SQIsign

Past, present and future

Luca De Feo

IBM Research Zürich

March 4, 2024, UK Crypto Day

Why isogenies in 2024?

- Still the smallest keys;

Why isogenies in 2024?

- Still the smallest keys;
- No progress on the generic isogeny problem, despite SIDH attacks;

Why isogenies in 2024?

- Still the smallest keys;
- No progress on the generic isogeny problem, despite SIDH attacks;
- Very active field, fast progress;

Why isogenies in 2024?

- Still the smallest keys;
- No progress on the generic isogeny problem, despite SIDH attacks;
- Very active field, fast progress;
- Credible alternative in case other pq-schemes fail;

Why isogenies in 2024?

- Still the smallest keys;
- No progress on the generic isogeny problem, despite SIDH attacks;
- Very active field, fast progress;
- Credible alternative in case other pq-schemes fail;
- . . . but still a long way to go!

Supersingular isogenies and signing

2012 SIDH PoKs (DF, Jao, Plût), signatures (Yoo, Azarderakhsh, Jao)

2022 Ternary SIDH PoKs (DF, Dobson, Galbraith, Zobernig)

2023 *Curves you can trust* (Basso, Codogni, Connolly, DF, Fouotsa, Lido, Morrison, Panny, Patranabis, Wesolowski)

SIDH		
Best security		

Supersingular isogenies and signing

2012 SIDH PoKs (DF, Jao, Plût), signatures (Yoo, Azarderakhsh, Jao)

2019 SeaSign (DF, Galbraith)

CSI-FiSh (Beullens, Kleinjung, Vercauteren)

2022 Ternary SIDH PoKs (DF, Dobson, Galbraith, Zobernig)

2023 *Curves you can trust* (Basso, Codogni, Connolly, DF, Fouotsa, Lido, Morrison, Panny, Patranabis, Wesolowski)

SIDH	CSIDH	
Best security	Group, ring, threshold, ...	

Supersingular isogenies and signing

2012	SIDH PoKs (DF, Jao, Plût), signatures (Yoo, Azarderakhsh, Jao)
2017	Galbraith–Petit–Silva
2019	SeaSign (DF, Galbraith)
	CSI-FiSh (Beullens, Kleinjung, Vercauteren)
2020	SQIsign (DF, Kohel, Leroux, Petit, Wesolowski)
2022	Ternary SIDH PoKs (DF, Dobson, Galbraith, Zobernig)
2023	*Curves you can trust* (Basso, Codogni, Connolly, DF, Fouotsa, Lido, Morrison, Panny, Patranabis, Wesolowski)
2024	SQIsignHD (Dartois, Leroux, Robert, Wesolowski)

SIDH	CSIDH	Deuring
Best security	Group, ring, threshold, . . .	Most compact

SQIsign: Signatures from the effective Deuring correspondence

$$
\begin{tikzcd}
 & E_0 \arrow[r, "\psi"] \arrow[dl, dashed, "\tau"'] & E_1 \arrow[d, "\varphi"] \\
E_A \arrow[rr, "\sigma"] & & E_2
\end{tikzcd}
$$

Most compact PQ signature scheme: PK + Signature combined **5 $\times$ smaller** than Falcon.

Secret Key (bytes)	Public Key (bytes)	Signature (bytes)	Security
782	64	177	NIST-1
1138	96	263	NIST-3
1509	128	335	NIST-5

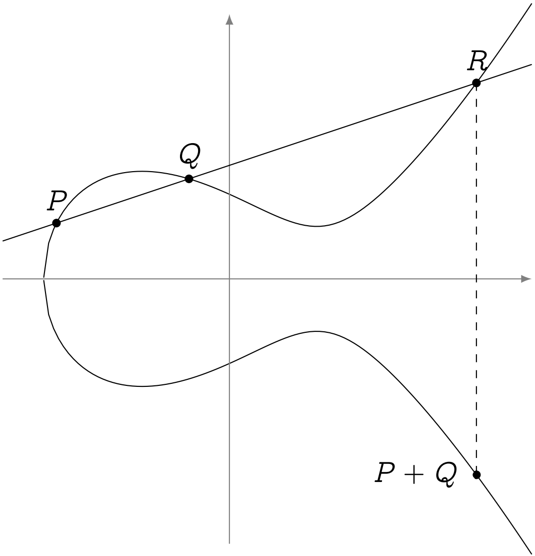
Elliptic curves

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

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.

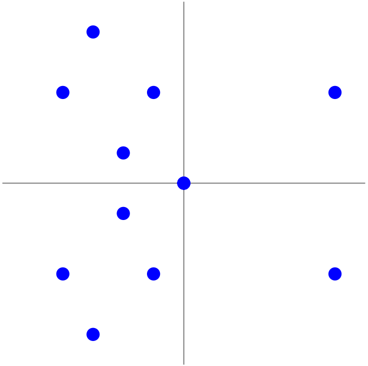


Isogenies = finite-kernel group morphisms: $E \to E/K$

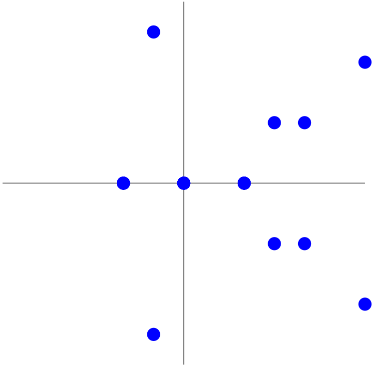
Endomorphisms = isogenies $E \to E$

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

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



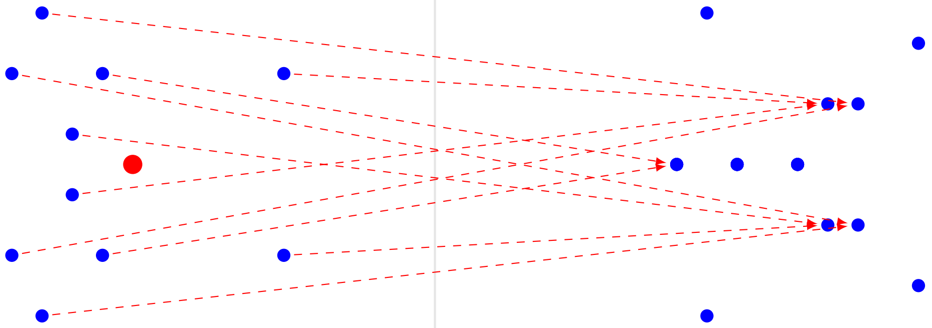
$$E' \; : \; y^2 = x^3 - 4x$$



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

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

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



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

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

Some endomorphisms

Scalar multiplication: $[N] : E \to E$

Frobenius: $(x, y) \mapsto (x^p, y^p)$ (on curves over $\mathbb{F}_p$)

Automorphisms: $(x, y) \mapsto (-x, iy)$ (on curve $y^2 = x^3 + x$)

Endomorphisms = imaginary quadratic integers

Endomorphisms form a ring:

$$\omega \circ (\varphi + \psi) \quad = \quad \omega \circ \varphi + \omega \circ \psi$$

Every endomorphism satisfies a quadratic equation

$$\omega^2 - t\omega + n = 0$$

with $t, n \in \mathbb{Z}$ and $t^2 - 4n \leq 0$.

Endomorphism rings = Ideal lattices

$\mathrm{End}(E)$ is a free $\mathbb{Z}$-module of rank 1, 2 or 4. As a ring:

1) $\mathrm{End}(E) \simeq \mathbb{Z}$;

2) $\mathrm{End}(E)$ is isomorphic to an order[1] of a quadratic imaginary field;

4) $\mathrm{End}(E)$ is isomorphic to a maximal order[1] of the quaternion algebra ramified at p and ∞.

[1] order = subring of maximal rank

An example

The curve of j-invariant 1728

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

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

Endomorphisms

$\operatorname{End}(E) \subset \mathbb{Q}\langle\iota, \pi\rangle$, with:

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

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

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

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

N-torsion

$$E[N] \quad \simeq \quad \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$$

*over an algebraically closed field

Endomorphisms = 2×2 matrices

Fix any basis $\langle P, Q\rangle$ of $E[N]$

$$\begin{aligned} \omega : E[N] &\longrightarrow E[N] \\ \begin{pmatrix} x \\ y \end{pmatrix} &\longmapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \mod N \end{aligned}$$

Tate's isogeny theorem

When E is supersingular:

$$\mathrm{End}(E)/N\,\mathrm{End}(E) \simeq \mathcal{M}_{2\times 2}(\mathbb{Z}/N\mathbb{Z})$$

When E is ordinary:

$$\mathrm{End}(E)/N\,\mathrm{End}(E) \simeq \{\text{Diagonal matrices}\} \subset \mathcal{M}_{2\times 2}(\mathbb{Z}/N\mathbb{Z})$$

Isogenies = Ideals

$$E' \xleftarrow{\varphi} E$$

$$\varphi \in \mathrm{Hom}(E, E')$$

Isogenies = Ideals

$$\begin{tikzcd} E' & E \arrow[l, "\varphi"'] \arrow[loop right, "\omega"] \end{tikzcd}$$

$$\varphi \circ \omega \in \mathrm{Hom}(E, E')$$

Isogenies = Ideals

$$\begin{tikzcd} E' \arrow[loop left, "\omega'"] & & E \arrow[ll, "\varphi"'] \end{tikzcd}$$

$$\omega' \circ \varphi \in \mathrm{Hom}(E, E')$$

The Deuring correspondences

Ellitpic curves	Number fields / Quaternion algebras
Endomorphisms	Algebraic integers
Endomorphism ring	(Maximal) order
Isogeny	Invertible ideal
Isogeny degree	Ideal norm
Isogeny composition	Ideal multiplication
Isogenies $\bullet \rightrightarrows \bullet$	Ideal classes
Dual isogeny	Conjugate ideal

Two computational worlds

	Ordinary / CSIDH	Supersingular
$\mathrm{rank}\,\mathrm{Hom}(E, E')$	2	4
Endomorphism algebra	number field	quaternion algebra
Maximal orders	one	many
Ideal class...	...group	...set
Find isogeny $E \to E'$	hard	hard
Convert isogenies $\leftrightarrow$ ideals	easy-ish[1]	easy[1]
Compute $\mathrm{End}(E)$	easy	hard

[1]When $\mathrm{End}(E)$ is known

A loose analogy: discrete log groups

Input	Output	
Curve E, isogeny $\phi : E \to E'$	E'	easy
Curves E, E'	$\phi : E \to E'$	hard
Generator g, exponent a	g^a	easy
Elements g, h	$\log_g(h)$	hard

The Deuring correspondence (for supersingular curves)

An equivalence of categories (roughly)

$\{\omega \in B_{p,\infty} \mid \omega I = I\}$
left order

connecting ideal

$\{\omega \in B_{p,\infty} \mid I\omega = I\}$
right order

$$\begin{tikzcd}
\mathcal{O} \arrow[rr, "I"] & & \mathcal{O}' \\
E \arrow[rr, "\phi_I"'] & & E'
\end{tikzcd}$$

supersingular curve

isogeny

supersingular curve

The effective Deuring correspondence

Input	Output	
random E	$\mathrm{End}(E)$	hard
random E	$\omega \in \mathrm{End}(E)$	hard
random E	$\phi : E_0 \to E$	hard
$\mathrm{End}(E)$	E	easy
$\mathrm{End}(E), \mathrm{End}(E')$	connecting ideal	easy
$I \subset \mathrm{End}(E)$	$\phi_I : E \to E'$	easy
$\mathrm{End}(E), \quad \phi : E \to E'$	$I_\phi \subset \mathrm{End}(E), \quad \mathrm{End}(E')$	easy

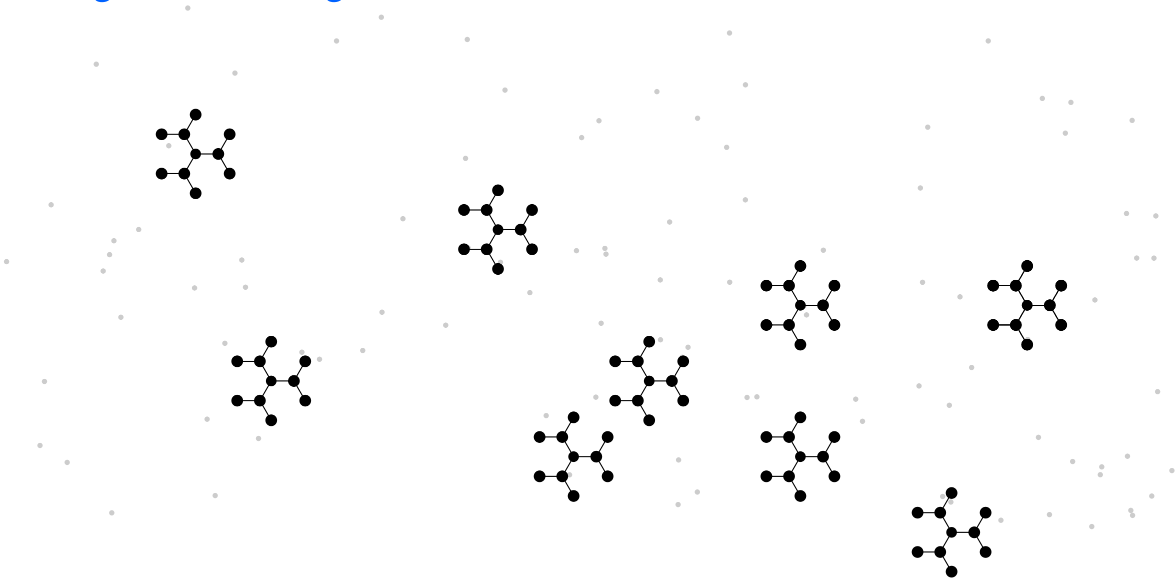
The endomorphism ring problem

Given a random supersingular curve E, compute $\mathtt{End}(E)$

Contagious knowledge

Contagious knowledge

Contagious knowledge



Galbraith–Petit–Silva (2017)

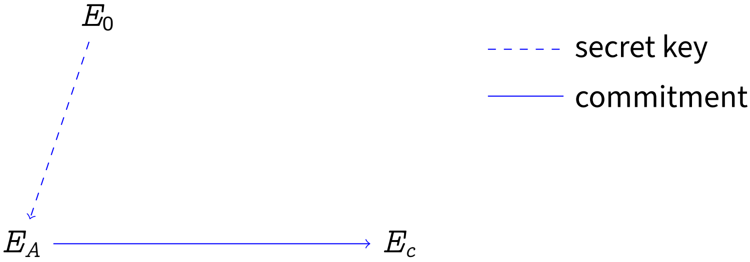
Σ-protocol with binary challenge:

$$\begin{tikzcd} E_0 \arrow[d, dashed] \\ E_A \end{tikzcd}$$

- - - - - - secret key

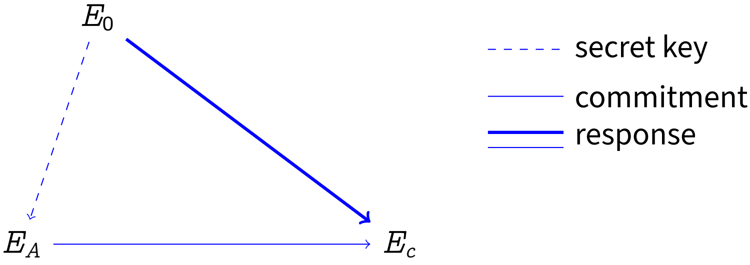
Galbraith–Petit–Silva (2017)

Σ-protocol with binary challenge:



Galbraith–Petit–Silva (2017)

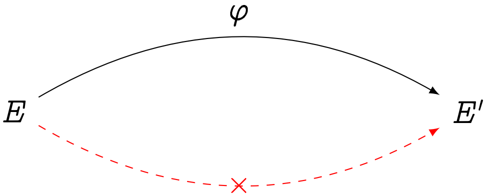
Σ-protocol with binary challenge:



Equivalent isogenies $\leftrightarrow$ equivalent ideals (KLPT)

$$\begin{tikzcd} E \arrow[r, bend left, "\varphi"] & E' \end{tikzcd}$$

Equivalent isogenies ↔ equivalent ideals (KLPT)



Equivalent isogenies $\leftrightarrow$ equivalent ideals (KLPT)

$$E \xrightarrow{\varphi} E'$$

$$\mathrm{End}(E) \xrightarrow{I_\varphi} \mathrm{End}(E')$$

Equivalent isogenies $\leftrightarrow$ equivalent ideals (KLPT)

$$\begin{tikzcd} E \arrow[rr, bend left, "\varphi"] & & E' \end{tikzcd}$$

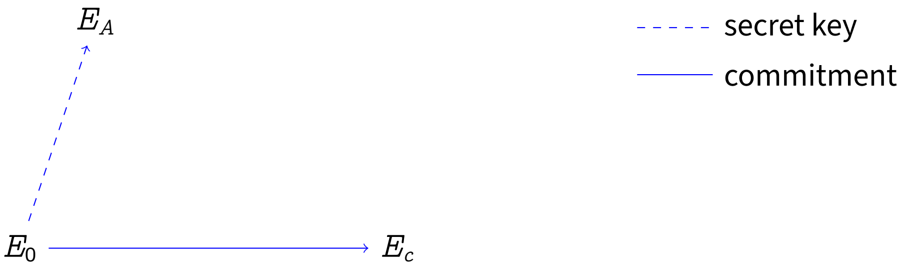
$$\begin{tikzcd} \mathrm{End}(E) \arrow[rr, bend left, "I_\varphi"] \arrow[rr, bend right, "J = I_\varphi \alpha"'] & & \mathrm{End}(E') \end{tikzcd}$$

Equivalent isogenies $\leftrightarrow$ equivalent ideals (KLPT)

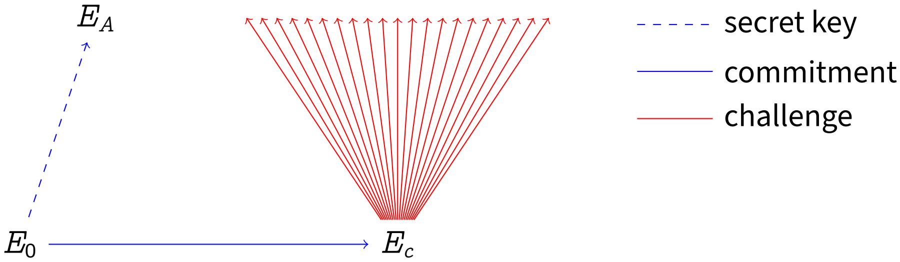
$$\begin{tikzcd} E \arrow[r, bend left, "\varphi"] \arrow[r, bend right, "\varphi_J"'] & E' \end{tikzcd}$$

$$\begin{tikzcd} \mathrm{End}(E) \arrow[r, bend left, "I_\varphi"] \arrow[r, bend right, "J = I_\varphi \alpha"'] & \mathrm{End}(E') \end{tikzcd}$$

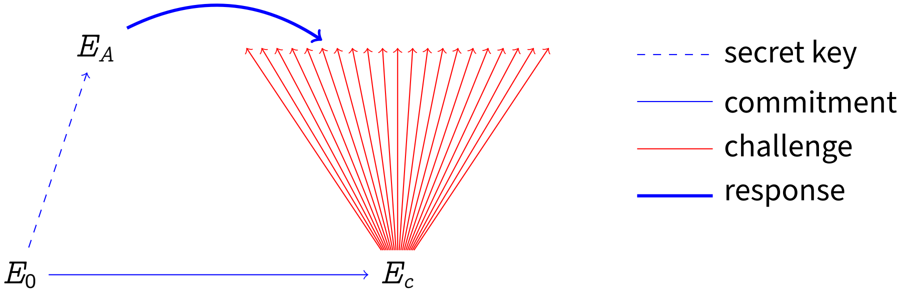
Seeking a larger challenge space



Seeking a larger challenge space



Seeking a larger challenge space



SQIsign: Signatures from the effective Deuring correspondence

$$
\begin{tikzcd}
 & E_0 \arrow[r, "\psi"] \arrow[dl, dashed, "\tau"'] & E_1 \arrow[d, "\varphi"] \\
E_A \arrow[rr, "\sigma"] & & E_2
\end{tikzcd}
$$

- commitment isogeny (prover)
- challenge isogeny (verifier)
- response isogeny (prover)
- secret key isogeny

Most compact PQ signature scheme: PK + Signature combined **5×smaller** than Falcon.

Bytes			Mcycles			
Secret Key	Public Key	Signature	Keygen	Sign	Verify	Security
782	64	177	3,728	5,779	108	NIST-1
1,138	96	263	23,734	43,760	654	NIST-3
1,509	128	335	91,049	158,544	2,177	NIST-5

SQIsign: the future

	AprèsSQI (CKMR24)	SQIsignHD (DLRW24)
Technique	Extension fields	*SIDH attacks*
Pros	Faster verification	Way faster signing Smaller signatures *Better* securty proof Easy scaling
Cons	Complex implementation	Slower verification Monstrous mathematics Annoying proof artifact

Thank you

`https://defeo.lu/`

@luca_defeo@ioc.exchange

@luca_defeo