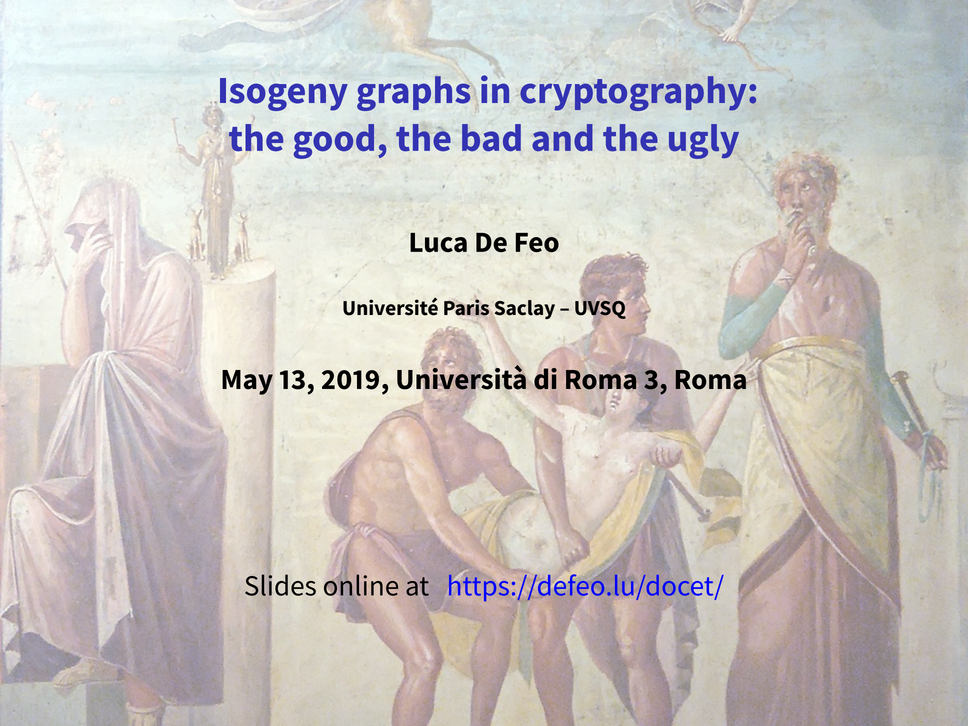


Isogeny graphs in cryptography: the good, the bad and the ugly

Luca De Feo

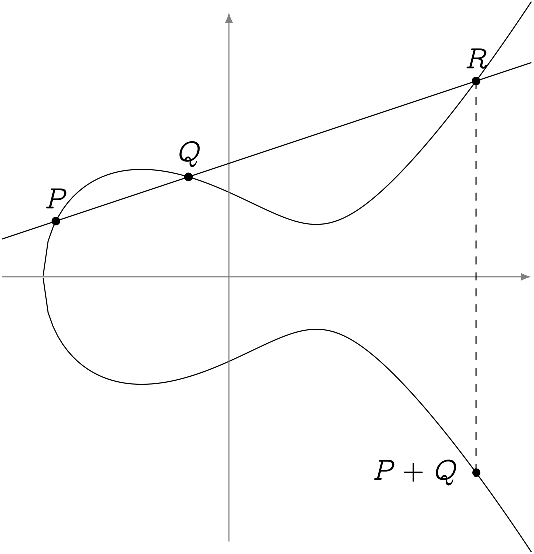
Université Paris Saclay – UVSQ

May 13, 2019, Università di Roma 3, Roma

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

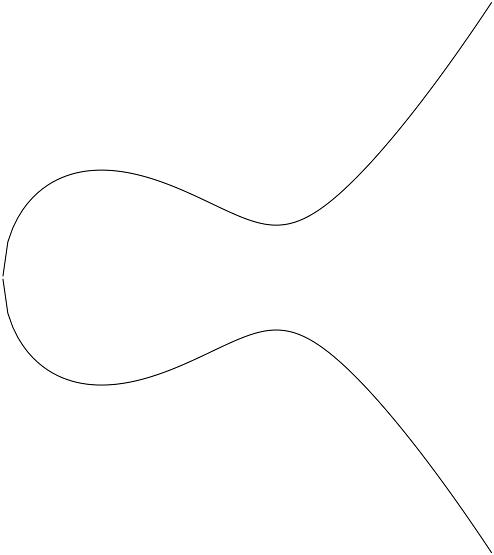
Elliptic curves

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



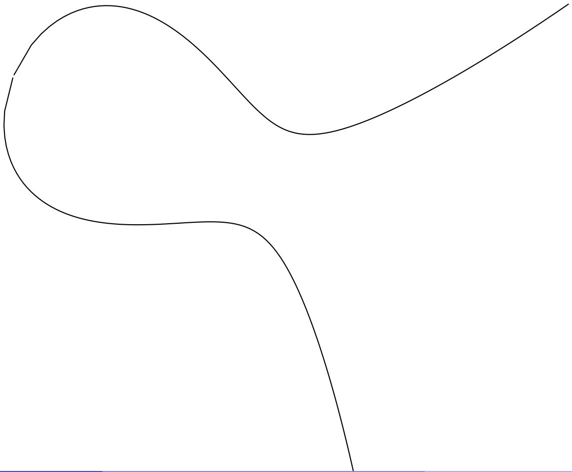
Elliptic curves

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



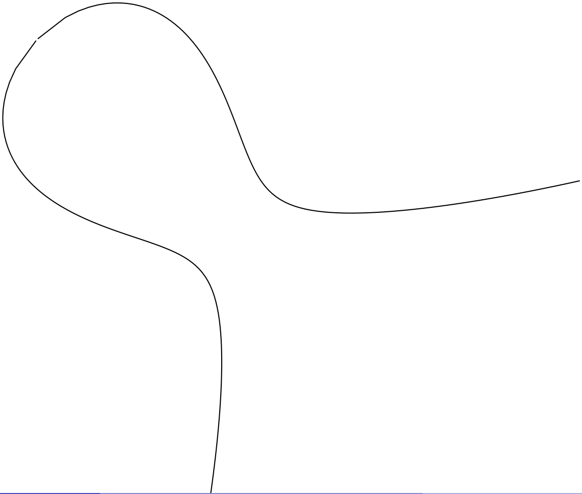
Elliptic curves

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



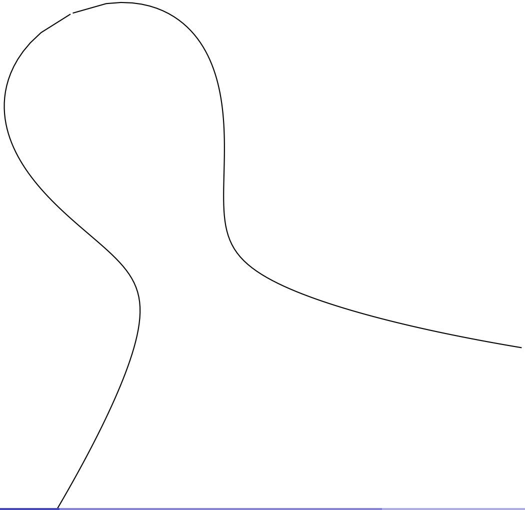
Elliptic curves

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



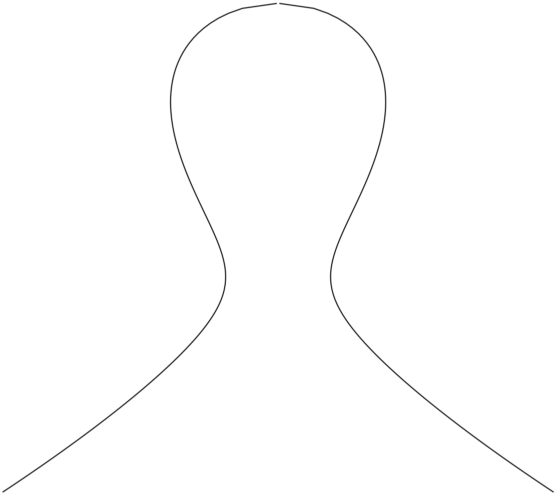
Elliptic curves

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



Elliptic curves

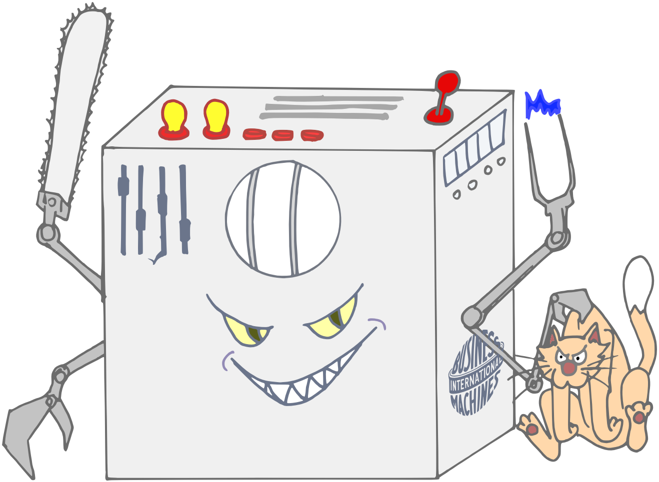
Let $E : y^2 = x^3 + ax + b$ be an elliptic curve…



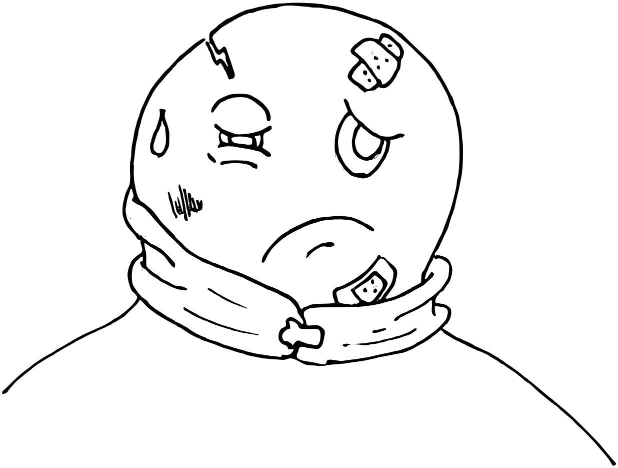
Elliptic curves

I power 70% of WWW traffic!

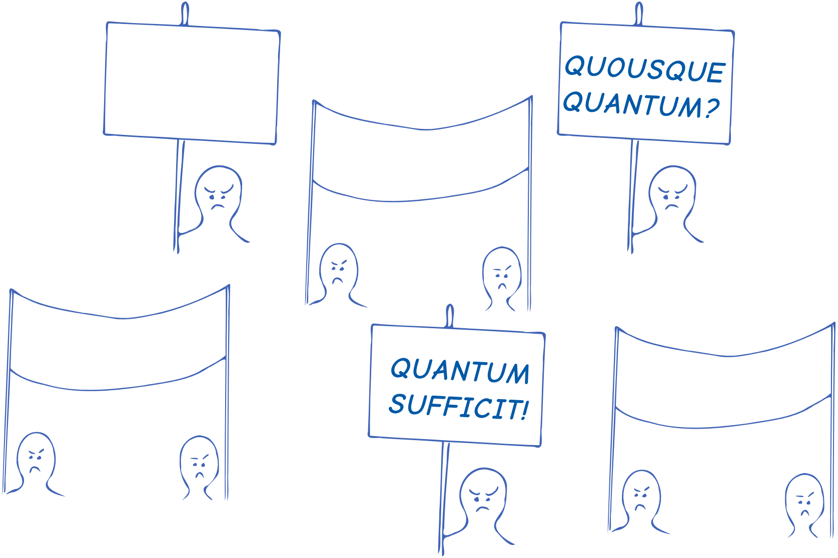
The Q Menace



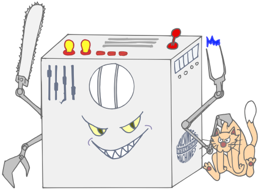
Post-quantum cryptographer?



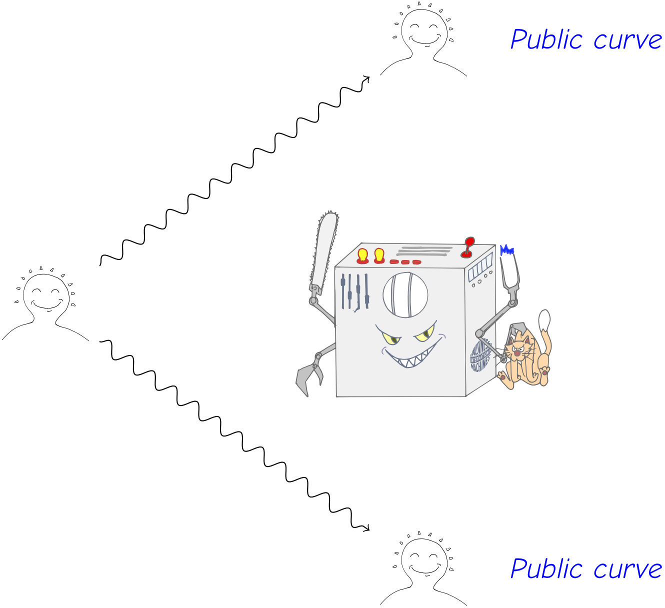
Elliptic curves of the world, UNITE!



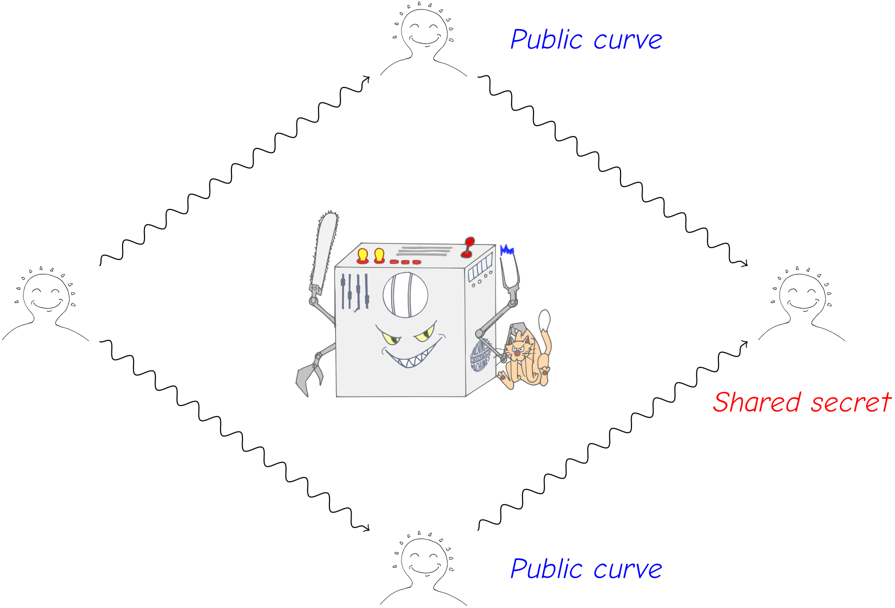
And so, they found a way around the Q...



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



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



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.

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.

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.

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.

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.

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 $\cancel{m^2}\ \#H$.

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~~ $\cancel{E[m]} \cancel{\simeq} \cancel{(\mathbb{Z}/m\mathbb{Z})^2}$ 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:

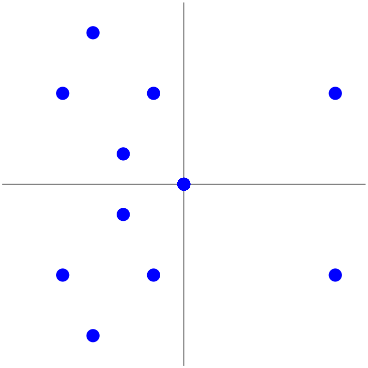
$$0 \to H \to E \xrightarrow{\phi} E' \to 0$$

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

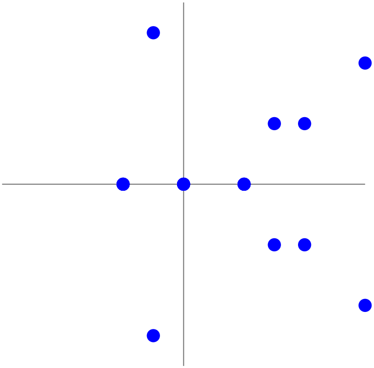
$$E/H \stackrel{\text{def}}{=} E'.$$

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

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



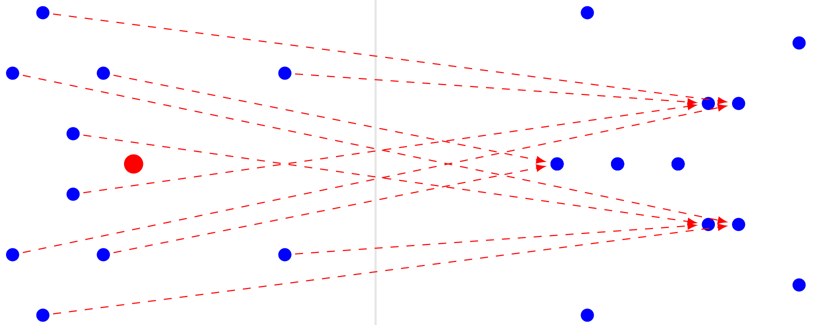
$$E' \ : \ y^2 = x^3 - 4x$$



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

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

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



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

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

Computing Isogenies

Vélu's formulas

Input: A subgroup $H \subset E$,

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

Complexity: $O(\ell)$ — Vélu 1971, …

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

Computing Isogenies

Vélu's formulas

Input: A subgroup $H \subset E$,

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

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

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

Explicit Isogeny Problem

Input: Curve E, (prime) integer ℓ

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

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

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

Computing Isogenies

Explicit Isogeny Problem (2)

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

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

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

Why?
- Count points of elliptic curves.

Computing Isogenies

Explicit Isogeny Problem (2)

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

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

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

Why?
- Count points of elliptic curves.

Isogeny Walk Problem

Input: Isogenous curves E, E'.

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

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

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

History of isogeny-based cryptography

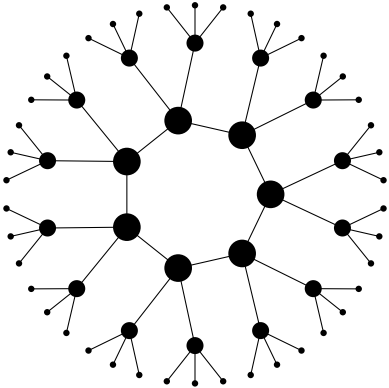
1996	Couveignes introduces Hard Homogeneous Spaces. His work stays unpublished for 10 years.
2006	Rostovtsev & Stolbunov independently rediscover Couveignes ideas, suggest isogeny-based Diffie–Hellman as a quantum-resistant primitive.
2006-2010	Other isogeny-based protocols by Teske and Charles, Goren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

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.



Endomorphisms

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.

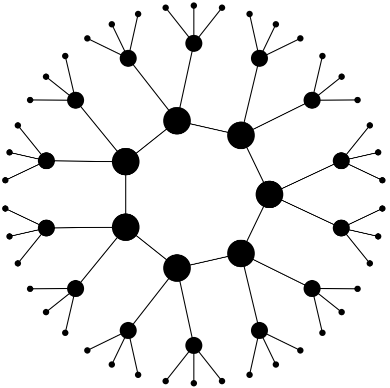
- Any order $\mathcal{O} \subset K$ can be written as $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$ for an integer f, called the conductor of $\mathcal{O}$, denoted by $[\mathcal{O}_K : \mathcal{O}]$.
- If D_K is the discriminant of K, the discriminant of $\mathcal{O}$ is $f^2 D_K$.
- If $\mathcal{O},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

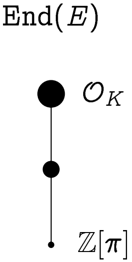
$$\begin{tikzcd}
 & \mathcal{O}_K \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Z} + 2\mathcal{O}_K \arrow[d, dash] \arrow[dr, dash] & \mathbb{Z} + 3\mathcal{O}_K \arrow[dl, dash] \arrow[dr, dash] & \mathbb{Z} + 5\mathcal{O}_K \arrow[dl, dash] \arrow[d, dash] \\
\mathbb{Z} + 6\mathcal{O}_K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

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.



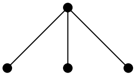


Ordinary isogeny volcano of degree $\ell = 3$.

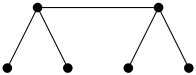
Volcanology (Kohel 1996)

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

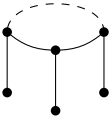
$\mathcal{O}_K$: maximal order of K,
D_K: discriminant of K.



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



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



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

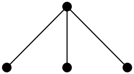
		Horizontal	**Ascending**	**Descending**
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$	$1 + \left(\frac{D_K}{\ell}\right)$		
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O} : \mathbb{Z}[\pi]]$	$1 + \left(\frac{D_K}{\ell}\right)$		$\ell - \left(\frac{D_K}{\ell}\right)$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

Volcanology (Kohel 1996)

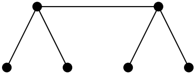
Let E be ordinary,
$\mathrm{End}(E) \subset K$.

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

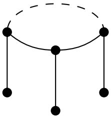
Height $= v_\ell([\mathcal{O}_K : \mathbb{Z}[\pi]])$.



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



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



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

		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	

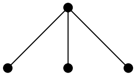
Volcanology (Kohel 1996)

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

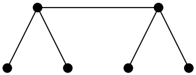
$\mathcal{O}_K$: maximal order of K,
D_K: discriminant of K.

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

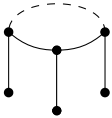
How large is the crater?



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



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



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

		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	

How large is the crater of a volcano?

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

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

The class group

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

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

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

Complex multiplication

The $\mathfrak{a}$-torsion

- Let $\mathfrak{a} \subset \mathcal{O}$ be an (integral invertible) ideal of $\mathcal{O}$;
- Let $E[\mathfrak{a}]$ be the subgroup of E annihilated by $\mathfrak{a}$:
$$E[\mathfrak{a}] = \{P \in E \mid \alpha(P) = 0 \text{ for all } \alpha \in \mathfrak{a}\};$$
- Let $\phi : E \to E_{\mathfrak{a}}$, where $E_{\mathfrak{a}} = E/E[\mathfrak{a}]$.

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

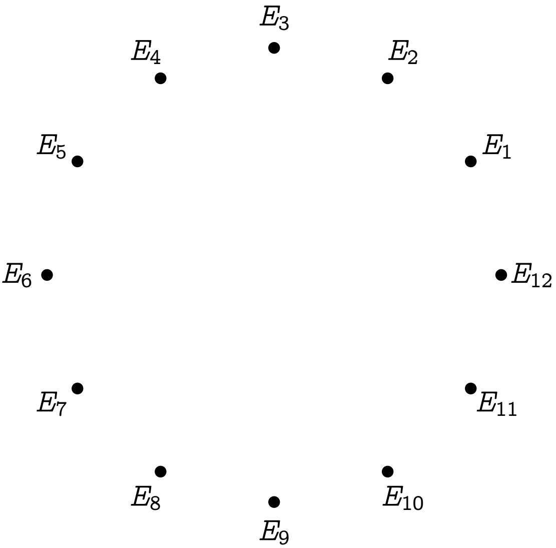
Theorem (Complex multiplication)

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

Corollary

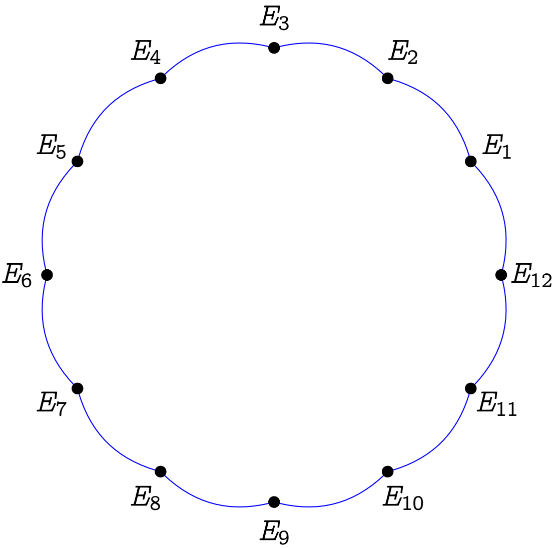
Let $\mathrm{End}(E)$ have discriminant D. Assume that $\left(\frac{D}{\ell}\right) = 1$, then E is on a crater of size N of an ℓ-volcano, and $N | h(\mathrm{End}(E))$

Complex multiplication graphs



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

Complex multiplication graphs

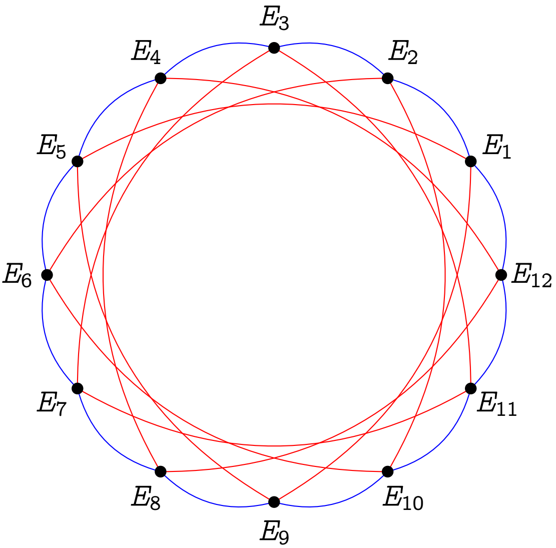


Vertices are elliptic curves with complex multiplication by $\mathcal{O}_K$ (i.e., $\mathrm{End}(E) \simeq \mathcal{O}_K \subset \mathbb{Q}(\sqrt{-D})$).

Edges are horizontal isogenies of bounded prime degree.

— degree 2

Complex multiplication graphs



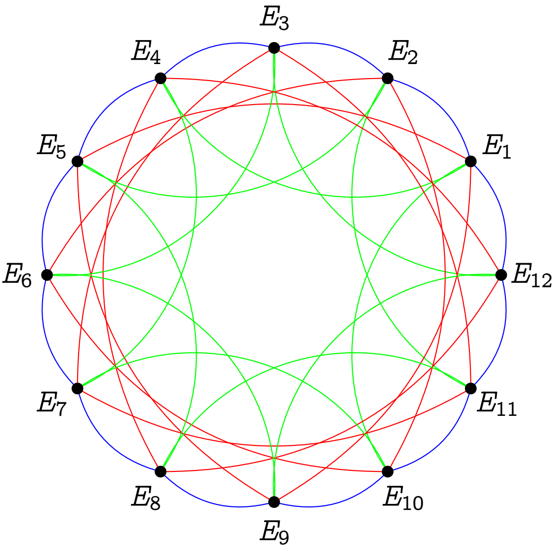
Vertices are elliptic curves with complex multiplication by $\mathcal{O}_K$ (i.e., $\mathtt{End}(E) \simeq \mathcal{O}_K \subset \mathbb{Q}(\sqrt{-D})$).

Edges are horizontal isogenies of bounded prime degree.

— degree 2

— degree 3

Complex multiplication graphs



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

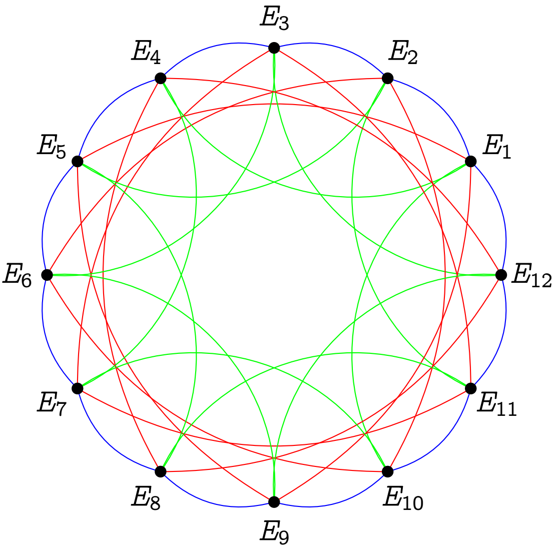
Edges are horizontal isogenies of bounded prime degree.

— degree 2

— degree 3

— degree 5

Complex multiplication graphs

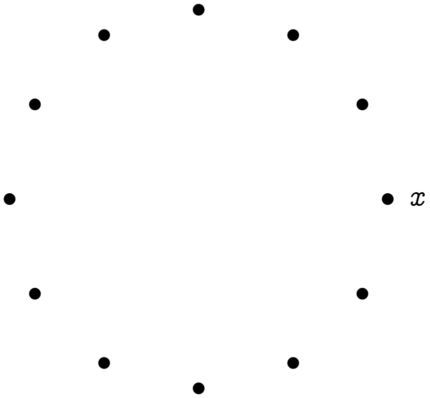


Vertices are elliptic curves with complex multiplication by $\mathcal{O}_K$ (i.e., $\mathrm{End}(E) \simeq \mathcal{O}_K \subset \mathbb{Q}(\sqrt{-D})$).

Edges are horizontal isogenies of bounded prime degree.

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

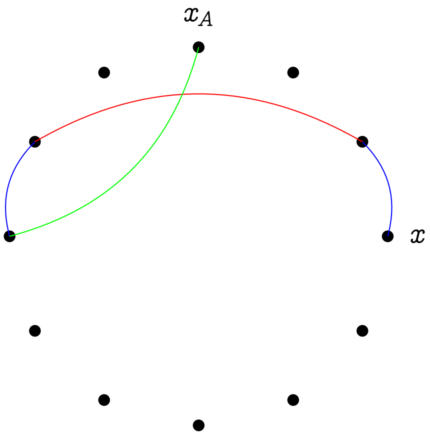
Key exchange from Cayley graphs



Public parameters:

- A commutative group G acting on a set X;
- A starting point $x \in X$;
- A subset $G \supset S = \{s_1, s_2, s_3, \dots\}$.

Key exchange from Cayley graphs

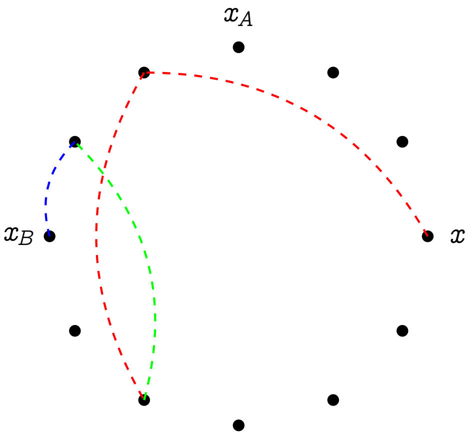


Public parameters:

- A commutative group G acting on a set X;
- A starting point $x \in X$;
- A subset $G \supset S = \{s_1, s_2, s_3, \dots\}$.

1. **Alice** takes a secret random walk $s_A = s_1^{e_1} \cdot s_2^{e_2} \cdot s_3^{e_3} \cdots$ landing on $x_A = s_A * x$;

Key exchange from Cayley graphs

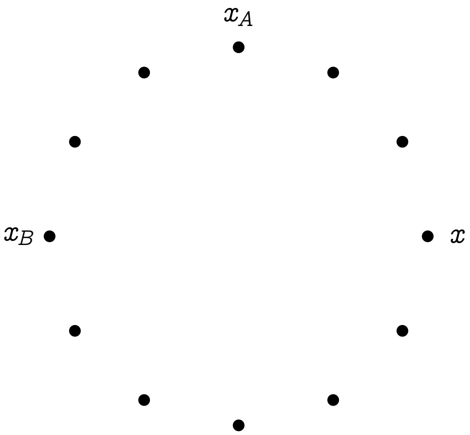


Public parameters:

- A commutative group G acting on a set X;
- A starting point $x \in X$;
- A subset $G \supset S = \{s_1, s_2, s_3, \dots\}$.

1. **Alice** takes a secret random walk $s_A = s_1^{e_1} \cdot s_2^{e_2} \cdot s_3^{e_3} \cdots$ landing on $x_A = s_A * x$;
2. **Bob** does the same;

Key exchange from Cayley graphs

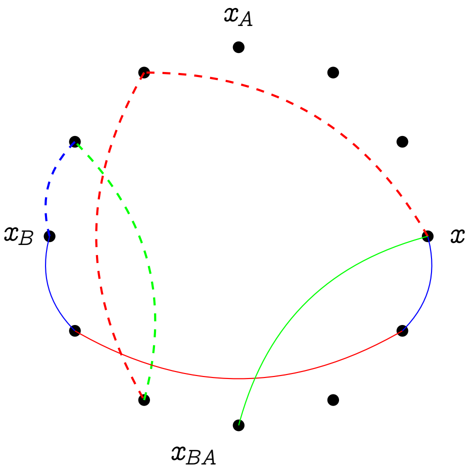


Public parameters:

- A commutative group G acting on a set X;
- A starting point $x \in X$;
- A subset $G \supset S = \{s_1, s_2, s_3, \dots\}$.

1. **Alice** takes a secret random walk $s_A = s_1^{e_1} \cdot s_2^{e_2} \cdot s_3^{e_3} \cdots$ landing on $x_A = s_A * x$;
2. **Bob** does the same;
3. They publish x_A and x_B;

Key exchange from Cayley graphs

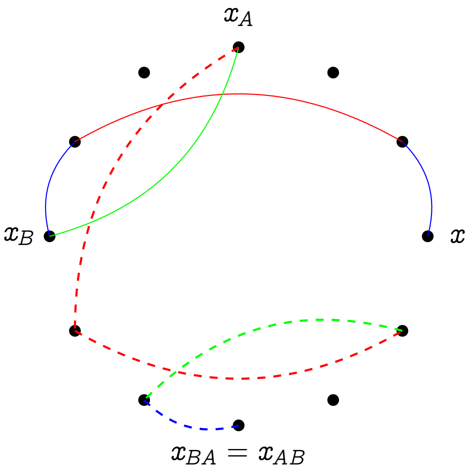


Public parameters:

- A commutative group G acting on a set X;
- A starting point $x \in X$;
- A subset $G \supset S = \{s_1, s_2, s_3, \dots\}$.

1. **Alice** takes a secret random walk $s_A = s_1^{e_1} \cdot s_2^{e_2} \cdot s_3^{e_3} \cdots$ landing on $x_A = s_A * x$;
2. **Bob** does the same;
3. They publish x_A and x_B;
4. **Alice** repeats her secret walk s_A starting from x_B.

Key exchange from Cayley graphs

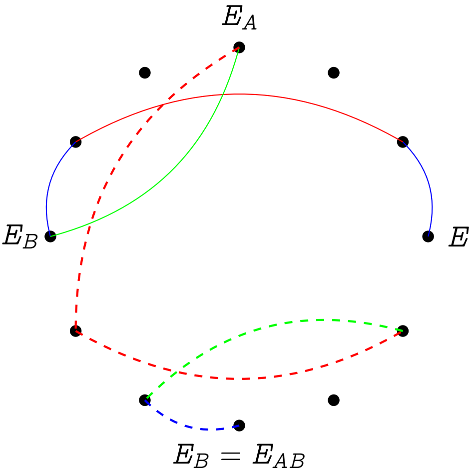


Public parameters:

- A commutative group G acting on a set X;
- A starting point $x \in X$;
- A subset $G \supset S = \{s_1, s_2, s_3, \dots\}$.

1. **Alice** takes a secret random walk $s_A = s_1^{e_1} \cdot s_2^{e_2} \cdot s_3^{e_3} \cdots$ landing on $x_A = s_A * x$;
2. **Bob** does the same;
3. They publish x_A and x_B;
4. **Alice** repeats her secret walk s_A starting from x_B.
5. **Bob** repeats his secret walk s_B starting from x_A.

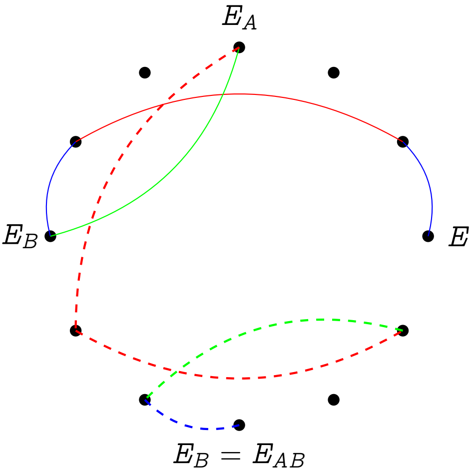
Couveignes–Rostovtsev–Stolbunov key exchange



Now, with isogenies

- $G = \mathrm{Cl}(\mathcal{O}_K)$, a class group;
- $X =$ elliptic curves with CM by $\mathcal{O}_K$;
- A starting curve E;
- $S =$ set of small degree isogenies.

Couveignes–Rostovtsev–Stolbunov key exchange

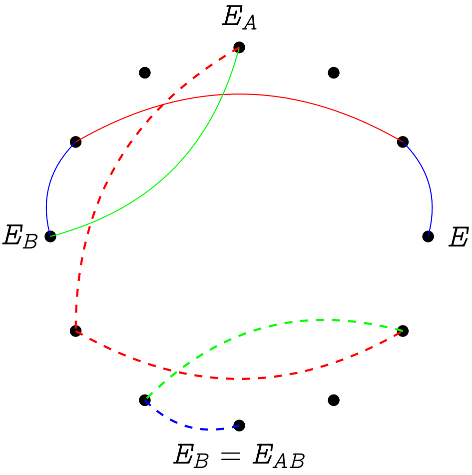


Now, with isogenies

- $G = \mathrm{Cl}(\mathcal{O}_K)$, a class group;
- $X =$ elliptic curves with CM by $\mathcal{O}_K$;
- A starting curve E;
- $S =$ set of small degree isogenies.

But why?!

Couveignes–Rostovtsev–Stolbunov key exchange



Now, with isogenies

- $G = \mathrm{Cl}(\mathcal{O}_K)$, a class group;
- X = elliptic curves with CM by $\mathcal{O}_K$;
- A starting curve E;
- S = set of small degree isogenies.

But why?!

Because the Shor/Kitaev quantum algorithm does not apply to Diffie-Hellman on Cayley graphs!

CSIDH (pron.: *sea-side*)

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

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

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

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

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.

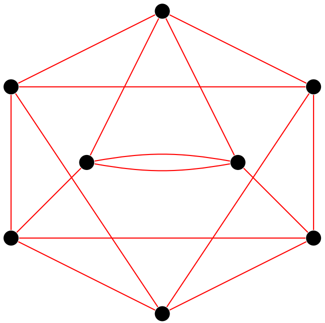


Figure: 3-isogeny graph on $\mathbb{F}_{97^2}$.

Key exchange with full supersingular graphs (over $\mathbb{F}_{p^2}$)

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.

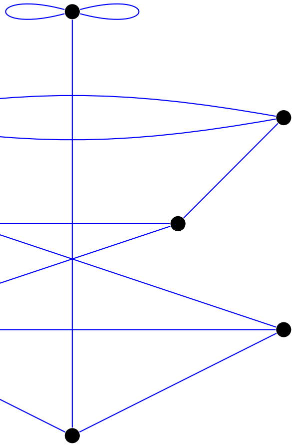


Figure: 2- and 3-isogeny graphs on $\mathbb{F}_{97^2}$.

Key exchange with full supersingular graphs (over $\mathbb{F}_{p^2}$)

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.

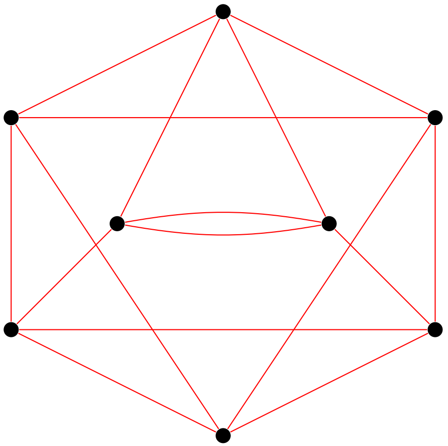


Figure: 2- and 3-isogeny graphs on $\mathbb{F}_{97^2}$.

Key exchange with full supersingular graphs (over $\mathbb{F}_{p^2}$)

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.

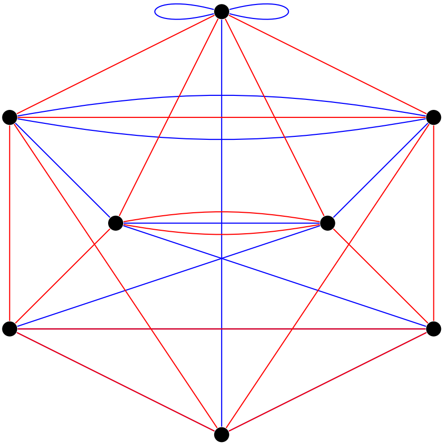


Figure: 2- and 3-isogeny graphs on $\mathbb{F}_{97^2}$.

Key exchange with full supersingular graphs (over $\mathbb{F}_{p^2}$)

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

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

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

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

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

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

SIKE: Supersingular Isogeny Key Encapsulation

- Submission to the NIST PQ competition:
  - SIKE.PKE: El Gamal-type system with IND-CPA security proof,
  - SIKE.KEM: generically transformed system with IND-CCA security proof.
- Security levels 1, 3 and 5.
- Smallest communication complexity among all proposals in each level.
- Slowest among all benchmarked proposals in each level.
- A team of 14 submitters, from 8 universities and companies.
- Visit https://sike.org/.

	p	cl. security	q. security	speed	comm.
SIKEp503	$2^{250}3^{159}-1$	126 bits	84 bits	10ms	0.4KB
SIKEp751	$2^{372}3^{239}-1$	188 bits	125 bits	30ms	0.6KB
SIKEp964	$2^{486}3^{301}-1$	241 bits	161 bits		0.8KB

From 10 minutes to 10ms in 20 years

Couveignes' key exchange

1996

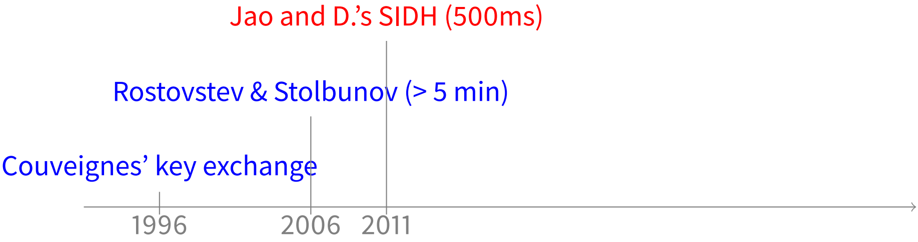
From 10 minutes to 10ms in 20 years

Rostovstev & Stolbunov (> 5 min)

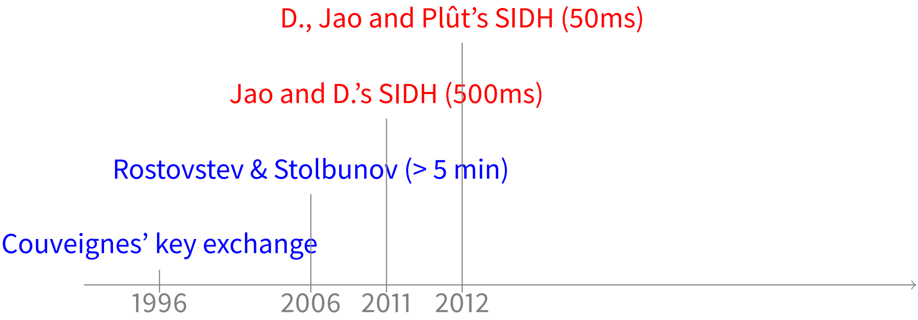
Couveignes' key exchange

1996 2006

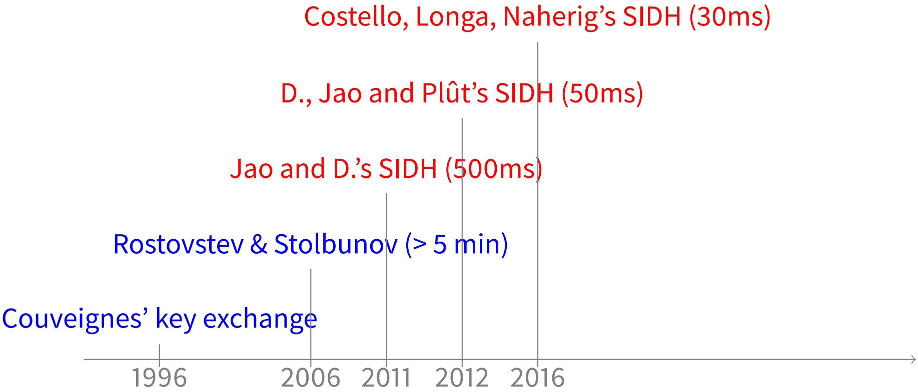
From 10 minutes to 10ms in 20 years



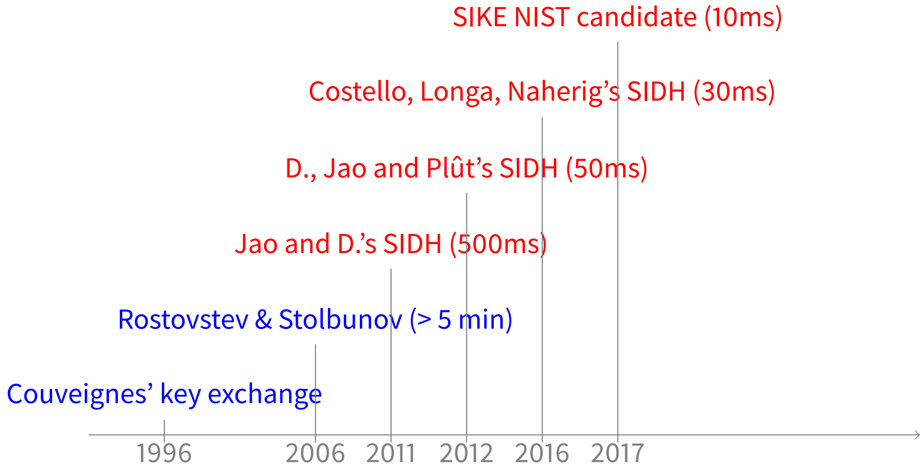
From 10 minutes to 10ms in 20 years



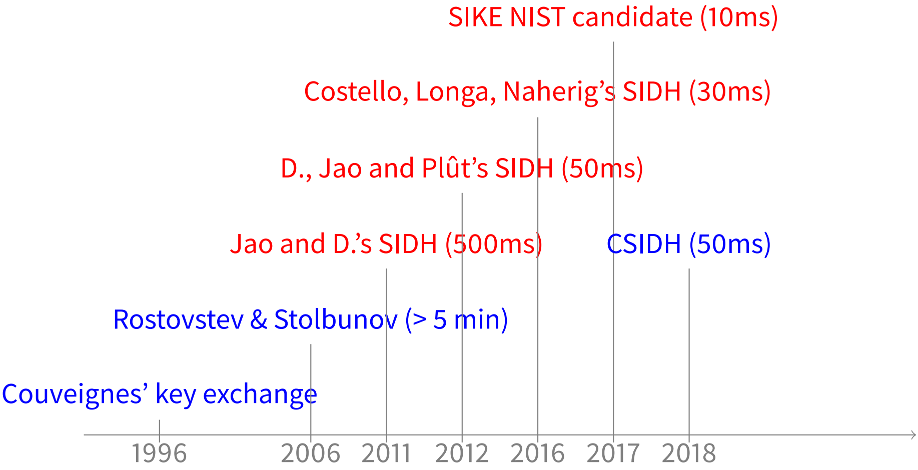
From 10 minutes to 10ms in 20 years



From 10 minutes to 10ms in 20 years



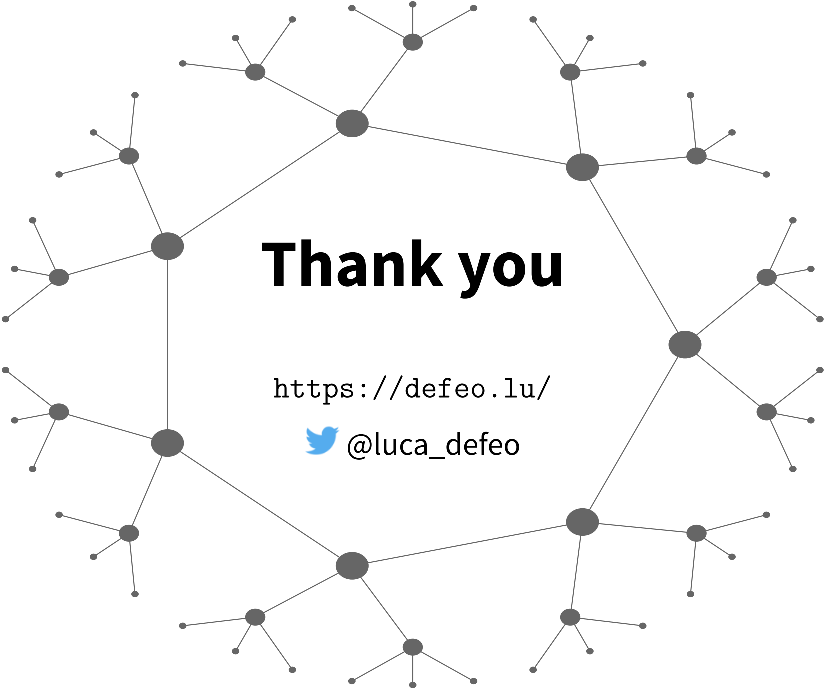
From 10 minutes to 10ms in 20 years



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

CSIDH vs SIDH

	CSIDH	SIDH
Speed (NIST 1)	<100ms	$\sim$ 10ms
Public key size (NIST 1)	64B	378B
Key compression[1]		
↳ speed		$\sim$ 15ms[2]
↳ size		222B
Constant time impl.	not yet	yes
Submitted to NIST	no	yes
Best classical attack	$p^{1/4}$	$p^{1/4}$
Best quantum attack	$\tilde{O}\left(3^{\sqrt{\log_3 p}}\right)$	$p^{1/6}$
Key size scales	quadratically	linearly
Security assumption	isogeny walk problem	ad hoc
CPA security	yes	yes
CCA security	yes	Fujisaki-Okamoto
Non-interactive key ex.	yes	no
Signatures	short but slooow!	big and slow

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

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

Signatures (a different story)

- No analogue of Schnorr signatures for DH on Cayley graphs.
- All known isogeny constructions are basic Fiat-Shamir applied to zero-knowledge identification protocols.

SIDH signatures

- Identification protocol also proposed by D.F., Jao, Plût;
- Only one bit per iteration $\rightarrow$ 128 iterations of SIDH primitive;
- Slow, large signatures;
- Even slower variants by Galbraith, Petit, and Silva 2016.

CSIDH signatures (SeaSign)

- (Flawed) id protocol already realized by Couveignes, Stolbunov;
- SeaSign (De Feo and Galbraith 2019): fixes flaw using Fiat-Shamir with aborts (Lyubashevsky 2009) (+ hash trees);
- Small signatures, still extremely slow (minutes).

Article citations I

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.

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.

Article citations II

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.

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 III

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 IV

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 V

Zanon, Gustavo H. M., Marcos A. Simplicio, Geovandro C. C. F. Pereira, Javad Doliskani, and Paulo S. L. M. Barreto (2018). "Faster Isogeny-Based Compressed Key Agreement." In: Post-Quantum Cryptography. Ed. by Tanja Lange and Rainer Steinwandt. Cham: Springer International Publishing, Pp. 248–268.

Galbraith, Steven D., Christophe Petit, and Javier Silva (2016). Signature Schemes Based On Supersingular Isogeny Problems. Cryptology ePrint Archive, Report 2016/1154. http://eprint.iacr.org/2016/1154.

De Feo, Luca and Steven D. Galbraith (2019). "SeaSign: Compact isogeny signatures from class group actions." In: Eurocrypt 2019.

Article citations VI

Lyubashevsky, Vadim (2009).
"Fiat-Shamir with Aborts: Applications to Lattice and Factoring-Based Signatures."
In: ASIACRYPT 2009.
Ed. by M. Matsui.
Vol. 5912.
LNCS.
Springer,
Pp. 598–616.