Lollipops on unknown degree level structures

Max Duparc

Swissogeny Day 4 : 26th November 2025

Introduction

- Many new PKE security [BF23, BM25, Mor24, KHKL25] rely on *unknown degree level structure*.
- *They claim*: Unknown degree $\implies$ known attacks do not work.

Introduction

- Many new PKE security [BF23, BM25, Mor24, KHKL25] rely on *unknown degree level structure*.
- *They claim*: Unknown degree $\implies$ known attacks do not work.

▶ Reality is more complex.

Introduction

- Many new PKE security [BF23, BM25, Mor24, KHKL25] rely on *unknown degree level structure*.
- *They claim*: Unknown degree $\implies$ known attacks do not work.
  - ▶ Reality is more complex.

In this presentation

1. There exists conditional attacks on unknown degree level structure.
2. This opens interesting research directions.

Introduction

- Many new PKE security [BF23, BM25, Mor24, KHKL25] rely on *unknown degree level structure*.
- *They claim*: Unknown degree $\implies$ known attacks do not work.
  - Reality is more complex.

In this presentation

1. There exists conditional attacks on unknown degree level structure.
2. This opens interesting research directions.

Figure: Today's weapon

Level Structures Isogeny Problem

Definition: Level Structures Isogeny Problem [DFP24]

Let $\phi : E \to E'$ of degree d. $E[N] = \langle P, Q \rangle$, with N smooth[a]. Let $\Gamma \subset \mathrm{GL}_2(\mathbb{Z}_N)$, with $\gamma \in_{\$} \Gamma$:

[a] and $\gcd(d, N) = 1$

Level Structures Isogeny Problem

Definition: Level Structures Isogeny Problem [DFP24]

Let $\phi : E \to E'$ of degree d. $E[N] = \langle P, Q \rangle$, with N smooth[a]. Let $\Gamma \subset \mathrm{GL}_2(\mathbb{Z}_N)$, with $\gamma \in_{\$} \Gamma$:

- The Γ-SSI_d problem:

$$d, \begin{pmatrix} P \\ Q \end{pmatrix} \text{ and } \begin{pmatrix} S \\ T \end{pmatrix} = \gamma \cdot \phi \begin{pmatrix} P \\ Q \end{pmatrix} \xrightarrow{\text{Compute}} \phi$$

[a] and $\gcd(d, N) = 1$

Level Structures Isogeny Problem

Definition: Level Structures Isogeny Problem [DFP24]

Let $\phi : E \to E'$ of degree d. $E[N] = \langle P, Q \rangle$, with N smooth[a]. Let $\Gamma \subset \mathrm{GL}_2(\mathbb{Z}_N)$, with $\gamma \in_\$ \Gamma$:

- The Γ-SSI_d problem:

$$d, \begin{pmatrix} P \\ Q \end{pmatrix} \text{ and } \begin{pmatrix} S \\ T \end{pmatrix} = \gamma \cdot \phi \begin{pmatrix} P \\ Q \end{pmatrix} \xrightarrow{\text{Compute}} \phi$$

- The Γ-SSI problem:

$$\begin{pmatrix} P \\ Q \end{pmatrix} \text{ and } \begin{pmatrix} S \\ T \end{pmatrix} = \gamma \cdot \phi \begin{pmatrix} P \\ Q \end{pmatrix} \xrightarrow{\text{Compute}} \phi$$

[a] and $\gcd(d, N) = 1$

Level Structures Isogeny Problem

Definition: Level Structures Isogeny Problem [DFP24]

Let $\phi : E \to E'$ of degree d. $E[N] = \langle P, Q \rangle$, with N smooth[a]. Let $\Gamma \subset \mathrm{GL}_2(\mathbb{Z}_N)$, with $\gamma \in_\$ \Gamma$:

- The Γ-SSI$_d$ problem:

$$d, \begin{pmatrix} P \\ Q \end{pmatrix} \text{ and } \begin{pmatrix} S \\ T \end{pmatrix} = \gamma \cdot \phi \begin{pmatrix} P \\ Q \end{pmatrix} \xrightarrow{\text{Compute}} \phi$$

- The Γ-SSI problem:

$$\begin{pmatrix} P \\ Q \end{pmatrix} \text{ and } \begin{pmatrix} S \\ T \end{pmatrix} = \gamma \cdot \phi \begin{pmatrix} P \\ Q \end{pmatrix} \xrightarrow{\text{Compute}} \phi$$

[a] and $\gcd(d, N) = 1$

- Defines a hierarchy.

Level Structures Ladder

$$\begin{tikzcd}
\mathrm{GL}_2(\mathbb{Z}_N)\text{-SSI}_d \arrow[r] & \mathrm{GL}_2(\mathbb{Z}_N)\text{-SSI} \\
\left(\begin{smallmatrix} a & c \\ 0 & b \end{smallmatrix}\right)\text{-SSI}_d \arrow[r] \arrow[u] & \left(\begin{smallmatrix} a & c \\ 0 & b \end{smallmatrix}\right)\text{-SSI} \arrow[u] \\
\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)\text{-SSI}_d \arrow[r] \arrow[u] & \left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)\text{-SSI} \arrow[u] \\
\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)\text{-SSI}_d \arrow[r] \arrow[u] & \left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)\text{-SSI} \arrow[u] \\
\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\text{-SSI}_d \arrow[r] \arrow[u] & \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\text{-SSI} \arrow[u]
\end{tikzcd}$$

Figure: Level structure ladder

- Going $\nearrow$ increases the difficulty.

Level Structures Ladder

$$
\begin{tikzcd}
\mathrm{GL}_2(\mathbb{Z}_N)\text{-SSI}_d \arrow[r] & \mathrm{GL}_2(\mathbb{Z}_N)\text{-SSI} \\
\left(\begin{smallmatrix} a & c \\ 0 & b \end{smallmatrix}\right)\text{-SSI}_d \arrow[u] \arrow[r] & \left(\begin{smallmatrix} a & c \\ 0 & b \end{smallmatrix}\right)\text{-SSI} \arrow[u] \\
\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)\text{-SSI}_d \arrow[u] \arrow[r] & \left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)\text{-SSI} \arrow[u] \\
\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)\text{-SSI}_d \arrow[u] \arrow[r] & \left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)\text{-SSI} \arrow[u] \\
\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\text{-SSI}_d \arrow[u] \arrow[r] & \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\text{-SSI} \arrow[u] \arrow[l, bend right]
\end{tikzcd}
$$

Figure: Level structure ladder

- Going $\nearrow$ increases the difficulty.
- We are searching for $\swarrow$ transformations.

Level Structures Ladder

$$
\begin{tikzcd}
\mathrm{GL}_2(\mathbb{Z}_N)\text{-SSI}_d \arrow[r] & \mathrm{GL}_2(\mathbb{Z}_N)\text{-SSI} \\
\begin{pmatrix} a & c \\ 0 & b \end{pmatrix}\text{-SSI}_d \arrow[r] \arrow[u] \arrow[d, dashed, bend right] & \begin{pmatrix} a & c \\ 0 & b \end{pmatrix}\text{-SSI} \arrow[u] \\
\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\text{-SSI}_d \arrow[r] \arrow[u] & \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\text{-SSI} \arrow[u] \\
\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}\text{-SSI}_d \arrow[r] \arrow[u] & \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}\text{-SSI} \arrow[u] \\
\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\text{-SSI}_d \arrow[r] \arrow[u] & \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\text{-SSI} \arrow[u] \arrow[l, bend right]
\end{tikzcd}
$$

Figure: Level structure ladder

- Going $\nearrow$ increases the difficulty.
- We are searching for $\swarrow$ transformations.
  - [DFP24]: $\dashrightarrow$

Level Structures Ladder

$$
\begin{tikzcd}
\mathrm{GL}_2(\mathbb{Z}_N)\text{-SSI}_d \arrow[r] & \mathrm{GL}_2(\mathbb{Z}_N)\text{-SSI} \\
\left(\begin{smallmatrix} a & c \\ 0 & b \end{smallmatrix}\right)\text{-SSI}_d \arrow[r] \arrow[u] \arrow[d, bend right, dashed] & \left(\begin{smallmatrix} a & c \\ 0 & b \end{smallmatrix}\right)\text{-SSI} \arrow[u] \\
\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)\text{-SSI}_d \arrow[r] \arrow[u] \arrow[dd, bend right=60, green] & \left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)\text{-SSI} \arrow[u] \\
\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)\text{-SSI}_d \arrow[r] \arrow[u] \arrow[d, bend right, green] & \left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)\text{-SSI} \arrow[u] \\
\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\text{-SSI}_d \arrow[r] \arrow[u] & \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\text{-SSI} \arrow[u] \arrow[l, bend right]
\end{tikzcd}
$$

Figure: Level structure ladder

- Going $\nearrow$ increases the difficulty.
- We are searching for $\swarrow$ transformations.
  - [DFP24]: $\dashrightarrow$
  - [CV23]: $\longrightarrow$

Level Structures Ladder

$$
\begin{tikzcd}
\mathrm{GL}_2(\mathbb{Z}_N)\text{-SSI}_d \arrow[r] & \mathrm{GL}_2(\mathbb{Z}_N)\text{-SSI} \\
\begin{pmatrix} a & c \\ 0 & b \end{pmatrix}\text{-SSI}_d \arrow[u] \arrow[r] \arrow[d, dashed, bend right] & \begin{pmatrix} a & c \\ 0 & b \end{pmatrix}\text{-SSI} \arrow[u] \\
\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\text{-SSI}_d \arrow[u] \arrow[r] \arrow[dd, bend right, color=green] & \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\text{-SSI} \arrow[u] \\
\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}\text{-SSI}_d \arrow[u] \arrow[r] \arrow[d, bend right, color=green] & \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}\text{-SSI} \arrow[u] \\
\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\text{-SSI}_d \arrow[u] \arrow[r] & \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\text{-SSI} \arrow[u] \arrow[l, bend right]
\end{tikzcd}
$$

Figure: Level structure ladder

- Going $\nearrow$ increases the difficulty.
- We are searching for $\swarrow$ transformations.
  - [DFP24]: $\dashrightarrow$
  - [CV23]: $\longrightarrow$

- Goal: generalise $\longrightarrow$ to the unknown degree setting.

[CV23] Generalised lollipop attack

$$\begin{tikzcd}
E \arrow[d, "\sigma_*\phi"'] & E \arrow[l, "\sigma"] \arrow[l, bend right, "\omega"'] \arrow[d, "\phi"] \\
E'' & E' \arrow[l, "\phi_*\sigma"']
\end{tikzcd}$$

Figure: Generalised lollipop diagram

Generalised lollipop

Let $\omega, \sigma \in \mathrm{End}(E)$ with $\phi_*\sigma$ computable and $\forall \gamma \in \Gamma, (\widehat{\sigma} \circ \omega)\left(\gamma \cdot \binom{P}{Q}\right) = \gamma \cdot \left(\widehat{\sigma} \circ \omega\binom{P}{Q}\right) = \gamma \cdot \mathbf{M}\binom{P}{Q}$.

[CV23] Generalised lollipop attack

$$\begin{tikzcd}
E \arrow[d, "\sigma_*\phi"'] & E \arrow[l, "\sigma"] \arrow[l, bend right, "\omega"'] \arrow[d, "\phi"] \\
E'' & E' \arrow[l, "\phi_*\sigma"']
\end{tikzcd}$$

Figure: Generalised lollipop diagram

Generalised lollipop

Let $\omega, \sigma \in \mathrm{End}(E)$ with $\phi_*\sigma$ computable and $\forall \gamma \in \Gamma, (\widehat{\sigma} \circ \omega)\left(\gamma \cdot \binom{P}{Q}\right) = \gamma \cdot \left(\widehat{\sigma} \circ \omega \binom{P}{Q}\right) = \gamma \cdot \mathbf{M}\binom{P}{Q}$.

We define $\psi = \sigma_*\phi \circ \omega \circ \widehat{\phi} : E' \to E''$ and have that

$$[\deg(\sigma)] \cdot \psi \begin{pmatrix} S \\ T \end{pmatrix} = [d] \cdot \mathbf{M} \cdot \phi_*\sigma \begin{pmatrix} S \\ T \end{pmatrix}$$

Downgrading the level structure

Key Observation

In the unknown degree setting, the generalised lollipop still downgrades the level structure.

$$[d^{-1}] \cdot \psi\begin{pmatrix} S \\ T \end{pmatrix} = [\deg(\sigma)^{-1}] \cdot \mathbf{M} \cdot \phi_* \sigma \begin{pmatrix} S \\ T \end{pmatrix}$$

Downgrading the level structure

Key Observation

In the unknown degree setting, the generalised lollipop still downgrades the level structure.

$$[d^{-1}] \cdot \psi \begin{pmatrix} S \\ T \end{pmatrix} = [\deg(\sigma)^{-1}] \cdot \mathbf{M} \cdot \phi_* \sigma \begin{pmatrix} S \\ T \end{pmatrix}$$

$$\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)\text{-SSI}(\phi) \xrightarrow{\textit{reduction}^*} \begin{pmatrix} d^{-1} & 0 \\ 0 & d^{-1} \end{pmatrix}\text{-SSI}(\psi)$$

Note: reduction is not perfect and eats part of ϕ oriented by $\widehat{\sigma} \circ \omega$.

Downgrading the level structure

Key Observation

In the unknown degree setting, the generalised lollipop still downgrades the level structure.

$$[d^{-1}] \cdot \psi\begin{pmatrix} S \\ T \end{pmatrix} = [\deg(\sigma)^{-1}] \cdot \mathbf{M} \cdot \phi_*\sigma\begin{pmatrix} S \\ T \end{pmatrix}$$

$$\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)\text{-SSI}(\phi) \xrightarrow{\textit{reduction}^*} \begin{pmatrix} d^{-1} & 0 \\ 0 & d^{-1} \end{pmatrix}\text{-SSI}(\psi)$$

- How hard is $\begin{pmatrix} d^{-1} & 0 \\ 0 & d^{-1} \end{pmatrix}$-SSI ?

Note: reduction is not perfect and eats part of ϕ oriented by $\widehat{\sigma} \circ \omega$.

Erased degree level structure

Definition: $\begin{pmatrix} d^{-1} & 0 \\ 0 & d^{-1} \end{pmatrix}$-SSI problem

$\psi : E' \to E''$ is a *cyclic* isogeny of degree d^2, and let $E'[N] = \langle S, T \rangle$ be a basis of $E'[N]$. We define the *erased degree level structure* as:

$$\begin{pmatrix} S \\ T \end{pmatrix} \text{ and } \begin{pmatrix} d^{-1} & 0 \\ 0 & d^{-1} \end{pmatrix} \cdot \psi \begin{pmatrix} S \\ T \end{pmatrix} \xrightarrow{\text{Compute}} \psi$$

[0]For simplicity, we take $\omega = id$.

Erased degree level structure

Definition: $\begin{pmatrix} d^{-1} & 0 \\ 0 & d^{-1} \end{pmatrix}$-SSI problem

$\psi : E' \to E''$ is a *cyclic* isogeny of degree d^2, and let $E'[N] = \langle S, T \rangle$ be a basis of $E'[N]$. We define the *erased degree level structure* as:

$$\begin{pmatrix} S \\ T \end{pmatrix} \text{ and } \begin{pmatrix} d^{-1} & 0 \\ 0 & d^{-1} \end{pmatrix} \cdot \psi \begin{pmatrix} S \\ T \end{pmatrix} \xrightarrow{\text{Compute}} \psi$$

- Trivial attacks do not work.
  - Prevents recovering d via any pairing.

$$e_N \left([d^{-1}]\psi(S), [d^{-1}]\psi(T) \right) = e_N(S, T)$$

[0] For simplicity, we take $\omega = id$.

Erased degree level structure

Definition: $\begin{pmatrix} d^{-1} & 0 \\ 0 & d^{-1} \end{pmatrix}$**-SSI problem**

$\psi : E' \to E''$ is a *cyclic* isogeny of degree d^2, and let $E'[N] = \langle S, T \rangle$ be a basis of $E'[N]$. We define the *erased degree level structure* as:

$$\begin{pmatrix} S \\ T \end{pmatrix} \text{ and } \begin{pmatrix} d^{-1} & 0 \\ 0 & d^{-1} \end{pmatrix} \cdot \psi \begin{pmatrix} S \\ T \end{pmatrix} \xrightarrow{\text{Compute}} \psi$$

- Trivial attacks do not work.
  - Prevents recovering d via any pairing.

$$e_N \left([d^{-1}]\psi(S), [d^{-1}]\psi(T) \right) = e_N(S, T)$$

  - It is an isogeny that cannot be interpolated.

$$[d^{-1}]\psi \text{ is an isogeny of degree } (1 + k_{N,d} N)^2 \gg N^2$$

[0] For simplicity, we take $\omega = id$.

Unknown degree vs. Unknown degree

- Though d is unknown, its distribution $\mathcal{D}$ is known!

Unknown degree vs. Unknown degree

- Though d is unknown, its distribution $\mathcal{D}$ is known!
  - If not $\implies$ RUN !

Unknown degree vs. Unknown degree

- Though d is unknown, its distribution $\mathcal{D}$ is known!
  - If not $\implies$ RUN !

Properties of $\mathcal{D}$

- $\text{size}(\mathcal{D}) = |\{d \in \mathcal{D}\}|$
- $\text{supp}(\mathcal{D}) = \{q \text{ prime s.t. } \exists d \in \mathcal{D} \text{ s.t. } q|d\}$

Unknown degree vs. Unknown degree

- Though d is unknown, its distribution $\mathcal{D}$ is known!
  - If not $\implies$ RUN !

Properties of $\mathcal{D}$

- $\mathrm{size}(\mathcal{D}) = |\{d \in \mathcal{D}\}|$
- $\mathrm{supp}(\mathcal{D}) = \{q \text{ prime s.t. } \exists d \in \mathcal{D} \text{ s.t. } q|d\}$
- $\mathrm{ht}_q(\mathcal{D}) = \max\{e \text{ s.t. } \exists d \in \mathcal{D} \text{ s.t. } q^e|d\}$
- $\mathrm{lcm}(\mathcal{D}) = \{D \in \mathbb{N} \text{ s.t. } \forall d \in \mathcal{D}, d|D\}$

Unknown degree vs. Unknown degree

- Though d is unknown, its distribution $\mathcal{D}$ is known!
  - If not $\implies$ RUN !

Properties of $\mathcal{D}$

- $\mathrm{size}(\mathcal{D}) = |\{d \in \mathcal{D}\}|$
- $\mathrm{supp}(\mathcal{D}) = \{q \text{ prime s.t. } \exists d \in \mathcal{D} \text{ s.t. } q|d\}$
- $\mathrm{ht}_q(\mathcal{D}) = \max\{e \text{ s.t. } \exists d \in \mathcal{D} \text{ s.t. } q^e|d\}$
- $\mathrm{lcm}(\mathcal{D}) = \{D \in \mathbb{N} \text{ s.t. } \forall d \in \mathcal{D}, d|D\}$

- For isogenies: $\mathrm{size}(\mathcal{D}) = O(2^\lambda)$ and $\mathrm{ht}(\mathcal{D}) = \max_{q \in \mathrm{supp}(\mathcal{D})}\{\mathrm{ht}_q(\mathcal{D})\} = \mathrm{poly}(\lambda)$.

Unknown degree vs. Unknown degree

- Though d is unknown, its distribution $\mathcal{D}$ is known!
  - If not $\implies$ RUN !

Properties of $\mathcal{D}$

- $\text{size}(\mathcal{D}) = |\{d \in \mathcal{D}\}|$
- $\text{supp}(\mathcal{D}) = \{q \text{ prime s.t. } \exists d \in \mathcal{D} \text{ s.t. } q|d\}$
- $\text{ht}_q(\mathcal{D}) = \max\{e \text{ s.t. } \exists d \in \mathcal{D} \text{ s.t. } q^e|d\}$
- $\text{lcm}(\mathcal{D}) = \{D \in \mathbb{N} \text{ s.t. } \forall d \in \mathcal{D}, d|D\}$

- For isogenies: $\text{size}(\mathcal{D}) = O(2^\lambda)$ and $\text{ht}(\mathcal{D}) = \max_{q \in \text{supp}(\mathcal{D})}\{\text{ht}_q(\mathcal{D})\} = \text{poly}(\lambda)$.
- $\mathcal{D}$ has **small support** if $|\text{supp}(\mathcal{D})| = \text{poly}(\lambda) \implies \text{lcm}(\mathcal{D}) = \exp(\lambda)$

Attacking the erased degree level structure

Theorem

For $d \in \mathcal{D}$ small supp and for N big-enough

$$\text{solving } \begin{pmatrix} d^{-1} & 0 \\ 0 & d^{-1} \end{pmatrix}\text{-SSI is easy}$$

Attacking the erased degree level structure

Theorem

For $d \in \mathcal{D}$ small supp and for N big-enough

$$\text{solving } \begin{pmatrix} d^{-1} & 0 \\ 0 & d^{-1} \end{pmatrix}\text{-SSI is easy}$$

$$[d^{-1}]\psi(E[N])$$

Attacking the erased degree level structure

Theorem

For $d \in \mathcal{D}$ small supp and for N big-enough

$$\text{solving } \begin{pmatrix} d^{-1} & 0 \\ 0 & d^{-1} \end{pmatrix}\text{-SSI is easy}$$

$$[d^{-1}]\psi(E[N]) \xrightarrow{[\mathrm{lcm}(\mathcal{D})]} [\mathrm{lcm}(\mathcal{D})/d]\psi(E[N])$$

Attacking the erased degree level structure

Theorem

For $d \in \mathcal{D}$ small supp and for N big-enough

$$\text{solving } \begin{pmatrix} d^{-1} & 0 \\ 0 & d^{-1} \end{pmatrix}\text{-SSI is easy}$$

$$[d^{-1}]\psi(E[N]) \xrightarrow{[\mathrm{lcm}(\mathcal{D})]} [\mathrm{lcm}(\mathcal{D})/d]\psi(E[N])$$

- It is of *known* degree $\mathrm{lcm}(\mathcal{D})^2$.

Attacking the erased degree level structure

Theorem

For $d \in \mathcal{D}$ small supp and for N big-enough

$$\text{solving } \begin{pmatrix} d^{-1} & 0 \\ 0 & d^{-1} \end{pmatrix}\text{-SSI is easy}$$

$$[d^{-1}]\psi(E[N]) \xrightarrow{[\mathrm{lcm}(\mathcal{D})]} [\mathrm{lcm}(\mathcal{D})/d]\psi(E[N])$$

- It is of *known* degree $\mathrm{lcm}(\mathcal{D})^2$.
- If $N \geq \mathrm{lcm}(\mathcal{D})$, it can be interpolated.

Attacking the erased degree level structure (rational)

- small supp. $\implies$ testing each $q_i \in \operatorname{supp}(\mathcal{D})$ gives some info.

Attacking the erased degree level structure (rational)

- small supp. $\implies$ testing each $q_i \in \mathrm{supp}(\mathcal{D})$ gives some info.
- *If supp*$(\mathcal{D})$ *rational.* $\forall q_i \in \mathrm{supp}(\mathcal{D})$

$$\begin{cases} [\widehat{\mathrm{lcm}(\mathcal{D})/d}]\psi(E''[q_i]) = 0 & \implies q_i^{\mathrm{ht}_{q_i}(\mathcal{D})} \text{ does not divide } d \\ [\widehat{\mathrm{lcm}(\mathcal{D})/d}]\psi(E''[q_i]) \neq 0 & \implies [\widehat{\mathrm{lcm}(\mathcal{D})/d}]\psi(E''[q_i]) = \ker(\psi)[q_i] \end{cases}$$

Attacking the erased degree level structure (rational)

- small supp. $\implies$ testing each $q_i \in \mathrm{supp}(\mathcal{D})$ gives some info.
- *If supp*$(\mathcal{D})$ *rational.* $\forall q_i \in \mathrm{supp}(\mathcal{D})$

$$\begin{cases} [\widehat{\mathrm{lcm}(\mathcal{D})/d}]\psi(E''[q_i]) = 0 & \implies q_i^{\mathrm{ht}_{q_i}(\mathcal{D})} \text{ does not divide } d \\ [\widehat{\mathrm{lcm}(\mathcal{D})/d}]\psi(E''[q_i]) \neq 0 & \implies [\widehat{\mathrm{lcm}(\mathcal{D})/d}]\psi(E''[q_i]) = \ker(\psi)[q_i] \end{cases}$$

  - We have recovered $\ker(\psi)[d_0]$, with $d = d_0 d_1$.

Attacking the erased degree level structure (rational)

- small supp. $\implies$ testing each $q_i \in \mathrm{supp}(\mathcal{D})$ gives some info.
- *If supp*$(\mathcal{D})$ *rational.* $\forall q_i \in \mathrm{supp}(\mathcal{D})$

$$\begin{cases} [\mathrm{lcm}\widehat{(\mathcal{D})/}d]\psi(E''[q_i]) = 0 & \implies q_i^{\mathrm{ht}_{q_i}(\mathcal{D})} \text{ does not divide } d \\ [\mathrm{lcm}\widehat{(\mathcal{D})/}d]\psi(E''[q_i]) \neq 0 & \implies [\mathrm{lcm}\widehat{(\mathcal{D})/}d]\psi(E''[q_i]) = \ker(\psi)[q_i] \end{cases}$$

  - We have recovered $\ker(\psi)[d_0]$, with $d = d_0 d_1$.
  - By repeating the process, we recover a chain corresponding to ψ.

Attacking the erased degree level structure (rational)

- small supp. $\implies$ testing each $q_i \in \mathrm{supp}(\mathcal{D})$ gives some info.
- *If supp*$(\mathcal{D})$ *rational*. $\forall q_i \in \mathrm{supp}(\mathcal{D})$

$$\begin{cases} [\widehat{\mathrm{lcm}(\mathcal{D})/d}]\psi(E''[q_i]) = 0 & \implies q_i^{\mathrm{ht}_{q_i}(\mathcal{D})} \text{ does not divide } d \\ [\widehat{\mathrm{lcm}(\mathcal{D})/d}]\psi(E''[q_i]) \neq 0 & \implies [\widehat{\mathrm{lcm}(\mathcal{D})/d}]\psi(E''[q_i]) = \ker(\psi)[q_i] \end{cases}$$

  - We have recovered $\ker(\psi)[d_0]$, with $d = d_0 d_1$.
  - By repeating the process, we recover a chain corresponding to ψ.
- *In the irrational case*, we can do this prime testing using the `IsogenyDiv` algo [MW25].

Attacking the erased degree level structure (rational)

- small supp. $\implies$ testing each $q_i \in \mathrm{supp}(\mathcal{D})$ gives some info.
- *If supp*$(\mathcal{D})$ *rational*. $\forall q_i \in \mathrm{supp}(\mathcal{D})$

$$\begin{cases} [\widehat{\mathrm{lcm}(\mathcal{D})/d}]\psi(E''[q_i]) = 0 & \implies q_i^{\mathrm{ht}_{q_i}(\mathcal{D})} \text{ does not divide } d \\ [\widehat{\mathrm{lcm}(\mathcal{D})/d}]\psi(E''[q_i]) \neq 0 & \implies [\widehat{\mathrm{lcm}(\mathcal{D})/d}]\psi(E''[q_i]) = \ker(\psi)[q_i] \end{cases}$$

  - We have recovered $\ker(\psi)[d_0]$, with $d = d_0 d_1$.
  - By repeating the process, we recover a chain corresponding to ψ.
- *In the irrational case*, we can do this prime testing using the `IsogenyDiv` algo [MW25].

$$[\mathrm{lcm}(\mathcal{D})/d]\psi(E[N]) \xrightarrow{\texttt{IsogenyDiv}} [d/d]\psi(E[N])$$

Cryptanalytic consequences

By design: Rationality $\implies$ small support.

Cryptanalytic consequences

By design: Rationality $\implies$ small support.

- $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$-SSI: It is technically possible to backdoor terSIDH. (using special basis and small endomorphism).
  - The countermeasures in [BF23, §3.4] are important !

Cryptanalytic consequences

By design: Rationality $\implies$ small support.

- $\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)$-SSI: It is technically possible to backdoor terSIDH. (using special basis and small endomorphism).
  - The countermeasures in [BF23, §3.4] are important !
- $\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$-SSI: Given $\phi : E_0 \to E$, if the distribution has small supp, then we can recover ϕ independently of the shape of N.
  - Can be used constructively.

Cryptanalytic consequences

By design: Rationality $\implies$ small support.

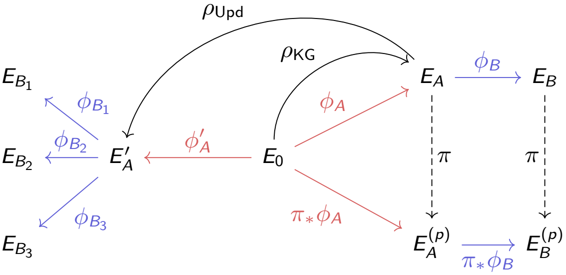
- $\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)$-SSI: It is technically possible to backdoor terSIDH. (using special basis and small endomorphism).
  - The countermeasures in [BF23, §3.4] are important !
- $\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$-SSI: Given $\phi : E_0 \to E$, if the distribution has small supp, then we can recover ϕ independently of the shape of N.
  - Can be used constructively.
- For POKE et al. [BM25, KHKL25], no attacks (yet). (As $\mathrm{lcm}(\mathcal{D}) \geq 2^{\vartheta(2^{\lambda})}$).
  - Their security comes more from $\mathcal{D}$ than from Γ.

Construct using lollipops

- Can instantiate SETA [DDF+21]-like trapdoor on $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$-SSI.

Construct using lollipops

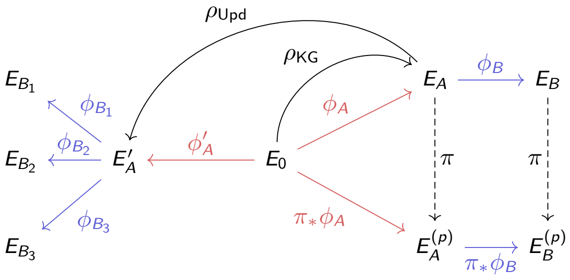
- Can instantiate SETA [DDF+21]-like trapdoor on $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$-SSI.
- Can be applied to construct a more efficient SILBE UPKE [DFV24].
  - + Base prime p about 2.7x smaller.
  - + Just need $(3,3)$ and $(3,3,3,3)$ HD-isogenies.
  - + Should provide a 2^{32}x speed-up on original.
  - - but p still 4700 bits for $\lambda = 128$.



Simplified overview of SILBE

Construct using lollipops

- Can instantiate SETA [DDF+21]-like trapdoor on $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$-SSI.
- Can be applied to construct a more efficient SILBE UPKE [DFV24].
  - + Base prime p about 2.7x smaller.
  - + Just need $(3,3)$ and $(3,3,3,3)$ HD-isogenies.
  - + Should provide a 2^{32}x speed-up on original.
  - - but p still 4700 bits for $\lambda = 128$.
- ▶ Giant step in the direction of efficient UPKE.
  - ▶ Work is still needed.



Simplified overview of SILBE

Is $\begin{pmatrix} d^{-1} & 0 \\ 0 & d^{-1} \end{pmatrix}$-SSI more profound ?

Level structure as partial maps

Let $\mathcal{SS}$ be the supersingular category. Assume $N = \ell^e$.

$$\eta : \mathrm{Hom}(E_1, E_2) \rightharpoonup \mathrm{Hom}(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}_{\ell^e}$$
$$\eta(\phi) = \phi \otimes \sqrt{\deg(\phi)}$$

Is $\begin{pmatrix} d^{-1} & 0 \\ 0 & d^{-1} \end{pmatrix}$-SSI more profound ?

Level structure as partial maps

Let $\mathcal{SS}$ be the supersingular category. Assume $N = \ell^e$.

$$\eta : \mathrm{Hom}(E_1, E_2) \rightharpoonup \mathrm{Hom}(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}_{\ell^e}$$

$$\eta(\phi) = \phi \otimes \sqrt{\deg(\phi)}$$

$$\begin{pmatrix} d^{-1} & 0 \\ 0 & d^{-1} \end{pmatrix}\text{-SSI} \iff \text{compute preimage of } \eta$$

Is $\begin{pmatrix} d^{-1} & 0 \\ 0 & d^{-1} \end{pmatrix}$-SSI more profound ?

Level structure as partial maps

Let $\mathcal{SS}$ be the supersingular category. Assume $N = \ell^e$.

$$\eta : \mathrm{Hom}(E_1, E_2) \rightharpoonup \mathrm{Hom}(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}_{\ell^e}$$
$$\eta(\phi) = \phi \otimes \sqrt{\deg(\phi)}$$

$$\begin{pmatrix} d^{-1} & 0 \\ 0 & d^{-1} \end{pmatrix}\text{-SSI} \iff \text{compute preimage of } \eta$$

η is stable. Can go to the (inverse) limit

Is $\begin{pmatrix} d^{-1} & 0 \\ 0 & d^{-1} \end{pmatrix}$-SSI more profound ?

Level structure as partial maps

Let $\mathcal{SS}$ be the supersingular category. Assume $N = \ell^e$.

$$\eta : \mathrm{Hom}(E_1, E_2) \rightharpoonup \mathrm{Hom}(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}_{\ell^e}$$
$$\eta(\phi) = \phi \otimes \sqrt{\deg(\phi)}$$

$$\begin{pmatrix} d^{-1} & 0 \\ 0 & d^{-1} \end{pmatrix}\text{-SSI} \iff \text{compute preimage of } \eta$$

η is stable. Can go to the (inverse) limit

$$\eta : \mathrm{Hom}(E_1, E_2) \rightharpoonup \mathrm{Hom}(E_1, E_2) \otimes_{\mathbb{Z}} \mathbf{Z}_{\ell} \simeq \mathrm{Hom}(T_{\ell}(E_1), T_{\ell}(E_2))$$

Is $\begin{pmatrix} d^{-1} & 0 \\ 0 & d^{-1} \end{pmatrix}$-SSI more profound ?

Level structure as partial maps

Let $\mathcal{SS}$ be the supersingular category. Assume $N = \ell^e$.

$$\eta : \mathrm{Hom}(E_1, E_2) \rightharpoonup \mathrm{Hom}(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}_{\ell^e}$$

$$\eta(\phi) = \phi \otimes \sqrt{\deg(\phi)}$$

$$\begin{pmatrix} d^{-1} & 0 \\ 0 & d^{-1} \end{pmatrix}\text{-SSI} \iff \text{compute preimage of } \eta$$

η is stable. Can go to the (inverse) limit

$$\eta : \mathrm{Hom}(E_1, E_2) \rightharpoonup \mathrm{Hom}(E_1, E_2) \otimes_{\mathbb{Z}} \mathbf{Z}_\ell \simeq \mathrm{Hom}(T_\ell(E_1), T_\ell(E_2))$$

- Can we study $\begin{pmatrix} d^{-1} & 0 \\ 0 & d^{-1} \end{pmatrix}$-SSI using algebraic homology ?

Conclusion

$$
\begin{tikzcd}
\mathrm{GL}_2(\mathbb{Z}_N)\text{-SSI}_d \arrow[r] & \mathrm{GL}_2(\mathbb{Z}_N)\text{-SSI} \\
\left(\begin{smallmatrix} a & c \\ 0 & b \end{smallmatrix}\right)\text{-SSI}_d \arrow[r] \arrow[u] \arrow[d, dashed, bend right] & \left(\begin{smallmatrix} a & c \\ 0 & b \end{smallmatrix}\right)\text{-SSI} \arrow[u] \\
\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)\text{-SSI}_d \arrow[r] \arrow[u] \arrow[dd, bend right] & \left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)\text{-SSI} \arrow[u] \arrow[dd, bend left] \\
\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)\text{-SSI}_d \arrow[r] \arrow[u] \arrow[d, bend right] & \left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)\text{-SSI} \arrow[u] \arrow[d, bend left] \\
\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\text{-SSI}_d \arrow[r] \arrow[u] & \begin{pmatrix} d^{-1} & 0 \\ 0 & d^{-1} \end{pmatrix}\text{-SSI} \arrow[u] \arrow[l, dotted, bend right]
\end{tikzcd}
$$

Figure: NEW Level structure ladder

Lollipops are boomerang !

Happy to discuss your comments & questions !

References I

- Andrea Basso and Tako Boris Fouotsa, *New SIDH countermeasures for a more efficient key exchange*, ASIACRYPT 2023, Part VIII (Jian Guo and Ron Steinfeld, eds.), LNCS, vol. 14445, Springer, Singapore, December 2023, pp. 208–233.
- Andrea Basso and Luciano Maino, *POKÉ: A compact and efficient PKE from higher-dimensional isogenies*, EUROCRYPT 2025, Part II (Serge Fehr and Pierre-Alain Fouque, eds.), LNCS, vol. 15602, Springer, Cham, May 2025, pp. 94–123.
- Wouter Castryck and Frederik Vercauteren, *A polynomial time attack on instances of M-SIDH and FESTA*, ASIACRYPT 2023, Part VII (Jian Guo and Ron Steinfeld, eds.), LNCS, vol. 14444, Springer, Singapore, December 2023, pp. 127–156.
- Luca De Feo, Cyprien Delpech de Saint Guilhem, Tako Boris Fouotsa, Péter Kutas, Antonin Leroux, Christophe Petit, Javier Silva, and Benjamin Wesolowski, *Séta: Supersingular encryption from torsion attacks*, ASIACRYPT 2021, Part IV (Mehdi Tibouchi and Huaxiong Wang, eds.), LNCS, vol. 13093, Springer, Cham, December 2021, pp. 249–278.

References II

- Luca De Feo, Tako Boris Fouotsa, and Lorenz Panny, *Isogeny problems with level structure*, EUROCRYPT 2024, Part VII (Marc Joye and Gregor Leander, eds.), LNCS, vol. 14657, Springer, Cham, May 2024, pp. 181–204.
- Max Duparc, Tako Boris Fouotsa, and Serge Vaudenay, *SILBE: An updatable public key encryption scheme from lollipop attacks*, SAC 2024, Part I (Maria Eichlseder and Sébastien Gambs, eds.), LNCS, vol. 15516, Springer, Cham, August 2024, pp. 151–177.
- Hyeonhak Kim, Seokhie Hong, Suhri Kim, and Sangjin Lee, *INKE: Fast isogeny-based PKE using intermediate curves*, Cryptology ePrint Archive, Report 2025/1458, 2025.
- Tomoki Moriya, *LIT-SiGamal: An efficient isogeny-based PKE based on a LIT diagram*, Cryptology ePrint Archive, Report 2024/521, 2024.
- Arthur Herlédan Le Merdy and Benjamin Wesolowski, *The supersingular endomorphism ring problem given one endomorphism*, CiC **2** (2025), no. 1, 6.