Unconditional foundations of supersingular isogeny-based cryptography

Arthur Herlédan Le Merdy Benjamin Wesolowski

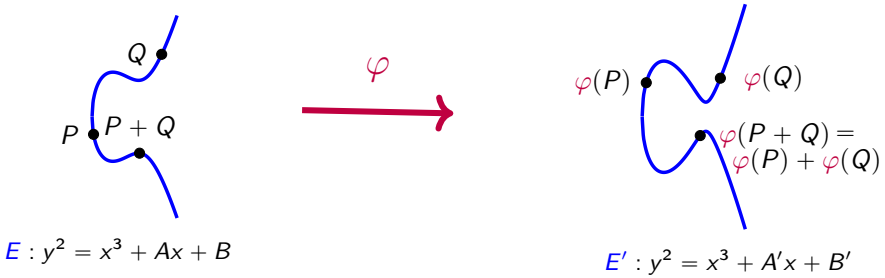
ENS de Lyon, CNRS, UMPA

Friday 4th April, 2025

Outline

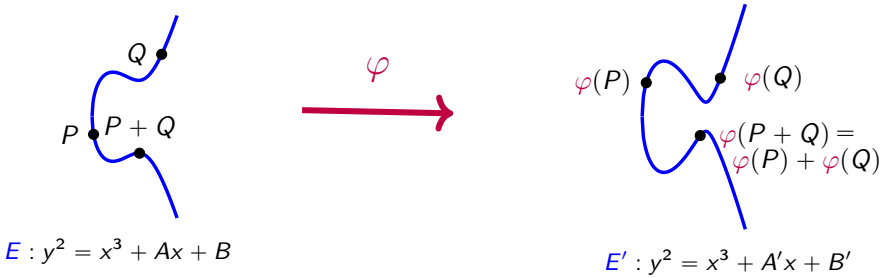
Hard problems in isogeny-based cryptography

Elliptic curves, isogenies and schemes



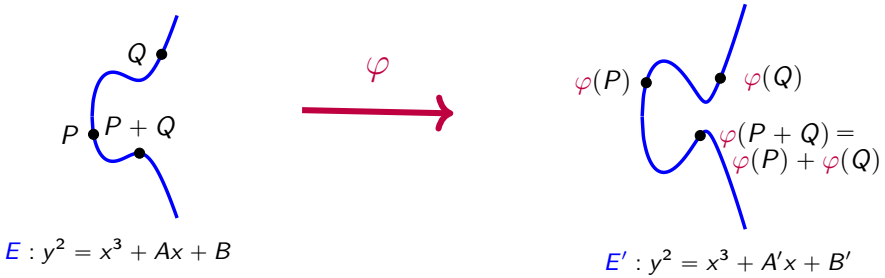
- **Elliptic curve:** smooth projective curve given by an affine model such as above.
- **Isogeny:** non-constant rational map inducing a group homomorphism.

Elliptic curves, isogenies and schemes



- **Elliptic curve:** smooth projective curve given by an affine model such as above.
- **Isogeny:** non-constant rational map inducing a group homomorphism.
- Here **elliptic curves** are **supersingular**, defined over $\mathbb{F}_{p^2}$, for p a fixed prime, and most isogenies are **separable**, i.e. $\deg \varphi = \# \ker \varphi$.

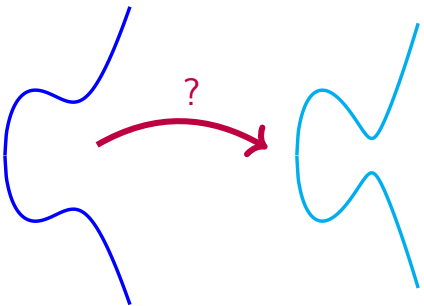
Elliptic curves, isogenies and schemes



- **Elliptic curve:** smooth projective curve given by an affine model such as above.
- **Isogeny:** non-constant rational map inducing a group homomorphism.
- Here **elliptic curves** are **supersingular**, defined over $\mathbb{F}_{p^2}$, for p a fixed prime, and most isogenies are **separable**, i.e. $\deg \varphi = \# \ker \varphi$.
- **Hash function** (CGL), **Key exchange** (CSIDH), **Digital signature** (SQISign) and more.

Hard problems Zoo

Isogeny Problem



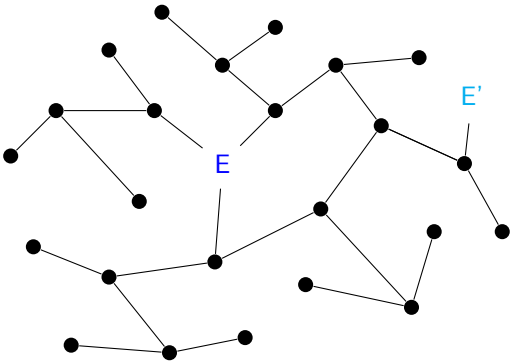
Isogeny

Polynomial reductions between isogeny-based problems

Hard problems Zoo

Let $\ell \neq p$ a prime.

ℓ-IsogenyPath Problem



ℓ-IsogenyPath

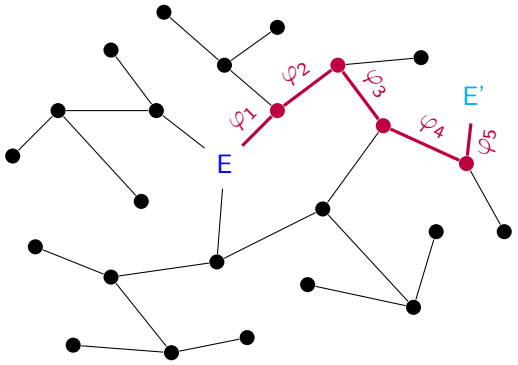
Isogeny

Polynomial reductions between isogeny-based problems

Hard problems Zoo

Let $\ell \neq p$ a prime.

ℓ-IsogenyPath Problem



$\varphi_5 \circ \varphi_4 \circ \varphi_3 \circ \varphi_2 \circ \varphi_1 : E \to E'$

ℓ-IsogenyPath

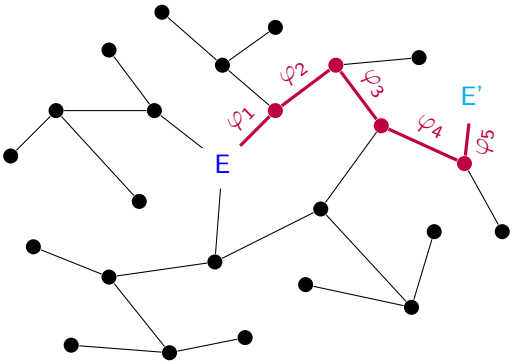
Isogeny

Polynomial reductions between isogeny-based problems

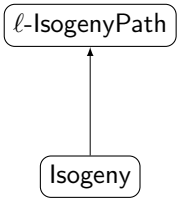
Hard problems Zoo

Let $\ell \neq p$ a prime.

ℓ-IsogenyPath Problem



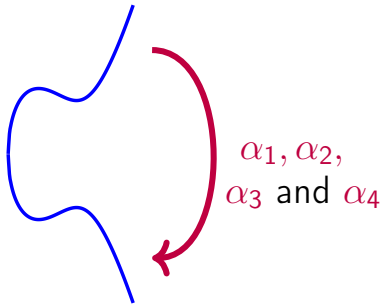
$\varphi_5 \circ \varphi_4 \circ \varphi_3 \circ \varphi_2 \circ \varphi_1 : E \to E'$



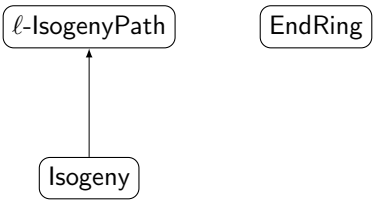
Polynomial reductions between isogeny-based problems

Hard problems Zoo

Endomorphism Ring problem



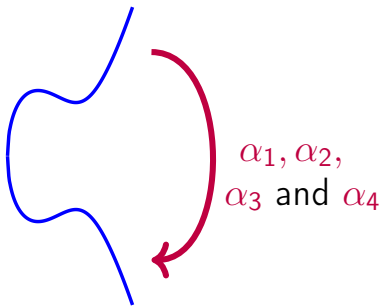
$\mathsf{End}(\curvearrowleft) = \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z} + \alpha_3\mathbb{Z} + \alpha_4\mathbb{Z}$



Polynomial reductions between isogeny-based problems

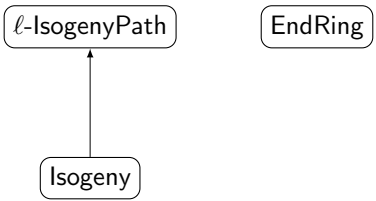
Hard problems Zoo

Endomorphism Ring problem



$$\mathsf{End}(\mathcal{E}) = \mathbb{Z} + \alpha_2\mathbb{Z} + \alpha_3\mathbb{Z} + \alpha_4\mathbb{Z}$$

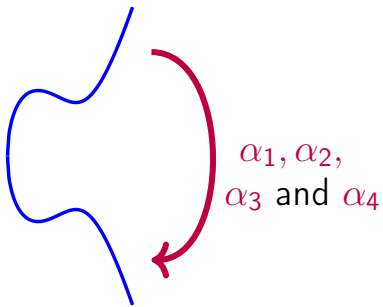
$n \mapsto [n]$ s.t. $[n]P = \underbrace{P + \cdots + P}_{n \text{ times}}$



Polynomial reductions between isogeny-based problems

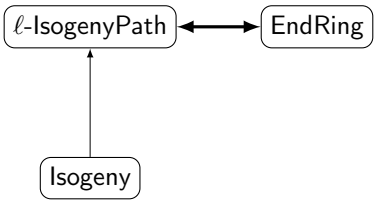
Hard problems Zoo

Endomorphism Ring problem



$$\mathrm{End}(\curvearrowright) = \mathbb{Z} + \alpha_2\mathbb{Z} + \alpha_3\mathbb{Z} + \alpha_4\mathbb{Z}$$

$n \mapsto [n]$ s.t. $[n]P = \underbrace{P + \cdots + P}_{n \text{ times}}$



Polynomial reductions between isogeny-based problems

Deuring Correspondence

Let $E_1/\mathbb{F}_{p^2}$ and $E_2/\mathbb{F}_{p^2}$ be supersingular elliptic curves, then there exists a prime q_p such that

Deuring Correspondence

Let $E_1/\mathbb{F}_{p^2}$ and $E_2/\mathbb{F}_{p^2}$ be supersingular elliptic curves, then there exists a prime q_p such that

$\mathrm{End}(E_i)$	$\mathcal{O}_i$ maximal order in $(\frac{-p,-q_p}{\mathbb{Q}})^*$

Deuring correspondence

* : $(\frac{-p,-q_p}{\mathbb{Q}}) = \mathbb{Q}+i\mathbb{Q}+j\mathbb{Q}+ij\mathbb{Q}$ such that $i^2 = -p$, $j^2 = -q_p$ and $ij = -ji$ is a quaternion algebra.

Deuring Correspondence

Let $E_1/\mathbb{F}_{p^2}$ and $E_2/\mathbb{F}_{p^2}$ be supersingular elliptic curves, then there exists a prime q_p such that

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

Deuring correspondence

* : $(\frac{-p,-q_p}{\mathbb{Q}}) = \mathbb{Q}+i\mathbb{Q}+j\mathbb{Q}+ij\mathbb{Q}$ such that $i^2 = -p$, $j^2 = -q_p$ and $ij = -ji$ is a quaternion algebra.

Deuring Correspondence

Let $E_1/\mathbb{F}_{p^2}$ and $E_2/\mathbb{F}_{p^2}$ be supersingular elliptic curves, then there exists a prime q_p such that

$\mathrm{End}(E_i)$	$\mathcal{O}_i$ maximal order in $(\frac{-p,-q_p}{\mathbb{Q}})$*
$\varphi : E_1 \to E_2$	I_φ integral left $\mathcal{O}_1$-ideal and right $\mathcal{O}_2$-ideal
$\varphi : E_1 \to E_2$ and $\psi : E_1 \to E_2$	$I_\varphi \sim I_\psi$, i.e. $I = J\beta$ for $\beta \in (\frac{-p,-q_p}{\mathbb{Q}})$

Deuring correspondence

* : $(\frac{-p,-q_p}{\mathbb{Q}}) = \mathbb{Q}+i\mathbb{Q}+j\mathbb{Q}+ij\mathbb{Q}$ such that $i^2 = -p$, $j^2 = -q_p$ and $ij = -ji$ is a quaternion algebra.

Deuring Correspondence

Let $E_1/\mathbb{F}_{p^2}$ and $E_2/\mathbb{F}_{p^2}$ be supersingular elliptic curves, then there exists a prime q_p such that

$\mathrm{End}(E_i)$	$\mathcal{O}_i$ maximal order in $(\frac{-p,-q_p}{\mathbb{Q}})$*
$\varphi : E_1 \to E_2$	I_φ integral left $\mathcal{O}_1$-ideal and right $\mathcal{O}_2$-ideal
$\varphi : E_1 \to E_2$ and $\psi : E_1 \to E_2$	$I_\varphi \sim I_\psi$, i.e. $I = J\beta$ for $\beta \in (\frac{-p,-q_p}{\mathbb{Q}})$
$\deg \varphi$	norm of I

Deuring correspondence

* : $(\frac{-p,-q_p}{\mathbb{Q}}) = \mathbb{Q}+i\mathbb{Q}+j\mathbb{Q}+ij\mathbb{Q}$ such that $i^2 = -p$, $j^2 = -q_p$ and $ij = -ji$ is a quaternion algebra.

Deuring Correspondence

Let $E_1/\mathbb{F}_{p^2}$ and $E_2/\mathbb{F}_{p^2}$ be supersingular elliptic curves, then there exists a prime q_p such that

$\mathrm{End}(E_i)$	$\mathcal{O}_i$ maximal order in $(\frac{-p,-q_p}{\mathbb{Q}})^*$
$\varphi : E_1 \to E_2$	I_φ integral left $\mathcal{O}_1$-ideal and right $\mathcal{O}_2$-ideal
$\varphi : E_1 \to E_2$ and $\psi : E_1 \to E_2$	$I_\varphi \sim I_\psi$, i.e. $I = J\beta$ for $\beta \in (\frac{-p,-q_p}{\mathbb{Q}})$
$\deg \varphi$	norm of I
$\varphi \circ \psi$	$I_{\varphi\circ\psi} = I_\psi \cdot I_\varphi$

Deuring correspondence

* : $(\frac{-p,-q_p}{\mathbb{Q}}) = \mathbb{Q}+i\mathbb{Q}+j\mathbb{Q}+ij\mathbb{Q}$ such that $i^2 = -p$, $j^2 = -q_p$ and $ij = -ji$ is a quaternion algebra.

Deuring Correspondence

Let $E_1/\mathbb{F}_{p^2}$ and $E_2/\mathbb{F}_{p^2}$ be supersingular elliptic curves, then there exists a prime q_p such that

$\mathrm{End}(E_i)$	$\mathcal{O}_i$ maximal order in $(\frac{-p,-q_p}{\mathbb{Q}})^*$
$\varphi : E_1 \to E_2$	I_φ integral left $\mathcal{O}_1$-ideal and right $\mathcal{O}_2$-ideal
$\varphi : E_1 \to E_2$ and $\psi : E_1 \to E_2$	$I_\varphi \sim I_\psi$, i.e. $I = J\beta$ for $\beta \in (\frac{-p,-q_p}{\mathbb{Q}})$
$\deg \varphi$	norm of I
$\varphi \circ \psi$	$I_{\varphi\circ\psi} = I_\psi \cdot I_\varphi$

Deuring correspondence

ℓ-IsogenyPath solutions $\longleftrightarrow$ ℓ-QuaternionPath solutions

$$\varphi_n \circ \ldots \circ \varphi_1 \qquad I_1 \cdot \ldots \cdot I_n$$

* : $(\frac{-p,-q_p}{\mathbb{Q}}) = \mathbb{Q}+i\mathbb{Q}+j\mathbb{Q}+ij\mathbb{Q}$ such that $i^2 = -p$, $j^2 = -q_p$ and $ij = -ji$ is a quaternion algebra.

Deuring Correspondence

Let $E_1/\mathbb{F}_{p^2}$ and $E_2/\mathbb{F}_{p^2}$ be supersingular elliptic curves, then there exists a prime q_p such that

$\mathrm{End}(E_i)$	$\mathcal{O}_i$ maximal order in $(\frac{-p,-q_p}{\mathbb{Q}})^*$
$\varphi : E_1 \to E_2$	I_φ integral left $\mathcal{O}_1$-ideal and right $\mathcal{O}_2$-ideal
$\varphi : E_1 \to E_2$ and $\psi : E_1 \to E_2$	$I_\varphi \sim I_\psi$, i.e. $I = J\beta$ for $\beta \in (\frac{-p,-q_p}{\mathbb{Q}})$
$\deg \varphi$	norm of I
$\varphi \circ \psi$	$I_{\varphi\circ\psi} = I_\psi \cdot I_\varphi$

Deuring correspondence

ℓ-IsogenyPath solutions $\longleftrightarrow$ ℓ-QuaternionPath solutions

$$\varphi_n \circ \ldots \circ \varphi_1 \qquad I_1 \cdot \ldots \cdot I_n$$

Solving ℓ-IsogenyPath : **Hard**
Solving ℓ-QuaternionPath : **Easy**

* : $(\frac{-p,-q_p}{\mathbb{Q}}) = \mathbb{Q}+i\mathbb{Q}+j\mathbb{Q}+ij\mathbb{Q}$ such that $i^2 = -p$, $j^2 = -q_p$ and $ij = -ji$ is a quaternion algebra.

Deuring Correspondence

Let $E_1/\mathbb{F}_{p^2}$ and $E_2/\mathbb{F}_{p^2}$ be supersingular elliptic curves, then there exists a prime q_p such that

$\mathrm{End}(E_i)$	$\mathcal{O}_i$ maximal order in $(\frac{-p,-q_p}{\mathbb{Q}})^*$
$\varphi : E_1 \to E_2$	I_φ integral left $\mathcal{O}_1$-ideal and right $\mathcal{O}_2$-ideal
$\varphi : E_1 \to E_2$ and $\psi : E_1 \to E_2$	$I_\varphi \sim I_\psi$, i.e. $I = J\beta$ for $\beta \in (\frac{-p,-q_p}{\mathbb{Q}})$
$\deg \varphi$	norm of I
$\varphi \circ \psi$	$I_{\varphi\circ\psi} = I_\psi \cdot I_\varphi$

Deuring correspondence

ℓ-IsogenyPath solutions $\longleftrightarrow$ ℓ-QuaternionPath solutions

$$\varphi_n \circ \ldots \circ \varphi_1 \overset{\text{Easy}}{\rightsquigarrow} I_1 \cdot \ldots \cdot I_n$$

Solving ℓ-IsogenyPath : **Hard**
Solving ℓ-QuaternionPath : **Easy**

* : $(\frac{-p,-q_p}{\mathbb{Q}}) = \mathbb{Q}+i\mathbb{Q}+j\mathbb{Q}+ij\mathbb{Q}$ such that $i^2 = -p$, $j^2 = -q_p$ and $ij = -ji$ is a quaternion algebra.

Deuring Correspondence

Let $E_1/\mathbb{F}_{p^2}$ and $E_2/\mathbb{F}_{p^2}$ be supersingular elliptic curves, then there exists a prime q_p such that

$\mathrm{End}(E_i)$	$\mathcal{O}_i$ maximal order in $(\frac{-p,-q_p}{\mathbb{Q}})$*
$\varphi : E_1 \to E_2$	I_φ integral left $\mathcal{O}_1$-ideal and right $\mathcal{O}_2$-ideal
$\varphi : E_1 \to E_2$ and $\psi : E_1 \to E_2$	$I_\varphi \sim I_\psi$, i.e. $I = J\beta$ for $\beta \in (\frac{-p,-q_p}{\mathbb{Q}})$
$\deg \varphi$	norm of I
$\varphi \circ \psi$	$I_{\varphi\circ\psi} = I_\psi \cdot I_\varphi$

Deuring correspondence

ℓ-IsogenyPath solutions $\longleftrightarrow$ ℓ-QuaternionPath solutions

$$\varphi_n \circ \ldots \circ \varphi_1 \overset{\text{Easy}^*}{\leftsquigarrow} I_1 \cdot \ldots \cdot I_n$$

* `IdealToIsogeny` is easy if:

Solving ℓ-IsogenyPath : **Hard**

Solving ℓ-QuaternionPath : **Easy**

* : $(\frac{-p,-q_p}{\mathbb{Q}}) = \mathbb{Q}+i\mathbb{Q}+j\mathbb{Q}+ij\mathbb{Q}$ such that $i^2 = -p$, $j^2 = -q_p$ and $ij = -ji$ is a quaternion algebra.

Deuring Correspondence

Let $E_1/\mathbb{F}_{p^2}$ and $E_2/\mathbb{F}_{p^2}$ be supersingular elliptic curves, then there exists a prime q_p such that

$\mathrm{End}(E_i)$	$\mathcal{O}_i$ maximal order in $(\frac{-p,-q_p}{\mathbb{Q}})^*$
$\varphi : E_1 \to E_2$	I_φ integral left $\mathcal{O}_1$-ideal and right $\mathcal{O}_2$-ideal
$\varphi : E_1 \to E_2$ and $\psi : E_1 \to E_2$	$I_\varphi \sim I_\psi$, i.e. $I = J\beta$ for $\beta \in (\frac{-p,-q_p}{\mathbb{Q}})$
$\deg \varphi$	norm of I
$\varphi \circ \psi$	$I_{\varphi\circ\psi} = I_\psi \cdot I_\varphi$

Deuring correspondence

ℓ-IsogenyPath solutions $\longleftrightarrow$ ℓ-QuaternionPath solutions

$$\varphi_n \circ \ldots \circ \varphi_1 \overset{\text{Easy}^*}{\dashleftarrow} I_1 \cdot \ldots \cdot I_n$$

* `IdealToIsogeny` is easy if:

1. The ideal is smooth enough

Solving ℓ-IsogenyPath : **Hard**

Solving ℓ-QuaternionPath : **Easy**

* : $(\frac{-p,-q_p}{\mathbb{Q}}) = \mathbb{Q}+i\mathbb{Q}+j\mathbb{Q}+ij\mathbb{Q}$ such that $i^2 = -p$, $j^2 = -q_p$ and $ij = -ji$ is a quaternion algebra.

Deuring Correspondence

Let $E_1/\mathbb{F}_{p^2}$ and $E_2/\mathbb{F}_{p^2}$ be supersingular elliptic curves, then there exists a prime q_p such that

$\mathrm{End}(E_i)$	$\mathcal{O}_i$ maximal order in $(\frac{-p,-q_p}{\mathbb{Q}})^*$
$\varphi : E_1 \to E_2$	I_φ integral left $\mathcal{O}_1$-ideal and right $\mathcal{O}_2$-ideal
$\varphi : E_1 \to E_2$ and $\psi : E_1 \to E_2$	$I_\varphi \sim I_\psi$, i.e. $I = J\beta$ for $\beta \in (\frac{-p,-q_p}{\mathbb{Q}})$
$\deg \varphi$	norm of I
$\varphi \circ \psi$	$I_{\varphi\circ\psi} = I_\psi \cdot I_\varphi$

Deuring correspondence

ℓ-IsogenyPath solutions $\longleftrightarrow$ ℓ-QuaternionPath solutions

$$\varphi_n \circ \ldots \circ \varphi_1 \overset{\text{Easy}^*}{\leftsquigarrow} I_1 \cdot \ldots \cdot I_n$$

* `IdealToIsogeny` is easy if:

1. The ideal is smooth enough
2. We know a **special curve** E_0, i.e. such that $\varepsilon : \mathcal{O}_0 \xrightarrow{\sim} \mathrm{End}(E_0)$ is explicit.

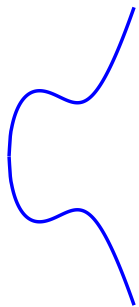
Solving ℓ-IsogenyPath : **Hard**

Solving ℓ-QuaternionPath : **Easy**

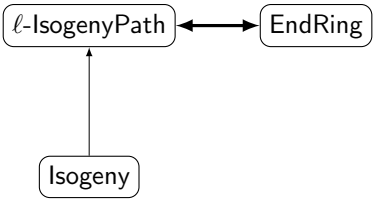
* : $(\frac{-p,-q_p}{\mathbb{Q}}) = \mathbb{Q}+i\mathbb{Q}+j\mathbb{Q}+ij\mathbb{Q}$ such that $i^2 = -p$, $j^2 = -q_p$ and $ij = -ji$ is a quaternion algebra.

Hard problems Zoo

Maximal Order problem



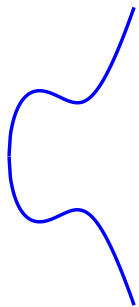
$\mathrm{End}(\curvearrowleft) \simeq \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z} + \alpha_3\mathbb{Z} + \alpha_4\mathbb{Z}$
where α_i are quaternions in $(\frac{-p,-q_p}{\mathbb{Q}})$



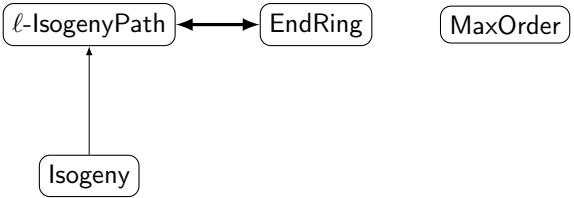
Polynomial reductions between isogeny-based problems

Hard problems Zoo

Maximal Order problem



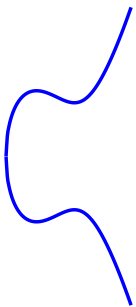
$\mathrm{End}(\curvearrowleft) \simeq \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z} + \alpha_3\mathbb{Z} + \alpha_4\mathbb{Z}$
where α_i are quaternions in $(\frac{-p,-q_p}{\mathbb{Q}})$



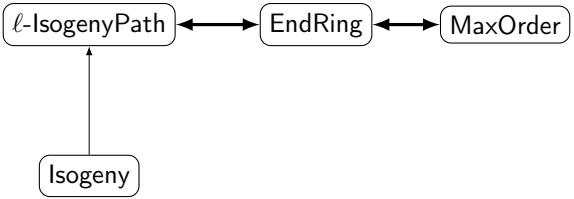
Polynomial reductions between isogeny-based problems

Hard problems Zoo

Maximal Order problem



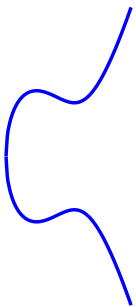
$\mathrm{End}(\curvearrowleft) \simeq \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z} + \alpha_3\mathbb{Z} + \alpha_4\mathbb{Z}$
where α_i are quaternions in $(\frac{-p,-q_p}{\mathbb{Q}})$



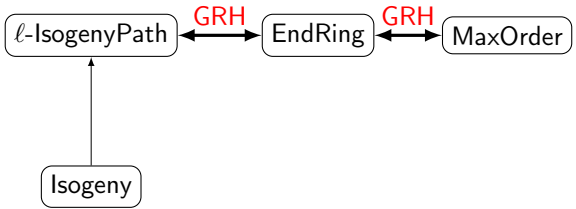
Polynomial reductions between isogeny-based problems

Hard problems Zoo

Maximal Order problem



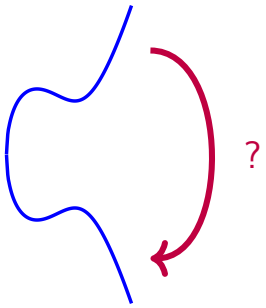
$\mathrm{End}(\curvearrowleft) \simeq \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z} + \alpha_3\mathbb{Z} + \alpha_4\mathbb{Z}$
where α_i are quaternions in $(\frac{-p,-q_p}{\mathbb{Q}})$

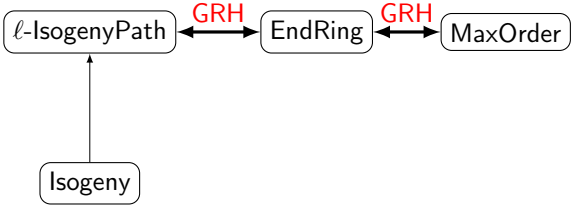


Polynomial reductions between isogeny-based problems
(Non trivial reductions under GRH [Wes21] and
before under heuristics [EHM17; PL17; Eis+18])

Hard problems Zoo

One Endomorphism problem

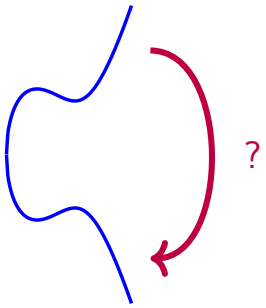


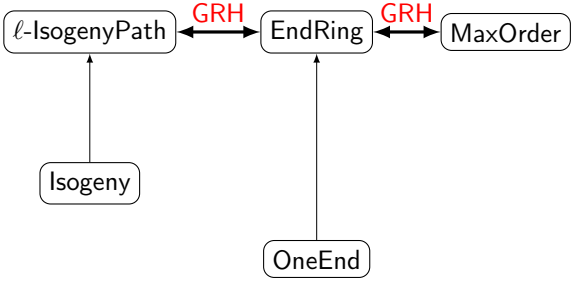


Polynomial reductions between isogeny-based problems

Hard problems Zoo

One Endomorphism problem

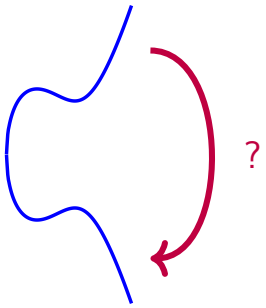


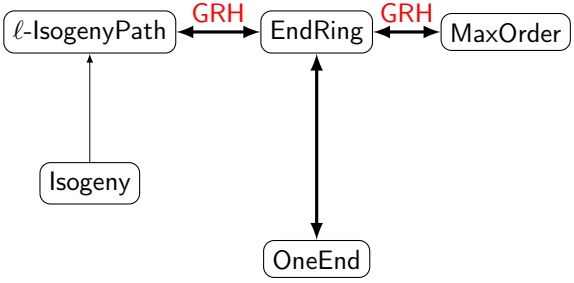


Polynomial reductions between isogeny-based problems

Hard problems Zoo

One Endomorphism problem

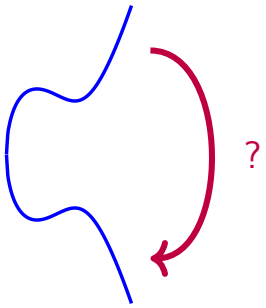


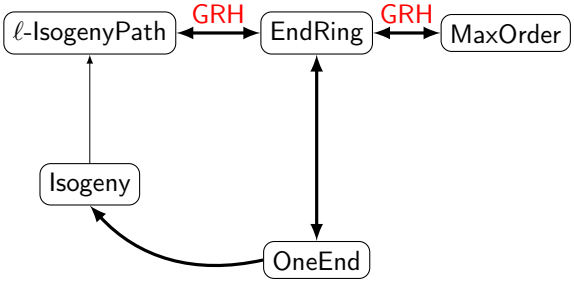


Polynomial reductions between isogeny-based problems

Hard problems Zoo

One Endomorphism problem

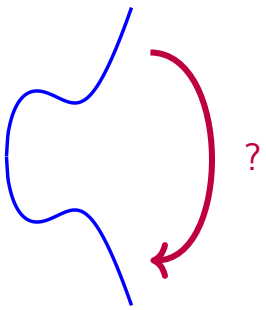


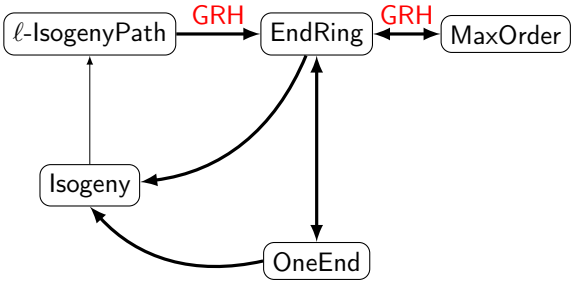


Polynomial reductions between isogeny-based problems

Hard problems Zoo

One Endomorphism problem

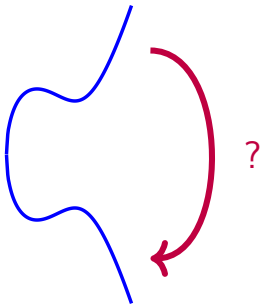


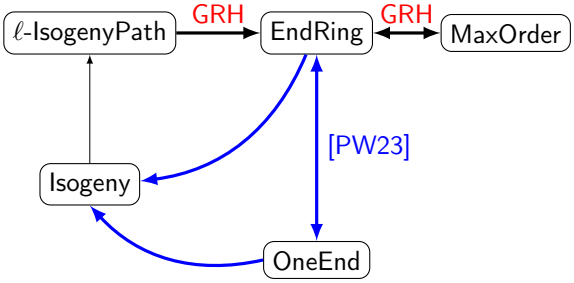


Polynomial reductions between isogeny-based problems

Hard problems Zoo

One Endomorphism problem

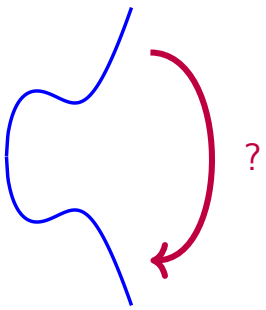


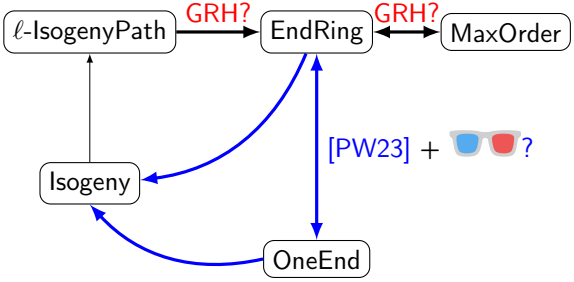


Polynomial reductions between isogeny-based problems

Hard problems Zoo

One Endomorphism problem



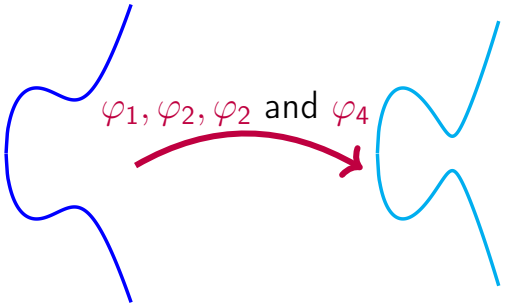


Polynomial reductions between isogeny-based problems

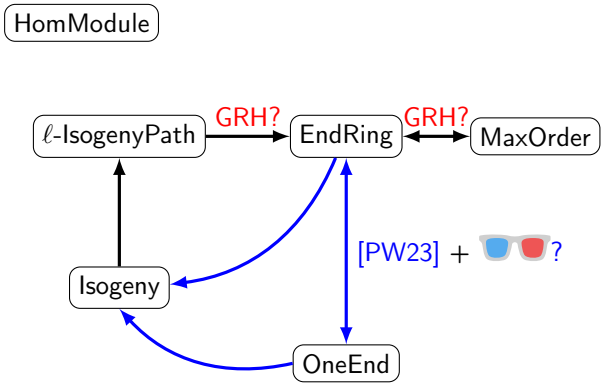
: higher dimensional results published after SIDH's attacks [CSV22; Mai+23; Rob22a]

Hard problems Zoo

Homomorphism Module Problem

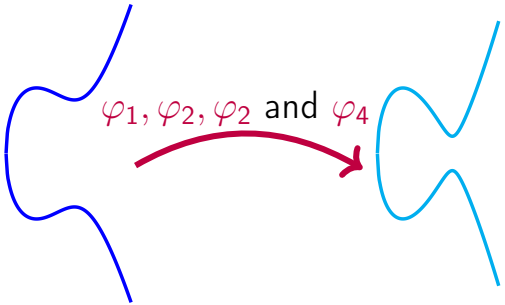


$\mathsf{Hom}(\mathcal{E}, \mathcal{E}) = \varphi_1\mathbb{Z} + \varphi_2\mathbb{Z} + \varphi_3\mathbb{Z} + \varphi_4\mathbb{Z}$

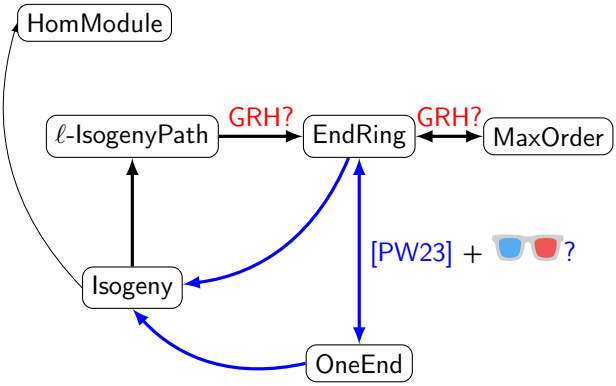


Hard problems Zoo

Homomorphism Module Problem

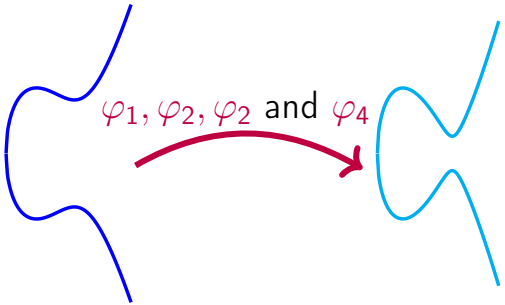


$$\mathsf{Hom}(\text{E}_1, \text{E}_2) = \varphi_1\mathbb{Z} + \varphi_2\mathbb{Z} + \varphi_3\mathbb{Z} + \varphi_4\mathbb{Z}$$

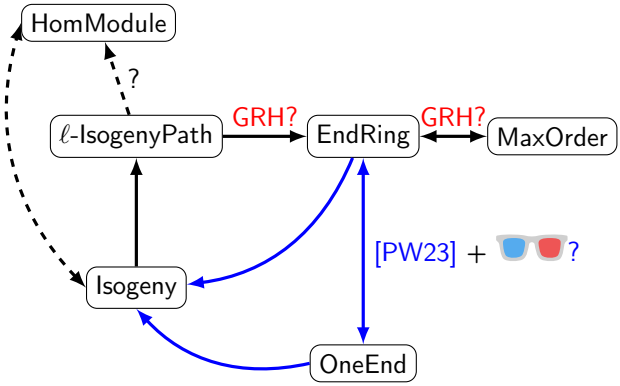


Hard problems Zoo

Homomorphism Module Problem



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



The Generalised Riemann hypothesis

The Riemann hypothesis (RH):

Let ζ be the complex Riemann zeta function (defined from $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \forall \Re(s) > 1$).
For every $s \in \mathbb{C} \setminus 2\mathbb{Z}_{<0}$, if $\zeta(s) = 0$, then $\Re(s) = 1/2$.

The Generalised Riemann hypothesis

The Riemann hypothesis (RH):

Let ζ be the complex Riemann zeta function (defined from $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \forall \Re(s) > 1$).
For every $s \in \mathbb{C} \setminus 2\mathbb{Z}_{<0}$, if $\zeta(s) = 0$, then $\Re(s) = 1/2$.

What for?

The Generalised Riemann hypothesis

The Riemann hypothesis (RH):

Let ζ be the complex Riemann zeta function (defined from $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \forall \Re(s) > 1$).
For every $s \in \mathbb{C} \setminus 2\mathbb{Z}_{<0}$, if $\zeta(s) = 0$, then $\Re(s) = 1/2$.

What for? Counting primes!

$$\textbf{RH} \iff \pi(x) := |\{p \text{ prime} \leqslant x\}| = \int_0^x \frac{dt}{\ln t} + O(\sqrt{x}\ln(x)).$$

The Generalised Riemann hypothesis

The Riemann hypothesis (RH):

Let ζ be the complex Riemann zeta function (defined from $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \forall \Re(s) > 1$).
For every $s \in \mathbb{C} \setminus 2\mathbb{Z}_{<0}$, if $\zeta(s) = 0$, then $\Re(s) = 1/2$.

What for? Counting primes!

$$\textbf{RH} \iff \pi(x) := |\{p \text{ prime} \leqslant x\}| = \int_0^x \frac{dt}{\ln t} + O(\sqrt{x}\ln(x)).$$

Why do we need **generalised** Riemann hypothesis?

The Generalised Riemann hypothesis

The Riemann hypothesis (RH):

Let ζ be the complex Riemann zeta function (defined from $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \forall \Re(s) > 1$).
For every $s \in \mathbb{C} \setminus 2\mathbb{Z}_{<0}$, if $\zeta(s) = 0$, then $\Re(s) = 1/2$.

What for? Counting primes!

$$\textbf{RH} \iff \pi(x) := |\{p \text{ prime} \leqslant x\}| = \int_0^x \frac{dt}{\ln t} + O(\sqrt{x}\ln(x)).$$

Why do we need **generalised** Riemann hypothesis? To deal with **more** sets of primes!

The Generalised Riemann hypothesis

The Riemann hypothesis (RH):

Let ζ be the complex Riemann zeta function (defined from $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \forall \Re(s) > 1$).
For every $s \in \mathbb{C} \setminus 2\mathbb{Z}_{<0}$, if $\zeta(s) = 0$, then $\Re(s) = 1/2$.

What for? Counting primes!

$$\textbf{RH} \iff \pi(x) := |\{p \text{ prime} \leqslant x\}| = \int_0^x \frac{dt}{\ln t} + O(\sqrt{x}\ln(x)).$$

Why do we need **generalised** Riemann hypothesis? To deal with **more** sets of primes!

The Generalised Riemann hypothesis

The Riemann hypothesis (RH):

Let ζ be the complex Riemann zeta function (defined from $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \forall \Re(s) > 1$).
For every $s \in \mathbb{C} \setminus 2\mathbb{Z}_{<0}$, if $\zeta(s) = 0$, then $\Re(s) = 1/2$.

What for? Counting primes!

$$\textbf{RH} \iff \pi(x) := |\{p \text{ prime} \leqslant x\}| = \int_0^x \frac{dt}{\ln t} + O(\sqrt{x}\ln(x)).$$

Why do we need **generalised** Riemann hypothesis? To deal with **more** sets of primes!

$$\textbf{GRH} \implies \pi(x, a, d) := |\{p \text{ prime s.t } p \leqslant x \text{ and } p \equiv a \mod d\}| = \frac{1}{\varphi(d)} \int_2^x \frac{dt}{lnt} + O(\sqrt{x}\ln x)$$

GRH for our reductions

1. Finding q_p such that $\mathrm{End}(E) \simeq \mathcal{O} \subset (\frac{-p,-q_p}{\mathbb{Q}})$ when $p \equiv 1 \mod 8$:

GRH for our reductions

1. Finding q_p such that $\mathrm{End}(E) \simeq \mathcal{O} \subset (\frac{-p,-q_p}{\mathbb{Q}})$ when $p \equiv 1 \mod 8$:

[Eis+18] with **GRH**, $q_p = O(\log(p)^2)$,
[Lag77] without **GRH**, $q_p = \mathrm{poly}(p)$.

GRH for our reductions

1. Finding q_p such that $\mathrm{End}(E) \simeq \mathcal{O} \subset (\frac{-p,-q_p}{\mathbb{Q}})$ when $p \equiv 1 \mod 8$:

[Eis+18] with **GRH**, $q_p = O(\log(p)^2)$,
[Lag77] without **GRH**, $q_p = \mathrm{poly}(p)$.

2. Solving ℓ-QuaternionPath:

GRH for our reductions

1. Finding q_p such that $\mathrm{End}(E) \simeq \mathcal{O} \subset \left(\frac{-p,-q_p}{\mathbb{Q}}\right)$ when $p \equiv 1 \mod 8$:

[Eis+18] with **GRH**, $q_p = O(\log(p)^2)$,
[Lag77] without **GRH**, $q_p = \mathrm{poly}(p)$.

2. Solving ℓ-QuaternionPath:

[Koh+14] Efficient algorithm under heuristics (**KLPT**),
[Wes22] Proven version under **GRH**.

GRH for our reductions

1. Finding q_p such that $\mathrm{End}(E) \simeq \mathcal{O} \subset (\frac{-p,-q_p}{\mathbb{Q}})$ when $p \equiv 1 \mod 8$:

[Eis+18] with **GRH**, $q_p = O(\log(p)^2)$,
[Lag77] without **GRH**, $q_p = \mathrm{poly}(p)$.

2. Solving ℓ-QuaternionPath:

[Koh+14] Efficient algorithm under heuristics (**KLPT**),
[Wes22] Proven version under **GRH**.

3. Counting primes represented by quadratic forms.

Reductions **without** the generalised Riemann hypothesis

No GRH for our reductions

1. Finding q_p such that $\mathrm{End}(E) \simeq \mathcal{O} \subset (\frac{-p,-q_p}{\mathbb{Q}})$ when $p \equiv 1 \mod 8$:

No GRH for our reductions

1. Finding q_p such that $\mathrm{End}(E) \simeq \mathcal{O} \subset (\frac{-p,-q_p}{\mathbb{Q}})$ when $p \equiv 1 \mod 8$:

Solution: Find $a, b \in \mathbb{Z}_{>0}$ such that $\mathrm{End}(E) \simeq \mathcal{O} \subseteq (\frac{-a,-b}{\mathbb{Q}}) \simeq (\frac{-p,-q_p}{\mathbb{Q}})$

No GRH for our reductions

1. Finding q_p such that $\mathrm{End}(E) \simeq \mathcal{O} \subset \left(\frac{-p,-q_p}{\mathbb{Q}}\right)$ when $p \equiv 1 \mod 8$:

Solution: Find $a, b \in \mathbb{Z}_{>0}$ such that $\mathrm{End}(E) \simeq \mathcal{O} \subseteq \left(\frac{-a,-b}{\mathbb{Q}}\right) \simeq \left(\frac{-p,-q_p}{\mathbb{Q}}\right)$

⚠ Make sure to work in the same quaternion algebra [Csa+22]

No GRH for our reductions

1. Finding q_p such that $\mathrm{End}(E) \simeq \mathcal{O} \subset (\frac{-p,-q_p}{\mathbb{Q}})$ when $p \equiv 1 \mod 8$:

Solution: Find $a, b \in \mathbb{Z}_{>0}$ such that $\mathrm{End}(E) \simeq \mathcal{O} \subseteq (\frac{-a,-b}{\mathbb{Q}}) \simeq (\frac{-p,-q_p}{\mathbb{Q}})$

- ⚠ Make sure to work in the same quaternion algebra [Csa+22]
- ⚠ No known special curve

No GRH for our reductions

1. Finding q_p such that $\mathrm{End}(E) \simeq \mathcal{O} \subset (\frac{-p,-q_p}{\mathbb{Q}})$ when $p \equiv 1 \mod 8$:

Solution: Find $a, b \in \mathbb{Z}_{>0}$ such that $\mathrm{End}(E) \simeq \mathcal{O} \subseteq (\frac{-a,-b}{\mathbb{Q}}) \simeq (\frac{-p,-q_p}{\mathbb{Q}})$

- ⚠ Make sure to work in the same quaternion algebra [Csa+22]
- ⚠ No known special curve

2. Solving ℓ-QuaternionPath:

No GRH for our reductions

1. Finding q_p such that $\mathrm{End}(E) \simeq \mathcal{O} \subset \left(\frac{-p,-q_p}{\mathbb{Q}}\right)$ when $p \equiv 1 \mod 8$:

Solution: Find $a, b \in \mathbb{Z}_{>0}$ such that $\mathrm{End}(E) \simeq \mathcal{O} \subseteq \left(\frac{-a,-b}{\mathbb{Q}}\right) \simeq \left(\frac{-p,-q_p}{\mathbb{Q}}\right)$

- ⚠ Make sure to work in the same quaternion algebra [Csa+22]
- ⚠ No known special curve

2. Solving ℓ-QuaternionPath:

Solution: Use unconditional polynomial time `IdealToIsogeny` algorithm [PR23, `CLAPOTI`] 

No GRH for our reductions

1. Finding q_p such that $\mathrm{End}(E) \simeq \mathcal{O} \subset (\frac{-p,-q_p}{\mathbb{Q}})$ when $p \equiv 1 \mod 8$:

Solution: Find $a, b \in \mathbb{Z}_{>0}$ such that $\mathrm{End}(E) \simeq \mathcal{O} \subseteq (\frac{-a,-b}{\mathbb{Q}}) \simeq (\frac{-p,-q_p}{\mathbb{Q}})$

- ⚠ Make sure to work in the same quaternion algebra [Csa+22]
- ⚠ No known special curve

2. Solving ℓ-QuaternionPath:

Solution: Use unconditional polynomial time `IdealToIsogeny` algorithm [PR23, `CLAPOTI`] 

3. Counting primes represented by quadratic forms.

Solution: Not needed anymore

No GRH for our reductions

1. Finding q_p such that $\mathrm{End}(E) \simeq \mathcal{O} \subset (\frac{-p,-q_p}{\mathbb{Q}})$ when $p \equiv 1 \mod 8$:

Solution: Find $a, b \in \mathbb{Z}_{>0}$ such that $\mathrm{End}(E) \simeq \mathcal{O} \subseteq (\frac{-a,-b}{\mathbb{Q}}) \simeq (\frac{-p,-q_p}{\mathbb{Q}})$

⚠ Make sure to work in the same quaternion algebra [Csa+22]

⚠ No known special curve

2. Solving ℓ-QuaternionPath:

Solution: Use unconditional polynomial time `IdealToIsogeny` algorithm [PR23, `CLAPOTI`] 

3. Counting primes represented by quadratic forms.

Solution: Not needed anymore

OneEnd reduces to MaxOrder

Goal: Compute an endomorphism $\theta \in \mathrm{End}(E) \setminus \mathbb{Z}$, given a MaxOrder oracle.

OneEnd reduces to MaxOrder

Goal: Compute an endomorphism $\theta \in \mathrm{End}(E)\backslash\mathbb{Z}$, given a MaxOrder oracle.

1. Get a maximal order $\mathcal{O}$ such that there is an (**unknown**) isomorphism $\varepsilon : \mathcal{O} \to \mathrm{End}(E)$.

OneEnd reduces to MaxOrder

Goal: Compute an endomorphism $\theta \in \mathrm{End}(E)\backslash\mathbb{Z}$, given a MaxOrder oracle.

1. Get a maximal order $\mathcal{O}$ such that there is an (**unknown**) isomorphism $\varepsilon : \mathcal{O} \to \mathrm{End}(E)$.
2. Compute α a non-trivial element in $\mathcal{O}$ and denote $\theta := \varepsilon(\alpha) \in \mathrm{End}(E)\backslash\mathbb{Z}$.

OneEnd reduces to MaxOrder

Goal: Compute an endomorphism $\theta \in \mathrm{End}(E)\backslash\mathbb{Z}$, given a MaxOrder oracle.

1. Get a maximal order $\mathcal{O}$ such that there is an (**unknown**) isomorphism $\varepsilon : \mathcal{O} \to \mathrm{End}(E)$.
2. Compute α a non-trivial element in $\mathcal{O}$ and denote $\theta := \varepsilon(\alpha) \in \mathrm{End}(E)\backslash\mathbb{Z}$.

`IsogenyInterpolation` algorithm [Rob24] 

Let $\varphi : E \to E'$ be an isogeny. Given $\varphi(E[\ell_i]^*)$, for enough small primes ℓ_i, one can compute φ in polynomial time.

*: $E[\ell] := \{P \in E \text{ such that } [\ell]P = 0_E\}$.

OneEnd reduces to MaxOrder

Goal: Compute an endomorphism $\theta \in \mathrm{End}(E)\backslash\mathbb{Z}$, given a MaxOrder oracle.

1. Get a maximal order $\mathcal{O}$ such that there is an (**unknown**) isomorphism $\varepsilon : \mathcal{O} \to \mathrm{End}(E)$.
2. Compute α a non-trivial element in $\mathcal{O}$ and denote $\theta := \varepsilon(\alpha) \in \mathrm{End}(E)\backslash\mathbb{Z}$.

`IsogenyInterpolation` algorithm [Rob24] 

Let $\varphi : E \to E'$ be an isogeny. Given $\varphi(E[\ell_i]^*)$, for enough small primes ℓ_i, one can compute φ in polynomial time.

Proposition [HLM. Wesolowski 2025]

Given an oracle access to MaxOrder, one can compute in polynomial time either the isomorphism ε restricted to $\mathcal{O}/\ell\mathcal{O} \to \mathrm{End}(E[\ell])$ or an endomorphism $\gamma \in \mathrm{End}(E)\backslash\mathbb{Z}$.

*: $E[\ell] := \{P \in E \text{ such that } [\ell]P = 0_E\}$.

OneEnd reduces to MaxOrder

Goal: Compute an endomorphism $\theta \in \mathrm{End}(E)\backslash\mathbb{Z}$, given a MaxOrder oracle.

1. Get a maximal order $\mathcal{O}$ such that there is an (**unknown**) isomorphism $\varepsilon : \mathcal{O} \to \mathrm{End}(E)$.
2. Compute α a non-trivial element in $\mathcal{O}$ and denote $\theta := \varepsilon(\alpha) \in \mathrm{End}(E)\backslash\mathbb{Z}$.
3. Compute $\theta(E[\ell_i])$ for ℓ_i such that $\prod_i \ell_i > \deg(\theta)$.

`IsogenyInterpolation` algorithm [Rob24] 

Let $\varphi : E \to E'$ be an isogeny. Given $\varphi(E[\ell_i]^*)$, for enough small primes ℓ_i, one can compute φ in polynomial time.

Proposition [HLM. Wesolowski 2025]

Given an oracle access to MaxOrder, one can compute in polynomial time either the isomorphism ε restricted to $\mathcal{O}/\ell\mathcal{O} \to \mathrm{End}(E[\ell])$ or an endomorphism $\gamma \in \mathrm{End}(E)\backslash\mathbb{Z}$.

*: $E[\ell] := \{P \in E \text{ such that } [\ell]P = 0_E\}$.

OneEnd reduces to MaxOrder

Goal: Compute an endomorphism $\theta \in \mathrm{End}(E)\backslash\mathbb{Z}$, given a MaxOrder oracle.

1. Get a maximal order $\mathcal{O}$ such that there is an (**unknown**) isomorphism $\varepsilon : \mathcal{O} \to \mathrm{End}(E)$.
2. Compute α a non-trivial element in $\mathcal{O}$ and denote $\theta := \varepsilon(\alpha) \in \mathrm{End}(E)\backslash\mathbb{Z}$.
3. Compute $\theta(E[\ell_i])$ for ℓ_i such that $\prod_i \ell_i > \deg(\theta)$.
4. Interpolate $\theta := \varepsilon(\alpha)$.

`IsogenyInterpolation` algorithm [Rob24] 

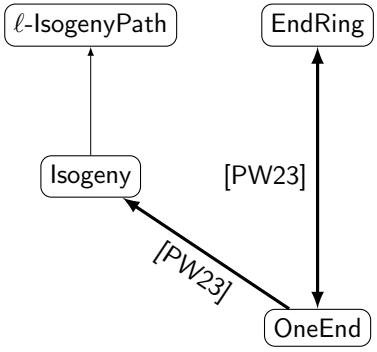
Let $\varphi : E \to E'$ be an isogeny. Given $\varphi(E[\ell_i]^*)$, for enough small primes ℓ_i, one can compute φ in polynomial time.

Proposition [HLM. Wesolowski 2025]

Given an oracle access to MaxOrder, one can compute in polynomial time either the isomorphism ε restricted to $\mathcal{O}/\ell\mathcal{O} \to \mathrm{End}(E[\ell])$ or an endomorphism $\gamma \in \mathrm{End}(E)\backslash\mathbb{Z}$.

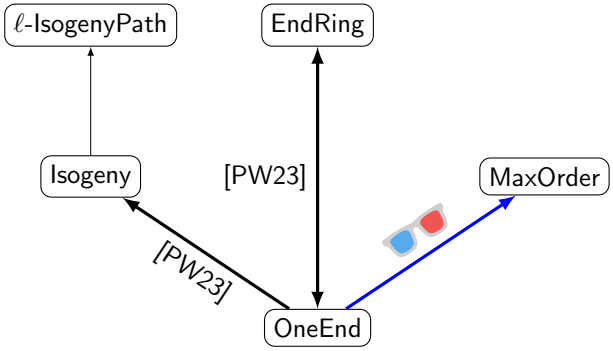
*: $E[\ell] := \{P \in E \text{ such that } [\ell]P = 0_E\}$.

Summary of unconditional reductions



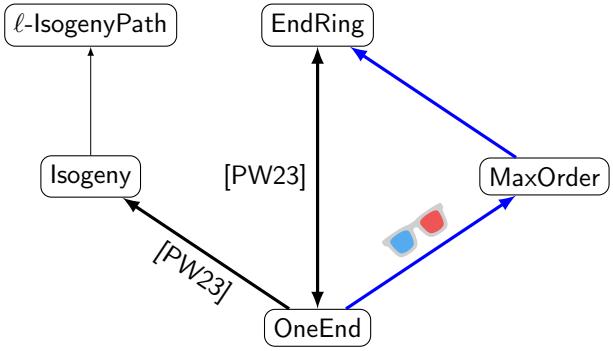
Polynomial reductions without GRH.

Summary of unconditional reductions



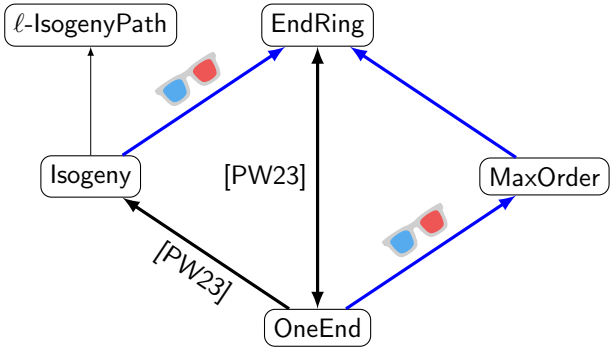
Polynomial reductions without GRH.

Summary of unconditional reductions



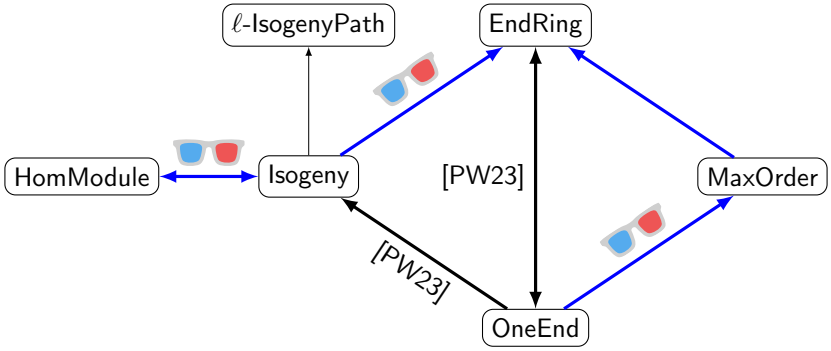
Polynomial reductions without GRH.

Summary of unconditional reductions



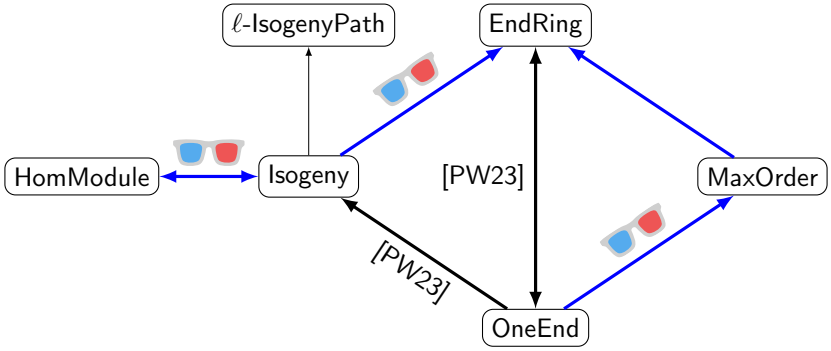
Polynomial reductions without GRH.

Summary of unconditional reductions



Polynomial reductions without GRH.

Summary of unconditional reductions

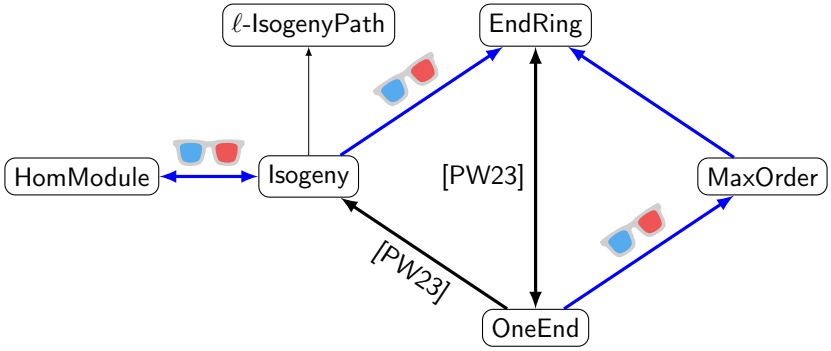


Polynomial reductions without GRH.

Theorem ([HLM. Wesolowski 2025; PW23])

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

Summary of unconditional reductions



Polynomial reductions without GRH.

Theorem ([HLM. Wesolowski 2025; PW23])

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

Worst-case to average-case reductions

Worst-case to average-case reductions

- **Core hardness assumption:**
  There exist hard instances of the Isogeny problem, i.e. **the worst-case is hard**.

Worst-case to average-case reductions

- **Core hardness assumption:**
  There exist hard instances of the Isogeny problem, i.e. **the worst-case is hard**.
- Schemes mostly use **average instances** of hard problems.

Worst-case to average-case reductions

- **Core hardness assumption:**
  There exist hard instances of the Isogeny problem, i.e. **the worst-case is hard**.
- Schemes mostly use **average instances** of hard problems.
- Worst-case hardness $\overset{?}{\Longrightarrow}$ Average-case hardness.

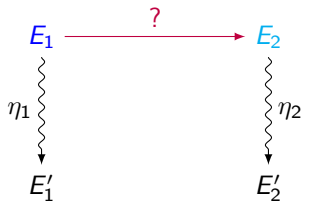
Worst-case to average-case reductions

- **Core hardness assumption:**
  There exist hard instances of the Isogeny problem, i.e. **the worst-case is hard**.
- Schemes mostly use **average instances** of hard problems.
- Worst-case hardness $\overset{?}{\Longrightarrow}$ Average-case hardness.

(ℓ-)Isogeny(Path) worst-case to average-case reduction

Worst-case to average-case reductions

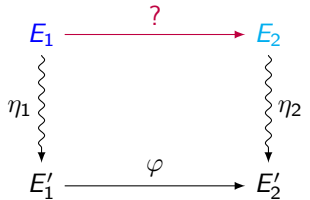
- **Core hardness assumption:**
  There exist hard instances of the Isogeny problem, i.e. **the worst-case is hard**.
- Schemes mostly use **average instances** of hard problems.
- Worst-case hardness $\overset{?}{\Longrightarrow}$ Average-case hardness.



(ℓ-)Isogeny(Path) worst-case to average-case reduction

Worst-case to average-case reductions

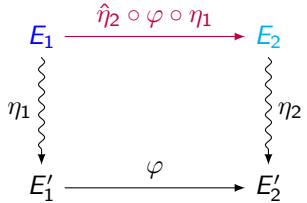
- **Core hardness assumption:**
  There exist hard instances of the Isogeny problem, i.e. **the worst-case is hard**.
- Schemes mostly use **average instances** of hard problems.
- Worst-case hardness $\overset{?}{\Longrightarrow}$ Average-case hardness.



(ℓ-)Isogeny(Path) worst-case to average-case reduction

Worst-case to average-case reductions

- **Core hardness assumption:**
  There exist hard instances of the Isogeny problem, i.e. **the worst-case is hard**.
- Schemes mostly use **average instances** of hard problems.
- Worst-case hardness $\overset{?}{\Longrightarrow}$ Average-case hardness.



(ℓ-)Isogeny(Path) worst-case to average-case reduction

Conclusion

Theorem ([HLM. Wesolowski 2025])

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

Isogeny, EndRing, OneEnd, HomModule *and* **MaxOrder**

we have an unconditional probabilistic polynomial time reduction

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

except if $Q =$ **MaxOrder** *and* $p \equiv 1 \mod 8$.

Conclusion

Theorem ([HLM. Wesolowski 2025])

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

Isogeny, EndRing, OneEnd, HomModule *and* **MaxOrder**

we have an unconditional probabilistic polynomial time reduction

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

except if $Q =$ **MaxOrder** *and* $p \equiv 1 \mod 8$.
(Recall: They are all unconditionally equivalent in the worst-case.)

Conclusion

Theorem ([HLM. Wesolowski 2025])

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

Isogeny, EndRing, OneEnd, HomModule *and* **MaxOrder**

we have an unconditional probabilistic polynomial time reduction

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

except if $Q =$ **MaxOrder** *and* $p \equiv 1 \mod 8$.
(Recall: They are all unconditionally equivalent in the worst-case.)

Open questions:

- How to unconditionally reduce worst-case problems to MaxOrder average-case?

Conclusion

Theorem ([HLM. Wesolowski 2025])

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

Isogeny, EndRing, OneEnd, HomModule *and* **MaxOrder**

we have an unconditional probabilistic polynomial time reduction

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

except if $Q =$ **MaxOrder** *and* $p \equiv 1 \mod 8$.
(Recall: They are all unconditionally equivalent in the worst-case.)

Open questions:

- How to unconditionally reduce worst-case problems to MaxOrder average-case?
- Can we reduce ℓ-IsogenyPath to another problem without GRH?

Conclusion

Theorem ([HLM. Wesolowski 2025])

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

Isogeny, EndRing, OneEnd, HomModule *and* **MaxOrder**

we have an unconditional probabilistic polynomial time reduction

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

except if $Q =$ **MaxOrder** *and* $p \equiv 1 \mod 8$.
(Recall: They are all unconditionally equivalent in the worst-case.)

Open questions:

- How to unconditionally reduce worst-case problems to MaxOrder average-case?
- Can we reduce ℓ-IsogenyPath to another problem without GRH?

Thanks for your attention!
https://ia.cr/2025/271

Bibliography I

[Csa+22] Tímea Csahók et al. "Explicit isomorphisms of quaternion algebras over quadratic global fields". In: Research in Number Theory 8.4 (2022). Publisher: Springer, p. 77.

[CSV22] Wouter Castryck, Jana Sotáková, and Frederik Vercauteren. "Breaking the Decisional Diffie–Hellman Problem for Class Group Actions Using Genus Theory: Extended Version". en. In: Journal of Cryptology 35.4 (Oct. 2022), p. 24. issn: 0933-2790, 1432-1378. doi: 10.1007/s00145-022-09435-1. url: https://link.springer.com/10.1007/s00145-022-09435-1 (visited on 02/14/2023).

[EHM17] Kirsten Eisentraeger, Sean Hallgren, and Travis Morrison. On the Hardness of Computing Endomorphism Rings of Supersingular Elliptic Curves. Cryptology ePrint Archive, Paper 2017/986. 2017. url: https://eprint.iacr.org/2017/986.

Bibliography II

[Eis+18] Kirsten Eisentraeger et al.
Supersingular isogeny graphs and endomorphism rings: reductions and solutions.
Published: Cryptology ePrint Archive, Paper 2018/371. 2018. url: https://eprint.iacr.org/2018/371.

[HLMW23] Arthur Herlédan Le Merdy and Benjamin Wesolowski.
The supersingular endomorphism ring problem given one endomorphism.
Published: Cryptology ePrint Archive, Paper 2023/1448. 2023. url: https://eprint.iacr.org/2023/1448.

[Koh+14] David Kohel et al. On the quaternion \ell-isogeny path problem. _eprint: 1406.0981. 2014.

[Lag77] Odlyzko Lagarias. "Effective Versions of the Chebotarev Density Theorem". en. In: (1977).

Bibliography III

[Mai+23] Luciano Maino et al. "A Direct Key Recovery Attack on SIDH". In: Advances in Cryptology – EUROCRYPT 2023. Ed. by Carmit Hazay and Martijn Stam. Cham: Springer Nature Switzerland, 2023, pp. 448–471. isbn: 978-3-031-30589-4.

[PL17] Christophe Petit and Kristin Lauter. Hard and Easy Problems for Supersingular Isogeny Graphs. Cryptology ePrint Archive, Paper 2017/962. 2017. url: https://eprint.iacr.org/2017/962.

[PR23] Aurel Page and Damien Robert. "Introducing Clapoti(s): Evaluating the isogeny class group action in polynomial time". en. In: (2023).

[PW23] Aurel Page and Benjamin Wesolowski. The supersingular Endomorphism Ring and One Endomorphism problems are equivalent. Published: Cryptology ePrint Archive, Paper 2023/1399. 2023. url: https://eprint.iacr.org/2023/1399.

[Rob22a] Damien Robert. Breaking SIDH in polynomial time. Published: Cryptology ePrint Archive, Paper 2022/1038. 2022. url: https://eprint.iacr.org/2022/1038.

Bibliography IV

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

[Rob24] Damien Robert. "On the efficient representation of isogenies". en. In: (2024).

[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, Denve IEEE, 2021, pp. 1100–1111. doi: 10.1109/FOCS52979.2021.00109. url: https://doi.org/10.1109/FOCS52979.2021.00109.

Bibliography V

[Wes22] Benjamin Wesolowski. "The supersingular isogeny path and endomorphism ring problems are equivalent". en. In: 2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS). Denver, CO, USA: IEEE, Feb. 2022, pp. 1100–1111. isbn: 978-1-66542-055-6. doi: 10.1109/FOCS52979.2021.00109. url: https://ieeexplore.ieee.org/document/9719728/ (visited on 11/14/2022).

Finding q_p

Why computing this quaternion algebra $\left(\frac{-p,-q_p}{\mathbb{Q}}\right)$?

Finding q_p

Why computing this quaternion algebra $(\frac{-p,-q_p}{\mathbb{Q}})$?

- To work in the same quaternion algebra,

Finding q_p

Why computing this quaternion algebra $\left(\frac{-p,-q_p}{\mathbb{Q}}\right)$?

- To work in the same quaternion algebra,
- To get a special curve E_0.

Finding q_p

Why computing this quaternion algebra $(\frac{-p,-q_p}{\mathbb{Q}})$?

- To work in the same quaternion algebra,
- To get a special curve E_0.

Proposition [Csa+22]

Let A_1, A_2 be two quaternion algebras isomorphic to $(\frac{-p,-q_p}{\mathbb{Q}})$.
Given $\mathcal{O}_1$ (resp. $\mathcal{O}_2$) a maximal order in A_1 (resp. A_2), one can compute an isomorphism between A_1 and A_2 in polynomial time.

Finding q_p

Why computing this quaternion algebra $(\frac{-p,-q_p}{\mathbb{Q}})$?

- To work in the same quaternion algebra,
- To get a special curve E_0.

Proposition [Csa+22]

Let A_1, A_2 be two quaternion algebras isomorphic to $(\frac{-p,-q_p}{\mathbb{Q}})$.
Given $\mathcal{O}_1$ (resp. $\mathcal{O}_2$) a maximal order in A_1 (resp. A_2), one can compute an isomorphism between A_1 and A_2 in polynomial time.

Finding q_p

Why computing this quaternion algebra $(\frac{-p,-q_p}{\mathbb{Q}})$?

- To work in the same quaternion algebra,
- To get a special curve E_0.

Proposition [Csa+22]

Let A_1, A_2 be two quaternion algebras isomorphic to $(\frac{-p,-q_p}{\mathbb{Q}})$.
Given $\mathcal{O}_1$ (resp. $\mathcal{O}_2$) a maximal order in A_1 (resp. A_2), one can compute an isomorphism between A_1 and A_2 in polynomial time.

`MaxOrder`

Given E a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$, compute a quaternion algebra $(\frac{-a,-b}{\mathbb{Q}})$ isomorphic to $(\frac{-p,-q_p}{\mathbb{Q}})$ together with a maximal order $\mathcal{O} \subset (\frac{-a,-b}{\mathbb{Q}})$ isomorphic to $\mathrm{End}(E)$.

Finding q_p

Why computing this quaternion algebra $(\frac{-p,-q_p}{\mathbb{Q}})$?

- To work in the same quaternion algebra,
- To get a special curve E_0.

Proposition [Csa+22]

Let A_1, A_2 be two quaternion algebras isomorphic to $(\frac{-p,-q_p}{\mathbb{Q}})$.
Given $\mathcal{O}_1$ (resp. $\mathcal{O}_2$) a maximal order in A_1 (resp. A_2), one can compute an isomorphism between A_1 and A_2 in polynomial time.

`MaxOrder`

Given E a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$, compute a quaternion algebra $(\frac{-a,-b}{\mathbb{Q}})$ isomorphic to $(\frac{-p,-q_p}{\mathbb{Q}})$ together with a maximal order $\mathcal{O} \subset (\frac{-a,-b}{\mathbb{Q}})$ isomorphic to $\mathrm{End}(E)$.

This does not solve the special curve issue.

Finding q_p

Why computing this quaternion algebra $(\frac{-p,-q_p}{\mathbb{Q}})$?

- To work in the same quaternion algebra,
- To get a special curve E_0.

Proposition [Csa+22]

Let A_1, A_2 be two quaternion algebras isomorphic to $(\frac{-p,-q_p}{\mathbb{Q}})$.
Given $\mathcal{O}_1$ (resp. $\mathcal{O}_2$) a maximal order in A_1 (resp. A_2), one can compute an isomorphism between A_1 and A_2 in polynomial time.

`MaxOrder`

Given E a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$, compute a quaternion algebra $(\frac{-a,-b}{\mathbb{Q}})$ isomorphic to $(\frac{-p,-q_p}{\mathbb{Q}})$ together with a maximal order $\mathcal{O} \subset (\frac{-a,-b}{\mathbb{Q}})$ isomorphic to $\mathrm{End}(E)$.

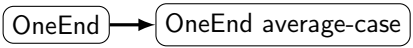
This does not solve the special curve issue.

Worst-case to Average-case reductions

OneEnd

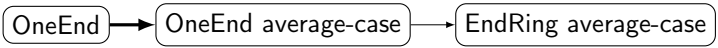
Summary of worst-case to average-case reductions

Worst-case to Average-case reductions



Summary of worst-case to average-case reductions

Worst-case to Average-case reductions

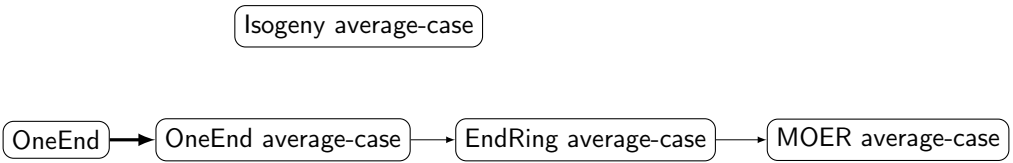


Summary of worst-case to average-case reductions

Worst-case to Average-case reductions

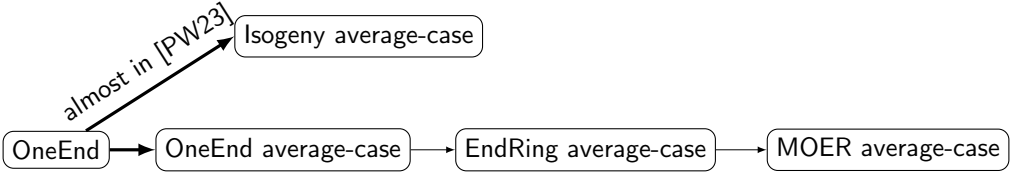
Summary of worst-case to average-case reductions

Worst-case to Average-case reductions



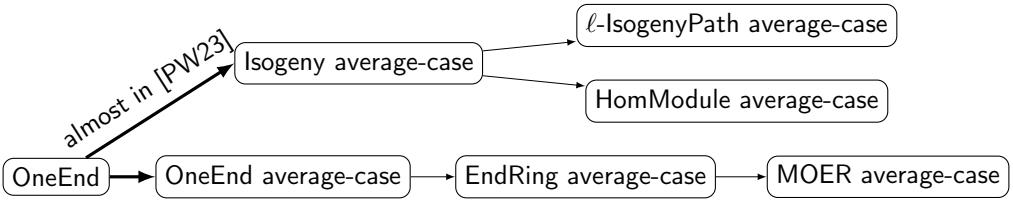
Summary of worst-case to average-case reductions

Worst-case to Average-case reductions



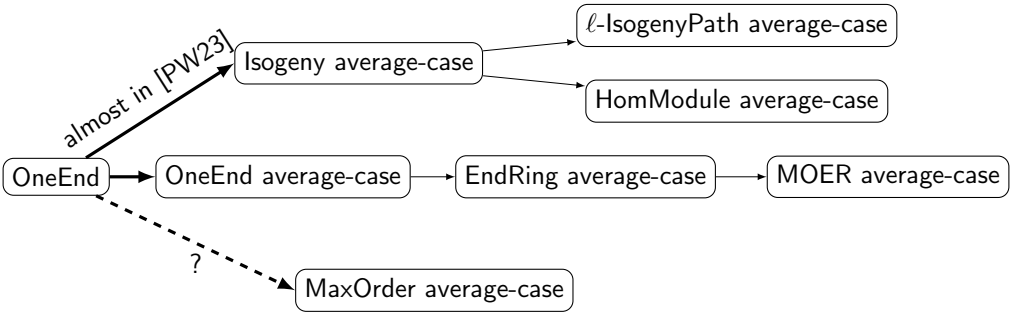
Summary of worst-case to average-case reductions

Worst-case to Average-case reductions



Summary of worst-case to average-case reductions

Worst-case to Average-case reductions

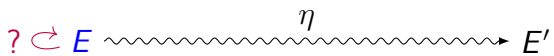


Summary of worst-case to average-case reductions

OneEnd worst-case to MaxOrder average-case

MOER worst-case to MaxOrder average-case

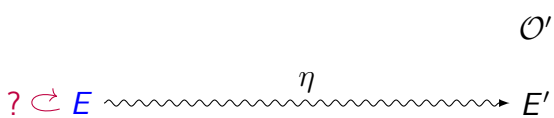
OneEnd worst-case to MaxOrder average-case



MOER worst-case to MaxOrder average-case

OneEnd worst-case to MaxOrder average-case

Oracle output: $\mathcal{O}' \subseteq (\frac{-a,-b}{\mathbb{Q}})$ such that $\mathcal{O}' \simeq \mathrm{End}(E')$



MOER worst-case to MaxOrder average-case

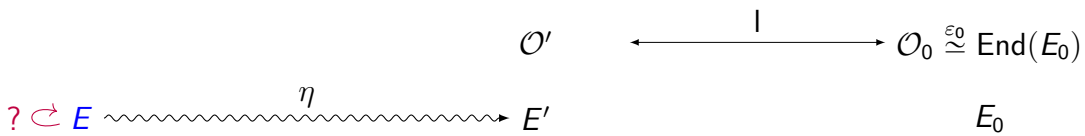
OneEnd worst-case to MaxOrder average-case

Oracle output: $\mathcal{O}' \subseteq (\frac{-a,-b}{\mathbb{Q}})$ such that $\mathcal{O}' \simeq \mathsf{End}(E')$

MOER worst-case to MaxOrder average-case

OneEnd worst-case to MaxOrder average-case

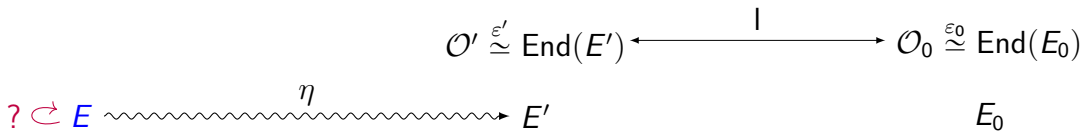
Oracle output: $\mathcal{O}' \subseteq (\frac{-a,-b}{\mathbb{Q}})$ such that $\mathcal{O}' \simeq \mathsf{End}(E')$



MOER worst-case to MaxOrder average-case

OneEnd worst-case to MaxOrder average-case

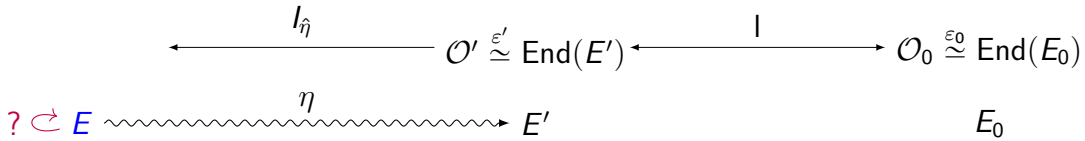
Oracle output: $\mathcal{O}' \subseteq (\frac{-a,-b}{\mathbb{Q}})$ such that $\mathcal{O}' \simeq \mathsf{End}(E')$



MOER worst-case to MaxOrder average-case

OneEnd worst-case to MaxOrder average-case

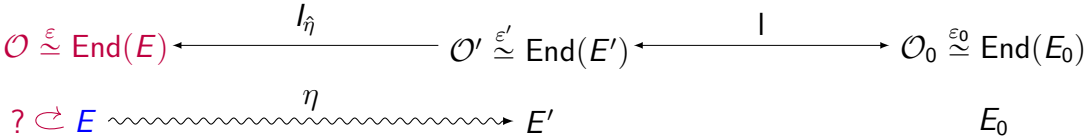
Oracle output: $\mathcal{O}' \subseteq (\frac{-a,-b}{\mathbb{Q}})$ such that $\mathcal{O}' \simeq \mathrm{End}(E')$



MOER worst-case to MaxOrder average-case

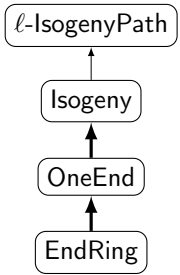
OneEnd worst-case to MaxOrder average-case

Oracle output: $\mathcal{O}' \subseteq (\frac{-a,-b}{\mathbb{Q}})$ such that $\mathcal{O}' \simeq \mathsf{End}(E')$



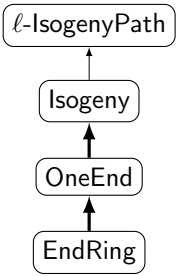
MOER worst-case to MaxOrder average-case

HomModule reduces to ℓ-IsogenyPath



Polynomial reductions [PW23]

HomModule reduces to ℓ-IsogenyPath



Polynomial reductions [PW23]

+

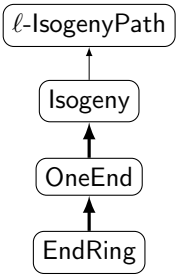
Lemma

Let $\varphi : E \to E'$ be a separable isogeny. Then,

$$\mathrm{span}_{\mathbb{Z}}(\mathrm{End}(E')\varphi\,\mathrm{End}(E)) = m\,\mathrm{Hom}(E, E'),$$

where $m \in \mathbb{Z}$ is the largest integer dividing φ.

HomModule reduces to ℓ-IsogenyPath



Polynomial reductions [PW23]

+

Lemma

Let $\varphi : E \to E'$ be a separable isogeny. Then,

$$\mathrm{span}_{\mathbb{Z}}(\mathrm{End}(E')\varphi\,\mathrm{End}(E)) = m\,\mathrm{Hom}(E, E'),$$

where $m \in \mathbb{Z}$ is the largest integer dividing φ.

The reduction

1. Compute $\mathrm{End}(E)$ and $\mathrm{End}(E')$
2. Compute $\varphi : E \to E'$
3. Compute a basis $(\gamma_1, \ldots, \gamma_4)$ of $\mathrm{span}_{\mathbb{Z}}(\mathrm{End}(E')\varphi\,\mathrm{End}(E)) = m\,\mathrm{Hom}(E, E')$
4. Return this basis divided by m [Rob22b; HLMW23]