# SQIPrime & SILBE: New isogeny based cryptographic protocols

Master thesis defense

Max Duparc

Supervision: Dr. Tako Boris Fouotsa
Professor: Serge Vaudenay

February 19, 2024

# Outline

We present two new isogenies based cryptosystems:

- **SQIPrime**: A post-quantum identification scheme that relies on isogenies of big prime degree.
- **SILBE**: A post-quantum Updatable Public Key Encryption (UPKE) scheme based on the generalised lollipop attacks over M-SIDH.

- Both protocols make extensive usage of the multiple isogeny representations used in cryptography.

# Outline

We present two new isogenies based cryptosystems:

- **SQIPrime**: A post-quantum identification scheme that relies on isogenies of big prime degree.
- **SILBE**: A post-quantum Updatable Public Key Encryption (UPKE) scheme based on the generalised lollipop attacks over M-SIDH.

▶ Both protocols make extensive usage of the multiple isogeny representations used in cryptography.

# Outline

We present two new isogenies based cryptosystems:

- **SQIPrime**: A post-quantum identification scheme that relies on isogenies of big prime degree.
- **SILBE**: A post-quantum Updatable Public Key Encryption (UPKE) scheme based on the generalised lollipop attacks over M-SIDH.

- Both protocols make extensive usage of the multiple isogeny representations used in cryptography.

# Outline

We present two new isogenies based cryptosystems:

- **SQIPrime**: A post-quantum identification scheme that relies on isogenies of big prime degree.
- **SILBE**: A post-quantum Updatable Public Key Encryption (UPKE) scheme based on the generalised lollipop attacks over M-SIDH.

- Both protocols make extensive usage of the multiple isogeny representations used in cryptography.

# Table of Contents

# Elliptic curves

- *Weierstrass equations*:

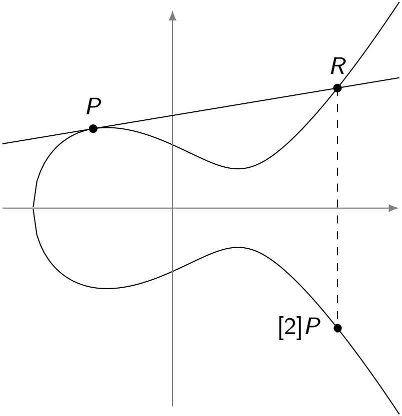
$$E : y^2 = x^3 + Ax + B$$

with $4A^3 + 27B^2 \neq 0$.

- *Abelian groups*.
- *j-invariant*:

$$j(E) = 1728 \frac{4A^3}{4A^3 + 27B^2}$$

characterises isomorphism.




▶ $\simeq 70\%$ of all TLS connections use ECDH.

# Elliptic curves

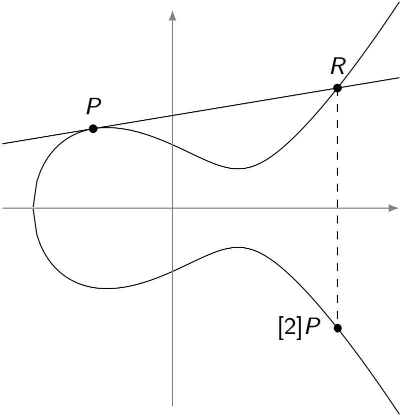
- *Weierstrass equations*:

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

  with $4A^3 + 27B^2 \neq 0$.
- *Abelian groups*.
- *j-invariant*:

$$j(E) = 1728 \frac{4A^3}{4A^3 + 27B^2}$$

  characterises isomorphism.




▶ $\simeq$ 70% of all TLS connections use ECDH.

# Isogenies

## Isogenies

Isogenies are rational maps $\phi : E \to E'$ that preserve the group structure.

- Have finite kernel.




$E : y^2 = x^3 - 3x + 3$ $\qquad$ $E' : y^2 = x^3 + 5x + 6$

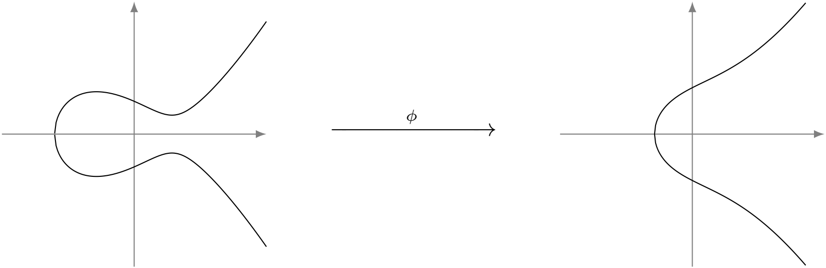
$$\phi : (x, y) \to \left( \frac{x^2 + 6x + 1}{x - 7}, \frac{x^2 - x - 4}{(x-7)^2} y \right) \text{ of degree 2 in } \mathbb{F}_{13}$$

# Isogenies

## Isogenies

Isogenies are rational maps $\phi : E \to E'$ that preserve the group structure.

- Have finite kernel.




$E : y^2 = x^3 - 3x + 3$ $\qquad$ $E' : y^2 = x^3 + 5x + 6$

$$\phi : (x, y) \to \left( \frac{x^2 + 6x + 1}{x - 7}, \frac{x^2 - x - 4}{(x-7)^2} y \right) \text{ of degree 2 in } \mathbb{F}_{13}$$

# Efficient representations

## Natural examples

- *Scalar maps*:

$$[n] : E \to E$$

- *Frobenius isogeny*:

$$\pi : E \to E^{(p)}$$

$$(x, y) \mapsto (x^p, y^p)$$

## Efficient isogeny representation

Let $\phi : E \to E'$ be an isogeny. An *efficient representation* of $\phi$ is:

- $D$: data of size polylog(deg $\phi$) that *uniquely* define $\phi$.
- $\mathcal{A}$: a *universal* algorithm that for any $P \in E$:

$$\mathcal{A}(D, P) \mapsto \phi(P)$$

in time polylog(deg $\phi$).

# Efficient representations

## Natural examples

- *Scalar maps*:

$$[n] : E \to E$$

- *Frobenius isogeny*:

$$\pi : E \to E^{(p)}$$
$$(x, y) \mapsto (x^p, y^p)$$

## Efficient isogeny representation

Let $\phi : E \to E'$ be an isogeny. An *efficient representation* of $\phi$ is:

- $D$: data of size polylog$(\deg \phi)$ that *uniquely* define $\phi$.
- $\mathcal{A}$: a *universal* algorithm that for any $P \in E$:

$$\mathcal{A}(D, P) \mapsto \phi(P)$$

  in time polylog$(\deg \phi)$.

# Kernel representation

**Theorem**

Let $G$ a finite subgroup of $E$, it uniquely defines

$$\phi : E \to E/G$$

an isogeny of degree $|G|$ up to isomorphism.

**Isogeny isomorphism**

$\phi : E \to F$ and $\psi : E' \to F'$ are isomorphic if

$$\begin{array}{ccc} E & \xrightarrow{\quad\phi\quad} & F \\ \iota\Big\| & & \Big\|\kappa \\ E' & \xrightarrow{\quad\psi\quad} & F' \end{array}$$

- Any isogeny $\phi : E \to E'$ induces a dual isogeny $\widehat{\phi} : E' \to E$:

$$\phi \circ \hat{\phi} = \hat{\phi} \circ \phi = [\deg(\phi)]$$

- Given $E[n] = \ker([n])$, we have that $E[n] = \mathbb{Z}_n \times \mathbb{Z}_n$ for any $n$ coprime to $p$.

**Vélu's formulas**

Given $G \subset E$ a subgroup, we can compute $\phi : E \to E/G$ in time $O(|G|)$.

# Kernel representation

**Theorem**

Let $G$ a finite subgroup of $E$, it uniquely defines

$$\phi : E \to E/G$$

an isogeny of degree $|G|$ up to isomorphism.

**Isogeny isomorphism**

$\phi : E \to F$ and $\psi : E' \to F'$ are isomorphic if

$$\begin{array}{ccc} E & \xrightarrow{\phi} & F \\ \iota \Big\| & & \Big\| \kappa \\ E' & \xrightarrow{\psi} & F' \end{array}$$

- Any isogeny $\phi : E \to E'$ induces a dual isogeny $\widehat{\phi} : E' \to E$:

$$\phi \circ \hat{\phi} = \hat{\phi} \circ \phi = [\deg(\phi)]$$

- Given $E[n] = \ker([n])$, we have that $E[n] = \mathbb{Z}_n \times \mathbb{Z}_n$ for any $n$ coprime to $p$.

**Vélu's formulas**

Given $G \subset E$ a subgroup, we can compute $\phi : E \to E/G$ in time $O(|G|)$.

# Kernel representation

### Theorem

Let $G$ a finite subgroup of $E$, it uniquely defines

$$\phi : E \to E/G$$

an isogeny of degree $|G|$ up to isomorphism.

### Isogeny isomorphism

$\phi : E \to F$ and $\psi : E' \to F'$ are isomorphic if

$$\begin{array}{ccc} E & \xrightarrow{\phi} & F \\ \iota \Big\| & & \Big\| \kappa \\ E' & \xrightarrow{\psi} & F' \end{array}$$

- Any isogeny $\phi : E \to E'$ induces a dual isogeny $\widehat{\phi} : E' \to E$:

$$\phi \circ \hat{\phi} = \hat{\phi} \circ \phi = [\deg(\phi)]$$

- Given $E[n] = \ker([n])$, we have that $E[n] = \mathbb{Z}_n \times \mathbb{Z}_n$ for any $n$ coprime to $p$.

### Vélu's formulas

Given $G \subset E$ a subgroup, we can compute $\phi : E \to E/G$ in time $O(|G|)$.

# Kernel representation

**Theorem**

Let $G$ a finite subgroup of $E$, it uniquely defines

$$\phi : E \to E/G$$

an isogeny of degree $|G|$ up to isomorphism.

**Isogeny isomorphism**

$\phi : E \to F$ and $\psi : E' \to F'$ are isomorphic if

$$\begin{array}{ccc} E & \xrightarrow{\phi} & F \\ \iota \Big\| & & \Big\| \kappa \\ E' & \xrightarrow{\psi} & F' \end{array}$$

- Any isogeny $\phi : E \to E'$ induces a dual isogeny $\widehat{\phi} : E' \to E$:

$$\phi \circ \hat{\phi} = \hat{\phi} \circ \phi = [\deg(\phi)]$$

- Given $E[n] = \ker([n])$, we have that $E[n] = \mathbb{Z}_n \times \mathbb{Z}_n$ for any $n$ coprime to $p$.

**Vélu's formulas**

Given $G \subset E$ a subgroup, we can compute $\phi : E \to E/G$ in time $O(|G|)$.

# Kernel representation

## Kernel representation

Let $\phi : E \to E'$ be a cyclic isogeny of *smooth* degree $d$. Its *kernel representation* is:

- $K \in E[d]$ s.t. $\langle K \rangle = \ker(\phi)$.
- **KernelToIsogeny**

$$E \xrightarrow{\phi_1} E_1 \xrightarrow{\phi_2} E_2 \xrightarrow{\phi_3} \cdots \xrightarrow{\phi_n} E' \quad (\phi : E \to E')$$

with $\deg(\phi) = \prod_{i=1}^{n} p_i$ and $\deg(\phi_i) = p_i$.

Drawbacks:

- Only efficient on *smooth* isogenies.

Advantages:

- Compact.
- Very efficient
- Evaluate all points.

# Kernel representation

## Kernel representation

Let $\phi : E \to E'$ be a cyclic isogeny of *smooth* degree $d$. Its *kernel representation* is:

- $K \in E[d]$ s.t. $\langle K \rangle = \ker(\phi)$.
- **KernelToIsogeny**

$$E \xrightarrow{\phi_1} E_1 \xrightarrow{\phi_2} E_2 \xrightarrow{\phi_3} \cdots \xrightarrow{\phi_n} E', \qquad \phi : E \to E'$$

with $\deg(\phi) = \prod_{i=1}^{n} p_i$ and $\deg(\phi_i) = p_i$.

Drawbacks:

- Only efficient on *smooth* isogenies.

Advantages:

- Compact.
- Very efficient
- Evaluate all points.

# Kernel representation

## Kernel representation

Let $\phi : E \to E'$ be a cyclic isogeny of *smooth* degree $d$. Its *kernel representation* is:

- $K \in E[d]$ s.t. $\langle K \rangle = \ker(\phi)$.
- **KernelToIsogeny**

$$E \xrightarrow{\phi_1} E_1 \xrightarrow{\phi_2} E_2 \xrightarrow{\phi_3} \cdots \xrightarrow{\phi_n} E', \qquad \phi : E \to E'$$

with $\deg(\phi) = \prod_{i=1}^{n} p_i$ and $\deg(\phi_i) = p_i$.

DRAWBACKS:

- Only efficient on *smooth* isogenies.

ADVANTAGES:

- Compact.
- Very efficient
- Evaluate all points.

# Supersingularity

**Theorem**

Let $E$ be an elliptic curve defined over $\overline{\mathbb{F}_p}$.

- End($E$) is an order[a] of a complex quadratic field $\mathbb{Q}(\sqrt{D})$.
  - $E$ is an *ordinary* curve.
- End($E$) is a maximal order of a quaternion algebra $\mathbf{B}_{p,\infty}$.
  - $E$ is a *supersingular* curve.

[a] full rank lattices that are also subrings

Supersingular curves are SUPER nice:

- All are defined in $\mathbb{F}_{p^2}$ up to isomorphism.
- $E(\mathbb{F}_{p^2}) \cong \mathbb{Z}_{p\pm1} \times \mathbb{Z}_{p\pm1}$.
- Supersingularity is preserved by isogenies.
- All supersingular curves are isogeneous.

# Supersingularity

**Theorem**

Let $E$ be an elliptic curve defined over $\overline{\mathbb{F}_p}$.

- End($E$) is an order[a] of a complex quadratic field $\mathbb{Q}(\sqrt{D})$.
  - $E$ is an *ordinary* curve.
- End($E$) is a maximal order of a quaternion algebra $\mathbf{B}_{p,\infty}$.
  - $E$ is a *supersingular* curve.

[a] full rank lattices that are also subrings

Supersingular curves are SUPER nice:

- All are defined in $\mathbb{F}_{p^2}$ up to isomorphism.
- $E(\mathbb{F}_{p^2}) \cong \mathbb{Z}_{p\pm 1} \times \mathbb{Z}_{p\pm 1}$.
- Supersingularity is preserved by isogenies.
- All supersingular curves are isogeneous.

# Supersingular isogeny graphs

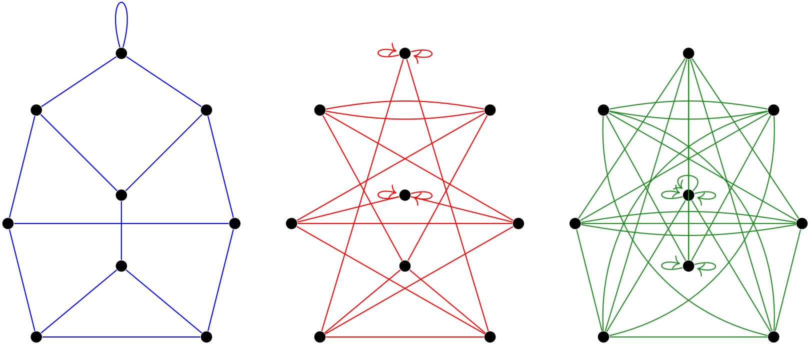
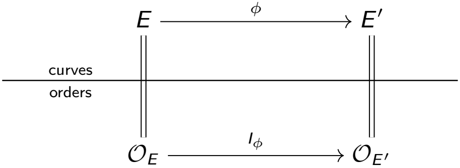


Figure: Supersingular isogeny graphs $\mathcal{G}^2_{109}$, $\mathcal{G}^3_{109}$ and $\mathcal{G}^5_{109}$

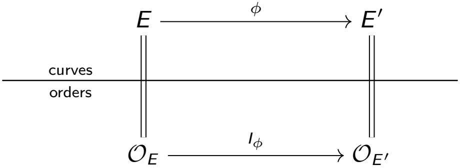
# Deuring Correspondence




| Supersingular $j$-invariants on $\mathbb{F}_{p^2}$ | Maximal orders in $B_{p,\infty}$ |
|---|---|
| $j(E)$ | $\mathcal{O}_E$ |
| $\phi \circ \psi$ | $I_\psi I_\phi$ |
| $\deg(\phi)$ | $n(I_\phi)$ |
| $\widehat{\phi}$ | $\overline{I_\phi}$ |
| $\psi_* \phi$ | $[I_\psi]_* I_\phi = \frac{1}{n(I_\psi)} \overline{I_\psi}(I_\psi \cap I_\phi)$ |
| $\gamma \in \mathrm{End}(E)$ | $\mathcal{O}_E \gamma$ |

$I_\phi = \{\alpha \in \mathcal{O}_E \mid \alpha(\ker(\phi)) = 0\}$ $\qquad$ $\ker(\phi_I) = \{P \in E \mid \alpha(P) = 0 \ \forall \alpha \in I\}$

# Deuring Correspondence




| **Supersingular $j$-invariants on $\mathbb{F}_{p^2}$** | **Maximal orders in $\mathbf{B}_{p,\infty}$** |
|---|---|
| $j(E)$ | $\mathcal{O}_E$ |
| $\phi \circ \psi$ | $I_\psi I_\phi$ |
| $\deg(\phi)$ | $n(I_\phi)$ |
| $\widehat{\phi}$ | $\overline{I_\phi}$ |
| $\psi_*\phi$ | $[I_\psi]_* I_\phi = \frac{1}{n(I_\psi)} \overline{I_\psi}(I_\psi \cap I_\phi)$ |
| $\gamma \in \mathrm{End}(E)$ | $\mathcal{O}_E \gamma$ |

$$I_\phi = \{\alpha \in \mathcal{O}_E \mid \alpha(\ker(\phi)) = 0\} \qquad \ker(\phi_I) = \{P \in E \mid \alpha(P) = 0 \ \forall \alpha \in I\}$$

# Ideal representation

Handful of special curves have known $\mathcal{O}_E$ (ex: $j(E_0) = 1728$).

## Ideal representation

Let $\phi : E_1 \to E_2$ be an isogeny of degree $d$. Its *ideal representation* is:

- $J$ the ideal corresponding to $\phi$, $\mathcal{O}_0$, $\rho_i : E_0 \to E_i$ and $I_i$.
- **EvalTorsion**

**EvalTorsion**:

1. Find $\gamma \in \mathcal{O}_0$ s.t. $\mathcal{O}_0\gamma = I_1 J \overline{I_2}$.
2. Evaluate $\gamma \circ \widehat{\rho_1}(P)$.
3. return $\phi_J(P) := [(d_1 d_2)^{-1}]\rho_2 \circ \gamma \circ \widehat{\rho_1}(P) \mod N$.

$\deg(\rho_i) = d_i$ and $P \in E[N]$.




DRAWBACKS:

- Need knowledge of endomorphism ring.
- Can only evaluate points of order coprime to $d_1 d_2$.

ADVANTAGES:

- Works on any degree.
- Relatively efficient.
- Enables new computations.

# Ideal representation

Handful of special curves have known $\mathcal{O}_E$ (ex: $j(E_0) = 1728$).

## Ideal representation

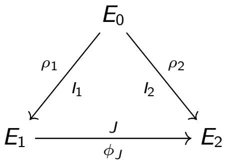
Let $\phi : E_1 \to E_2$ be an isogeny of degree $d$. Its *ideal representation* is:

- $J$ the ideal corresponding to $\phi$, $\mathcal{O}_0$, $\rho_i : E_0 \to E_i$ and $I_i$.
- **EvalTorsion**

**EvalTorsion**:

1. Find $\gamma \in \mathcal{O}_0$ s.t. $\mathcal{O}_0\gamma = I_1 J \overline{I_2}$.
2. Evaluate $\gamma \circ \widehat{\rho_1}(P)$.
3. return $\phi_J(P) := [(d_1 d_2)^{-1}]\rho_2 \circ \gamma \circ \widehat{\rho_1}(P) \mod N$.

$\deg(\rho_i) = d_i$ and $P \in E[N]$.




DRAWBACKS:

- Need knowledge of endomorphism ring.
- Can only evaluate points of order coprime to $d_1 d_2$.

ADVANTAGES:

- Works on any degree.
- Relatively efficient.
- Enables new computations.

# Ideal representation

Handful of special curves have known $\mathcal{O}_E$ (ex: $j(E_0) = 1728$).

## Ideal representation

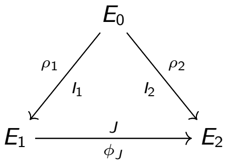
Let $\phi : E_1 \to E_2$ be an isogeny of degree $d$. Its *ideal representation* is:

- $J$ the ideal corresponding to $\phi$, $\mathcal{O}_0$, $\rho_i : E_0 \to E_i$ and $I_i$.
- **EvalTorsion**

**EvalTorsion**:

1. Find $\gamma \in \mathcal{O}_0$ s.t. $\mathcal{O}_0\gamma = I_1 J \overline{I_2}$.
2. Evaluate $\gamma \circ \widehat{\rho_1}(P)$.
3. return $\phi_J(P) := [(d_1 d_2)^{-1}]\rho_2 \circ \gamma \circ \widehat{\rho_1}(P) \mod N$.

$\deg(\rho_i) = d_i$ and $P \in E[N]$.




DRAWBACKS:

- Need knowledge of endomorphism ring.
- Can only evaluate points of order coprime to $d_1 d_2$.

ADVANTAGES:

- Works on any degree.
- Relatively efficient.
- Enables new computations.

# Kani's Lemma

Let $A, B, A', B'$ be *abelian varieties* with commutative diagram:

$$\begin{array}{ccc} A & \xrightarrow{\;f\;} & B \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle g'} \\ A' & \xrightarrow{\;f'\;} & B' \end{array}$$

- $\deg(f) = \deg(f')$
- $\deg(g) = \deg(g')$

**Kani's Lemma**

1. The following map is an isogeny such that $\deg(F) = \deg(f) + \deg(g)$

$$F := \begin{pmatrix} \tilde{f} & -\tilde{g} \\ g' & f' \end{pmatrix} : B \times A' \to A \times B'$$

2. Its kernel is

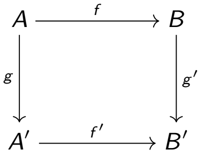
$$\ker(F) = \left\{ (f(P), -g(P)) \,\middle|\, P \in A[\deg(F)] \right\}$$

**HDKernelToIsogeny**

Given $\mathcal{B}$ a basis of $\ker(\phi)$ with $\phi : A \to A'$ a $B$-smooth *dim k* isogeny of degree $d$, we can compute $\phi$ in time $O(B^k \log(d))$.

# Kani's Lemma

Let $A, B, A', B'$ be *abelian varieties* with commutative diagram:




- $\deg(f) = \deg(f')$
- $\deg(g) = \deg(g')$

## Kani's Lemma

1. The following map is an isogeny such that $\deg(F) = \deg(f) + \deg(g)$

$$F := \begin{pmatrix} \tilde{f} & -\tilde{g} \\ g' & f' \end{pmatrix} : B \times A' \to A \times B'$$

2. Its kernel is

$$\ker(F) = \left\{ (f(P), -g(P)) \middle| P \in A[\deg(F)] \right\}$$

## HDKernelToIsogeny

Given $\mathcal{B}$ a basis of $\ker(\phi)$ with $\phi : A \to A'$ a $B$-smooth *dim $k$* isogeny of degree $d$, we can compute $\phi$ in time $O(B^k \log(d))$.

# HD representation

## HD representation

Let $\phi : E \to E'$ be an isogeny of degree $d$, its *HD representation* is:

- $\big(P, Q, \phi(P), \phi(Q)\big)$ with $\langle P, Q\rangle = E[N]$, $N$ *smooth*, coprime to $d$ with $N \geq \sqrt{d}$.
- **EvalKani**

**EvalKani**:

1. Find $\{a_i\}_{i=1}^{g}$ s.t. $\sum_{i=1}^{g} a_i^2 = N - \deg(\phi)$.
2. Compute $\alpha_g$ depending on $g$.
3. Compute $F$ Kani's isogeny in dim $2g$.
4. Evaluate $\phi$ using $F$.

with $\langle P, Q\rangle = E[N]$ and knowing $\phi(P), \phi(Q)$.




$$\alpha_2 := \begin{pmatrix} a_1 & -a_2 \\ a_2 & a_1 \end{pmatrix}$$

Drawbacks:

- Relatively slow

Advantages:

- Works for any degree.
- Works for any points.

# HD representation

## HD representation

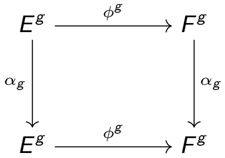
Let $\phi : E \to E'$ be an isogeny of degree $d$, its *HD representation* is:

- $\big(P, Q, \phi(P), \phi(Q)\big)$ with $\langle P, Q\rangle = E[N]$, $N$ *smooth*, coprime to $d$ with $N \geq \sqrt{d}$.
- **EvalKani**

**EvalKani**:

1. Find $\{a_i\}_{i=1}^{g}$ s.t. $\sum_{i=1}^{g} a_i^2 = N - \deg(\phi)$.
2. Compute $\alpha_g$ depending on $g$.
3. Compute $F$ Kani's isogeny in dim $2g$.
4. Evaluate $\phi$ using $F$.

with $\langle P, Q\rangle = E[N]$ and knowing $\phi(P), \phi(Q)$.




$$\alpha_2 := \begin{pmatrix} a_1 & -a_2 \\ a_2 & a_1 \end{pmatrix}$$

Drawbacks:

- Relatively slow

Advantages:

- Works for any degree.
- Works for any points.

# HD representation

## HD representation

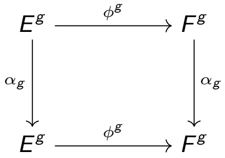
Let $\phi : E \to E'$ be an isogeny of degree $d$, its *HD representation* is:

- $\big(P, Q, \phi(P), \phi(Q)\big)$ with $\langle P, Q\rangle = E[N]$, $N$ *smooth*, coprime to $d$ with $N \geq \sqrt{d}$.
- **EvalKani**

**EvalKani**:

1. Find $\{a_i\}_{i=1}^{g}$ s.t. $\sum_{i=1}^{g} a_i^2 = N - \deg(\phi)$.
2. Compute $\alpha_g$ depending on $g$.
3. Compute $F$ Kani's isogeny in dim $2g$.
4. Evaluate $\phi$ using $F$.

with $\langle P, Q\rangle = E[N]$ and knowing $\phi(P), \phi(Q)$.




$$\alpha_2 := \begin{pmatrix} a_1 & -a_2 \\ a_2 & a_1 \end{pmatrix}$$

Drawbacks:

- Relatively slow

Advantages:

- Works for any degree.
- Works for any points.

# Isogeny representation (TL;DR)

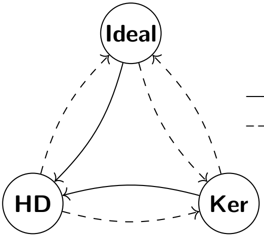
| | **Kernel** | **Ideal** | **HD** |
|---|---|---|---|
| **Isogeny** | smooth | any | any |
| **Evaluation** | any points | coprime to $d_1 d_2$ | any points |
| **Ad. info** | none | endomorphism ring | none |
| **Speed** | quick | resonably quick | slow |

Table: Comparison of different isogeny representation

# Isogeny representation (TL;DR)

| | **Kernel** | **Ideal** | **HD** |
|---|---|---|---|
| **Isogeny** | smooth | any | any |
| **Evaluation** | any points | coprime to $d_1 d_2$ | any points |
| **Ad. info** | none | endomorphism ring | none |
| **Speed** | quick | resonably quick | slow |

Table: Comparison of different isogeny representation




⟶ Immediate transformations

⇢ Technical transformations

## Table of Contents

# SQIPrime Intro

**SQIPrime**: A post-quantum *identification scheme* that relies on prime isogenies.

- A derivative of *SQISignHD*, itself a variant of *SQISign*.
- Expand its usage of Kani's Lemma.



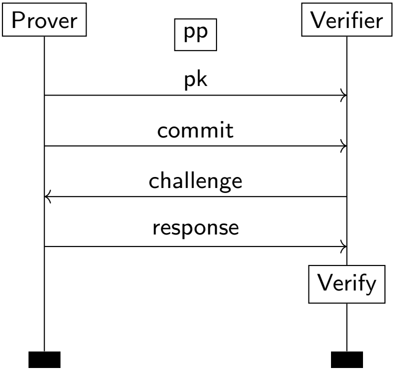

The *SQISign Family* relies on the following problems:

- Endomorphism problem: $E \rightarrow \mathcal{O}_E$ ✗
- Isogeny walk problem: $E, E' \rightarrow \phi$ ✗
- Linking ideal problem: $\mathcal{O}_E, \mathcal{O}_{E'} \rightarrow I$ ✓

# SQIPrime Intro

**SQIPrime**: A post-quantum *identification scheme* that relies on prime isogenies.

- A derivative of *SQISignHD*, itself a variant of *SQISign*.
- Expand its usage of Kani's Lemma.



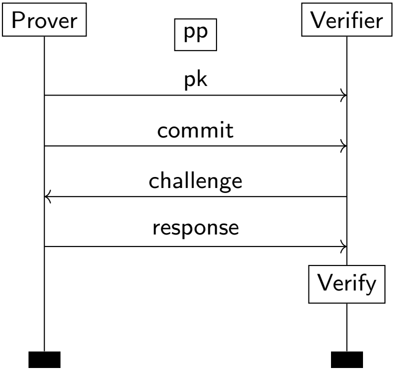

The *SQISign Family* relies on the following problems:

- Endomorphism problem: $E \to \mathcal{O}_E$ ✗
- Isogeny walk problem: $E, E' \to \phi$ ✗
- Linking ideal problem: $\mathcal{O}_E, \mathcal{O}_{E'} \to I$ ✓

# SQIPrime Intro

**SQIPrime**: A post-quantum *identification scheme* that relies on prime isogenies.

- A derivative of *SQISignHD*, itself a variant of *SQISign*.
- Expand its usage of Kani's Lemma.

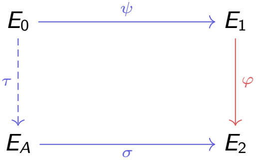



The *SQISign Family* relies on the following problems:

- Endomorphism problem: $E \to \mathcal{O}_E$ ✗
- Isogeny walk problem: $E, E' \to \phi$ ✗
- Linking ideal problem: $\mathcal{O}_E, \mathcal{O}_{E'} \to I$ ✓

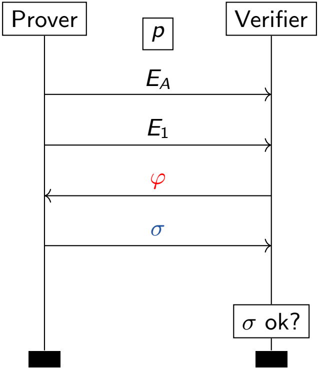
# SQISign & SQISignHD

## SQISign :

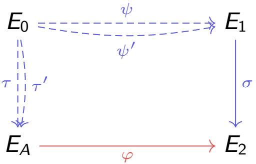



- $\sigma$ long ($\simeq p^4$) smooth.
- Given in kernel representation.
- $2^f T | (p^2 - 1)$ $T \geq p^{5/4}$.

\+ Compact. (177 B)
– Slow signature.
\+ Quick verification.
– Hard to scale.
– Ad-Hoc security assumptions.




## SQISignHD :

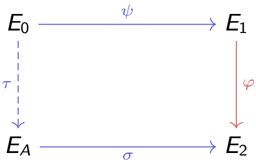



- $\sigma$ short ($\simeq \sqrt{p}$) prime.
- Given in HD representation.
- $p = 2^\lambda 3^{\lambda'} f - 1$.

\+ Very compact. (109 B)
\+ Quick signature.
– Long verification.
\+ Easy to scale.
\+ Simpler security assumptions.

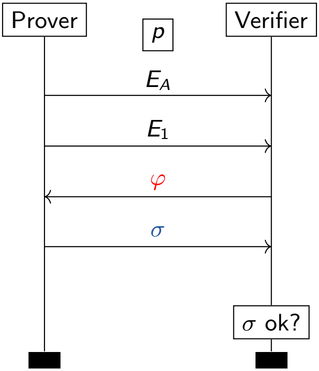
# SQISign & SQISignHD

## SQISign :

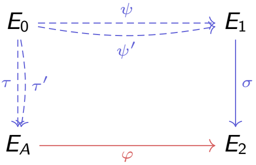



- $\sigma$ long ($\simeq p^4$) smooth.
- Given in kernel representation.
- $2^f T | (p^2 - 1)$ $T \geq p^{5/4}$.

\+ Compact. (177 B)
− Slow signature.
\+ Quick verification.
− Hard to scale.
− Ad-Hoc security assumptions.




## SQISignHD :

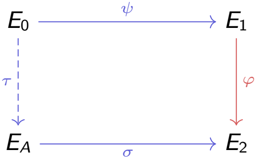



- $\sigma$ short ($\simeq \sqrt{p}$) prime.
- Given in HD representation.
- $p = 2^\lambda 3^{\lambda'} f - 1$.

\+ Very compact. (109 B)
\+ Quick signature.
− Long verification.
\+ Easy to scale.
\+ Simpler security assumptions.

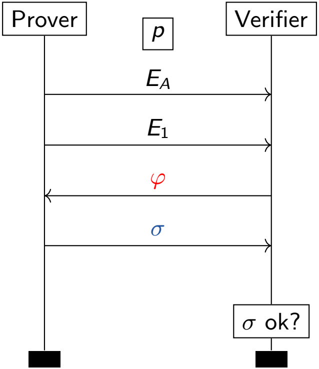
# SQISign & SQISignHD

SQISign :

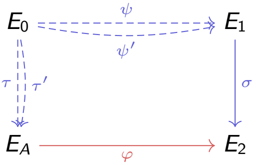



- $\sigma$ long ($\simeq p^4$) smooth.
- Given in kernel representation.
- $2^f T | (p^2 - 1)$ $T \geq p^{5/4}$.

\+ Compact. (177 B)
– Slow signature.
\+ Quick verification.
– Hard to scale.
– Ad-Hoc security assumptions.




SQISignHD :



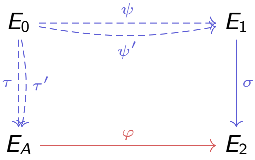

- $\sigma$ short ($\simeq \sqrt{p}$) prime.
- Given in HD representation.
- $p = 2^\lambda 3^{\lambda'} f - 1$.

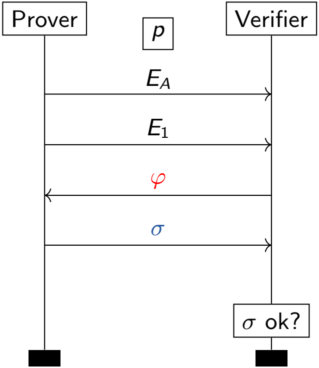
\+ Very compact. (109 B)
\+ Quick signature.
– Long verification.
\+ Easy to scale.
\+ Simpler security assumptions.

# SQIPrime (The changes compare to SQISignHD)

**Problems:**

1. How do we make $\tau$ and $\psi$ prime?
2. How do we make $\varphi$ prime?
3. How to verify $\sigma$?




**Solutions:**

1. Use Kani's Lemma in dim 2 to split $\gamma \in \mathrm{End}(E_0)$.
2. Sample $C_1 \in E_A[q]$.
3. Use $\kappa = \widehat{\sigma} \circ \varphi$ with Kani's Lemma in dim 4 and split in the middle.




- More complex in reality.

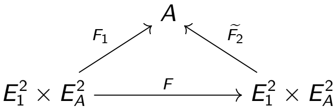
# SQIPrime (The changes compare to SQISignHD)

**Problems:**

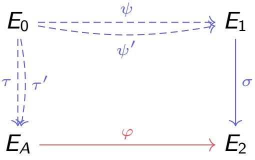
1. How do we make $\tau$ and $\psi$ prime?
2. How do we make $\varphi$ prime?
3. How to verify $\sigma$?

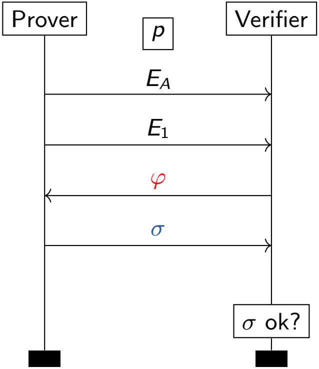
**Solutions:**

1. Use Kani's Lemma in dim 2 to split $\gamma \in \mathrm{End}(E_0)$.
2. Sample $C_1 \in E_A[q]$.
3. Use $\kappa = \widehat{\sigma} \circ \varphi$ with Kani's Lemma in dim 4 and split in the middle.




- More complex in reality.



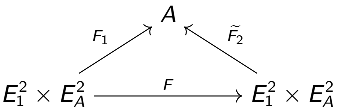
# SQIPrime (The changes compare to SQISignHD)

**Problems:**

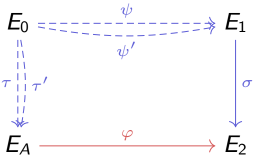
1. How do we make $\tau$ and $\psi$ prime?
2. How do we make $\varphi$ prime?
3. How to verify $\sigma$?

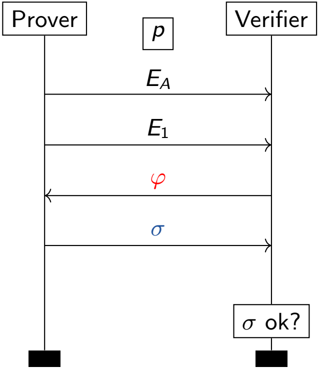
**Solutions:**

1. Use Kani's Lemma in dim 2 to split $\gamma \in \mathrm{End}(E_0)$.
2. Sample $C_1 \in E_A[q]$.
3. Use $\kappa = \widehat{\sigma} \circ \varphi$ with Kani's Lemma in dim 4 and split in the middle.




- More complex in reality.



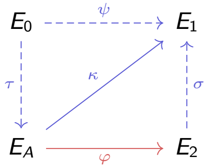



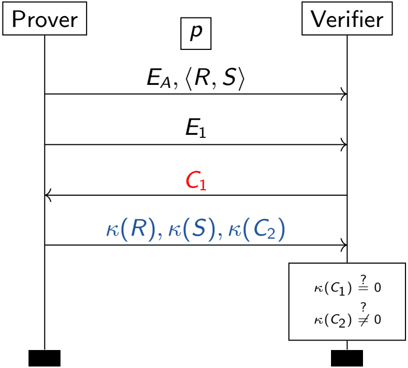
# SQIPrime (in its prime)

$p = 2^{2\lambda} f - 1$ s.t. $p+1 = 2Nq$, with $q \simeq 2^{\lambda}$.

- KeyGen:
  - pk : $E_A$ and special basis $\langle R, S \rangle$ of $E_A[q]$.
  - sk : $\tau : E_0 \to E_A$ and $I_\tau$.
- Commit:
  - com : $E_1$.
  - sec : $\psi : E_0 \to E_1$ and $I_\psi$.
- Challenge: $C_1 \in E_A[q]$ with $E_A[q] = \langle C_1, C_2 \rangle$.
- Response: Find $I_\sigma$ and evaluate $\kappa = \sigma \circ \varphi$ over $R, S, C_2$.
- Verify: Checks:
  - $\kappa$ valid isogeny.
  - $\ker(\kappa) \cap E[q] = \ker(\varphi)$

▶ Same security as SQISignHD.



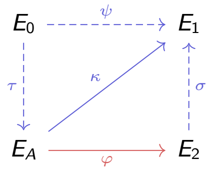



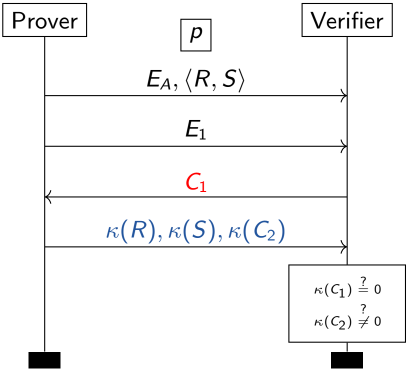
## SQIPrime (in its prime)

$p = 2^{2\lambda} f - 1$ s.t. $p + 1 = 2Nq$, with $q \simeq 2^{\lambda}$.

- KeyGen:
  - pk : $E_A$ and special basis $\langle R, S \rangle$ of $E_A[q]$.
  - sk : $\tau : E_0 \to E_A$ and $I_\tau$.
- Commit:
  - com : $E_1$.
  - sec : $\psi : E_0 \to E_1$ and $I_\psi$.
- Challenge: $C_1 \in E_A[q]$ with $E_A[q] = \langle C_1, C_2 \rangle$.
- Response: Find $I_\sigma$ and evaluate $\kappa = \sigma \circ \varphi$ over $R, S, C_2$.
- Verify: Checks:
  - $\kappa$ valid isogeny.
  - $\ker(\kappa) \cap E[q] = \ker(\varphi)$

▶ Same security as SQISignHD.



# Parameters

SQIPrime-friendly prime are easy to find:

$$p + 1 = 2^{2\cdot 120} \cdot 167 \cdot 397 \simeq 2^{256.01}$$
$$p - 1 = 2 \cdot 3 \cdot 7 \cdot 11 \cdot 41 \cdot 5683514583831199 \cdot 500402127095125861 \cdot q$$
$$q = 217442272953827514442892286379246833521 9 \simeq 2^{130.67}$$

| | SQISign | SQISignHD | SQIPrime |
|---|---|---|---|
| prime | $2^f T \mid (p^2 - 1)$ and $T = DT'$ | $p + 1 = 2^{\lambda} 3^{\lambda'} f$ | $p = 2^{2\lambda} f - 1$ and $p - 1 = 2Nq$ |
| Key gen | $2^{\bullet}$ isogenies | $2^{\lambda}$ isogenies | $(2, 2)$-isogenies |
| Commitment | $T'$ isogenies | $2^{\lambda}$ isogenies | $(2, 2)$-isogenies |
| Challenge | $D$ isogenies | $3^{\lambda'}$ isogenies | $C_1 \in E_A[q]$ |
| Response | Kernel representation | HD rep. | HD representation |
| Verification | $2^{\bullet}$ isogenies | $(2, 2, 2, 2)$-isogenies | $(2, 2, 2, 2)$-isogenies |

Table: Comparison of the SQISign Family

# Table of Contents

# SILBE intro

**SILBE**: A post-quantum *Updatable Public Key Encryption* (UPKE) scheme based on the generalised lollipop attacks over M-SIDH.

- **First** isogeny-based UPKE not based on group actions.
- Inspired by SETA adapted to the generalised lollipop.

## UPKE

An *UPKE* scheme is given 6 PPT($\lambda$) with Setup($1^\lambda$) $\rightarrow$ pp:

- $\mathrm{KG}(\mathrm{pp}) \xrightarrow{\$} (\mathrm{sk}, \mathrm{pk})$
- $\mathrm{Enc}(\mathrm{pk}, \mathrm{m}) \xrightarrow{\$} \mathrm{ct}$
- $\mathrm{Dec}(\mathrm{sk}, \mathrm{ct}) \longrightarrow \mathrm{m}$
- $\mathrm{UG}(\mathrm{pp}) \xrightarrow{\$} \mu$
- $\mathrm{Upk}(\mathrm{pk}, \mu) \longrightarrow \mathrm{pk}'$
- $\mathrm{Usk}(\mathrm{sk}, \mu) \longrightarrow \mathrm{sk}'$

Ensures:

- Correctness.
- Asynchronous key update.
- Forward Security.
- Post-Compromise Security.

# SILBE intro

**SILBE**: A post-quantum *Updatable Public Key Encryption* (UPKE) scheme based on the generalised lollipop attacks over M-SIDH.

- **First** isogeny-based UPKE not based on group actions.
- Inspired by SETA adapted to the generalised lollipop.

## UPKE

An *UPKE* scheme is given 6 PPT($\lambda$) with $\mathsf{Setup}(1^\lambda) \to \mathsf{pp}$:

- $\mathsf{KG}(\mathsf{pp}) \xrightarrow{\$} (\mathsf{sk}, \mathsf{pk})$
- $\mathsf{Enc}(\mathsf{pk}, \mathsf{m}) \xrightarrow{\$} \mathsf{ct}$
- $\mathsf{Dec}(\mathsf{sk}, \mathsf{ct}) \longrightarrow \mathsf{m}$
- $\mathsf{UG}(\mathsf{pp}) \xrightarrow{\$} \mu$
- $\mathsf{Upk}(\mathsf{pk}, \mu) \longrightarrow \mathsf{pk}'$
- $\mathsf{Usk}(\mathsf{sk}, \mu) \longrightarrow \mathsf{sk}'$

Ensures:

- Correctness.
- Asynchronous key update.
- Forward Security.
- Post-Compromise Security.

# SILBE intro

**SILBE**: A post-quantum *Updatable Public Key Encryption* (UPKE) scheme based on the generalised lollipop attacks over M-SIDH.

- **First** isogeny-based UPKE not based on group actions.
- Inspired by SETA adapted to the generalised lollipop.

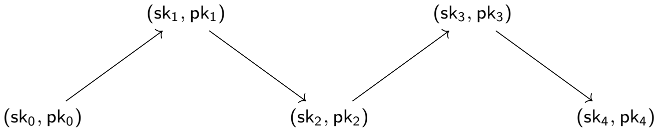
## UPKE

An *UPKE* scheme is given 6 PPT($\lambda$) with $\mathsf{Setup}(1^\lambda) \to \mathsf{pp}$:

- $\mathsf{KG}(\mathsf{pp}) \xrightarrow{\$} (\mathsf{sk}, \mathsf{pk})$
- $\mathsf{Enc}(\mathsf{pk}, \mathsf{m}) \xrightarrow{\$} \mathsf{ct}$
- $\mathsf{Dec}(\mathsf{sk}, \mathsf{ct}) \longrightarrow \mathsf{m}$
- $\mathsf{UG}(\mathsf{pp}) \xrightarrow{\$} \mu$
- $\mathsf{Upk}(\mathsf{pk}, \mu) \longrightarrow \mathsf{pk}'$
- $\mathsf{Usk}(\mathsf{sk}, \mu) \longrightarrow \mathsf{sk}'$

Ensures:

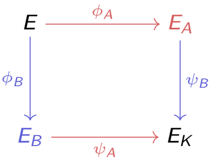
- Correctness.
- Asynchronous key update.
- Forward Security.
- Post-Compromise Security.



# M-SIDH

M-SIDH public parameters:

- $p = ABf - 1$ prime with $A = \prod_{i=1}^{n_A} p_i$ and $B = \prod_{j=1}^{n_B} q_j$.
- $\langle P_A, Q_A \rangle = E[A]$
- $\langle P_B, Q_B \rangle = E[B]$




$$\mu_2(N) = \{n \in \mathbb{Z}_N | n^2 = 1\}$$

## M-SIDH

| **Alice**(pp) | **black**(pp) |
|---|---|
| $s_A \leftarrow_\$ \mathbb{Z}_A, \alpha \leftarrow_\$ \mu_2(B)$ | $s_B \leftarrow_\$ \mathbb{Z}_B, \beta \leftarrow_\$ \mu_2(A)$ |
| $R_A \leftarrow P_A + [s_A]Q_A$ | $R_B \leftarrow P_B + [s_B]Q_B$ |
| $\phi_A, E_A \leftarrow$ **KernelToIso.**$(E, R_A)$ | $\phi_B, E_B \leftarrow$ **KernelToIso.**$(E, R_B)$ |
| $S_A \leftarrow [\alpha]\phi_A(P_B)$ | $S_B \leftarrow [\beta]\phi_B(P_A)$ |
| $T_A \leftarrow [\alpha]\phi_A(Q_B)$ | $T_B \leftarrow [\beta]\phi_B(Q_A)$ |

$$\xrightarrow{E_A,\, S_A,\, T_A}$$

$$\xleftarrow{E_B,\, S_B,\, T_B}$$

| | |
|---|---|
| $U_A \leftarrow S_B + [s_A]T_B$ | $U_B \leftarrow S_A + [s_B]T_A$ |
| $\psi_A, E_K \leftarrow$ **KernelToIso.**$(E_B, U_A)$ | $\psi_B, E_K \leftarrow$ **KernelToIso.**$(E_A, U_B)$ |
| $K \leftarrow \mathrm{KDF}(j(E_K))$ | $K \leftarrow \mathrm{KDF}(j(E_K))$ |

**Supersingular isogeny problem with MASKED torsion point information**

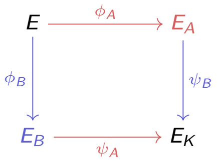
Let $\phi : E \to E'$ be an isogeny of degree $d$, $\langle P, Q \rangle = E[N]$ with $N$ coprime to $d$, $m \in \mu_2(N)$.

$$P, Q, [m]\phi(P), [m]\phi(Q) \xrightarrow{?} \phi$$

# M-SIDH

M-SIDH public parameters:

- $p = ABf - 1$ prime with $A = \prod_{i=1}^{n_A} p_i$ and $B = \prod_{j=1}^{n_B} q_j$.
- $\langle P_A, Q_A \rangle = E[A]$
- $\langle P_B, Q_B \rangle = E[B]$




$$\mu_2(N) = \{n \in \mathbb{Z}_N | n^2 = 1\}$$

## M-SIDH

| **Alice**(pp) | **black**(pp) |
|---|---|
| $s_A \leftarrow_\$ \mathbb{Z}_A, \alpha \leftarrow_\$ \mu_2(B)$ | $s_B \leftarrow_\$ \mathbb{Z}_B, \beta \leftarrow_\$ \mu_2(A)$ |
| $R_A \leftarrow P_A + [s_A]Q_A$ | $R_B \leftarrow P_B + [s_B]Q_B$ |
| $\phi_A, E_A \leftarrow$ **KernelToIso.**$(E, R_A)$ | $\phi_B, E_B \leftarrow$ **KernelToIso.**$(E, R_B)$ |
| $S_A \leftarrow [\alpha]\phi_A(P_B)$ | $S_B \leftarrow [\beta]\phi_B(P_A)$ |
| $T_A \leftarrow [\alpha]\phi_A(Q_B)$ | $T_B \leftarrow [\beta]\phi_B(Q_A)$ |

$$\xrightarrow{E_A, S_A, T_A}$$

$$\xleftarrow{E_B, S_B, T_B}$$

| | |
|---|---|
| $U_A \leftarrow S_B + [s_A]T_B$ | $U_B \leftarrow S_A + [s_B]T_A$ |
| $\psi_A, E_K \leftarrow$ **KernelToIso.**$(E_B, U_A)$ | $\psi_B, E_K \leftarrow$ **KernelToIso.**$(E_A, U_B)$ |
| $K \leftarrow \mathrm{KDF}(j(E_K))$ | $K \leftarrow \mathrm{KDF}(j(E_K))$ |

### Supersingular isogeny problem with MASKED torsion point information

Let $\phi : E \to E'$ be an isogeny of degree $d$, $\langle P, Q \rangle = E[N]$ with $N$ coprime to $d$, $m \in \mu_2(N)$.

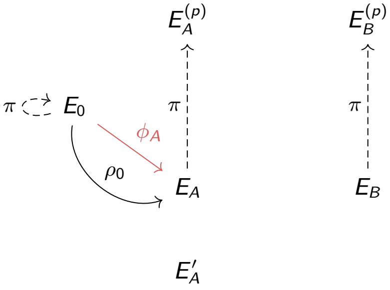
$$P, Q, [m]\phi(P), [m]\phi(Q) \xrightarrow{?} \phi$$

# SILBE (spelled out)

- KeyGen:
  - Alice computes $\rho_0 : E_0 \to E_A$ long.
  - Finds sk $:= \phi_A : E_0 \to E_A$ short prime, pk $= E_A$.
- Enc:
  - Bob computes $\phi : E_A \to E_B$, mask using m.
- Dec:
  - Alice computes generalized lollipop

$$\psi = \pi_*(\phi_B \circ \phi_A) \circ \phi_A \circ \phi_B$$

  - Use Kani's Lemma in dim 4.
- UG:
  - Sample random $\langle K \rangle = \ker(\rho_1)$.
- Upk:
  - Bob constructs $\rho_1 : E_A \to E'_A$.
- Usk:
  - Alice computes $\rho_1 : E_A \to E_A$.
  - Finds sk$' := \phi'_A : E_A \to E'_A$.
- FAR more complex in reality.




- Isogeny with masked torsion points problem over random curves hard $\implies$ SILBE OW-qCPA-U secure.

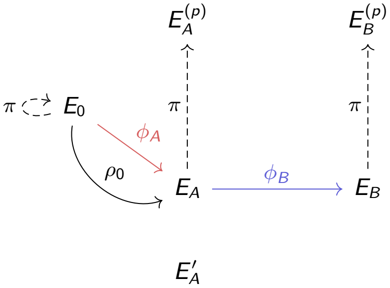
# SILBE (spelled out)

- KeyGen:
  - Alice computes $\rho_0 : E_0 \to E_A$ long.
  - Finds sk $:= \phi_A : E_0 \to E_A$ short prime, pk $= E_A$.
- Enc:
  - Bob computes $\phi : E_A \to E_B$, mask using m.
- Dec:
  - Alice computes generalized lollipop

$$\psi = \pi_*(\phi_B \circ \phi_A) \circ \phi_A \circ \phi_B$$

  - Use Kani's Lemma in dim 4.
- UG:
  - Sample random $\langle K \rangle = \ker(\rho_1)$.
- Upk:
  - Bob constructs $\rho_1 : E_A \to E'_A$.
- Usk:
  - Alice computes $\rho_1 : E_A \to E_A$.
  - Finds sk$' := \phi'_A : E_A \to E'_A$.

▶ FAR more complex in reality.




▶ Isogeny with masked torsion points problem over random curves hard $\implies$ SILBE OW-qCPA-U secure.

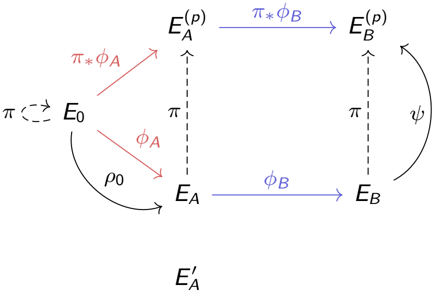
# SILBE (spelled out)

- KeyGen:
  - Alice computes $\rho_0 : E_0 \to E_A$ long.
  - Finds sk $:= \phi_A : E_0 \to E_A$ short prime, pk $= E_A$.
- Enc:
  - Bob computes $\phi : E_A \to E_B$, mask using m.
- Dec:
  - Alice computes generalized lollipop

$$\psi = \pi_*(\phi_B \circ \phi_A) \circ \phi_A \circ \phi_B$$

  - Use Kani's Lemma in dim 4.
- UG:
  - Sample random $\langle K \rangle = \ker(\rho_1)$.
- Upk:
  - Bob constructs $\rho_1 : E_A \to E'_A$.
- Usk:
  - Alice computes $\rho_1 : E_A \to E_A$.
  - Finds sk$' := \phi'_A : E_A \to E'_A$.

▶ FAR more complex in reality.




▶ Isogeny with masked torsion points problem over random curves hard $\implies$ SILBE OW-qCPA-U secure.

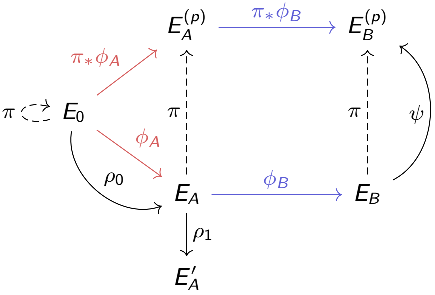
# SILBE (spelled out)

- KeyGen:
  - Alice computes $\rho_0 : E_0 \to E_A$ long.
  - Finds sk $:= \phi_A : E_0 \to E_A$ short prime, pk $= E_A$.
- Enc:
  - Bob computes $\phi : E_A \to E_B$, mask using m.
- Dec:
  - Alice computes generalized lollipop

$$\psi = \pi_*(\phi_B \circ \phi_A) \circ \phi_A \circ \phi_B$$

  - Use Kani's Lemma in dim 4.
- UG:
  - Sample random $\langle K \rangle = \ker(\rho_1)$.
- Upk:
  - Bob constructs $\rho_1 : E_A \to E'_A$.
- Usk:
  - Alice computes $\rho_1 : E_A \to E_A$.
  - Finds sk$' := \phi'_A : E_A \to E'_A$.

▶ FAR more complex in reality.




▶ Isogeny with masked torsion points problem over random curves hard $\implies$ SILBE OW-qCPA-U secure.

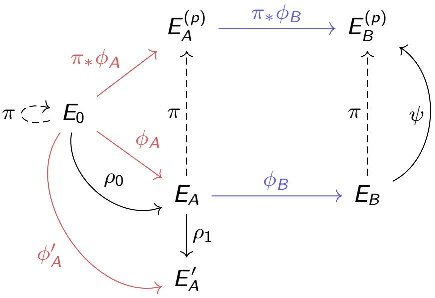
# SILBE (spelled out)

- KeyGen:
  - Alice computes $\rho_0 : E_0 \to E_A$ long.
  - Finds sk $:= \phi_A : E_0 \to E_A$ short prime, pk $= E_A$.
- Enc:
  - Bob computes $\phi : E_A \to E_B$, mask using m.
- Dec:
  - Alice computes generalized lollipop

$$\psi = \pi_*(\phi_B \circ \phi_A) \circ \phi_A \circ \phi_B$$

  - Use Kani's Lemma in dim 4.
- UG:
  - Sample random $\langle K \rangle = \ker(\rho_1)$.
- Upk:
  - Bob constructs $\rho_1 : E_A \to E_A'$.
- Usk:
  - Alice computes $\rho_1 : E_A \to E_A$.
  - Finds sk$' := \phi_A' : E_A \to E_A'$.

▶ FAR more complex in reality.



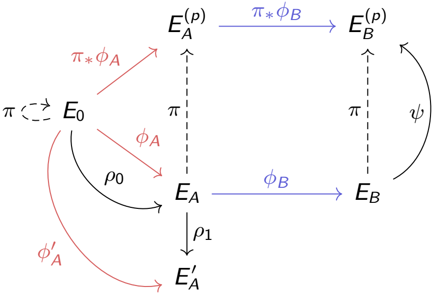

▶ Isogeny with masked torsion points problem over random curves hard $\implies$ SILBE OW-qCPA-U secure.

# SILBE (spelled out)

- KeyGen:
  - Alice computes $\rho_0 : E_0 \to E_A$ long.
  - Finds sk $:= \phi_A : E_0 \to E_A$ short prime, pk $= E_A$.
- Enc:
  - Bob computes $\phi : E_A \to E_B$, mask using m.
- Dec:
  - Alice computes generalized lollipop

$$\psi = \pi_*(\phi_B \circ \phi_A) \circ \phi_A \circ \phi_B$$

  - Use Kani's Lemma in dim 4.
- UG:
  - Sample random $\langle K \rangle = \ker(\rho_1)$.
- Upk:
  - Bob constructs $\rho_1 : E_A \to E'_A$.
- Usk:
  - Alice computes $\rho_1 : E_A \to E_A$.
  - Finds sk$' := \phi'_A : E_A \to E'_A$.
- FAR more complex in reality.




- Isogeny with masked torsion points problem over random curves hard $\implies$ SILBE OW-qCPA-U secure.

# Parameters

$p = 3^\beta Nf + 1$ with $N = \prod_{i=1}^n p_i$ such that:

- $N \geq 3^\beta \sqrt{p} \log(p)$.
- $N_t = \prod_{i=t}^n p_i \geq 3^{\beta/2} \implies n - t \geq \lambda$.

| $\lambda$ | $\beta$ | $N$ | $f$ | $n$ | $\log_2(p)$ |
|---|---|---|---|---|---|
| 128 | 2043 | $5 \times 7 \times 11 \times \cdots \times 6863$ | 1298 | 881 | 13013 |
| 192 | 3229 | $5 \times 7 \times 11 \times \cdots \times 10789$ | 1790 | 1312 | 20538 |
| 256 | 4461 | $5 \times 7 \times 11 \times \cdots \times 14879$ | 16706 | 1741 | 28346 |

Table: Parameters for SILBE

Kani's Lemma over such prime is not practical.

- Decryption requires $7^5 \lambda^5 \log(\lambda)^4$ operations.
  - $\lambda = 128 \implies 2^{60}$ operations.

# Parameters

$p = 3^\beta N f + 1$ with $N = \prod_{i=1}^{n} p_i$ such that:

- $N \geq 3^\beta \sqrt{p} \log(p)$.
- $N_t = \prod_{i=t}^{n} p_i \geq 3^{\beta/2} \implies n - t \geq \lambda$.

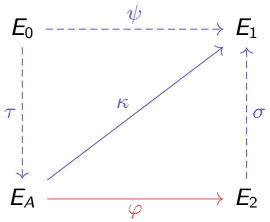
| $\lambda$ | $\beta$ | $N$ | $f$ | $n$ | $\log_2(p)$ |
|---|---|---|---|---|---|
| 128 | 2043 | $5 \times 7 \times 11 \times \cdots \times 6863$ | 1298 | 881 | 13013 |
| 192 | 3229 | $5 \times 7 \times 11 \times \cdots \times 10789$ | 1790 | 1312 | 20538 |
| 256 | 4461 | $5 \times 7 \times 11 \times \cdots \times 14879$ | 16706 | 1741 | 28346 |

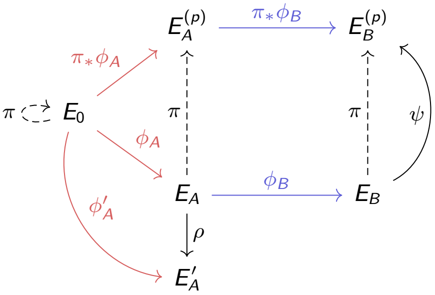
Table: Parameters for SILBE

Kani's Lemma over such prime is not practical.

- Decryption requires $7^5 \lambda^5 \log(\lambda)^4$ operations.
  - $\lambda = 128 \implies 2^{60}$ operations.

# Future directions




**SQIPrime**:

- Work on an implementation.
- Further consideration on distribution over multiple $\mathcal{G}_p^\ell$.

**SILBE**:

- See if its principles are usable over FESTA.

**Happy to discuss your comments and questions !!!**

- e-prints coming soon.

# Table of Contents

## Endomorphism ring in cryptography

1. There are **handfull of** curves such that we know the correspondence for all $p$.
   - If $p = 3 \mod 4$, $j(E_0) = 1728$ is supersingular and

$$\mathcal{O}_0 = \mathbb{Z} + \mathbf{i}\mathbb{Z} + \frac{\mathbf{i}+\mathbf{j}}{2}\mathbb{Z} + \frac{1+\mathbf{ij}}{2}\mathbb{Z}$$

   with $\mathbf{i} : (x, y) \to (-x, \sqrt{-1}y)$ and $\mathbf{j} = \pi$.

2. Knowing $\mathrm{End}(E) \cong \mathcal{O}_E = \langle \alpha_1, \cdots, \alpha_4 \rangle$ with an efficient representation of all $\alpha_i$.
   - We can evaluate ANY $\gamma \in \mathrm{End}(E)$.
3. For any isogeny $\rho : E \to E'$, knowing $\mathcal{O}_E \implies$ knowing $\mathcal{O}_{E'}$.
4. For any *smooth* isogeny $\rho : E \to E'$, knowing $\mathcal{O}_E \implies$ computing $I_\rho$ is easy.

# Endomorphism ring in cryptography

1. There are **handfull of** curves such that we know the correspondence for all $p$.
   - If $p = 3 \mod 4$, $j(E_0) = 1728$ is supersingular and

     $$\mathcal{O}_0 = \mathbb{Z} + \mathbf{i}\mathbb{Z} + \frac{\mathbf{i}+\mathbf{j}}{2}\mathbb{Z} + \frac{1+\mathbf{ij}}{2}\mathbb{Z}$$

     with $\mathbf{i} : (x, y) \to (-x, \sqrt{-1}y)$ and $\mathbf{j} = \pi$.
2. Knowing $\text{End}(E) \cong \mathcal{O}_E = \langle \alpha_1, \cdots, \alpha_4 \rangle$ with an efficient representation of all $\alpha_i$.
   - We can evaluate ANY $\gamma \in \text{End}(E)$.
3. For any isogeny $\rho : E \to E'$, knowing $\mathcal{O}_E \implies$ knowing $\mathcal{O}_{E'}$.
4. For any *smooth* isogeny $\rho : E \to E'$, knowing $\mathcal{O}_E \implies$ computing $I_\rho$ is easy.

# Endomorphism ring in cryptography

1. There are **handfull of** curves such that we know the correspondence for all $p$.
   - If $p = 3 \mod 4$, $j(E_0) = 1728$ is supersingular and
     $$\mathcal{O}_0 = \mathbb{Z} + \mathbf{i}\mathbb{Z} + \frac{\mathbf{i}+\mathbf{j}}{2}\mathbb{Z} + \frac{1+\mathbf{ij}}{2}\mathbb{Z}$$
     with $\mathbf{i} : (x, y) \to (-x, \sqrt{-1}y)$ and $\mathbf{j} = \pi$.
2. Knowing $\text{End}(E) \cong \mathcal{O}_E = \langle \alpha_1, \cdots, \alpha_4 \rangle$ with an efficient representation of all $\alpha_i$.
   - We can evaluate ANY $\gamma \in \text{End}(E)$.
3. For any isogeny $\rho : E \to E'$, knowing $\mathcal{O}_E \implies$ knowing $\mathcal{O}_{E'}$.
4. For any *smooth* isogeny $\rho : E \to E'$, knowing $\mathcal{O}_E \implies$ computing $I_\rho$ is easy.

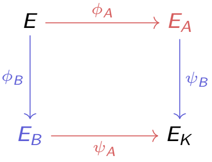
# Endomorphism ring in cryptography

1. There are **handfull of** curves such that we know the correspondence for all $p$.
   - If $p = 3 \mod 4$, $j(E_0) = 1728$ is supersingular and
   $$\mathcal{O}_0 = \mathbb{Z} + \mathbf{i}\mathbb{Z} + \frac{\mathbf{i}+\mathbf{j}}{2}\mathbb{Z} + \frac{1+\mathbf{ij}}{2}\mathbb{Z}$$
   with $\mathbf{i} : (x, y) \to (-x, \sqrt{-1}y)$ and $\mathbf{j} = \pi$.
2. Knowing $\text{End}(E) \cong \mathcal{O}_E = \langle \alpha_1, \cdots, \alpha_4 \rangle$ with an efficient representation of all $\alpha_i$.
   - We can evaluate ANY $\gamma \in \text{End}(E)$.
3. For any isogeny $\rho : E \to E'$, knowing $\mathcal{O}_E \implies$ knowing $\mathcal{O}_{E'}$.
4. For any *smooth* isogeny $\rho : E \to E'$, knowing $\mathcal{O}_E \implies$ computing $I_\rho$ is easy.

# SIDH

SIDH public parameters:

- $p = \ell_A^{e_A} \ell_B^{e_B} f - 1$ a prime.
- $\langle P_A, Q_A \rangle = E[\ell_A^{e_A}]$
- $\langle P_B, Q_B \rangle = E[\ell_B^{e_B}]$.




**SIDH**

| **Alice**(pp) | **Bob**(pp) |
|---|---|
| $s_A \leftarrow_\$ \mathbb{Z}_{\ell_A^{e_A}}$ | $s_B \leftarrow_\$ \mathbb{Z}_{\ell_B^{e_B}}$ |
| $R_A \leftarrow P_A + [s_A]Q_A$ | $R_B \leftarrow P_B + [s_B]Q_B$ |
| $\phi_A, E_A \leftarrow$ **KernelToIso.**$(E, R_A)$ | $\phi_B, E_B \leftarrow$ **KernelToIso.**$(E, R_B)$ |
| $S_A \leftarrow \phi_A(P_B),\ T_A \leftarrow \phi_A(Q_B)$ | $S_B \leftarrow \phi_B(P_A),\ T_B \leftarrow \phi_B(Q_A)$ |

$$\xrightarrow{E_A, S_A, T_A}$$

$$\xleftarrow{E_B, S_B, T_B}$$

| | |
|---|---|
| $U_A \leftarrow S_B + [s_A]T_B$ | $U_B \leftarrow S_A + [s_B]T_A$ |
| $\psi_A, E_K \leftarrow$ **KernelToIso.**$(E_B, U_A)$ | $\psi_B, E_K \leftarrow$ **KernelToIso.**$(E, U_B)$ |
| $K \leftarrow \mathrm{KDF}(j(E_K))$ | $K \leftarrow \mathrm{KDF}(j(E_K))$ |

**Supersingular isogeny problem with torsion point information**

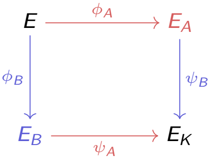
Let $\phi : E \to E'$ be an isogeny of degree $d$, $\langle P, Q \rangle = E[N]$ with $N$ coprime to $d$.

$$P, Q, \phi(P), \phi(Q) \xrightarrow{?} \phi$$

# SIDH

SIDH public parameters:

- $p = \ell_A^{e_A} \ell_B^{e_B} f - 1$ a prime.
- $\langle P_A, Q_A \rangle = E[\ell_A^{e_A}]$
- $\langle P_B, Q_B \rangle = E[\ell_B^{e_B}]$.




## SIDH

| **Alice**(pp) | **Bob**(pp) |
| --- | --- |
| $s_A \leftarrow_\$ \mathbb{Z}_{\ell_A^{e_A}}$ | $s_B \leftarrow_\$ \mathbb{Z}_{\ell_B^{e_B}}$ |
| $R_A \leftarrow P_A + [s_A]Q_A$ | $R_B \leftarrow P_B + [s_B]Q_B$ |
| $\phi_A, E_A \leftarrow$ **KernelToIso.**$(E, R_A)$ | $\phi_B, E_B \leftarrow$ **KernelToIso.**$(E, R_B)$ |
| $S_A \leftarrow \phi_A(P_B)$, $T_A \leftarrow \phi_A(Q_B)$ | $S_B \leftarrow \phi_B(P_A)$, $T_B \leftarrow \phi_B(Q_A)$ |

$$\xrightarrow{E_A, S_A, T_A}$$

$$\xleftarrow{E_B, S_B, T_B}$$

| | |
| --- | --- |
| $U_A \leftarrow S_B + [s_A]T_B$ | $U_B \leftarrow S_A + [s_B]T_A$ |
| $\psi_A, E_K \leftarrow$ **KernelToIso.**$(E_B, U_A)$ | $\psi_B, E_K \leftarrow$ **KernelToIso.**$(E, U_B)$ |
| $K \leftarrow \mathrm{KDF}(j(E_K))$ | $K \leftarrow \mathrm{KDF}(j(E_K))$ |

### Supersingular isogeny problem with torsion point information

Let $\phi : E \to E'$ be an isogeny of degree $d$, $\langle P, Q \rangle = E[N]$ with $N$ coprime to $d$.

$$P, Q, \phi(P), \phi(Q) \xrightarrow{?} \phi$$

# A prime new Commitment and KeyGen

Three main ideas:

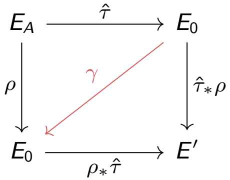
1. Use Kani's Lemma to split isogenies.

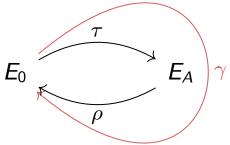
$$F : E_0^2 \to E \times E'$$

$$\ker(F) = \left\{ ([\ell](P), \gamma(P)) \middle| P \in E_0[N] \right\}$$

   $\deg(\tau)$ and $\deg(\rho)$ coprime.

2. Finding $\gamma \in \mathrm{End}(E_0)$ with $\deg(\gamma) = N$ is easy if $N > p$.
3. Finding $I_\tau$ from $\gamma$ is easy.




**Commit & KeyGen**:

- Sample $\ell \simeq \sqrt{p}$ prime and find $\gamma$, $\deg(\gamma) = \ell(2^{2\lambda} - \ell)$ with $2^{2\lambda} \simeq p$.
- Get $F$ and $I_\tau$.
- Compute a *special basis* over $E_A$ in **KeyGen**.

▶ $E_A$ distribution is computationally indistinguishable from uniform.

# A prime new Commitment and KeyGen

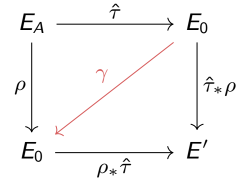
Three main ideas:

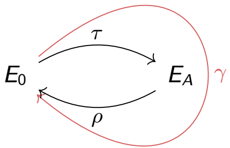
1. Use Kani's Lemma to split isogenies.

$$F : E_0^2 \to E \times E'$$

$$\ker(F) = \left\{ ([\ell](P), \gamma(P)) \middle| \, P \in E_0[N] \right\}$$

   $\deg(\tau)$ and $\deg(\rho)$ coprime.
2. Finding $\gamma \in \mathrm{End}(E_0)$ with $\deg(\gamma) = N$ is easy if $N > p$.
3. Finding $I_\tau$ from $\gamma$ is easy.




**Commit & KeyGen**:

- Sample $\ell \simeq \sqrt{p}$ prime and find $\gamma$, $\deg(\gamma) = \ell(2^{2\lambda} - \ell)$ with $2^{2\lambda} \simeq p$.
- Get $F$ and $I_\tau$.
- Compute a *special basis* over $E_A$ in **KeyGen**.

▶ $E_A$ distribution is computationally indistinguishable from uniform.

# A prime new Commitment and KeyGen

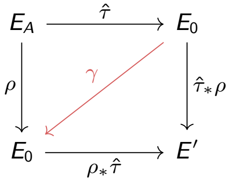
Three main ideas:

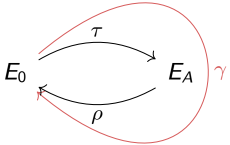
1. Use Kani's Lemma to split isogenies.

$$F : E_0^2 \to E \times E'$$

$$\ker(F) = \left\{ ([\ell](P), \gamma(P)) \middle| \; P \in E_0[N] \right\}$$

   $\deg(\tau)$ and $\deg(\rho)$ coprime.
2. Finding $\gamma \in \text{End}(E_0)$ with $\deg(\gamma) = N$ is easy if $N > p$.
3. Finding $I_\tau$ from $\gamma$ is easy.




**Commit & KeyGen**:

- Sample $\ell \simeq \sqrt{p}$ prime and find $\gamma$, $\deg(\gamma) = \ell(2^{2\lambda} - \ell)$ with $2^{2\lambda} \simeq p$.
- Get $F$ and $I_\tau$.
- Compute a *special basis* over $E_A$ in **KeyGen**.

- $E_A$ distribution is computationally indistinguishable from uniform.

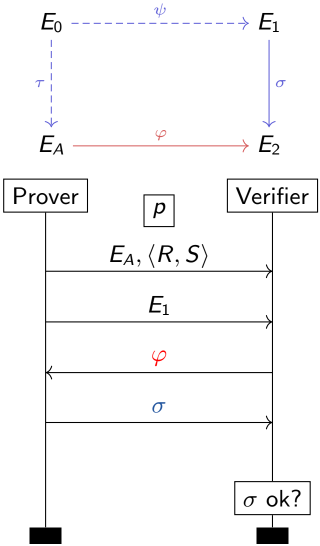
# SQIPrime [2]

$p = 2^{2\lambda} f - 1$

- KeyGen:
  - pk : $E_A$ and special basis $\langle R, S \rangle$.
  - sk : $\tau : E_0 \to E_A$ and $I_\tau$.
- Commit:
  - com : $E_1$.
  - sec : $\psi : E_0 \to E_1$ and $I_\psi$.

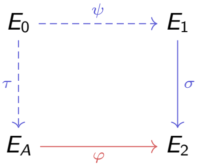
**How do we make $\varphi$ prime ?**

**How to verify ?**



# The real challenge

Let $\langle C_1 \rangle = \ker(\varphi)$ with $\deg(\varphi) = q \simeq 2^\lambda$




**Problems:**

1. How does the Prover compute $I_\varphi$?
2. How does the Prover evaluate $\sigma$?
3. How does the Verifier know $E_2$?

**Solutions:**

1. Use *special basis*.

$$\ker(\varphi) = \langle [a]P + [b]Q \rangle \implies I_\varphi = [a + b\iota]_* I_P$$

$\iota(P) = Q$.

2. Evaluate $\kappa = \sigma \circ \varphi$ instead.
3. Check $\ker(\kappa) \cap E_A[q] = \ker(\varphi)$.

# The real challenge

Let $\langle C_1 \rangle = \ker(\varphi)$ with $\deg(\varphi) = q \simeq 2^\lambda$




**Problems:**

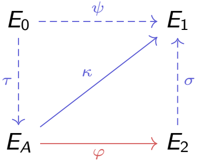
1. How does the Prover compute $I_\varphi$?
2. How does the Prover evaluate $\sigma$?
3. How does the Verifier know $E_2$?

**Solutions:**

1. Use *special basis*.

   $$\ker(\varphi) = \langle [a]P + [b]Q \rangle \implies I_\varphi = [a + b\iota]_* I_P$$

   $\iota(P) = Q$.
2. Evaluate $\kappa = \sigma \circ \varphi$ instead.
3. Check $\ker(\kappa) \cap E_A[q] = \ker(\varphi)$.

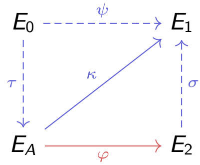


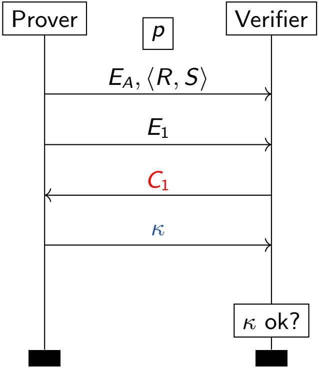
# SQIPrime [3]

$p = 2^{2\lambda} f - 1$ s.t. $p + 1 = 2Nq$, with $q \simeq 2^{\lambda}$ prime.

- KeyGen:
  - pk : $E_A$ and special basis $\langle R, S \rangle$ of $E_A[q]$.
  - sk : $\tau : E_0 \to E_A$ and $I_\tau$.
- Commit:
  - com : $E_1$.
  - sec : $\psi : E_0 \to E_1$ and $I_\psi$.
- Challenge: $C_1 \in E_A[q]$ with $\ker(\varphi) = \langle C_1 \rangle$.
- Response: Find $I_\sigma$ and send $\kappa = \sigma \circ \varphi$ in HD representation.

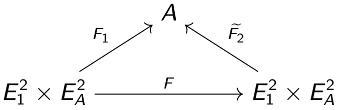
**How to verify ?**



# Efficient verification

- Like SQISignHD, we use Kani's Lemma in dimension 4.
- $\kappa$ too long $\deg(\kappa) \simeq p \log(p) > 2^{2\lambda}$.
  - Have to split $F = F_2 \circ F_1$ and evaluate at the middle with $\deg(F_i) = d_i$.

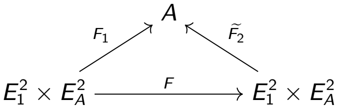



$$F \begin{pmatrix} 0 \\ 0 \\ X \\ 0 \end{pmatrix} = \begin{pmatrix} [a_1]X \\ [-a_2]X \\ Y \\ 0 \end{pmatrix} \iff [d_2]F_1 \begin{pmatrix} 0 \\ 0 \\ X \\ 0 \end{pmatrix} = \widetilde{F}_2 \begin{pmatrix} [a_1]X \\ [-a_2]X \\ Y \\ 0 \end{pmatrix}$$

  - Requires sending a 3rd point $C_2$.

# Efficient verification

- Like SQISignHD, we use Kani's Lemma in dimension 4.
- $\kappa$ too long $\deg(\kappa) \simeq p \log(p) > 2^{2\lambda}$.
- Have to split $F = F_2 \circ F_1$ and evaluate at the middle with $\deg(F_i) = d_i$.




$$F \begin{pmatrix} 0 \\ 0 \\ X \\ 0 \end{pmatrix} = \begin{pmatrix} [a_1]X \\ [-a_2]X \\ Y \\ 0 \end{pmatrix} \iff [d_2]F_1 \begin{pmatrix} 0 \\ 0 \\ X \\ 0 \end{pmatrix} = \widetilde{F_2} \begin{pmatrix} [a_1]X \\ [-a_2]X \\ Y \\ 0 \end{pmatrix}$$

- Requires sending a 3rd point $C_2$.

# OW-PCA-U Game

$\mathcal{G}^{\text{OW-PCA-U}}(\mathcal{A}_1, \mathcal{A}_2)$

$i = 0$
$\text{Upd\_list} = \text{Cor\_list} = \emptyset$
$\text{sk}_0, \text{pk}_0 \xleftarrow{\$} \text{KG}(\text{pp})$
$\text{j}, \text{st} \longleftarrow \mathcal{A}_1^{\text{Oracles}}(\text{pk}_0)$
**if** $j > i$ **do return** $\perp$
$\text{m} \xleftarrow{\$} \mathcal{M}$
$\text{ct} \xleftarrow{\$} \text{Enc}(\text{pk}_\text{j}, \text{m})$
$\text{n} \longleftarrow \mathcal{A}_2^{\text{Oracles}}(\text{ct}, \text{st})$
**if** $\text{IsFresh}(j)$ **do**
    **return** $m \stackrel{?}{=} n$
**return** $\perp$

$\text{IsFresh}(j)$

**return not** $j \stackrel{?}{\in} \text{Cor\_list}$

$\text{Fresh\_Upd}() \to \text{pk}_\text{i}$

$\mu \xleftarrow{\$} \text{UG}(1^\lambda)$
$\text{sk}_{\text{i}+1} \xleftarrow{\$} \text{Usk}(\text{sk}_\text{i}, \mu)$
$\text{pk}_{\text{i}+1} \xleftarrow{\$} \text{Upk}(\text{pk}_\text{i}, \mu)$
$i \leftarrow i + 1$
**return** $\text{pk}_\text{i}$

$\text{Given\_Upd}(\mu) \to \text{pk}_\text{i}$

$\text{sk}_{\text{i}+1} \xleftarrow{\$} \text{Usk}(\text{sk}_\text{i}, \mu)$
$\text{pk}_{\text{i}+1} \xleftarrow{\$} \text{Upk}(\text{pk}_\text{i}, \mu)$
$\text{Upd\_list} += \{(i, i+1)\}$
$i \leftarrow i + 1$
**return** $\text{pk}_\text{i}$

$\text{Corrupt}(j) \to \text{sk}_\text{j}$

$\text{Cor\_list} = \text{Cor\_list} \cup \{j\}$
$i, k \leftarrow j$
**while** $(i-1, i) \in \text{Upd\_list}$ :
    $\text{Cor\_list} += \{i - 1\}$
    $i \leftarrow i - 1$
**while** $(k, k+1) \in \text{Upd\_list}$ :
    $\text{Cor\_list} += \{k + 1\}$
    $k \leftarrow k + 1$
**return** $\text{sk}_\text{j}$

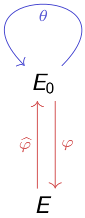
$\text{Plaintext\_Check}(\text{m}, \text{c}, \text{j}) \to b$

**if** $\text{m} \notin \mathcal{M}$ **or** $j > i$ **do**
    **return** $\perp$
**else do**
    **return** $\text{m} \stackrel{?}{=} \text{Dec}(\text{sk}_\text{j}, \text{c})$

# Lollipops attacks

[Pet17]: Petit's original lollipop attack:

- Given $\varphi(E_0[N])$ of degree $d$.
- Find $\theta \in \mathrm{End}(E_0)$ s.t. $\deg(\tau) = N$, $\tau = \varphi \circ \theta \circ \widehat{\varphi} + [n]$
- $\ker(\tau)$ is known as $\tau|_{E[N]} = [d]\theta|_{E_0[N]} + [n]\mathbf{Id}$.
- $\ker(\widehat{\varphi}) \simeq \ker(\tau - [n]) \cap E[d]$.

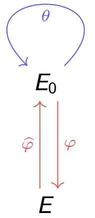



Many development on lollipops:

- [dQKL+20]: Improved lollipop
- [FP21]: Adaptive attack over SIDH
- [CV23]: Generalised lollipop:
  - Works on M-SIDH.
  - Requires $E_0$ defined over $\mathbb{F}_p$.

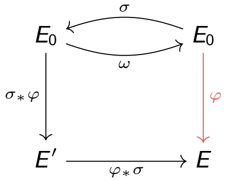
[Pet17]: Petit's original lollipop attack:

- Given $\varphi(E_0[N])$ of degree $d$.
- Find $\theta \in \text{End}(E_0)$ s.t. $\deg(\tau) = N$, $\tau = \varphi \circ \theta \circ \widehat{\varphi} + [n]$
- $\ker(\tau)$ is known as $\tau|_{E[N]} = [d]\theta|_{E_0[N]} + [n]\mathbf{Id}$.
- $\ker(\widehat{\varphi}) \simeq \ker(\tau - [n]) \cap E[d]$.




Many development on lollipops:

- [dQKL+20]: Improved lollipop
- [FP21]: Adaptive attack over SIDH
- [CV23]: Generalised lollipop:
  - Works on M-SIDH.
  - Requires $E_0$ defined over $\mathbb{F}_p$.



# Security

## Low walk distribution

Let $\phi : E \to E'$ be an $\ell^h$-isogeny obtained from a non-backtracking random walk over $\mathcal{G}_p^\ell$. Then, for all $\varepsilon \in ]0, 2]$,

$$\text{dist}\left\{ E' \text{ codomain of } \phi \,\middle|\, E' \text{ uniform in } \mathcal{G}_p^\ell \right\} = O(p^{-\varepsilon/2})$$

provided that $h \geq (1+\varepsilon)\log_\ell(p)$.

## Security SILBE as a PKE

The security of SILBE as an OW-PCA PKE reduces to the *supersingular isogeny problem with masked torsion point information* over random curves.

## Security SILBE as an UPKE

$$\text{SILBE is OW-PCA secure} \iff \text{SILBE is OW-PCA-U secure}$$

- Using [AW23], we can make of SILBE an IND-CU-CCA UPKE in the ROM.

# Security

**Low walk distribution**

Let $\phi : E \to E'$ be an $\ell^h$-isogeny obtained from a non-backtracking random walk over $\mathcal{G}_p^\ell$. Then, for all $\varepsilon \in ]0, 2]$,

$$\text{dist}\left\{E' \text{ codomain of } \phi \middle| E' \text{ uniform in } \mathcal{G}_p^\ell\right\} = O(p^{-\varepsilon/2})$$

provided that $h \geq (1 + \varepsilon)\log_\ell(p)$.

**Security SILBE as a PKE**

The security of SILBE as an OW-PCA PKE reduces to the *supersingular isogeny problem with masked torsion point information* over random curves.

**Security SILBE as an UPKE**

SILBE is OW-PCA secure $\iff$ SILBE is OW-PCA-U secure

- Using [AW23], we can make of SILBE an IND-CU-CCA UPKE in the ROM.

# Security

## Low walk distribution

Let $\phi : E \to E'$ be an $\ell^h$-isogeny obtained from a non-backtracking random walk over $\mathcal{G}_p^\ell$. Then, for all $\varepsilon \in ]0, 2]$,

$$\text{dist}\left\{ E' \text{ codomain of } \phi \,\middle|\, E' \text{ uniform in } \mathcal{G}_p^\ell \right\} = O(p^{-\varepsilon/2})$$

provided that $h \geq (1+\varepsilon)\log_\ell(p)$.

## Security SILBE as a PKE

The security of SILBE as an OW-PCA PKE reduces to the *supersingular isogeny problem with masked torsion point information* over random curves.

## Security SILBE as an UPKE

SILBE is OW-PCA secure $\iff$ SILBE is OW-PCA-U secure

- Using [AW23], we can make of SILBE an IND-CU-CCA UPKE in the ROM.

## Security

### Low walk distribution

Let $\phi : E \to E'$ be an $\ell^h$-isogeny obtained from a non-backtracking random walk over $\mathcal{G}_p^\ell$. Then, for all $\varepsilon \in ]0, 2]$,

$$\text{dist}\left\{E' \text{ codomain of } \phi \,\middle|\, E' \text{ uniform in } \mathcal{G}_p^\ell\right\} = O(p^{-\varepsilon/2})$$

provided that $h \geq (1 + \varepsilon)\log_\ell(p)$.

### Security SILBE as a PKE

The security of SILBE as an OW-PCA PKE reduces to the *supersingular isogeny problem with masked torsion point information* over random curves.

### Security SILBE as an UPKE

$$\text{SILBE is OW-PCA secure} \iff \text{SILBE is OW-PCA-U secure}$$

- Using [AW23], we can make of SILBE an IND-CU-CCA UPKE in the ROM.

# Encryption & Decryption

$$p = 3^{\beta} N f + 1 \text{ with } N = \prod_{i=1}^{n} p_i$$
$$\langle P_0, Q_0 \rangle = E_0[N]$$

- Alice knows $\phi_A$ and Bob $E_A$, $m \in \mu_2(N)$.
- Encryption:
  - Bob computes $\phi : E_A \to E_B$ $\deg(\phi_B) = 3^{\beta}$
  - Computes $\binom{R_1}{R_2} = [m]\phi_B\binom{P_A}{Q_A}$ with $\langle P_A, Q_A \rangle = E_A[N]$.
  - Sends $E_B, R_1, R_2$.
- Decryption:
  - Alice computes $\psi(E_B[N])$ as
    $$\psi\begin{pmatrix} S \\ T \end{pmatrix} = 3^{\beta} \deg(\phi_A) \mathbf{M}_{\pi}^{-1} \mathbf{M}_{\phi_A} \pi \begin{pmatrix} R_1 \\ R_2 \end{pmatrix}$$
    with $\binom{S}{T} = \phi_B \circ \phi_A \binom{P_0}{Q_0}$
  - Uses Kani's Lemma in dim 4 to get
    $$\psi(E[3^{\beta}]) = \ker(\psi)[3^{\beta}] = \ker(\widehat{\phi_B})$$
  - Uses discrete log to retrieve $m$.




$$\psi = \pi_*(\phi_B \circ \phi_A) \circ \phi_A \circ \phi_B$$

- Need $N > 3^{\beta} \deg(\phi_A) \simeq 3^{\beta} \sqrt{p} \log(p)$.

# Encryption & Decryption

- Alice knows $\phi_A$ and Bob $E_A$, $m \in \mu_2(N)$.
- Encryption:
  - Bob computes $\phi : E_A \to E_B$ $\deg(\phi_B) = 3^\beta$
  - Computes $\binom{R_1}{R_2} = [m]\phi_B\binom{P_A}{Q_A}$ with $\langle P_A, Q_A\rangle = E_A[N]$.
  - Sends $E_B, R_1, R_2$.
- Decryption:
  - Alice computes $\psi(E_B[N])$ as

$$\psi\begin{pmatrix} S \\ T \end{pmatrix} = 3^\beta \deg(\phi_A)\mathbf{M}_\pi^{-1}\mathbf{M}_{\phi_\mathbf{A}}\pi\begin{pmatrix} R_1 \\ R_2 \end{pmatrix}$$

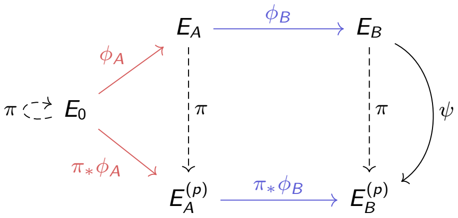
    with $\binom{S}{T} = \phi_B \circ \phi_A\binom{P_0}{Q_0}$
  - Uses Kani's Lemma in dim 4 to get

$$\psi(E[3^\beta]) = \ker(\psi)[3^\beta] = \ker(\widehat{\phi_B})$$

  - Uses discrete log to retrieve $m$.

$$p = 3^\beta Nf + 1 \text{ with } N = \prod_{i=1}^{n} p_i$$

$$\langle P_0, Q_0\rangle = E_0[N]$$




$$\psi = \pi_*(\phi_B \circ \phi_A) \circ \phi_A \circ \phi_B$$

- Need $N > 3^\beta \deg(\phi_A) \simeq 3^\beta\sqrt{p}\log(p)$.

# Encryption & Decryption

- Alice knows $\phi_A$ and Bob $E_A$, $m \in \mu_2(N)$.
- Encryption:
  - Bob computes $\phi : E_A \to E_B$ $\deg(\phi_B) = 3^\beta$
  - Computes $\binom{R_1}{R_2} = [m]\phi_B\binom{P_A}{Q_A}$ with $\langle P_A, Q_A \rangle = E_A[N]$.
  - Sends $E_B, R_1, R_2$.
- Decryption:
  - Alice computes $\psi(E_B[N])$ as

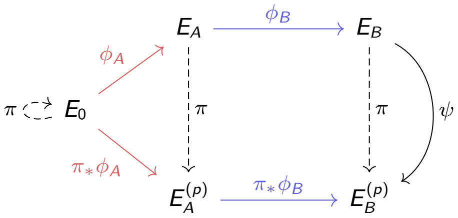
    $$\psi\begin{pmatrix} S \\ T \end{pmatrix} = 3^\beta \deg(\phi_A)\mathbf{M}_\pi^{-1}\mathbf{M}_{\phi_\mathbf{A}}\pi\begin{pmatrix} R_1 \\ R_2 \end{pmatrix}$$

    with $\binom{S}{T} = \phi_B \circ \phi_A\binom{P_0}{Q_0}$
  - Uses Kani's Lemma in dim 4 to get

    $$\psi(E[3^\beta]) = \ker(\psi)[3^\beta] = \ker(\widehat{\phi_B})$$
  - Uses discrete log to retrieve $m$.

$$p = 3^\beta Nf + 1 \text{ with } N = \prod_{i=1}^{n} p_i$$

$$\langle P_0, Q_0 \rangle = E_0[N]$$

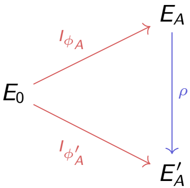



$$\psi = \pi_*(\phi_B \circ \phi_A) \circ \phi_A \circ \phi_B$$

- Need $N > 3^\beta \deg(\phi_A) \simeq 3^\beta \sqrt{p}\log(p)$.

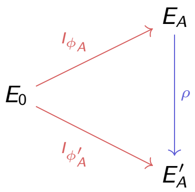
# Key Update

- Alice knows $\phi_A$ and Bob $E_A$ and $\langle U_A, V_A \rangle = E_A[3^\beta]$
- UG: $\eta \in \mathbb{Z}_{3^\beta}$.
- Upk:
  - Computes $\rho : E_A \to E'_A$ $\ker(\rho) = \langle U_A + [\eta]V_A \rangle$
- Usk:
  - Computes $\rho : E_A \to E'_A$ $\ker(\rho) = \langle U_A + [\eta]V_A \rangle$
  - Find $I_\rho$ using $\mathcal{O}_{E_A}$.
  - Find small prime ideal $I_{\phi'_A}$.
  - Use HD rep. to find $\mathcal{O}_{E'_A}$.
- More complex in reality.



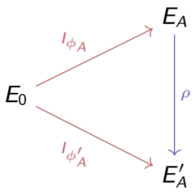
# Key Update

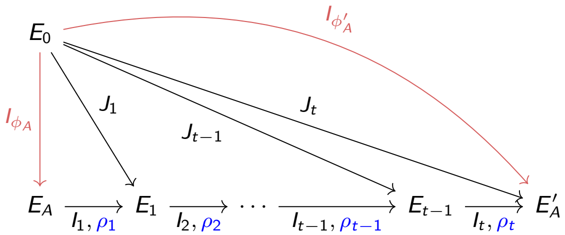
- Alice knows $\phi_A$ and Bob $E_A$ and $\langle U_A, V_A \rangle = E_A[3^\beta]$
- UG: $\eta \in \mathbb{Z}_{3^\beta}$.
- Upk:
  - Computes $\rho : E_A \to E'_A$ $\ker(\rho) = \langle U_A + [\eta]V_A \rangle$
- Usk:
  - Computes $\rho : E_A \to E'_A$ $\ker(\rho) = \langle U_A + [\eta]V_A \rangle$
  - Find $I_\rho$ using $\mathcal{O}_{E_A}$.
  - Find small prime ideal $I_{\phi'_A}$.
  - Use HD rep. to find $\mathcal{O}_{E'_A}$.
- More complex in reality.



# Key Update

- Alice knows $\phi_A$ and Bob $E_A$ and $\langle U_A, V_A\rangle = E_A[3^\beta]$
- UG: $\eta \in \mathbb{Z}_{3^\beta}$.
- Upk:
  - Computes $\rho : E_A \to E'_A$ $\ker(\rho) = \langle U_A + [\eta]V_A\rangle$
- Usk:
  - Computes $\rho : E_A \to E'_A$ $\ker(\rho) = \langle U_A + [\eta]V_A\rangle$
  - Find $I_\rho$ using $\mathcal{O}_{E_A}$.
  - Find small prime ideal $I_{\phi'_A}$.
  - Use HD rep. to find $\mathcal{O}_{E'_A}$.
- More complex in reality.



# References I


- Kyoichi Asano and Yohei Watanabe, *Updatable public key encryption with strong cca security: Security analysis and efficient generic construction*, Cryptology ePrint Archive, Paper 2023/976, 2023, https://eprint.iacr.org/2023/976.
- Daniel J Bernstein, Luca De Feo, Antonin Leroux, and Benjamin Smith, *Faster computation of isogenies of large prime degree*, Open Book Series **4** (2020), no. 1, 39–55.
- Andrea Basso, Luciano Maino, and Giacomo Pope, *Festa: Fast encryption from supersingular torsion attacks*, Cryptology ePrint Archive, Paper 2023/660, 2023, https://eprint.iacr.org/2023/660.
- Wouter Castryck and Thomas Decru, *An efficient key recovery attack on sidh*, Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2023, pp. 423–447.
- Wouter Castryck and Frederik Vercauteren, *A polynomial-time attack on instances of m-sidh and festa*, Cryptology ePrint Archive, Paper 2023/1433, 2023, https://eprint.iacr.org/2023/1433.

# References II


- Max Deuring, *Die typen der multiplikatorenringe elliptischer funktionenkörper*, Abhandlungen aus dem mathematischen Seminar der Universität Hamburg, vol. 14, Springer Berlin/Heidelberg, 1941, pp. 197–272.
- Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, and Benjamin Wesolowski, *Sqisign: compact post-quantum signatures from quaternions and isogenies*, Advances in Cryptology–ASIACRYPT 2020: 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7–11, 2020, Proceedings, Part I 26, Springer, 2020, pp. 64–93.
- Pierrick Dartois, Antonin Leroux, Damien Robert, and Benjamin Wesolowski, *Sqisignhd: New dimensions in cryptography*, Cryptology ePrint Archive, Paper 2023/436, 2023, `https://eprint.iacr.org/2023/436`.
- Victoria de Quehen, Péter Kutas, Chris Leonardi, Chloe Martindale, Lorenz Panny, Christophe Petit, and Katherine E. Stange, *Improved torsion-point attacks on sidh variants*, Cryptology ePrint Archive, Paper 2020/633, 2020, `https://eprint.iacr.org/2020/633`.

# References III


- Cyprien Delpech de Saint Guilhem, Péter Kutas, Christophe Petit, and Javier Silva, *Séta: Supersingular encryption from torsion attacks.*, IACR Cryptol. ePrint Arch. **2019** (2019), 1291.
- Edward Eaton, David Jao, Chelsea Komlo, and Youcef Mokrani, *Towards post-quantum key-updatable public-key encryption via supersingular isogenies*, International Conference on Selected Areas in Cryptography, Springer, 2021, pp. 461–482.
- Tako Boris Fouotsa, Tomoki Moriya, and Christophe Petit, *M-sidh and md-sidh: countering sidh attacks by masking information*, Cryptology ePrint Archive, Paper 2023/013, 2023, `https://eprint.iacr.org/2023/013`.
- Tako Boris Fouotsa and Christophe Petit, *A new adaptive attack on sidh*, Cryptology ePrint Archive, Paper 2021/1322, 2021, `https://eprint.iacr.org/2021/1322`.
- David Jao and Luca De Feo, *Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies*, Post-Quantum Cryptography: 4th International Workshop, PQCrypto 2011, Taipei, Taiwan, November 29–December 2, 2011. Proceedings 4, Springer, 2011, pp. 19–34.

# References IV


- Ernst Kani, *The number of curves of genus two with elliptic differentials.*
- Antonin Leroux, *Quaternion algebra and isogeny-based cryptography*, Ph.D. thesis, Ecole doctorale de l'Institut Polytechnique de Paris, 2022.
- Antonin Leroux, *Verifiable random function from the deuring correspondence and higher dimensional isogenies*, Cryptology ePrint Archive, Paper 2023/1251, 2023, https://eprint.iacr.org/2023/1251.
- Antonin Leroux and Maxime Roméas, *Updatable encryption from group actions*, Cryptology ePrint Archive (2022).
- Luciano Maino, Chloe Martindale, Lorenz Panny, Giacomo Pope, and Benjamin Wesolowski, *A direct key recovery attack on sidh*, Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2023, pp. 448–471.
- Kohei Nakagawa and Hiroshi Onuki, *Qfesta: Efficient algorithms and parameters for festa using quaternion algebras*, Cryptology ePrint Archive, Paper 2023/1468, 2023, https://eprint.iacr.org/2023/1468.

# References V


- Christophe Petit, *Faster algorithms for isogeny problems using torsion point images*, Advances in Cryptology–ASIACRYPT 2017: 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part II 23, Springer, 2017, pp. 330–353.
- Damien Robert, *Fonctions thêta et applications à la cryptographie*, Ph.D. thesis, Université Henri Poincaré-Nancy I, 2010.
- ______, *Evaluating isogenies in polylogarithmic time*.
- ______, *Breaking sidh in polynomial time*, Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2023, pp. 472–503.
- Jacques Vélu, *Isogénies entre courbes elliptiques*, Comptes-Rendus de l'Académie des Sciences **273** (1971), 238–241.