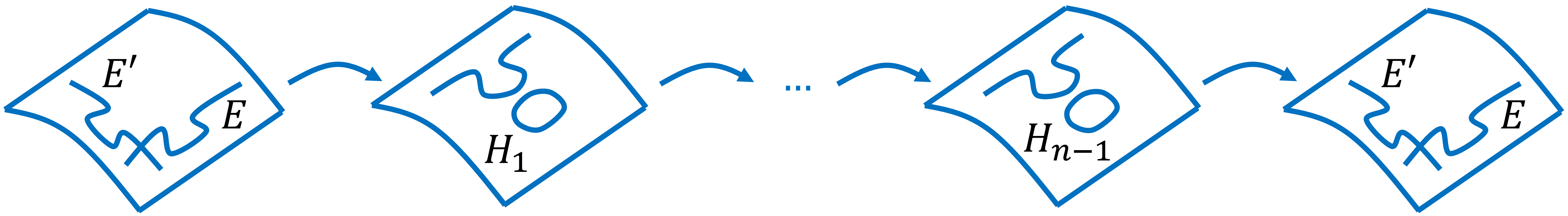
# Breaking SIKE: math and aftermath

Wouter Castryck (KU Leuven)




Latincrypt, Universitad de las Fuerzas Armadas, Quito, 4 October 2023

COSIC

KU LEUVEN

# 1. Post-quantum cryptography

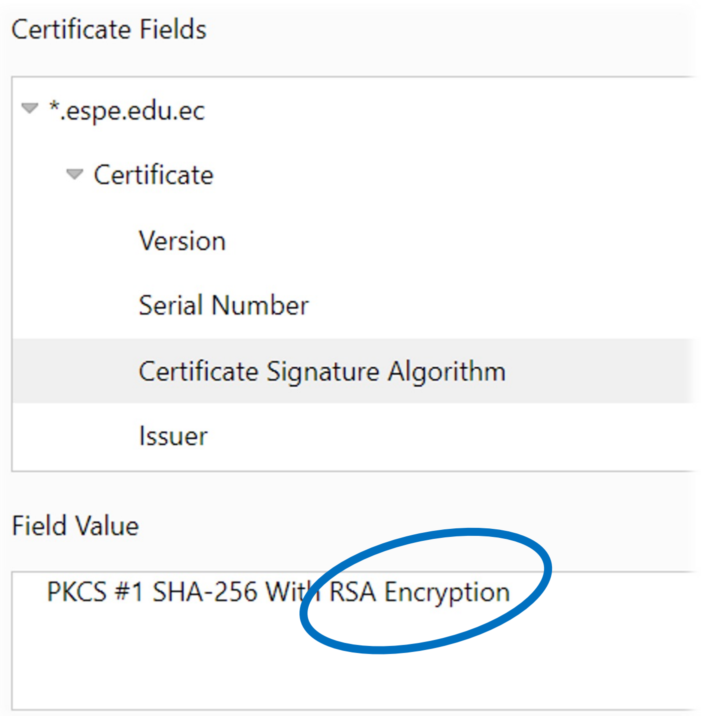
Nearly all currently deployed public-key cryptography is based on hardness of:

- 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. Post-quantum cryptography

Will (universal) quantum computers become real? **Mixed opinions**.

More consensus: **risk** that this happens in the nearish future is **non-negligible**.

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

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

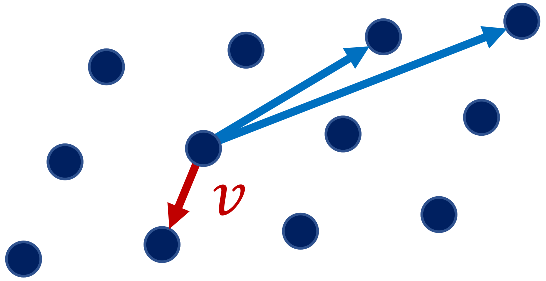
cryptography that

- runs on classical computers,
- resists quantum computers

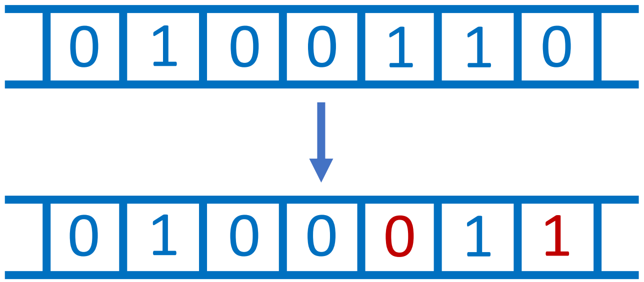
**2017:** NIST initiates "standardization effort" for key encapsulation and signatures

# 1. Post-quantum cryptography

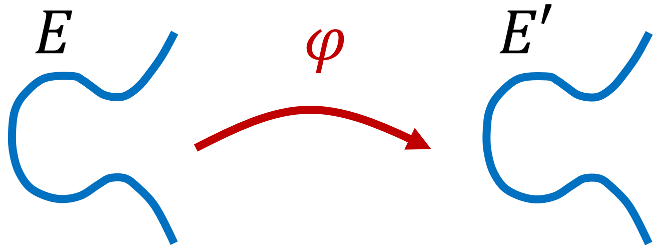
Main contending hard problems:




finding short vectors in lattices



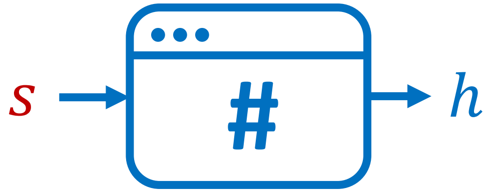

decoding for random linear codes




finding isogenies between elliptic curves

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

solving non-linear systems of equations




finding preimages under hash functions

# 1. Post-quantum cryptography

**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]

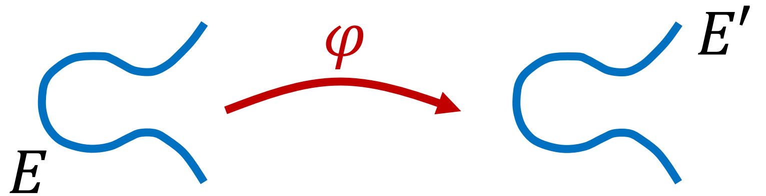
**2023**: Renewed competition for signatures

# 2. 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.




Facts:

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

facts:
- if $\varphi$ is separable then $\#\ker\varphi = \deg\varphi$
- every finite subgroup $K \subset E$ is the kernel of a separable isogeny $\varphi\colon E \to E'$ **(e.g., via Vélu's formulae)**

  and this is unique up to post-composing $\varphi$ with an isomorphism

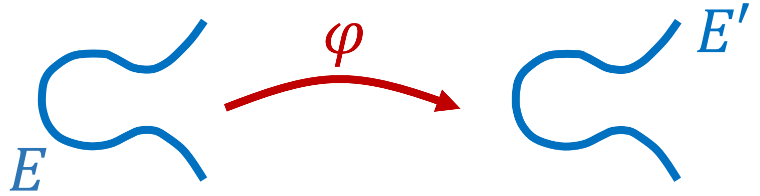
**makes sense to write $E' = E/K$**

# 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:

- isogenies are **surjective group homomorphisms** with **finite kernel** (on $\bar{k}$-points),
- 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 $\#E(\mathbf{F}_q) = \#E'(\mathbf{F}_q)$
- **output:** an $\mathbf{F}_q$-isogeny $\varphi: E \to E'$

Best known general algorithms:
- exponential time complexity,
- quantum computers do not seem to help

# 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, can write $\varphi$ as composition of small-degree isogenies.

**default understanding of "outputting an isogeny"**


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

**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 $\varphi$ as composition of small-degree isogenies.

**default understanding of "returning an isogeny"**


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

**(for the moment, forget about this)**

most important by-product of attack [Rob22a]

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

High-level idea:

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

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

... and likewise for Alice

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

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

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

**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 $\varphi_B(A) = \langle \varphi_B(P_A) + a\varphi_B(Q_A) \rangle$

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

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

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

**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**

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

Very important to note: recovering Alice's 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!

- Recurring issue in cryptographic design.
- Torsion point information was already shown to reveal $\varphi_A$ 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:

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

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

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

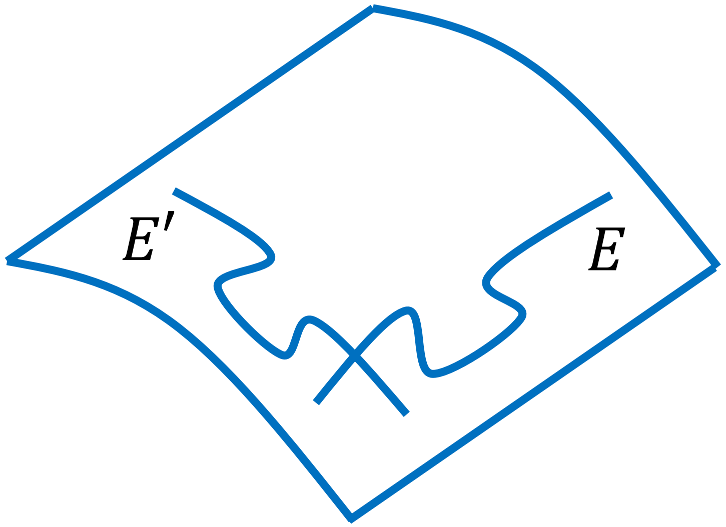
**Lemma** [JU18]

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

# 4. 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:** $N > d$

$$N - d = a^2 \text{ is square}$$

Consider:

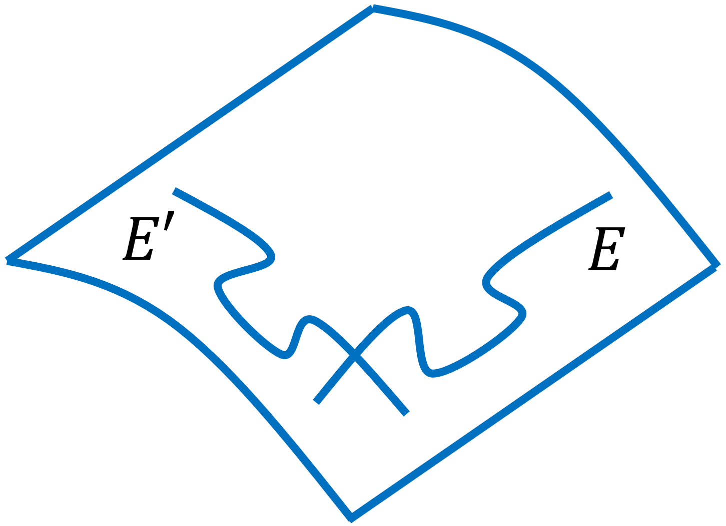
$$\Phi : E \times E' \xrightarrow{\begin{pmatrix} a & \hat{\varphi} \\ -\varphi & a \end{pmatrix}} E \times E'$$

One checks $\widehat{\Phi} \circ \Phi = \Phi \circ \widehat{\Phi} = N$, i.e., $\Phi$ is an $(N, N)$-isogeny.

# 4. Recovering an isogeny from torsion point information

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

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




**Special first case:** $N > d$

$$N - d = a^2 \text{ is square}$$

Consider:

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

One checks $\widehat{\Phi} \circ \Phi = \Phi \circ \widehat{\Phi} = N$, i.e., $\Phi$ is an $(N$

*Proof:*

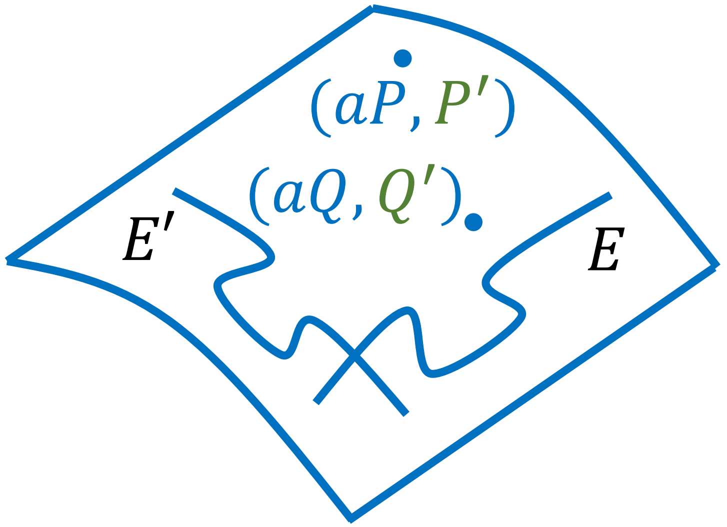
$$\widehat{\Phi} \circ \Phi = \begin{pmatrix} a & -\hat{\varphi} \\ \varphi & a \end{pmatrix} \begin{pmatrix} a & \hat{\varphi} \\ -\varphi & a \end{pmatrix} =$$

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

# 4. Recovering an isogeny from torsion point information

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

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




**Special first case:** $N > d$

$$N - d = a^2 \text{ is square}$$

Consider:

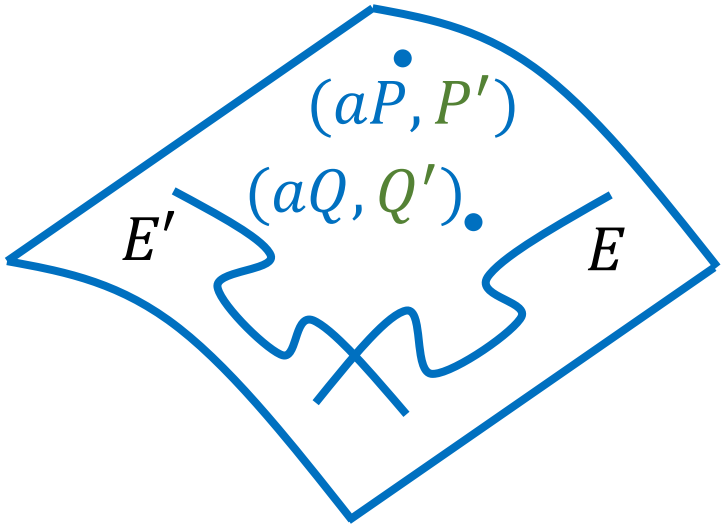
$$\Phi : E \times E' \xrightarrow{\begin{pmatrix} a & \hat{\varphi} \\ -\varphi & a \end{pmatrix}} E \times E'$$

One checks $\widehat{\Phi} \circ \Phi = \Phi \circ \widehat{\Phi} = N$, i.e., $\Phi$ is an $(N, N)$-isogeny.

**Crucially:** we know $\ker \Phi = \langle\, (aP, P'), (aQ, Q')\, \rangle$.

# 4. 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:** $N > d$

$$N - d = a^2 \text{ is square}$$

Consider:

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

One checks $\hat{\Phi} \circ \Phi = \Phi \circ \hat{\Phi} = N$, i.e., $\Phi$ is an $(N$

**Crucially:** we know $\ker \Phi = \langle\, (aP, P'), (aQ, Q')\,\rangle$.

*Proof sketch:*

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

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

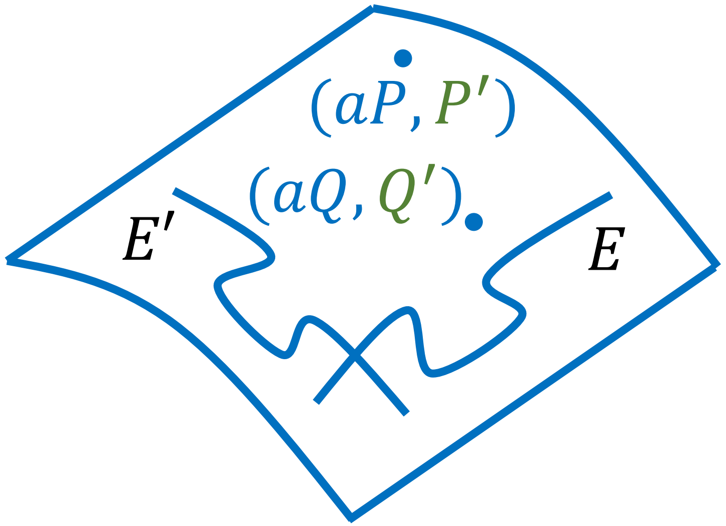
*and likewise for* $(aQ, Q')$.

# 4. Recovering an isogeny from torsion point information

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

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

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




**Special first case:** $N > d$

$$N - d = a^2 \text{ is square}$$

Consider:

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

One checks $\widehat{\Phi} \circ \Phi = \Phi \circ \widehat{\Phi} = N$, i.e., $\Phi$ is an $(N, N)$-isogeny. !

**Crucially:** we know $\ker \Phi = \langle\, (aP, P'), (aQ, Q')\, \rangle$ .

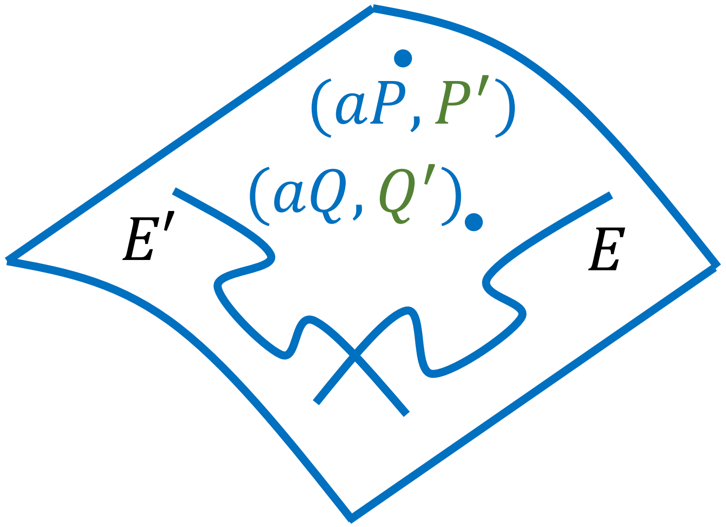
**Consequence:**
using two-dimensional analogues of Vélu, **we can compute** $\varphi(X)$ as the first component of $-\Phi(X, \infty)$, for any $X \in E$

easy to determine $\ker \varphi$ from this

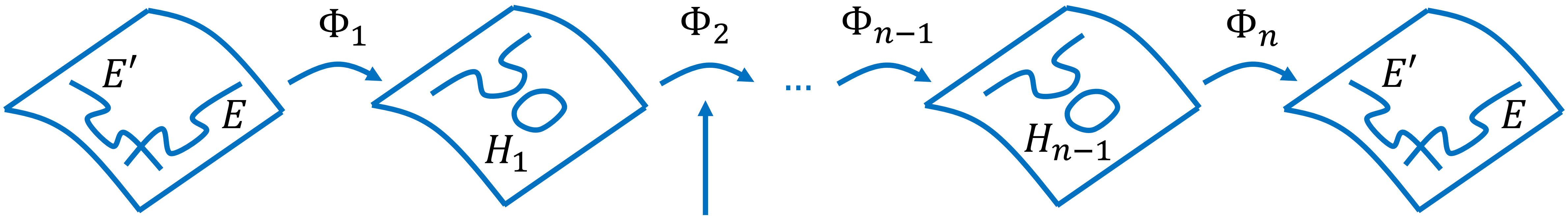
# 4. Recovering an isogeny from torsion point information

**Particularly nice** case: $N = 2^n$

Then $\Phi$ is a composition of $(2,2)$-isogenies.




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



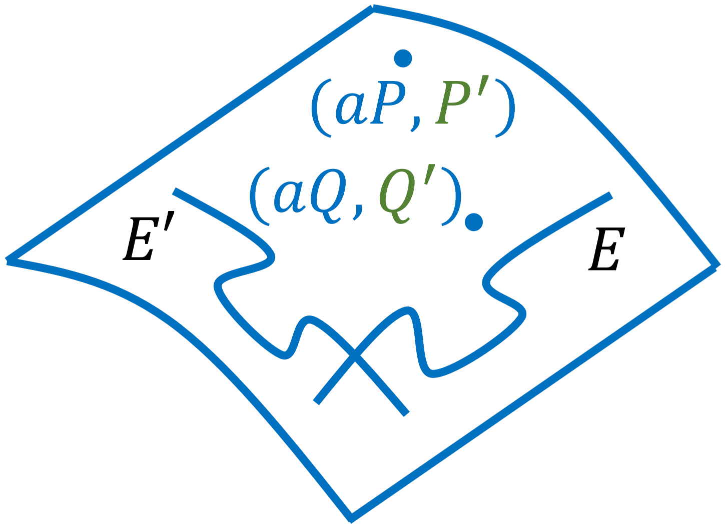

$\ker \Phi_2 = 2^{n-2} \Phi_1(\ker \Phi)$

and so on …

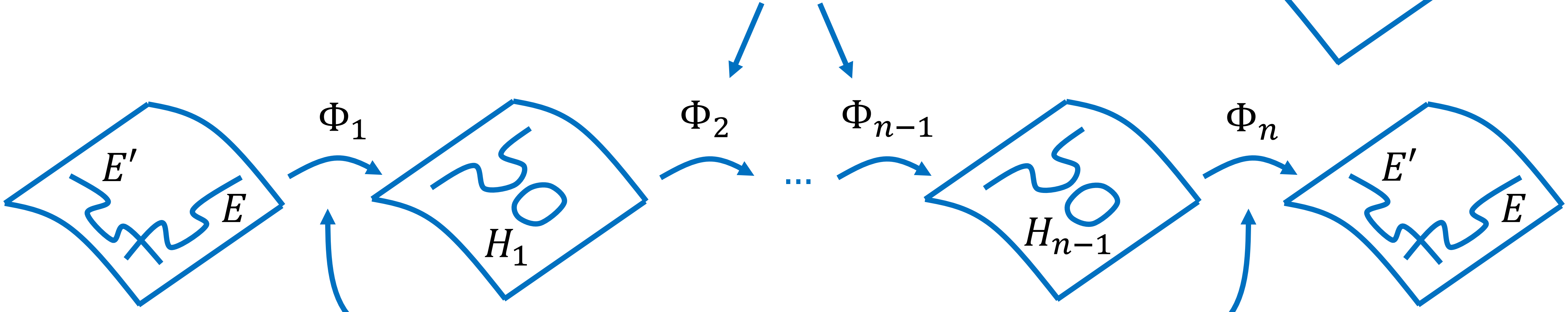
# 4. Recovering an isogeny from torsion point information

Particularly nice case: $N = 2^n$

Then $\Phi$ is a composition of (2,2)-isogenies.




Richelot isogenies (19th century)




explicit gluing formulae [HLP00]

Also explicit: (3,3)-isogenies [BFT14]; otherwise 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:** $N > d$

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

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

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

**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

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

# 4. Recovering an isogeny from torsion point information

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

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

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

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

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

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

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:** $N > \sqrt{d}$

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

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

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

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

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

# 4. Recovering an isogeny from torsion point information

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

**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 $\Phi$ as $\widehat{\widehat{\Phi}}_2 \circ \Phi_1$

# 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. Aftermath

Reality check?

- SIDH/SIKE is dead, despite having withstood 11 years of cryptanalysis
- Rainbow [Beu22] was broken 17 years after its proposal
- Quantum threat is being taken very seriously …
- … but aren't we underestimating the risk of algorithmic breakthrough (even in the case of integer factorization and discrete logarithm computation)?
- Plea for:
  - not rushing things,
  - hybrid encryption for long-term secrets,
  - adaptable cryptography (quick drop-in replacements).

# 5. Aftermath

next big thing in isogeny-based crypto

Future of isogeny-based cryptography?

- Finding isogenies remains hard: schemes like **CSIDH**, **SQISign**, … unaffected.
- Remains very active topic, but **knocked back to high-level research phase**.
- There is also **good news** [Rob22a]: the attack is so efficient that one can now **efficiently represent** isogeny $\varphi: E \to E'$ by specifying
  - $\deg \varphi$,
  - $\varphi(P), \varphi(Q)$ for basis $P, Q \in E[N]$ with $N > 2\sqrt{d}$.
- Led to multiple **constructive uses**: SQISignHD [DLR+23], FESTA [BMP23], SCALLOP-HD [CL23], …

# 5. Aftermath

Mathematical updates:

- Recall:

**Lemma** [JU18]

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

At Bristol/Banff workshop 2023: made **fully algorithmic**.

- Other applications [Rob22b]:
  - **computing** End($E$) for ordinary $E/\mathbf{F}_q$ in polytime, given factorization of discriminant,
  - **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 $\ell$th **modular polynomial**.

# 6. Analysis of a countermeasure (M-SIDH)

We recall:

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

**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 $\lambda$!

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

# 6. Analysis of a countermeasure (M-SIDH)

Leads to following variant:

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

- **input:**
  - $E, E'/\mathbf{F}_q$ connected by an $\mathbf{F}_q$-isogeny $\varphi$ of **known degree** $d$,
  - a basis $P, Q \in E[N] \subset E(\mathbf{F}_q)$ for **smooth** $N > d$,
  - $P' = \lambda\varphi(P), Q' = \lambda\varphi(Q) \in E'[N]$ for some $\lambda \in (\mathbf{Z}/N\mathbf{Z})^*$
- **output:** a representation of $\varphi$.

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 $\lambda^2$

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

# 6. Analysis of a countermeasure (M-SIDH)

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

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

$P$, $Q$ 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 $\sigma$ 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 $\varphi$ from this

# 6. Analysis of a countermeasure (M-SIDH)

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

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

$P$, $Q$

$P' = \lambda\varphi(P)$
$Q' = \lambda\varphi(Q)$

Similar observation: write $\Pi$ for matrix of $\hat{\pi}_p$ with respect to $P, Q \in E[N]$, then

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

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

**if cyclic: recover $\varphi$ from this**

# 6. Analysis of a countermeasure (M-SIDH)

Combination:

$$
\begin{tikzcd}
E^{(p)} \arrow[rr, "\varphi^{(p)}"] & & E'^{(p)} \\
E \arrow[u, "\pi_p"'] \arrow[u, bend left=60, "\sigma"] \arrow[rr, "\varphi"'] & & E' \arrow[u, "\pi_p"']
\end{tikzcd}
$$

$P$ $\qquad$ $P' = \lambda\varphi(P)$

$Q$ $\qquad$ $Q' = \lambda\varphi(Q)$

**existence of smallish $\sigma$ may be hard to detect (backdoors)**

Now: write $\Omega$ for matrix of $\hat{\pi}_p \circ \sigma$ with respect to $P, Q \in E[N]$, then

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

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

**if cyclic and $N > d\sqrt{\deg\sigma}$: recover $\varphi$ from this**

# ¿Preguntas?

Muchísimas gracias por su atención!

# References


[Beu22] Beullens, Breaking Rainbow takes a weekend on a laptop
[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*
[DF+23] De Feo et al, *Modular isogeny problems*
[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*
[JU18] Jao, Urbanik, *The problem landscape of SIDH*
[Kan97] Kani, *The number of curves of genus two with elliptic differentials*
[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*