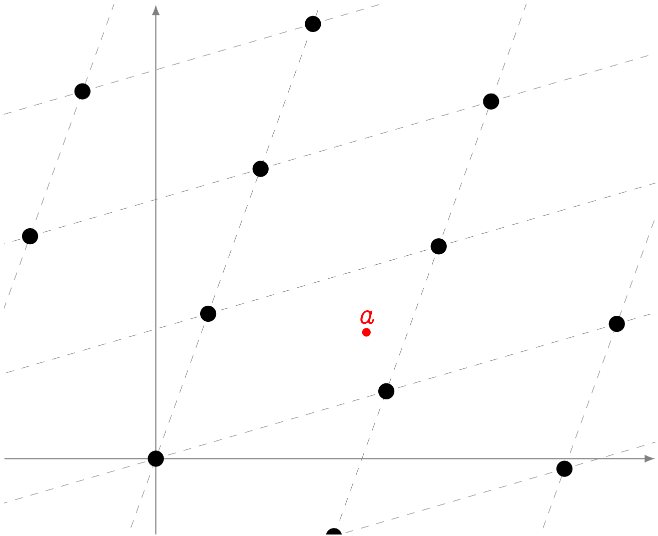
# Homotheties




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

$$\alpha\Lambda_1 = \Lambda_2$$

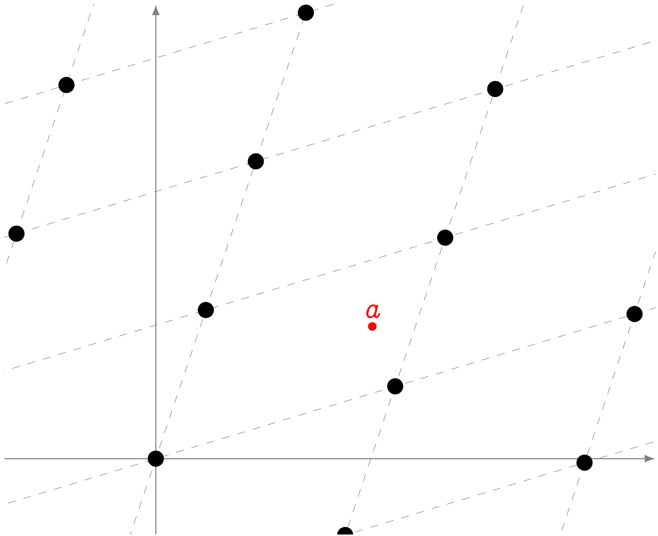
# Homotheties




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

$$\alpha\Lambda_1 = \Lambda_2$$

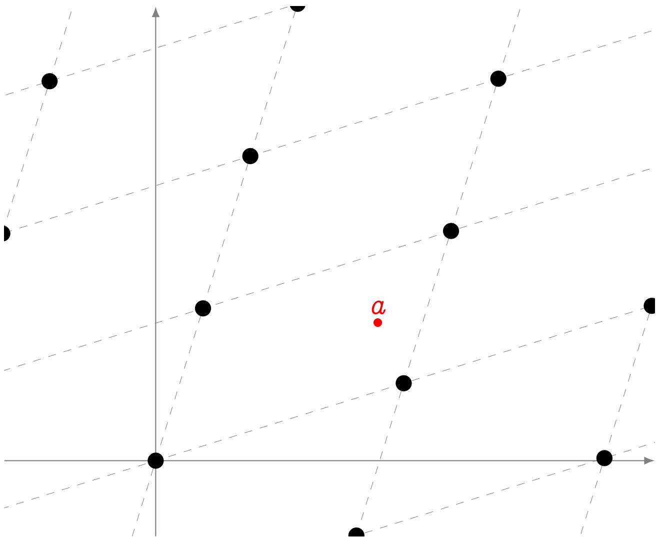
# Homotheties




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

$$\alpha\Lambda_1 = \Lambda_2$$

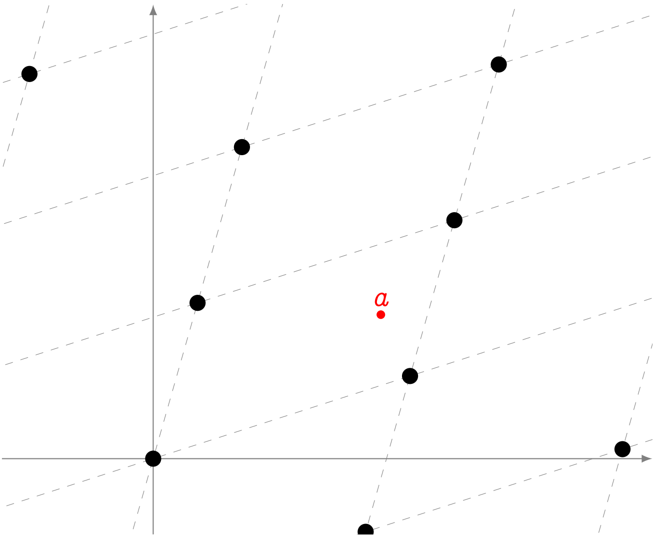
# Homotheties




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

$$\alpha\Lambda_1 = \Lambda_2$$

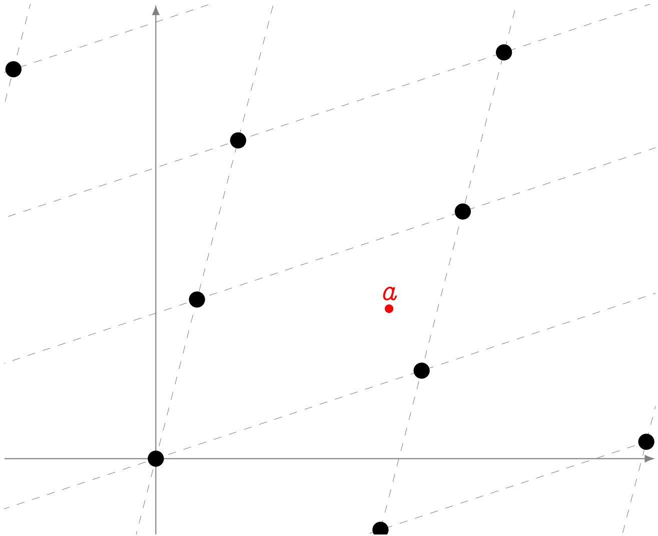
# Homotheties




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

$$\alpha\Lambda_1 = \Lambda_2$$

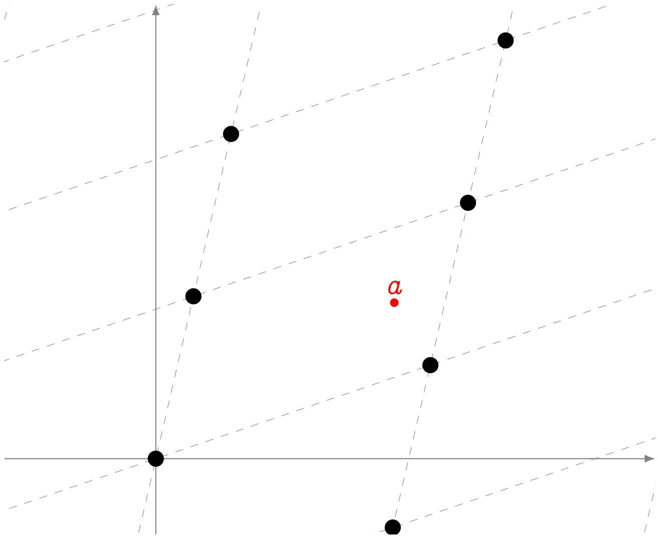
# Homotheties




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

$$\alpha\Lambda_1 = \Lambda_2$$

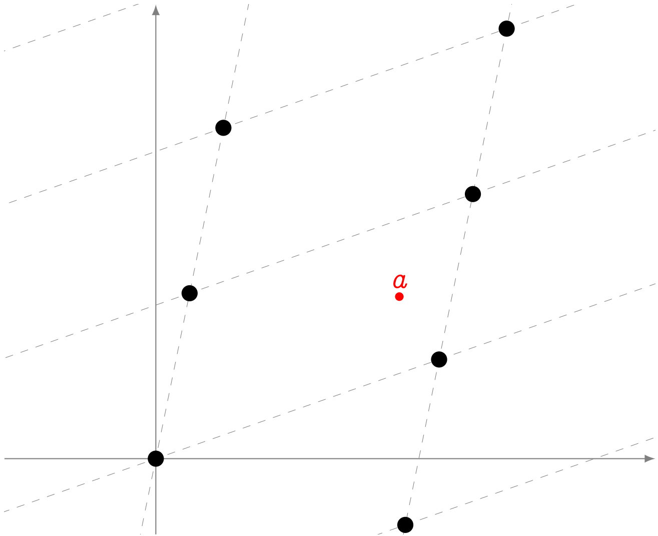
# Homotheties




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

$$\alpha\Lambda_1 = \Lambda_2$$

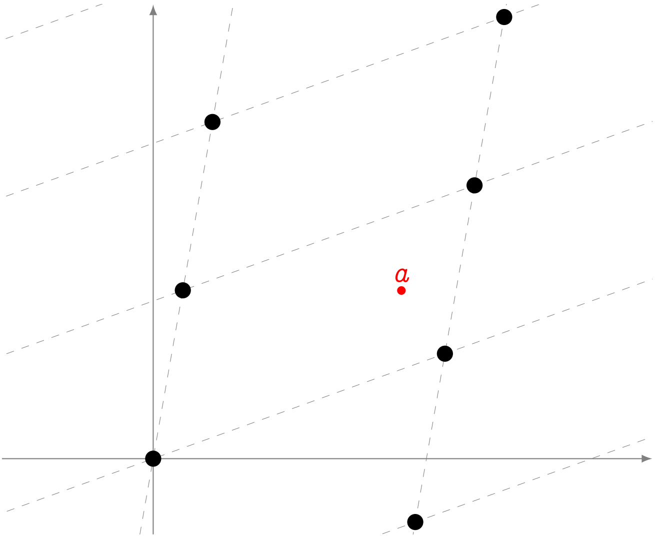
# Homotheties




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

$$\alpha \Lambda_1 = \Lambda_2$$

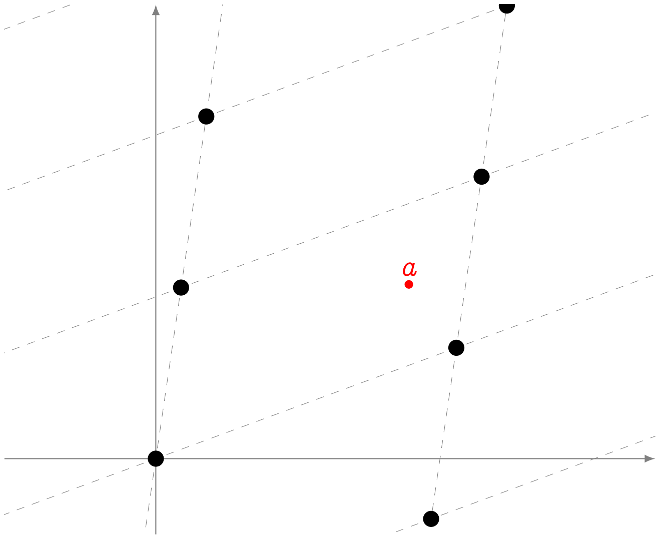
# Homotheties




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

$$\alpha\Lambda_1 = \Lambda_2$$

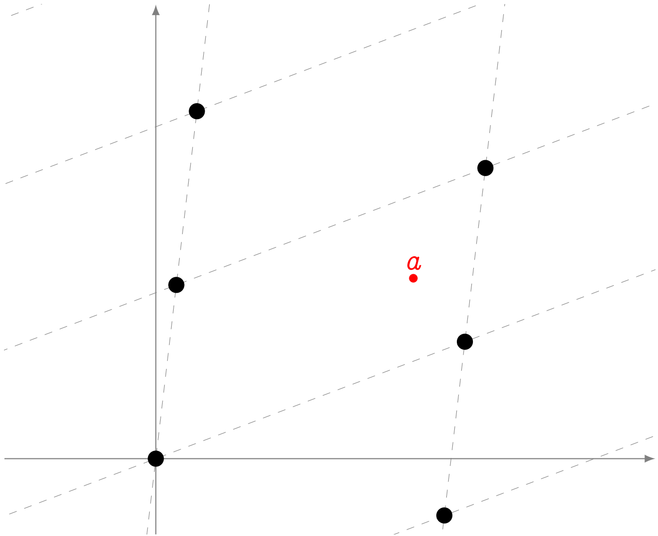
# Homotheties




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

$$\alpha\Lambda_1 = \Lambda_2$$

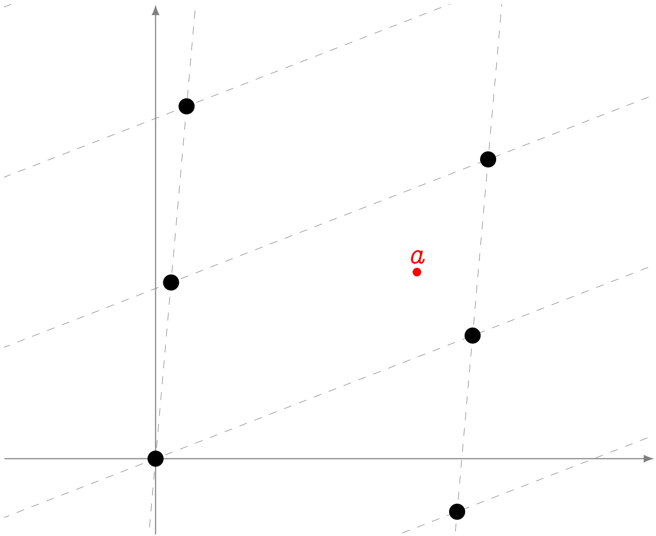
# Homotheties




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

$$\alpha\Lambda_1 = \Lambda_2$$

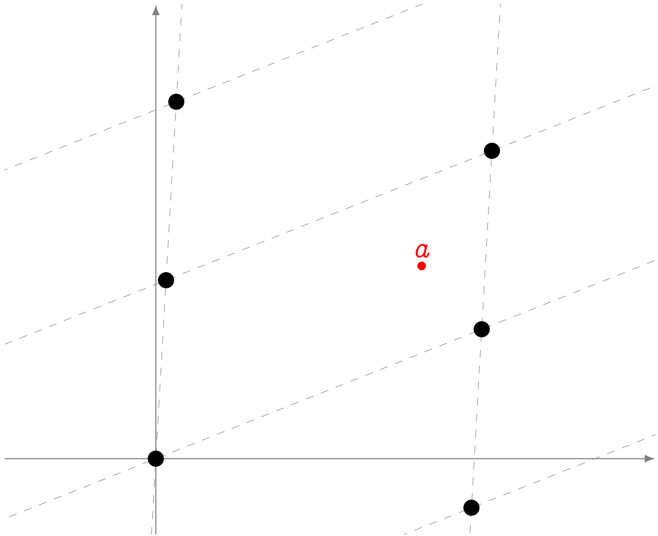
# Homotheties




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

$$\alpha\Lambda_1 = \Lambda_2$$

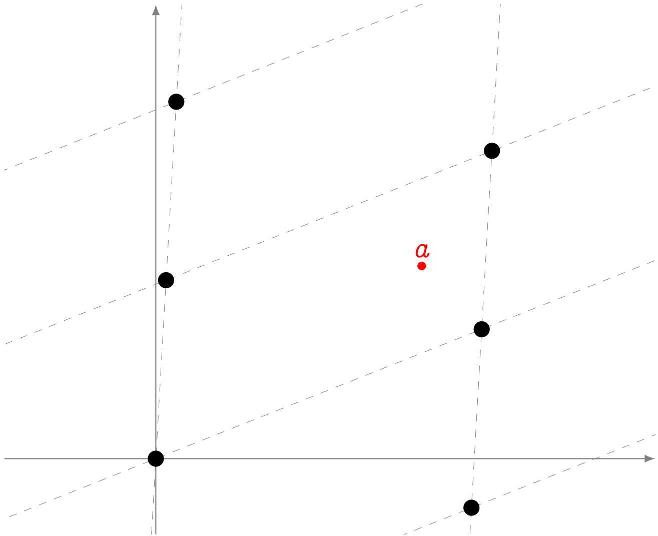
# Homotheties




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 $\Lambda$ 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 $\Lambda$ be a complex lattice, the modular $j$-invariant is

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

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

# Elliptic curves over $\mathbb{C}$

## Weierstrass $\wp$ function

Let $\Lambda$ be a complex lattice, the Weierstrass $\wp$ function associated to $\Lambda$ 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 $\Lambda$, 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 $\Lambda$ 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

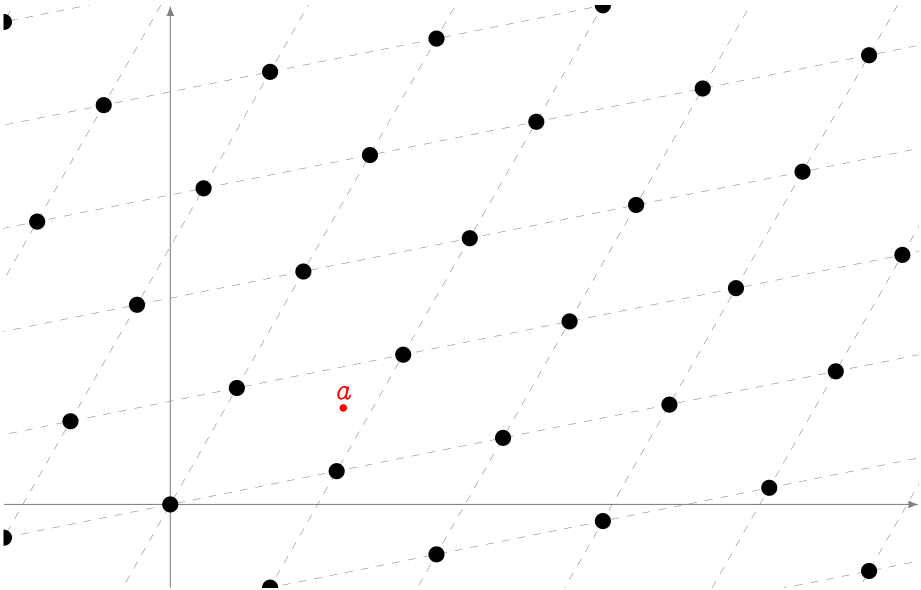
$$E \;:\; y^2 = x^3 + ax + b$$

there is a unique complex lattice $\Lambda$ such that

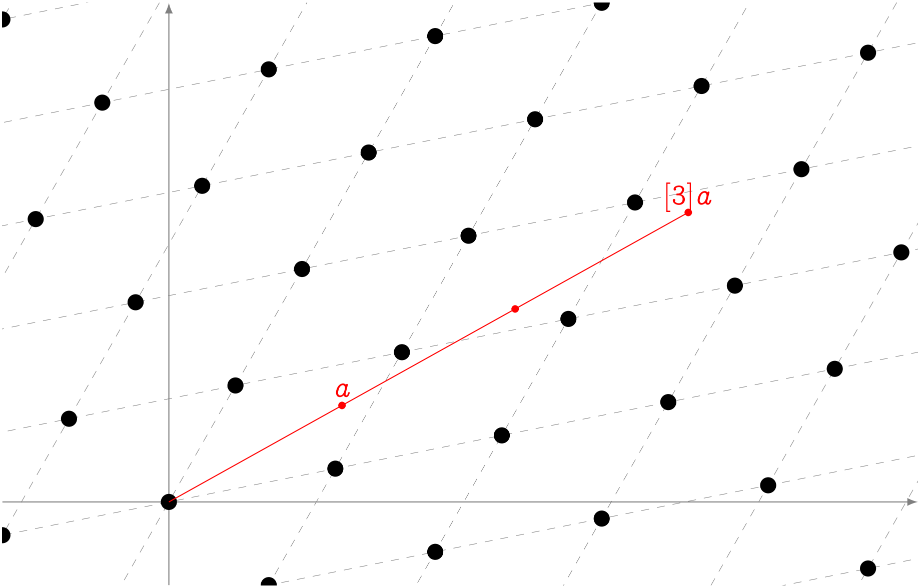
$$g_2(\Lambda) = -4a, \qquad g_3(\Lambda) = -4b.$$

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

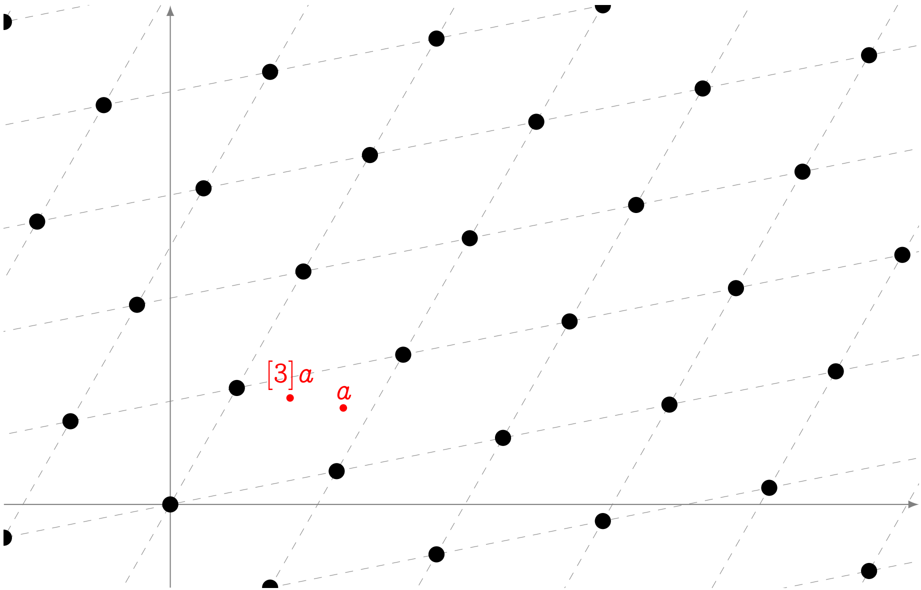
# Multiplication



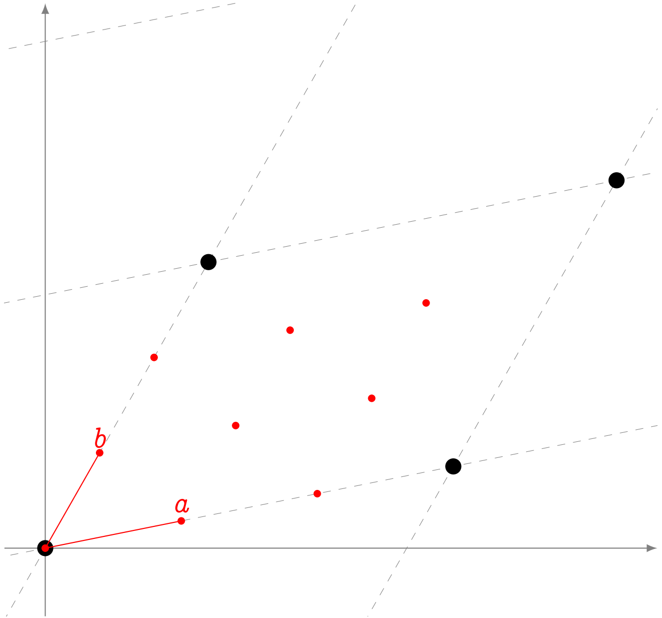
# Multiplication



# Multiplication



# Torsion subgroups



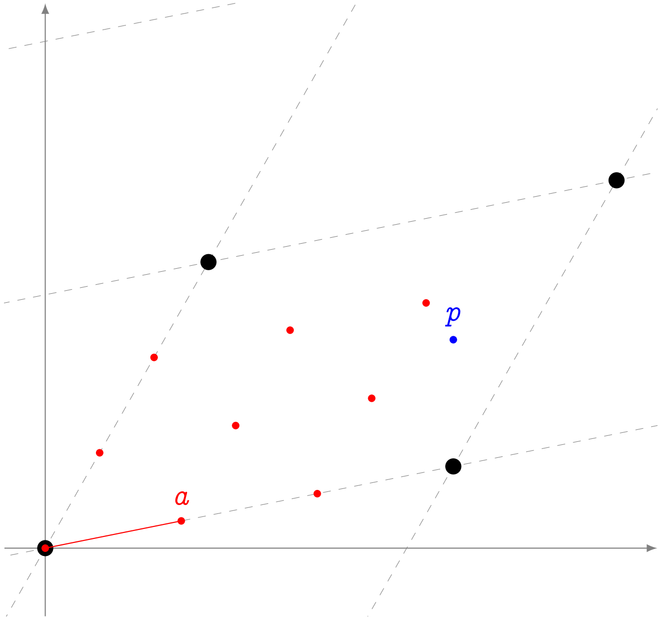

The $\ell$-torsion subgroup is made up by the points

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

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 $\ell$-torsion point, and let

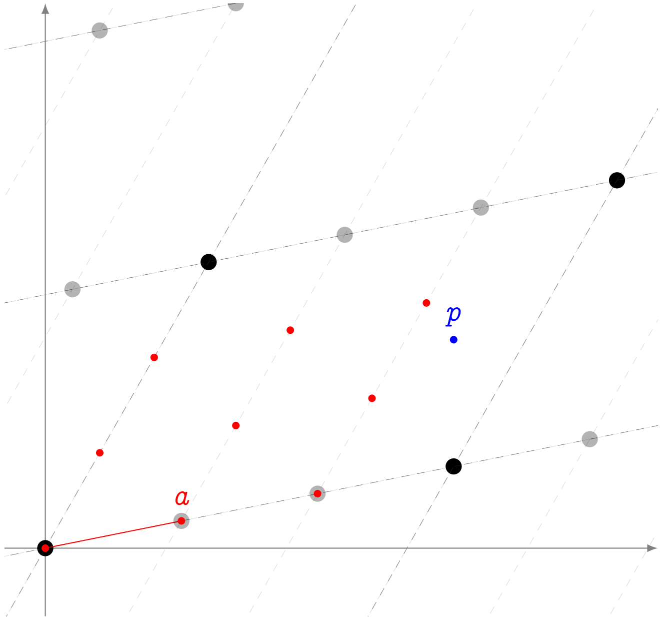
$$\Lambda_2 = a\mathbb{Z} \oplus \Lambda_1$$

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

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

$\phi$ is a morphism of complex Lie groups and is called an isogeny.

# Isogenies




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

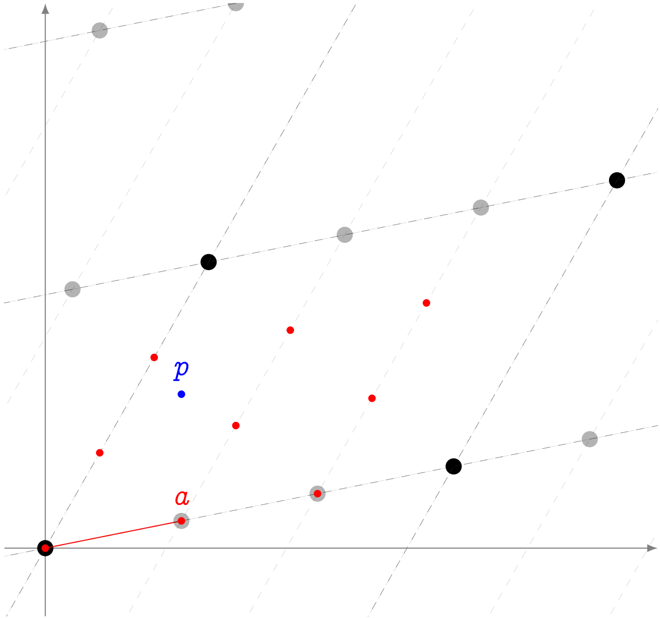
$$\Lambda_2 = a\mathbb{Z} \oplus \Lambda_1$$

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

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

$\phi$ is a morphism of complex Lie groups and is called an isogeny.

# Isogenies




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

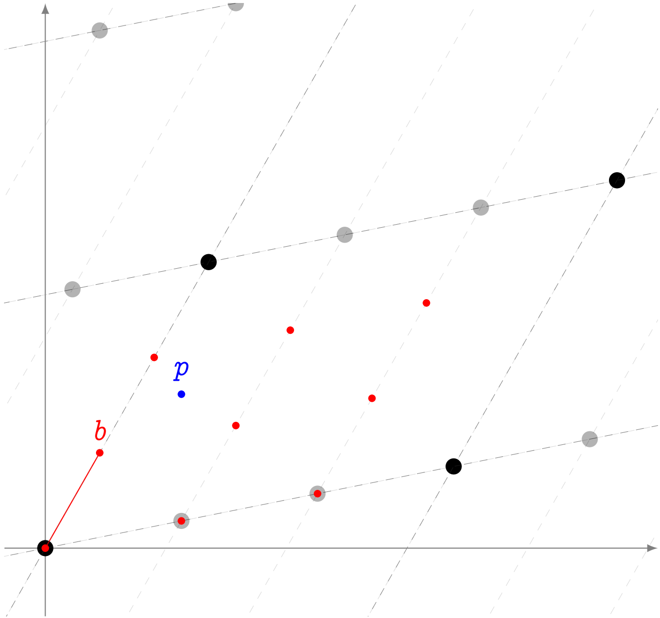
$$\Lambda_2 = a\mathbb{Z} \oplus \Lambda_1$$

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

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

$\phi$ is a morphism of complex Lie groups and is called an isogeny.

# Isogenies



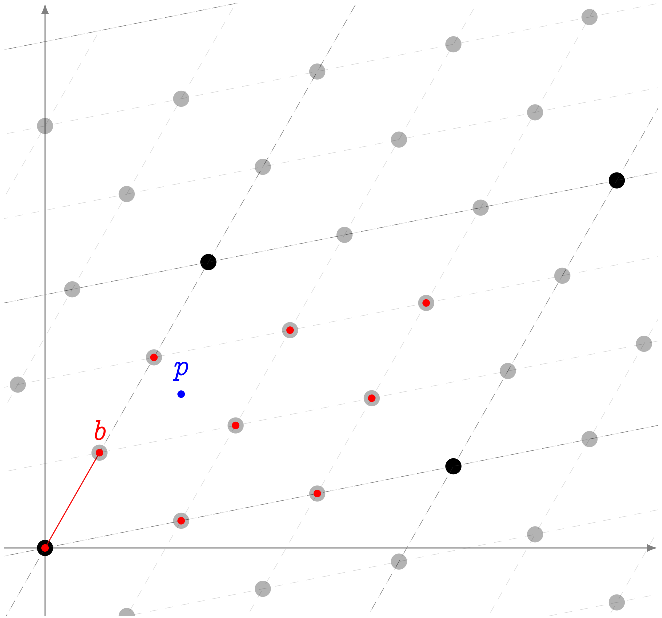

Taking a point $b$ not in the kernel of $\phi$, we obtain a new degree $\ell$ cover

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

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

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

# Isogenies



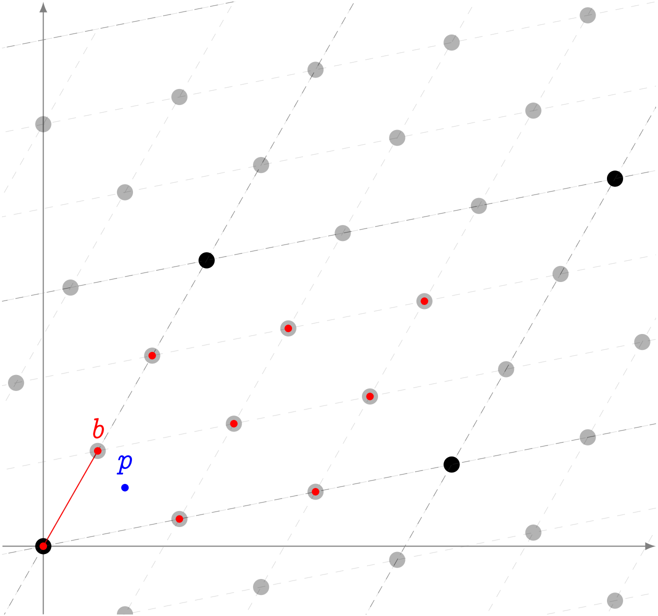

Taking a point $b$ not in the kernel of $\phi$, we obtain a new degree $\ell$ cover

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

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

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

# Isogenies




Taking a point $b$ not in the kernel of $\phi$, we obtain a new degree $\ell$ cover

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

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

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

# 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 $\phi$ is $\deg \phi = [k(E) : \phi^* k(E')]$. It is always finite.
2. $\phi$ is said to be separable, inseparable, or purely inseparable if the extension of function fields is.
3. If $\phi$ is separable, then $\deg \phi = \# \ker \phi$.
4. If $\phi$ 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 $\phi$ is $\deg \phi = [k(E) : \phi^* k(E')]$. It is always finite.
2. $\phi$ is said to be separable, inseparable, or purely inseparable if the extension of function fields is.
3. If $\phi$ is separable, then $\deg \phi = \# \ker \phi$.
4. If $\phi$ 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 $\phi$, 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 $\phi$; it has the following properties:

1. $\hat{\phi}$ is defined over $k$ if and only if $\phi$ 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 $\infty$)

# The finite field case

## Theorem (Hasse)

Let $E$ be defined over a finite field. Its Frobenius endomorphism $\pi$ 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 $\pi$. 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, $\pi$ 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 $d' | d$.

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

# Isogeny volcanoes

## Serre-Tate theorem reloaded

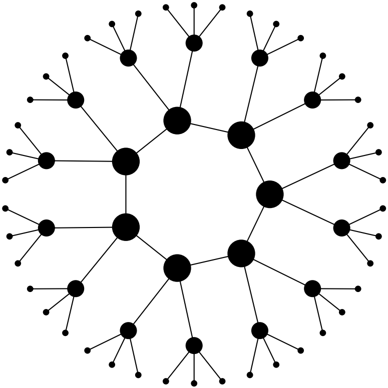
Two elliptic curves $E$, $E'$ defined over a finite field are isogenous iff their endomorphism algebras $\mathrm{End}(E) \otimes \mathbb{Q}$ and $\mathrm{End}(E') \otimes \mathbb{Q}$ are isomorphic.

### Isogeny graphs

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

### Isogeny volcanoes

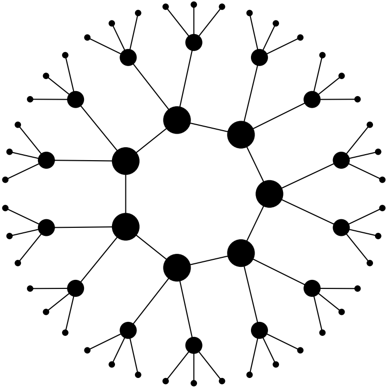
- Curves are ordinary,
- Isogenies all have degree a prime $\ell$.

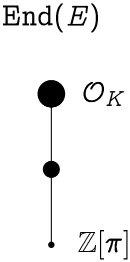


# Volcanology I

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

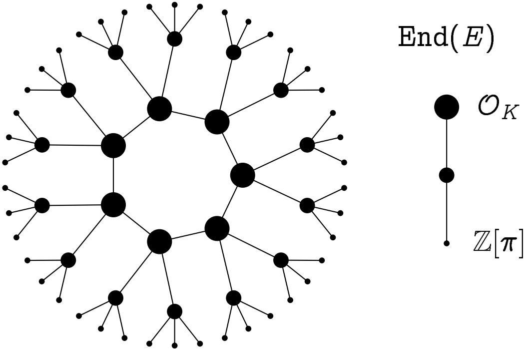
if $\mathcal{O} = \mathcal{O}'$, $\phi$ is horizontal;
if $[\mathcal{O}' : \mathcal{O}] = \ell$, $\phi$ is ascending;
if $[\mathcal{O} : \mathcal{O}'] = \ell$, $\phi$ is descending.






Isogeny volcano of degree $\ell = 3$.

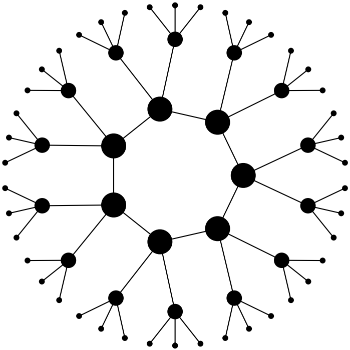
# Volcanology II

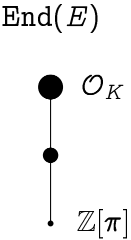



| | | **Horizontal** | **Ascending** | **Descending** |
|---|---|---|---|---|
| $\ell \nmid [\mathcal{O}_K : \mathcal{O}]$ | $\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$ | $1 + \left(\frac{D_K}{\ell}\right)$ | | |
| $\ell \nmid [\mathcal{O}_K : \mathcal{O}]$ | $\ell \mid [\mathcal{O} : \mathbb{Z}[\pi]]$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

# Volcanology II

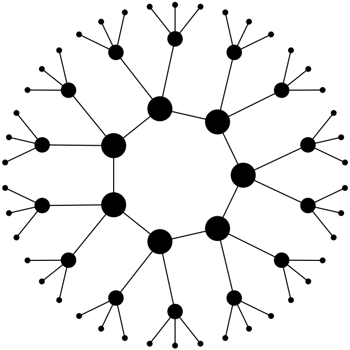
Height $= v_\ell([\mathcal{O}_K : \mathbb{Z}[\pi]])$.

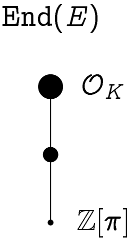





| | | **Horizontal** | **Ascending** | **Descending** |
|---|---|---|---|---|
| $\ell \nmid [\mathcal{O}_K : \mathcal{O}]$ | $\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$ | $1 + \left(\frac{D_K}{\ell}\right)$ | | |
| $\ell \nmid [\mathcal{O}_K : \mathcal{O}]$ | $\ell \mid [\mathcal{O} : \mathbb{Z}[\pi]]$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

# Volcanology II






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

How large is the crater?

| | | **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 | $\ell$ |
| $\ell \mid [\mathcal{O}_K : \mathcal{O}]$ | $\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$ | | 1 | |

# 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

## 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., $\phi$ 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 an $\ell$-volcano, and the crater contains $h(\mathrm{End}(E))$ curves.*

# Supersingular graphs

- Every supersingular curve is defined over $\mathbb{F}_{p^2}$.
- For every maximal order type of the quaternion algebra $\mathbb{Q}_{p,\infty}$ 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 $\sim p/12$.
- Left ideals act on the set of maximal orders like isogenies.
- The graph of $\ell$-isogenies is $(\ell+1)$-regular.

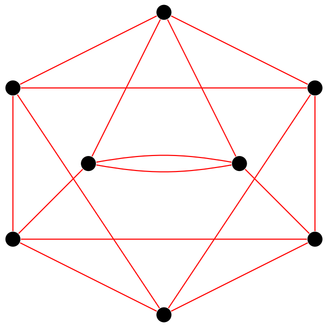


Figure: 3-isogeny graph on $\mathbb{F}_{97^2}$.

# Overview

1. Foundations
   - Elliptic curves
   - Isogenies
   - Complex multiplication

2. Isogeny-based cryptography
   - Isogeny walks
   - Key exchange from ordinary graphs
   - Key exchange from supersingular graphs
   - The SIKE submission

# Isogeny graphs

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

## Ordinary case

- $\ell$-isogeny graphs form volcanoes.
- The height of the volcano is given by the conductor of $\mathbb{Z}[\pi]$.
- All curves on the same level have the same endomorphism ring (have complex multiplication by the same order $\mathcal{O}$).
- Type of summit (one curve, two curves, crater) determined by $\left(\frac{D}{\ell}\right)$.
- Size of the crater is $h(\mathcal{O})$, and $\mathrm{Cl}(\mathcal{O})$ acts on it.

## Supersingular case

- There are $\sim p/12$ supersingular $j$-invariants, all defined over $\mathbb{F}_{p^2}$.
- $\ell$-isogeny graphs are $(\ell+1)$-regular and connected.

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

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

In the ordinary case, for all primes $\ell \nmid t^2 - 4q$:

- 50% of $\ell$-isogeny graphs are isolated points, $\left(\frac{D_K}{\ell}\right) = -1$
- 50% of $\ell$-isogeny graphs are cycles. $\left(\frac{D_K}{\ell}\right) = +1$

## 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.

# Isogeny based cryptography is 20 years old!

1996 Couveignes suggests isogeny-based key-exchange at a seminar in École Normale Supérieure;

1997 He submits "Hard Homogeneous Spaces" to Crypto;

# Isogeny based cryptography is 20 years old!

1996 Couveignes suggests isogeny-based key-exchange at a seminar in École Normale Supérieure;

1997 He submits “Hard Homogeneous Spaces” to Crypto;

1997 His paper gets rejected;

# Isogeny based cryptography is 20 years old!

| | |
|---|---|
| 1996 | Couveignes suggests isogeny-based key-exchange at a seminar in École Normale Supérieure; |
| 1997 | He submits "Hard Homogeneous Spaces" to Crypto; |
| 1997 | His paper gets rejected; |
| 1997–2006 | …Nothing happens for about 10 years. |

# Isogeny based cryptography is 20 years old!

- **1996** Couveignes suggests isogeny-based key-exchange at a seminar in École Normale Supérieure;
- **1997** He submits “Hard Homogeneous Spaces” to Crypto;
- **1997** His paper gets rejected;
- **1997–2006** …Nothing happens for about 10 years.

Ok. Let’s move on to the next 10 years!

# Isogeny problems

## Isogeny computation

Given an elliptic curve $E$ with Frobenius endomorphism $\pi$, and a subgroup $G \subset E$ such that $\pi(G) = G$, compute the rational fractions and the image curve of the separable isogeny $\phi : E \to E/G$.

## Explicit isogeny

Given two elliptic curves $E$, $E'$ over a finite field, isogenous of known degree $d$, find an isogeny $\phi : E \to E'$ of degree $d$.

## Isogeny walk

Given two elliptic curves $E$, $E'$ over a finite field $k$, such that $\#E = \#E'$, find an isogeny $\phi : E \to E'$ of smooth degree.

# Isogeny problems

## Isogeny computation $\mathrm{poly}(\#G)$

Given an elliptic curve $E$ with Frobenius endomorphism $\pi$, and a subgroup $G \subset E$ such that $\pi(G) = G$, compute the rational fractions and the image curve of the separable isogeny $\phi : E \to E/G$.

## Explicit isogeny

Given two elliptic curves $E$, $E'$ over a finite field, isogenous of known degree $d$, find an isogeny $\phi : E \to E'$ of degree $d$.

## Isogeny walk

Given two elliptic curves $E$, $E'$ over a finite field $k$, such that $\#E = \#E'$, find an isogeny $\phi : E \to E'$ of smooth degree.

# Isogeny problems

## Isogeny computation  poly($\#G$)

Given an elliptic curve $E$ with Frobenius endomorphism $\pi$, and a subgroup $G \subset E$ such that $\pi(G) = G$, compute the rational fractions and the image curve of the separable isogeny $\phi : E \to E/G$.

## Explicit isogeny  poly($d$)

Given two elliptic curves $E$, $E'$ over a finite field, isogenous of known degree $d$, find an isogeny $\phi : E \to E'$ of degree $d$.

## Isogeny walk

Given two elliptic curves $E$, $E'$ over a finite field $k$, such that $\#E = \#E'$, find an isogeny $\phi : E \to E'$ of smooth degree.

# Isogeny problems

## Isogeny computation — $\mathrm{poly}(\#G)$

Given an elliptic curve $E$ with Frobenius endomorphism $\pi$, and a subgroup $G \subset E$ such that $\pi(G) = G$, compute the rational fractions and the image curve of the separable isogeny $\phi : E \to E/G$.

## Explicit isogeny — $\mathrm{poly}(d)$

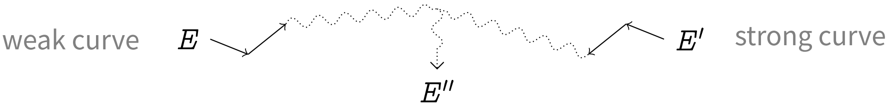
Given two elliptic curves $E$, $E'$ over a finite field, isogenous of known degree $d$, find an isogeny $\phi : E \to E'$ of degree $d$.

## Isogeny walk — $\exp(\log \#k)$

Given two elliptic curves $E$, $E'$ over a finite field $k$, such that $\#E = \#E'$, find an isogeny $\phi : E \to E'$ of smooth degree.

# Isogeny walks and cryptanalysis[2] (circa 2000)

Fact: Having a weak DLP is not (always) isogeny invariant.




## Fourth root attacks

- Start two random walks from the two curves and wait for a collision.
- Over $\mathbb{F}_q$, the average size of an isogeny class is $h(\mathcal{O}_K) \sim \sqrt{q}$.
- A collision is expected after $O(\sqrt{h(\mathcal{O}_K)}) = O(q^{\frac{1}{4}})$ steps.

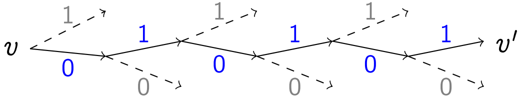
Note: Can be used to build trapdoor systems[1].

[1] Teske 2006.

[2] Galbraith 1999; Galbraith, Hess, and Smart 2002; Bisson and Sutherland 2011.

# 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.

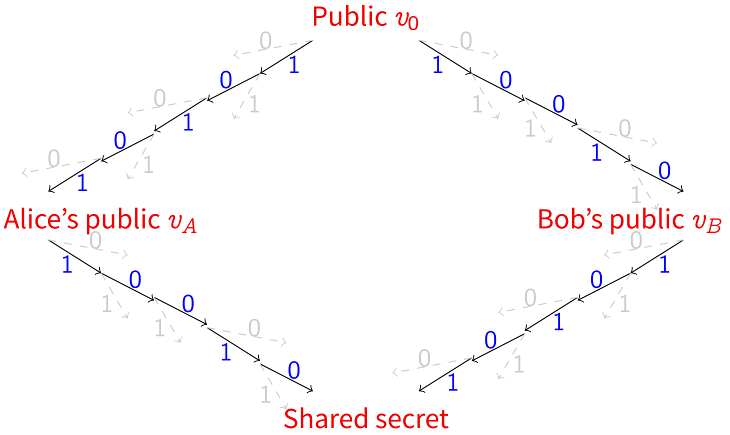
## Provably secure hash functions

- Use the expander graph of supersingular 2-isogenies;[a]
- Collision resistance = hardness of finding cycles in the graph;
- Preimage resistance = hardness of finding a path from $v$ to $v'$.

[a] Charles, K. E. Lauter, and Goren 2009; Doliskani, Pereira, and Barreto 2017.

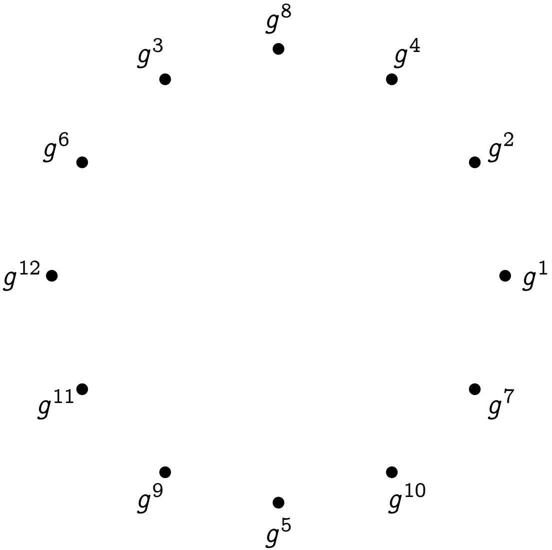
# Random walks and key exchange

Let's try something harder...



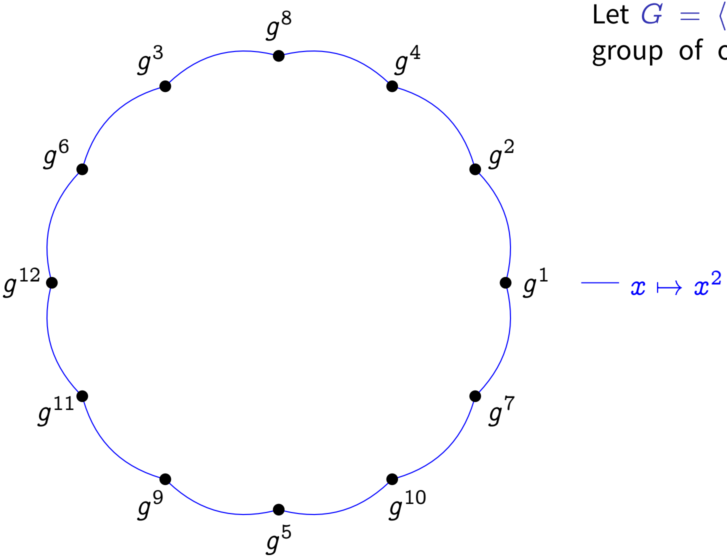

...is this even possible?

# Expander graphs from groups



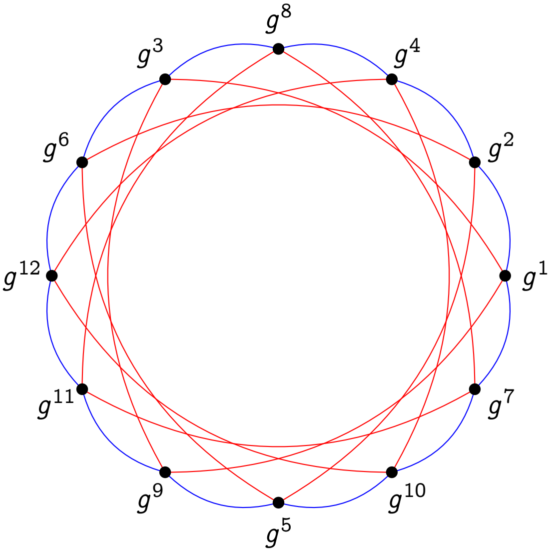

Let $G = \langle g \rangle$ be a cyclic group of order $p$.

# Expander graphs from groups




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

# Expander graphs from groups

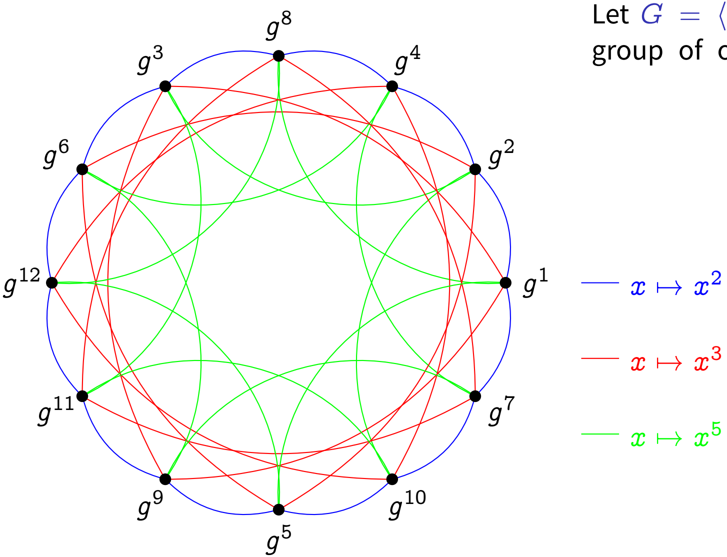



Let $G = \langle g \rangle$ be a cyclic group of order $p$.

$x \mapsto x^2$

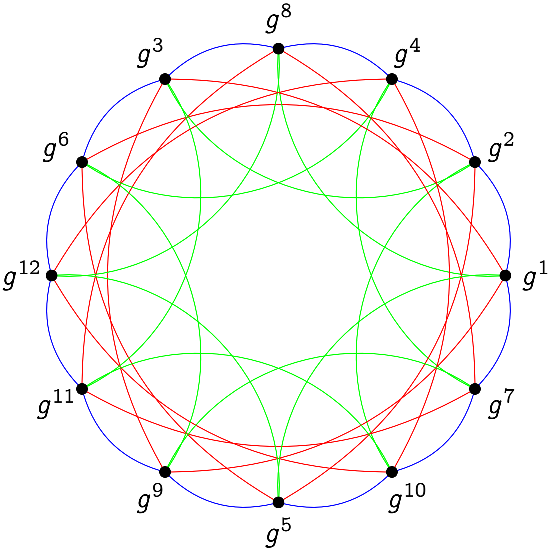
$x \mapsto x^3$

# 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. $S^{-1} \subset S$.

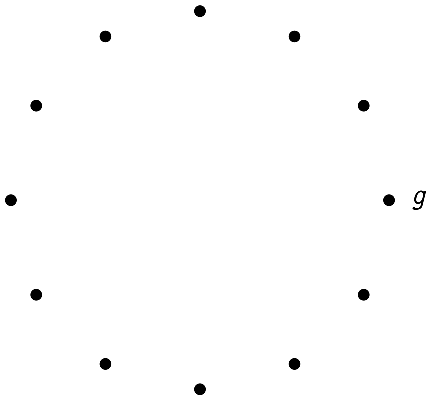
The Schreier graph of $(S, G \setminus \{1\})$ is (usually) an expander.

— $x \mapsto x^2$

— $x \mapsto x^3$

— $x \mapsto x^5$

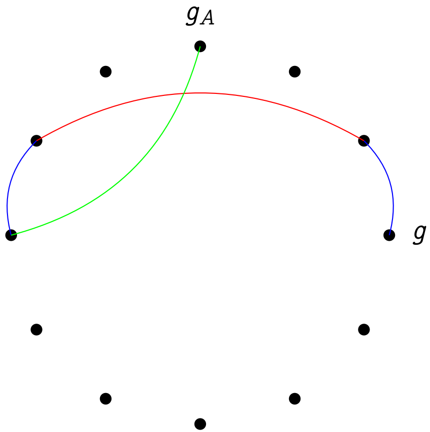
# Key exchange from Schreier graphs




**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

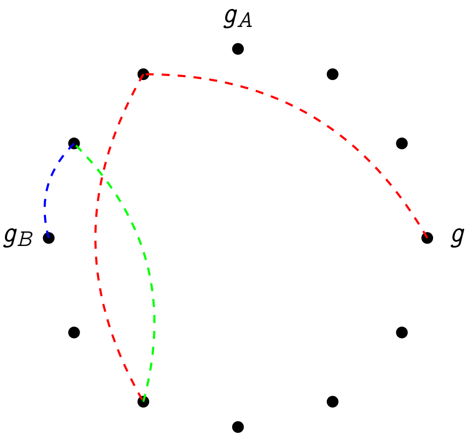



**Public parameters:**

- 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

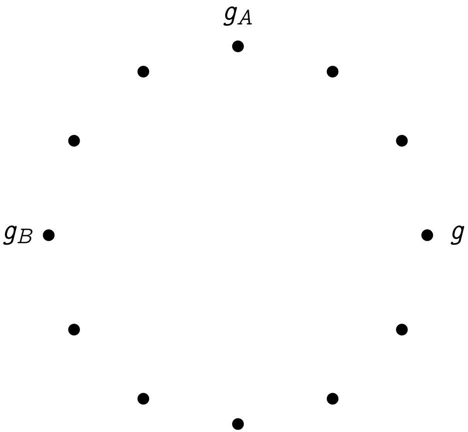



**Public parameters:**

- 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

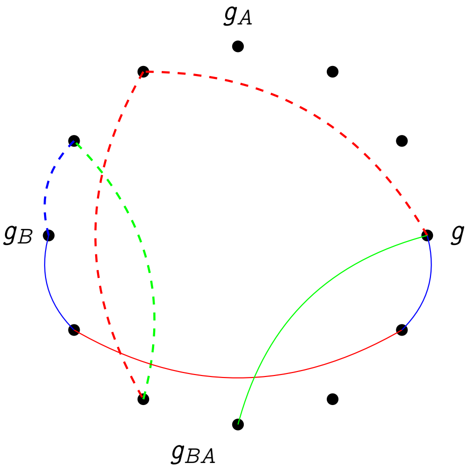



**Public parameters:**

- 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

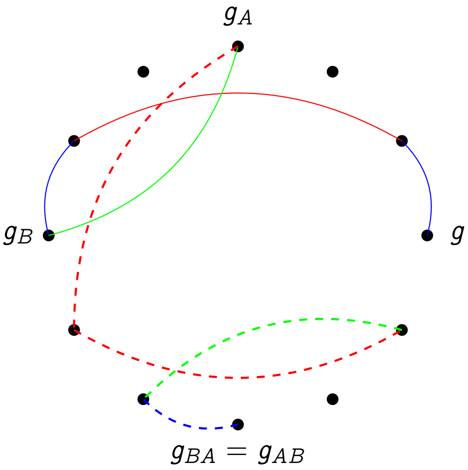



**Public parameters:**

- 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

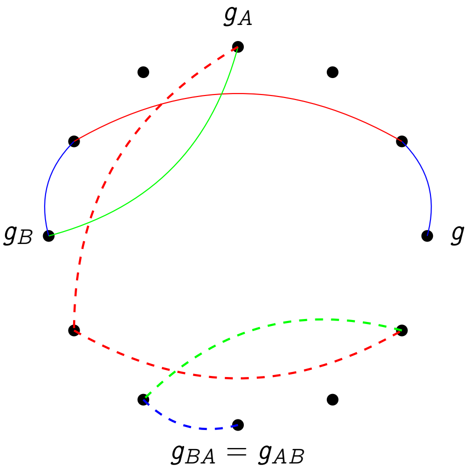



**Public parameters:**

- 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

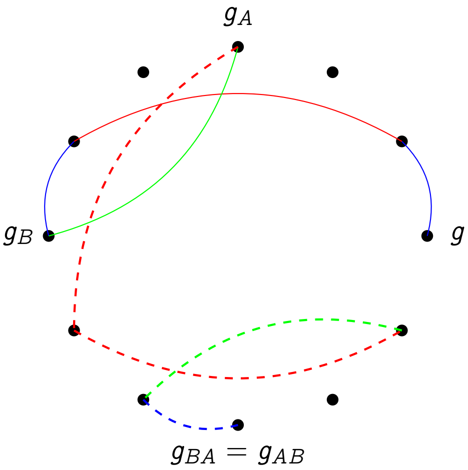



**Why does this work?**

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

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

# Key exchange from Schreier graphs



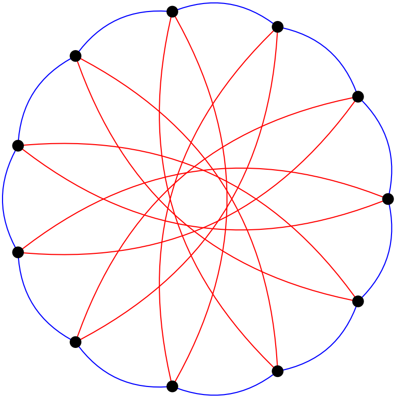

**Why does this work?**

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

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!

# Group action on isogeny graphs



—— $\ell_1$-isogenies

—— $\ell_2$-isogenies

- There is a group action of the ideal class group $\mathrm{Cl}(\mathcal{O})$ on the set of ordinary curves with complex multiplication by $\mathcal{O}$.
- Its Schreier graph is an isogeny graph (and an expander if we take enough generators)

# Key exchange in graphs of ordinary isogenies[3] (circa 2006)

Parameters:

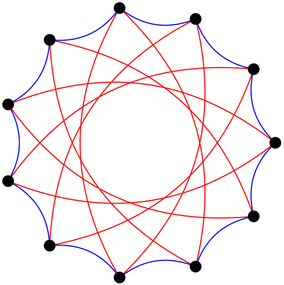
- $E/\mathbb{F}_p$ ordinary elliptic curve with *Frobenius endomorphism* $\pi$,
- primes $\ell_1$,$\ell_2$,... such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.
- A *direction* for each $\ell_i$ (i.e. a choice of a root of $\pi^2 - t\pi + q \mod \ell$).

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

$$\begin{tikzcd}
 & E \arrow[dl, "\ell_1^{a_1}\ell_2^{a_2}\cdots = \mathcal{N}(\mathfrak{a})"'] \arrow[dr, "\mathcal{N}(\mathfrak{b}) = \ell_1^{b_1}\ell_2^{b_2}\cdots"] & \\
\mathfrak{a} * E \arrow[dr] & & \mathfrak{b} * E \arrow[dl] \\
 & \mathfrak{ab} * E = \mathfrak{ba} * E &
\end{tikzcd}$$

[3] Couveignes 2006; Rostovtsev and Stolbunov 2006.

# CRS key exchange



Key generation: compose small degree isogenies
(Isogeny Computation Problem)
polynomial in the length of the random walk.

Attack: Isogeny Walk Problem
polynomial in the degree, exponential in the length.

Open problem: Make this thing practical!

# Security of CRS

Size of the graph: $h(\mathcal{O}) \sim \sqrt{p}$,

Key space size: Exponential in the number of primes $\ell_1$,$\ell_2$,...

Meet in the middle attack: $O(\sqrt[4]{p})$.

## The Abelian Hidden Shift Problem

Let $G$ be a group and $S$ be a set. Given two oracles $f_0, f_1 : G \to S$ such that $f_0(g) = f_1(gs)$ for some $s \in G$, find $s$.

## Ordinary isogeny walk $\to$ Hidden shift

To find a secret isogeny walk $E_0 \to E_1$, set

$$f_0 : \mathrm{Cl}(\mathcal{O}) \to V \qquad \mathfrak{a} \mapsto \mathfrak{a} * E_0$$

$$f_1 : \mathrm{Cl}(\mathcal{O}) \to V \qquad \mathfrak{a} \mapsto \mathfrak{a} * E_1$$

Then the hidden shift is $\mathfrak{s}$ such that $\mathfrak{s} * E_0 = E_1$.

# Quantum attack on CRS[4]

1. $L_p(1/2, \sqrt{3}/2)$ classical algorithm for evaluating $f_0, f_1$.
2. Hidden Shift Problem $\rightarrow$ Dihedral Hidden Subgroup Problem.

## Quantum algorithms for dihedral HSP

Kuperberg[a]: $2^{O(\sqrt{\log|G|})}$ quantum time, space and query complexity.

Regev[b]: $L_{|G|}(\frac{1}{2}, \sqrt{2})$ quantum time and query complexity, $\mathrm{poly}(\log(|G|)$ quantum space.

[a] Kuperberg 2005.
[b] Regev 2004.

[4] Childs, Jao, and Soukharev 2010.

# 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.

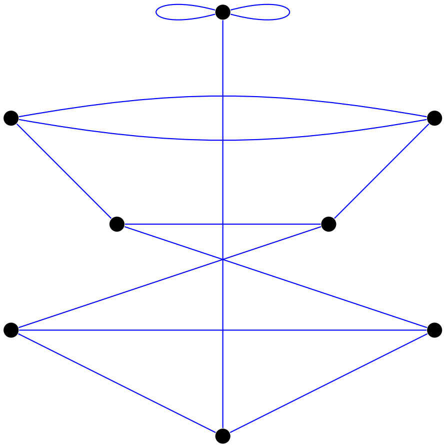


Figure: 2- and 3-isogeny graphs on $\mathbb{F}_{97^2}$.

# 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.

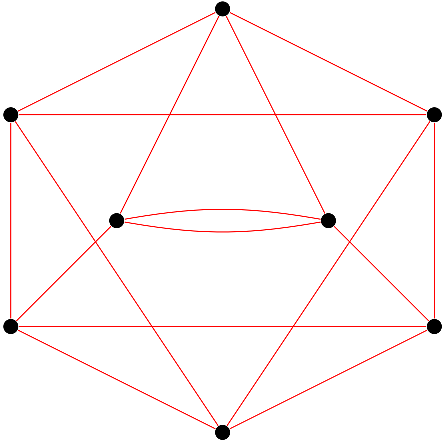


Figure: 2- and 3-isogeny graphs on $\mathbb{F}_{97^2}$.

# 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.

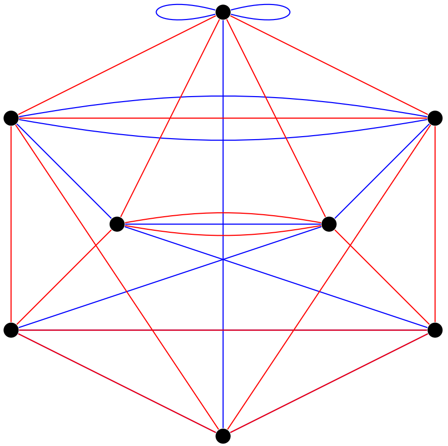


Figure: 2- and 3-isogeny graphs on $\mathbb{F}_{97^2}$.

# Key exchange with supersingular curves

- Fix small primes $\ell_A$, $\ell_B$;
- No canonical labeling of the $\ell_A$- and $\ell_B$-isogeny graphs; however…

**Walk of length $e_A$**

$=$

**Isogeny of degree $\ell_A^{e_A}$**

$=$

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

$$\ker\phi = \langle P\rangle \subset E[\ell_A^{e_A}]$$
$$\ker\psi = \langle Q\rangle \subset E[\ell_B^{e_B}]$$
$$\ker\phi' = \langle\psi(P)\rangle$$
$$\ker\psi' = \langle\phi(Q)\rangle$$

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

# Supersingular Isogeny Diffie-Hellman[5]

**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:**

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

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

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

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

# Supersingular Isogeny Diffie-Hellman[5]

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:

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

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

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

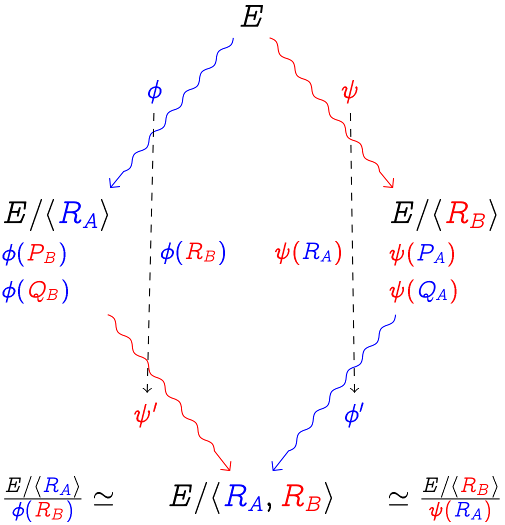
# Supersingular Isogeny Diffie-Hellman[5]

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:

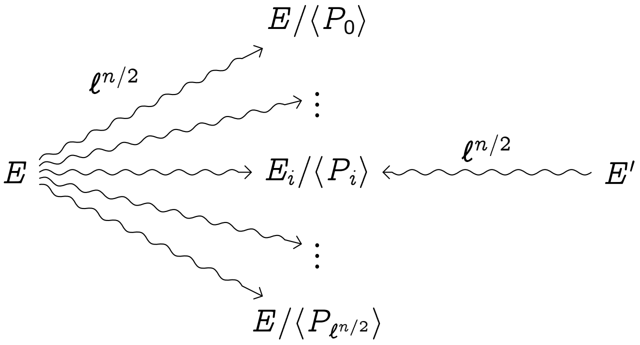
- $R_A = m_A P_A + n_A Q_A$,
- $R_B = m_B P_B + n_B Q_B$,




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

# Generic attacks

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




- With high probability $\phi$ is the unique collision (or *claw*) $O(\ell^{n/2})$.
- A quantum claw finding[6] algorithm solves the problem in $O(\ell^{n/3})$.

[6] 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[7]

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 $\psi$;
- 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.

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

# Bonus: a ZK proof of knowledge[8]

Secret: knowledge of the kernel of a degree $\ell_A^{e_A}$ isogeny from $E$ to $E/\langle S\rangle$.

$$E \xrightarrow{\quad\quad\phi\quad\quad} E/\langle S\rangle$$

[8] De Feo, Jao, and Plût 2014.

# Bonus: a ZK proof of knowledge[8]

Secret: knowledge of the kernel of a degree $\ell_A^{e_A}$ isogeny from $E$ to $E/\langle S\rangle$.

$$
\begin{tikzcd}
E \arrow[r, dash, "\phi"] \arrow[d, dash, "?"'] & E/\langle S\rangle \arrow[d, dash, "?"] \\
E/\langle P\rangle \arrow[r, dash, "?"'] & E/\langle P, S\rangle
\end{tikzcd}
$$

1. Choose a random point $P \in E[\ell_B^{e_B}]$, compute the diagram;
2. Publish the curves $E/\langle P\rangle$ and $E/\langle P, S\rangle$;

[8] De Feo, Jao, and Plût 2014.

# Bonus: a ZK proof of knowledge[8]

Secret: knowledge of the kernel of a degree $\ell_A^{e_A}$ isogeny from $E$ to $E/\langle S\rangle$.

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

1. Choose a random point $P \in E[\ell_B^{e_B}]$, compute the diagram;
2. Publish the curves $E/\langle P\rangle$ and $E/\langle P, S\rangle$;
3. The verifier asks one of the two questions:
   - Reveal the degree $\ell_B^{e_B}$ isogenies;

[8] De Feo, Jao, and Plût 2014.

# Bonus: a ZK proof of knowledge[8]

Secret: knowledge of the kernel of a degree $\ell_A^{e_A}$ isogeny from $E$ to $E/\langle S\rangle$.

$$\begin{tikzcd}
E \arrow[r, dash, "\phi"] \arrow[d, dash, "?"'] & E/\langle S\rangle \arrow[d, dash, "?"] \\
E/\langle P\rangle \arrow[r, dash, "\phi'"'] & E/\langle P, S\rangle
\end{tikzcd}$$

1. Choose a random point $P \in E[\ell_B^{e_B}]$, compute the diagram;
2. Publish the curves $E/\langle P\rangle$ and $E/\langle P, S\rangle$;
3. The verifier asks one of the two questions:
   - Reveal the degree $\ell_B^{e_B}$ isogenies;
   - Reveal the bottom isogeny.

[8] De Feo, Jao, and Plût 2014.

# Bonus: a ZK proof of knowledge[8]

Secret: knowledge of the kernel of a degree $\ell_A^{e_A}$ isogeny from $E$ to $E/\langle S\rangle$.

$$\begin{tikzcd}
E \arrow[r, no head, "\phi"] \arrow[d, no head, "?"'] & E/\langle S\rangle \arrow[d, no head, "?"] \\
E/\langle P\rangle \arrow[r, no head, "\phi'"'] & E/\langle P, S\rangle
\end{tikzcd}$$

1. Choose a random point $P \in E[\ell_B^{e_B}]$, compute the diagram;
2. Publish the curves $E/\langle P\rangle$ and $E/\langle P, S\rangle$;
3. The verifier asks one of the two questions:
   - Reveal the degree $\ell_B^{e_B}$ isogenies;
   - Reveal the bottom isogeny.

Can derive Fiat-Shamir signatures: secure under SIDH…but very slow!

[8] De Feo, Jao, and Plût 2014.

# 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.
- Download the package here.

| | $p$ | cl. security | q. security | speed | comm. |
|---|---|---|---|---|---|
| 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 |
| SIKEp964 | $2^{486}3^{301}-1$ | 241 bits | 161 bits | | 0.8KB |

# Parameter choices

For efficiency: $p = 2^a 3^b - 1$, with $a$ even;

For security:

$$a \sim (\log_2 3) b \geq \begin{cases} 2 \times \text{classical security parameter}, \\ 3 \times \text{quantum security parameter}; \end{cases}$$

For verifiability:

- Special starting curve $E_0 \ : \ y^2 = x^3 + x$;
- $P_A$, $Q_A$, $P_B$, $Q_B$ chosen as the lexicographically first points satisfying the necessary conditions.

# Implementation: finite field

## Arithmetic in $\mathbb{F}_p$

- $p = 2^a 3^b - 1$ lends itself to optimizations:
  - Adapted Comba-based Montgomery reduction[a],
  - Adapted Barret reduction[b];
  - Assembly optimized.

[a] Costello, Longa, and Naehrig 2016.
[b] Karmakar, Roy, Vercauteren, and Verbauwhede 2016.

## Arithmetic in $\mathbb{F}_{p^2}$

Because $p = -1 \mod 4$, then $-1$ is not a quadratic residue in $\mathbb{F}_p$. We define $\mathbb{F}_{p^2} = \mathbb{F}_p[i] = \mathbb{F}_p[X]/(X^2 + 1)$.

- Arithmetic similar to $\mathbb{Q}[i]$;
- Karatsuba-like formulas for multiplication and squaring;
- Inversion only requires one inversion in $\mathbb{F}_p$;
- Optimizations similar to pairing-base crypto (e.g., BN254).

# Implementation: curves

## Montgomery curves

Not a Weierstrass equation:

$$by^2 = x^3 + ax^2 + x$$

- Only possible for curves with a 4-torsion point (we're lucky);
- Very efficient arithmetic in $XZ$-coordinates: identify $\pm P$ by dropping the $Y$-coordinate

Doubling:

$$[2](X : \cdot : Z) = \left((X^2 - Z^2)^2 : \cdot : 4XZ(X^2 + aXZ + Z^2)\right)$$

Tripling:

$$[3](X : \cdot : Z) = \left(X(X^4 - 6X^2Z^2 - 4aXZ^3 - 3Z^4) : \cdot : Z(3X^4 + 4aX^3Z + 6X^2Z^3 - Z^4)\right)$$

# Implementation: curves

## Computing $mP + nQ$

- Observe that $mP + nQ$ and $P + (n/m)Q$ generate the same isogeny kernel;
- Constant time Montgomery ladder tailored[a] to $P + cQ$.
- For simplicity and constant-time sampling, SIKE secret keys are restricted to $P + cQ$ with $c \in [0, \dots, 2^x - 1]$.

[a] Faz-Hernández, López, Ochoa-Jiménez, and Rodríguez-Henríquez 2017.

**Input** $P = (X_P : Z_P), Q = (X_Q : Z_Q), P - Q = (X_{P-Q} : Z_{P-Q})$, a scalar $c$;

**Output** $P + cQ$.

1. Set $R_0 = Q, \quad R_1 = P, \quad R_2 = Q - P$
2. For $i$ from 0 to $\lfloor \log_2 c \rfloor$:
   - if $c_i = 0$, let $R_0, R_1 = 2R_0, \; R_0 + R_1$;
   - if $c_i = 1$, let $R_0, R_2 = 2R_0, \; R_0 + R_2$;
3. Return $R_1$.

# Implementation: isogenies

## Vélu's formulas

Given a group $G \subset E$, the isogeny $\phi : E \to E/G$ is defined by:

$$\phi(P) = \left( x(P) + \sum_{Q \in G \setminus \{\mathcal{O}\}} x(P+Q) - x(Q),\ \ y(P) + \sum_{Q \in G \setminus \{\mathcal{O}\}} y(P+Q) - y(Q) \right).$$

## 3-isogenies of Montgomery curves

Let $P = (X_3 : Z_3)$ be a point of order 3 on $by^2 = x^3 + ax^2 + x$. The curve $E/\langle P \rangle$ has equation $by^2 = x^3 + a'x^2 + x$ where

$$a' = (aX_3Z_3 + 6(Z_3^2 - X_3^2))X_3 / Z_3^3.$$

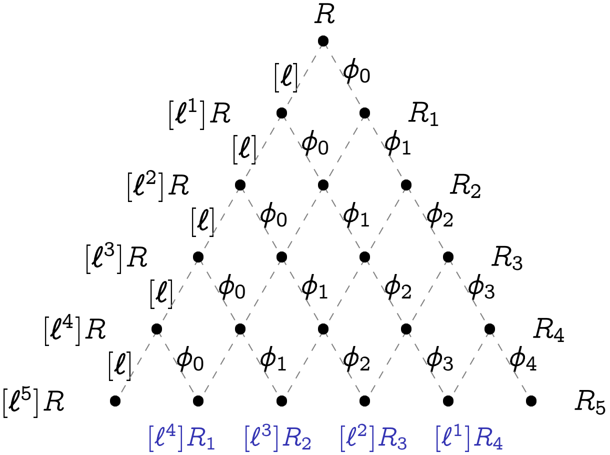
It is defined by the map

$$\phi(X : Z) = \left(X(X_3X - Z_3Z)^2 \ :\ Z(Z_3X - X_3Z)^2\right).$$

Similar formula for 4-isogenies.

# Implementation: isogeny walks

$\mathtt{ord}(R) = \ell^e$ and $\phi = \phi_0 \circ \phi_1 \circ \cdots \circ \phi_{e-1}$, each of degree $\ell$




For each $i$, one needs to compute $[\ell^{e-i}]R_i$ in order to compute $\phi_i$.

# Implementation: isogeny walks

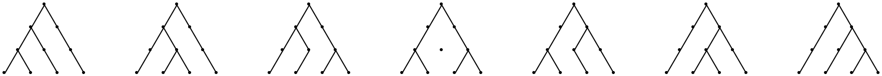


Figure: The seven well formed strategies for $e = 4$.

- Right edges are $\ell$-isogeny evaluation;
- Left edges are multiplications by $\ell$ (about twice as expensive);
- The best strategy can be precomputed offline and hardcoded.
- Evaluation is done in constant time!
- Pre-computed optimized strategies are given in the SIKE submission document.

# Example

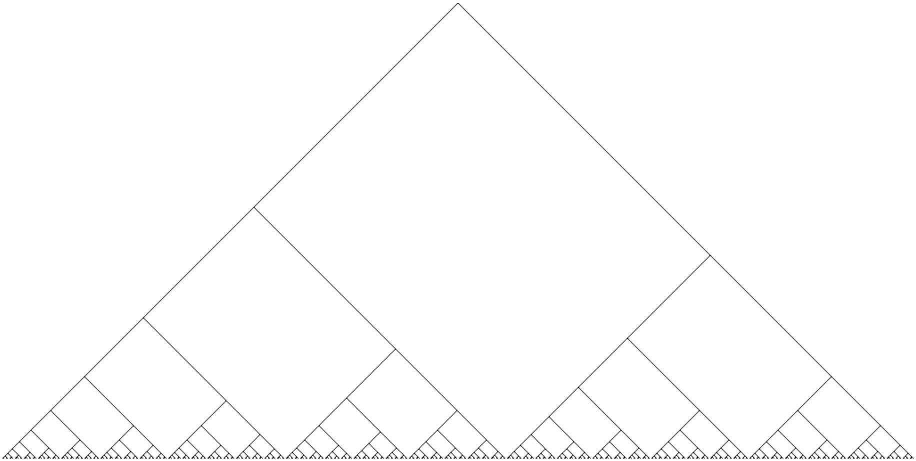


Figure: Optimal strategy for $e = 512, \ell = 2$.

# Implementation: constant time

- Secret key sampling in constant time by restricting key space;
- $P + cQ$ in constant time via Montgomery ladder;
- Isogeny walk in constant time via any strategy.

## Finite field operations in constant time

Only problem is to avoid inversions as much as possible, but Vélu's formulas require one inversion per curve on the walk.

**Solution**[a]**:** projectivize curve equations

$$E \ : \ CBy^2 = Cx^3 + Ax^2 + Cx.$$

- Slightly increases operation counts of formulas;
- Delays all inversions to the very end;
- Only the value $(A : C)$ is needed in computations. Then:

$$j(E) = \frac{256(A^2 - 3C^2)}{C^4(A^2 - 4C^2)}.$$

[a] Costello, Longa, and Naehrig 2016.

# Summary

## Public parameters:

- $p = 2^a 3^b - 1$,
- Staring curve $E \ : \ y^2 = x^3 + x$,
- Torsion generators

$$\begin{aligned} P_A &= (X_{a1} : Z_{a1}), & Q_A &= (X_{a2} : Z_{a2}), & P_A - Q_A &= (X_{a3} : Z_{a3}), \\ P_B &= (X_{b1} : Z_{b1}), & Q_B &= (X_{b2} : Z_{b2}), & P_B - Q_B &= (X_{b3} : Z_{b3}). \end{aligned}$$

## Secret keys:

- $R_A = P_A + cQ_A$ with $c \in [0, \dots, 2^a - 1]$,
- $R_B = P_A + cQ_A$ with $c \in [0, \dots, 2^{b\lfloor \log_2 3 \rfloor} - 1]$.

## Public keys (curve equation can be interpolated from three points):

- $\phi(P_B), \phi(Q_B), \phi(P_B - Q_B)$,
- $\psi(P_A), \psi(Q_A), \psi(P_A - Q_A)$.

## Shared secret:

- $j = 256(A^2 - 3C^2)/C^4(A^2 - 4C^2)$.

# Thank you

`http://defeo.lu/`

@luca_defeo

# References I


Pizer, Arnold K. (1990).
"Ramanujan graphs and Hecke operators."
In: Bull. Amer. Math. Soc. (N.S.) 23.1.

— (1998).
"Ramanujan graphs."
In: Computational perspectives on number theory (Chicago, IL, 1995).
Vol. 7.
AMS/IP Stud. Adv. Math.
Providence, RI: Amer. Math. Soc.

Jao, David, Stephen D. Miller, and Ramarathnam Venkatesan (June 2009).
"Expander graphs based on GRH with an application to elliptic curve cryptography."
In: Journal of Number Theory 129.6,
Pp. 1491–1504.

# References II


Teske, Edlyn (Jan. 2006).
"An Elliptic Curve Trapdoor System."
In: Journal of Cryptology 19.1,
Pp. 115–133.

Galbraith, Steven D. (1999).
"Constructing Isogenies between Elliptic Curves Over Finite Fields."
In: LMS Journal of Computation and Mathematics 2,
Pp. 118–138.

Galbraith, Steven D., Florian Hess, and Nigel P. Smart (2002).
"Extending the GHS Weil descent attack."
In: Advances in cryptology—EUROCRYPT 2002 (Amsterdam).
Vol. 2332.
Lecture Notes in Comput. Sci.
Berlin: Springer,
Pp. 29–44.

# References III


Bisson, Gaetan and Andrew V. Sutherland (June 2011).
"A low-memory algorithm for finding short product representations in finite groups."
In: Designs, Codes and Cryptography 63.1,
Pp. 1–13.

Charles, Denis X., Kristin E. Lauter, and Eyal Z. Goren (Jan. 2009).
"Cryptographic Hash Functions from Expander Graphs."
In: Journal of Cryptology 22.1,
Pp. 93–113.

Doliskani, Javad, Geovandro C. C. F. Pereira, and Paulo S. L. M. Barreto (2017).
Faster Cryptographic Hash Function From Supersingular Isogeny Graphs.
Cryptology ePrint Archive, Report 2017/1202.
https://eprint.iacr.org/2017/1202.

# References IV


Couveignes, Jean-Marc (2006).
Hard Homogeneous Spaces.

Rostovtsev, Alexander and Anton Stolbunov (2006).
Public-key cryptosystem based on isogenies.
http://eprint.iacr.org/2006/145/.

Kuperberg, Greg (2005).
"A subexponential-time quantum algorithm for the dihedral hidden subgroup problem."
In: SIAM J. Comput. 35.1,
Pp. 170–188.
eprint: quant-ph/0302112.

Regev, Oded (June 2004).
A Subexponential Time Algorithm for the Dihedral Hidden Subgroup Problem with Polynomial Space.
arXiv: quant-ph/0406151.

# References V


Childs, Andrew M., David Jao, and Vladimir Soukharev (Dec. 2010).
"Constructing elliptic curve isogenies in quantum subexponential time."

Jao, David and Luca De Feo (2011).
"Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies."
In: Post-Quantum Cryptography.
Ed. by Bo-Yin Yang.
Vol. 7071.
Lecture Notes in Computer Science.
Taipei, Taiwan: Springer Berlin / Heidelberg.
Chap. 2, pp. 19–34.

# References VI


De Feo, Luca, David Jao, and Jérôme Plût (2014).
"Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies."
In: Journal of Mathematical Cryptology 8.3,
Pp. 209–247.

Tani, Seiichiro (2009).
"Claw finding algorithms using quantum walk."
In: Theoretical Computer Science 410.50,
Pp. 5285–5297.

Kohel, David, Kristin Lauter, Christophe Petit, and Jean-Pierre Tignol (2014).
"On the quaternion-isogeny path problem."
In: LMS Journal of Computation and Mathematics 17.A,
Pp. 418–432.

# References VII

Galbraith, Steven D., Christophe Petit, Barak Shani, and Yan Bo Ti (2016).
"On the security of supersingular isogeny cryptosystems."
In: Advances in Cryptology–ASIACRYPT 2016: 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part I 22.
Springer,
Pp. 63–91.

Costello, Craig, Patrick Longa, and Michael Naehrig (2016).
"Efficient Algorithms for Supersingular Isogeny Diffie-Hellman."
In: Advances in Cryptology – CRYPTO 2016: 36th Annual International Cryptology Conference.
Ed. by Matthew Robshaw and Jonathan Katz.
Springer Berlin Heidelberg,
Pp. 572–601.

# References VIII


Karmakar, Angshuman, Sujoy Sinha Roy, Frederik Vercauteren, and Ingrid Verbauwhede (2016).
"Efficient Finite Field Multiplication for Isogeny Based Post Quantum Cryptography."
In: Proceedings of WAIFI 2016.

Faz-Hernández, Armando, Julio López, Eduardo Ochoa-Jiménez, and Francisco Rodríguez-Henríquez (2017).
A Faster Software Implementation of the Supersingular Isogeny Diffie-Hellman Key Exchange Protocol.
Cryptology ePrint Archive, Report 2017/1015.
http://eprint.iacr.org/2017/1015.