Signing with higher dimensional isogenies

Pierrick Dartois

Joint work with Antonin Leroux, Damien Robert and Benjamin Wesolowski
Acknowledgements to Luca De Feo

12 October 2023
1 The Deuring correspondence

2 Effective Deuring correspondence and higher dimensional isogenies

3 SQIsignHD
The Deuring correspondence
Isogenies

\[ \varphi(P + Q) = \varphi(P) + \varphi(Q) \]
<table>
<thead>
<tr>
<th>Supersingular elliptic curves</th>
<th>Quaternions</th>
</tr>
</thead>
<tbody>
<tr>
<td>$j(E)$ or $j(E)^p$ supersingular</td>
<td>$\mathcal{O} \cong \text{End}(E)$ maximal order in $B_{p,\infty}$</td>
</tr>
<tr>
<td>$\varphi : E \to E'$</td>
<td>left $\mathcal{O}$-ideal and right $\mathcal{O}'$-ideal $l_{\varphi}$</td>
</tr>
<tr>
<td>$\varphi, \psi : E \to E'$</td>
<td>$l_{\varphi} \sim l_{\psi}$ ($l_{\psi} = l_{\varphi}\alpha$)</td>
</tr>
<tr>
<td>$\varphi \circ \psi$</td>
<td>$l_{\varphi} \cdot l_{\psi}$</td>
</tr>
<tr>
<td>$\theta \in \text{End}(E)$</td>
<td>Principal ideal $\mathcal{O}\theta$</td>
</tr>
<tr>
<td>$\deg(\varphi)$</td>
<td>$\text{nrd}(l_{\varphi})$</td>
</tr>
</tbody>
</table>
Let $E_1$ and $E_2$ of known endomorphism rings $\mathcal{O}_1 \cong \text{End}(E_1)$ and $\mathcal{O}_2 \cong \text{End}(E_2)$.

- Compute a connecting ideal $I$ between $\mathcal{O}_1$ and $\mathcal{O}_2$.
- Compute $J \sim I$ of smooth norm via [KLPT14].
- Translate $J$ into an isogeny $\varphi_J : E_1 \rightarrow E_2$. 

✓ Takes polynomial time.
✓ Becomes hard when $\text{End}(E_1)$ or $\text{End}(E_2)$ is unknown.
Computing isogenies via the Deuring correspondence

- Let $E_1$ and $E_2$ of known endomorphism rings $\mathcal{O}_1 \cong \text{End}(E_1)$ and $\mathcal{O}_2 \cong \text{End}(E_2)$.
- Compute a connecting ideal $I$ between $\mathcal{O}_1$ and $\mathcal{O}_2$.
- Compute $J \sim I$ of smooth norm via [KLPT14].
- Translate $J$ into an isogeny $\varphi_J : E_1 \rightarrow E_2$.

✓ Takes polynomial time.
Computing isogenies via the Deuring correspondence

- Let $E_1$ and $E_2$ of known endomorphism rings $\mathcal{O}_1 \cong \text{End}(E_1)$ and $\mathcal{O}_2 \cong \text{End}(E_2)$.
- Compute a connecting ideal $I$ between $\mathcal{O}_1$ and $\mathcal{O}_2$.
- Compute $J \sim I$ of smooth norm via [KLPT14].
- Translate $J$ into an isogeny $\varphi_J : E_1 \rightarrow E_2$.

✓ Takes polynomial time.

✓ Becomes hard when $\text{End}(E_1)$ or $\text{End}(E_2)$ is unknown.
Computing isogenies via the Deuring correspondence

- Let \( E_1 \) and \( E_2 \) of known endomorphism rings \( \mathcal{O}_1 \cong \text{End}(E_1) \) and \( \mathcal{O}_2 \cong \text{End}(E_2) \).
- Compute a connecting ideal \( I \) between \( \mathcal{O}_1 \) and \( \mathcal{O}_2 \).
- Compute \( J \sim I \) of smooth norm via [KLPT14].
- Translate \( J \) into an isogeny \( \varphi_J : E_1 \rightarrow E_2 \).

✓ Takes polynomial time.

✓ Becomes hard when \( \text{End}(E_1) \) or \( \text{End}(E_2) \) is unknown.

✗ Slow because of the red steps.
Effective Deuring correspondence and higher dimensional isogenies
Kani’s embedding lemma

**Theorem (Robert, 2022)**

Let \( \sigma : E_1 \rightarrow E_2 \) such that \( \deg(\sigma) + a_1^2 + a_2^2 = \ell^e \). Then:

- \( \sigma : E_1 \rightarrow E_2 \) can be represented in dimension 4 by the \( \ell^e \)-isogeny:

\[
F := \begin{pmatrix}
    a_1 & a_2 & \hat{\sigma} & 0 \\
   -a_2 & a_1 & 0 & \hat{\sigma} \\
    -\sigma & 0 & a_1 & -a_2 \\
    0 & -\sigma & a_2 & a_1
\end{pmatrix} \in \text{End}(E_1^2 \times E_2^2).
\]

- \( F \) can be computed by evaluating \( \sigma \) on \( E_1[\ell^e] \).
Kani’s embedding lemma

Corollary (Robert, 2022)

Let \( \sigma : E_1 \rightarrow E_2 \) of degree \( q < \ell^e \) such that \( \ell^e - q \) is a prime \( \equiv 1 \mod 4 \). There exists a polynomial time algorithm with:

- **Input:** \( (\sigma(P_1), \sigma(P_2)) \), where \( (P_1, P_2) \) is a basis of \( E_1[\ell^e] \) and \( Q \in E_1(\mathbb{F}_{p^2}) \).

- **Output:** \( \sigma(Q) \).
Corollary (Robert, 2022)

Let $\sigma : E_1 \rightarrow E_2$ of degree $q < \ell^e$ such that $\ell^e - q$ is a prime $\equiv 1 \pmod{4}$. There exists a polynomial time algorithm with:

- **Input:** $(\sigma(P_1), \sigma(P_2))$, where $(P_1, P_2)$ is a basis of $E_1[\ell^e]$ and $Q \in E_1(\mathbb{F}_{p^2})$.
- **Output:** $\sigma(Q)$.

**Context:** This idea comes from the attacks against SIDH [CD23; MM22; Rob23].
Problem: Given $\phi : E_1 \rightarrow E_2$, $I_\phi$, $\mathcal{O}_1 \cong \text{End}(E_1)$ and $\mathcal{O}_2 \cong \text{End}(E_2)$ (secret), find another path $\sigma : E_1 \rightarrow E_2$. 
A new algorithm for effective Deuring correspondence

**Problem:** Given $\phi : E_1 \rightarrow E_2$, $I_{\phi}$, $\mathcal{O}_1 \cong \text{End}(E_1)$ and $\mathcal{O}_2 \cong \text{End}(E_2)$ (secret), find another path $\sigma : E_1 \rightarrow E_2$.

The SQIsign way [DKLPW20]

- Compute $I \sim I_{\phi}$ random of smooth norm $\sim p^{15/4}$ via [KLPT14].
A new algorithm for effective Deuring correspondence

**Problem:** Given $\phi : E_1 \to E_2$, $I_\phi$, $O_1 \simeq \text{End}(E_1)$ and $O_2 \simeq \text{End}(E_2)$ (secret), find another path $\sigma : E_1 \to E_2$.

**The SQIsign way [DKLPW20]**

- Compute $I \sim I_\phi$ random of smooth norm $\simeq p^{15/4}$ via [KLPT14].
- Translate $I$ into
  $\sigma : E_1 \to E_2$. 
A new algorithm for effective Deuring correspondence

**Problem:** Given $\phi : E_1 \rightarrow E_2$, $I_\phi$, $O_1 \cong \text{End}(E_1)$ and $O_2 \cong \text{End}(E_2)$ (secret), find another path $\sigma : E_1 \rightarrow E_2$.

**The SQIsign way [DKLPW20]**
- Compute $l \sim I_\phi$ random of smooth norm $\sim p^{15/4}$ via [KLPT14].
- Translate $l$ into $\sigma : E_1 \rightarrow E_2$.

**The SQIsignHD way [DLRW23]**
- Compute $l \sim I_\phi$ of norm $q \sim \sqrt{p}$ such that $\ell^e - q$ is a prime $\equiv 1$ mod 4.
A new algorithm for effective Deuring correspondence

**Problem:** Given $\phi : E_1 \to E_2$, $I_\phi$, $O_1 \cong \text{End}(E_1)$ and $O_2 \cong \text{End}(E_2)$ (secret), find another path $\sigma : E_1 \to E_2$.

**The SQIsign way [DKLPW20]**
- Compute $I \sim I_\phi$ random of smooth norm $\approx p^{15/4}$ via [KLPT14].
- Translate $I$ into $\sigma : E_1 \to E_2$.

**The SQIsignHD way [DLRW23]**
- Compute $I \sim I_\phi$ of norm $q \approx \sqrt{p}$ such that $\ell^e - q$ is a prime $\equiv 1 \mod 4$.
- Evaluate $\sigma : E_1 \to E_2$ associated to $I$ on $E_1[\ell^e]$, using $\phi$. 
A new algorithm for effective Deuring correspondence

**Problem:** Given $\phi : E_1 \to E_2$, $I_\phi$, $O_1 \cong \text{End}(E_1)$ and $O_2 \cong \text{End}(E_2)$ (secret), find another path $\sigma : E_1 \to E_2$.

**The SQIsign way [DKLPW20]**
- Compute $l \sim I_\phi$ random of smooth norm $\sim p^{15/4}$ via [KLPT14].
- Translate $l$ into $\sigma : E_1 \to E_2$.

**The SQIsignHD way [DLRW23]**
- Compute $l \sim I_\phi$ of norm $q \sim \sqrt{p}$ such that $\ell^e - q$ is a prime $\equiv 1 \pmod{4}$.
- Evaluate $\sigma : E_1 \to E_2$ associated to $l$ on $E_1[\ell^e]$, using $\phi$.
- $(q, \sigma(E_1[\ell^e]))$, is sufficient to represent $\sigma$.
- We can then compute $F \in \text{End}(E_1^2 \times E_2^2)$ embedding $\sigma$. 
The SQIsignHD identification scheme [DLRW23]

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

- **public**
- **Prover’s secret**
- **published by Verifier**
- **published by Prover**

Prover

Verifier

Statement: I know \( \tau \)
The SQIsignHD identification scheme [DLRW23]

The protocol
Performance and security

The Deuring correspondence
Effective Deuring correspondence and higher dimensional isogenies

SQIsignHD

The SQIsignHD identification scheme [DLRW23]

Prover

Statement: I know $\tau$

Commitment: $E_1$

Verifier

$E_0 \xrightarrow{\tau} E_A$

$E_1$

- black: public
- red: Prover's secret
- blue: published by Verifier
- green: published by Prover

$\psi$
The SQIsignHD identification scheme [DLRW23]

The Deuring correspondence
Effective Deuring correspondence and higher dimensional isogenies

SQIsignHD
The protocol
Performance and security

The SQIsignHD identification scheme [DLRW23]

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

\[ \psi \]

\[ \varphi \]

Statement : I know \( \tau \)

Commitment: \( E_1 \)

Challenge: \( \varphi \)

public

Prover’s secret

published by Verifier

published by Prover
The SQIsignHD identification scheme [DLRW23]

Statement: I know $\tau$

Commitment: $E_1$

Challenge: $\varphi$

Response: $\sigma$

$E_0 \xrightarrow{\tau} E_A$

$E_1 \xrightarrow{\psi} E_2$

$E_0 \xrightarrow{\tau} E_A$

$E_1 \xrightarrow{\psi} E_2$

- public
- Prover’s secret
- published by Verifier
- published by Prover
The SQIsignHD identification scheme [DLRW23]

The protocol
Performance and security

The Deuring correspondence
Effective Deuring correspondence and higher dimensional isogenies
SQIsignHD

Statement: I know $\tau$

Commitment: $E_1$

Challenge: $\varphi$

Response: $\sigma$

Accept if $\sigma$ is correct

$E_0$ $\xrightarrow{\tau} E_A$

$E_1$ $\xrightarrow{\sigma} E_2$

$\psi$ $\varphi$

- public
- Prover’s secret
- published by Verifier
- published by Prover

Prover

Verifier
The SQIsignHD identification scheme [DLRW23]

Response: \((q, \sigma(P_1), \sigma(P_2))\), where:

- \((P_1, P_2)\) is a basis of \(E_1[\ell^e]\);
- \(q := \deg(\sigma)\).
The SQIsignHD identification scheme [DLRW23]

**Response:** \((q, \sigma(P_1), \sigma(P_2))\),
where:
- \((P_1, P_2)\) is a basis of \(E_1[\ell^e]\);
- \(q := \text{deg}(\sigma)\).

Very fast! 28 ms in C.
The SQIsignHD identification scheme [DLRW23]

Response: \((q, \sigma(P_1), \sigma(P_2))\),
where:
- \((P_1, P_2)\) is a basis of \(E_1[\ell^e]\);
- \(q := \text{deg}(\sigma)\).

Very fast! 28 ms in C.

Verification: Compute the embedding \(F \in \text{End}(E_1^2 \times E_2^2)\) of \(\sigma\).
The SQIsignHD identification scheme [DLRW23]

Response: \((q, \sigma(P_1), \sigma(P_2))\),
where:
- \((P_1, P_2)\) is a basis of \(E_1[\ell^e]\);
- \(q \coloneqq \deg(\sigma)\).

Very fast! 28 ms in C.

Verification: Compute the embedding \(F \in \text{End}(E_1^2 \times E_2^2)\) of \(\sigma\).

Proof of concept.
850 ms in sagemath.
## Comparison of SQIsignHD with SQIsign

<table>
<thead>
<tr>
<th></th>
<th>SQIsign</th>
<th>SQIsignHD</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security</strong></td>
<td>× Ad-hoc heuristic:</td>
<td>✓ Simpler heuristics:</td>
</tr>
<tr>
<td></td>
<td>• Distribution of $\sigma$.</td>
<td>• Oracle (RUGDIO);</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Distribution of $E_1$.</td>
</tr>
<tr>
<td><strong>Signing time</strong></td>
<td>× 400 ms for NIST-1</td>
<td>✓ 28 ms for NIST-1</td>
</tr>
<tr>
<td><strong>Signature size</strong></td>
<td>✓ 204 bytes for NIST-1</td>
<td>✓ 109 bytes for NIST-1</td>
</tr>
<tr>
<td><strong>Verification</strong></td>
<td>✓ Fast (6 ms for NIST-1)</td>
<td>× 850 ms for NIST-1 in sagemath</td>
</tr>
</tbody>
</table>
Thank you for listening.

Find our pre-print here: https://eprint.iacr.org/2023/436