Isogeny Based Cryptography: an Introduction

Luca De Feo

IBM Research Zürich

November 28, 2019
NTNU, Trondheim

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

Why isogenies?

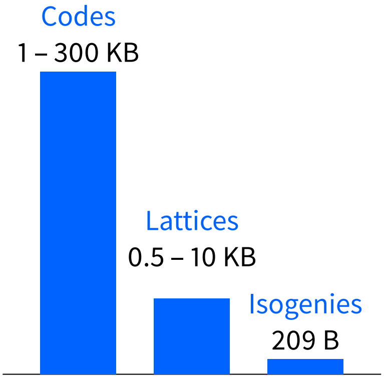
Six families still in NIST post-quantum competition:

Lattices	9 encryption	3 signature
Codes	7 encryption	
Multivariate		4 signature
Isogenies	1 encryption	
Hash-based		1 signature
MPC		1 signature

Why isogenies?

Six families still in NIST post-quantum competition:

Lattices	9 encryption	3 signature
Codes	7 encryption	
Multivariate		4 signature
Isogenies	1 encryption	
Hash-based		1 signature
MPC		1 signature

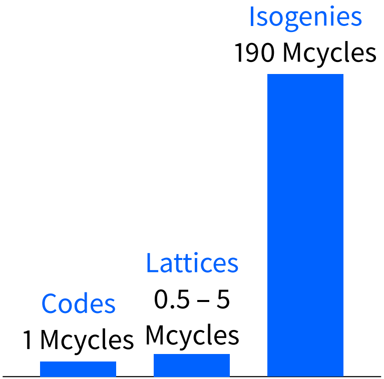


Public key size
NIST-1 level (AES128)
(not to scale)

Why isogenies?

Six families still in NIST post-quantum competition:

Lattices	9 encryption	3 signature
Codes	7 encryption	
Multivariate		4 signature
Isogenies	1 encryption	
Hash-based		1 signature
MPC		1 signature



Encryption performance

NIST-1 level (AES128)

(not to scale)

"We found that CECPQ2 ([NTRU] the ostrich) outperformed CECPQ2b ([SIKE] the turkey), for the majority of connections in the experiment, indicating that ***fast algorithms with large keys may be more suitable for TLS than slow algorithms with small keys****. However,* ***we observed the opposite****—that CECPQ2b outperformed CECPQ2—**for the slowest connections on some devices**, including Windows computers and Android mobile devices. One possible explanation for this is packet fragmentation and packet loss."*

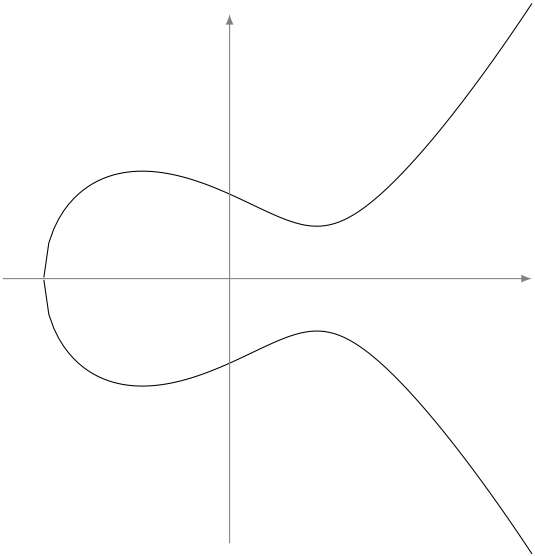
— K. Kwiatkowski, L. Valenta (Cloudflare)
The TLS Post-Quantum Experiment
https://blog.cloudflare.com/the-tls-post-quantum-experiment/

Weierstrass equations

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

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

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



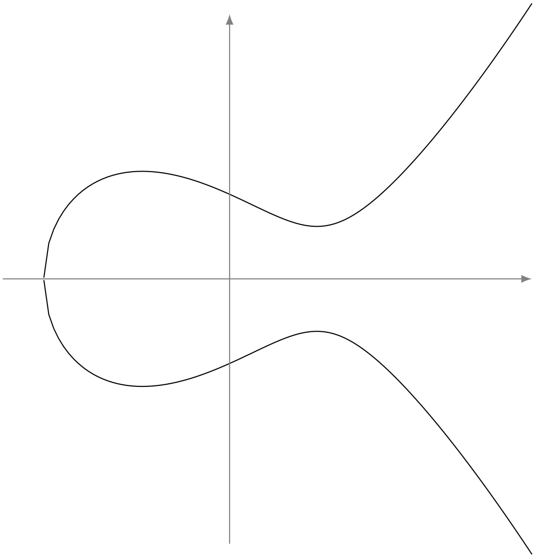
Weierstrass equations

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

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

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

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



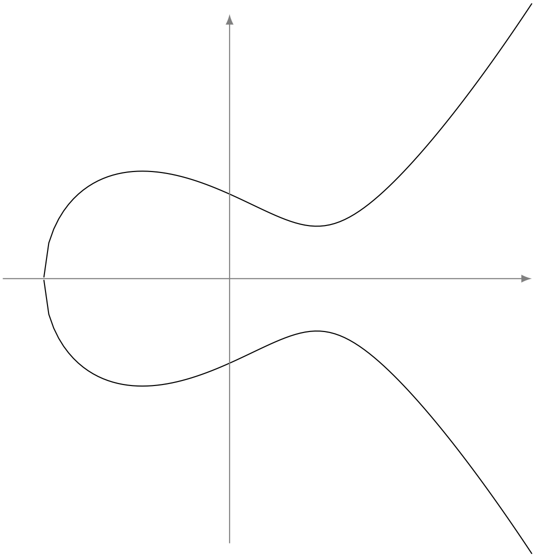
Weierstrass equations

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

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

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

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

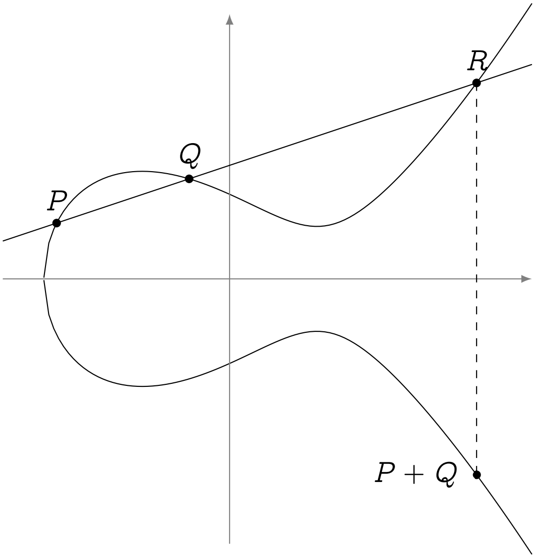


The group law

Bezout's theorem

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

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



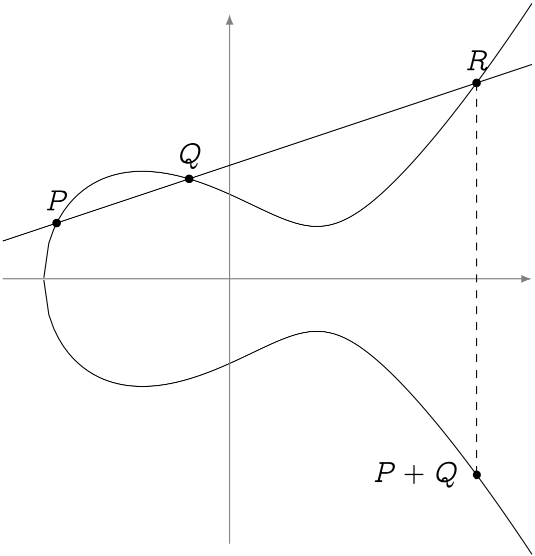
The group law

Bezout's theorem

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

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

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



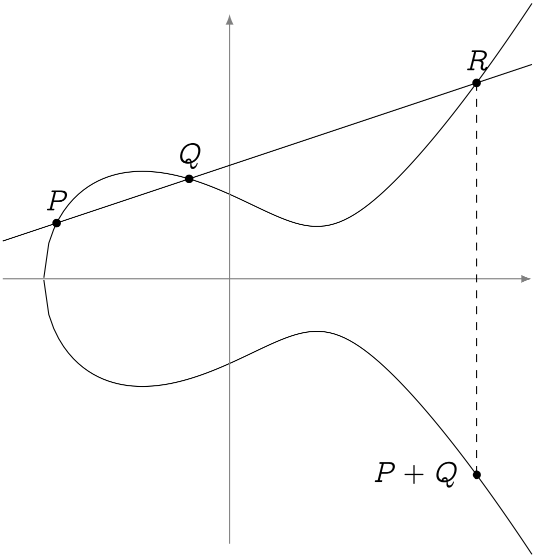
The group law

Bezout's theorem

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

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

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



Maps: isomorphisms

Isomorphisms

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

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

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

j-Invariant

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

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

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

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

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

Maps: what's 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.

Maps: what's ~~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.

Maps: what's ~~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.

Maps: what's ~~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.

Maps: what's ~~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.

Maps: what's ~~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 $E[m] \simeq (\mathbb{Z}/m\mathbb{Z})^2$~~ any finite subgroup $H \subset E$),
- surjective (in the algebraic closure),
- given by rational maps of degree $\cancel{m^2}\ \#H$.

Maps: what's ~~scalar multiplication~~ an isogeny?

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

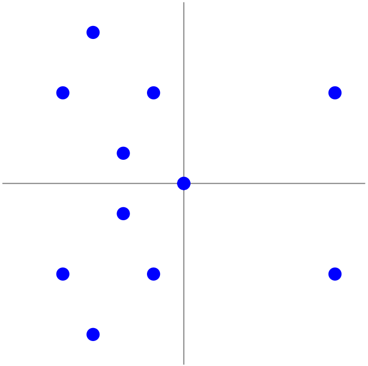
- A map $E \to \cancel{E}\, E'$,
- a group morphism,
- with finite kernel
  (~~the torsion group $E[n] \simeq (\mathbb{Z}/n\mathbb{Z})^2$~~ any finite subgroup $H \subset E$),
- surjective (in the algebraic closure),
- given by rational maps of degree $\cancel{n^2}\ \#H$.

(Separable) isogenies $\Leftrightarrow$ finite subgroups:

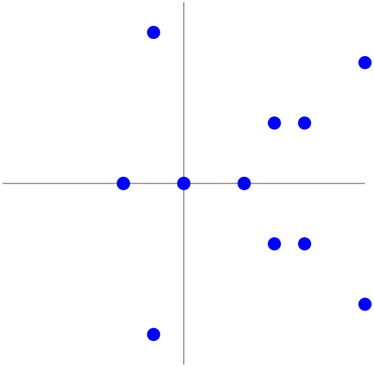
$$0 \to H \to E \xrightarrow{\phi} E' \to 0$$

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

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

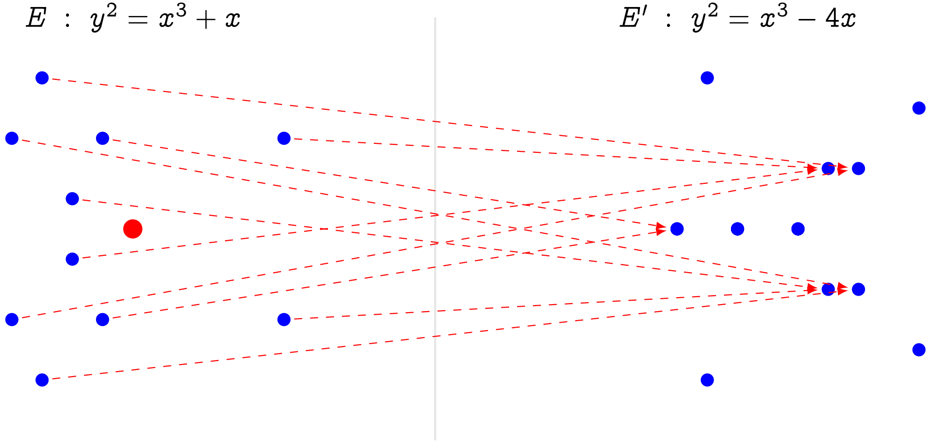


$$E' : y^2 = x^3 - 4x$$



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

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 $\mathbb{F}_q^*$.

Maps: isogenies

Theorem

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

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

If they hold ϕ is called an isogeny.

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

Example: Multiplication-by-m

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

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

Isogeny lexicon

Degree

- $\approx$ degree of the rational fractions defining the isogeny;
- Rough measure of the information needed to encode it.

Separable, inseparable, cyclic

An isogeny ϕ is separable iff $\deg\phi = \#\ker\phi$.

- Given $H \subset E$ finite, write $\phi : E \to E/H$ for the unique separable isogeny s.t. $\ker\phi = H$.
- ϕ inseparable $\Rightarrow$ p divides $\deg\phi$.
- Cyclic isogeny $\equiv$ separable isogeny with cyclic kernel.
  - Non-example: the multiplication map $[m] : E \to E$.

The dual isogeny

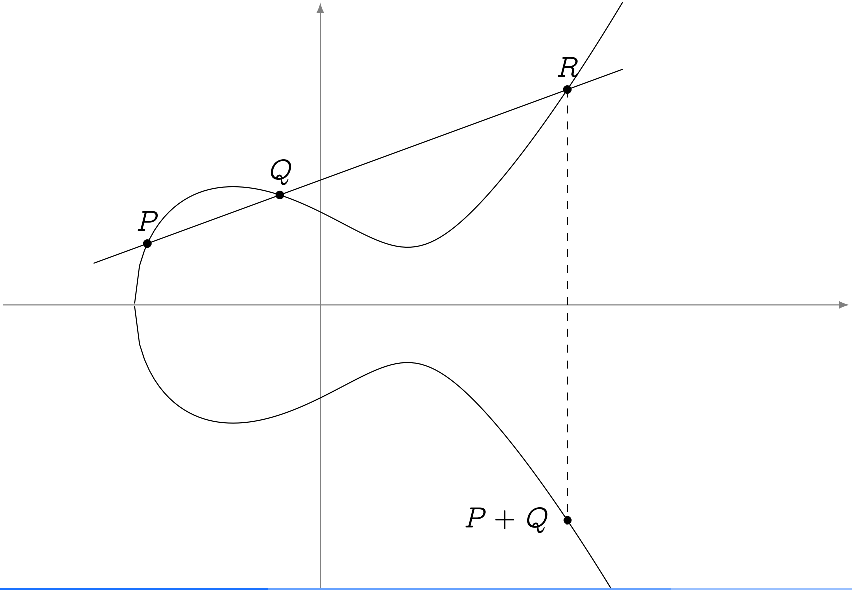
Let $\phi : E \to E'$ be an isogeny of degree m. There is a unique isogeny $\hat{\phi} : E' \to E$ such that

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

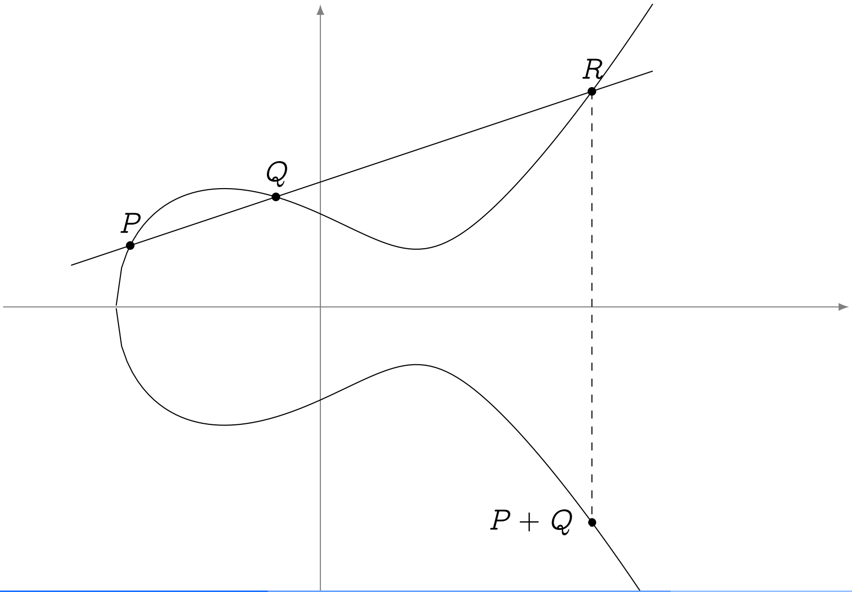
$\hat{\phi}$ is called the dual isogeny of ϕ; it has the following properties:

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. $\hat{\hat{\phi}} = \phi$.

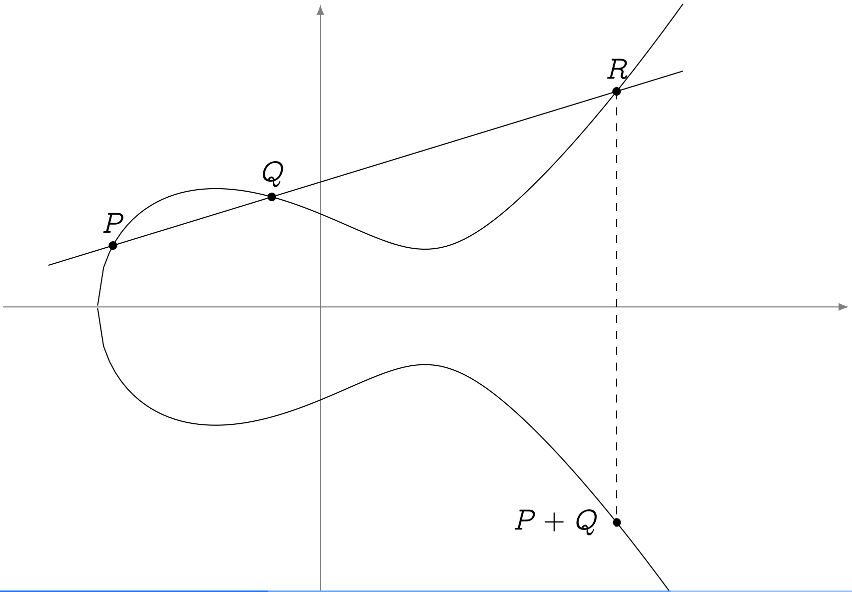
Up to isomorphism



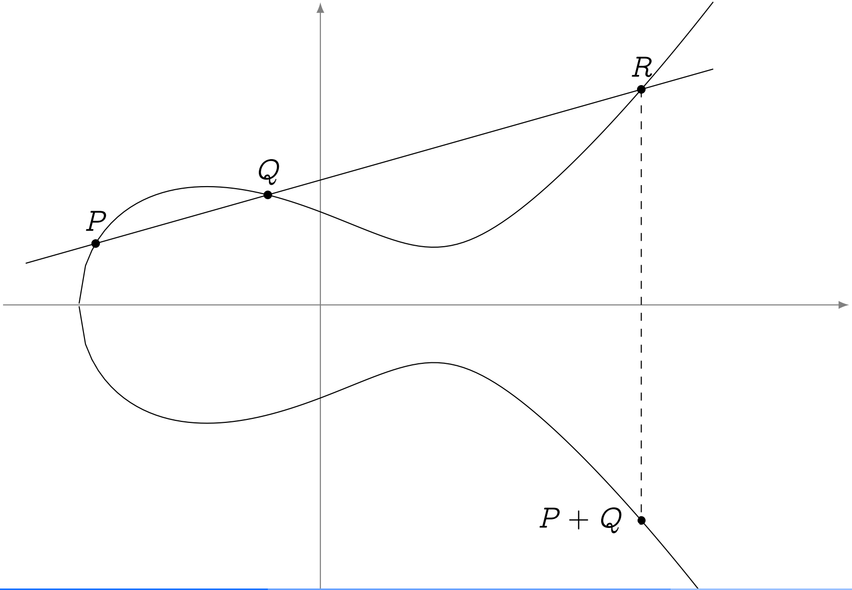
Up to isomorphism



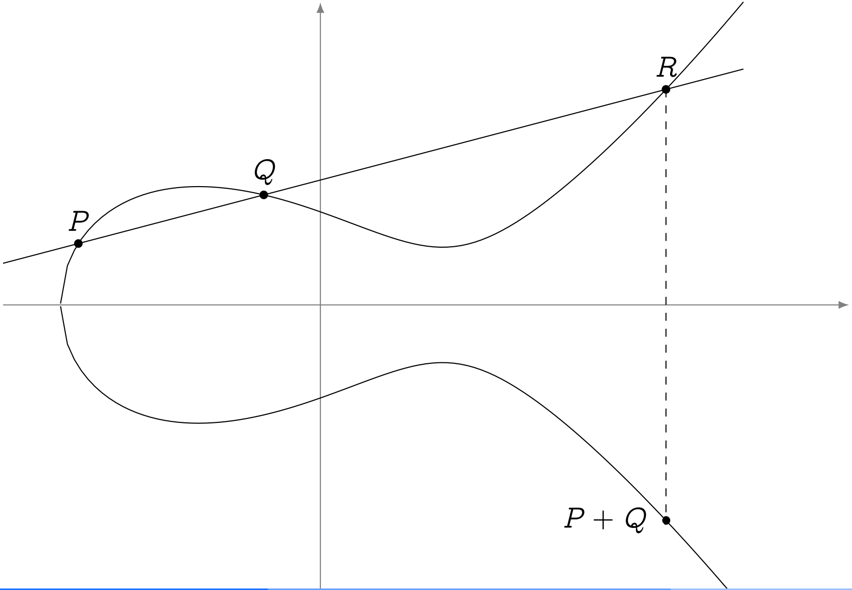
Up to isomorphism



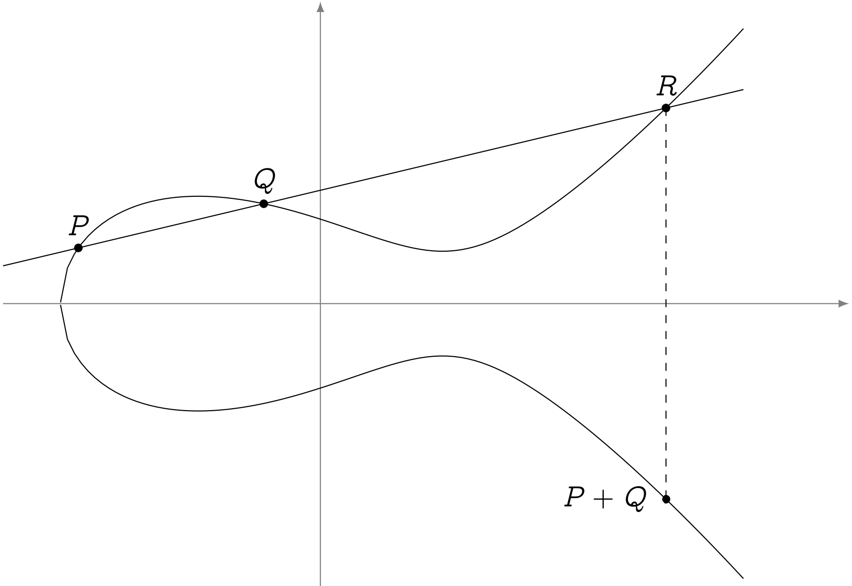
Up to isomorphism



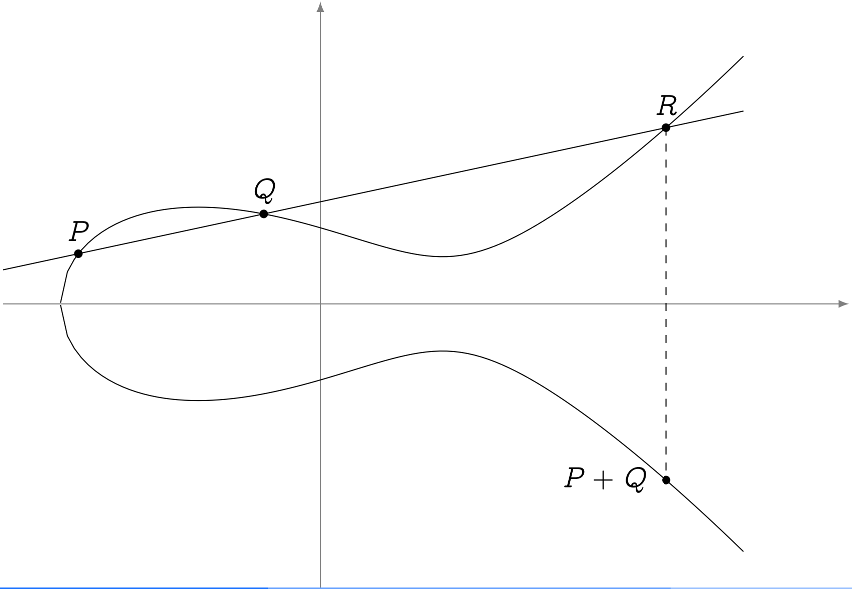
Up to isomorphism



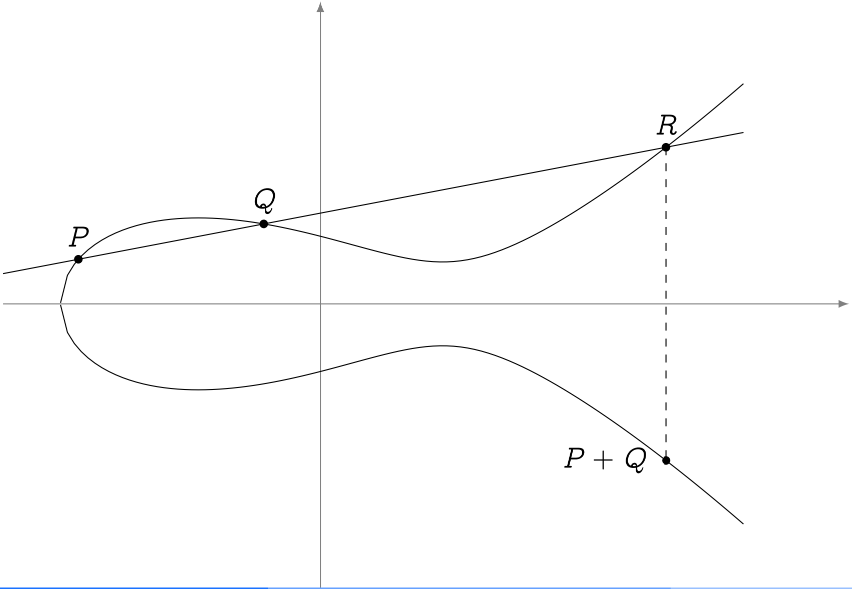
Up to isomorphism



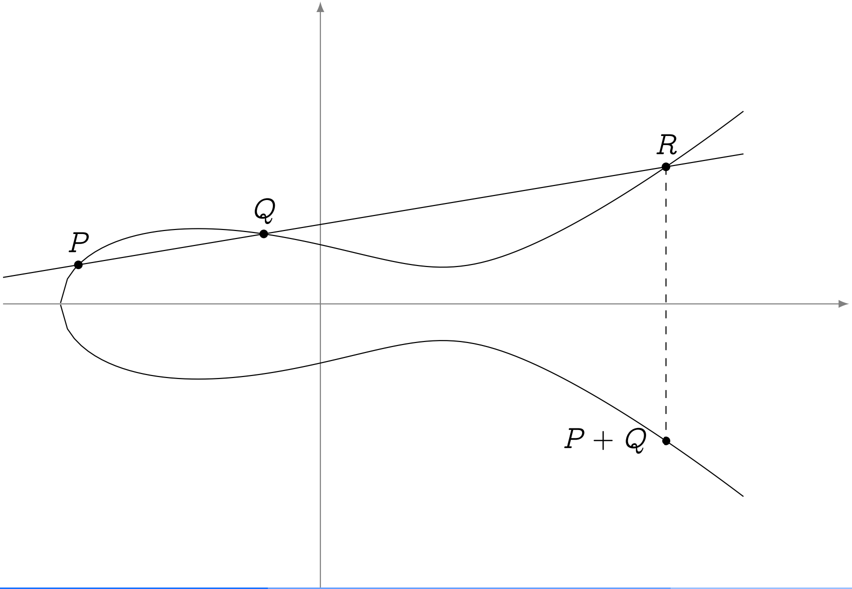
Up to isomorphism



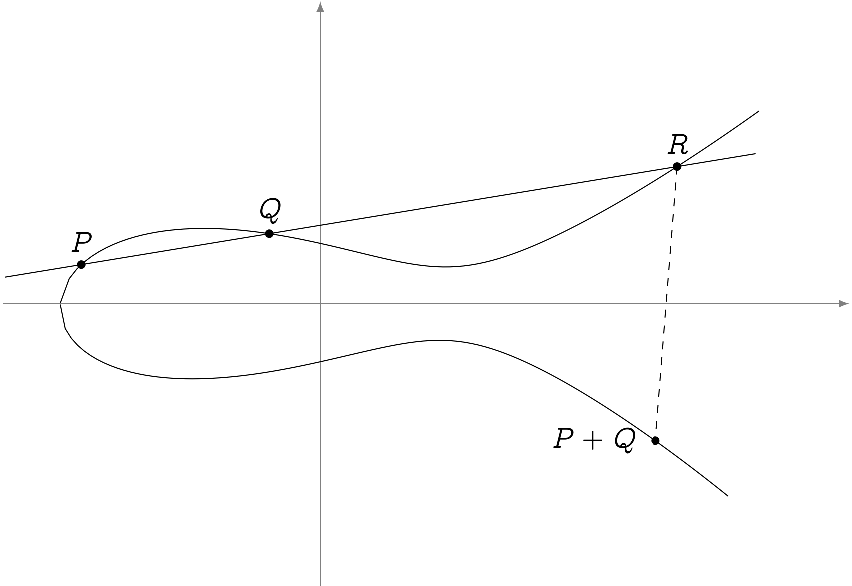
Up to isomorphism



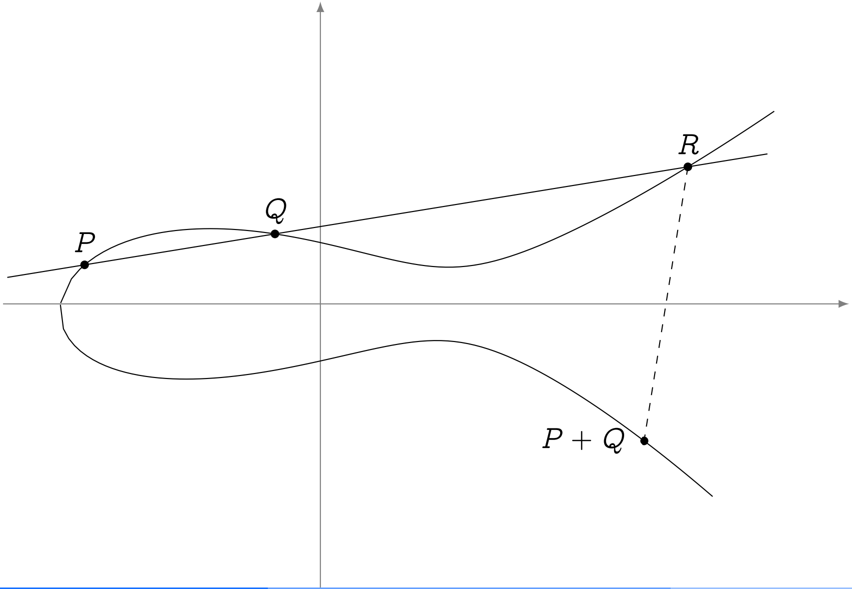
Up to isomorphism



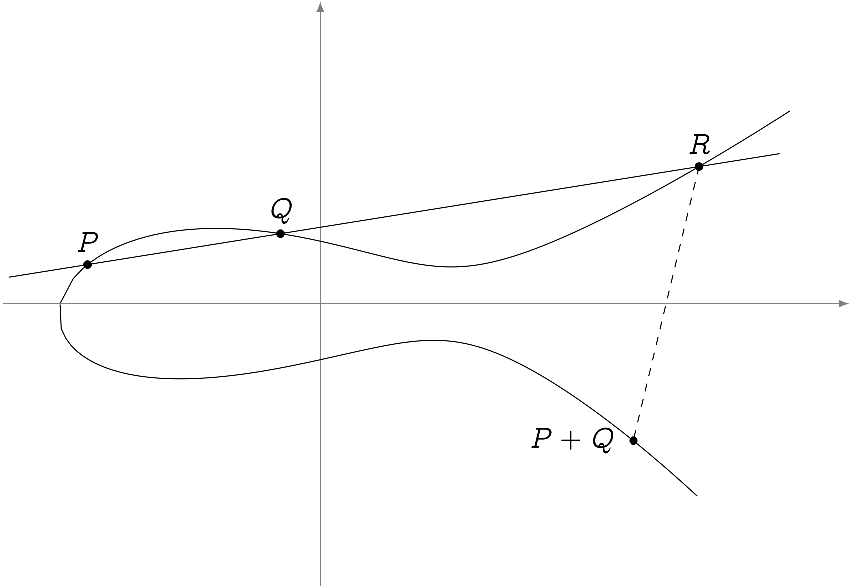
Up to isomorphism



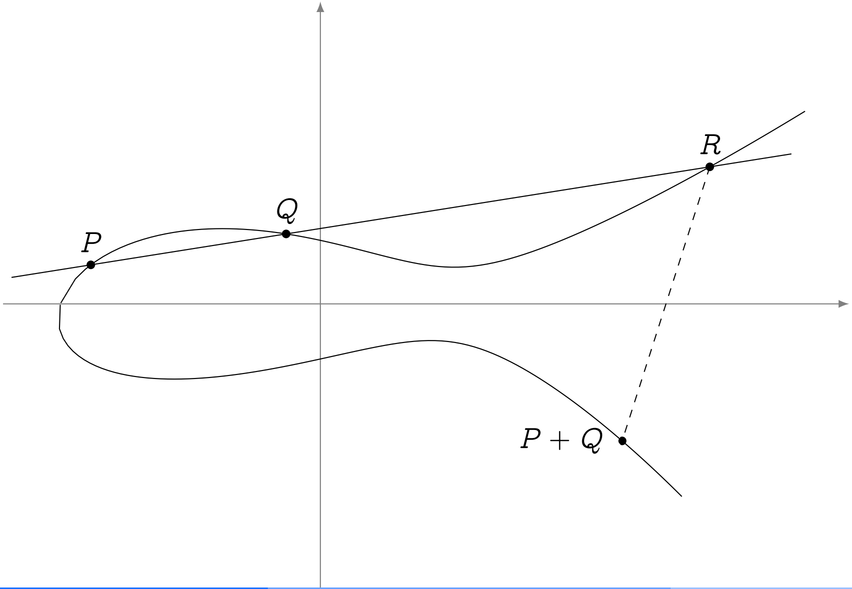
Up to isomorphism



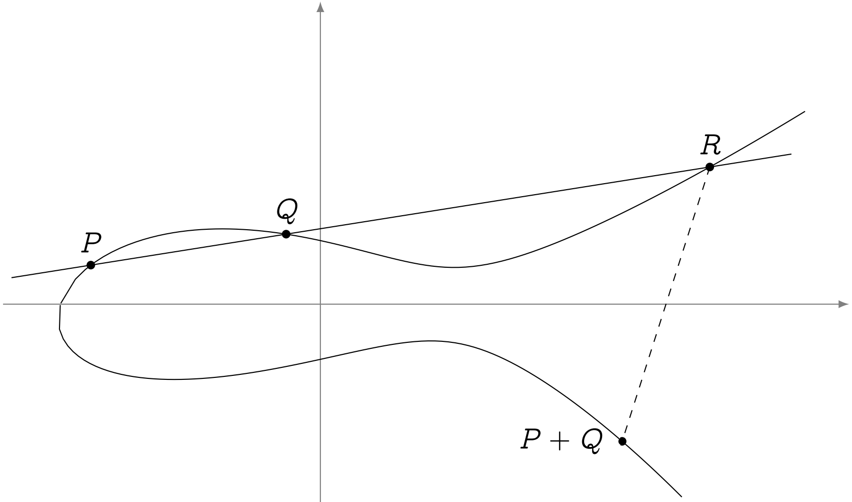
Up to isomorphism



Up to isomorphism

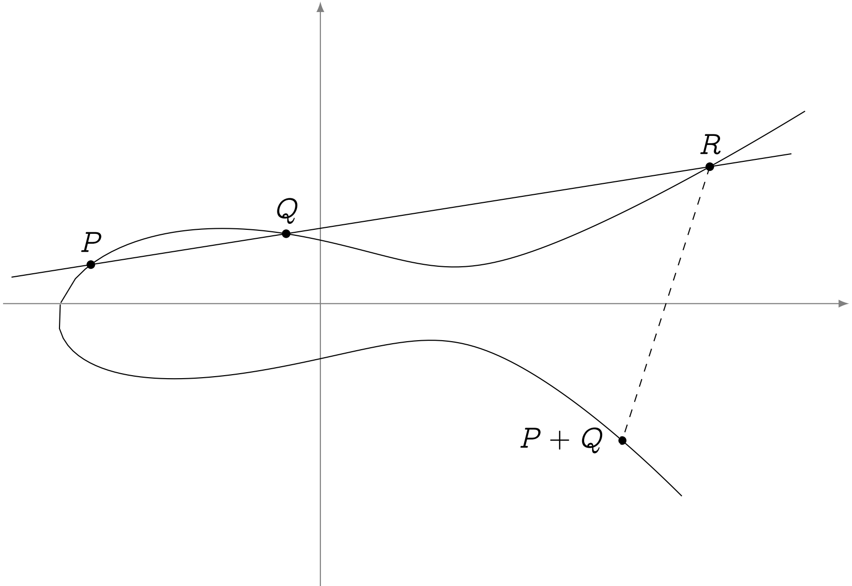


Up to isomorphism

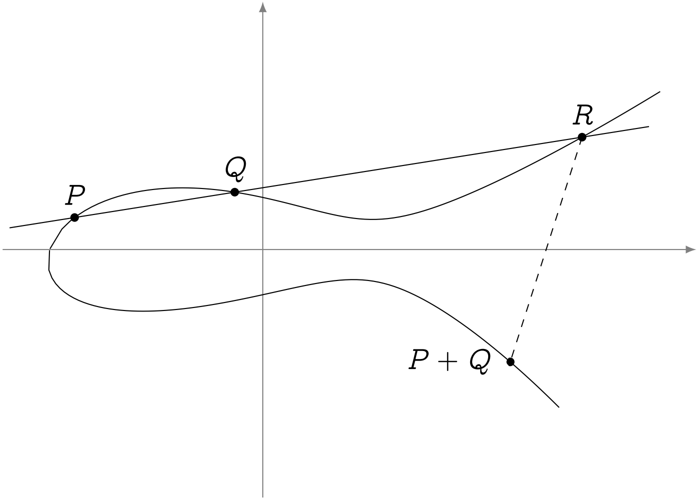


$$y^2 = x^3 + ax + b \quad \longrightarrow \quad j = 1728\frac{4a^3}{4a^3+27b^2}$$

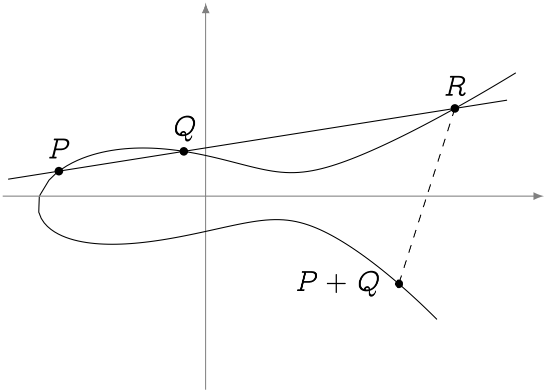
Up to isomorphism



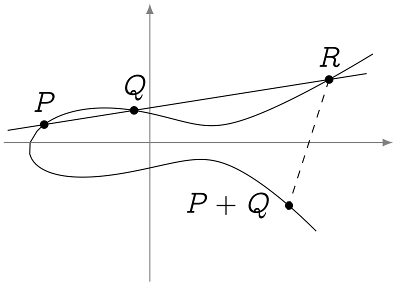
Up to isomorphism



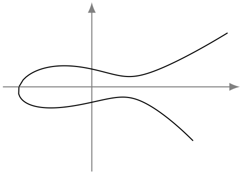
Up to isomorphism



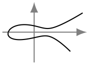
Up to isomorphism



Up to isomorphism



Up to isomorphism



Up to isomorphism

$j = 1728$

Up to isomorphism

$$j = 1728 \xrightarrow{\phi} j = 287496$$

Up to isomorphism

Isogeny graphs

Serre-Tate theorem

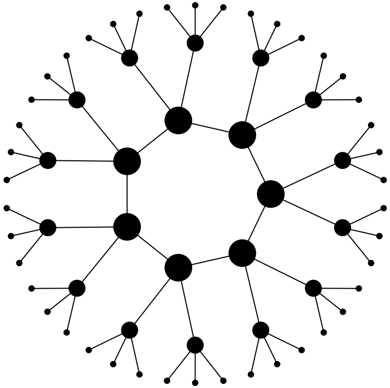
Two elliptic curves E, E' defined over a finite field $\mathbb{F}_q$ are isogenous (over $\mathbb{F}_q$) iff $\#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q)$.

Isogeny graphs

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

Isogeny volcanoes

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



The endomorphism ring

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

Theorem (Deuring)

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

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

  E is ordinary.
- An order $\mathcal{O}$ in a quadratic imaginary field:

  E is ordinary with complex multiplication by $\mathcal{O}$.
- Only if $p > 0$, a maximal order in a quaternion algebra[a]:

  E is supersingular.

[a] (ramified at p and ∞)

Algebras, orders

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

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

Orders

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

Examples:

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

The finite field case

Frobenius endomorphism

$$\pi : (x, y) \mapsto (x^q, y^q)$$

Theorem (Hasse): π satisfies a quadratic equation

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

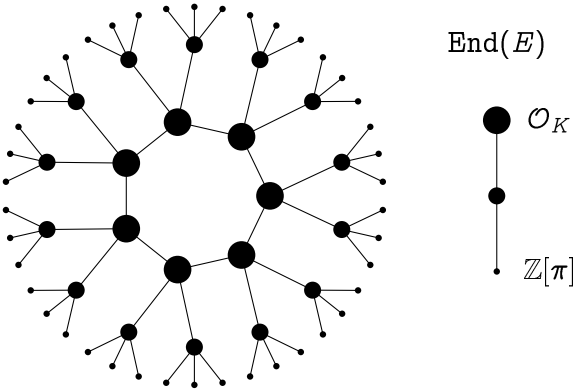
- t is the trace,
- $D_\pi = t^2 - 4q \leq 0$ is the discriminant,
- $t = 0 \mod p$ iff the curve is supersingular.
- In the ordinary case $D_\pi \neq 0$ and

$$\mathbb{Z}[\pi] \subset \mathrm{End}(E) \subset \mathbb{Q}(\sqrt{D_\pi}).$$

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.

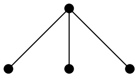


Ordinary isogeny volcano of degree $\ell = 3$.

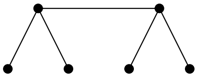
Volcanology (Kohel 1996)

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

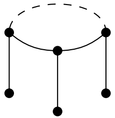
$\mathcal{O}_K$: maximal order of K,
D_K: discriminant of K.



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



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



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

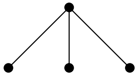
		Horizontal	Ascending	Descending
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$	$1 + \left(\frac{D_K}{\ell}\right)$		
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O} : \mathbb{Z}[\pi]]$	$1 + \left(\frac{D_K}{\ell}\right)$		$\ell - \left(\frac{D_K}{\ell}\right)$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

Volcanology (Kohel 1996)

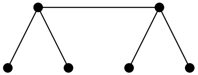
Let E be ordinary, $\mathrm{End}(E) \subset K$.

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

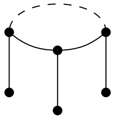
Height $= v_\ell([\mathcal{O}_K : \mathbb{Z}[\pi]])$.



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



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



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

		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	

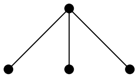
Volcanology (Kohel 1996)

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

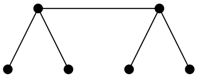
$\mathcal{O}_K$: maximal order of K,
D_K: discriminant of K.

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

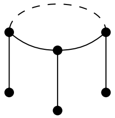
How large is the crater?



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



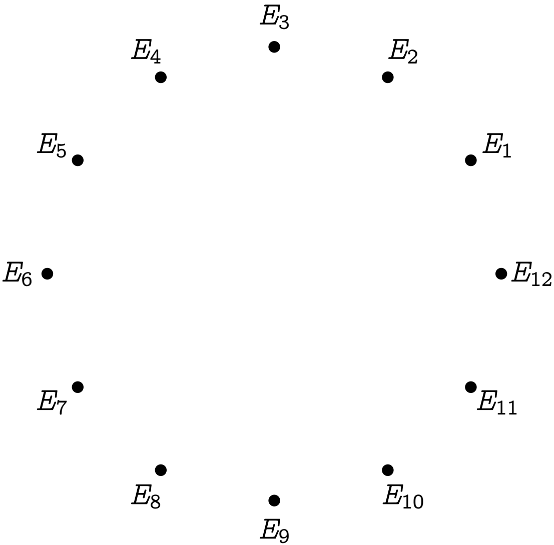
$\left(\frac{D_K}{\ell}\right) = 0$



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

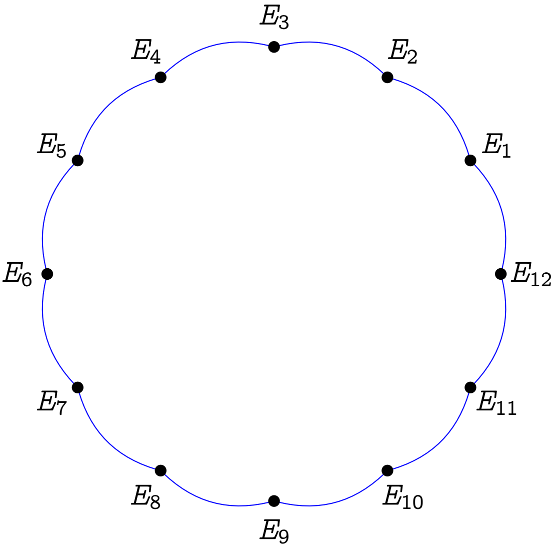
		Horizontal	Ascending	Descending
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$	$1 + \left(\frac{D_K}{\ell}\right)$		
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O} : \mathbb{Z}[\pi]]$	$1 + \left(\frac{D_K}{\ell}\right)$		$\ell - \left(\frac{D_K}{\ell}\right)$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

Vortex Surfer



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

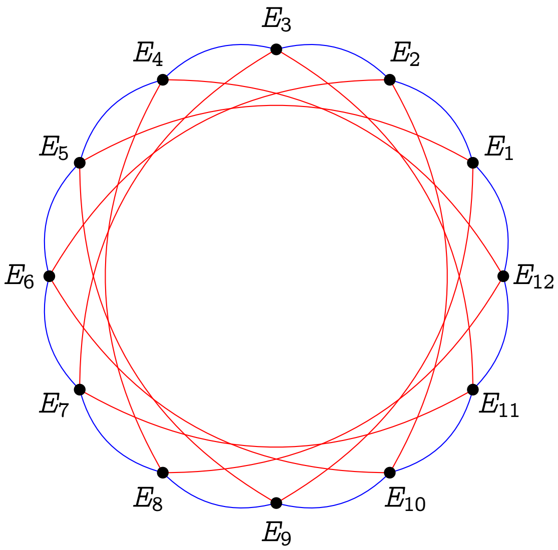
Vortex Surfer



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

— degree 2

Vortex Surfer



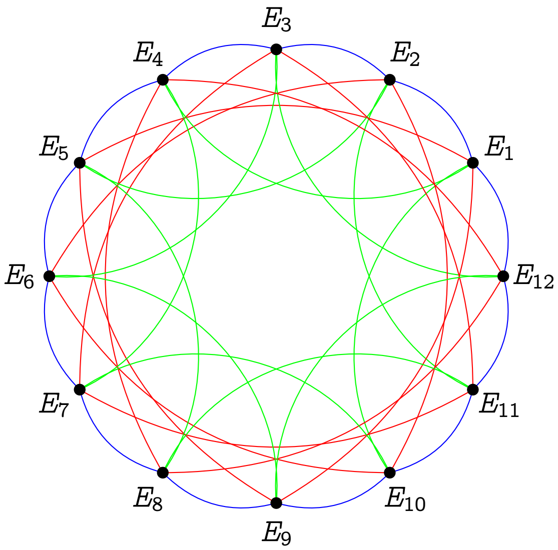
Vertices are elliptic curves with complex multiplication by $\mathcal{O}_K$ (i.e., $\mathrm{End}(E) \simeq \mathcal{O}_K \subset \mathbb{Q}(\sqrt{-D})$).

Edges are horizontal isogenies of bounded prime degree.

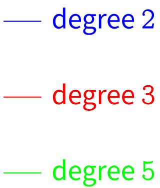
— degree 2

— degree 3

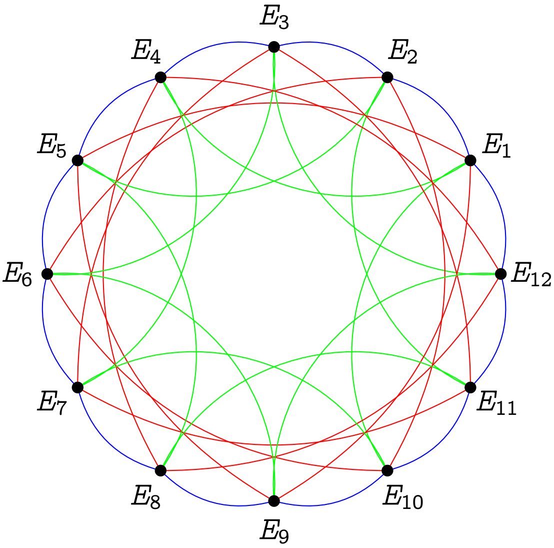
Vortex Surfer



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.



Vortex Surfer



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

What's happening here? Algebra!

Isogenies $\leftrightarrow$ Ideals of $\mathrm{End}(E)$

Horizontal Isogenies	**Invertible Ideals**
$\ker\phi_{\mathfrak{a}} = \{P \in E \mid \alpha(P) = 0 \text{ for all } \alpha \in \mathfrak{a}\}$	$\mathfrak{a} \subset \mathrm{End}(E)$

Isogenies $\leftrightarrow$ Ideals of $\mathrm{End}(E)$

Horizontal Isogenies	Invertible Ideals
$\ker\phi_{\mathfrak{a}} = \{P \in E \mid \alpha(P) = 0 \text{ for all } \alpha \in \mathfrak{a}\}$	$\mathfrak{a} \subset \mathrm{End}(E)$
degree	norm
dual	conjugate
composition	product
"direction" on the ℓ-isogeny cycle	ideal of norm ℓ

Isogenies $\leftrightarrow$ Ideals of $\mathrm{End}(E)$

Horizontal Isogenies	**Invertible Ideals**
$\ker \phi_{\mathfrak{a}} = \{P \in E \mid \alpha(P) = 0 \text{ for all } \alpha \in \mathfrak{a}\}$	$\mathfrak{a} \subset \mathrm{End}(E)$
degree	norm
dual	conjugate
composition	product
“direction” on the ℓ-isogeny cycle	ideal of norm ℓ
endomorphism	principal
$$\begin{tikzcd} E \arrow[r, bend left, "\phi_{\mathfrak{b}}"] \arrow[r, bend right, "\phi_{\mathfrak{a}}"'] & E' \end{tikzcd}$$	$\mathfrak{a}/\mathfrak{b}$ is principal

Isogenies $\leftrightarrow$ Ideals of $\mathrm{End}(E)$

Horizontal Isogenies	**Invertible Ideals**
$\ker \phi_{\mathfrak{a}} = \{P \in E \mid \alpha(P) = 0 \text{ for all } \alpha \in \mathfrak{a}\}$	$\mathfrak{a} \subset \mathrm{End}(E)$
degree	norm
dual	conjugate
composition	product
"direction" on the ℓ-isogeny cycle	ideal of norm ℓ
endomorphism	principal
$\begin{tikzcd} E \arrow[r, bend left, "\phi_{\mathfrak{b}}"] \arrow[r, bend right, "\phi_{\mathfrak{a}}"'] & E' \end{tikzcd}$	$\mathfrak{a}/\mathfrak{b}$ is principal
Elliptic curves with CM by $\mathcal{O}$	Invertible ideals / Principal ideals

Class group action

Class group

The class group of an order $\mathcal{O} \subset \mathbb{Q}(\sqrt{-D})$ is the quotient

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

It is a finite abelian group.

Main theorem of complex multiplication

The class group of $\mathcal{O}$ acts faithfully and transitively on the set of elliptic curves with CM by $\mathcal{O}$ by

$$\begin{aligned}\mathrm{Cl}(\mathcal{O}) \times \mathrm{Ell}(\mathcal{O}) &\to \mathrm{Ell}(\mathcal{O}) \\ \mathfrak{a} * E &= E/E[\mathfrak{a}]\end{aligned}$$

Corollary

$$\#\,\mathrm{Cl}(\mathcal{O}) = \#\mathrm{Ell}(\mathcal{O}).$$

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.
- $\pi = \pm\sqrt{q} \in \mathbb{Z}$, hence no complex multiplication.

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

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

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

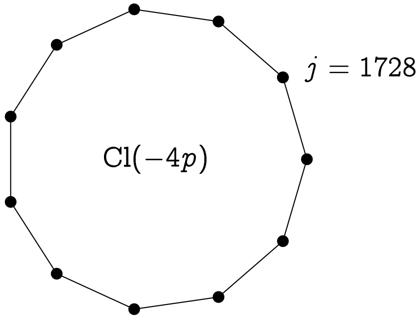
  where $i \in \mathbb{F}_{p^2}$ is a 4-th root of unity. Clearly, $\iota^2 = -1$.

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

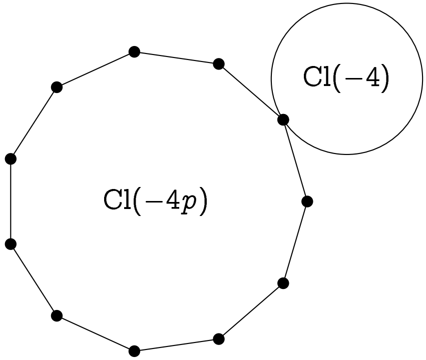
Class group action party

$\bullet\ j = 1728$

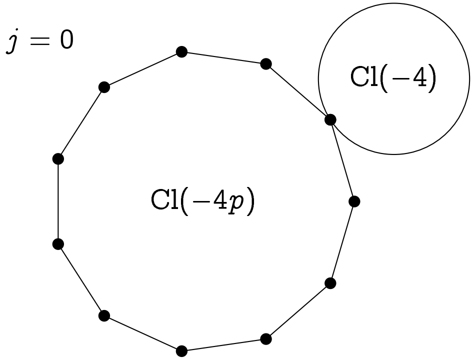
Class group action party



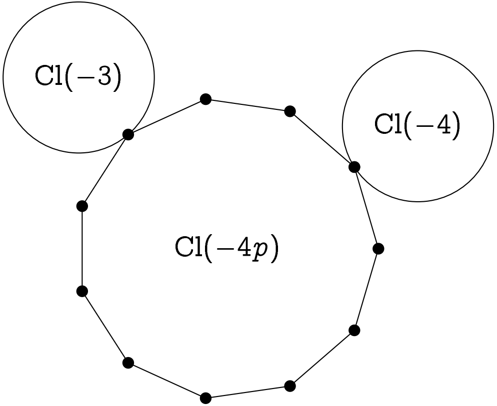
Class group action party



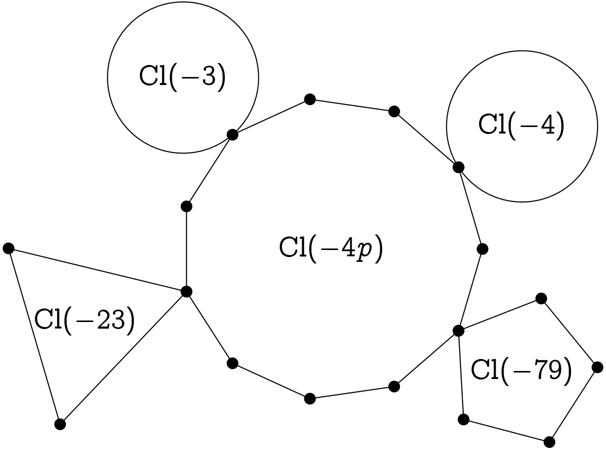
Class group action party



Class group action party



Class group action party



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.

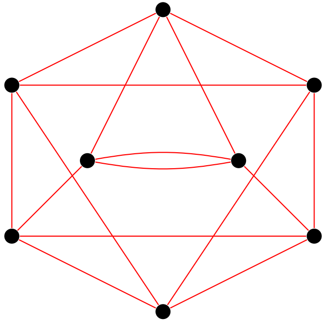


Figure: 3-isogeny graph on $\mathbb{F}_{97^2}$.

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.
Diameter:	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)

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, Venkatesan)

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

[a] May contain traces of GRH.

Executive summary

- Separable ℓ-isogeny = finite kernel = subgroup of $E[\ell]$ (= ideal of norm ℓ),
- Isogeny graphs have j-invariants for vertices and "some" isogenies for edges.
- By varying the choices for the vertex and the isogeny set, we obtain graphs with different properties.
- ℓ-isogeny graphs of ordinary curves are volcanoes, (full) ℓ-isogeny graphs of supersingular curves are finite $(\ell + 1)$-regular.
- CM theory naturally leads to define graphs of horizontal isogenies (both in the ordinary and the supersingular case) that are isomorphic to Cayley graphs of class groups.
- CM graphs are expanders. Supersingular full ℓ-isogeny graphs are Ramanujan.

Isogeny Based Cryptography: an Introduction

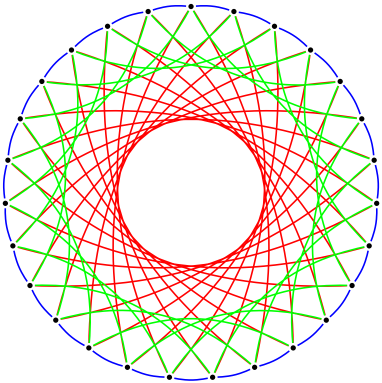
Luca De Feo
IBM Research Zürich

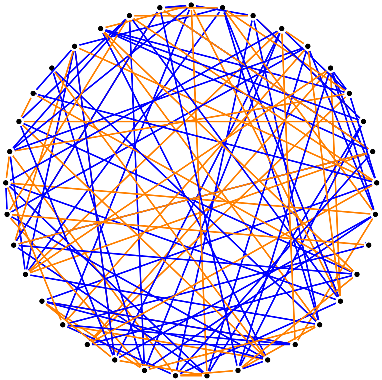
November 28, 2019
NTNU, Trondheim

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

The beauty and the beast (credit: Lorenz Panny)

Components of particular isogeny graphs look like this:

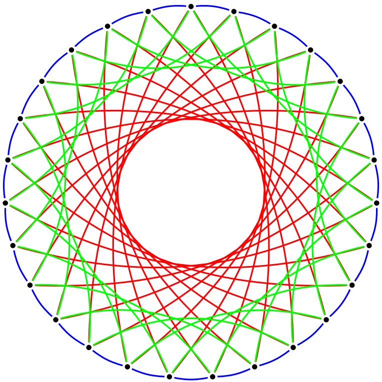


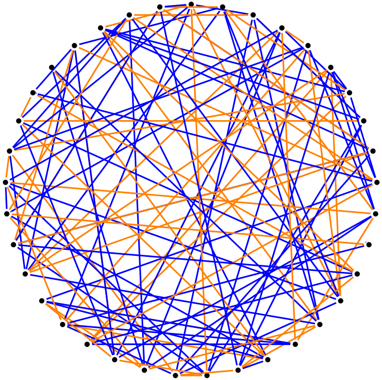


Which of these is good for crypto?

The beauty and the beast (credit: Lorenz Panny)

Components of particular isogeny graphs look like this:

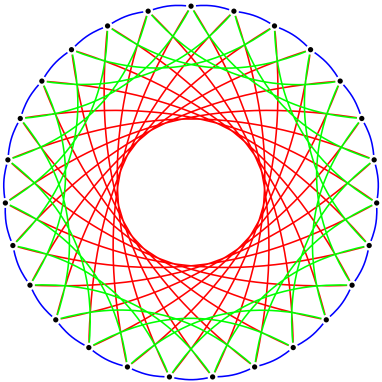




Which of these is good for crypto? **Both.**

The beauty and the beast (credit: Lorenz Panny)

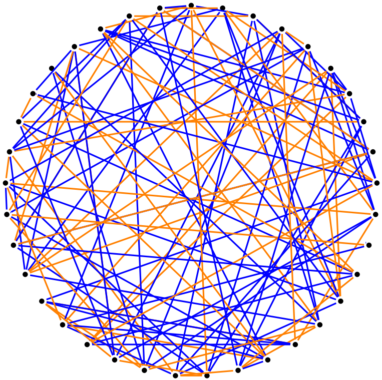
At this time, there are two distinct families of systems:



$\mathbb{F}_p$

CSIDH [pron.: sea-side]

`https://csidh.isogeny.org`



$\mathbb{F}_{p^2}$

SIDH

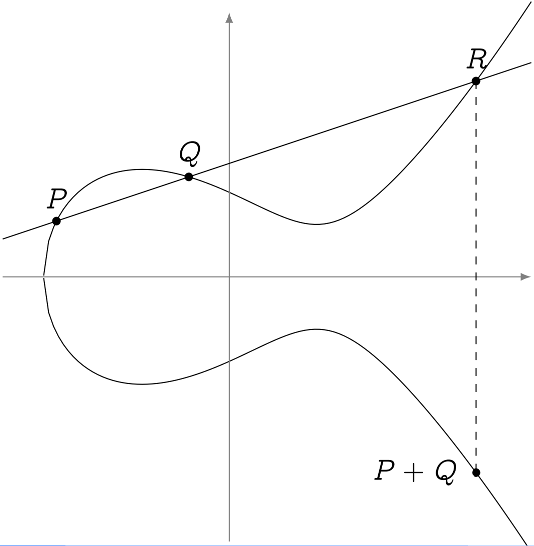
`https://sike.org`

Brief history of isogeny-based cryptography

- **1997** Couveignes introduces the Hard Homogeneous Spaces framework. His work stays unpublished for 10 years.
- **2006** Rostovtsev & Stolbunov independently rediscover Couveignes ideas, suggest isogeny-based Diffie–Hellman as a quantum-resistant primitive.
- **2006-2010** Other isogeny-based protocols by Teske and Charles, Goren & Lauter.
- **2011-2012** D., Jao & Plût introduce SIDH, an efficient post-quantum key exchange inspired by Couveignes, Rostovtsev, Stolbunov, Charles, Goren, Lauter.
- **2017** SIDH is submitted to the NIST competition (with the name SIKE, only isogeny-based candidate).
- **2018** D., Kieffer & Smith *resurrect* the Couveignes–Rostovtsev–Stolbunov protocol, Castryck, Lange, Martindale, Panny & Renes create an efficient variant named CSIDH.
- **2019** The year of proofs of isogeny knowledge: SeaSign (D. & Galbraith; Decru, Panny & Vercauteren), CSI-FiSh (Beullens, Kleinjung & Vercauteren), VDF (D., Masson, Petit & Sanso), threshold (D. & Meyer).

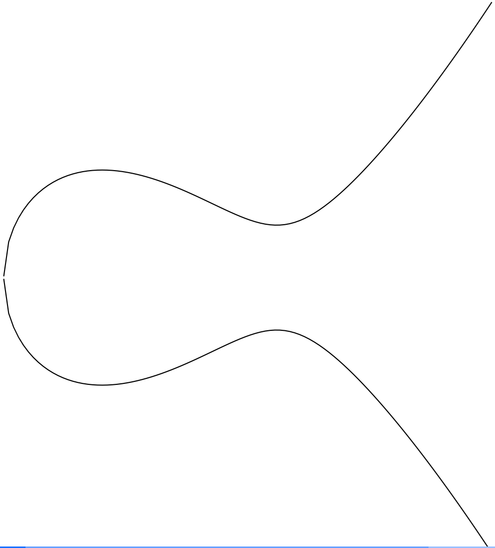
Elliptic curves

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



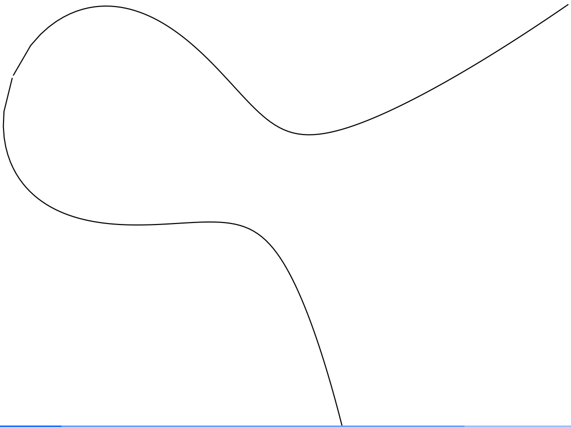
Elliptic curves

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



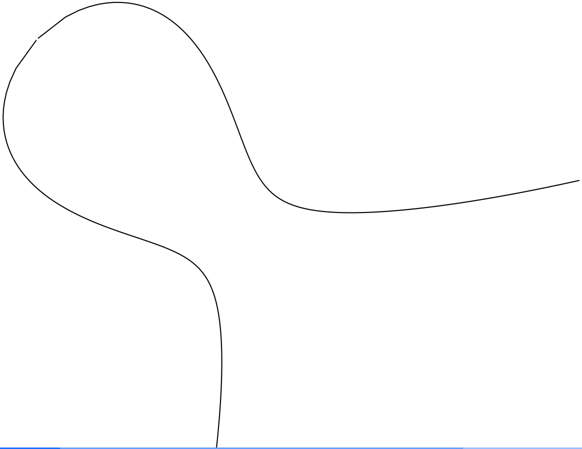
Elliptic curves

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



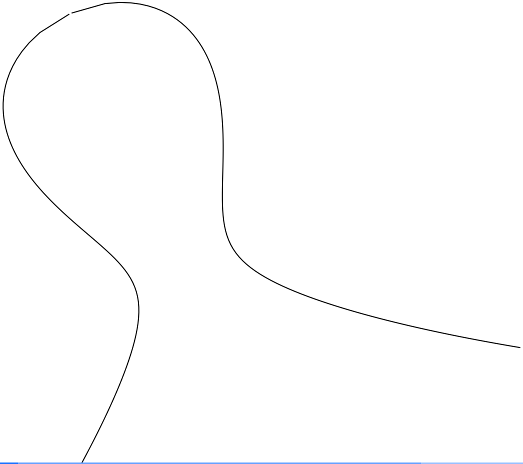
Elliptic curves

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



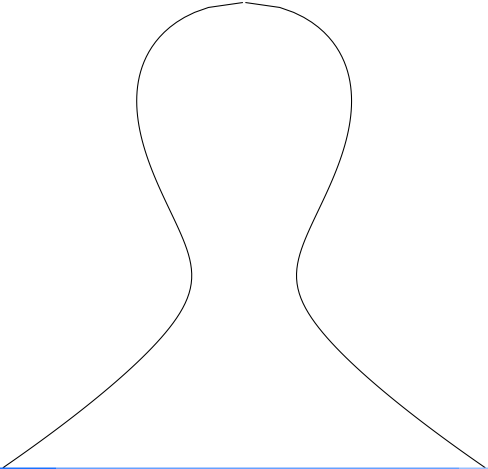
Elliptic curves

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



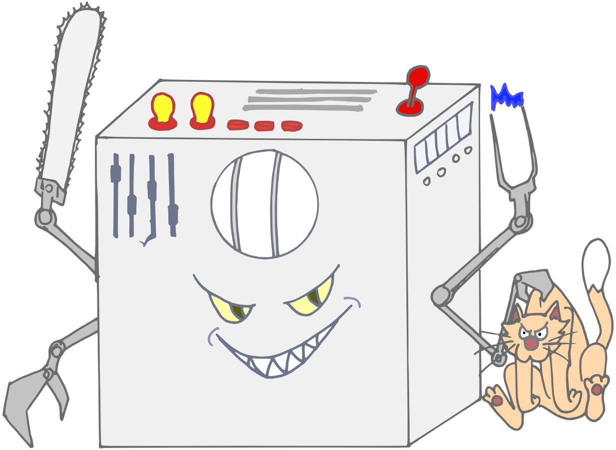
Elliptic curves

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

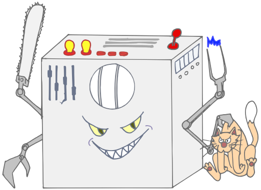


Elliptic curves

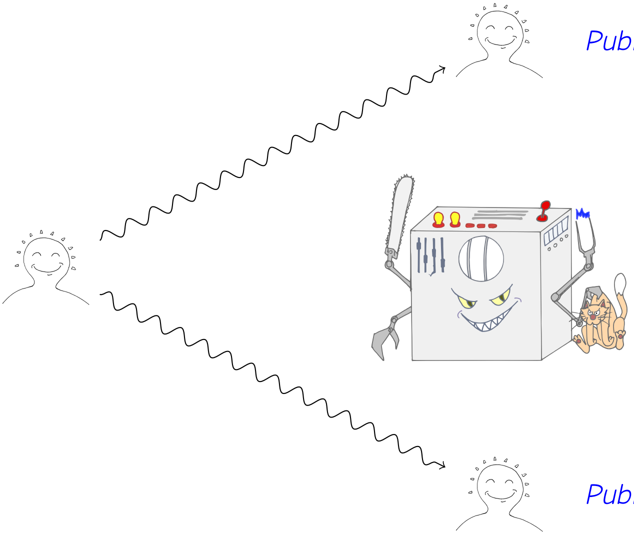
The QUANTHOM Menace



Basically every isogeny-based key-exchange...



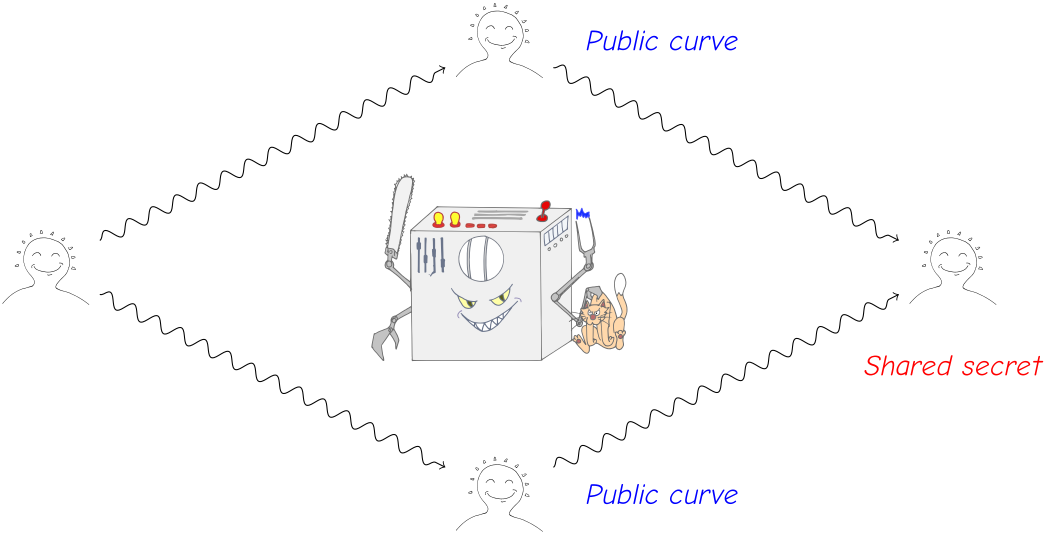
Basically every isogeny-based key-exchange...



Public curve

Public curve

Basically every isogeny-based key-exchange...



Hard Homogeneous Spaces[1]

Principal Homogeneous Space

$\mathcal{G} \circlearrowright \mathcal{E}$: A (finite) set $\mathcal{E}$ acted upon by a group $\mathcal{G}$ faithfully and transitively:

$$\begin{aligned} * : \mathcal{G} \times \mathcal{E} &\longrightarrow \mathcal{E} \\ \mathfrak{g} * E &\longmapsto E' \end{aligned}$$

Compatibility: $\mathfrak{g}' * (\mathfrak{g} * E) = (\mathfrak{g}'\mathfrak{g}) * E$ for all $\mathfrak{g}, \mathfrak{g}' \in \mathcal{G}$ and $E \in \mathcal{E}$;

Identity: $\mathfrak{e} * E = E$ if and only if $\mathfrak{e} \in \mathcal{G}$ is the identity element;

Transitivity: for all $E, E' \in \mathcal{E}$ there exist a unique $\mathfrak{g} \in \mathcal{G}$ such that $\mathfrak{g} * E' = E$.

Example: the set of elliptic curves with complex multiplication by $\mathcal{O}$ is a PHS for the class group $\mathrm{Cl}(\mathcal{O})$.

[1] Couveignes 2006.

Hard Homogeneous Spaces

Hard Homogeneous Space (HHS)

A Principal Homogeneous Space $\mathcal{G} \circlearrowright \mathcal{E}$ such that $\mathcal{G}$ is commutative and:

- Evaluating $E' = \mathfrak{g} * E$ is easy;
- Inverting the action is hard.

HHS Diffie–Hellman

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) HHS $\mathcal{G} \circlearrowright \mathcal{E}$ of order N.

$$\begin{array}{ccc} \textbf{Alice} & & \textbf{Bob} \\ \text{pick random } \mathfrak{a} \in \mathcal{G} & & \text{pick random } \mathfrak{b} \in \mathcal{G} \\ \text{compute } E_A = \mathfrak{a} * E_0 & & \text{compute } E_B = \mathfrak{b} * E_0 \\ & \xrightarrow{\quad E_A \quad} & \\ & \xleftarrow[\quad E_B \quad]{} & \end{array}$$

Shared secret is $\mathfrak{a} * E_B = (\mathfrak{a}\mathfrak{b}) * E_0 = \mathfrak{b} * E_A$

HHSDH from complex multiplication

Obstacles:

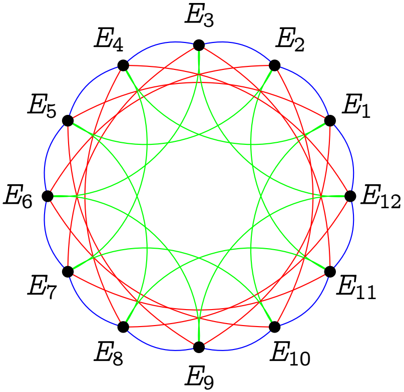
- The group size of $\mathrm{Cl}(\mathcal{O})$ is unknown.
- Only ideals of small norm (isogenies of small degree) are efficient to evaluate.

Solution:

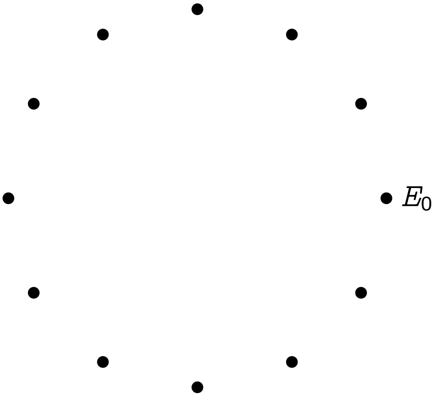
- Restrict to elements of $\mathrm{Cl}(\mathcal{O})$ of the form

$$\mathfrak{g} = \prod \mathfrak{a}_i^{e_i}$$

  for a basis of $\mathfrak{a}_i$ of small norm.
- Equivalent to doing isogeny walks of smooth degree.



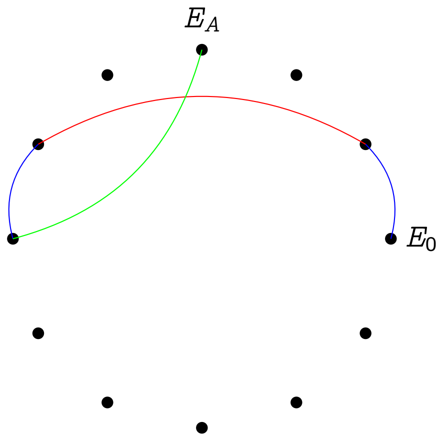
CSIDH key exchange



Public parameters:

- A supersingular curve $E_0/\mathbb{F}_p$;
- A set of small prime degree isogenies.

CSIDH key exchange

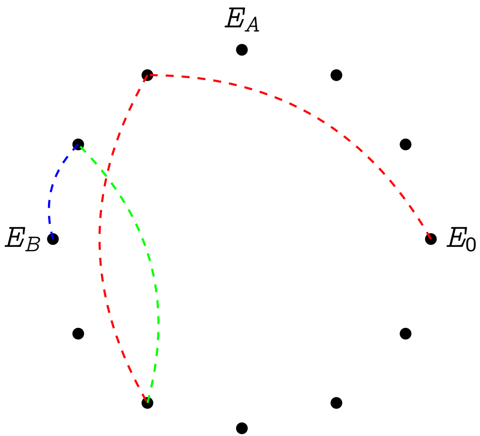


Public parameters:

- A supersingular curve $E_0/\mathbb{F}_p$;
- A set of small prime degree isogenies.

1. **Alice** takes a secret random walk $\phi_A : E_0 \to E_A$ of length $O(\log p)$;

CSIDH key exchange

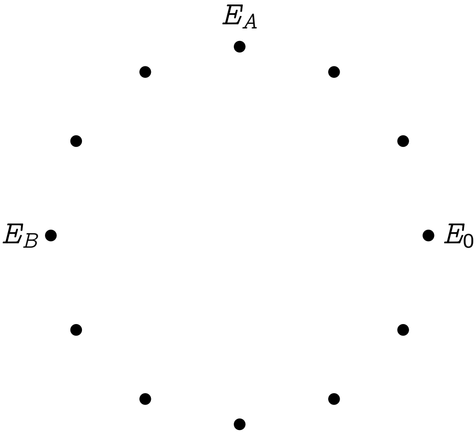


Public parameters:

- A supersingular curve $E_0/\mathbb{F}_p$;
- A set of small prime degree isogenies.

1. **Alice** takes a secret random walk $\phi_A : E_0 \to E_A$ of length $O(\log p)$;
2. **Bob** does the same;

CSIDH key exchange

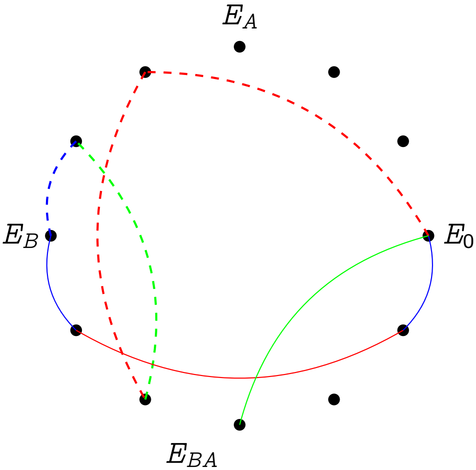


Public parameters:

- A supersingular curve $E_0/\mathbb{F}_p$;
- A set of small prime degree isogenies.

1. **Alice** takes a secret random walk $\phi_A : E_0 \to E_A$ of length $O(\log p)$;
2. **Bob** does the same;
3. They publish E_A and E_B;

CSIDH key exchange

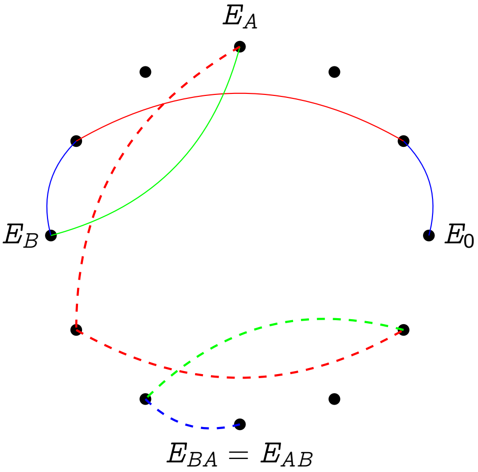


Public parameters:

- A supersingular curve $E_0/\mathbb{F}_p$;
- A set of small prime degree isogenies.

1. **Alice** takes a secret random walk $\phi_A : E_0 \to E_A$ of length $O(\log p)$;
2. **Bob** does the same;
3. They publish E_A and E_B;
4. **Alice** repeats her secret walk ϕ_A starting from E_B.

CSIDH key exchange



Public parameters:

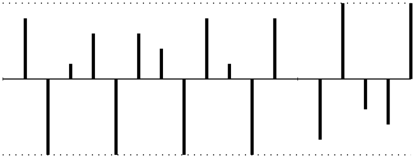
- A supersingular curve $E_0/\mathbb{F}_p$;
- A set of small prime degree isogenies.

1. **Alice** takes a secret random walk $\phi_A : E_0 \to E_A$ of length $O(\log p)$;
2. **Bob** does the same;
3. They publish E_A and E_B;
4. **Alice** repeats her secret walk ϕ_A starting from E_B.
5. **Bob** repeats his secret walk ϕ_B starting from E_A.

CSIDH data flow

Your secret: a vector of number of isogeny steps for each degree

$$(5, 1, -4, \dots)$$



Your public key: (the j-invariant of) a supersingular elliptic curve

$$j = \mathtt{0x23baf75419531a44f3b97cc9d8291a275047fcdae0c9a0c0ebb993964f821f2}$$
$$\mathtt{0c11058a4200ff38c4a85e208345300033b0d3119ff4a7c1be0acd62a622002a9}$$

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 superposition[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.

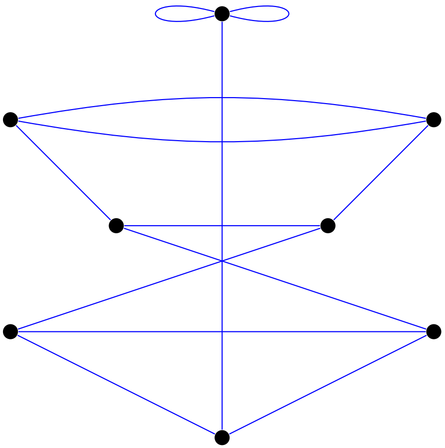


Figure: 2- and 3-isogeny graphs on $\mathbb{F}_{97^2}$.

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.

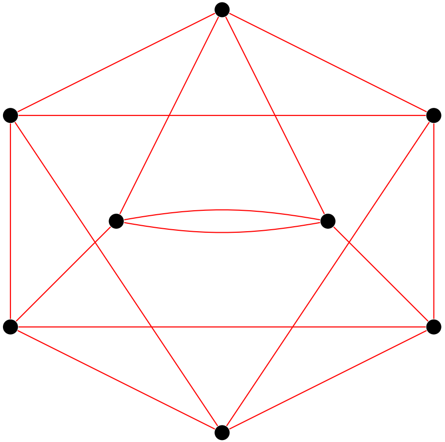


Figure: 2- and 3-isogeny graphs on $\mathbb{F}_{97^2}$.

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.

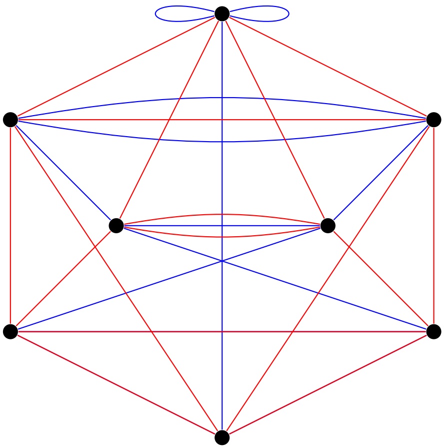


Figure: 2- and 3-isogeny graphs on $\mathbb{F}_{97^2}$.

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[2]

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:

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

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

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

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

Supersingular Isogeny Diffie-Hellman[2]

Parameters:

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

Secret data:

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

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

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

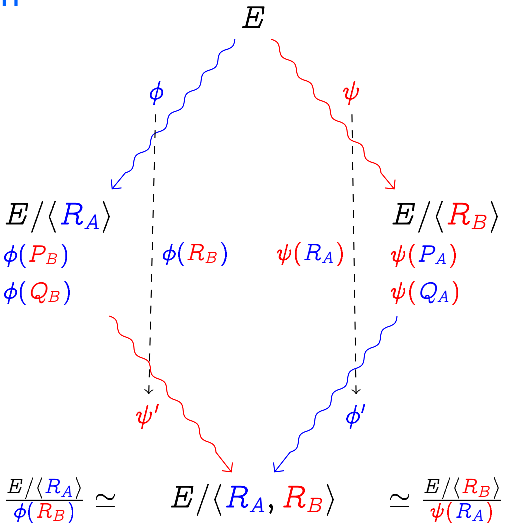
Supersingular Isogeny Diffie-Hellman[2]

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:

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



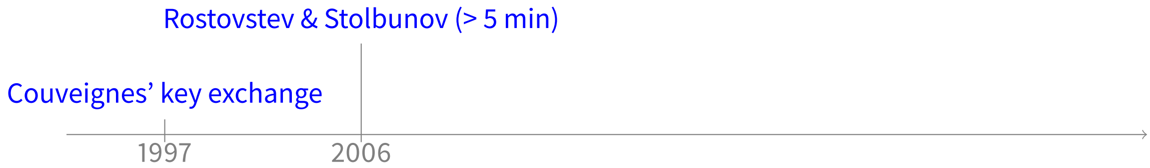
[2] Jao and De Feo 2011; De Feo, Jao, and Plût 2014.

From 10 minutes to 10ms in 20 years

Couveignes' key exchange

1997

From 10 minutes to 10ms in 20 years



From 10 minutes to 10ms in 20 years

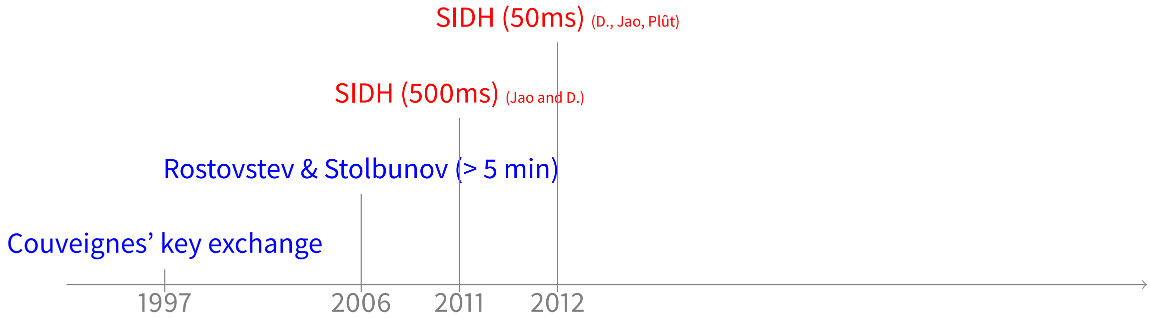
SIDH (500ms) (Jao and D.)

Rostovstev & Stolbunov (> 5 min)

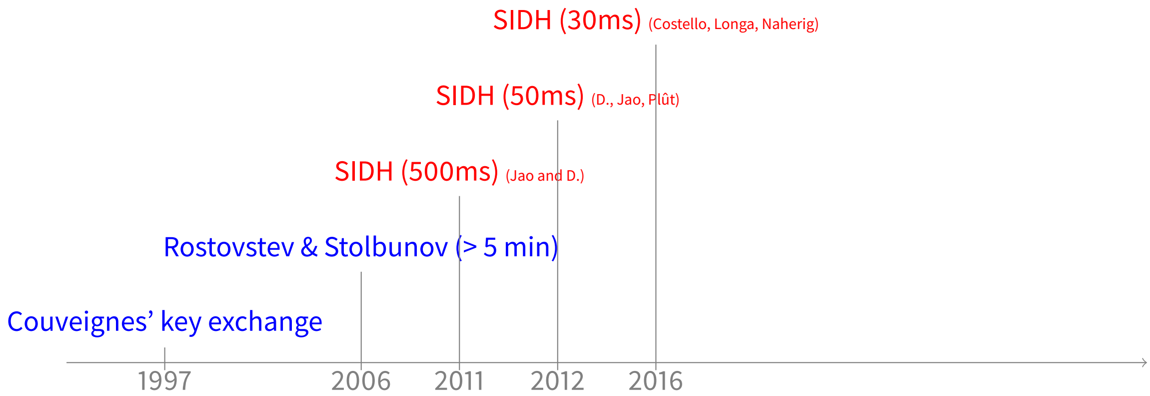
Couveignes' key exchange

1997 2006 2011

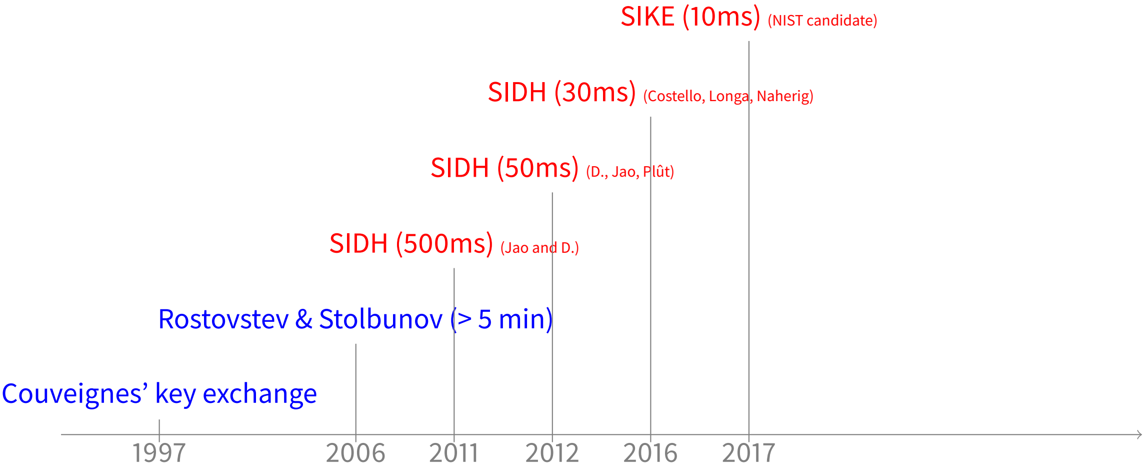
From 10 minutes to 10ms in 20 years



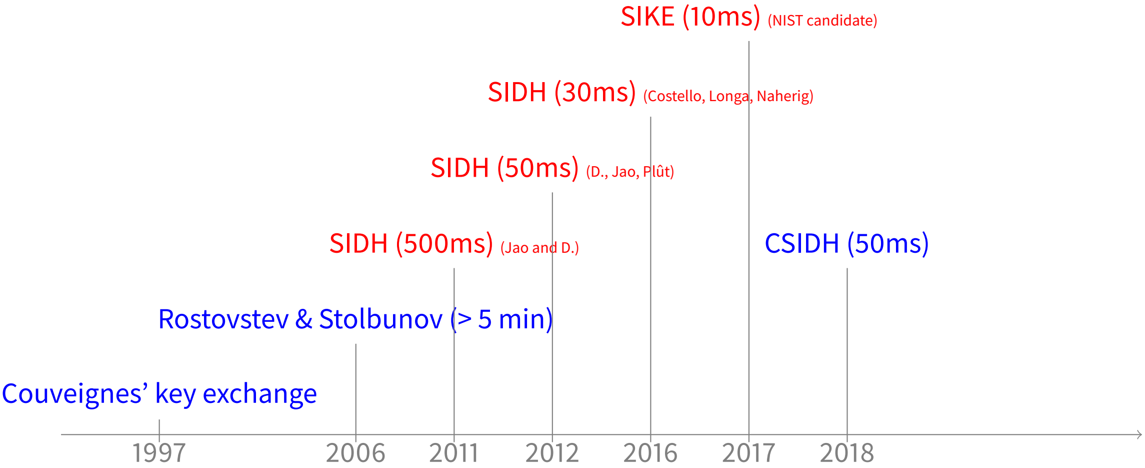
From 10 minutes to 10ms in 20 years



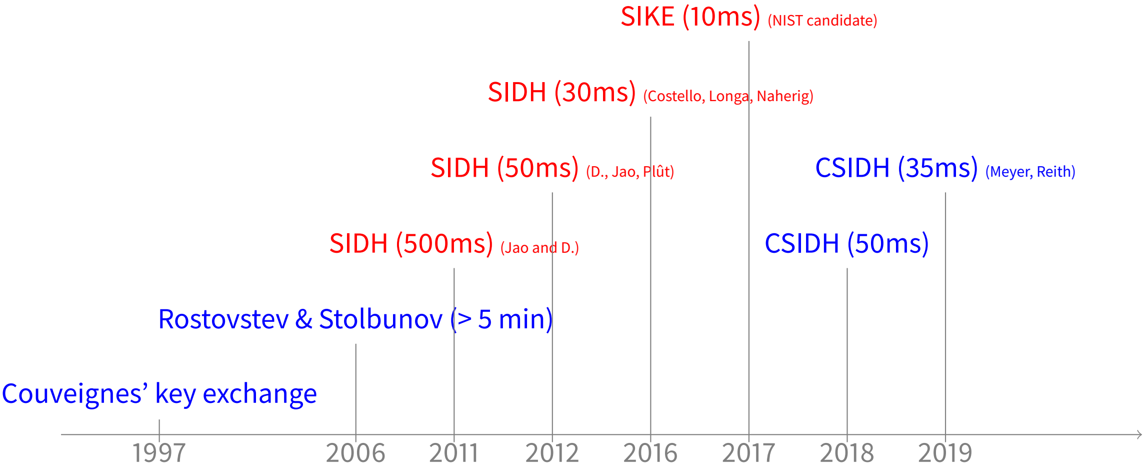
From 10 minutes to 10ms in 20 years



From 10 minutes to 10ms in 20 years



From 10 minutes to 10ms in 20 years



CSIDH vs SIDH

	CSIDH	**SIDH**
Speed (on x64 arch., NIST 1)	$\sim$ 35ms	$\sim$ 6ms
Public key size (NIST 1)	64B	346B
Key compression		
↳ speed		$\sim$ 11ms
↳ size		209B
Submitted to NIST	no	yes
TRL	4	6
Best classical attack	$p^{1/4}$	$p^{1/4} \quad (p^{3/8})$
Best quantum attack	$\tilde{O}\left(3^{\sqrt{\log_3 p}}\right)$	$p^{1/6} \quad (p^{3/8})$
Key size scales	quadratically	linearly
CPA security	yes	yes
CCA security	yes	Fujisaki-Okamoto
Constant time	it's complicated	yes
Non-interactive key exchange	yes	no
Signatures	short but (slow | do not scale)	big and slow

Why prove a secret isogeny?

Public: Curves E, E'
Secret: An isogeny walk $E \to E'$

Why?

- For interactive identification;
- For signing messages;
- For validating public keys (esp. SIDH);
- More...

Some properties

	Zero knowledge			
	Statistical	Computational	Quantum resistance	Succinctness
CSIDH	✓		✓ /sort of	
SIDH		✓	✓	
Pairings				✓

Security assumptions in Isogeny-based Cryptography

Isogeny walk problem

Input Two isogenous elliptic curves E, E' over $\mathbb{F}_q$.

Output A path $E \to E'$ in an isogeny graph.

SIDH problem (1)

Input Elliptic curves E, E' over $\mathbb{F}_q$, isogenous of degree $\ell_A^{e_A}$.

Output The unique path $E \to E'$ of length e_A in the ℓ_A-isogeny graph.

SIDH problem (2)

Input
- Elliptic curves E, E' over $\mathbb{F}_q$, isogenous of degree $\ell_A^{e_A}$;
- The action of the isogeny on $E[\ell_B^{e_B}]$.

Output The unique path $E \to E'$ of length e_A in the ℓ_A-isogeny graph.

A Σ-protocol from Diffie–Hellman[3]

- A key pair (s, g^s);

$$g \xrightarrow{\quad s \quad} g^s$$

[3] Kids, do not try this at home! Use Schnorr!

A Σ-protocol from Diffie–Hellman[3]

- A key pair (s, g^s);
- Commit to a random element g^r;

$$\begin{tikzcd} g \arrow[r, "s"] \arrow[d, "r"'] & g^s \\ g^r & \end{tikzcd}$$

[3] Kids, do not try this at home! Use Schnorr!

A Σ-protocol from Diffie–Hellman[3]

- A key pair (s, g^s);
- Commit to a random element g^r;
- Challenge with bit $b \in \{0, 1\}$;

$$\begin{tikzcd} g \arrow[rr, "s"] \arrow[dr, "r"'] & & g^s \\ & g^r & \end{tikzcd}$$

[3] Kids, do not try this at home! Use Schnorr!

A Σ-protocol from Diffie–Hellman[3]

- A key pair (s, g^s);
- Commit to a random element g^r;
- Challenge with bit $b \in \{0, 1\}$;
- Respond with $c = r - b \cdot s \mod \#G$;

$$\begin{tikzcd}
g \arrow[rr, "s"] \arrow[dr, "r"'] & & g^s \arrow[dl, dashed, "r-s"] \\
& g^r &
\end{tikzcd}$$

[3] Kids, do not try this at home! Use Schnorr!

A Σ-protocol from Diffie–Hellman[3]

- A key pair (s, g^s);
- Commit to a random element g^r;
- Challenge with bit $b \in \{0, 1\}$;
- Respond with $c = r - b \cdot s \mod \#G$;
- Verify that $g^c(g^s)^b = g^r$.

$$
\begin{tikzcd}
g \arrow[rr, "s"] \arrow[dr, "r"'] & & g^s \arrow[dl, dashed, "r - s"] \\
& g^r &
\end{tikzcd}
$$

[3]Kids, do not try this at home! Use Schnorr!

A Σ-protocol from Diffie–Hellman[3]

- A key pair (s, g^s);
- Commit to a random element g^r;
- Challenge with bit $b \in \{0, 1\}$;
- Respond with $c = r - b \cdot s \mod \#G$;
- Verify that $g^c(g^s)^b = g^r$.

$$\begin{tikzcd}
g \arrow[rr, "s"] \arrow[dr, "r"'] & & g^s \arrow[dl, dashed, "r - s"] \\
& g^r &
\end{tikzcd}$$

Zero-knowledge

Does not leak because:
c is uniformly distributed and independent from s.

[3] Kids, do not try this at home! Use Schnorr!

A Σ-protocol from Diffie–Hellman[3]

- A key pair (s, g^s);
- Commit to a random element g^r;
- Challenge with bit $b \in \{0, 1\}$;
- Respond with $c = r - b \cdot s \mod \#G$;
- Verify that $g^c(g^s)^b = g^r$.

$$
\begin{tikzcd}
E_1 \arrow[rr, "g^s"] \arrow[dr, "g^r"'] & & E_s \arrow[dl, dashed, "g^{r-s}"] \\
& E_r &
\end{tikzcd}
$$

Zero-knowledge

Does not leak because:
c is uniformly distributed and independent from s.

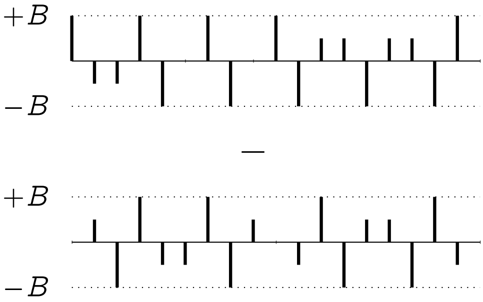
Unlike Schnorr, compatible with
group action Diffie–Hellman.

[3] Kids, do not try this at home! Use Schnorr!

The trouble with groups of unknown structure

In CSIDH secrets look like: $g^{\vec{s}} = g_2^{s_2} g_3^{s_3} g_5^{s_5} \cdots$

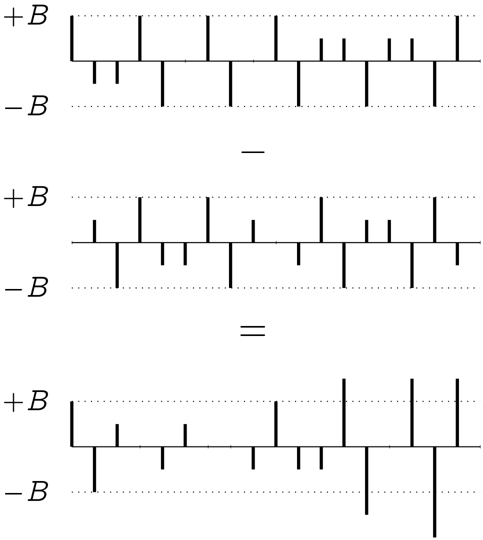
- the elements g_i are fixed,
- the secret is the exponent vector $\vec{s} = (s_2, s_3, \dots) \in [-B, B]^n$,
- secrets must be sampled in a box $[-B, B]^n$ "large enough"…



The trouble with groups of unknown structure

In CSIDH secrets look like: $g^{\vec{s}} = g_2^{s_2} g_3^{s_3} g_5^{s_5} \cdots$

- the elements g_i are fixed,
- the secret is the exponent vector $\vec{s} = (s_2, s_3, \dots) \in [-B, B]^n$,
- secrets must be sampled in a box $[-B, B]^n$ "large enough"…



The leakage

With $\vec{s}, \vec{r} \xleftarrow{\$} [-B, B]^n$, the distribution of $\vec{r} - \vec{s}$ depends on the long term secret $\vec{s}$!

The two fixes

Do like the lattice people

SeaSign: D. and Galbraith 2019

- Use Fiat–Shamir with aborts (Lyubashevsky 2009).
  - Huge increase in signature size and time.
- Compromise signature size/time with public key size (still slow).

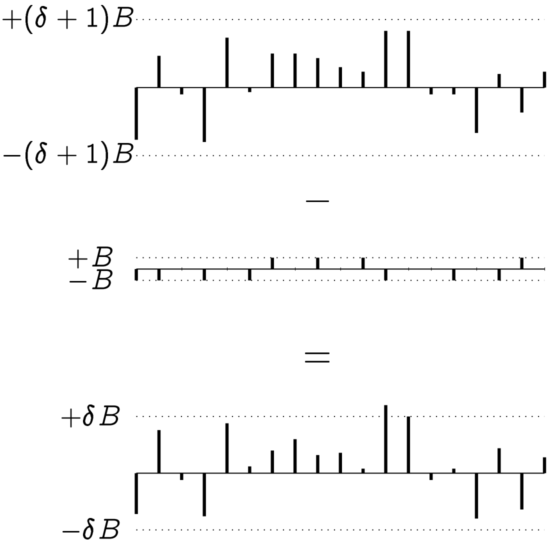
Compute the group structure and stop whining

CSI-FiSh: Beullens, Kleinjung and Vercauteren 2019

- Already suggested by Couveignes (1996) and Stolbunov (2006).
- Computationally intensive (subexponential parameter generation).
- Decent parameters, e.g.: 263 bytes, 390 ms, @NIST-1.
  - Technically not post-quantum (signing requires solving ApproxCVP).

Rejection sampling

- Sample long term secret $\vec{s}$ in the usual box $[-B, B]^n$,
- Sample ephemeral $\vec{r}$ in a larger box $[-(\delta+1)B, (\delta+1)B]^n$,
- Throw away $\vec{r} - \vec{s}$ if it is out of the box $[-\delta B, \delta B]^n$.



Zero-knowledge

Theorem: $\vec{r} - \vec{s}$ is uniformly distributed in $[-\delta B, \delta B]^n$.

Problem: set δ so that rejection probability is low.

SeaSign Performance (NIST-1)

	$t = 1$ **bit challenges**	$t = 16$ **bits challenges**	**PK compression**
Sig size	20 KiB	978 B	3136 B
PK size	64 B	4 MiB	32 B
SK size	32 B	16 B	1 MiB
Est. keygen time	30 ms	30 mins	30 mins
Est. sign time	30 hours	6 mins	6 mins
Est. verify time	10 hours	2 mins	2 mins
Asymptotic sig size	$O(\lambda^2 \log(\lambda))$	$O(\lambda t \log(\lambda))$	$O(\lambda^2 t)$

Speed/size compromises by Decru, Panny and Vercauteren 2019

Sig size	36 KiB	2 KiB	—
Est. sign time	30 mins	80 s	—
Est. verify time	20 mins	20 s	—

CSI-FiSh[5]

- Record breaking class group computation for CSIDH-512, hard to scale to larger primes;
- Effectively (but not asymptotically) makes CSIDH into an HHS:
  - Compatible with secret sharing in the exponent, yields decent threshold signatures.[4]

S	t	k	$\|\mathrm{sk}\|$	$\|\mathrm{sk}\|$	$\|\mathrm{sig}\|$	KeyGen	Sign	Verify
2^1	56	16	16 B	128 B	1880 B	100 ms	2.92 s	2.92 s
2^2	38	14	16 B	256 B	1286 B	200 ms	1.98 s	1.97 s
2^3	28	16	16 B	512 B	956 B	400 ms	1.48 s	1.48 s
2^4	23	13	16 B	1 KB	791 B	810 ms	1.20 s	1.19 s
2^6	16	16	16 B	4 KB	560 B	3.3 s	862 ms	859 ms
2^8	13	11	16 B	16 KB	461 B	13 s	671 ms	670 ms
2^{10}	11	7	16 B	64 KB	395 B	52 s	569 ms	567 ms
2^{12}	9	11	16 B	256 KB	329 B	3.5 m	471 ms	469 ms
2^{15}	7	16	16 B	2 MB	263 B	28 m	395 ms	393 ms

[4] De Feo and Meyer 2019.
[5] Beullens, Kleinjung, and Vercauteren 2019.

A Σ-protocol for SIDH

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

$\frac{1}{3}$-soundness

Secret ϕ of degree $\ell_A^{e_A}$.

A Σ-protocol for SIDH

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

$\frac{1}{3}$-soundness

Secret ϕ of degree $\ell_A^{e_A}$.

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

A Σ-protocol for SIDH

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

$\frac{1}{3}$-soundness

Secret ϕ of degree $\ell_A^{e_A}$.

1. Choose a random point $P \in E[\ell_B^{e_B}]$, compute the diagram;
2. Publish the curves $E/\langle P\rangle$ and $E/\langle P, S\rangle$;
3. The verifier challenges to reveal one out of the 3 sides
   - Isogenies ψ, ψ' (degree $\ell_B^{e_B}$) unrelated to secret;

A Σ-protocol for SIDH

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

$\frac{1}{3}$-soundness

Secret ϕ of degree $\ell_A^{e_A}$.

1. Choose a random point $P \in E[\ell_B^{e_B}]$, compute the diagram;
2. Publish the curves $E/\langle P\rangle$ and $E/\langle P, S\rangle$;
3. The verifier challenges to reveal one out of the 3 sides
   - Isogenies ψ, ψ' (degree $\ell_B^{e_B}$) unrelated to secret;

A Σ-protocol for SIDH

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

$\frac{1}{3}$-soundness

Secret ϕ of degree $\ell_A^{e_A}$.

1. Choose a random point $P \in E[\ell_B^{e_B}]$, compute the diagram;
2. Publish the curves $E/\langle P\rangle$ and $E/\langle P, S\rangle$;
3. The verifier challenges to reveal one out of the 3 sides
   - Isogenies ψ, ψ' (degree $\ell_B^{e_B}$) unrelated to secret;
   - Isogeny ϕ' conjectured to not reveal useful information on ϕ.

A Σ-protocol for SIDH

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

$\frac{1}{3}$-soundness

Secret ϕ of degree $\ell_A^{e_A}$.

1. Choose a random point $P \in E[\ell_B^{e_B}]$, compute the diagram;
2. Publish the curves $E/\langle P\rangle$ and $E/\langle P, S\rangle$;
3. The verifier challenges to reveal one out of the 3 sides
   - Isogenies ψ, ψ' (degree $\ell_B^{e_B}$) unrelated to secret;
   - Isogeny ϕ' conjectured to not reveal useful information on ϕ.

Improving to $\frac{1}{2}$-soundness

- Reveal ψ, ψ' simultaneously;
- Reveals action of ϕ on $E[\ell_B^{e_B}]$ $\Rightarrow$ Stronger security assumption.

SIDH signature performance (NIST-1)

According to Yoo, Azarderakhsh, Jalali, Jao and Vladimir Soukharev 2017:

Size: $\approx 100KB$,

Time: seconds.

SIDH signature performance (NIST-1)

According to Yoo, Azarderakhsh, Jalali, Jao and Vladimir Soukharev 2017:

Size: $\approx 100KB$,

Time: seconds.

Galbraith, Petit and Silva 2017

- Concept similar to CSI-FiSh: exploits known structure of endomorphism ring;
- Statistical zero knowledge (under heuristic assumptions);
- Based on the generic isogeny walk problem (requires special starting curve, though);
- Size/performance comparable to Yoo *et al.* (and possibly slower).

Verifiable delay functions[6]

Wanted

Function (family) $f : X \to Y$ s.t.:

- Evaluating $f(x)$ takes long time:
  - uniformly long time,
  - on almost all random inputs x,
  - even after having seen many values of $f(x')$,
  - even given massive number of processors;
- Verifying $y = f(x)$ is efficient:
  - ideally, exponential separation between evaluation and verification.

Why?

- Distributed lottery;
- Distributed consensus protocols (blockchains);
- ...

[6] Boneh, Bonneau, Bünz, and Fisch 2018.

Weil pairing and isogenies

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

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

Isogeny VDF[7]

Idea

Evaluation: Evaluate a long chain of isogenies at a random point.

Verification: Check a pairing equation.

- Verification time independent of the length of the isogeny chain.
- Constraints:
  - Pairing friendly curves,
  - Large field size for pairing security,
  - Must be difficult to find “shortcuts”:
    - Large isogeny graph,
    - Unknown endomorphism rings $\Rightarrow$ Trusted setup!

$\Rightarrow$ Supersingular curves over $\approx$ 1500 bit fields.

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

Conclusion

- Repeat with me: I need isogeny-based crypto!
- Different isogeny graphs enable different applications, different security assumptions.
- Public key encryption based on isogenies is a reality, although maybe not your #1 choice for TLS.
- Post-quantum isogeny signatures are still far from practical.
- Practical isogeny signatures do exists (CSI-FiSh); you can start using them now if you are an isogeny hippie, are ok for threshold signatures, but they do not scale.
- Pairing-based isogeny proofs are usable, but not interesting for signatures: look into succinctness, instead!

Thank you

`https://defeo.lu/`

@luca_defeo

Article citations I

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

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 II

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 III

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.

Article citations IV

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.

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.

Article citations V

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.

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.

Article citations VI

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.

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.

Article citations VII

De Feo, Luca and Michael Meyer (2019).
Threshold Schemes from Isogeny Assumptions.
Cryptology ePrint Archive, Report 2019/1288.
URL: https://eprint.iacr.org/2019/1288.

Beullens, Ward, Thorsten Kleinjung, and Frederik Vercauteren (2019).
CSI-FiSh: Efficient Isogeny based Signatures through Class Group Computations.
Cryptology ePrint Archive, Report 2019/498.
https://eprint.iacr.org/2019/498.

Boneh, Dan, Joseph Bonneau, Benedikt Bünz, and Ben Fisch (2018).
"Verifiable Delay Functions."
In: Advances in Cryptology – CRYPTO 2018.
Ed. by Hovav Shacham and Alexandra Boldyreva.
Cham: Springer International Publishing,
Pp. 757–788.

Article citations VIII

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.