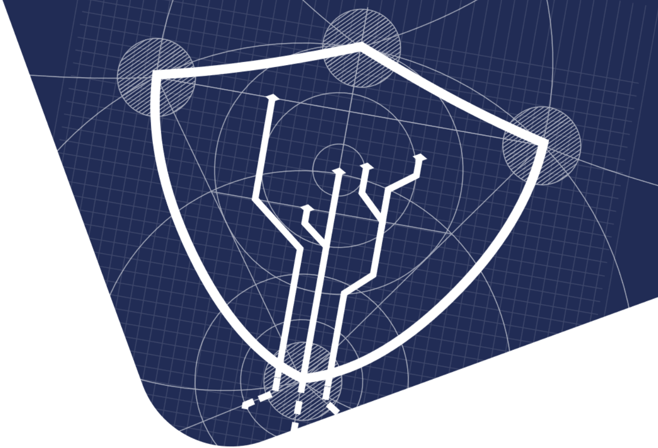


Selected Area of Cryptography 2024

SILBE: an Updatable Public Key Encryption Scheme from Lollipop Attacks

Max Duparc[1,2], Tako Boris Fouotsa[2], Serge Vaudenay[2]

[1]Kudelski IoT, [2]LASEC EPFL

Motivation:

- At SAC 21, [EJKM21] considered the feasibility of Isogenies based UPKEs:
  - Using group action (CSIDH).
  - Using torsion information (SIDH).
- In the second case: "a viable construction in practice is hindered by existing mathematical limitations".

Contribution:

- Viable constructions are possible.
  - These mathematical limitations can be circonveign.
  - We construct **SILBE**: an "SIDH-like" viable UPKE.

Motivation:

- At SAC 21, [EJKM21] considered the feasibility of Isogenies based UPKEs:
  - Using group action (CSIDH).
  - Using torsion information (SIDH).
- In the second case: "a viable construction in practice is hindered by existing mathematical limitations".

Contribution:

- Viable constructions are possible.
  - These mathematical limitations can be circonveign.
  - We construct **SILBE**: an "SIDH-like" viable UPKE.

EPFL LASEC KUDELSKI IoTHINGS

Motivation:

- At SAC 21, [EJKM21] considered the feasibility of Isogenies based UPKEs:
  - Using group action (CSIDH).
  - Using torsion information (SIDH).
- In the second case: "a viable construction in practice is hindered by existing mathematical limitations".

Contribution:

- Viable constructions are possible.
  - These mathematical limitations can be circonveign.
  - We construct **SILBE**: an "SIDH-like" viable UPKE.

UPKE

Definition

An *UPKE* scheme is a PKE

- $\mathsf{KeyGen}(1^\lambda) \xrightarrow{\$} (\mathsf{sk}, \mathsf{pk})$
- $\mathsf{Enc}(\mathsf{pk}, \mathsf{m}) \xrightarrow{\$} \mathsf{ct}$
- $\mathsf{Dec}(\mathsf{sk}, \mathsf{ct}) \longrightarrow \mathsf{m}$

with a *Key-Update* mechanism

- $\mathsf{UpdGen}(1^\lambda) \xrightarrow{\$} \mu$
- $\mathsf{UpdPk}(\mathsf{pk}, \mu) \longrightarrow \mathsf{pk}'$
- $\mathsf{UpdSk}(\mathsf{sk}, \mu) \longrightarrow \mathsf{sk}'$

Must ensure:

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

$$\mathsf{sk}_0 \longrightarrow \mathsf{sk}_1 \longrightarrow \mathsf{sk}_2 \longrightarrow \mathsf{sk}_3$$

UPKE

Definition

An *UPKE* scheme is a PKE

- $\mathsf{KeyGen}(1^\lambda) \xrightarrow{\$} (\mathsf{sk}, \mathsf{pk})$
- $\mathsf{Enc}(\mathsf{pk}, \mathsf{m}) \xrightarrow{\$} \mathsf{ct}$
- $\mathsf{Dec}(\mathsf{sk}, \mathsf{ct}) \longrightarrow \mathsf{m}$

with a *Key-Update* mechanism

- $\mathsf{UpdGen}(1^\lambda) \xrightarrow{\$} \mu$
- $\mathsf{UpdPk}(\mathsf{pk}, \mu) \longrightarrow \mathsf{pk}'$
- $\mathsf{UpdSk}(\mathsf{sk}, \mu) \longrightarrow \mathsf{sk}'$

Must ensure:

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

$$\mathsf{sk}_0 \longrightarrow \mathsf{sk}_1 \longrightarrow \mathsf{sk}_2 \longrightarrow \mathsf{sk}_3$$

UPKE

Definition

An *UPKE* scheme is a PKE

- $\mathsf{KeyGen}(1^\lambda) \xrightarrow{\$} (\mathsf{sk}, \mathsf{pk})$
- $\mathsf{Enc}(\mathsf{pk}, \mathsf{m}) \xrightarrow{\$} \mathsf{ct}$
- $\mathsf{Dec}(\mathsf{sk}, \mathsf{ct}) \longrightarrow \mathsf{m}$

with a *Key-Update* mechanism

- $\mathsf{UpdGen}(1^\lambda) \xrightarrow{\$} \mu$
- $\mathsf{UpdPk}(\mathsf{pk}, \mu) \longrightarrow \mathsf{pk}'$
- $\mathsf{UpdSk}(\mathsf{sk}, \mu) \longrightarrow \mathsf{sk}'$

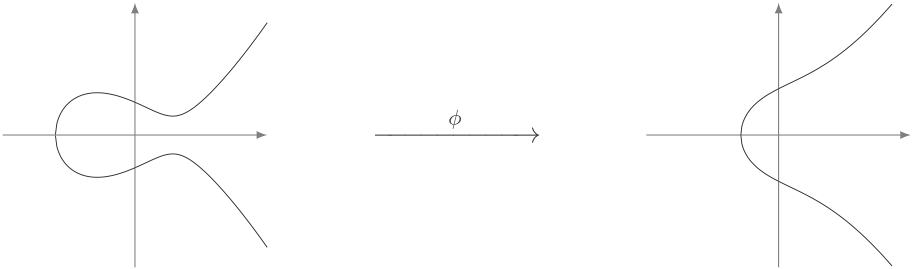
Must ensure:

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

$$\mathsf{sk}_0 \longrightarrow \mathsf{sk}_1 \longrightarrow \mathsf{sk}_2 \longrightarrow \mathsf{sk}_3$$

Isogenies

- Surjective group morphism between elliptic curves.

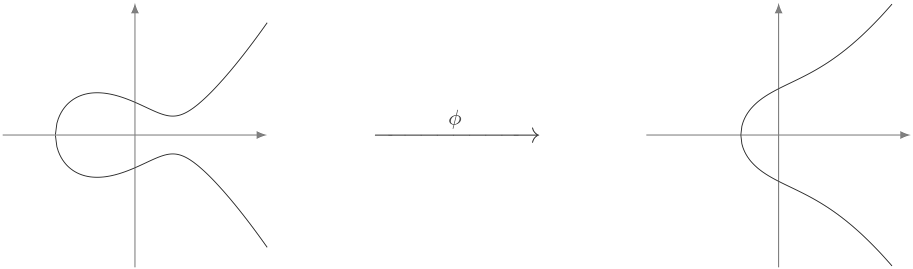


$E : y^2 = x^3 - 3x + 3$ $\qquad\qquad$ $E' : y^2 = x^3 + 5x + 6$

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

Isogenies

- Surjective group morphism between elliptic curves.



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

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

Isogenies

- **scalar maps**:

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

$$\ker([n]) = E[n] \cong \mathbb{Z}_n^2$$

- **Frobenius map**:

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

$$\pi(x, y) := (x^p, y^p)$$

- When **separable**:

$$\phi : E \to E' \text{ determined}^{1} \text{ by } \ker(\phi)$$

- The degree $\mathbf{deg}(\phi) = |\ker(\phi)|$.
- The **dual** $\widehat{\phi} : E' \to E$ s.t.

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

[1] up to isomorphism

Isogenies

- **scalar maps**:

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

$$\ker([n]) = E[n] \cong \mathbb{Z}_n^2$$

- **Frobenius map**:

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

$$\pi(x, y) := (x^p, y^p)$$

- When **separable**:

$\phi : E \to E'$ determined[1] by $\ker(\phi)$

- The degree **deg**$(\phi) = |\ker(\phi)|$.
- The **dual** $\widehat{\phi} : E' \to E$ s.t.

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

[1] up to isomorphism

EPFL LASEC KUDELSKI IoTHINGS

Isogenies

- **scalar maps**:

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

$$\ker([n]) = E[n] \cong \mathbb{Z}_n^2$$

- **Frobenius map**:

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

$$\pi(x, y) := (x^p, y^p)$$

- When **separable**:

$$\phi : E \to E' \text{ determined}^1 \text{ by } \ker(\phi)$$

- The degree $\mathbf{deg}(\phi) = |\ker(\phi)|$.
- The **dual** $\widehat{\phi} : E' \to E$ s.t.

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

[1] up to isomorphism

Isogenies

- **scalar maps**:

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

$$\ker([n]) = E[n] \cong \mathbb{Z}_n^2$$

- **Frobenius map**:

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

$$\pi(x, y) := (x^p, y^p)$$

- When **separable**:

$$\phi : E \to E' \text{ determined}^1 \text{ by } \ker(\phi)$$

- The degree **deg**$(\phi) = |\ker(\phi)|$.
- The **dual** $\widehat{\phi} : E' \to E$ s.t.

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

[1] up to isomorphism

KLPT

- When working with supersingular curves, we have additional tools.

$$\mathrm{End}(E) + \phi : E \to E' \xrightarrow{\textbf{KLPT}} \psi : E \to E'$$

- [KLPT14] **Original**: $\deg(\psi)$ smooth and large $O(p^3)$.
- [DLRW24] **New**: $\deg(\psi)$ generic and relatively small $O(p^{0.5})$.

KLPT

- When working with supersingular curves, we have additional tools.

$$\mathrm{End}(E) + \phi : E \to E' \xrightarrow{\textbf{KLPT}} \psi : E \to E'$$

- [KLPT14] **Original**: $\deg(\psi)$ smooth and large $O(p^3)$.
- [DLRW24] **New**: $\deg(\psi)$ generic and relatively small $O(p^{0.5})$.

KLPT

- When working with supersingular curves, we have additional tools.

$$\mathrm{End}(E) + \phi : E \to E' \xrightarrow{\textbf{KLPT}} \psi : E \to E'$$

- [KLPT14] **Original**: $\deg(\psi)$ smooth and large $O(p^3)$.

- [DLRW24] **New**: $\deg(\psi)$ generic and relatively small $O(p^{0.5})$.

SIDH

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

$$\begin{tikzcd} E \arrow[r, "\phi_A"] \arrow[d, "\phi_B"'] & E_A \\ E_B & \end{tikzcd}$$

- Alice share:
  - $E_A, \phi_A(P_B), \phi_A(Q_B)$.
- Bob share:
  - $E_B, \phi_B(P_A), \phi_B(Q_A)$.

Pushforward: $\ker(\phi_* \psi) = \phi(\ker(\psi))$

Problem (SIP + torsion)

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

- $p = \ell_A^{e_A} \ell_B^{e_B} f - 1$ prime:
  - $\langle P_A, Q_A \rangle = E[\ell_A^{e_A}]$
  - $\langle P_B, Q_B \rangle = E[\ell_B^{e_B}]$
- Alice share:
  - $E_A, \phi_A(P_B), \phi_A(Q_B)$.
- Bob share:
  - $E_B, \phi_B(P_A), \phi_B(Q_A)$.

Pushforward: $\ker(\phi_* \psi) = \phi(\ker(\psi))$

$$\begin{tikzcd}
E \arrow[r, "\phi_A"] \arrow[d, "\phi_B"'] & E_A \arrow[d, "{[\phi_A]_* \phi_B}"] \\
E_B \arrow[r, "{[\phi_B]_* \phi_A}"'] & E_K
\end{tikzcd}$$

Problem (SIP + torsion)

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

- $p = \ell_A^{e_A} \ell_B^{e_B} f - 1$ prime:
  - $\langle P_A, Q_A \rangle = E[\ell_A^{e_A}]$
  - $\langle P_B, Q_B \rangle = E[\ell_B^{e_B}]$
- Alice share:
  - $E_A, \phi_A(P_B), \phi_A(Q_B)$.
- Bob share:
  - $E_B, \phi_B(P_A), \phi_B(Q_A)$.

Pushforward: $\ker(\phi_* \psi) = \phi(\ker(\psi))$

$$\begin{tikzcd}
E \arrow[r, "\phi_A"] \arrow[d, "\phi_B"'] & E_A \arrow[d, "{[\phi_A]_* \phi_B}"] \\
E_B \arrow[r, "{[\phi_B]_* \phi_A}"'] & E_K
\end{tikzcd}$$

Problem (SIP + torsion)

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

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

EPFL LASEC KUDELSKI IoTHINGS

[EJKM21]: SIDH style "online"-UPKE

$$
\begin{tikzcd}
E_0 \arrow[r, "\phi_{A_1}"] \arrow[d, "\phi_{B_0}"'] & E_{A_1} \arrow[r, "\phi_{A_2}"] \arrow[d, "\phi_{B_1}"] & \cdots \arrow[r, "\phi_{A_{t-1}}"] \arrow[d] & E_{A_{t-1}} \arrow[d, "\phi_{B_{t-1}}"] \\
E_B \arrow[r, "\psi_{A_1}"] & E_{BA_1} \arrow[r, "\psi_{A_2}"] & \cdots \arrow[r, "\psi_{A_{t-1}}"] & E_{BA_{t-1}}
\end{tikzcd}
$$

This has several limitations:

1. SIDH is not secure. [CD23, MMP+23, Rob23].
2. No Asynchronous key update.
3. **KLPT** outputs very large isogenies $\implies$ impractical with SIDH parameters.

EPFL LASEC KUDELSKI IOTHINGS

[EJKM21]: SIDH style "online"-UPKE

$$
\begin{tikzcd}
E_0 \arrow[r, "\phi_{A_1}"] \arrow[d, "\phi_{B_0}"'] & E_{A_1} \arrow[r, "\phi_{A_2}"] \arrow[d, "\phi_{B_1}"] & \cdots \arrow[r, "\phi_{A_{t-1}}"] \arrow[d] & E_{A_{t-1}} \arrow[r, "\phi_{A_t}"] \arrow[d, "\phi_{B_{t-1}}"] & E_{A_t} \\
E_B \arrow[r, "\psi_{A_1}"] & E_{BA_1} \arrow[r, "\psi_{A_2}"] & \cdots \arrow[r, "\psi_{A_{t-1}}"] & E_{BA_{t-1}} &
\end{tikzcd}
$$

This has several limitations:

1. SIDH is not secure. [CD23, MMP$^+$23, Rob23].
2. No Asynchronous key update.
3. **KLPT** outputs very large isogenies $\Longrightarrow$ impractical with SIDH parameters.

[EJKM21]: SIDH style "online"-UPKE

$$\begin{tikzcd}
E_0 \arrow[r, "\phi_{A_1}"] \arrow[d, "\phi_{B_0}"'] & E_{A_1} \arrow[r, "\phi_{A_2}"] \arrow[d, "\phi_{B_1}"] & \cdots \arrow[r, "\phi_{A_{t-1}}"] \arrow[d] & E_{A_{t-1}} \arrow[r, "\phi_{A_t}"] \arrow[d, "\phi_{B_{t-1}}"] & E_{A_t} \arrow[d, "\phi_{B_t}"] \\
E_B \arrow[r, "\psi_{A_1}"] & E_{BA_1} \arrow[r, "\psi_{A_2}"] & \cdots \arrow[r, "\psi_{A_{t-1}}"] & E_{BA_{t-1}} \arrow[r, "\psi_{A_t}"] & E_{BA_t}
\end{tikzcd}$$

This has several limitations:

1. SIDH is not secure. [CD23, MMP$^+$23, Rob23].
2. No Asynchronous key update.
3. **KLPT** outputs very large isogenies $\implies$ impractical with SIDH parameters.

EPFL LASEC KUDELSKI IoTHINGS

[EJKM21]: SIDH style "online"-UPKE

$$
\begin{tikzcd}
E_0 \arrow[r, "\phi_{A_1}"] \arrow[rrrr, bend left, "\phi'_A"] \arrow[d, "\phi_{B_0}"'] & E_{A_1} \arrow[r, "\phi_{A_2}"] \arrow[d, "\phi_{B_1}"] & \cdots \arrow[r, "\phi_{A_{t-1}}"] \arrow[d] & E_{A_{t-1}} \arrow[r, "\phi_{A_t}"] \arrow[d, "\phi_{B_{t-1}}"] & E_{A_t} \arrow[d, "\phi_{B_t}"] \\
E_B \arrow[r, "\psi_{A_1}"] & E_{BA_1} \arrow[r, "\psi_{A_2}"] & \cdots \arrow[r, "\psi_{A_{t-1}}"] & E_{BA_{t-1}} \arrow[r, "\psi_{A_t}"] & E_{BA_t}
\end{tikzcd}
$$

This has several limitations:

1. SIDH is not secure. [CD23, MMP$^+$23, Rob23].
2. No Asynchronous key update.
3. **KLPT** outputs very large isogenies $\implies$ impractical with SIDH parameters.

[EJKM21]: SIDH style "online"-UPKE

$$
\begin{tikzcd}
E_0 \arrow[r, "\phi_{A_1}"] \arrow[rrrr, bend left, "\phi'_A"] \arrow[d, "\phi_{B_0}"'] & E_{A_1} \arrow[r, "\phi_{A_2}"] \arrow[d, "\phi_{B_1}"] & \cdots \arrow[r, "\phi_{A_{t-1}}"] \arrow[d] & E_{A_{t-1}} \arrow[r, "\phi_{A_t}"] \arrow[d, "\phi_{B_{t-1}}"] & E_{A_t} \arrow[d, "\phi_{B_t}"] \\
E_B \arrow[r, "\psi_{A_1}"] & E_{BA_1} \arrow[r, "\psi_{A_2}"] & \cdots \arrow[r, "\psi_{A_{t-1}}"] & E_{BA_{t-1}} \arrow[r, "\psi_{A_t}"] & E_{BA_t}
\end{tikzcd}
$$

This has several limitations:

1. SIDH is not secure. [CD23, MMP$^+$23, Rob23].
2. No Asynchronous key update.
3. **KLPT** outputs very large isogenies $\implies$ impractical with SIDH parameters.

Masked torsion information

Theorem ([Rob22]: SIP + torsion is easy)

Let $\phi : E \to E'$ be an isogeny of degree d, $\langle P, Q \rangle = E[N]$ with $N^2 > d$ a smooth integer.

$$P, Q, \phi(P), \phi(Q) \longrightarrow \phi$$

Problem (SIP + masked torsion)

Let $\phi : E \to E'$ be an isogeny of degree d, $\langle P, Q \rangle = E[N]$ and $m \in \mathbb{Z}_N$ with $N = \prod_{i=1}^{n} p_i$.

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

EPFL LASEC KUDELSKI IoTHINGS

Masked torsion information

Theorem ([Rob22]: SIP + torsion is easy)

Let $\phi : E \to E'$ be an isogeny of degree d, $\langle P, Q\rangle = E[N]$ with $N^2 > d$ a smooth integer.

$$P, Q, \phi(P), \phi(Q) \longrightarrow \phi$$

Problem (SIP + masked torsion)

Let $\phi : E \to E'$ be an isogeny of degree d, $\langle P, Q\rangle = E[N]$ and $m \in \mathbb{Z}_N$ with $N = \prod_{i=1}^{n} p_i$.

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

Lollipops

$$\textbf{masked torsion info on } \phi_B \xrightarrow{\text{lollipop}} \textbf{torsion info on } \psi$$

- Use $\psi = [m]\phi_B \circ \theta \circ \widehat{\phi_B}[m]$
  $= \phi_B \circ \theta \circ \widehat{\phi_B}$
  with $N^2 > \deg(\psi)$.
- [CV23]: Use $\psi = \pi_*(\phi_B) \circ \widehat{\phi_B}$
- Construct a trapdoor with
  $\psi = \pi_*(\varphi_B \circ \phi_A) \circ \widehat{\phi_A} \circ \widehat{\phi_B}$

$$\begin{tikzcd} E_A \arrow[loop left, "\theta"] \arrow[r, shift left, "\phi_B"] & E_B \arrow[l, shift left, "\widehat{\phi_B}"] \end{tikzcd}$$

key $:= E_A$

trapdoor $:= \phi_A$

Lollipops

$$\textbf{masked torsion info on } \phi_B \xrightarrow{\text{lollipop}} \textbf{torsion info on } \psi$$

- Use $\psi = [m]\phi_B \circ \theta \circ \widehat{\phi_B}[m]$
  $= \phi_B \circ \theta \circ \widehat{\phi_B}$
  with $N^2 > \deg(\psi)$.
- [CV23]: Use $\psi = \pi_*(\phi_B) \circ \widehat{\phi_B}$
- Construct a trapdoor with
  $\psi = \pi_*(\varphi_B \circ \phi_A) \circ \widehat{\phi_A} \circ \widehat{\phi_B}$

$$\begin{tikzcd}
E_A \arrow[loop left, dashed, "\pi"] \arrow[r, "\phi_B"] \arrow[dr, "\pi_*\phi_B"'] & E_B \arrow[d, dashed, "\pi"] \arrow[d, bend left, "\psi"] \\
 & E_B^{(p)}
\end{tikzcd}$$

key $:= E_A$

trapdoor $:= \phi_A$

Lollipops

$$\textbf{masked torsion info on } \phi_B \xrightarrow{\text{lollipop}} \textbf{torsion info on } \psi$$

- Use $\psi = [m]\phi_B \circ \theta \circ \widehat{\phi_B}[m]$
  $= \phi_B \circ \theta \circ \widehat{\phi_B}$
  with $N^2 > \deg(\psi)$.
- [CV23]: Use $\psi = \pi_*(\phi_B) \circ \widehat{\phi_B}$
- Construct a trapdoor with
  $\psi = \pi_*(\varphi_B \circ \phi_A) \circ \widehat{\phi_A} \circ \widehat{\phi_B}$

$$\text{key} := E_A$$

$$\text{trapdoor} := \phi_A$$

$$\begin{tikzcd}
 & E_A \arrow[r, "\phi_B"] \arrow[dd, dashed, "\pi"] & E_B \arrow[dd, dashed, "\pi"] \arrow[dd, bend left, "\psi"] \\
E_0 \arrow[loop left, dashed, "\pi"] \arrow[ur, "\phi_A"] \arrow[dr, "\pi_*\phi_A"'] & & \\
 & E_A^{(p)} \arrow[r, "\pi_*\phi_B"] & E_B^{(p)}
\end{tikzcd}$$

Lollipop Trapdoor

Lemma

Lollipop trapdoor is one-way function $\iff$ ***SIP + masked torsion*** *hard*

- Works for any curve E_A:
  - There always exists $\phi_A : E_0 \to E_A$, $\deg(\phi_A) \simeq \sqrt{p}$.
  - Computable with the **newKLPT**.

▶ How to Generate/Update the key and trapdoor (E_A, ϕ_A) ?

Lollipop Trapdoor

Lemma

Lollipop trapdoor is one-way function $\iff$ ***SIP + masked torsion** hard*

- Works for any curve E_A:
  - There always exists $\phi_A : E_0 \to E_A$, $\deg(\phi_A) \simeq \sqrt{p}$.
  - Computable with the **newKLPT**.

▶ How to Generate/Update the key and trapdoor (E_A, ϕ_A) ?

Lollipop Trapdoor

Lemma

Lollipop trapdoor is one-way function $\iff$ ***SIP*** $+$ ***masked torsion*** *hard*

- Works for any curve E_A:
  - There always exists $\phi_A : E_0 \to E_A$, $\deg(\phi_A) \simeq \sqrt{p}$.
  - Computable with the **newKLPT**.

▶ How to Generate/Update the key and trapdoor (E_A, ϕ_A) ?

Sampling random curves

Theorem

Let $\rho : E \to E'$ be an ℓ^h-isogeny, with $h \geq (1 + 2\lambda \log_p(2))$. Then;

$$E' \text{ is } \lambda\text{-statistically indistinguishable from uniform.}$$

- Easy to compute.

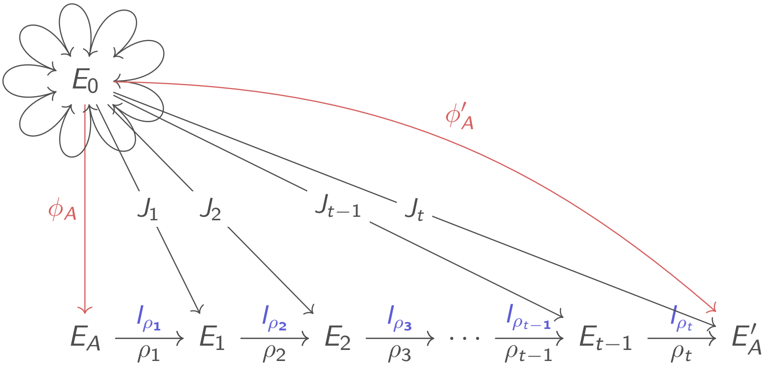
$$\begin{tikzcd} E \arrow[r, "\rho_1"] \arrow[rrrr, bend left, "\rho"] & E_1 \arrow[r, "\rho_2"] & E_2 \arrow[r, "\rho_3"] & \cdots \arrow[r, "\rho_t"] & E' \end{tikzcd}$$

with $\deg(\rho_i) = \ell^{h_i}$ and $\ell^{h_i} | p \pm 1$.

With **newKLPT**, we can update the trapdoor.

EPFL LASEC KUDELSKI IoTHINGS

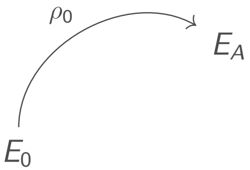
More complex in reality



SILBE

$$E_0$$

SILBE



SILBE

$$\begin{tikzcd} E_0 \arrow[r, "\phi_A"'] \arrow[r, bend left, "\rho_0"] & E_A \end{tikzcd}$$

SILBE

$$\begin{tikzcd}
 & E_A \arrow[r, "\phi_B"] & E_B \\
E_0 \arrow[ur, "\phi_A"'] \arrow[ur, bend left, "\rho_0"] & &
\end{tikzcd}$$

SILBE

$$
\begin{tikzcd}
 & E_A \arrow[r, "\phi_B"] \arrow[dd, dashed, "\pi"] & E_B \arrow[dd, dashed, "\pi"'] \\
E_0 \arrow[ur, "\phi_A"] \arrow[ur, bend left, "\rho_0"] \arrow[dr, "\pi_*\phi_A"'] & & \\
 & E_A^{(p)} \arrow[r, "\pi_*\phi_B"'] & E_B^{(p)}
\end{tikzcd}
$$

SILBE

$$
\begin{tikzcd}
 & & E_A \arrow[r, "\phi_B"] \arrow[d, dashed, "\pi"] \arrow[dll, bend right, "\rho_1"'] & E_B \arrow[d, dashed, "\pi"'] \\
E'_A & E_0 \arrow[ur, "\phi_A"] \arrow[dr, "\pi_*\phi_A"'] \arrow[ur, bend left, "\rho_0"] & & \\
 & & E_A^{(p)} \arrow[r, "\pi_*\phi_B"'] & E_B^{(p)}
\end{tikzcd}
$$

SILBE

$$
\begin{tikzcd}
 & & E_A \arrow[r, "\phi_B"] \arrow[d, dashed, "\pi"] \arrow[ll, bend right=60, "\rho_1"'] & E_B \arrow[d, dashed, "\pi"'] \\
E'_A & E_0 \arrow[l, "\phi'_A"'] \arrow[ur, "\phi_A"] \arrow[ur, bend left=60, "\rho_0"] \arrow[dr, "\pi_*\phi_A"'] & & \\
 & & E_A^{(p)} \arrow[r, "\pi_*\phi_B"'] & E_B^{(p)}
\end{tikzcd}
$$

SILBE

$$
\begin{tikzcd}
E_{B_1} & & & E_A \arrow[r, "\phi_B"] \arrow[dd, dashed, "\pi"] \arrow[dll, bend right, "\rho_1"'] & E_B \arrow[dd, dashed, "\pi"'] \\
& E'_A \arrow[ul, "\phi_{B_1}"'] & E_0 \arrow[l, "\phi'_A"'] \arrow[ur, "\phi_A"] \arrow[ur, bend left=60, "\rho_0"] \arrow[dr, "\pi_*\phi_A"'] & & \\
& & & E_A^{(p)} \arrow[r, "\pi_*\phi_B"'] & E_B^{(p)}
\end{tikzcd}
$$

SILBE

$$
\begin{tikzcd}
E_{B_1} & & & E_A \arrow[r, "\phi_B"] \arrow[dd, dashed, "\pi"] \arrow[dll, bend right, "\rho_1"'] & E_B \arrow[dd, dashed, "\pi"'] \\
E_{B_2} & E'_A \arrow[ul, "\phi_{B_1}"'] \arrow[l, "\phi_{B_2}"'] \arrow[dl, "\phi_{B_3}"] & E_0 \arrow[l, "\phi'_A"'] \arrow[ur, "\phi_A"] \arrow[ur, bend left, "\rho_0"] \arrow[dr, "\pi_*\phi_A"'] & & \\
E_{B_3} & & & E_A^{(p)} \arrow[r, "\pi_*\phi_B"'] & E_B^{(p)}
\end{tikzcd}
$$

SILBE's Security

Lemma

SILBE is OW-PCA secure $\iff$ ***SIP*** $+$ ***masked torsion*** *hard*

Lemma

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

[AW23] : OW-PCA-U $\xrightarrow{\text{U-FO}}$ IND-CCA-U in the ROM

SILBE's Security

Lemma

SILBE is OW-PCA secure $\iff$ ***SIP* + *masked torsion* hard**

Lemma

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

[AW23] : OW-PCA-U $\xrightarrow{\text{U-FO}}$ IND-CCA-U in the ROM

SILBE's Security

Lemma

SILBE is OW-PCA secure $\iff$ ***SIP + masked torsion*** *hard*

Lemma

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

$$\text{[AW23] : OW-PCA-U} \xrightarrow{\text{U-FO}} \text{IND-CCA-U in the ROM}$$

Conclusion:

- The attacks on SIDH have become a new essential tool in isogeny based cryptography:
  - SQISignHD, SQISign2D-East/West, SQIPrime.
  - FESTA, Q-FESTA, POKE.
  - SCALLOP-HD
- SILBE, a **viable** "SIDH-like" UPKE.

Future work:

- Can we improve its **efficiency** ?
  - Currently, primes for $\lambda = 128$ are $\simeq 13000$ bit large.

Conclusion:

- The attacks on SIDH have become a new essential tool in isogeny based cryptography:
  - SQISignHD, SQISign2D-East/West, SQIPrime.
  - FESTA, Q-FESTA, POKE.
  - SCALLOP-HD
- SILBE, a **viable** "SIDH-like" UPKE.

Future work:

- Can we improve its **efficiency** ?
  - Currently, primes for $\lambda = 128$ are $\simeq 13000$ bit large.

Conclusion:

- The attacks on SIDH have become a new essential tool in isogeny based cryptography:
  - SQISignHD, SQISign2D-East/West, SQIPrime.
  - FESTA, Q-FESTA, POKE.
  - SCALLOP-HD
- SILBE, a **viable** "SIDH-like" UPKE.

Future work:

- Can we improve its **efficiency** ?
  - Currently, primes for $\lambda = 128$ are $\simeq 13000$ bit large.

SILBE

$$
\begin{tikzcd}
E_{B_1} & & & E_A \arrow[r, "\phi_B"] \arrow[d, dashed, "\pi"] \arrow[dll, bend right, "\rho_1"'] & E_B \arrow[d, dashed, "\pi"'] \\
E_{B_2} & E'_A \arrow[l, "\phi_{B_2}"'] \arrow[ul, "\phi_{B_1}"'] \arrow[dl, "\phi_{B_3}"] & E_0 \arrow[l, "\phi'_A"'] \arrow[ur, "\phi_A"] \arrow[dr, "\pi_*\phi_A"'] \arrow[ur, bend left=60, "\rho_0"] & & \\
E_{B_2} & & & E_A^{(p)} \arrow[r, "\pi_*\phi_B"'] & E_B^{(p)}
\end{tikzcd}
$$

Happy to discuss your comments and questions !

SILBE's Parameters

SIP + masked torsion hard over $p = 3^{\beta} N f + 1$ with $N = \prod_{i=1}^{n} p_i$ if:

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

λ	β	N	f	n	$\log(p)$
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

Lemma

*Let A, B, A', B' be **abelian varieties**:*

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "g"'] & B \arrow[d, "g'"] \\ A' \arrow[r, "f'"] & B' \end{tikzcd} \qquad \Longrightarrow \qquad F := \begin{pmatrix} \tilde{f} & -\tilde{g} \\ g' & f' \end{pmatrix} : B \times A' \to A \times B'$$

$$\deg(F) = deg(f) + deg(g)$$

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

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

Let $\phi : E \to E'$ be an isogeny of degree d, $\langle P, Q \rangle = E[N]$ with $N^2 > d$ a smooth integer.

$$\textbf{HD-rep} : P, Q, \phi(P), \phi(Q) \longrightarrow \phi$$

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`.

Andrea Basso, Luca De Feo, Pierrick Dartois, Antonin Leroux, Luciano Maino, Giacomo Pope, Damien Robert, and Benjamin Wesolowski, *SQIsign2D-west: The fast, the small, and the safer*, Cryptology ePrint Archive, Paper 2024/760, 2024, `https://eprint.iacr.org/2024/760`.

Andrea Basso, Luciano Maino, and Giacomo Pope, *FESTA: Fast Encryption from a Supersingular Torsion Attacks*, Advances in Cryptology – ASIACRYPT 2023 (Singapore) (Jian Guo and Ron Steinfeld, eds.), Springer Nature Singapore, 2023, pp. 98–126.

References II

- 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*, International Conference on the Theory and Application of Cryptology and Information Security, Springer, 2023, pp. 127–156.
- Max Duparc and Tako Boris Fouotsa, *SQIPrime: A dimension 2 variant of SQISignHD with non-smooth challenge isogenies*, Cryptology ePrint Archive, Paper 2024/773, 2024, `https://eprint.iacr.org/2024/773`.
- Luca De Feo, David Jao, and Jérôme Plût, *Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies*, Journal of Mathematical Cryptology **8** (2014), no. 3, 209–247.

References III

Pierrick Dartois, Antonin Leroux, Damien Robert, and Benjamin Wesolowski, *SQISignHD: new dimensions in cryptography*, Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2024, pp. 3–32.

Edward Eaton, David Jao, Chelsea Komlo, and Youcef Mokrani, *Towards Post-Quantum 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*, Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2023, pp. 282–309.

References IV

Ernst Kani, *The number of curves of genus two with elliptic differentials.*, Walter de Gruyter, Berlin/New York Berlin, New York, 1997.

David Kohel, Kristin Lauter, Christophe Petit, and Jean-Pierre Tignol, *On the quaternion-isogeny path problem*, LMS Journal of Computation and Mathematics **17** (2014), no. A, 418–432.

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

- ———, *SQIsign2D-east: A new signature scheme using 2-dimensional isogenies*, Cryptology ePrint Archive, Paper 2024/771, 2024, https://eprint.iacr.org/2024/771.
- Damien Robert, *Evaluating isogenies in polylogarithmic time*, Cryptology ePrint Archive, Paper 2022/1068, 2022, https://eprint.iacr.org/2022/1068.
- Damien Robert, *Breaking SIDH in polynomial time*, Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2023, pp. 472–503.