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

Inria
Institut de Mathématiques de Bordeaux
CANARI

The Deuring correspondence

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 $\mathcal{O}\theta$
$\deg(\varphi)$	$\mathrm{nrd}(I_\varphi)$

Hard and easy problems

Hard problems

- **Supersingular Isogeny Problem:** Given two supersingular elliptic curves $E_1, E_2/\mathbb{F}_{p^2}$, find an isogeny $\varphi : E_1 \longrightarrow E_2$.
- **Supersingular End Ring Problem:** Given a supersingular elliptic curve $E/\mathbb{F}_{p^2}$, compute $\mathrm{End}(E)$.
- These two problems are equivalent [Wes22].

Easy problems

- **Connecting ideal:** Given two maximal orders $\mathcal{O}_1, \mathcal{O}_2 \subset \mathcal{B}_{p,\infty}$, find a left $\mathcal{O}_1$-ideal I that is also a right $\mathcal{O}_2$-ideal.
- **Vélu**: Given $G = \ker(\varphi)$ (with $\#G$ smooth), compute φ [Vél71].
- **Quaternion path problem:** Given a left $\mathcal{O}$-ideal I, find $J \sim I$ of smooth norm [KLPT14].
- **Ideal translation:** Given a left $\mathcal{O}$-ideal I of smooth norm, compute the associated isogeny φ_I [DKLPW20].

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 KLPT.
- Translate J into an isogeny $\varphi_J : E_1 \longrightarrow E_2$.

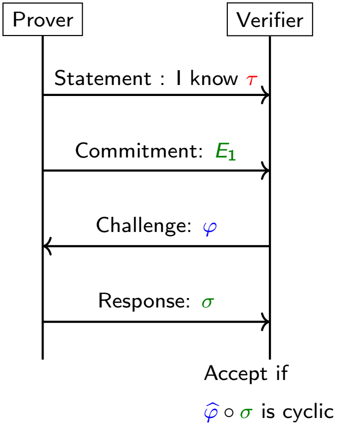
Becomes hard when $\mathrm{End}(E_1)$ or $\mathrm{End}(E_2)$ is unknown.

SQIsign and effective Deuring correspondence

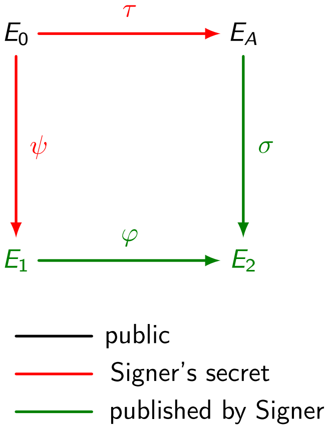
The SQIsign identification scheme [DKLPW20; FLLW23]

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

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



Fiat-Shamir transform [FS87]



Signature: message m, public key E_A, secret key τ.

- Commitment $\psi : E_0 \longrightarrow E_1$.
- Challenge $\varphi := H(E_1, m)$ (where H is a hash function).
- Compute and send signature (E_1, σ) to the verifier.

Verification: $E_A, m, (E_1, \sigma)$.

- Recompute $\varphi := H(E_1, m)$.
- Verify that $\widehat{\varphi} \circ \sigma$ is cyclic.

How to compute the signature σ ?

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

- Compute $J := \overline{I_\tau} \cdot I_\psi \cdot I_\varphi$.
- Find $I \sim J$ random of norm $\mathrm{nrd}(I) = \ell^e$ (KLPT).
- Compute σ associated to I.

Ideal-to-isogeny I [GPS20]

Input: $E/\mathbb{F}_{p^2}$ supersingular, $\mathcal{O} \cong \mathrm{End}(E)$ and I a left $\mathcal{O}$-ideal of smooth norm.

Output: $\varphi_I : E \longrightarrow E_I$.

- Compute
$$E[I] := \{P \in E \mid \forall \alpha \in I, \quad \alpha(P) = 0\}.$$
- Compute φ_I of kernel $E[I]$ in $O(\mathrm{poly}(\max_{\ell | \mathrm{nrd}(I)} \ell))$ operations over $\mathbb{F}_{p^k}$, where $E[I] \subseteq E(\mathbb{F}_{p^k})$.

Issue: If I is a KLPT output, then $\mathrm{nrd}(I) \simeq p^{15/4} \gg p$ so k is exponentially big. Not practical for SQIsign !

Ideal-to-isogeny II [FLLW23]

Main idea: Cut the computation into smaller pieces. Write

$$I = I_0 \cdot I_1 \cdots I_{n-1} \quad \text{and} \quad \varphi_I = \varphi_{n-1} \circ \cdots \circ \varphi_1 \circ \varphi_0$$

with $\mathrm{nrd}(I_0) = \cdots = \mathrm{nrd}(I_{n-1}) = \ell^f$.

$$\begin{tikzcd}
E = E_0 \arrow[r, "I_0", "\varphi_0"'] & E_1 \arrow[loop above, "\theta_1"] \arrow[r, "I_1", "\varphi_1"'] & E_2 \arrow[loop above, "\theta_2"] & \cdots & E_{n-1} \arrow[loop above, "\theta_{n-1}"] \arrow[r, "I_{n-1}", "\varphi_{n-1}"'] & E_n = E_I
\end{tikzcd}$$

The endomorphisms θ_i are meant to refresh the ℓ^f-torsion.

Torsion requirements: $\ell^f T | p^2 - 1$ so that $E[\ell^f T] \subseteq E(\mathbb{F}_{p^4})$, where $\deg(\theta_i) = T^2$ and $T \simeq p^{5/4}$.

Issue: This is slow!

Higher dimensional isogenies

Another method to compute σ [DLRW23]

Issue in SQIsign: $\deg(\sigma)$ has to be smooth $\deg(\sigma) = \ell^e \simeq p^{15/4}$.

Our idea: Take $\deg(\sigma)$ non smooth. Then $\deg(\sigma) \simeq \sqrt{p}$.

- Evaluate σ on $E_A[\ell^e] \subseteq E_A(\mathbb{F}_{p^2})$.
- Use the following algorithm to evaluate σ everywhere.

Theorem (Robert, 2022)

Let $\sigma : E \longrightarrow E'$ of degree $q < \ell^e$. There exists a polynomial time algorithm with:

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

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

Evaluating σ

Main idea: Use the alternate path $\varphi \circ \psi \circ \widehat{\tau}$.

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

- Let $\gamma := \widehat{\psi} \circ \widehat{\varphi} \circ \sigma \circ \tau \in \mathrm{End}(E_0)$.
- We have $\mathcal{O}_0\gamma = I_\tau \cdot I \cdot \overline{I_\varphi} \cdot \overline{I_\psi}$ so we can compute γ.
- Then:
$$[D_\psi D_\varphi D_\tau]\sigma = \varphi \circ \psi \circ \gamma \circ \widehat{\tau}$$
- We can evaluate σ on $P \in E_A[\ell^e]$ provided $(D_\psi D_\varphi D_\tau) \wedge \ell = 1$:
$$\sigma(P) = [\lambda]\varphi \circ \psi \circ \gamma \circ \widehat{\tau}(P),$$
with $\lambda D_\psi D_\varphi D_\tau \equiv 1 \mod \ell^e$.

d-isogenies and the dual isogeny in higher dimension

Definition (d-isogeny)

Let $\varphi : (A, \lambda_A) \longrightarrow (B, \lambda_B)$ be an isogeny between two principally polarized abelian varieties (PPAV). We define:

- $\widetilde{\varphi} := \lambda_A^{-1} \circ \widehat{\varphi} \circ \lambda_B : B \longrightarrow A$.

$$B \xrightarrow{\lambda_B} \widehat{B} \xrightarrow{\widehat{\varphi}} \widehat{A} \xrightarrow{\lambda_A^{-1}} A$$

- We say that φ is a <u>d-isogeny</u> if $\widetilde{\varphi} \circ \varphi = [d]_A$.

Kani's embedding lemma [Kan97]

Definition (isogeny diamond)

An (a, b)-isogeny diamond is a commutative diagram s.t.:

$$\begin{tikzcd} A' \arrow[r, "\varphi'"] & B' \\ A \arrow[u, "\psi"] \arrow[r, "\varphi"] & B \arrow[u, "\psi'"'] \end{tikzcd}$$

where φ, φ' are a-isogenies and ψ, ψ' are b-isogenies.

Lemma (Kani)

Consider the (a, b)-isogeny diamond on the left. Then:

- $F : A \times B' \longrightarrow B \times A'$,

$$F := \begin{pmatrix} \varphi & \widetilde{\psi}' \\ -\psi & \widetilde{\varphi}' \end{pmatrix}$$

is a d-isogeny with $d = a + b$.

- *If $a \wedge b = 1$, then*

$$\ker(F) = \{(\widetilde{\varphi}(x), \psi'(x)) \mid x \in B[d]\}.$$

Application of Kani's lemma to SQIsignHD

Embedding σ in higher dimension:

- Let $q = \deg(\sigma)$.
- Let $a_1, a_2 \in \mathbb{Z}$ s.t. $a_1^2 + a_2^2 + q = \ell^e$.
- q should be good: $\ell^e - q$ prime $\equiv 1 \mod 4$.
- Consider the isogeny diamond:

$$\begin{tikzcd} E_2^2 \arrow[r, "\alpha_2"] & E_2^2 \\ E_A^2 \arrow[u, "\Sigma"] \arrow[r, "\alpha_A"] & E_A^2 \arrow[u, "\Sigma"'] \end{tikzcd}$$

where $\Sigma := \mathrm{Diag}(\sigma, \sigma)$ and for $i = A, 2$,

$$\alpha_i := \begin{pmatrix} a_1 & a_2 \\ -a_2 & a_1 \end{pmatrix} \in \mathrm{End}(E_i^2).$$

Application of Kani's lemma to SQIsignHD

Embedding σ in higher dimension:

- Then
$$F := \begin{pmatrix} \alpha_1 & \widetilde{\Sigma} \\ -\Sigma & \widetilde{\alpha}_A \end{pmatrix} \in \mathrm{End}(E_A^2 \times E_2^2).$$
is an ℓ^e-isogeny.
- And
$$\ker(F) = \{([a_1]R - [a_2]S, [a_2]R + [a_1]S, \sigma(R), \sigma(S)) \mid R, S \in E_A[\ell^e]\}.$$
- F can be computed in polynomial time [LR12; LR15; LR23; DLRW23].

Algorithm for higher dimensional isogeny computations

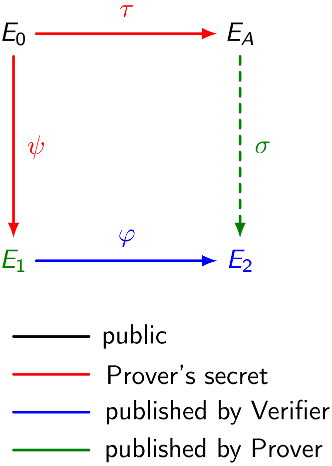
- The ℓ^e-isogeny F can be computed as a chain of ℓ-isogenies:

$$\mathcal{A}_0 \xrightarrow{F_0} \mathcal{A}_1 \xrightarrow{F_2} \mathcal{A}_2 \quad \cdots \quad \mathcal{A}_{e-1} \xrightarrow{F_e} \mathcal{A}_e$$

- Each ℓ-isogeny can be computed in $O(\ell^g)$ efficiently in the Θ-model [LR12; LR15; LR23; DLRW23].
- The whole chain can be computed in time $O(\ell^g e \log(e))$ [JD11; DLRW23].
- This method is valid in any dimension g.

SQIsignHD: signing with higher dimensional isogenies

SQIsignHD identification scheme [DLRW23]



Secret key: τ

Commitment: E_1

Challenge: φ

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

- Compute $I \sim \overline{I_\tau} \cdot I_\psi \cdot I_\varphi$ random of norm $q \simeq \sqrt{p}$.
- Compute a canonical basis (P_1, P_2) of $E_A[\ell^e]$.
- Evaluate $\sigma = \varphi_I$ on (P_1, P_2).
- Send $(q, \sigma(P_1), \sigma(P_2))$.

Very fast !

SQIsignHD identification scheme [DLRW23]

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

public

Prover's secret

published by Verifier

published by Prover

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

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

- Find $a_1, a_2 \in \mathbb{Z}$ such that $a_1^2 + a_2^2 + q = \ell^e$ (Cornacchia).
- Compute the canonical basis (P_1, P_2) of $E_A[\ell^e]$.
- Compute $\ker(F)$, knowing $a_1, a_2, P_1, P_2, \sigma(P_1), \sigma(P_2)$.
- Compute F.
- Accept if $F \in \mathrm{End}(E_A^2 \times E_2^2)$ and $F(Q, 0, 0, 0) = ([a_1]Q, -[a_2]Q, *, 0)$.

Proof of concept.

Fiat-Shamir transform [FS87] of SQIsignHD

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

public

Signer's secret

published by Signer

Signature: message m, public key E_A, secret key τ.

- Commitment $\psi : E_0 \longrightarrow E_1$.
- Challenge $\varphi := H(E_1, m)$ (where H is a hash function).
- Compute and send signature $(E_1, q, \sigma(P_1), \sigma(P_2))$ to the verifier.

Verification: $E_A, m, (E_1, q, \sigma(P_1), \sigma(P_2))$.

- Recompute $\varphi := H(E_1, m)$.
- Use $\varphi, q, \sigma(P_1), \sigma(P_2)$ to compute the embedding F of σ.
- Check that $F \in \mathrm{End}(E_A^2 \times E_2^2)$ and $F(Q, 0, 0, 0) = ([a_1]Q, -[a_2]Q, *, 0)$.

Parameter choice

- **Characteristic:** as in SIDH,

$$p = c\ell^f \ell'^{f'} - 1.$$

  with c small.

- In practice $\ell = 2$ and $\ell' = 3$. For NIST-1, $p = 13 \cdot 2^{126} \cdot 3^{78} - 1$.
- **Use of ℓ^f-torsion:** the 4-dimensional isogeny F.
- **Use of $\ell'^{f'}$-torsion:** τ, ψ, φ.
- $E_0 : y^2 = x^3 + x$ defined over $\mathbb{F}_p$ ($p \equiv 3 \mod 4$). $\mathrm{End}(E_0)$ is known.

Outline of the security analysis

Theorem (Fiat-Shamir, 1986)

Let ID be an identification protocol that is:

- ***Complete:*** *a honest execution is always accepted by the verifier.*
- ***Sound:*** *an attacker cannot "guess" a response.*
- ***Zero-knowledge:*** *the response does not leak any information on the secret key.*

Then the Fiat-Shamir transform of ID is a universally unforgeable signature under chosen message attacks in the random oracle model.

Soundness

Similar to SQIsign

Proposition (Special soundness)

Given two transcripts $(E_1, \varphi, q, \sigma(P_1), \sigma(P_2)), (E_1, \varphi', q', \sigma'(P_1'), \sigma'(P_2'))$ *with the same commitment* E_1 *and* $\varphi \neq \varphi'$, *we can extract* $\alpha \in \mathrm{End}(E_A)$ *non-scalar.*

Proof.

- Exctract σ from $(q, \sigma(P_1), \sigma(P_2))$ and σ' from $(q', \sigma'(P_1'), \sigma'(P_2'))$.
- Then $\alpha := \widehat{\sigma'} \circ \varphi' \circ \widehat{\varphi} \circ \sigma \in \mathrm{End}(E_A)$ is non-scalar.

$\square$

Zero-knowledge

Definition (Recall)

We say that an integer q is **good** if $\ell^e - q$ is a prime $\equiv 1 \mod 4$.

Definition (RUGDIO)

A random uniform good degree isogeny oracle (RUGDIO):
Input: A supersingular elliptic curve $E/\mathbb{F}_{p^2}$.
Output: An isogeny $\sigma : E \longrightarrow E'$ of good degree q s.t.

- E' is uniform among supersingular elliptic curves.
- Given E', σ is uniform among isogenies of good degree $E \longrightarrow E'$.

Zero-knowledge

Theorem

Assume that:

- *E_1 is computationally close to uniform.*
- *We have access to a RUGDIO.*

Then SQIsignHD is computationally honest-verifier zero-knowledge.

Proof.

We build a simulator $\mathcal{S}$ of protocol transcripts:

- $\mathcal{S}$ calls the RUGDIO to generate $(q, \sigma(P_1), \sigma(P_2))$.
- $\mathcal{S}$ generates a random challenge $\widehat{\varphi} : E_2 \longrightarrow E_1$.
- $\mathcal{S}$ outputs $(E_1, \varphi, q, \sigma(P_1), \sigma(P_2))$.

$\square$

Zero-knowledge: comparison with SQIsign

Heuristic assumptions to prove the zero-knowledge property

In SQIsign:

- $\sigma : E_1 \longrightarrow E_2$ is computationally indistinguishable from a random isogeny of degree ℓ^e.

In SQIsignHD:

- E_1 is computationally close to uniform.
- We have access to a RUGDIO.

Fast and compact signatures

- **Signature time:** 28 ms on a 13th Gen Intel(R) Core(TM) i5-1335U (4600MHz) CPU.

Signature size comparison

	In SQIsign	In SQIsignHD
Asymptotic (in bits)	$\sim 23/4 \log_2(p)$	$\sim 13/4 \log_2(p)$
NIST-1 security level (in bytes)	204	109

A promising POC for the verification

Timing: 855 ms in `sagemath` with $p = 13 \cdot 2^{126} \cdot 3^{78} - 1$ on a 13th Gen Intel(R) Core(TM) i5-1335U (4600MHz) CPU.

- **Challenge computation (φ):** 60 ms.
- **Dimension 4 2^{142}-isogeny:** 770 ms with Θ-coordinates of level 2.
  - $F \in \mathrm{End}(E_A^2 \times E_2^2)$ is divided in two:

$$E_A^2 \times E_2^2 \xrightarrow{F_1} \mathcal{C} \xleftarrow{\widetilde{F}_2} E_A^2 \times E_2^2$$

  - Compute F_1 and $\widetilde{F}_2$.
  - Check that codomains of F_1 and $\widetilde{F}_2$ match.
  - Compute $F_2 := \widetilde{\widetilde{F}}_2$
- **Isogeny evaluation:** 25 ms.

$$F(Q,0,0,0) = F_2 \circ F_1(Q,0,0,0)$$

Conclusion

Comparison of SQIsignHD with SQIsign

	SQIsign	SQIsignHD
Security	✗ Ad-hoc heuristic: • Distribution of σ.	✓ Simpler heuristics: • 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