How to prove a secret isogeny

Luca De Feo

Université Paris Saclay – UVSQ, France

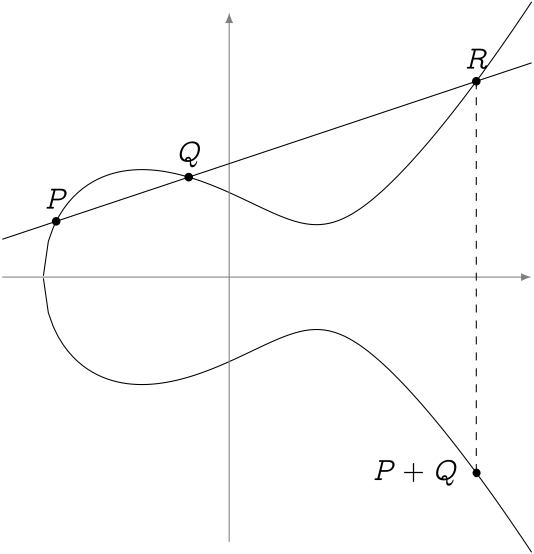
June 4, 2019, CTCrypt, Svetlogorsk

based on joint work with
J. Burdges, S. Galbraith,
S. Masson, C. Petit, A. Sanso

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

Elliptic curves

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



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

What's ~~scalar multiplication~~ an isogeny?

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

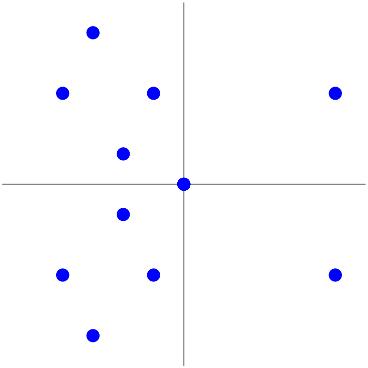
- A map $E \to \cancel{E}\, E'$,
- a group morphism,
- with finite kernel
  (~~the torsion group~~ $\cancel{E[m] \simeq (\mathbb{Z}/m\mathbb{Z})^2}$ any finite subgroup $H \subset E$),
- surjective (in the algebraic closure),
- given by rational maps of degree $\cancel{m^2}\ \#H$.

(Separable) isogenies ⇔ finite subgroups:

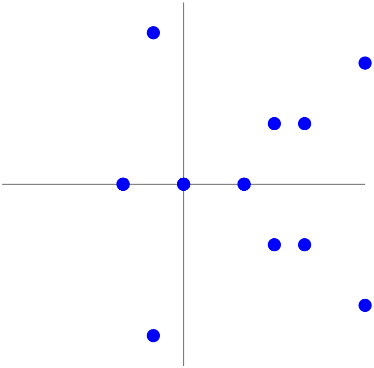
$$0 \to H \to E \xrightarrow{\phi} E' \to 0$$

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

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



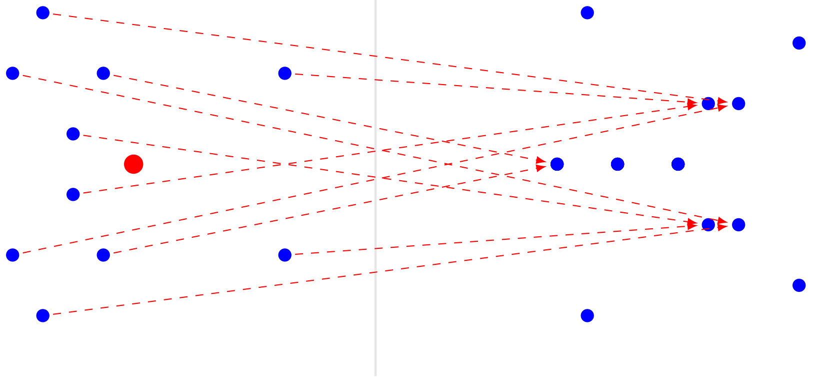
$$E' \;:\; y^2 = x^3 - 4x$$



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

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

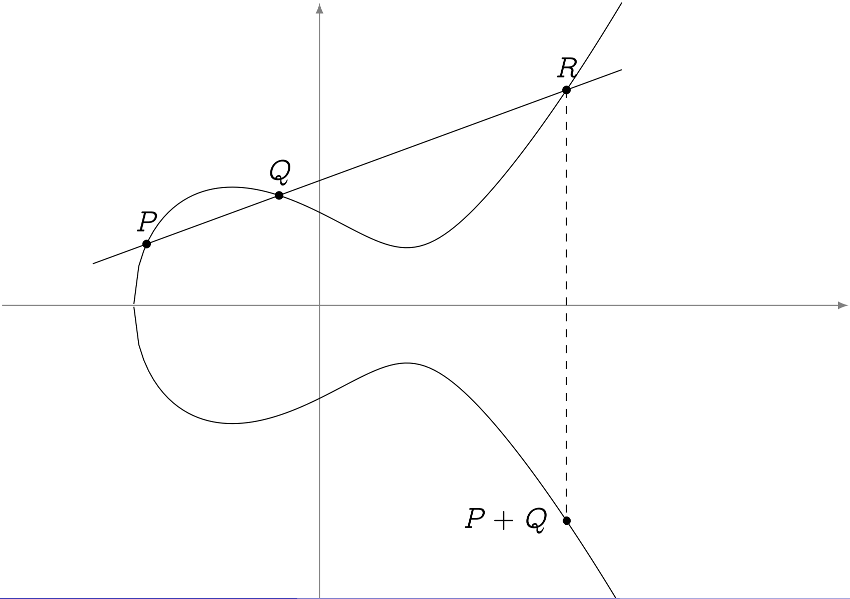
$E \; : \; y^2 = x^3 + x$ $\qquad\qquad$ $E' \; : \; y^2 = x^3 - 4x$



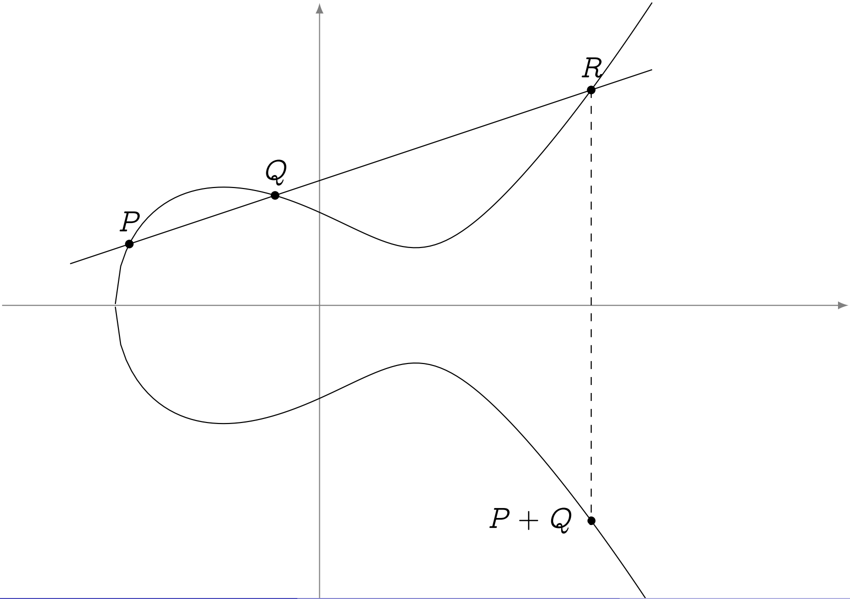
$$\phi(x, y) = \left(\frac{x^2 + 1}{x}, \quad y\frac{x^2 - 1}{x^2} \right)$$

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

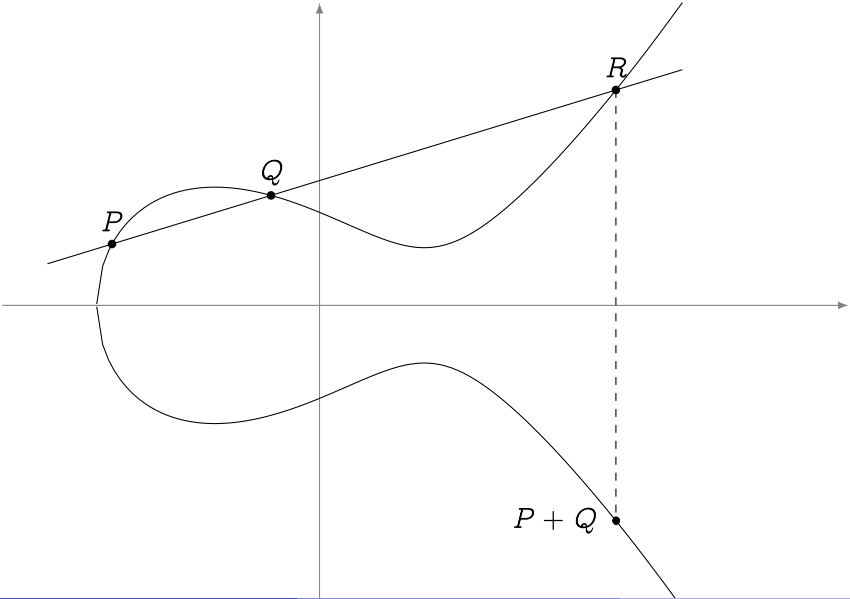
Up to isomorphism



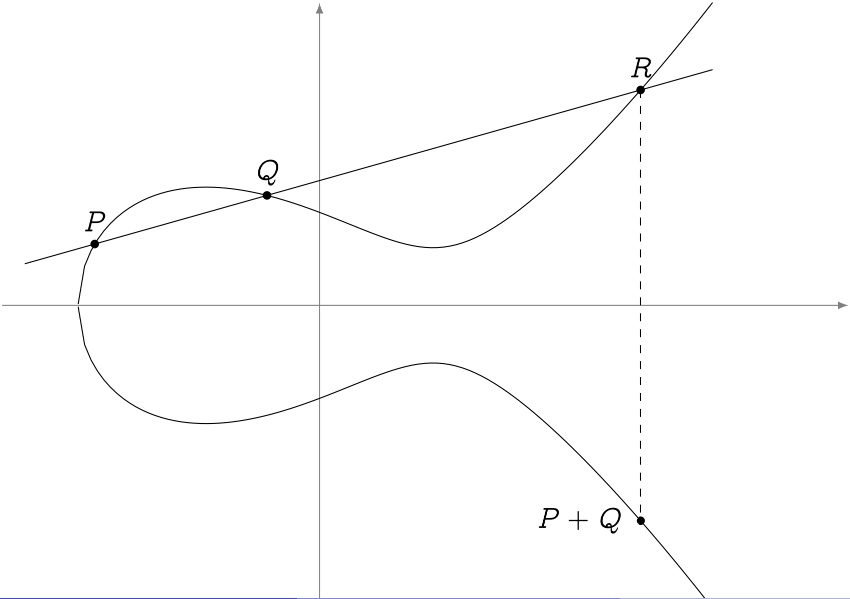
Up to isomorphism



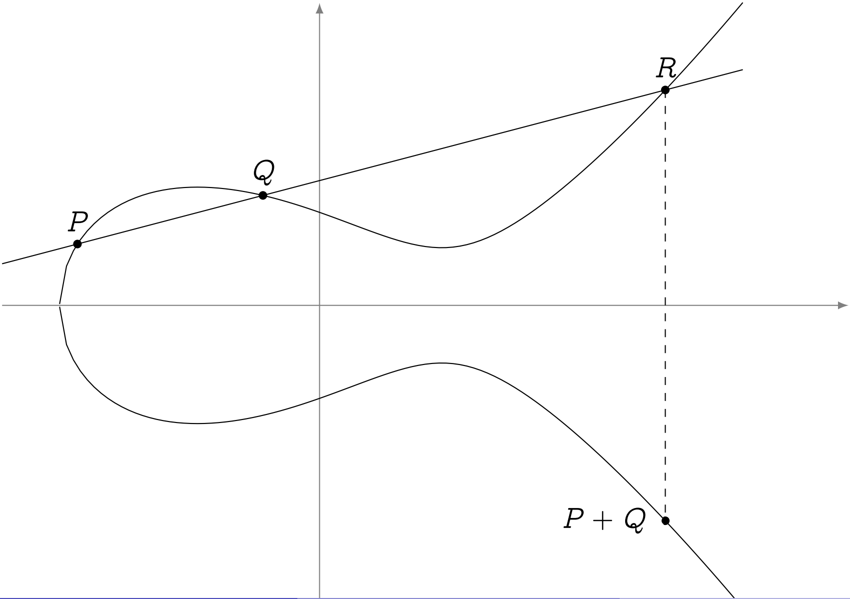
Up to isomorphism



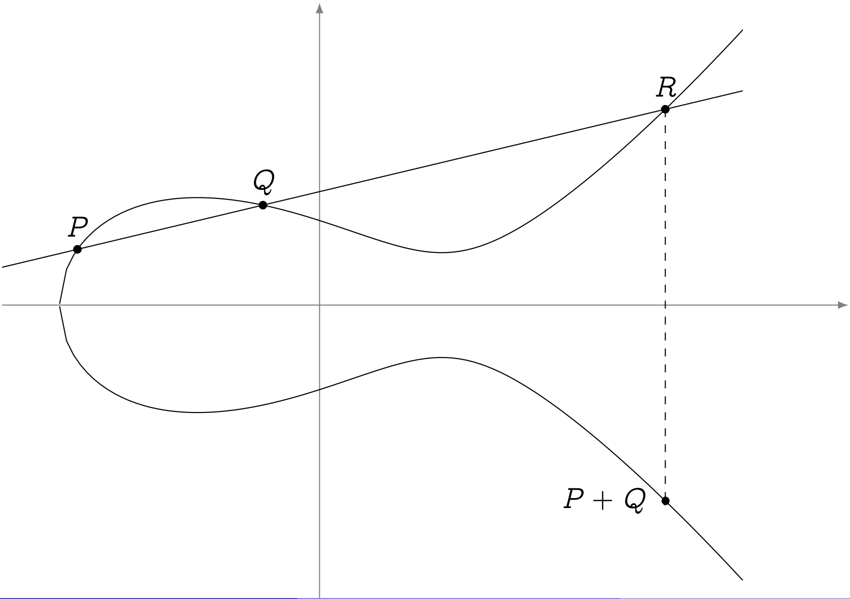
Up to isomorphism



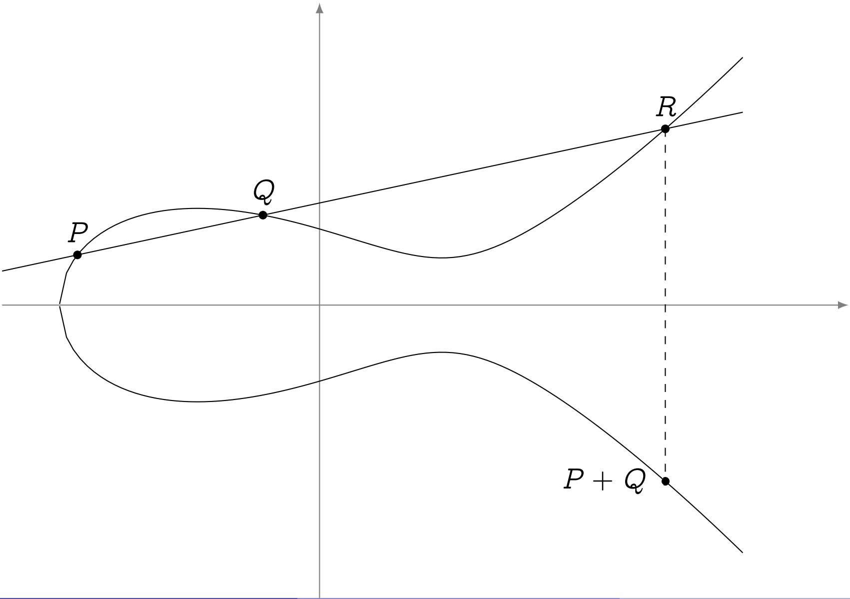
Up to isomorphism



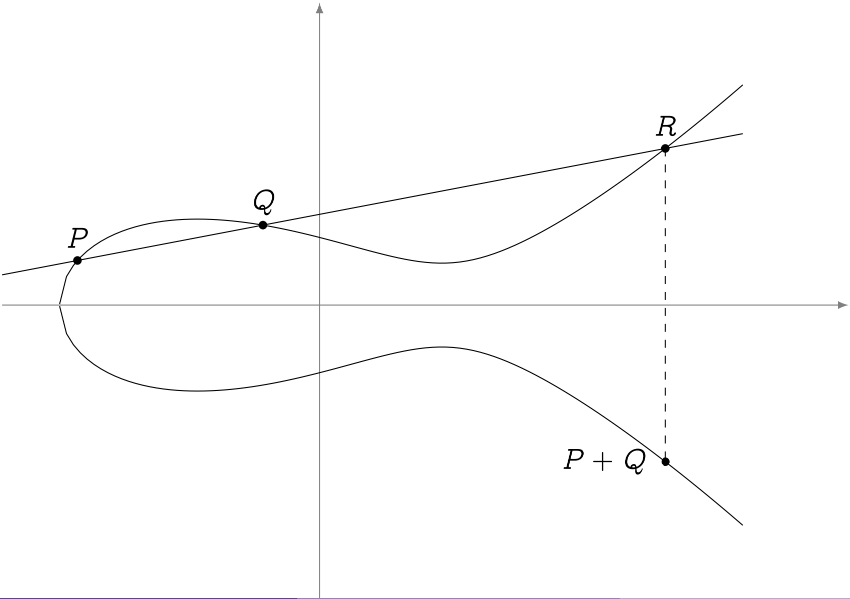
Up to isomorphism



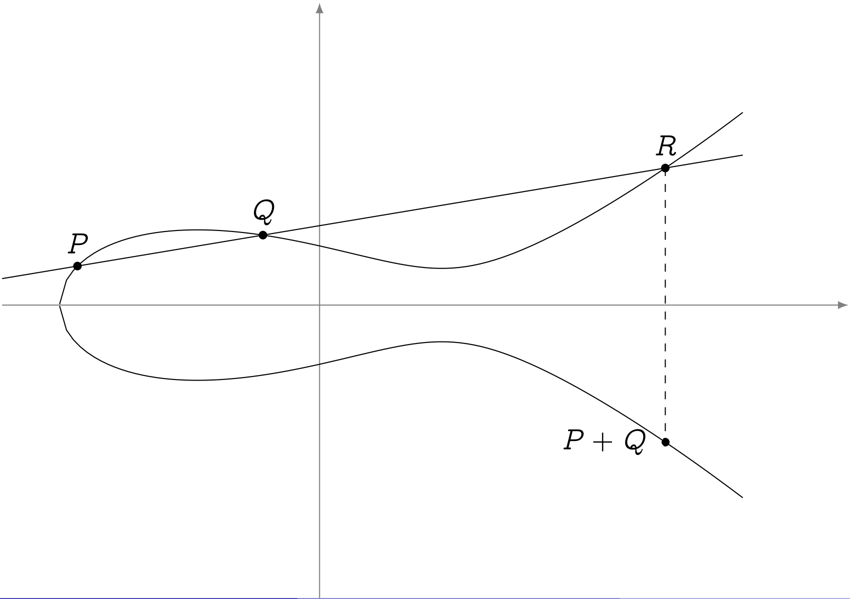
Up to isomorphism



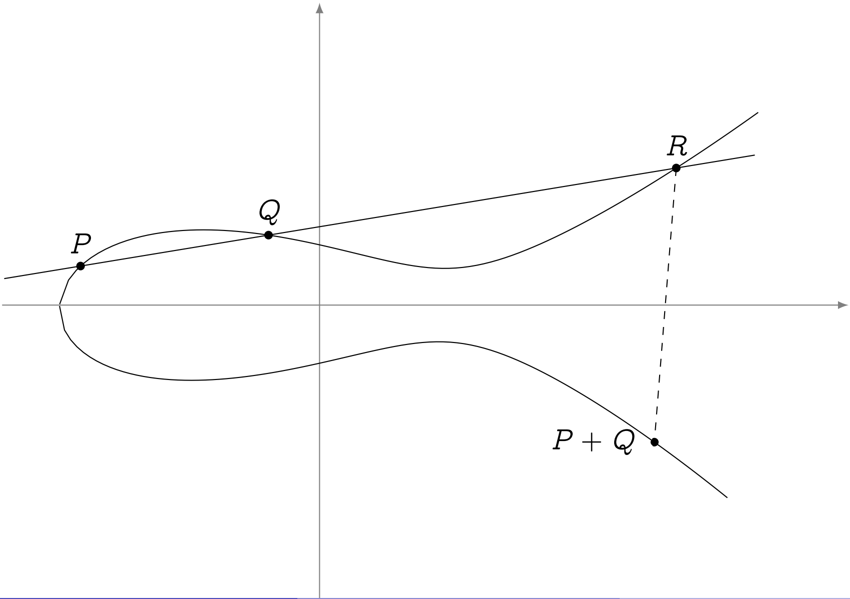
Up to isomorphism



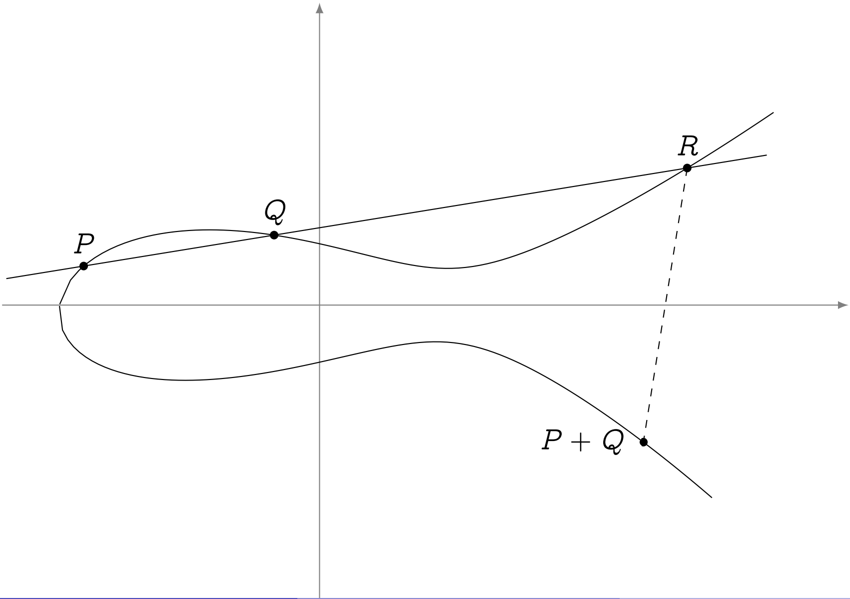
Up to isomorphism



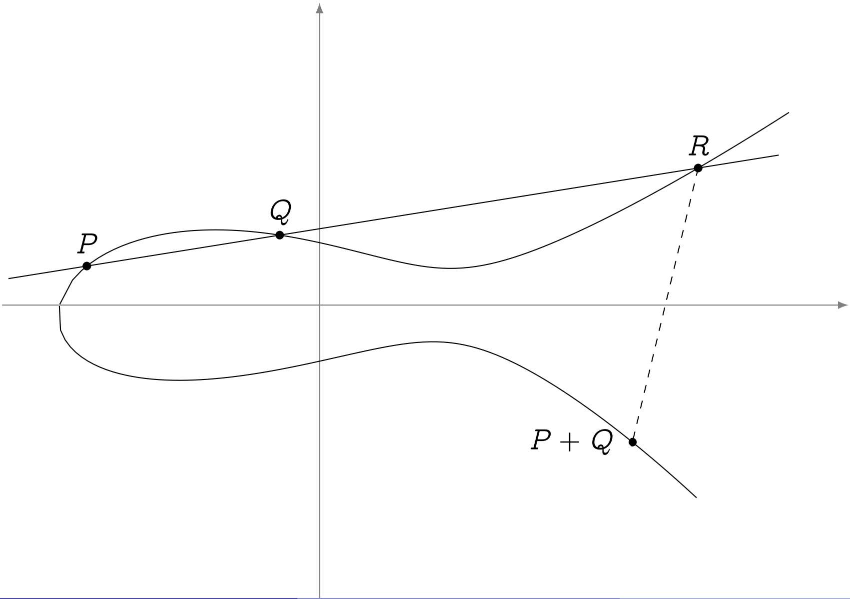
Up to isomorphism



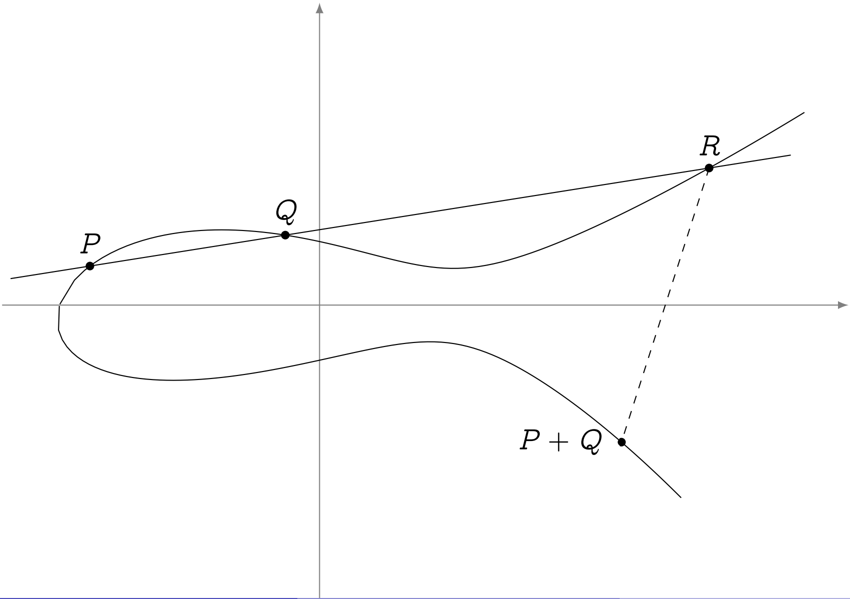
Up to isomorphism



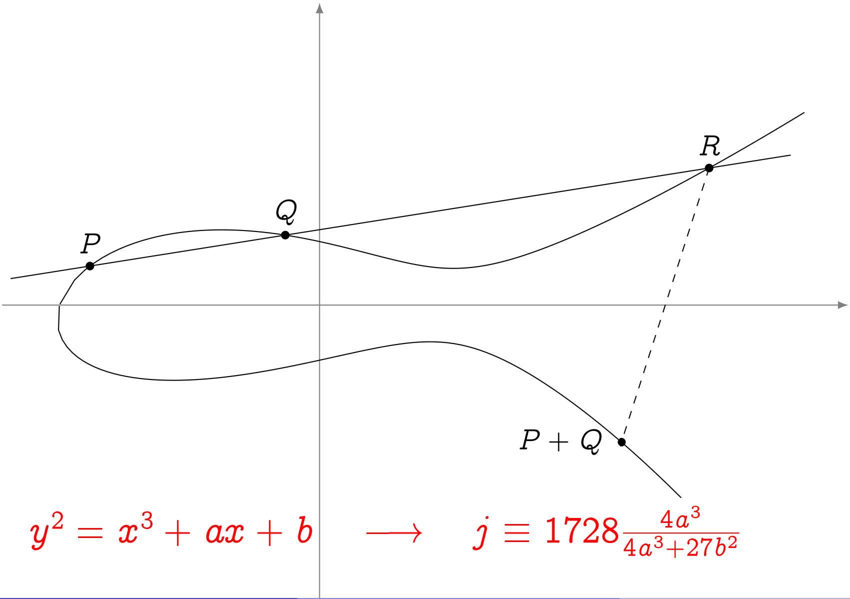
Up to isomorphism



Up to isomorphism

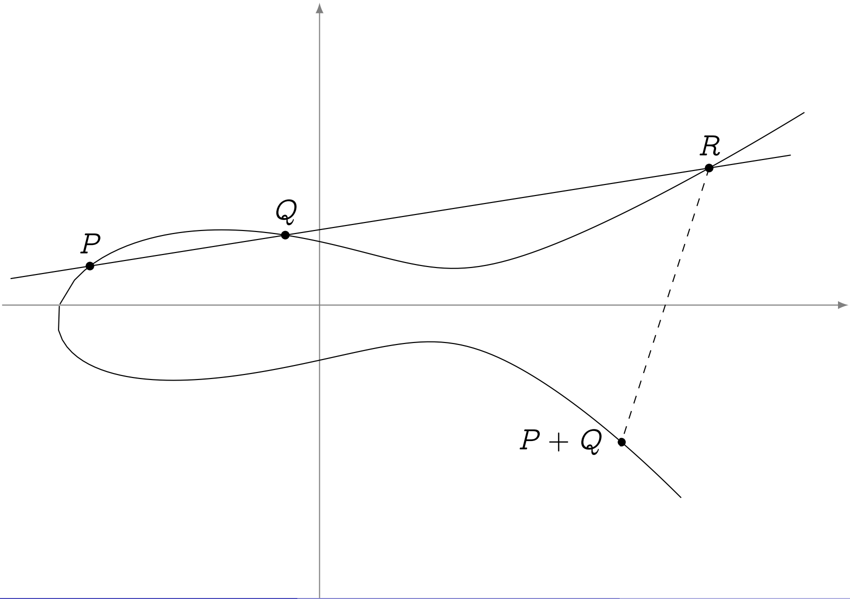


Up to isomorphism

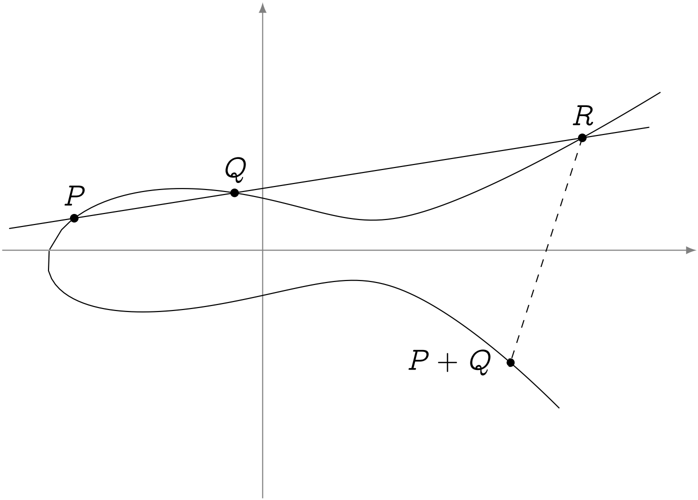


$$y^2 = x^3 + ax + b \quad \longrightarrow \quad j \equiv 1728\frac{4a^3}{4a^3+27b^2}$$

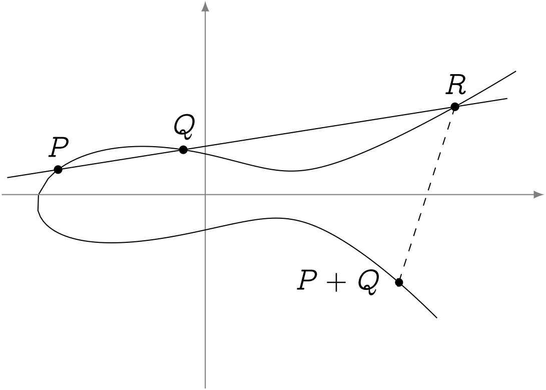
Up to isomorphism



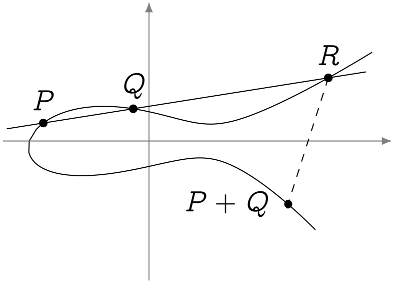
Up to isomorphism



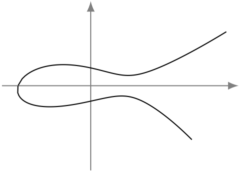
Up to isomorphism



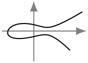
Up to isomorphism



Up to isomorphism



Up to isomorphism



Up to isomorphism

$j = 1728$

Up to isomorphism

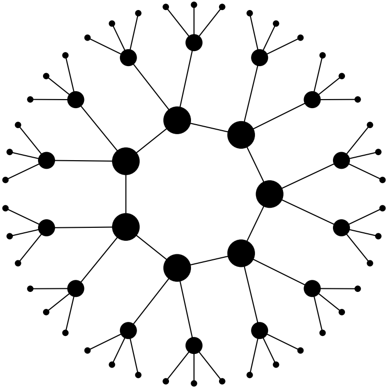
$$j = 1728 \xrightarrow{\phi} j = 287496$$

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.



The graph of isogenies of prime degree $\ell \neq p$

All graphs are undirected (dual isogeny theorem).

Ordinary case (isogeny volcanoes)

- Nodes can have degree $0, 1, 2$ or $\ell + 1$.
  - For $\sim 50\%$ of the primes ℓ, graphs are just isolated points;
  - For other $\sim 50\%$, graphs are 2-regular;
  - other cases only happen for finitely many ℓ's.

Supersingular case ($\mathbb{F}_p$)

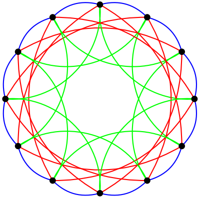
- If $\ell = 2$ nodes have degree $1, 2$ or 3;
- For $\sim 50\%$ of ℓ, graphs are isolated points;
- For other $\sim 50\%$, graphs are 2-regular;

Supersingular case ($\mathbb{F}_{p^2}$)

- The graph is $\ell + 1$-regular.
- There is a unique (finite) connected component made of all supersingular curves with the same number of points.

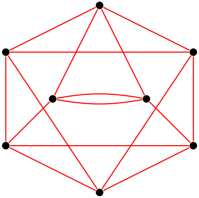
Isogeny graphs taxonomy

Complex Multiplication (CM) graphs



- Ordinary / Supersingular ($\mathbb{F}_p$)
- Superposition of isogeny cycles (one color per degree)
- Isomorphic to Cayley graph of a quadratic class group
- Large automorphism group
- Typical size $O(\sqrt{p})$
- Used in: **CSIDH**

Full **supersingular graphs**



- Supersingular ($\mathbb{F}_{p^2}$)
- One isogeny degree
- $(\ell + 1)$-regular
- Tiny automorphism group
- Size $\approx p/12$
- Used in: **SIDH**

Post-quantum isogeny primitives

SIDH (Jao, De Feo 2011)

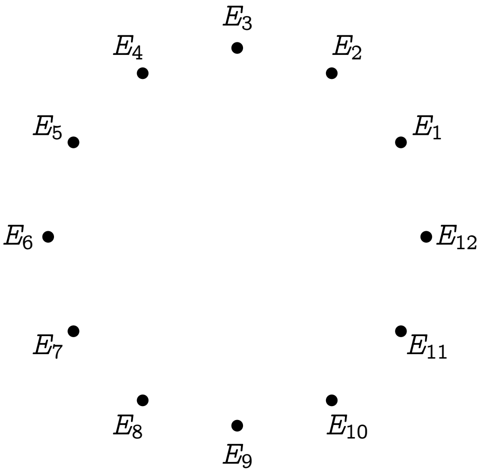
- Pronounce S–I–D–H;
- Based on isogeny walks in the full supersingular graph over $\mathbb{F}_{p^2}$;
- Basis for the NIST KEM candidate SIKE;
- Better asymptotic quantum security;
- Short keys, slow.

CSIDH (Couveignes 1996; Rostovtsev, Stolbunov 2006; Castryck, Lange, Martindale, Panny, Renes 2018)

- Pronounce Sea–Side;
- Based on isogeny walks in the supersingular CM graph over $\mathbb{F}_p$;
- Straightforward generalization of Diffie–Hellman;
- More “natural” security assumption;
- Shorter keys, slower.

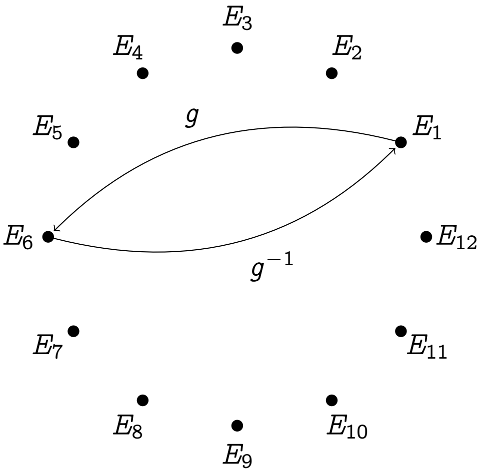
CSIDH key exchange

- A set of supersingular elliptic curves over $\mathbb{F}_p$;



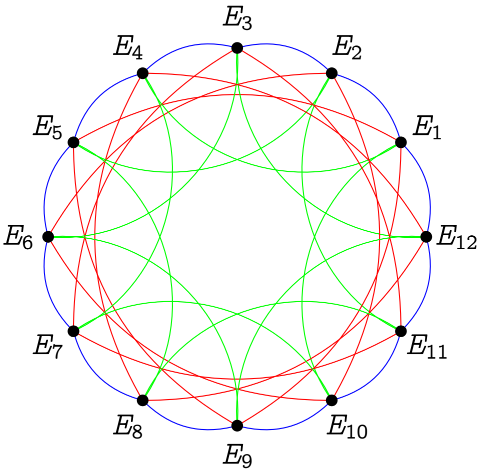
CSIDH key exchange

- A set of supersingular elliptic curves over $\mathbb{F}_p$;
- A group action by a commutative class group G;



CSIDH key exchange

- A set of supersingular elliptic curves over $\mathbb{F}_p$;
- A group action by a commutative class group G;
- Small degree generators of G: degree 2, degree 3, degree 5, …

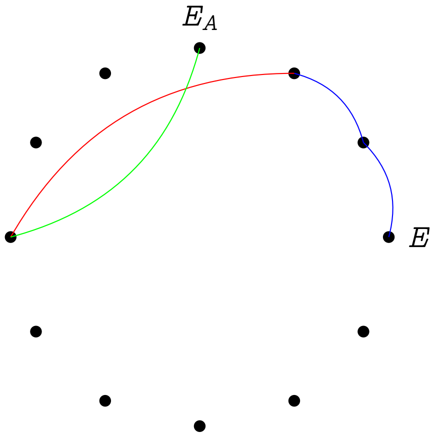


CSIDH key exchange

- A set of supersingular elliptic curves over $\mathbb{F}_p$;
- A group action by a commutative class group G;
- Small degree generators of G: degree 2, degree 3, degree 5, …

Key exchange:

- Alice picks secret $a = g_2^{a_2} g_3^{a_3} g_5^{a_5} \cdots$,

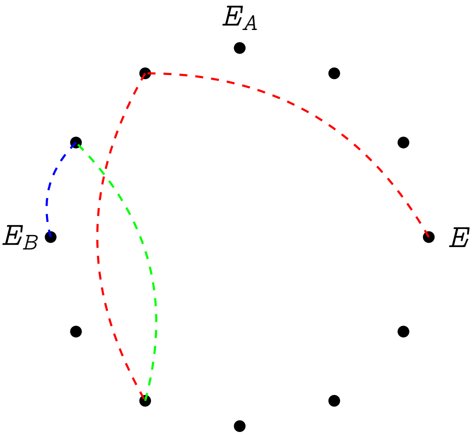


CSIDH key exchange

- A set of supersingular elliptic curves over $\mathbb{F}_p$;
- A group action by a commutative class group G;
- Small degree generators of G: degree 2, degree 3, degree 5, …

Key exchange:

- Alice picks secret $a = g_2^{a_2} g_3^{a_3} g_5^{a_5} \cdots,$
- Bob picks secret $b = g_2^{b_2} g_3^{b_3} g_5^{b_5} \cdots,$

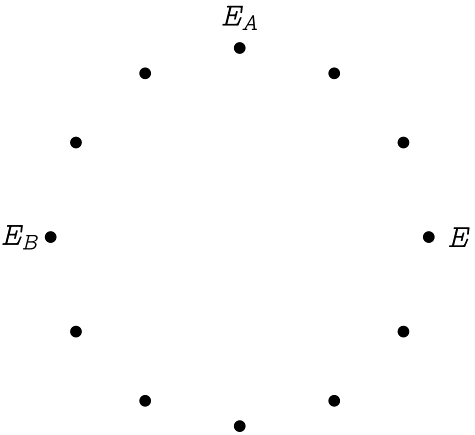


CSIDH key exchange

- A set of supersingular elliptic curves over $\mathbb{F}_p$;
- A group action by a commutative class group G;
- Small degree generators of G: degree 2, degree 3, degree 5, …

Key exchange:

- Alice picks secret $a = g_2^{a_2} g_3^{a_3} g_5^{a_5} \cdots,$
- Bob picks secret $b = g_2^{b_2} g_3^{b_3} g_5^{b_5} \cdots,$
- They exchange $E_A = a * E_1$ and $E_B = b * E_1$,

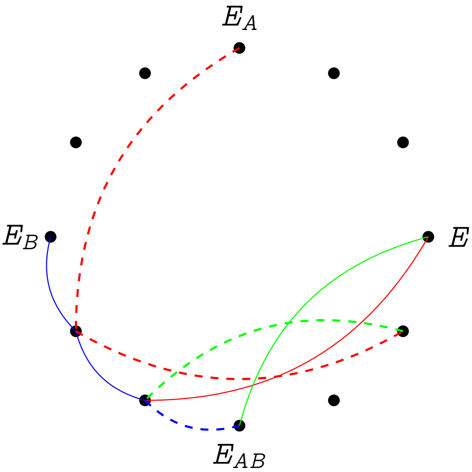


CSIDH key exchange

- A set of supersingular elliptic curves over $\mathbb{F}_p$;
- A group action by a commutative class group G;
- Small degree generators of G: degree 2, degree 3, degree 5, …

Key exchange:

- Alice picks secret $a = g_2^{a_2} g_3^{a_3} g_5^{a_5} \cdots$,
- Bob picks secret $b = g_2^{b_2} g_3^{b_3} g_5^{b_5} \cdots$,
- They exchange $E_A = a * E_1$ and $E_B = b * E_1$,
- Shared secret is $E_{AB} = (ab) * E_1 = a * E_B = b * E_A$.



SIDH key exchange

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.

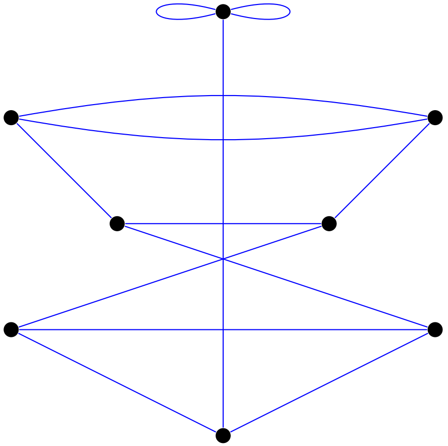


Figure: 2- and 3-isogeny graphs on $\mathbb{F}_{97^2}$.

SIDH key exchange

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.

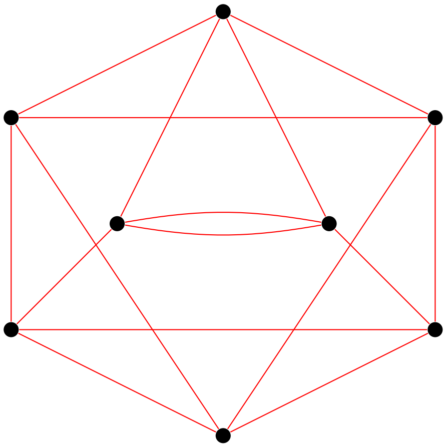


Figure: 2- and 3-isogeny graphs on $\mathbb{F}_{97^2}$.

SIDH key exchange

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.

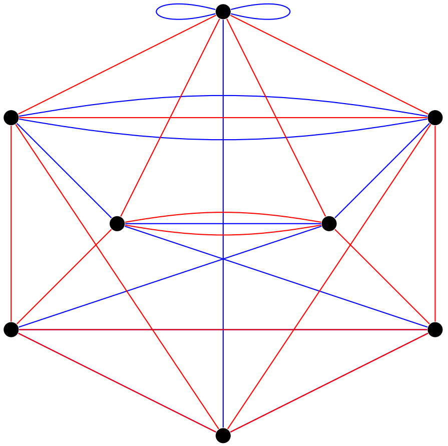


Figure: 2- and 3-isogeny graphs on $\mathbb{F}_{97^2}$.

SIDH key exchange

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

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

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

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

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

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

Security assumptions

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.

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	✓		✓	
SIDH		✓	✓	
Pairings				✓

A Σ-protocol from Diffie–Hellman[1]

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

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

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

A Σ-protocol from Diffie–Hellman[1]

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

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

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

A Σ-protocol from Diffie–Hellman[1]

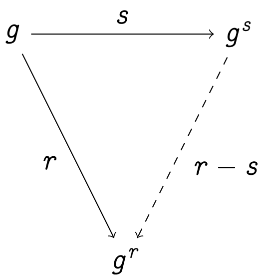
- A key pair (s, g^s);
- Commit to a random element g^r;
- Challenge with bit $b \in \{0, 1\}$;

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

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

A Σ-protocol from Diffie–Hellman[1]

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



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

A Σ-protocol from Diffie–Hellman[1]

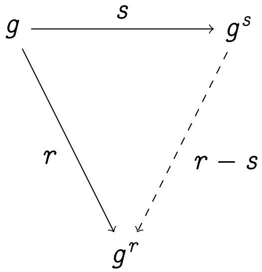
- A key pair (s, g^s);
- Commit to a random element g^r;
- Challenge with bit $b \in \{0, 1\}$;
- Respond with $c = r - b \cdot s \mod \#G$;
- Verify that $g^c(g^s)^b = g^r$.

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

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

A Σ-protocol from Diffie–Hellman[1]

- 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 $g^c (g^s)^b = g^r$.



Zero-knowledge

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

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

A Σ-protocol from Diffie–Hellman[1]

- 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.

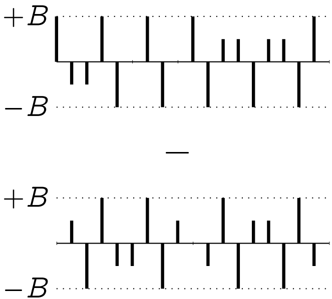
Unlike Schnorr, compatible with
group action Diffie–Hellman.

[1] 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"…

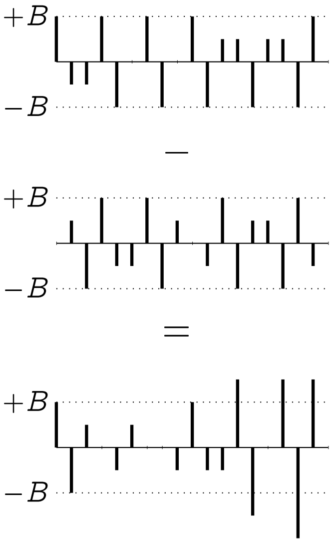


The trouble with groups of unknown structure

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

Compute the group structure and stop whining

CSI-FiSh: Beullens, Kleinjung and Vercauteren 2019 (eprint:2019/498)

- 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.

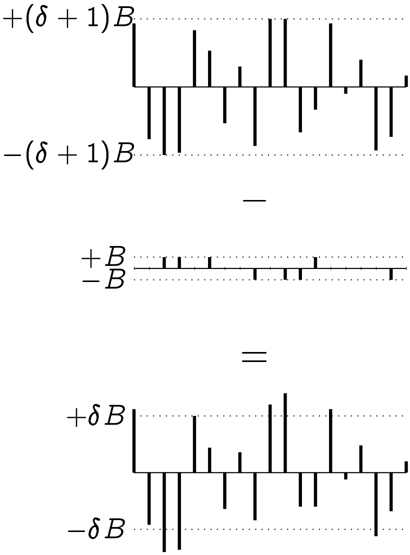
Do like the lattice people

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).

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.

Performance

- For λ-bit security, protocol must be repeated λ times in parallel;
- $\delta = \lambda n$ for a rejection probability $\leq 1/3$;
- Signature size $\approx \lambda n$ coefficients $\in [-\delta B, \delta B]$;
- Sign/verify time linear in $\|\vec{r} - \vec{s}\|_\infty \approx \lambda^2 n^2 B$.

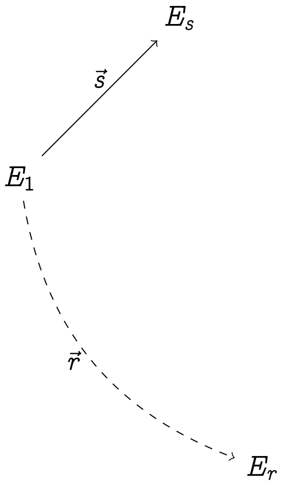
CSIDH instantiation (NIST-1)

Parameters:	$\lambda = 128$, $n = 74$, $B = 5$;
PK size:	64 B
SK size:	32 B
Signature:	20 KiB
Verify time:	10 hours
Sign time:	$3\times$ verify

Key/signature size compromise

- One key pair $(\vec{s}, E_s)$;
- Challenge $b \in \{0, 1\}$;
- Reveal $\vec{r} - b\vec{s}$;

$\rightarrow$ λ iterations;



Key/signature size compromise

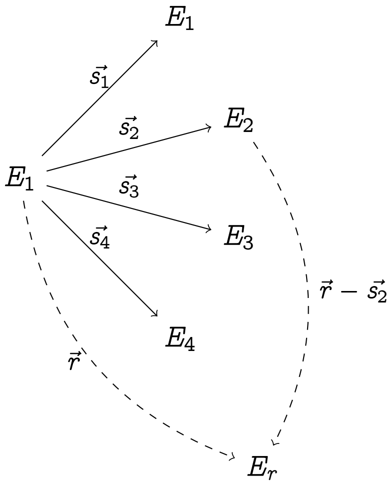
- One key pair $(\vec{s}, E_s)$;
- Challenge $b \in \{0, 1\}$;
- Reveal $\vec{r} - b\vec{s}$;

$\rightarrow$ λ iterations;

Compromise: $\mathbf{t}$-bit challenges

- $\mathbf{2^t}$ key pairs $(\vec{s_i}, E_i)$;
- Challenge $b \in \{0, 2^t\}$;
- Reveal $\vec{r} - \vec{s_b}$;

$\rightarrow$ $\lambda/\mathbf{t}$ iterations;



Key/signature size compromise

- One key pair $(\vec{s}, E_s)$;
- Challenge $b \in \{0, 1\}$;
- Reveal $\vec{r} - b\vec{s}$;

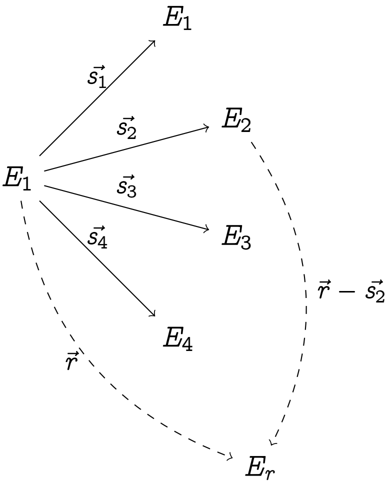
$\rightarrow$ λ iterations;

$\rightarrow$ Sample $r \xleftarrow{\$} [-\lambda nB, \lambda nB]$.

Compromise: t-bit challenges

- 2^t key pairs $(\vec{s_i}, E_i)$;
- Challenge $b \in \{0, 2^t\}$;
- Reveal $\vec{r} - \vec{s_b}$;

$\rightarrow$ λ/t iterations;



Key/signature size compromise

- One key pair $(\vec{s}, E_s)$;
- Challenge $b \in \{0, 1\}$;
- Reveal $\vec{r} - b\vec{s}$;

$\rightarrow$ λ iterations;

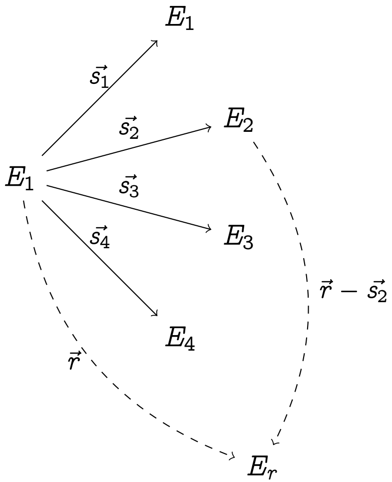
$\rightarrow$ Sample $r \xleftarrow{\$} [-\lambda nB, \lambda nB]$.

Compromise: $\mathbf{t}$-bit challenges

- $\mathbf{2^t}$ key pairs $(\vec{s_i}, E_i)$;
- Challenge $b \in \{0, 2^t\}$;
- Reveal $\vec{r} - \vec{s_b}$;

$\rightarrow$ $\lambda/\mathbf{t}$ iterations;

$\rightarrow$ Sample $r \xleftarrow{\$} [-\lambda nB/\mathbf{t}, \lambda nB/\mathbf{t}]$.



Public key compression

$$
\begin{tikzcd}[row sep=small]
 & E_1 \\
 & E_2 \\
E_1 \arrow[ruu] \arrow[ru] \arrow[rd] \arrow[rdd] & \\
 & E_3 \\
 & E_4
\end{tikzcd}
$$

Public key compression

$$
\begin{tikzcd}
& E_1 \arrow[r] & H(E_1) \arrow[dr] & & \\
& & & H(\bullet,\bullet) \arrow[ddr] & \\
& E_2 \arrow[r] & H(E_2) \arrow[ur] & & \\
E_1 \arrow[uuur] \arrow[ur] \arrow[dr] \arrow[dddr] & & & & H(\bullet,\bullet) = pk \\
& E_3 \arrow[r] & H(E_3) \arrow[dr] & & \\
& & & H(\bullet,\bullet) \arrow[uur] & \\
& E_4 \arrow[r] & H(E_4) \arrow[ur] & &
\end{tikzcd}
$$

- Construct Merkle tree on top of public keys, root is the new public key;

Public key compression

$$\begin{tikzcd}
 & E_1 \arrow[r] & H(E_1) \arrow[dr] & & \\
 & & & H(\bullet,\bullet) \arrow[ddr] & \\
 & E_2 \arrow[r] & H(E_2) \arrow[ur] & & \\
E_1 \arrow[uuur] \arrow[ur] \arrow[dr] \arrow[dddr] & & & & H(\bullet,\bullet) = pk \\
 & E_3 \arrow[r] & H(E_3) \arrow[dr] & & \\
 & & & H(\bullet,\bullet) \arrow[uur] & \\
 & E_4 \arrow[r] & H(E_4) \arrow[ur] & &
\end{tikzcd}$$

- Construct Merkle tree on top of public keys, root is the new public key;
- Include Merkle proof in the signature.

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	$O(\lambda^2 \log(\lambda))$	$O(\lambda t \log(\lambda))$	$O(\lambda^2 t)$

Recent speed/size compromises by Decru, Panny and Vercauteren

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

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

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

$\frac{1}{3}$-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

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

$\frac{1}{3}$-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

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

$\frac{1}{3}$-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

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

$\frac{1}{3}$-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).

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

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

Refresher: Boneh–Lynn–Shacham (BLS) signatures

Setup:

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

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

Public key: sP.

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

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

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

US patent 8,250,367 (Broker, Charles and Lauter 2012)

Signatures from isogenies + pairings

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

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

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

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

Pairing proofs: what for?

- Non-interactive, not post-quantum, not zero knowledge;
- Useful for (partially) validating SIDH public keys;
- Succinct: proof size, verification time independent of walk length!

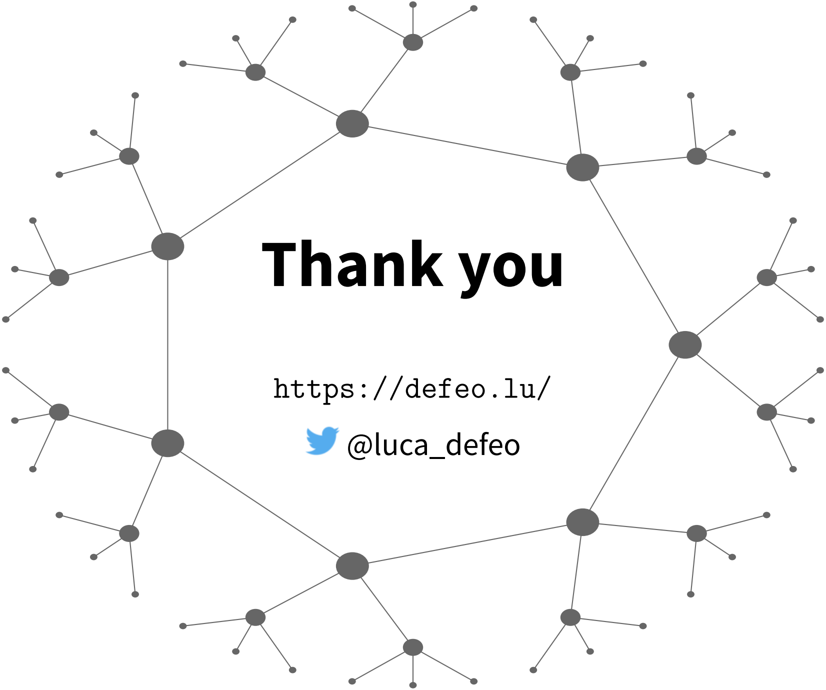
Application: Verifiable Delay Functions

D., Masson, Petit and Sanso 2019 (eprint:2019/166):

- Similar to time-lock puzzles;
- No secret: everything is public;
- Generating proof takes configurable *sequential* time T;
- Verifying proof takes time independent from T;
- Security assumptions very different and new!
- Applications to blockchains: randomness beacons, consensus protocols, …

Conclusion

- Different isogeny graphs enable different styles of proofs, different security assumptions.
- 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, but they do not scale.
- Pairing-based proofs are usable, but not interesting for signatures: look into succinctness, instead!
- Tons of open questions on classical and quantum security, on security proofs, and on constructions.
- Proofs can be chained easily: useful for multi-party supersingular curve generation (work in progress with J. Burdges).
- The isogenista dream: a one-pass post-quantum signature scheme based on walks in isogeny graphs.



Thank you

https://defeo.lu/

@luca_defeo