SQIsignHD: New Dimensions in Cryptography

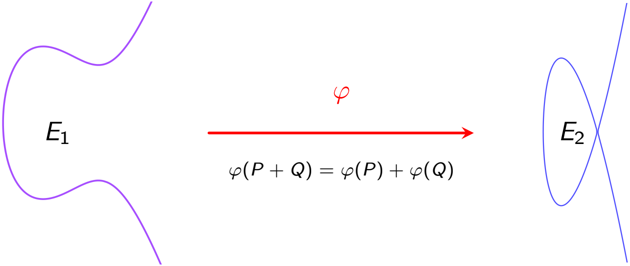
Pierrick Dartois
Joint work with Antonin Leroux, Damien Robert and Benjamin Wesolowski

Acknowledgements to Luca De Feo

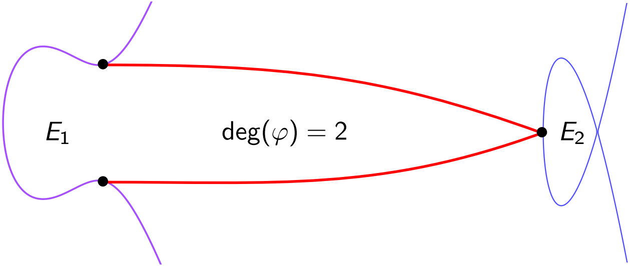
Eurocrypt 2024, May 27

The Deuring correspondence

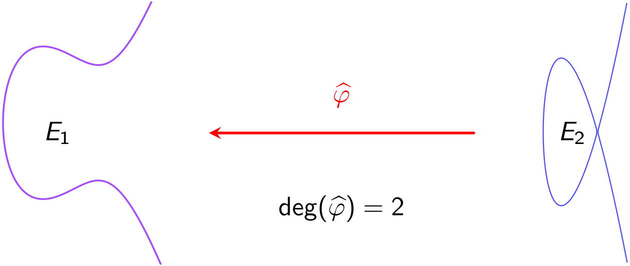
Isogenies



Isogenies - degree



Isogenies - the dual isogeny



Isogeny chains

$$\deg(\varphi_n \circ \cdots \circ \varphi_1) = \prod_{i=1}^{n} \deg(\varphi_i)$$

Isogeny chains

- Conversely, if:

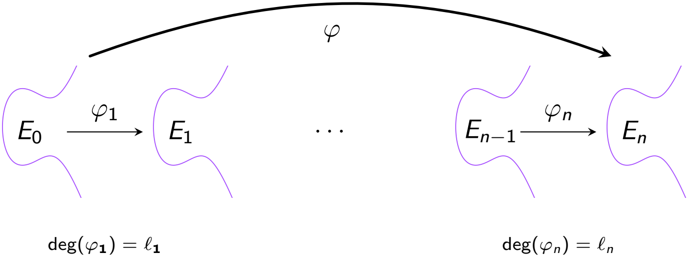
$$\deg(\varphi) = \prod_{i=1}^{n} \ell_i$$

Isogeny chains

- Conversely, if:

$$\deg(\varphi) = \prod_{i=1}^{n} \ell_i$$

- Then, we can decompose $\varphi = \varphi_n \circ \cdots \circ \varphi_1$.

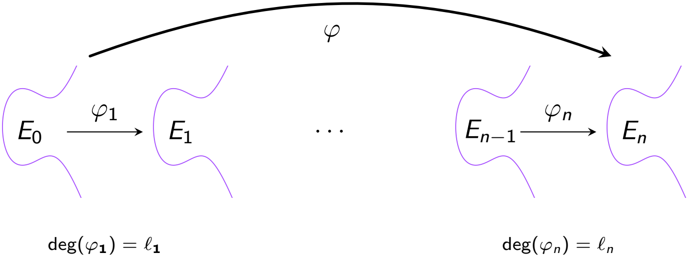


Isogeny chains

- Conversely, if:

$$\deg(\varphi) = \prod_{i=1}^{n} \ell_i$$

- Then, we can decompose $\varphi = \varphi_n \circ \cdots \circ \varphi_1$.



- Knowing $\ker(\varphi)$, φ can be computed in polynomial time.

Quaternions and supersingular elliptic curves

Definition (Quaternion algebra)

- Let p be a prime $\equiv 3 \mod 4$. The **quaternion algebra** ramifying at p and ∞ is:
$$\mathcal{B}_{p,\infty} := \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}ij,$$
with $i^2 = -1$, $j^2 = -p$, $ij = -ji$.
- An **order** $\mathcal{O} \subseteq \mathcal{B}_{p,\infty}$ is a rank 4 lattice which is also a subring.

Quaternions and supersingular elliptic curves

Definition (Quaternion algebra)

- Let p be a prime $\equiv 3 \mod 4$. The **quaternion algebra** ramifying at p and ∞ is:

$$\mathcal{B}_{p,\infty} := \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}ij,$$

  with $i^2 = -1$, $j^2 = -p$, $ij = -ji$.
- An **order** $\mathcal{O} \subseteq \mathcal{B}_{p,\infty}$ is a rank 4 lattice which is also a subring.

Definition (Endomorphism ring)

Let E be an elliptic curve, the **endomorphism ring** of E is:

$$\text{End}(E) = \{\text{Isogenies } \varphi : E \longrightarrow E\} \cup \{0\}$$

Quaternions and supersingular elliptic curves

Definition (Quaternion algebra)

- Let p be a prime $\equiv 3 \mod 4$. The **quaternion algebra** ramifying at p and ∞ is:
$$\mathcal{B}_{p,\infty} := \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}ij,$$
with $i^2 = -1$, $j^2 = -p$, $ij = -ji$.
- An **order** $\mathcal{O} \subseteq \mathcal{B}_{p,\infty}$ is a rank 4 lattice which is also a subring.

Definition (Endomorphism ring)

Let E be an elliptic curve, the **endomorphism ring** of E is:

$$\mathrm{End}(E) = \{\text{Isogenies } \varphi : E \longrightarrow E\} \cup \{0\}$$

Definition (Supersingular elliptic curve)

An elliptic curve E defined over $\overline{\mathbb{F}}_p$ is **supersingular** if $\mathrm{End}(E)$ is isomorphic to a maximal order of $\mathcal{B}_{p,\infty}$ (maximal for the inclusion).

The Deuring correspondence

Supersingular elliptic curves	Quaternions
$j(E)$ or $j(E)^p$ supersingular	$\mathcal{O} \cong \mathrm{End}(E)$ maximal order in $\mathcal{B}_{p,\infty}$

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

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
$\varphi, \psi : E \longrightarrow E'$	$I_\varphi \sim I_\psi$ $(I_\psi = I_\varphi \alpha,\ \alpha \in \mathcal{B}_{p,\infty})$

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
$\varphi, \psi : E \longrightarrow E'$	$I_\varphi \sim I_\psi$ $(I_\psi = I_\varphi \alpha,\ \alpha \in \mathcal{B}_{p,\infty})$
$\widehat{\varphi}$	$\overline{I_\varphi}$

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
$\varphi, \psi : E \longrightarrow E'$	$I_\varphi \sim I_\psi$ $(I_\psi = I_\varphi \alpha,\ \alpha \in \mathcal{B}_{p,\infty})$
$\widehat{\varphi}$	$\overline{I_\varphi}$
$\varphi \circ \psi$	$I_\psi \cdot I_\varphi$

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
$\varphi, \psi : E \longrightarrow E'$	$I_\varphi \sim I_\psi$ $(I_\psi = I_\varphi \alpha,\ \alpha \in \mathcal{B}_{p,\infty})$
$\widehat{\varphi}$	$\overline{I_\varphi}$
$\varphi \circ \psi$	$I_\psi \cdot I_\varphi$
$\deg(\varphi)$	$\mathrm{nrd}(I_\varphi) = \sqrt{[\mathcal{O} : I_\varphi]}$

Computing isogenies via the Deuring correspondence

Problem: How to compute isogenies between elliptic curves of known endomorphism rings?

Computing isogenies via the Deuring correspondence

Problem: How to compute isogenies between elliptic curves of known endomorphism rings?

- 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 $\mathcal{O}_2$ (left $\mathcal{O}_1$-ideal and right $\mathcal{O}_2$-ideal).
- 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

Problem: How to compute isogenies between elliptic curves of known endomorphism rings?

- 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 $\mathcal{O}_2$ (left $\mathcal{O}_1$-ideal and right $\mathcal{O}_2$-ideal).
- 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

Problem: How to compute isogenies between elliptic curves of known endomorphism rings?

- 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 $\mathcal{O}_2$ (left $\mathcal{O}_1$-ideal and right $\mathcal{O}_2$-ideal).
- 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

Problem: How to compute isogenies between elliptic curves of known endomorphism rings?

- 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 $\mathcal{O}_2$ (left $\mathcal{O}_1$-ideal and right $\mathcal{O}_2$-ideal).
- 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 in practice 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* $\deg(\sigma) + a_1^2 + a_2^2 = 2^e$*. Then:*

- $\sigma : E_1 \longrightarrow E_2$ *can be represented by the dimension 4 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* $E_1[2^e]$*.*

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

Kani's embedding lemma

More on Robert's theorem:

- $\ker(F)$ can be computed with $\sigma(E_1[2^e])$.

Kani's embedding lemma

More on Robert's theorem:

- $\ker(F)$ can be computed with $\sigma(E_1[2^e])$.
- F can be decomposed into a chain of "smaller" dimension 4 isogenies:

$$E_1^2 \times E_2^2 \xrightarrow{F_1} \mathcal{A}_1 \xrightarrow{F_2} \mathcal{A}_2 \quad \cdots \quad \mathcal{A}_{e-1} \xrightarrow{F_e} E_1^2 \times E_2^2$$

- Using theta coordinates, this chain can be computed with $O(e \log(e))$ finite field operations.

Kani's embedding lemma

More on Robert's theorem:

- $\ker(F)$ can be computed with $\sigma(E_1[2^e])$.
- F can be decomposed into a chain of "smaller" dimension 4 isogenies:

$$E_1^2 \times E_2^2 \xrightarrow{F_1} \mathcal{A}_1 \xrightarrow{F_2} \mathcal{A}_2 \quad \cdots \quad \mathcal{A}_{e-1} \xrightarrow{F_e} E_1^2 \times E_2^2$$

- Using theta coordinates, this chain can be computed with $O(e\log(e))$ finite field operations.
- We have:

$$F(P,0,0,0) = ([a_1]P, -[a_2]P, -\sigma(P), 0)$$

so we can evaluate σ by evaluating F.

Kani's embedding lemma

Corollary (Robert, 2022)

Let $\sigma : E_1 \longrightarrow E_2$ *of degree* $q < 2^e$ *such that* $2^e - q$ *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* $E_1[2^e]$ *and* $Q \in E_1(\mathbb{F}_{p^2})$.
- ***Output:*** $\sigma(Q)$.

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 isogeny $\sigma : E_1 \longrightarrow E_2$.

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 isogeny $\sigma : E_1 \longrightarrow E_2$.

In SQIsign [DFKLPW20]

1. 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 isogeny $\sigma : E_1 \longrightarrow E_2$.

In SQIsign [DFKLPW20]

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

In SQIsign [DFKLPW20]

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

In SQIsignHD (this work)

1. Compute $I \sim I_\phi$ random of norm $q \simeq \sqrt{p}$ such that $2^e - q$ is a prime $\equiv 1 \mod 4$.

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 isogeny $\sigma : E_1 \longrightarrow E_2$.

In SQIsign [DFKLPW20]

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

In SQIsignHD (this work)

1. Compute $I \sim I_\phi$ random of norm $q \simeq \sqrt{p}$ such that $2^e - q$ is a prime $\equiv 1 \mod 4$.
2. Evaluate $\sigma : E_1 \longrightarrow E_2$ associated to I on $E_1[2^e]$, 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 isogeny $\sigma : E_1 \longrightarrow E_2$.

In SQIsign [DFKLPW20]

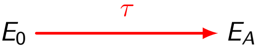
1. Compute $I \sim I_\phi$ random of smooth norm $\simeq p^{15/4}$ via [KLPT14].
2. Translate I into $\sigma : E_1 \longrightarrow E_2$.

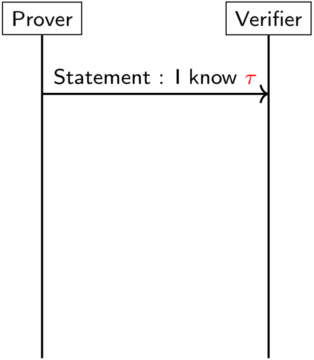
In SQIsignHD (this work)

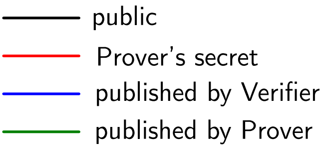
1. Compute $I \sim I_\phi$ random of norm $q \simeq \sqrt{p}$ such that $2^e - q$ is a prime $\equiv 1 \mod 4$.
2. Evaluate $\sigma : E_1 \longrightarrow E_2$ associated to I on $E_1[2^e]$, using ϕ.
3. $(q, \sigma(E_1[2^e]))$, is sufficient to represent σ.
4. Compute $F \in \mathrm{End}(E_1^2 \times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

SQIsignHD

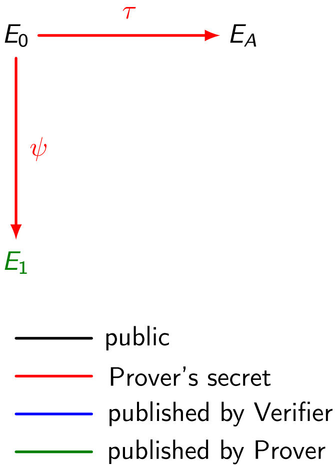
The SQIsignHD identification scheme

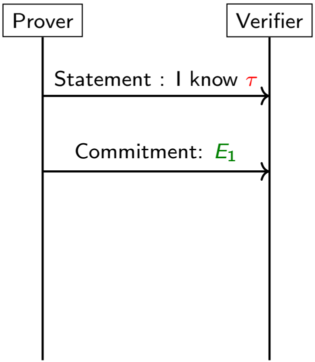




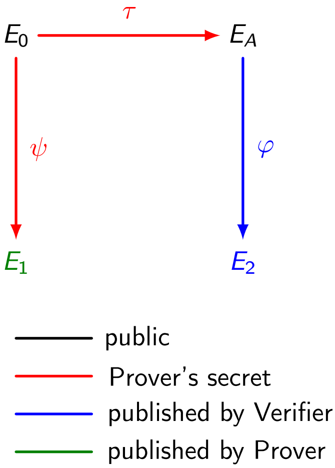


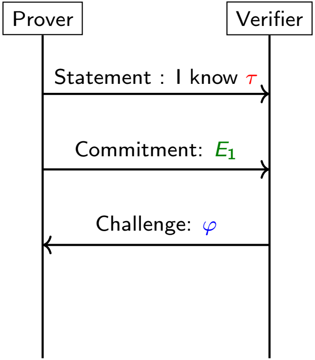
The SQIsignHD identification scheme



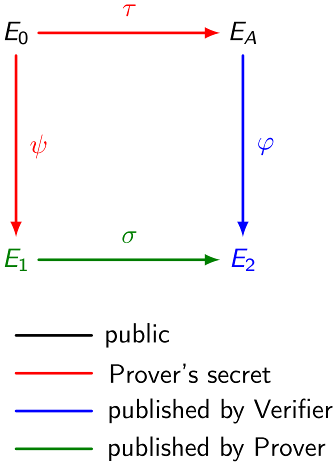


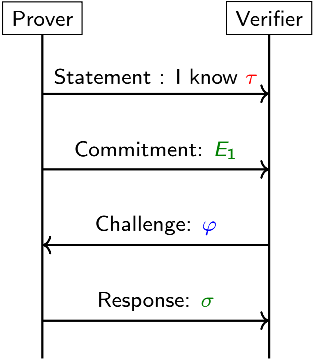
The SQIsignHD identification scheme



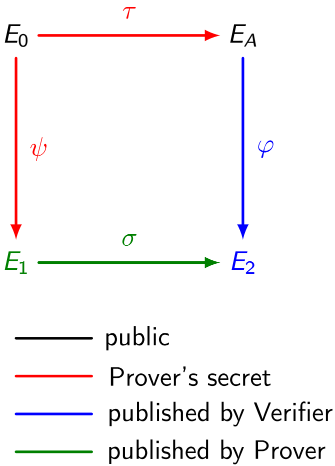


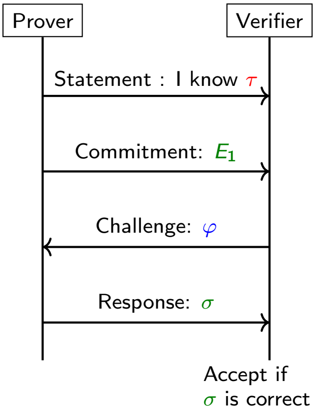
The SQIsignHD identification scheme



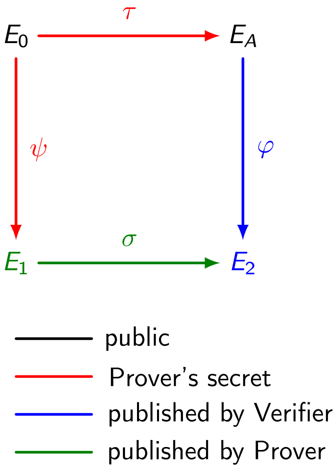


The SQIsignHD identification scheme





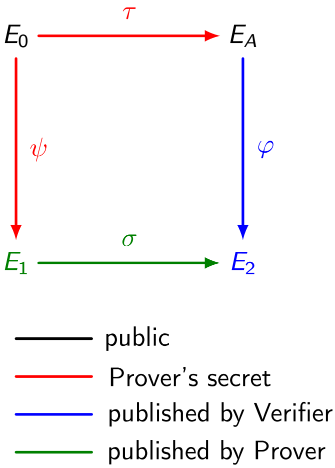
The SQIsignHD identification scheme



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

- (P_1, P_2) is a basis of $E_1[2^e]$;
- $q := \deg(\sigma)$.

The SQIsignHD identification scheme

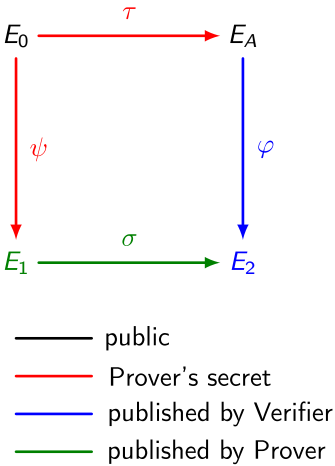


Response: $(q, \sigma(P_1), \sigma(P_2))$, where:

- (P_1, P_2) is a basis of $E_1[2^e]$;
- $q := \deg(\sigma)$.

Very fast ! 28 ms in C.

The SQIsignHD identification scheme



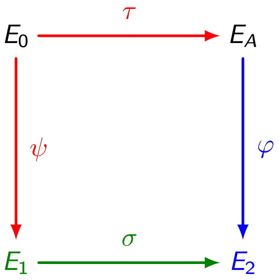
Response: $(q, \sigma(P_1), \sigma(P_2))$, where:

- (P_1, P_2) is a basis of $E_1[2^e]$;
- $q := \deg(\sigma)$.

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



- 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 $E_1[2^e]$;
- $q := \deg(\sigma)$.

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.
600 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.
Scalability	✗ $\prod_{i=1}^{n} \ell_i \| p^2 - 1$	✓ $p = c \cdot 2^f \cdot 3^{f'} - 1$
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)	✗ 600 ms for NIST-1 in sagemath