Exploring Isogeny Graphs
Around the Volcano in 2^{80} Days

Luca De Feo
hand drawings by Rachel Deyts

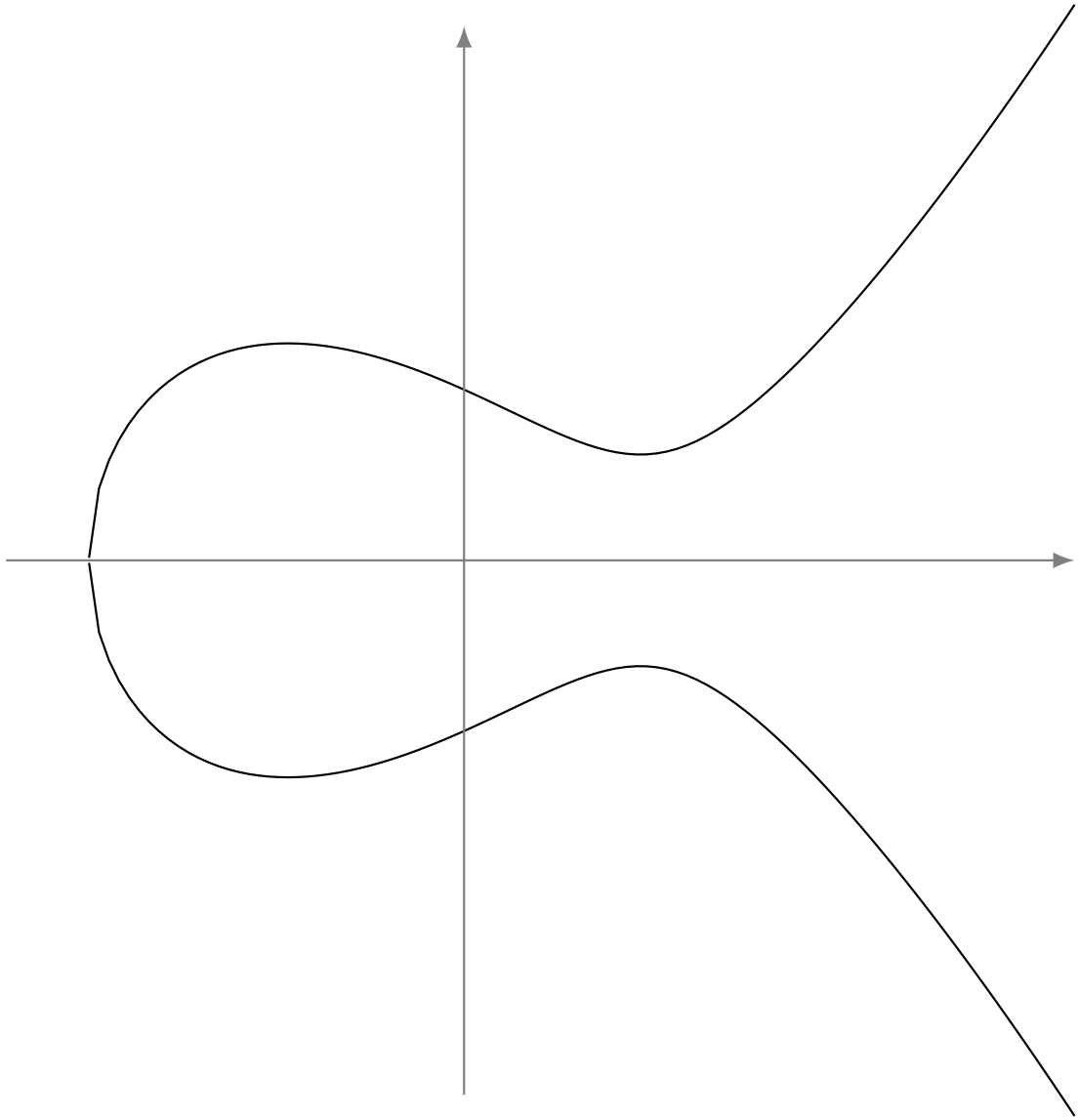
Université Paris Saclay – UVSQ

Dec 14, 2018, UVSQ, Versailles

Elliptic curves

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

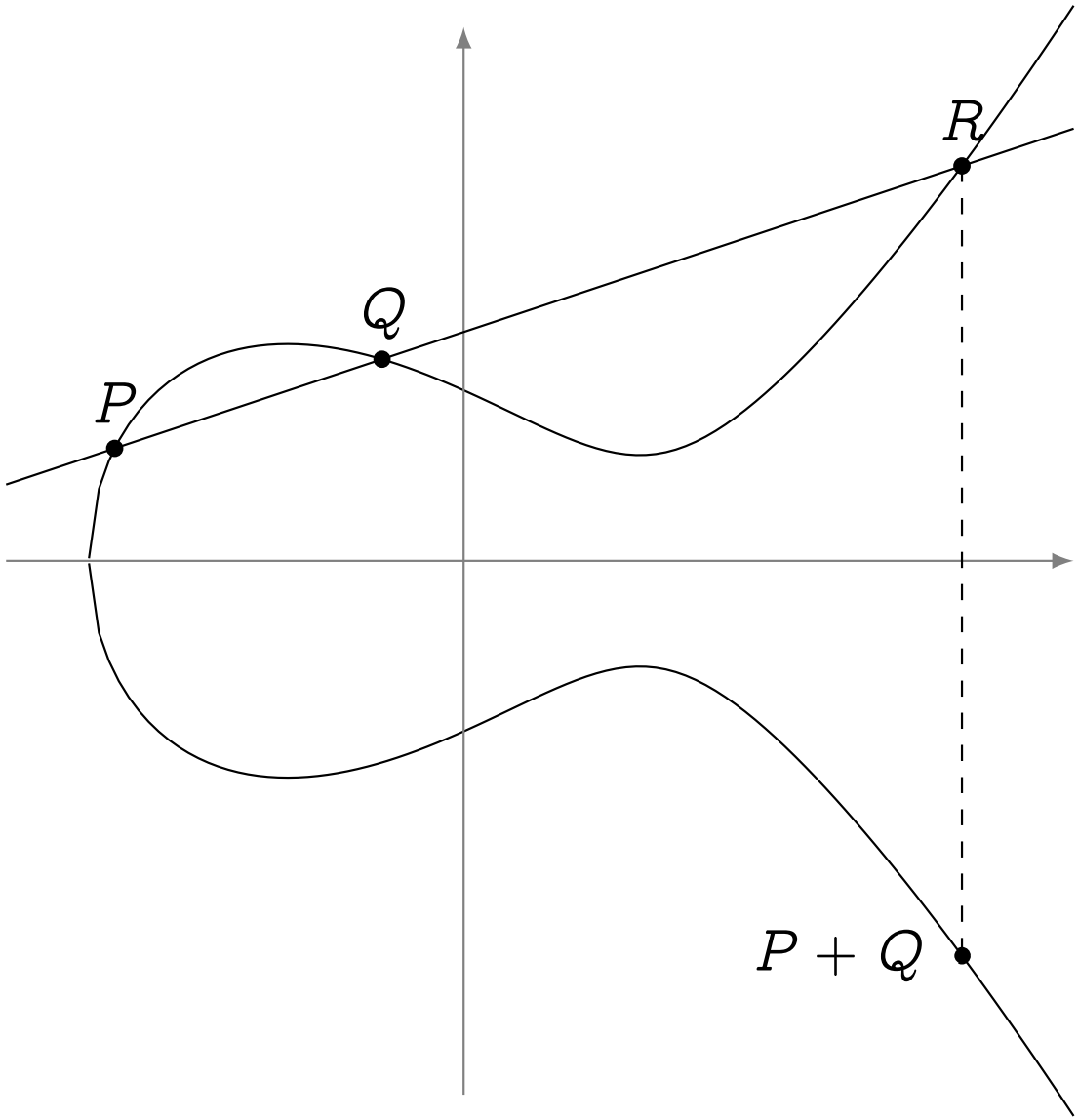
- An algebraic curve,



Elliptic curves

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

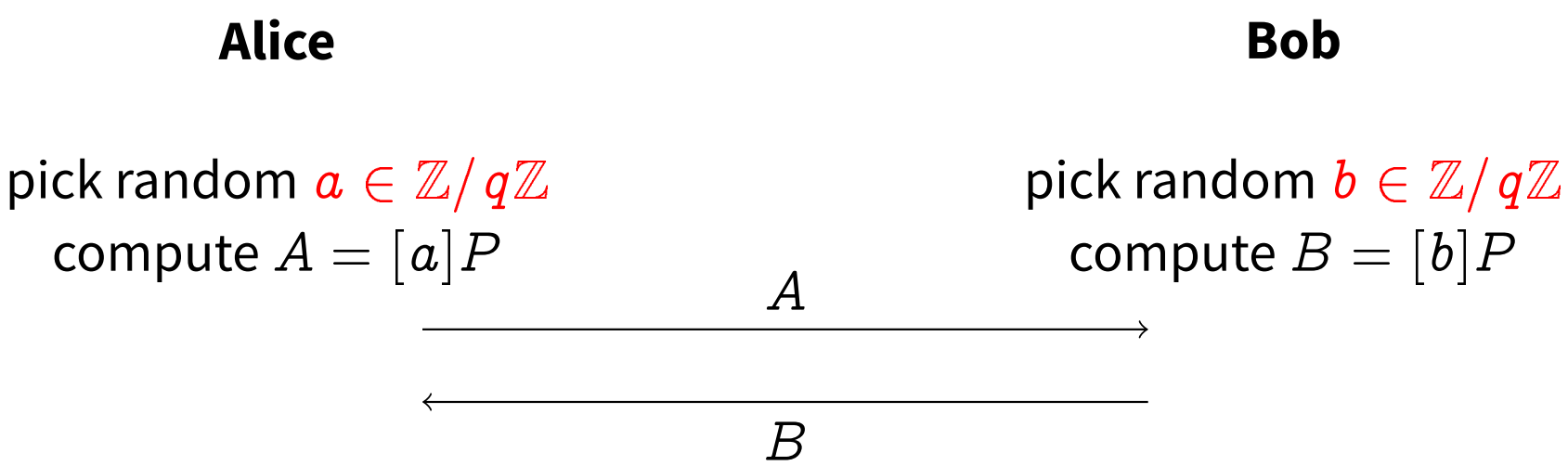
- An algebraic curve,
- A group.



Why should I care? (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 $E(\mathbb{F}_p) = \langle P \rangle$ of (prime) order q.



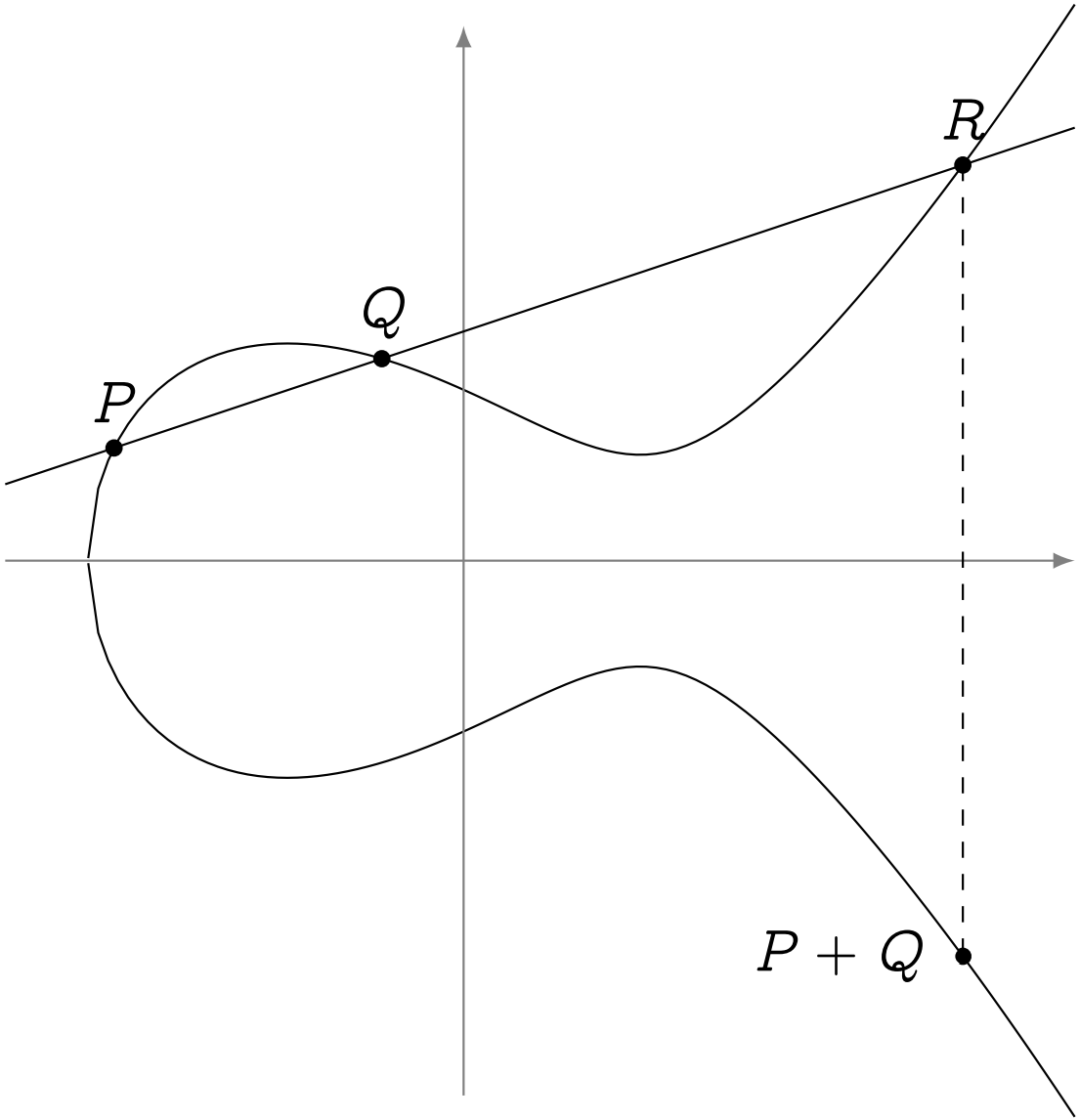
Shared secret is $[a]B = [ab]P = [b]A$

Why should I care?

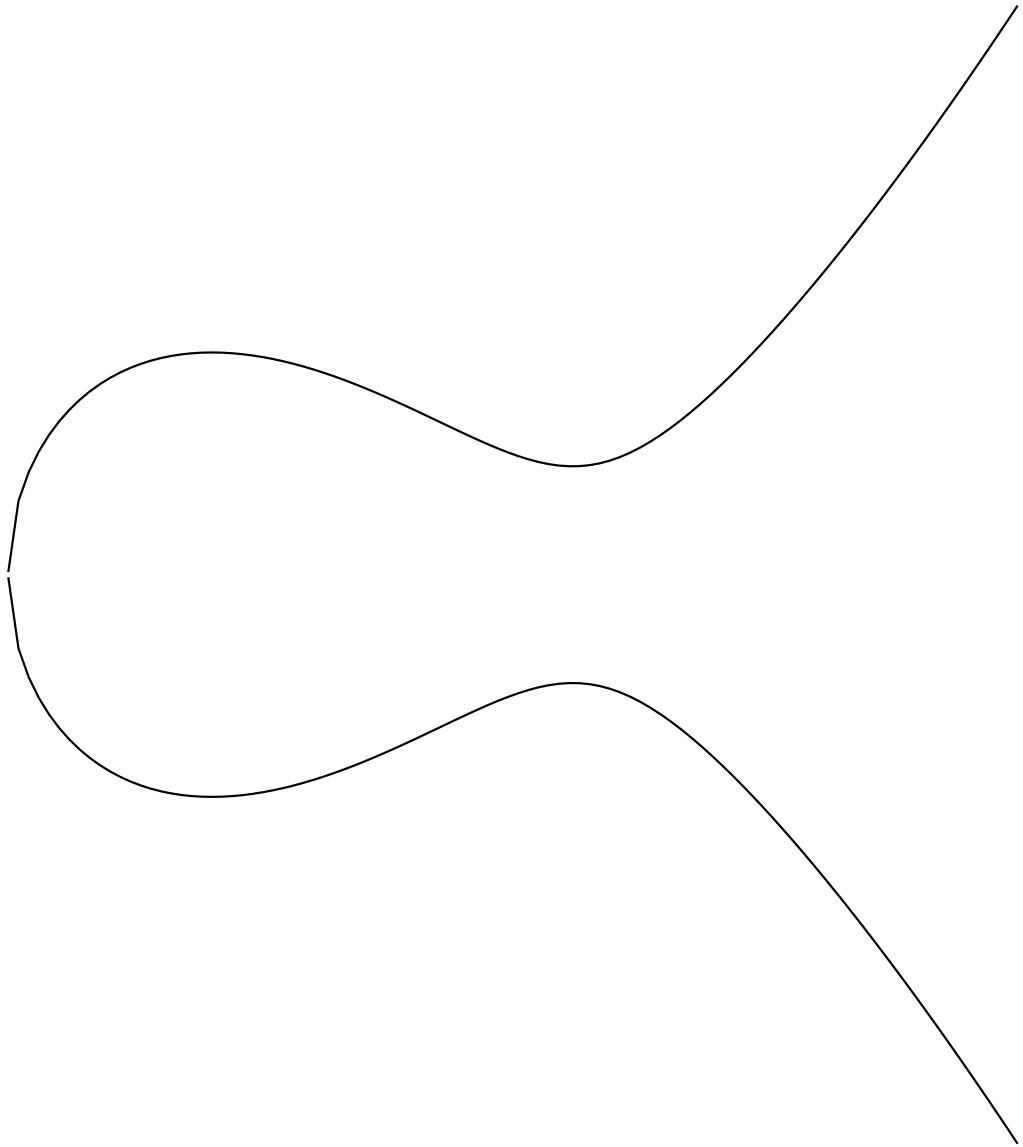
But, also:

- Elliptic Curve Factoring Method (Lenstra ’85);
- Elliptic Curve Primality Proving (Atkin, Morain ’86-’93);
- Efficient normal bases for finite fields (Couveignes, Lercier ’10);
- …

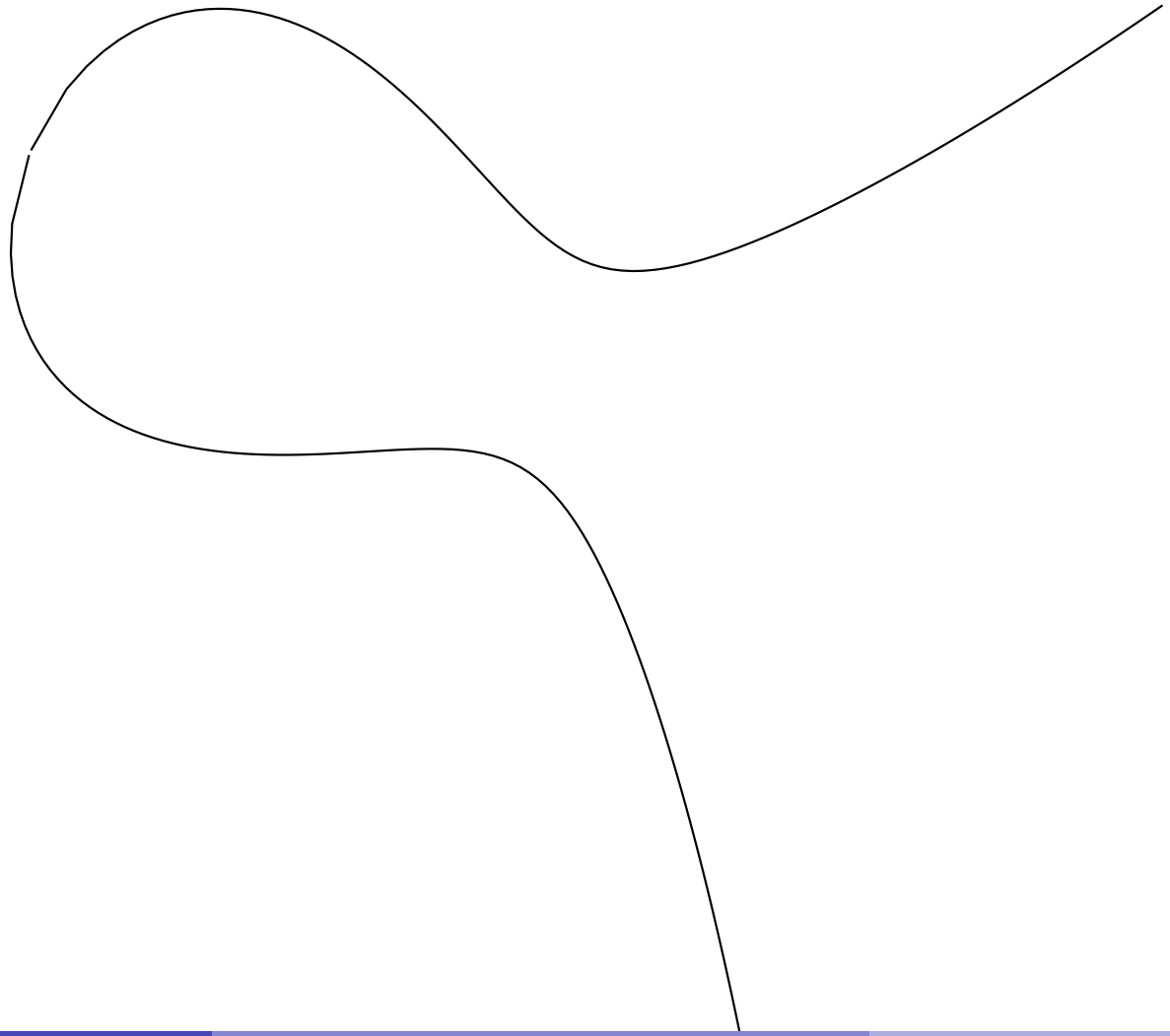
Why should I care?



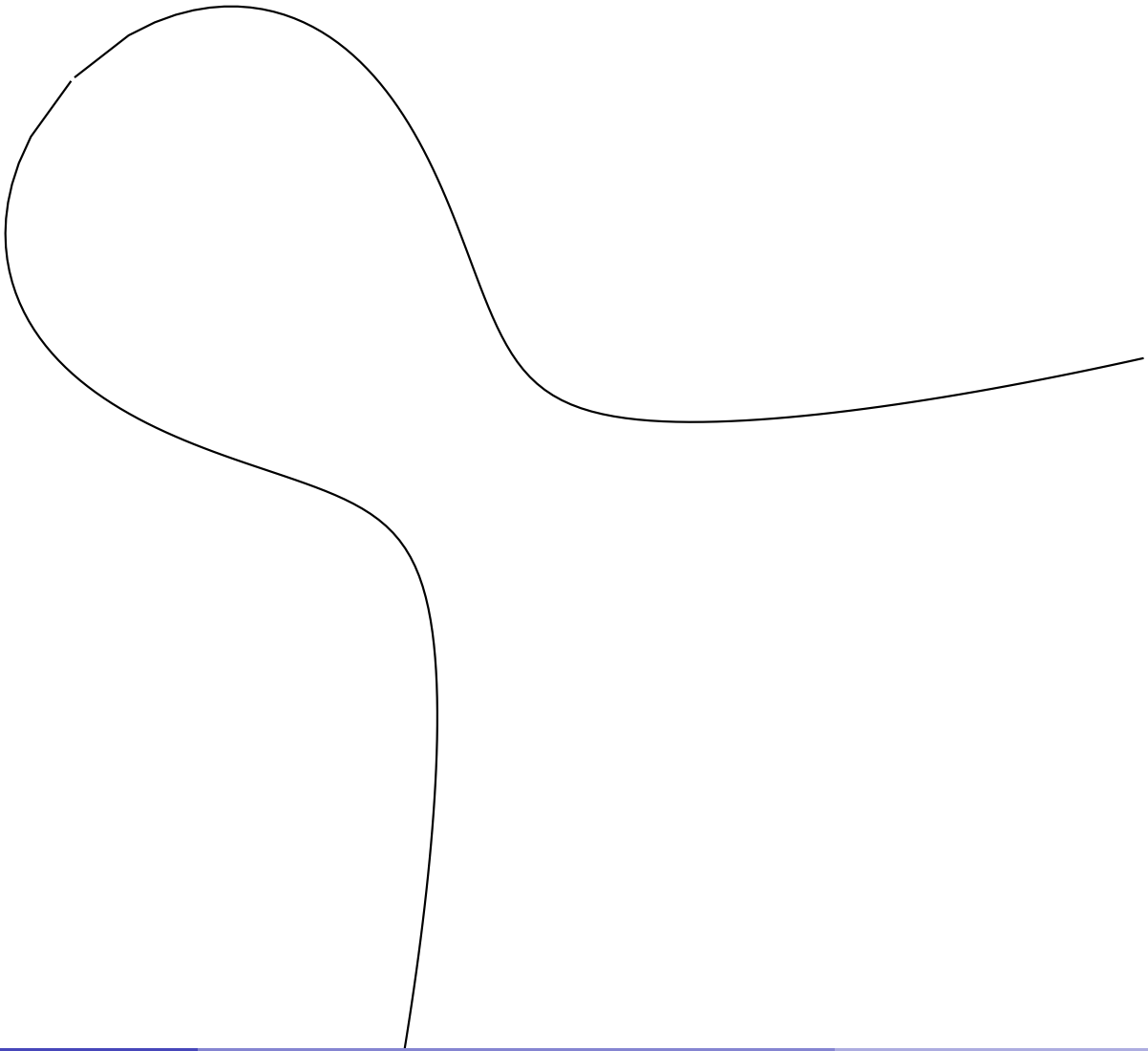
Why should I care?



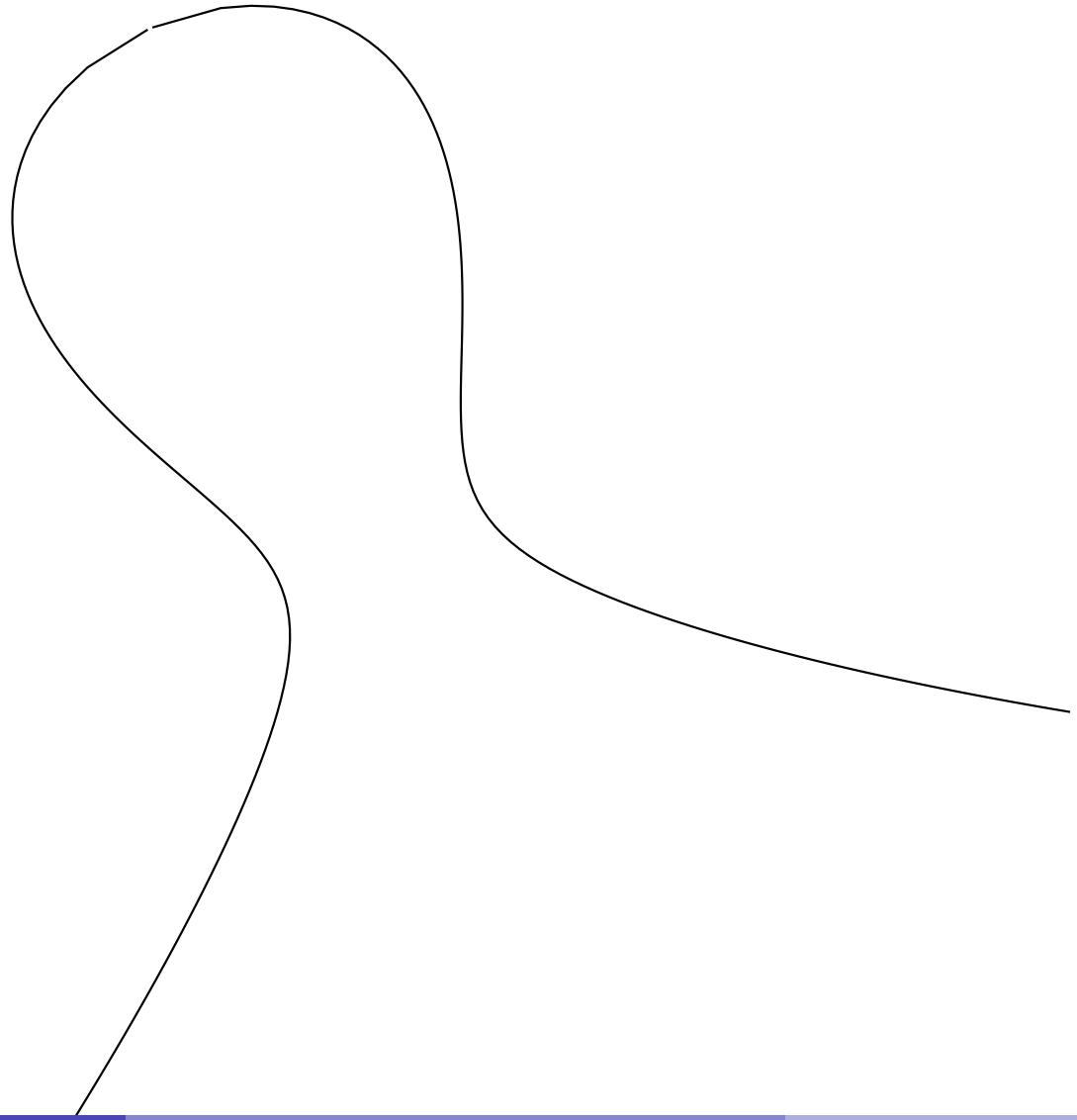
Why should I care?



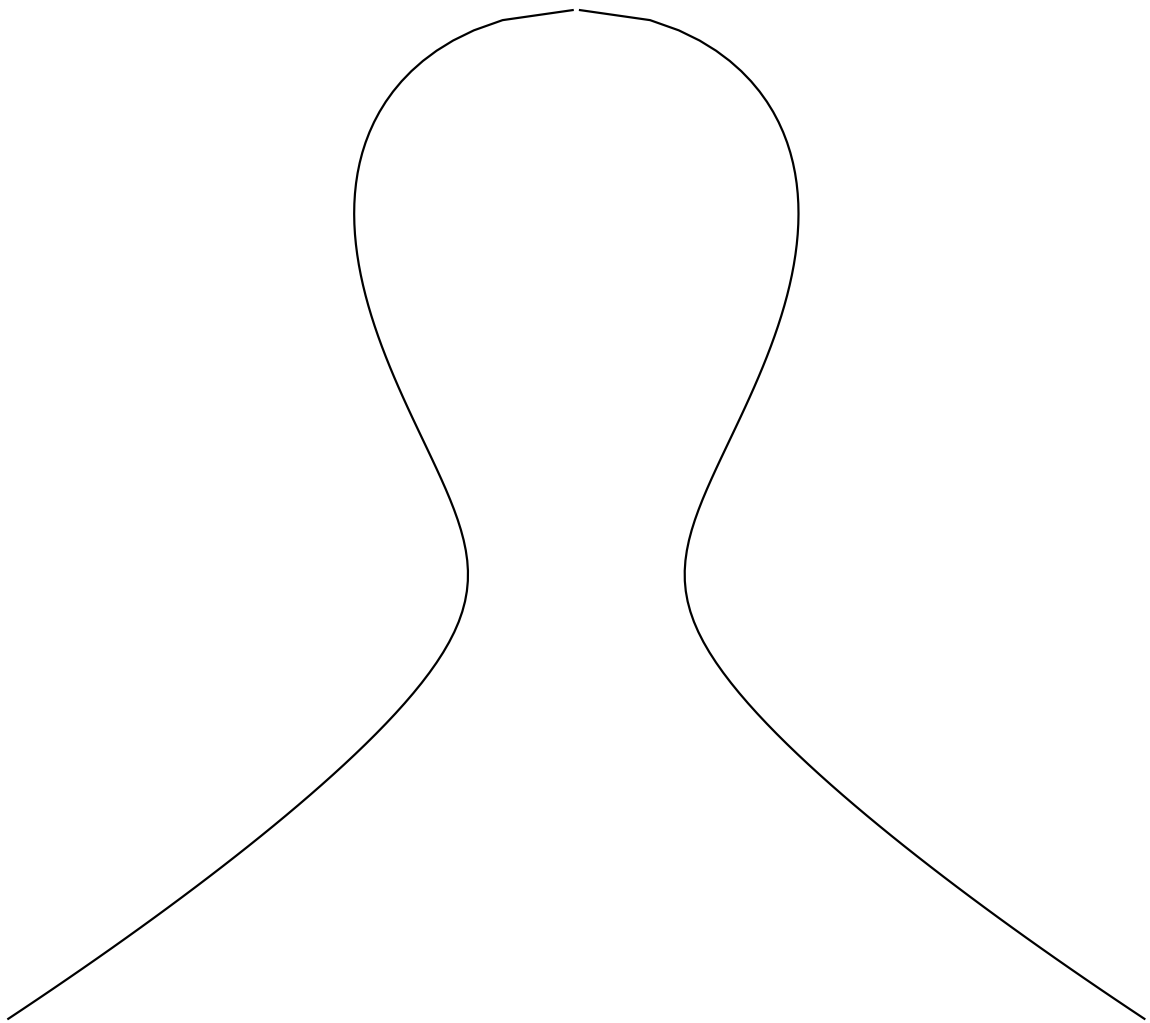
Why should I care?



Why should I care?



Why should I care?



Elliptic curves

I power 70% of WWW traffic!

What is scalar multiplication?

$$[n] \ : \ P \mapsto \underbrace{P + P + \cdots + P}_{n \text{ times}}$$

- A map $E \to E$,
- a group morphism,
- with finite kernel
  (the torsion group $E[n] \simeq (\mathbb{Z}/n\mathbb{Z})^2$),
- surjective (in the algebraic closure),
- given by rational maps of degree n^2.

What is scalar multiplication an isogeny?

$$[n] \; : \; P \mapsto \underbrace{P + P + \cdots + P}_{n \text{ times}}$$

- A map $E \to E$,
- a group morphism,
- with finite kernel
  (the torsion group $E[n] \simeq (\mathbb{Z}/n\mathbb{Z})^2$),
- surjective (in the algebraic closure),
- given by rational maps of degree n^2.

What is ~~scalar multiplication~~ an isogeny?

$$\phi \ : \ P \mapsto \phi(P)$$

- A map $E \to E$,
- a group morphism,
- with finite kernel
  (the torsion group $E[n] \simeq (\mathbb{Z}/n\mathbb{Z})^2$),
- surjective (in the algebraic closure),
- given by rational maps of degree n^2.

What is ~~scalar multiplication~~ an isogeny?

$$\phi \ : \ P \mapsto \phi(P)$$

- A map $E \to E'$,
- a group morphism,
- with finite kernel
  (the torsion group $E[n] \simeq (\mathbb{Z}/n\mathbb{Z})^2$),
- surjective (in the algebraic closure),
- given by rational maps of degree n^2.

What is scalar multiplication an isogeny?

$$\phi \ : \ P \mapsto \phi(P)$$

- A map $E \to E'$,
- a group morphism,
- with finite kernel (the torsion group $E[n] \simeq (\mathbb{Z}/n\mathbb{Z})^2$ any finite subgroup $H \subset E$),
- surjective (in the algebraic closure),
- given by rational maps of degree n^2.

What is scalar multiplication an isogeny?

$$\phi \ : \ P \mapsto \phi(P)$$

- A map $E \to E'$,
- a group morphism,
- with finite kernel (the torsion group $E[n]$ / any finite subgroup $H \subset E$),
- surjective (in the algebraic closure),
- given by rational maps of degree n^2 / $\#H$.

What is scalar multiplication an isogeny?

$$\phi \ : \ P \mapsto \phi(P)$$

- A map $E \to E'$,
- a group morphism,
- with finite kernel (the torsion group $E[m] \simeq (\mathbb{Z}/m\mathbb{Z})^2$ any finite subgroup $H \subset E$),
- surjective (in the algebraic closure),
- given by rational maps of degree m^2 $\#H$.

(Separable) isogenies $\Leftrightarrow$ finite subgroups:

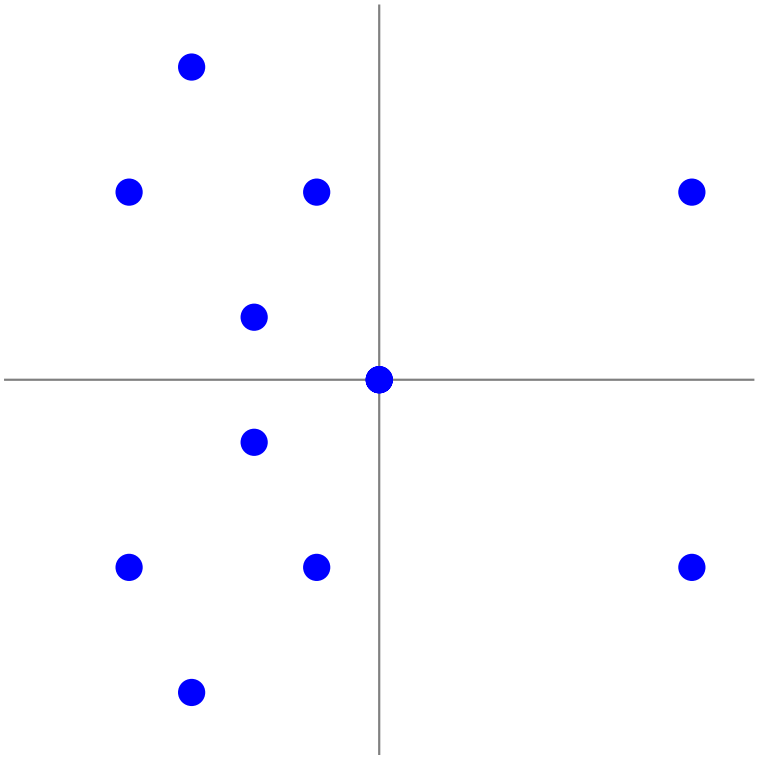
$$0 \longrightarrow H \longrightarrow E \xrightarrow{\phi} E' \to 0$$

The kernel H determines the image curve E' up to isomorphism

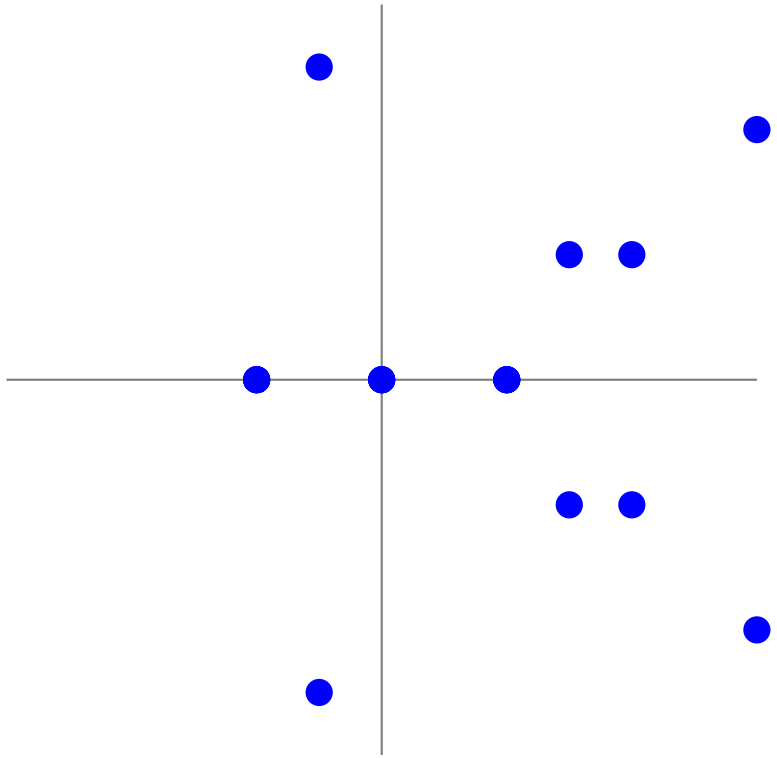
$$E/H \overset{\text{def}}{=} E'.$$

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

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



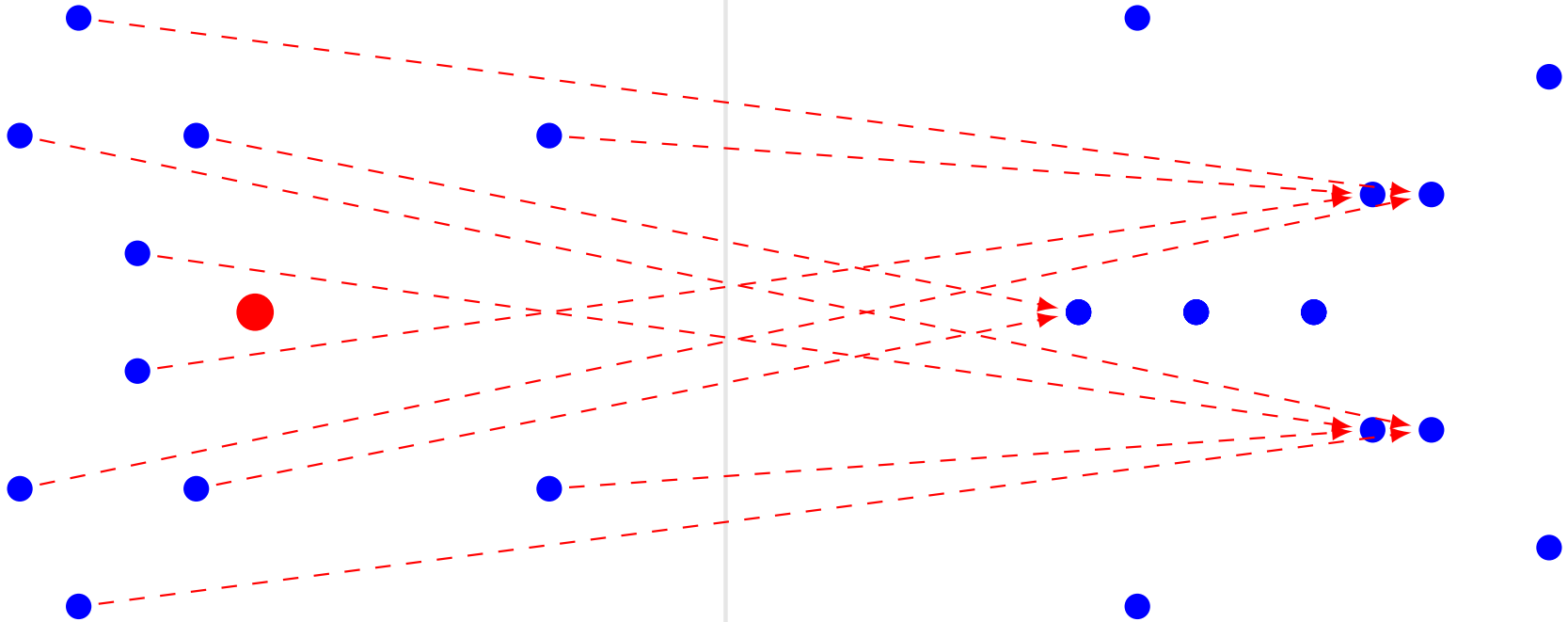
$$E' \ : \ y^2 = x^3 - 4x$$



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

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

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



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

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

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 Éric 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 Éric Schost 2016; Lairez and Vaccon 2016, ...

Why?
- Count points of elliptic curves.

Isogeny Walk Problem

Input: Isogenous curves E, E'.

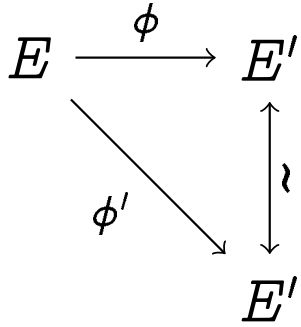
Output: An isogeny $\phi : E \to E'$ of smooth degree.

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

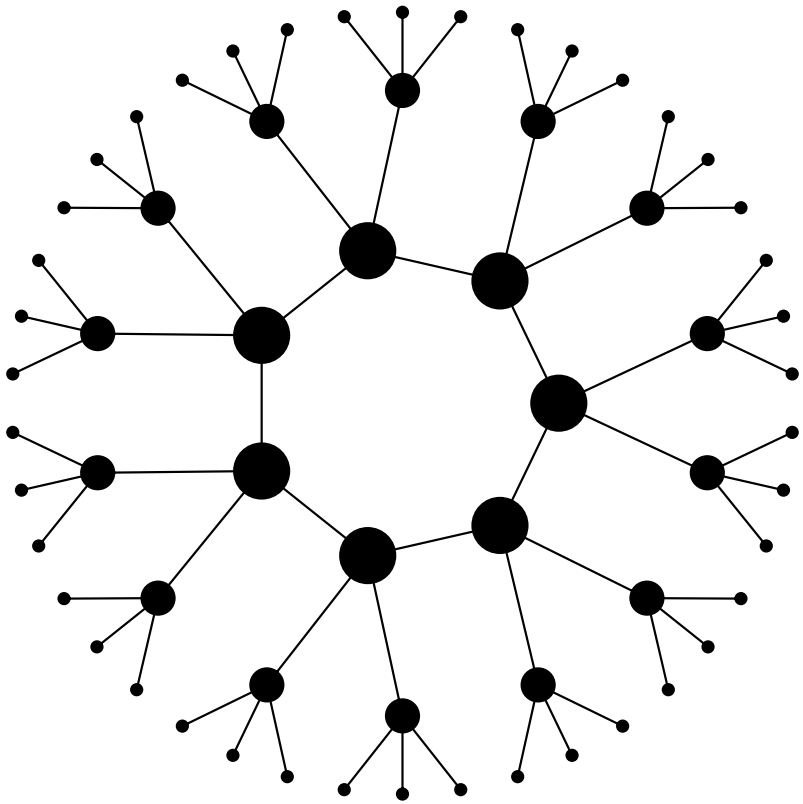
Why?
- Cryptanalysis (ECC);
- Foundational problem for isogeny-based cryptography.

Isogeny graphs

We look at the graph of elliptic curves with isogenies up to isomorphism. We say two isogenies ϕ, ϕ' are isomorphic if:



Example: Finite field, ordinary case, graph of isogenies of degree 3.



What do isogeny graphs look like?

Torsion subgroups (ℓ prime)

In an algebraically closed field:

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

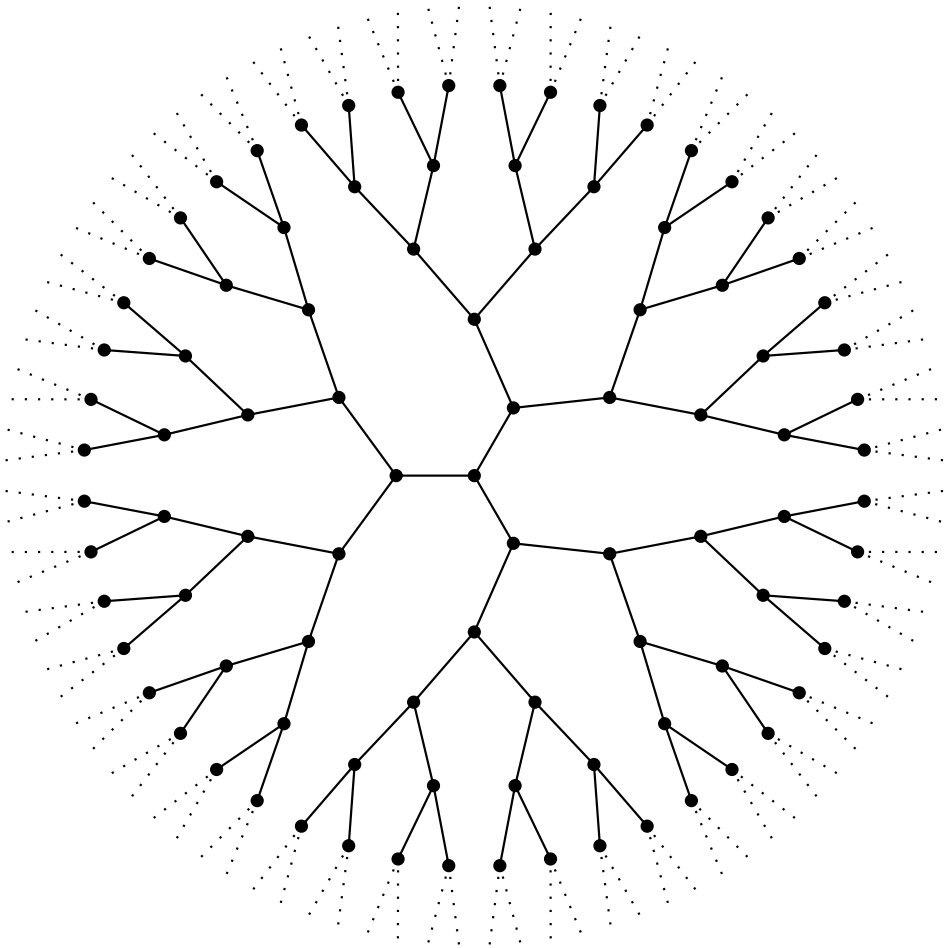
$$\Downarrow$$

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

$$\langle P \rangle, \langle P + Q \rangle, \dots \langle P + (\ell - 1)Q \rangle$$

$$\Downarrow$$

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 $E[\ell]$

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

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 $E[\ell]$

$$cP + dQ$$

$$aP + bQ$$

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 $E[\ell]$

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

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 $E[\ell]$

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

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 $E[\ell]$

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

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 $E[\ell]$

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

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
- $\pi|E[\ell] \sim \left(\begin{smallmatrix} \lambda & 0 \\ 0 & \mu \end{smallmatrix}\right)$ 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 $\rightarrow$ no isogeny

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

Endomorphisms

An isogeny $E \to E$ is also called an endomorphism. Examples:

- scalar multiplication $[n]$,
- Frobenius map π.

With addition and composition, the endomorphisms form a ring $\mathrm{End}(E)$.

Theorem (Deuring): $\mathrm{End}(E)$ is isomorphic to one of the following:

- An order $\mathcal{O}$ in a quadratic imaginary field $K = \mathbb{Q}(\sqrt{-D})$: E is ordinary with complex multiplication by $\mathcal{O}$.
- A maximal order in a quaternion algebra E is supersingular.

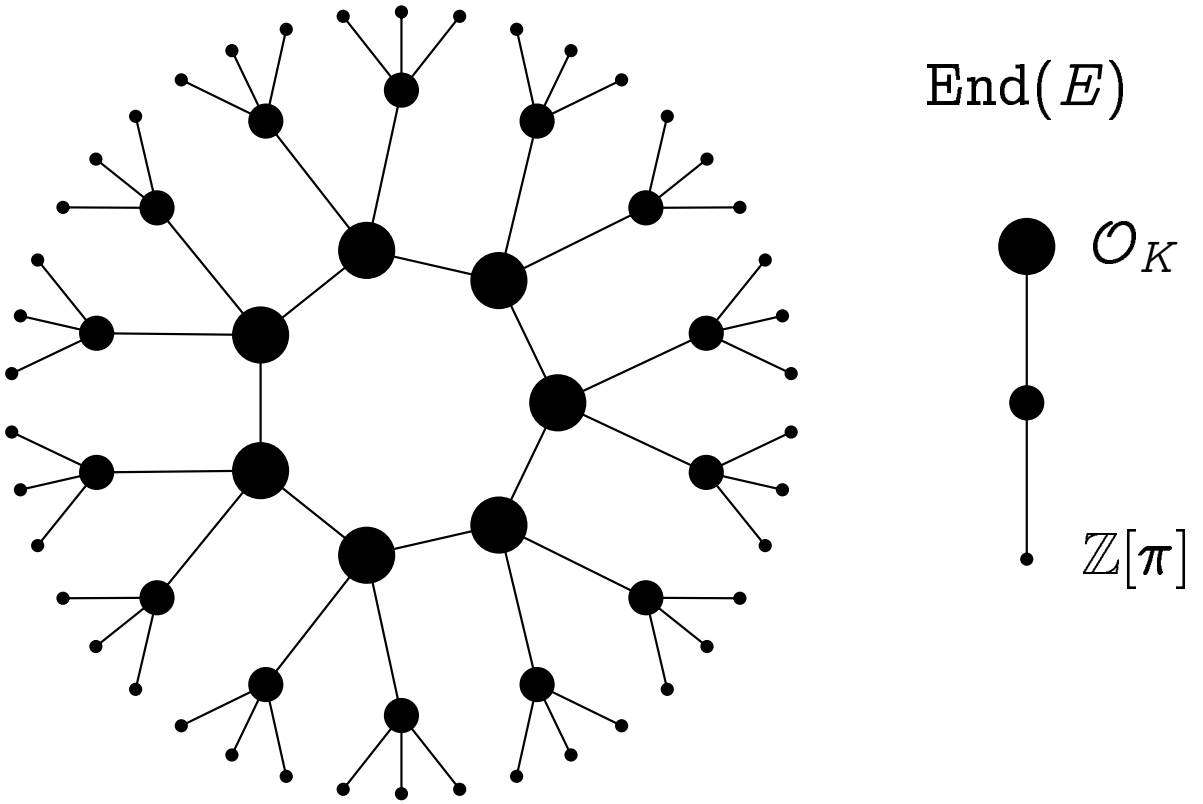
Theorem (Serre-Tate): E, E' are isogenous iff $\mathrm{End}(E) \otimes \mathbb{Q} \simeq \mathrm{End}(E') \otimes \mathbb{Q}$.

Corollary: $E/\mathbb{F}_p$ and $E'/\mathbb{F}_p$ are isogenous iff $\#E(\mathbb{F}_p) = \#E'(\mathbb{F}_p)$.

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.

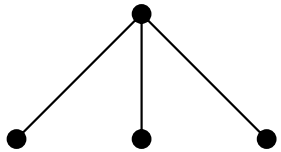


Ordinary isogeny volcano of degree $\ell = 3$.

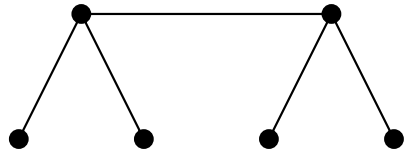
Volcanology (Kohel 1996)

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

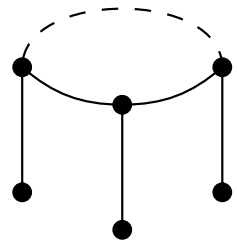
$\mathcal{O}_K$: maximal order of K,
D_K: discriminant of K.



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



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



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

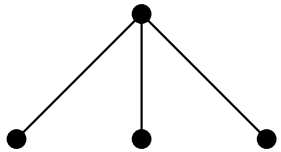
		Horizontal	**Ascending**	**Descending**
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$	$1 + \left(\frac{D_K}{\ell}\right)$		
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O} : \mathbb{Z}[\pi]]$	$1 + \left(\frac{D_K}{\ell}\right)$		$\ell - \left(\frac{D_K}{\ell}\right)$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

Volcanology (Kohel 1996)

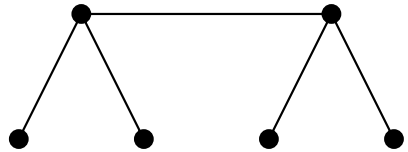
Let E be ordinary,
$\mathrm{End}(E) \subset K$.

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

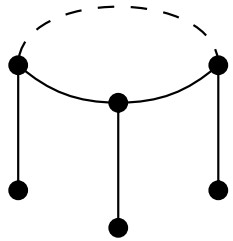
Height $= v_\ell([\mathcal{O}_K : \mathbb{Z}[\pi]])$.



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



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



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

		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	

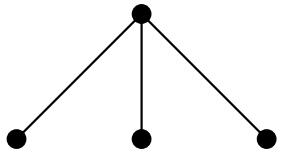
Volcanology (Kohel 1996)

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

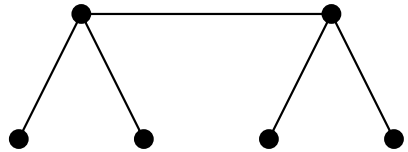
$\mathcal{O}_K$: maximal order of K,
D_K: discriminant of K.

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

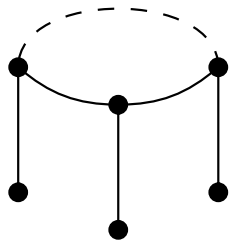
How large is the crater?



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



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

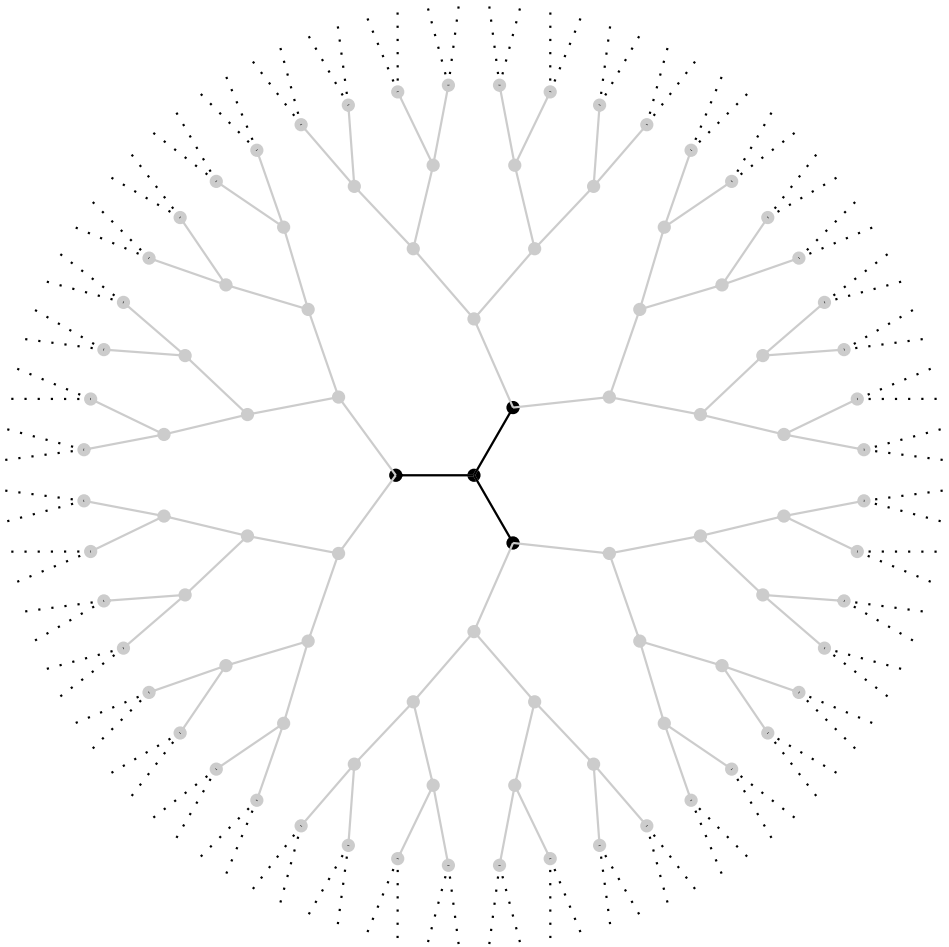


$\left(\frac{D_K}{\ell}\right) = +1$

		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	

Exploring isogeny graphs

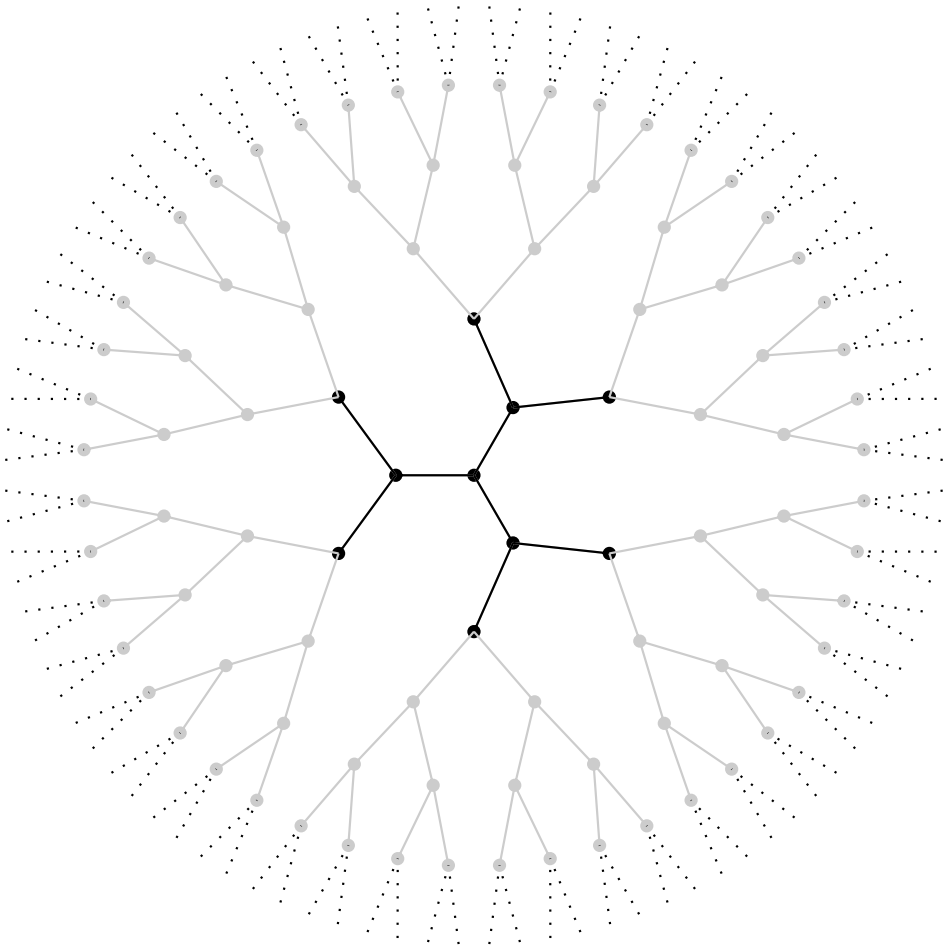
Detecting the structure of a graph



$$\pi | E[\ell^1] \ : \ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mod \ell^1$$

Exploring isogeny graphs

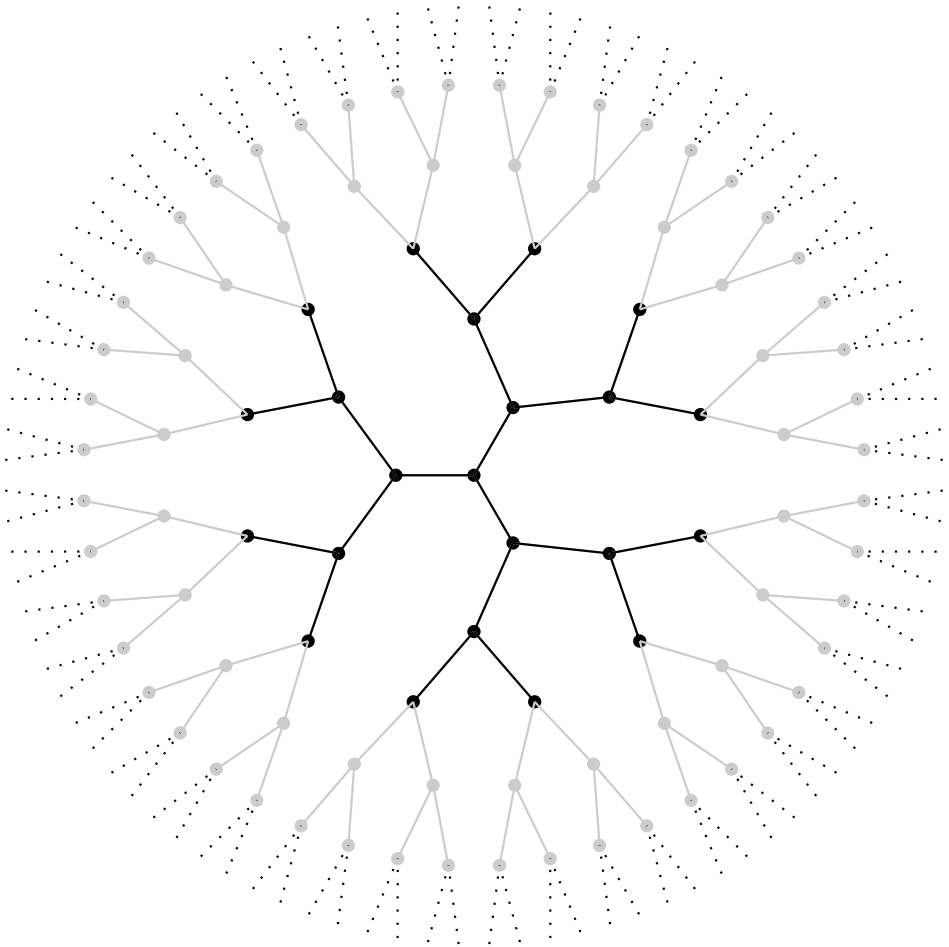
Detecting the structure of a graph



$$\pi\big|E[\ell^2] \ : \ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mod \ell^2$$

Exploring isogeny graphs

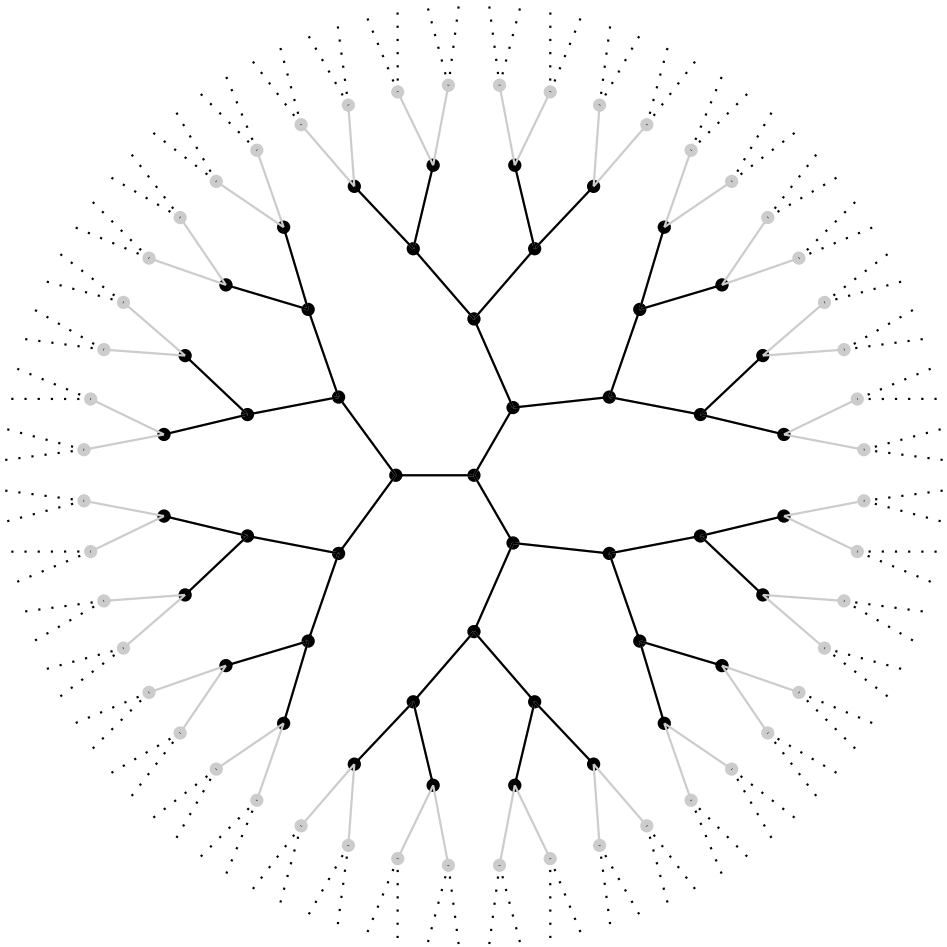
Detecting the structure of a graph



$$\pi | E[\ell^3] \ : \ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mod \ell^3$$

Exploring isogeny graphs

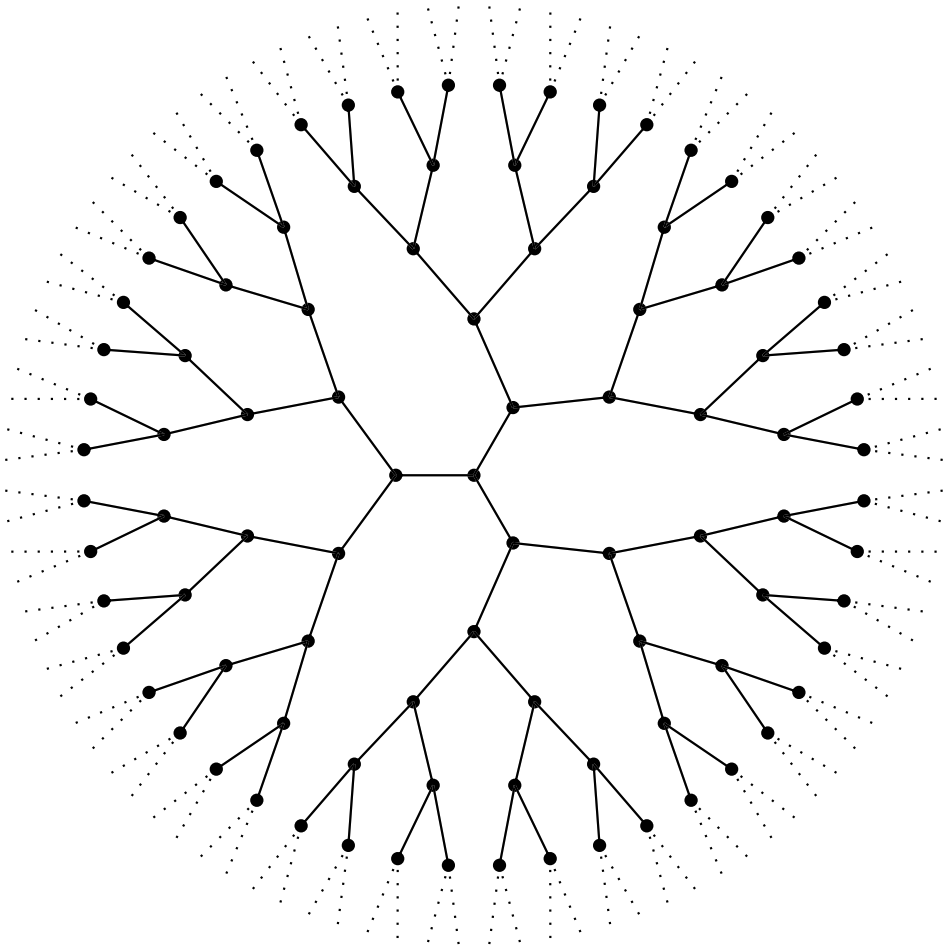
Detecting the structure of a graph



$$\pi \big| E[\ell^4] \ : \ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mod \ell^4$$

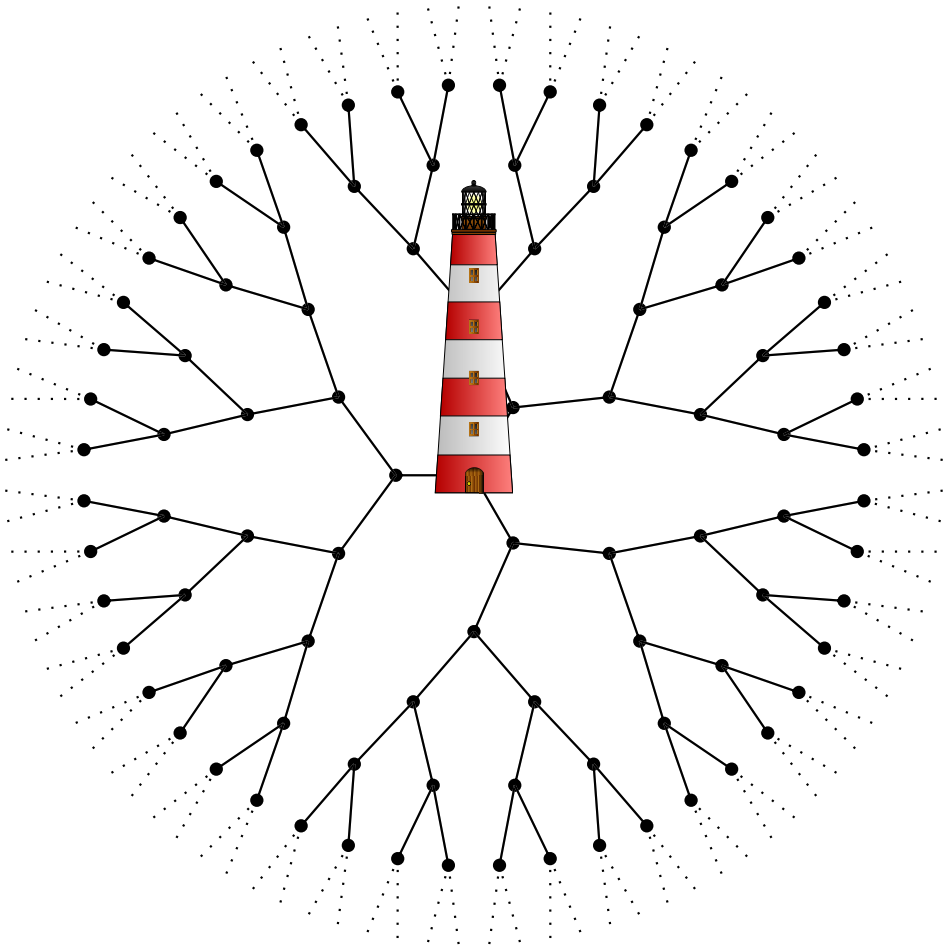
Exploring isogeny graphs

Detecting the structure of a graph



$$\pi\big|E[\ell^5] \ : \ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mod \ell^5$$

Exploring isogeny graphs



Detecting the structure of a graph

$$\pi|T_\ell(E) \ : \ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(\mathbb{Z}_\ell)$$

The Tate module

Projective limit of the torsion:

$$T_\ell(E) = \varprojlim E[\ell^n] \simeq (\mathbb{Z}_\ell)^2$$

Tate's isogeny theorem:

$$\mathrm{Hom}_{\mathbb{F}_p}(E, E') \otimes \mathbb{Z}_\ell$$
$$\simeq$$
$$\mathrm{Hom}_{\mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)}(T_\ell(E), T_\ell(E'))$$

Bathymetry

Theorem (De Feo, Hugounenq, Plût, and Éric Schost 2016)

Let $E/\mathbb{F}_p$ be an ordinary elliptic curve with Frobenius endomorphism π. Assume that the characteristic polynomial of π has two distinct roots λ, μ in $\mathbb{Z}_\ell$, and let $h = v_\ell(\lambda - \mu) = v_\ell(\sqrt{\Delta_\pi/\Delta_K})$. Then there exists a unique $e \in \{0, h\}$ such that $\pi | T_\ell(E)$ is conjugate, over $\mathbb{Z}_\ell$, to the matrix $\left(\begin{smallmatrix} \lambda & \ell^e \\ 0 & \mu \end{smallmatrix}\right)$. Moreover, $h = v_\ell([\mathcal{O}_K : \mathbb{Z}[\pi]])$ is the height of the graph of E; if E lies at the surface, then $e = h$, otherwise $h - e$ is the depth of E.

Computing $\pi | T_\ell(E)$ lets us:

- Determine the height of the ℓ-volcano,
- Determine the level of E in the volcano,
- Associate the eigenvalues λ, μ to two opposite directions on the crater.

Application: best known algorithm for the Explicit Isogeny Problem (2).

Computing $T_\ell(E)$ to finite precision

$T_\ell(E)$ "modulo" ℓ^n is just $E[\ell^n]$: $\pi \;:\; \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mod \ell^n$

Problem: fields of definition get increasingly large

$$\begin{array}{ccccccccc} & & E[\ell] & \subset & E[\ell^2] & \cdots & E[\ell^n] & \cdots \\ & & \cap & & \cap & & \cap & \\ E(\mathbb{F}_p) & \subset & E(\mathbb{F}_{p^{\ell-1}}) & \subset & E(\mathbb{F}_{p^{\ell(\ell-1)}}) & \cdots & E(\mathbb{F}_{p^{\ell^{n-1}(\ell-1)}}) & \cdots \end{array}$$

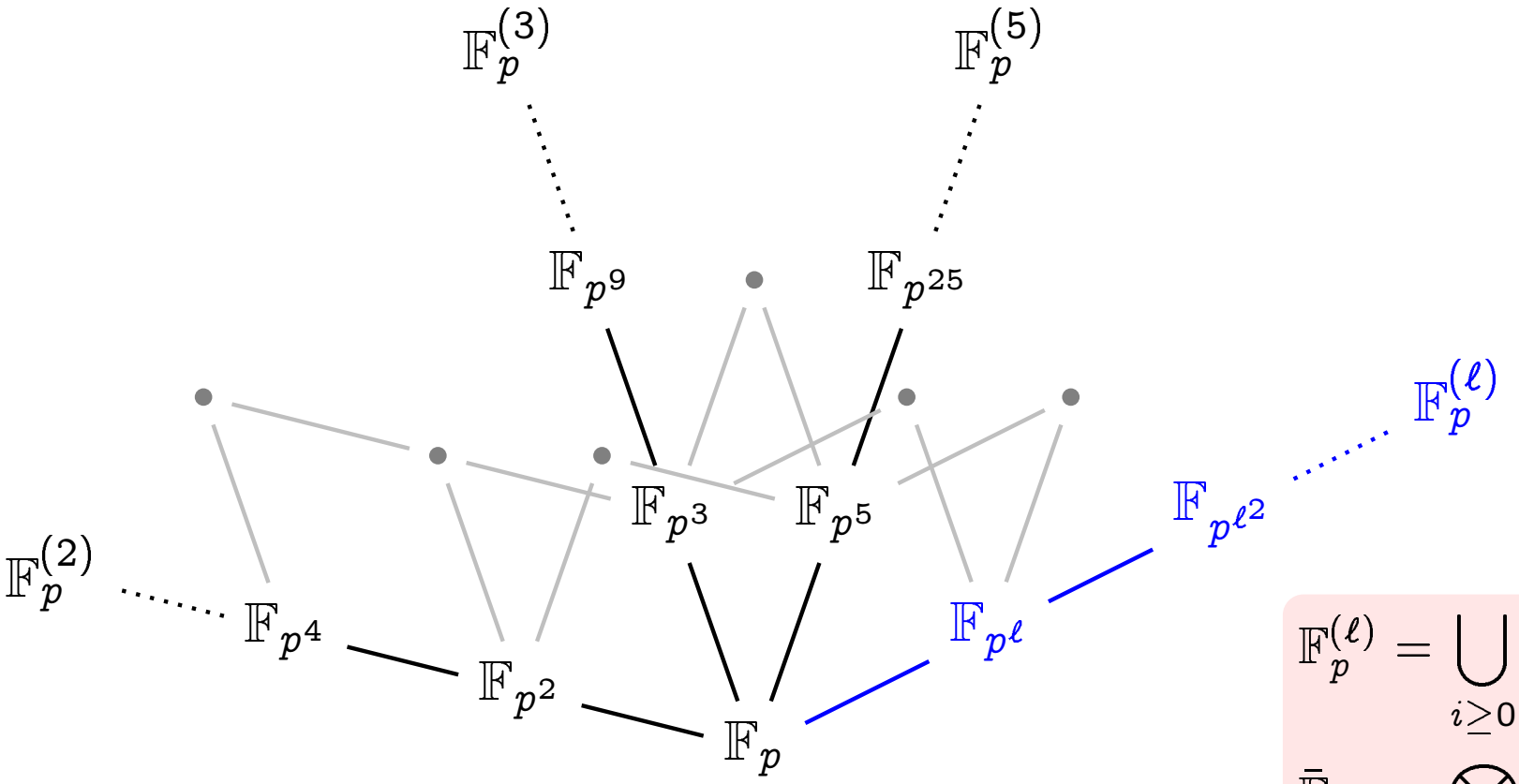
Solution: fast arithmetic in towers of finite fields

What: tower of fields $\mathbb{F}_p \subset \mathbb{F}_{p^a} \subset \mathbb{F}_{p^{ab}} \subset \cdots$;

Wanted:
- Optimal representation of each field;
- Fast algorithms for $+, \times, {}^{-1}$ in each field;
- Fast algorithms to convert between two adjacent fields.

Solutions: Lenstra 1991; Lübeck 2008; Bosma, Cannon, and Steel 1997; Allombert 2002; De Feo, Doliskani, and Éric Schost 2013, 2014; Brieulle, De Feo, Doliskani, Flori, and Éric Schost 2018; van der Hoeven, and Lecerf 2018, …

Why stop at towers?



$$\mathbb{F}_p^{(\ell)} = \bigcup_{i \geq 0} \mathbb{F}_{p^{\ell^i}},$$

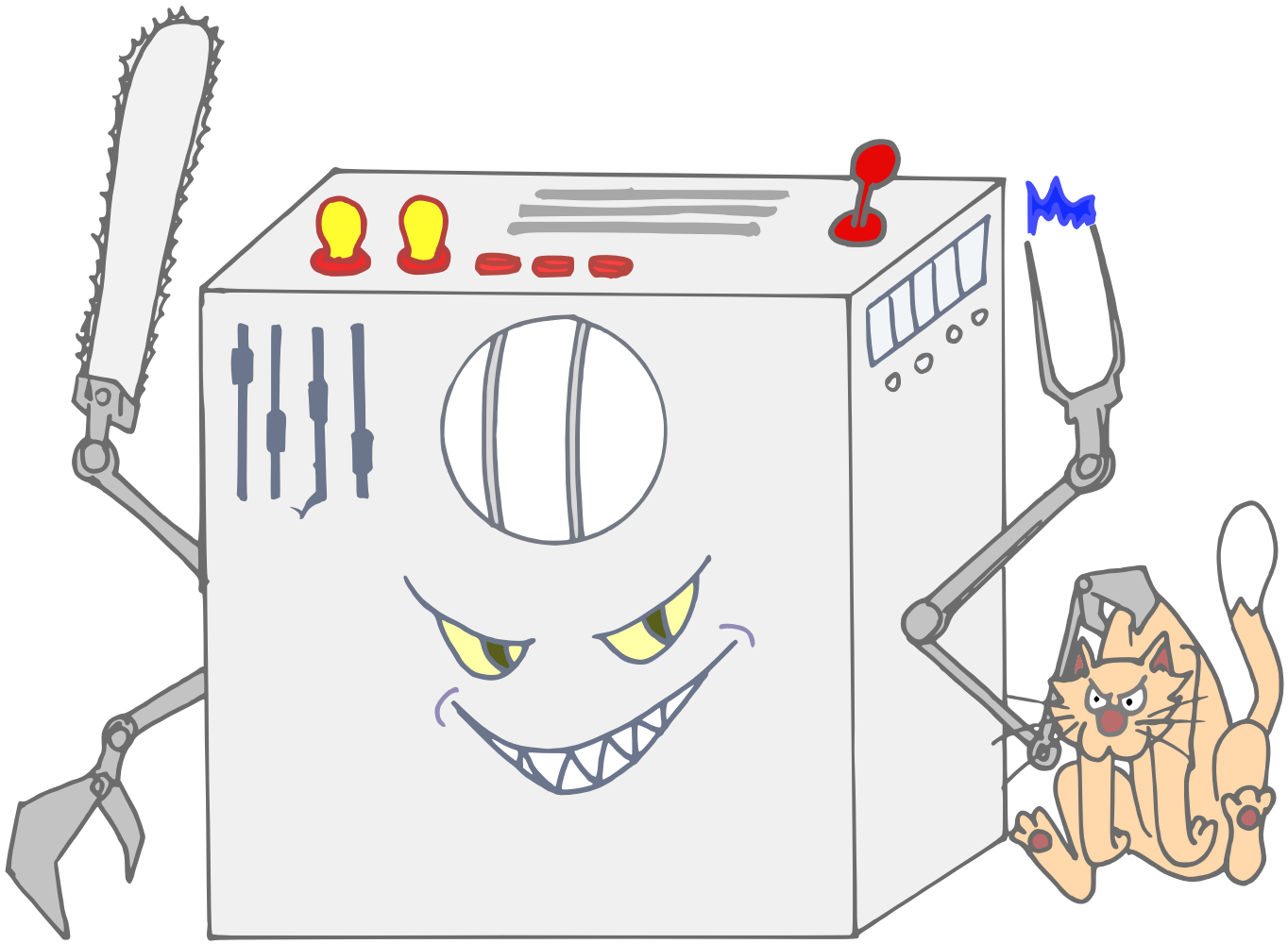
$$\bar{\mathbb{F}}_p \simeq \bigotimes_{\ell \text{ prime}} \mathbb{F}_p^{(\ell)}$$

Work in progress with: H.Randriam, É. Rousseau, É. Schost. Demo.

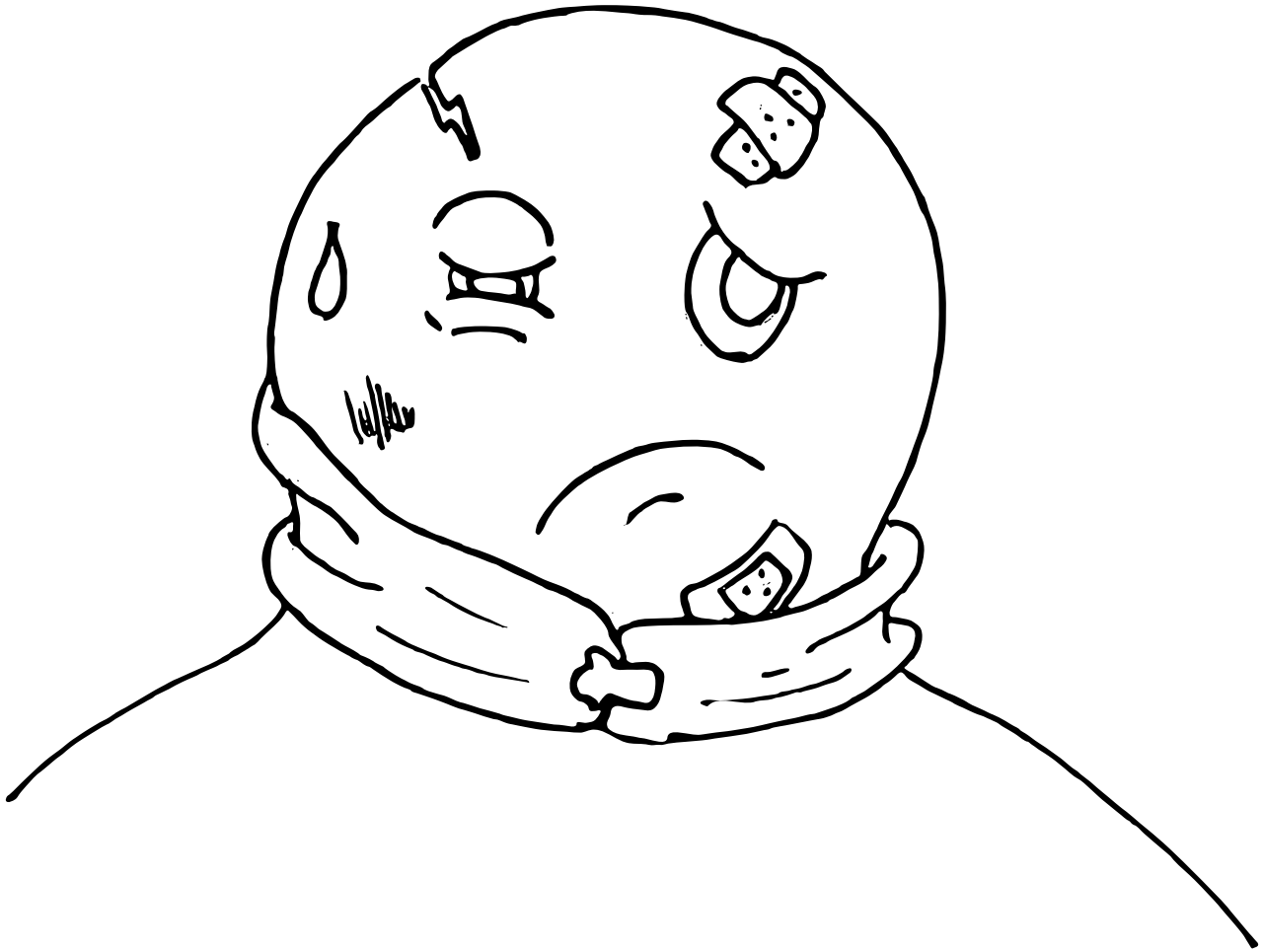
Let's get back to elliptic curves

I make the world a safer place!

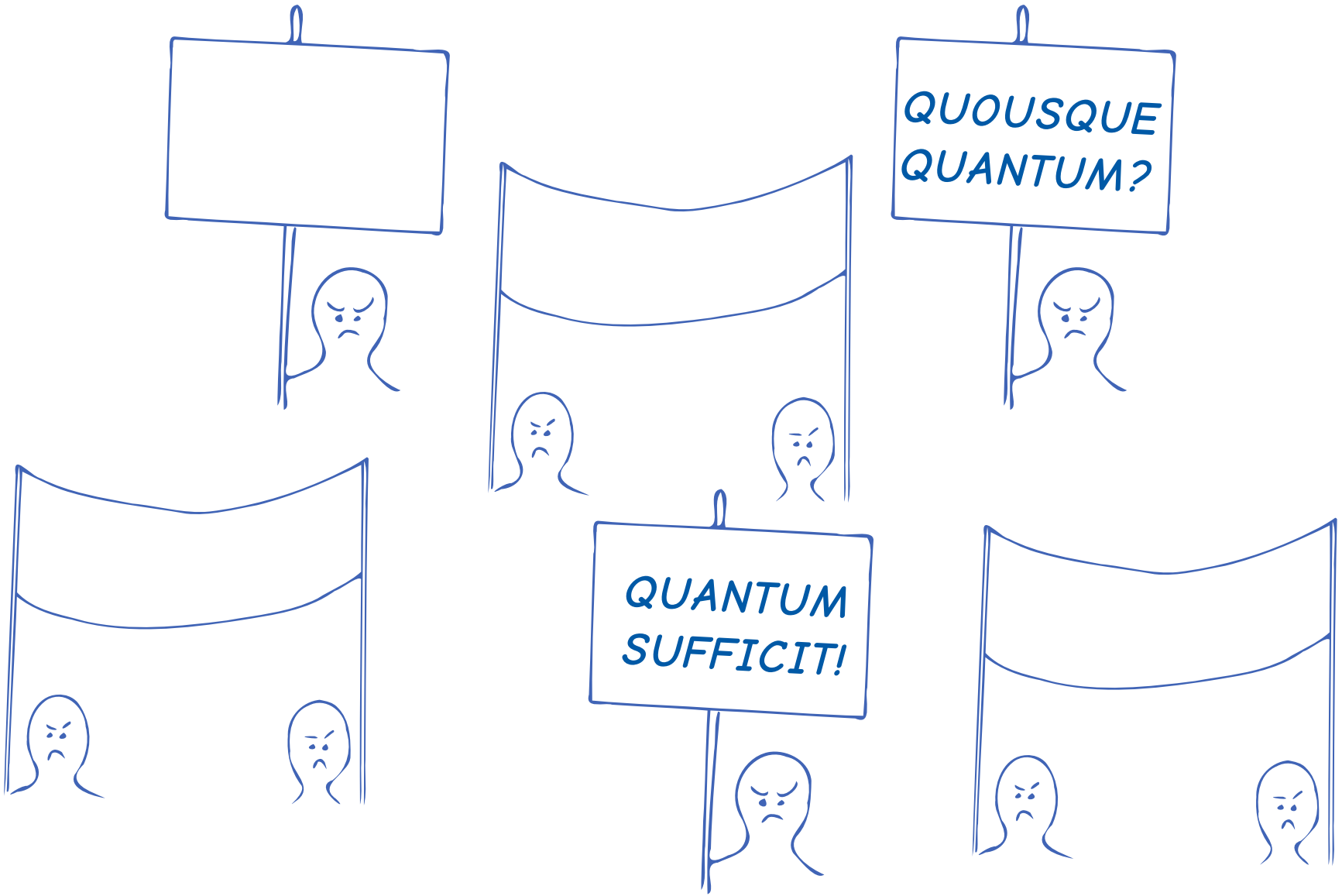
The QUANTOM Menace



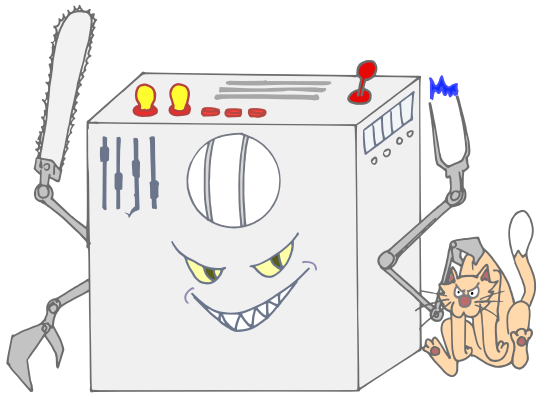
Post-quantum cryptographer?



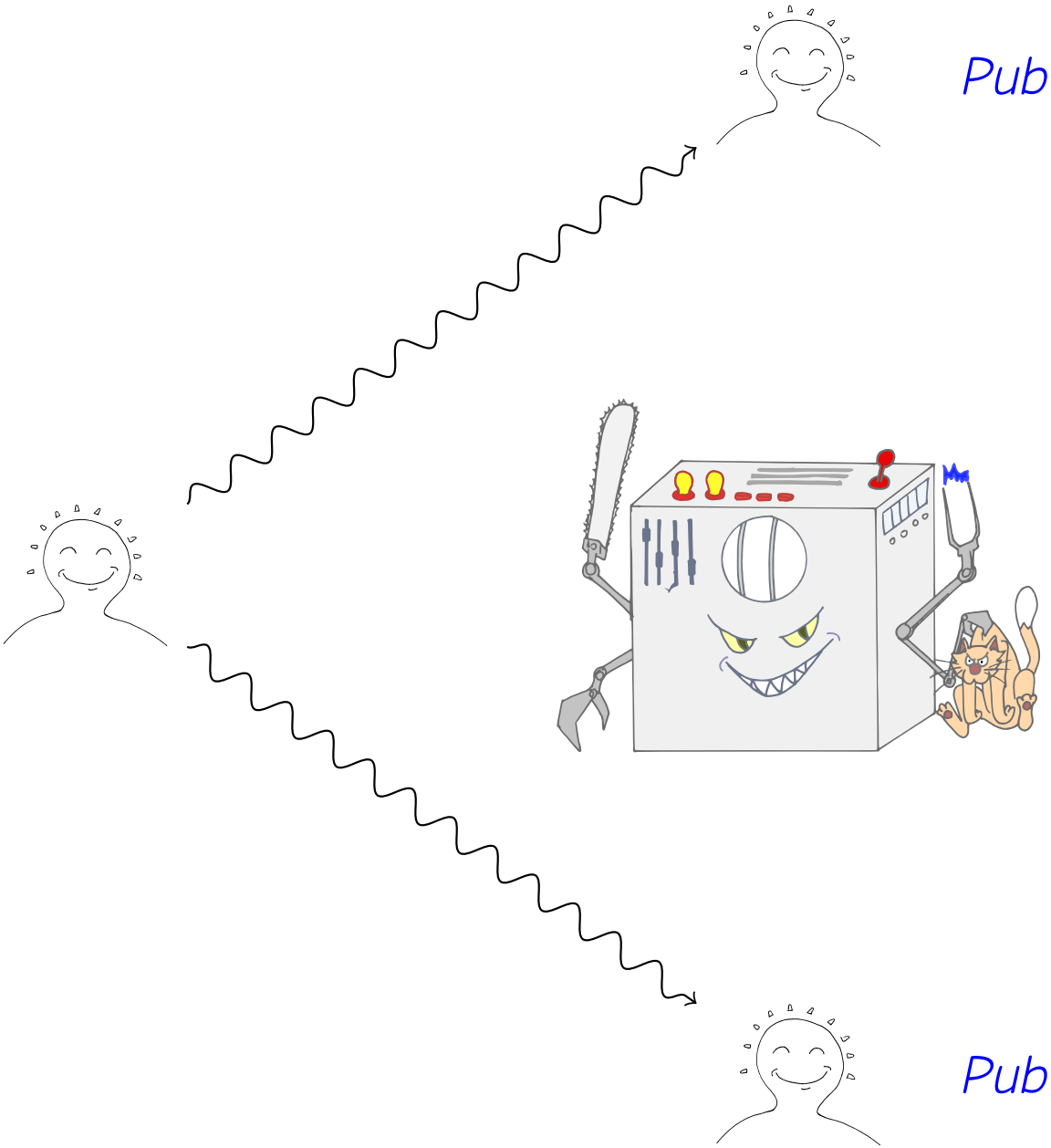
Elliptic curves of the world, UNITE!



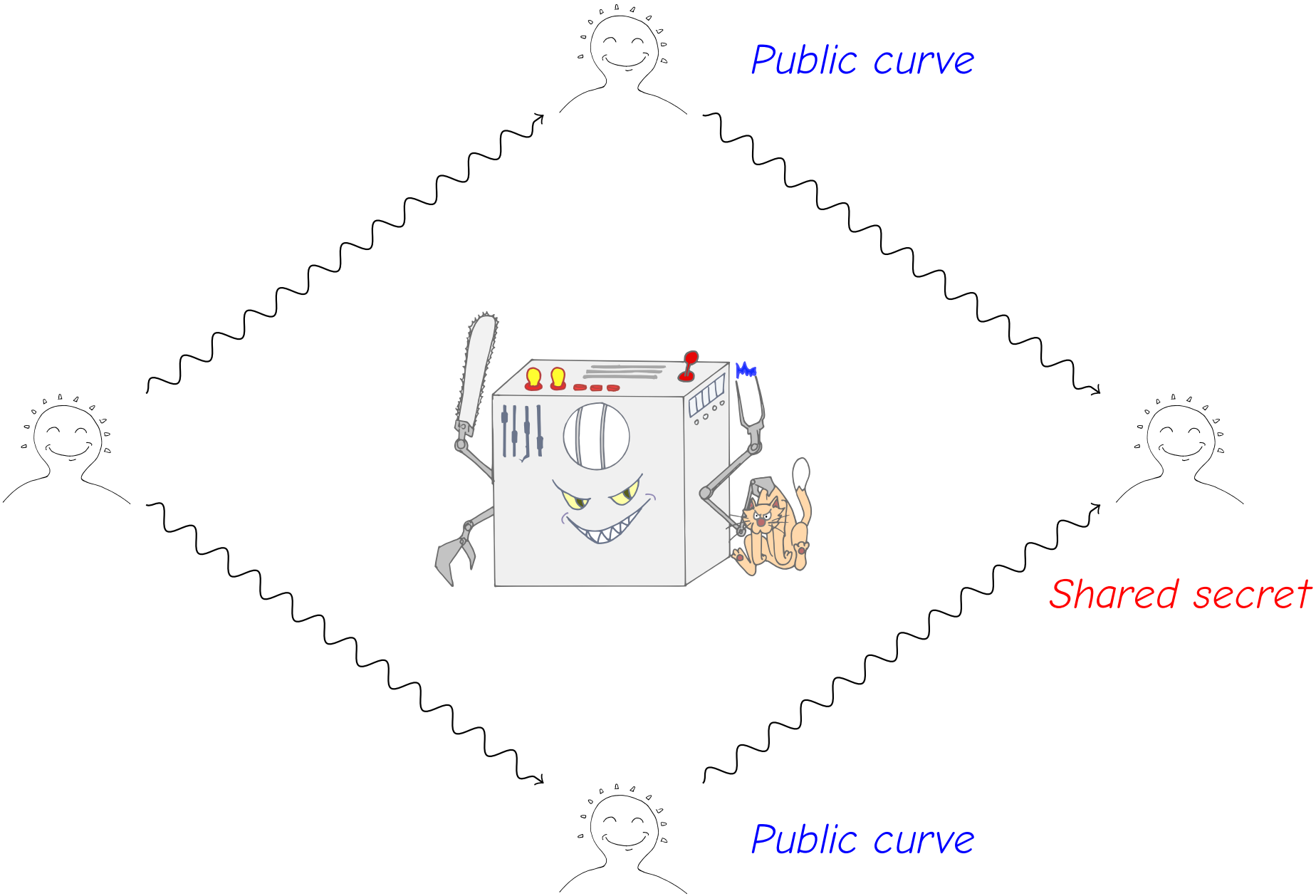
And so, they found a way around the QUANTOM



And so, they found a way around the QUANTOM



And so, they found a way around the QUANTOM



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

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

- 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).

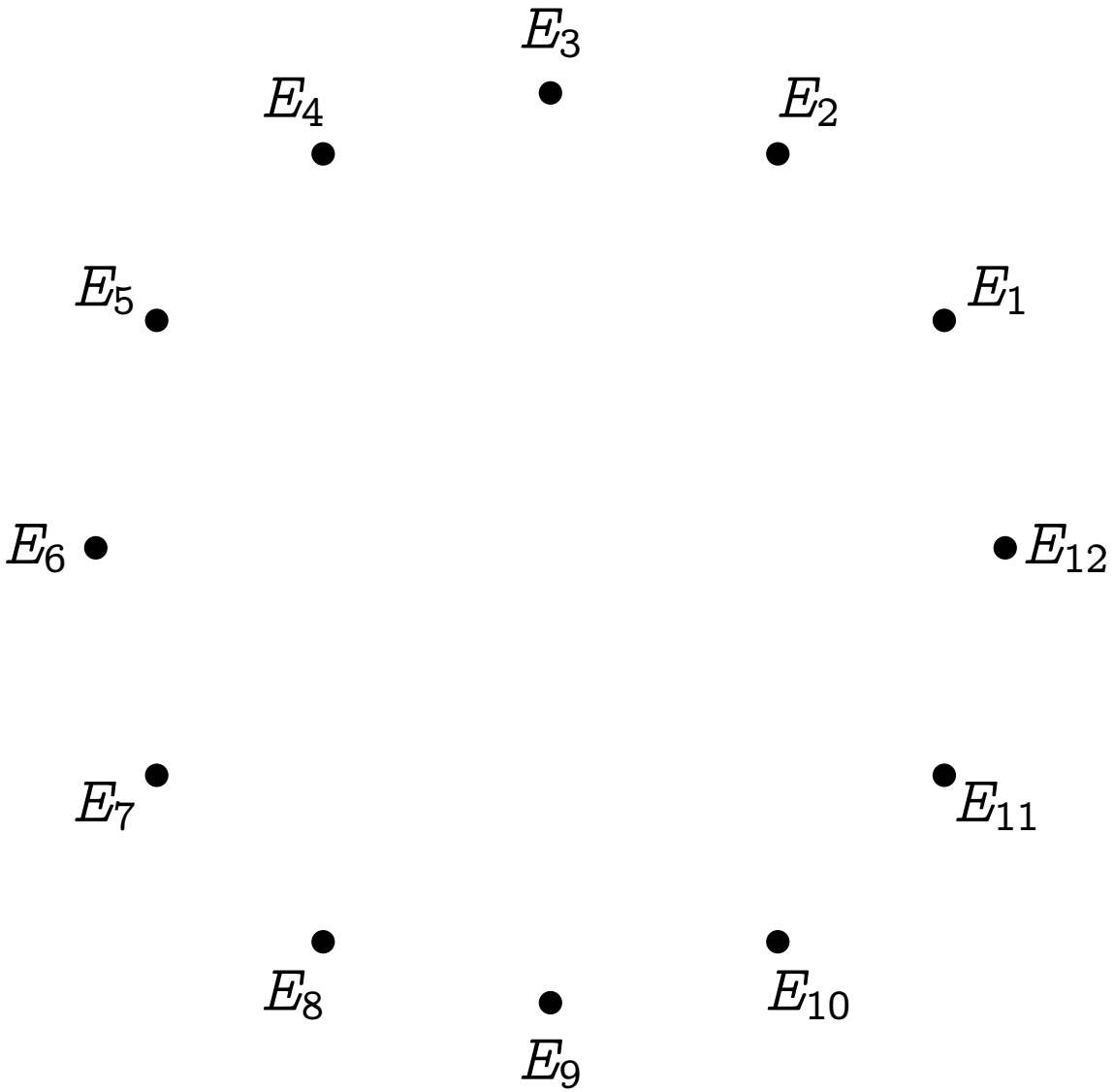
Theorem (Complex multiplication)

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

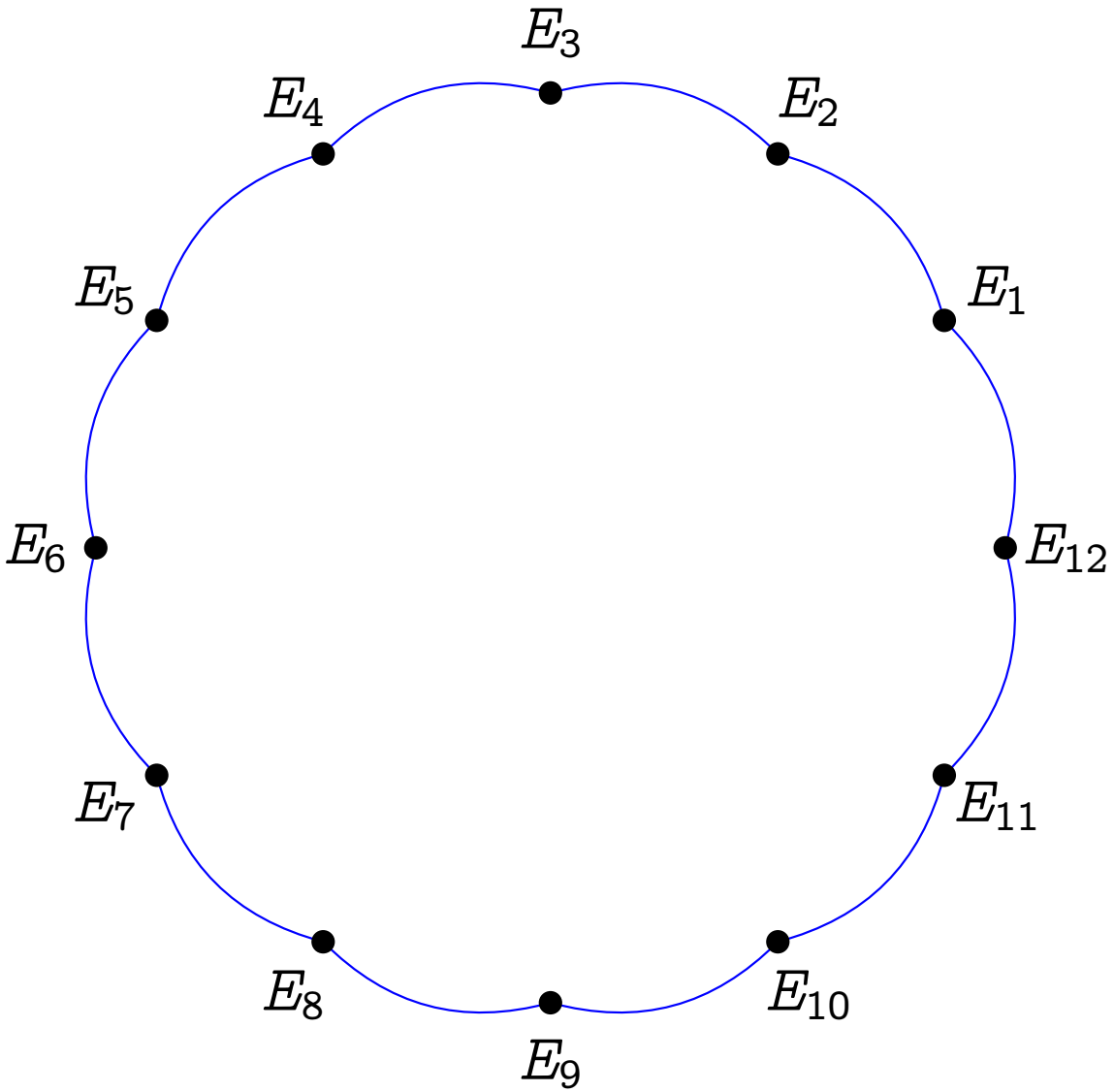
Let $\mathrm{End}(E)$ have discriminant D. Assume that $\left(\frac{D}{\ell}\right) = 1$, then E is on a crater of an ℓ-volcano, and the crater contains $h(\mathrm{End}(E))$ curves.

Complex multiplication graphs



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

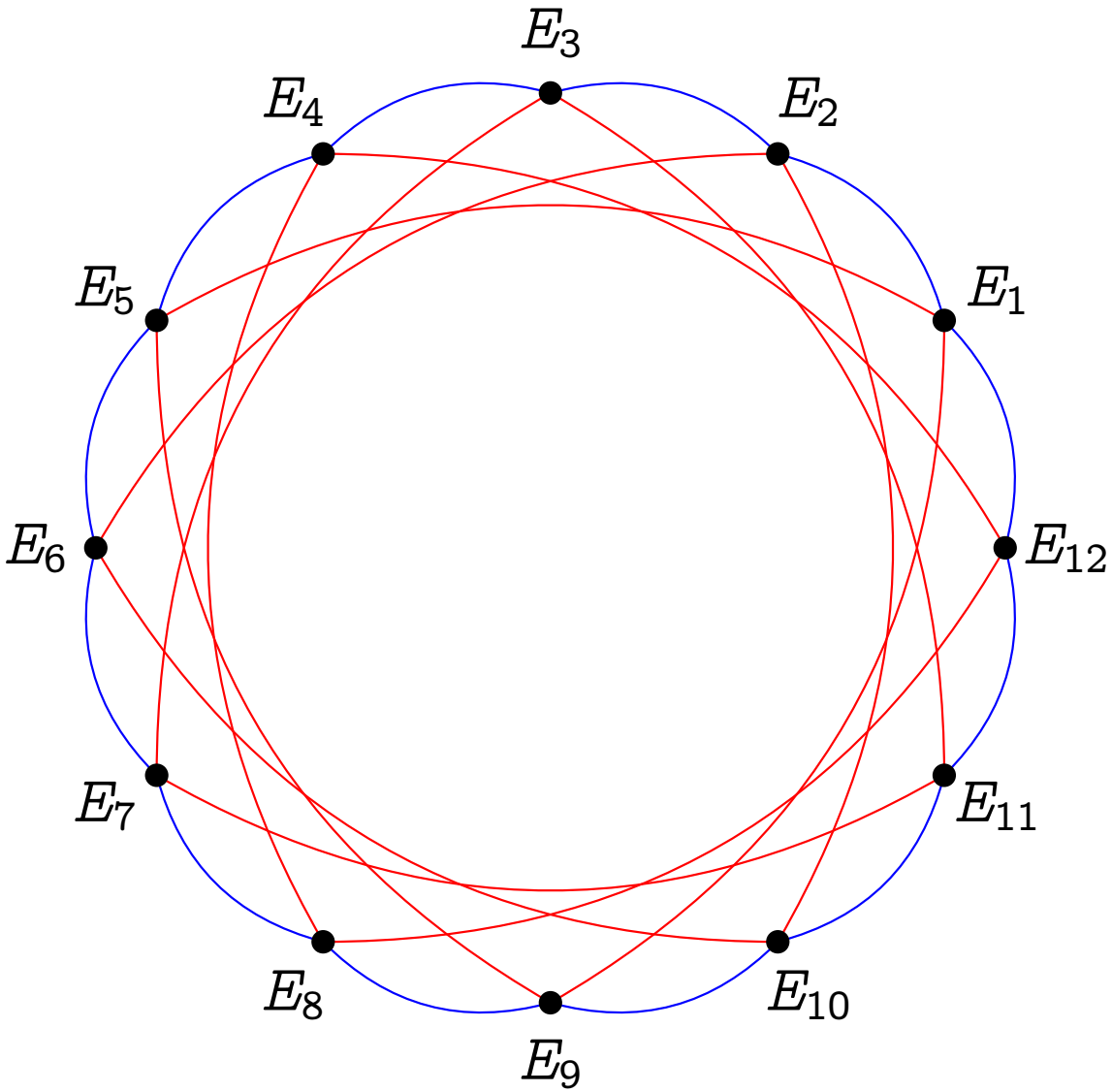
Complex multiplication graphs



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

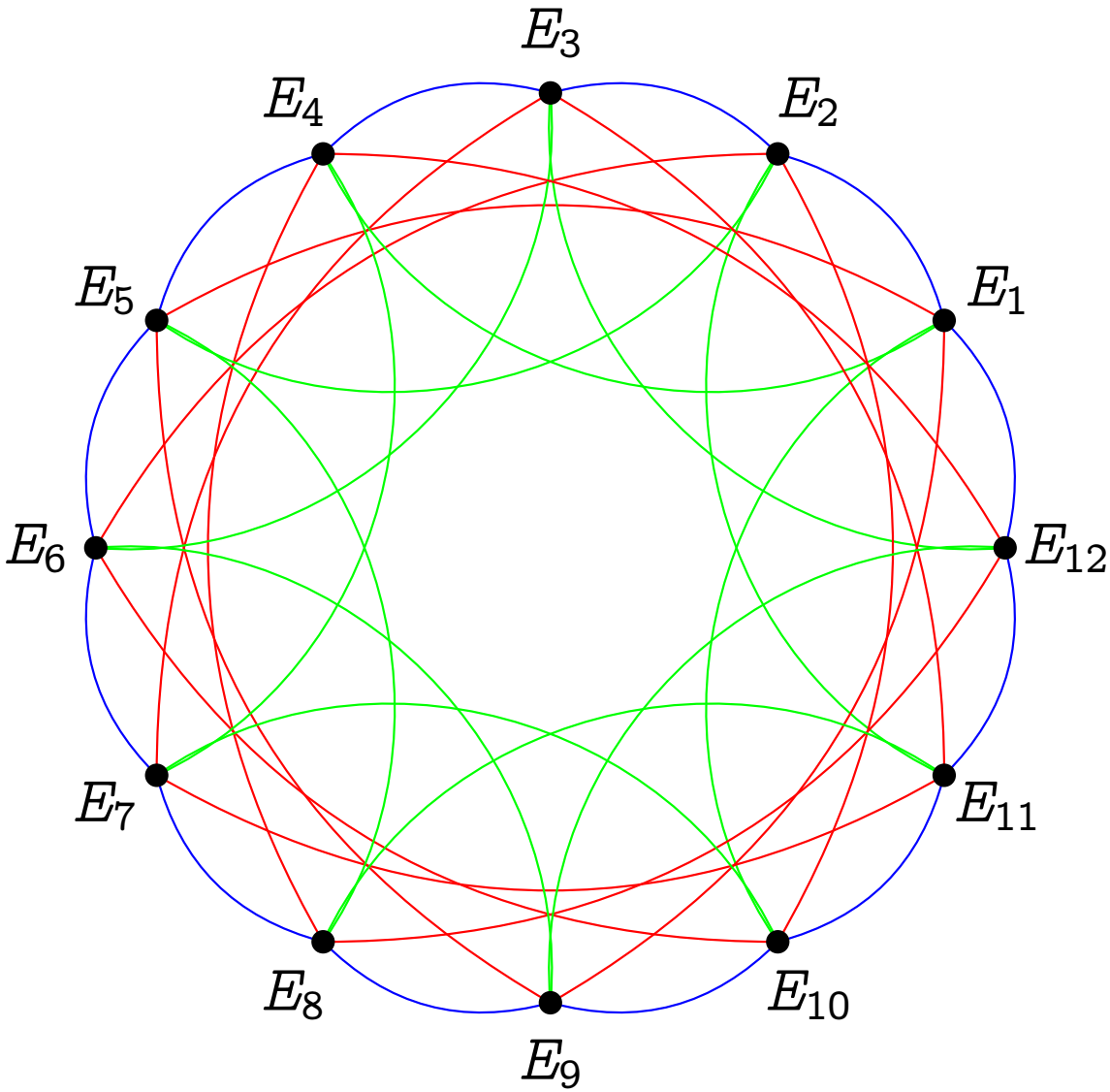


Vertices are elliptic curves with complex multiplication by $\mathcal{O}_K$ (i.e., $\mathrm{End}(E) \simeq \mathcal{O}_K \subset \mathbb{Q}(\sqrt{-D})$).
Edges are horizontal isogenies of bounded prime degree.

— degree 2

— degree 3

Complex multiplication graphs



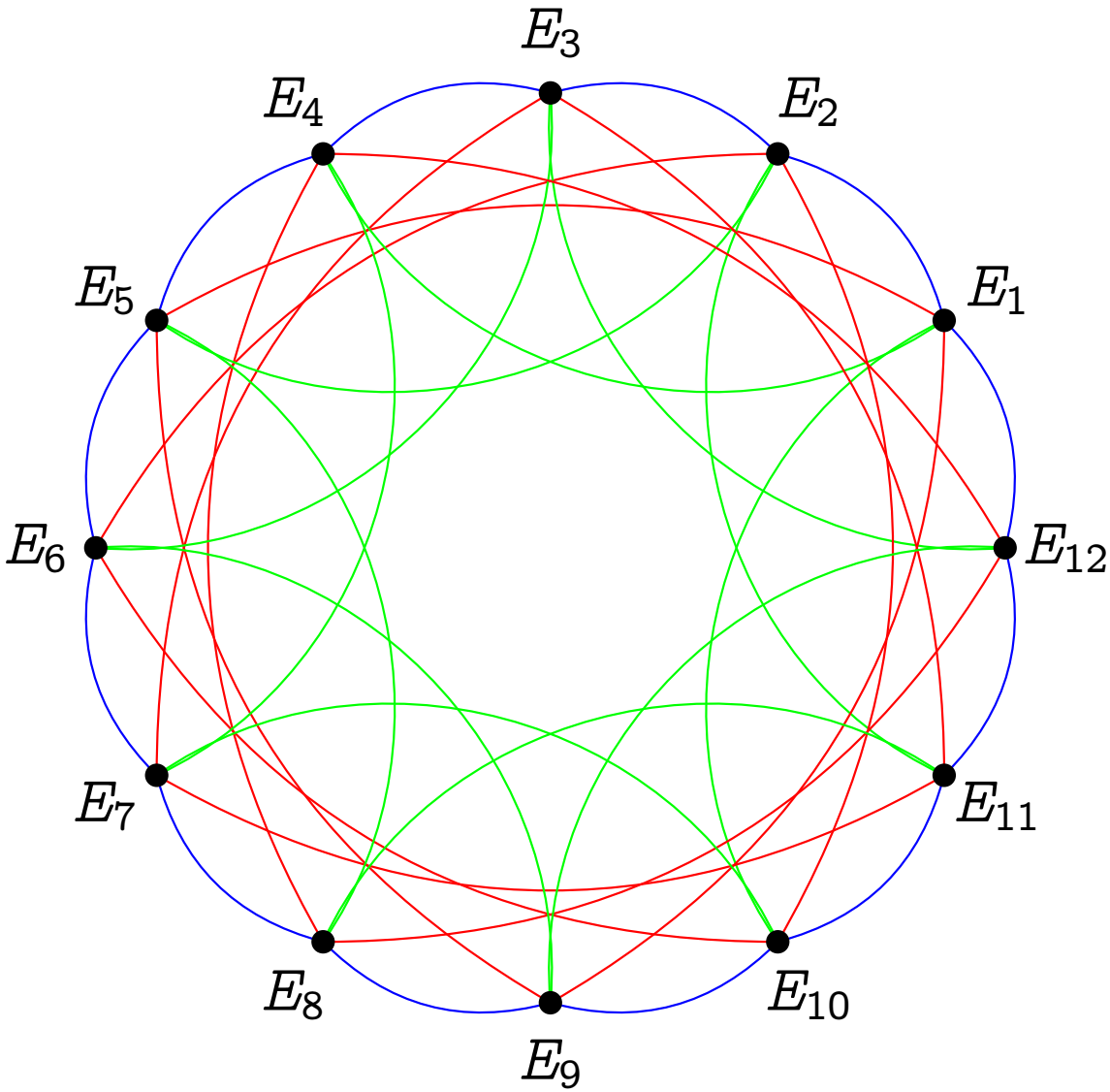
Vertices are elliptic curves with complex multiplication by $\mathcal{O}_K$ (i.e., $\mathrm{End}(E) \simeq \mathcal{O}_K \subset \mathbb{Q}(\sqrt{-D})$).
Edges are horizontal isogenies of bounded prime degree.

— degree 2

— degree 3

— degree 5

Complex multiplication graphs



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

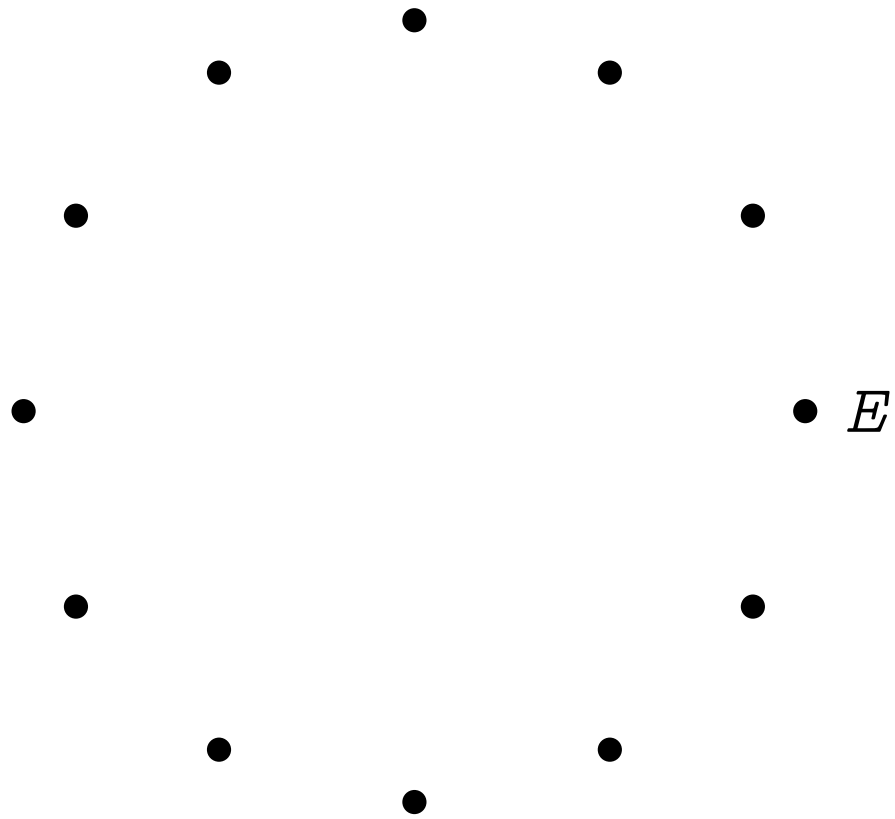
— degree 2

— degree 3

— degree 5

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

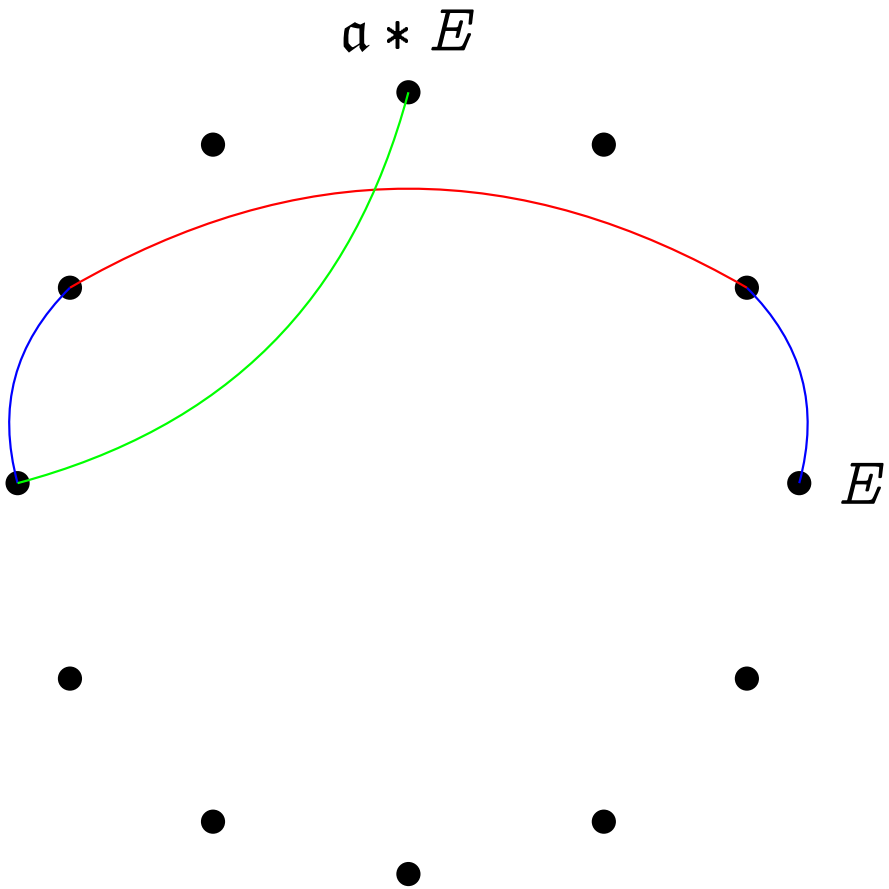
Couveignes–Rostovtsev–Stolbunov key exchange



Public parameters:

- A starting curve $E/\mathbb{F}_p$ with CM by $\mathcal{O}_K$;
- A set of ideals of small norm $S \subset \mathrm{Cl}(\mathcal{O}_K)$.

Couveignes–Rostovtsev–Stolbunov key exchange

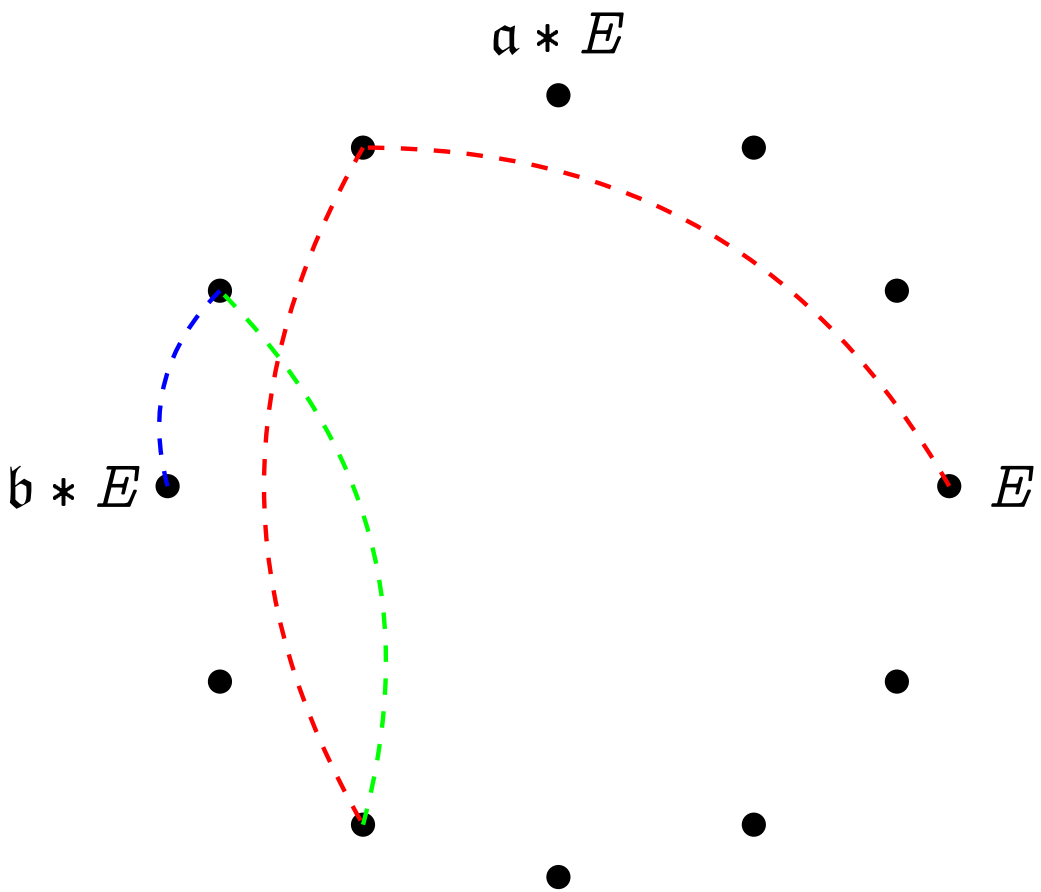


Public parameters:

- A starting curve $E/\mathbb{F}_p$ with CM by $\mathcal{O}_K$;
- A set of ideals of small norm $S \subset \mathrm{Cl}(\mathcal{O}_K)$.

1. **Alice** takes a secret random walk $\mathfrak{a} = \prod_{\mathfrak{s} \in S} \mathfrak{s}^{e_\mathfrak{s}}$ defining an isogeny $E \to \mathfrak{a} * E$;

Couveignes–Rostovtsev–Stolbunov key exchange

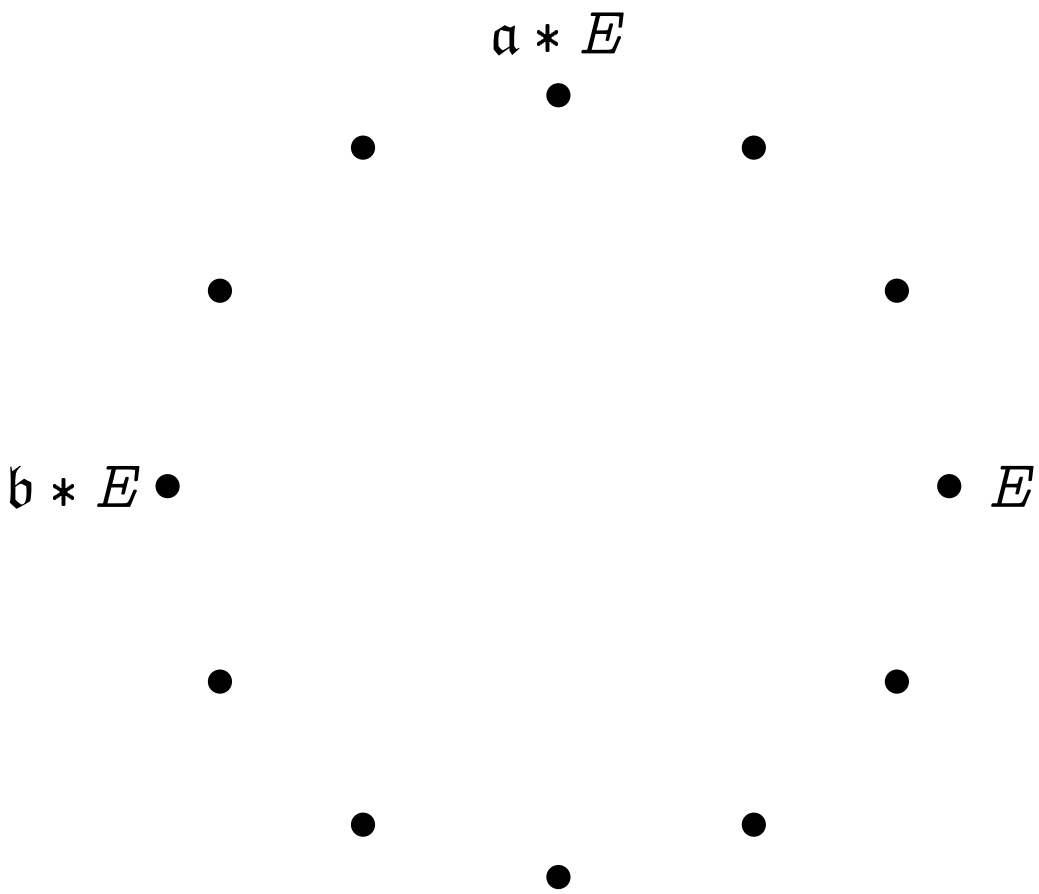


Public parameters:

- A starting curve $E/\mathbb{F}_p$ with CM by $\mathcal{O}_K$;
- A set of ideals of small norm $S \subset \mathrm{Cl}(\mathcal{O}_K)$.

1. **Alice** takes a secret random walk $\mathfrak{a} = \prod_{\mathfrak{s} \in S} \mathfrak{s}^{e_\mathfrak{s}}$ defining an isogeny $E \to \mathfrak{a} * E$;
2. **Bob** does the same;

Couveignes–Rostovtsev–Stolbunov key exchange

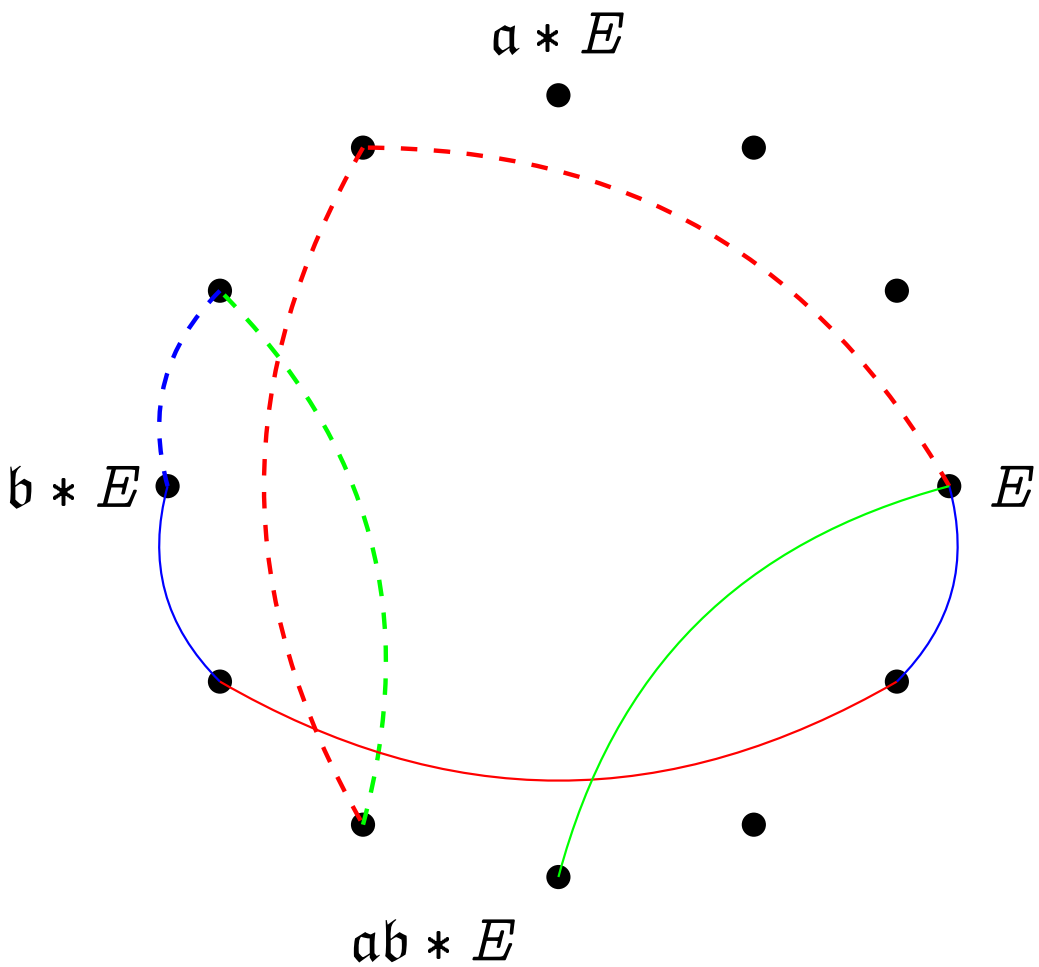


Public parameters:

- A starting curve $E/\mathbb{F}_p$ with CM by $\mathcal{O}_K$;
- A set of ideals of small norm $S \subset \mathrm{Cl}(\mathcal{O}_K)$.

1. **Alice** takes a secret random walk $\mathfrak{a} = \prod_{\mathfrak{s} \in S} \mathfrak{s}^{e_\mathfrak{s}}$ defining an isogeny $E \to \mathfrak{a} * E$;
2. **Bob** does the same;
3. They publish $\mathfrak{a} * E$ and $\mathfrak{b} * E$;

Couveignes–Rostovtsev–Stolbunov key exchange

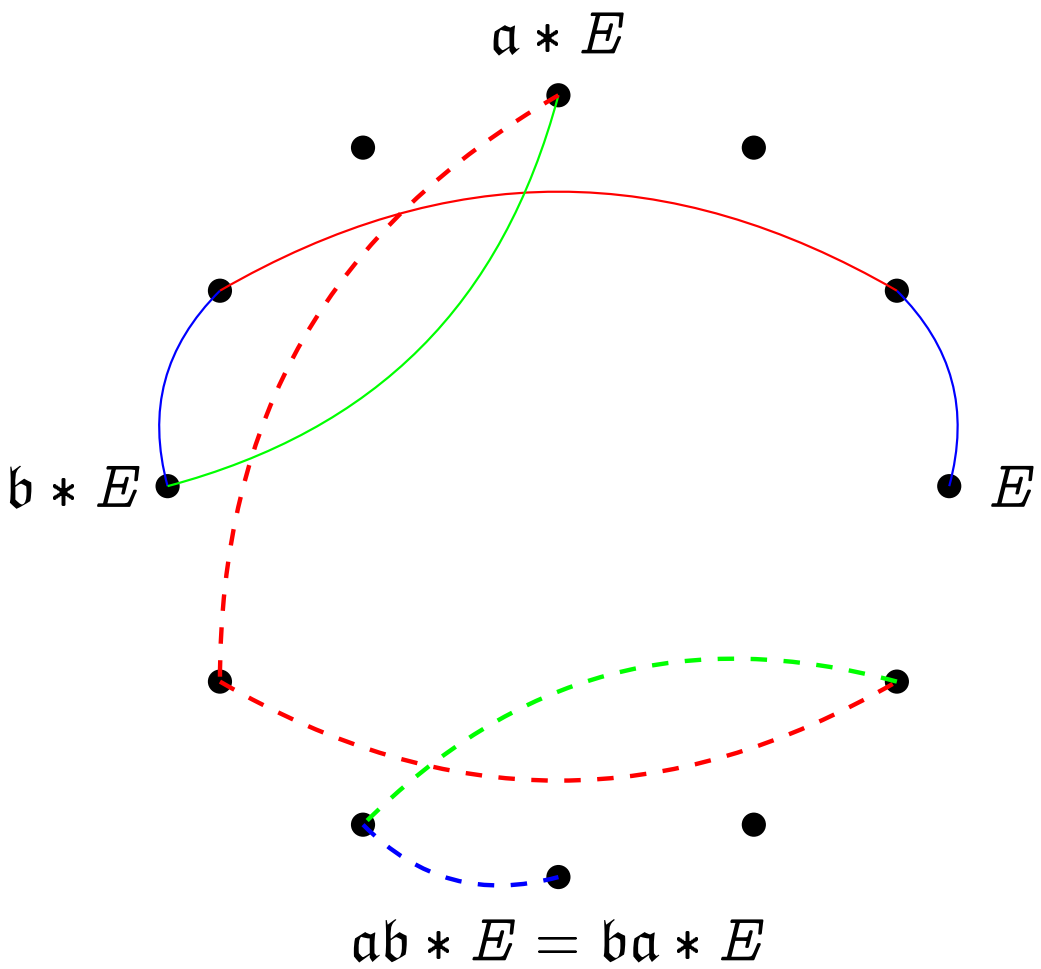


Public parameters:

- A starting curve $E/\mathbb{F}_p$ with CM by $\mathcal{O}_K$;
- A set of ideals of small norm $S \subset \mathrm{Cl}(\mathcal{O}_K)$.

1. **Alice** takes a secret random walk $\mathfrak{a} = \prod_{\mathfrak{s} \in S} \mathfrak{s}^{e_\mathfrak{s}}$ defining an isogeny $E \to \mathfrak{a} * E$;
2. **Bob** does the same;
3. They publish $\mathfrak{a} * E$ and $\mathfrak{b} * E$;
4. **Alice** repeats her secret walk $\mathfrak{a}$ starting from $\mathfrak{b} * E$.

Couveignes–Rostovtsev–Stolbunov key exchange



Public parameters:

- A starting curve $E/\mathbb{F}_p$ with CM by $\mathcal{O}_K$;
- A set of ideals of small norm $S \subset \mathrm{Cl}(\mathcal{O}_K)$.

1. **Alice** takes a secret random walk $\mathfrak{a} = \prod_{\mathfrak{s} \in S} \mathfrak{s}^{e_\mathfrak{s}}$ defining an isogeny $E \to \mathfrak{a} * E$;
2. **Bob** does the same;
3. They publish $\mathfrak{a} * E$ and $\mathfrak{b} * E$;
4. **Alice** repeats her secret walk $\mathfrak{a}$ starting from $\mathfrak{b} * E$.
5. **Bob** repeats his secret walk $\mathfrak{b}$ starting from $\mathfrak{a} * E$.

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.

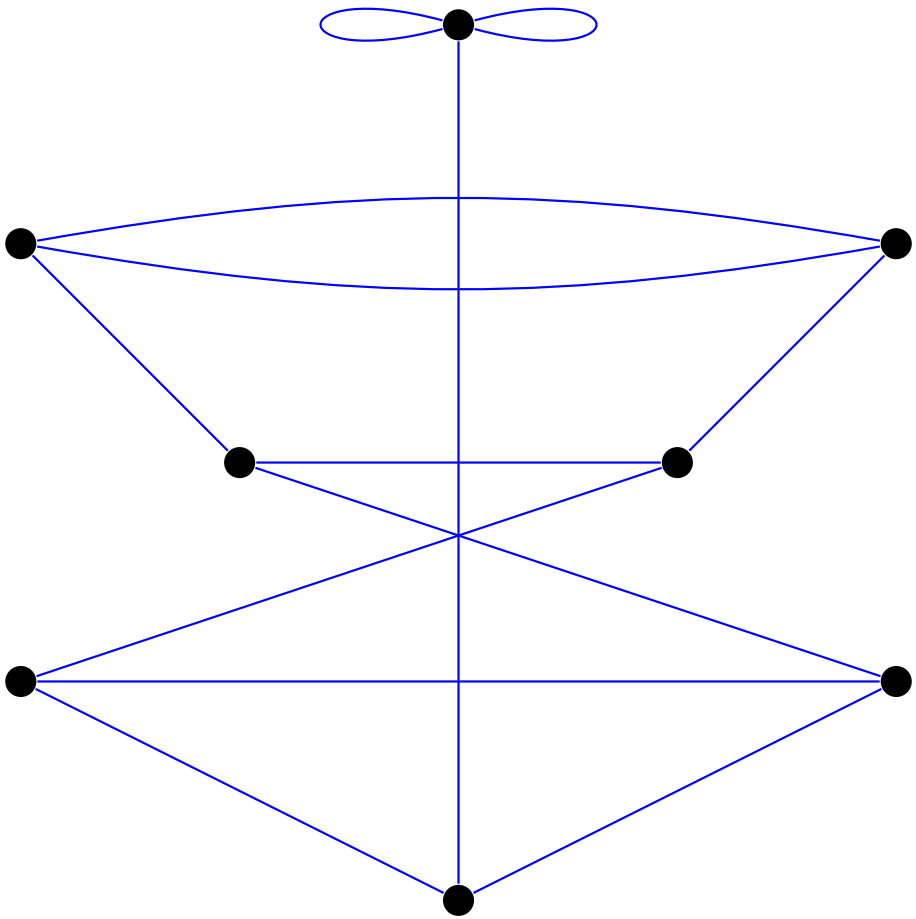


Figure: 2- and 3-isogeny graphs on $\mathbb{F}_{97^2}$.

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.

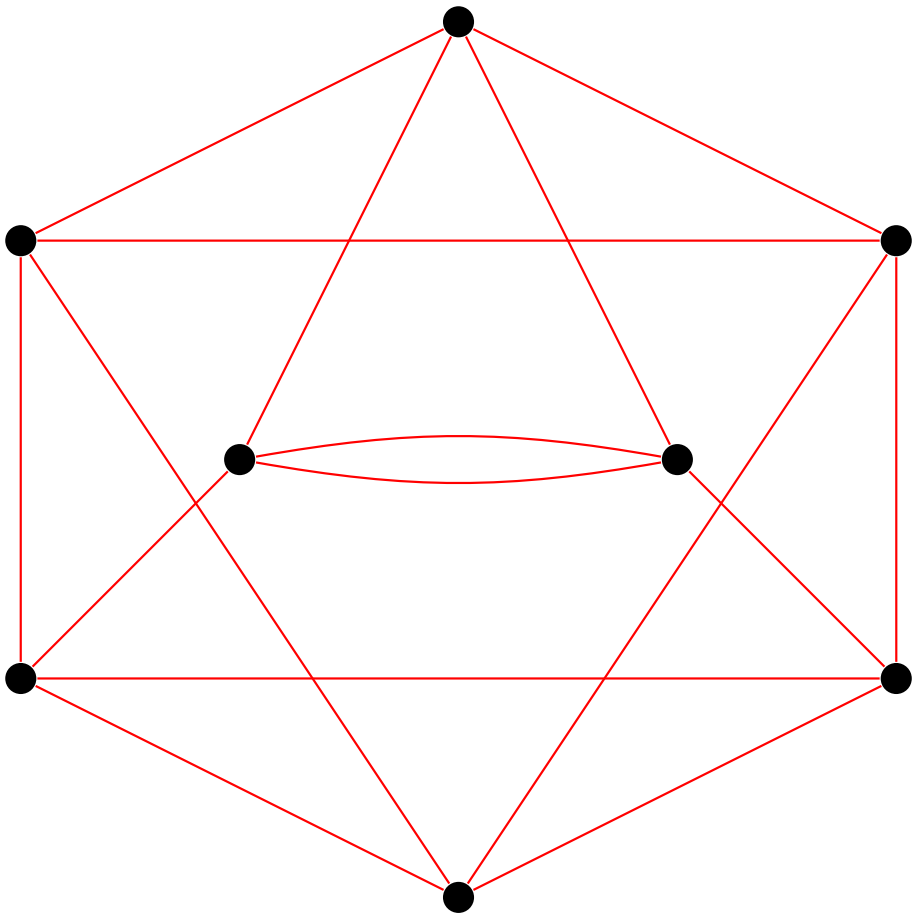


Figure: 2- and 3-isogeny graphs on $\mathbb{F}_{97^2}$.

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.

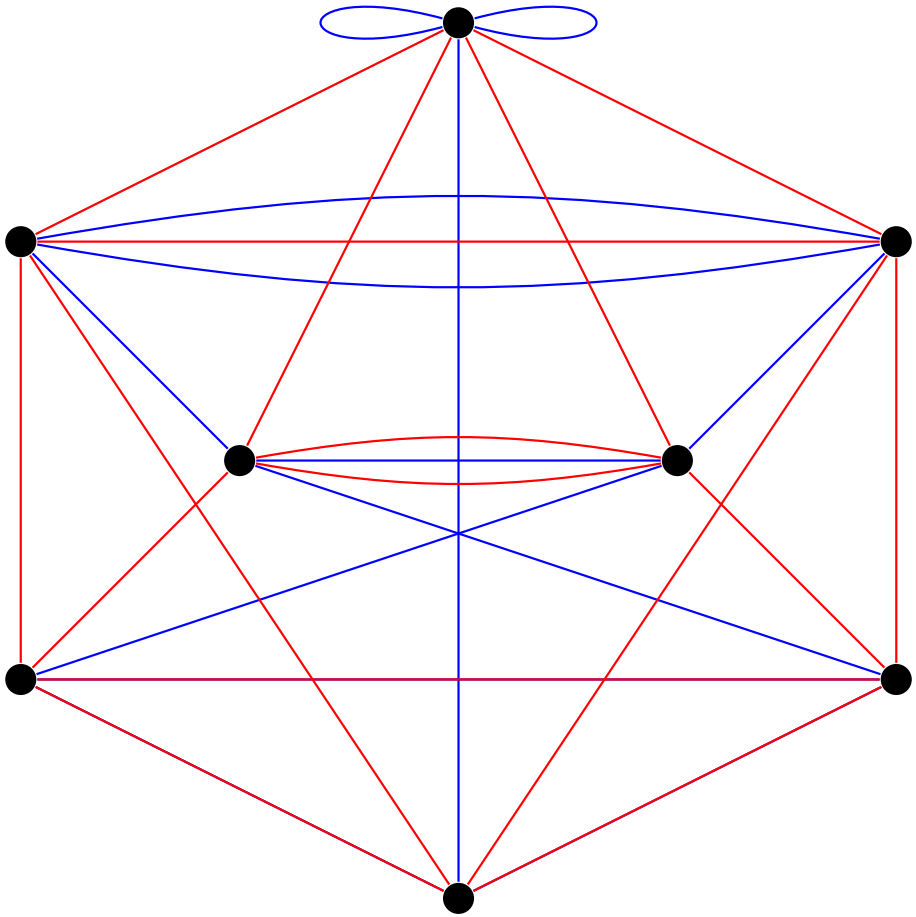


Figure: 2- and 3-isogeny graphs on $\mathbb{F}_{97^2}$.

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 $\ell_A^{e_A}$

$=$

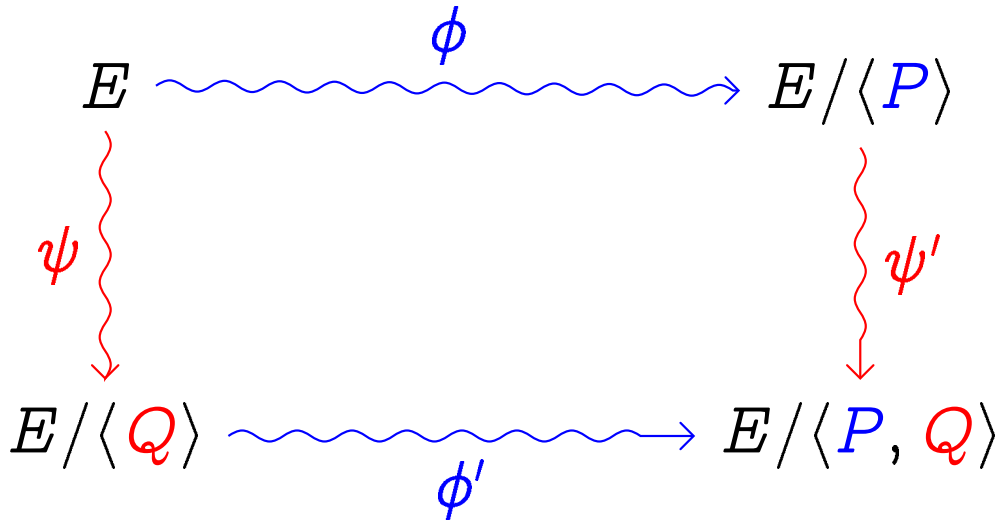
Kernel $\langle P \rangle \subset E[\ell_A^{e_A}]$

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

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

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

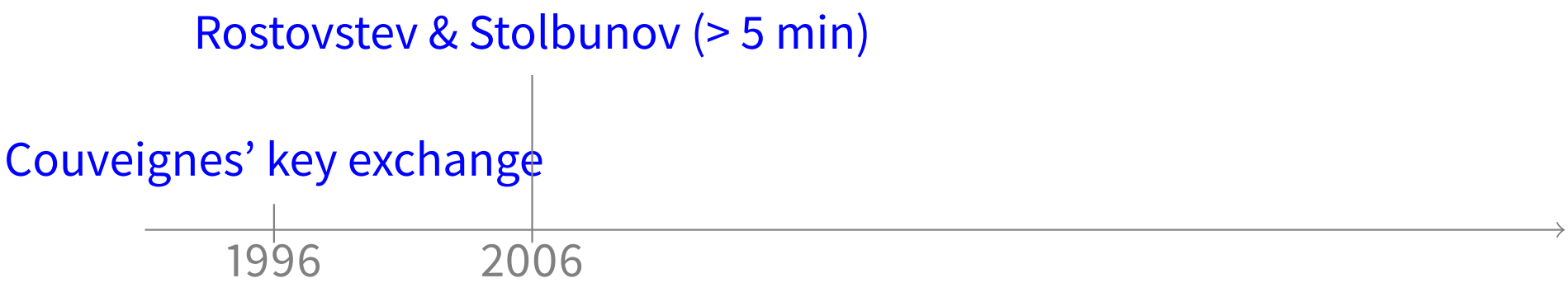
$$\ker \psi' = \langle \phi(Q) \rangle$$



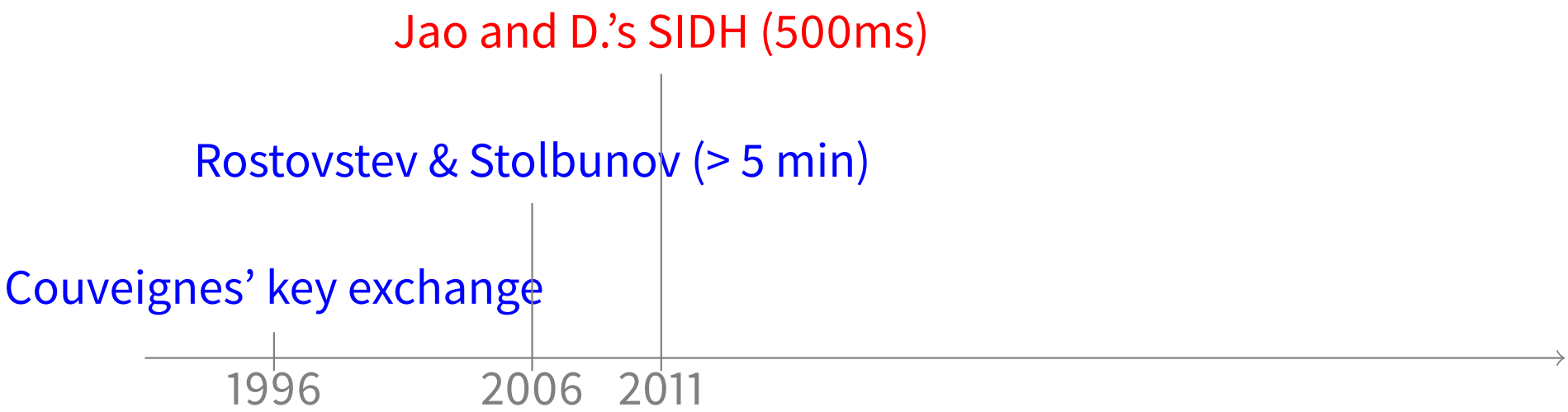
From 10 minutes to 10ms in 20 years

Couveignes' key exchange

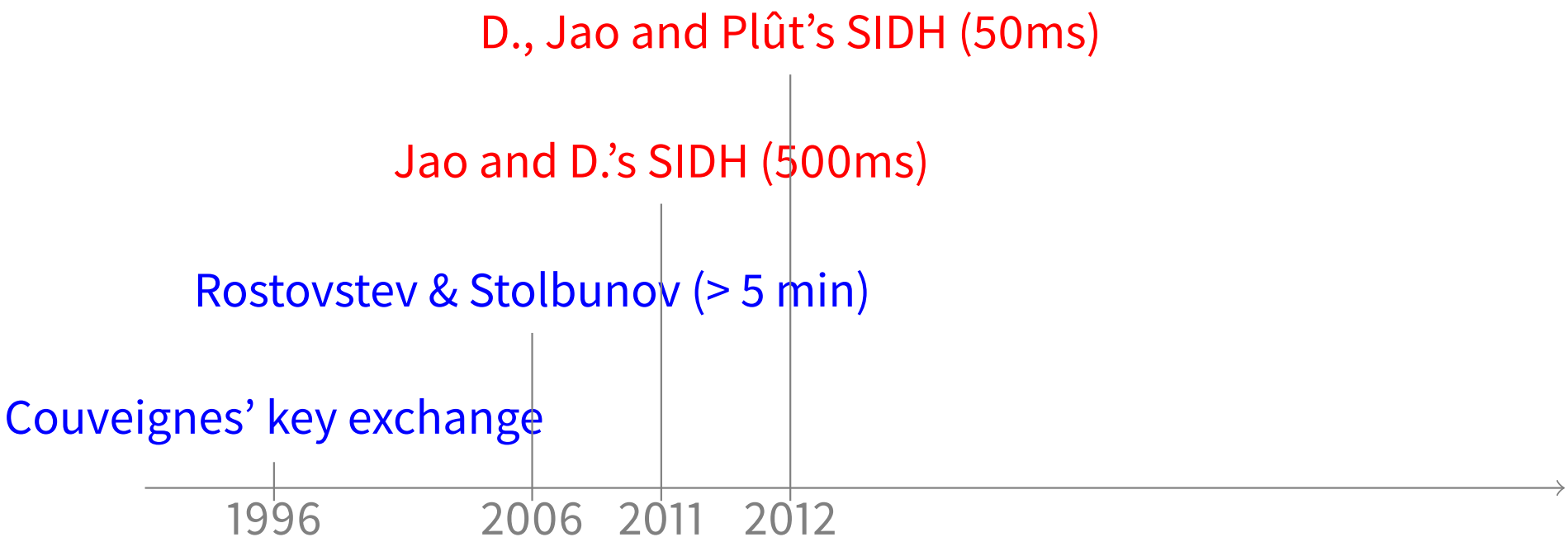
From 10 minutes to 10ms in 20 years



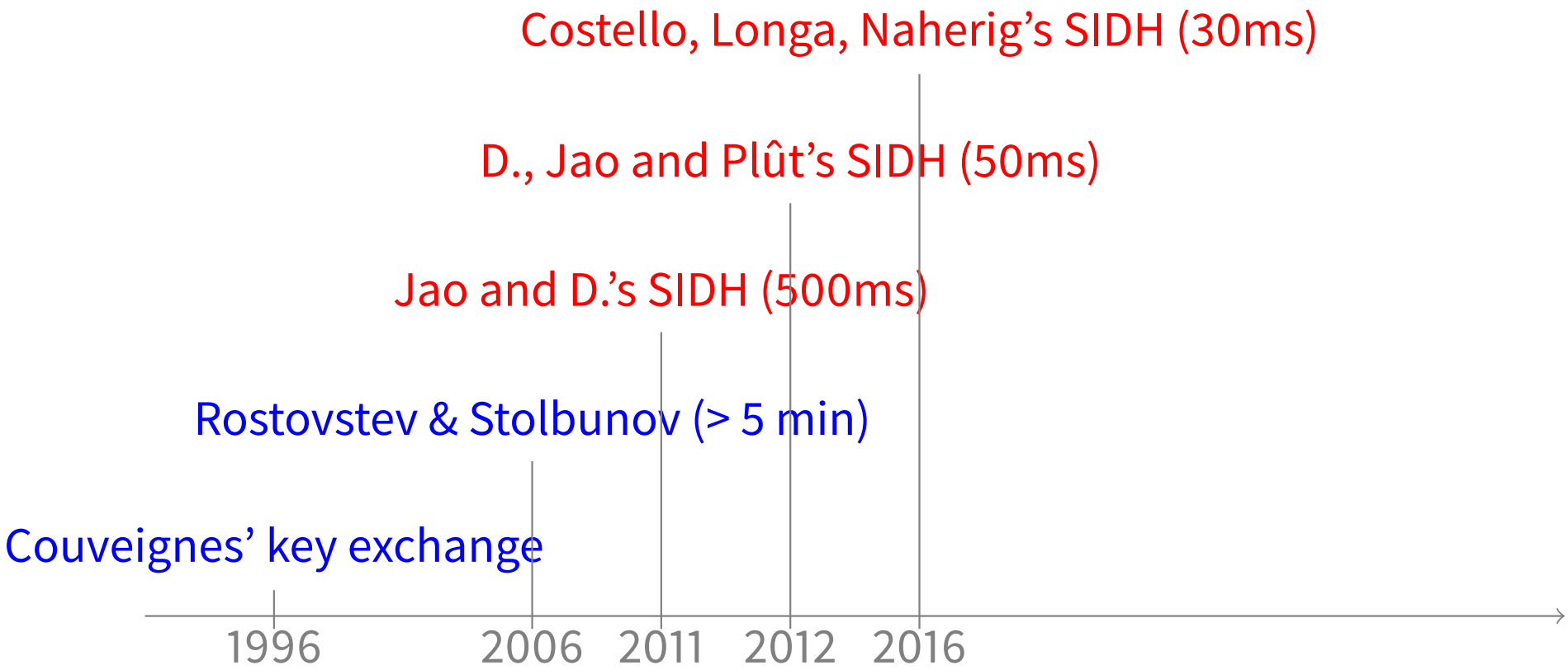
From 10 minutes to 10ms in 20 years



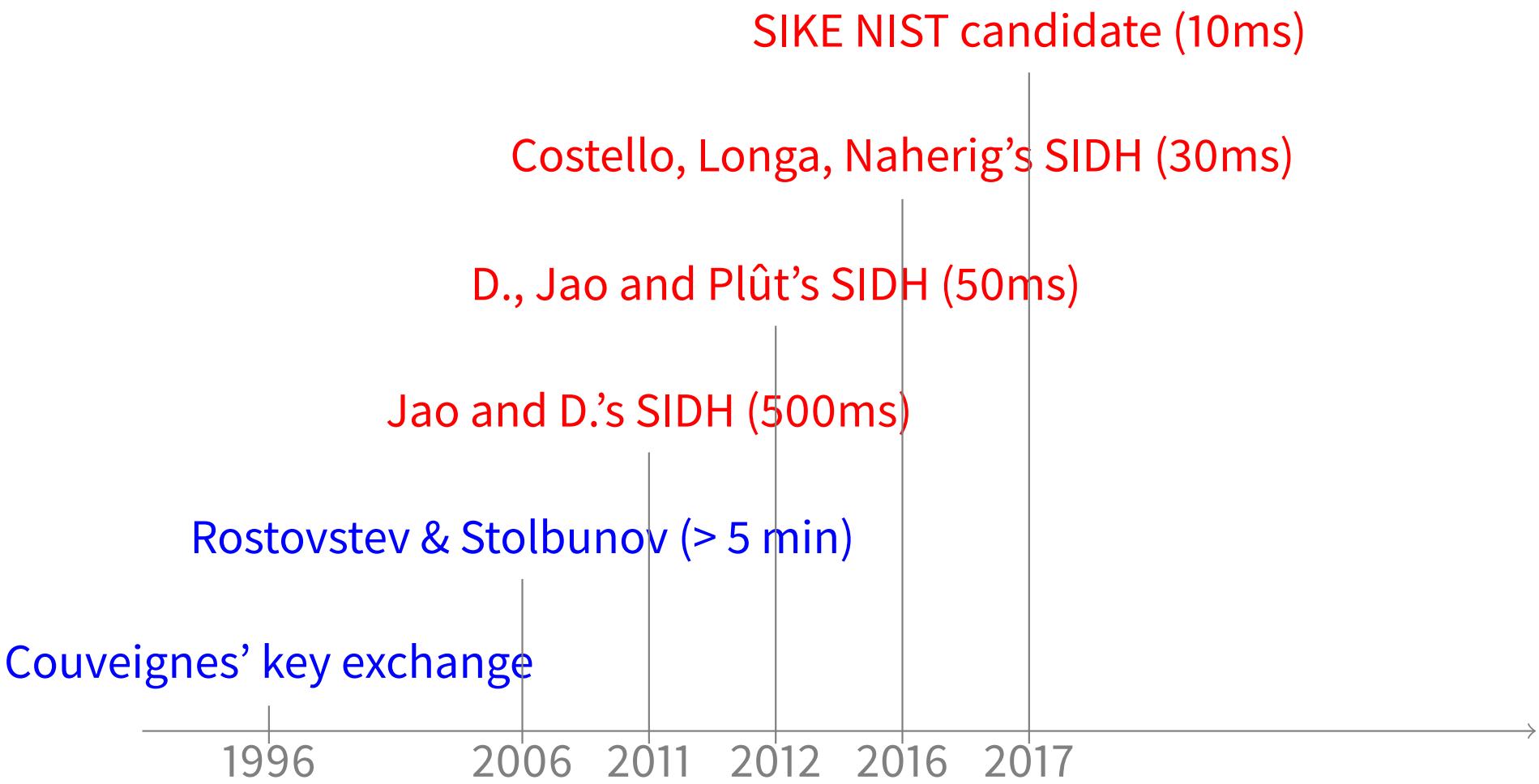
From 10 minutes to 10ms in 20 years



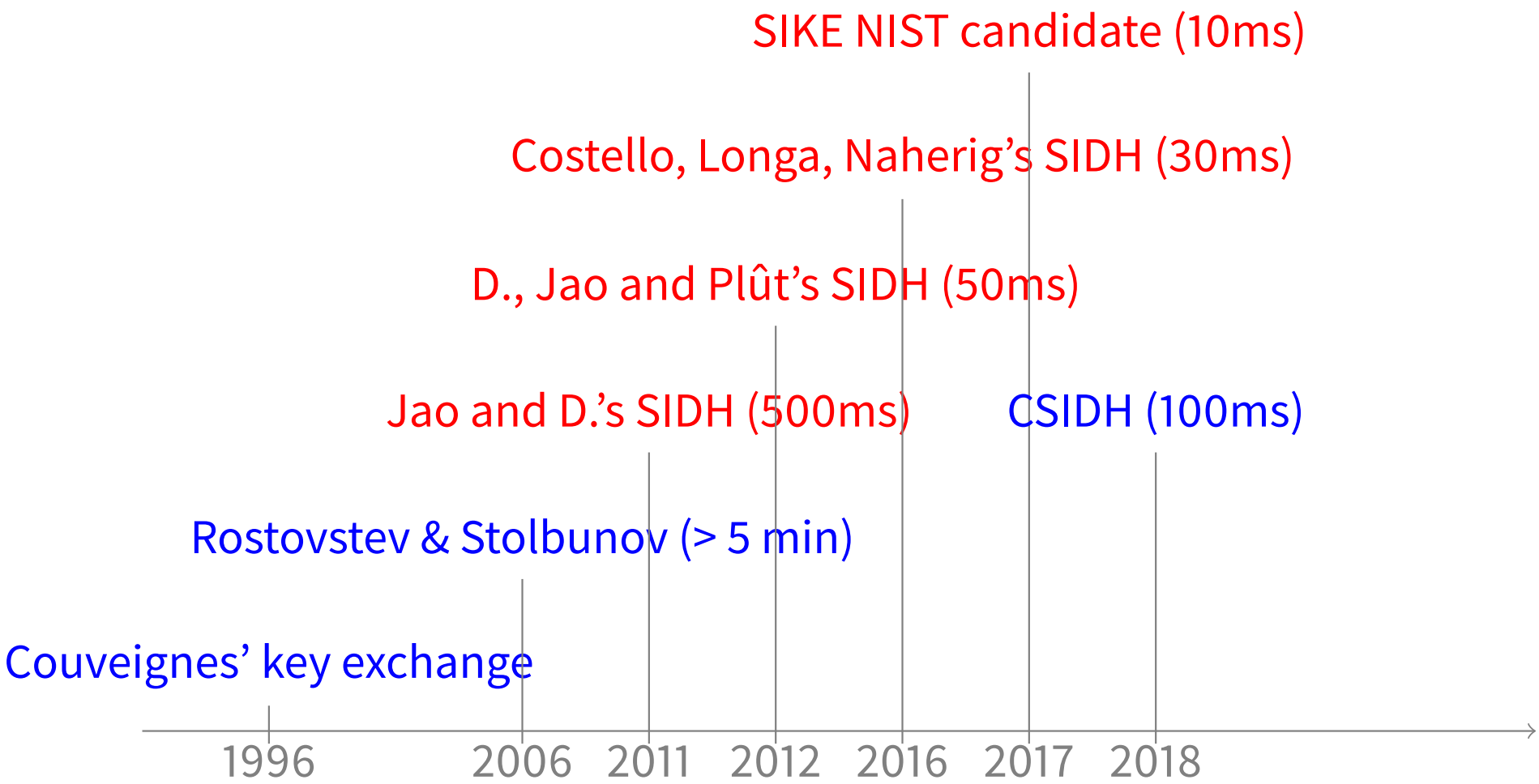
From 10 minutes to 10ms in 20 years



From 10 minutes to 10ms in 20 years



From 10 minutes to 10ms in 20 years



CSIDH (pron.: *sea-side*)

Speeding up the CRS key exchange (De Feo, Kieffer, and Smith 2018)

- Choose p such that $\ell \mid (p+1)$ for many small primes ℓ;
- Look for random ordinary curves such that: HARD!
  - $\ell \mid E(\mathbb{F}_p)$,
  - technical condition;
- Use Vélu's formulas for those primes ℓ.
- $\sim$5 minutes for a 128-bit secure key exchange ☹

CSIDH (Castryck, Lange, Martindale, Panny, and Renes 2018)

- Choose p such that $\ell \mid (p+1)$ for many small primes ℓ;
- Select a supersingular curve $E/\mathbb{F}_p$, automatically EASY!
  - $\#E(\mathbb{F}_p) = p+1$,
  - technical condition always satisfied;
- $\sim$100ms for a 128 bits secure key exchange ☺

Research perspectives

Fundamentals

- Generalizations to other isogeny graphs (e.g., graphs of abelian varieties of higher dimension).
- Attacks on the primitives: solving isogeny problems, computing endomorphism rings of supersingular isogenies, computations in quaternion algebras.
- Security proofs: proving properties of sampling in Cayley graphs.

Research perspectives

Quantum

- Fundamental algorithms: Kuperberg's algorithm (CSIDH), claw finding (SIDH).
- *Ad hoc* algorithms: exploiting the non-generic structure in SIDH, CSIDH.
- Constructive algorithms: SeaSign can be considerably sped up by a quantum pre-computation.
- Security proofs in the QROM.

Protocols

- Efficient signatures.
- New primitives/properties, mix and match CSIDH/SIDH/pairings.
- More uses of CSIDH as a Diffie–Hellman replacement (e.g., NIKE).

Research perspectives

Implementations

- Constrained devices: SIDH still very slow on IOT gear, high memory footprint.
- Side-channel resistance: constant time (lacking for CISDH), analysis of proposed hardware attacks, countermeasures.

Tools

- Develop tools for educational/prototyping purposes: lower the entry barrier to isogenies.
- SageMath most popular (open source) platform for number theory/computer algebra. Improve functionality for elliptic curves / pairings / isogenies.

Thank you

https://defeo.lu/

@luca_defeo