Signing with higher dimensional isogenies

Pierrick Dartois

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

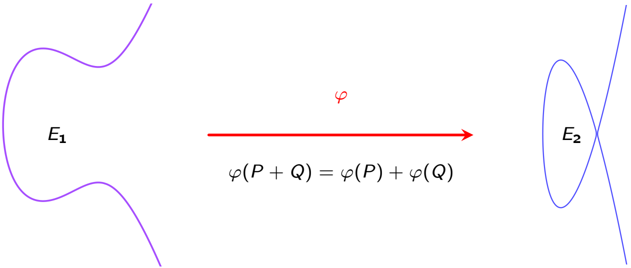
12 October 2023

Institut de Mathématiques de Bordeaux

CANARI

The Deuring correspondence

Isogenies



The Deuring correspondence

Supersingular elliptic curves	Quaternions
$j(E)$ or $j(E)^p$ supersingular	$\mathcal{O} \cong \mathrm{End}(E)$ maximal order in $\mathcal{B}_{p,\infty}$
$\varphi : E \longrightarrow E'$	left $\mathcal{O}$-ideal and right $\mathcal{O}'$-ideal I_φ
$\varphi, \psi : E \longrightarrow E'$	$I_\varphi \sim I_\psi$ $(I_\psi = I_\varphi \alpha)$
$\widehat{\varphi}$	$\overline{I_\varphi}$
$\varphi \circ \psi$	$I_\psi \cdot I_\varphi$
$\theta \in \mathrm{End}(E)$	Principal ideal $\mathcal{O}\theta$
$\deg(\varphi)$	$\mathrm{nrd}(I_\varphi)$

Computing isogenies via the Deuring correspondence

- Let E_1 and E_2 of known endomorphism rings $\mathcal{O}_1 \cong \mathrm{End}(E_1)$ and $\mathcal{O}_2 \cong \mathrm{End}(E_2)$.
- 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 $\varphi_J : E_1 \longrightarrow E_2$.

Computing isogenies via the Deuring correspondence

- Let E_1 and E_2 of known endomorphism rings $\mathcal{O}_1 \cong \mathrm{End}(E_1)$ and $\mathcal{O}_2 \cong \mathrm{End}(E_2)$.
- 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 $\varphi_J : E_1 \longrightarrow E_2$.

✓ Takes polynomial time.

Computing isogenies via the Deuring correspondence

- Let E_1 and E_2 of known endomorphism rings $\mathcal{O}_1 \cong \mathrm{End}(E_1)$ and $\mathcal{O}_2 \cong \mathrm{End}(E_2)$.
- 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 $\varphi_J : E_1 \longrightarrow E_2$.

✓ Takes polynomial time.

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

Computing isogenies via the Deuring correspondence

- Let E_1 and E_2 of known endomorphism rings $\mathcal{O}_1 \cong \mathrm{End}(E_1)$ and $\mathcal{O}_2 \cong \mathrm{End}(E_2)$.
- 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 $\varphi_J : E_1 \longrightarrow E_2$.

✓ Takes polynomial time.

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

✗ Slow because of the red steps.

Effective Deuring correspondence and higher dimensional isogenies

Kani's embedding lemma

Theorem (Robert, 2022)

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

- *$\sigma : E_1 \longrightarrow E_2$ can be represented in dimension 4 by the ℓ^e-isogeny:*

$$F := \begin{pmatrix} a_1 & a_2 & \widehat{\sigma} & 0 \\ -a_2 & a_1 & 0 & \widehat{\sigma} \\ -\sigma & 0 & a_1 & -a_2 \\ 0 & -\sigma & a_2 & a_1 \end{pmatrix} \in \mathrm{End}(E_1^2 \times E_2^2).$$

- *F can be computed by evaluating σ on $E_1[\ell^e]$.*

Kani's embedding lemma

Corollary (Robert, 2022)

Let $\sigma : E_1 \longrightarrow E_2$ 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:*** $\sigma(Q)$.

Kani's embedding lemma

Corollary (Robert, 2022)

Let $\sigma : E_1 \longrightarrow E_2$ 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:*** $\sigma(Q)$.

Context: This idea comes from the attacks against SIDH [CD23; MM22; Rob23].

A new algorithm for effective Deuring correspondence

Problem: Given $\phi : E_1 \longrightarrow E_2$, I_ϕ, $\mathcal{O}_1 \cong \mathrm{End}(E_1)$ and $\mathcal{O}_2 \cong \mathrm{End}(E_2)$ (secret), find another path $\sigma : E_1 \longrightarrow E_2$.

A new algorithm for effective Deuring correspondence

Problem: Given $\phi : E_1 \longrightarrow E_2$, I_ϕ, $\mathcal{O}_1 \cong \mathrm{End}(E_1)$ and $\mathcal{O}_2 \cong \mathrm{End}(E_2)$ (secret), find another path $\sigma : E_1 \longrightarrow E_2$.

The SQIsign way [DKLPW20]

- Compute $I \sim I_\phi$ random of smooth norm $\simeq p^{15/4}$ via [KLPT14].

A new algorithm for effective Deuring correspondence

Problem: Given $\phi : E_1 \longrightarrow E_2$, I_ϕ, $\mathcal{O}_1 \cong \mathrm{End}(E_1)$ and $\mathcal{O}_2 \cong \mathrm{End}(E_2)$ (secret), find another path $\sigma : E_1 \longrightarrow E_2$.

The SQIsign way [DKLPW20]

- Compute $I \sim I_\phi$ random of smooth norm $\simeq p^{15/4}$ via [KLPT14].
- Translate I into $\sigma : E_1 \longrightarrow E_2$.

A new algorithm for effective Deuring correspondence

Problem: Given $\phi : E_1 \longrightarrow E_2$, I_ϕ, $\mathcal{O}_1 \cong \mathrm{End}(E_1)$ and $\mathcal{O}_2 \cong \mathrm{End}(E_2)$ (secret), find another path $\sigma : E_1 \longrightarrow E_2$.

The SQIsign way [DKLPW20]

- Compute $I \sim I_\phi$ random of smooth norm $\simeq p^{15/4}$ via [KLPT14].
- Translate I into $\sigma : E_1 \longrightarrow E_2$.

The SQIsignHD way [DLRW23]

- Compute $I \sim I_\phi$ of norm $q \simeq \sqrt{p}$ such that $\ell^e - q$ is a prime $\equiv 1 \bmod 4$.

A new algorithm for effective Deuring correspondence

Problem: Given $\phi : E_1 \longrightarrow E_2$, I_ϕ, $\mathcal{O}_1 \cong \mathrm{End}(E_1)$ and $\mathcal{O}_2 \cong \mathrm{End}(E_2)$ (secret), find another path $\sigma : E_1 \longrightarrow E_2$.

The SQIsign way [DKLPW20]

- Compute $I \sim I_\phi$ random of smooth norm $\simeq p^{15/4}$ via [KLPT14].
- Translate I into $\sigma : E_1 \longrightarrow E_2$.

The SQIsignHD way [DLRW23]

- Compute $I \sim I_\phi$ of norm $q \simeq \sqrt{p}$ such that $\ell^e - q$ is a prime $\equiv 1 \bmod 4$.
- Evaluate $\sigma : E_1 \longrightarrow E_2$ associated to I on $E_1[\ell^e]$, using ϕ.

A new algorithm for effective Deuring correspondence

Problem: Given $\phi : E_1 \longrightarrow E_2$, I_ϕ, $\mathcal{O}_1 \cong \mathrm{End}(E_1)$ and $\mathcal{O}_2 \cong \mathrm{End}(E_2)$ (secret), find another path $\sigma : E_1 \longrightarrow E_2$.

The SQIsign way [DKLPW20]

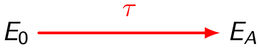
- Compute $I \sim I_\phi$ random of smooth norm $\simeq p^{15/4}$ via [KLPT14].
- Translate I into $\sigma : E_1 \longrightarrow E_2$.

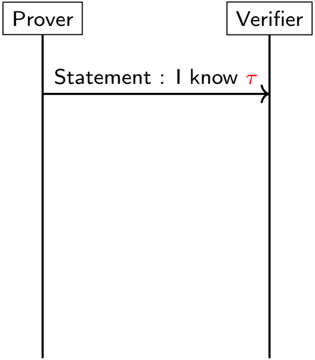
The SQIsignHD way [DLRW23]

- Compute $I \sim I_\phi$ of norm $q \simeq \sqrt{p}$ such that $\ell^e - q$ is a prime $\equiv 1 \mod 4$.
- Evaluate $\sigma : E_1 \longrightarrow E_2$ associated to I on $E_1[\ell^e]$, using ϕ.
- $(q, \sigma(E_1[\ell^e]))$, is sufficient to represent σ.
- We can then compute $F \in \mathrm{End}(E_1^2 \times E_2^2)$ embedding σ.

SQIsignHD

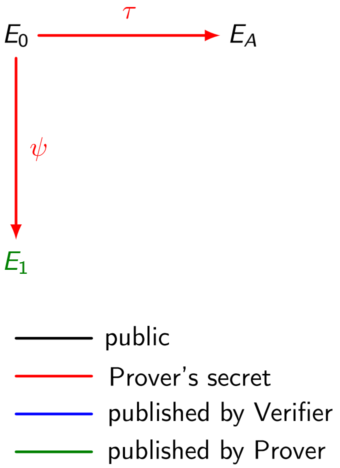
The SQIsignHD identification scheme [DLRW23]

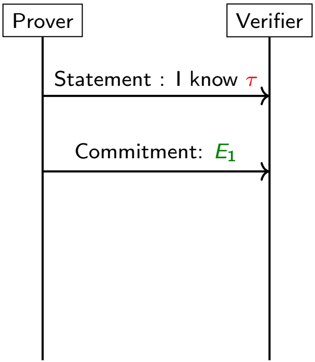




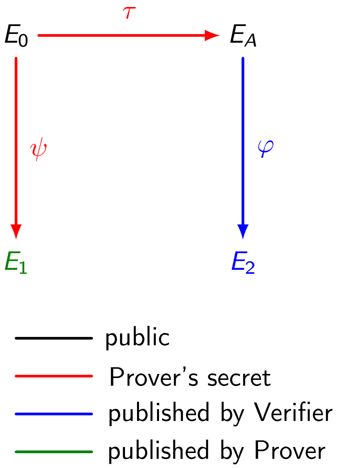
- public
- Prover's secret
- published by Verifier
- published by Prover

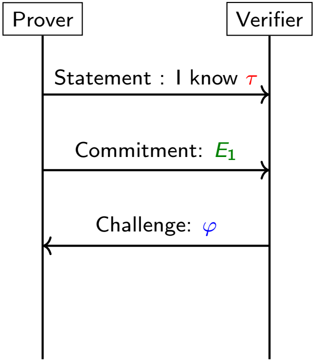
The SQIsignHD identification scheme [DLRW23]





The SQIsignHD identification scheme [DLRW23]

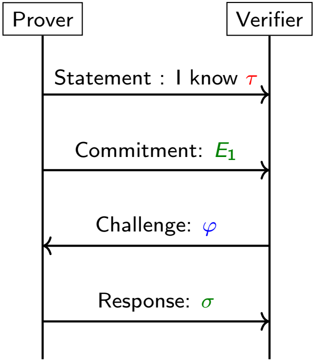




The SQIsignHD identification scheme [DLRW23]

$$\begin{tikzcd} E_0 \arrow[r, "\tau"] \arrow[d, "\psi"] & E_A \arrow[d, "\varphi"] \\ E_1 \arrow[r, "\sigma"] & E_2 \end{tikzcd}$$

public
Prover's secret
published by Verifier
published by Prover



The SQIsignHD identification scheme [DLRW23]

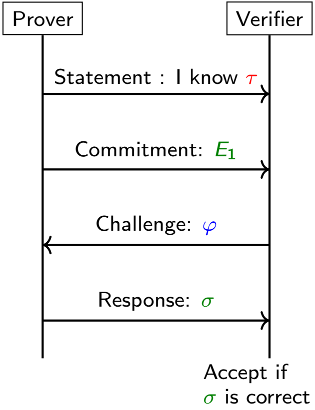
$$\begin{tikzcd} E_0 \arrow[r, "\tau"] \arrow[d, "\psi"'] & E_A \arrow[d, "\varphi"] \\ E_1 \arrow[r, "\sigma"] & E_2 \end{tikzcd}$$

public

Prover's secret

published by Verifier

published by Prover



The SQIsignHD identification scheme [DLRW23]

$$\begin{tikzcd}
E_0 \arrow[r, "\tau"] \arrow[d, "\psi"] & E_A \arrow[d, "\varphi"] \\
E_1 \arrow[r, "\sigma"] & E_2
\end{tikzcd}$$

public
Prover's secret
published by Verifier
published by Prover

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]

$$\begin{tikzcd} E_0 \arrow[r, "\tau"] \arrow[d, "\psi"] & E_A \arrow[d, "\varphi"] \\ E_1 \arrow[r, "\sigma"] & E_2 \end{tikzcd}$$

public

Prover's secret

published by Verifier

published by Prover

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

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

Very fast ! 28 ms in C.

The SQIsignHD identification scheme [DLRW23]

$$\begin{tikzcd} E_0 \arrow[r, "\tau"] \arrow[d, "\psi"] & E_A \arrow[d, "\varphi"] \\ E_1 \arrow[r, "\sigma"] & E_2 \end{tikzcd}$$

public

Prover's secret

published by Verifier

published by Prover

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

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

Very fast ! 28 ms in C.

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

The SQIsignHD identification scheme [DLRW23]

$$\begin{tikzcd} E_0 \arrow[r, "\tau"] \arrow[d, "\psi"'] & E_A \arrow[d, "\varphi"] \\ E_1 \arrow[r, "\sigma"] & E_2 \end{tikzcd}$$

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

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

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

Very fast ! 28 ms in C.

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

Proof of concept.
850 ms in `sagemath`.

Comparison of SQIsignHD with SQIsign

	SQIsign	SQIsignHD
Security	✗ Ad-hoc heuristic: • Distribution of σ.	✓ Simpler heuristics: • Oracle (RUGDIO); • Distribution of E_1.
Signing time	✗ 400 ms for NIST-1	✓ 28 ms for NIST-1
Signature size	✓ 204 bytes for NIST-1	✓ 109 bytes for NIST-1
Verification	✓ Fast (6 ms for NIST-1)	✗ 850 ms for NIST-1 in `sagemath`

Thank you for listening.

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