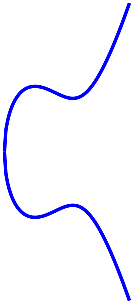
The endomorphism ring problem given an endomorphism

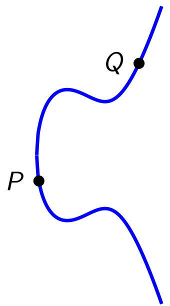
Arthur Herlédan Le Merdy
Supervisors: Guillaume Hanrot & Benjamin Wesolowski

Monday 16^{th} October, 2023



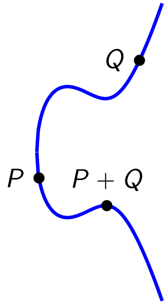
$E : y^2 = x^3 + Ax + B$

- **Elliptic curve:** smooth projective curve given by an affine model such as above.



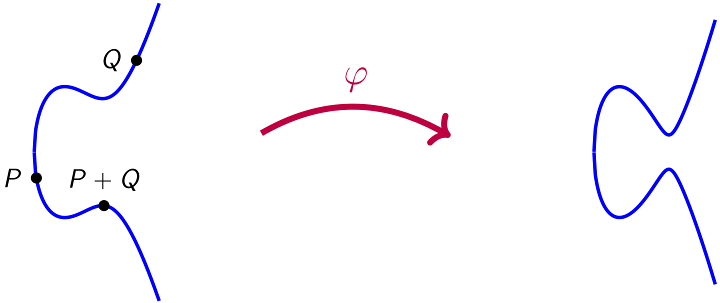
$E : y^2 = x^3 + Ax + B$

- **Elliptic curve:** smooth projective curve given by an affine model such as above.



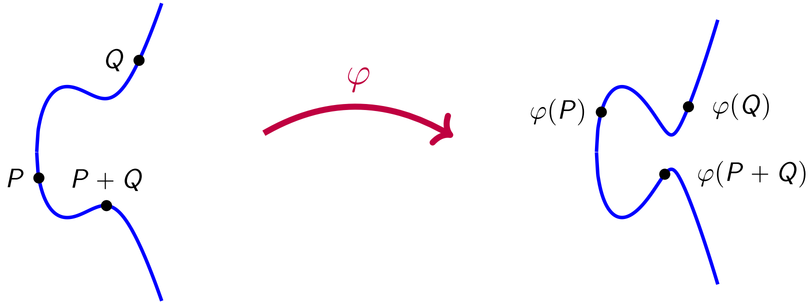
$E : y^2 = x^3 + Ax + B$

- **Elliptic curve:** smooth projective curve given by an affine model such as above.



$E : y^2 = x^3 + Ax + B$ $\qquad$ $E' : y^2 = x^3 + A'x + B'$

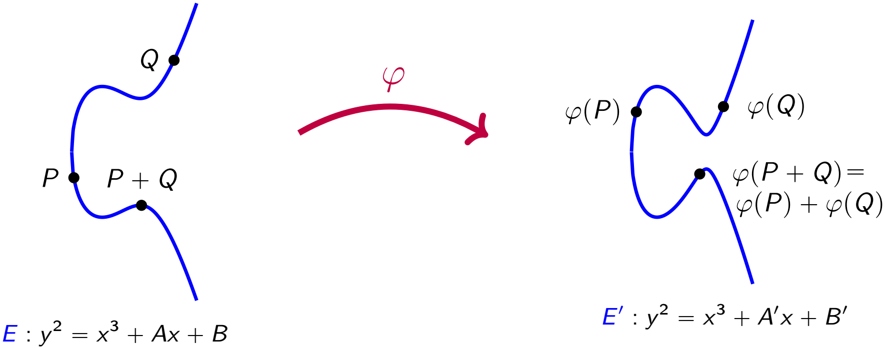
- **Elliptic curve:** smooth projective curve given by an affine model such as above.
- **Isogeny:** non-constant rational map inducing a group homomorphism.



$E : y^2 = x^3 + Ax + B$ $\qquad$ $E' : y^2 = x^3 + A'x + B'$

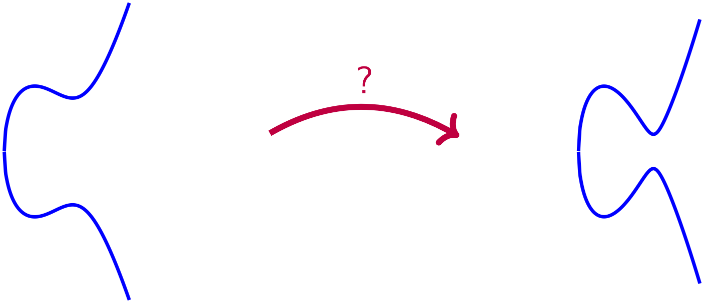
- **Elliptic curve:** smooth projective curve given by an affine model such as above.
- **Isogeny:** non-constant rational map inducing a group homomorphism.

Elliptic curves and isogenies



- **Elliptic curve:** smooth projective curve given by an affine model such as above.
- **Isogeny:** non-constant rational map inducing a group homomorphism.

Isogeny hard problem



$E : y^2 = x^3 + Ax + B$

$E' : y^2 = x^3 + A'x + B'$

The Isogeny Problem

Given two elliptic curves E and E', find an isogeny between them.

Endomorphism ring

An isogeny $\varphi : E \to E$ is an **endomorphism**.
We denote $\mathrm{End}(E) := \{\varphi : E \to E\} \cup \{0\}$.

Endomorphism ring

An isogeny $\varphi : E \to E$ is an **endomorphism**.
We denote $\mathrm{End}(E) := \{\varphi : E \to E\} \cup \{0\}$.

- $(\mathrm{End}(E), +, \circ)$ is the **endomorphism ring** of E, where for every $P \in E$:

$$(\varphi + \psi)(P) = \varphi(P) + \psi(P) \quad \text{and} \quad (\varphi \circ \psi)(P) = \varphi(\psi(P)).$$

Endomorphism ring

An isogeny $\varphi : E \to E$ is an **endomorphism**.
We denote $\mathrm{End}(E) := \{\varphi : E \to E\} \cup \{0\}$.

- $(\mathrm{End}(E), +, \circ)$ is the **endomorphism ring** of E, where for every $P \in E$:

$$(\varphi + \psi)(P) = \varphi(P) + \psi(P) \qquad \text{and} \qquad (\varphi \circ \psi)(P) = \varphi(\psi(P)).$$

- $\mathbb{Z} \hookrightarrow \mathrm{End}(E)$ as **subring**. For every $n \in \mathbb{Z}$, we have the endomorphism

$$\begin{aligned} [n] : E &\to E \\ P &\mapsto [n]P := \underbrace{P + \cdots + P}_{n \text{ times}}. \end{aligned}$$

Endomorphism ring

An isogeny $\varphi : E \to E$ is an **endomorphism**.
We denote $\mathrm{End}(E) := \{\varphi : E \to E\} \cup \{0\}$.

- $(\mathrm{End}(E), +, \circ)$ is the **endomorphism ring** of E, where for every $P \in E$:
  $(\varphi+\psi)(P) = \varphi(P) + \psi(P)$ and $(\varphi\circ\psi)(P) = \varphi(\psi(P))$.
- $\mathbb{Z} \hookrightarrow \mathrm{End}(E)$ as **subring**. For every $n \in \mathbb{Z}$, we have the endomorphism
$$\begin{aligned}[n] : E &\to E \\ P &\mapsto [n]P := \underbrace{P + \cdots + P}_{n \text{ times}}.\end{aligned}$$
- $(\mathrm{End}(E), +)$ is a lattice of dimension
  - **2** then $\mathrm{End}(E) \simeq \mathbb{Z} \oplus \alpha\mathbb{Z}$,
    or
  - **4** then $\mathrm{End}(E) \simeq \mathbb{Z} \oplus \alpha\mathbb{Z} \oplus \beta\mathbb{Z} \oplus \gamma\mathbb{Z}$.

Endomorphism ring

An isogeny $\varphi : E \to E$ is an **endomorphism**.
We denote $\mathrm{End}(E) := \{\varphi : E \to E\} \cup \{0\}$.

- $(\mathrm{End}(E), +, \circ)$ is the **endomorphism ring** of E, where for every $P \in E$:

  $(\varphi+\psi)(P) = \varphi(P) + \psi(P)$ and $(\varphi\circ\psi)(P) = \varphi(\psi(P))$.

- $\mathbb{Z} \hookrightarrow \mathrm{End}(E)$ as **subring**. For every $n \in \mathbb{Z}$, we have the endomorphism

$$\begin{aligned}[n] : E &\to E \\ P &\mapsto [n]P := \underbrace{P + \cdots + P}_{n \text{ times}}.\end{aligned}$$

- $(\mathrm{End}(E), +)$ is a lattice of dimension
  - **2** then $\mathrm{End}(E) \simeq \mathbb{Z} \oplus \alpha\mathbb{Z}$, $\}$ E is **ordinary**.

    or
  - **4** then $\mathrm{End}(E) \simeq \mathbb{Z} \oplus \alpha\mathbb{Z} \oplus \beta\mathbb{Z} \oplus \gamma\mathbb{Z}$. $\}$ E is **supersingular**.

Supersingular endomorphism ring problem

The 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 Endomorphism Ring Problem (EndRing):

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

- The **Endomorphism Ring Problem** is equivalent to the **Isogeny Problem**. [Wes22b]

Supersingular endomorphism ring problem

The Endomorphism Ring Problem (EndRing):

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

- The **Endomorphism Ring Problem** is equivalent to the **Isogeny Problem**. [Wes22b]
- Some protocols give additional information such as a public endomorphism $\theta \in \mathrm{End}(E) \backslash \mathbb{Z}$. (CSIDH, [Cas+18], SCALLOP [Feo+23])

Supersingular endomorphism ring problem

The Endomorphism Ring Problem (EndRing):

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

- The **Endomorphism Ring Problem** is equivalent to the **Isogeny Problem**. [Wes22b]
- Some protocols give additional information such as a public endomorphism $\theta \in \mathrm{End}(E) \setminus \mathbb{Z}$. (CSIDH, [Cas+18], SCALLOP [Feo+23])

The Endomorphism Ring Problem given one Endomorphism :

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

Supersingular endomorphism ring problem

`The Endomorphism Ring Problem (EndRing):`

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

- The **Endomorphism Ring Problem** is equivalent to the **Isogeny Problem**. [Wes22b]
- Some protocols give additional information such as a public endomorphism $\theta \in \mathrm{End}(E)\backslash\mathbb{Z}$. (CSIDH, [Cas+18], SCALLOP [Feo+23])

`The 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
Classic	$p^{1/2}$	$(\deg\theta)^{1/4}$
Quantum	$p^{1/4}$	subexponential in $\log\deg\theta$

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

Orientations [CK20],[Onu20]

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

- $\mathbb{Z}[\theta] \simeq \mathbb{Z}[X] / < X^2 + aX + b >$ for some $a, b \in \mathbb{Z}$, i.e. $\mathbb{Z}[\theta]$ is a **quadratic ring**.
- $\mathbb{Z}[\theta] \hookrightarrow \mathrm{End}(E)$.

Orientations [CK20],[Onu20]

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

- $\mathbb{Z}[\theta] \simeq \mathbb{Z}[X]/ < X^2 + aX + b >$ for some $a, b \in \mathbb{Z}$, i.e. $\mathbb{Z}[\theta]$ is a **quadratic ring**.
- $\mathbb{Z}[\theta] \hookrightarrow \mathrm{End}(E)$.

Let $\mathfrak{O}$ be a quadratic ring.

- An embedding $\iota : \mathfrak{O} \hookrightarrow \mathrm{End}(E)$ is called an $\mathfrak{O}$-**orientation**.
- It is a **primitive** $\mathfrak{O}$-orientation if for any quadratic ring $\mathfrak{O}' \supseteq \mathfrak{O}$, it is impossible to extend ι to $\mathfrak{O}'$ such that $\iota : \mathfrak{O}' \hookrightarrow \mathrm{End}(E)$.
- The ideal class group $\mathcal{C}l(\mathfrak{O})$ **acts** on elliptic curves endowed with an $\mathfrak{O}$-orientation.

Orientations [CK20],[Onu20]

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

- $\mathbb{Z}[\theta] \simeq \mathbb{Z}[X]/ < X^2 + aX + b >$ for some $a, b \in \mathbb{Z}$, i.e. $\mathbb{Z}[\theta]$ is a **quadratic ring**.
- $\mathbb{Z}[\theta] \hookrightarrow \mathrm{End}(E)$.

Let $\mathfrak{O}$ be a quadratic ring.

- An embedding $\iota : \mathfrak{O} \hookrightarrow \mathrm{End}(E)$ is called an $\mathfrak{O}$-**orientation**.
- It is a **primitive** $\mathfrak{O}$-orientation if for any quadratic ring $\mathfrak{O}' \supseteq \mathfrak{O}$, it is impossible to extend ι to $\mathfrak{O}'$ such that $\iota : \mathfrak{O}' \hookrightarrow \mathrm{End}(E)$.
- The ideal class group $\mathcal{C}l(\mathfrak{O})$ **acts** on elliptic curves endowed with an $\mathfrak{O}$-orientation.

The $\mathfrak{O}$-oriented Endomorphism Ring Problem ($\mathfrak{O}$-EndRing):

Given a supersingular elliptic curve $\boldsymbol{E}$ and a **primitive orientation** $\boldsymbol{\iota} : \mathfrak{O} \hookrightarrow \mathrm{End}(E)$, find a basis of its endomorphism ring $\mathbf{End}\,(\boldsymbol{E})$.

`EndRing` given an endomorphism

$\boxed{E \text{ and } \theta \in \mathrm{End}(E)\backslash\mathbb{Z}}$

$\boxed{\text{A basis of } \mathrm{End}(E)}$

EndRing given an endomorphism

$$\begin{tikzcd} \boxed{E \text{ and } \theta \in \mathrm{End}(E) \backslash \mathbb{Z}} \arrow[d, "1"'] \\ \boxed{E \text{ and } \iota : \mathbb{Z}[\theta] \hookrightarrow \mathrm{End}(E)} \end{tikzcd}$$

$$\boxed{\text{A basis of } \mathrm{End}(E)}$$

① Immediate.

EndRing given an endomorphism

$$\begin{tikzcd}
\boxed{E \text{ and } \theta \in \mathrm{End}(E)\backslash\mathbb{Z}} \arrow[d, "1"'] \\
\boxed{E \text{ and } \iota : \mathbb{Z}[\theta] \hookrightarrow \mathrm{End}(E)} \arrow[d, "2\quad \texttt{Primitivisation}"'] \\
\boxed{E \text{ and } \iota : \mathbb{Z}[\theta] \hookrightarrow \mathrm{End}(E) \textbf{ primitive}} \\
\\
\boxed{\text{A basis of } \mathrm{End}(E)}
\end{tikzcd}$$

① Immediate.

② Hard problem with a subexponential quantum complexity. [Arp+23]

EndRing given an endomorphism

$$\begin{tikzcd}
\boxed{E \text{ and } \theta \in \mathrm{End}(E)\backslash\mathbb{Z}} \arrow[d, "1"'] \\
\boxed{E \text{ and } \iota : \mathbb{Z}[\theta] \hookrightarrow \mathrm{End}(E)} \arrow[d, "2\quad \texttt{Primitivisation}"'] \\
\boxed{E \text{ and } \iota : \mathbb{Z}[\theta] \hookrightarrow \mathrm{End}(E) \textbf{ primitive}} \\
\\
\boxed{\text{A basis of } \mathrm{End}(E)}
\end{tikzcd}$$

① Immediate.

② ~~Hard problem with a subexponential quantum complexity~~. [Arp+23]

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

EndRing given an endomorphism

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

$\downarrow$ 1

E and $\iota : \mathbb{Z}[\theta] \hookrightarrow \mathrm{End}(E)$

$\downarrow$ 2 `Primitivisation`

E and $\iota : \mathbb{Z}[\theta] \hookrightarrow \mathrm{End}(E)$ **primitive**

$\downarrow$ 3 $\mathfrak{O}$-`EndRing`

A basis of $\mathrm{End}(E)$

① Immediate.

② ~~Hard problem with a subexponential quantum complexity~~. [Arp+23]

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

③ Known complexity under some heuristics. [Wes22a]

EndRing given an endomorphism

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

① Immediate.

② ~~Hard problem with a subexponential quantum complexity~~. [Arp+23]

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

③ ~~Known complexity under some heuristics.~~ [Wes22a]

Rigorous complexity analysis.

What's next ?

What's next ?

- Constructive applications

What's next ?

- Constructive applications
- Attacks by climbing volcanoes of ℓ-isogenies

What's next ?

- Constructive applications
- Attacks by climbing volcanoes of ℓ-isogenies

Thanks for your attention!

https://eprint.iacr.org/2023/1448

Bibliography I

[Arp+23] Sarah Arpin et al. "Orienteering with one endomorphism". In: La Matematica (2023), pp. 1–60.

[Cas+18] Wouter Castryck et al. "CSIDH: an efficient post-quantum commutative group action". In: Advances in Cryptology–ASIACRYPT 2018. 2018, pp. 395–427.

[CK20] Leonardo Colò and David Kohel. "Orienting supersingular isogeny graphs". In: Journal of Mathematical Cryptology 14.1 (Oct. 2020), pp. 414–437.

[Feo+23] Luca De Feo et al. SCALLOP: scaling the CSI-FiSh. Published: Cryptology ePrint Archive, Paper 2023/058. 2023. url: https://eprint.iacr.org/2023/058.

[Onu20] Hiroshi Onuki. On oriented supersingular elliptic curves. 2020. doi: 10.48550/ARXIV.2002.09894. url: https://arxiv.org/abs/2002.09894.

[Wes22a] Benjamin Wesolowski. "Orientations and the supersingular endomorphism ring problem". In: Annual International Conference on the Theory and Applications of Cryptographic Techniq Springer. 2022, pp. 345–371.

Bibliography II

[Wes22b] Benjamin Wesolowski. "The supersingular isogeny path and endomorphism ring problems are equivalent". In: 2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS). IEEE. 2022, pp. 1100–1111.