Breaking SIKE: math and aftermath

Wouter Castryck (KU Leuven)
1. Post-quantum cryptography

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

- integer factorization (RSA)

\[ n = p \cdot q \quad \rightarrow \quad p, q \ ? \]

- discrete logarithm problem (ECC)

\[ P, dP \in E(F_q) \quad \rightarrow \quad d \ ? \]

1994: Peter Shor describes an \( O(\log^3 n) \) quantum algorithm solving both problems

\[ O(\log^3 q) \]
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.

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
- 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)

2023: Renewed competition for signatures

broken few weeks after selection
[CD23], [MMP+23], [Rob23]
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).
- If $\varphi$ is separable then $\# \ker \varphi = \deg \varphi$.
- Every finite subgroup $K \subset E$ is the kernel of a separable isogeny $\varphi: E \to E'$ (e.g., via Vélu's formulae).

Makes sense to write $E' = E/K$ and this is unique up to post-composing $\varphi$ with an isomorphism.
2. The isogeny-finding problem

**Definition**

A homomorphism between two elliptic curves $E$ and $E'$ over a field $k$ is a morphism $\varphi: E \rightarrow E'$ 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 $\varphi: E \rightarrow E'$ there is a unique **dual isogeny** $\hat{\varphi}: E' \rightarrow E$ such that $\varphi \circ \hat{\varphi} = \deg \varphi$, $\hat{\varphi} \circ \varphi = \deg \varphi$, being **isogenous** is an equivalence relation.
2. The isogeny-finding problem

**Theorem [Tat66]**

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

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

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

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

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 $\mathbb{F}_q$-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 $E[N] \subset E(\mathbb{F}_q)$ 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 $\mathbb{F}_q$-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 $E[N] \subseteq E(\mathbb{F}_q)$ 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)
3. Supersingular isogeny Diffie-Hellman (SIDH/SIKE)

High-level idea:

\[ E \xrightarrow{\varphi_A} E_A = E/A \]

\[ E_B = E/B \]

\[ E_{AB} = E_A/\varphi_A(B) \]

\[ E/(A + B) \]

\[ E_{BA} = E_B/\varphi_B(A) \]

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 $P_A, Q_A \in E[N_A]$, $P_B, Q_B \in E[N_B]$

\[
\begin{align*}
E & \xrightarrow{\varphi_A} E_A = E/A \\
A &= \langle P_A + aQ_A \rangle \\
B &= \langle P_B + bQ_B \rangle \\
E_B = E/B & \xrightarrow{\varphi_B} E_{BA} \cong E_{AB} \\
\end{align*}
\]

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

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 $P_A, Q_A \in E[N_A], P_B, Q_B \in E[N_B]$

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

$A = \langle P_A + aQ_A \rangle$

$B = \langle P_B + bQ_B \rangle$

$E_B = E/B$

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)

Very important to note: recovering Alice’s secret isogeny

\[ E \xrightarrow{\varphi_A} E_A = E/A \]

\[ \varphi_A(P_B), \varphi_A(Q_B) \]

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:

\[
\begin{align*}
    E & \xrightarrow{\varphi} E' \\
    P, Q & \quad P' = \varphi(P), Q' = \varphi(Q)
\end{align*}
\]

- **input:**
  - \(E, E'/\mathbb{F}_q\) connected by an \(\mathbb{F}_q\)-isogeny \(\varphi\) of known degree \(d\),
  - a basis \(P, Q \in E[N] \subset E(\mathbb{F}_q)\) 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.

\[N > 2\sqrt{d} \text{ would be the optimal assumption}\]
4. Recovering an isogeny from torsion point information

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

Special first case: \( N > d \)
\[ N - d = a^2 \text{ is square} \]

Consider:
\[
\begin{pmatrix}
a & \hat{\varphi} \\
-\varphi & a
\end{pmatrix}
\]
\( \Phi : E \times E' \rightarrow E \times E' \)

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].

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

Consider:

\[
\begin{pmatrix}
  a & \hat{\phi} \\
  -\phi & a
\end{pmatrix}
\]

\( \Phi : E \times E' \longrightarrow E \times E' \)

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

Proof:

\[
\hat{\Phi} \circ \Phi = \begin{pmatrix}
  a & -\phi \\
  \phi & a
\end{pmatrix}
\begin{pmatrix}
  a & \phi \\
  -\phi & a
\end{pmatrix} = \begin{pmatrix}
  a^2 + \phi \phi & 0 \\
  0 & a^2 + \phi \phi
\end{pmatrix} = \begin{pmatrix}
  a^2 + d & 0 \\
  0 & a^2 + d
\end{pmatrix}
\]
4. Recovering an isogeny from torsion point information

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

\[ E \xrightarrow{\varphi} E' \]

\[ P, Q \quad P' = \varphi(P), Q' = \varphi(Q) \]

**Special first case:** \( N > d \)

\( N - d = a^2 \) is square

Consider:

\[
\begin{pmatrix}
  a & \hat{\varphi} \\
  -\varphi & a
\end{pmatrix}
\]

\[ \Phi : E \times E' \xrightarrow{\varphi} E \times E' \]

One checks \( \hat{\Phi} \circ \Phi = \Phi \circ \hat{\Phi} = N \), 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].

\[ \begin{align*}
E & \xrightarrow{\varphi} E' \\
P, Q & \quad P' = \varphi(P), Q' = \varphi(Q)
\end{align*} \]

**Special first case:** \( N > d \)

\( N - d = a^2 \) is square

Consider:

\[
\begin{pmatrix} a & \hat{\varphi} \\ -\varphi & a \end{pmatrix}
\]

\( \Phi : E \times E' \rightarrow E \times E' \)

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

**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].

\[ E \xrightarrow{\varphi} E' \]
\[ P, Q \]
\[ P' = \varphi(P), Q' = \varphi(Q) \]

**Special first case:** \( N > d \)
\[ N - d = a^2 \text{ is square} \]

Consider:
\[
\begin{pmatrix}
  a & \hat{\phi} \\
  -\varphi & a
\end{pmatrix}
\]

\[ \Phi : E \times E' \xrightarrow{} E \times E' \]

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

**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.

\begin{align*}
\text{Consequence:} & \\
\text{we know } \ker \Phi &= \langle (aP,P'), (aQ,Q') \rangle \cdot
\end{align*}
Particularly nice case: $N = 2^n$

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

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

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

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)

Also explicit: $(3,3)$-isogenies [BFT14]; otherwise resort to [LR22].
4. Recovering an isogeny from torsion point information

Next case: $N > d$

$N - d = a_1^2 + a_2^2$ is sum of two squares

Approach: same, but use

$$
\Phi : E^2 \times E'^2 \rightarrow E^2 \times E'^2
$$

Now must resort to algorithms from [LR22].
4. Recovering an isogeny from torsion point information

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

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

\[
\begin{pmatrix}
a_1 & -a_2 & -a_3 & -a_4 & \phi & 0 & 0 & 0 \\
a_2 & a_1 & a_4 & -a_3 & 0 & \phi & 0 & 0 \\
a_3 & -a_4 & a_1 & a_2 & 0 & 0 & \phi & 0 \\
a_4 & a_3 & -a_2 & a_1 & 0 & 0 & 0 & \phi \\
-\varphi & 0 & 0 & 0 & a_1 & a_2 & a_3 & a_4 \\
0 & -\varphi & 0 & 0 & -a_2 & a_1 & -a_4 & a_3 \\
0 & 0 & -\varphi & 0 & -a_3 & a_4 & a_1 & -a_2 \\
0 & 0 & 0 & -\varphi & -a_4 & -a_3 & a_2 & a_1
\end{pmatrix}
\]
4. Recovering an isogeny from torsion point information

\[
\begin{align*}
E & \xrightarrow{\varphi} E' \\
P, Q & \quad P' = \varphi(P), Q' = \varphi(Q)
\end{align*}
\]

**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 \( \frac{1}{N} P, \frac{1}{N} Q \in E[N^2] \).

\[
\begin{align*}
A & \xrightarrow{\Phi ?} A \\
\quad E^r \times E'^r & \quad \text{we no longer know ker } \Phi...
\end{align*}
\]
4. Recovering an isogeny from torsion point information

\[
\begin{align*}
E & \xrightarrow{\varphi} E' \\
P, Q & \quad P' = \varphi(P), Q' = \varphi(Q)
\end{align*}
\]

**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 \(\frac{1}{N} P, \frac{1}{N} Q \in E[N^2]\).

\[
\begin{align*}
A & \xrightarrow{\Phi_1} X \xleftarrow{\Phi_2} A \\
E^r \times E'^r & \quad \text{we also know } N(\ker \hat{\Phi})
\end{align*}
\]

but we do know \(N(\ker \Phi)\)!
4. Recovering an isogeny from torsion point information

\[
\begin{align*}
E & \xrightarrow{\varphi} E' \\
P, Q & \quad P' = \varphi(P), Q' = \varphi(Q)
\end{align*}
\]

**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 \textbf{as if we know} the images of \( \frac{1}{N} P, \frac{1}{N} Q \in E[N^2] \).

\[
\begin{align*}
A & \xrightarrow{\Phi_1} X & \quad \xleftarrow{\Phi_2} A \\
\| & \quad E^r \times E'^r
\end{align*}
\]

so we recover \( \Phi \) as \( \widehat{\Phi}_2 \circ \Phi_1 \)
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,
- \(|N_A - N_B| = a_1^2 + a_2^2\) 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,

\[ E: y^2 = x^3 + x \]

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

\[ \Phi : E \times E' \to E \times C \]

\[ \Phi : E \times E' \to E \times C \]

- $|N_A - N_B| = a_1^2 + a_2^2$ 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

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 \( \varphi: E \rightarrow E' \) 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** $\text{End}(E)$ for ordinary $E/\mathbb{F}_q$ in polytime, given factorization of discriminant,
  
  - **point counting** on $E/\mathbb{F}_{p^n}$ in time $O(n^2 \cdot \text{poly}(\log p))$,
  
  - unconditional $\tilde{O}(\ell^3)$-algorithm for computing $\ell$th **modular polynomial**.
6. Analysis of a countermeasure (M-SIDH)

We recall:

\[ E = \mathbb{E}(E) \]

\[ A = \langle P_A + aQ_A \rangle \]

\[ E_A = E / A \]

Alice reveals

\[ \varphi_A(P_B), \varphi_A(Q_B) \]

allows Bob to compute

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

Bob reveals

\[ \varphi_B(P_A), \varphi_B(Q_A) \]

allows Alice to compute

\[ \varphi_B(A) = \langle \varphi_B(P_A) + a\varphi_B(Q_A) \rangle \]

Observation

It suffices to reveal \( \lambda\varphi_A(P_B), \lambda\varphi_A(Q_B) \) for some secret \( \lambda \)!
6. Analysis of a countermeasure (M-SIDH)

Leads to following variant:

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

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

- **output:** a representation of \(\varphi\).

Weil pairing: \(e_N(P', Q') = e_N(\lambda \varphi(P), \lambda \varphi(Q)) = e_N(P, Q)^{\lambda^2d} \rightarrow \text{reveals } \lambda^2\)

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]

Observation: write $\Sigma \in (\mathbb{Z}/N\mathbb{Z})^{2\times 2}$ 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 $\mathbb{F}_p$: variation on this idea [CV23]

$\pi_p \quad E \quad \varphi(p) \quad E'(p) \quad \pi_p$

$\varphi \quad P \quad Q \quad \lambda \mathbf{P}$

$\lambda \mathbf{Q}$

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

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

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

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

if cyclic: recover $\varphi$ from this
6. Analysis of a countermeasure (M-SIDH)

Combination:

\[ \begin{array}{c}
E(p) \quad \varphi(p) \quad E'(p) \\
\sigma \quad \pi_p \quad \pi_p \\
E \quad P \quad E' \\
P \quad Q \quad P' = \lambda \varphi(P) \\
Q \quad Q' = \lambda \varphi(Q) \\
\end{array} \]

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 \(\left(3^n, 3^n\right)\)-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