# Isogeny Based Cryptography
## the new frontier of number theoretic cryptography

Luca De Feo
IBM Research Zürich

February 17, 2021
Annual Iranian Mathematics Conference 2021

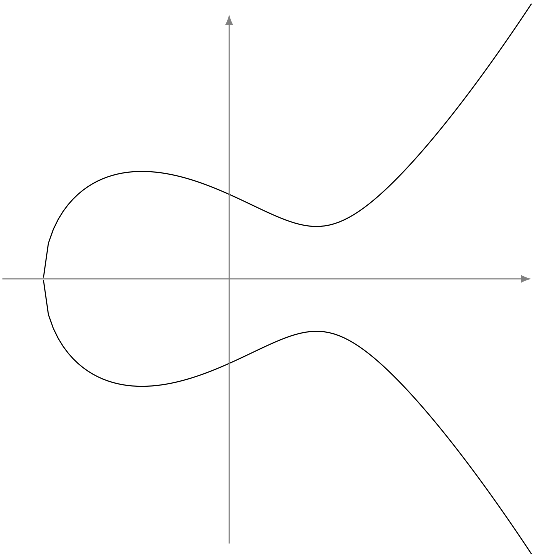
# Elliptic curves

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

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

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

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



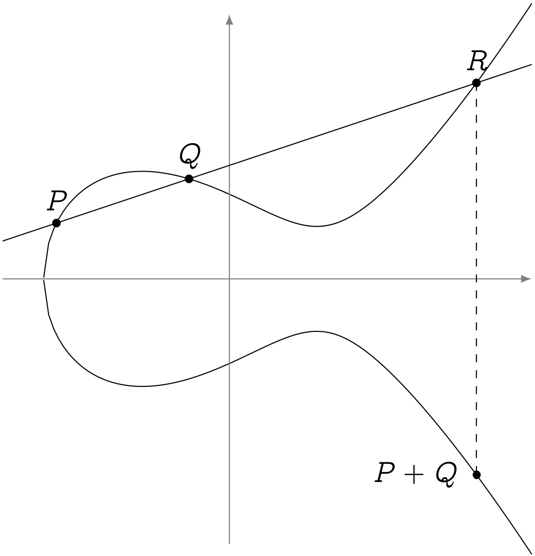
# The group law

## Bezout's theorem

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

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

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



# Why do cryptographers care? (Diffie–Hellman key exchange)

Goal: Alice and Bob have never met before. They are chatting over a public channel, and want to agree on a shared secret to start a private conversation.

Setup: They agree on a (large) cyclic group $G = \langle g \rangle$ of order $N$.

| **Alice** | | **Bob** |
|---|---|---|
| pick random $a \in \mathbb{Z}/N\mathbb{Z}$ | | pick random $b \in \mathbb{Z}/N\mathbb{Z}$ |
| compute $A = g^a$ | $\xrightarrow{\quad A \quad}$ | compute $B = g^b$ |
| | $\xleftarrow[\quad B \quad]{}$ | |

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

# Brief history of DH key exchange

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

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

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

1994 Shor publishes his quantum discrete logarithm / factoring algorithm.

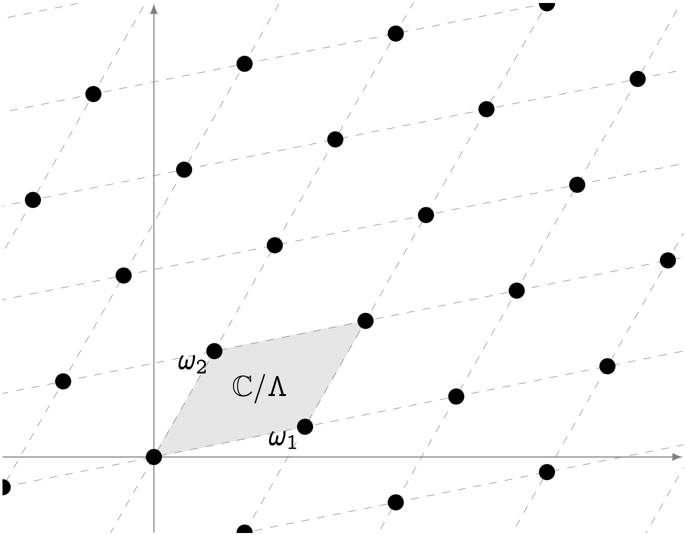
2005 NSA standardizes elliptic curve key agreement (ECDH) and signatures ECDSA.

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

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

2020 NIST calls the finalists for the competition. Elliptic curves are still running, thanks to SIKE, the Supersingular Isogeny Key Encapsulation scheme.

# Elliptic curves

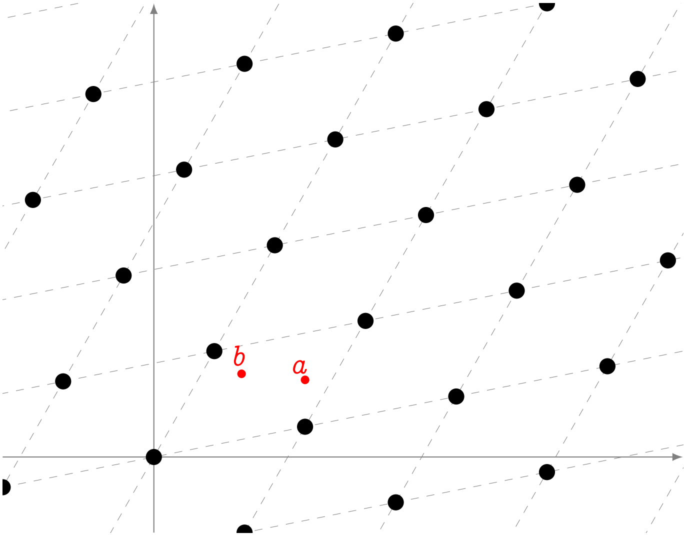



Let $\omega_1, \omega_2 \in \mathbb{C}$ be linearly independent complex numbers. Set

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

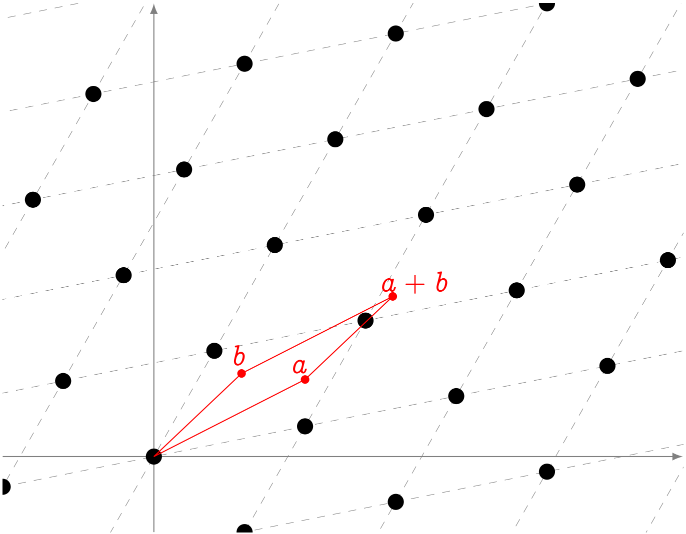
$\mathbb{C}/\Lambda$ is an elliptic curve.

# Elliptic curves



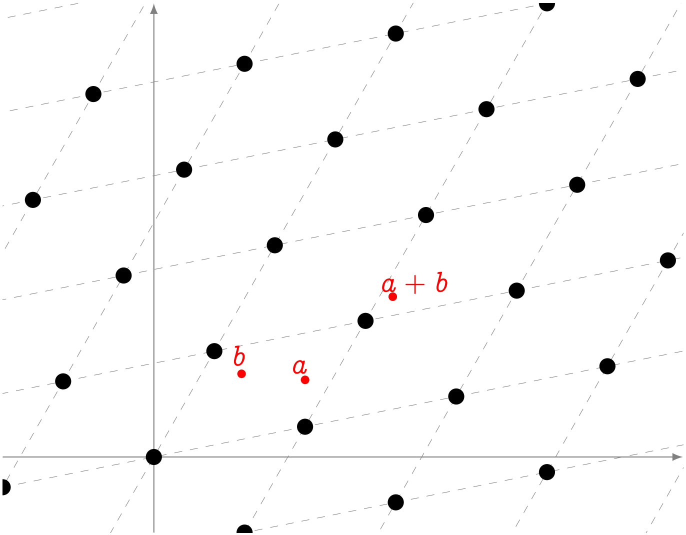

Addition law induced by addition on $\mathbb{C}$.

# Elliptic curves



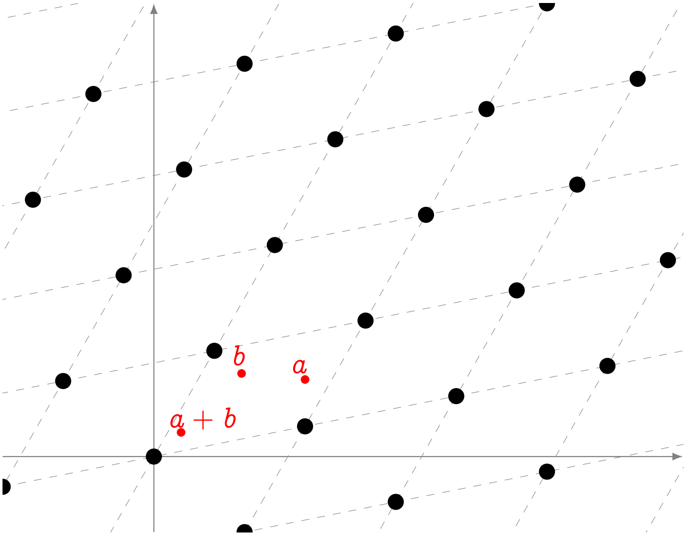

Addition law induced by addition on $\mathbb{C}$.

# Elliptic curves



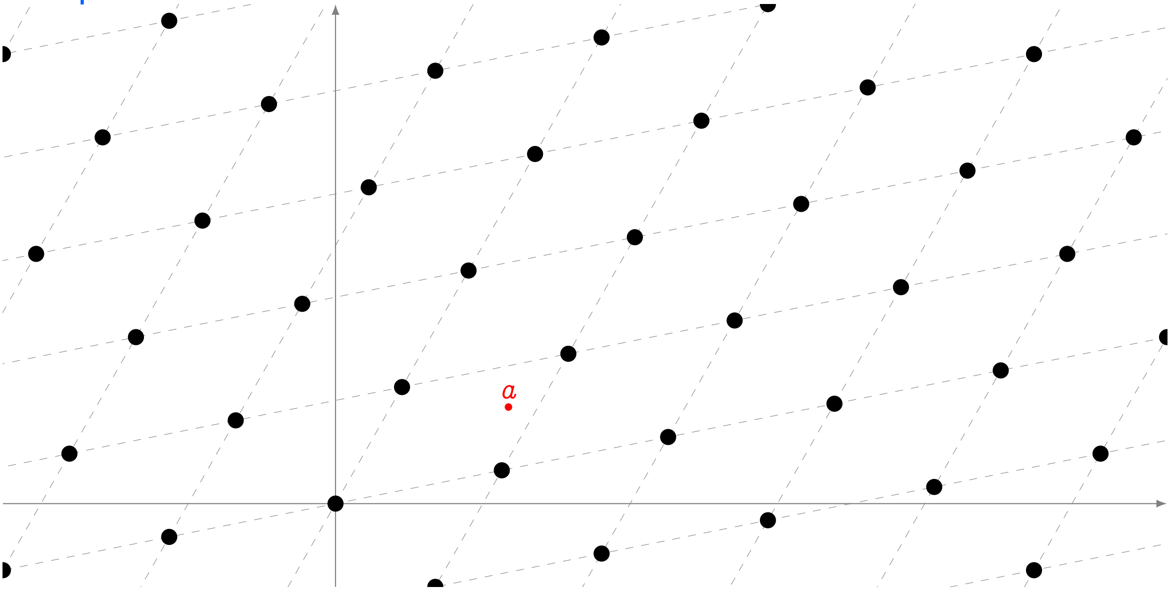

Addition law induced by addition on $\mathbb{C}$.

# Elliptic curves

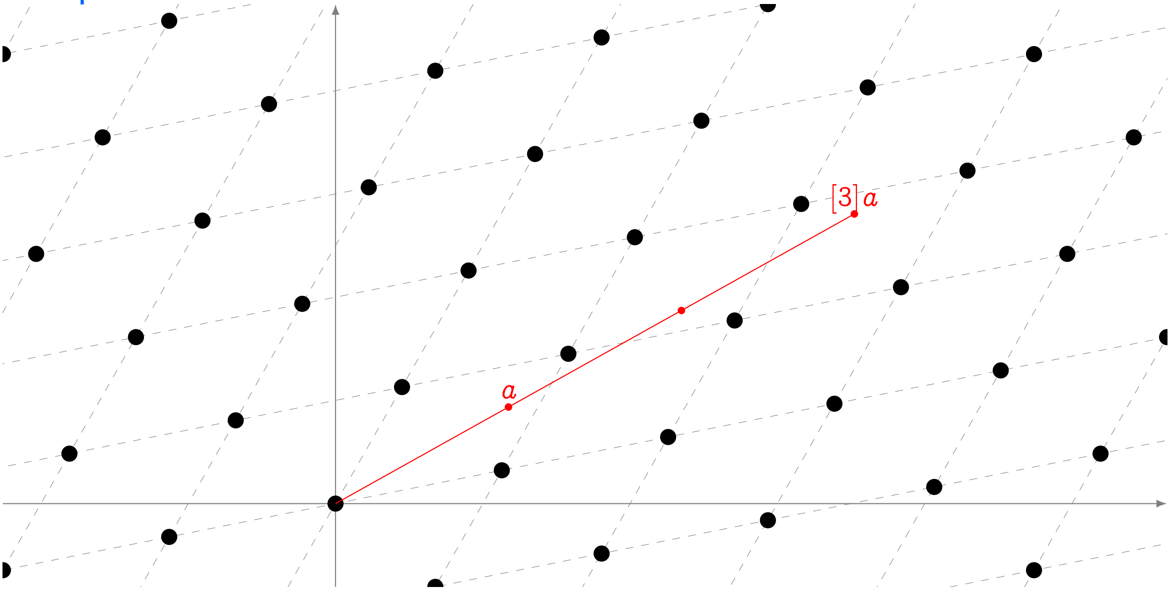



Addition law induced by addition on $\mathbb{C}$.

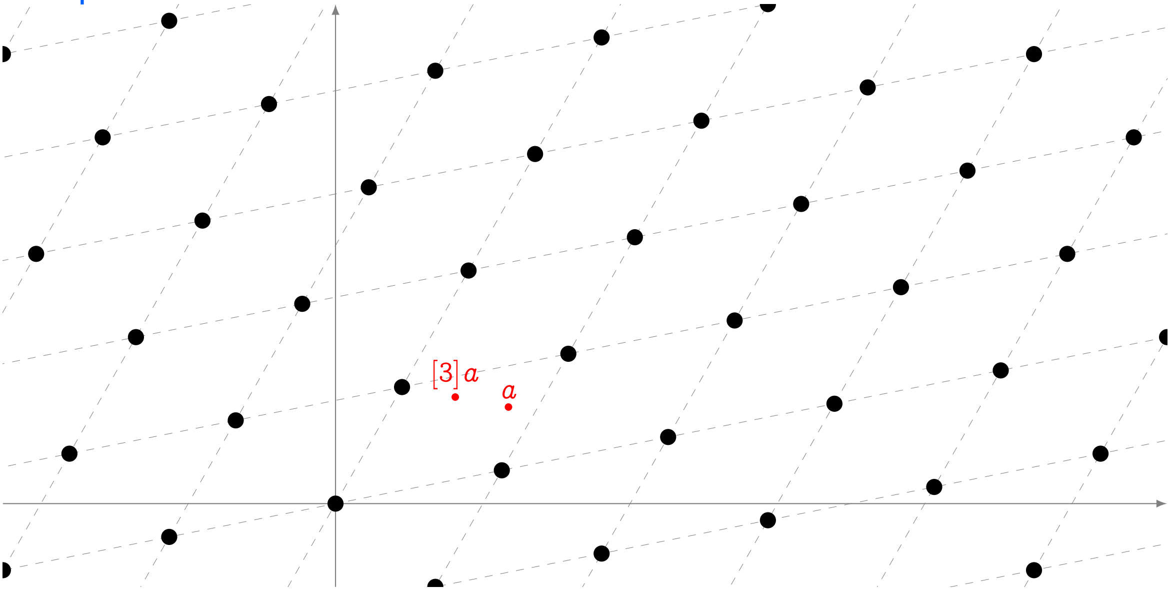
# Multiplication



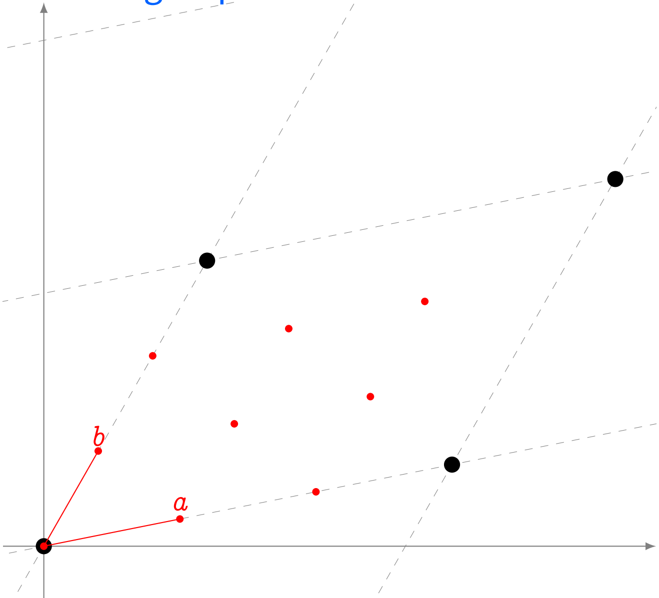
# Multiplication



# Multiplication



# Torsion subgroups



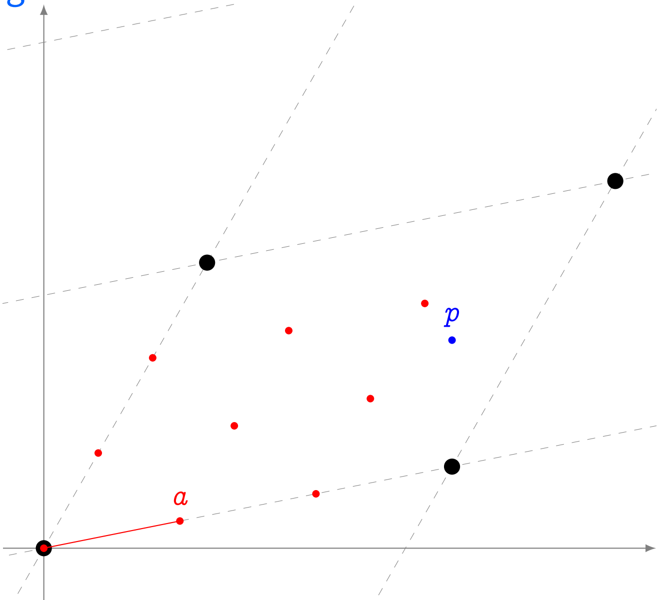

The $\ell$-torsion subgroup is made up by the points

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

It is a group of rank two

$$\begin{aligned} E[\ell] &= \langle a, b \rangle \\ &\simeq (\mathbb{Z}/\ell\mathbb{Z})^2 \end{aligned}$$

# Isogenies




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

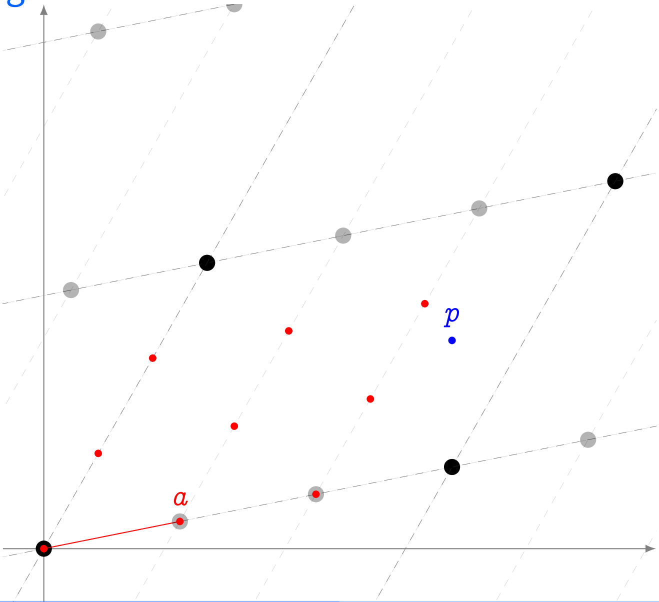
$$\Lambda_2 = a\mathbb{Z} \oplus \Lambda_1$$

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

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

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

# Isogenies




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

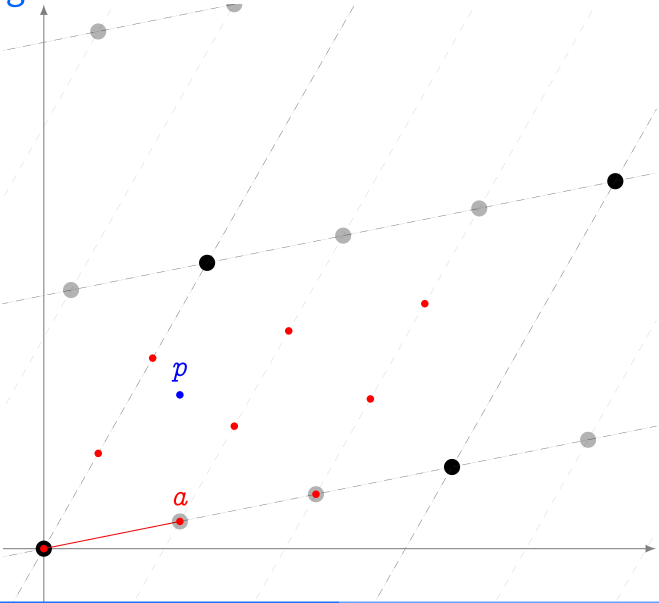
$$\Lambda_2 = a\mathbb{Z} \oplus \Lambda_1$$

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

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

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

# Isogenies




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

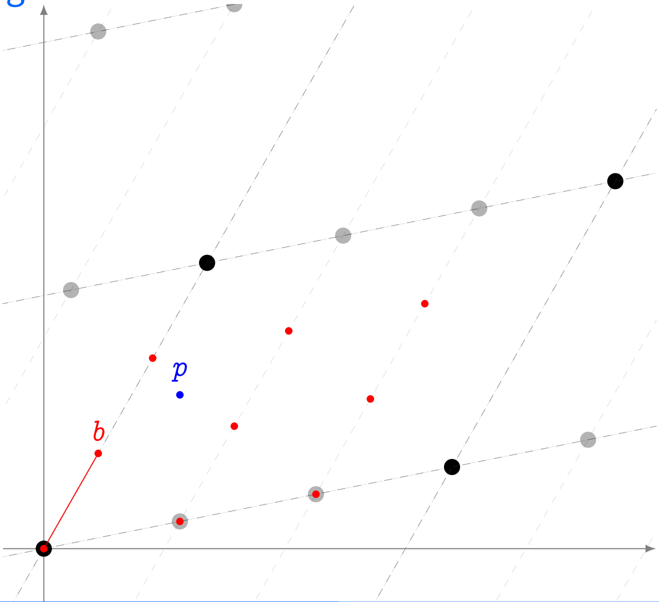
$$\Lambda_2 = a\mathbb{Z} \oplus \Lambda_1$$

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

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

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

# Isogenies

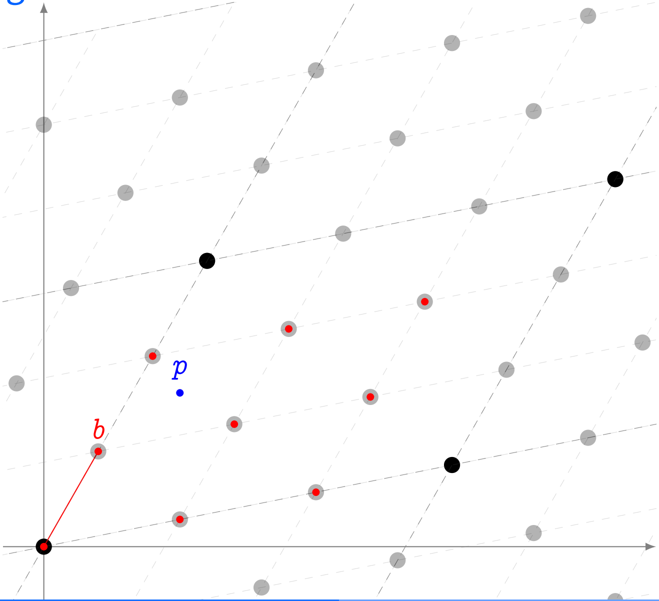



Taking a point $b$ not in the kernel of $\phi$, we obtain a new degree $\ell$ cover

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

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

# Isogenies

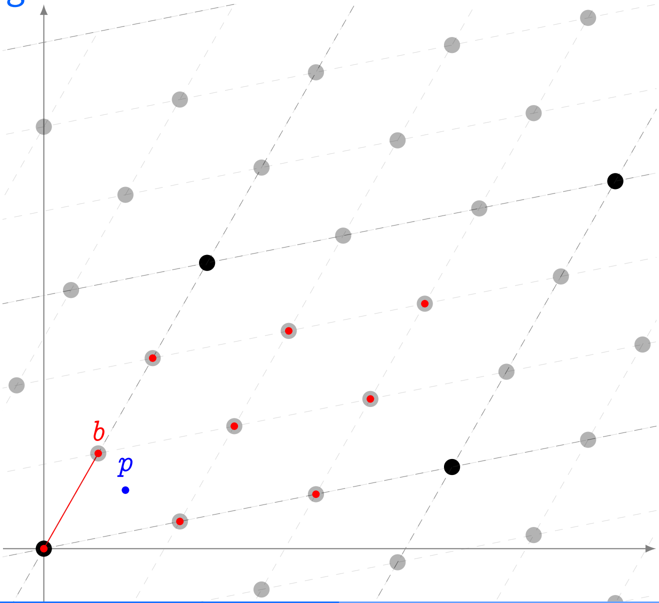



Taking a point $b$ not in the kernel of $\phi$, we obtain a new degree $\ell$ cover

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

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

# Isogenies




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

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

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

# What is scalar multiplication?

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

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

# What is ~~scalar multiplication~~ an isogeny?

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

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

# What is ~~scalar multiplication~~ an isogeny?

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

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

# What is ~~scalar multiplication~~ an isogeny?

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

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

# What is ~~scalar multiplication~~ an isogeny?

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

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

# What is ~~scalar multiplication~~ an isogeny?

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

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

# What is ~~scalar multiplication~~ an isogeny?

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

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

(Separable) isogenies ⇔ finite subgroups:

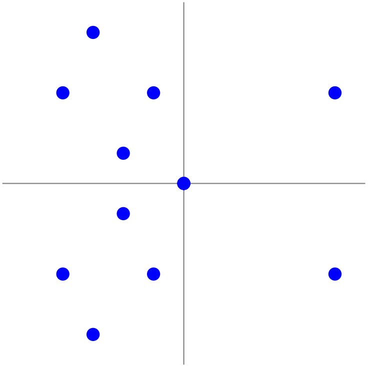
$$0 \longrightarrow H \longrightarrow E \xrightarrow{\phi} E' \to 0$$

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

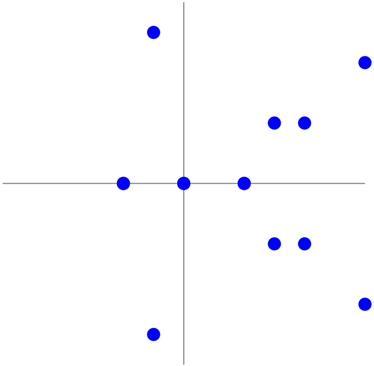
$$E/H \stackrel{\text{def}}{=} E'.$$

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

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



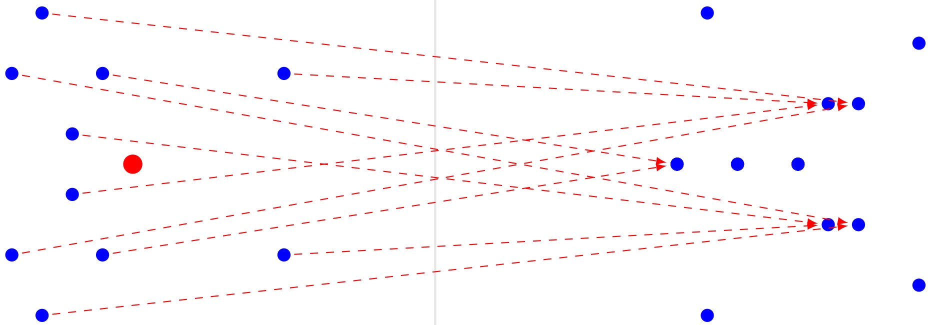
$$E' \;:\; y^2 = x^3 - 4x$$



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

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

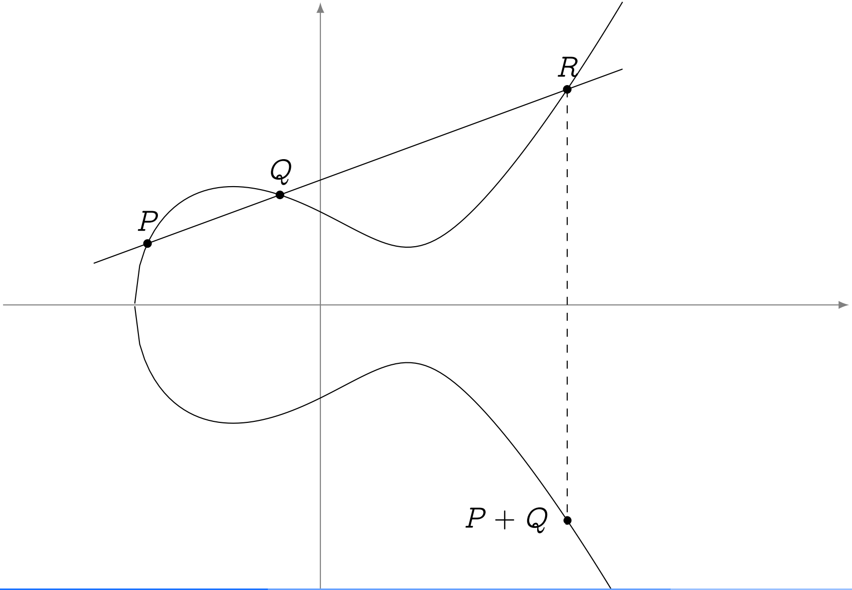
$E : y^2 = x^3 + x$ $\qquad$ $E' : y^2 = x^3 - 4x$



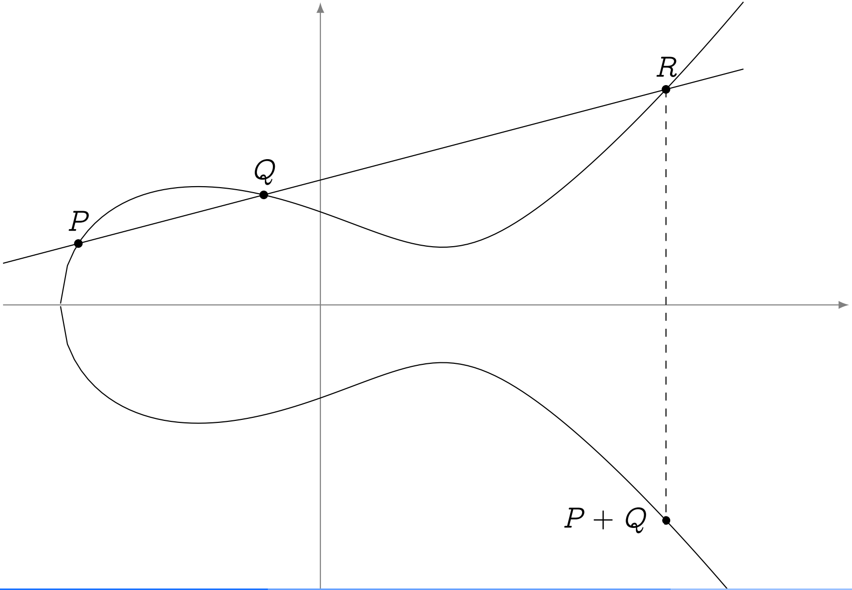
$$\phi(x, y) = \left(\frac{x^2+1}{x}, \quad y\frac{x^2-1}{x^2}\right)$$

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

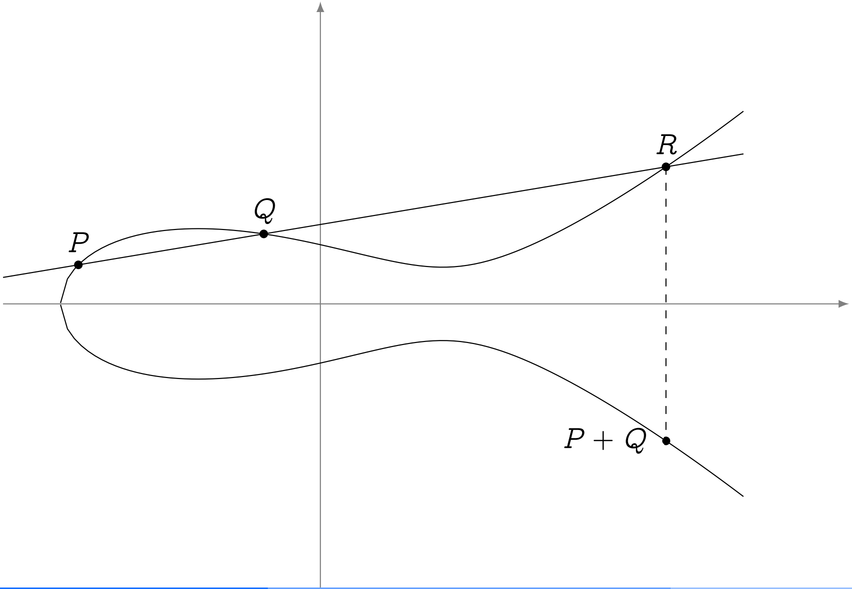
# Up to isomorphism



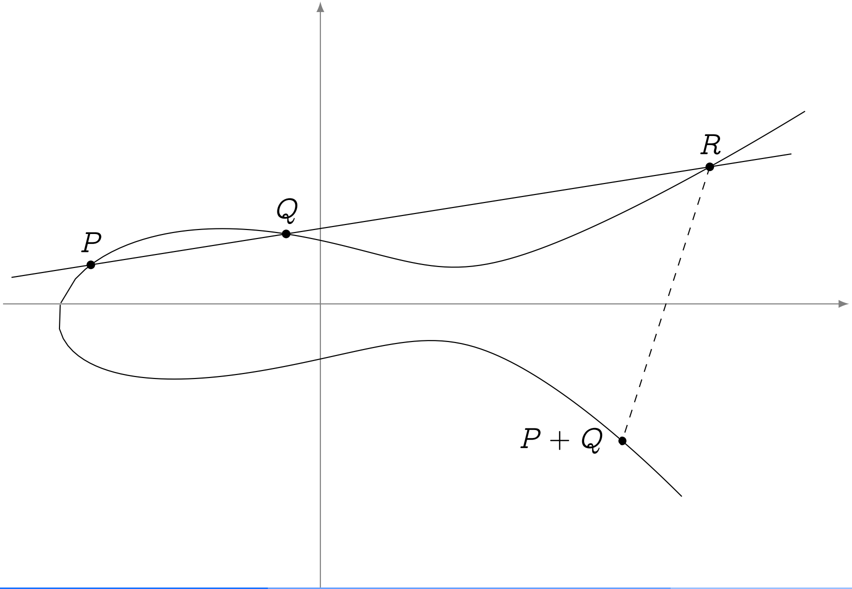
# Up to isomorphism



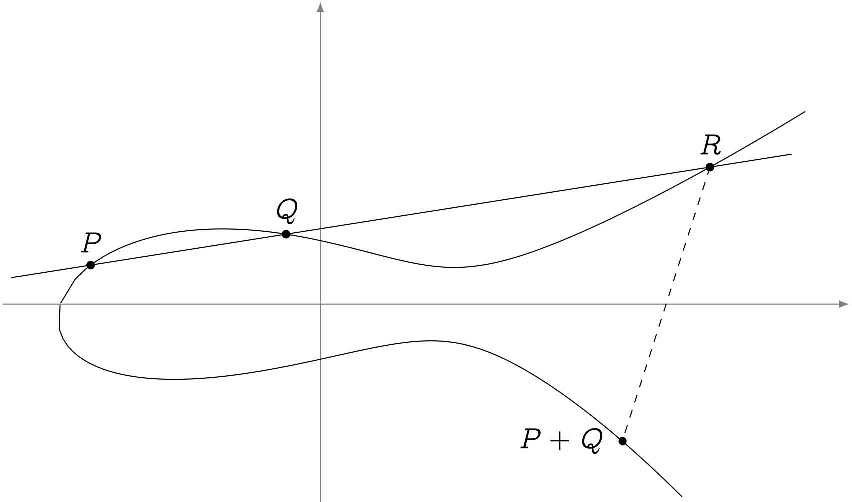
# Up to isomorphism



# Up to isomorphism

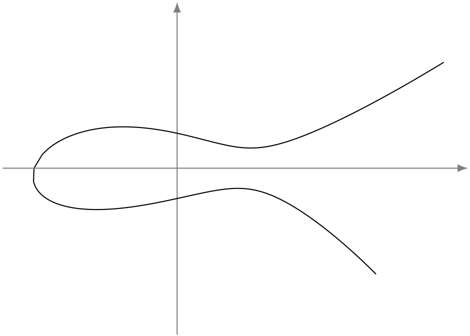


# Up to isomorphism

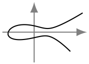



$$y^2 = x^3 + ax + b \quad \longrightarrow \quad j = 1728\frac{4a^3}{4a^3+27b^2}$$

# Up to isomorphism



# Up to isomorphism



# Up to isomorphism

$j = 1728$

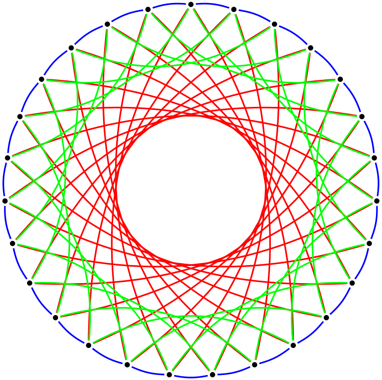
# Up to isomorphism

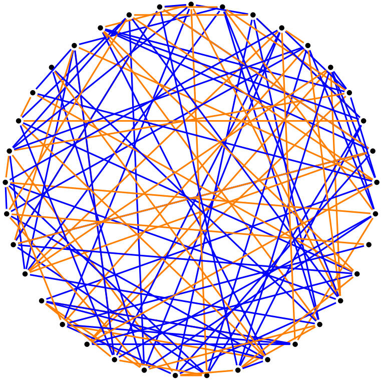
$$j = 1728 \xrightarrow{\phi} j = 287496$$

# Up to isomorphism

# The beauty and the beast (credit: Lorenz Panny)

Components of particular isogeny graphs look like this:

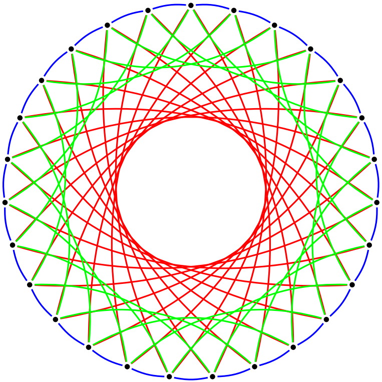




*Which of these is good for crypto?*

# The beauty and the beast (credit: Lorenz Panny)

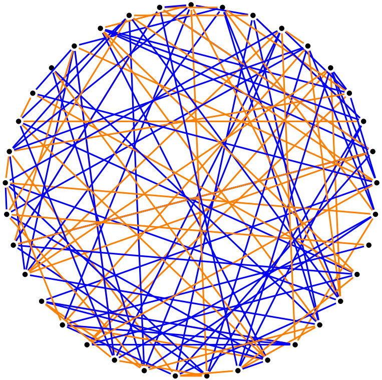
At this time, there are <u>two distinct families</u> of systems:



$\mathbb{F}_p$

**CSIDH** [pron.: sea-side]

`https://csidh.isogeny.org`



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

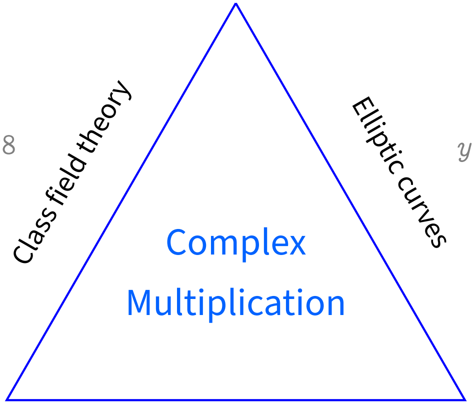
**SIDH**

`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 | Castryck, Lange, Martindale, Panny & Renes create an efficient variant of the Couveignes–Rostovtsev–Stolbunov protocol, named CSIDH. |
| 2019 | Isogeny signature craze: SeaSign (D. & Galbraith; Decru, Panny & Vercauteren), CSI-FiSh (Beullens, Kleinjung & Vercauteren), VDF (D., Masson, Petit & Sanso). |
| 2020 | Isogeny signatures get interesting: SQISign (D., Kohel, Leroux, Petit, Wesolowski). SIKE is an Alternate candidate finalist in NIST's 3rd round. |

$$H(j) = j - 1728$$




$$y^2 = x^3 - ax - b$$

Modular functions

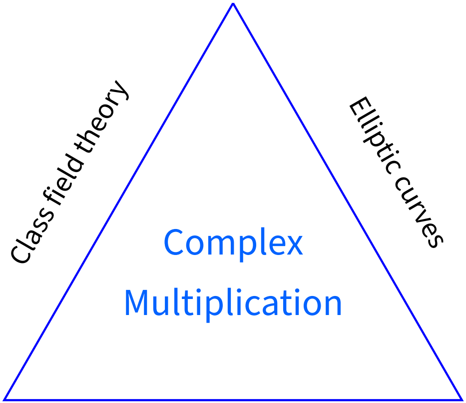
$$j(z) = \frac{1}{q} + 744 + 196884q + \cdots$$

Abelian extensions

of $\mathbb{Q}(\sqrt{-D})$

Elliptic curves with

$\mathtt{End}(E) \subset \mathbb{Q}(\sqrt{-D})$

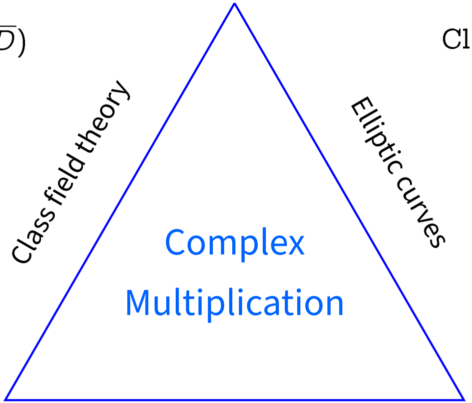



Modular functions

Galois group of $K/\mathbb{Q}(\sqrt{-D})$

$\simeq$

Class group $\mathrm{Cl}(-D)$




$\mathrm{Cl}(-D)$ acts on set of $E$ s.t.

$\mathrm{End}(E) \subset \mathbb{Q}(\sqrt{-D})$

Modular functions

# Complex multiplication dictionary

| Quadratic imaginary fields | Elliptic curves |
|---:|:---|
| Integers of $\mathbb{Q}(\sqrt{-D})$ | Endomorphisms of $E$ |
| Integral ideals of $\mathbb{Q}(\sqrt{-D})$ | Isogenies of $E$ |
| Ideal classes in $\mathrm{Cl}(-D)$ | Isogenies $\begin{tikzcd} \bullet \arrow[r, bend left] \arrow[r, bend right] & \bullet \end{tikzcd}$ |
| Ideal norm | Isogeny degree |
| Conjugate ideal | Dual isogeny |

## Group action

$\mathcal{G} \circlearrowright \mathcal{E}$: 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 $\mathfrak{g} * E' = E$.

## Hard Homogeneous Space (HHS) — Couveignes 1996

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

| **Alice** | | **Bob** |
|---|---|---|
| pick random $\mathfrak{a} \in \mathcal{G}$ | | pick random $\mathfrak{b} \in \mathcal{G}$ |
| compute $E_A = \mathfrak{a} * E_0$ | | compute $E_B = \mathfrak{b} * E_0$ |
| | $\xrightarrow{\quad E_A \quad}$ | |
| | $\xleftarrow[\quad E_B \quad]{}$ | |

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

# HHSDH from complex multiplication

**Obstacles:**

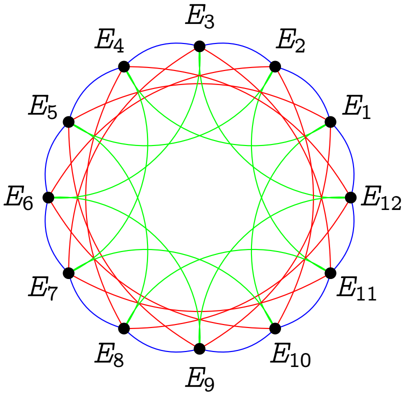
- The group size of $\mathrm{Cl}(-D)$ is unknown.
- Only ideals of small norm (isogenies of small degree) are efficient to evaluate.

**Solution:**

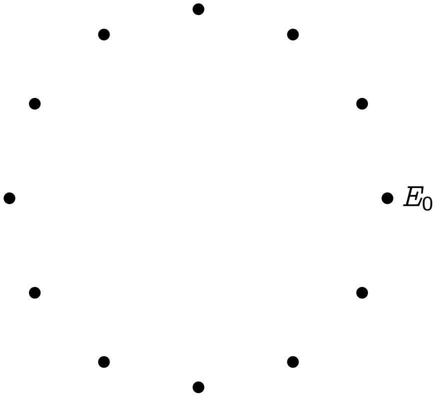
- Restrict to elements of $\mathrm{Cl}(-D)$ of the form

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

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



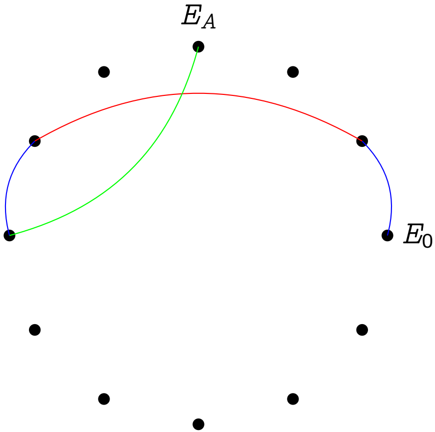
# Couveignes/Rostovtsev–Stolbunov/CSIDH key exchange




**Public parameters:**

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

# Couveignes/Rostovtsev–Stolbunov/CSIDH key exchange

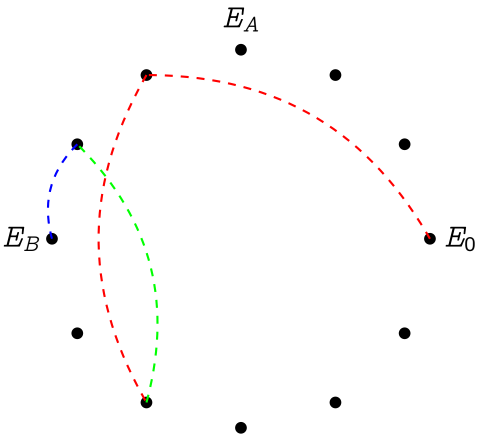



**Public parameters:**

- A starting 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 $O(\log p)$;

# Couveignes/Rostovtsev–Stolbunov/CSIDH key exchange

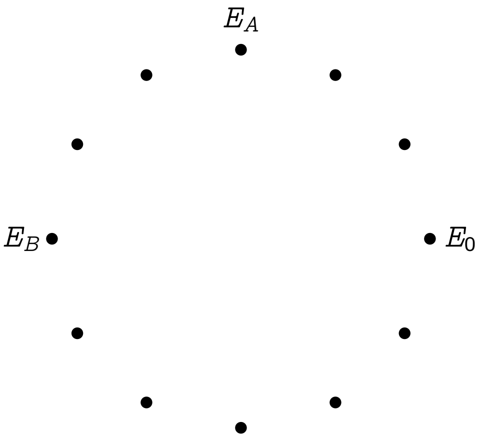



**Public parameters:**

- A starting 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;

# Couveignes/Rostovtsev–Stolbunov/CSIDH key exchange

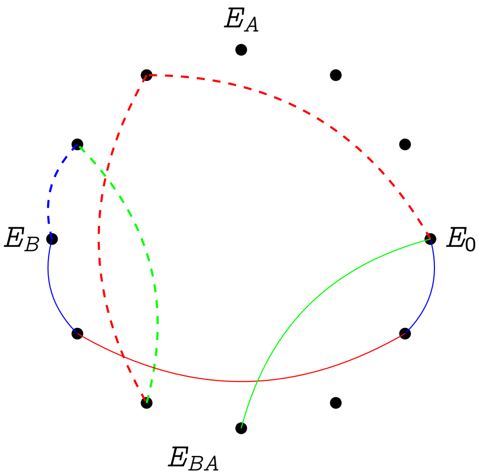



**Public parameters:**

- A starting 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 $E_B$;

# Couveignes/Rostovtsev–Stolbunov/CSIDH key exchange

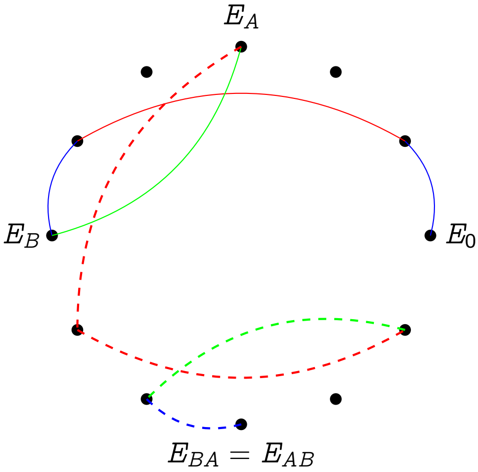



**Public parameters:**

- A starting 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 $\phi_A$ starting from $E_B$.

# Couveignes/Rostovtsev–Stolbunov/CSIDH key exchange




**Public parameters:**

- A starting 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 $\phi_A$ starting from $E_B$.
5. **Bob** repeats his secret walk $\phi_B$ starting from $E_A$.

# 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 (subexpoential cost);
- Well known reduction from the hidden shift to the dihedral (non-abelian) hidden subgroup problem;
- Kuperberg's algorithm solves the dHSP with a subexponential number of class group evaluations.
- Recent work suggests that $2^{64}$-qbit security is achieved somewhere in $512 < \log p < 2048$.

# Supersingular curves

## Theorem (Deuring)

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

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

  $E$ is ordinary.

- An order $\mathcal{O}$ in a quadratic imaginary field:

  $E$ is ordinary with complex multiplication by $\mathcal{O}$.

- Only if $p > 0$, a maximal order in a quaternion algebra[a]:

  $E$ is supersingular.

---

[a] (ramified at $p$ and $\infty$)

# Key exchange with supersingular curves (Jao & D. 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.

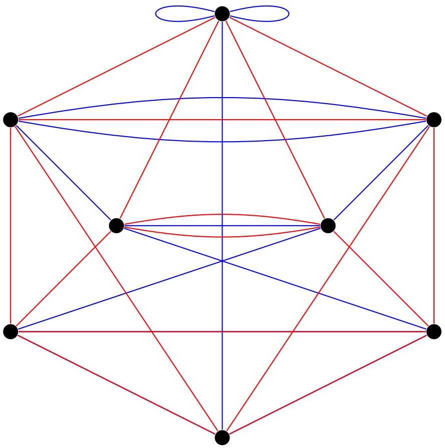


Figure: 2- and 3-isogeny graphs on $\mathbb{F}_{97^2}$.

# Key exchange with supersingular curves (Jao & D. 2011)

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

**Walk of length $e_A$**

$=$

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

$=$

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

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

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

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

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

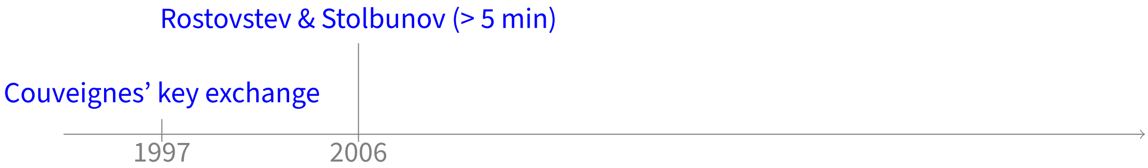
$$\begin{tikzcd}
E \arrow[r, rightsquigarrow, "\phi"] \arrow[d, rightsquigarrow, "\psi"'] & E/\langle P\rangle \arrow[d, rightsquigarrow, "\psi'"] \\
E/\langle Q\rangle \arrow[r, rightsquigarrow, "\phi'"'] & E/\langle P, Q\rangle
\end{tikzcd}$$

# From 10 minutes to 10ms in 20 years

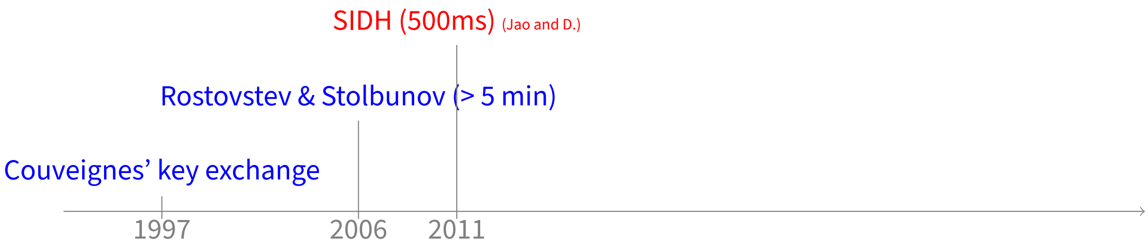
Couveignes' key exchange

1997

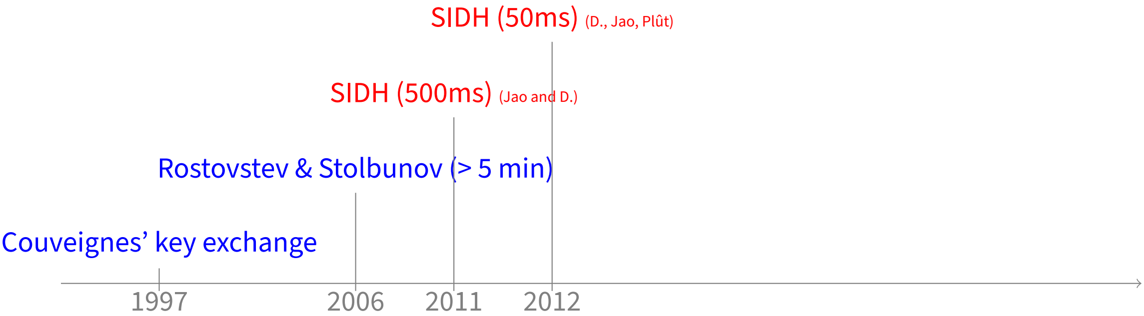
# From 10 minutes to 10ms in 20 years



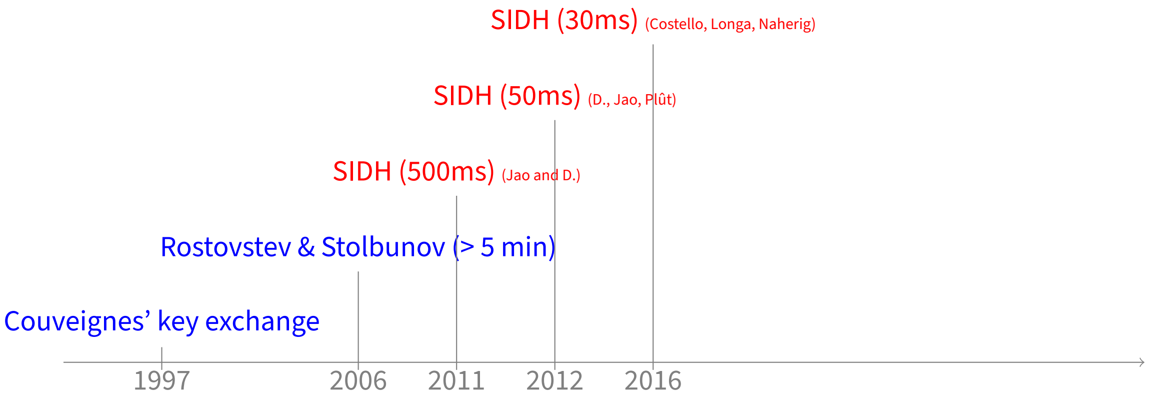
# From 10 minutes to 10ms in 20 years



# From 10 minutes to 10ms in 20 years



# From 10 minutes to 10ms in 20 years



# From 10 minutes to 10ms in 20 years

SIKE (10ms) (NIST candidate)

SIDH (30ms) (Costello, Longa, Naherig)

SIDH (50ms) (D., Jao, Plût)

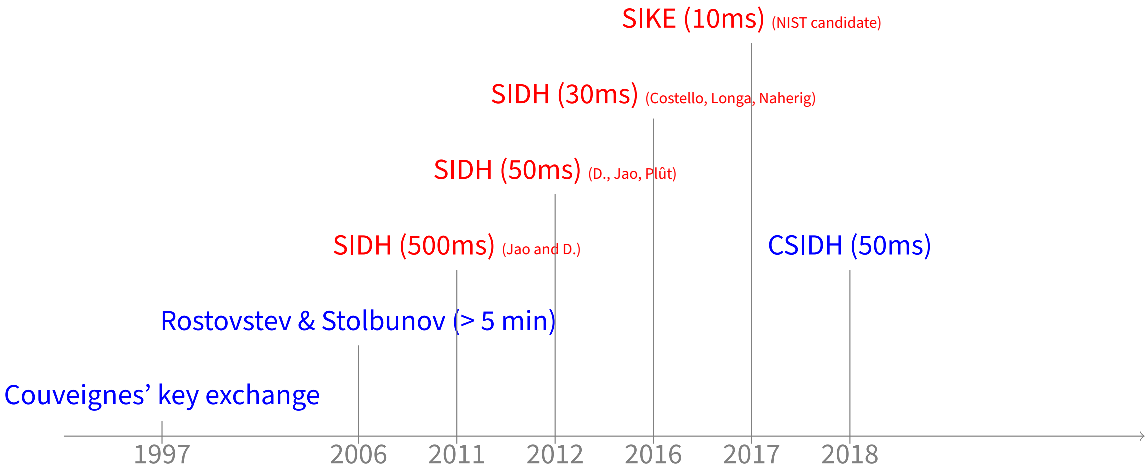
SIDH (500ms) (Jao and D.)

Rostovstev & Stolbunov (> 5 min)

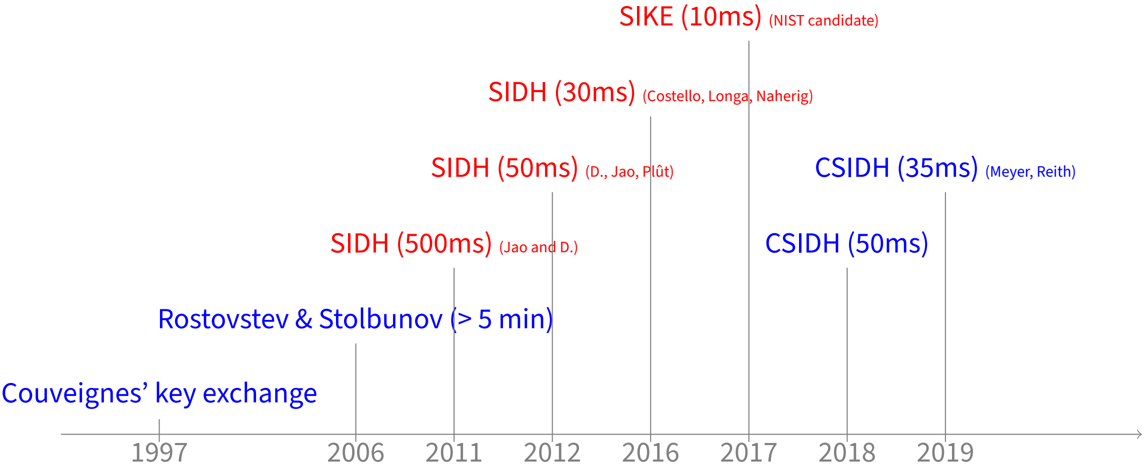
Couveignes' key exchange

1997 2006 2011 2012 2016 2017

# From 10 minutes to 10ms in 20 years



# From 10 minutes to 10ms in 20 years



# Contemporary research

- Efficient signature schemes and proofs of knowledge;
- Quaternionic multiplication $\rightarrow$ SQISign;
- Higher dimensional abelian varieties;
- Cryptanalysis;
- Side-channel protections;
- Lower complexity bounds and delay protocols;
- Trusted generation of random supersingular curves;
- Prime searches;
- …

# Thank you

`https://defeo.lu/`

@luca_defeo