The Deuring Correspondence in isogeny-based cryptography: SQISign and new isogeny problems.

Antonin Leroux
International Workshop on Post-Quantum Cryptography, 11/12/2021

DGA, Ecole Polytechnique, Institut Polytechnique de Paris, Inria Saclay
Generic Isogeny feature: compact keys (unless specific tradeoffs).
Isogeny-based Signatures

Generic Isogeny feature: compact keys (unless specific tradeoffs).

- [Yoo+17] Digital Signature: Based on SIDH,
  Multiple rounds ⇒ long sig, slow.

---

Yoo et al. “A post-quantum digital signature scheme based on supersingular isogenies”
Isogeny-based Signatures

Generic Isogeny feature: compact keys (unless specific tradeoffs).

- [Yoo+17] Digital Signature: Based on SIDH,
  Multiple rounds ⇒ long sig, slow.
- [GPS17] GPS signature: Based on quaternions ⇒ weaker assumption,
  Multiple rounds ⇒ long sig, no implem.

Galbraith, Petit, and Silva “Identification Protocols and Signature Schemes Based on Supersingular Isogeny Problems”
Isogeny-based Signatures

Generic Isogeny feature: compact keys (unless specific tradeoffs).

- [Yoo+17] Digital Signature: Based on SIDH, Multiple rounds $\Rightarrow$ long sig, slow.
- [GPS17] GPS signature: Based on quaternions $\Rightarrow$ weaker assumption, Multiple rounds $\Rightarrow$ long sig, no implem.
- [DG19] SeaSign: Based on CSIDH, Multiple rounds $\Rightarrow$ slow, size tradeoffs.

De Feo and Galbraith “SeaSign: Compact isogeny signatures from class group actions”
Isogeny-based Signatures

Generic Isogeny feature: compact keys (unless specific tradeoffs).

- [Yoo+17] Digital Signature: Based on SIDH, Multiple rounds $\Rightarrow$ long sig, slow.
- [GPS17] GPS signature: Based on quaternions $\Rightarrow$ weaker assumption, Multiple rounds $\Rightarrow$ long sig, no implem.
- [DG19] SeaSign: Based on CSIDH, Multiple rounds $\Rightarrow$ slow, size tradeoffs.
- [BKV19] CSI-FiSh: Based on CSIDH + precomp. $\Rightarrow$ bad scaling, similar to SeaSign with improved efficiency and sizes.

Beullens, Kleinjung, and Vercauteren “CSI-FiSh: Efficient isogeny based signatures through class group computations”
Signature:\(^1\) one round, high soundness from Deuring Correspondence.

---

\(^1\)"SQISign: Compact Post-Quantum Signatures from Isogenies and Quaternions", L. De Feo, D. Kohel, A. Leroux, C. Petit and B. Wesolowski, ASIACRYPT 2020
Signature:¹ one round, high soundness from Deuring Correspondence. Most compact PQ signature scheme: PK + Signature combined $5 \times$ smaller than Falcon (most compact NIST Round 3 candidate).

¹"SQISign: Compact Post-Quantum Signatures from Isogenies and Quaternions", L. De Feo, D. Kohel, A. Leroux, C. Petit and B. Wesolowski, ASIACRYPT 2020
SQISign: Short Quaternion Isogeny Signature

Signature: one round, high soundness from Deuring Correspondence. Most compact PQ signature scheme: PK + Signature combined $5 \times$ smaller than Falcon (most compact NIST Round 3 candidate).

<table>
<thead>
<tr>
<th>Secret Key (bytes)</th>
<th>Public Key (bytes)</th>
<th>Signature (bytes)</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>64</td>
<td>204</td>
<td>NIST-1</td>
</tr>
</tbody>
</table>

$^{1}$"SQISign: Compact Post-Quantum Signatures from Isogenies and Quaternions", L. De Feo, D. Kohel, A. Leroux, C. Petit and B. Wesolowski, ASIACRYPT 2020
SQISign: Short Quaternion Isogeny Signature

Signature: one round, high soundness from Deuring Correspondence. Most compact PQ signature scheme: PK + Signature combined 5× smaller than Falcon (most compact NIST Round 3 candidate).

<table>
<thead>
<tr>
<th>Secret Key (bytes)</th>
<th>Public Key (bytes)</th>
<th>Signature (bytes)</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>64</td>
<td>204</td>
<td>NIST-1</td>
</tr>
</tbody>
</table>

Efficient verification and reasonably efficient signature.

1"SQISign: Compact Post-Quantum Signatures from Isogenies and Quaternions", L. De Feo, D. Kohel, A. Leroux, C. Petit and B. Wesolowski, ASIACRYPT 2020
**SQISign: Short Quaternion Isogeny Signature**

Signature: one round, high soundness from Deuring Correspondence. Most compact PQ signature scheme: PK + Signature combined 5× smaller than Falcon (most compact NIST Round 3 candidate).

<table>
<thead>
<tr>
<th>Secret Key (bytes)</th>
<th>Public Key (bytes)</th>
<th>Signature (bytes)</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>64</td>
<td>204</td>
<td>NIST-1</td>
</tr>
</tbody>
</table>

Efficient verification and reasonably efficient signature.

<table>
<thead>
<tr>
<th>Keygen</th>
<th>Sign</th>
<th>Verify</th>
</tr>
</thead>
<tbody>
<tr>
<td>ms</td>
<td>575</td>
<td>2,279</td>
</tr>
</tbody>
</table>

¹"SQISign: Compact Post-Quantum Signatures from Isogenies and Quaternions", L. De Feo, D. Kohel, A. Leroux, C. Petit and B. Wesolowski, ASIACRYPT 2020
 SQISign: Short Quaternion Isogeny Signature

Signature: \(^1\) one round, high soundness from Deuring Correspondence. Most compact PQ signature scheme: PK + Signature combined \(5 \times\) smaller than Falcon (most compact NIST Round 3 candidate).

<table>
<thead>
<tr>
<th>Secret Key (bytes)</th>
<th>Public Key (bytes)</th>
<th>Signature (bytes)</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>64</td>
<td>204</td>
<td>NIST-1</td>
</tr>
</tbody>
</table>

Efficient verification and reasonably efficient signature.

<table>
<thead>
<tr>
<th></th>
<th>Keygen</th>
<th>Sign</th>
<th>Verify</th>
</tr>
</thead>
<tbody>
<tr>
<td>ms</td>
<td>575</td>
<td>2,279</td>
<td>42</td>
</tr>
</tbody>
</table>

New security assumption.

\(^1\)"SQISign: Compact Post-Quantum Signatures from Isogenies and Quaternions", L. De Feo, D. Kohel, A. Leroux, C. Petit and B. Wesolowski, ASIACRYPT 2020
The Deuring Correspondence
The Quaternion algebra $H(a, b)$ is

$$H(a, b) = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + k\mathbb{Q} \text{ with } i^2 = a, j^2 = b$$

\(^2\)similary for the right order $\mathcal{O}_R(I)$
The Quaternion algebra $H(a, b)$ is

$$H(a, b) = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + k\mathbb{Q} \text{ with } i^2 = a, j^2 = b$$

Fractional ideals are $\mathbb{Z}$-lattices of rank 4 inside $H(a, b)$

$$I = \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z} + \alpha_3\mathbb{Z} + \alpha_4\mathbb{Z}$$

The Reduced norm $n(I) = \{\gcd(n(\alpha)), \alpha \in I\}$

\[\text{similary for the right order } \mathcal{O}_R(I)\]
The Quaternion algebra $H(a, b)$ is

$$H(a, b) = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + k\mathbb{Q} \text{ with } i^2 = a, j^2 = b$$

Fractional ideals are $\mathbb{Z}$-lattices of rank 4 inside $H(a, b)$

$$I = \alpha_1 \mathbb{Z} + \alpha_2 \mathbb{Z} + \alpha_3 \mathbb{Z} + \alpha_4 \mathbb{Z}$$

The Reduced norm $n(I) = \{\gcd(n(\alpha)), \alpha \in I\}$

An order $\mathcal{O}$ is an ideal which is also a ring, it is maximal when not contained in another order.

\[^2\text{similary for the right order } \mathcal{O}_R(I)\]
The **Quaternion algebra** $H(a, b)$ is

$$H(a, b) = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + k\mathbb{Q} \text{ with } i^2 = a, j^2 = b$$

**Fractional ideals** are $\mathbb{Z}$-lattices of rank 4 inside $H(a, b)$

$$I = \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z} + \alpha_3\mathbb{Z} + \alpha_4\mathbb{Z}$$

The **Reduced norm** $n(I) = \{\gcd(n(\alpha)), \alpha \in I\}$

An **order** $\mathcal{O}$ is an **ideal** which is also a **ring**, it is **maximal** when not contained in another order.

The **(maximal) left order** $^2 \mathcal{O}_L(I)$ of an **ideal** is

$$\mathcal{O}_L(I) = \{\alpha \in H(a, b), \alpha I \subset I\}$$

$^2$similary for the **right order** $\mathcal{O}_R(I)$
<table>
<thead>
<tr>
<th>Supersingular elliptic curves over $\mathbb{F}_{p^2}$</th>
<th>Maximal Orders in $\mathcal{A}_p$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$E$</td>
<td>$\mathcal{O} \cong \text{End}(E)$</td>
</tr>
<tr>
<td>Isogeny with $\varphi : E \to E_1$</td>
<td>Ideal $I_\varphi$ left $\mathcal{O}$-ideal and right $\mathcal{O}_1$-ideal</td>
</tr>
<tr>
<td>Degree $\text{deg}(\varphi)$</td>
<td>Norm $n(I_\varphi)$</td>
</tr>
<tr>
<td>Supersingular elliptic curves over $\mathbb{F}_{p^2}$</td>
<td>Maximal Orders in $\mathcal{A}_p$</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>$E$</td>
<td>$\mathcal{O} \cong \text{End}(E)$</td>
</tr>
<tr>
<td>Isogeny with $\varphi : E \rightarrow E_1$</td>
<td>Ideal $I_\varphi$ left $\mathcal{O}$-ideal and right $\mathcal{O}_1$-ideal</td>
</tr>
<tr>
<td>Degree $\deg(\varphi)$</td>
<td>Norm $n(I_\varphi)$</td>
</tr>
</tbody>
</table>

**Example:** $p \equiv 3 \mod 4$, $\mathcal{A}_p = H(-1, -p)$. 
### The Deuring Correspondence

<table>
<thead>
<tr>
<th>Supersingular elliptic curves over $\mathbb{F}_{p^2}$</th>
<th>Maximal Orders in $\mathcal{A}_p$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$E$</td>
<td>$\mathcal{O} \cong \text{End}(E)$</td>
</tr>
<tr>
<td>Isogeny with $\varphi : E \to E_1$</td>
<td>Ideal $I_\varphi$ left $\mathcal{O}$-ideal and right $\mathcal{O}_1$-ideal</td>
</tr>
<tr>
<td>Degree $\deg(\varphi)$</td>
<td>Norm $n(I_\varphi)$</td>
</tr>
</tbody>
</table>

**Example:** $p \equiv 3 \mod 4$, $\mathcal{A}_p = H(-1, -p)$.  

$$E_0 : y^2 = x^3 + x$$

$$\text{End}(E_0) = \langle 1, \iota, \frac{i + \pi}{2}, \frac{1 + i\pi}{2} \rangle \cong \langle 1, i, \frac{i + j}{2}, \frac{1 + k}{2} \rangle$$
Supersingular elliptic curves over $\mathbb{F}_{p^2}$

<table>
<thead>
<tr>
<th>$E$</th>
<th>Maximal Orders in $A_p$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mathcal{O} \cong \text{End}(E)$</td>
<td></td>
</tr>
</tbody>
</table>

Isogeny with $\varphi : E \rightarrow E_1$

Ideal $I_\varphi$ left $\mathcal{O}$-ideal and right $\mathcal{O}_1$-ideal

Degree $\deg(\varphi)$

Norm $n(I_\varphi)$

**Example:** $p \equiv 3 \mod 4$, $A_p = H(-1, -p)$.

$$E_0 : y^2 = x^3 + x$$

$$\text{End}(E_0) = \langle 1, \zeta, \frac{\zeta + \pi}{2}, \frac{1 + \zeta \pi}{2} \rangle \cong \langle 1, i, \frac{i + j}{2}, \frac{1 + k}{2} \rangle$$

$\pi : (x, y) \mapsto (x^p, y^p)$ is the Frobenius
The Deuring Correspondence

<table>
<thead>
<tr>
<th>Supersingular elliptic curves over $\mathbb{F}_{p^2}$</th>
<th>Maximal Orders in $\mathcal{A}_p$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$E$</td>
<td>$\mathcal{O} \cong \text{End}(E)$</td>
</tr>
<tr>
<td>Isogeny with $\varphi : E \rightarrow E_1$</td>
<td>Ideal $l_\varphi$ left $\mathcal{O}$-ideal and right $\mathcal{O}_1$-ideal</td>
</tr>
<tr>
<td>Degree $\text{deg}(\varphi)$</td>
<td>Norm $n(l_\varphi)$</td>
</tr>
</tbody>
</table>

**Example:** $p \equiv 3 \mod 4$, $\mathcal{A}_p = H(-1, -p)$.

$$E_0 : y^2 = x^3 + x$$

$$\text{End}(E_0) = \langle 1, \iota, \frac{i + \pi}{2}, \frac{1 + i\pi}{2} \rangle \cong \langle 1, i, \frac{i + j}{2}, \frac{1 + k}{2} \rangle$$

$\pi : (x, y) \mapsto (x^p, y^p)$ is the *Frobenius*

$\iota : (x, y) \mapsto (-x, \sqrt{-1}y)$ is the *twisting automorphism* of $E_0$. 
A new security problem?

**Supersingular \( \ell \)-Isogeny Problem**: Given a prime \( p \) and two supersingular curves \( E_1 \) and \( E_2 \) over \( \mathbb{F}_{p^2} \), compute an \( \ell^e \)-isogeny \( \varphi : E_1 \rightarrow E_2 \) for \( e \in \mathbb{N}^* \).
A new security problem?

**Supersingular \( \ell \)-Isogeny Problem**: Given a prime \( p \) and two supersingular curves \( E_1 \) and \( E_2 \) over \( \mathbb{F}_{p^2} \), compute an \( \ell^e \)-isogeny
\[
\varphi : E_1 \to E_2 \quad \text{for} \quad e \in \mathbb{N}^*.
\]

\[
\uparrow
\]

**Quaternion \( \ell \)-Isogeny Path Problem**: Given a prime number \( p \), two maximal orders \( \mathcal{O}_1, \mathcal{O}_2 \) of \( \mathcal{A}_p \), find an ideal \( J \) of norm \( \ell^e \) for \( e \in \mathbb{N}^* \) with
\[
\mathcal{O}_L(J) \cong \mathcal{O}_1, \quad \mathcal{O}_R(J) \cong \mathcal{O}_2.
\]
A new security problem?

**Supersingular ℓ-Isogeny Problem:** Given a prime \( p \) and two supersingular curves \( E_1 \) and \( E_2 \) over \( \mathbb{F}_{p^2} \), compute an \( ℓ^e \)-isogeny \( \varphi : E_1 \to E_2 \) for \( e \in \mathbb{N}^* \).

\[
\uparrow
\]

**Quaternion ℓ-Isogeny Path Problem:** Given a prime number \( p \), two maximal orders \( \mathcal{O}_1, \mathcal{O}_2 \) of \( \mathcal{A}_p \), find an ideal \( J \) of norm \( ℓ^e \) for \( e \in \mathbb{N}^* \) with \( \mathcal{O}_L(J) \cong \mathcal{O}_1, \mathcal{O}_R(J) \cong \mathcal{O}_2 \).

[Koh+14]: heuristic polynomial time algorithm KLPT for quaternion path problem.

---

Kohel et al. “On the quaternion ℓ-isogeny path problem”
Algorithmic summary of effective Deuring Correspondence

Problems with ✗ are hard, ✓ are easy. All ✓ are obtained using KLPT.

\[ E \rightarrow O \; ✗ \; O \rightarrow E \; ✓ \]

\[ \phi \rightarrow I \; ✗ \; I \rightarrow \phi \; ✓ \]

\[ E_1, E_2 \rightarrow \phi \; ✗ \; O_1, O_2 \rightarrow I \; ✓ \]

[ Eis+18; Wes22]: use KLPT to prove polynomial time reduction from supersingular ℓ-isogeny problem to:

\textbf{Endomorphism Ring Problem}: Given a supersingular elliptic curve \( E \) over \( \mathbb{F}_p^2 \), compute its endomorphism ring.

Eisenträger et al. "Supersingular Isogeny Graphs and Endomorphism Rings: Reductions and Solutions" and Wesolowski "The supersingular isogeny path and endomorphism ring problems are equivalent"
Algorithmic summary of effective Deuring Correspondence

Problems with ✗ are hard, ✓ are easy. All ✓ are obtained using KLPT.

\[
\begin{align*}
    E &\rightarrow \mathcal{O} \quad \text{✗} & \quad \mathcal{O} &\rightarrow E \quad \text{✓} \\
    \varphi &\rightarrow I_\varphi \quad \text{✗} & \quad I_\varphi &\rightarrow \varphi \quad \text{✓} \\
    E_1, E_2 &\rightarrow \varphi \quad \text{✗} & \quad \mathcal{O}_1, \mathcal{O}_2 &\rightarrow I \quad \text{✓}
\end{align*}
\]
Algorithmic summary of effective Deuring Correspondence

Problems with ✗ are hard, ✓ are easy. All ✓ are obtained using KLPT.

\[
E \rightarrow O \quad ✗ \quad O \rightarrow E \quad ✓
\]

\[
\varphi \rightarrow I_\varphi \quad ✗ \quad I_\varphi \rightarrow \varphi \quad ✓
\]

\[
E_1, E_2 \rightarrow \varphi \quad ✗ \quad O_1, O_2 \rightarrow I \quad ✓
\]

[Eis+18; Wes22]: use KLPT to prove \textit{polynomial} time reduction from supersingular \(\ell\)-isogeny problem to:

**Endomorphism Ring Problem:** Given a \textit{supersingular elliptic curve} \(E\) over \(\mathbb{F}_{p^2}\), compute its \textit{endomorphism ring}.

---

Eisenträger et al. “Supersingular Isogeny Graphs and Endomorphism Rings: Reductions and Solutions” and Wesolowski “The supersingular isogeny path and endomorphism ring problems are equivalent”
Proof of Knowledge of Endomorphism Ring
The knowledge of the endomorphism ring of a curve $E$ lets us perform powerful operations otherwise impossible.
The knowledge of the **endomorphism ring** of a curve $E$ lets us perform *powerful operations* otherwise impossible.

Use **KLPT** to prove knowledge of **endomorphism ring**?
The knowledge of the endomorphism ring of a curve $E$ lets us perform powerful operations otherwise impossible.

Use KLPT to prove knowledge of endomorphism ring?

First attempt: GPS Signature in 2017, derived from 2-special sound identification protocol.
The knowledge of the endomorphism ring of a curve $E$ lets us perform powerful operations otherwise impossible.

Use KLPT to prove knowledge of endomorphism ring?

First attempt: GPS Signature in 2017, derived from 2-special sound identification protocol.

**SQISign contributions:**

- A new generic KLPT algorithm to reach high soundness.
- New algorithmic tools to make the scheme practical.

---

Galbraith, Petit, and Silva “Identification Protocols and Signature Schemes Based on Supersingular Isogeny Problems”
[GPS17]: A 2-special sound *identification* protocol.
[GPS17]: A 2-special sound identification protocol.

**Prover** wants to *demonstrate knowledge* of $\text{End}(E_A)$ for public key $E_A$. $E_0$ is a **public** special curve.
[GPS17]: A 2-special sound identification protocol.

Prover wants to demonstrate knowledge of $\text{End}(E_A)$ for public key $E_A$. $E_0$ is a public special curve.

\[ E_0 \xrightarrow{\tau} E_A \]

---

secret key isogeny
[GPS17]: A 2-special sound \textit{identification} protocol.

**Prover** wants to \textit{demonstrate knowledge} of \textit{End}(\textit{E}_A) for \textit{public key} \textit{E}_A.

\( E_0 \) is a \textbf{public special curve}.

\[
\begin{align*}
E_0 &\quad \xrightarrow{\tau} \quad \text{commitment isogeny (prover)} \\
\text{E}_A &\quad \xrightarrow{\sigma_0} \quad \text{secret key isogeny} \\
\end{align*}
\]
[GPS17]: A 2-special sound identification protocol.

Prover wants to demonstrate knowledge of \( \text{End}(E_A) \) for public key \( E_A \). \( E_0 \) is a public special curve.
[GPS17]: A 2-special sound identification protocol.

**Prover** wants to demonstrate knowledge of $\text{End}(E_A)$ for public key $E_A$. $E_0$ is a public special curve.
[GPS17]: A 2-special sound identification protocol.

**Prover** wants to demonstrate knowledge of $\text{End}(E_A)$ for public key $E_A$. $E_0$ is a public special curve.

$E_0$ is a public special curve.

$E_A \xrightarrow{\tau} E_0$  

$E_0 \xrightarrow{\sigma_b} b \in \{0, 1\}$  

$E_0 \xrightarrow{\sigma_{1-b}} E$  

$\text{commitment isogeny (prover)}$  

$\bullet$  

$\text{challenge bit (verifier)}$  

$\text{response isogeny (prover)}$  

$\text{secret key isogeny}$
[GPS17]: A 2-special sound identification protocol.

Prover wants to demonstrate knowledge of $\text{End}(E_A)$ for public key $E_A$. $E_0$ is a public special curve.

Repeat this $\lambda$ times to reach $2^\lambda$-bits of soundness.
SQISign: A $2^\lambda$-sound identification protocol.
SQISign: A $2^\lambda$-sound identification protocol.

Prover wants to demonstrate knowledge of $\text{End}(E_A)$ for public key $E_A$. $E_0$ is a public special curve.

\[ E_0 \xrightarrow{\tau} E_A \]

--- secret key isogeny
**SQISign Identification Scheme**

**SQISign**: A $2^\lambda$-sound *identification* protocol.

Prover wants to *demonstrate knowledge* of $\text{End}(E_A)$ for public key $E_A$. $E_0$ is a *public* special curve.

Diagram:

- $E_0$ to $E_1$ via $\psi$: commitment isogeny (prover)
- $E_A$ to $\ldots$ via $\tau$: secret key isogeny
SQISign Identification Scheme

**SQISign**: A $2^\lambda$-sound identification protocol.

Prover wants to *demonstrate knowledge* of $\text{End}(E_A)$ for public key $E_A$. $E_0$ is a **public** special curve.

![Diagram](image.png)

- $E_0$ → $E_1$: Commitment isogeny (prover)
- $E_1$ → $E_2$: Challenge isogeny (verifier)
- $E_A$: Secret key isogeny
SQISign Identification Scheme

**SQISign**: A $2^\lambda$-sound *identification* protocol.

Prover wants to *demonstrate knowledge* of $\text{End}(E_A)$ for public key $E_A$.

$E_0$ is a **public** special curve.
SQISign: A $2^\lambda$-sound identification protocol.

Prover wants to demonstrate knowledge of $\text{End}(E_A)$ for public key $E_A$. $E_0$ is a public special curve.

Probability to cheat without knowledge of $\text{End}(E_A)$: $O\left(\frac{1}{\deg \varphi}\right)$. 

**Diagram:**
- $E_0 \xrightarrow{\psi} E_1$
- $E_A \xrightarrow{\sigma} E_2$
- $\tau$
- $\varphi$

- commitment isogeny (prover)
- challenge isogeny (verifier)
- response isogeny (prover)
- secret key isogeny
Proving the Soundness

**Soundness:** Given *two valid transcripts* for *two different challenges* for the *same commitment*, some knowledge is revealed on the secret key.
Soundness: Given two valid transcripts for two different challenges for the same commitment, some knowledge is revealed on the secret key.
Soundness: Given two valid transcripts for two different challenges for the same commitment, some knowledge is revealed on the secret key.
Proving the Soundness

**Soundness**: Given *two valid transcripts for two different challenges for the same commitment*, some knowledge is revealed on the secret key.

**Smooth Endomorphism Problem**: Given a *supersingular elliptic curve* $E$ over $\mathbb{F}_{p^2}$, compute a non-trivial *endomorphism* $\theta \in \text{End}(E)$ of *smooth norm*. 
Proving the Soundness

**Soundness:** Given two valid transcripts for two different challenges for the same commitment, some knowledge is revealed on the secret key.

**Smooth Endomorphism Problem:** Given a supersingular elliptic curve $E$ over $\mathbb{F}_{p^2}$, compute a non-trivial endomorphism $\theta \in \text{End}(E)$ of smooth norm.

[Eis+18]: prove heuristic polynomial reduction to the **Endomorphism Ring Problem**.
Zero-Knowledge: It is possible to generate a transcript indistinguishable from a valid one with the sole knowledge of the public key.
The KLPT algorithm and the Zero-knowledge

**Zero-Knowledge:** It is possible to generate a transcript indistinguishable from a valid one with the *sole knowledge* of the public key.

![Diagram]

- $E_0$: commitment isogeny (prover)
- $E_1$: challenge isogeny (verifier)
- $E_2$: response isogeny (prover)
- $E_A$: secret key isogeny

---

Show that $\sigma$ is a random isogeny $\Rightarrow$ depends on the alg. to compute $\sigma$. Solution from [Koh+14]: $\sigma$ reveal a path to $E_0$. We propose a new *SigningKLPT* algorithm.
**Zero-Knowledge:** It is possible to generate a transcript indistinguishable from a valid one with the sole knowledge of the public key.

Show that $\sigma$ is a random isogeny $\Rightarrow$ depends on the alg. to compute $\sigma$. 
Zero-Knowledge: It is possible to generate a transcript indistinguishable from a valid one with the sole knowledge of the public key.

Show that $\sigma$ is a random isogeny $\Rightarrow$ depends on the alg. to compute $\sigma$.

Solution from [Koh+14]: $\sigma$ reveal a path to $E_0$. 
The KLPT algorithm and the Zero-knowledge

**Zero-Knowledge:** It is possible to generate a transcript indistinguishable from a valid one with the sole knowledge of the public key.

Show that $\sigma$ is a random isogeny $\Rightarrow$ depends on the alg. to compute $\sigma$.

Solution from [Koh+14]: $\sigma$ reveal a path to $E_0$.

We propose a new **SigningKLPT** algorithm.
Lemma: Fix $D$ as $\sigma$’s degree. There exists $\mathcal{P}_{\text{deg}(\tau)}$ a set of isogenies of degree $D$ such that:

$\text{SigningKLPT}$ outputs an uniform element in $\{\rho, \rho = [\tau] \ast \iota, \iota \in \mathcal{P}_{\text{deg}(\tau)}\}$. 

$E_0 \quad E_1 \quad E_2 \quad E_A \quad \tau \quad \iota \quad \sigma = [\tau] \ast \iota$ 

$\text{ZK}$ reduces to the distinguishing problem between:

1. $\sigma$ is uniformly random isogeny of degree $D$;
2. $\sigma$ is uniformly random in $[\tau] \ast \mathcal{P}_{\text{deg}(\tau)}$.

$\mathcal{P}_{\text{deg}(\tau)}$ can be computed from $\text{deg}(\tau)$ only and has exponential size.
Lemma: Fix $D$ as $\sigma$’s degree. There exists $\mathcal{P}_{\deg(\tau)}$ a set of isogenies of degree $D$ such that: $\text{SigningKLPT}$ outputs an uniform element in $\{\rho, \rho = [\tau]_* \iota, \iota \in \mathcal{P}_{\deg(\tau)}\}$.
Lemma: Fix $D$ as $\sigma$’s degree. There exists $\mathcal{P}_{\deg(\tau)}$ a set of isogenies of degree $D$ such that: $\text{SigningKLPT}$ outputs an uniform element in $\\{\rho, \rho = [\tau]_* \iota, \iota \in \mathcal{P}_{\deg(\tau)}\}$.

ZK reduces to the distinguishing problem between:

1. $\sigma$ is uniformly random isogeny of degree $D$;
Lemma: Fix $D$ as $\sigma$’s degree. There exists $\mathcal{P}_{\deg(\tau)}$ a set of isogenies of degree $D$ such that: $\text{SigningKLPT}$ outputs an uniform element in $\{\rho, \rho = [\tau]_* \iota, \iota \in \mathcal{P}_{\deg(\tau)}\}$.

ZK reduces to the distinguishing problem between:

1. $\sigma$ is uniformly random isogeny of degree $D$;
2. $\sigma$ is uniformly random in $[\tau]_* \mathcal{P}_{\deg(\tau)}$.

$\mathcal{P}_{\deg(\tau)}$ can be computed from $\deg(\tau)$ only and has exponential size.
The effective Deuring Correspondence: algorithmic challenges
**SigningKLPT** computes an *ideal*. Translate into the *isogeny* $\sigma$.
SigningKLPT computes an ideal. Translate into the isogeny $\sigma$.

[GPS17]: $\text{IdealToIsogeny} : J \mapsto \sigma$ polynomial alg. for degree $D$, domain $E$ with $E[D]$ and action of $\text{End}(E)$ on this set. No implementation!
SigningKLPT computes an ideal. Translate into the isogeny $\sigma$.

[GPS17]: IdealToIsogeny : $J \mapsto \sigma$ polynomial alg. for degree $D$, domain $E$ with $E[D]$ and action of $\text{End}(E)$ on this set. No implementation!

We have $D \gg p^2$ and the kernel cannot be represented in $\mathbb{F}_{p^2}$. 
From Ideals to Isogenies

\textbf{SigningKLPT} computes an ideal. Translate into the isogeny $\sigma$.

[GPS17]: \textbf{IdealToIsogeny} : $J \mapsto \sigma$ polynomial alg. for degree $D$, domain $E$ with $E[D]$ and action of $\text{End}(E)$ on this set. \textbf{No implementation}!

We have $D \gg p^2$ and the kernel cannot be represented in $\mathbb{F}_{p^2}$. Two solutions:

- Take $D$ powersmooth $\mapsto E[D]$ in $\sim$ small extension ([GPS17]).
SigningKLPT computes an ideal. Translate into the isogeny $\sigma$.

[GPS17]: $\text{IdealToIsogeny}: J \mapsto \sigma$ polynomial alg. for degree $D$, domain $E$ with $E[D]$ and action of $\text{End}(E)$ on this set. No implementation!

We have $D \gg p^2$ and the kernel cannot be represented in $\mathbb{F}_{p^2}$. Two solutions:

- Take $D$ powersmooth $\rightarrow E[D]$ in $\sim$ small extension ([GPS17]).
- Take $D = \ell^f$ and split $\sigma$ in smaller isogenies of degree $\ell^e$ and apply $\text{IdealToIsogeny}$ for each ($\text{SQISign}$).

New Pb: for generic $E$ of known $\text{End}(E)$, hard to evaluate $\text{End}(E)$...
Choice of Parameters for SQISign

For fast verification we take $\sigma$ of degree $2^f$, $f = O(\log_2(p))$. 

Bottleneck of the signature: $\Theta(\frac{f}{e})T$-isogeny computations.
Choice of Parameters for SQISign

For fast verification we take $\sigma$ of degree $2^f$, $f = O(\log_2(p))$.

For efficient signature: need a prime $p$ such that $p^2 - 1$ is divided by $2^e T$ with odd smooth $T$ satisfying $T^2 \sim p^3$. 

We found a 256 bits prime $p$ with $e=33$, $f=1000$ and $2^{13}$-smooth integer of 395 bits: 

$$T = 5^{21} \cdot 7^{2} \cdot 11 \cdot 31 \cdot 83 \cdot 107 \cdot 137 \cdot 751 \cdot 827 \cdot 3691 \cdot 4019 \cdot 6983 \cdot 3^{53} \cdot 43 \cdot 103 \cdot 109 \cdot 199 \cdot 227 \cdot 419 \cdot 491 \cdot 569 \cdot 631 \cdot 677 \cdot 857 \cdot 859 \cdot 883 \cdot 1019 \cdot 2713 \cdot 4283$$

Bottleneck of the signature: $\Theta(f/e) T$-isogeny computations.
Choice of Parameters for SQISign

For fast verification we take $\sigma$ of degree $2^f$, $f = O(\log_2(p))$.

**For efficient signature:** need a prime $p$ such that $p^2 - 1$ is divided by $2^eT$ with odd smooth $T$ satisfying $T^2 \sim p^3$.

We found a 256 bits prime $p$ with $e = 33$, $f = 1000$ and $2^{13}$-smooth integer of 395 bits:

$$T = 5^{21} \cdot 7^2 \cdot 11 \cdot 31 \cdot 83 \cdot 107 \cdot 137 \cdot 751 \cdot 827 \cdot 3691 \cdot 4019 \cdot 6983$$

$$3^{53} \cdot 43 \cdot 103 \cdot 109 \cdot 199 \cdot 227 \cdot 419 \cdot 491 \cdot 569 \cdot 631 \cdot 677 \cdot 857 \cdot 859$$

$$883 \cdot 1019 \cdot 2713 \cdot 4283$$
Choice of Parameters for SQISign

For fast verification we take $\sigma$ of degree $2^f$, $f = O(\log_2(p))$.

**For efficient signature:** need a prime $p$ such that $p^2 - 1$ is divided by $2^e T$ with odd smooth $T$ satisfying $T^2 \sim p^3$.

We found a 256 bits prime $p$ with $e = 33, f = 1000$ and $2^{13}$-smooth integer of 395 bits:

$$T = 5^{21} \cdot 7^2 \cdot 11 \cdot 31 \cdot 83 \cdot 107 \cdot 137 \cdot 751 \cdot 827 \cdot 3691 \cdot 4019 \cdot 6983 \cdot 3^{53} \cdot 43 \cdot 103 \cdot 109 \cdot 199 \cdot 227 \cdot 419 \cdot 491 \cdot 569 \cdot 631 \cdot 677 \cdot 857 \cdot 859 \cdot 883 \cdot 1019 \cdot 2713 \cdot 4283$$

**Bottleneck** of the signature: $\Theta(f/e) T$-isogeny computations.
What now?
GPS and SQISign are the first applications of constructive Deuring correspondence but there is still lot of room for improvements and new discoveries. Some follow-up work and future direction:

• Improve the KLPT algorithm and ideal to isogeny translation mechanism.
• Study the new ZK assumption.
• "SETA: Supersingular Encryption from Torsion Attacks", DDFKLPSW, ASIACRYPT 2021
• "A New Isogeny Representation and Applications to Cryptography", L (preprint).
GPS and SQISign are the first applications of constructive Deuring correspondence but there is still lot of room for improvements and new discoveries. Some follow-up work and future direction:

- Improve the KLPT algorithm and ideal to isogeny translation mechanism.
GPS and SQISign are the first applications of constructive Deuring correspondence but there is still lot of room for improvements and new discoveries. Some follow-up work and future direction:

- Improve the KLPT algorithm and ideal to isogeny translation mechanism.
- Study the new ZK assumption.
Conclusion and Important Problems

GPS and SQISign are the first applications of constructive Deuring correspondence but there is still lot of room for improvements and new discoveries. Some follow-up work and future direction:

- Improve the KLPT algorithm and ideal to isogeny translation mechanism.
- Study the new ZK assumption.
- "SETA: Supersingular Encryption from Torsion Attacks", DDFKLPSW, ASIACRYPT 2021
GPS and SQISign are the first applications of constructive Deuring correspondence but there is still lot of room for improvements and new discoveries. Some follow-up work and future direction:

- Improve the KLPT algorithm and ideal to isogeny translation mechanism.
- Study the new ZK assumption.
- "SETA: Supersingular Encryption from Torsion Attacks", DDFKLPSSW, ASIACRYPT 2021