Unconditional foundations for supersingular isogeny-based cryptography

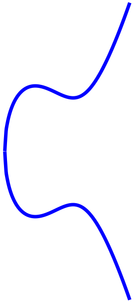
Arthur Herlédan Le Merdy[1] and Benjamin Wesolowski[2]

[1]ENS de Lyon and COSIC, KU LEUVEN
[2]ENS de Lyon and CNRS

TCC 2025, December 4, 2025, Aarhus, Denmark

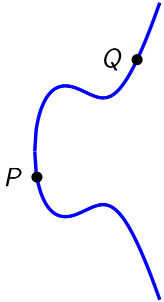
European Research Council
Established by the European Commission

The Isogeny Problem



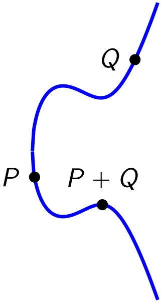
$E : y^2 = x^3 + Ax + B$

The Isogeny Problem



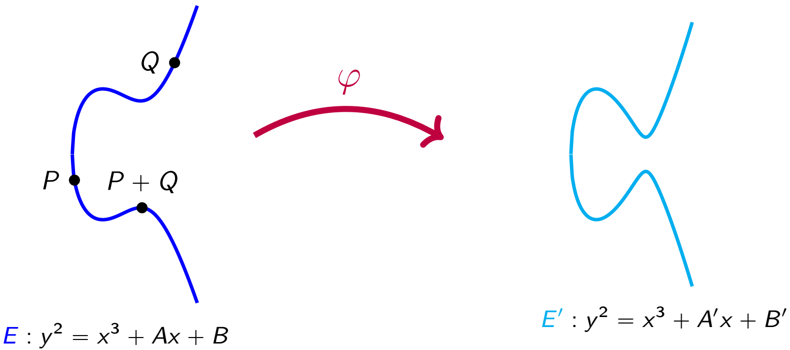
$E : y^2 = x^3 + Ax + B$

The Isogeny Problem



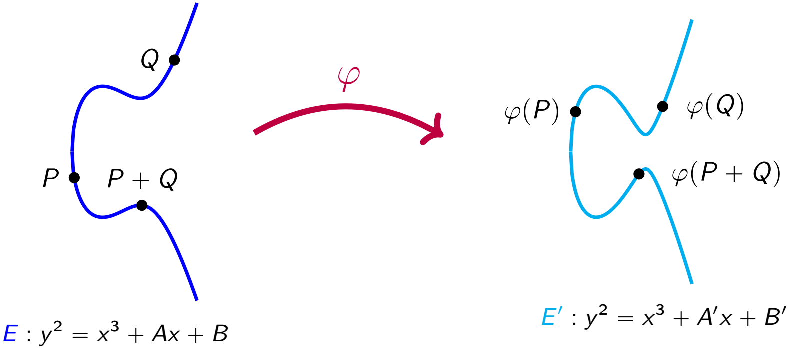
$E : y^2 = x^3 + Ax + B$

The Isogeny Problem



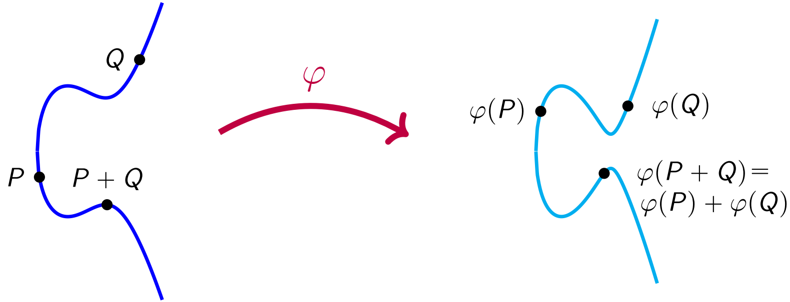
An **Isogeny** is a nice map between elliptic curves.

The Isogeny Problem



An **Isogeny** is a nice map between elliptic curves.

The Isogeny Problem

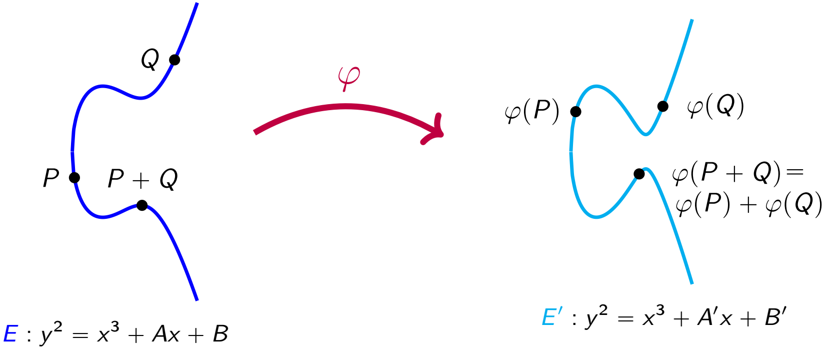


$E : y^2 = x^3 + Ax + B$

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

An **Isogeny** is a nice map between elliptic curves.

The Isogeny Problem

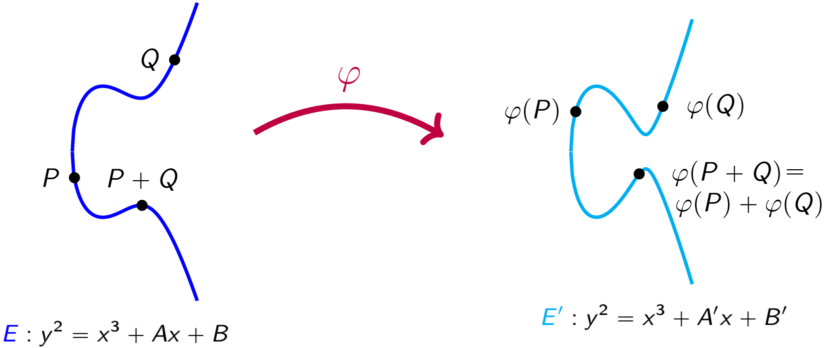


An **Isogeny** is a nice map between elliptic curves.

The supersingular Isogeny problem

Given two supersingular **elliptic curves** E and E' defined over $\mathbb{F}_{p^2}$, for a fixed prime p, find an **isogeny** $\varphi : E \rightarrow E'$.

The Isogeny Problem

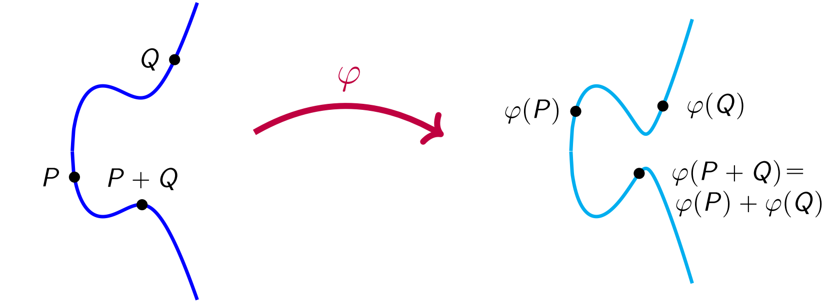


An **Isogeny** is a nice map between elliptic curves.

The supersingular Isogeny problem

Given two supersingular **elliptic curves** E and E' **defined over** $\mathbb{F}_{p^2}$, for a fixed prime p, find an **isogeny** $\varphi : E \to E'$.

The Isogeny Problem



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

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

An **Isogeny** is a nice map between elliptic curves.

The supersingular Isogeny problem

Given two **supersingular elliptic curves** E and E' **defined over** $\mathbb{F}_{p^2}$, for a fixed prime p, find an **isogeny** $\varphi : E \to E'$.

The ℓ-IsogenyPath Problem

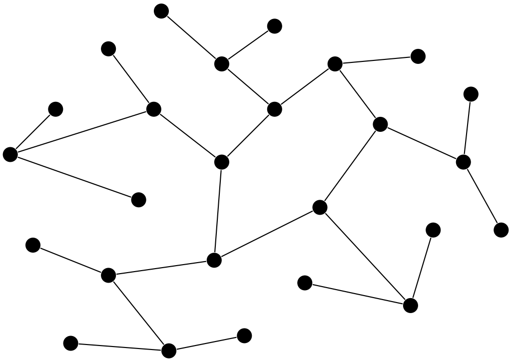
Let $\ell \neq p$ be a prime.

The ℓ-IsogenyPath Problem

Let $\ell \neq p$ be a prime.

The ℓ-IsogenyPath Problem

Let $\ell \neq p$ be a prime.



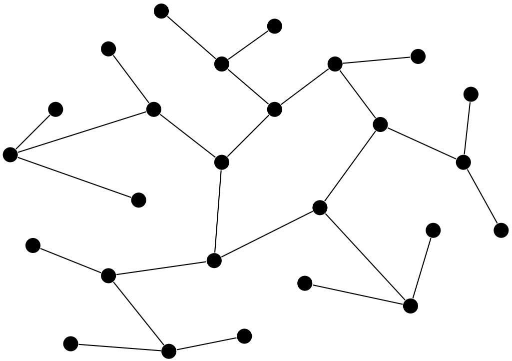
The ℓ-**isogeny graph** has

vertices: supersingular elliptic curves,

edges: isogenies of degree ℓ,

The ℓ-IsogenyPath Problem

Let $\ell \neq p$ be a prime.



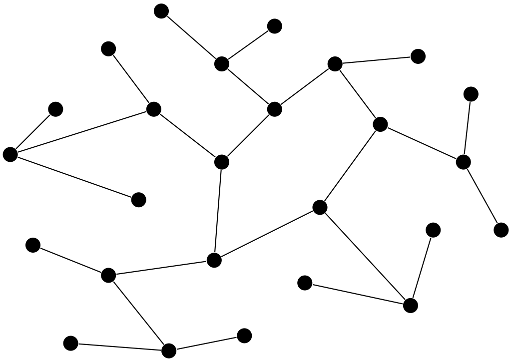
The ℓ-**isogeny graph** has

vertices: supersingular elliptic curves,

edges: isogenies of degree ℓ,
i.e. an isogeny φ such that $\# \ker \varphi = \ell$.

The ℓ-IsogenyPath Problem

Let $\ell \neq p$ be a prime.



The ℓ-**isogeny graph** has

vertices: supersingular elliptic curves,

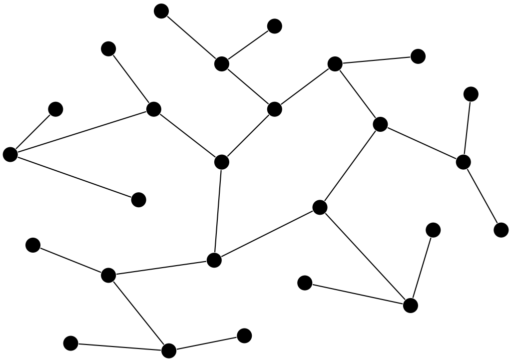
edges: isogenies of degree ℓ,
i.e. an isogeny φ such that $\# \ker \varphi = \ell$.

The ℓ-**isogeny graph** is

- $(\ell + 1)$-**regular**,

The ℓ-IsogenyPath Problem

Let $\ell \neq p$ be a prime.



The ℓ-**isogeny graph** has

vertices: supersingular elliptic curves,

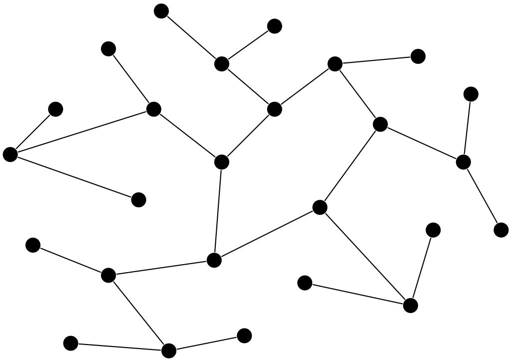
edges: isogenies of degree ℓ,
i.e. an isogeny φ such that $\# \ker \varphi = \ell$.

The ℓ-**isogeny graph** is

- $(\ell + 1)$-**regular**,
- **connected**,

The ℓ-IsogenyPath Problem

Let $\ell \neq p$ be a prime.



The ℓ-**isogeny graph** has

vertices: supersingular elliptic curves,

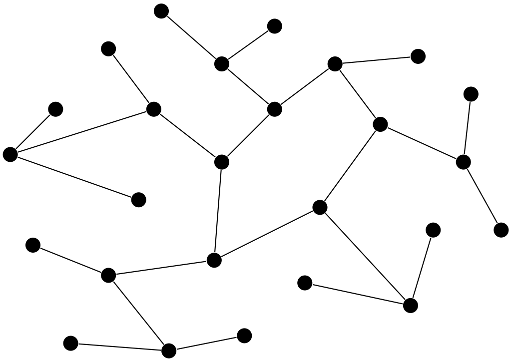
edges: isogenies of degree ℓ,
i.e. an isogeny φ such that $\# \ker \varphi = \ell$.

The ℓ-**isogeny graph** is

- $(\ell + 1)$-**regular**,
- **connected**,
- **rapidly mixing**,

The ℓ-IsogenyPath Problem

Let $\ell \neq p$ be a prime.



The ℓ-**isogeny graph** has

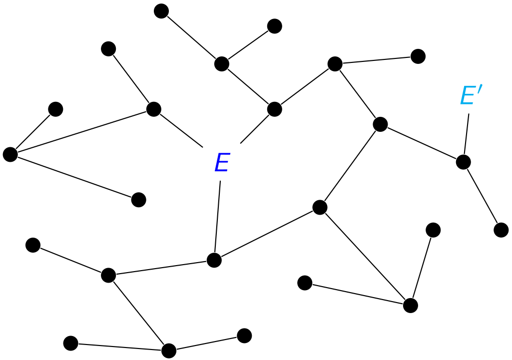
vertices: supersingular elliptic curves,

edges: isogenies of degree ℓ,
i.e. an isogeny φ such that $\# \ker \varphi = \ell$.

The ℓ-**isogeny graph** is

- $(\ell + 1)$-**regular**,
- **connected**,
- **rapidly mixing**,
- **huge** (around $p/12$ vertices).

Let $\ell \neq p$ be a prime.



The ℓ-**isogeny graph** has

vertices: supersingular elliptic curves,

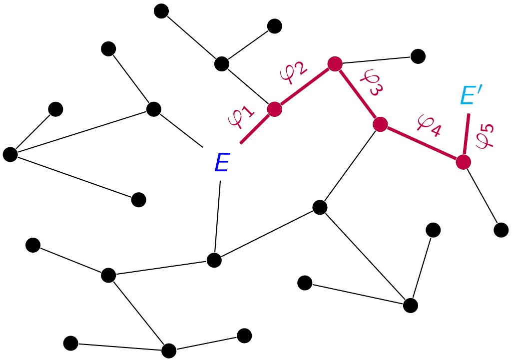
edges: isogenies of degree ℓ,
i.e. an isogeny φ such that $\# \ker \varphi = \ell$.

The ℓ-**isogeny graph** is

- $(\ell + 1)$-**regular**,
- **connected**,
- **rapidly mixing**,
- **huge** (around $p/12$ vertices).

The ℓ-IsogenyPath Problem

Let $\ell \neq p$ be a prime.



The ℓ-**isogeny graph** has

vertices: supersingular elliptic curves,

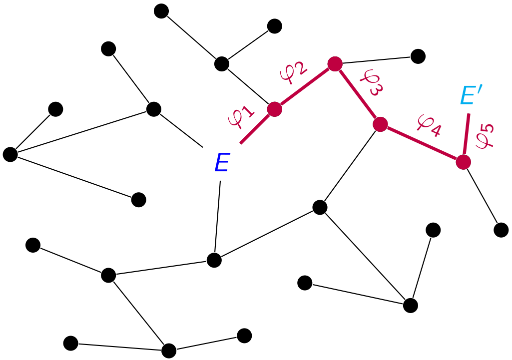
edges: isogenies of degree ℓ,
i.e. an isogeny φ such that $\# \ker \varphi = \ell$.

The ℓ-**isogeny graph** is

- $(\ell + 1)$-**regular**,
- **connected**,
- **rapidly mixing**,
- **huge** (around $p/12$ vertices).

The ℓ-IsogenyPath Problem

Let $\ell \neq p$ be a prime.



The ℓ-**isogeny graph** has

vertices: supersingular elliptic curves,

edges: isogenies of degree ℓ,
i.e. an isogeny φ such that $\# \ker \varphi = \ell$.

The ℓ-**isogeny graph** is

- $(\ell + 1)$-**regular**,
- **connected**,
- **rapidly mixing**,
- **huge** (around $p/12$ vertices).

The ℓ-IsogenyPath Problem

Given two **supersingular elliptic curves** E and E' defined over $\mathbb{F}_{p^2}$, and a prime $\ell \neq p$, find a **path** $\varphi_1 \circ \cdots \circ \varphi_n : E \to E'$ in the ℓ-isogeny graph.

The Endomorphism Ring and Maximal Order Problems

An **endomorphism** is an isogeny from a curve to itself or the zero morphism.

The Endomorphism Ring and Maximal Order Problems

An **endomorphism** is an isogeny from a curve to itself or the zero morphism.
$\text{End}(E) := \{\alpha : E \to E\}$ forms a **ring**.

The Endomorphism Ring and Maximal Order Problems

An **endomorphism** is an isogeny from a curve to itself or the zero morphism.

$\mathrm{End}(E) := \{\alpha : E \to E\}$ forms a **ring**. When E is **supersingular**, $\mathrm{End}(E)$ is a **lattice of dimension 4**.

The Endomorphism Ring and Maximal Order Problems

An **endomorphism** is an isogeny from a curve to itself or the zero morphism.
$\text{End}(E) := \{\alpha : E \to E\}$ forms a **ring**. When E is **supersingular**, $\text{End}(E)$ is a **lattice of dimension 4**.

The Endomorphism Ring Problem (EndRing)

Given $E/\mathbb{F}_{p^2}$, find **four endomorphisms** $\alpha_1, \ldots, \alpha_4 : E \to E$ such that

$$\text{End}(E) = \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z} + \alpha_3\mathbb{Z} + \alpha_4\mathbb{Z}.$$

The Endomorphism Ring and Maximal Order Problems

An **endomorphism** is an isogeny from a curve to itself or the zero morphism.
$\text{End}(E) := \{\alpha : E \to E\}$ forms a **ring**. When E is **supersingular**, $\text{End}(E)$ is a **lattice of dimension 4**.

The Endomorphism Ring Problem (EndRing)

Given $E/\mathbb{F}_{p^2}$, find **four endomorphisms** $\alpha_1, \ldots, \alpha_4 : E \to E$ such that

$$\text{End}(E) = \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z} + \alpha_3\mathbb{Z} + \alpha_4\mathbb{Z}.$$

The Maximal Order Problem (MaxOrder)

Given $E/\mathbb{F}_{p^2}$, find **four quaternions** $\alpha_1, \ldots, \alpha_4$ in $\left(\frac{-p,-q_p}{\mathbb{Q}}\right)^*$ such that

$$\text{End}(E) \simeq \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z} + \alpha_3\mathbb{Z} + \alpha_4\mathbb{Z}.$$

$* : \left(\frac{-p,-q_p}{\mathbb{Q}}\right) = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + ij\mathbb{Q}$ with $i^2 = -p$, $j^2 = -q_p$ and $ij = -ji$.

The Endomorphism Ring and Maximal Order Problems

An **endomorphism** is an isogeny from a curve to itself or the zero morphism.
$\text{End}(E) := \{\alpha : E \to E\}$ forms a **ring**. When E is **supersingular**, $\text{End}(E)$ is a **lattice of dimension 4**.

The Endomorphism Ring Problem (EndRing)

Given $E/\mathbb{F}_{p^2}$, find **four endomorphisms** $\alpha_1, \ldots, \alpha_4 : E \to E$ such that

$$\text{End}(E) = \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z} + \alpha_3\mathbb{Z} + \alpha_4\mathbb{Z}.$$

The Maximal Order Problem (MaxOrder)

Given $E/\mathbb{F}_{p^2}$, find **four quaternions** $\alpha_1, \ldots, \alpha_4$ in $\left(\frac{-p,-q_p}{\mathbb{Q}}\right)^*$ such that

$$\text{End}(E) \simeq \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z} + \alpha_3\mathbb{Z} + \alpha_4\mathbb{Z}.$$

$\text{End}(E)$	a maximal order $\mathcal{O}$ in $\left(\frac{-p,-q_p}{\mathbb{Q}}\right)$

Deuring correspondence in a nutshell

$*$: $\left(\frac{-p,-q_p}{\mathbb{Q}}\right) = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + ij\mathbb{Q}$ with $i^2 = -p$, $j^2 = -q_p$ and $ij = -ji$.

The Endomorphism Ring and Maximal Order Problems

An **endomorphism** is an isogeny from a curve to itself or the zero morphism.
$\mathrm{End}(E) := \{\alpha : E \to E\}$ forms a **ring**. When E is **supersingular**, $\mathrm{End}(E)$ is a **lattice of dimension 4**.

The Endomorphism Ring Problem (EndRing)

Given $E/\mathbb{F}_{p^2}$, find **four endomorphisms** $\alpha_1, \ldots, \alpha_4 : E \to E$ such that

$$\mathrm{End}(E) = \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z} + \alpha_3\mathbb{Z} + \alpha_4\mathbb{Z}.$$

The Maximal Order Problem (MaxOrder)

Given $E/\mathbb{F}_{p^2}$, find **four quaternions** $\alpha_1, \ldots, \alpha_4$ in $\left(\frac{-p,-q_p}{\mathbb{Q}}\right)^*$ such that

$$\mathrm{End}(E) \simeq \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z} + \alpha_3\mathbb{Z} + \alpha_4\mathbb{Z}.$$

$\mathrm{End}(E)$	a maximal order $\mathcal{O}$ in $\left(\frac{-p,-q_p}{\mathbb{Q}}\right)$
$\varphi : E_1 \to E_2$	

Deuring correspondence in a nutshell

$* : \left(\frac{-p,-q_p}{\mathbb{Q}}\right) = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + ij\mathbb{Q}$ with $i^2 = -p$, $j^2 = -q_p$ and $ij = -ji$.

The Endomorphism Ring and Maximal Order Problems

An **endomorphism** is an isogeny from a curve to itself or the zero morphism.
$\mathrm{End}(E) := \{\alpha : E \to E\}$ forms a **ring**. When E is **supersingular**, $\mathrm{End}(E)$ is a **lattice of dimension 4**.

The Endomorphism Ring Problem (EndRing)

Given $E/\mathbb{F}_{p^2}$, find **four endomorphisms** $\alpha_1, \ldots, \alpha_4 : E \to E$ such that

$$\mathrm{End}(E) = \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z} + \alpha_3\mathbb{Z} + \alpha_4\mathbb{Z}.$$

The Maximal Order Problem (MaxOrder)

Given $E/\mathbb{F}_{p^2}$, find **four quaternions** $\alpha_1, \ldots, \alpha_4$ in $\left(\frac{-p,-q_p}{\mathbb{Q}}\right)^*$ such that

$$\mathrm{End}(E) \simeq \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z} + \alpha_3\mathbb{Z} + \alpha_4\mathbb{Z}.$$

$\mathrm{End}(E)$	a maximal order $\mathcal{O}$ in $\left(\frac{-p,-q_p}{\mathbb{Q}}\right)$
$\varphi : E_1 \to E_2$	I_φ left $\mathcal{O}_1$-ideal and right $\mathcal{O}_2$-ideal

Deuring correspondence in a nutshell

$* : \left(\frac{-p,-q_p}{\mathbb{Q}}\right) = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + ij\mathbb{Q}$ with $i^2 = -p$, $j^2 = -q_p$ and $ij = -ji$.

The Endomorphism Ring and Maximal Order Problems

An **endomorphism** is an isogeny from a curve to itself or the zero morphism.
$\mathrm{End}(E) := \{\alpha : E \to E\}$ forms a **ring**. When E is **supersingular**, $\mathrm{End}(E)$ is a **lattice of dimension 4**.

The Endomorphism Ring Problem (EndRing)

Given $E/\mathbb{F}_{p^2}$, find **four endomorphisms** $\alpha_1, \ldots, \alpha_4 : E \to E$ such that

$$\mathrm{End}(E) = \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z} + \alpha_3\mathbb{Z} + \alpha_4\mathbb{Z}.$$

The Maximal Order Problem (MaxOrder)

Given $E/\mathbb{F}_{p^2}$, find **four quaternions** $\alpha_1, \ldots, \alpha_4$ in $\left(\frac{-p,-q_p}{\mathbb{Q}}\right)^*$ such that

$$\mathrm{End}(E) \simeq \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z} + \alpha_3\mathbb{Z} + \alpha_4\mathbb{Z}.$$

$\mathrm{End}(E)$	a maximal order $\mathcal{O}$ in $\left(\frac{-p,-q_p}{\mathbb{Q}}\right)$
$\varphi : E_1 \to E_2$	I_φ left $\mathcal{O}_1$-ideal and right $\mathcal{O}_2$-ideal
$\deg \varphi$	

Deuring correspondence in a nutshell

$* : \left(\frac{-p,-q_p}{\mathbb{Q}}\right) = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + ij\mathbb{Q}$ with $i^2 = -p$, $j^2 = -q_p$ and $ij = -ji$.

The Endomorphism Ring and Maximal Order Problems

An **endomorphism** is an isogeny from a curve to itself or the zero morphism.
$\mathrm{End}(E) := \{\alpha : E \to E\}$ forms a **ring**. When E is **supersingular**, $\mathrm{End}(E)$ is a **lattice of dimension 4**.

The Endomorphism Ring Problem (EndRing)

Given $E/\mathbb{F}_{p^2}$, find **four endomorphisms** $\alpha_1, \ldots, \alpha_4 : E \to E$ such that

$$\mathrm{End}(E) = \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z} + \alpha_3\mathbb{Z} + \alpha_4\mathbb{Z}.$$

The Maximal Order Problem (MaxOrder)

Given $E/\mathbb{F}_{p^2}$, find **four quaternions** $\alpha_1, \ldots, \alpha_4$ in $\left(\frac{-p,-q_p}{\mathbb{Q}}\right)^*$ such that

$$\mathrm{End}(E) \simeq \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z} + \alpha_3\mathbb{Z} + \alpha_4\mathbb{Z}.$$

$\mathrm{End}(E)$	a maximal order $\mathcal{O}$ in $\left(\frac{-p,-q_p}{\mathbb{Q}}\right)$
$\varphi : E_1 \to E_2$	I_φ left $\mathcal{O}_1$-ideal and right $\mathcal{O}_2$-ideal
$\deg \varphi$	norm of I

Deuring correspondence in a nutshell

$* : \left(\frac{-p,-q_p}{\mathbb{Q}}\right) = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + ij\mathbb{Q}$ with $i^2 = -p$, $j^2 = -q_p$ and $ij = -ji$.

The Endomorphism Ring and Maximal Order Problems

An **endomorphism** is an isogeny from a curve to itself or the zero morphism.
$\text{End}(E) := \{\alpha : E \to E\}$ forms a **ring**. When E is **supersingular**, $\text{End}(E)$ is a **lattice of dimension 4**.

The Endomorphism Ring Problem (`EndRing`)

Given $E/\mathbb{F}_{p^2}$, find **four endomorphisms** $\alpha_1, \ldots, \alpha_4 : E \to E$ such that

$$\text{End}(E) = \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z} + \alpha_3\mathbb{Z} + \alpha_4\mathbb{Z}.$$

The Maximal Order Problem (`MaxOrder`)

Given $E/\mathbb{F}_{p^2}$, find **four quaternions** $\alpha_1, \ldots, \alpha_4$ in $\left(\frac{-p,-q_p}{\mathbb{Q}}\right)^*$ such that

$$\text{End}(E) \simeq \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z} + \alpha_3\mathbb{Z} + \alpha_4\mathbb{Z}.$$

$\text{End}(E)$	a maximal order $\mathcal{O}$ in $\left(\frac{-p,-q_p}{\mathbb{Q}}\right)$
$\varphi : E_1 \to E_2$	I_φ left $\mathcal{O}_1$-ideal and right $\mathcal{O}_2$-ideal
$\deg \varphi$	norm of I
$\varphi \circ \psi$	

Deuring correspondence in a nutshell

$* : \left(\frac{-p,-q_p}{\mathbb{Q}}\right) = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + ij\mathbb{Q}$ with $i^2 = -p$, $j^2 = -q_p$ and $ij = -ji$.

The Endomorphism Ring and Maximal Order Problems

An **endomorphism** is an isogeny from a curve to itself or the zero morphism.
$\mathrm{End}(E) := \{\alpha : E \to E\}$ forms a **ring**. When E is **supersingular**, $\mathrm{End}(E)$ is a **lattice of dimension 4**.

The Endomorphism Ring Problem (EndRing)

Given $E/\mathbb{F}_{p^2}$, find **four endomorphisms** $\alpha_1, \ldots, \alpha_4 : E \to E$ such that

$$\mathrm{End}(E) = \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z} + \alpha_3\mathbb{Z} + \alpha_4\mathbb{Z}.$$

The Maximal Order Problem (MaxOrder)

Given $E/\mathbb{F}_{p^2}$, find **four quaternions** $\alpha_1, \ldots, \alpha_4$ in $\left(\frac{-p,-q_p}{\mathbb{Q}}\right)^*$ such that

$$\mathrm{End}(E) \simeq \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z} + \alpha_3\mathbb{Z} + \alpha_4\mathbb{Z}.$$

$\mathrm{End}(E)$	a maximal order $\mathcal{O}$ in $\left(\frac{-p,-q_p}{\mathbb{Q}}\right)$
$\varphi : E_1 \to E_2$	I_φ left $\mathcal{O}_1$-ideal and right $\mathcal{O}_2$-ideal
$\deg \varphi$	norm of I
$\varphi \circ \psi$	$I_{\varphi\circ\psi} = I_\psi \cdot I_\varphi$

Deuring correspondence in a nutshell

$* : \left(\frac{-p,-q_p}{\mathbb{Q}}\right) = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + ij\mathbb{Q}$ with $i^2 = -p$, $j^2 = -q_p$ and $ij = -ji$.

The Endomorphism Ring and Maximal Order Problems

An **endomorphism** is an isogeny from a curve to itself or the zero morphism.
$\mathrm{End}(E) := \{\alpha : E \to E\}$ forms a **ring**. When E is **supersingular**, $\mathrm{End}(E)$ is a **lattice of dimension 4**.

The Endomorphism Ring Problem (EndRing)

Given $E/\mathbb{F}_{p^2}$, find **four endomorphisms** $\alpha_1, \dots, \alpha_4 : E \to E$ such that

$$\mathrm{End}(E) = \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z} + \alpha_3\mathbb{Z} + \alpha_4\mathbb{Z}.$$

The Maximal Order Problem (MaxOrder)

Given $E/\mathbb{F}_{p^2}$, find **four quaternions** $\alpha_1, \dots, \alpha_4$ in $\left(\frac{-p,-q_p}{\mathbb{Q}}\right)^*$ such that

$$\mathrm{End}(E) \simeq \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z} + \alpha_3\mathbb{Z} + \alpha_4\mathbb{Z}.$$

	$\mathrm{End}(E)$	a maximal order $\mathcal{O}$ in $\left(\frac{-p,-q_p}{\mathbb{Q}}\right)$
Hard to compute $\to$	$\varphi : E_1 \to E_2$	I_φ left $\mathcal{O}_1$-ideal and right $\mathcal{O}_2$-ideal
	$\deg \varphi$	norm of I
	$\varphi \circ \psi$	$I_{\varphi\circ\psi} = I_\psi \cdot I_\varphi$

Deuring correspondence in a nutshell

$* : \left(\frac{-p,-q_p}{\mathbb{Q}}\right) = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + ij\mathbb{Q}$ with $i^2 = -p$, $j^2 = -q_p$ and $ij = -ji$.

The Endomorphism Ring and Maximal Order Problems

An **endomorphism** is an isogeny from a curve to itself or the zero morphism.
$\text{End}(E) := \{\alpha : E \to E\}$ forms a **ring**. When E is **supersingular**, $\text{End}(E)$ is a **lattice of dimension 4**.

The Endomorphism Ring Problem (EndRing)

Given $E/\mathbb{F}_{p^2}$, find **four endomorphisms** $\alpha_1, \ldots, \alpha_4 : E \to E$ such that

$$\text{End}(E) = \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z} + \alpha_3\mathbb{Z} + \alpha_4\mathbb{Z}.$$

The Maximal Order Problem (MaxOrder)

Given $E/\mathbb{F}_{p^2}$, find **four quaternions** $\alpha_1, \ldots, \alpha_4$ in $\left(\frac{-p,-q_p}{\mathbb{Q}}\right)^*$ such that

$$\text{End}(E) \simeq \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z} + \alpha_3\mathbb{Z} + \alpha_4\mathbb{Z}.$$

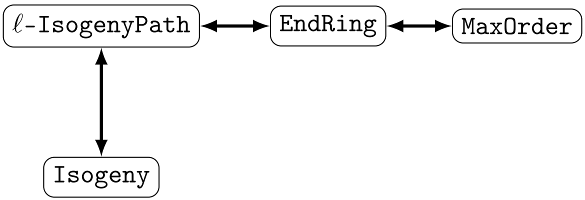
$\text{End}(E)$	a maximal order $\mathcal{O}$ in $\left(\frac{-p,-q_p}{\mathbb{Q}}\right)$
$\varphi : E_1 \to E_2$	I_φ left $\mathcal{O}_1$-ideal and right $\mathcal{O}_2$-ideal
$\deg \varphi$	norm of I
$\varphi \circ \psi$	$I_{\varphi\circ\psi} = I_\psi \cdot I_\varphi$

Hard to compute → (left column: $\varphi : E_1 \to E_2$) ← **Easy to compute** (right column: I_φ)

Deuring correspondence in a nutshell

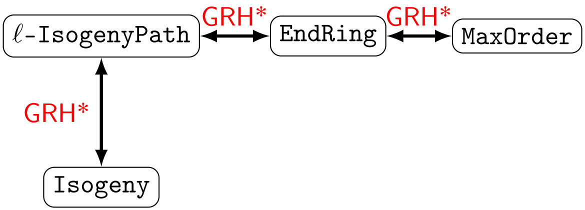
$* : \left(\frac{-p,-q_p}{\mathbb{Q}}\right) = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + ij\mathbb{Q}$ with $i^2 = -p$, $j^2 = -q_p$ and $ij = -ji$.

Previous state-of-the-art



Polynomial reductions between isogeny-based problems

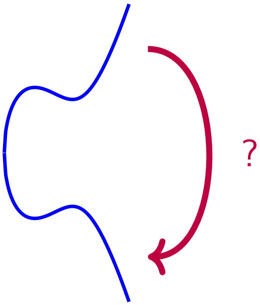
Previous state-of-the-art

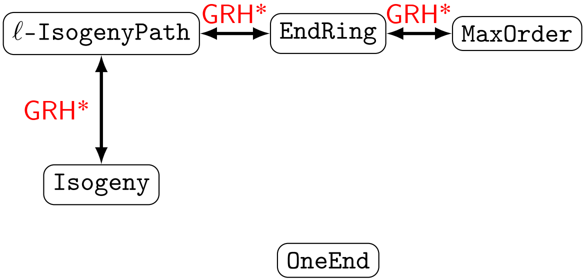


Polynomial reductions between isogeny-based problems

*: Proven under heuristics [Eis+18] then under the Generalised Riemann Hypothesis [Wes22].

One Endomorphism problem

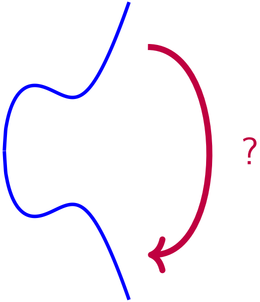


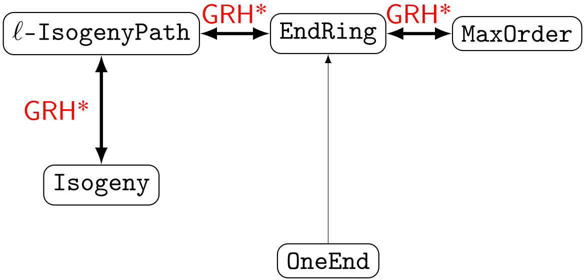


Polynomial reductions between isogeny-based problems

*: Proven under heuristics [Eis+18] then under the Generalised Riemann Hypothesis [Wes22].

One Endomorphism problem

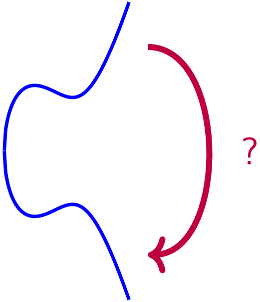


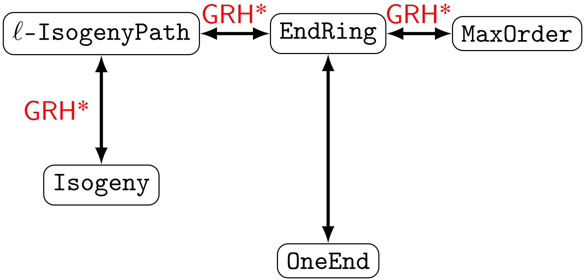


Polynomial reductions between isogeny-based problems

*: Proven under heuristics [Eis+18] then under the Generalised Riemann Hypothesis [Wes22].

One Endomorphism problem

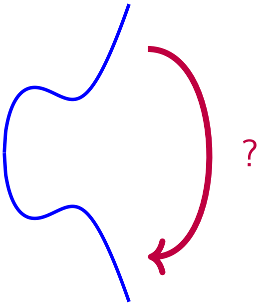


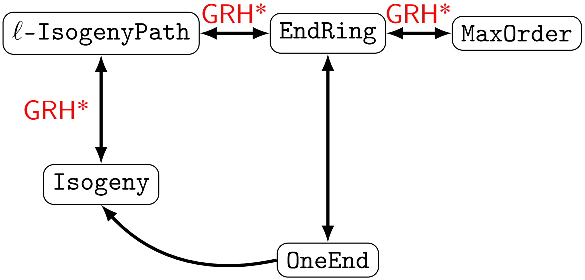


Polynomial reductions between isogeny-based problems

*: Proven under heuristics [Eis+18] then under the Generalised Riemann Hypothesis [Wes22].

One Endomorphism problem

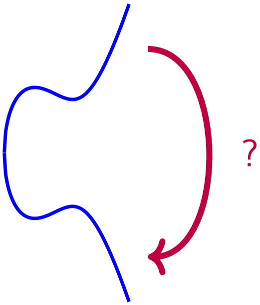


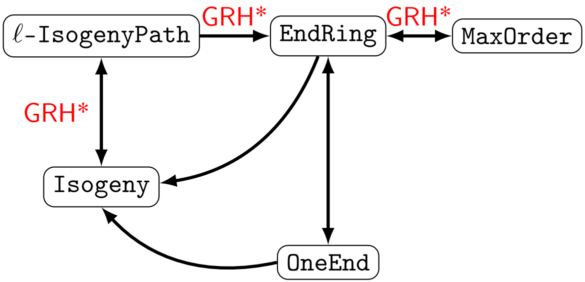


Polynomial reductions between isogeny-based problems

*: Proven under heuristics [Eis+18] then under the Generalised Riemann Hypothesis [Wes22].

One Endomorphism problem

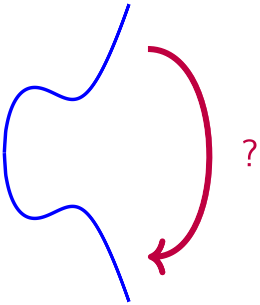


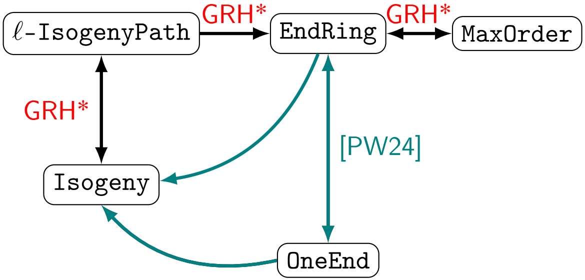


Polynomial reductions between isogeny-based problems

*: Proven under heuristics [Eis+18] then under the Generalised Riemann Hypothesis [Wes22].

One Endomorphism problem



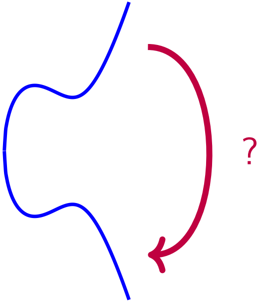


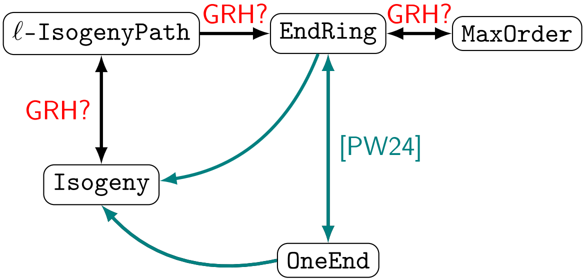
Polynomial reductions between isogeny-based problems

*: Proven under heuristics [Eis+18] then under the Generalised Riemann Hypothesis [Wes22].

Previous state-of-the-art

One Endomorphism problem



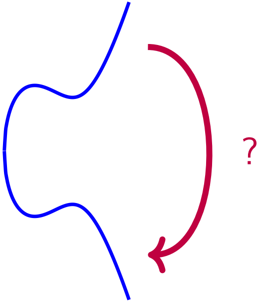


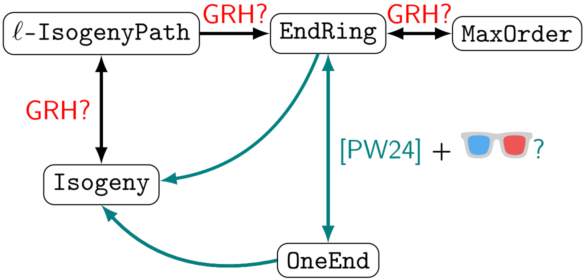
Polynomial reductions between isogeny-based problems

*: Proven under heuristics [Eis+18] then under the Generalised Riemann Hypothesis [Wes22].

Previous state-of-the-art

One Endomorphism problem





Polynomial reductions between isogeny-based problems

*: Proven under heuristics [Eis+18] then under the Generalised Riemann Hypothesis [Wes22].

: higher dimensional results following SIDH's attacks [CD23; Mai+23; Rob23]

Why consider such a variety of problems?

OneEnd

EndRing

Why consider such a variety of problems?

Good for security proofs

OneEnd

EndRing

Why consider such a variety of problems?

Good for security proofs

`OneEnd`

Good for attacks

`EndRing`

Why consider such a variety of problems?

Good for security proofs

`OneEnd`

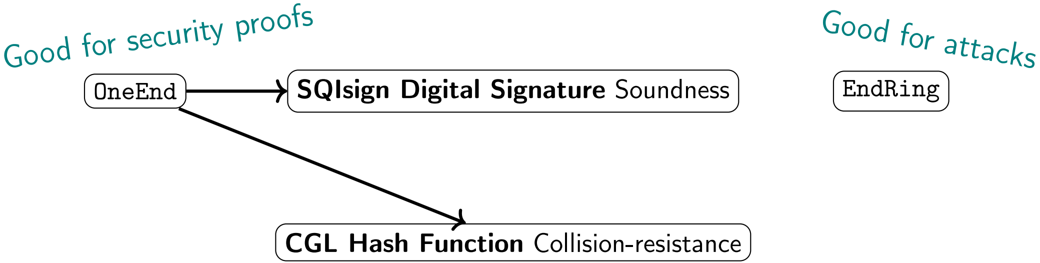
SQIsign Digital Signature Soundness

Good for attacks

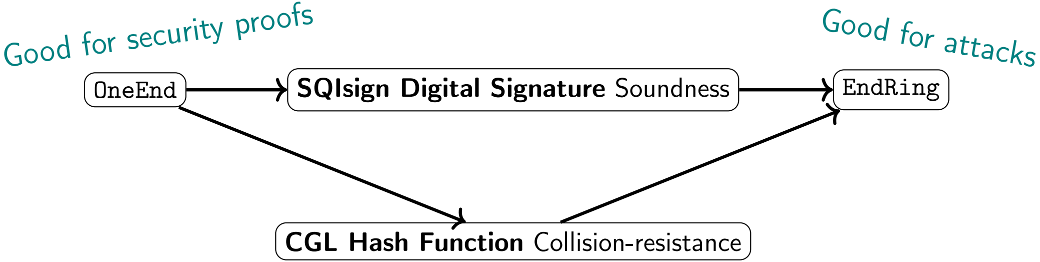
`EndRing`

CGL Hash Function Collision-resistance

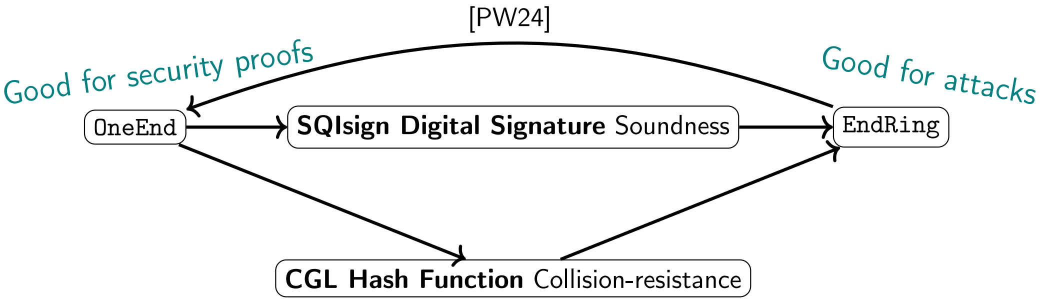
Why consider such a variety of problems?



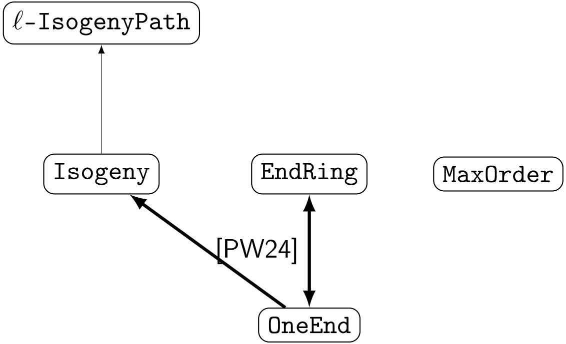
Why consider such a variety of problems?



Why consider such a variety of problems?

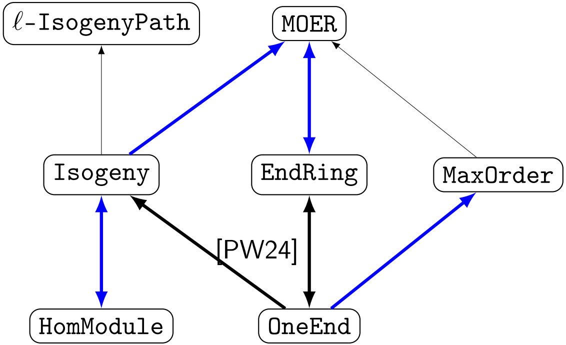


Equivalences **without GRH**



Polynomial reductions between isogeny-based problems **without GRH**

Equivalences **without GRH**

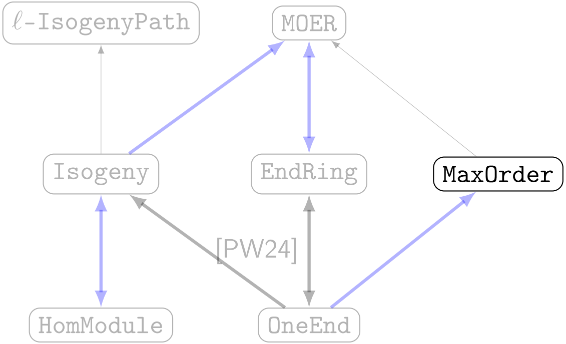


Polynomial reductions between isogeny-based problems **without GRH**

The Maximal Order Problem (MaxOrder)

Given $E/\mathbb{F}_{p^2}$, find **four quaternions** $\alpha_1, \dots, \alpha_4$ in $\left(\frac{-p,-q_p}{\mathbb{Q}}\right)$ such that

$$\mathrm{End}(E) \simeq \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z} + \alpha_3\mathbb{Z} + \alpha_4\mathbb{Z}.$$

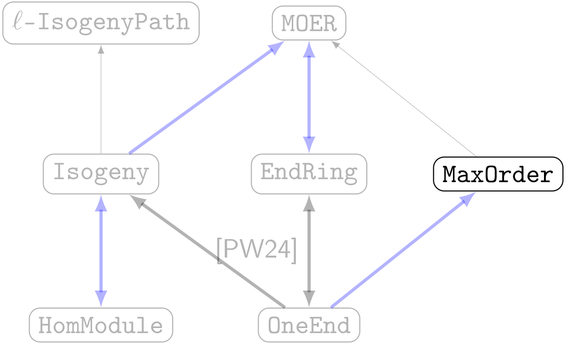


Polynomial reductions between isogeny-based problems **without GRH**

The Maximal Order Problem (MaxOrder)

Given $E/\mathbb{F}_{p^2}$, find **four quaternions** $\alpha_1, \ldots, \alpha_4$ in $\left(\frac{-p,-q_p}{\mathbb{Q}}\right)$ such that

$$\mathrm{End}(E) \simeq \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z} + \alpha_3\mathbb{Z} + \alpha_4\mathbb{Z}.$$



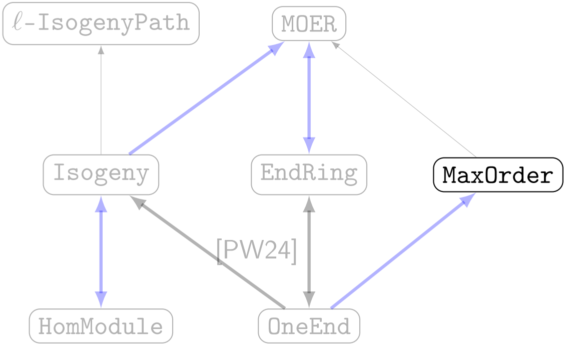
Polynomial reductions between isogeny-based problems **without GRH**

Equivalences **without GRH**

The MaxOrder Problem (MaxOrder)

Given $E/\mathbb{F}_{p^2}$, compute
two integers $a, b \in \mathbb{Z}_{>0}$ and
four quaternions $\alpha_1, \ldots, \alpha_4$ in $\left(\frac{-a,-b}{\mathbb{Q}}\right)$
such that

$$\mathrm{End}(E) \simeq \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z} + \alpha_3\mathbb{Z} + \alpha_4\mathbb{Z}.$$



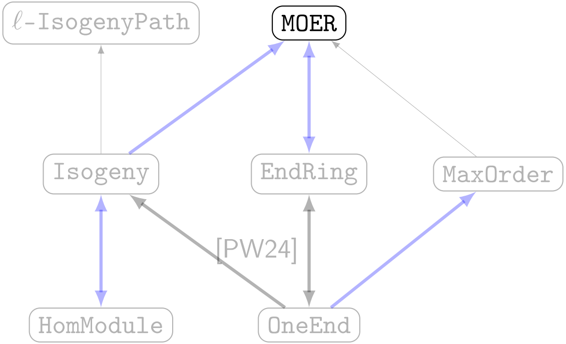
Polynomial reductions between isogeny-based problems **without GRH**

Equivalences **without GRH**

The MaxOrder + EndRing Problem (MOER)

Given $E/\mathbb{F}_{p^2}$, compute
two integers $a, b \in \mathbb{Z}_{>0}$ and
four quaternions $\alpha_1, \ldots, \alpha_4$ in $\left(\frac{-a,-b}{\mathbb{Q}}\right)$
and **an isomorphism**

$$\varepsilon : \mathrm{End}(E) \xrightarrow{\sim} \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z} + \alpha_3\mathbb{Z} + \alpha_4\mathbb{Z}.$$



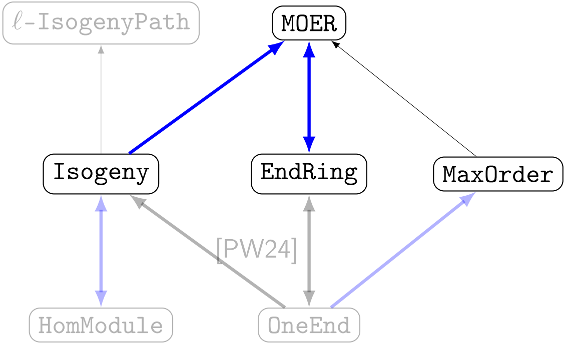
Polynomial reductions between isogeny-based problems **without GRH**

Equivalences **without GRH**

The MaxOrder + EndRing Problem (MOER)

Given $E/\mathbb{F}_{p^2}$, compute
two integers $a, b \in \mathbb{Z}_{>0}$ and
four quaternions $\alpha_1, \ldots, \alpha_4$ in $\left(\frac{-a,-b}{\mathbb{Q}}\right)$
and **an isomorphism**

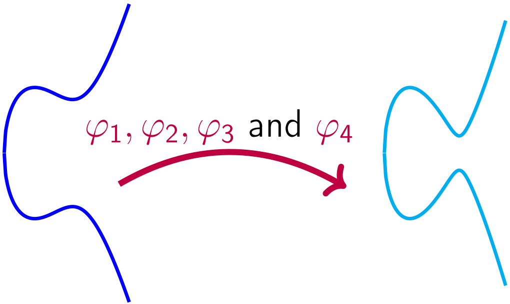
$$\varepsilon : \mathrm{End}(E) \xrightarrow{\sim} \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z} + \alpha_3\mathbb{Z} + \alpha_4\mathbb{Z}.$$

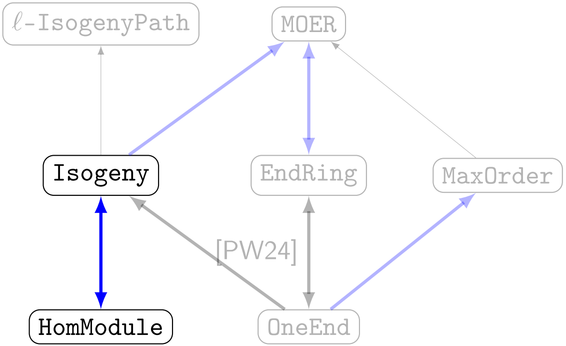


Polynomial reductions between isogeny-based problems **without GRH**

Adding a new problem

Homomorphism Module Problem



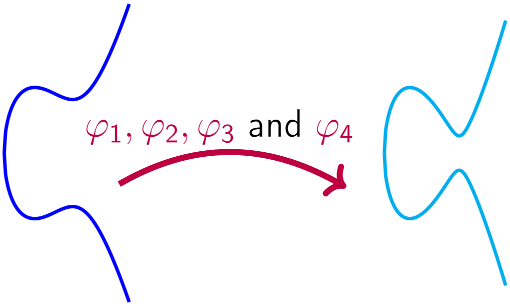


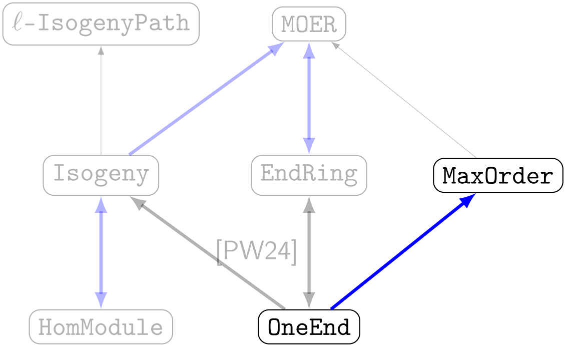
$$\mathrm{Hom}(\ ,\ ) = \varphi_1\mathbb{Z} + \varphi_2\mathbb{Z} + \varphi_3\mathbb{Z} + \varphi_4\mathbb{Z}$$

Polynomial reductions between isogeny-based problems **without GRH**

Adding a new problem

Homomorphism Module Problem





$$\mathrm{Hom}(\;,\;) = \varphi_1\mathbb{Z} + \varphi_2\mathbb{Z} + \varphi_3\mathbb{Z} + \varphi_4\mathbb{Z}$$

Polynomial reductions between isogeny-based problems **without GRH**

Reducing `OneEnd` to `MaxOrder`

Goal: Compute a non-scalar endomorphism $\alpha \in \text{End}(E) \backslash \mathbb{Z}$ given a `MaxOrder` oracle.

Reducing OneEnd to MaxOrder

Goal: Compute a non-scalar endomorphism $\alpha \in \mathrm{End}(E)\backslash\mathbb{Z}$ given a MaxOrder oracle.

Idea: $\mathcal{O} \overset{\varepsilon}{\simeq} \mathrm{End}(E)$

Reducing OneEnd to MaxOrder

Goal: Compute a non-scalar endomorphism $\alpha \in \mathrm{End}(E) \backslash \mathbb{Z}$ given a MaxOrder oracle.

Idea: Choose a non-scalar $\beta \in \mathcal{O} \overset{\varepsilon}{\simeq} \mathrm{End}(E)$

Reducing OneEnd to MaxOrder

Goal: Compute a non-scalar endomorphism $\alpha \in \mathrm{End}(E) \backslash \mathbb{Z}$ given a MaxOrder oracle.

Idea: Choose a non-scalar $\beta \in \mathcal{O} \overset{\varepsilon}{\simeq} \mathrm{End}(E)$ and compute $\alpha = \varepsilon(\beta)$.

Reducing `OneEnd` to `MaxOrder`

Goal: Compute a non-scalar endomorphism $\alpha \in \mathrm{End}(E) \backslash \mathbb{Z}$ given a `MaxOrder` oracle.

Idea: Choose a non-scalar $\beta \in \mathcal{O} \overset{\varepsilon}{\simeq} \mathrm{End}(E)$ and compute $\alpha = \varepsilon(\beta)$. We don't know ε...

Reducing OneEnd to MaxOrder

Goal: Compute a non-scalar endomorphism $\alpha \in \mathrm{End}(E) \backslash \mathbb{Z}$ given a MaxOrder oracle.

Idea: Choose a non-scalar $\beta \in \mathcal{O} \overset{\varepsilon}{\simeq} \mathrm{End}(E)$ and compute $\alpha = \varepsilon(\beta)$. We don't know ε...

Step 1: Compute a "local" correspondence between isogenies and ideals for a small prime ℓ.

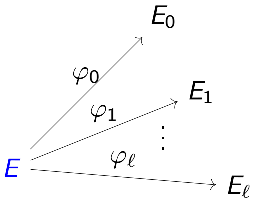
E

Reducing OneEnd to MaxOrder

Goal: Compute a non-scalar endomorphism $\alpha \in \mathrm{End}(E) \backslash \mathbb{Z}$ given a MaxOrder oracle.

Idea: Choose a non-scalar $\beta \in \mathcal{O} \overset{\varepsilon}{\simeq} \mathrm{End}(E)$ and compute $\alpha = \varepsilon(\beta)$. We don't know ε...

Step 1: Compute a "local" correspondence between isogenies and ideals for a small prime ℓ.



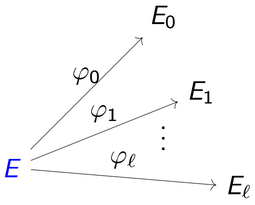
Compute all the isogenies of degree ℓ from E

Reducing `OneEnd` to `MaxOrder`

Goal: Compute a non-scalar endomorphism $\alpha \in \mathrm{End}(E) \backslash \mathbb{Z}$ given a `MaxOrder` oracle.

Idea: Choose a non-scalar $\beta \in \mathcal{O} \overset{\varepsilon}{\simeq} \mathrm{End}(E)$ and compute $\alpha = \varepsilon(\beta)$. We don't know ε...

Step 1: Compute a "local" correspondence between isogenies and ideals for a small prime ℓ.



Compute all the isogenies of degree ℓ from E

$\mathcal{O} \simeq \mathrm{End}(E)$

$\mathcal{O}_0 \simeq \mathrm{End}(E_0)$

$\mathcal{O}_1 \simeq \mathrm{End}(E_1)$

$\vdots$

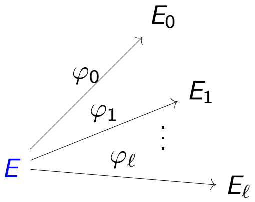
$\mathcal{O}_\ell \simeq \mathrm{End}(E_\ell)$

Reducing `OneEnd` to `MaxOrder`

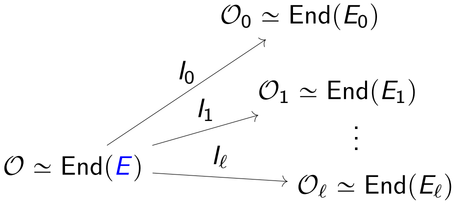
Goal: Compute a non-scalar endomorphism $\alpha \in \mathrm{End}(E) \backslash \mathbb{Z}$ given a `MaxOrder` oracle.

Idea: Choose a non-scalar $\beta \in \mathcal{O} \overset{\varepsilon}{\simeq} \mathrm{End}(E)$ and compute $\alpha = \varepsilon(\beta)$. We don't know ε...

<u>**Step 1:**</u> Compute a "local" correspondence between isogenies and ideals for a small prime ℓ.



Compute all the isogenies of degree ℓ from E

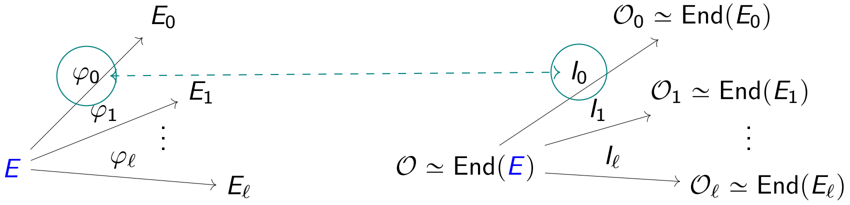


Connect all the maximal orders with ideals of norm ℓ

Goal: Compute a non-scalar endomorphism $\alpha \in \mathrm{End}(E) \backslash \mathbb{Z}$ given a MaxOrder oracle.

Idea: Choose a non-scalar $\beta \in \mathcal{O} \overset{\varepsilon}{\simeq} \mathrm{End}(E)$ and compute $\alpha = \varepsilon(\beta)$. We don't know ε...

Step 1: Compute a "local" correspondence between isogenies and ideals for a small prime ℓ.



Compute all the isogenies of degree ℓ from E

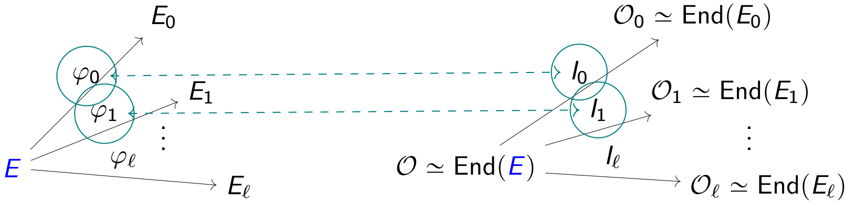
Connect all the maximal orders with ideals of norm ℓ

Reducing OneEnd to MaxOrder

Goal: Compute a non-scalar endomorphism $\alpha \in \mathrm{End}(E) \backslash \mathbb{Z}$ given a MaxOrder oracle.

Idea: Choose a non-scalar $\beta \in \mathcal{O} \overset{\varepsilon}{\simeq} \mathrm{End}(E)$ and compute $\alpha = \varepsilon(\beta)$. We don't know ε...

Step 1: Compute a "local" correspondence between isogenies and ideals for a small prime ℓ.



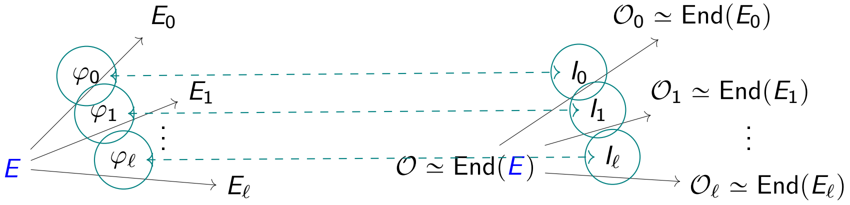
Compute all the isogenies of degree ℓ from E

Connect all the maximal orders with ideals of norm ℓ

Goal: Compute a non-scalar endomorphism $\alpha \in \mathrm{End}(E) \backslash \mathbb{Z}$ given a MaxOrder oracle.

Idea: Choose a non-scalar $\beta \in \mathcal{O} \overset{\varepsilon}{\simeq} \mathrm{End}(E)$ and compute $\alpha = \varepsilon(\beta)$. We don't know ε...

Step 1: Compute a "local" correspondence between isogenies and ideals for a small prime ℓ.



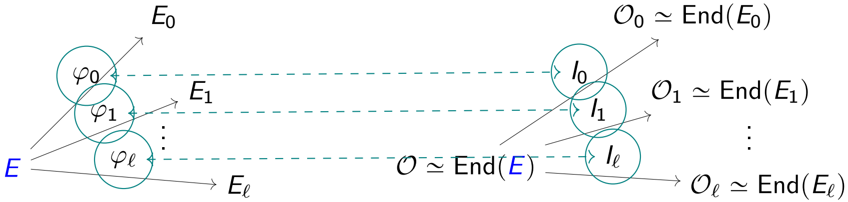
Compute all the isogenies of degree ℓ from E

Connect all the maximal orders with ideals of norm ℓ

Goal: Compute a non-scalar endomorphism $\alpha \in \mathrm{End}(E)\backslash\mathbb{Z}$ given a MaxOrder oracle.

Idea: Choose a non-scalar $\beta \in \mathcal{O} \overset{\varepsilon}{\simeq} \mathrm{End}(E)$ and compute $\alpha = \varepsilon(\beta)$. We don't know ε...

Step 1: Compute a "local" correspondence between isogenies and ideals for a small prime ℓ.



Compute all the isogenies of degree ℓ from E

Connect all the maximal orders with ideals of norm ℓ

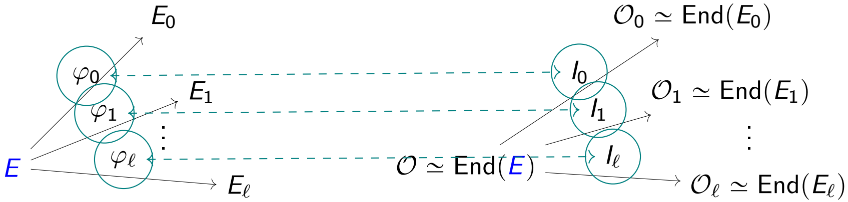
Step 2: Compute a "local" isomorphism $\varepsilon_\ell : \mathcal{O}/\ell\mathcal{O} \xrightarrow{\sim} \mathrm{End}(E[\ell])$.

Reducing OneEnd to MaxOrder

Goal: Compute a non-scalar endomorphism $\alpha \in \mathrm{End}(E)\backslash\mathbb{Z}$ given a `MaxOrder` oracle.

Idea: Choose a non-scalar $\beta \in \mathcal{O} \overset{\varepsilon}{\simeq} \mathrm{End}(E)$ and compute $\alpha = \varepsilon(\beta)$. We don't know ε...

Step 1: Compute a "local" correspondence between isogenies and ideals for a small prime ℓ.



Compute all the isogenies of degree ℓ from E

Connect all the maximal orders with ideals of norm ℓ

Step 2: Compute a "local" isomorphism $\varepsilon_\ell : \mathcal{O}/\ell\mathcal{O} \xrightarrow{\sim} \mathrm{End}(E[\ell])$.

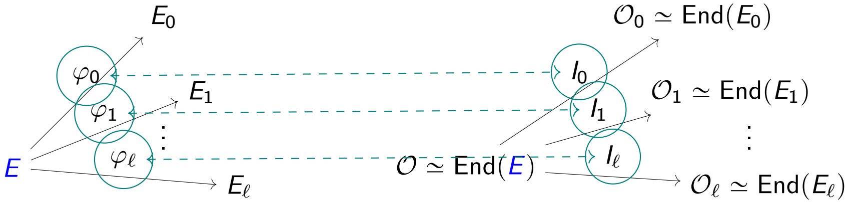
$$\forall \gamma \in \mathcal{O}, \forall P \in E \text{ of order } \ell, \text{we have that } \varepsilon_\ell(\gamma)(P) = \varepsilon(\gamma)(P).$$

Reducing OneEnd to MaxOrder

Goal: Compute a non-scalar endomorphism $\alpha \in \mathrm{End}(E)\backslash\mathbb{Z}$ given a MaxOrder oracle.

Idea: Choose a non-scalar $\beta \in \mathcal{O} \overset{\varepsilon}{\simeq} \mathrm{End}(E)$ and compute $\alpha = \varepsilon(\beta)$. We don't know ε...

Step 1: Compute a "local" correspondence between isogenies and ideals for a small prime ℓ.



Compute all the isogenies of degree ℓ from E

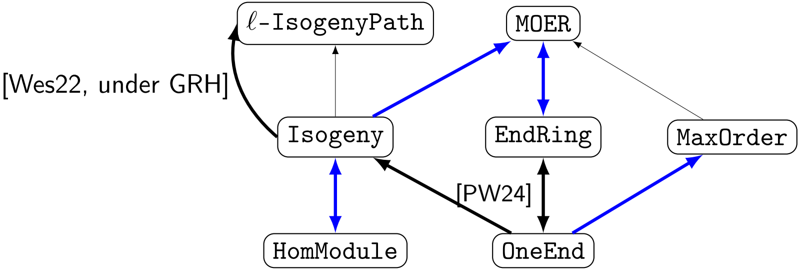
Connect all the maximal orders with ideals of norm ℓ

Step 2: Compute a "local" isomorphism $\varepsilon_\ell : \mathcal{O}/\ell\mathcal{O} \xrightarrow{\sim} \mathrm{End}(E[\ell])$.

$$\forall \gamma \in \mathcal{O}, \forall P \in E \text{ of order } \ell, \text{we have that } \varepsilon_\ell(\gamma)(P) = \varepsilon(\gamma)(P).$$

Step 3: Interpolate $\alpha = \varepsilon(\beta)$ from its evaluations on many small points.

New state-of-the-art

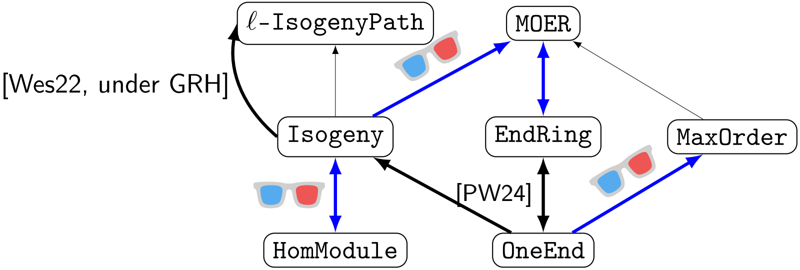


Polynomial reductions between isogeny-based problems.

Theorem (This paper)

The **Isogeny**, **EndRing**, **MaxOrder**, **OneEnd**, **MOER** *and* **HomModule** *problems are equivalent under classical probabilistic polynomial reductions.*

New state-of-the-art



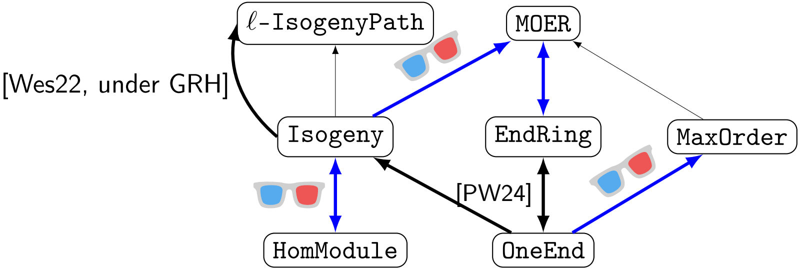
Polynomial reductions between isogeny-based problems.

Theorem (This paper)

The **Isogeny**, **EndRing**, **MaxOrder**, **OneEnd**, **MOER** *and* **HomModule** *problems are equivalent under classical probabilistic polynomial reductions.*

: HD results following SIDH's attacks [CD23; Mai+23; Rob23]

New state-of-the-art



Polynomial reductions between isogeny-based problems.

Theorem (This paper)

The **Isogeny**, **EndRing**, **MaxOrder**, **OneEnd**, **MOER** *and* **HomModule** *problems are equivalent under classical probabilistic polynomial reductions.*

: HD results following SIDH's attacks [CD23; Mai+23; Rob23] including IsogenyInterpolation [Rob24], IdealToIsogeny [PR23] and IsogenyDivision[Rob22; HW25] algorithms.

Worst-case to average-case reductions

Theorem (This paper)

For any pair of problems (P, Q) chosen from the problems

$$\mathtt{Isogeny}, \ell\text{-}\mathtt{IsogenyPath}, \mathtt{EndRing}, \mathtt{OneEnd}, \mathtt{MaxOrder}, \mathtt{MOER} \textit{ and } \mathtt{HomModule},$$

there exists an unconditional probabilistic polynomial time reduction

$$P \textit{ worst-case} \longrightarrow Q \textit{ average-case},$$

Worst-case to average-case reductions

Theorem (This paper)

For any pair of problems (P, Q) chosen from the problems

$$\mathtt{Isogeny}, \ell\text{-}\mathtt{IsogenyPath}, \mathtt{EndRing}, \mathtt{OneEnd}, \mathtt{MaxOrder}, \mathtt{MOER} \text{ and } \mathtt{HomModule},$$

there exists an unconditional probabilistic polynomial time reduction

$$P \text{ worst-case} \longrightarrow Q \text{ average-case},$$

$$\text{except if } \begin{cases} & P = \ell\text{-}\mathtt{IsogenyPath} \\ \text{or} & Q = \mathtt{MaxOrder} \text{ and } p \equiv 1 \bmod 8 \end{cases} \text{ then one needs to assume GRH.}$$

Conclusion

Corollary

Isogeny *worst-case hardness* $\Longrightarrow$ **Isogeny**, ℓ-**IsogenyPath**, **MOER**, **OneEnd**, **EndRing**, **HomModule**, (**MaxOrder** *if* $p \not\equiv 1 \bmod 8$) *average-case hardness.*

Conclusion

Corollary

Isogeny *worst-case hardness* $\Longrightarrow$ **Isogeny**, **ℓ-IsogenyPath**, **MOER**, **OneEnd**, **EndRing**, **HomModule**, (**MaxOrder** *if* $p \not\equiv 1 \bmod 8$) *average-case hardness.*

Open questions:

Conclusion

Corollary

$\texttt{Isogeny}$ *worst-case hardness* $\Longrightarrow$ $\texttt{Isogeny}$, ℓ-$\texttt{IsogenyPath}$, $\texttt{MOER}$, $\texttt{OneEnd}$, $\texttt{EndRing}$, $\texttt{HomModule}$, ($\texttt{MaxOrder}$ *if* $p \not\equiv 1 \bmod 8$) *average-case hardness.*

Open questions:

- Can we reduce ℓ-`IsogenyPath` to another problem?
- Can we reduce a problem to `MaxOrder` in the average case when $p \equiv 1 \bmod 8$?

Conclusion

Corollary

Isogeny *worst-case hardness* $\Longrightarrow$ **Isogeny**, **ℓ-IsogenyPath**, **MOER**, **OneEnd**, **EndRing**, **HomModule**, (**MaxOrder** *if* $p \not\equiv 1 \bmod 8$) *average-case hardness.*

Open questions:

- Can we reduce ℓ-IsogenyPath to another problem?
- Can we reduce a problem to MaxOrder in the average case when $p \equiv 1 \bmod 8$?
- What are the problems to consider in higher dimensions? Are these problems equivalent?

Corollary

Isogeny *worst-case hardness* $\Longrightarrow$ **Isogeny**, **ℓ-IsogenyPath**, **MOER**, **OneEnd**, **EndRing**, **HomModule**, (**MaxOrder** *if* $p \not\equiv 1 \bmod 8$) *average-case hardness.*

Open questions:

- Can we reduce ℓ-IsogenyPath to another problem?
- Can we reduce a problem to MaxOrder in the average case when $p \equiv 1 \bmod 8$?
- What are the problems to consider in higher dimensions? Are these problems equivalent?

Thank you for your attention!

Bibliography I

[CD23] Wouter Castryck and Thomas Decru. "An Efficient Key Recovery Attack on SIDH". In: 2023, pp. 423–447. doi: 10.1007/978-3-031-30589-4_15.

[Eis+18] Kirsten Eisenträger et al. "Supersingular Isogeny Graphs and Endomorphism Rings: Reductions and Solutions". In: 2018, pp. 329–368. doi: 10.1007/978-3-319-78372-7_11.

[HW25] Arthur Herlédan Le Merdy and Benjamin Wesolowski. "The supersingular endomorphism ring problem given one endomorphism". In: IACR Communications in Cryptology 2.1 (Apr. 8, 2025). issn: 3006-5496. doi: 10.62056/akgyivrzn.

[Mai+23] Luciano Maino et al. "A Direct Key Recovery Attack on SIDH". In: 2023, pp. 448–471. doi: 10.1007/978-3-031-30589-4_16.

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

Bibliography II

[PW24] Aurel Page and Benjamin Wesolowski. "The Supersingular Endomorphism Ring and One Endomorphism Problems are Equivalent". In: 2024, pp. 388–417. doi: 10.1007/978-3-031-58751-1_14.

[Rob22] Damien Robert. Some applications of higher dimensional isogenies to elliptic curves (overview of results). Cryptology ePrint Archive, Report 2022/1704. 2022. url: https://eprint.iacr.org/2022/1704.

[Rob23] Damien Robert. "Breaking SIDH in Polynomial Time". In: 2023, pp. 472–503. doi: 10.1007/978-3-031-30589-4_17.

[Rob24] Damien Robert. On the efficient representation of isogenies (a survey). Cryptology ePrint Archive, Report 2024/1071. 2024. url: https://eprint.iacr.org/2024/1071.

[Wes22] Benjamin Wesolowski. "The supersingular isogeny path and endomorphism ring problems are equivalent". In: 2022, pp. 1100–1111. doi: 10.1109/FOCS52979.2021.00109.