Ideal-to-isogeny algorithm using 2-dimensional isogenies and its application to SQIsign

Hiroshi Onuki[1], Kohei Nakagawa[2]

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

2024.12.10

Overview

- We propose an *ideal-to-isogeny algorithm* using 2-dimensional isogenies (Kani's lemma).
- This can be used to compute φ_{sk}, φ_{com}, and φ_{rsp} in SQIsign.
- This *improves the efficiency* of (KLPT-based) SQIsign.
- This talk focuses on the computation of φ_{rsp}.

Ideal-to-isogeny Algorithm

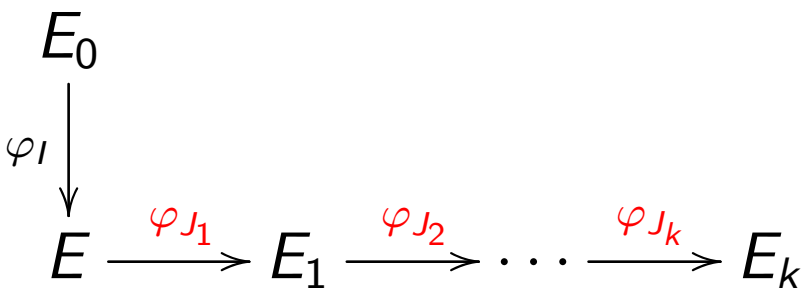
Setting

$2^f \mid p+1$,

I : a left $\mathcal{O}_0$-ideal of odd norm,

$\mathrm{End}(E) \cong \mathcal{O}$ (induced by φ_I),

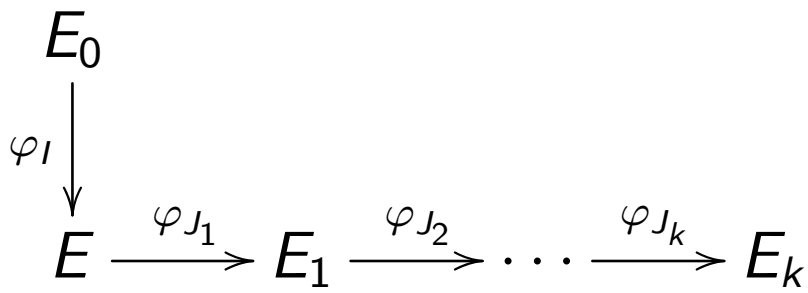
J : a left $\mathcal{O}$-ideal of norm 2^{kf}, $J = J_1 \cdots J_k$, where $\mathrm{n}(J_i) = 2^f$.



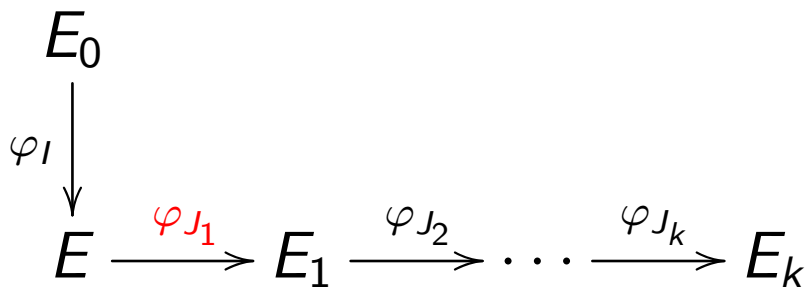
Given: E, I, $\mathcal{O}$, J, φ_I,

Output: $\{\varphi_{J_i}\}_{i=1\cdots k}$. $\leftarrow$ *representation of* φ_{rsp}

Issue to solve



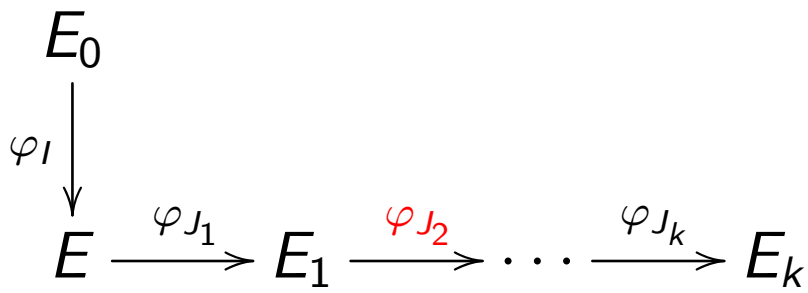
Issue to solve



We can compute

$$\ker \varphi_{J_1} = \varphi_I(E_0[IJ_1] \cap E_0[2^f]).$$

Issue to solve



We can compute

$$\ker \varphi_{J_1} = \varphi_I(E_0[IJ_1] \cap E_0[2^f]).$$

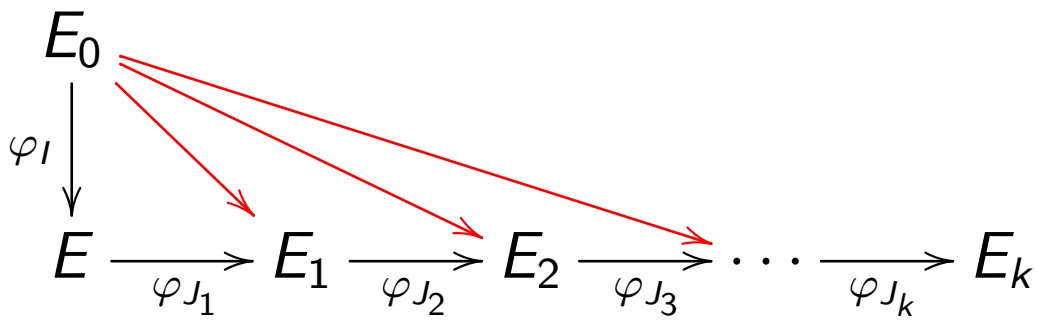
But we CANNOT compute

$$\ker \varphi_{J_2} = \varphi_{J_1} \circ \varphi_I(E_0[IJ_1J_2] \cap E_0[2^{2f}])$$

because $E_0[2^{2f}] \not\subset E_0(\mathbb{F}_{p^2})$

Idea in SQIsign

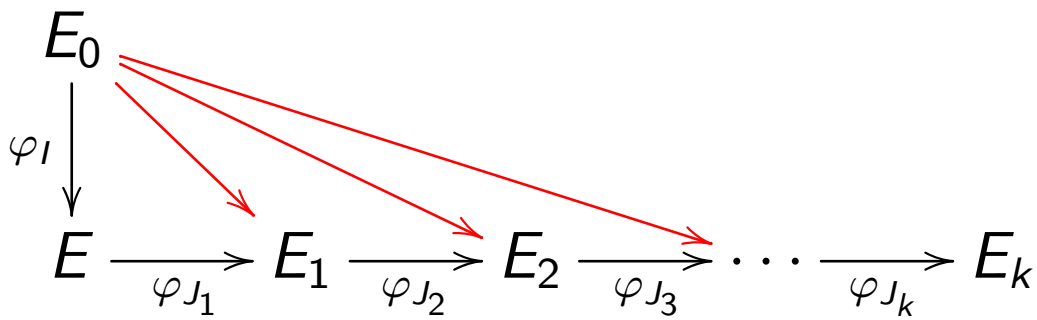
The idea in the original method:



Using odd degree isogenies: $E_0 \to E_i$.

Idea in SQIsign

The idea in the original method:

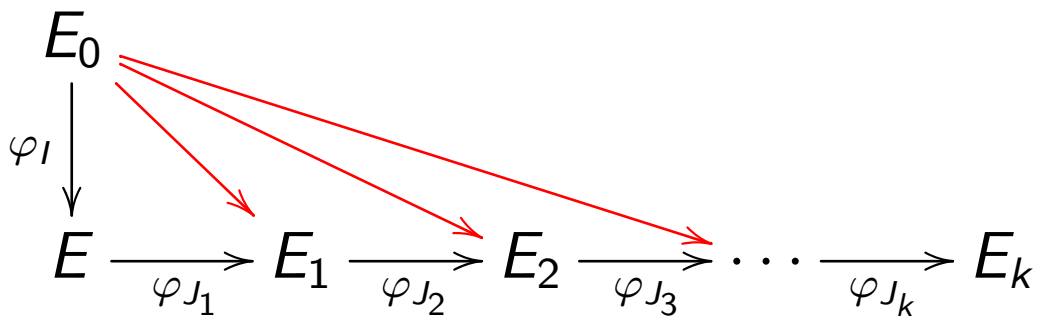


Using odd degree isogenies: $E_0 \to E_i$.

- Compute I_i equivalent to $IJ_1 \cdots J_i$ s.t. $\mathrm{n}(I_i)$ is odd.
- Compute φ_{I_i} by Vélu's formula.

Idea in SQIsign

The idea in the original method:



Using odd degree isogenies: $E_0 \to E_i$.

- Compute I_i equivalent to $IJ_1 \cdots J_i$ s.t. $\mathrm{n}(I_i)$ is odd.
- Compute φ_{I_i} by Vélu's formula.

Then

$$\ker \varphi_{J_{i+1}} = \varphi_{I_i}(E_i[I_i J_{i+1}] \cap E_0[2^f]).$$

Restriction on p

Since φ_{I_i} is computed by Vélu's formula, we require

$$\deg \varphi_{I_i} = \mathrm{n}(I_i) \text{ is smooth and } \ker \varphi_{I_i} \subset E_0(\mathbb{F}_{p^2}).$$

Restriction on p

Since φ_{I_i} is computed by Vélu's formula, we require

$$\deg \varphi_{I_i} = \mathrm{n}(I_i) \text{ is smooth and } \ker \varphi_{I_i} \subset E_0(\mathbb{F}_{p^2}).$$

$\Rightarrow$ $p^2 - 1$ has a smooth odd factor T of size $p^{1.5}$.

Restriction on p

Since φ_{I_i} is computed by Vélu's formula, we require

$$\deg \varphi_{I_i} = \mathrm{n}(I_i) \text{ is smooth and } \ker \varphi_{I_i} \subset E_0(\mathbb{F}_{p^2}).$$

$\Rightarrow$ $p^2 - 1$ has a smooth odd factor T of size $p^{1.5}$.

$\Rightarrow$ $\deg \varphi_{I_i}$ has large prime factors.

$\Rightarrow$ the computation of φ_{I_i} is inefficient.

Restriction on p

Since φ_{I_i} is computed by Vélu's formula, we require

$$\deg \varphi_{I_i} = \mathrm{n}(I_i) \text{ is smooth and } \ker \varphi_{I_i} \subset E_0(\mathbb{F}_{p^2}).$$

$\Rightarrow$ $p^2 - 1$ has a smooth odd factor T of size $p^{1.5}$.

$\Rightarrow$ $\deg \varphi_{I_i}$ has large prime factors.

$\Rightarrow$ the computation of φ_{I_i} is inefficient.

Note:
[De Feo, Leroux, Longa, Wesolowski, 2022] improved $p^{1.5}$ to $p^{1.25}$.

Restriction on p

Since φ_{I_i} is computed by Vélu's formula, we require

$$\deg \varphi_{I_i} = \mathrm{n}(I_i) \text{ is smooth and } \ker \varphi_{I_i} \subset E_0(\mathbb{F}_{p^2}).$$

$\Rightarrow$ $p^2 - 1$ has a smooth odd factor T of size $p^{1.5}$.

$\Rightarrow$ $\deg \varphi_{I_i}$ has large prime factors.

$\Rightarrow$ the computation of φ_{I_i} is inefficient.

Note:
[De Feo, Leroux, Longa, Wesolowski, 2022] improved $p^{1.5}$ to $p^{1.25}$.

For the NIST level 1,

$$\begin{aligned} T =& 3^{36} \cdot 7^4 \cdot 11 \cdot 13 \cdot 23^2 \cdot 37 \cdot 59^2 \cdot 89 \cdot 97 \cdot 101^2 \cdot 107 \cdot 109^2 \\ & \cdot 131 \cdot 137 \cdot 197^2 \cdot 223 \cdot 239 \cdot 383 \cdot 389 \cdot 491^2 \cdot 499 \cdot 607 \\ & \cdot 743^2 \cdot 1033 \cdot 1049 \cdot 1193 \cdot 1913^2 \cdot 1973 \end{aligned}$$

Our idea

Replacing T-isogenies with $(2^{f_2}, 2^{f_2})$-*isogenies*.

- We do not require T divides $p^2 - 1$.
- $p = 2^{f_1+f_2} \cdot c - 1$, where $2^{f_2} > \sqrt{p}$ and c is small.

Our setting

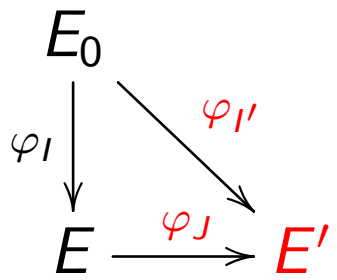
Setting

I : a left $\mathcal{O}_0$-ideal of odd norm,

$\mathrm{End}(E) \cong \mathcal{O}$ (induced by φ_I),

J : a left $\mathcal{O}$-ideal of norm 2^{f_1},

$I' \sim IJ$ s.t. $\mathrm{n}(I')$ is odd and $< 2^{f_2}$. (NOT require $\mathrm{n}(I')$ is smooth.)

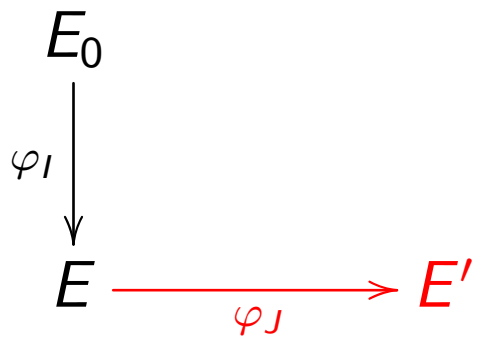


Given: E, I, $\mathcal{O}$, J, φ_I,

Output: E', I', φ_J, $\varphi_{I'}$.

Our algorithm (1/4)

1. Compute φ_J and E' by Vélu's formula.



$\ker \varphi_J = \varphi_I(E_0[IJ] \cap E_0[2^{f_1}])$.

Our algorithm (2/4)

2. Find $a, b \in \mathbb{Z}$ and $\beta \in IJ$ s.t.
   - $D := \mathrm{n}(\beta)/\mathrm{n}(IJ)$ is odd,
   - $a^2 + b^2 + D = 2^{f_2}$.

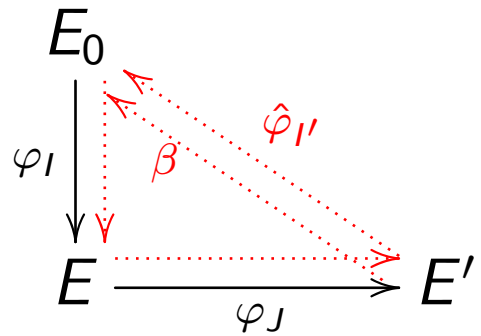
Computed by the lattice enumeration and Cornacchia's algorithm.

Our algorithm (2/4)

2. Find $a, b \in \mathbb{Z}$ and $\beta \in IJ$ s.t.
   - $D := \mathrm{n}(\beta)/\mathrm{n}(IJ)$ is odd,
   - $a^2 + b^2 + D = 2^{f_2}$.

Computed by the lattice enumeration and Cornacchia's algorithm.

Let $I' := IJ\bar{\beta}/\mathrm{n}(IJ)$.
$\Rightarrow I' \sim IJ$ and $\mathrm{n}(I') = D$, $\quad \beta = \hat{\varphi}_{I'} \circ \varphi_J \circ \varphi_I \in \mathrm{End}(E_0)$.



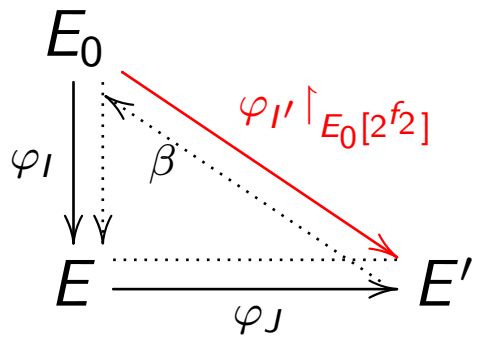
Note: $\varphi_{I'}$ is not yet computed.

Our algorithm (3/4)

3. Compute $\varphi_{I'}\restriction_{E_0[2^{f_2}]}$ *i.e.*, the images of a basis of $E_0[2^{f_2}]$ under $\varphi_{I'}$.

We use

$$\varphi_J \circ \varphi_I \circ \bar{\beta} = \varphi_J \circ \varphi_I \circ \hat{\varphi}_I \circ \hat{\varphi}_J \circ \varphi_{I'} = 2^{f_1} \cdot \mathrm{n}(I) \cdot \varphi_{I'}$$



Our algorithm (3/4)

3. Compute $\varphi_{I'}\restriction_{E_0[2^{f_2}]}$ *i.e.*, the images of a basis of $E_0[2^{f_2}]$ under $\varphi_{I'}$.

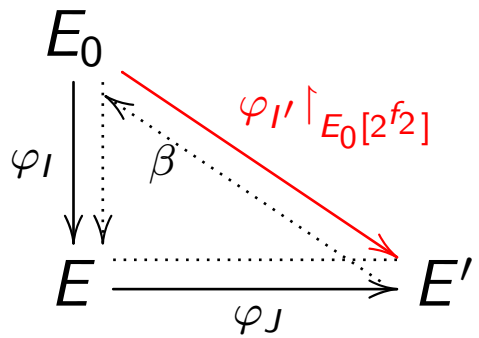
We use

$$\varphi_J \circ \varphi_I \circ \bar{\beta} = \varphi_J \circ \varphi_I \circ \hat{\varphi}_I \circ \hat{\varphi}_J \circ \varphi_{I'} = 2^{f_1} \cdot \mathrm{n}(I) \cdot \varphi_{I'}$$

Let (P, Q) be a basis of $E_0[2^{f_1+f_2}] \subset E_0(\mathbb{F}_{p^2})$.

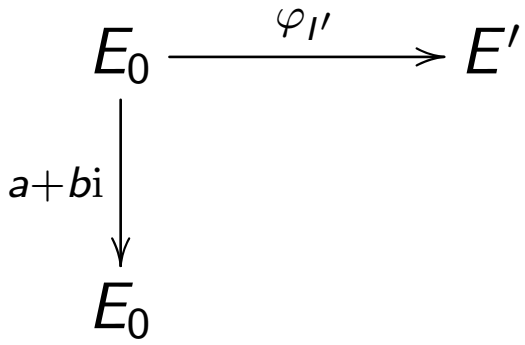
Then $([2^{f_1} \cdot \mathrm{n}(I)]P, [2^{f_2} \cdot \mathrm{n}(I)]Q)$ is a basis of $E_0[2^{f_2}]$.

$$\varphi_{I'}([2^{f_2} \cdot \mathrm{n}(I)](P)) = \varphi_J \circ \varphi_I \circ \bar{\beta}(P).$$



Our algorithm (4/4)

4. Compute $\varphi_{I'}$ by Kani's lemma on the diagram

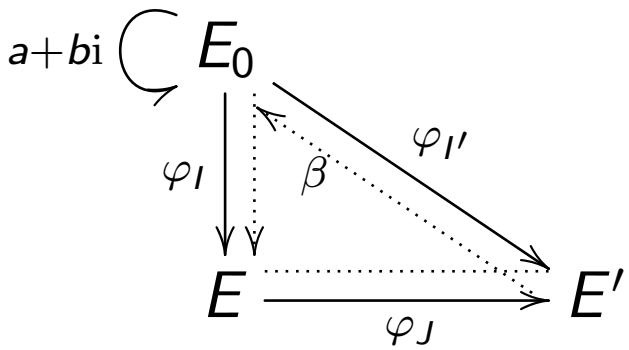


We can apply Kani's lemma since

- $\deg(a+b\mathrm{i}) + \deg\varphi_{I'} = a^2 + b^2 + D = 2^{f_2}$.
- We have $\varphi_{I'} \restriction_{E_0[2^{f_2}]}$ and can evaluate $a+b\mathrm{i}$ on $E_0[2^{f_2}]$.

Summary of our algorithm

1. Compute $\ker \varphi_J$ by Vélu's formula.
2. Find $a, b \in \mathbb{Z}$ and $\beta \in IJ$ suitable for Kani's lemma and let $I' := IJ\bar{\beta}/\mathrm{n}(IJ)$.
3. Compute $\varphi_{I'}\restriction_{E_0[2^{f_2}]}$.
4. Compute $\varphi_{I'}$ by Kani's lemma.



Impact on SQIsign (level 1)

Consider the NIST level 1 case:

Our (conservative) estimation shows

(The cost of a T-isogeny) $\approx$ (the cost of a $(2^{f_2}, 2^{f_2})$-isogeny).

Impact on SQIsign (level 1)

Consider the NIST level 1 case:

Our (conservative) estimation shows

(The cost of a T-isogeny) $\approx$ (the cost of a $(2^{f_2}, 2^{f_2})$-isogeny).

Table: Num. of isogenies

	T-isogeny	$(2^{f_2}, 2^{f_2})$-isogeny
Keygen	16	7
Signing	29	11

Impact on SQIsign (level 1)

Consider the NIST level 1 case:

Our (conservative) estimation shows

(The cost of a T-isogeny) $\approx$ (the cost of a $(2^{f_2}, 2^{f_2})$-isogeny).

Table: Num. of isogenies

	T-isogeny	$(2^{f_2}, 2^{f_2})$-isogeny
Keygen	16	7
Signing	29	11

$\Rightarrow$ We can expect

- the key generation time is at least *2 times faster*,
- the signing time is at least *3 times faster*.

Impact on SQIsign (level 1)

Consider the NIST level 1 case:

Our (conservative) estimation shows

(The cost of a T-isogeny) $\approx$ (the cost of a $(2^{f_2}, 2^{f_2})$-isogeny).

Table: Num. of isogenies

	T-isogeny	$(2^{f_2}, 2^{f_2})$-isogeny
Keygen	16	7
Signing	29	11

$\Rightarrow$ We can expect

- the key generation time is at least *2 times faster*,
- the signing time is at least *3 times faster*.

At the higher levels, the impact is more significant.

Conclusion & Remark

- We propose an ideal-to-isogeny algorithm using 2-dimensional isogenies.
- The idea is to replace T-isogenies with $(2^{f_2}, 2^{f_2})$-isogenies.
- This improves the efficiency of SQIsign.
  (other higher-dimensional variants are more efficient...)

Conclusion & Remark

- We propose an ideal-to-isogeny algorithm using 2-dimensional isogenies.
- The idea is to replace T-isogenies with $(2^{f_2}, 2^{f_2})$-isogenies.
- This improves the efficiency of SQIsign.
  (other higher-dimensional variants are more efficient...)

Remark

Other ideal-to-isogeny algorithms using 2-dimensional isogenies:

- DeuringVRF [Leroux, 23]
- SILBE [Duparc-Fouotsa-Vaudenay, 2024]
- SQIsign2D-West [Basso, De Feo, Dartois, Leroux, Maino, Pope, Robert, Wesolowski, 2024]

- **Future work**: Finding new applications of these algorithms.