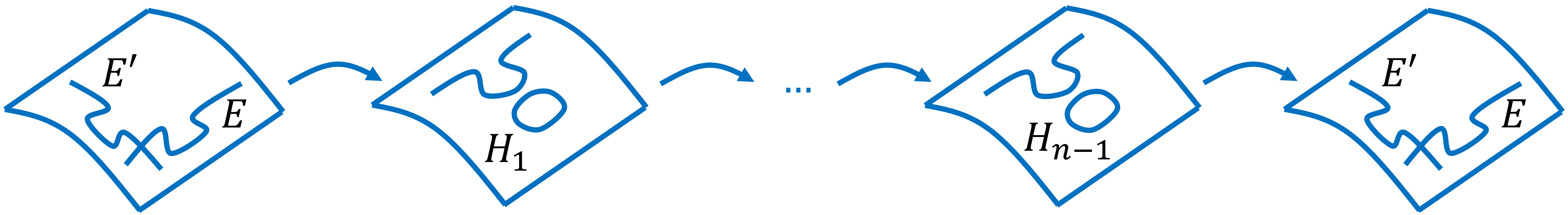
Interpolating isogenies between elliptic curves: destructive and constructive applications



Wouter Castryck (KU Leuven)

The Mathematics of Post-Quantum Cryptography, MPI Bonn, 4 December 2024

COSIC

KU LEUVEN

1. Some context

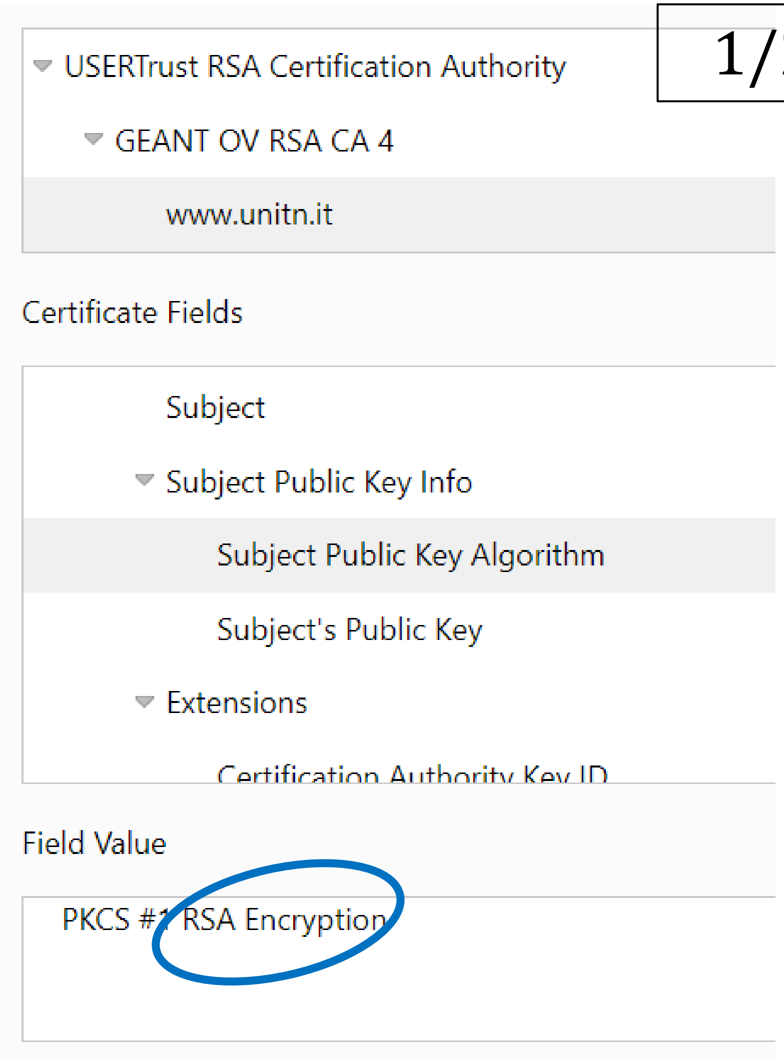
Nearly all currently deployed public-key cryptography is based on the hardness of:

- integer factorization (**RSA**)

$$n = p \cdot q \longrightarrow p, q\ ?$$

- discrete logarithm problem (**ECC**)

$$P, dP \in E(\mathbf{F}_q) \longrightarrow d\ ?$$



1994: Peter Shor describes an $\begin{cases} O(\log^3 n) \\ O(\log^3 q) \end{cases}$ **quantum** algorithm solving both problems

1. Some context

Mixed opinions on when/whether (universal) quantum computers will become real.

More **consensus**: there is non-negligible risk for this to happen in the nearish future.

↓

motivates rapid transition to **post-quantum cryptography**:

- long pipeline from proposal to deployment,
- long-term secrets are under threat now

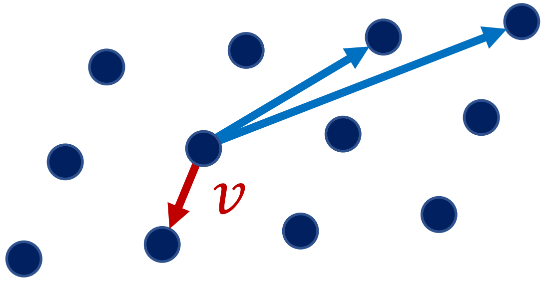
cryptography that

- runs on classical computers,
- resists quantum computers

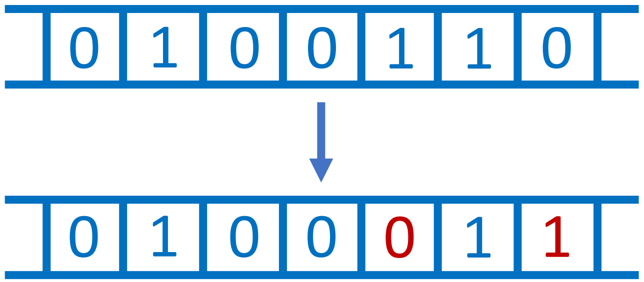
2017: NIST initiates “standardization effort” for key encapsulation and signatures

1. Some context

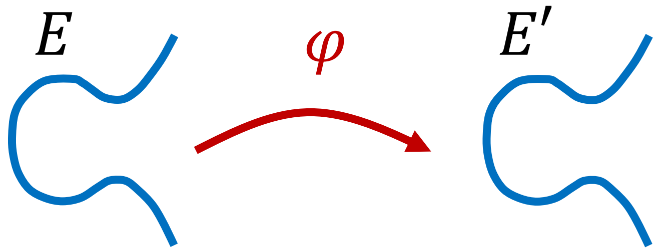
Main contending hard problems:



finding short vectors in lattices



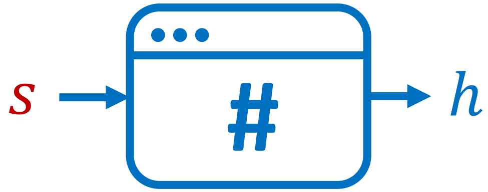
decoding for random linear codes



finding isogenies between elliptic curves

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

solving non-linear systems of equations



finding preimages under hash functions

1. Some context

2020: Preliminary NIST standards:

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

2022: First main NIST standards:

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

Moved to extra round of scrutiny:

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

broken few weeks after selection [CD23], [MMP+23], [Rob23]

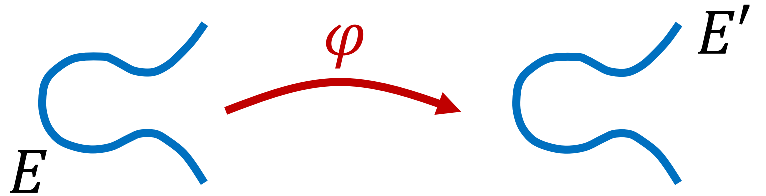
2023: Renewed competition for signatures (includes: SQISign)

2. The isogeny-finding problem

Definition

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

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



Facts:

- on $\bar{k}$-points, isogenies are **surjective group homomorphisms** with **finite kernel**

notes:
- if φ is separable then $\# \ker \varphi = \deg \varphi$
- every finite subgroup $K \subset E$ is the kernel of a separable isogeny

$$\varphi: E \to E' \qquad \text{(e.g., via Vélu's formulae)}$$

and this is unique up to post-composing φ with an isomorphism

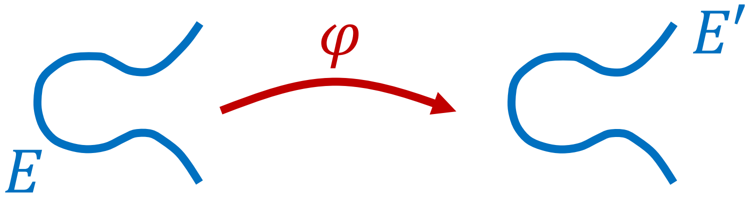
makes sense to write $E' = E/K$

2. The isogeny-finding problem

Definition

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

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



Facts:

- on $\bar{k}$-points, isogenies are **surjective group homomorphisms** with **finite kernel**
- for each isogeny $\varphi: E \to E'$ there is a unique **dual isogeny** $\hat{\varphi}: E' \to E$ such that

$$\varphi \circ \hat{\varphi} = [\deg \varphi], \qquad \hat{\varphi} \circ \varphi = [\deg \varphi]$$

being **isogenous** is an equivalence relation

2. The isogeny-finding problem

Theorem [Tat66]

Two elliptic curves E, E' over $\mathbf{F}_q$ are isogenous over $\mathbf{F}_q$ if and only if

$$\#E(\mathbf{F}_q) = \#E'(\mathbf{F}_q).$$

The isogeny-finding problem is to find an efficient algorithm with

- **input:** two elliptic curves E, E' over $\mathbf{F}_q$ satisfying $\#E(\mathbf{F}_q) = \#E'(\mathbf{F}_q)$
- **return:** an $\mathbf{F}_q$-isogeny $\varphi: E \to E'$

Best known general algorithms:

- exponential time complexity, usually $O(q^{1/4})$,
- quantum computers do not seem to help (beyond quadratic speed-up via Grover)

2. The isogeny-finding problem

Remark: in general non-trivial how to **represent** an $\mathbf{F}_q$-isogeny $\varphi: E \to E'$ ...

- If $\deg \varphi$ is smooth, return φ as composition of small-degree isogenies.

default understanding of "returning an isogeny"

- If $E[N] \subset E(\mathbf{F}_{q^r})$ for smooth $N > 2\sqrt{\deg \varphi}$ and small r, return
  - $\deg \varphi$
  - $\varphi(P), \varphi(Q)$ for some basis $P, Q \in E[N]$.

probably most important by-product of attack [Rob22a]

2. The isogeny-finding problem

Remark: in general non-trivial how to **represent** an $\mathbf{F}_q$-isogeny $\varphi : E \to E'$ ...

- If $\deg \varphi$ is smooth, return φ as composition of small-degree isogenies.

default understanding of "returning an isogeny"

- If $E[N] \subset E(\mathbf{F}_{q^r})$ for smooth $N > 2\sqrt{\deg \varphi}$ and small r, return
  - $\deg \varphi$
  - $\varphi(P), \varphi(Q)$ for some basis $P, Q \in E[N]$.

(for the moment, forget about this)

probably most important ... attack [Rob22a]

SEE LATER

3. Supersingular isogeny Diffie-Hellman (SIDH/SIKE)

High-level idea:

$$E \xrightarrow{\varphi_A} E_A = E/A$$

$$E \xrightarrow{\varphi_B} E_B = E/B$$

$$E_A \xrightarrow{\varphi_{A*}\varphi_B} E_{AB} = E_A/\varphi_A(B)$$

$$E_B \xrightarrow{\varphi_{B*}\varphi_A} E_{BA} = E_B/\varphi_B(A)$$

$$E_{AB} = E_A/\varphi_A(B) \cong E/(A+B) \cong E_{BA} = E_B/\varphi_B(A)$$

Constructive problem:

how do we allow Bob to determine $\varphi_A(B)$ **without revealing φ_A**?

... and likewise for Alice

3. Supersingular isogeny Diffie-Hellman (SIDH/SIKE)

Solution [JDF11]: choose public bases $P_A, Q_A \in E[N_A]$, $P_B, Q_B \in E[N_B]$

$$E \xrightarrow[A = \langle P_A + aQ_A \rangle]{\varphi_A} E_A = E/A$$

Alice reveals

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

allows Bob to compute

$\varphi_A(B) = \langle \varphi_A(P_B) + b\varphi_A(Q_B) \rangle$

φ_B $B = \langle P_B + bQ_B \rangle$

$\varphi_{A*}\varphi_B$

$$E_B = E/B \xrightarrow{\varphi_{B*}\varphi_A} E_{BA} \cong E_{AB}$$

Bob reveals

$\varphi_B(P_A), \varphi_B(Q_A)$ → allows Alice to compute $\varphi_B(A) = \langle \varphi_B(P_A) + a\varphi_B(Q_A) \rangle$

3. Supersingular isogeny Diffie-Hellman (SIDH/SIKE)

Solution [JDF11]: choose public bases $P_A, Q_A \in E[N_A]$, $P_B, Q_B \in E[N_B]$

$$E \xrightarrow[A = \langle P_A + aQ_A \rangle]{\varphi_A} E_A = E/A$$

$$E \xrightarrow[B = \langle P_B + bQ_B \rangle]{\varphi_B} E_B = E/B$$

Technical remarks:

- $N_A = \deg \varphi_A$, $N_B = \deg \varphi_B$ must be **smooth**
- why **supersingular**?
  - makes for hardest isogeny-finding problem,
  - good control over torsion / base field
  - **not crucial for attack**

3. Supersingular isogeny Diffie-Hellman (SIDH/SIKE)

Important: recovering secret isogeny

$$E \xrightarrow{\varphi_A} E_A = E/A$$

P_B, Q_B $\qquad$ $\varphi_A(P_B), \varphi_A(Q_B)$

known smooth degree

"torsion point information"

is **not a pure instance** of the isogeny-finding problem!

- Recurring issue in cryptographic design.
- Torsion point information was already shown to reveal φ_A if $N_B \gg N_A$ [Pet17], [dQKL+20].
- Pure isogeny-finding problem **remains hard**.

4. Recovering an isogeny from torsion point information

Henceforth, focus on following problem:

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

P, Q $\qquad$ $P' = \varphi(P), Q' = \varphi(Q)$

$N > 2\sqrt{d}$ **would be the optimal assumption**

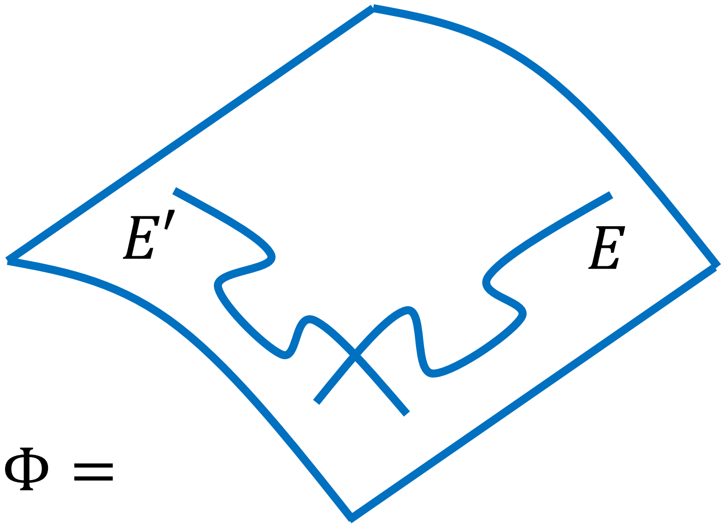
- **input:**
  - $E, E'/\mathbf{F}_q$ connected by an $\mathbf{F}_q$-isogeny φ of **known degree** d,
  - a basis $P, Q \in E[N] \subset E(\mathbf{F}_{q^r})$ for **smooth** and **large enough** N, small r,
  - $P' = \varphi(P), Q' = \varphi(Q) \in E'[N]$.
- **return:** a representation of φ.

Lemma [JU18]

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

4. Recovering an isogeny from torsion point information

We follow approach of [Rob23].



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

P, Q $\qquad$ $P' = \varphi(P), Q' = \varphi(Q)$

Special first case: $N > d, \gcd(N, d) = 1$

$N - d = a^2$ is square

Consider:

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

Easy to check that $\hat{\Phi} \circ \Phi = \Phi \circ \hat{\Phi} = [N]$,

i.e., Φ is an (N, N)-isogeny.

E.g., $\hat{\Phi} \circ \Phi =$

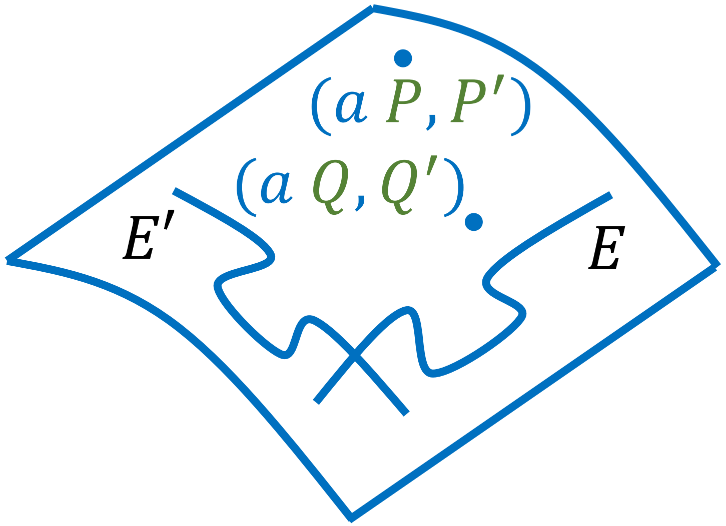
$$\begin{pmatrix} a & -\hat{\varphi} \\ \varphi & a \end{pmatrix} \begin{pmatrix} a & \hat{\varphi} \\ -\varphi & a \end{pmatrix} =$$

$$\begin{pmatrix} a^2 + \hat{\varphi}\varphi & 0 \\ 0 & a^2 + \hat{\varphi}\varphi \end{pmatrix} =$$

$$\begin{pmatrix} a^2 + d & 0 \\ 0 & a^2 + d \end{pmatrix}$$

4. Recovering an isogeny from torsion point information

We follow approach of [Rob23].



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

P, Q $\qquad\qquad$ $P' = \varphi(P), Q' = \varphi(Q)$

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

Consider:

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

Easy to check that $\hat{\Phi} \circ \Phi = \Phi \circ \hat{\Phi} = [N]$,

i.e., Φ is an (N, N)-isogeny.

Note:

$$\Phi(a\,P, P') = \begin{pmatrix} a & \hat{\varphi} \\ -\varphi & a \end{pmatrix} \begin{pmatrix} aP \\ \varphi(P) \end{pmatrix}$$

$$= \begin{pmatrix} (a^2 + d)P \\ \infty' \end{pmatrix} = (\infty, \infty')$$

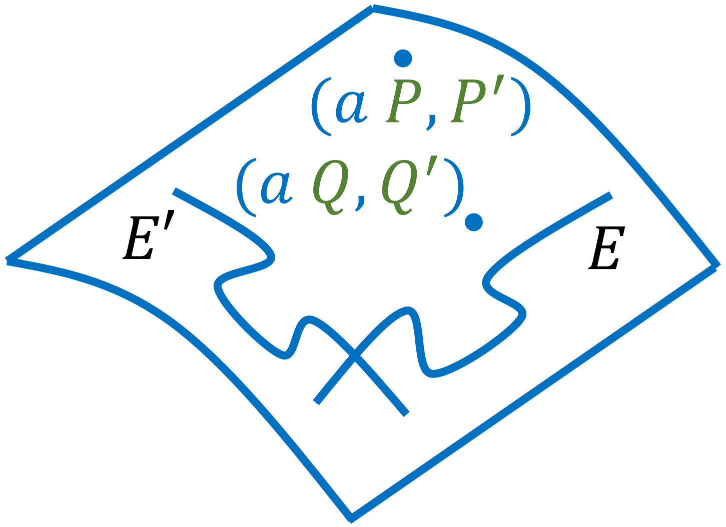
and likewise for $(a\,Q, Q')$.

4. Recovering an isogeny from torsion point information

We follow approach of [Rob23].

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

P, Q $\qquad$ $P' = \varphi(P), Q' = \varphi(Q)$



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

Consider:

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

but this determines Φ!
(up to post-composition with $\cong$)

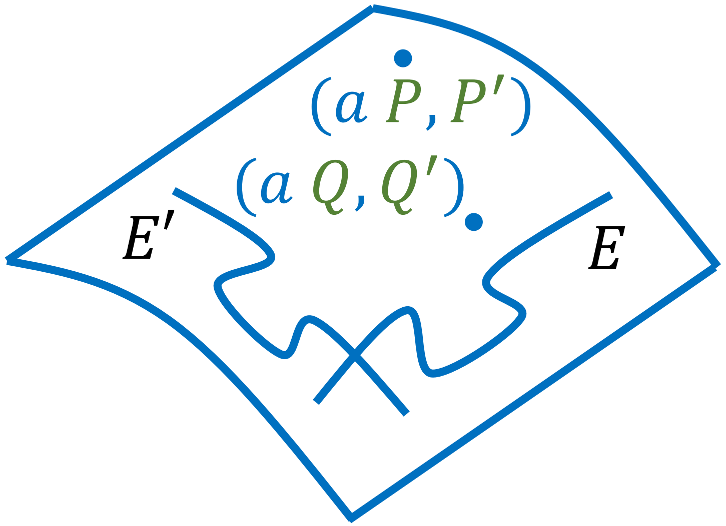
We find that the (N, N)-subgroup $\langle (a\,P, P'), (a\,Q, Q') \rangle$ must be all of $\ker \Phi$.

4. Recovering an isogeny from torsion point information

We follow approach of [Rob23].

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

P, Q $\qquad\qquad$ $P' = \varphi(P), Q' = \varphi(Q)$



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

our efficient representation
(easy to determine $\cong$ if $N > 2\sqrt{d}$)

Consider:

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

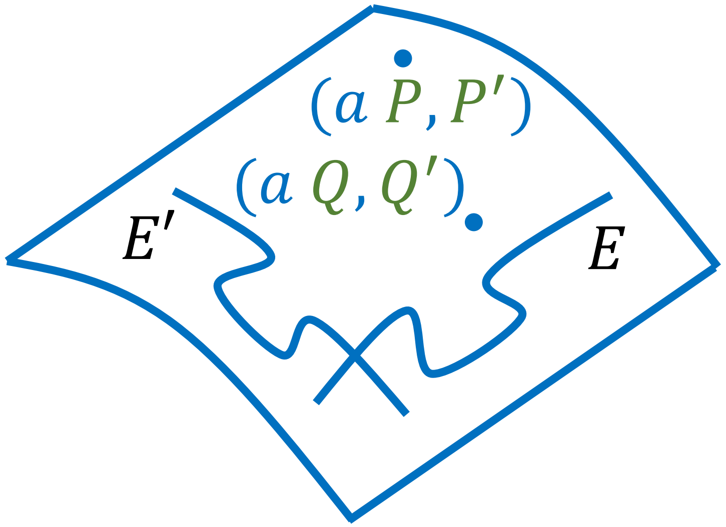
apply to basis of $E[d]$
for recovering $\ker \varphi$
(needs smooth d, as
in SIDH/SIKE)

Conclusion: using higher-dimensional analogues of Vélu,
can essentially compute $\varphi(X)$ via $-\Phi(X, 0)$, for any $X \in E$.

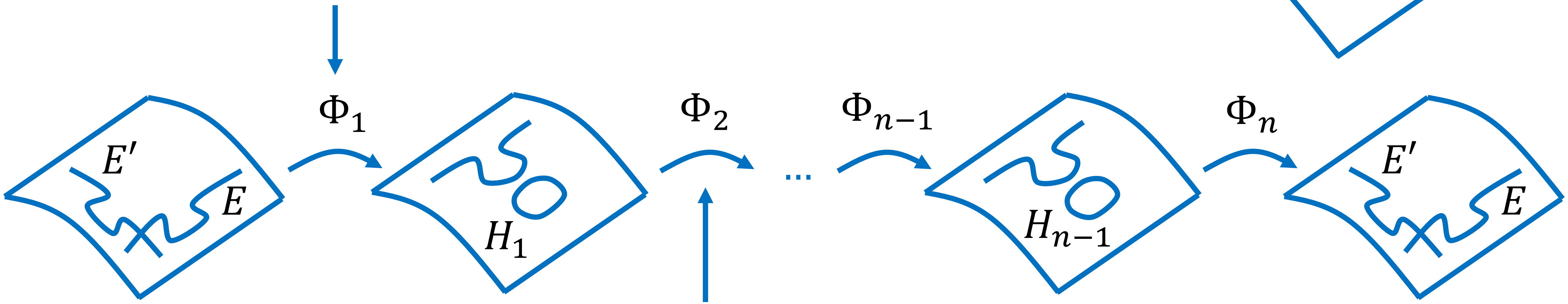
4. Recovering an isogeny from torsion point information

Particularly nice case: $N = 2^n$

Then Φ is a composition of (2,2)-isogenies.



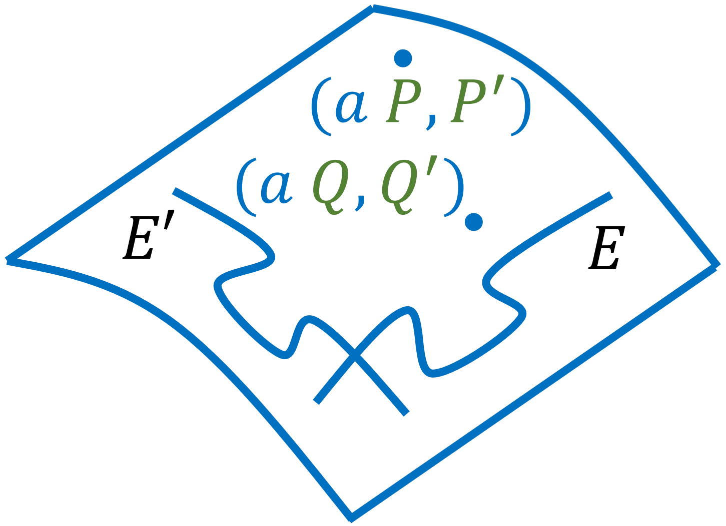
$\ker \Phi_1 = 2^{n-1} \ker \Phi = \langle (2^{n-1} aP, 2^{n-1} P'), (2^{n-1} aQ, 2^{n-1} Q') \rangle$



$\ker \Phi_2 = 2^{n-2} \Phi_1(\ker \Phi)$

and so on ...

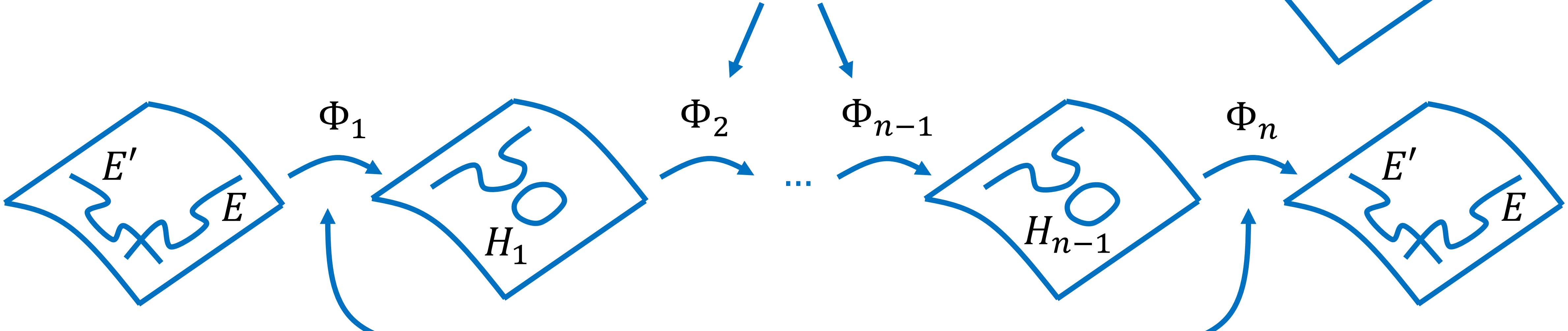
4. Recovering an isogeny from torsion point information



Particularly nice case: $N = 2^n$

Then Φ is a composition of (2,2)-isogenies.

Richelot isogenies (19th century!)



explicit **gluing formulae** [HLP00]

Also explicit: (3,3)-isogenies [BFT14]; in general resort to [LR22].

4. Recovering an isogeny from torsion point information

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

P, Q $\qquad$ $P' = \varphi(P), Q' = \varphi(Q)$

Next case: $N > d, \gcd(N, d) = 1$
$N - d = a_1^2 + a_2^2$ is sum of two squares

Approach: same, but use

$$\Phi : E^2 \times E'^2 \xrightarrow{\begin{pmatrix} a_1 & a_2 & \hat{\varphi} & 0 \\ -a_2 & a_1 & 0 & \hat{\varphi} \\ -\varphi & 0 & a_1 & -a_2 \\ 0 & -\varphi & a_2 & a_1 \end{pmatrix}} E^2 \times E'^2$$

Now must resort to algorithms from [LR22].

4. Recovering an isogeny from torsion point information

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

P, Q $\qquad\qquad$ $P' = \varphi(P), Q' = \varphi(Q)$

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

$N - d = a_1^2 + a_2^2 + a_3^2 + a_4^2$ is sum of four squares (Lagrange)

Approach:

work on $E^4 \times E'^4$ and use

(**Zarhin's trick**)

$$\begin{pmatrix} a_1 & -a_2 & -a_3 & -a_4 & \hat{\varphi} & 0 & 0 & 0 \\ a_2 & a_1 & a_4 & -a_3 & 0 & \hat{\varphi} & 0 & 0 \\ a_3 & -a_4 & a_1 & a_2 & 0 & 0 & \hat{\varphi} & 0 \\ a_4 & a_3 & -a_2 & a_1 & 0 & 0 & 0 & \hat{\varphi} \\ -\varphi & 0 & 0 & 0 & a_1 & a_2 & a_3 & a_4 \\ 0 & -\varphi & 0 & 0 & -a_2 & a_1 & -a_4 & a_3 \\ 0 & 0 & -\varphi & 0 & -a_3 & a_4 & a_1 & -a_2 \\ 0 & 0 & 0 & -\varphi & -a_4 & -a_3 & a_2 & a_1 \end{pmatrix}$$

4. Recovering an isogeny from torsion point information

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

P, Q $\qquad$ $P' = \varphi(P), Q' = \varphi(Q)$

Full case: $N > \sqrt{d}, \gcd(N, d) = 1$

$N^2 - d = a^2$ or $a_1^2 + a_2^2$ or $a_1^2 + a_2^2 + a_3^2 + a_4^2$

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

$$A \xrightarrow{\Phi?} A$$

$A = E^r \times E'^r$

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

4. Recovering an isogeny from torsion point information

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

P, Q $\qquad$ $P' = \varphi(P), Q' = \varphi(Q)$

Full case: $N > \sqrt{d}, \gcd(N, d) = 1$

$N^2 - d = a^2$ or $a_1^2 + a_2^2$ or $a_1^2 + a_2^2 + a_3^2 + a_4^2$

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

$$A \xrightarrow{\Phi_1} X \xleftarrow{\widehat{\Phi}_2} A$$

$A = E^r \times E'^r$

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

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

4. Recovering an isogeny from torsion point information

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

P, Q $\qquad$ $P' = \varphi(P), Q' = \varphi(Q)$

Full case: $N > \sqrt{d}, \gcd(N, d) = 1$

$N^2 - d = a^2$ or $a_1^2 + a_2^2$ or $a_1^2 + a_2^2 + a_3^2 + a_4^2$

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

$$A \xrightarrow{\Phi_1} X \xleftarrow{\widehat{\Phi}_2} A$$

$A = E^r \times E'^r$

so we recover Φ as $\widehat{\widehat{\Phi}}_2 \circ \theta \circ \Phi_1$ for some $\theta \in \mathrm{Aut}(X)$

(can be a bit subtle)

4. Recovering an isogeny from torsion point information

Breaking SIDH/SIKE **in practice**:

- prefer to use (2,2)-isogenies or (3,3)-isogenies (until [LR22] is practical),
- good news: $N_A = 2^n$ and $N_B = 3^m$ and either $N_A > N_B$ or $N_B > N_A$,
- bad news: $|N_A - N_B| = a^2$ extremely unlikely,

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

? ?

- $|N_A - N_B| = a_1^2 + a_2^2$ more likely, but **can we avoid dimension 4?**

Yes for special starting curves E!

4. Recovering an isogeny from torsion point information

Breaking SIDH/SIKE **in practice**:

- prefer to use (2,2)-isogenies or (3,3)-isogenies (until [LR22] is practical),
- good news: $N_A = 2^n$ and $N_B = 3^m$ and either $N_A > N_B$ or $N_B > N_A$,
- bad news: $|N_A - N_B| = a^2$ extremely unlikely,

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

$\mathbf{i} : E \to E: (x, y) \mapsto (-x, \sqrt{-1}y)$

$$\Phi : E \times E' \xrightarrow{\begin{pmatrix} a_1 + \mathbf{i}a_2 & \hat{\varphi} \\ -(a_1 + \mathbf{i}a_2)_* \varphi & \varphi_*(a_1 + \mathbf{i}a_2) \end{pmatrix}} E \times C$$

- $|N_A - N_B| = a_1^2 + a_2^2$ more likely,
- breaks all security levels of SIKE in **seconds** on a laptop [OP22], [DK23]

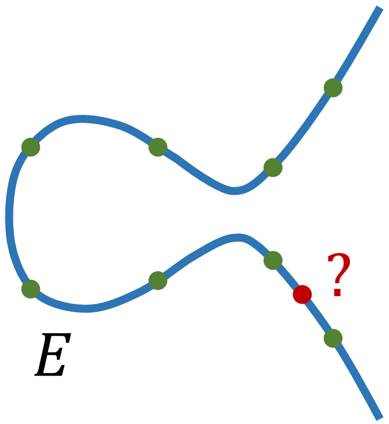
5. Isogeny interpolation: general statement

Variations on this idea lead to:

Theorem [Rob23,DFP24,CDM+24]

There is an algorithm for the evaluation of an isogeny $\varphi : E \to E'$ over $\mathbf{F}_q$ of **known degree** d at any given point, upon input of interpolation data

$$P_1, \varphi(P_1), \qquad P_2, \varphi(P_2), \qquad \dots, \qquad P_r, \varphi(P_r)$$



such that the group $\langle P_1, P_2, \dots, P_r \rangle$ has order N with

$$N \text{ smooth}, \quad N > 4d, \quad \gcd(q, N) = 1,$$

with a running time that is **polynomial** in the input size and in the degrees of the defining fields of $E\left[\ell^{\lceil e/2 \rceil}\right]$ for all prime powers $\ell^e \mid N$.

($N > 4d$) → optimal [JU18]

5. Isogeny interpolation: general statement

Variations on this idea lead to:

Theorem [Rob23,DFP24,CDM+24]

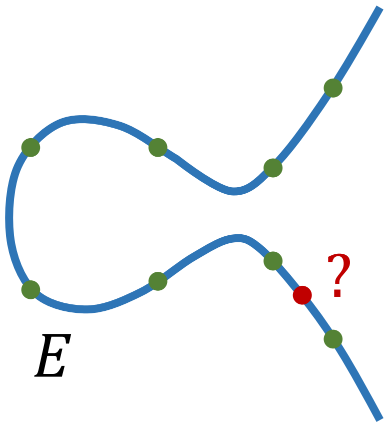
There is an algorithm for the evaluation of an isogeny $\varphi : E \to E'$ over $\mathbf{F}_q$ of known degree d at any given point, upon input of interpolation data

$$P_1, \varphi(P_1), \quad P_2, \varphi(P_2), \quad \dots, \quad P_r, \varphi(P_r)$$

such that the group $\langle P_1, P_2, \dots, P_r \rangle$ has order N with

$$N \text{ smooth}, \quad N > 4d, \quad \gcd(q, N) = 1,$$

with a running time that is polynomial in the input size and in the degrees of the defining fields of $E\left[\ell^{\lceil e/2 \rceil}\right]$ for all prime powers $\ell^e \mid N$.



empty conditions in supersingular case

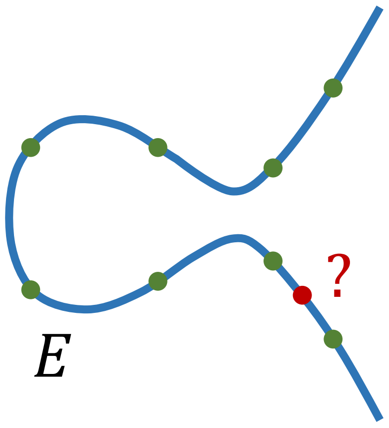
5. Isogeny interpolation: general statement

Variations on this idea lead to:

Theorem [Rob23,DFP24,CDM+24]

There is an algorithm for the evaluation of an isogeny $\varphi : E \to E'$ over $\mathbf{F}_q$ of **known degree** d at any given point, upon input of interpolation data

$$P_1, \varphi(P_1), \quad P_2, \varphi(P_2), \quad \dots, \quad P_r, \varphi(P_r)$$



such that the group $\langle P_1, P_2, \dots, P_r \rangle$ has order N with

$$N \text{ smooth}, \quad N > 4d, \quad \gcd(q, N) = 1,$$

with a running time that is **polynomial** in the input size and in the degrees of the defining fields of $E\left[\ell^{\lceil e/2 \rceil}\right]$ for all prime powers $\ell^e \mid N$.

might be liftable in general (Dieudonné modules)

6. Isogeny representation

Re: what does it mean to **represent** a degree-d isogeny $\varphi: E \to E'$?

- As a **rational map** ?

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

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

  Feasible **only if d is smooth** → write φ as composition of small-degree isogenies

  pre-2022: default understanding of isogeny representation

6. Isogeny representation

Re: what does it mean to represent a degree-d isogeny $\varphi: E \to E'$?

- Via its kernel G?

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

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

- Via its kernel ideal I_φ?

  Requires sufficient knowledge of the endomorphism ring.

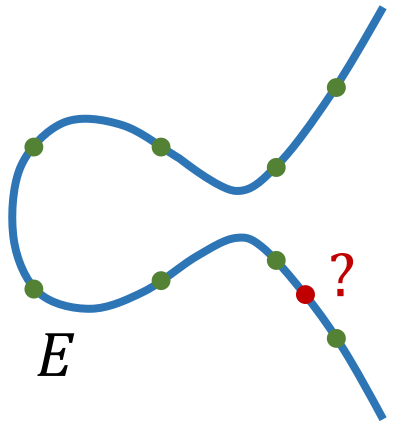
  To be useful, must be smoothened via [KLP+14] or lattice reduction.

SEE LATER

6. Isogeny representation

Re: what does it mean to **represent** a degree-d isogeny $\varphi: E \to E'$?

- Via **interpolation data** !



Two caveats:

- interpolation data must be provided,
- efficiency much depends on parameters (ideally dim 2 and $N = 2^n$).

7. Isogeny generation

Kani's lemma [Kan97]

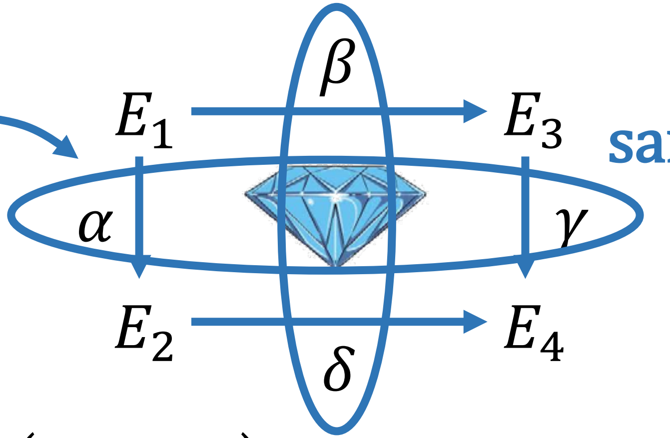
main source of inspiration for the SIDH attacks

7. Isogeny generation

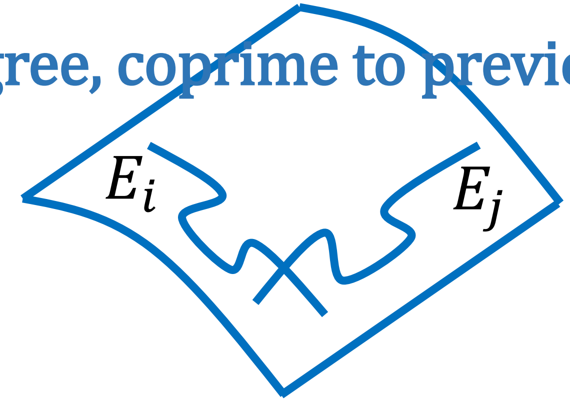
Kani's lemma [Kan97]

Consider a commuting diagram of isogenies:

"isogeny diamond"



same degree, coprime to previous



Then the map

same degree

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

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

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

7. Isogeny generation

Kani's lemma [Kan97]

Consider a commuting diagram of isogenies:

$$\begin{array}{ccc} E_1 & \xrightarrow{\beta} & E_3 \\ \alpha \downarrow & & \downarrow \gamma \\ E_2 & \xrightarrow[\delta]{} & E_4 \end{array}$$

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

$$\left\{ \left(\alpha(P), \beta(P)\right) \,\middle|\, P \in E_1[\deg \alpha + \deg \beta] \right\}.$$

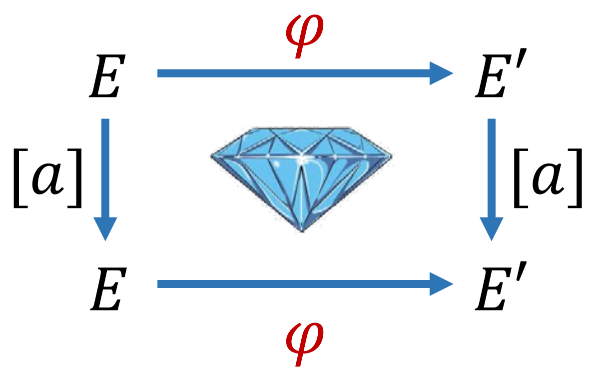
can also be written as

$$\left\{ \left([\deg \alpha]Q, \beta\hat{\alpha}(Q)\right) \,\middle|\, Q \in E_2[\deg \alpha + \deg \beta] \right\}$$

7. Isogeny generation

Special case revisited:

$$N > d, \gcd(N, d) = 1$$
$$N - d = a^2 \text{ is square}$$



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

7. Isogeny generation

Useful subroutine in isogeny-based cryptography:

- **input:** supersingular E with known endomorphism ring
  large prime ℓ
- **output:** random isogeny

$$\varphi : E \longrightarrow E'$$

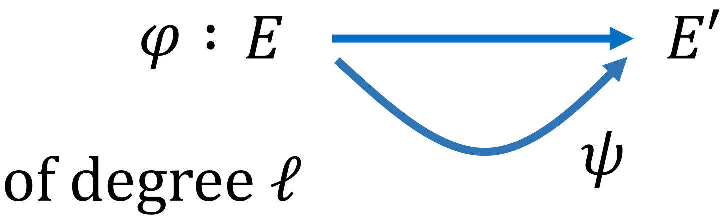
of degree ℓ

7. Isogeny generation

Useful subroutine in isogeny-based cryptography:

- **input:** supersingular E with known endomorphism ring
  large prime ℓ

- **output:** random isogeny

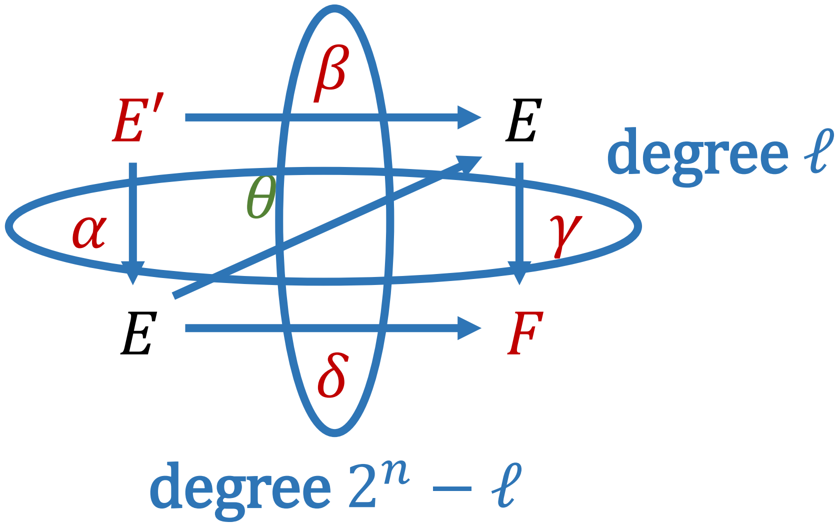


Cumbersome solution: generate ideal I_φ of norm ℓ,
find equivalent ideal $I_\psi \sim I_\varphi$ of smooth norm via [KLP+14],
convert I_ψ into isogeny and recover $\varphi = (\psi \circ \hat{\psi}\varphi)/\deg\psi$

7. Isogeny generation

Nakagawa-Onuki trick aka QFESTA [NO23]:

- generate $\theta \in \mathrm{End}(E)$ with norm $\ell(2^n - \ell)$, necessarily fits in diagram

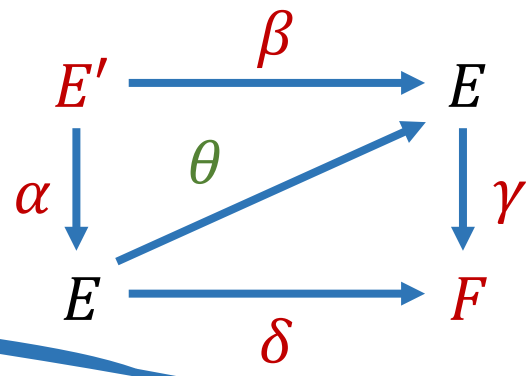


$(\ \theta = \beta \circ \hat{\alpha}\ )$

7. Isogeny generation

Nakagawa-Onuki trick aka QFESTA [NO23]:

- generate $\theta \in \mathrm{End}(E)$ with norm $\ell(2^n - \ell)$, necessarily fits in diagram



recover E' and interpolation data for $\varphi = \hat{\alpha}$

$$\{ (\ell(Q), \theta(Q)) \mid Q \in E[2^n] \}$$
$$\|$$
$$\{ (\alpha(P), \beta(P)) \mid P \in E'[2^n] \}$$
$$\|$$

- compute isogeny $\Phi : E \times E \xrightarrow{\begin{pmatrix} \hat{\alpha} & \hat{\beta} \\ -\delta & \gamma \end{pmatrix}} E' \times F$ from **known kernel**

- generalizes from endomorphism factorization to **isogeny factorization**

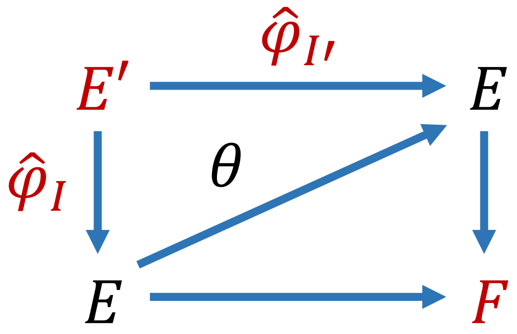
7. Isogeny generation

Clapoti [PR23,BDD+24]: given ideal $I_\varphi \subseteq \mathrm{End}(E)$, compute $\varphi : E \to E'$

- high-level idea: find $I \sim I' \sim I_\varphi$ with $N(I) + N(I') = 2^n$,
- then $I' = I \frac{\bar{\theta}}{N(I)}$ for some $\theta \in \mathrm{End}(E)$, implies $\hat{\varphi}_{I'} \circ \varphi_I = \theta$,

can be relaxed to
$uN(I) + vN(I') = 2^n$

- fits in diamond



from which we recover φ_I and E',

- likewise $I = I_\varphi \frac{\bar{\eta}}{N(I_\varphi)}$ for some $\eta \in \mathrm{End}(E)$ ⟶ $\varphi = \varphi_I \eta / N(I)$
- turns CM ideal-class group action into an **effective group action**

6. Cryptographic application: PRISM [BCC+24]

Simplified version:

- secret and public key:

$$E_0 \xrightarrow{\tau_{\mathrm{sk}}} E_{\mathrm{pk}} \xrightarrow{\sigma} E_{\mathrm{sig}}$$

- signing message msg: using knowledge of τ_{sk}, produce interpolation data for

$$\sigma : E_{\mathrm{pk}} \to E_{\mathrm{sig}}$$

  of degree $\ell = H\left(\mathrm{msg} \| E_{\mathrm{pk}}\right) \in \{\text{primes} \leq B\}$

- verifying a signature for msg:

  verify that data interpolates isogeny of degree $\ell = H\left(\mathrm{msg} \| E_{\mathrm{pk}}\right)$

6. Cryptographic application: SQIsignHD [DLR+24]

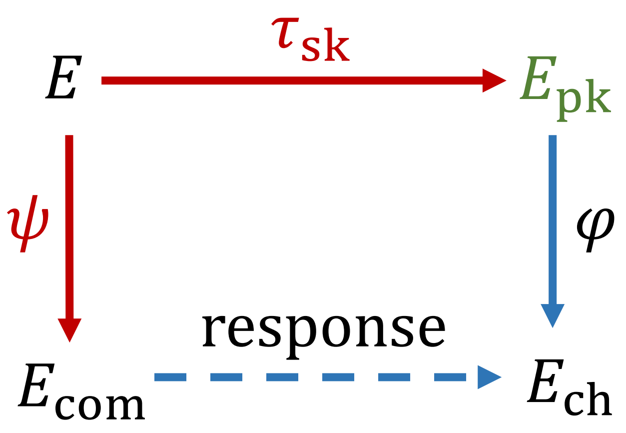
Intermediate version between SQIsign [DKL+20] and SQIsign2D-West [BDD+24].

competitor in renewed NIST competition
updated version for 2nd round

6. Cryptographic application: SQIsignHD [DLR+24]

Intermediate version between SQIsign [DKL+20] and SQIsign2D-West [BDD+24].

Built from identification scheme:



- ✓ cleaner security assumption
- ✓ better scaling
- ✓ faster signing
- ✓ smaller signatures
- ✗ slower verification

Original: respond by smoothening $\varphi \circ \tau_{\mathrm{sk}} \circ \hat{\psi} : E_{\mathrm{com}} \to E_{\mathrm{ch}}$ via generalized KLPT.

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

7. Surprising application [Rob22b]

Let $E/\mathbf{F}_q$ be an ordinary elliptic curve. We know:

$$\mathbf{Z}[\pi_q] \subseteq \mathrm{End}(E) \subseteq O_K \quad \text{with} \quad K = \mathbf{Q}\left(\sqrt{t^2 - 4q}\right)$$

↑

but where exactly?

7. Surprising application [Rob22b]

Let $E/\mathbf{F}_q$ be an ordinary elliptic curve. We know:

$$\underbrace{\mathbf{Z}[\pi_q] \subseteq \mathrm{End}(E) \subseteq O_K}_{\text{index } f} \quad \text{with} \quad K = \mathbf{Q}\left(\sqrt{t^2 - 4q}\right)$$

7. Surprising application [Rob22b]

Let $E/\mathbf{F}_q$ be an ordinary elliptic curve. We know:

$$\mathbf{Z}[\pi_q] \subseteq \mathrm{End}(E) \subseteq O_K \quad \text{with} \quad K = \mathbf{Q}\left(\sqrt{t^2 - 4q}\right)$$

divisible by which prime powers dividing f ?

small order coprime with b

To test a prime power $b \mid f$, we:

- determine $a \in \mathbf{Z}$ such that $\mathrm{charpol}_{\pi_q}(X) \equiv (X - a)^2 \bmod b$,
- evaluate hypothetical endomorphism $\frac{\pi_q - a}{b}$ on sufficiently many points
- run isogeny interpolation: algorithm will crash iff $b \nmid \left[\mathrm{End}(E) : \mathbf{Z}[\pi_q]\right]$

7. Surprising application [Rob22b]

Let $E/\mathbf{F}_q$ be an ordinary elliptic curve. We know:

$$\mathbf{Z}[\pi_q] \subseteq \mathrm{End}(E) \subseteq O_K \quad \text{with} \quad K = \mathbf{Q}\left(\sqrt{t^2 - 4q}\right)$$

divisible by which prime powers dividing *f* ?

To test a prime power $b \mid f$, we: **requires factorization of *f***

- determine $a \in \mathbf{Z}$ such that $\mathrm{charpol}_{\pi_q}(X) \equiv (X - a)^2 \bmod b$,
- evaluate hypothetical endomorphism $\frac{\pi_q - a}{b}$ on sufficiently many points
- run isogeny interpolation: algorithm will crash iff $b \nmid \left[\mathrm{End}(E) : \mathbf{Z}[\pi_q]\right]$

Questions?

Danke schön!