WaterSQI: SQIing on the Sea Side

A proof of knowledge of the endomorphism ring for oriented curves

Tako Boris Fouotsa, EPFL

Swissogeny days #3, ETH Zurich - June 26 2025

Outline

Motivation

Supersingular isogenies and the Deuring correspondence

SQISign

WaterSQI

Motivation

Identification protocols

$\mathcal{L} = \{ \ (x, w) \ \}$ arising from a hard relation

Prover(x, w)		**Verifier**(x)
$(\mathsf{com}, \mathsf{P}_{\mathsf{state}}) \leftarrow \mathcal{P}_1(x, w)$	$\xrightarrow{\ \mathsf{com}\ }$	
	$\xleftarrow{\ \mathsf{ch}\ }$	$\mathsf{ch} \leftarrow\!\!\$\ \mathcal{C}$
$\mathsf{rsp} \leftarrow \mathcal{P}_2(\mathsf{P}_{\mathsf{state}}, \mathsf{ch})$	$\xrightarrow{\ \mathsf{rsp}\ }$	
		$\mathcal{V}(x, \mathsf{com}, \mathsf{ch}, \mathsf{rsp}) = \text{Accept/Reject}$

Identification protocols

Prover(x, w)		**Verifier**(x)
$(\mathsf{com}, \mathsf{P}_{\mathsf{state}}) \leftarrow \mathcal{P}_1(x, w)$	$\xrightarrow{\mathsf{com}}$	
	$\xleftarrow{\mathsf{ch}}$	$\mathsf{ch} \leftarrow\!\!\$\ \mathcal{C}$
$\mathsf{rsp} \leftarrow \mathcal{P}_2(\mathsf{P}_{\mathsf{state}}, \mathsf{ch})$	$\xrightarrow{\mathsf{rsp}}$	
		$\mathcal{V}(x, \mathsf{com}, \mathsf{ch}, \mathsf{rsp}) = \mathrm{Accept}/\mathrm{Reject}$

Completeness: V accepts when P knows a witness and they follow the protocol.
Special Soundness: $w \leftarrow \mathsf{extract}(x, (com, ch, rsp), (com, ch', rsp'))$, $ch \neq ch'$.
Special HVZK: given ch, $(com, ch, rsp) \leftarrow \mathsf{simulate}(x, ch)$ that is valid.

Identification protocols (2)

A dishonest P can always fool V with probability at least $1/\#\mathcal{C}$: guess *ch* and simulate the transcript.

In practice, we have two cases:

- $\#\mathcal{C} = O(\mathsf{exp}(\lambda))$, $1/\#\mathcal{C}$ is negligible, great!
  - ⋆ The case for SQIsign
- $\#\mathcal{C} = O(\mathsf{poly}(\lambda))$ (2 for example), $1/\#\mathcal{C}$ is not negligible, not great!
  - Solution: repeat the sigma protocol several times.
  - Consequence: huge efficiency/size overhead.
  - ⋆ The case for CSIDH (and friends) type identification protocols.

Question: Can we adapt SQIsign to the CSIDH (and friends) setting?

λ is the security parameter

Supersingular isogenies and the Deuring correspondence

Supersingular Isogenies

An *isogeny* $\phi : E \to E'$ is a rational map which is also a group morphism. The kernel of an isogeny is always finite.

Given a kernel, the corresponding isogeny can be computed using Vélu formulas.

The (seperable) degree of an isogeny is the size of its kernel.

Dual isogeny: $\widehat{\phi} : E' \to E$ such that $\widehat{\phi} \circ \phi = [\deg \phi]_E$ and $\phi \circ \widehat{\phi} = [\deg \phi]_{E'}$.

Pure (supersingular) isogeny problem: *given two supersingular elliptic curves E_1 and E_2, compute an isogeny $\phi : E_1 \to E_2$.*

Endomorphism ring problem: *given a supersingular elliptic curves E, compute its endomorphism ring $End(E)$.*

Endomorphism rings of supersingular elliptic curves

The endomorphism ring of a supersingular elliptic curve is isomorphic to a maximal order $\mathcal{O}$ in the quaternion algebra $\mathbb{Q}_{p,\infty}$.

If E is defined over $\mathbb{F}_p$, then

$$\mathcal{O}_p =: \mathrm{End}_{\mathbb{F}_p}(E) = \mathbb{Z}[\pi] \qquad \text{or} \qquad \mathcal{O}_p =: \mathrm{End}_{\mathbb{F}_p}(E) = \mathbb{Z}\left[\frac{\pi+1}{2}\right].$$

$\mathbb{F}_p$-rational isogenies (except the vertical 2-isogenies) arise from the action of the class group $\mathrm{cl}(\mathcal{O}_p)$. In this case, isogenies can be identified as ideals of $\mathcal{O}_p$ in a straightforward way.

Generally, if E is defined over $\mathbb{F}_{p^2}$, an isogeny $E \to E'$ can be seen as a left ideal of the endomorphism ring $\mathcal{O}$ of E; the translations from ideal to isogeny and isogeny to ideal are are less straightforward.

Deuring correspondence

Deuring correspondence		
$j(E)$, E supersingular	$\leftrightarrow$	Maximal orders $\mathcal{O}$ in $\mathcal{B}_{p,\infty}$
Isogeny $\phi : E_1 \to E_2$	$\leftrightarrow$	$\mathcal{O}_1$ − left $\mathcal{O}_2$ − right ideal I_ϕ
$\phi_1 : E_1 \to E_2, \phi_2 : E_1 \to E_2$	$\leftrightarrow$	Equivalent ideals $I_{\phi_1} \sim I_{\phi_2}(I_{\phi_1} = wI_{\phi_2})$
$\theta \in \mathrm{End}(E)$	$\leftrightarrow$	Principal ideal $\mathcal{O}w_\theta$
$Hom(E_1, E_2)$	$\leftrightarrow$	The rank 4 $\mathbb{Z}$ − lattice $I(\mathcal{O}_1, \mathcal{O}_2)$

Computing the correspondence: $\rightarrow$ *(hard)* $\leftarrow$ *(easy)*.

Most problems become easy when you know the endomorphism rings of the supersingular curves at play.

Our favourite curve E_0

$E_0 : y^2 = x^3 + x$ is supersingular if and only if $p \equiv 3 \mod 4$.

$\mathrm{End}(E_0)$ is generated by $1, \iota, \frac{\iota+\pi}{2}, \frac{1+\iota\circ\pi}{2}$ where $\iota : (x, y) \mapsto (-x, iy)$ $(i^2 = -1)$.

$\mathrm{End}(E_0)$ corresponds to the maximal order $\mathcal{O}_0$ generated by $1, i, \frac{i+j}{2}, \frac{1+k}{2}$ in $\mathbb{Q}_{p,\infty}$.

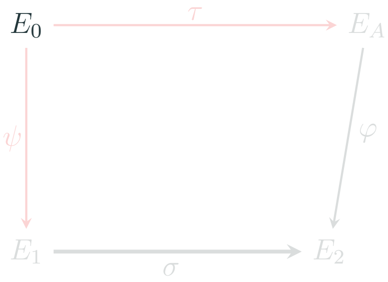
Most algorithms are best efficient when they involve E_0:

- IsogenyToIdeal (KernelToIdeal): takes a kernel point $R \in E_0$ returns the left $\mathcal{O}_0$ ideal I_R corresponding to the isogeny $\phi_R : E_0 \to E_R := E_0/\langle R\rangle$.
- IdealToIsogeny: takes a left $\mathcal{O}_0$ ideal I and returns a representation of the isogeny $\phi_I : E_o \to E_I := E_0/E_0[I]$ corresponding to the ideal I.

They can be generalised to any starting curve E with known endomorphism ring.

SQISign

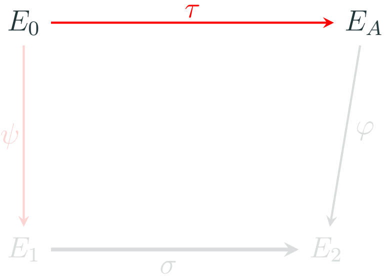
SQISign identification scheme



- Key generation: $\tau : E_0 \longrightarrow E_A$
- Commitment: $\psi : E_0 \longrightarrow E_1$
- Challenge: $\varphi : E_A \longrightarrow E_2$
- Response:
  - Translate φ into an ideal I_φ
  - Sample a random ideal I_σ equivalent to $\overline{I_\tau} \cdot I_\psi \cdot I_\varphi$
  - Return a representation of the isogeny $\sigma : E_1 \to E_2$
- Verification: check that $\sigma : E_1 \to E_2$ is an isogeny

SQISign identification scheme

⋮



- Key generation: $\tau : E_0 \longrightarrow E_A$
- Commitment: $\psi : E_0 \longrightarrow E_1$
- Challenge: $\varphi : E_A \longrightarrow E_2$
- Response:
  - Translate φ into an ideal I_φ
  - Sample a random ideal I_σ equivalent to $\overline{I_\tau} \cdot I_\psi \cdot I_\varphi$
  - Return a representation of the isogeny $\sigma : E_1 \to E_2$
- Verification: check that $\sigma : E_1 \to E_2$ is an isogeny

Sample a random ideal and use IdealToIsogeny

SQISign identification scheme

⋮

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

- Key generation: $\tau : E_0 \longrightarrow E_A$
- Commitment: $\psi : E_0 \longrightarrow E_1$
- Challenge: $\varphi : E_A \longrightarrow E_2$
- Response:
  - Translate φ into an ideal I_φ
  - Sample a random ideal I_σ equivalent to $\overline{I_\tau} \cdot I_\psi \cdot I_\varphi$
  - Return a representation of the isogeny $\sigma : E_1 \to E_2$
- Verification: check that $\sigma : E_1 \to E_2$ is an isogeny

Sample a random ideal and use IdealToIsogeny

SQISign identification scheme

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

- Key generation: $\tau : E_0 \longrightarrow E_A$
- Commitment: $\psi : E_0 \longrightarrow E_1$
- Challenge: $\varphi : E_A \longrightarrow E_2$
- Response:
  - Translate φ into an ideal I_φ
  - Sample a random ideal I_σ equivalent to $\overline{I_\tau} \cdot I_\psi \cdot I_\varphi$
  - Return a representation of the isogeny $\sigma : E_1 \to E_2$
- Verification: check that $\sigma : E_1 \to E_2$ is an isogeny

$$\deg \varphi > 2^\lambda$$

SQISign identification scheme

:

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

- Key generation: $\tau : E_0 \longrightarrow E_A$
- Commitment: $\psi : E_0 \longrightarrow E_1$
- Challenge: $\varphi : E_A \longrightarrow E_2$
- Response:
  - Translate φ into an ideal I_φ
  - Sample a random ideal I_σ equivalent to $\overline{I_\tau} \cdot I_\psi \cdot I_\varphi$
  - Return a representation of the isogeny $\sigma : E_1 \to E_2$
- Verification: check that $\sigma : E_1 \to E_2$ is an isogeny

SQISign identification scheme

:

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

- Key generation: $\tau : E_0 \longrightarrow E_A$
- Commitment: $\psi : E_0 \longrightarrow E_1$
- Challenge: $\varphi : E_A \longrightarrow E_2$
- Response:
  - Translate φ into an ideal I_φ
  - Sample a random ideal I_σ equivalent to $\overline{I_\tau} \cdot I_\psi \cdot I_\varphi$
  - Return a representation of the isogeny $\sigma : E_1 \to E_2$
- Verification: check that $\sigma : E_1 \to E_2$ is an isogeny

Soundness in SQISign

SQISign is sound with respect to the following hard language:

$$\mathcal{L} = \{(E_A, \alpha) \mid \alpha \in \mathrm{End}(E_A) \setminus \mathbb{Z}\}$$

In fact, given two valid transcripts (E_1, φ, σ) and (E_1, φ', σ') with the same commitment E_1 but different challenges $\varphi \neq \varphi'$, one can easily show that $\widehat{\varphi} \circ \sigma \circ \widehat{\sigma'} \circ \varphi'$ is a non scalar endomorphism of E_A.

WaterSQI

SQISign is not secure if τ is $\mathbb{F}_p$-rational

Well finding a witness for

$$\mathcal{L} = \{(E_A, \alpha) \mid \alpha \in \mathrm{End}(E_A) \setminus \mathbb{Z}, E_A/\mathbb{F}_p\}$$

is easy, just return π.

One instead considers the language:

$$\mathcal{L}_p = \{(E_A, \alpha) \mid \alpha \in \mathrm{End}(E_A) \setminus \mathrm{End}_{\mathbb{F}_p}(E_A),\ E_A/\mathbb{F}_p\}$$

Question: Can one design a variant of SQISign for the language $\mathcal{L}_p$?

$$
\begin{tikzcd}
E_0 \arrow[r, "\mathfrak{a}"] \arrow[d, "\mathfrak{b}"'] & E_A \arrow[d, "\mathfrak{c}"] \\
E_1 \arrow[r, "\sigma"'] & E_2
\end{tikzcd}
$$

- Key gen.: $\varphi_{\mathfrak{a}} : E_0 \longrightarrow E_A := \mathfrak{a} \star E_0$
- Com.: $\varphi_{\mathfrak{b}} : E_0 \longrightarrow E_1 := \mathfrak{b} \star E_0$
- Chal.: $\varphi_{\mathfrak{c}} : E_A \longrightarrow E_2 ; = \mathfrak{c} \star E_A$
- Resp.: $\sigma : E_1 \longrightarrow E_2$

But, is it secure?

What is the field of definition of the response σ?

Either $\mathbb{F}_p$

- Then it becomes a proof of knowledge of a relation in the class group.
- The class group can be computed in quantum poly. time.

Or $\mathbb{F}_{p^2}$

- Then $\sigma : E_1 \to E_2$ is a non $\mathbb{F}_p$-rational isogeny between two $\mathbb{F}_p$ supersingular curves.
- We have $\theta = \sigma^{(p)} \circ \widehat{\sigma} \in \mathrm{End}(E_2) \setminus \mathrm{End}_{\mathbb{F}_p}(E_2)$. Hence each signature reveals non $\mathbb{F}_p$-rational endomorphism $\widehat{\varphi} \circ \theta \circ \varphi$ of E_A.

$$\begin{tikzcd}
E_1 \arrow[r, "\sigma"] \arrow[d, "\pi"'] & E_2 \arrow[d, "\pi"] \\
E_1 \arrow[r, "\sigma^{(p)}"'] & E_2
\end{tikzcd}$$

Fig. 3. Attack when the challenge curve E_2 is defined over $\mathbb{F}_p$ (diagram on the left) or the $\mathbb{F}_{p^2}$ part of the challenge isogeny φ is relatively short (diagram on the right).

Solution

- The response should be an isogeny of prime degree d where d is inert in $\mathbb{Z}[\pi]$.
- The commitment curve must be defined over $\mathbb{F}_{p^2}$ (so that a single signature does not reveal an endomorphism of E_A).
- The very first step of the challenge isogeny shouldn't be $\mathbb{F}_p$ rational.

When these conditions are satisfied, one can show that given two valid transcripts (E_1, φ, σ) and (E_1, φ', σ') with the same commitment E_1 but different challenges $\varphi \neq \varphi'$, $\widehat{\varphi} \circ \sigma \circ \widehat{\sigma'} \circ \varphi' \in \mathrm{End}(E_A) \setminus \mathrm{End}_{\mathbb{F}_p}(E_A)$.

WaterSQI identification scheme

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

- Key gen.: $\varphi_{\mathfrak{a}} : E_0 \longrightarrow E_A := \mathfrak{a} \star E_0$
- Commitment: $\psi : E_0 \longrightarrow E_1$
- Challenge: $\varphi : E_A \longrightarrow E_2$
- Response:
  - Translate φ into an ideal I_φ
  - Sample a random ideal I_σ equivalent to $\overline{I_\tau} \cdot I_\psi \cdot I_\varphi$ and of prime norm d such that d is inert in $\mathcal{O}_p$
  - Return a representation of the isogeny $\sigma : E_1 \to E_2$
- Verification: check that $\sigma : E_1 \to E_2$ is an isogeny of prime degree d inert in $\mathrm{End}_{\mathbb{F}_p}(E_0)$

WaterSQI identification scheme

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

- Key gen.: $\varphi_{\mathfrak{a}} : E_0 \longrightarrow E_A := \mathfrak{a} \star E_0$
- Commitment: $\psi : E_0 \longrightarrow E_1$
- Challenge: $\varphi : E_A \longrightarrow E_2$
- Response:
  - Translate φ into an ideal I_φ
  - Sample a random ideal I_σ equivalent to $\overline{I_\tau} \cdot I_\psi \cdot I_\varphi$ and of prime norm d such that d is inert in $\mathcal{O}_p$
  - Return a representation of the isogeny $\sigma : E_1 \to E_2$
- Verification: check that $\sigma : E_1 \to E_2$ is an isogeny of prime degree d inert in $\mathrm{End}_{\mathbb{F}_p}(E_0)$

Sample a random ideal $\mathfrak{a}$ of $\mathcal{O}_p$ and use IdealToIsogeny

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

- Key gen.: $\varphi_{\mathfrak{a}} : E_0 \longrightarrow E_A := \mathfrak{a} \star E_0$
- Commitment: $\psi : E_0 \longrightarrow E_1$
- Challenge: $\varphi : E_A \longrightarrow E_2$
- Response:
  - Translate φ into an ideal I_φ
  - Sample a random ideal I_σ equivalent to $\overline{I_\tau} \cdot I_\psi \cdot I_\varphi$ and of prime norm d such that d is inert in $\mathcal{O}_p$
  - Return a representation of the isogeny $\sigma : E_1 \to E_2$
- Verification: check that $\sigma : E_1 \to E_2$ is an isogeny of prime degree d inert in $\mathrm{End}_{\mathbb{F}_p}(E_0)$

Sample a random ideal and use IdealToIsogeny, restart if $j(E_1) \in \mathbb{F}_p$.

WaterSQI identification scheme

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

- Key gen.: $\varphi_{\mathfrak{a}} : E_0 \longrightarrow E_A := \mathfrak{a} \star E_0$
- Commitment: $\psi : E_0 \longrightarrow E_1$
- Challenge: $\varphi : E_A \longrightarrow E_2$
- Response:
  - Translate φ into an ideal I_φ
  - Sample a random ideal I_σ equivalent to $\overline{I_\tau} \cdot I_\psi \cdot I_\varphi$ and of prime norm d such that d is inert in $\mathcal{O}_p$
  - Return a representation of the isogeny $\sigma : E_1 \to E_2$
- Verification: check that $\sigma : E_1 \to E_2$ is an isogeny of prime degree d inert in $\mathrm{End}_{\mathbb{F}_p}(E_0)$

$\deg \varphi > 2^\lambda$, prime power, and the first step is not $\mathbb{F}_p$-rational

WaterSQI identification scheme

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

- Key gen.: $\varphi_{\mathfrak{a}} : E_0 \longrightarrow E_A := \mathfrak{a} \star E_0$
- Commitment: $\psi : E_0 \longrightarrow E_1$
- Challenge: $\varphi : E_A \longrightarrow E_2$
- Response:
  - Translate φ into an ideal I_φ
  - Sample a random ideal I_σ equivalent to $\overline{I_\tau} \cdot I_\psi \cdot I_\varphi$ and of prime norm d such that d is inert in $\mathcal{O}_p$
  - Return a representation of the isogeny $\sigma : E_1 \to E_2$
- Verification: check that $\sigma : E_1 \to E_2$ is an isogeny of prime degree d inert in $\mathrm{End}_{\mathbb{F}_p}(E_0)$

WaterSQI identification scheme

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

- Key gen.: $\varphi_{\mathfrak{a}} : E_0 \longrightarrow E_A := \mathfrak{a} \star E_0$
- Commitment: $\psi : E_0 \longrightarrow E_1$
- Challenge: $\varphi : E_A \longrightarrow E_2$
- Response:
  - Translate φ into an ideal I_φ
  - Sample a random ideal I_σ equivalent to $\overline{I_\tau} \cdot I_\psi \cdot I_\varphi$ and of prime norm d such that d is inert in $\mathcal{O}_p$
  - Return a representation of the isogeny $\sigma : E_1 \to E_2$
- Verification: check that $\sigma : E_1 \to E_2$ is an isogeny of prime degree d inert in $\mathrm{End}_{\mathbb{F}_p}(E_0)$

To be continued