SQIsign2DPush

Kohei Nakagawa[1] and Hiroshi Onuki[2]

[1]NTT Social Informatics Laboratories, [2]The University of Tokyo

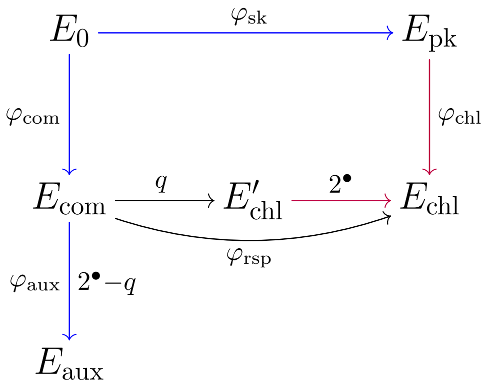
SQIparty 2025/4/28

Overview

- We propose a new SQIsign variant, **SQIsign2DPush**.
- Construct a **new algorithm** for the **auxiliary isogeny**.
- Also use DoublePath in SQIsignHD.
- We can reduce the number of $(2, 2)$-isogenies in signing.

This talk manly focuses on how to compute the **auxiliary isogeny**.

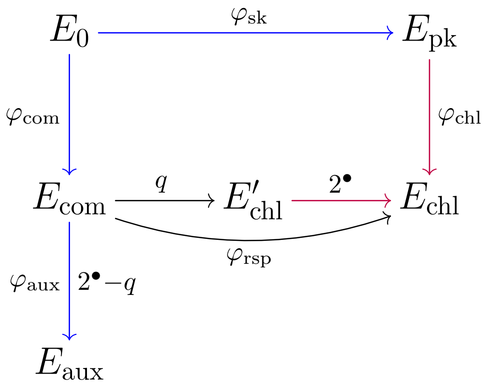
Motivation



In the NIST SQIsign,

- Blue isogenies by IdealToIsogeny in SQIsign2D-West.
- Purple isogenies by Vélu's formula.

Motivation

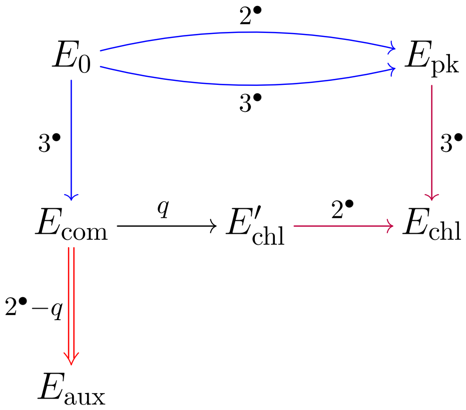


In the NIST SQIsign,

- Blue isogenies by IdealToIsogeny in SQIsign2D-West.
- Purple isogenies by Vélu's formula.

Many $(2,2)$-isogenies in signing $\Rightarrow$ We want to reduce.

Diagram of SQIsign2DPush



- Blue isogenies by DoublePath in SQIsignHD.
- Purple isogenies by Vélu's formula.
- **Red isogeny** by **Our new algorithm**.

Notation

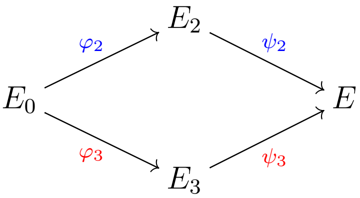
- $p = c \cdot 2^{e_2} \cdot 3^{e_3} - 1$ is a prime number ($2^{e_2} > \sqrt{p}$).
- $E, E^\bullet, E_\bullet, \dots$: supersingular elliptic curves over $\mathbb{F}_{p^2}$
- $E_0 : y^2 = x^3 + x/\mathbb{F}_p$, $j(E_0) = 1728$.
- Identify $\mathrm{End}(E_0)$ with $\mathcal{O}_0 = \mathbb{Z} + \mathbb{Z}\mathbf{i} + \mathbb{Z}\frac{\mathbf{i}+\mathbf{j}}{2} + \mathbb{Z}\frac{1+\mathbf{k}}{2}$.

DoublePath [DLRW 2024]

Input: E_0

Output:

- two random 2^{e_2}-isogenies $E_0 \xrightarrow{\varphi_2} E_2 \xrightarrow{\psi_2} E$,
- the left $\mathcal{O}_0$-ideal I_2 corresponding to $\psi_2 \circ \varphi_2$,
- two random 3^{e_3}-isogenies $E_0 \xrightarrow{\varphi_3} E_3 \xrightarrow{\psi_3} E$,
- the left $\mathcal{O}_0$-ideal I_3 corresponding to $\psi_3 \circ \varphi_3$.



Note : $p = c \cdot 2^{e_2} \cdot 3^{e_3} - 1$.

Kani's lemma

Setting

$$E_1 \xrightarrow{\varphi_1} E_2 \xrightarrow{\varphi_2} E_3$$

$d_1 := \deg \varphi_1$ and $d_2 := \deg \varphi_2$

$\gcd(d_1, d_2) = 1$ and $d_1 + d_2 = 2^e$

Kani's lemma

Setting

$$E_1 \xrightarrow{\varphi_1} E_2 \xrightarrow{\varphi_2} E_3$$

$$d_1 \coloneqq \deg \varphi_1 \text{ and } d_2 \coloneqq \deg \varphi_2$$
$$\gcd(d_1, d_2) = 1 \text{ and } d_1 + d_2 = 2^e$$

$\exists$ algorithm s.t.

Input : E_1, E_3, d_1, d_2, $(\varphi_2 \circ \varphi_1) \restriction_{E_1[2^e]}$

Output : E_2, φ_1, $\widehat{\varphi_2}$.

Kani's lemma

Setting

$$E_1 \xrightarrow{\varphi_1} E_2 \xrightarrow{\varphi_2} E_3$$

$$d_1 := \deg \varphi_1 \text{ and } d_2 := \deg \varphi_2$$
$$\gcd(d_1, d_2) = 1 \text{ and } d_1 + d_2 = 2^e$$

$\exists$ algorithm s.t.

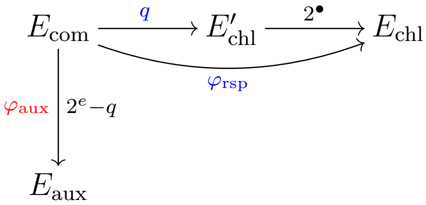
Input : E_1, E_3, d_1, d_2, $(\varphi_2 \circ \varphi_1) \restriction_{E_1[2^e]}$

Output : E_2, φ_1, $\widehat{\varphi_2}$.

Note:

- Using a $(2^e, 2^e)$-isogeny
- d_1 and d_2 are not necessarily smooth.

Auxiliary isogeny



Let q be the odd part of $\deg \varphi_{\mathrm{rsp}}$.

- $q < 2^{e_2}$.
- $3 \nmid q$ (so that $\widehat{\varphi_{\mathrm{rsp}}} \circ \varphi_{\mathrm{chl}}$ is cyclic).

We want to compute φ_{aux} of degree $2^e - q$ for some $e \leq e_2$.

Auxiliary isogeny

We want to compute φ_{aux} of degree $2^e - q$ for some $e \leq e_2$.

Auxiliary isogeny

We want to compute φ_{aux} of degree $2^e - q$ for some $e \le e_2$.

- Divide φ_{aux} into $\varphi_{\mathrm{aux}}^{(3)} \circ \varphi'_{\mathrm{aux}}$ s.t. $\deg \varphi_{\mathrm{aux}}^{(3)} = 3^{\bullet}$ and $3 \nmid \deg \varphi'_{\mathrm{aux}}$.

$$E_{\mathrm{aux}} \xleftarrow{\varphi_{\mathrm{aux}}^{(3)}} E'_{\mathrm{aux}} \xleftarrow{\varphi'_{\mathrm{aux}}} E_{\mathrm{com}}$$

Auxiliary isogeny

We want to compute φ_{aux} of degree $2^e - q$ for some $e \leq e_2$.

- Divide φ_{aux} into $\varphi_{\mathrm{aux}}^{(3)} \circ \varphi'_{\mathrm{aux}}$ s.t. $\deg \varphi_{\mathrm{aux}}^{(3)} = 3^\bullet$ and $3 \nmid \deg \varphi'_{\mathrm{aux}}$.

$$E_{\mathrm{aux}} \xleftarrow{\varphi_{\mathrm{aux}}^{(3)}} E'_{\mathrm{aux}} \xleftarrow{\varphi'_{\mathrm{aux}}} E_{\mathrm{com}}$$

- $\varphi_{\mathrm{aux}}^{(3)}$ is computed by Vélu's formula.

Auxiliary isogeny

We want to compute φ_{aux} of degree $2^e - q$ for some $e \leq e_2$.

- Divide φ_{aux} into $\varphi^{(3)}_{\mathrm{aux}} \circ \varphi'_{\mathrm{aux}}$ s.t. $\deg \varphi^{(3)}_{\mathrm{aux}} = 3^{\bullet}$ and $3 \nmid \deg \varphi'_{\mathrm{aux}}$.

$$E_{\mathrm{aux}} \xleftarrow{\varphi^{(3)}_{\mathrm{aux}}} E'_{\mathrm{aux}} \xleftarrow{\varphi'_{\mathrm{aux}}} E_{\mathrm{com}}$$

- $\varphi^{(3)}_{\mathrm{aux}}$ is computed by Vélu's formula.
- Let $d := \deg \varphi'_{\mathrm{aux}}$. $(2^e - q = d \cdot 3^{\bullet})$

Auxiliary isogeny

We want to compute $\varphi_{\rm aux}$ of degree $2^e - q$ for some $e \le e_2$.

- Divide $\varphi_{\rm aux}$ into $\varphi^{(3)}_{\rm aux} \circ \varphi'_{\rm aux}$ s.t. $\deg \varphi^{(3)}_{\rm aux} = 3^\bullet$ and $3 \nmid \deg \varphi'_{\rm aux}$.

$$E_{\rm aux} \xleftarrow{\varphi^{(3)}_{\rm aux}} E'_{\rm aux} \xleftarrow{\varphi'_{\rm aux}} E_{\rm com}$$

- $\varphi^{(3)}_{\rm aux}$ is computed by Vélu's formula.
- Let $d := \deg \varphi'_{\rm aux}$. $(2^e - q = d \cdot 3^\bullet)$
- There is $e' \le e$ s.t. $2^{e'} > d$ and $3 \nmid 2^{e'} - d$.

  (If $\varphi^{(3)}_{\rm aux} = \mathrm{id}$ then $e' = e$. Otherwise, e or $e-1$ is OK.)

Auxiliary isogeny

We want to compute φ_{aux} of degree $2^e - q$ for some $e \le e_2$.

- Divide φ_{aux} into $\varphi_{\text{aux}}^{(3)} \circ \varphi'_{\text{aux}}$ s.t. $\deg \varphi_{\text{aux}}^{(3)} = 3^\bullet$ and $3 \nmid \deg \varphi'_{\text{aux}}$.

$$E_{\text{aux}} \xleftarrow{\varphi_{\text{aux}}^{(3)}} E'_{\text{aux}} \xleftarrow{\varphi'_{\text{aux}}} E_{\text{com}}$$

- $\varphi_{\text{aux}}^{(3)}$ is computed by Vélu's formula.
- Let $d := \deg \varphi'_{\text{aux}}$. $(2^e - q = d \cdot 3^\bullet)$
- There is $e' \le e$ s.t. $2^{e'} > d$ and $3 \nmid 2^{e'} - d$.

  (If $\varphi_{\text{aux}}^{(3)} = \text{id}$ then $e' = e$. Otherwise, e or $e - 1$ is OK.)

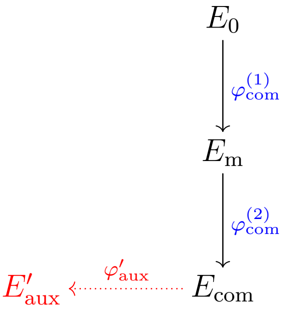
For simplicity, we assume $e' = e$, i.e., $3 \nmid 2^e - d$.

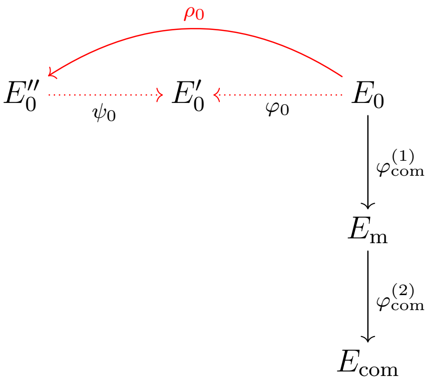
How to compute φ'_{aux}

Input: $\varphi_{\mathrm{com}}^{(1)}$, $\varphi_{\mathrm{com}}^{(2)}$, d, e s.t.

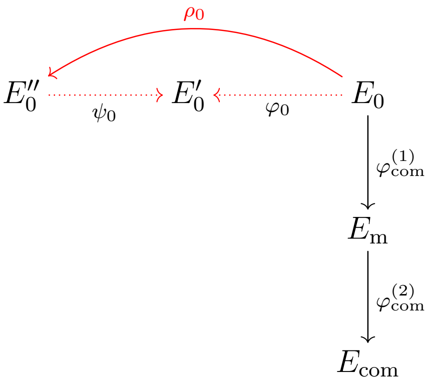
- $\deg \varphi_{\mathrm{com}}^{(1)} = \deg \varphi_{\mathrm{com}}^{(2)} = 3^{e_3}$
- $e \leq e_2$ and $2^e > d$.
- $3 \nmid d$ and $3 \nmid 2^e - d$.

Output: $\varphi'_{\mathrm{aux}} \restriction_{E_{\mathrm{com}}[2^{e_2}]}$ of degree d from E_{com}.

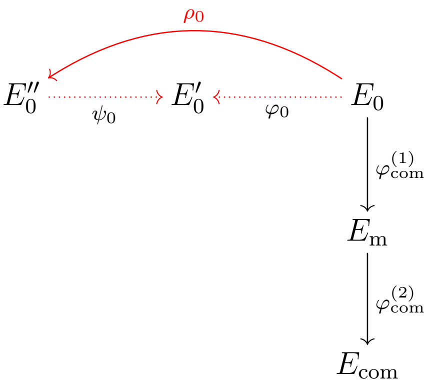




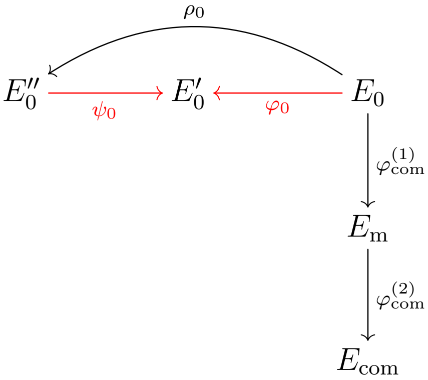
1. Compute $\alpha \in \mathrm{End}(E_0)$ s.t. $\deg \alpha = 3^{e_3} \cdot d(2^e - d)$.



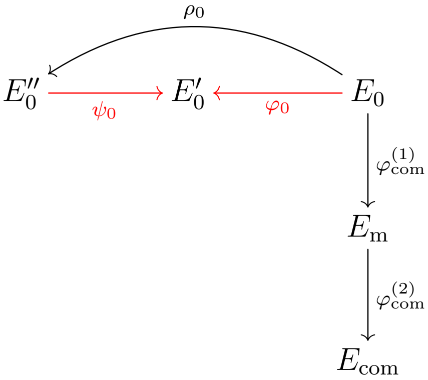
1. Compute $\alpha \in \mathrm{End}(E_0)$ s.t. $\deg \alpha = 3^{e_3} \cdot d(2^e - d)$.
2. Divide α into $\widehat{\varphi_0} \circ \psi_0 \circ \rho_0$ s.t.
   $\deg \rho_0 = 3^{e_3}$, $\deg \psi_0 = 2^e - d$, and $\deg \varphi_0 = d$.



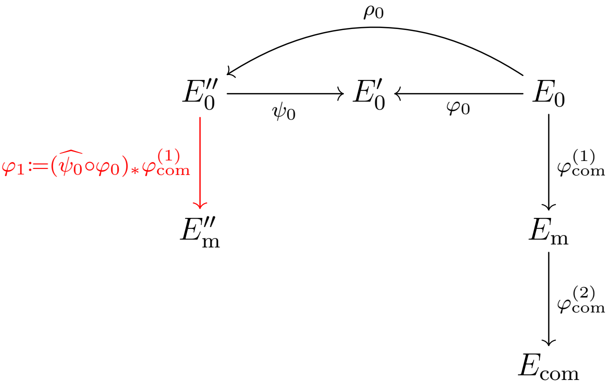
1. Compute $\alpha \in \mathrm{End}(E_0)$ s.t. $\deg \alpha = 3^{e_3} \cdot d(2^e - d)$.
2. Divide α into $\widehat{\varphi_0} \circ \psi_0 \circ \rho_0$ s.t. $\deg \rho_0 = 3^{e_3}$, $\deg \psi_0 = 2^e - d$, and $\deg \varphi_0 = d$.
3. Compute ρ_0 by Vélu's formula.



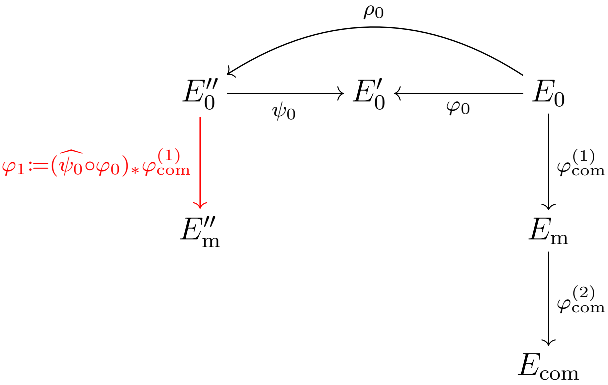
4. Compute $(\widehat{\psi_0} \circ \varphi_0) \restriction_{E_0[2^e]}$ by α and ρ_0.



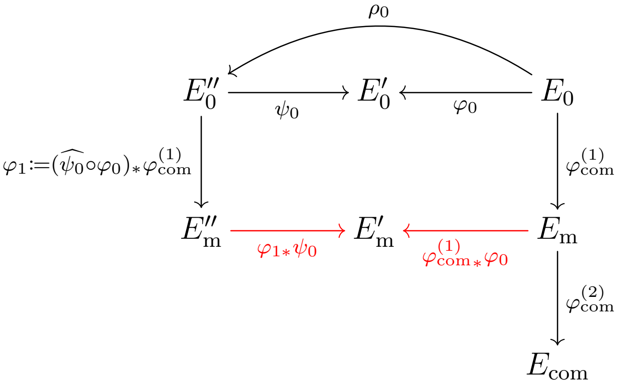
4. Compute $(\widehat{\psi_0} \circ \varphi_0) \restriction_{E_0[2^e]}$ by α and ρ_0.
5. Compute ψ_0 and φ_0 by Kani's lemma.



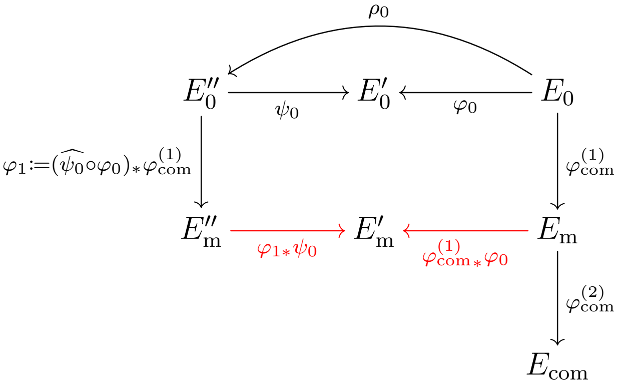
6. Compute $\widehat{\psi_0} \circ \varphi_0(\ker \varphi_{\mathrm{com}}^{(1)})$ by ψ_0 and φ_0.



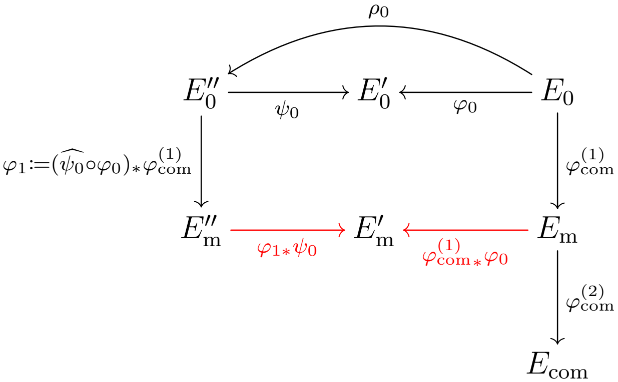
6. Compute $\widehat{\psi_0} \circ \varphi_0(\ker \varphi_{\mathrm{com}}^{(1)})$ by ψ_0 and φ_0.
7. Compute $\varphi_1 := (\widehat{\psi_0} \circ \varphi_0)_* \varphi_{\mathrm{com}}^{(1)}$ by Vélu's formula.



8. Compute $\widehat{\varphi_{1*}\psi_0} \circ ({\varphi_{\mathrm{com}}^{(1)}}_* \varphi_0) \restriction_{E_{\mathrm{m}}[2^e]}$.

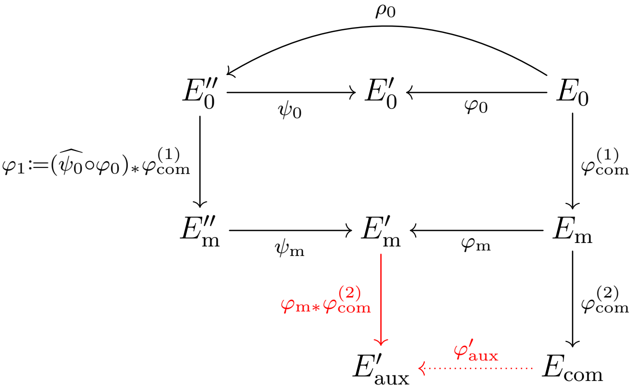


8. Compute $\widehat{\varphi_{1*}\psi_0} \circ (\varphi_{\mathrm{com}*}^{(1)}\varphi_0) \restriction_{E_{\mathrm{m}}[2^e]}$.
9. Compute $\varphi_{1*}\psi_0$ and $\varphi_{\mathrm{com}*}^{(1)}\varphi_0$ by Kani's lemma.

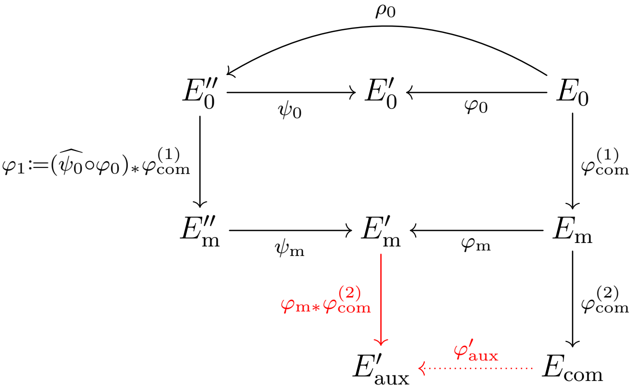


8. Compute $\widehat{\varphi_{1*}\psi_0} \circ (\varphi_{\mathrm{com}*}^{(1)}\varphi_0) \restriction_{E_{\mathrm{m}}[2^e]}$.
9. Compute $\varphi_{1*}\psi_0$ and $\varphi_{\mathrm{com}*}^{(1)}\varphi_0$ by Kani's lemma.

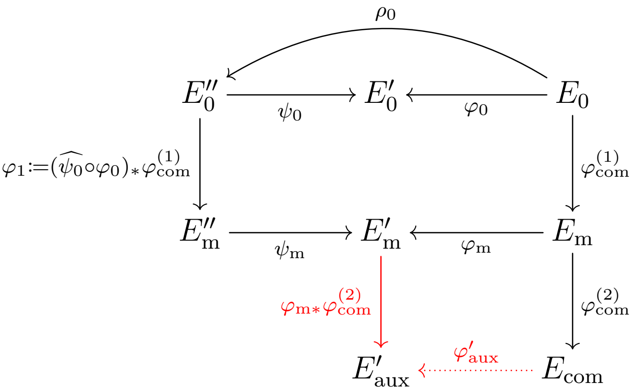
   (Let $\psi_{\mathrm{m}} := \varphi_{1*}\psi_0$ and $\varphi_{\mathrm{m}} := \varphi_{\mathrm{com}*}^{(1)}\varphi_0$.)



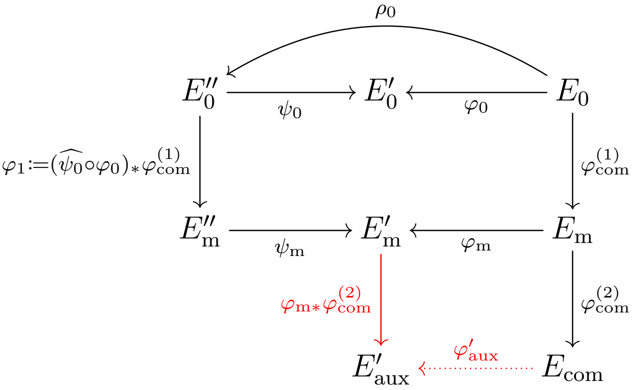
8. Compute $\varphi_{\mathrm{m}}(\ker \varphi^{(2)}_{\mathrm{com}})$ by φ_{m}.



8. Compute $\varphi_{\mathrm{m}}(\ker \varphi_{\mathrm{com}}^{(2)})$ by φ_{m}.
9. Compute $\varphi_{\mathrm{m}*}\varphi_{\mathrm{com}}^{(2)}$ by Vélu's formula.



8. Compute $\varphi_{\mathrm{m}}(\ker \varphi_{\mathrm{com}}^{(2)})$ by φ_{m}.
9. Compute $\varphi_{\mathrm{m}*}\varphi_{\mathrm{com}}^{(2)}$ by Vélu's formula.
10. Let $\varphi_{\mathrm{aux}}' \coloneqq {\varphi_{\mathrm{com}}^{(2)}}_* \varphi_{\mathrm{m}}$.



8. Compute $\varphi_{\mathrm{m}}(\ker \varphi_{\mathrm{com}}^{(2)})$ by φ_{m}.
9. Compute $\varphi_{\mathrm{m}*}\varphi_{\mathrm{com}}^{(2)}$ by Vélu's formula.
10. Let $\varphi_{\mathrm{aux}}' \coloneqq \varphi_{\mathrm{com}}^{(2)}{}_* \varphi_{\mathrm{m}}$.
11. Compute $\varphi_{\mathrm{aux}}' \restriction_{E_{\mathrm{com}}[2^{e_2}]}$ by $\varphi_{\mathrm{com}}^{(2)}$, φ_{m}, $\varphi_{\mathrm{m}*}\varphi_{\mathrm{com}}^{(2)}$.

Advantage of SQIsign2DPush

Fewer $(2,2)$-isogenies in signing.

Table: Approximate numbers of isogenies in signing (λ bits security)

	2	3	$(2,2)$
Push	$\mathbf{2}\lambda$	$\mathbf{7}\lambda$	$\mathbf{2}\lambda$
West	1λ	0	9λ
East	1λ	0	6λ

We expect that SQIsign2DPush is faster than other SQIsign variants.

Advantage of SQIsign2DPush

Fewer $(2,2)$-isogenies in signing.

Table: Approximate numbers of isogenies in signing (λ bits security)

	2	3	$(2,2)$
Push	$\mathbf{2}\lambda$	$\mathbf{7}\lambda$	$\mathbf{2}\lambda$
West	1λ	0	9λ
East	1λ	0	6λ

We expect that SQIsign2DPush is faster than other SQIsign variants.

Note: The verification of SQIsign2DPush is slightly less efficient.

$\because$ The cyclicity check of $\widehat{\varphi_{\mathrm{rsp}}} \circ \varphi_{\mathrm{chl}}$ requires a point evaluation by $(2,2)$-isogenies.

Security

We need ad hoc security assumption:

- The distributions of E_{pk} and E_{com} come from DoublePath.
- φ_{aux} is the push-forward of an isogeny from RepresentInteger.

Security

We need ad hoc security assumption:

- The distributions of E_{pk} and E_{com} come from DoublePath.
- φ_{aux} is the push-forward of an isogeny from RepresentInteger.

Better than SQIsign2D-East:

- φ_{aux} in East depends on φ_{sk}.

Security

We need ad hoc security assumption:

- The distributions of E_{pk} and E_{com} come from DoublePath.
- φ_{aux} is the push-forward of an isogeny from RepresentInteger.

Better than SQIsign2D-East:

- φ_{aux} in East depends on φ_{sk}.

Trying to prove the security in a similar way to the NIST SQIsign.

Still ongoing...

Parameters & Sizes

Security (bits)	p	Public key (bytes)	Sign (bytes)
128	$2^{131} \cdot 3^{78} - 1$	66	152
192	$2^{191} \cdot 3^{117} - 1$	98	220
256	$2^{263} \cdot 3^{156} - 1$	130	297

The sizes are almost the same as the NIST SQIsign.

Summary

- We proposed a new SQIsign variant, SQIsign2DPush.
- We reduced the number of $(2, 2)$-isogenies in signing ☺
- The verification is slightly less efficient 😐
- The security assumption is ad hoc ☹