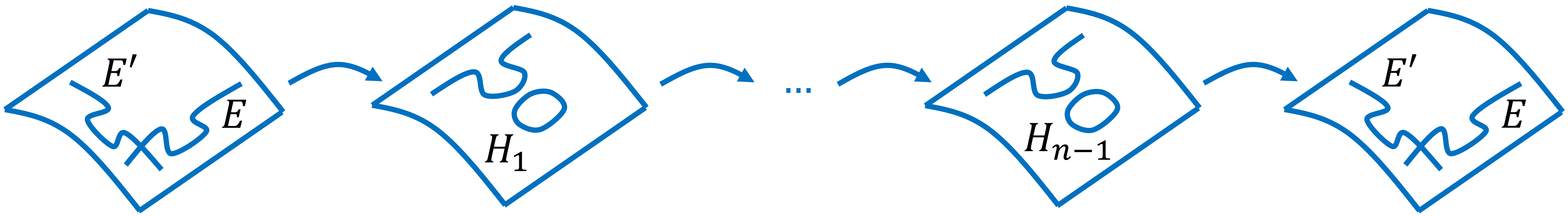
An efficient break of Supersingular Isogeny Diffie-Hellman

Wouter Castryck (KU Leuven)



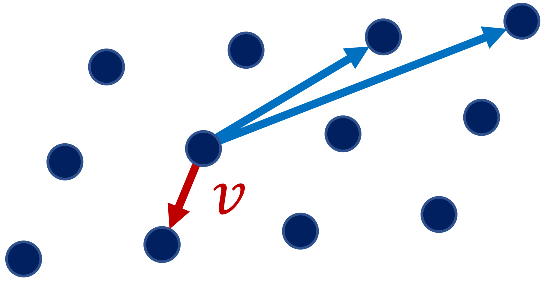
CAIPI Symposium, IRMAR, Université de Rennes, 29 April 2024

COSIC

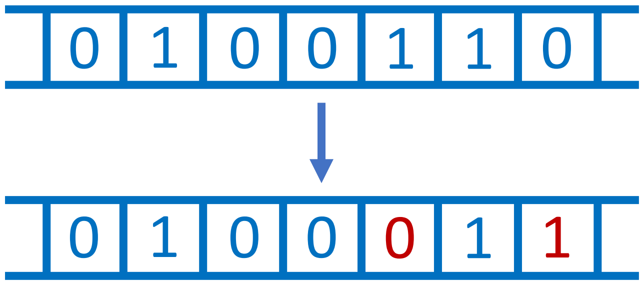
KU LEUVEN

Context

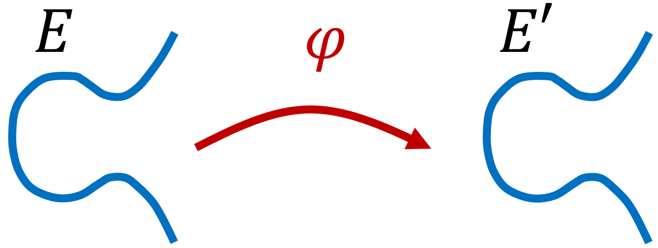
Main contending hard problems in post-quantum cryptography standardization:



finding short vectors in lattices



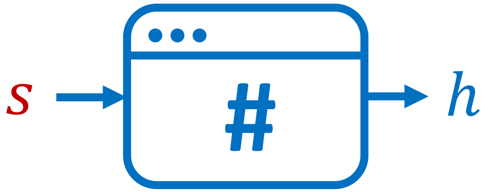
decoding for random linear codes



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

Context

2020: Preliminary NIST standards:

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

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

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)

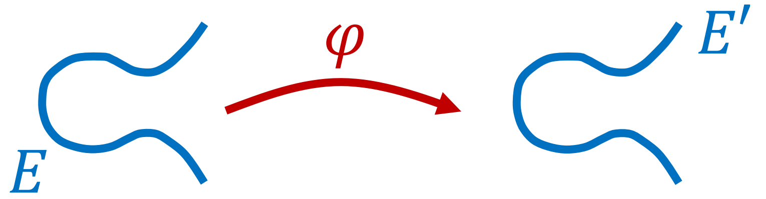
2023: Renewed competition for signatures (includes: **SQISign**)

The isogeny-finding problem

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 recap:

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

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

being **isogenous** is an equivalence relation

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,
- quantum computers do not seem to help

The isogeny-finding problem

Recall: 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]

The isogeny-finding problem

Recall: 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 by-product of attack [Rob22a]

Supersingular isogeny Diffie-Hellman (SIDH/SIKE)

Recall from Benjamin's talk [JDF11]: fix public bases $P_A, Q_A \in E[N_A]$, $P_B, Q_B \in E[N_B]$

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

Alice reveals

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

allows Bob to compute

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

Bob reveals

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

Supersingular isogeny Diffie-Hellman (SIDH/SIKE)

Recall from Benjamin's talk [JDF11]: fix public bases $P_A, Q_A \in E[N_A]$, $P_B, Q_B \in E[N_B]$

$$\begin{array}{ccc} E & \xrightarrow[A = \langle P_A + aQ_A \rangle]{\varphi_A} & E_A = E/A \\ \varphi_B \Big\downarrow B = \langle P_B + bQ_B \rangle & & \\ E_B = E/B & & \end{array}$$

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**

Supersingular isogeny Diffie-Hellman (SIDH/SIKE)

Important: recovering secret isogeny

known smooth degree

$$\begin{array}{ccc} E & \xrightarrow{\varphi_A} & E_A = E/A \\ P_B, Q_B & & \varphi_A(P_B), \varphi_A(Q_B) \end{array}$$

"torsion point information"

is **not a pure instance** of the isogeny-finding problem (but of **SSI-T**)!

- 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**.

Recovering an isogeny from torsion point information

Henceforth, focus on following **interpolation** problem:

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

- **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.

Recovering an isogeny from torsion point information

Henceforth, focus on following interpolation problem:

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

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

- **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

<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—Schwartz:

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

- This implies $\deg(\varphi_1 - \varphi_2) \leq 4d$ ↯

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

Lemma [JU18]

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

Recovering an isogeny from torsion point information

Henceforth, focus on following **interpolation** problem:

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

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

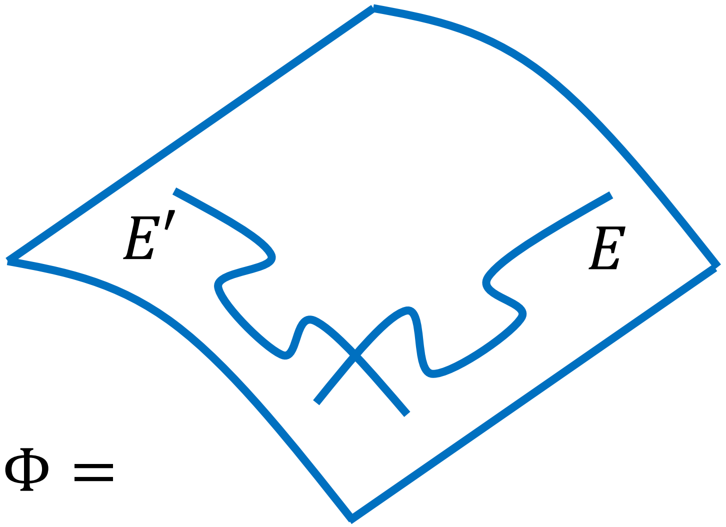
- **input:**
  - $E, E'/\mathbf{F}_q$ connected by an $\mathbf{F}_q$-isogeny φ of **known degree** d,
  - a basis $P, Q \in E[N] \subset E(\mathbf{F}_{q^r})$ for **smooth** and **large enough** N, small r,
  - $P' = \varphi(P), Q' = \varphi(Q) \in E'[N]$.
- **return:** a representation of φ.

Lemma [JU18]

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

Recovering an isogeny from torsion point information

We follow approach of [Rob23]. Inspiration: [Kan97].



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

Special first case: $N > d$

$N - d = a^2$ 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., $\hat{\Phi} \circ \Phi =$

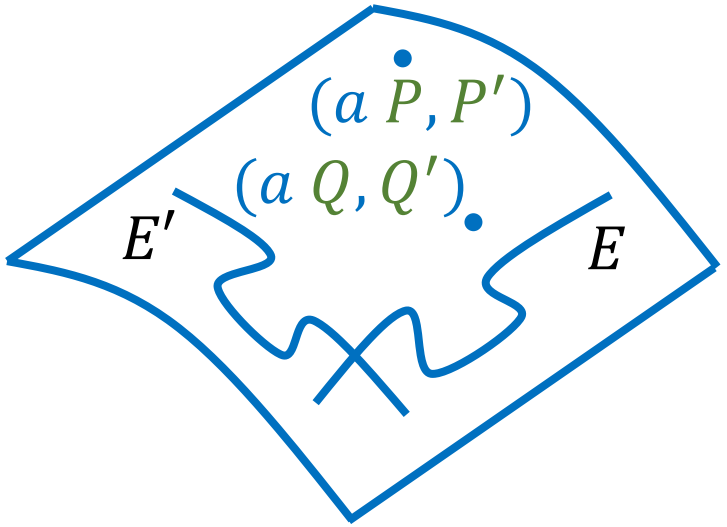
$$\begin{pmatrix} a & -\hat{\varphi} \\ \varphi & a \end{pmatrix} \begin{pmatrix} a & \hat{\varphi} \\ -\varphi & a \end{pmatrix} =$$

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

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

Recovering an isogeny from torsion point information

We follow approach of [Rob23]. Inspiration: [Kan97].



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

Special first case: $N > d$

$N - d = a^2$ 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:

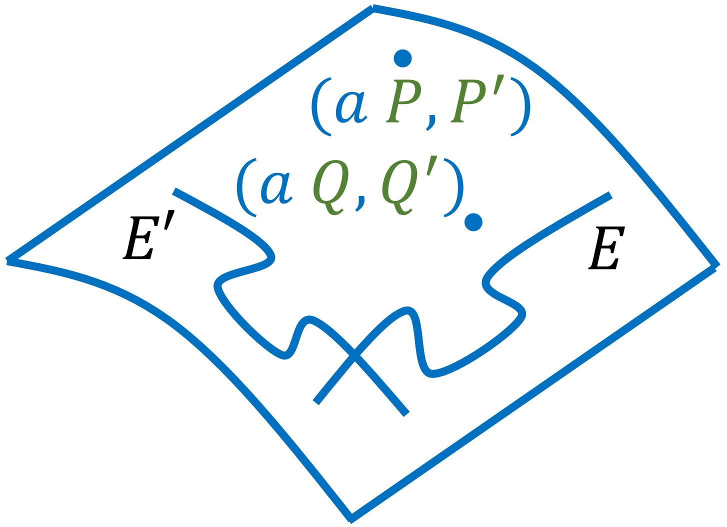
$$\Phi(a\,P, P') = \begin{pmatrix} a & \hat{\varphi} \\ -\varphi & a \end{pmatrix} \begin{pmatrix} aP \\ \varphi(P) \end{pmatrix}$$

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

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

Recovering an isogeny from torsion point information

We follow approach of [Rob23]. Inspiration: [Kan97].



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

Special first case: $N > d$

$N - d = a^2$ is square

Consider:

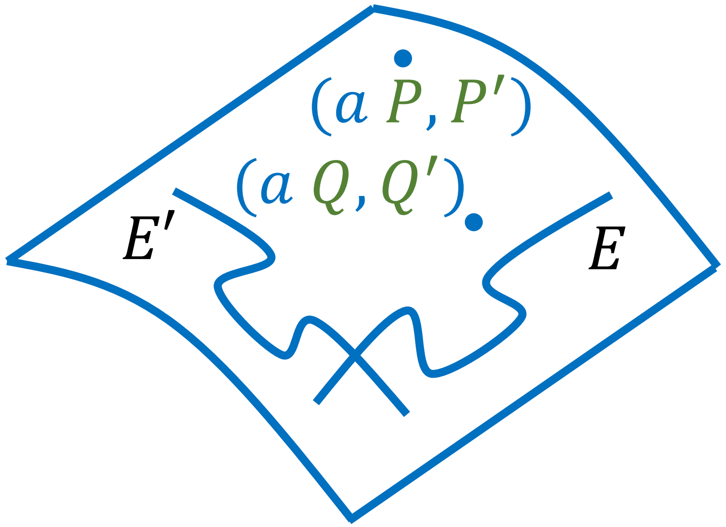
$$\Phi : E \times E' \xrightarrow{\begin{pmatrix} a & \hat{\varphi} \\ -\varphi & a \end{pmatrix}} E \times E'$$

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 $\ker \Phi$.

Recovering an isogeny from torsion point information



We follow approach of [Rob23]. Inspiration: [Kan97].

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

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

Special first case: $N > d$

$N - d = a^2$ is square

Consider:

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

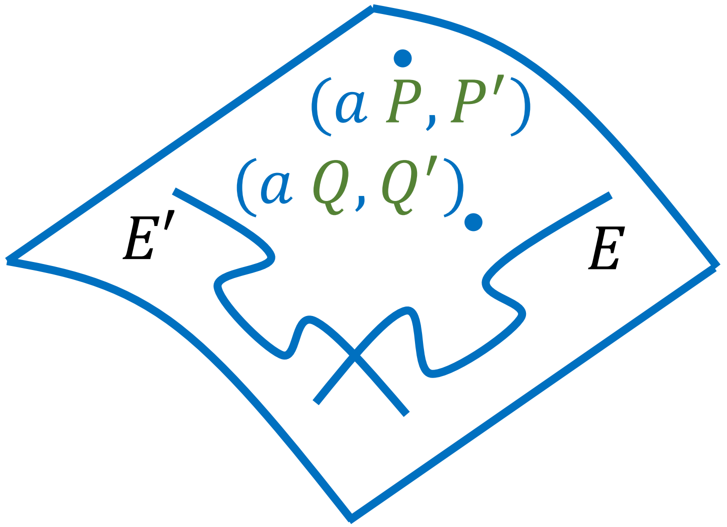
Conclusion: using higher-dimensional analogues of Vélu, can essentially compute $\varphi(X)$ via $-\Phi(X, 0)$, for any $X \in E$.

our efficient representation

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

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

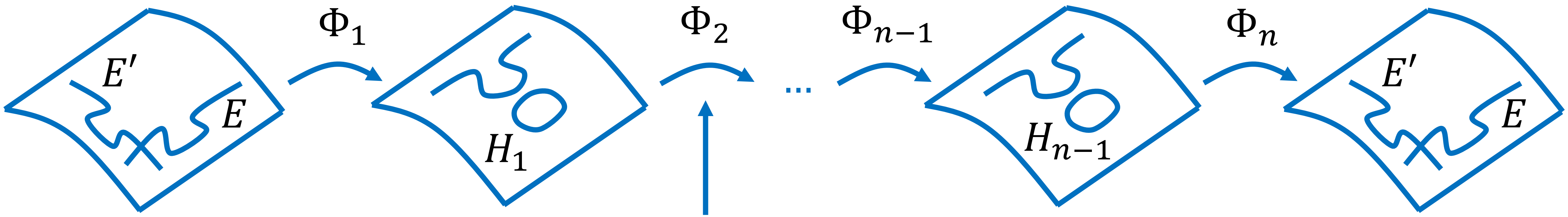
Recovering an isogeny from torsion point information



Particularly nice case: $N = 2^n$

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

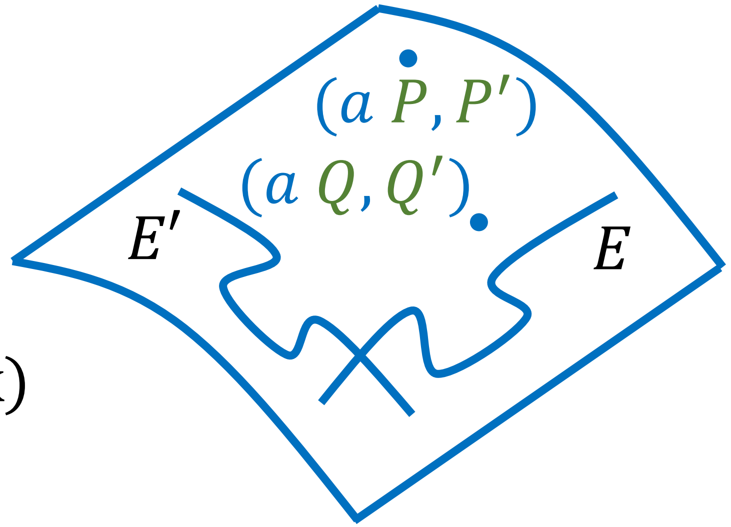
$\ker \Phi_1 = 2^{n-1} \ker \Phi = \langle (2^{n-1} aP, 2^{n-1}P'), (2^{n-1}aQ, 2^{n-1}Q') \rangle$



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

and so on ...

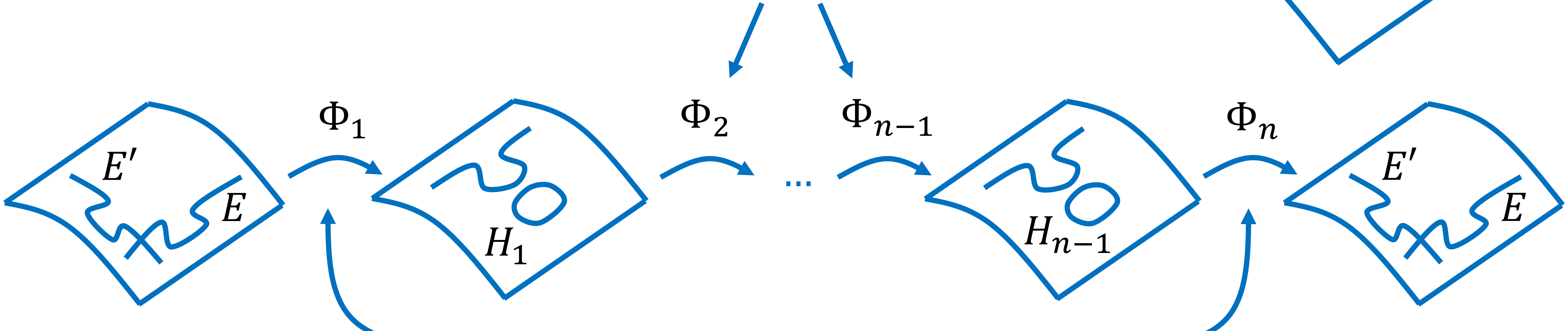
Recovering an isogeny from torsion point information



Particularly nice case: $N = 2^n$

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

Richelot isogenies (see Sabrina's talk)



explicit **gluing formulae** [HLP00]

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

Recovering an isogeny from torsion point information

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

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

Next case: $N > d$

$N - d = a_1^2 + a_2^2$ 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].

Recovering an isogeny from torsion point information

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

Next case: $N > d$

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

Approach:

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

(**Zarhin's trick**)

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

Recovering an isogeny from torsion point information

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

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

Full case: $N > \sqrt{d}$

$N^2 - d = a^2$ 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 $\frac{1}{N}P, \frac{1}{N}Q \in E[N^2]$.

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

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

Recovering an isogeny from torsion point information

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

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

Full case: $N > \sqrt{d}$

$N^2 - d = a^2$ 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 $\frac{1}{N}P, \frac{1}{N}Q \in E[N^2]$.

$$\begin{array}{c} A \\ \| \\ E^r \times E'^r \end{array} \xrightarrow{\Phi_1} X \xleftarrow{\widehat{\Phi}_2} A$$

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

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

Recovering an isogeny from torsion point information

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

Full case: $N > \sqrt{d}$

$$N^2 - d = a^2 \quad \text{or} \quad a_1^2 + a_2^2 \quad \text{or} \quad a_1^2 + a_2^2 + a_3^2 + a_4^2$$

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

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

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

(can be a bit subtle)

Attacking SIDH

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,

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

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

Yes for special starting curves E!

Attacking SIDH

Breaking SIDH/SIKE **in practice** (assume $N_A > N_B$ for concreteness):

- starting curve $E : y^2 = x^3 + x$ comes with endomorphism

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

satisfying $\mathbf{i}^2 = -1$

- diagram for $N_A - N_B = a^2$:

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

Attacking SIDH

Breaking SIDH/SIKE **in practice** (assume $N_A > N_B$ for concreteness):

- starting curve $E : y^2 = x^3 + x$ comes with endomorphism

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

satisfying $\mathbf{i}^2 = -1$

- diagram for $N_A - N_B = a_1^2 + a_2^2$:

$$\begin{tikzcd} E \arrow[r, "\varphi"] \arrow[d, "a_1 + \mathbf{i}a_2"'] & E' \arrow[d, "\varphi_*(a_1 + \mathbf{i}a_2)"] \\ E \arrow[r, "(a_1 + \mathbf{i}a_2)_*\varphi"'] & C \end{tikzcd}$$

- can now consider:

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

Attacking SIDH

Breaking SIDH/SIKE **in practice** (assume $N_A > N_B$ for concreteness):

- starting curve $E : y^2 = x^3 + x$ comes with endomorphism

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

  satisfying $\mathbf{i}^2 = -1$

- diagram for $N_A - N_B = a_1^2 + a_2^2$:

$$\begin{tikzcd} E \arrow[r, "\varphi"] \arrow[d, "a_1 + \mathbf{i}a_2"'] & E' \arrow[d, "\varphi_*(a_1 + \mathbf{i}a_2)"] \\ E \arrow[r, "(a_1 + \mathbf{i}a_2)_*\varphi"'] & C \end{tikzcd}$$

$$\ker \Phi = \langle ((a_1 - \mathbf{i}a_2)P, P'), ((a_1 - \mathbf{i}a_2)Q, Q') \rangle$$

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

(meeting half-way no longer possible)

Attacking SIDH

Breaking SIDH/SIKE **in practice** (assume $N_A > N_B$ for concreteness):

- recall: $N_A = 2^n$ and $N_B = 3^m$
- find very small ϵ, δ such that

$$2^{n-\epsilon} - 3^{m-\delta} = a_1^2 + a_2^2$$

(requires factorization)

$$\begin{tikzcd}
E \arrow[r, "\varphi"] \arrow[d, "a_1 + \mathbf{i}a_2"'] & E' \arrow[d, "\varphi_*(a_1 + \mathbf{i}a_2)"] \\
E \arrow[r, "(a_1 + \mathbf{i}a_2)_*\varphi"'] & C
\end{tikzcd}$$

shorten φ by guessing last δ steps

Attacking SIDH

Breaking SIDH/SIKE **in practice** (assume $N_A > N_B$ for concreteness):

- recall: $N_A = 2^n$ and $N_B = 3^m$
- find very small ϵ, δ such that

$$2^{n-\epsilon} - 3^{m-\delta} = a_1^2 + a_2^2$$

  (requires factorization)

- use Richelot isogenies to compute

$$\varphi(P), \varphi(Q)$$

  for basis P, Q of $E[2^n]$ and solve $\varphi(\lambda P + \mu Q) = \lambda\varphi(P) + \mu\varphi(Q) = 0$

- breaks all security levels of SIKE in **seconds** on a laptop [OP22], [DK23]

$$\begin{tikzcd} E \arrow[r, "\tilde{\varphi}"] \arrow[d, "a_1 + \mathbf{i}a_2"'] & \tilde{E}' \arrow[d, "\tilde{\varphi}_*(a_1 + \mathbf{i}a_2)"] \\ E \arrow[r, "(a_1 + \mathbf{i}a_2)_*\tilde{\varphi}"'] & \tilde{C} \end{tikzcd}$$

Analysis of a countermeasure (M-SIDH)

We recall:

$$\begin{array}{ccc} E & \xrightarrow[A = \langle P_A + aQ_A \rangle]{\varphi_A} & E_A = E/A \\ {\scriptstyle \varphi_B}\downarrow {\scriptstyle B = \langle P_B + bQ_B \rangle} & & \\ E_B = E/B & & \end{array}$$

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

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

Observation

It suffices to reveal $\lambda\varphi_A(P_B), \lambda\varphi_A(Q_B)$ for some secret λ!

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

Analysis of a countermeasure (M-SIDH)

Leads to following variant:

$$\begin{array}{ccc} E & \xrightarrow{\quad\quad\varphi\quad\quad} & E' \\ P, Q & & P' = \lambda\varphi(P), Q' = \lambda\varphi(Q) \end{array}$$

- **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** $N > d$, small r,
  - $P' = \lambda\varphi(P), Q' = \lambda\varphi(Q) \in E'[N]$ for some $\lambda \in (\mathbf{Z}/N\mathbf{Z})^*$
- **return:** a representation of φ.

Weil pairing: $e_N(P', Q') = e_N\big(\lambda\varphi(P), \lambda\varphi(Q)\big) = e_N(P, Q)^{\lambda^2 d} \longrightarrow$ reveals λ^2

Must assume N has **many distinct prime factors** in order to keep λ secret [FMP23].

Analysis of a countermeasure (M-SIDH)

If E or E' carries small non-scalar endomorphism σ: lollipop attack [FMP23]

$$\begin{tikzcd} E \arrow[loop left, "\sigma"] \arrow[r, shift right, "\varphi"'] & E' \arrow[l, shift right, "\hat{\varphi}"'] \end{tikzcd}$$

P, Q on E; $P' = \lambda\varphi(P)$, $Q' = \lambda\varphi(Q)$ on E'

Observation: write $\Sigma \in (\mathbf{Z}/N\mathbf{Z})^{2\times 2}$ for matrix of σ with respect to $P, Q \in E[N]$, then

$$(\varphi \circ \sigma \circ \hat{\varphi})\begin{pmatrix} P' \\ Q' \end{pmatrix} = d\,(\varphi \circ \sigma)\begin{pmatrix} \lambda\, P \\ \lambda\, Q \end{pmatrix} = d\,\varphi\,\Sigma\begin{pmatrix} \lambda\, P \\ \lambda\, Q \end{pmatrix} = d\,\Sigma\begin{pmatrix} P' \\ Q' \end{pmatrix}$$

If $N > \sqrt{\deg(\hat{\varphi} \circ \sigma \circ \varphi)} = d\sqrt{\deg \sigma}$, results in a representation of $\hat{\varphi} \circ \sigma \circ \varphi$.

if cyclic: recover φ from this

Analysis of a countermeasure (M-SIDH)

If E is defined over $\mathbf{F}_p$:
variation on this idea [CV23]

$$\begin{tikzcd} & & E'^{(p)} \\ E \arrow[loop left, "\pi_p"] \arrow[urr, "\varphi^{(p)}"] \arrow[rr, "\varphi"'] & & E' \arrow[u, "\pi_p"'] \end{tikzcd}$$

P, Q on E; $P' = \lambda\varphi(P)$, $Q' = \lambda\varphi(Q)$ on E'

Similar observation: write Π for matrix of π_p with respect to $P, Q \in E[N]$, then

$$\left(\varphi^{(p)} \circ \hat{\varphi}\right)\begin{pmatrix} P' \\ Q' \end{pmatrix} = d\,\varphi^{(p)}\begin{pmatrix} \lambda P \\ \lambda Q \end{pmatrix} = d\,\left(\varphi^{(p)} \circ \pi_p\right)\Pi^{-1}\begin{pmatrix} \lambda P \\ \lambda Q \end{pmatrix}$$

$$= d\,\left(\pi_p \circ \varphi\right)\Pi^{-1}\begin{pmatrix} \lambda P \\ \lambda Q \end{pmatrix} = d\,\Pi^{-1}\begin{pmatrix} P' \\ Q' \end{pmatrix}$$

if cyclic: recover φ from this

Some non-destructive applications

Main by-product [Rob22a]: can **efficiently represent** isogeny $\varphi: E \to E'$ by specifying

- $\deg \varphi$,
- $\varphi(P), \varphi(Q)$ for basis $P, Q \in E[N]$ with $N > 2\sqrt{d}$.

Constructive uses in cryptography:

SQISignHD [DLR+23], FESTA [BMP23], efficient handling of oriented elliptic curves

Other applications [Rob22b], [KR24]:

- **computing** $\mathrm{End}(E)$ for ordinary $E/\mathbf{F}_q$ in polynomial time, given factorization of $\Delta_{\pi_q} = t_{\pi_q}^2 - 4q$,
- **point counting** on $E/\mathbf{F}_{p^n}$ in time $O(n^2 \cdot \mathrm{poly}(\log p))$,
- unconditional $\tilde{O}(\ell^3)$-algorithm for computing **modular polynomial** $\Phi_\ell(X, Y)$

Questions?

Thanks for sitting this out!

References

[BFT14] Bruin, Flynn, Testa, *Descent via* $(3,3)$*-isogeny on Jacobians of genus 2 curves*
[BMP23] Basso, Maino, Pope, *FESTA: fast encryption from supersingular torsion attacks*
[CD23] Castryck, Decru, *An efficient key recovery attack on SIDH*
[CV23] Castryck, Vercauteren, *A polynomial time attack on instances of M-SIDH and FESTA*
[DLR+23] Dartois, Leroux, Robert, Wesolowski, *SQISignHD: new dimensions in cryptography*
[DK23] Decru, Kunzweiler, *Efficient computation of* $(3^n, 3^n)$*-isogenies*
[dQKL+20] de Quehen, Kutas, Leonardi, Martindale, Panny, Petit, Stange, *Improved torsion-point attacks on SIDH variants*
[FMP23] Fouotsa, Moriya, Petit, *M-SIDH and MD-SIDH: countering SIDH attacks by masking information*
[HLP00] Howe, Leprévost, Poonen, *Large torsion subgroups of split Jacobians of curves of genus two or three*
[JDF11] Jao, De Feo, *Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies*
[Kan97] Kani, *The number of curves of genus two with elliptic differentials*
[KR24] Kunzweiler, Robert, *Computing modular polynomials by deformation*
[LR22] Lubicz, Robert, *Fast change of level and applications to isogenies*
[MMP+23] Maino, Martindale, Panny, Pope, Wesolowski, *A direct key recovery attack on SIDH*
[OP22] Oudompheng, Pope, *A note on reimplementing the Castryck-Decru attack and lessons learned for SageMath*
[Pet17] Petit, *Faster algorithms for isogeny problems using torsion point images*
[Rob22a] Robert, *Evaluating isogenies in polylogarithmic time*
[Rob22b] Robert, *Some applications of higher dimensional isogenies to elliptic curves (overview of results)*
[Rob23] Robert, *Breaking SIDH in polynomial time*
[Tat66] Tate, *Endomorphisms of abelian varieties over finite fields*