The endomorphism ring problem given an endomorphism

Arthur Herlédan Le Merdy
Supervisors: Guillaume Hanrot & Benjamin Wesolowski

Monday 16th October, 2023
Elliptic curves and isogenies

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.
Elliptic curves and isogenies

\[ E : y^2 = x^3 + Ax + B \]

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

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

\[ E : y^2 = x^3 + Ax + B \]

- **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.
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.

\[ E : y^2 = x^3 + Ax + B \]
\[ E' : y^2 = x^3 + A'x + B' \]
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.
The Isogeny Problem

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

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

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

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

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

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

4 / 10
An isogeny $\varphi : E \to E$ is an **endomorphism**.
We denote $\text{End}(E) := \{\varphi : E \to E\} \cup \{0\}$.

- $(\text{End}(E), +, \circ)$ is the **endomorphism ring** of $E$, where for every $P \in E$:
  $$(\varphi + \psi)(P) = \varphi(P) + \psi(P) \quad \text{and} \quad (\varphi \circ \psi)(P) = \varphi(\psi(P)).$$

- $\mathbb{Z} \hookrightarrow \text{End}(E)$ as **subring**. For every $n \in \mathbb{Z}$, we have the endomorphism
  $$[n] : E \to E$$
  $$P \mapsto [n]P := \underbrace{P + \cdots + P}_{n \text{ times}}.$$
An isogeny $\varphi : E \to E$ is an endomorphism. We denote $\text{End}(E) := \{\varphi : E \to E\} \cup \{0\}$.

- $(\text{End}(E), +, \circ)$ is the endomorphism ring of $E$, where for every $P \in E$:
  $$(\varphi + \psi)(P) = \varphi(P) + \psi(P) \quad \text{and} \quad (\varphi \circ \psi)(P) = \varphi(\psi(P)).$$

- $\mathbb{Z} \hookrightarrow \text{End}(E)$ as subring. For every $n \in \mathbb{Z}$, we have the endomorphism
  $$[n] : E \to E$$
  $$P \mapsto [n]P := P + \cdots + P \quad \text{n times}.$$

- $(\text{End}(E), +)$ is a lattice of dimension
  - 2 then $\text{End}(E) \simeq \mathbb{Z} \oplus \alpha\mathbb{Z}$, or
  - 4 then $\text{End}(E) \simeq \mathbb{Z} \oplus \alpha\mathbb{Z} \oplus \beta\mathbb{Z} \oplus \gamma\mathbb{Z}$.
Endomorphism ring

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

- \((\text{End}(E), +, \circ)\) is the **endomorphism ring** of \( E \), where for every \( P \in E \):
  \[
  (\varphi + \psi)(P) = \varphi(P) + \psi(P) \quad \text{and} \quad (\varphi \circ \psi)(P) = \varphi(\psi(P)).
  \]

- \( \mathbb{Z} \hookrightarrow \text{End}(E) \) as subring. For every \( n \in \mathbb{Z} \), we have the endomorphism \( [n] : E \to E \)
  \[
  P \mapsto [n]P := P + \cdots + P \quad \text{\( n \) times}.
  \]

- \((\text{End}(E), +)\) is a lattice of dimension
  - \( 2 \) then \( \text{End}(E) \cong \mathbb{Z} \oplus \alpha \mathbb{Z} \), \( E \) is **ordinary**.
  - \( 4 \) then \( \text{End}(E) \cong \mathbb{Z} \oplus \alpha \mathbb{Z} \oplus \beta \mathbb{Z} \oplus \gamma \mathbb{Z} \). \( E \) is **supersingular**.
The Endomorphism Ring Problem (EndRing):

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

- The Endomorphism Ring Problem is equivalent to the Isogeny Problem. \cite{Wes22b}
- Some protocols give additional information such as a public endomorphism $\theta \in \text{End}(E)$.

- (CSIDH, \cite{Cas+18}, SCALLOP \cite{Feo+23})

The Endomorphism Ring Problem given one endomorphism $\theta$:

Given a supersingular elliptic curve $E$ and an endomorphism $\theta \in \text{End}(E)$, find a basis of its endomorphism ring $\text{End}(E)$. 

- **Classic**
  - $p \leq 2^{p^{\deg \theta} + 1} \leq 2^{16}$
- **Quantum**
  - $p \leq 2^{4 \deg \theta} \leq 2^{1.7}$
  - Subexponential in $\log \deg \theta$
The Endomorphism Ring Problem (EndRing):

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

- 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 $E$, find a basis of its endomorphism ring $\text{End}(E)$.

- The Endomorphism Ring Problem is equivalent to the Isogeny Problem. [Wes22b]
The Endomorphism Ring Problem (EndRing):

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

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

The Endomorphism Ring Problem (EndRing):
Given a supersingular elliptic curve $E$, find a basis of its endomorphism ring $\text{End}(E)$.

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

The Endomorphism Ring Problem given one Endomorphism:
Given a supersingular elliptic curve $E$ and an endomorphism $\theta \in \text{End}(E) \setminus \mathbb{Z}$, find a basis of its endomorphism ring $\text{End}(E)$. 
Supersingular endomorphism ring problem

The Endomorphism Ring Problem (EndRing):
Given a supersingular elliptic curve $E$, find a basis of its endomorphism ring $\text{End}(E)$.

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

The Endomorphism Ring Problem given one Endomorphism:
Given a supersingular elliptic curve $E$ and an endomorphism $\theta \in \text{End}(E)\backslash \mathbb{Z}$, find a basis of its endomorphism ring $\text{End}(E)$.

<table>
<thead>
<tr>
<th>EndRing</th>
<th>EndRing given one endomorphism $\theta$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classic</td>
<td>$p^{1/2}$</td>
</tr>
<tr>
<td>Quantum</td>
<td>$p^{1/4}$</td>
</tr>
</tbody>
</table>

Complexity of EndRing and its variant for an elliptic curve defined over $\mathbb{F}_{p^2}$, with $p$ a prime.
Let $\theta \in \text{End}(E) \setminus \mathbb{Z}$.

- $\mathbb{Z}[\theta] \cong \mathbb{Z}[X]/\langle X^2 + aX + b \rangle$ for some $a, b \in \mathbb{Z}$, i.e. $\mathbb{Z}[\theta]$ is a quadratic ring.
- $\mathbb{Z}[\theta] \hookrightarrow \text{End}(E)$. 

Orientations [CK20],[Onu20]
Orientations [CK20],[Onu20]

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

Let \( \mathcal{O} \) be a quadratic ring.
- An embedding \( \iota : \mathcal{O} \hookrightarrow \text{End}(E) \) is called an \( \mathcal{O} \)-orientation.
- It is a primitive \( \mathcal{O} \)-orientation if for any quadratic ring \( \mathcal{O}' \supseteq \mathcal{O} \), it is impossible to extend \( \iota \) to \( \mathcal{O}' \) such that \( \iota : \mathcal{O}' \hookrightarrow \text{End}(E) \).
- The ideal class group \( \mathcal{C}l(\mathcal{O}) \) acts on elliptic curves endowed with an \( \mathcal{O} \)-orientation.
Orientations [CK20],[Onu20]

Let $\theta \in \text{End}(E) \setminus \mathbb{Z}$.

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

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

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

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

Given a supersingular elliptic curve $E$ and a **primitive orientation** $\iota : \mathcal{O} \hookrightarrow \text{End}(E)$, find a basis of its endomorphism ring $\text{End}(E)$. 
EndRing given an endomorphism

\[ E \text{ and } \theta \in \text{End}(E)\backslash \mathbb{Z} \]

A basis of \text{End}(E)
EndRing given an endomorphism

1. Immediate.

A basis of \( \text{End}(E) \)
EndRing given an endomorphism

1. Immediate.

2. Hard problem with a subexponential quantum complexity. [Arp+23]
EndRing given an endomorphism

1. EndRing given an endomorphism

\[ E \text{ and } \theta \in \text{End}(E) \setminus \mathbb{Z} \]

2. Primitivisation

\[ E \text{ and } \iota : \mathbb{Z}[	heta] \hookrightarrow \text{End}(E) \]

\[ E \text{ and } \iota : \mathbb{Z}[	heta] \hookrightarrow \text{End}(E) \text{ primitive} \]

A basis of \text{End}(E)

1. Immediate.

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

Polynomial time given the factorisation of the discriminant of \( \mathbb{Z}[	heta] \).
EndRing given an endomorphism

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]

\[ E \text{ and } \theta \in \text{End}(E) \setminus \mathbb{Z} \]

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

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

\[ \mathcal{O}\text{-EndRing} \]

\[ \text{A basis of End}(E) \]
EndRing given an endomorphism

1. $E$ and $\theta \in \text{End}(E) \setminus \mathbb{Z}$

2. Primitivisation
   
   $E$ and $\iota : \mathbb{Z}[\theta] \hookrightarrow \text{End}(E)$

3. $\mathcal{O}$-EndRing
   
   A basis of $\text{End}(E)$

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]
   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 $\ell$-isogenies

Thanks for your attention!
https://eprint.iacr.org/2023/1448


