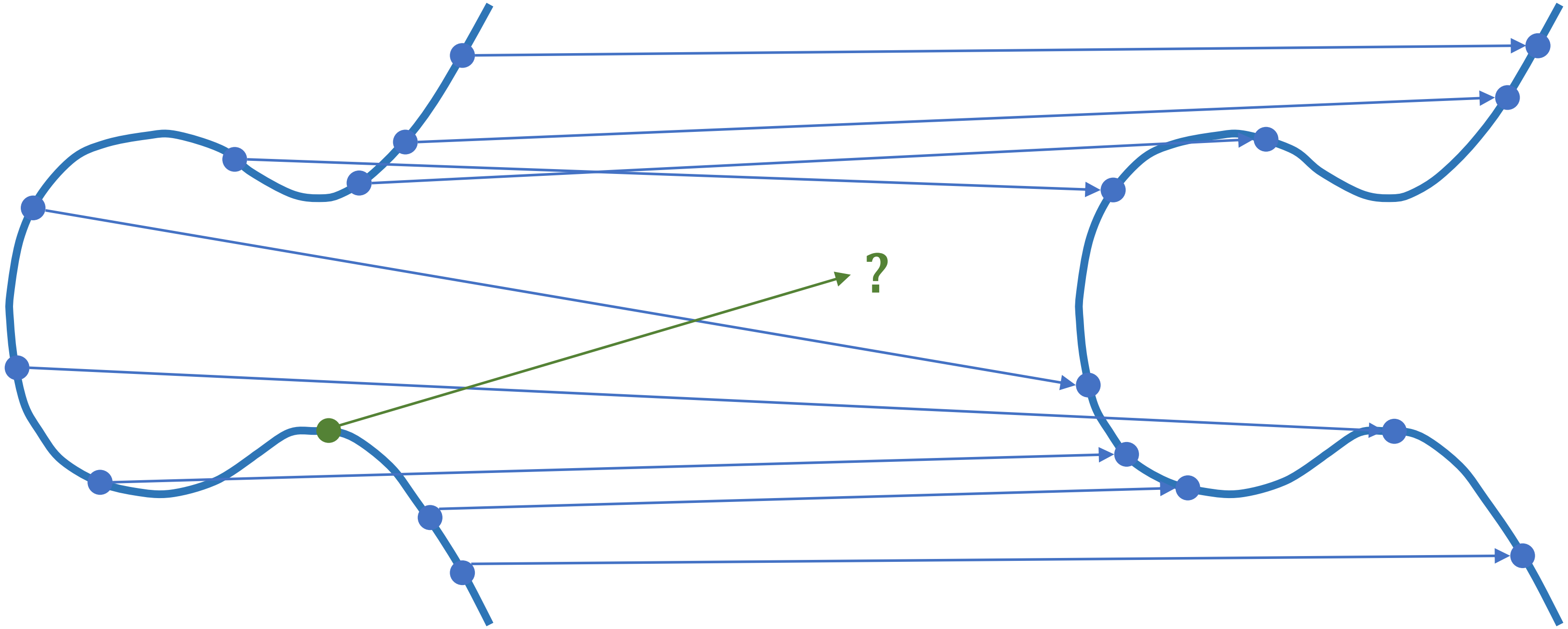
Isogeny interpolation for elliptic curves, and applications

Wouter Castryck, Thomas Decru, Luciano Maino, Chloe Martindale,
Lorenz Panny, Giacomo Pope, Damien Robert, Benjamin Wesolowski



ANTS XVI, Massachusetts Institute of Technology, Cambridge, 15/07/2024

COSIC

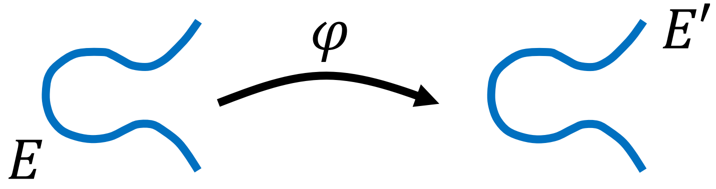
KU LEUVEN

1. Problem statement and main result

Definition

A **homomorphism** between two elliptic curves E and E' over a field k is a morphism $\varphi\colon E \to E'$ such that $\varphi(\infty) = \infty'$.

An **isogeny** is a non-constant homomorphism.



<u>Example:</u> let $E\colon y^2 = x^3 + 1$ and $E'\colon y^2 = x^3 - 27$, then

$$\varphi\colon E \to E'\colon \infty \mapsto \infty, (x,y) \mapsto \begin{cases} \left(\dfrac{x^3+4}{x^2}, y\dfrac{x^3-8}{x^3}\right) & \text{if } (x,y) \neq (0, \pm 1), \\ \infty \text{ if not} & \end{cases}$$

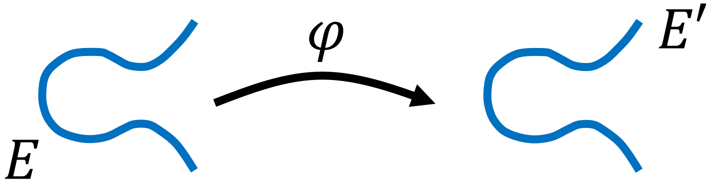
is an isogeny of degree 3.

1. Problem statement and main result

Definition

A **homomorphism** between two elliptic curves E and E' over a field k is a morphism $\varphi\colon E \to E'$ such that $\varphi(\infty) = \infty'$.

An **isogeny** is a non-constant homomorphism.



Quick facts:

- on $\bar{k}$-points, isogenies are **surjective group homomorphisms** with finite kernel,
- $\#\ker\varphi \leq \deg\varphi$, where equality holds if and only if φ is separable.

Cauchy—Schwarz inequality

For any pair of isogenies $\varphi_1\colon E \to E'$ and $\varphi_2\colon E \to E'$ we have:

$$|\deg(\varphi_1 - \varphi_2) - \deg\varphi_1 - \deg\varphi_2| \leq 2\sqrt{\deg\varphi_1 \deg\varphi_2}.$$

E.g., **Hasse's theorem** for $k = \mathbf{F}_q$: $\left|\#E\left(\mathbf{F}_q\right) - q - 1\right| = \left|\deg\left(\mathrm{Frob}_q - \mathrm{id}\right) - q - 1\right| \leq 2\sqrt{q}$.

1. Problem statement and main result

Corollary [JU18]

A degree-d isogeny $\varphi: E \to E'$ is **uniquely determined** by the images of any $4d+1$ points.

<u>Proof:</u>
- Let $\varphi_1 \neq \varphi_2$ be degree-d isogenies coinciding on $\geq 4d+1$ points.
- Then $\deg(\varphi_1 - \varphi_2) \geq \#\ker(\varphi_1 - \varphi_2) \geq 4d+1$, but by Cauchy—Schwarz:

$$|\deg(\varphi_1 - \varphi_2) - d - d| \leq 2\sqrt{d \cdot d} \quad \Rightarrow \quad \deg(\varphi_1 - \varphi_2) \leq 4d \;\; ↯$$

Bound is **sharp**: φ and $-\varphi$ agree on $[2]^{-1}(\ker \varphi)$.

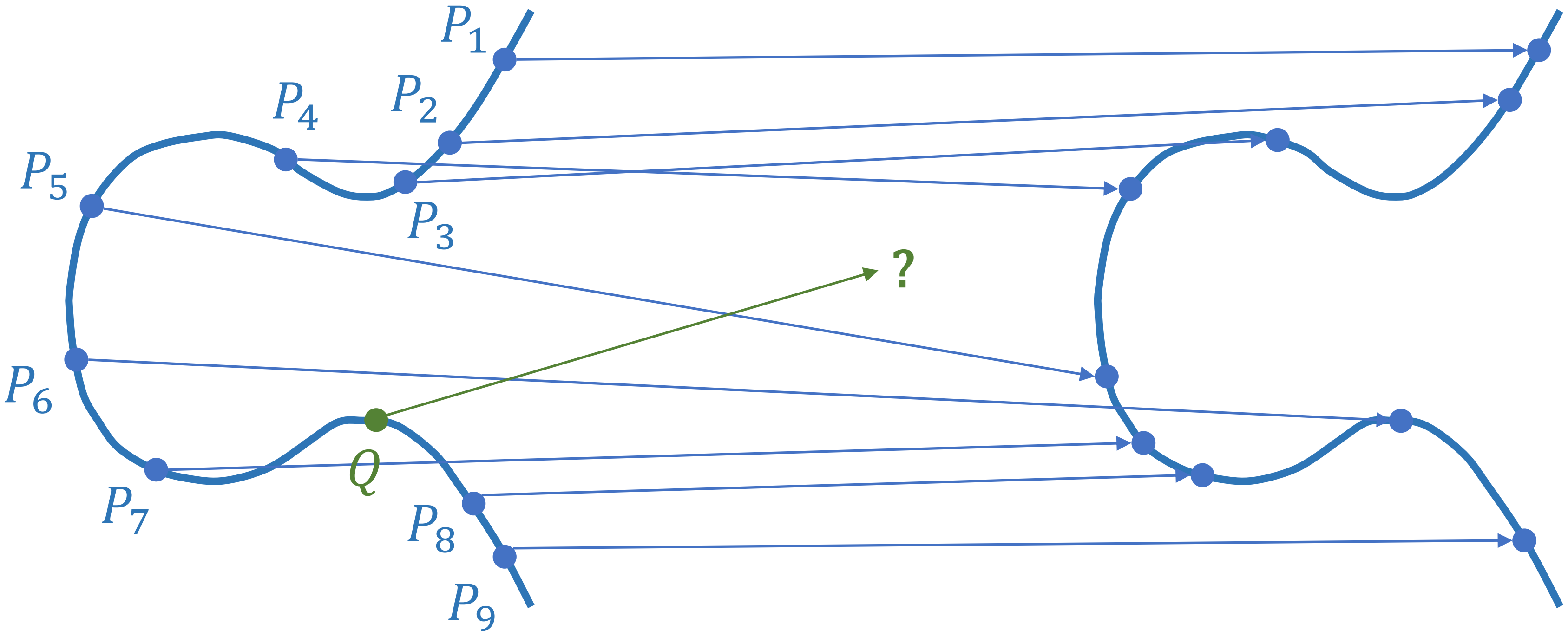
Isogeny interpolation problem

- Let $\varphi: E \to E'$ be an unknown isogeny of (known) degree d.
- Let us be given a set $\{P_1, \dots, P_r\} \subset E$ generating a group of size at least $4d+1$, along with the image points $\varphi(P_i) \in E'$ for $i = 1, \dots, r$.
- Given any $Q \in E$, compute $\varphi(Q)$.

1. Problem statement and main result

Isogeny interpolation problem

- Let $\varphi: E \to E'$ be an unknown isogeny of (known) degree d.
- Let us be given a set $\{P_1, \dots, P_r\} \subset E$ generating a group of size at least $4d + 1$, along with the image points $\varphi(P_i) \in E'$ for $i = 1, \dots, r$.
- Given any $Q \in E$, compute $\varphi(Q)$.



1. Problem statement and main result

Isogeny interpolation problem

- Let $\varphi: E \to E'$ be an unknown isogeny of (known) degree d.
- Let us be given a set $\{P_1, \ldots, P_r\} \subset E$ generating a group of size at least $4d+1$, along with the image points $\varphi(P_i) \in E'$ for $i = 1, \ldots, r$.
- Given any $Q \in E$, compute $\varphi(Q)$.

Theorem [CDM+24]

Assume $k = \mathbf{F}_q$, write $G = \langle P_1, \ldots, P_r \rangle$, and assume $\gcd(\#G, q) = 1$. There is an algorithm for the isogeny interpolation problem, whose running time is polynomial in:

- the length of the input,
- the maximum of ℓ and the degree of the field of definition of $E\left[\ell^{\lfloor e/2 \rfloor}\right]$, over all prime powers ℓ^e dividing $\#G$.

1. Problem statement and main result

Theorem [CDM+24]

Assume $k = \mathbf{F}_q$, write $G = \langle P_1, \dots, P_r \rangle$, and assume $\gcd(\#G, q) = 1$. There is **an algorithm for the isogeny interpolation problem**, whose running time is polynomial in:

- the length of the input,
- the maximum of ℓ and the degree of the field of definition of $E\left[\ell^{\lfloor e/2 \rfloor}\right]$,

  over all prime powers ℓ^e dividing $\#G$.

Remarks:

- polynomial time, but concrete **runtime varies largely with parameters**,
- supersingular: conditions on $\gcd(\#G, q)$ and $E\left[\ell^{\lfloor e/2 \rfloor}\right]$ are void,
- ordinary: condition on $\gcd(\#G, q)$ likely removable via Dieudonné modules,
- much generalizes to p.p. abelian varieties of dim $g \geq 1$, or to arbitrary fields supporting efficient arithmetic, but full extent not clear yet.

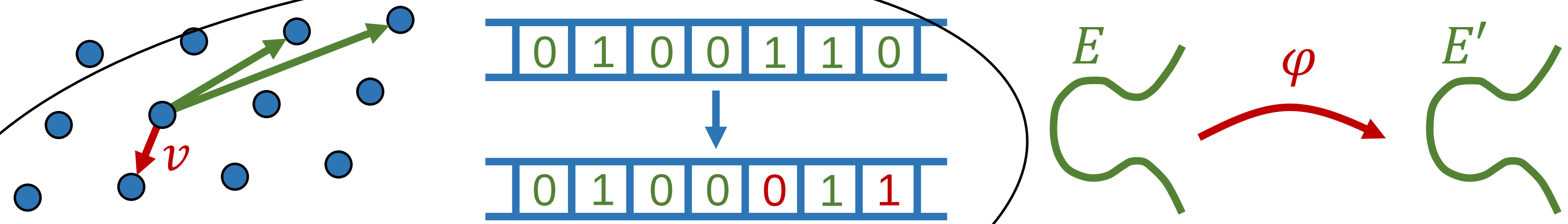
2. Context: post-quantum cryptography standardization

1994: “Polynomial-time algorithms for **prime factorization** and **discrete logarithms** on a quantum computer” by P. Shor [Sho94]

gradually growing concern

2017: NIST initiates “standardization effort” for post-quantum key exchange and signatures

Main contending **hard mathematical problems**:



$$\begin{cases} f_1(s_1, \dots, s_n) = 0 \\ \vdots \\ f_m(s_1, \dots, s_n) = 0 \end{cases}$$

finding short vectors in lattices

decoding for random linear codes

finding isogenies between elliptic curves

solving non-linear systems of equations

“noisy linear algebra”

2. Context: post-quantum cryptography standardization

2020: Preliminary NIST standards:

- **LMS** (stateful signatures)
- **XMSS** (stateful signatures)

2022: First main NIST standards:

- **Kyber** (key encapsulation)
- **Dilithium** (signatures)
- **Falcon** (signatures)
- **SPHINCS+** (signatures)

few months earlier [Beu22]

$$\begin{cases} f_1(s_1, \dots, s_n) = 0 \\ \vdots \\ f_m(s_1, \dots, s_n) = 0 \end{cases}$$

~~**Rainbow** (signatures)~~

now broken [CD23,MMP+23,Rob23]

Moved to extra round of scrutiny:

- **BIKE** (key encapsulation)
- **McEliece** (key encapsulation)
- **HQC** (key encapsulation)
- ~~**SIKE** (key encapsulation)~~

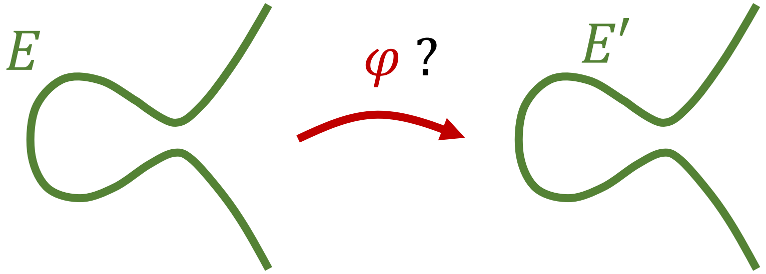
2023: New NIST call:

verification. NIST is open to receiving additional submissions based on structured lattices, but is intent on diversifying the post-quantum signature standards. As such

3. Isogeny-based cryptography 1.x

The isogeny-finding problem:

Input: two isogenous elliptic curves E, E' over $\mathbf{F}_q$



Output: an isogeny $\varphi: E \to E'$

easily tested via point counting, in view of Tate's isogeny theorem [Tat66]

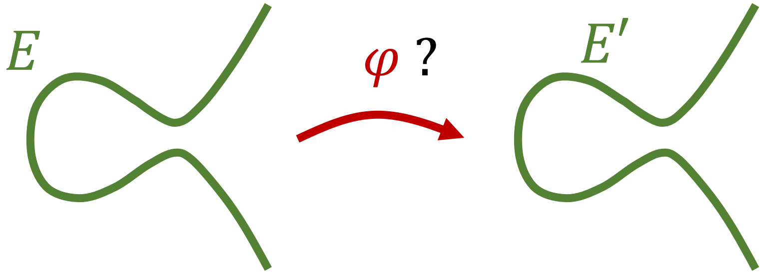
e.g., as a composition of small-degree isogenies

SEE LATER

3. Isogeny-based cryptography 1.x

The isogeny-finding problem:

Input: two isogenous elliptic curves E, E' over $\mathbf{F}_q$



Output: an isogeny $\varphi: E \to E'$

Best attacks in general:[1, 2] $\tilde{O}(q^{1/4})$ classical and $\tilde{O}(q^{1/8})$ quantum [BJS14].

Main selling point: low bandwidth requirements (as in classical elliptic-curve cryptography)

---

[1] Large classes of elliptic curves admit more efficient attacks.

[2] For exceptional classes of ordinary elliptic curves, the best-known complexity worsens to $\tilde{O}(q^{2/5})$; see talk Steven Galbraith.

3. Isogeny-based cryptography 1.x

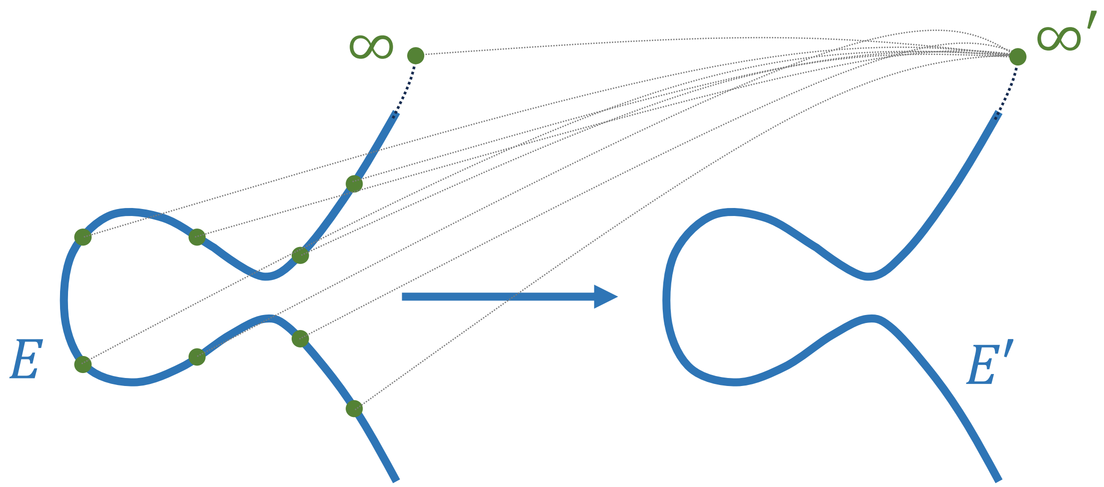
Flagship protocol until 2022: Supersingular Isogeny Key Encapsulation [JD11]

- Another quick fact: for any finite subgroup $G \subset E$ there exists a separable isogeny

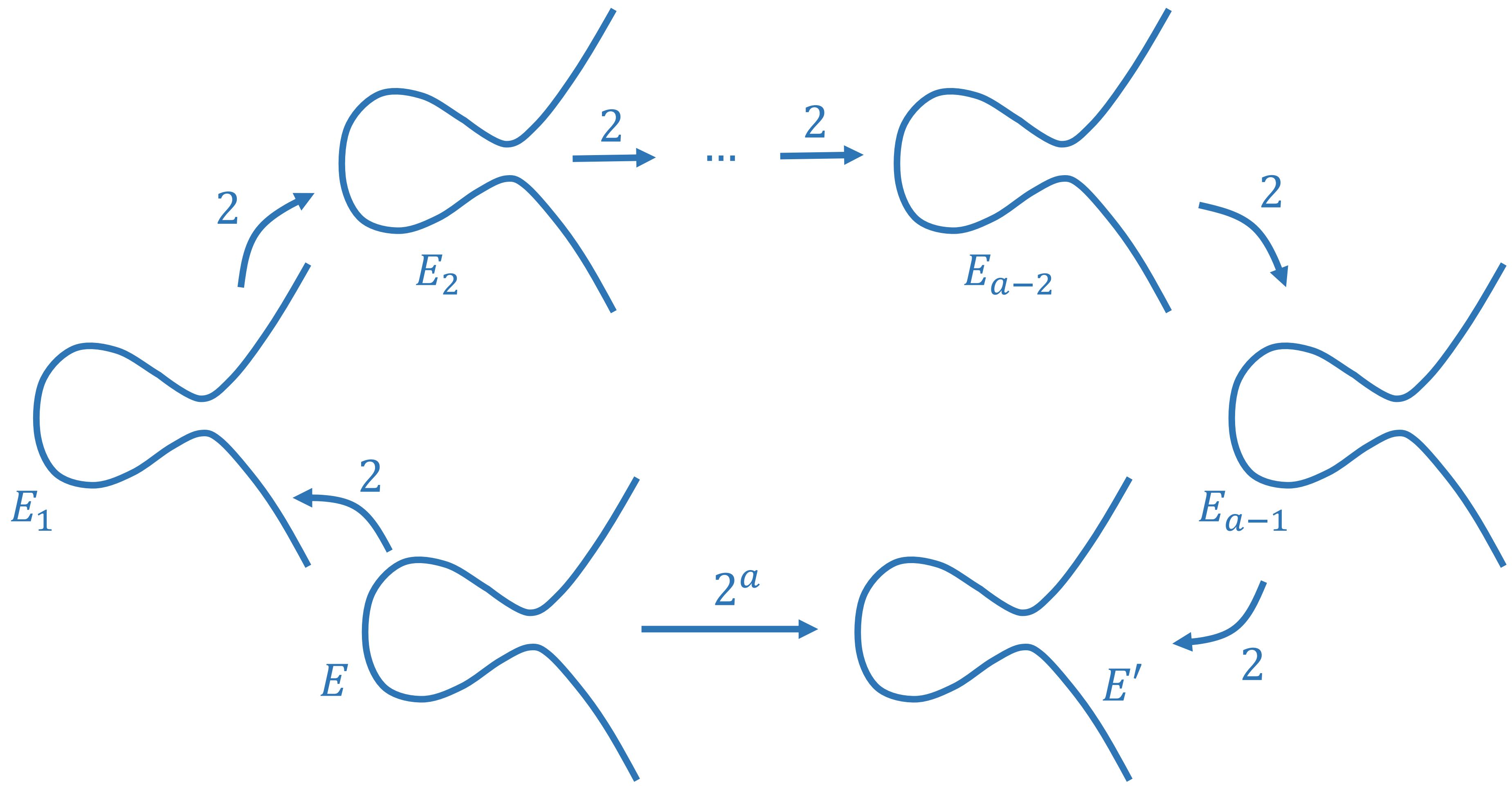
$$\varphi: E \to E' \text{ with } G = \ker(\varphi)$$

and this isogeny is unique up to composition (on the right) with an isomorphism.

makes sense to write $E' = E/G$



- Vélu's formulas [Vél73] compute φ and E', but only efficient when $\#G$ is smooth.



- Vélu's formulas [Vél73] compute φ and E', but only efficient when $\#G$ is smooth.

3. Isogeny-based cryptography 1.x

SIKE's high-level idea: Alice and Bob choose secret subgroups $A \subset E[2^a]$, $B \subset E[3^b]$

$$
\begin{tikzcd}
E \arrow[r, "\varphi_A"] \arrow[d, "\varphi_B"'] & E_A = E/A \arrow[d] \\
E_B = E/B \arrow[dr] & E_{AB} = E_A/\varphi_A(B) \\
 & E/(A+B) \arrow[u, phantom, "\cong"] \\
 & E_{BA} = E_B/\varphi_B(A) \arrow[u, phantom, "\cong"]
\end{tikzcd}
$$

Constructive problem:

allow Bob to determine $\varphi_A(B)$
without revealing φ_A

... and likewise
for Alice

3. Isogeny-based cryptography 1.x

Solution [JD11]: Alice and Bob choose public bases $P_A, Q_A \in E[2^a]$, $P_B, Q_B \in E[3^b]$

$$\begin{tikzcd}
E \arrow[rr, "\varphi_A", "A = \langle P_A + \alpha Q_A \rangle"'] \arrow[d, "\varphi_B"', "B = \langle P_B + \beta Q_B \rangle"] & & E_A = E/A \arrow[d] \\
E_B = E/B \arrow[rr] & & E_{BA} \cong E_{AB}
\end{tikzcd}$$

Alice reveals
$\varphi_A(P_B), \varphi_A(Q_B)$

allows Bob to compute
$\varphi_A(B) = \langle \varphi_A(P_B) + \beta \varphi_A(Q_B) \rangle$

Bob reveals
$\varphi_B(P_A), \varphi_B(Q_A)$ $\longrightarrow$ allows Alice to compute $\varphi_B(A) = \langle \varphi_B(P_A) + \alpha \varphi_B(Q_A) \rangle$

3. Isogeny-based cryptography 1.x

Solution [JD11]: Alice and Bob choose public bases $P_A, Q_A \in E[2^a]$, $P_B, Q_B \in E[3^b]$

$$\begin{tikzcd}[column sep=huge, row sep=huge]
E \arrow[r, "\varphi_A", "A = \langle P_A + \alpha Q_A \rangle"'] \arrow[d, "\varphi_B"', "B = \langle P_B + \beta Q_B \rangle"] & E_A = E/A \arrow[d] \\
E_B = E/B \arrow[r] & E_{BA} \cong E_{AB}
\end{tikzcd}$$

Alice reveals
$\varphi_A(P_B), \varphi_A(Q_B)$

Bob reveals
$\varphi_B(P_A), \varphi_B(Q_A)$

Dramatically weakens the system!

- compute $\varphi_A(P_A), \varphi_A(Q_A)$ using isogeny interpolation
- find α as an (easy) discrete log.

4. Isogeny interpolation: balanced case

"The number of curves of genus two with elliptic differentials" by E. Kani [Kan97]

Lemma. *Consider a commuting diagram of isogenies:*

$$\begin{tikzcd} E_1 \arrow[r, "\beta"] \arrow[d, "\alpha"'] & E_3 \arrow[d, "\gamma"] \\ E_2 \arrow[r, "\delta"'] & E_4 \end{tikzcd}$$

same degree

same degree

4. Isogeny interpolation: balanced case

"The number of curves of genus two with elliptic differentials" by E. Kani [Kan97]

Lemma. *Consider a commuting diagram of isogenies:*

"isogeny diamonds"

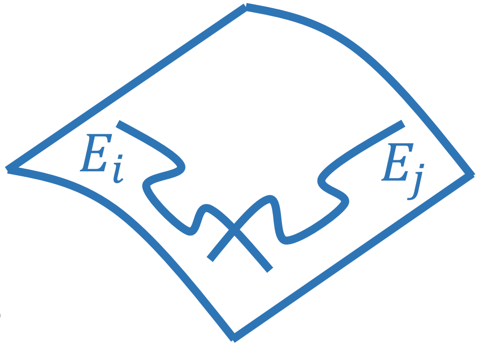
$$\begin{tikzcd} E_1 \arrow[r, "\beta"] \arrow[d, "\alpha"'] & E_3 \arrow[d, "\gamma"] \\ E_2 \arrow[r, "\delta"'] & E_4 \end{tikzcd}$$

4. Isogeny interpolation: balanced case

"The number of curves of genus two with elliptic differentials" by E. Kani [Kan97]

Lemma. *Consider a commuting diagram of isogenies:*

$$\begin{tikzcd} E_1 \arrow[r, "\beta"] \arrow[d, "\alpha"'] & E_3 \arrow[d, "\gamma"] \\ E_2 \arrow[r, "\delta"'] & E_4 \end{tikzcd}$$



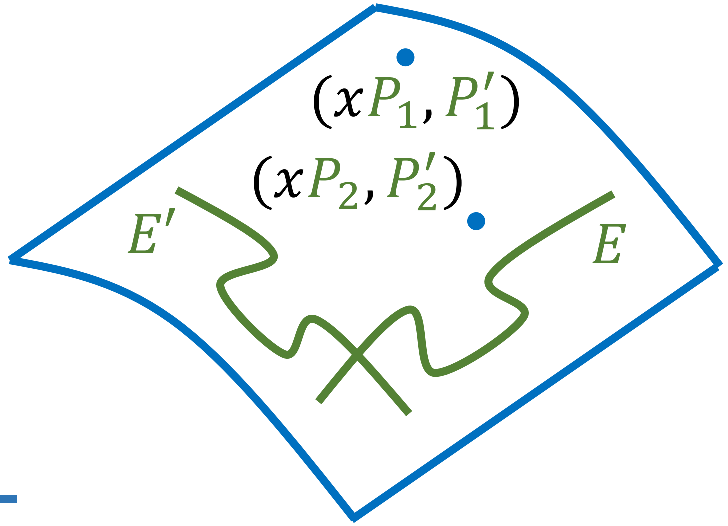
with $\deg\alpha = \deg\gamma$ *and* $\deg\beta = \deg\delta$ *coprime. Then the map*

$$\Phi : E_2 \times E_3 \xrightarrow{\begin{pmatrix} \hat{\alpha} & \hat{\beta} \\ -\delta & \gamma \end{pmatrix}} E_1 \times E_4$$

is a $(\deg\alpha + \deg\beta, \deg\alpha + \deg\beta)$*-isogeny of p.p. abelian surfaces with kernel*

$$\{ (\alpha(P), \beta(P)) \mid P \in E_1[\deg\alpha + \deg\beta] \}.$$

4. Isogeny interpolation: balanced case



Assume $G = E[N] = \langle P_1, P_2 \rangle$ with $N^2 \geq 4d + 1$.

$$\begin{array}{ccc} E & \xrightarrow{\quad\quad\varphi\quad\quad} & E' \\ P_1, P_2 & & P_1' = \varphi(P_1), P_2' = \varphi(P_2) \end{array}$$

Special first case: $\gcd(N, d) = 1$ and $N > d$
$N - d = x^2$ is square

Consider the isogeny diamond

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

Note: $\deg \varphi + \deg[x] = d + x^2 = N$.

Kani's lemma:

$$\Phi : E \times E' \xrightarrow{\begin{pmatrix} [x] & \hat{\varphi} \\ -\varphi & [x] \end{pmatrix}} E \times E'$$

is an (N, N)-isogeny with kernel

$$\{ (xP, \varphi(P)) \mid P \in E[N] \}.$$

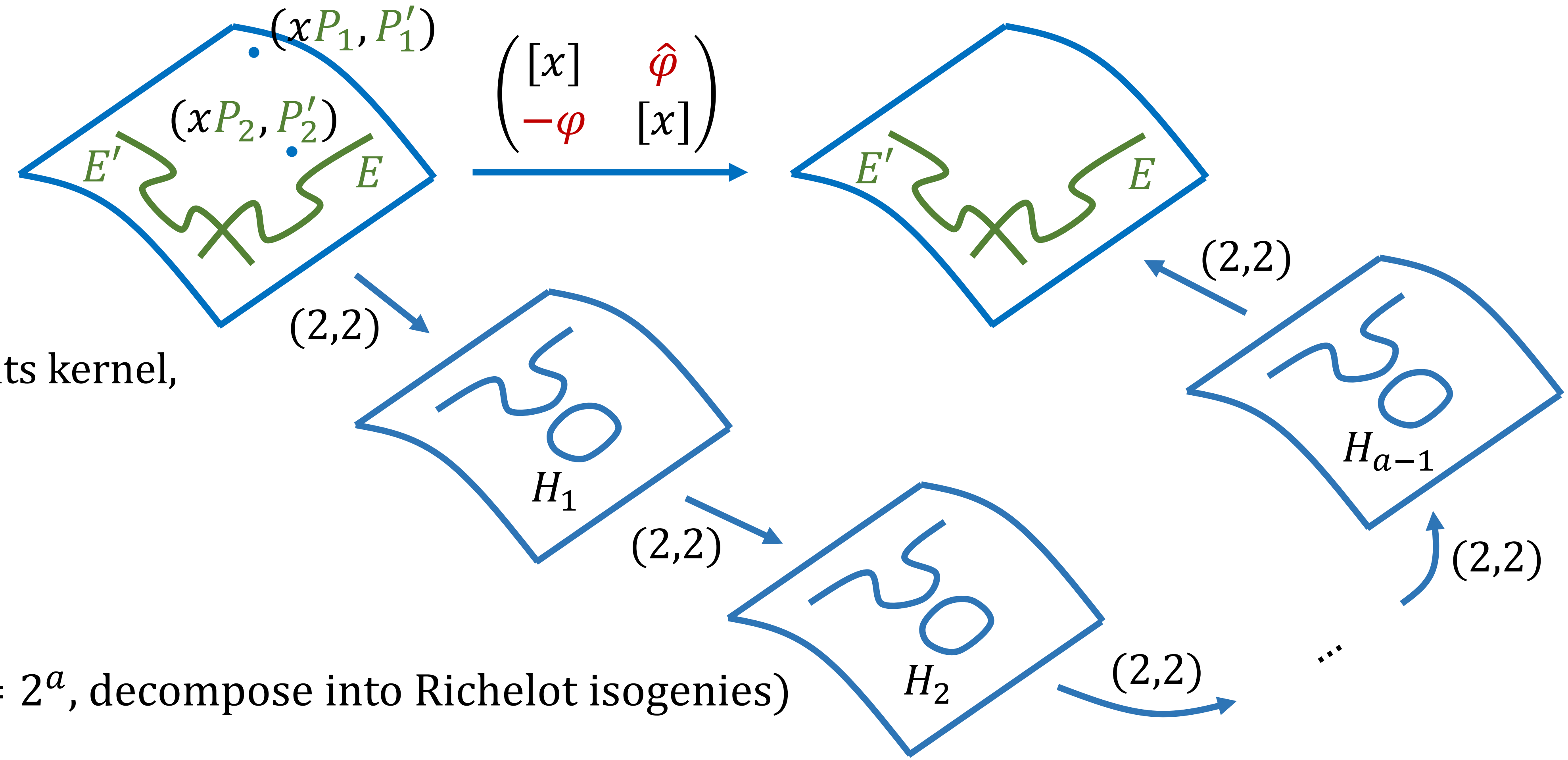
completely known!

4. Isogeny interpolation: balanced case

Algorithm (requires N **smooth**):

- using higher-dimensional analogs of Vélu's formulae, compute the (N, N)-isogeny

Φ :



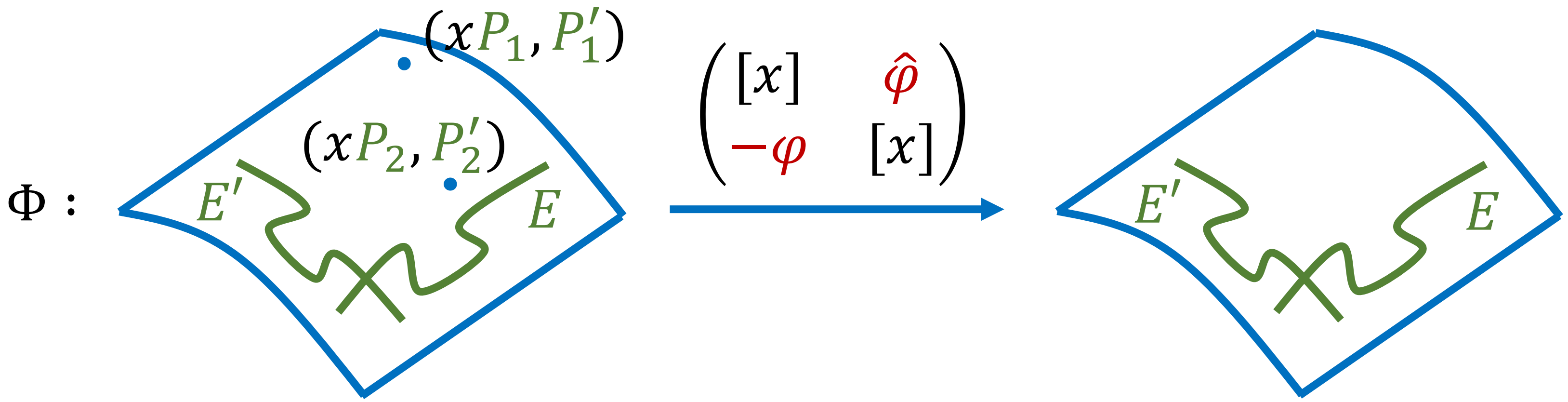
from its kernel,

(e.g., if $N = 2^a$, decompose into Richelot isogenies)

4. Isogeny interpolation: balanced case

Algorithm (requires N **smooth**):

- using higher-dimensional analogs of Vélu's formulae, compute the (N, N)-isogeny



from its kernel,

- compute $-\Phi(Q, \infty) = (-xQ, \varphi(Q))$,
- extract $\varphi(Q)$ as the second component.

4. Isogeny interpolation: balanced case

Assume $G = E[N] = \langle P_1, P_2 \rangle$ with $N^2 \geq 4d + 1$.

$$\begin{array}{ccc} E & \xrightarrow{\qquad\qquad\varphi\qquad\qquad} & E' \\ P_1, P_2 & & P_1' = \varphi(P_1), P_2' = \varphi(P_2) \end{array}$$

Next case: $\gcd(N, d) = 1$ and $N > d$
$N - d = x_1^2 + x_2^2$ is sum of two squares

Same, but use

$$\Phi : E^2 \times E'^2 \xrightarrow{\begin{pmatrix} [x_1] & [x_2] & \hat{\varphi} & 0 \\ [-x_2] & [x_1] & 0 & \hat{\varphi} \\ -\varphi & 0 & [x_1] & [-x_2] \\ 0 & -\varphi & [x_2] & [x_1] \end{pmatrix}} E^2 \times E'^2$$

(higher-dimensional variant of Kani's lemma).

4. Isogeny interpolation: balanced case

Assume $G = E[N] = \langle P_1, P_2 \rangle$ with $N^2 \geq 4d + 1$.

$$\begin{array}{ccc} E & \xrightarrow{\varphi} & E' \\ P_1, P_2 & & P_1' = \varphi(P_1), P_2' = \varphi(P_2) \end{array}$$

Next case: $\gcd(N, d) = 1$ and $N > d$

$N - d = x_1^2 + x_2^2 + x_3^2 + x_4^2$ via Lagrange's four-square theorem

Now work on $E^4 \times E'^4$ and use (**Zarhin's trick**)

$$\begin{pmatrix} [x_1] & [-x_2] & [-x_3] & [-x_4] & \hat{\varphi} & 0 & 0 & 0 \\ [x_2] & [x_1] & [x_4] & [-x_3] & 0 & \hat{\varphi} & 0 & 0 \\ [x_3] & [-x_4] & [x_1] & [x_2] & 0 & 0 & \hat{\varphi} & 0 \\ [x_4] & [x_3] & [-x_2] & [x_1] & 0 & 0 & 0 & \hat{\varphi} \\ -\varphi & 0 & 0 & 0 & [x_1] & [x_2] & [x_3] & [x_4] \\ 0 & -\varphi & 0 & 0 & [-x_2] & [x_1] & [-x_4] & [x_3] \\ 0 & 0 & -\varphi & 0 & [-x_3] & [x_4] & [x_1] & [-x_2] \\ 0 & 0 & 0 & -\varphi & [-x_4] & [-x_3] & [x_2] & [x_1] \end{pmatrix}$$

4. Isogeny interpolation: balanced case

Assume $G = E[N] = \langle P_1, P_2 \rangle$ with $N^2 \geq 4d + 1$.

$$\begin{array}{ccc} E & \xrightarrow{\quad\varphi\quad} & E' \\ P_1, P_2 & & P_1' = \varphi(P_1), P_2' = \varphi(P_2) \end{array}$$

Near-general case: $\gcd(N, d) = 1$
$N - d = x_1^2 + \cdots + x_r^2$ is sum of $r = 1,2,4$ squares

Approach: proceed **as if we would know** the images of $\frac{1}{N}P_1, \frac{1}{N}P_2 \in E[N^2]$.

$$\begin{array}{ccc} A & \xrightarrow{\quad\Phi?\quad} & A \\ \| & & \\ E^r \times E'^r & & \end{array}$$

we no longer know $\ker \Phi$...

4. Isogeny interpolation: balanced case

Assume $G = E[N] = \langle P_1, P_2 \rangle$ with $N^2 \geq 4d + 1$.

$$\begin{array}{ccc} E & \xrightarrow{\quad\quad\quad\varphi\quad\quad\quad} & E' \\ P_1, P_2 & & P_1' = \varphi(P_1), P_2' = \varphi(P_2) \end{array}$$

Near-general case: $\gcd(N, d) = 1$
$N - d = x_1^2 + \cdots + x_r^2$ is sum of $r = 1,2,4$ squares

Approach: proceed **as if we would know** the images of $\frac{1}{N}P_1, \frac{1}{N}P_2 \in E[N^2]$.

$$\begin{array}{ccccc} A & \xrightarrow{\quad\Phi_1\quad} & X & \xleftarrow{\quad\widehat{\Phi}_2\quad} & A \\ \parallel & & & & \\ E^r \times E'^r & & & & \end{array}$$

we also know $N(\ker \widehat{\Phi})$

but we do know $N(\ker \Phi)$!

4. Isogeny interpolation: balanced case

Assume $G = E[N] = \langle P_1, P_2 \rangle$ with $N^2 \geq 4d + 1$.

$$\begin{array}{ccc} E & \xrightarrow{\quad\quad\varphi\quad\quad} & E' \\ P_1, P_2 & & P_1' = \varphi(P_1), P_2' = \varphi(P_2) \end{array}$$

Near-general case: $\gcd(N, d) = 1$

$N - d = x_1^2 + \cdots + x_r^2$ is sum of $r = 1,2,4$ squares

Approach: proceed **as if we would know** the images of $\frac{1}{N}P_1, \frac{1}{N}P_2 \in E[N^2]$.

$$\begin{array}{ccccc} A & \xrightarrow{\quad\Phi_1\quad} & X & \xleftarrow{\quad\widehat{\Phi}_2\quad} & A \\ \parallel & & & & \\ E^r \times E'^r & & & & \end{array}$$

so we recover Φ as $\widehat{\widehat{\Phi}}_2 \circ \Phi_1$

(gluing in the middle is subtle)

5. Isogeny interpolation: glimpse at the general case

E.g., assume $G = \langle P_1 \rangle$ cyclic of order $N \geq 4d + 1$.

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

$$P_1 \qquad\qquad P_1' = \varphi(P_1)$$

$$P_2 \qquad\qquad \varphi(P_2) = \mu P_2' + \lambda P_1'$$

Approach:

- extend to bases $P_1, P_2 \in E[N]$ and $P_1', P_2' \in E'[N]$,

5. Isogeny interpolation: glimpse at the general case

E.g., assume $G = \langle P_1 \rangle$ cyclic of order $N \geq 4d + 1$.

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

$$P_1 \qquad\qquad P_1' = \varphi(P_1)$$

$$P_2 \qquad\qquad \varphi(P_2) = \mu P_2' + \lambda P_1'$$

Approach:

- extend to bases $P_1, P_2 \in E[N]$ and $P_1', P_2' \in E'[N]$,
- use identity $e_N\big(\varphi(P_1), \varphi(P_2)\big) = e_N\big(P_1', \varphi(P_2)\big) = e_N(P_1, P_2)^d$ to determine μ,

5. Isogeny interpolation: glimpse at the general case

E.g., assume $G = \langle P_1 \rangle$ cyclic of order $N \geq 4d + 1$.

$$
\begin{array}{ccccc}
E & \xrightarrow{\quad\varphi\quad} & E' & \xrightarrow{\quad\psi\quad} & E'/\langle P_1' \rangle \\
P_1 & & P_1' = \varphi(P_1) & & \infty \\
P_2 & & \varphi(P_2) = \mu P_2' + \lambda P_1' & & \mu\psi(P_2')
\end{array}
$$

Approach:

- extend to bases $P_1, P_2 \in E[N]$ and $P_1', P_2' \in E'[N]$,
- use identity $e_N\big(\varphi(P_1), \varphi(P_2)\big) = e_N\big(P_1', \varphi(P_2)\big) = e_N(P_1, P_2)^d$ to determine μ,
- compose with $\psi: E' \to E'/\langle P_1' \rangle$,
- apply (slight generalization of) previous algorithm to $G = E[N]$ and $\psi \circ \varphi$.

note: $N^2 \geq 4Nd + N \geq 4Nd + 1 = 4\deg(\psi \circ \varphi) + 1$

6. Isogeny representations

What does it mean to **represent** / **output** a degree-d isogeny $\varphi: E \to E'$?

- As a **rational map** ?

$$\text{E.g.,} \quad \varphi : (x, y) \mapsto \left(\frac{x^3 + x^2 + x + 2}{(x-5)^2}, y\frac{x^3 - 4x^2 + 2}{(x-5)^3} \right)$$

Object of size $O((\log q)\, d)$.

Feasible **only if d is smooth** $\longrightarrow$ write φ as a composition of small-degree isogenies.

pre-2022: default understanding of isogeny representation

6. Isogeny representations

What does it mean to represent / output a degree-d isogeny $\varphi: E \to E'$?

- Via its kernel G ?

  If the points in G are defined over $\mathbf{F}_{q^f}$: object of size $O((\log q) f)$.

  Requires conversion to be useful (e.g., to rational map via Vélu, needs smoothness).

- For certain isogenies: via its kernel ideal I_φ (via Deuring correspondence) ?

  Requires sufficient knowledge of the endomorphism ring.

  Requires conversion to be useful; ideal can often be smoothened, e.g., via [KLP+14].

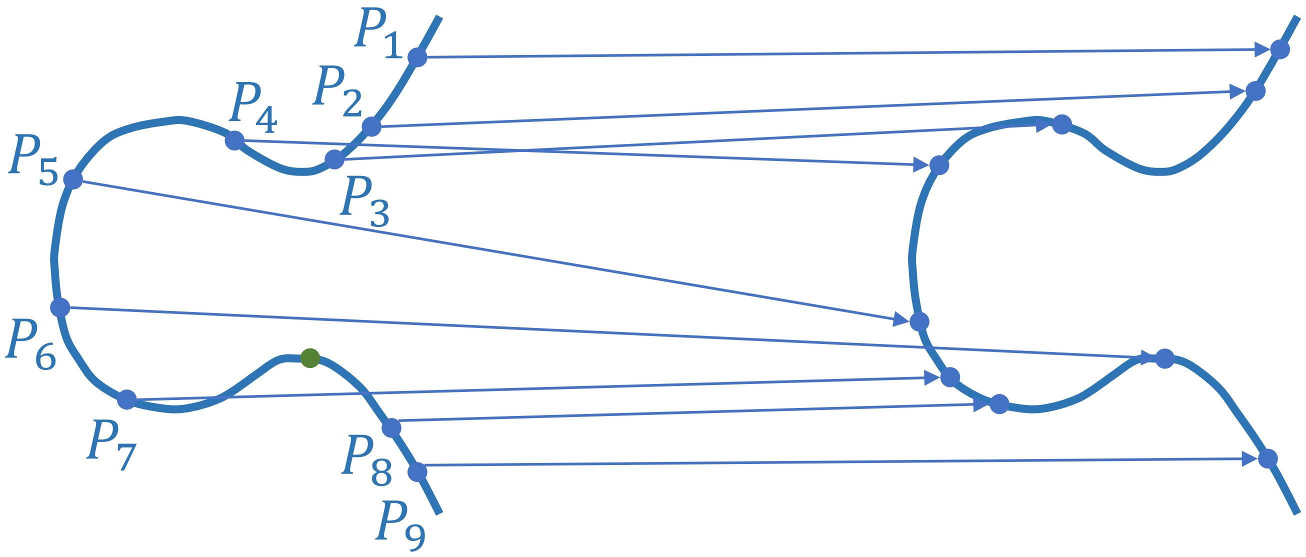
$$\begin{tikzcd} E \arrow[r, bend left, "\varphi"] \arrow[r, bend right, "\psi"'] & E' \end{tikzcd} \qquad \varphi = \frac{1}{\deg \psi} \cdot \psi \circ (\hat{\psi} \circ \varphi)$$

SEE LATER

6. Isogeny representations

What does it mean to **represent** / **output** a degree-d isogeny $\varphi : E \to E'$?

➢ Via **interpolation data** !



Two caveats:

- interpolation data must be provided,
- efficiency strongly depends on parameters (ideally **want** dim 2 **and** $N = 2^a$).

7. Isogeny-based cryptography 2.0

Example application: a signature scheme [Ler23].

$$E \xrightarrow{\tau_{\mathrm{sk}}} E_A$$

$P, Q \in E_A[\ell]$ large prime

Sign:

- compute $R = P + \mathrm{H}(E_A, \text{message}) \cdot Q$,
- using knowledge of $\mathrm{End}(E_A)$, provide interpolation data for $\varphi: E_A \to E_A/\langle R \rangle$.

this is the **signature**

Verify:

- compute $R = P + \mathrm{H}(E_A, \text{message}) \cdot Q$,
- check that $\varphi(R) = \infty$ using isogeny interpolation.

7. Isogeny-based cryptography 2.0

Mother(s) of applications: HD variants [BDD+24,DF24,DLR+24,NO24] of **SQIsign** [DKL+20].

very compact signature scheme (on par with ECC),
submitted to renewed NIST competition

$$\begin{tikzcd} E \arrow[r, "\tau_{\mathrm{sk}}"] \arrow[d, "\psi"'] & E_A \arrow[d, "\varphi"] \\ E_{\mathrm{com}} \arrow[r, dashed, "\text{response}"] & E_{\mathrm{ch}} \end{tikzcd}$$

ad-hoc security assumption
slow and hard to scale

Original: respond with smoothening of $\varphi \circ \tau_{\mathrm{sk}} \circ \hat{\psi} : E_{\mathrm{com}} \to E_{\mathrm{ch}}$ through "**generalized** [KLP+14]".

7. Isogeny-based cryptography 2.0

Mother(s) of applications: HD variants [BDD+24,DF24,DLR+24,NO24] of SQIsign [DKL+20].

very compact signature scheme (on par with ECC),
submitted to renewed NIST competition

$$\begin{tikzcd}
E \arrow[r, "\tau_{\mathrm{sk}}"] \arrow[d, "\psi"'] & E_A \arrow[d, "\varphi"] \\
E_{\mathrm{com}} \arrow[r, dashed, "\text{response}"] & E_{\mathrm{ch}}
\end{tikzcd}$$

~~ad-hoc security assumption~~

~~slow and hard to scale~~

Original: respond with smoothening of $\varphi \circ \tau_{\mathrm{sk}} \circ \hat{\psi} : E_{\mathrm{com}} \to E_{\mathrm{ch}}$ through "generalized [KLP+14]".

HD: respond with interpolation data for random bounded-degree isogeny $\sigma\colon E_{\mathrm{com}} \to E_{\mathrm{ch}}$.

7. Isogeny-based cryptography 2.0

The Nakagawa-Onuki trick [NO23] :

$$\begin{tikzcd} F \\ E \arrow[u, "\psi"] \end{tikzcd} \qquad \deg\psi = q?$$

7. Isogeny-based cryptography 2.0

The Nakagawa-Onuki trick [NO23] :

$$\begin{tikzcd} F \\ E \arrow[u, "\psi"] \arrow[u, bend right, "2^a"'] \end{tikzcd}$$

old method: compute I_ψ of norm q, smoothen using [KLP+14]

7. Isogeny-based cryptography 2.0

The Nakagawa-Onuki trick [NO23] :

$$\begin{tikzcd}
F \arrow[r, "\varphi"] & E \\
E \arrow[u, "\psi"] \arrow[ur, "\theta"] \arrow[r, "\varphi'"'] & F' \arrow[u, "\psi'"']
\end{tikzcd}$$

trick: generate $\theta \in \mathrm{End}(E)$ of degree $q(2^a - q)$

7. Isogeny-based cryptography 2.0

The **Nakagawa—Onuki trick** [NO23] :

$$\begin{tikzcd} F \arrow[r, "\varphi"] \arrow[d, "\hat{\psi}"'] & E \arrow[d, "\hat{\psi}'"] \\ E \arrow[r, "\varphi'"'] & F' \end{tikzcd}$$

recover F and interpolation data for ψ

Kani:

$$\Phi : E \times E \xrightarrow{\begin{pmatrix} \psi & \hat{\varphi} \\ -\varphi' & \hat{\psi}' \end{pmatrix}} F \times F'$$

$$\left\{ \left(qQ, \theta(Q)\right) \,\middle|\, Q \in E[2^a] \right\} \longrightarrow \textbf{known!}$$

$$\shortparallel$$

has kernel $\left\{ \left(\hat{\psi}(P), \varphi(P)\right) \,\middle|\, P \in F[2^a] \right\}$

(Generalizes from endomorphism factorization to **isogeny factorization**.)

7. Isogeny-based cryptography 2.0

Clapoti [PR23]: converting an ideal I into an isogeny **without smoothening**.

$$E \xrightarrow[I]{} E_I$$

7. Isogeny-based cryptography 2.0

Clapoti [PR23]: converting an ideal I into an isogeny **without smoothening**.

$$
\begin{tikzcd}
F \arrow[r] & E \arrow[d, "I_2"] \\
E \arrow[u] \arrow[ur, "\theta"] \arrow[r, "I_1"'] & E_I
\end{tikzcd}
$$

$$I_1 \sim I_2 \sim I$$

$$n(I_1) + n(I_2) = 2^a$$

Likewise, compute isogeny

$$\Phi : E \times E \longrightarrow F \times E_I \quad \text{with kernel} \left\{ \left(n(I_2) \cdot Q, \theta(Q)\right) \,\middle|\, Q \in E[2^a] \right\}$$

and extract E_I and interpolation data for φ_{I_1}, then convert into interpolation data for φ_I.

8. Non-cryptographic applications

Other applications [Rob22,KR24]:

- **computing** $\mathrm{End}(E)$ for ordinary $E/\mathbf{F}_q$ in polytime, given factorization of Δ_{Frob_q},

  idea: provide interpolation data for hypothetical $\frac{\mathrm{Frob}_q - \lambda}{m} \in \mathrm{End}(E)$
  run interpolation to check if this is indeed an endomorphism

- **point counting** on $E/\mathbf{F}_{p^n}$ in time $O(n^2 \cdot \mathrm{poly}(\log p))$,

  idea: provide interpolation data for the Verschiebung on E
  study how Kani's endomorphism acts on differentials on $E \times E$
  extract how the Verschiebung acts on on differentials on E

- unconditional $\tilde{O}(\ell^3)$-algorithm for computing **modular polynomial** $\Phi_\ell(X, Y)$.

  see next talk by Sabrina Kunzweiler!

Thanks for sitting this out!

References

[BDD+24] Basso, De Feo, Dartois, Leroux, Maino, Pope, Robert, Wesolowski, *SQIsign2D-West: the fast, the small, and the safer*
[BJS14] Biasse, Jao, Sankar, *A quantum algorithm for computing isogenies between supersingular elliptic curves*
[Beu22] Beullens, *Breaking Rainbow takes a weekend on a laptop*
[CD23] Castryck, Decru, *An efficient key recovery attack on SIDH*
[CDM+24] Castryck, Decru, Maino, Martindale, Panny, Pope, Robert, Wesolowski, *in preparation*
[DLR+23] Dartois, Leroux, Robert, Wesolowski, *SQISignHD: new dimensions in cryptography*
[DKL+20] De Feo, Kohel, Leroux, Petit, Wesolowski, *SQIsign: compact post-quantum signatures from quaternions and isogenies*
[DF24] Duparc, Fouotsa, *SQIPrime: a dimension 2 variant of SQIsignHD with non-smooth challenge isogenies*
[JD11] Jao, De Feo, *Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies*
[JU18] Jao, Urbanik, *The problem landscape of SIDH*
[Kan97] Kani, *The number of curves of genus two with elliptic differentials*
[KLP+14] Kohel, Lauter, Petit, Tignol, *On the quaternion ℓ-isogeny path problem*
[KR24] Kunzweiler, Robert, *Computing modular polynomials by deformation*
[Ler23] Leroux, *Verifiable random function from the Deuring correspondence and higher dimensional isogenies*
[MMP+23] Maino, Martindale, Panny, Pope, Wesolowski, *A direct key recovery attack on SIDH*
[NO23] Nakagawa, Onuki, *QFESTA: efficient algorithms and parameters for FESTA using quaternion algebras*
[NO24] Nakagawa, Onuki, *SQIsign2D-East: a new signature scheme using 2-dimensional isogenies*
[PR23] Page, Robert, *Introducing Clapoti(s): evaluating the isogeny class group action in polynomial time*
[Rob22] Robert, *Some applications of higher dimensional isogenies to elliptic curves (overview of results)*
[Rob23] Robert, *Breaking SIDH in polynomial time*
[Sho94] Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*
[Tat66] Tate, *Endomorphisms of abelian varieties over finite fields*