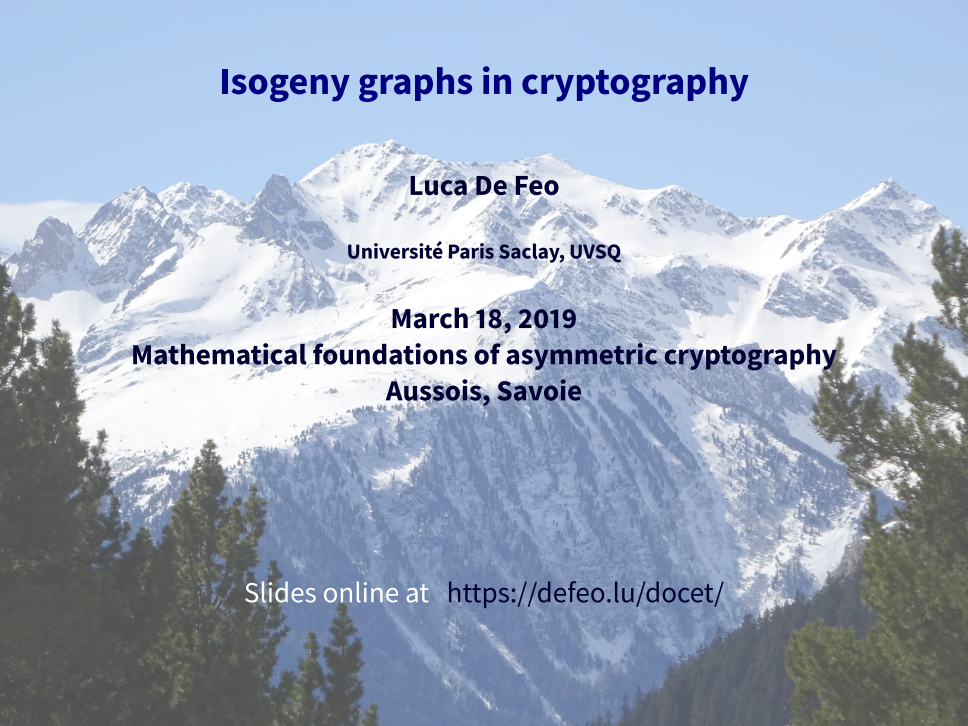


Isogeny graphs in cryptography

Luca De Feo

Université Paris Saclay, UVSQ

March 18, 2019
Mathematical foundations of asymmetric cryptography
Aussois, Savoie

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

Overview

1. Isogeny graphs
   - Elliptic Curves
   - Isogenies
   - Isogeny graphs
   - Endomorphism rings
   - Ordinary graphs
   - Supersingular graphs
2. Cryptography
   - Isogeny walks and Hash functions
   - Pairing verification and Verifiable Delay Functions
   - Key exchange
   - Open Problems

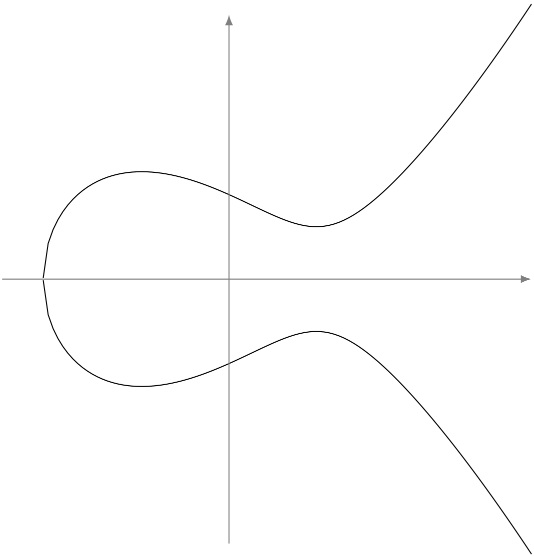
Elliptic curves

Let k be a field of characteristic $\neq 2, 3$.

An elliptic curve *defined over* k is the locus in the projective space $\mathbb{P}^2(\bar{k})$ of an equation

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

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



Elliptic curves

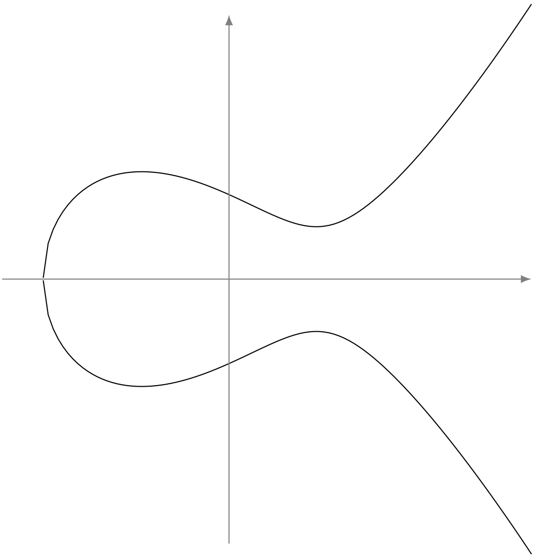
Let k be a field of characteristic $\neq 2, 3$.

An elliptic curve *defined over* k is the locus in the projective space $\mathbb{P}^2(\bar{k})$ 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;



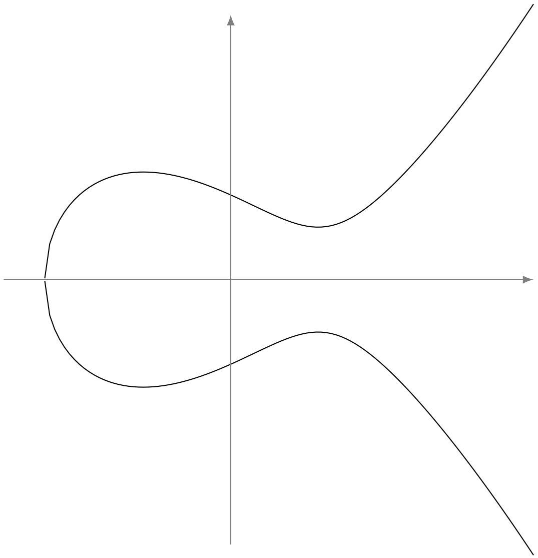
Elliptic curves

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

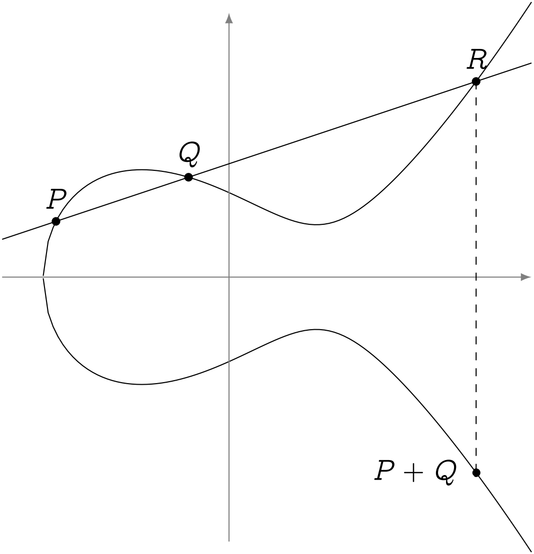


The group law

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.



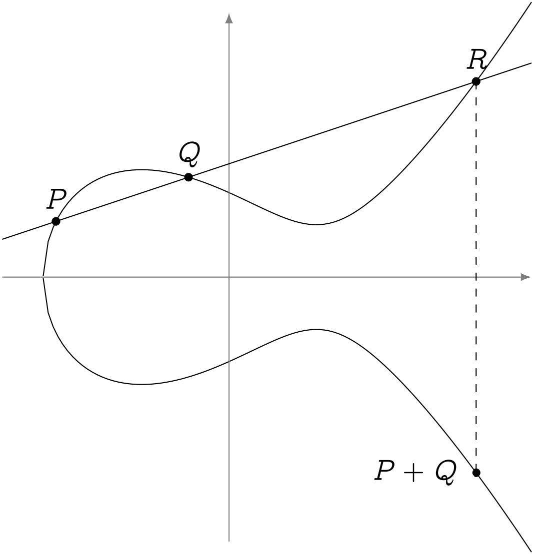
The group law

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*);



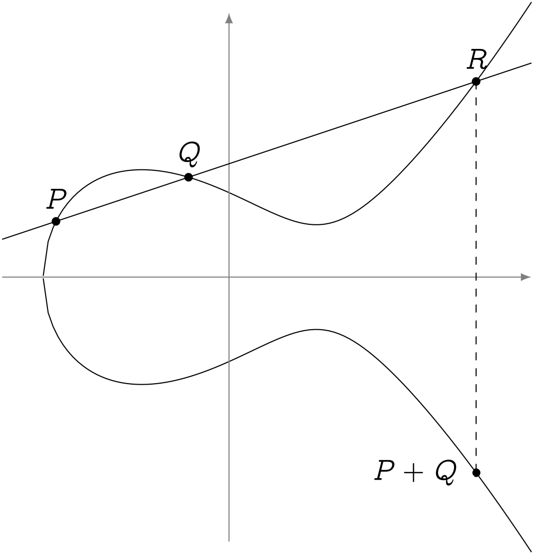
The group law

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.



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 $G = \langle g \rangle$ of (prime) order q.

$$\begin{array}{ccc}
\textbf{Alice} & & \textbf{Bob} \\[2em]
\text{pick random } a \in \mathbb{Z}/q\mathbb{Z} & & \text{pick random } b \in \mathbb{Z}/q\mathbb{Z} \\
\text{compute } A = g^a & & \text{compute } B = g^b \\
& \xrightarrow{\quad\quad\quad\quad A \quad\quad\quad\quad} & \\
& \xleftarrow[\quad\quad\quad\quad B \quad\quad\quad\quad]{} &
\end{array}$$

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

Brief history of DH key exchange

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

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

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

1994 Shor publishes his quantum polynomial time discrete logarithm / factoring algorithm.

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

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

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

Why should I care? (cont'd)

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);
- …

What are elliptic curves?

For mathematicians

- The smooth projective curves of genus 1 (with a distinguished point);
- The simplest abelian varieties (dimension 1);
- Finitely generated abelian groups of mysterious free rank (aka BSD conjecture);
- What you use to make examples.

What are elliptic curves?

For mathematicians

- The smooth projective curves of genus 1 (with a distinguished point);
- The simplest abelian varieties (dimension 1);
- Finitely generated abelian groups of mysterious free rank (aka BSD conjecture);
- What you use to make examples.

For cryptographers

- Finite abelian groups (often cyclic);
- Easy to compute the order;
- "2-dimensional" generalizations of μ_k (the roots of unity of k)…
- …with bilinear maps (aka pairings)!

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 $j(E) = j(E')$.

Group structure

Torsion structure

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

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

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

Finite fields (Hasse's theorem)

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

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

In particular, there exist integers n_1 and $n_2 | \gcd(n_1, q-1)$ such that

$$E(\mathbb{F}_q) \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}.$$

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

What is ~~scalar multiplication~~ an isogeny?

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

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

(Separable) isogenies ⇔ finite subgroups:

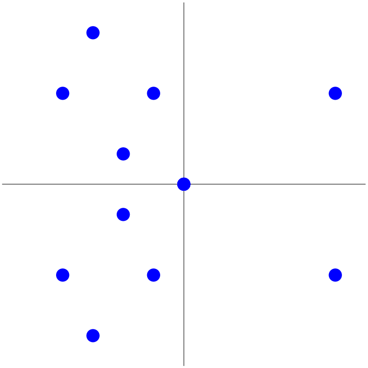
$$0 \longrightarrow H \longrightarrow E \xrightarrow{\phi} E' \to 0$$

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

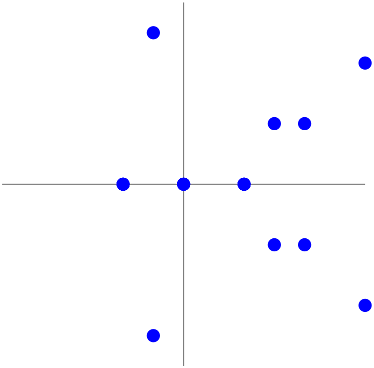
$$E/H \stackrel{\text{def}}{=} E'.$$

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

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

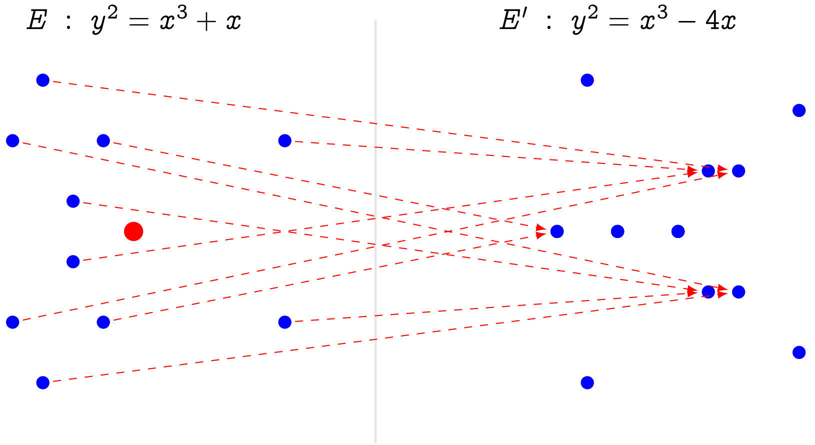


$$E' \;:\; y^2 = x^3 - 4x$$



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

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



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

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

Isogeny properties

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

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

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

Degree, separability

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

Isogeny properties

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

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

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

Degree, separability

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

The dual isogeny

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

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

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

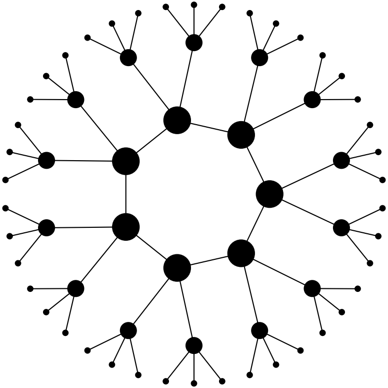
1. $\hat{\phi}$ is defined over k if and only if ϕ is;
2. $\widehat{\psi \circ \phi} = \hat{\phi} \circ \hat{\psi}$ for any isogeny $\psi : E' \to E''$;
3. $\widehat{\psi + \phi} = \hat{\psi} + \hat{\phi}$ for any isogeny $\psi : E \to E'$;
4. $\deg \phi = \deg \hat{\phi}$;
5. $\hat{\hat{\phi}} = \phi$.

Isogeny graphs

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

$$\begin{tikzcd} E \arrow[r, "\phi"] \arrow[dr, "\phi'"'] & E' \arrow[d, leftrightarrow, "\wr"] \\ & E' \end{tikzcd}$$

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:

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

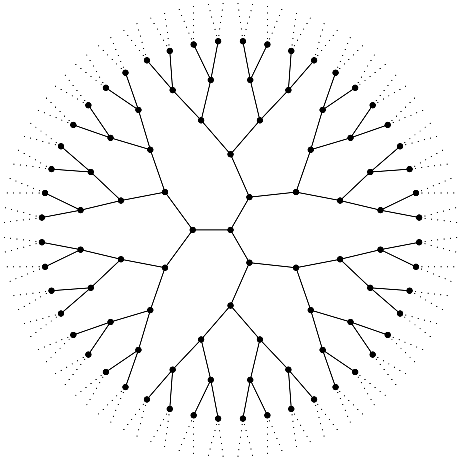
$$\Downarrow$$

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

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

$$\Downarrow$$

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



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

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

Rational isogenies ($\ell \neq p$)

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

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

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

Enter the Frobenius map

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

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

The Frobenius action on $E[\ell]$

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

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

Rational isogenies ($\ell \neq p$)

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

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

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

Enter the Frobenius map

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

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

The Frobenius action on $E[\ell]$

$$aP + bQ$$

$$cP + dQ$$

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

Rational isogenies ($\ell \neq p$)

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

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

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

Enter the Frobenius map

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

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

The Frobenius action on $E[\ell]$

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

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

Rational isogenies ($\ell \neq p$)

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

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

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

Enter the Frobenius map

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

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

The Frobenius action on $E[\ell]$

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

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

Rational isogenies ($\ell \neq p$)

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

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

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

Enter the Frobenius map

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

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

The Frobenius action on $E[\ell]$

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

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

Rational isogenies ($\ell \neq p$)

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

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

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

Enter the Frobenius map

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

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

The Frobenius action on $E[\ell]$

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

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

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

Galois invariant subgroups of $E[\ell]$

=

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

=

rational isogenies of degree ℓ

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

Galois invariant subgroups of $E[\ell]$

=

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

=

rational isogenies of degree ℓ

How many Galois invariant subgroups?

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

Weil pairing

Let $(N, p) = 1$, fix any basis $E[N] = \langle R, S\rangle$. For any points $P, Q \in E[N]$

$$P = aR + bS$$
$$Q = cR + dS$$

the form $\det_N(P, Q) = \det\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = ad - bc \in \mathbb{Z}/N\mathbb{Z}$
is bilinear, non-degenerate, and independent from the choice of basis.

Theorem

Let $E/\mathbb{F}_q$ be a curve, there exists a Galois invariant bilinear map

$$e_N : E[N] \times E[N] \longrightarrow \mu_N \subset \bar{\mathbb{F}}_q,$$

called the Weil pairing of order N, and a primitive N-th root of unity $\zeta \in \bar{\mathbb{F}}_q$ such that

$$e_N(P, Q) = \zeta^{\det_N(P,Q)}.$$

The degree k of the smallest extension such that $\zeta \in \mathbb{F}_{q^k}$ is called the embedding degree of the pairing.

Weil pairing and isogenies

Note

The Weil pairing is Galois invariant $\Leftrightarrow$ $\det(\pi|E[N]) = q$.

Theorem

Let $\phi : E \to E'$ be an isogeny and $\hat{\phi} : E' \to E$ its dual.
Let e_N be the Weil pairing of E and e'_N that of E'. Then, for

$$e_N(P, \hat{\phi}(Q)) = e'_N(\phi(P), Q),$$

for any $P \in E[N]$ and $Q \in E'[N]$.

Corollary

$$e'_N(\phi(P), \phi(Q)) = e_N(P, Q)^{\deg \phi}.$$

From local to global

Theorem (Hasse)

Let E be defined over a finite field $\mathbb{F}_q$. Its Frobenius map π satisfies a quadratic equation

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

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

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 $\mathrm{End}(E)$.

The endomorphism ring

Theorem (Deuring)

Let E be an ordinary elliptic curve defined over a finite field $\mathbb{F}_q$.
Let π be its Frobenius endomorphism, and $D_\pi = t^2 - 4q < 0$ the discriminant of its minimal polynomial.
Then $\mathrm{End}(E)$ is isomorphic to an order $\mathcal{O}$ of the quadratic imaginary field $\mathbb{Q}(\sqrt{D_\pi})$.[a]

[a] An order is a subring that is a $\mathbb{Z}$-module of rank 2 (equiv., a 2-dimensional $\mathbb{R}$-lattice).

In this case, we say that E has complex multiplication (CM) by $\mathcal{O}$.

Theorem (Serre-Tate)

CM elliptic curves 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 over $\mathbb{F}_p$ iff $\#E(\mathbb{F}_p) = \#E'(\mathbb{F}_p)$.

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.

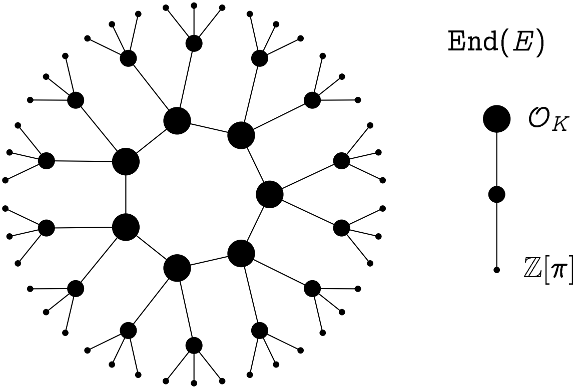
- Any order $\mathcal{O} \subset K$ can be written as $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$ for an integer f, called the conductor of $\mathcal{O}$, denoted by $[\mathcal{O}_K : \mathcal{O}]$.
- If D_K is the discriminant of K, the discriminant of $\mathcal{O}$ is $f^2 D_K$.
- If $\mathcal{O}$,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

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

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.

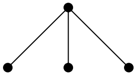


Ordinary isogeny volcano of degree $\ell = 3$.

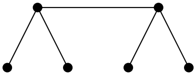
Volcanology (Kohel 1996)

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

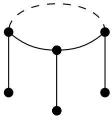
$\mathcal{O}_K$: maximal order of K,
D_K: discriminant of K.



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



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



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

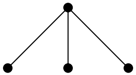
		Horizontal	**Ascending**	**Descending**
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$	$1 + \left(\frac{D_K}{\ell}\right)$		
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O} : \mathbb{Z}[\pi]]$	$1 + \left(\frac{D_K}{\ell}\right)$		$\ell - \left(\frac{D_K}{\ell}\right)$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

Volcanology (Kohel 1996)

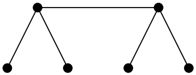
Let E be ordinary,
$\mathtt{End}(E) \subset K$.

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

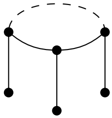
Height $= v_\ell([\mathcal{O}_K : \mathbb{Z}[\pi]])$.



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



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



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

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

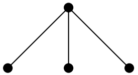
Volcanology (Kohel 1996)

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

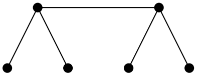
$\mathcal{O}_K$: maximal order of K,
D_K: discriminant of K.

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

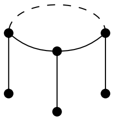
How large is the crater?



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



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



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

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

How large is the crater of a volcano?

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

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

The class group

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

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

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

Complex multiplication

The $\mathfrak{a}$-torsion

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

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

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

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

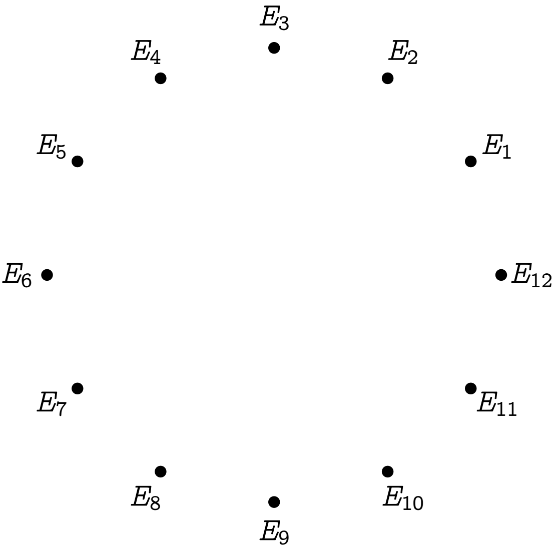
Theorem (Complex multiplication)

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

Corollary

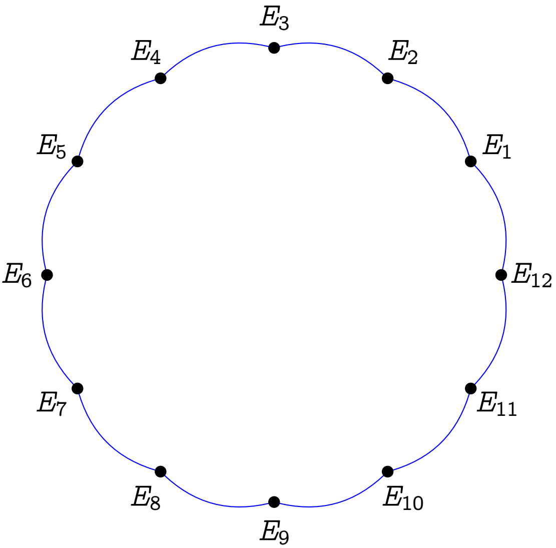
Let $\mathrm{End}(E)$ have discriminant D. Assume that $\left(\frac{D}{\ell}\right) = 1$, then E is on a crater of size N of an ℓ-volcano, and $N | h(\mathrm{End}(E))$

Complex multiplication graphs



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

Complex multiplication graphs

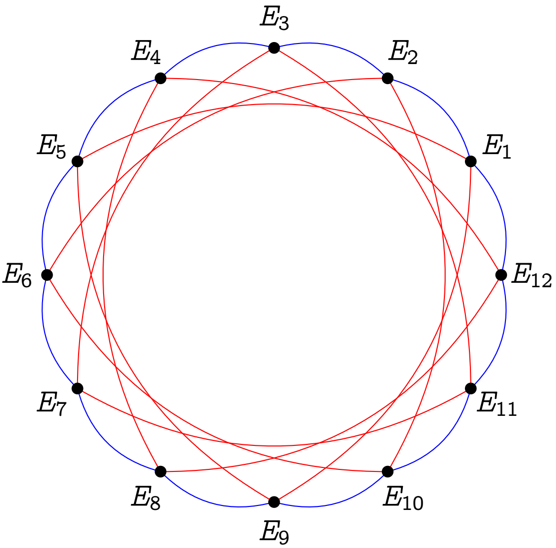


Vertices are elliptic curves with complex multiplication by $\mathcal{O}_K$ (i.e., $\mathtt{End}(E) \simeq \mathcal{O}_K \subset \mathbb{Q}(\sqrt{-D})$).

Edges are horizontal isogenies of bounded prime degree.

—— degree 2

Complex multiplication graphs



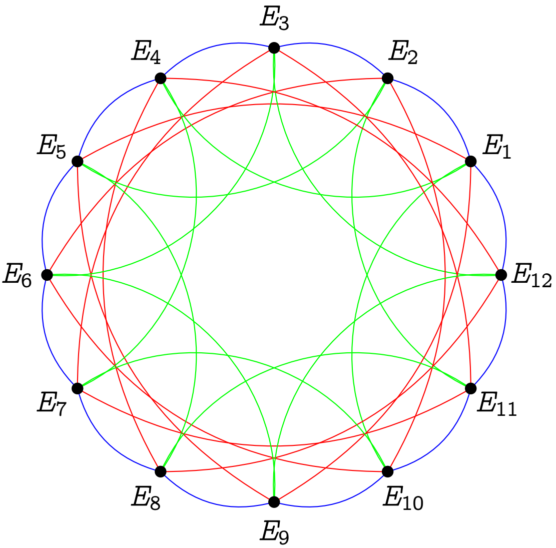
Vertices are elliptic curves with complex multiplication by $\mathcal{O}_K$ (i.e., $\mathrm{End}(E) \simeq \mathcal{O}_K \subset \mathbb{Q}(\sqrt{-D})$).

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., $\mathrm{End}(E) \simeq \mathcal{O}_K \subset \mathbb{Q}(\sqrt{-D})$).

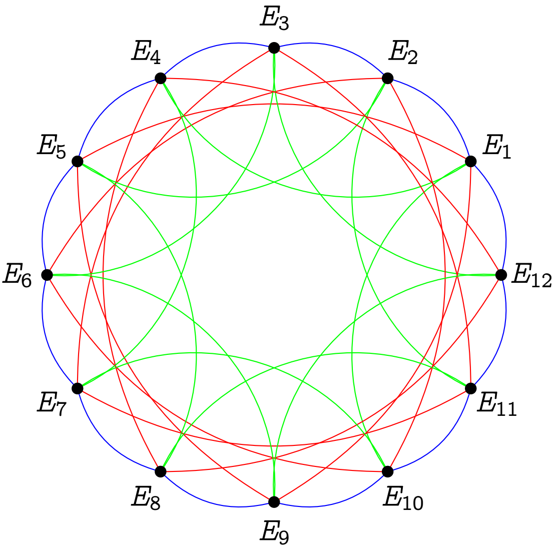
Edges are horizontal isogenies of bounded prime degree.

— degree 2

— degree 3

— degree 5

Complex multiplication graphs



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

Edges are horizontal isogenies of bounded prime degree.

— degree 2

— degree 3

— degree 5

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

Supersingular endomorphisms

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

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

with $t = 0 \mod p$.

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

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

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

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

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

Supersingular complex multiplication

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

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

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

Theorem (Delfs and Galbraith 2016)

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

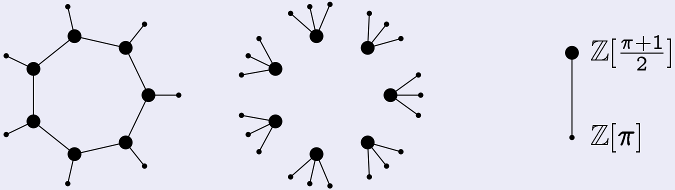
$$\mathbb{Z}[\pi] \subset \mathrm{End}_{\mathbb{F}_p}(E) \subset \mathbb{Q}(\sqrt{-p}).$$

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

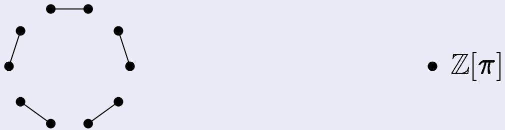
- If $p = 1 \mod 4$, then $\mathbb{Z}[\pi]$ is the maximal order.
- If $p = -1 \mod 4$, then $\mathbb{Z}[\frac{\pi+1}{2}]$ is the maximal order, and $[\mathbb{Z}[\frac{\pi+1}{2}] : \mathbb{Z}[\pi]] = 2$.

Supersingular CM graphs

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



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



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

The full endomorphism ring

Theorem (Deuring)

Let E be a supersingular elliptic curve, then

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

In particular:

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

An example

The curve of j-invariant 1728

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

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

Endomorphisms

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

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

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

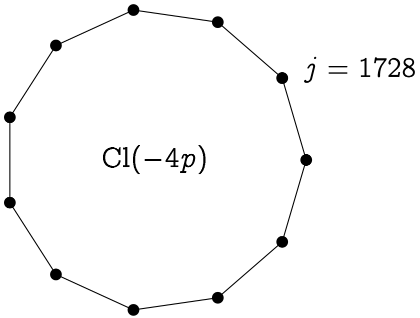
  where $i \in \mathbb{F}_{p^2}$ is a 4-th root of unity. Clearly, $\iota^2 = -1$.

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

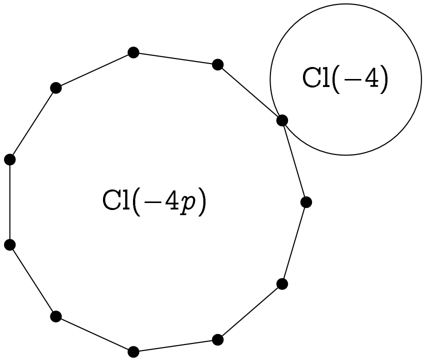
Class group action party

$\bullet\ j = 1728$

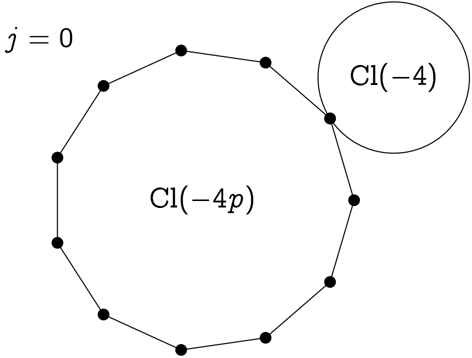
Class group action party



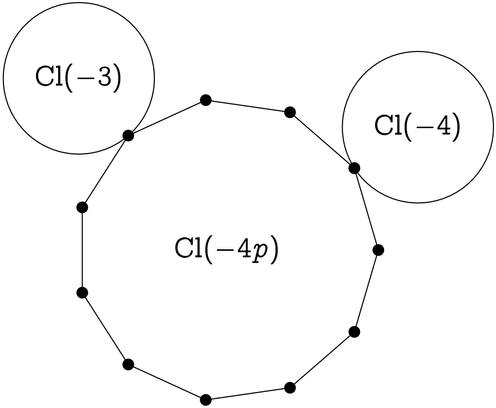
Class group action party



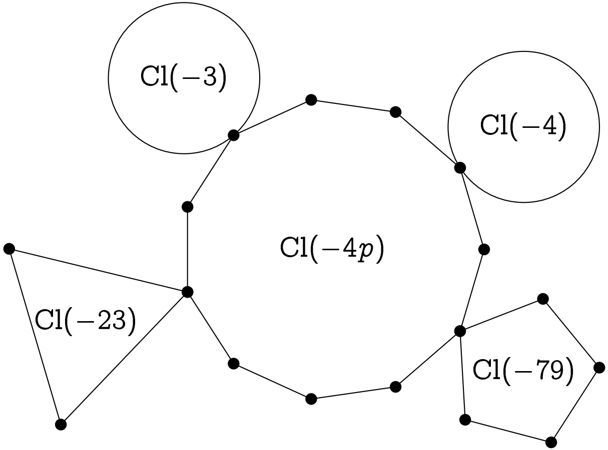
Class group action party



Class group action party



Class group action party



Quaternion algebra?! WTF?[2]

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

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

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

Supersingular graphs

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

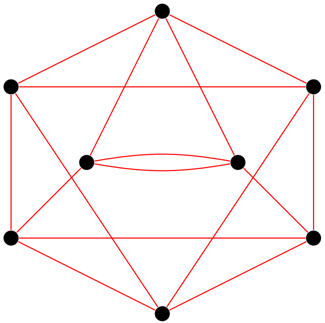


Figure: 3-isogeny graph on $\mathbb{F}_{97^2}$.

Graphs lexicon

Degree: Number of (outgoing/ingoing) edges.

k-regular: All vertices have degree k.

Connected: There is a path between any two vertices.

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

Diamater: The longest distance between two vertices.

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

Expander graphs

Proposition

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

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

Expander families

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

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

Expander graphs from isogenies

Theorem (Pizer 1990, 1998)

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

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

Theorem (Jao, Miller, and Venkatesan 2009)

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

[a] May contain traces of GRH.

Overview

1. Isogeny graphs
   - Elliptic Curves
   - Isogenies
   - Isogeny graphs
   - Endomorphism rings
   - Ordinary graphs
   - Supersingular graphs

2. Cryptography
   - Isogeny walks and Hash functions
   - Pairing verification and Verifiable Delay Functions
   - Key exchange
   - Open Problems

History of isogeny-based cryptography

1996 Couveignes introduces the Hard Homogeneous Spaces (HHS). His work stays unpublished for 10 years.

2006 Rostovtsev & Stolbunov independently rediscover Couveignes ideas, suggest isogeny-based Diffie–Hellman as a quantum-resistant primitive.

2007 Charles, Goren & Lauter propose supersingular 2-isogeny graphs as a foundation for a “provably secure” hash function.

2011-2012 D., Jao & Plût introduce SIDH, an efficient post-quantum key exchange inspired by Couveignes, Rostovtsev, Stolbunov, Charles, Goren, Lauter.

2017 SIDH is submitted to the NIST competition (with the name SIKE, only isogeny-based candidate).

2018 Castryck, Lange, Martindale, Panny & Renes publish an efficient variant of HHS named CSIDH.

2019 New isogeny protocols: Signatures, Verifiable Delay Functions, …

Computing Isogenies

Vélu's formulas

Input: A subgroup $H \subset E$,

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

Complexity: $O(\ell)$ — Vélu 1971, …

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

Computing Isogenies

Vélu's formulas

Input: A subgroup $H \subset E$,

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

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

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

Explicit Isogeny Problem

Input: Curve E, (prime) integer ℓ

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

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

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

Computing Isogenies

Explicit Isogeny Problem (2)

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

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

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

Why?
- Count points of elliptic curves.

Computing Isogenies

Explicit Isogeny Problem (2)

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

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

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

Why?
- Count points of elliptic curves.

Isogeny Walk Problem

Input: Isogenous curves E, E'.

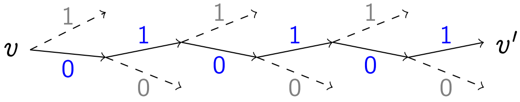
Output: An isogeny $\phi : E \to E'$ of smooth degree.

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

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

Random walks and hash functions (circa 2006)

Any expander graph gives rise to a hash function.



$$H(010101) = v'$$

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

(Denis X. Charles, Kristin E. Lauter, and Goren 2009) hash function (CGL)

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

Hardness of CGL

Finding cycles

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

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

Finding paths $E \to E'$

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

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

Kohel, K. Lauter, Petit, and Tignol 2014 (KLPT)

Input:
- Maximal order $\mathcal{O} \subset B_{p,\infty}$ and associated curve E,
- Left ideal $I \subset \mathcal{O}$.

Output:
- Maximal order $\mathcal{O}' \subset B_{p,\infty}$ s.t. I connects $\mathcal{O}$ to $\mathcal{O}'$,
- Equivalent ideal J (i.e., also connecting $\mathcal{O}$ to $\mathcal{O}'$) of [smooth/power-smooth] norm.
- Isogeny walk associated to J.

- Complexity: $\mathrm{polylog}(p)$,
- Output size: $\mathrm{polylog}(p)$,
- Useful for:
  - "Shortening" isogeny walks (see VDFs),
  - "Reducing" isogeny walks (see Signatures),

  when these start from a curve with known endomorphism ring! (think $j = 0, 1728$ and other curves with small CM discriminant)

Sampling supersingular curves

How to sample:

- A supersingular curve $E/\mathbb{F}_p$?
- A supersingular curve $E/\mathbb{F}_{p^2}$?

Random walks

- Start from a supersingular curve E_0 with small CM discriminant (e.g.: $j = 1728$),
- Do a random walk $E_0 \to E$ until reaching the mixing bound ($O(\log(p))$ steps).

Problem: the random walk reveals $\mathrm{End}(E)$ via the KLPT algorithm.

Open problem

Give an algorithm to sample (uniformly) random supersingular curves in a way that does not reveal the endomorphism ring.

Boneh, Lynn, and Shacham 2004 signatures (BLS)

Setup:
- Elliptic curve $E/\mathbb{F}_p$, s.t $N | \#E(\mathbb{F}_p)$ for a large prime N,
- (Weil) pairing $e_N : E[N] \times E[N] \to \mathbb{F}_{p^k}$ for some small embedding degree k,
- A decomposition $E[N] = X_1 \times X_2$, with $X_1 = \langle P \rangle$.
- A hash function $H : \{0, 1\}^* \to X_2$.

Private key: $s \in \mathbb{Z}/N\mathbb{Z}$.

Public key: sP.

Sign: $m \mapsto sH(m)$.

Verifiy: $e_N(P, sH(m)) = e_N(sP, H(m))$.

$$\begin{tikzcd}
X_1 \times X_2 \arrow[r, "{[s] \times 1}"] \arrow[d, "{1 \times [s]}"'] & X_1 \times X_2 \arrow[d, "e_N"] \\
X_1 \times X_2 \arrow[r, "e_N"'] & \mathbb{F}_{p^k}
\end{tikzcd}$$

US patent 8,250,367[3]

Signatures from isogenies + pairings

- Replace the secret $[s] : E \to E$ with an isogeny $\phi : E \to E'$;
- Define decompositions

$$E[N] = X_1 \times X_2, \qquad E'[N] = Y_1 \times Y_2,$$

  s.t. $\phi(X_1) = Y_1$ and $\phi(X_2) = Y_2$;
- Define a hash function $H : \{0,1\}^* \to Y_2$.

$$\begin{tikzcd}
X_1 \times Y_2 \arrow[r, "\phi \times 1"] \arrow[d, "1 \times \hat{\phi}"'] & Y_1 \times Y_2 \arrow[d, "e'_N"] \\
X_1 \times X_2 \arrow[r, "e_N"'] & \mathbb{F}_{p^k}
\end{tikzcd}$$

[3] Broker, Denis X Charles, and Kristin E Lauter 2012.

US patent 8,250,367[3]

Signatures from isogenies + pairings

- Replace the secret $[s] : E \to E$ with an isogeny $\phi : E \to E'$;
- Define decompositions

$$E[N] = X_1 \times X_2, \qquad E'[N] = Y_1 \times Y_2,$$

  s.t. $\phi(X_1) = Y_1$ and $\phi(X_2) = Y_2$;
- Define a hash function $H : \{0,1\}^* \to Y_2$.

$$\begin{tikzcd}
X_1 \times Y_2 \arrow[r, "\phi \times 1"] \arrow[d, "1 \times \hat{\phi}"'] & Y_1 \times Y_2 \arrow[d, "e'_N"] \\
X_1 \times X_2 \arrow[r, "e_N"'] & \mathbb{F}_{p^k}
\end{tikzcd}$$

Useless, but nice!

[3] Broker, Denis X Charles, and Kristin E Lauter 2012.

Verifiable Delay Functions

A Verifiable Delay Function (VDF) is a function $f : X \to Y$ s.t.:

- Evaluating f at random $x \in X$ is provably "slow" (e.g., $\mathrm{poly}(\#X)$),
- Given $x \in X$ and $y \in Y$,
  verifying that $f(x) = y$ can be done "fast" (e.g., $\mathrm{polylog}(\#X)$).

(non)-Example: time-lock puzzles

- Take a trapdoor group G of (e.g., $G = \mathbb{Z}/N\mathbb{Z}$ with $N = pq$);
- Define $f : G \to G$ as $f(g) = g^{2^T}$:
  - Best algorithm if p, q known: compute $g^{2^T \bmod \varphi(pq)}$ — $\mathrm{polylog}(N)$
  - Best algorithm if p, q unknown: T squarings — $O(T)$

However, in VDFs we want to let anyone verify efficiently.

VDFs from groups of unknown order

Interactive verification protocol (Wesolowski 2019)

1. Verifier chooses a prime ℓ in a set of small primes $\mathcal{P}$;
2. Prover computes $2^T = a\ell + b$, sends g^{2^T}, g^a to verifier;
3. Verifier computes $2^T = a\ell + b$, checks that

$$g^{2^T} = (g^a)^\ell g^b$$

Can be made non-interactive via Fiat-Shamir.

Candidate groups of unknown order:

- RSA groups $\mathbb{Z}/N\mathbb{Z}$, needs trusted third party to generate $N = pq$;
- Quadratic imaginary class groups $\mathrm{Cl}(-D)$ for large random discriminants $-D < 0$.

VDFs from isogenies and pairings[4]

$$\begin{tikzcd} X_1 \times Y_2 \arrow[r, "\phi \times 1"] \arrow[d, "1 \times \hat{\phi}"'] & Y_1 \times Y_2 \arrow[d, "e'_N"] \\ X_1 \times X_2 \arrow[r, "e_N"'] & \mathbb{F}_{p^k} \end{tikzcd}$$

Setup:
- Supersingular curve $E/\mathbb{F}_p$ with (Weil) pairing e_N;
- Public isogeny $\phi : E \to E'$ of degree 2^T;
- The dual isogeny $\hat{\phi} : E' \to E$;
- A generator $\langle P \rangle = X_1 \subset E[N]$, compute $\phi(P)$.

Evaluate: On input a random $Q \in Y_2 \subset E'[N]$, compute $\hat{\phi}(Q)$.

Verify: Check that $e_N(P, \hat{\phi}(Q)) = e'_N(\phi(P), Q)$.

[4] De Feo, Masson, Petit, and Sanso 2019.

Security

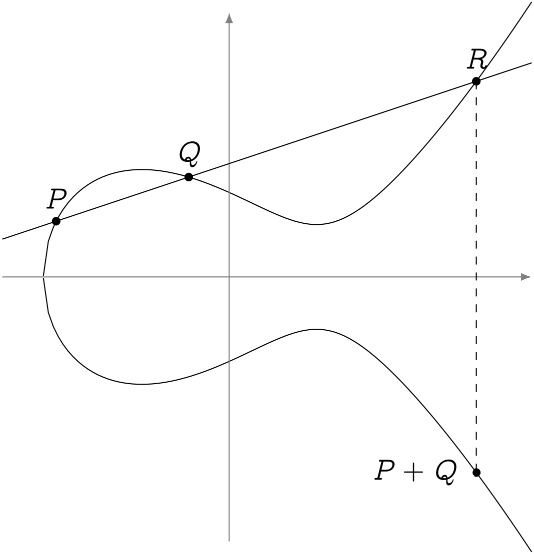
Obvious attack: Pairing inversion must be hard (not post-quantum).

Wanted: No better way to evaluate $\hat{\phi} : E' \to E$ than composing T degree 2 isogenies.

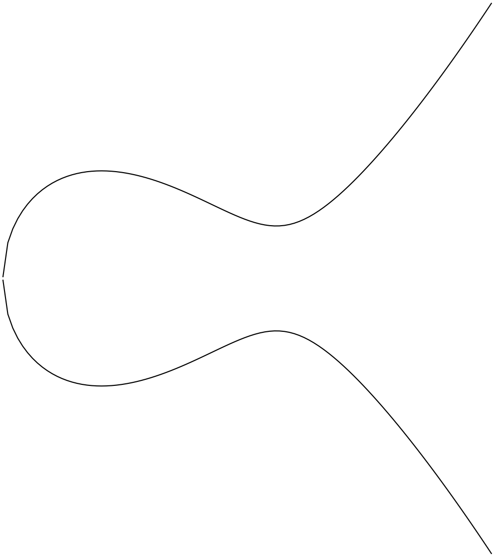
Shortcuts

- If we can find a shorter way from E to E', we can evaluate $\hat{\phi}$ faster.
- Shortcuts are easy to compute:
  - If the isogeny graph is small (excludes ordinary pairing friendly curves);
  - If $\mathrm{End}(E)$ or $\mathrm{End}(E')$ is known (via KLPT).
- Needed: choose $E/\mathbb{F}_p$ in a way that does not reveal $\mathrm{End}(E)$;
- Only known solution: let a trusted third party generate E.

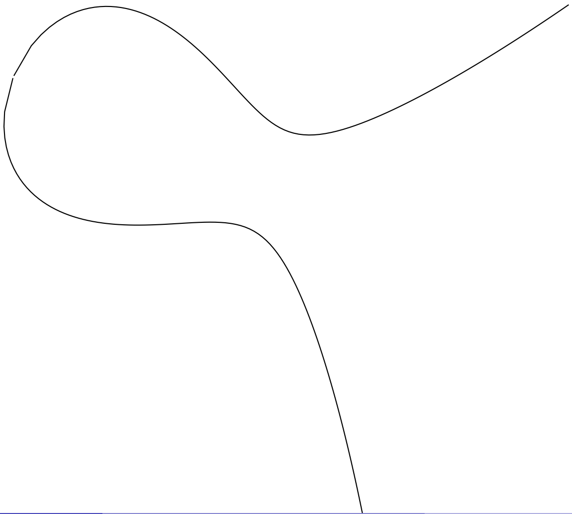
Let's get back to Diffie-Hellman



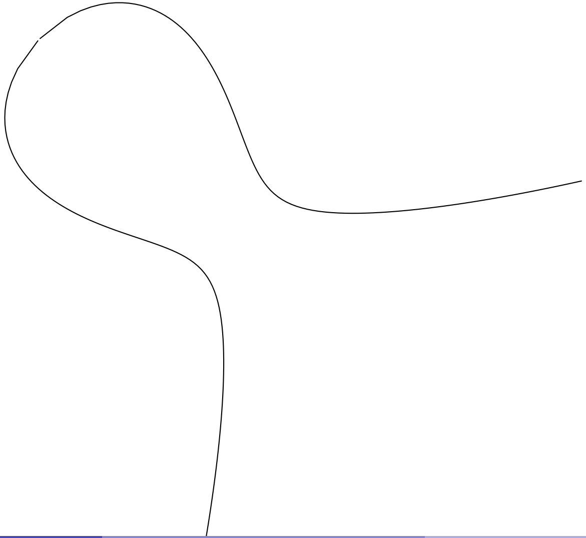
Let’s get back to Diffie-Hellman



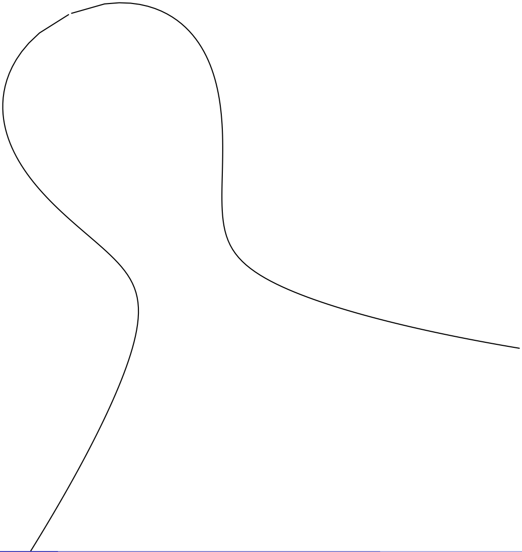
Let's get back to Diffie-Hellman



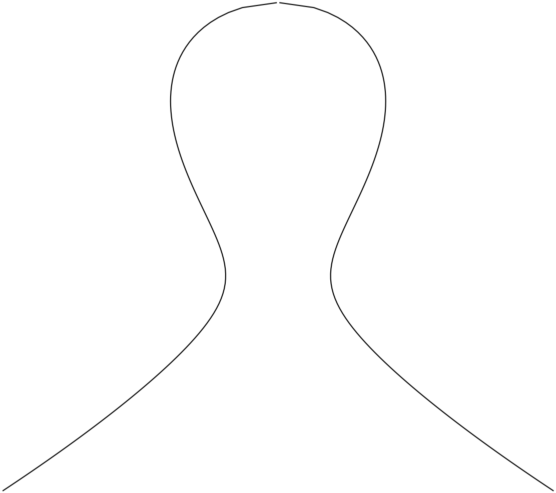
Let's get back to Diffie-Hellman



Let's get back to Diffie-Hellman



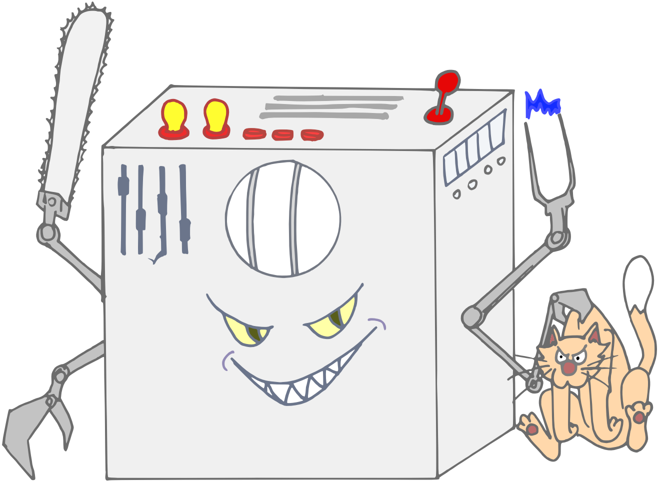
Let's get back to Diffie-Hellman



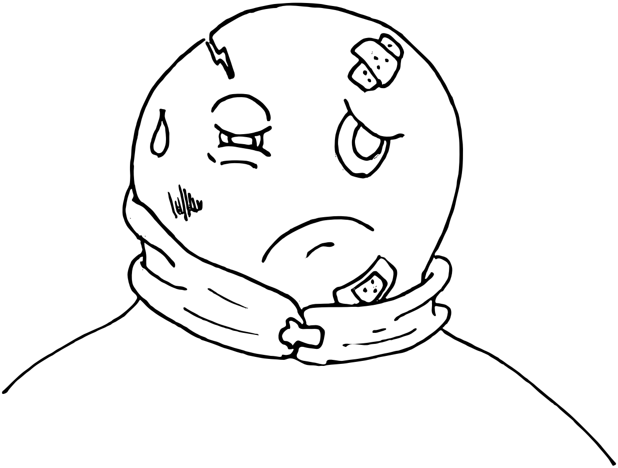
Elliptic curves

I power 70% of WWW traffic!

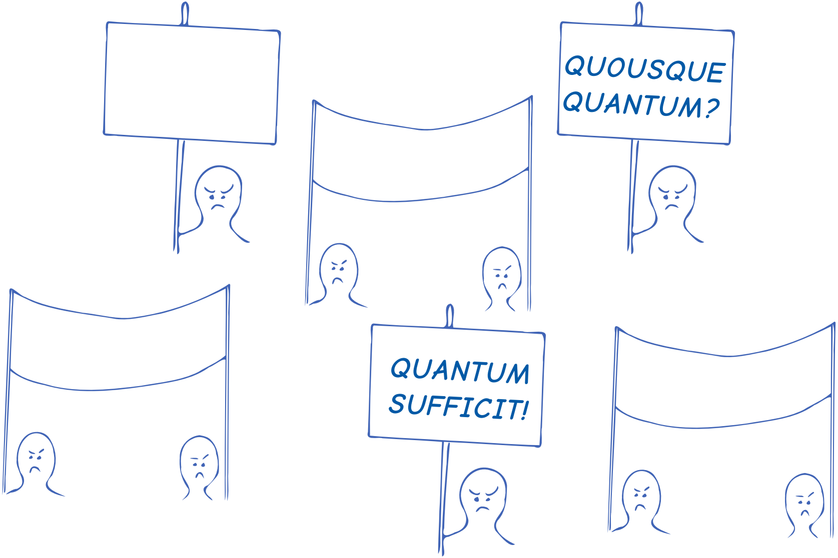
The Q Menace



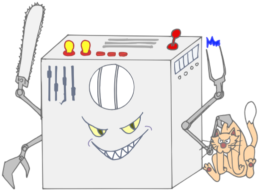
Post-quantum cryptographer?



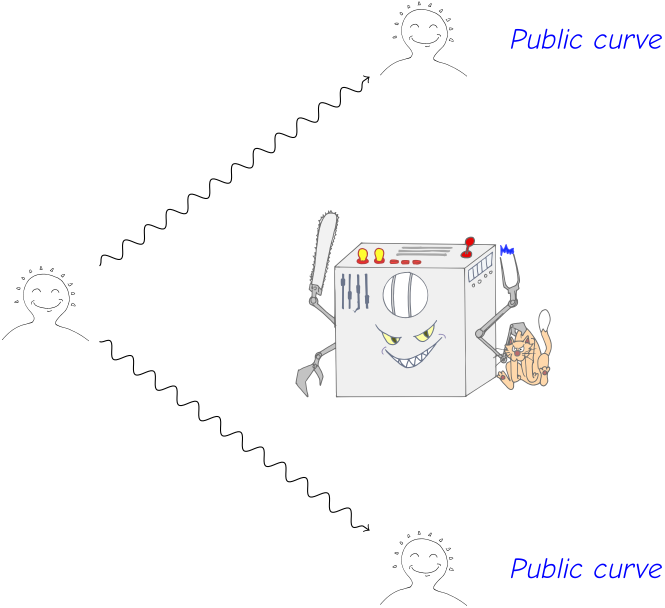
Elliptic curves of the world, UNITE!



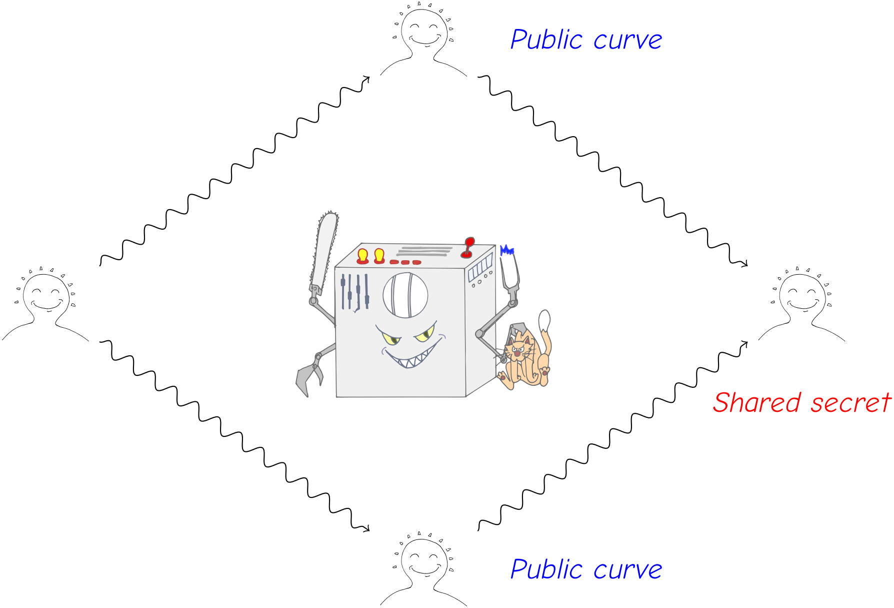
And so, they found a way around the Q...



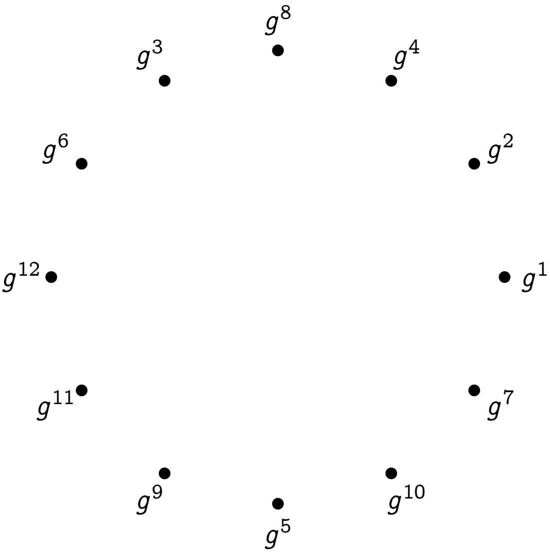
And so, they found a way around the Q...



And so, they found a way around the Q...

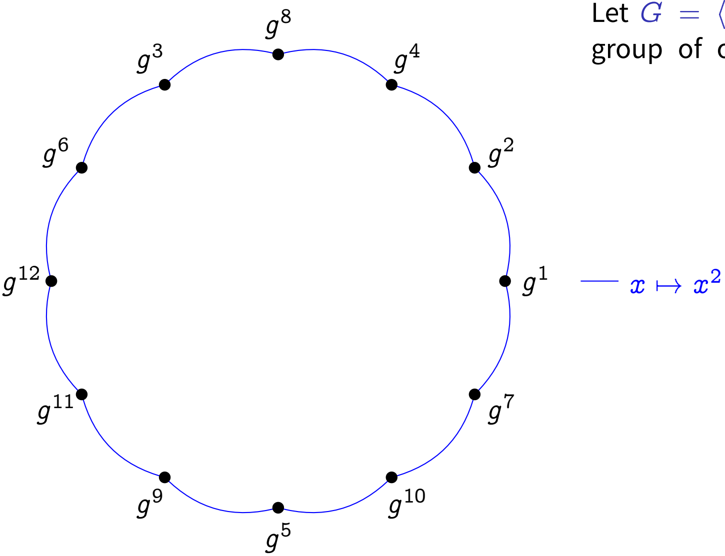


Expander graphs from groups



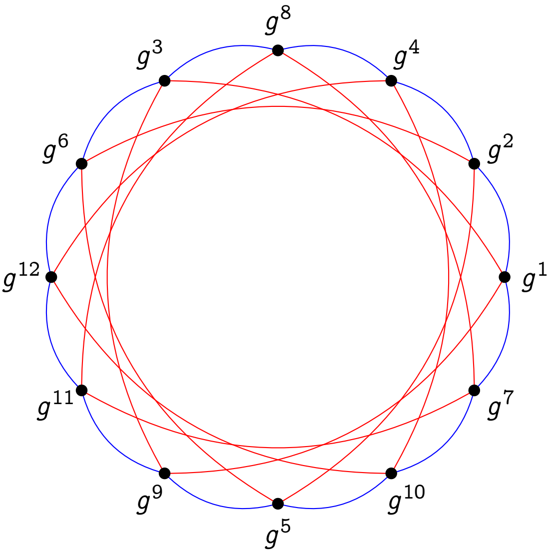
Let $G = \langle g \rangle$ be a cyclic group of order p.

Expander graphs from groups



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

Expander graphs from groups

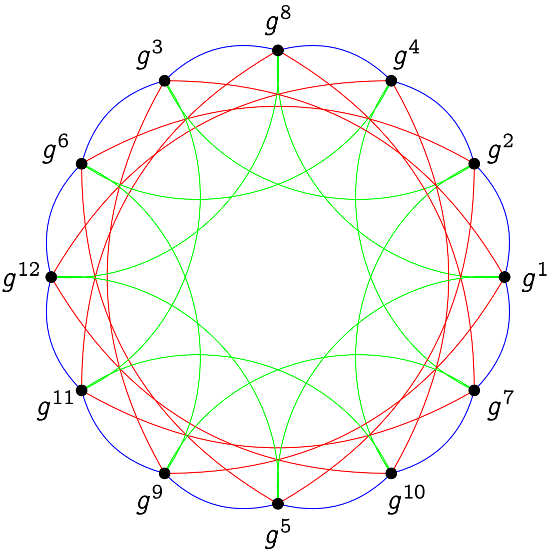


Let $G = \langle g \rangle$ be a cyclic group of order p.

— $x \mapsto x^2$

— $x \mapsto x^3$

Expander graphs from groups



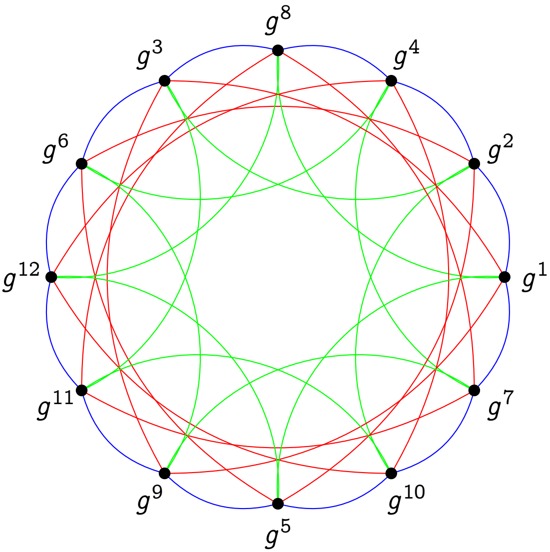
Let $G = \langle g \rangle$ be a cyclic group of order p.

— $x \mapsto x^2$

— $x \mapsto x^3$

— $x \mapsto x^5$

Expander graphs from groups



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

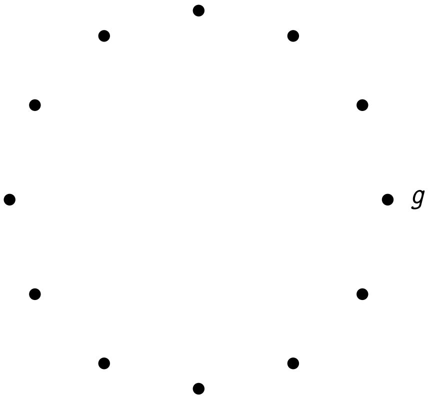
The Schreier graph of $(S, G \setminus \{1\})$ is (usually) an expander.

— $x \mapsto x^2$

— $x \mapsto x^3$

— $x \mapsto x^5$

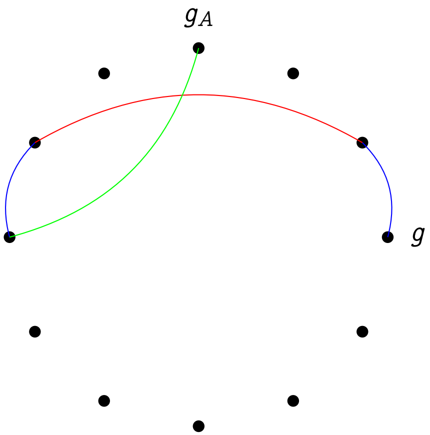
Key exchange from Schreier graphs



Public parameters:

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

Key exchange from Schreier graphs

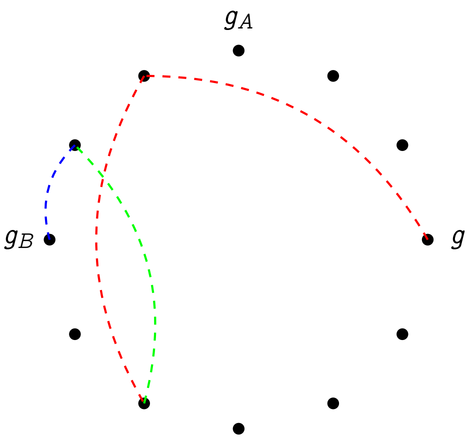


Public parameters:

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

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

Key exchange from Schreier graphs

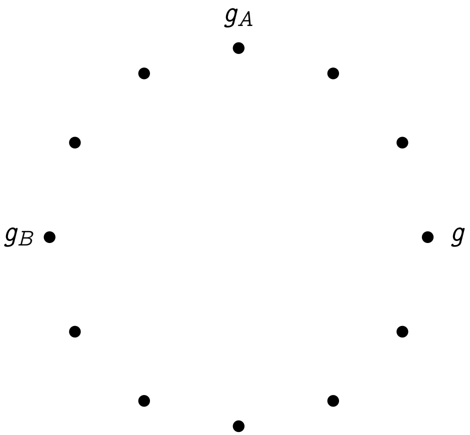


Public parameters:

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

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

Key exchange from Schreier graphs

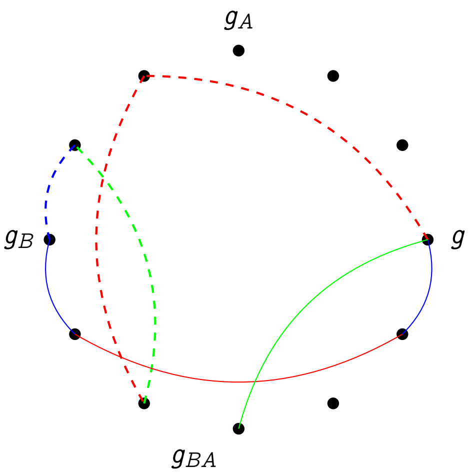


Public parameters:

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

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

Key exchange from Schreier graphs

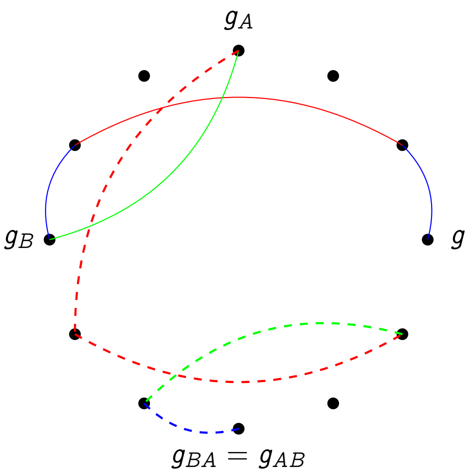


Public parameters:

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

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

Key exchange from Schreier graphs

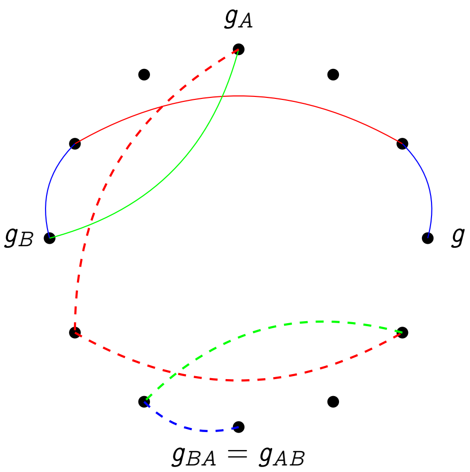


Public parameters:

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

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

Key exchange from Schreier graphs

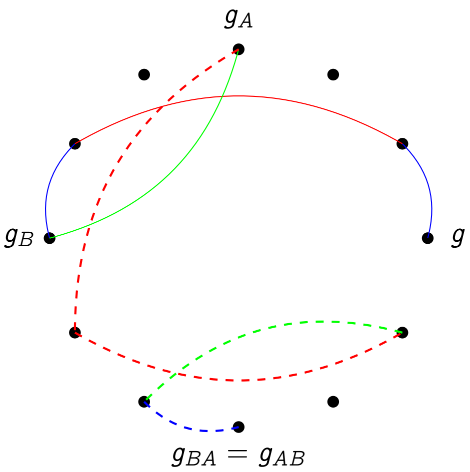


Why does this work?

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

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

Key exchange from Schreier graphs



Why does this work?

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

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

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

Key exchange in graphs of ordinary isogenies[5] (CRS)

Parameters:

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

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

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

[5] Couveignes 2006; Rostovtsev and Stolbunov 2006.

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

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

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

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

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

Parameters size / performance

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

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

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

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

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

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

Vélu to the rescue?

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

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

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

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

Speeding up the class group action

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

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

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

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

Vélu to the rescue?

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

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

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

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

Speeding up the class group action

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

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

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

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

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

Vélu to the rescue?

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

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

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

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

Speeding up the class group action

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

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

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

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

Time to evaluate the isogeny action: Still 5 minutes!

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

Supersingular to the rescue!

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

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

CSIDH *(pron.: Seaside)*

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

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

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

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

Quantum security

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

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

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

[a] Childs, Jao, and Soukharev 2014.

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

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

Key exchange with supersingular curves (2011)

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

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

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

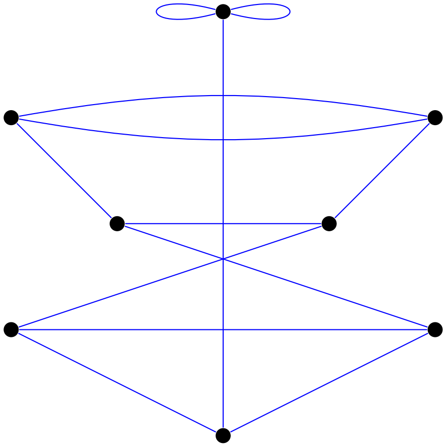


Figure: 2- and 3-isogeny graphs on $\mathbb{F}_{97^2}$.

Key exchange with supersingular curves (2011)

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

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

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

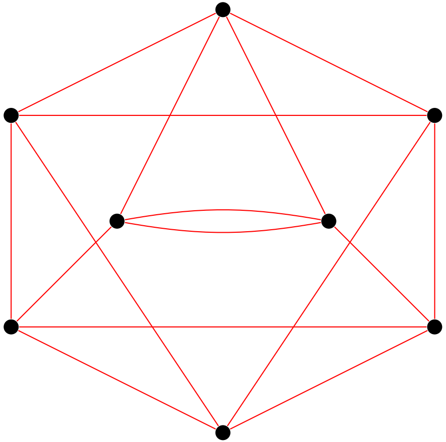


Figure: 2- and 3-isogeny graphs on $\mathbb{F}_{97^2}$.

Key exchange with supersingular curves (2011)

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

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

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

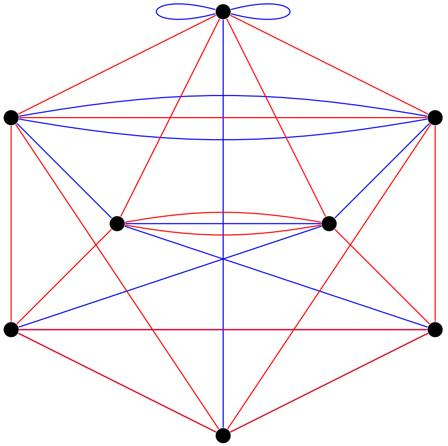


Figure: 2- and 3-isogeny graphs on $\mathbb{F}_{97^2}$.

Key exchange with supersingular curves (2011)

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

Walk of length e_A

$=$

Isogeny of degree $\ell_A^{e_A}$

$=$

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

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

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

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

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

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

Supersingular Isogeny Diffie-Hellman[6]

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:

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

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

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

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

Supersingular Isogeny Diffie-Hellman[6]

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:

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

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

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

---

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

Supersingular Isogeny Diffie-Hellman[6]

Parameters:

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

Secret data:

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

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

$\phi(P_B)$ $\quad \phi(R_B)$ $\quad \psi(R_A)$ $\quad \psi(P_A)$

$\phi(Q_B)$ $\quad \psi(Q_A)$

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

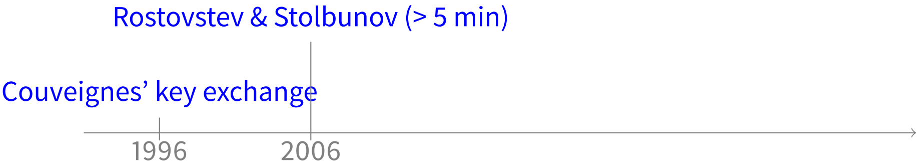
[6] Jao and De Feo 2011; De Feo, Jao, and Plût 2014.

From 10 minutes to 10ms in 20 years

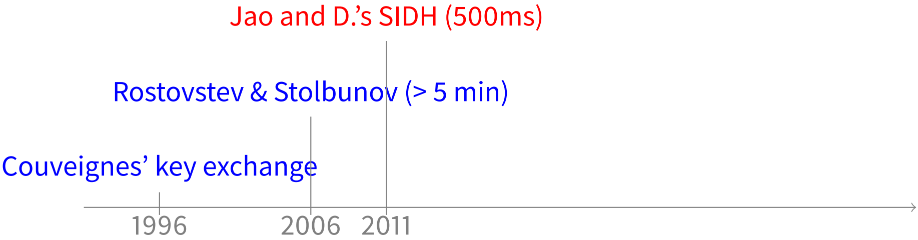
Couveignes' key exchange

1996

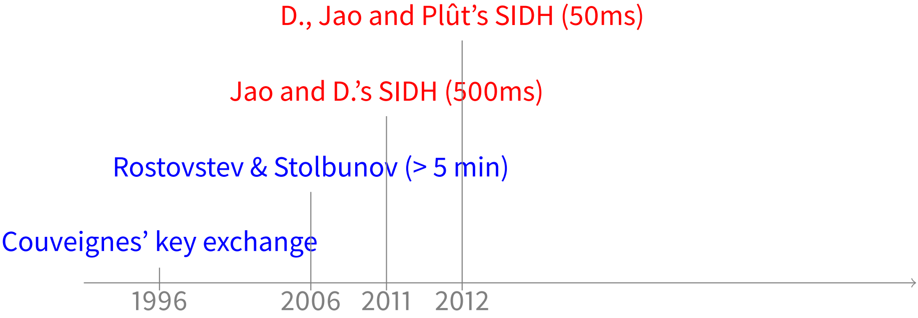
From 10 minutes to 10ms in 20 years



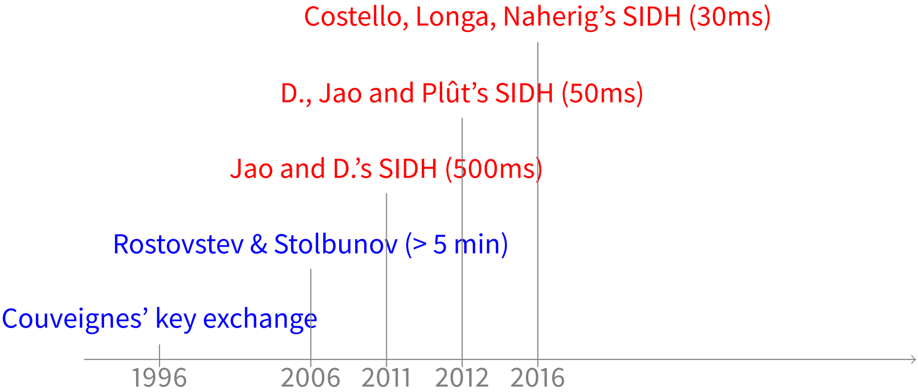
From 10 minutes to 10ms in 20 years



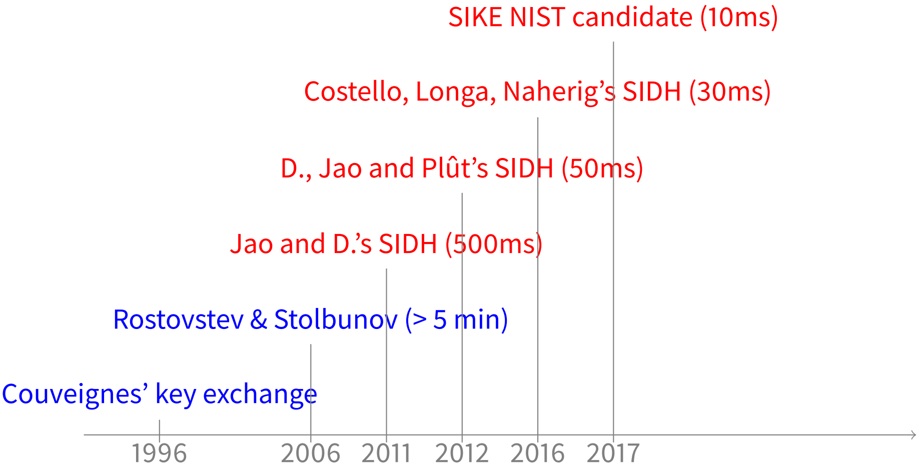
From 10 minutes to 10ms in 20 years



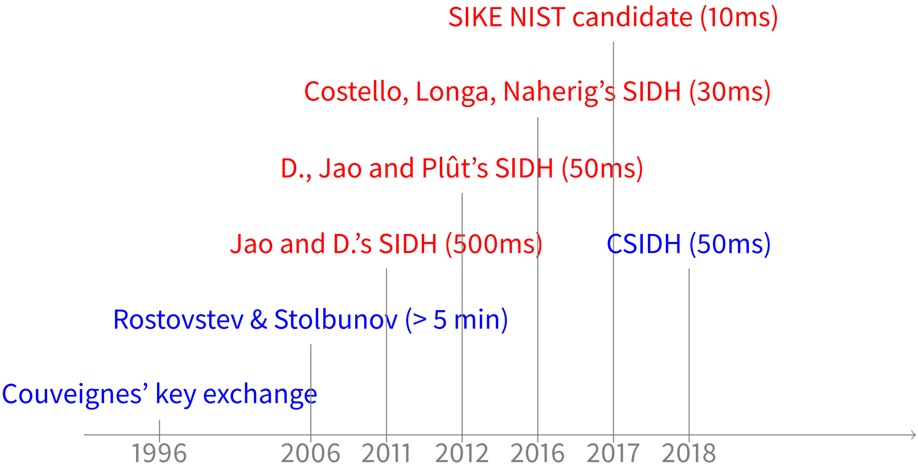
From 10 minutes to 10ms in 20 years



From 10 minutes to 10ms in 20 years



From 10 minutes to 10ms in 20 years

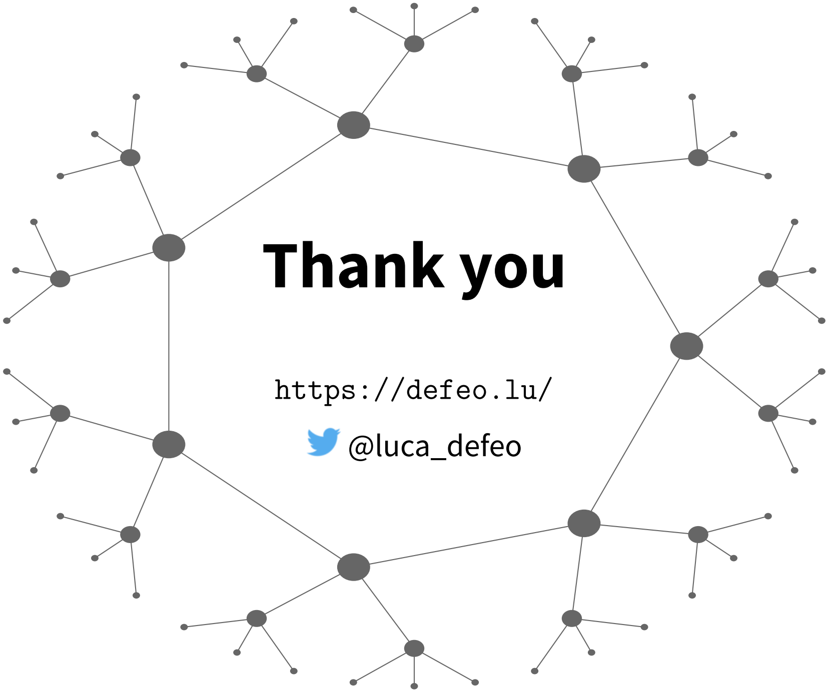


Open problems

From easier to harder:

- Give a convincing constant-time implementation of CSIDH.
- Find new isogeny-based primitives/protocols.
- Precisely asses the quantum security of CRS/CSIDH.
- Find an efficient post-quantum isogeny-based signature scheme.
- Exploit the extra information transmitted in SIDH/SIKE for cryptanalytic purposes.
- Sample supersingular curves without revealing endomorphism rings.
- Compute endomorphism rings of supersingular curves.

Thank you



https://defeo.lu/

@luca_defeo

References I

Surveys

- Steven D. Galbraith and Frederik Vercauteren (Aug. 2018). "Computational problems in supersingular elliptic curve isogenies." In: Quantum Information Processing 17.10, p. 265.
- Luca De Feo (2017). Mathematics of Isogeny Based Cryptography. arXiv: 1711.04062. URL: http://arxiv.org/abs/1711.04062.
- Luca De Feo (2018). "Exploring Isogeny Graphs." Habilitation thesis. Université de Versailles. URL: https://defeo.lu/hdr.

References II

Elliptic curves and isogenies

- Joseph H. Silverman (1986). The Arithmetic of Elliptic Curves. Graduate Texts in Mathematics 106. Springer.
- James S. Milne (1996). Elliptic curves. URL: https://www.jmilne.org/math/Books/ectext6.pdf.
- Ian F. Blake, Gadiel Seroussi, and Niegel P. Smart (1999). Elliptic curves in cryptography. New York, NY, USA: Cambridge University Press.

References III

Isogeny graphs

- David Kohel (1996). "Endomorphism rings of elliptic curves over finite fields." PhD thesis. University of California at Berkley.
- Christina Delfs and Steven D. Galbraith (2016). "Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$." In: Des. Codes Cryptography 78.2, pp. 425–440.
- Anamaria Costache, Brooke Feigon, Kristin Lauter, Maike Massierer, and Anna Puskas (2018). Ramanujan graphs in cryptography. Cryptology ePrint Archive, Report 2018/593. URL: https://eprint.iacr.org/2018/593.

References IV

Complex multiplication

- Joseph H. Silverman (Jan. 1994). Advanced Topics in the Arithmetic of Elliptic Curves (Graduate Texts in Mathematics). Springer.
- David A Cox (2011). Primes of the form x2+ ny2: Fermat, class field theory, and complex multiplication. Vol. 34. John Wiley & Sons.

Quaternion algebras

- Marie-France Vignéras (1980). Arithmetic of quaternion algebras. Vol. 800.
- John Voight (2018). Quaternion Algebras. URL: https://math.dartmouth.edu/~jvoight/quat-book.pdf.

Article citations I

Delfs, Christina and Steven D. Galbraith (2016).
"Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$."
In: Des. Codes Cryptography 78.2,
Pp. 425–440.

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.

Article citations II

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.
URL: http://dx.doi.org/10.1016/j.jnt.2008.11.006.

Vélu, Jean (1971).
"Isogénies entre courbes elliptiques."
In: Comptes Rendus de l'Académie des Sciences de Paris 273,
Pp. 238–241.

Elkies, Noam D. (1992).
"Explicit isogenies."
manuscript, Boston MA.

Article citations III

Couveignes, Jean-Marc (1996).
"Computing l-Isogenies Using the p-Torsion."
In: ANTS-II: Proceedings of the Second International Symposium on Algorithmic Number Theory.
London, UK: Springer-Verlag,
Pp. 59–65.

Lercier, Reynald and Thomas Sirvent (2008).
"On Elkies subgroups of ℓ-torsion points in elliptic curves defined over a finite field."
In: Journal de théorie des nombres de Bordeaux 20.3,
Pp. 783–797.
URL: http://perso.univ-rennes1.fr/reynald.lercier/file/LS08.pdf.

Article citations IV

De Feo, Luca (May 2011).
"Fast algorithms for computing isogenies between ordinary elliptic curves in small characteristic."
In: Journal of Number Theory 131.5,
Pp. 873–893.

De Feo, Luca, Cyril Hugounenq, Jérôme Plût, and Éric Schost (2016).
"Explicit isogenies in quadratic time in any characteristic."
In: LMS Journal of Computation and Mathematics 19.A,
Pp. 267–282.

Article citations V

Lairez, Pierre and Tristan Vaccon (2016).
"On p-Adic Differential Equations with Separation of Variables."
In: Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation.
ISSAC '16.
Waterloo, ON, Canada: ACM,
Pp. 319–323.

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.

Article citations VI

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.
URL: http://dx.doi.org/10.1007/s00145-007-9002-x.

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.

Article citations VII

Eisenträger, Kirsten, Sean Hallgren, Kristin Lauter, Travis Morrison, and Christophe Petit (2018).
"Supersingular Isogeny Graphs and Endomorphism Rings: Reductions and Solutions."
In: Advances in Cryptology – EUROCRYPT 2018.
Ed. by Jesper Buus Nielsen and Vincent Rijmen.
Springer International Publishing,
Pp. 329–368.

Cerviño, Juan M. (Apr. 2004).
On the Correspondence between Supersingular Elliptic Curves and maximal quaternionic Orders.
arXiv: math/0404538.
URL: http://arxiv.org/abs/math/0404538.

Article citations VIII

Boneh, Dan, Ben Lynn, and Hovav Shacham (Sept. 2004).
"Short Signatures from the Weil Pairing."
In: Journal of Cryptology 17.4,
Pp. 297–319.

Broker, Reinier M, Denis X Charles, and Kristin E Lauter (Aug. 2012).
Cryptographic applications of efficiently evaluating large degree isogenies.
US Patent 8,250,367.

Wesolowski, Benjamin (2019).
Efficient verifiable delay functions.
to appear at EuroCrypt 2019.
URL: https://eprint.iacr.org/2018/623.

Article citations IX

De Feo, Luca, Simon Masson, Christophe Petit, and Antonio Sanso (2019).
Verifiable Delay Functions from Supersingular Isogenies and Pairings.
Cryptology ePrint Archive, Report 2019/166.
URL: https://eprint.iacr.org/2019/166.

Couveignes, Jean-Marc (2006).
Hard Homogeneous Spaces.
URL: http://eprint.iacr.org/2006/291/.

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

Article citations X

De Feo, Luca, Jean Kieffer, and Benjamin Smith (2018).
"Towards Practical Key Exchange from Ordinary Isogeny Graphs."
In: Advances in Cryptology – ASIACRYPT 2018.
Ed. by Thomas Peyrin and Steven D. Galbraith.
Springer International Publishing,
Pp. 365–394.

Castryck, Wouter, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes (2018).
"CSIDH: An Efficient Post-Quantum Commutative Group Action."
In: Advances in Cryptology – ASIACRYPT 2018.
Ed. by Thomas Peyrin and Steven D. Galbraith.
Springer International Publishing,
Pp. 395–427.

Article citations XI

Childs, Andrew, David Jao, and Vladimir Soukharev (2014).
"Constructing elliptic curve isogenies in quantum subexponential time."
In: Journal of Mathematical Cryptology 8.1,
Pp. 1–29.

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`.

Article citations XII

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

Article citations XIII

Kuperberg, Greg (2013).
"Another Subexponential-time Quantum Algorithm for the Dihedral Hidden Subgroup Problem."
In: 8th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2013).
Ed. by Simone Severini and Fernando Brandao.
Vol. 22.
Leibniz International Proceedings in Informatics (LIPIcs).
Dagstuhl, Germany: Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik,
Pp. 20–34.
URL: http://drops.dagstuhl.de/opus/volltexte/2013/4321.

Bonnetain, Xavier and María Naya-Plasencia (2018).
Hidden Shift Quantum Cryptanalysis and Implications.
Cryptology ePrint Archive, Report 2018/432.
https://eprint.iacr.org/2018/432.

Article citations XIV

Bonnetain, Xavier and André Schrottenloher (2018).
Quantum Security Analysis of CSIDH and Ordinary Isogeny-based Schemes.
Cryptology ePrint Archive, Report 2018/537.
https://eprint.iacr.org/2018/537.

Biasse, Jean-François, Michael J Jacobson Jr, and Annamaria Iezzi (2018).
"A note on the security of CSIDH."
In: arXiv preprint arXiv:1806.03656.
URL: https://arxiv.org/abs/1806.03656.

Jao, David, Jason LeGrow, Christopher Leonardi, and Luiz Ruiz-Lopez (2018).
"A polynomial quantum space attack on CRS and CSIDH."
In: MathCrypt 2018.
To appear.

Article citations XV

Bernstein, Daniel J., Tanja Lange, Chloe Martindale, and Lorenz Panny (2018).
Quantum circuits for the CSIDH: optimizing quantum evaluation of isogenies.
To appear at EuroCrypt 2019.
URL: https://eprint.iacr.org/2018/1059.

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.

Article citations XVI

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.

Galbraith, Steven D. and Frederik Vercauteren (Aug. 2018).
"Computational problems in supersingular elliptic curve isogenies."
In: Quantum Information Processing 17.10,
P. 265.

De Feo, Luca (2017).
Mathematics of Isogeny Based Cryptography.
arXiv: 1711.04062.
URL: http://arxiv.org/abs/1711.04062.

Article citations XVII

Milne, James S. (1996).
Elliptic curves.
URL: https://www.jmilne.org/math/Books/ectext6.pdf.

Costache, Anamaria, Brooke Feigon, Kristin Lauter, Maike Massierer, and Anna Puskas (2018).
Ramanujan graphs in cryptography.
Cryptology ePrint Archive, Report 2018/593.
URL: https://eprint.iacr.org/2018/593.