EUROCRYPT
2025
Madrid

Computing the endomorphism ring of a supersingular elliptic curve from a full rank suborder

***Mingjie Chen**, Christophe Petit*

COSIC
KU Leuven

Outline

Background

Main problem: Suborder to Endomorphism Ring

Another problem: Isogeny to Endomorphism Ring

Main ideas

Applications

Background

Elliptic curves

Elliptic curves are curves defined by equations of the form

$$y^2 = x^3 + ax + b.$$

Elliptic curves

Elliptic curves are curves defined by equations of the form

$$y^2 = x^3 + ax + b.$$

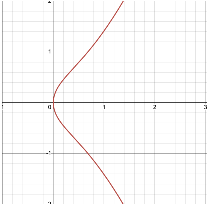


Figure: $y^2 = x^3 + x$

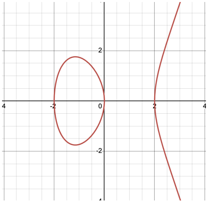


Figure: $y^2 = x^3 - 4x$

We will be working with elliptic curves over finite fields of characteristic p.

Isogenies

An **isogeny** sends points from one elliptic curve to another.

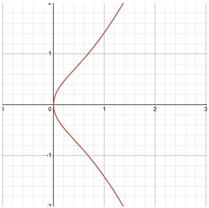


Figure: $y^2 = x^3 + x$

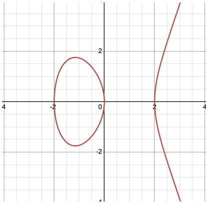


Figure: $y^2 = x^3 - 4x$

Isogenies

An **isogeny** sends points from one elliptic curve to another.

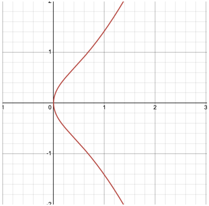


Figure: $y^2 = x^3 + x$

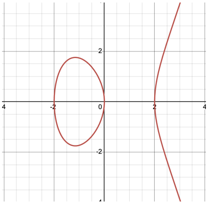


Figure: $y^2 = x^3 - 4x$

$$\phi : (x, y) \mapsto (\frac{x^2 + 1}{x}, \frac{x^2 - 1}{x^2} y)$$

This is an isogeny of **degree** 2.

Endomorphisms

An **endomorphism** is an isogeny from an elliptic curve to itself.

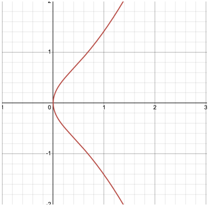


Figure: $y^2 = x^3 + x$

Endomorphisms

An **endomorphism** is an isogeny from an elliptic curve to itself.

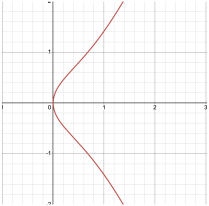


Figure: $y^2 = x^3 + x$

Examples:

$\iota : (x, y) \mapsto (-x, \mathbf{i}y)$ where $\mathbf{i} \in \mathbb{F}_{p^2}$ such that $\mathbf{i}^2 = -1$

$\pi_p : (x, y) \mapsto (x^p, y^p)$

Anything else? **fact&hint**: elliptic curve points form a group

Endomorphism ring

Consider the set of endomorphisms on a supersingular elliptic curve:

- it is a (non-commutative) ring
- it is a rank 4 $\mathbb{Z}$-lattice

This is the **endomorphism ring** of a supersingular elliptic curve.

Endomorphism ring

Consider the set of endomorphisms on a supersingular elliptic curve:

- it is a (non-commutative) ring
- it is a rank 4 $\mathbb{Z}$-lattice

This is the **endomorphism ring** of a supersingular elliptic curve.

Let $E_0 : y^2 = x^3 + x$, then we already know that

$$\mathrm{End}(E_0) \supseteq \mathbb{Z} + \mathbb{Z}\iota + \mathbb{Z}\pi_p + \mathbb{Z}\iota \circ \pi_p.$$

Endomorphism ring

Consider the set of endomorphisms on a supersingular elliptic curve:

- it is a (non-commutative) ring
- it is a rank 4 $\mathbb{Z}$-lattice

This is the **endomorphism ring** of a supersingular elliptic curve.

Let $E_0 : y^2 = x^3 + x$, then we already know that

$$\mathrm{End}(E_0) \supseteq \mathbb{Z} + \mathbb{Z}\iota + \mathbb{Z}\pi_p + \mathbb{Z}\iota \circ \pi_p.$$

Problem (EndRing)

Let p be a prime and $E/\mathbb{F}_{p^2}$ be a supersingular elliptic curve, compute $\mathrm{End}(E)$. More explicitly, it asks to find a basis of $\mathrm{End}(E)$ as a $\mathbb{Z}$-lattice.

Main problem: Suborder to Endomorphism Ring

Suborder to Endomorphism Ring

Problem (SubOrderEndRing)

Let p be a prime and $E/\mathbb{F}_{p^2}$ be a supersingular elliptic curve and $\mathcal{R}_E \subseteq \mathrm{End}(E)$ be a suborder of rank 4 of discriminant $\Delta_{\mathcal{R}}$. Compute $\mathrm{End}(E)$.

Suborder to Endomorphism Ring

Problem (SubOrderEndRing)

Let p be a prime and $E/\mathbb{F}_{p^2}$ be a supersingular elliptic curve and $\mathcal{R}_E \subseteq \mathrm{End}(E)$ be a suborder of rank 4 of discriminant $\Delta_{\mathcal{R}}$. Compute $\mathrm{End}(E)$.

Suborder

- a sublattice
- closed under multiplication

Input

- $\mathcal{R}_E$ will be given by efficient representations of a lattice basis
- we assume the representations are polynomial in $\log\Delta_{\mathcal{R}}$

Naive approach

Problem (forgetting the multiplicative structure)

Suppose

- *These is an unknown target lattice $\mathcal{L}$ that contains a known lattice $\mathcal{R}$ with known index $[\mathcal{L} : \mathcal{R}]$.*
- *There is also an efficient algorithm that detects if a superlattice $\mathcal{L}'$ containing $\mathcal{R}$ is contained in $\mathcal{L}$ or not.*

The question is, how to find $\mathcal{L}$.

Naive approach

Problem (forgetting the multiplicative structure)

Suppose

- *These is an unknown target lattice $\mathcal{L}$ that contains a known lattice $\mathcal{R}$ with known index $[\mathcal{L} : \mathcal{R}]$.*
- *There is also an efficient algorithm that detects if a superlattice $\mathcal{L}'$ containing $\mathcal{R}$ is contained in $\mathcal{L}$ or not.*

The question is, how to find $\mathcal{L}$.

- We can list all the superlattices containing $\mathcal{R}$ and use the detecting algorithm.
- We can deal with one factor in the index at a time.
- The hard cases are when the index $[\mathcal{L} : \mathcal{R}]$ contains large prime factors.

Known result and main theorem

Known Result (heuristic)

There is a polynomial time quantum algorithm that solves the SubOrderEndRing problem when the suborder $\mathcal{R}_E$ is an embedding of an order of the form $\mathbb{Z} + D\,\mathrm{End}(E_0) \hookrightarrow \mathrm{End}(E)$ where $D \neq p$ is a prime. [**C**IIKLP23]

Known result and main theorem

Known Result (heuristic)

There is a polynomial time quantum algorithm that solves the SubOrderEndRing problem when the suborder $\mathcal{R}_E$ is an embedding of an order of the form $\mathbb{Z} + D\,\mathrm{End}(E_0) \hookrightarrow \mathrm{End}(E)$ where $D \neq p$ is a prime. [**C**IIKLP23]

- This was the hard problem underlying a key exchange protocol called pSIDH.

Known result and main theorem

Known Result (heuristic)

There is a polynomial time quantum algorithm that solves the SubOrderEndRing problem when the suborder $\mathcal{R}_E$ is an embedding of an order of the form $\mathbb{Z} + D\,\mathrm{End}(E_0) \hookrightarrow \mathrm{End}(E)$ where $D \neq p$ is a prime. [**C**IIKLP23]

- This was the hard problem underlying a key exchange protocol called pSIDH.

Theorem (heuristic,SubOrderEndRing)

Let E be a supersingular elliptic curve over $\mathbb{F}_{p^2}$. Given a full rank suborder $\mathcal{R}_E \subseteq \mathrm{End}(E)$ of discriminant $\Delta_{\mathcal{R}}$, there exists a quantum algorithm that computes $\mathrm{End}(E)$ *in polynomial time in* $\log \Delta_{\mathcal{R}}$.

Another problem: Isogeny to Endomorphism Ring

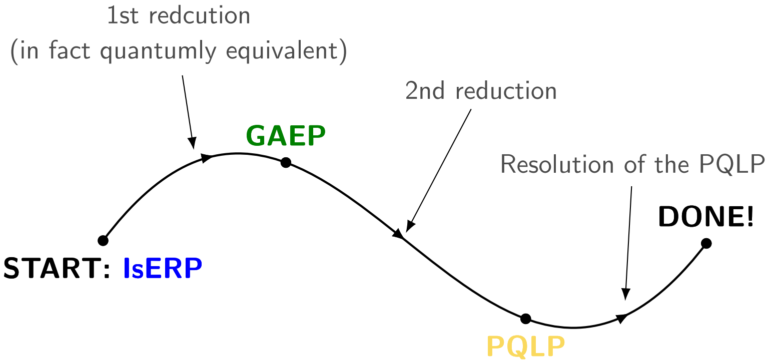
The isogeny to endomorphism ring problem

Problem (IsERP)

Let E_0, E be supersingular elliptic curves over $\mathbb{F}_{p^2}$ and $\varphi : E_0 \to E$ be an isogeny of degree N. Given the endomorphism ring $\mathrm{End}(E_0)$ and a weak isogeny representation [a] of φ, compute $\mathrm{End}(E)$.

[a] meaning that we know the evaluation of φ on points up to a scalar

Roadmap from [CIIKLP23]



- Isogeny to Endomorphism Ring Problem (**IsERP**)
- Group Action Evaluation Problem (**GAEP**)
- Powersmooth Quaternion Lifting Problem (**PQLP**)

[CIIKLP23] main results

Theorem (heuristic, PQLP)

Let $N = \prod \ell_i^{e_i} \neq p$ *be an odd integer and has* $O(\log(\log p))$ *distinct factors, then there exists a randomized polynomial time classical algorithm that solves the PQLP.*

[CIIKLP23] main results

Theorem (heuristic, PQLP)

Let $N = \prod \ell_i^{e_i} \neq p$ be an odd integer and has $O(\log(\log p))$ distinct factors, then there exists a randomized polynomial time classical algorithm that solves the PQLP.

Theorem (heuristic, IsERP)

Let $N = \prod \ell_i^{e_i} \neq p$ that is of size polynomial in p and has $O(\log(\log p))$ distinct factors, then there exists a polynomial time quantum algorithm that solves the IsERP.

Main ideas

Two tasks

A Reduce the SubOrderEndRing problem to an instance of the IsERP.

A0 We derive an embedding $\mathbb{Z} + N\,\mathrm{End}(E_0)$ to $\mathrm{End}(E)$ for smallest such N.

A1 We first show the existence of an isogeny $\varphi : E_0 \to E$.

A2 We then show how to get a weak isogeny representation of φ.

Two tasks

A Reduce the SubOrderEndRing problem to an instance of the IsERP.

A0 We derive an embedding $\mathbb{Z} + N\,\mathrm{End}(E_0)$ to $\mathrm{End}(E)$ for smallest such N.

A1 We first show the existence of an isogeny $\varphi : E_0 \to E$.

A2 We then show how to get a weak isogeny representation of φ.

Remark

A1,A2 have been done in [Leroux22] when pSIDH was introduced, but only for $N = D$ is a prime not equal to p. Our method is greatly inspired by the technique in [Leroux22].

Two tasks

A Reduce the SubOrderEndRing problem to an instance of the IsERP.

A0 We derive an embedding $\mathbb{Z} + N\,\mathrm{End}(E_0)$ to $\mathrm{End}(E)$ for smallest such N.

A1 We first show the existence of an isogeny $\varphi : E_0 \to E$.

A2 We then show how to get a weak isogeny representation of φ.

Remark

A1,A2 have been done in [Leroux22] when pSIDH was introduced, but only for $N = D$ is a prime not equal to p. Our method is greatly inspired by the technique in [Leroux22].

B Solve the PQLP in full generality.

Task B - Powersmooth Quaternion Lifting Problem

Problem (Powersmooth Quaternion Lift Problem (PQLP))

Let $\mathcal{O}$ be a maximal order in $\mathcal{B}_{p,\infty}$. Given an integer $(N, p) = 1$ and an element $\sigma_0 \in \mathcal{O}$ such that $(n(\sigma_0), N) = 1$, find $\sigma \in \mathcal{O}$ and $\lambda \in (\mathbb{Z}/N\mathbb{Z})^\times$ such that $\sigma = \lambda\sigma_0 \bmod N\mathcal{O}$ and that $n(\sigma)$ is powersmooth.

Task B - Powersmooth Quaternion Lifting Problem

Problem (Powersmooth Quaternion Lift Problem (PQLP))

Let $\mathcal{O}$ be a maximal order in $\mathcal{B}_{p,\infty}$. Given an integer $(N, p) = 1$ and an element $\sigma_0 \in \mathcal{O}$ such that $(n(\sigma_0), N) = 1$, find $\sigma \in \mathcal{O}$ and $\lambda \in (\mathbb{Z}/N\mathbb{Z})^\times$ such that $\sigma = \lambda\sigma_0 \bmod N\mathcal{O}$ and that $n(\sigma)$ is powersmooth.

Think of

- $\mathcal{O}$ as $\mathrm{End}(E_0)$.
- $\mathcal{B}_{p,\infty}$ as $\mathrm{End}(E_0) \otimes_{\mathbb{Z}} \mathbb{Q}$.
- σ_0, σ as endomorphisms of E_0.
- $n(\sigma_0), n(\sigma)$ as their degrees.
- $\sigma = \lambda\sigma_0 \bmod N\mathcal{O}$ as these two endomorphisms having the same action (up to a scalar) on $E_0[N]$ (kernel of $[N] : E_0 \to E_0$).

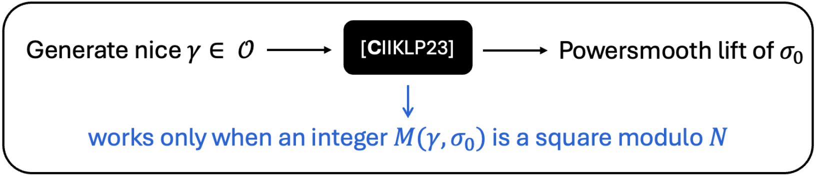
Task B - main idea

Generate nice $\gamma \in \mathcal{O}$ $\longrightarrow$ [CIIKLP23] $\longrightarrow$ Powersmooth lift of σ_0

$\downarrow$

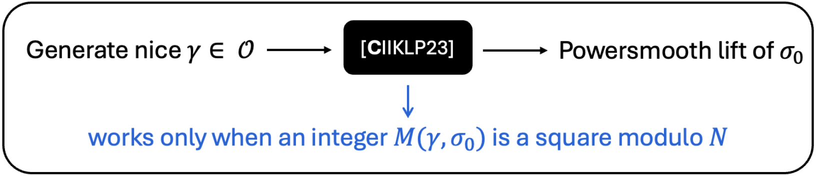
works only when an integer $M(\gamma, \sigma_0)$ is a square modulo N

Task B - main idea



Intuition: Let k be the number of prime factors of N. A random number has $1/2^k$ chance of being a square modulo N, however, it is usually a square modulo half of the prime divisors of N.

Task B - main idea



Intuition: Let k be the number of prime factors of N. A random number has $1/2^k$ chance of being a square modulo N, however, it is usually a square modulo half of the prime divisors of N.

- Find σ_1 which is not perfect lift but $\sigma_0 \equiv \sigma_1 \bmod N_1\mathcal{O}$ where N_1 divides N and $N_1 \approx \sqrt{N}$.
- We now solve the PQLP for $\sigma_0' := \sigma_0\sigma_1^{-1}$, we will be able to lift σ_0' for N_2 such that $N_1 \mid N_2$ and $N_2 > N_1$. I.e., we can find σ_2 such that $\sigma_0' \equiv \sigma_2 \bmod N_2\mathcal{O}$.
- Therefore, $\sigma_2\sigma_1 \equiv \sigma_0\sigma_1^{-1}\sigma_1 \bmod N_2\mathcal{O}$, and $n(\sigma_2\sigma_1)$ is powersmooth.

Applications

More hard problems in isogeny-based cryptography

- EndRing: Given a supersingular elliptic curve $E/\mathbb{F}_{p^2}$, compute $\mathrm{End}(E)$.
- ℓ-Isogeny: Given two supersingular elliptic curves E_1, E_2, compute an ℓ-power isogeny between them.
- Isogeny: Given two supersingular elliptic curves E_1, E_2, compute an arbitrary isogeny between them.
- OneEnd: Given a supersingular elliptic curve $E/\mathbb{F}_{p^2}$, compute a non-trivial endomorphism $\theta \in \mathrm{End}(E)$. underlies the security of the SQIsign digital signature
- FullSubOrder: Given a supersingular elliptic curve $E/\mathbb{F}_{p^2}$, compute a full rank suborder $\mathcal{R}_E \subseteq \mathrm{End}(E)$.

Classical reduction

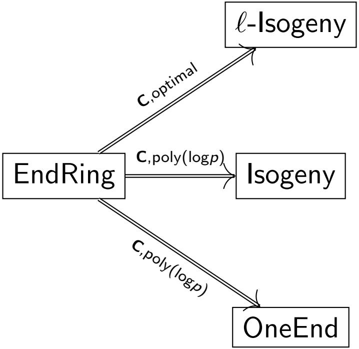


Figure: Polynomial time reductions of EndRing to other hard problems. On the edges, "**C**" represents *classical* reductions. Labels "optimal, poly(log$p$)" measure the query complexity of each reduction.

Remark

In the case when p is a prime of 256-bits, 2^{208} queries to the oracle O that outputs a solution for OneEnd are needed in the worst case. [PW24].

Quantum reduction

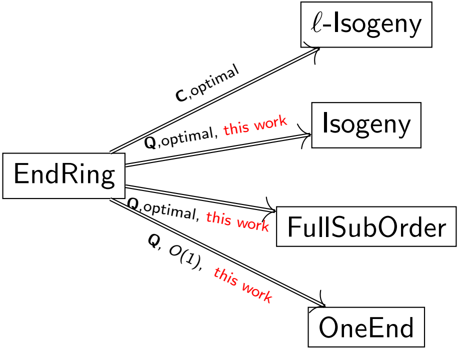


Figure: Polynomial time reductions of EndRing to other hard problems. On the edges, "$\mathbf{C}, \mathbf{Q}$" represents *classical* and *quantum* reductions respectively. Labels "optimal, $O(1)$" measure the query complexity of each reduction.

Thank you!