A Look at SQISignHD

Isogeny-Based Cryptography

Tako Boris Fouotsa, LASEC-EPFL

Leuven Isogeny Days, 4th Edition, Leuven, Oct 12, 2023

Outline

Overview of SQISignHD

Returning to BSIDH primes

SQI-Fish: Skiing on the Sea Side



Overview of SQISignHD

SQISign

p prime s.t. $p^2 - 1 = 2^e T f - 1$, $T > p^{5/4}$ as smooth as possible.
Special curve E_0: easy to evaluate endomorphisms (e.g. 1728).

SQISign identification scheme:

- Key generation: $\tau : E_0 \longrightarrow E_A$
- Commitment: $\psi : E_0 \longrightarrow E_1$
- Challenge: $\varphi : E_1 \longrightarrow E_2$
- Response: $\sigma : E_A \longrightarrow E_2$

SQISign

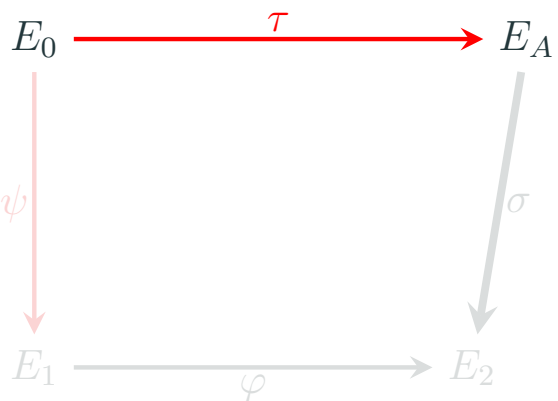
p prime s.t. $p^2 - 1 = 2^e T f - 1$, $T > p^{5/4}$ as smooth as possible.
Special curve E_0: easy to evaluate endomorphisms (e.g. 1728).

SQISign identification scheme:

- Key generation: $\tau : E_0 \longrightarrow E_A$
- Commitment: $\psi : E_0 \longrightarrow E_1$
- Challenge: $\varphi : E_1 \longrightarrow E_2$
- Response: $\sigma : E_A \longrightarrow E_2$

SQISign

p prime s.t. $p^2 - 1 = 2^e T f - 1$, $T > p^{5/4}$ as smooth as possible.
Special curve E_0: easy to evaluate endomorphisms (e.g. 1728).



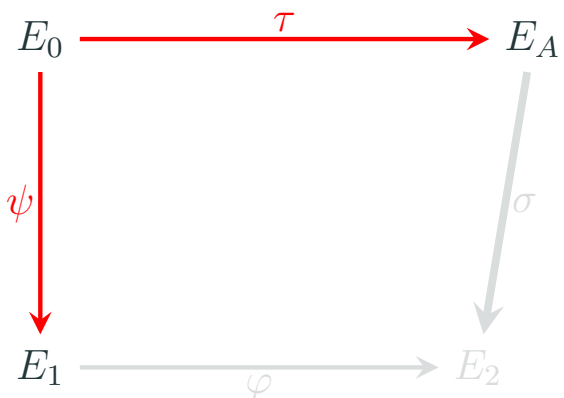
SQISign identification scheme:

- Key generation: $\tau : E_0 \longrightarrow E_A$
- Commitment: $\psi : E_0 \longrightarrow E_1$
- Challenge: $\varphi : E_1 \longrightarrow E_2$
- Response: $\sigma : E_A \longrightarrow E_2$

$$\deg \tau \approx 2^{2\lambda} \approx p$$

SQISign

p prime s.t. $p^2 - 1 = 2^e T f - 1$, $T > p^{5/4}$ as smooth as possible.
Special curve E_0: easy to evaluate endomorphisms (e.g. 1728).



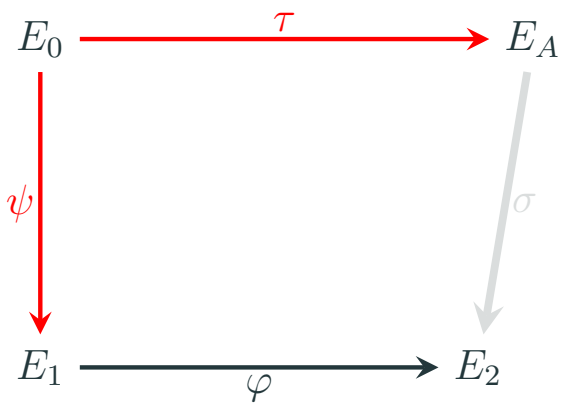
SQISign identification scheme:

- Key generation: $\tau : E_0 \longrightarrow E_A$
- Commitment: $\psi : E_0 \longrightarrow E_1$
- Challenge: $\varphi : E_1 \longrightarrow E_2$
- Response: $\sigma : E_A \longrightarrow E_2$

$$\deg \psi \approx 2^{2\lambda} \approx p$$

SQISign

p prime s.t. $p^2 - 1 = 2^e T f - 1$, $T > p^{5/4}$ as smooth as possible.
Special curve E_0: easy to evaluate endomorphisms (e.g. 1728).



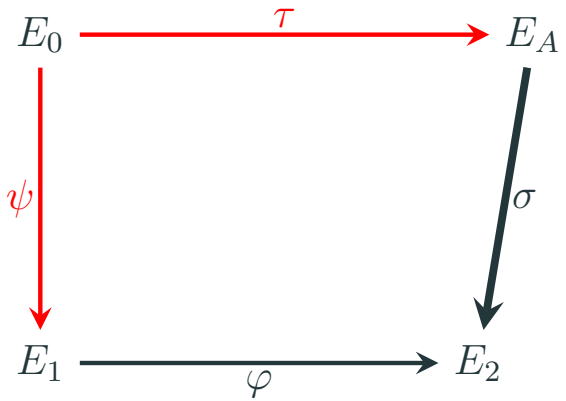
SQISign identification scheme:

- Key generation: $\tau : E_0 \longrightarrow E_A$
- Commitment: $\psi : E_0 \longrightarrow E_1$
- Challenge: $\varphi : E_1 \longrightarrow E_2$
- Response: $\sigma : E_A \longrightarrow E_2$

$$\deg \varphi \approx 2^\lambda$$

SQISign

p prime s.t. $p^2 - 1 = 2^e T f - 1$, $T > p^{5/4}$ as smooth as possible.
Special curve E_0: easy to evaluate endomorphisms (e.g. 1728).



SQISign identification scheme:

- Key generation: $\tau : E_0 \longrightarrow E_A$
- Commitment: $\psi : E_0 \longrightarrow E_1$
- Challenge: $\varphi : E_1 \longrightarrow E_2$
- Response: $\sigma : E_A \longrightarrow E_2$

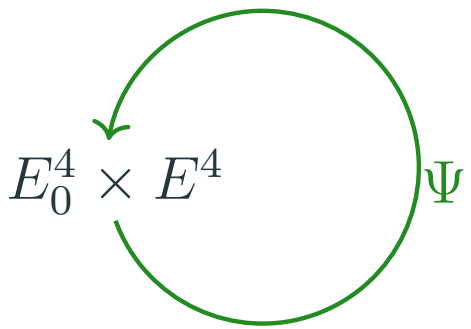
$$J_0 = I_\varphi \cdot I_\psi \cdot \overline{I_\tau}, \qquad J = KLPT_{2^*}(J_0)$$
$$\sigma := \varphi_J = IdealToIsogeny(J). \qquad \deg \sigma \approx p^{15/4}.$$

New isogeny representation

HD Isogeny Representation ($Repr_N$)

Let $\phi : E_0 \to E$ be an isogeny of degree d. Let $N > d$ be a smooth integer and let $E_0[N] = \langle P, Q \rangle$. Given E_0, E, P, Q, $\phi(P)$, $\phi(Q)$, there exists a polynomial time algorithm that evaluates ϕ on rational torsion points.

Achieved by evaluating a higher dimension endomorphism* $\Psi \in \mathrm{End}(E_0^4 \times E^4)$ of degree N.

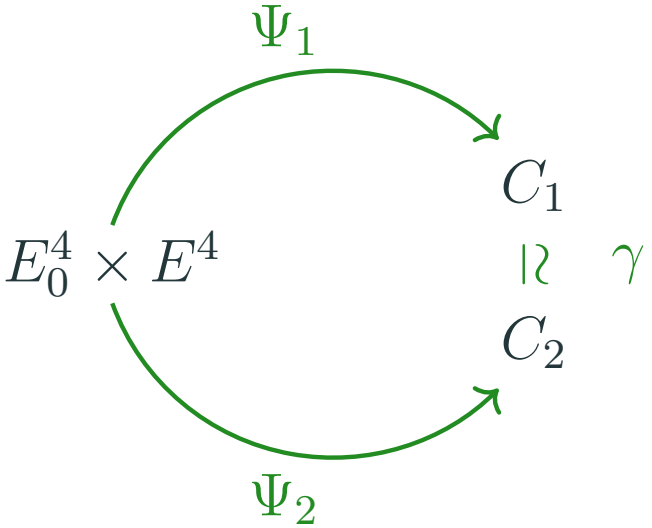


When $N - d = a_1^2 + a_2^2$, Ψ can be replaced by a similar endomorphism in dimension 4, which is more efficient to evaluate.

New isogeny representation

Less torsion, but Dlogs, two glueings,... ($SqrtRepr_N$)

Let $\phi : E_0 \to E$ be an isogeny of degree d. Let $N > \sqrt{d}$ be a smooth integer and let $E_0[N] = \langle P, Q \rangle$. Given E_0, E, P, Q, $\phi(P)$, $\phi(Q)$, there exists a polynomial time algorithm that evaluates ϕ on rational torsion points.



$$\Psi = \widehat{\Psi_2} \circ \gamma \circ \Psi_1,$$
$$\deg \Psi_i = N_i | N.$$
$$\ker \Psi_1 = \ker \Psi \cap (E_0^4 \times E^4)[N_1]$$
$$\ker \widehat{\Psi_2} = \Psi\left((E_0^4 \times E^4)[N_2]\right).$$

When $N^2 - d = a_1^2 + a_2^2$, Ψ, Ψ_1 and Ψ_2 can be replaced by a similar isogenies in dimension 4.

SQISignHD

$p = 2^a 3^b - 1$ prime s.t. $2^a \approx 3^b$, special curve E_0: easy to evaluate endomorphisms (e.g. 1728).

SQISignHD identification scheme:

- Key generation: $\tau : E_0 \longrightarrow E_A$
- Commitment: $\psi : E_0 \longrightarrow E_1$
- Challenge: $\varphi : E_1 \longrightarrow E_2$
- Response: $\sigma : E_A \longrightarrow E_2$

SQISignHD

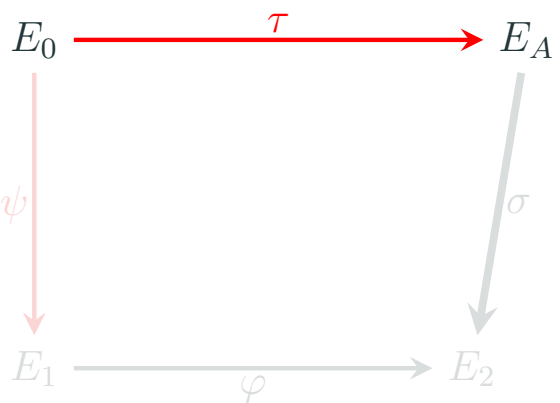
$p = 2^a 3^b - 1$ prime s.t. $2^a \approx 3^b$, special curve E_0: easy to evaluate endomorphisms (e.g. 1728).

SQISignHD identification scheme:

- Key generation: $\tau : E_0 \longrightarrow E_A$
- Commitment: $\psi : E_0 \longrightarrow E_1$
- Challenge: $\varphi : E_1 \longrightarrow E_2$
- Response: $\sigma : E_A \longrightarrow E_2$

SQISignHD

$p = 2^a 3^b - 1$ prime s.t. $2^a \approx 3^b$, special curve E_0: easy to evaluate endomorphisms (e.g. 1728).



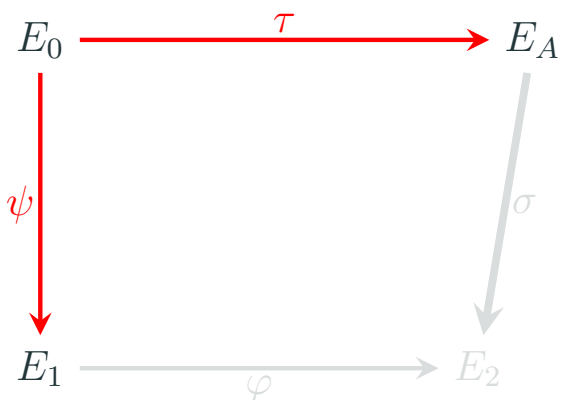
SQISignHD identification scheme:

- Key generation: $\tau : E_0 \longrightarrow E_A$
- Commitment: $\psi : E_0 \longrightarrow E_1$
- Challenge: $\varphi : E_1 \longrightarrow E_2$
- Response: $\sigma : E_A \longrightarrow E_2$

$$\deg \tau = 3^{2b'}, \quad b' \approx b$$

SQISignHD

$p = 2^a 3^b - 1$ prime s.t. $2^a \approx 3^b$, special curve E_0: easy to evaluate endomorphisms (e.g. 1728).



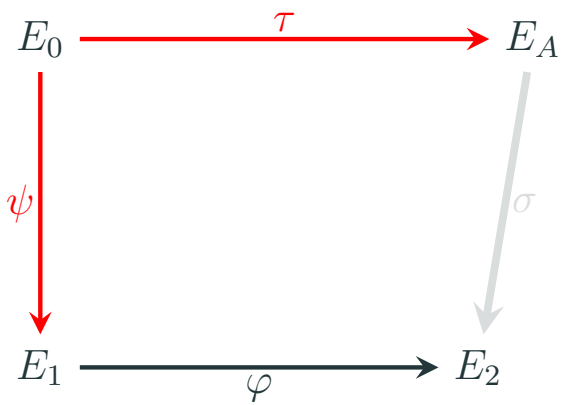
SQISignHD identification scheme:

- Key generation: $\tau : E_0 \longrightarrow E_A$
- Commitment: $\psi : E_0 \longrightarrow E_1$
- Challenge: $\varphi : E_1 \longrightarrow E_2$
- Response: $\sigma : E_A \longrightarrow E_2$

$$\deg \psi = 3^{2b''}, \quad b'' \approx b$$

SQISignHD

$p = 2^a 3^b - 1$ prime s.t. $2^a \approx 3^b$, special curve E_0: easy to evaluate endomorphisms (e.g. 1728).



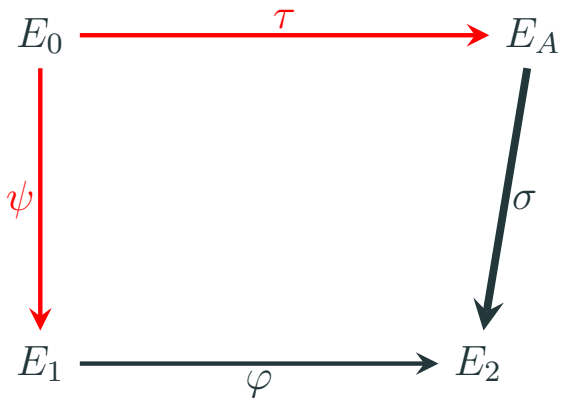
SQISignHD identification scheme:

- Key generation: $\tau : E_0 \longrightarrow E_A$
- Commitment: $\psi : E_0 \longrightarrow E_1$
- Challenge: $\varphi : E_1 \longrightarrow E_2$
- Response: $\sigma : E_A \longrightarrow E_2$

$$\deg \varphi = 3^b$$

SQISignHD

$p = 2^a 3^b - 1$ prime s.t. $2^a \approx 3^b$, special curve E_0: easy to evaluate endomorphisms (e.g. 1728).



SQISignHD identification scheme:

- Key generation: $\tau : E_0 \longrightarrow E_A$
- Commitment: $\psi : E_0 \longrightarrow E_1$
- Challenge: $\varphi : E_1 \longrightarrow E_2$
- Response: $\sigma : E_A \longrightarrow E_2$

$$J = RandShortEquivIdeal(I_\varphi \cdot I_\psi \cdot \overline{I_\tau}), \qquad \sigma = Repr_(\varphi_J)$$

There exists at least one J such that $N(J) \leq 2\sqrt{2p}/\pi$.
But for dim. 4 representation, $2^* - N(J) = a_1^2 + a_2^2$,
it is very likely that $N(J) \geq 2\sqrt{2p}/\pi > 2^a$.

$$\sigma = SqrtRepr_{2^{a-3}}(\varphi_J).$$

Returning to BSIDH primes

Returning to BSIDH primes

Why??

- Then you can have a larger 2^a-torsion to represent your isogeny
  - less Dlogs
  - less glueing
- Your secret isogeny τ and the commitment isogeny ψ can now have degree $\geq p$
  - better distribution for the curves E_A and E_2
  - good for security

But SQISign primes are hard to find !!

This ones are our friends, not too many constraints, they are easy to find, XGCD can already do a good job.

SQISignHD with friendly BSIDH primes

p prime s.t. $p^2 - 1 = 2^a T f - 1$ with $2^a \geq O(\log p)\sqrt{p}$, $T > \sqrt{p}$ is as smooth as possible

Special curve E_0: easy to evaluate endomorphisms (e.g. 1728).

The identification scheme:

- Key generation: $\tau : E_0 \longrightarrow E_A$
- Commitment: $\psi : E_0 \longrightarrow E_1$
- Challenge: $\varphi : E_1 \longrightarrow E_2$
- Response: $\sigma : E_A \longrightarrow E_2$

SQISignHD with friendly BSIDH primes

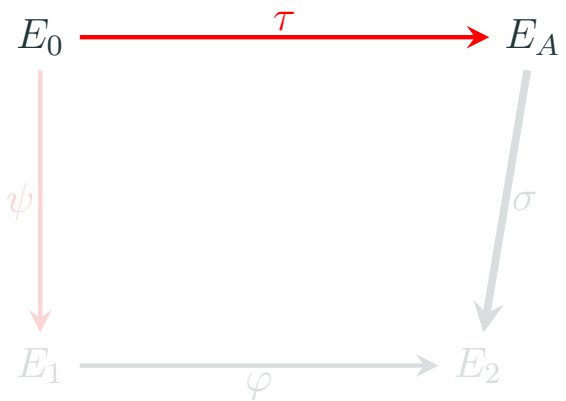
p prime s.t. $p^2 - 1 = 2^a T f - 1$ with $2^a \geq O(\log p)\sqrt{p}$, $T > \sqrt{p}$ is as smooth as possible
Special curve E_0: easy to evaluate endomorphisms (e.g. 1728).

The identification scheme:

- Key generation: $\tau : E_0 \longrightarrow E_A$
- Commitment: $\psi : E_0 \longrightarrow E_1$
- Challenge: $\varphi : E_1 \longrightarrow E_2$
- Response: $\sigma : E_A \longrightarrow E_2$

SQISignHD with friendly BSIDH primes

p prime s.t. $p^2 - 1 = 2^a T f - 1$ with $2^a \geq O(\log p)\sqrt{p}$, $T > \sqrt{p}$ is as smooth as possible
Special curve E_0: easy to evaluate endomorphisms (e.g. 1728).



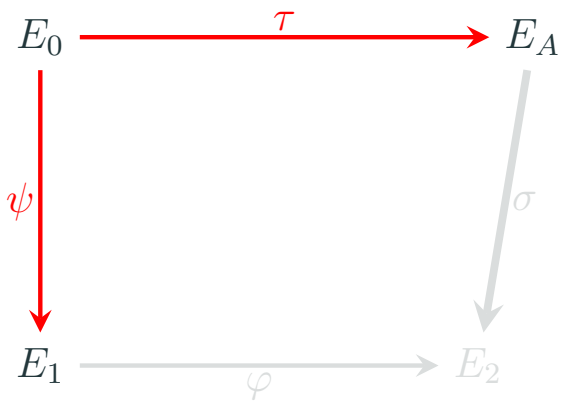
The identification scheme:

- Key generation: $\tau : E_0 \longrightarrow E_A$
- Commitment: $\psi : E_0 \longrightarrow E_1$
- Challenge: $\varphi : E_1 \longrightarrow E_2$
- Response: $\sigma : E_A \longrightarrow E_2$

$$\deg \tau = T'^2, \quad T' \approx T \quad T' | T$$

SQISignHD with friendly BSIDH primes

p prime s.t. $p^2 - 1 = 2^a T f - 1$ with $2^a \geq O(\log p)\sqrt{p}$, $T > \sqrt{p}$ is as smooth as possible
Special curve E_0: easy to evaluate endomorphisms (e.g. 1728).



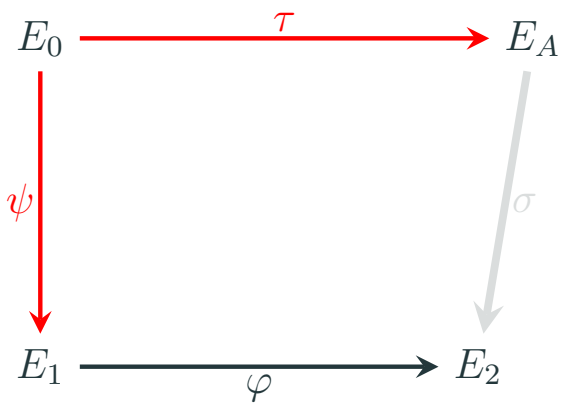
The identification scheme:

- Key generation: $\tau : E_0 \longrightarrow E_A$
- Commitment: $\psi : E_0 \longrightarrow E_1$
- Challenge: $\varphi : E_1 \longrightarrow E_2$
- Response: $\sigma : E_A \longrightarrow E_2$

$$\deg \psi = T''^2, \quad T'' \approx T \quad T''|T$$

SQISignHD with friendly BSIDH primes

p prime s.t. $p^2 - 1 = 2^a T f - 1$ with $2^a \geq O(\log p)\sqrt{p}$, $T > \sqrt{p}$ is as smooth as possible
Special curve E_0: easy to evaluate endomorphisms (e.g. 1728).

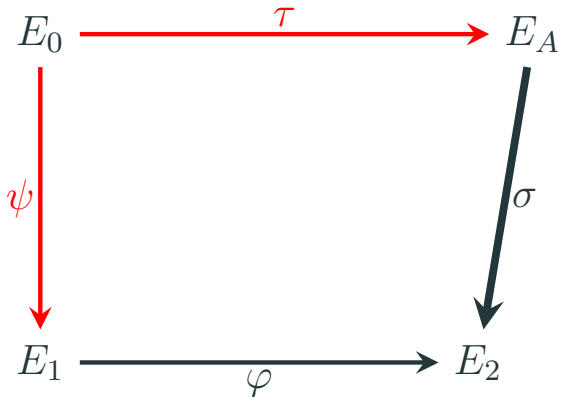


The identification scheme:

- Key generation: $\tau : E_0 \longrightarrow E_A$
- Commitment: $\psi : E_0 \longrightarrow E_1$
- Challenge: $\varphi : E_1 \longrightarrow E_2$
- Response: $\sigma : E_A \longrightarrow E_2$

SQISignHD with friendly BSIDH primes

p prime s.t. $p^2 - 1 = 2^a T f - 1$ with $2^a \geq O(\log p)\sqrt{p}$, $T > \sqrt{p}$ is as smooth as possible
Special curve E_0: easy to evaluate endomorphisms (e.g. 1728).



The identification scheme:

- Key generation: $\tau : E_0 \longrightarrow E_A$
- Commitment: $\psi : E_0 \longrightarrow E_1$
- Challenge: $\varphi : E_1 \longrightarrow E_2$
- Response: $\sigma : E_A \longrightarrow E_2$

$$J = RandEquivIdeal(I_\varphi \cdot I_\psi \cdot \overline{I_\tau}), \qquad 2^* - N(J) = a_1^2 + a_2^2$$

Under some heuristics (prime numb. theorem), $N(J) \leq 2^a$.

$$\sigma = Repr_{2^a}(\varphi_I).$$

Sample of such primes

λ	$\log p$	a	$\log T$	T
128	257	153	136	$3^{54}*5*7*11*19^2*29*31^2*37*73*89$
192	384	206	201	$3^{102}*5*7*11^2*17^2*19^2*31*41$
256	514	288	250	$5^3*41*3^{134}*7*31^2*59*71$

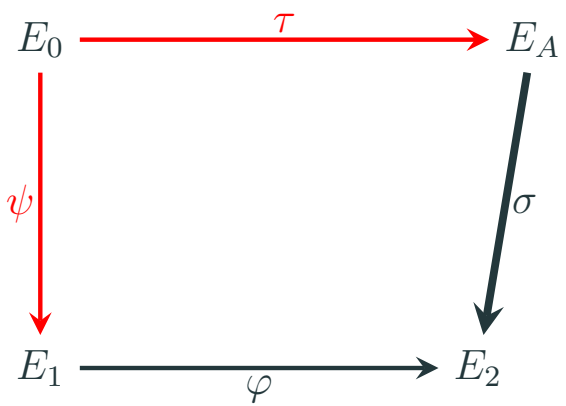
Some BSIDH friendly primes, $p^2 - 1 = 2^a T f$.



SQI-Fish: Skiing on the Sea Side

The key generation and the commitment in SQISignHD

$\sigma = Repr(\varphi_J)$ with $J \simeq I_\varphi \cdot I_\psi \cdot \overline{I_\tau}$
Signer knows I_ψ and $\overline{I_\tau}$ but not I_φ.

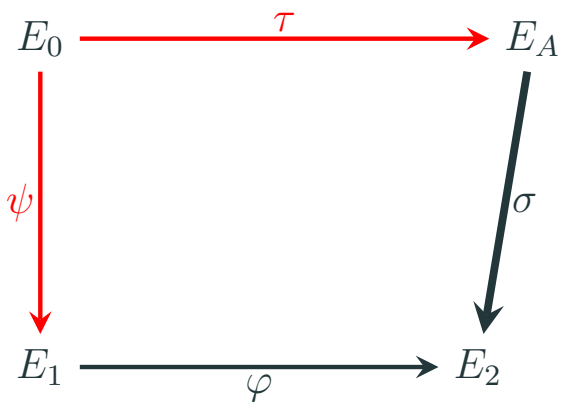


Translating φ into an ideal:

- Let $\psi' : E_0' \to E_1$, with E_0' special
- Compute $\ker[\psi']^*\varphi = \widehat{\psi'}(\ker\varphi)$
- Compute $[\psi']^*\varphi$ and its corresponding ideal $I_{[\psi]^*\varphi}$
- Compute I_φ as the push-forward ideal $[I_{\psi'}]_* I_{[\psi']^*\varphi}$.

One takes $E_0' = E_0$. For the pull-back and the push-forward to make sense, $\deg\psi'$ and $\deg\varphi$ must be co-prime. Hence $\psi \neq \psi'$.

The key generation and the commitment in SQISignHD



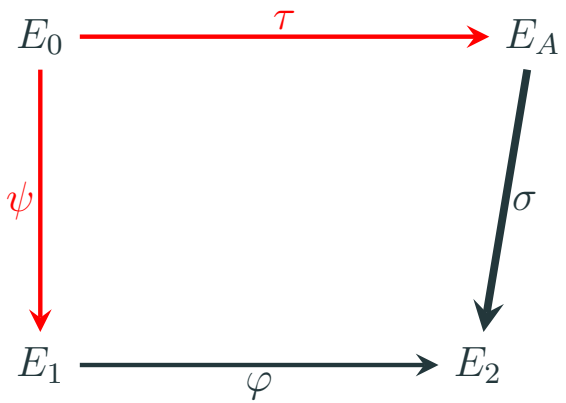
$\sigma = Repr(\varphi_J)$ with $J \simeq I_\varphi \cdot I_\psi \cdot \overline{I_\tau}$
Signer knows I_ψ and $\overline{I_\tau}$ but not I_φ.

Translating φ into an ideal:

- Let $\psi' : E_0' \to E_1$, with E_0' special
- Compute $\ker[\psi']^*\varphi = \widehat{\psi'}(\ker \varphi)$
- Compute $[\psi']^*\varphi$ and its corresponding ideal $I_{[\psi]^*\varphi}$
- Compute I_φ as the push-forward ideal $[I_{\psi'}]_* I_{[\psi']^*\varphi}$.

One takes $E_0' = E_0$. For the pull-back and the push-forward to make sense, $\deg \psi'$ and $\deg \varphi$ must be co-prime. Hence $\psi \neq \psi'$.

The key generation and the commitment in SQISignHD



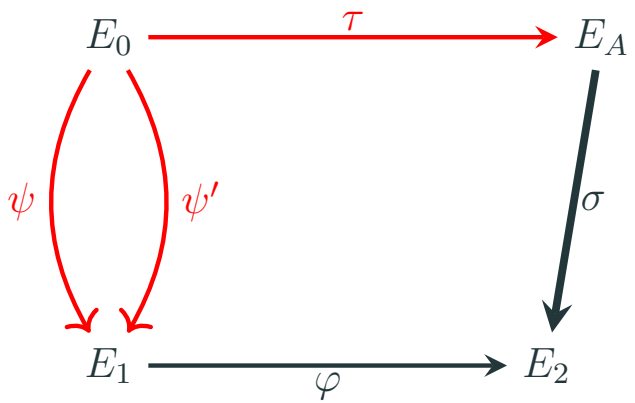
$\sigma = Repr(\varphi_J)$ with $J \simeq I_\varphi \cdot I_\psi \cdot \overline{I_\tau}$
Signer knows I_ψ and $\overline{I_\tau}$ but not I_φ.

Translating φ into an ideal:

- Let $\psi' : E_0' \to E_1$, with E_0' special
- Compute $\ker[\psi']^*\varphi = \widehat{\psi'}(\ker \varphi)$
- Compute $[\psi']^*\varphi$ and its corresponding ideal $I_{[\psi]^*\varphi}$
- Compute I_φ as the push-forward ideal $[I_{\psi'}]_* I_{[\psi']^*\varphi}$.

One takes $E_0' = E_0$. For the pull-back and the push-forward to make sense, $\deg \psi'$ and $\deg \varphi$ must be co-prime. Hence $\psi \neq \psi'$.

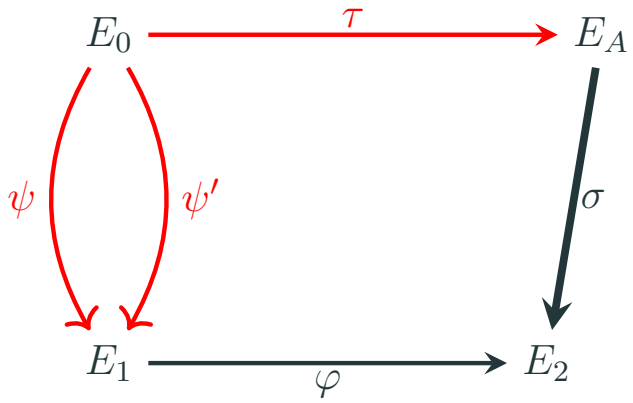
The key generation and the commitment in SQISignHD



One takes $E_0' = E_0$. For the pull-back and the push-forward to make sense, $\deg \psi'$ and $\deg \varphi$ must be co-prime. Hence $\psi \neq \psi'$.

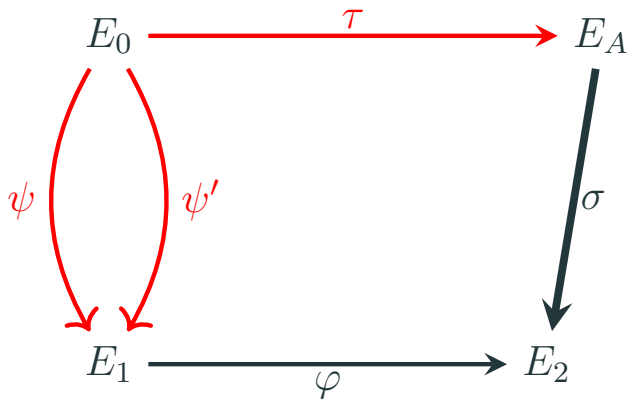
On sets $\deg \psi' \approx 2^{2a'}$ and $\deg \psi \approx 3^{2b'}$, $\quad a \approx a', \quad b \approx b'$.

The key generation and the commitment in SQISignHD



Question: Can you do better? Or worse?

The key generation and the commitment in SQISignHD



Question: Can you do better? Or worse?

Answer: You can do both both !!

The magic of group actions: use $\mathbb{F}_p$-isogenies !

Advantages

- Isogenies are ideals, ideals are isogenies (main dans la main)
- The degree of the isogeny is not totally* controlled by the amount of smooth torsion available
- One can exponentially reduce the gap between the distribution of E_A and E_1 on one hand, and the uniform distribution on the other
- Evaluation on the 2^a-torsion is straightforward
- Easier to describe, easier to implement,...

Disadvantages

- Sub-exp. quantum attacks implying large primes (several thousands bits)

The magic of group actions: use $\mathbb{F}_p$-isogenies !

Advantages

- Isogenies are ideals, ideals are isogenies (main dans la main)
- The degree of the isogeny is not totally* controlled by the amount of smooth torsion available
- One can exponentially reduce the gap between the distribution of E_A and E_1 on one hand, and the uniform distribution on the other
- Evaluation on the 2^a-torsion is straightforward
- Easier to describe, easier to implement,...

Disadvantages

- Sub-exp. quantum attacks implying large primes (several thousands bits)

SQI-Fish: Skiing on the Sea Side

$p = 2^a \ell_1 \cdots \ell_n f - 1$, $2^a > O(\log p)\sqrt{p}$.
Special curve E_0: easy to evaluate endomorphisms (e.g. 1728).

SQI-Fish identification scheme:

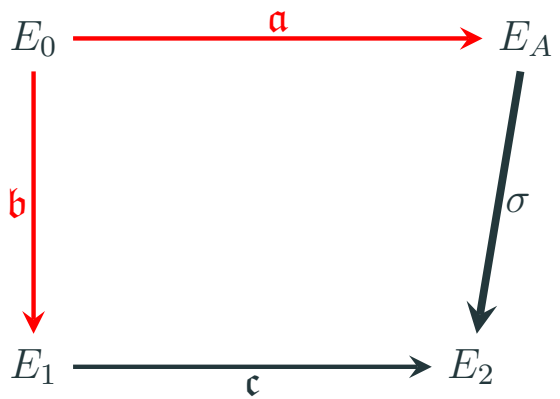
- Key gen.: $\varphi_{\mathfrak{a}} : E_0 \longrightarrow E_A := \mathfrak{a} \star E_0$
- Com.: $\varphi_{\mathfrak{b}} : E_0 \longrightarrow E_1 := \mathfrak{b} \star E_0$
- Chal.: $\varphi_{\mathfrak{c}} : E_1 \longrightarrow E_2; = \mathfrak{c} \star E_1$
- Resp.: $\sigma : E_A \longrightarrow E_2$

$J = RandEquivIdeal(\mathfrak{c} \cdot \mathfrak{b} \cdot \overline{\mathfrak{a}})$, $\quad 2^a - N(J) = a_1^2 + a_2^2$
$\sigma = Repr_{2^a}(\varphi_J)$

Similar security assumptions as in SQISignHD, but for $\mathbb{F}_p$ curves.

SQI-Fish: Skiing on the Sea Side

$p = 2^a \ell_1 \cdots \ell_n f - 1$, $2^a > O(\log p)\sqrt{p}$.
Special curve E_0: easy to evaluate endomorphisms (e.g. 1728).



SQI-Fish identification scheme:

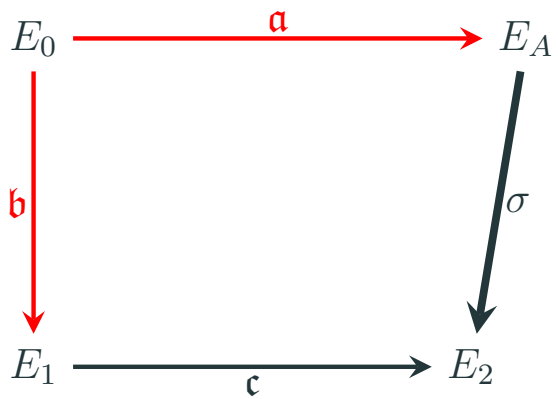
- Key gen.: $\varphi_{\mathfrak{a}} : E_0 \longrightarrow E_A := \mathfrak{a} \star E_0$
- Com.: $\varphi_{\mathfrak{b}} : E_0 \longrightarrow E_1 := \mathfrak{b} \star E_0$
- Chal.: $\varphi_{\mathfrak{c}} : E_1 \longrightarrow E_2; = \mathfrak{c} \star E_1$
- Resp.: $\sigma : E_A \longrightarrow E_2$

$J = RandEquivIdeal(\mathfrak{c} \cdot \mathfrak{b} \cdot \overline{\mathfrak{a}})$, $\quad 2^a - N(J) = a_1^2 + a_2^2$
$\sigma = Repr_{2^a}(\varphi_J)$

Similar security assumptions as in SQISignHD, but for $\mathbb{F}_p$ curves.

SQI-Fish: Skiing on the Sea Side

$p = 2^a \ell_1 \cdots \ell_n f - 1$, $2^a > O(\log p)\sqrt{p}$.
Special curve E_0: easy to evaluate endomorphisms (e.g. 1728).



SQI-Fish identification scheme:

- 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.: $\varphi_{\mathfrak{c}} : E_1 \longrightarrow E_2; = \mathfrak{c} \star E_1$
- Resp.: $\sigma : E_A \longrightarrow E_2$

$J = RandEquivIdeal(\mathfrak{c} \cdot \mathfrak{b} \cdot \overline{\mathfrak{a}})$, $\qquad 2^a - N(J) = a_1^2 + a_2^2$
$\sigma = Repr_{2^a}(\varphi_J)$

Similar security assumptions as in SQISignHD, but for $\mathbb{F}_p$ curves.

Finally, better or worse?

- For sufficient quantum security, primes are more than 10 times larger than in SQISignHD.
- The very long 2^a HD isogeny will definitely make the verification way much slower than in SQISignHD.
- But the simplicity of the signing procedure will make the signing highly efficient.

- Is it even fair to compare SQI-Fish to SQISignHD?
- No ! CSIDH-style signatures instead

Finally, better or worse?

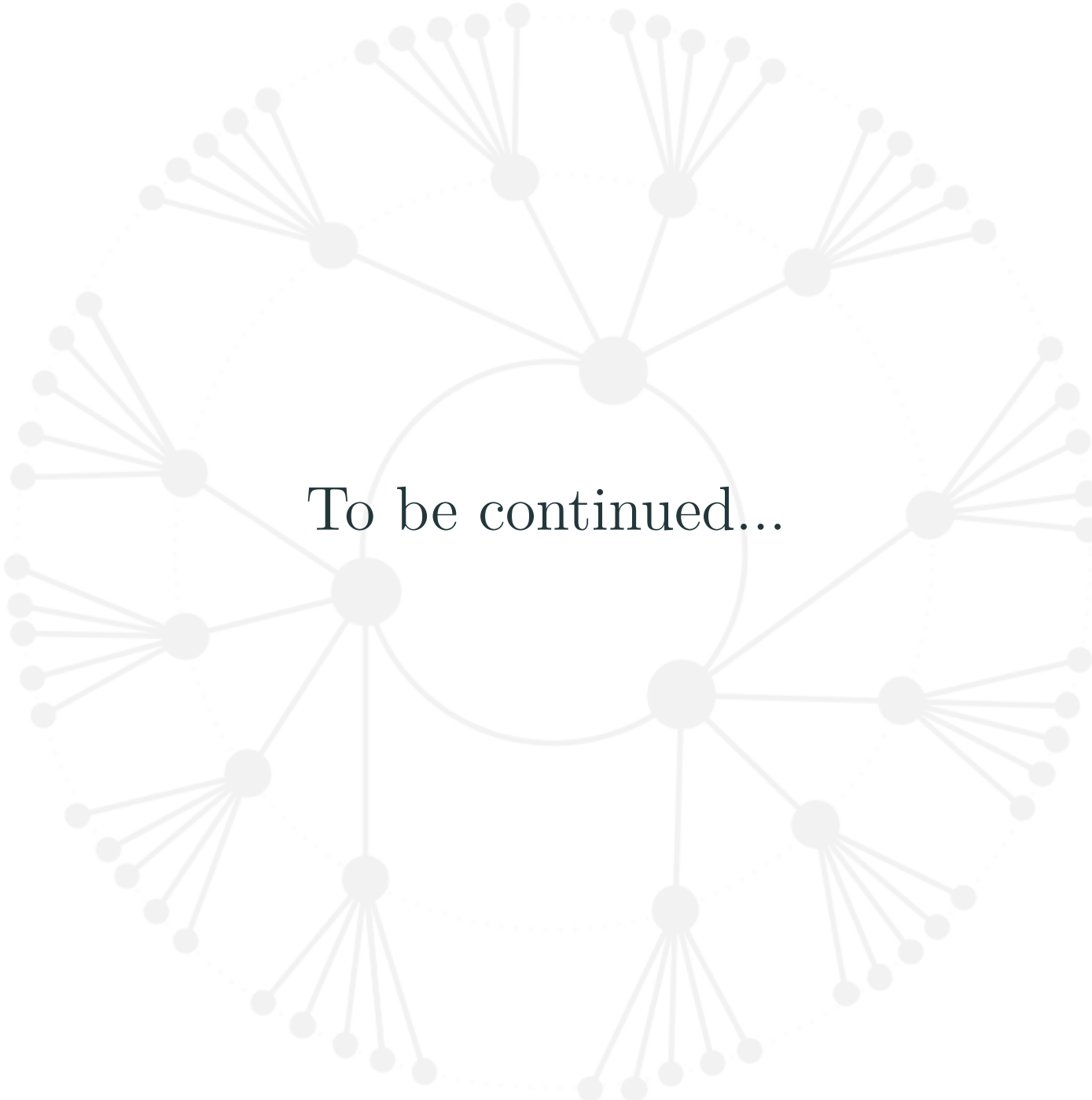
- For sufficient quantum security, primes are more than 10 times larger than in SQISignHD.
- The very long 2^a HD isogeny will definitely make the verification way much slower than in SQISignHD.
- But the simplicity of the signing procedure will make the signing highly efficient.

- Is it even fair to compare SQI-Fish to SQISignHD?
- No ! CSIDH-style signatures instead

Comparison with CSIDH-style signatures

	CSI-Fish	SCALLOP	SCALLOP-HD	SQI-Fish
class grp. struc.	✓	✓	✓	✗
exp. chal. space	✗	✗	✗	✓
chances of failure	✓	✓	✓	✗
Scalable	✗	✗	✓	✓
pk + sg. size	$O(\lambda)$	$O(\lambda)$	$O(\lambda)$	$O(1)$
Soundness	$\mathfrak{a} \star E_0 = E$	$\mathfrak{a} \star E_0 = E$	$\mathfrak{a} \star E_0 = E$	$\alpha \in \mathrm{End}(E) \setminus \mathbb{Z}[\pi]$

Moreover, SQI-Fish is for sure more efficient compared to SCALLOP and SCALLOP-HD. We believe with that with an optimised implementation of Higher dimension isogenies, SQI-Fish will be faster than CSI-Fish...



To be continued...