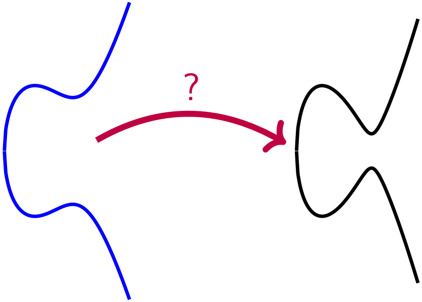
The endomorphism ring problem given an endomorphism

Arthur Herlédan Le Merdy, Benjamin Wesolowski

Tuesday 9$^{\text{th}}$ April, 2024

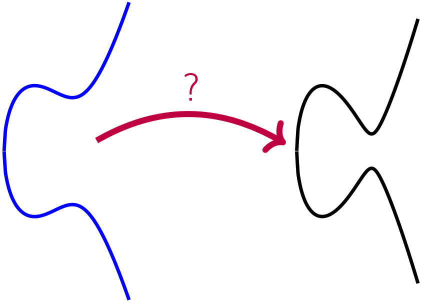
Hard problems

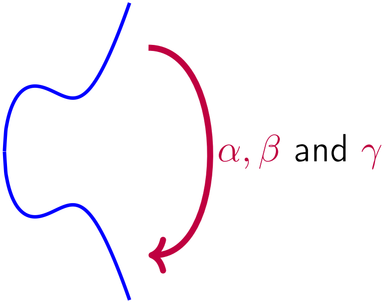
Isogeny Problem



Hard problems

Isogeny Problem $\iff$ Endomorphism Ring Problem





$$\mathrm{End}(\quad) = \mathbb{Z} + \alpha\mathbb{Z} + \beta\mathbb{Z} + \gamma\mathbb{Z}$$

Supersingular endomorphism ring problem

The supersingular endomorphism ring problem (EndRing):

Given a **supersingular** elliptic curve $\boldsymbol{E}$, find a basis of its endomorphism ring $\mathbf{End}(\boldsymbol{E})$.

Supersingular endomorphism ring problem

The supersingular endomorphism ring problem (EndRing):

Given a **supersingular** elliptic curve E, find a basis of its endomorphism ring $\mathbf{End}(E)$.

[Rob22b] Given some integer factorisation, solving **ordinary** `EndRing` takes polynomial time.

Supersingular endomorphism ring problem

The supersingular endomorphism ring problem (EndRing):

Given a **supersingular** elliptic curve $\boldsymbol{E}$, find a basis of its endomorphism ring $\mathbf{End}(\boldsymbol{E})$.

[Rob22b] Given some integer factorisation, solving **ordinary** `EndRing` takes polynomial time.

[Wes21] `EndRing` $\iff$ `Isogeny Problem` **under the Generalized Riemann Hypothesis**.

Supersingular endomorphism ring problem

The supersingular endomorphism ring problem (EndRing):

Given a **supersingular** elliptic curve $\boldsymbol{E}$, find a basis of its endomorphism ring $\mathbf{End}(\boldsymbol{E})$.

[Rob22b] Given some integer factorisation, solving **ordinary** `EndRing` takes polynomial time.

[Wes21] `EndRing` $\iff$ `Isogeny Problem` **under the Generalized Riemann Hypothesis**.

- Some protocols give **a public endomorphism** $\theta \in \mathrm{End}(E) \backslash \mathbb{Z}$:

  [Cas+18] CSIDH The Frobenius endomorphism $\pi_E : (x, y) \mapsto (x^p, y^p)$.

  [Feo+23] SCALLOP An $(\mathbb{Z} + f\mathbb{Z}[i])$-orientation with f a large prime.

Supersingular endomorphism ring problem given one endomorphism

The supersingular endomorphism ring problem given one endomorphism:

Given a supersingular elliptic curve $\boldsymbol{E}$ and an endomorphism $\boldsymbol{\theta} \in \mathrm{End}(E) \backslash \mathbb{Z}$,
find a basis of its endomorphism ring $\mathbf{End}\,(\boldsymbol{E})$.

Supersingular endomorphism ring problem given one endomorphism

The supersingular endomorphism ring problem given one endomorphism:

Given a supersingular elliptic curve $\boldsymbol{E}$ and an endomorphism $\boldsymbol{\theta} \in \mathrm{End}(E) \backslash \mathbb{Z}$, find a basis of its endomorphism ring $\mathbf{End}\,(\boldsymbol{E})$.

	EndRing	EndRing given one endomorphism θ
Classical	$p^{1/2}$	$\exp(\log \deg \theta)$ under heuristics
Quantum	$p^{1/4}$	$\mathrm{subexp}(\log \deg \theta)$ under heuristics

Complexity of EndRing and its variant for an elliptic curve defined over $\mathbb{F}_{p^2}$, with p a prime. [Arp+22]

Supersingular endomorphism ring problem given one endomorphism

The supersingular endomorphism ring problem given one endomorphism:

Given a supersingular elliptic curve $\boldsymbol{E}$ and an endomorphism $\boldsymbol{\theta} \in \mathrm{End}(E)\backslash\mathbb{Z}$, find a basis of its endomorphism ring $\mathbf{End}\,(\boldsymbol{E})$.

	EndRing	EndRing given one endomorphism θ
Classical	$p^{1/2}$	$\deg(\theta)^{1/4}$under GRH ~~under heuristics~~
Quantum	$p^{1/4}$	$\exp(O(\sqrt{\log(\deg\theta)\log\log(\deg\theta)}))$under GRH ~~under heuristics~~

Complexity of EndRing and its variant for an elliptic curve defined over $\mathbb{F}_{p^2}$, with p a prime. [Arp+22]

Supersingular endomorphism ring problem given one endomorphism

The supersingular endomorphism ring problem given one endomorphism:

Given a supersingular elliptic curve $\boldsymbol{E}$ and an endomorphism $\boldsymbol{\theta} \in \mathrm{End}(E) \backslash \mathbb{Z}$, find a basis of its endomorphism ring $\mathbf{End}(\boldsymbol{E})$.

	EndRing	EndRing given one endomorphism θ
Classical	$p^{1/2}$	$\deg(\theta)^{1/4}$under GRH ~~under heuristics~~
Quantum	$p^{1/4}$	subexp$(\log(\deg\theta))$under GRH ~~under heuristics~~

Complexity of EndRing and its variant for an elliptic curve defined over $\mathbb{F}_{p^2}$, with p a prime. [Arp+22]

Orientations [CK20]

Let $\theta \in \mathrm{End}(E) \backslash \mathbb{Z}$.

- $\mathbb{Z}[\theta] \simeq \mathbb{Z}[X]/ < X^2 + (\hat{\theta} + \theta)X + \deg\theta >$, i.e. $\mathbb{Z}[\theta]$ is a **quadratic order**.
- $\mathbb{Z}[\theta] \hookrightarrow \mathrm{End}(E)$.

Orientations [CK20]

Let $\theta \in \mathrm{End}(E)\backslash\mathbb{Z}$.

- $\mathbb{Z}[\theta] \simeq \mathbb{Z}[X]/ < X^2 + (\hat{\theta} + \theta)X + \deg\theta >$, i.e. $\mathbb{Z}[\theta]$ is a **quadratic order**.
- $\mathbb{Z}[\theta] \hookrightarrow \mathrm{End}(E)$.

Let $\mathfrak{O}$ be an order of an imaginary quadratic field K.

- An embedding $\iota : K \hookrightarrow \mathrm{End}(E) \otimes \mathbb{Q}$ is called an ***K*-orientation**, it is an **$\mathfrak{O}$-orientation** if $\iota(\mathfrak{O}) \subseteq \mathrm{End}(E)$.
- An $\mathbb{Z}[\omega]$-orientation ι is **entirely given by $\boldsymbol{\iota(\omega)} \in$ End $\boldsymbol{(E)}$**.

Orientations [CK20]

Let $\theta \in \mathrm{End}(E)\backslash\mathbb{Z}$.

- $\mathbb{Z}[\theta] \simeq \mathbb{Z}[X]/ < X^2 + (\hat{\theta} + \theta)X + \deg\theta >$, i.e. $\mathbb{Z}[\theta]$ is a **quadratic order**.
- $\mathbb{Z}[\theta] \hookrightarrow \mathrm{End}(E)$.

Let $\mathfrak{O}$ be an order of an imaginary quadratic field K.

- An embedding $\iota : K \hookrightarrow \mathrm{End}(E) \otimes \mathbb{Q}$ is called an ***K*-orientation**, it is an **$\mathfrak{O}$-orientation** if $\iota(\mathfrak{O}) \subseteq \mathrm{End}(E)$.
- An $\mathbb{Z}[\omega]$-orientation ι is **entirely given by $\boldsymbol{\iota(\omega)} \in$ End $\boldsymbol{(E)}$**.

Knowing an endomorphism $\longleftrightarrow$ Knowing an orientation

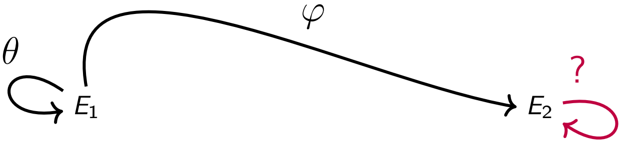
Oriented isogenies

Let $\iota : \mathbb{Z}[\omega] \hookrightarrow \mathrm{End}(E_1)$ be an orientation with $\iota(\omega) = \theta$. Let $\varphi : E_1 \to E_2$ an isogeny.

$$\begin{tikzcd} E_1 \arrow[loop left, "\theta"] \arrow[rr, bend left, "\varphi"] & & E_2 \end{tikzcd}$$

Oriented isogenies

Let $\iota : \mathbb{Z}[\omega] \hookrightarrow \mathrm{End}(E_1)$ be an orientation with $\iota(\omega) = \theta$. Let $\varphi : E_1 \to E_2$ an isogeny.



Oriented isogenies

Let $\iota : \mathbb{Z}[\omega] \hookrightarrow \mathrm{End}(E_1)$ be an orientation with $\iota(\omega) = \theta$. Let $\varphi : E_1 \to E_2$ an isogeny.

$$\begin{tikzcd} E_1 \arrow[loop left, "\theta"] \arrow[r, bend left, "\varphi"] & E_2 \arrow[l, bend left, "\hat{\varphi}"] \arrow[loop right, "?"] \end{tikzcd}$$

Oriented isogenies

Let $\iota : \mathbb{Z}[\omega] \hookrightarrow \mathrm{End}(E_1)$ be an orientation with $\iota(\omega) = \theta$. Let $\varphi : E_1 \to E_2$ an isogeny.

$$
\begin{tikzcd}
E_1 \arrow[loop left, "\theta"] \arrow[r, bend left, "\varphi"] & E_2 \arrow[l, bend left, "\hat{\varphi}"] \arrow[loop right, "\varphi_*(\theta) := \varphi \circ \theta \circ \hat{\varphi}"]
\end{tikzcd}
$$

Oriented isogenies

Let $\iota : \mathbb{Z}[\omega] \hookrightarrow \mathrm{End}(E_1)$ be an orientation with $\iota(\omega) = \theta$. Let $\varphi : E_1 \to E_2$ an isogeny.

$$\begin{tikzcd}
E_1 \arrow[loop left, "\theta"] \arrow[r, bend left, "\varphi"] & E_2 \arrow[l, bend left, "\hat{\varphi}"] \arrow[loop right]
\end{tikzcd}$$

$$\varphi_*(\theta) := \varphi \circ \theta \circ \hat{\varphi}$$

$$\hat{\varphi}_*(\varphi_*(\theta)) \stackrel{?}{=} \theta$$

Oriented isogenies

Let $\iota : \mathbb{Z}[\omega] \hookrightarrow \mathrm{End}(E_1)$ be an orientation with $\iota(\omega) = \theta$. Let $\varphi : E_1 \to E_2$ an isogeny.

$$\begin{tikzcd}
E_1 \arrow[loop left, "\theta"] \arrow[r, bend left, "\varphi"] & E_2 \arrow[l, bend left, "\hat{\varphi}"] \arrow[loop right]
\end{tikzcd}$$

$$\varphi_*(\theta) := \varphi \circ \theta \circ \hat{\varphi}$$

$$\hat{\varphi}_*(\varphi_*(\theta)) = (\deg \varphi)^2 \cdot \theta$$

Oriented isogenies

Let $\iota : \mathbb{Z}[\omega] \hookrightarrow \mathrm{End}(E_1)$ be an orientation with $\iota(\omega) = \theta$. Let $\varphi : E_1 \to E_2$ an isogeny.

$$\begin{tikzcd} E_1 \arrow[loop left, "\theta"] \arrow[r, bend left, "\varphi"] & E_2 \arrow[l, bend left, "\hat{\varphi}"] \arrow[loop right] \end{tikzcd}$$

$$\varphi_*(\theta) := \frac{\varphi \circ \theta \circ \hat{\varphi}}{\deg \varphi}$$

$$\hat{\varphi}_*(\varphi_*(\theta)) = \theta$$

Oriented isogenies

Let $\iota : \mathbb{Z}[\omega] \hookrightarrow \mathrm{End}(E_1)$ be an orientation with $\iota(\omega) = \theta$. Let $\varphi : E_1 \to E_2$ an isogeny.

$$\begin{tikzcd} E_1 \arrow[loop left, "\theta"] \arrow[rr, bend left, "\varphi"] & & E_2 \arrow[ll, bend left, "\hat{\varphi}"] \arrow[loop right, "\varphi_*(\theta)"] \end{tikzcd}$$

$$\varphi_*(\theta) := \frac{\varphi \circ \theta \circ \hat{\varphi}}{\deg \varphi}$$

$$\hat{\varphi}_*(\varphi_*(\theta)) = \theta$$

If $\iota(\mathbb{Z}[\omega]) = \iota(\mathbb{Q}(\omega)) \bigcap \mathrm{End}(E_1)$, then ι is a **primitive** $\mathbb{Z}[\omega]$-orientation.

Oriented isogenies

Let $\iota : \mathbb{Z}[\omega] \hookrightarrow \mathrm{End}(E_1)$ be an orientation with $\iota(\omega) = \theta$. Let $\varphi : E_1 \to E_2$ an isogeny.

$$\begin{tikzcd}
E_1 \arrow[loop left, "\theta"] \arrow[r, bend left, "\varphi"] & E_2 \arrow[l, bend left, "\hat{\varphi}"] \arrow[loop right]
\end{tikzcd}$$

$$\varphi_*(\theta) := \frac{\varphi \circ \theta \circ \hat{\varphi}}{\deg \varphi}$$

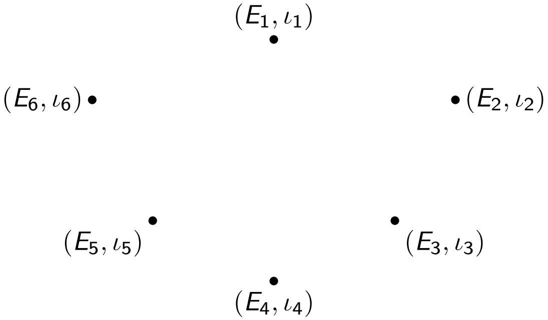
$$\hat{\varphi}_*(\varphi_*(\theta)) = \theta$$

If $\iota(\mathbb{Z}[\omega]) = \iota(\mathbb{Q}(\omega)) \bigcap \mathrm{End}(E_1)$, then ι is a **primitive** $\mathbb{Z}[\omega]$-orientation.

If $\varphi_*(\iota)$ is a primitive $\mathbb{Z}[\omega]$-orientation, then $\varphi : (E_1, \iota) \to (E_2, \varphi_*(\iota))$ is **horizontal**.

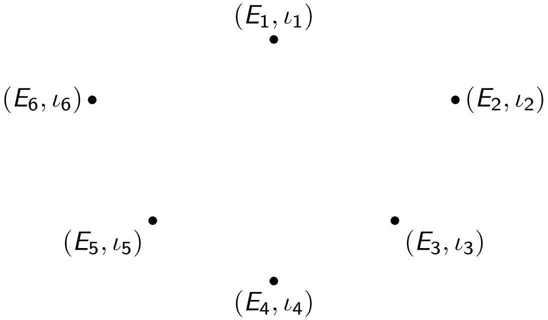
Class group action

Let $SS_{\mathfrak{O}}$ be the set of primitive $\mathfrak{O}$-oriented elliptic curves up to isomorphisms.



Class group action

Let $SS_{\mathfrak{O}}$ be the set of primitive $\mathfrak{O}$-oriented elliptic curves up to isomorphisms.

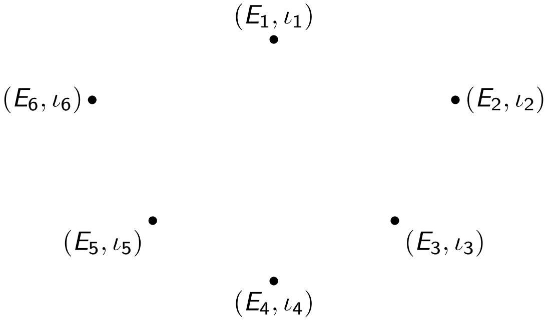


For all $(E, \iota) \in SS_{\mathfrak{O}}$ and invertible $\mathfrak{O}$-ideal $\mathfrak{a}$,

$$\forall \alpha \in \mathfrak{a},\ \iota(\alpha) \in \mathrm{End}(E).$$

Class group action

Let $SS_{\mathfrak{O}}$ be the set of primitive $\mathfrak{O}$-oriented elliptic curves up to isomorphisms.

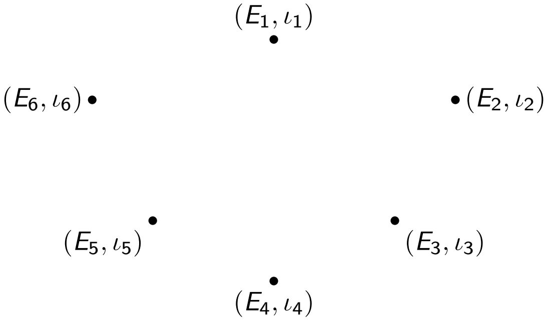


For all $(E, \iota) \in SS_{\mathfrak{O}}$ and invertible $\mathfrak{O}$-ideal $\mathfrak{a}$,

$$\forall \alpha \in \mathfrak{a}, \ \ker \iota(\alpha) < E.$$

Class group action

Let $SS_{\mathfrak{O}}$ be the set of primitive $\mathfrak{O}$-oriented elliptic curves up to isomorphisms.

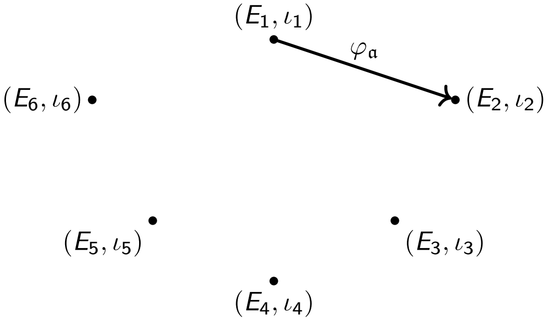


For all $(E, \iota) \in SS_{\mathfrak{O}}$ and invertible $\mathfrak{O}$-ideal $\mathfrak{a}$,

$$E[\mathfrak{a}] := \bigcap_{\alpha \in \mathfrak{a}} \ker(\iota(\alpha)) < E.$$

Class group action

Let $SS_{\mathfrak{O}}$ be the set of primitive $\mathfrak{O}$-oriented elliptic curves up to isomorphisms.



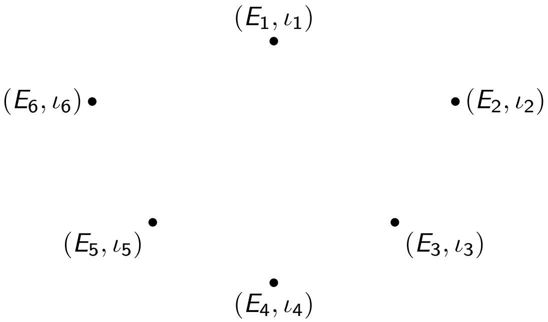
For all $(E, \iota) \in SS_{\mathfrak{O}}$ and invertible $\mathfrak{O}$-ideal $\mathfrak{a}$,

$$E[\mathfrak{a}] := \bigcap_{\alpha \in \mathfrak{a}} \ker(\iota(\alpha)) < E.$$

The isogeny $\varphi_{\mathfrak{a}}$ of kernel $E[\mathfrak{a}]$ is **horizontal**!

Class group action

Let $SS_{\mathfrak{O}}$ be the set of primitive $\mathfrak{O}$-oriented elliptic curves up to isomorphisms.



For all $(E, \iota) \in SS_{\mathfrak{O}}$ and invertible $\mathfrak{O}$-ideal $\mathfrak{a}$,

$$E[\mathfrak{a}] := \bigcap_{\alpha \in \mathfrak{a}} \ker(\iota(\alpha)) < E.$$

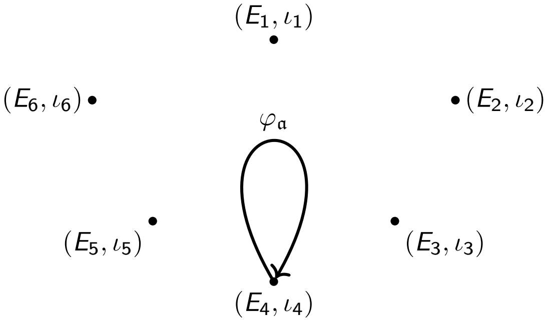
The isogeny $\varphi_{\mathfrak{a}}$ of kernel $E[\mathfrak{a}]$ is **horizontal**!

Proposition [Onu21]

The class group $\mathcal{C}l(\mathfrak{O})$ acts **freely** on $SS_{\mathfrak{O}}$ and has **at most two orbits**.

Class group action

Let $SS_{\mathfrak{O}}$ be the set of primitive $\mathfrak{O}$-oriented elliptic curves up to isomorphisms.



For all $(E, \iota) \in SS_{\mathfrak{O}}$ and invertible $\mathfrak{O}$-ideal $\mathfrak{a}$,

$$E[\mathfrak{a}] := \bigcap_{\alpha \in \mathfrak{a}} \ker(\iota(\alpha)) < E.$$

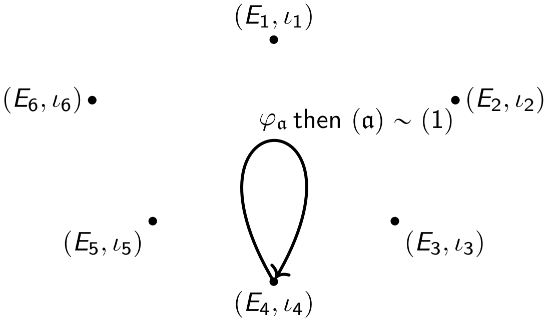
The isogeny $\varphi_{\mathfrak{a}}$ of kernel $E[\mathfrak{a}]$ is **horizontal**!

Proposition [Onu21]

The class group $\mathcal{C}l(\mathfrak{O})$ acts **freely** on $SS_{\mathfrak{O}}$ and has **at most two orbits**.

Class group action

Let $SS_{\mathfrak{O}}$ be the set of primitive $\mathfrak{O}$-oriented elliptic curves up to isomorphisms.



For all $(E, \iota) \in SS_{\mathfrak{O}}$ and invertible $\mathfrak{O}$-ideal $\mathfrak{a}$,

$$E[\mathfrak{a}] := \bigcap_{\alpha \in \mathfrak{a}} \ker(\iota(\alpha)) < E.$$

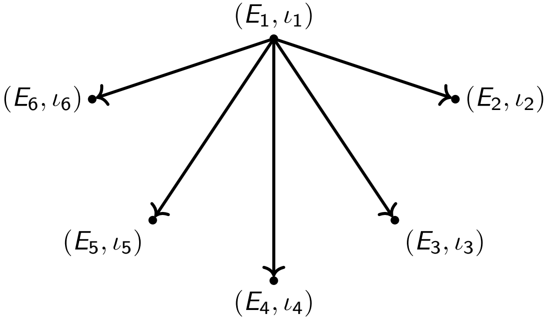
The isogeny $\varphi_{\mathfrak{a}}$ of kernel $E[\mathfrak{a}]$ is **horizontal**!

Proposition [Onu21]

The class group $\mathcal{C}\ell(\mathfrak{O})$ acts **freely** on $SS_{\mathfrak{O}}$ and has **at most two orbits**.

Class group action

Let $SS_{\mathfrak{O}}$ be the set of primitive $\mathfrak{O}$-oriented elliptic curves up to isomorphisms.



For all $(E, \iota) \in SS_{\mathfrak{O}}$ and invertible $\mathfrak{O}$-ideal $\mathfrak{a}$,

$$E[\mathfrak{a}] := \bigcap_{\alpha \in \mathfrak{a}} \ker(\iota(\alpha)) < E.$$

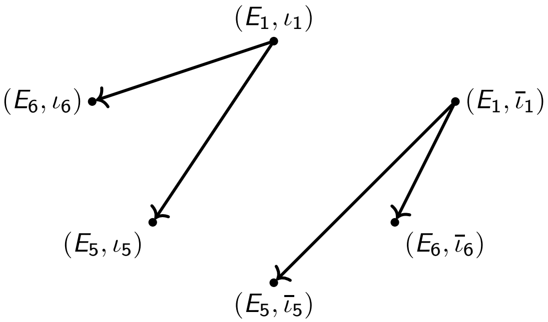
The isogeny $\varphi_{\mathfrak{a}}$ of kernel $E[\mathfrak{a}]$ is **horizontal**!

Proposition [Onu21]

The class group $\mathcal{C}l(\mathfrak{O})$ acts **freely** on $SS_{\mathfrak{O}}$ and has **at most two orbits**.

Class group action

Let $SS_{\mathfrak{O}}$ be the set of primitive $\mathfrak{O}$-oriented elliptic curves up to isomorphisms.



For all $(E, \iota) \in SS_{\mathfrak{O}}$ and invertible $\mathfrak{O}$-ideal $\mathfrak{a}$,

$$E[\mathfrak{a}] := \bigcap_{\alpha \in \mathfrak{a}} \ker(\iota(\alpha)) < E.$$

The isogeny $\varphi_{\mathfrak{a}}$ of kernel $E[\mathfrak{a}]$ is **horizontal**!

Proposition [Onu21]

The class group $\mathcal{C}\ell(\mathfrak{O})$ acts **freely** on $SS_{\mathfrak{O}}$ and has **<u>at most two orbits</u>**.

Some problems of orientations

$\underline{\mathfrak{O}\text{-}\texttt{Vectorisation:}}$

Some problems of orientations

$\mathfrak{O}$-`Vectorisation`:

(E_1, ι_1) $\bullet$

(E_2, ι_2) $\bullet$

Some problems of orientations

$\mathfrak{O}$-Vectorisation:

$$(E_1, \iota_1) \xrightarrow{\varphi_{\mathfrak{a}}} (E_2, \iota_2)$$

Some problems of orientations

$\mathfrak{O}$-Vectorisation:

$$(E_1, \iota_1) \xrightarrow{\varphi_{\mathfrak{a}}} (E_2, \iota_2)$$

Primitivisation:

Some problems of orientations

$\mathfrak{O}$-Vectorisation:

$$(E_1, \iota_1) \xrightarrow{\varphi_{\mathfrak{a}}} (E_2, \iota_2)$$

Primitivisation:

Knowing an endomorphism $\Longleftrightarrow$ Knowing an orientation

Some problems of orientations

$\mathfrak{O}$-Vectorisation:

$$(E_1, \iota_1) \xrightarrow{\varphi_{\mathfrak{a}}} (E_2, \iota_2)$$

Primitivisation:

$$\begin{tikzcd} \text{Knowing an endomorphism} \arrow[r, Leftrightarrow] & \text{Knowing an orientation} \\ & \text{Knowing a primitive orientation} \arrow[u, Rightarrow] \end{tikzcd}$$

Some problems of orientations

$\mathfrak{O}$-Vectorisation:

$$(E_1, \iota_1) \xrightarrow{\varphi_{\mathfrak{a}}} (E_2, \iota_2)$$

Primitivisation:

Knowing an endomorphism $\Longleftrightarrow$ Knowing an orientation

Knowing an endomorphism $\overset{?}{\Longrightarrow}$ Knowing a primitive orientation $\Longrightarrow$ Knowing an orientation

One more oriented problem

The $\mathfrak{O}$-oriented endomorphism ring problem ($\mathfrak{O}$-EndRing):

Given $(\boldsymbol{E}, \boldsymbol{\iota}) \in SS_{\mathfrak{O}}$, find a basis of its endomorphism ring $\mathbf{End}(\boldsymbol{E})$.

One more oriented problem

The $\mathfrak{O}$-oriented endomorphism ring problem ($\mathfrak{O}$-EndRing):

Given $(E, \iota) \in SS_{\mathfrak{O}}$, find a basis of its endomorphism ring $\mathbf{End}(E)$.

$\mathfrak{O}$-EndRing + factorisation of disc($\mathfrak{O}$)

[Wes22] $\Big\downarrow$ **GRH**

$\mathfrak{O}$-Vectorisation

One more oriented problem

The $\mathfrak{O}$-oriented endomorphism ring problem ($\mathfrak{O}$-EndRing):

Given $(\boldsymbol{E}, \iota) \in SS_{\mathfrak{O}}$, find a basis of its endomorphism ring $\mathbf{End}(\boldsymbol{E})$.

$\mathfrak{O}$-EndRing + factorisation of $\mathrm{disc}(\mathfrak{O})$

$\mathrm{disc}(\mathbb{Z}[\omega]) = (\bar{\omega} - \omega)^2$

[Wes22] **GRH**

$\mathfrak{O}$-Vectorisation

Proof outline

$$\begin{array}{c} \boxed{E \text{ and } \theta \in \mathrm{End}(E)\backslash\mathbb{Z}} \\ \downarrow \\ \boxed{\text{A basis of } \mathrm{End}(E)} \end{array}$$

➜ **Goal:** Give a complexity analysis of the `EndRing` problem given one endomorphism **under GRH only**.

Proof outline

$$
\begin{tikzcd}
\boxed{E \text{ and } \theta \in \mathrm{End}(E)\backslash\mathbb{Z}} \arrow[d, "1"'] \arrow[dd, bend right=60] \\
\boxed{E \text{ and } \iota : \mathbb{Z}[\theta] \hookrightarrow \mathrm{End}(E)} \\
\boxed{\text{A basis of } \mathrm{End}(E)}
\end{tikzcd}
$$

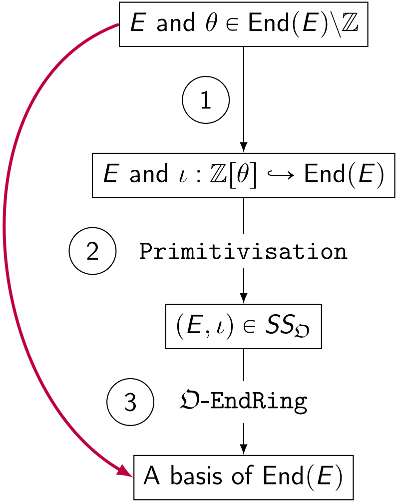
➜ **Goal:** Give a complexity analysis of the `EndRing` problem given one endomorphism **under GRH only**.

Proof outline

$$
\begin{tikzcd}
\boxed{E \text{ and } \theta \in \mathrm{End}(E)\backslash\mathbb{Z}} \arrow[d, "1"'] \arrow[ddd, bend right=60] \\
\boxed{E \text{ and } \iota : \mathbb{Z}[\theta] \hookrightarrow \mathrm{End}(E)} \arrow[d, "2\ \texttt{Primitivisation}"'] \\
\boxed{(E, \iota) \in SS_{\mathfrak{O}}} \\
\boxed{\text{A basis of } \mathrm{End}(E)}
\end{tikzcd}
$$

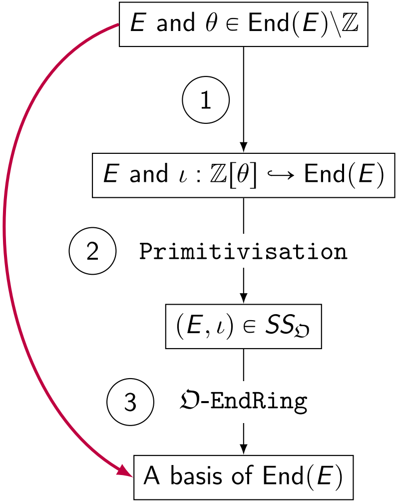
➜ **Goal:** Give a complexity analysis of the `EndRing` problem given one endomorphism **under GRH only**.

Proof outline



➜ **Goal:** Give a complexity analysis of the `EndRing` problem given one endomorphism **under GRH only**.

Proof outline



➜ **Goal:** Give a complexity analysis of the `EndRing` problem given one endomorphism **under GRH only**.

① Immediate.

Proof outline

$$\begin{tikzcd}
\boxed{E \text{ and } \theta \in \mathrm{End}(E)\backslash\mathbb{Z}} \arrow[d, "1"'] \arrow[ddd, bend right] \\
\boxed{E \text{ and } \iota : \mathbb{Z}[\theta] \hookrightarrow \mathrm{End}(E)} \arrow[d, "2 \quad \texttt{Primitivisation}"'] \\
\boxed{(E, \iota) \in SS_{\mathfrak{O}}} \arrow[d, "3 \quad \mathfrak{O}\text{-}\texttt{EndRing}"'] \\
\boxed{\text{A basis of } \mathrm{End}(E)}
\end{tikzcd}$$

➜ **Goal:** Give a complexity analysis of the `EndRing` problem given one endomorphism **under GRH only**.

① Immediate.

State of the art:

② Hard problem with a heuristic subexponential quantum complexity. [Arp+22]

Proof outline

$$\begin{tikzcd}
\boxed{E \text{ and } \theta \in \mathrm{End}(E)\backslash\mathbb{Z}} \arrow[d, "1"'] \arrow[ddd, bend right=60] \\
\boxed{E \text{ and } \iota : \mathbb{Z}[\theta] \hookrightarrow \mathrm{End}(E)} \arrow[d, "2\ \texttt{Primitivisation}"] \\
\boxed{(E, \iota) \in SS_{\mathfrak{O}}} \arrow[d, "3\ \mathfrak{O}\text{-}\texttt{EndRing}"] \\
\boxed{\text{A basis of } \mathrm{End}(E)}
\end{tikzcd}$$

➜ **Goal:** Give a complexity analysis of the `EndRing` problem given one endomorphism **under GRH only**.

① Immediate.

State of the art:

② Hard problem with a heuristic subexponential quantum complexity. [Arp+22]

③ Under some heuristics, classically in $|\mathrm{disc}(\mathfrak{O})|^{1/4}$ and quantumly in $\mathrm{subexp}(\log|\mathrm{disc}(\mathfrak{O})|)$. [Wes22]

Primitivisation problem [Arp+22]

`Primitivisation`:

Given $\boldsymbol{E}$ supersingular and $\boldsymbol{\theta} \in \mathrm{End}(E)$, find the **quadratic order** $\mathfrak{O} := \mathbb{Q}(\theta) \bigcap \mathrm{End}(E)$.

Primitivisation problem [Arp+22]

`Primitivisation`:

Given $\boldsymbol{E}$ supersingular and $\boldsymbol{\theta} \in \mathrm{End}(E)$, find the **quadratic order** $\mathfrak{O} := \mathbb{Q}(\theta) \bigcap \mathrm{End}(E)$.

Ordinary `EndRing`:

Given $\boldsymbol{E}$ ordinary and $\boldsymbol{\pi}$ the Frobenius, find the **quadratic order** $\mathrm{End}(E) \subseteq \mathbb{Q}(\pi)$.

Primitivisation problem [Arp+22]

`Primitivisation`:

Given $\boldsymbol{E}$ supersingular and $\boldsymbol{\theta} \in \mathrm{End}(E)$, find the **quadratic order** $\mathfrak{O} := \mathbb{Q}(\theta) \bigcap \mathrm{End}(E)$.

Ordinary `EndRing`:

Given $\boldsymbol{E}$ ordinary and $\boldsymbol{\pi}$ the Frobenius, find the **quadratic order** $\mathrm{End}(E) \subseteq \mathbb{Q}(\pi)$.

Solving Ordinary `EndRing`:

Primitivisation problem [Arp+22]

`Primitivisation`:

Given $\boldsymbol{E}$ supersingular and $\boldsymbol{\theta} \in \mathrm{End}(E)$, find the **quadratic order** $\mathfrak{O} := \mathbb{Q}(\theta) \bigcap \mathrm{End}(E)$.

Ordinary `EndRing`:

Given $\boldsymbol{E}$ ordinary and $\boldsymbol{\pi}$ the Frobenius, find the **quadratic order** $\mathrm{End}(E) \subseteq \mathbb{Q}(\pi)$.

Solving Ordinary `EndRing`:

- $\mathbb{Z}[\pi] \subseteq \mathrm{End}(E) \subseteq \mathcal{O}_{\mathbb{Q}(\pi)}$.

Primitivisation problem [Arp+22]

`Primitivisation`:

Given $\boldsymbol{E}$ supersingular and $\boldsymbol{\theta} \in \mathrm{End}(E)$, find the **quadratic order** $\mathfrak{O} := \mathbb{Q}(\theta) \bigcap \mathrm{End}(E)$.

Ordinary `EndRing`:

Given $\boldsymbol{E}$ ordinary and $\boldsymbol{\pi}$ the Frobenius, find the **quadratic order** $\mathrm{End}(E) \subseteq \mathbb{Q}(\pi)$.

Solving Ordinary `EndRing`:

- $\mathbb{Z}[\pi] \subseteq \mathrm{End}(E) \subseteq \mathcal{O}_{\mathbb{Q}(\pi)}$.
- Given the factorisation of $\mathrm{disc}(\mathbb{Z}[\pi])$, we can easily go through all $\mathcal{O} \supseteq \mathbb{Z}[\pi]$.

Primitivisation problem [Arp+22]

`Primitivisation`:

Given $\boldsymbol{E}$ supersingular and $\boldsymbol{\theta} \in \mathrm{End}(E)$, find the **quadratic order** $\mathfrak{O} := \mathbb{Q}(\theta) \bigcap \mathrm{End}(E)$.

Ordinary `EndRing`:

Given $\boldsymbol{E}$ ordinary and $\boldsymbol{\pi}$ the Frobenius, find the **quadratic order** $\mathrm{End}(E) \subseteq \mathbb{Q}(\pi)$.

Solving Ordinary `EndRing`:

- $\mathbb{Z}[\pi] \subseteq \mathrm{End}(E) \subseteq \mathcal{O}_{\mathbb{Q}(\pi)}$.
- Given the factorisation of $\mathrm{disc}(\mathbb{Z}[\pi])$, we can easily go through all $\mathcal{O} \supseteq \mathbb{Z}[\pi]$.
- It remains to check for each of them if $\mathcal{O} \subseteq \mathrm{End}(E)$. The maximal one will be $\mathrm{End}(E)$.

Primitivisation problem [Arp+22]

`Primitivisation`:

Given $\boldsymbol{E}$ supersingular and $\boldsymbol{\theta} \in \mathrm{End}(E)$, find the **quadratic order** $\mathfrak{O} := \mathbb{Q}(\theta) \bigcap \mathrm{End}(E)$.

Ordinary `EndRing`:

Given $\boldsymbol{E}$ ordinary and $\boldsymbol{\pi}$ the Frobenius, find the **quadratic order** $\mathrm{End}(E) \subseteq \mathbb{Q}(\pi)$.

Solving Ordinary `EndRing`:

- $\mathbb{Z}[\pi] \subseteq \mathrm{End}(E) \subseteq \mathcal{O}_{\mathbb{Q}(\pi)}$.
- Given the factorisation of $\mathrm{disc}(\mathbb{Z}[\pi])$, we can easily go through all $\mathcal{O} \supseteq \mathbb{Z}[\pi]$.
- It remains to check for each of them if $\mathcal{O} \subseteq \mathrm{End}(E)$. The maximal one will be $\mathrm{End}(E)$.

After SIDH's attacks, **checking an inclusion** is made by **dividing the Frobenius**. [Rob22b].

Division of endomorphism

(Higher dimensional) Interpolation [Rob22a]

Given coprime integers $\boldsymbol{N} < \boldsymbol{N'}$ and four points $\boldsymbol{P}_1, \boldsymbol{P}_2, \boldsymbol{Q}_1, \boldsymbol{Q}_2$ such that

$$\langle P_1, P_2 \rangle = E_1[N'] \text{ and } \langle Q_1, Q_2 \rangle = E_2[N'] \text{ with } N' \text{ a } B\text{-powersmooth integer.}$$

One can **check the existence** and **compute** in **poly** $(\boldsymbol{l}, \boldsymbol{B})$ time the isogeny of degree N

$$\varphi : E_1 \rightarrow E_2 \text{ such that } \varphi(P_1) = Q_1 \text{ and } \varphi(P_2) = Q_2.$$

Division of endomorphism

(Higher dimensional) Interpolation [Rob22a]

Given coprime integers $\boldsymbol{N} < \boldsymbol{N}'$ and four points $\boldsymbol{P}_1, \boldsymbol{P}_2, \boldsymbol{Q}_1, \boldsymbol{Q}_2$ such that

$$\langle P_1, P_2 \rangle = E_1[N'] \text{ and } \langle Q_1, Q_2 \rangle = E_2[N'] \text{ with } N' \text{ a } B\text{-powersmooth integer.}$$

One can **check the existence** and **compute** in **poly** $(\boldsymbol{l}, \boldsymbol{B})$ time the isogeny of degree N

$$\varphi : E_1 \to E_2 \text{ such that } \varphi(P_1) = Q_1 \text{ and } \varphi(P_2) = Q_2.$$

Division of endomorphism [Rob22b; HW23]

Given an endomorphism $\boldsymbol{\theta} \in \mathrm{End}(E)$ and an integer $\boldsymbol{n}$ such that $gcd(\deg \theta, np) = 1$, one can **check if** $\boldsymbol{\theta}/\boldsymbol{n} \in$ **End** $(\boldsymbol{E})$ and **compute it** in **poly** $(\boldsymbol{l})$ time.

Division of endomorphism

(Higher dimensional) Interpolation [Rob22a]

Given coprime integers $\boldsymbol{N} < \boldsymbol{N'}$ and four points $\boldsymbol{P_1}, \boldsymbol{P_2}, \boldsymbol{Q_1}, \boldsymbol{Q_2}$ such that

$$\langle P_1, P_2 \rangle = E_1[N'] \text{ and } \langle Q_1, Q_2 \rangle = E_2[N'] \text{ with } N' \text{ a } B\text{-powersmooth integer.}$$

One can **check the existence** and **compute** in **poly** $(\boldsymbol{l}, \boldsymbol{B})$ time the isogeny of degree N

$$\varphi : E_1 \to E_2 \text{ such that } \varphi(P_1) = Q_1 \text{ and } \varphi(P_2) = Q_2.$$

Division of endomorphism [Rob22b; HW23]

Given an endomorphism $\boldsymbol{\theta} \in \mathrm{End}(E)$ and an integer $\boldsymbol{n}$ such that $gcd(\deg \theta, np) = 1$, one can **check if** $\boldsymbol{\theta}/\boldsymbol{n} \in$ **End** $(\boldsymbol{E})$ and **compute it** in **poly** $(\boldsymbol{l})$ time.

sketch of proof:

1. Compute a basis $\langle P_1, P_2 \rangle$ of $E[N']$ with N' $(\log \deg \theta)$-powersmooth.

Division of endomorphism

(Higher dimensional) Interpolation [Rob22a]

Given coprime integers $\boldsymbol{N} < \boldsymbol{N'}$ and four points $\boldsymbol{P_1}, \boldsymbol{P_2}, \boldsymbol{Q_1}, \boldsymbol{Q_2}$ such that

$$\langle P_1, P_2 \rangle = E_1[N'] \text{ and } \langle Q_1, Q_2 \rangle = E_2[N'] \text{ with } N' \text{ a } B\text{-powersmooth integer.}$$

One can **check the existence** and **compute** in **poly** $(\boldsymbol{l}, \boldsymbol{B})$ time the isogeny of degree N

$$\varphi : E_1 \to E_2 \text{ such that } \varphi(P_1) = Q_1 \text{ and } \varphi(P_2) = Q_2.$$

Division of endomorphism [Rob22b; HW23]

Given an endomorphism $\boldsymbol{\theta} \in \mathrm{End}(E)$ and an integer $\boldsymbol{n}$ such that $gcd(\deg \theta, np) = 1$, one can **check if** $\boldsymbol{\theta/n} \in$ **End** $(\boldsymbol{E})$ and **compute it** in **poly** $(\boldsymbol{l})$ time.

sketch of proof:

1. Compute a basis $\langle P_1, P_2 \rangle$ of $E[N']$ with N' $(\log \deg \theta)$-powersmooth.
2. Compute $1/n \mod N'$

Division of endomorphism

(Higher dimensional) Interpolation [Rob22a]

Given coprime integers $\boldsymbol{N} < \boldsymbol{N'}$ and four points $\boldsymbol{P_1, P_2, Q_1, Q_2}$ such that

$$\langle P_1, P_2 \rangle = E_1[N'] \text{ and } \langle Q_1, Q_2 \rangle = E_2[N'] \text{ with } N' \text{ a } B\text{-powersmooth integer.}$$

One can **check the existence** and **compute** in **poly** $(\boldsymbol{l}, \boldsymbol{B})$ time the isogeny of degree N

$$\varphi : E_1 \to E_2 \text{ such that } \varphi(P_1) = Q_1 \text{ and } \varphi(P_2) = Q_2.$$

Division of endomorphism [Rob22b; HW23]

Given an endomorphism $\boldsymbol{\theta} \in \mathrm{End}(E)$ and an integer $\boldsymbol{n}$ such that $gcd(\deg \theta, np) = 1$, one can **check if** $\boldsymbol{\theta/n} \in \textbf{End}\,(\boldsymbol{E})$ and **compute it** in **poly** $(\boldsymbol{l})$ time.

sketch of proof:

1. Compute a basis $\langle P_1, P_2 \rangle$ of $E[N']$ with N' $(\log \deg \theta)$-powersmooth.
2. Compute $1/n \mod N' \longrightarrow Q_1 = \theta(P_1)/n$ and $Q_2 = \theta(P_2)/n$.

Division of endomorphism

(Higher dimensional) Interpolation [Rob22a]

Given coprime integers $\boldsymbol{N} < \boldsymbol{N'}$ and four points $\boldsymbol{P_1, P_2, Q_1, Q_2}$ such that

$$\langle P_1, P_2 \rangle = E_1[N'] \text{ and } \langle Q_1, Q_2 \rangle = E_2[N'] \text{ with } N' \text{ a } B\text{-powersmooth integer.}$$

One can **check the existence** and **compute** in **poly** $(\boldsymbol{l}, \boldsymbol{B})$ time the isogeny of degree N

$$\varphi : E_1 \to E_2 \text{ such that } \varphi(P_1) = Q_1 \text{ and } \varphi(P_2) = Q_2.$$

Division of endomorphism [Rob22b; HW23]

Given an endomorphism $\boldsymbol{\theta} \in \mathrm{End}(E)$ and an integer $\boldsymbol{n}$ such that $gcd(\deg \theta, np) = 1$, one can **check if** $\boldsymbol{\theta/n} \in$ **End** $(\boldsymbol{E})$ and **compute it** in **poly** $(\boldsymbol{l})$ time.

sketch of proof:

1. Compute a basis $\langle P_1, P_2 \rangle$ of $E[N']$ with N' $(\log \deg \theta)$-powersmooth.
2. Compute $1/n \mod N' \longrightarrow Q_1 = \theta(P_1)/n$ and $Q_2 = \theta(P_2)/n$.
3. Use the higher dimensional interpolation.

Applications to the Primitivisation problem

Proposition: `Primitivisation`

Given a $\mathbb{Z}[\omega]$-oriented elliptic curve (E, ι) and **the factorisation of disc** $(\mathbb{Z}[\omega])$, one can compute the **primitive orientation** $\iota' : \mathfrak{O} \hookrightarrow \mathrm{End}(E)$ such that $\mathfrak{O} \supseteq \mathbb{Z}[\omega]$ in **poly** (I).

Applications to the Primitivisation problem

Proposition: `Primitivisation`

Given a $\mathbb{Z}[\omega]$-oriented elliptic curve (E, ι) and **the factorisation of disc** $(\mathbb{Z}[\omega])$, one can compute the **primitive orientation** $\iota' : \mathfrak{O} \hookrightarrow \mathbf{End}(E)$ such that $\mathfrak{O} \supseteq \mathbb{Z}[\omega]$ in **poly** (I).

The factorisation of $\mathrm{disc}(\mathbb{Z}[\omega])$ gives the factorisation of its conductor f and $\Delta := \mathrm{disc}(\mathbb{Q}(\omega))$.

Applications to the Primitivisation problem

Proposition: `Primitivisation`

Given a $\mathbb{Z}[\omega]$-oriented elliptic curve $(\boldsymbol{E}, \boldsymbol{\iota})$ and **the factorisation of disc** $(\mathbb{Z}[\boldsymbol{\omega}])$, one can compute the **primitive orientation** $\iota' : \mathfrak{O} \hookrightarrow$ **End** $(\boldsymbol{E})$ such that $\mathfrak{O} \supseteq \mathbb{Z}[\omega]$ in **poly** $(\boldsymbol{l})$.

The factorisation of $\mathrm{disc}(\mathbb{Z}[\omega])$ gives the factorisation of its conductor f and $\Delta := \mathrm{disc}(\mathbb{Q}(\omega))$.

$$\mathbb{Z}[f\sqrt{\Delta}] \text{ `}{=}\text{' } \mathbb{Z}[\omega] \implies \iota : \mathbb{Z}[f\sqrt{\Delta}] \hookrightarrow \mathrm{End}(E)$$

Applications to the Primitivisation problem

Proposition: Primitivisation

Given a $\mathbb{Z}[\omega]$-oriented elliptic curve $(\boldsymbol{E}, \boldsymbol{\iota})$ and **the factorisation of disc** $(\mathbb{Z}[\boldsymbol{\omega}])$, one can compute the **primitive orientation** $\boldsymbol{\iota' : \mathfrak{O} \hookrightarrow}$ **End** $(\boldsymbol{E})$ such that $\mathfrak{O} \supseteq \mathbb{Z}[\omega]$ in **poly** $(\boldsymbol{l})$.

The factorisation of $\mathrm{disc}(\mathbb{Z}[\omega])$ gives the factorisation of its conductor f and $\Delta := \mathrm{disc}(\mathbb{Q}(\omega))$.

$$\mathbb{Z}[f\sqrt{\Delta}] \text{ `='} \ \mathbb{Z}[\omega] \implies \iota : \mathbb{Z}[f\sqrt{\Delta}] \hookrightarrow \mathrm{End}(E)$$

There exists some integer m dividing f such that $\mathfrak{O}$ '=' $\mathbb{Z}[\frac{f}{m}\sqrt{\Delta}]$.

Applications to the Primitivisation problem

Proposition: `Primitivisation`

Given a $\mathbb{Z}[\omega]$-oriented elliptic curve $(\boldsymbol{E}, \boldsymbol{\iota})$ and **the factorisation of disc** $(\mathbb{Z}[\boldsymbol{\omega}])$, one can compute the **primitive orientation** $\iota' : \mathfrak{O} \hookrightarrow$ **End** $(\boldsymbol{E})$ such that $\mathfrak{O} \supseteq \mathbb{Z}[\omega]$ in **poly** $(\boldsymbol{I})$.

The factorisation of $\mathrm{disc}(\mathbb{Z}[\omega])$ gives the factorisation of its conductor f and $\Delta := \mathrm{disc}(\mathbb{Q}(\omega))$.

$$\mathbb{Z}[f\sqrt{\Delta}] \text{ `='} \ \mathbb{Z}[\omega] \implies \iota : \mathbb{Z}[f\sqrt{\Delta}] \hookrightarrow \mathrm{End}(E)$$

There exists some integer m dividing f such that $\mathfrak{O}$ '=' $\mathbb{Z}[\frac{f}{m}\sqrt{\Delta}]$.
This integer m is the largest divisor of f such that $\iota(f\sqrt{\Delta})/m \in \mathrm{End}(E)$.

Applications to the Primitivisation problem

Proposition: `Primitivisation`

Given a $\mathbb{Z}[\omega]$-oriented elliptic curve $(\boldsymbol{E}, \boldsymbol{\iota})$ and **the factorisation of disc** $(\mathbb{Z}[\boldsymbol{\omega}])$, one can compute the **primitive orientation** $\boldsymbol{\iota' : \mathfrak{O} \hookrightarrow}$ **End** $(\boldsymbol{E})$ such that $\mathfrak{O} \supseteq \mathbb{Z}[\omega]$ in **poly** $(\boldsymbol{l})$.

The factorisation of $\mathrm{disc}(\mathbb{Z}[\omega])$ gives the factorisation of its conductor f and $\Delta := \mathrm{disc}(\mathbb{Q}(\omega))$.

$$\mathbb{Z}[f\sqrt{\Delta}] \text{ `='} \ \mathbb{Z}[\omega] \implies \iota : \mathbb{Z}[f\sqrt{\Delta}] \hookrightarrow \mathrm{End}(E)$$

There exists some integer m dividing f such that $\mathfrak{O}$ '=' $\mathbb{Z}[\frac{f}{m}\sqrt{\Delta}]$.
This integer m is the largest divisor of f such that $\iota(f\sqrt{\Delta})/m \in \mathrm{End}(E)$.

Thus successive divisions of $\iota(f\sqrt{\Delta})$ by the prime factors of f gives $\iota' : \mathfrak{O} \hookrightarrow \mathrm{End}(E)$.

Applications to the class group action

Before SIDH's attacks, one could compute actions of powersmooth ideals in polynomial time and, **under heuristics**, actions of any ideals in subexponential time.

Applications to the class group action

Before SIDH's attacks, one could compute actions of powersmooth ideals in polynomial time and, **under heuristics**, actions of any ideals in subexponential time.

Action of a prime ideal $\mathfrak{p}$ on (E, ι) in polynomial time

① Compute $E[\mathfrak{p}]$ and $\varphi_{\mathfrak{p}}$ with standard methods.

② Compute $(\varphi_{\mathfrak{p}})_*(\iota)$ using **the new division algorithm.**

Applications to the class group action

Before SIDH's attacks, one could compute actions of powersmooth ideals in polynomial time and, **under heuristics**, actions of any ideals in subexponential time.

Action of a prime ideal $\mathfrak{p}$ on (E, ι) in polynomial time

① Compute $E[\mathfrak{p}]$ and $\varphi_{\mathfrak{p}}$ with standard methods.

② Compute $(\varphi_{\mathfrak{p}})_*(\iota)$ using **the new division algorithm.**

Action of a smooth ideal $\mathfrak{a}$ on (E, ι) in polynomial time

① Decompose the ideal in product of prime ideals.

② Compute the action of each of them using **the new action of prime ideal algorithm.**

Applications to the class group action

Before SIDH's attacks, one could compute actions of powersmooth ideals in polynomial time and, **under heuristics**, actions of any ideals in subexponential time.

Action of a prime ideal $\mathfrak{p}$ on (E, ι) in polynomial time

① Compute $E[\mathfrak{p}]$ and $\varphi_{\mathfrak{p}}$ with standard methods.

② Compute $(\varphi_{\mathfrak{p}})_*(\iota)$ using **the new division algorithm.**

Action of a smooth ideal $\mathfrak{a}$ on (E, ι) in polynomial time

① Decompose the ideal in product of prime ideals.

② Compute the action of each of them using **the new action of prime ideal algorithm.**

Under GRH Action of an ideal $\mathfrak{a}$ on (E, ι) in subexponential time

① Compute a smooth ideal in the class of $\mathfrak{a}$ in subexponential time under GRH, [CJS14].

② Compute the action of this ideal using **the new action of smooth ideal algorithm.**

Applications to the class group action

Before SIDH's attacks, one could compute actions of powersmooth ideals in polynomial time and, **under heuristics**, actions of any ideals in subexponential time.

Action of a prime ideal $\mathfrak{p}$ on (E, ι) in polynomial time

① Compute $E[\mathfrak{p}]$ and $\varphi_\mathfrak{p}$ with standard methods.

② Compute $(\varphi_\mathfrak{p})_*(\iota)$ using **the new division algorithm.**

Action of a smooth ideal $\mathfrak{a}$ on (E, ι) in polynomial time

① Decompose the ideal in product of prime ideals.

② Compute the action of each of them using **the new action of prime ideal algorithm.**

Under GRH Action of an ideal $\mathfrak{a}$ on (E, ι) in subexponential time

① Compute a smooth ideal in the class of $\mathfrak{a}$ in subexponential time under GRH, [CJS14].

② Compute the action of this ideal using **the new action of smooth ideal algorithm.**

Remark [PR23], `CLAPOTI`: CLass group Action in POlynomial TIme!

Proof outline (updated)

$$
\begin{tikzcd}
\boxed{E \text{ and } \theta \in \mathrm{End}(E)\backslash\mathbb{Z}} \arrow[d, "1"'] \arrow[ddd, bend right] \\
\boxed{E \text{ and } \iota : \mathbb{Z}[\theta] \hookrightarrow \mathrm{End}(E)} \arrow[d, "2\ \texttt{Primitivisation}"] \\
\boxed{(E, \iota) \in SS_{\mathfrak{O}}} \arrow[d, "3\ \mathfrak{O}\text{-}\texttt{EndRing}"] \\
\boxed{\text{A basis of } \mathrm{End}(E)}
\end{tikzcd}
$$

➜ **Goal:** Give a complexity analysis of the `EndRing` problem given one endomorphism **under GRH only**.

① Immediate.

② ~~Hard problem with a subexponential quantum complexity~~.
Polynomial time given the factorisation of the discriminant of $\mathbb{Z}[\theta]$.

③ Under some heuristics, classically in $|\operatorname{disc}(\mathfrak{O})^{1/4}|$ and quantumly in $\operatorname{subexp}(\log|\operatorname{disc}(\mathfrak{O})|)$. [Wes22]

Solving $\mathfrak{O}$-Vect classically

Proposition: Classical $\mathfrak{O}$-`Vectorisation` **(GRH)**

Given $(\boldsymbol{E}_1, \boldsymbol{\iota}_1)$ and $(\boldsymbol{E}_2, \boldsymbol{\iota}_2)$ in $SS_{\mathfrak{O}}$, one can find an $\mathfrak{O}$-ideal $\mathfrak{a}$ such that $\varphi_{\mathfrak{a}} : (E_1, \iota_1) \to (E_2, \iota_2)$ in $\mathbf{poly}\,(\boldsymbol{l}) \cdot |\,\mathbf{disc}\,(\mathfrak{O})|^{1/4}$.

Solving $\mathfrak{O}$-Vect classically

Proposition: Classical $\mathfrak{O}$-Vectorisation **(GRH)**

Given $(\boldsymbol{E}_1, \boldsymbol{\iota}_1)$ and $(\boldsymbol{E}_2, \boldsymbol{\iota}_2)$ in $SS_{\mathfrak{O}}$, one can find an $\mathfrak{O}$-ideal $\mathfrak{a}$ such that $\varphi_{\mathfrak{a}} : (E_1, \iota_1) \to (E_2, \iota_2)$ in $\mathbf{poly}\left(\boldsymbol{l}\right) \cdot \left|\mathbf{disc}\left(\mathfrak{O}\right)\right|^{1/4}$.

Before SIDH's attacks, **under heuristics**, best algorithms were in $|\mathrm{disc}(\mathfrak{O})|^{1/4}$ using meet-in-the-middle approach.

Solving $\mathfrak{O}$-Vect classically

Proposition: Classical $\mathfrak{O}$-Vectorisation **(GRH)**

Given $(\boldsymbol{E}_1, \boldsymbol{\iota}_1)$ and $(\boldsymbol{E}_2, \boldsymbol{\iota}_2)$ in $SS_{\mathfrak{O}}$, one can find an $\mathfrak{O}$-ideal $\mathfrak{a}$ such that $\varphi_{\mathfrak{a}} : (E_1, \iota_1) \to (E_2, \iota_2)$ in $\textbf{poly}\,(\boldsymbol{l}) \cdot |\,\textbf{disc}\,(\mathfrak{O})|^{1/4}$.

Before SIDH's attacks, **under heuristics**, best algorithms were in $|\,\mathrm{disc}(\mathfrak{O})|^{1/4}$ using meet-in-the-middle approach.

[CJS14] Under GRH, the Cayley graph $(\mathcal{C}l(\mathfrak{O}), \{\text{small prime } \mathfrak{O}\text{-ideal}\})$ has good mixing properties $\implies$ MITM works.

Solving $\mathfrak{O}$-Vect classically

Proposition: Classical $\mathfrak{O}$-Vectorisation **(GRH)**

Given $(\boldsymbol{E}_1, \boldsymbol{\iota}_1)$ and $(\boldsymbol{E}_2, \boldsymbol{\iota}_2)$ in $SS_{\mathfrak{O}}$, one can find an $\mathfrak{O}$-ideal $\mathfrak{a}$ such that $\varphi_{\mathfrak{a}} : (E_1, \iota_1) \to (E_2, \iota_2)$ in **poly** $(\boldsymbol{l}) \cdot |\,\textbf{disc}\,(\mathfrak{O})|^{1/4}$.

Before SIDH's attacks, **under heuristics**, best algorithms were in $|\,\mathrm{disc}(\mathfrak{O})|^{1/4}$ using meet-in-the-middle approach.

[CJS14] Under GRH, the Cayley graph $(\mathcal{C}\mathrm{l}(\mathfrak{O}), \{\text{small prime } \mathfrak{O}\text{-ideal}\})$ has good mixing properties $\Longrightarrow$ MITM works.

- $|\mathcal{C}\mathrm{l}(\mathfrak{O})| = \tilde{O}(|\,\mathrm{disc}(\mathfrak{O})|^{1/2})$.

Solving $\mathfrak{O}$-Vect classically

Proposition: Classical $\mathfrak{O}$-Vectorisation **(GRH)**

Given $(\boldsymbol{E_1}, \boldsymbol{\iota_1})$ and $(\boldsymbol{E_2}, \boldsymbol{\iota_2})$ in $SS_{\mathfrak{O}}$, one can find an $\mathfrak{O}$-ideal $\mathfrak{a}$ such that $\varphi_{\mathfrak{a}} : (E_1, \iota_1) \to (E_2, \iota_2)$ in $\mathbf{poly}\,(\boldsymbol{l}) \cdot |\,\mathbf{disc}\,(\mathfrak{O})|^{1/4}$.

Before SIDH's attacks, **under heuristics**, best algorithms were in $|\,\mathrm{disc}(\mathfrak{O})|^{1/4}$ using meet-in-the-middle approach.

[CJS14] Under GRH, the Cayley graph $(\mathcal{C}\mathrm{l}(\mathfrak{O}), \{\text{small prime } \mathfrak{O}\text{-ideal}\})$ has good mixing properties $\implies$ MITM works.

- $|\,\mathcal{C}\mathrm{l}(\mathfrak{O})| = \tilde{O}(|\,\mathrm{disc}(\mathfrak{O})|^{1/2})$.
- Heuristics come from the powersmoothness constraint on the ideals' norms.

Solving $\mathfrak{O}$-Vect quantumly

Proposition: Quantum $\mathfrak{O}$-Vectorisation **(GRH)**

Given $(\boldsymbol{E}_1, \boldsymbol{\iota}_1)$ and $(\boldsymbol{E}_2, \boldsymbol{\iota}_2)$ in $SS_{\mathfrak{O}}$, one can find an $\mathfrak{O}$-ideal $\mathfrak{a}$ such that $\varphi_{\mathfrak{a}} : (E_1, \iota_1) \to (E_2, \iota_2)$ in $\mathbf{poly}(\boldsymbol{l}) \cdot \mathbf{subexp}(\mathbf{log}\,|\,\mathbf{disc}(\boldsymbol{\mathfrak{O}})|)$ using a quantum algorithm.

Solving $\mathfrak{O}$-Vect quantumly

Proposition: Quantum $\mathfrak{O}$-Vectorisation **(GRH)**

Given $(\boldsymbol{E}_1, \boldsymbol{\iota}_1)$ and $(\boldsymbol{E}_2, \boldsymbol{\iota}_2)$ in $SS_{\mathfrak{O}}$, one can find an $\mathfrak{O}$-ideal $\mathfrak{a}$ such that $\varphi_{\mathfrak{a}} : (E_1, \iota_1) \to (E_2, \iota_2)$ in $\mathbf{poly}\,(\boldsymbol{l}) \cdot \mathbf{subexp}\,(\,\mathbf{log}\,|\,\mathbf{disc}\,(\boldsymbol{\mathfrak{O}})|)$ using a quantum algorithm.

Before SIDH's attacks, **under heuristics**, best quantum algorithms were in $\mathrm{subexp}(\log|\mathrm{disc}(\mathfrak{O})|)$, see for instance [CJS14].

Solving $\mathfrak{O}$-Vect quantumly

Proposition: Quantum $\mathfrak{O}$-Vectorisation **(GRH)**

Given $(\boldsymbol{E}_1, \boldsymbol{\iota}_1)$ and $(\boldsymbol{E}_2, \boldsymbol{\iota}_2)$ in $SS_{\mathfrak{O}}$, one can find an $\mathfrak{O}$-ideal $\mathfrak{a}$ such that $\varphi_{\mathfrak{a}} : (E_1, \iota_1) \to (E_2, \iota_2)$ in $\mathbf{poly}(\boldsymbol{l}) \cdot \mathbf{subexp}(\mathbf{log} \,|\, \mathbf{disc}(\boldsymbol{\mathfrak{O}})|)$ using a quantum algorithm.

Before SIDH's attacks, **under heuristics**, best quantum algorithms were in $\mathrm{subexp}(\log|\mathrm{disc}(\mathfrak{O})|)$, see for instance [CJS14].

[Kup05] They use Kuperberg's algorithm $\implies$ computation of a subexponential number of actions.

Solving $\mathfrak{O}$-Vect quantumly

Proposition: Quantum $\mathfrak{O}$-Vectorisation **(GRH)**

Given $(\boldsymbol{E_1}, \boldsymbol{\iota_1})$ and $(\boldsymbol{E_2}, \boldsymbol{\iota_2})$ in $SS_{\mathfrak{O}}$, one can find an $\mathfrak{O}$-ideal $\mathfrak{a}$ such that $\varphi_{\mathfrak{a}} : (E_1, \iota_1) \to (E_2, \iota_2)$ in $\mathbf{poly}(\boldsymbol{l}) \cdot \mathbf{subexp}(\mathbf{log}\,|\,\mathbf{disc}(\mathfrak{O})|)$ using a quantum algorithm.

Before SIDH's attacks, **under heuristics**, best quantum algorithms were in $\mathrm{subexp}(\log|\,\mathrm{disc}(\mathfrak{O})|)$, see for instance [CJS14].

[Kup05] They use Kuperberg's algorithm $\Longrightarrow$ computation of a subexponential number of actions.

- Heuristics come from powersmoothing steps before computing those actions.

Proof outline (re-updated)

$$
\begin{tikzcd}
\boxed{E \text{ and } \theta \in \mathrm{End}(E)\backslash\mathbb{Z}} \arrow[d, "1"] \arrow[dd, bend right=60] \\
\boxed{E \text{ and } \iota : \mathbb{Z}[\theta] \hookrightarrow \mathrm{End}(E)} \arrow[d, "2\ \texttt{Primitivisation}"] \\
\boxed{(E, \iota) \in SS_{\mathfrak{O}}} \arrow[d, "3\ \mathfrak{O}\text{-}\texttt{EndRing}"] \\
\boxed{\text{A basis of } \mathrm{End}(E)}
\end{tikzcd}
$$

→ **Goal:** Give a complexity analysis of the `EndRing` problem given one endomorphism **under GRH only**.

① Immediate.

② ~~Hard problem with a subexponential quantum complexity~~.

Polynomial time given the factorisation of the discriminant of $\mathbb{Z}[\theta]$.

③ ~~Under some heuristics~~ Under GRH only, classically in $|\mathrm{disc}(\mathfrak{O})^{1/4}|$ and quantumly in $\mathrm{subexp}(\log|\mathrm{disc}(\mathfrak{O})|)$.

EndRing given one endomorphism

Theorem: Classical EndRing problem given one endomorphism **(GRH)**

Given an elliptic curve $\boldsymbol{E}$ and an endomorphism $\boldsymbol{\theta} \in \mathrm{End}(E)\backslash\mathbb{Z}$, one can compute a basis of the endomorphism ring $\mathbf{End}(\boldsymbol{E})$ in time $\mathbf{poly}(\boldsymbol{l}) \cdot |\mathbf{disc}(\mathbb{Z}[\boldsymbol{\theta}])|^{1/4}$.

Theorem: Quantum EndRing problem given one endomorphism **(GRH)**

Given an elliptic curve $\boldsymbol{E}$ and an endomorphism $\boldsymbol{\theta} \in \mathrm{End}(E)\backslash\mathbb{Z}$, one can quantumly compute a basis of the endomorphism ring $\mathbf{End}(\boldsymbol{E})$ in time $\mathbf{poly}(\boldsymbol{l}) \cdot \mathbf{subexp}(\mathbf{log}|\mathbf{disc}(\mathbb{Z}[\boldsymbol{\theta}])|)$.

EndRing given one endomorphism

Theorem: Classical EndRing problem given one endomorphism **(GRH)**

Given an elliptic curve $\boldsymbol{E}$ and an endomorphism $\boldsymbol{\theta} \in \mathrm{End}(E)\backslash\mathbb{Z}$, one can compute a basis of the endomorphism ring $\mathbf{End}(\boldsymbol{E})$ in time $\mathbf{poly}(\boldsymbol{l}) \cdot |\mathbf{disc}(\mathbb{Z}[\boldsymbol{\theta}])|^{1/4}$.

Theorem: Quantum EndRing problem given one endomorphism **(GRH)**

Given an elliptic curve $\boldsymbol{E}$ and an endomorphism $\boldsymbol{\theta} \in \mathrm{End}(E)\backslash\mathbb{Z}$, one can quantumly compute a basis of the endomorphism ring $\mathbf{End}(\boldsymbol{E})$ in time $\mathbf{poly}(\boldsymbol{l}) \cdot \mathbf{subexp}(\mathbf{log}\,|\mathbf{disc}(\mathbb{Z}[\boldsymbol{\theta}])|)$.

Remark: CSIDH and SCALLOP are safe! (At least in the face of this threat)

EndRing given one endomorphism

Theorem: Classical EndRing problem given one endomorphism **(GRH)**

Given an elliptic curve $\boldsymbol{E}$ and an endomorphism $\boldsymbol{\theta} \in \mathrm{End}(E)\backslash\mathbb{Z}$, one can compute a basis of the endomorphism ring $\mathbf{End}(\boldsymbol{E})$ in time $\mathbf{poly}(\boldsymbol{l}) \cdot |\mathbf{disc}(\mathbb{Z}[\boldsymbol{\theta}])|^{1/4}$.

Theorem: Quantum EndRing problem given one endomorphism **(GRH)**

Given an elliptic curve $\boldsymbol{E}$ and an endomorphism $\boldsymbol{\theta} \in \mathrm{End}(E)\backslash\mathbb{Z}$, one can quantumly compute a basis of the endomorphism ring $\mathbf{End}(\boldsymbol{E})$ in time $\mathbf{poly}(\boldsymbol{l}) \cdot \mathbf{subexp}(\mathbf{log}\,|\mathbf{disc}(\mathbb{Z}[\boldsymbol{\theta}])|)$.

Remark: CSIDH and SCALLOP are safe! (At least in the face of this threat)

What's next ?

- Keep digging in the implications of higher dimensional isogenies over security analysis.
- Improve the constructive applications.

EndRing given one endomorphism

Theorem: Classical EndRing problem given one endomorphism **(GRH)**

Given an elliptic curve $\boldsymbol{E}$ and an endomorphism $\boldsymbol{\theta} \in \mathrm{End}(E)\backslash\mathbb{Z}$, one can compute a basis of the endomorphism ring $\mathbf{End}(\boldsymbol{E})$ in time $\mathbf{poly}(\boldsymbol{l}) \cdot |\mathbf{disc}(\mathbb{Z}[\boldsymbol{\theta}])|^{1/4}$.

Theorem: Quantum EndRing problem given one endomorphism **(GRH)**

Given an elliptic curve $\boldsymbol{E}$ and an endomorphism $\boldsymbol{\theta} \in \mathrm{End}(E)\backslash\mathbb{Z}$, one can quantumly compute a basis of the endomorphism ring $\mathbf{End}(\boldsymbol{E})$ in time $\mathbf{poly}(\boldsymbol{l}) \cdot \mathbf{subexp}(\mathbf{log}|\mathbf{disc}(\mathbb{Z}[\boldsymbol{\theta}])|)$.

Remark: CSIDH and SCALLOP are safe! (At least in the face of this threat)

What's next ?

- Keep digging in the implications of higher dimensional isogenies over security analysis.
- Improve the constructive applications.

Thanks for your attention!

Bibliography I

[Arp+22] Sarah Arpin et al. “Orienteering with one endomorphism”. In: CoRR abs/2201.11079 (2022). arXiv: 2201.11079. url: https://arxiv.org/abs/2201.11079.

[Cas+18] Wouter Castryck et al. “CSIDH: An Efficient Post-Quantum Commutative Group Action”. In: Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory Ed. by Thomas Peyrin and Steven D. Galbraith. Vol. 11274. Lecture Notes in Computer Science. Springer, 2018, pp. 395–427. url: https://doi.org/10.1007/978-3-030-03332-3%5C_15.

[CJS14] Andrew M. Childs, David Jao, and Vladimir Soukharev. “Constructing elliptic curve isogenies in quantum subexponential time”. In: J. Math. Cryptol. 8.1 (2014), pp. 1–29. url: https://doi.org/10.1515/jmc-2012-0016.

[CK20] Leonardo Colò and David Kohel. “Orienting supersingular isogeny graphs”. In: IACR Cryptol. ePrint Arch. (2020), p. 985. url: https://eprint.iacr.org/2020/985.

Bibliography II

[Feo+23] Luca De Feo et al. "SCALLOP: scaling the CSI-FiSh". In: IACR International Conference on Public-Key Cryptography. Springer, 2023, pp. 345–375.

[HW23] Arthur Herlédan Le Merdy and Benjamin Wesolowski. The supersingular endomorphism ring problem given one endomorphism. Cryptology ePrint Archive, Paper 2023/1448. 2023. url: https://eprint.iacr.org/2023/1448.

[Kup05] Greg Kuperberg. "A Subexponential-Time Quantum Algorithm for the Dihedral Hidden Subgroup Problem". In: SIAM J. Comput. 35.1 (2005), pp. 170–188. url: https://doi.org/10.1137/S0097539703436345.

[Onu21] Hiroshi Onuki. "On oriented supersingular elliptic curves". In: Finite Fields Their Appl. 69 (2021), p. 101777. url: https://doi.org/10.1016/j.ffa.2020.101777.

Bibliography III

[PR23] Aurel Page and Damien Robert.
Introducing Clapoti(s): Evaluating the isogeny class group action in polynomial time.
Cryptology ePrint Archive, Paper 2023/1766. 2023. url:
https://eprint.iacr.org/2023/1766.

[Rob22a] Damien Robert. "Evaluating isogenies in polylogarithmic time". In:
IACR Cryptol. ePrint Arch. (2022), p. 1068. url:
https://eprint.iacr.org/2022/1068.

[Rob22b] Damien Robert. "Some applications of higher dimensional isogenies to elliptic curves (preliminary version)". In: IACR Cryptol. ePrint Arch. (2022), p. 1704. url:
https://eprint.iacr.org/2022/1704.

[Wes21] Benjamin Wesolowski.
"The supersingular isogeny path and endomorphism ring problems are equivalent". In:
62nd IEEE Annual Symposium on Foundations of Computer Science, FOCS 2021, Denver,
IEEE, 2021, pp. 1100–1111. url:
https://doi.org/10.1109/FOCS52979.2021.00109.

Bibliography IV

[Wes22] Benjamin Wesolowski. "Orientations and the Supersingular Endomorphism Ring Problem". In: Advances in Cryptology - EUROCRYPT 2022 - 41st Annual International Conference on tl
Ed. by Orr Dunkelman and Stefan Dziembowski. Vol. 13277. Lecture Notes in Computer Science. Springer, 2022, pp. 345–371. url: https://doi.org/10.1007/978-3-031-07082-2%5C_13.