

# PEGASIS

## Practical Efficient Class Group Action using 4-dimensional isogenies

*Joint with Pierrick Dartois, Jonathan Komada Eriksen, Tako Boris Fouotsa, Arthur Herledan Le Merdy, Riccardo Invernizzi, Damien Robert, Frederik Vercauteren and Benjamin Wesolowski*

<https://eprint.iacr.org/2025/401>

Ryan Rueger

IBM Research Zurich & Technical University of Munich

Practically **Efficient** Class **Group Action** using 4-dimensional isogenies

Practically Efficient Class Group Action using 4-dimensional isogenies

Practically Efficient **Class Group Action** using 4-dimensional isogenies

Practically Efficient Class Group Action using 4-dimensional isogenies

## Results

	Impl.	500	1000	1500	2000	4000
SCALLOP*	C++	35s	750s			
SCALLOP-HD*	Sage	88s	1140s			
PEARL-SCALLOP*	C++	30s	58s	710s		
KLaPoTi	Sage	207s				
	Rust	1.95s				
<b>PEGASIS</b>	Sage	1.53s	4.21s	10.5s	21.3s	121s

**Table:** Time measured in wall-clock time. Stars indicate different measuring hardware.

## Oriented Actions

Imaginary quadratic order  $\mathcal{O} = \mathbb{Z}[\alpha]$

Supersingular Elliptic curve  $E/F_{p^2}$

## Oriented Actions

Imaginary quadratic order  $\mathcal{O} = \mathbb{Z}[\alpha]$

Supersingular Elliptic curve  $E/F_{p^2}$

**Primitive orientation**  $\iota: \mathcal{O} \hookrightarrow \text{End}(E)$  defined by  $\alpha \mapsto \omega$  with  $\omega$  primitive



## Oriented Actions

Imaginary quadratic order  $\mathcal{O} = \mathbb{Z}[\alpha]$

Supersingular Elliptic curve  $E/F_{p^2}$

**Primitive orientation**  $\iota: \mathcal{O} \hookrightarrow \text{End}(E)$  defined by  $\alpha \mapsto \omega$  with  $\omega$  primitive

**Primitively oriented** elliptic curve  $(E, \iota)$

## Oriented Actions

Imaginary quadratic order  $\mathcal{O} = \mathbb{Z}[\alpha]$

Supersingular Elliptic curve  $E/F_{p^2}$

**Primitive orientation**  $\iota: \mathcal{O} \hookrightarrow \text{End}(E)$  defined by  $\alpha \mapsto \omega$  with  $\omega$  primitive

**Primitively oriented** elliptic curve  $(E, \iota)$

Integral invertible ideal  $\mathfrak{a}$  with  $p \nmid N(\mathfrak{a})$  yields isogeny  $\varphi_{\mathfrak{a}}: E \rightarrow E_{\mathfrak{a}}$

## Oriented Actions

Imaginary quadratic order  $\mathcal{O} = \mathbb{Z}[\alpha]$

Supersingular Elliptic curve  $E/F_{p^2}$

**Primitive orientation**  $\iota: \mathcal{O} \hookrightarrow \text{End}(E)$  defined by  $\alpha \mapsto \omega$  with  $\omega$  primitive

**Primitively oriented** elliptic curve  $(E, \iota)$

Integral invertible ideal  $\mathfrak{a}$  with  $p \nmid N(\mathfrak{a})$  yields isogeny  $\varphi_{\mathfrak{a}}: E \rightarrow E_{\mathfrak{a}}$

...with  $\ker(\varphi_{\mathfrak{a}}) = E[\mathfrak{a}] = \bigcap_{a \in \mathfrak{a}} \ker(a)$  and  $\deg(\varphi_{\mathfrak{a}}) = N(\mathfrak{a})$

## Oriented Actions

Imaginary quadratic order  $\mathcal{O} = \mathbb{Z}[\alpha]$

Supersingular Elliptic curve  $E/F_{p^2}$

**Primitive orientation**  $\iota: \mathcal{O} \hookrightarrow \text{End}(E)$  defined by  $\alpha \mapsto \omega$  with  $\omega$  primitive

**Primitively oriented** elliptic curve  $(E, \iota)$

Integral invertible ideal  $\mathfrak{a}$  with  $p \nmid N(\mathfrak{a})$  yields isogeny  $\varphi_{\mathfrak{a}}: E \rightarrow E_{\mathfrak{a}}$

...with  $\ker(\varphi_{\mathfrak{a}}) = E[\mathfrak{a}] = \bigcap_{a \in \mathfrak{a}} \ker(a)$  and  $\deg(\varphi_{\mathfrak{a}}) = N(\mathfrak{a})$

...and if  $\mathfrak{a}$  principal then  $\varphi_{\mathfrak{a}}$  is an endomorphism

## Oriented Actions

Imaginary quadratic order  $\mathcal{O} = \mathbb{Z}[\alpha]$

Supersingular Elliptic curve  $E/F_{p^2}$

**Primitive orientation**  $\iota: \mathcal{O} \hookrightarrow \text{End}(E)$  defined by  $\alpha \mapsto \omega$  with  $\omega$  primitive

**Primitively oriented** elliptic curve  $(E, \iota)$

Integral invertible ideal  $\mathfrak{a}$  with  $p \nmid N(\mathfrak{a})$  yields isogeny  $\varphi_{\mathfrak{a}}: E \rightarrow E_{\mathfrak{a}}$

...with  $\ker(\varphi_{\mathfrak{a}}) = E[\mathfrak{a}] = \bigcap_{a \in \mathfrak{a}} \ker(a)$  and  $\deg(\varphi_{\mathfrak{a}}) = N(\mathfrak{a})$

...and if  $\mathfrak{a}$  principal then  $\varphi_{\mathfrak{a}}$  is an endomorphism

Moreover  $(\varphi_{\mathfrak{a}})_*(\iota): \mathcal{O} \rightarrow \text{End}(E_{\mathfrak{a}}); \gamma \mapsto \varphi_{\mathfrak{a}}\iota(\gamma)\widetilde{\varphi}_{\mathfrak{a}}/[N(\mathfrak{a})]$  is a primitive orientation

## Oriented Actions

Imaginary quadratic order  $\mathcal{O} = \mathbb{Z}[\alpha]$

Supersingular Elliptic curve  $E/F_{p^2}$

**Primitive orientation**  $\iota: \mathcal{O} \hookrightarrow \text{End}(E)$  defined by  $\alpha \mapsto \omega$  with  $\omega$  primitive

**Primitively oriented** elliptic curve  $(E, \iota)$

Integral invertible ideal  $\mathfrak{a}$  with  $p \nmid N(\mathfrak{a})$  yields isogeny  $\varphi_{\mathfrak{a}}: E \rightarrow E_{\mathfrak{a}}$

...with  $\ker(\varphi_{\mathfrak{a}}) = E[\mathfrak{a}] = \bigcap_{a \in \mathfrak{a}} \ker(a)$  and  $\deg(\varphi_{\mathfrak{a}}) = N(\mathfrak{a})$

...and if  $\mathfrak{a}$  principal then  $\varphi_{\mathfrak{a}}$  is an endomorphism

Moreover  $(\varphi_{\mathfrak{a}})_*(\iota): \mathcal{O} \rightarrow \text{End}(E_{\mathfrak{a}}); \gamma \mapsto \varphi_{\mathfrak{a}}\iota(\gamma)\widetilde{\varphi}_{\mathfrak{a}}/[N(\mathfrak{a})]$  is a primitive orientation

...so  $(E_{\mathfrak{a}}, (\varphi_{\mathfrak{a}})_*(\iota))$  is **primitively oriented**

## Oriented Actions

Imaginary quadratic order  $\mathcal{O} = \mathbb{Z}[\alpha]$

Supersingular Elliptic curve  $E/F_{p^2}$

**Primitive orientation**  $\iota: \mathcal{O} \hookrightarrow \text{End}(E)$  defined by  $\alpha \mapsto \omega$  with  $\omega$  primitive

**Primitively oriented** elliptic curve  $(E, \iota)$

Integral invertible ideal  $\mathfrak{a}$  with  $p \nmid N(\mathfrak{a})$  yields isogeny  $\varphi_{\mathfrak{a}}: E \rightarrow E_{\mathfrak{a}}$

...with  $\ker(\varphi_{\mathfrak{a}}) = E[\mathfrak{a}] = \bigcap_{a \in \mathfrak{a}} \ker(a)$  and  $\deg(\varphi_{\mathfrak{a}}) = N(\mathfrak{a})$

...and if  $\mathfrak{a}$  principal then  $\varphi_{\mathfrak{a}}$  is an endomorphism

Moreover  $(\varphi_{\mathfrak{a}})_*(\iota): \mathcal{O} \rightarrow \text{End}(E_{\mathfrak{a}}); \gamma \mapsto \varphi_{\mathfrak{a}}\iota(\gamma)\widetilde{\varphi}_{\mathfrak{a}}/[N(\mathfrak{a})]$  is a primitive orientation

...so  $(E_{\mathfrak{a}}, (\varphi_{\mathfrak{a}})_*(\iota))$  is **primitively oriented**

We say  $\varphi: E \rightarrow E'$  is an  **$\mathcal{O}$ -isomorphism**  $(E, \iota) \rightarrow (E', \iota')$  if  $\iota' = (\varphi)_*(\iota)$

## Oriented Actions

Imaginary quadratic order  $\mathcal{O} = \mathbb{Z}[\alpha]$

Supersingular Elliptic curve  $E/F_{p^2}$

**Primitive orientation**  $\iota: \mathcal{O} \hookrightarrow \text{End}(E)$  defined by  $\alpha \mapsto \omega$  with  $\omega$  primitive

**Primitively oriented** elliptic curve  $(E, \iota)$

Integral invertible ideal  $\mathfrak{a}$  with  $p \nmid N(\mathfrak{a})$  yields isogeny  $\varphi_{\mathfrak{a}}: E \rightarrow E_{\mathfrak{a}}$

...with  $\ker(\varphi_{\mathfrak{a}}) = E[\mathfrak{a}] = \bigcap_{a \in \mathfrak{a}} \ker(a)$  and  $\deg(\varphi_{\mathfrak{a}}) = N(\mathfrak{a})$

...and if  $\mathfrak{a}$  principal then  $\varphi_{\mathfrak{a}}$  is an endomorphism

Moreover  $(\varphi_{\mathfrak{a}})_*(\iota): \mathcal{O} \rightarrow \text{End}(E_{\mathfrak{a}}); \gamma \mapsto \varphi_{\mathfrak{a}}\iota(\gamma)\widetilde{\varphi_{\mathfrak{a}}}/[N(\mathfrak{a})]$  is a primitive orientation

...so  $(E_{\mathfrak{a}}, (\varphi_{\mathfrak{a}})_*(\iota))$  is **primitively oriented**

We say  $\varphi: E \rightarrow E'$  is an  **$\mathcal{O}$ -isomorphism**  $(E, \iota) \rightarrow (E', \iota')$  if  $\iota' = (\varphi)_*(\iota)$

...and define  $\text{SS}_p^{\text{pr}}(\mathcal{O})$  to be  $\mathcal{O}$ -isomorphism classes of  $(E, \iota)$



## Oriented Actions

Imaginary quadratic order  $\mathcal{O} = \mathbb{Z}[\alpha]$

Supersingular Elliptic curve  $E/F_{p^2}$

**Primitive orientation**  $\iota: \mathcal{O} \hookrightarrow \text{End}(E)$  defined by  $\alpha \mapsto \omega$  with  $\omega$  primitive

**Primitively oriented** elliptic curve  $(E, \iota)$

Integral invertible ideal  $\mathfrak{a}$  with  $p \nmid N(\mathfrak{a})$  yields isogeny  $\varphi_{\mathfrak{a}}: E \rightarrow E_{\mathfrak{a}}$

...with  $\ker(\varphi_{\mathfrak{a}}) = E[\mathfrak{a}] = \bigcap_{a \in \mathfrak{a}} \ker(a)$  and  $\deg(\varphi_{\mathfrak{a}}) = N(\mathfrak{a})$

...and if  $\mathfrak{a}$  principal then  $\varphi_{\mathfrak{a}}$  is an endomorphism

Moreover  $(\varphi_{\mathfrak{a}})_*(\iota): \mathcal{O} \rightarrow \text{End}(E_{\mathfrak{a}}); \gamma \mapsto \varphi_{\mathfrak{a}}\iota(\gamma)\widetilde{\varphi}_{\mathfrak{a}}/[N(\mathfrak{a})]$  is a primitive orientation

...so  $(E_{\mathfrak{a}}, (\varphi_{\mathfrak{a}})_*(\iota))$  is **primitively oriented**

We say  $\varphi: E \rightarrow E'$  is an  **$\mathcal{O}$ -isomorphism**  $(E, \iota) \rightarrow (E', \iota')$  if  $\iota' = (\varphi)_*(\iota)$

...and define  $SS_p^{\text{pr}}(\mathcal{O})$  to be  $\mathcal{O}$ -isomorphism classes of  $(E, \iota)$

Finally we get an action of  $\text{Cl}(\mathcal{O})$  on  $SS_p^{\text{pr}}(\mathcal{O})$

## Oriented Actions

Imaginary quadratic order  $\mathcal{O} = \mathbb{Z}[\alpha]$

Supersingular Elliptic curve  $E/F_{p^2}$

**Primitive orientation**  $\iota: \mathcal{O} \hookrightarrow \text{End}(E)$  defined by  $\alpha \mapsto \omega$  with  $\omega$  primitive

**Primitively oriented** elliptic curve  $(E, \iota)$

Integral invertible ideal  $\mathfrak{a}$  with  $p \nmid N(\mathfrak{a})$  yields isogeny  $\varphi_{\mathfrak{a}}: E \rightarrow E_{\mathfrak{a}}$

...with  $\ker(\varphi_{\mathfrak{a}}) = E[\mathfrak{a}] = \bigcap_{a \in \mathfrak{a}} \ker(a)$  and  $\deg(\varphi_{\mathfrak{a}}) = N(\mathfrak{a})$

...and if  $\mathfrak{a}$  principal then  $\varphi_{\mathfrak{a}}$  is an endomorphism

Moreover  $(\varphi_{\mathfrak{a}})_*(\iota): \mathcal{O} \rightarrow \text{End}(E_{\mathfrak{a}}); \gamma \mapsto \varphi_{\mathfrak{a}}\iota(\gamma)\widetilde{\varphi_{\mathfrak{a}}}/[N(\mathfrak{a})]$  is a primitive orientation

...so  $(E_{\mathfrak{a}}, (\varphi_{\mathfrak{a}})_*(\iota))$  is **primitively oriented**

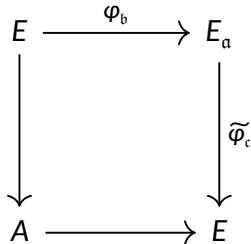
We say  $\varphi: E \rightarrow E'$  is an  **$\mathcal{O}$ -isomorphism**  $(E, \iota) \rightarrow (E', \iota')$  if  $\iota' = (\varphi)_*(\iota)$

...and define  $SS_p^{\text{pr}}(\mathcal{O})$  to be  $\mathcal{O}$ -isomorphism classes of  $(E, \iota)$

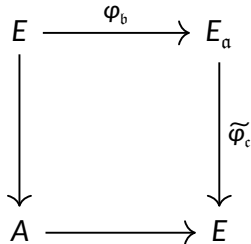
Finally we get an action of  $\text{Cl}(\mathcal{O})$  on  $SS_p^{\text{pr}}(\mathcal{O})$

**Theorem** (Onuki) This action is transitive with at most two orbits

# The Ideal2Isogeny Construction

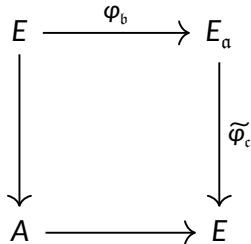


## The Ideal2Isogeny Construction



$$\begin{aligned}\ker(\Phi) &= \left\{ (N(\alpha)x, \widetilde{\varphi}_c \varphi_b(x)) \mid x \in E_u[\deg_p(\Phi)] \right\} \\ &= \left\{ (N(\alpha)x, \varphi_{\bar{c}b}(x)) \mid x \in E_u[\deg_p(\Phi)] \right\}\end{aligned}$$

## The Ideal2Isogeny Construction



$$\begin{aligned} \ker(\Phi) &= \left\{ (N(a)x, \widetilde{\varphi}_c(\varphi_b(x))) \mid x \in E_u[\deg_p(\Phi)] \right\} \\ &= \left\{ (N(a)x, \varphi_{\widetilde{c}b}(x)) \mid x \in E_u[\deg_p(\Phi)] \right\} \end{aligned}$$

Norm equation  $\deg_p(\Phi) = N(a) + N(b) \stackrel{!}{=} 2^f$

## The Ideal2Isogeny Construction

$$\begin{array}{ccc} E & \xrightarrow{\varphi_b} & E_a \\ \downarrow & & \downarrow \widetilde{\varphi_c} \\ A & \longrightarrow & E \end{array}$$

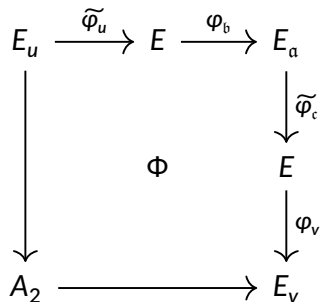
$$\begin{aligned} \ker(\Phi) &= \left\{ (N(a)x, \widetilde{\varphi_c} \varphi_b(x)) \mid x \in E_u[\deg_p(\Phi)] \right\} \\ &= \left\{ (N(a)x, \varphi_{\widetilde{c}b}(x)) \mid x \in E_u[\deg_p(\Phi)] \right\} \end{aligned}$$

Norm equation  $\deg_p(\Phi) = N(a) + N(b) \stackrel{!}{=} 2^f$

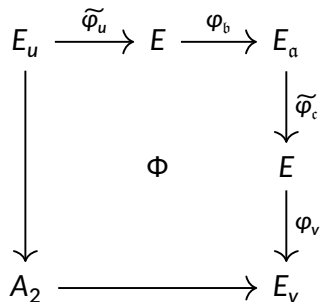
Requirements

1.  $f < e = v_2(p+1)$
2.  $\gcd(N(a), N(b)) = 1$

## The Ideal2Isogeny Construction: Iteration #2



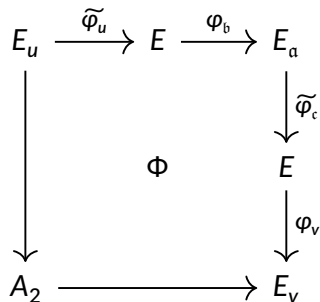
## The Ideal2Isogeny Construction: Iteration #2



$$\begin{aligned}
 & \ker(\Phi) \\
 &= \left\{ (uN(a)x, \varphi_v \tilde{\varphi}_c \varphi_b \tilde{\varphi}_u(x)) \mid x \in E_u[\deg_p(\Phi)] \right\} \\
 &= \left\{ (N(a)\varphi_u(y), \varphi_v \tilde{\varphi}_c \varphi_b(y)) \mid y \in E[\deg_p(\Phi)] \right\} \\
 &= \left\{ (N(a)\varphi_u(y), \varphi_v \varphi_{\tilde{c}b}(y)) \mid y \in E[\deg_p(\Phi)] \right\}
 \end{aligned}$$



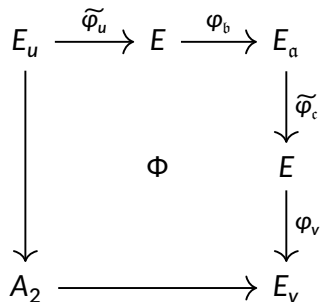
## The Ideal2Isogeny Construction: Iteration #2



$$\begin{aligned}
 & \ker(\Phi) \\
 &= \left\{ (uN(a)x, \varphi_v \widetilde{\varphi}_c \varphi_b \widetilde{\varphi}_u(x)) \mid x \in E_u[\deg_p(\Phi)] \right\} \\
 &= \left\{ (N(a)\varphi_u(y), \varphi_v \widetilde{\varphi}_c \varphi_b(y)) \mid y \in E[\deg_p(\Phi)] \right\} \\
 &= \left\{ (N(a)\varphi_u(y), \varphi_v \varphi_{\widetilde{c}b}(y)) \mid y \in E[\deg_p(\Phi)] \right\}
 \end{aligned}$$

Norm equation  $\deg_p(\Phi) = uN(a) + vN(b) \stackrel{!}{=} 2^f$

## The Ideal2Isogeny Construction: Iteration #2



$$\begin{aligned}
 \ker(\Phi) &= \left\{ (uN(a)x, \varphi_v \widetilde{\varphi}_c \varphi_b \widetilde{\varphi}_u(x)) \mid x \in E_u[\deg_p(\Phi)] \right\} \\
 &= \left\{ (N(a)\varphi_u(y), \varphi_v \widetilde{\varphi}_c \varphi_b(y)) \mid y \in E[\deg_p(\Phi)] \right\} \\
 &= \left\{ (N(a)\varphi_u(y), \varphi_v \varphi_{\widetilde{c}b}(y)) \mid y \in E[\deg_p(\Phi)] \right\}
 \end{aligned}$$

Norm equation  $\deg_p(\Phi) = uN(a) + vN(b) \stackrel{!}{=} 2^f$

Requirements

1.  $f < e = v_2(p+1)$
2.  $\gcd(uN(a), vN(b)) = 1$
3.  $u = \deg_p(\varphi_u), v = \deg_p(\varphi_v)$

## The Ideal2Isogeny Construction: Iteration #3

$$\begin{array}{ccccc} A_u & \xrightarrow{\widetilde{\varphi}_u} & E^d & \xrightarrow{\text{diag}(\varphi_e)} & E_a^d \\ \downarrow & & & & \downarrow \text{diag}(\widetilde{\varphi}_e) \\ & \Phi & & & E^d \\ & & & & \downarrow \varphi_v \\ A_2 & \xrightarrow{\quad\quad\quad} & A_v \end{array}$$

## The Ideal2Isogeny Construction: Iteration #3

$$\begin{array}{ccccc}
 A_u & \xrightarrow{\widetilde{\varphi}_u} & E^d & \xrightarrow{\text{diag}(\varphi_b)} & E_a^d \\
 \downarrow & & & & \downarrow \text{diag}(\widetilde{\varphi}_c) \\
 & & \Phi & & E^d \\
 & & & & \downarrow \varphi_v \\
 A_2 & \xrightarrow{\quad\quad\quad} & A_v
 \end{array}$$

$$\begin{aligned}
 \ker(\Phi) &= \left\{ (uN(a)x, \varphi_v \text{diag}(\widetilde{\varphi}_c \varphi_b) \widetilde{\varphi}_u(x)) \mid x \in E_u[\deg_p(\Phi)] \right\} \\
 &= \left\{ (N(a)\varphi_u(y), \varphi_v \text{diag}(\widetilde{\varphi}_c \varphi_b)(y)) \mid y \in E[\deg_p(\Phi)] \right\} \\
 &= \left\{ (N(a)\varphi_u(y), \varphi_v \text{diag}(\varphi_{\widetilde{c}b})(y)) \mid y \in E[\deg_p(\Phi)] \right\}
 \end{aligned}$$

## The Ideal2Isogeny Construction: Iteration #3

$$\begin{array}{ccccc}
 A_u & \xrightarrow{\widetilde{\varphi}_u} & E^d & \xrightarrow{\text{diag}(\varphi_b)} & E_a^d \\
 \downarrow & & & & \downarrow \text{diag}(\widetilde{\varphi}_c) \\
 & & \Phi & & E^d \\
 & & & & \downarrow \varphi_v \\
 A_2 & \xrightarrow{\quad\quad\quad} & A_v & & 
 \end{array}$$

$$\begin{aligned}
 \ker(\Phi) &= \left\{ (uN(a)x, \varphi_v \text{diag}(\widetilde{\varphi}_c \varphi_b) \widetilde{\varphi}_u(x)) \mid x \in E_u[\deg_p(\Phi)] \right\} \\
 &= \left\{ (N(a)\varphi_u(y), \varphi_v \text{diag}(\widetilde{\varphi}_c \varphi_b)(y)) \mid y \in E[\deg_p(\Phi)] \right\} \\
 &= \left\{ (N(a)\varphi_u(y), \varphi_v \text{diag}(\varphi_{\widetilde{c}b})(y)) \mid y \in E[\deg_p(\Phi)] \right\}
 \end{aligned}$$

Norm equation  $\deg_p(\Phi) = uN(a) + vN(b) \stackrel{!}{=} 2^f$

## The Ideal2Isogeny Construction: Iteration #3

$$\begin{array}{ccccc}
 A_u & \xrightarrow{\widetilde{\varphi}_u} & E^d & \xrightarrow{\text{diag}(\varphi_b)} & E_a^d \\
 \downarrow & & & & \downarrow \text{diag}(\widetilde{\varphi}_c) \\
 & & \Phi & & E^d \\
 & & & & \downarrow \varphi_v \\
 A_2 & \xrightarrow{\quad\quad\quad} & A_v & & 
 \end{array}$$

$$\begin{aligned}
 \ker(\Phi) &= \left\{ (uN(a)x, \varphi_v \text{diag}(\widetilde{\varphi}_c \varphi_b) \widetilde{\varphi}_u(x)) \mid x \in E_u[\deg_p(\Phi)] \right\} \\
 &= \left\{ (N(a)\varphi_u(y), \varphi_v \text{diag}(\widetilde{\varphi}_c \varphi_b)(y)) \mid y \in E[\deg_p(\Phi)] \right\} \\
 &= \left\{ (N(a)\varphi_u(y), \varphi_v \text{diag}(\varphi_{\widetilde{c}b})(y)) \mid y \in E[\deg_p(\Phi)] \right\}
 \end{aligned}$$

Norm equation  $\deg_p(\Phi) = uN(a) + vN(b) \stackrel{!}{=} 2^f$

Requirements

1.  $f < e = v_2(p+1)$
2.  $\gcd(uN(a), vN(b)) = 1$
3.  $u = \deg_p(\varphi_u), v = \deg_p(\varphi_v)$

# Solvability of the norm equation

## Frobenius Coin Problem

$uN(b) + vN(c) = 2^f$  has a solution if  $N(b)N(c) \leq 2^f - N(b) - N(c)$

# Solvability of the norm equation

## Frobenius Coin Problem

$uN(b) + vN(c) = 2^f$  has a solution if  $N(b)N(c) \leq 2^f - N(b) - N(c)$

## Minkowski Bound

Every class in  $Cl(\mathcal{O})$  has a representative of norm at most  $\sqrt{\text{Disc}(\mathcal{O})}$



# Solvability of the norm equation

## Frobenius Coin Problem

$uN(b) + vN(c) = 2^f$  has a solution if  $N(b)N(c) \leq 2^f - N(b) - N(c)$

## Minkowski Bound

Every class in  $Cl(\mathcal{O})$  has a representative of norm at most  $\sqrt{\text{Disc}(\mathcal{O})}$

## Tension

We only permit  $f < e$ , but  $N(b)N(c) \approx \text{Disc}(\mathcal{O}) = p = c2^e - 1 \not\leq 2^f - N(b) - N(c)$

# Solvability of the norm equation

## Frobenius Coin Problem

$uN(b) + vN(c) = 2^f$  has a solution if  $N(b)N(c) \leq 2^f - N(b) - N(c)$

## Minkowski Bound

Every class in  $Cl(\mathcal{O})$  has a representative of norm at most  $\sqrt{\text{Disc}(\mathcal{O})}$

## Tension

We only permit  $f < e$ , but  $N(b)N(c) \approx \text{Disc}(\mathcal{O}) = p = c2^e - 1 \not\leq 2^f - N(b) - N(c)$

# Solvability of the norm equation: An idea

## Recall

Ideals of  $\mathcal{O}$  prime to the conductor factorise uniquely as product of prime ideals

# Solvability of the norm equation: An idea

## Recall

Ideals of  $\mathcal{O}$  prime to the conductor factorise uniquely as product of prime ideals

## Idea

Factor the ideals  $\mathfrak{b} = \mathfrak{b}_e \mathfrak{b}_k, \mathfrak{c} = \mathfrak{c}_e \mathfrak{c}_k$  with action of  $\mathfrak{b}_e, \mathfrak{c}_e$  “easy”

# Solvability of the norm equation: An idea

## Recall

Ideals of  $\mathcal{O}$  prime to the conductor factorise uniquely as product of prime ideals

## Idea

Factor the ideals  $\mathfrak{b} = \mathfrak{b}_e \mathfrak{b}_k, \mathfrak{c} = \mathfrak{c}_e \mathfrak{c}_k$  with action of  $\mathfrak{b}_e, \mathfrak{c}_e$  “easy”

## In practice

Factor so that  $N(\mathfrak{b}_e), N(\mathfrak{c}_e)$  are products of small primes split in  $\mathcal{O}$

# Solvability of the norm equation: An idea

## Recall

Ideals of  $\mathcal{O}$  prime to the conductor factorise uniquely as product of prime ideals

## Idea

Factor the ideals  $\mathfrak{b} = \mathfrak{b}_e \mathfrak{b}_k, \mathfrak{c} = \mathfrak{c}_e \mathfrak{c}_k$  with action of  $\mathfrak{b}_e, \mathfrak{c}_e$  “easy”

## In practice

Factor so that  $N(\mathfrak{b}_e), N(\mathfrak{c}_e)$  are products of small primes split in  $\mathcal{O}$

Example  $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$

Here  $[\mathfrak{b}_e] \cdot E$  computed by successive Elkies isogenies defined over  $F_p$

# Solvability of the norm equation: An idea

## Recall

Ideals of  $\mathcal{O}$  prime to the conductor factorise uniquely as product of prime ideals

## Idea

Factor the ideals  $\mathfrak{b} = \mathfrak{b}_e \mathfrak{b}_k, \mathfrak{c} = \mathfrak{c}_e \mathfrak{c}_k$  with action of  $\mathfrak{b}_e, \mathfrak{c}_e$  “easy”

## In practice

Factor so that  $N(\mathfrak{b}_e), N(\mathfrak{c}_e)$  are products of small primes split in  $\mathcal{O}$

Example  $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$

Here  $[\mathfrak{b}_e] \cdot E$  computed by successive Elkies isogenies defined over  $F_p$

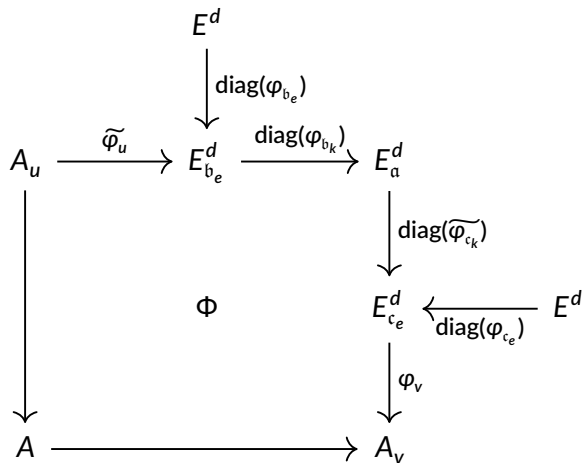
## Outlook

Compute easy part first, norm equation for  $\mathfrak{b}_k, \mathfrak{c}_k$

$$uN(\mathfrak{b}_k) + vN(\mathfrak{c}_k) = 2^f$$

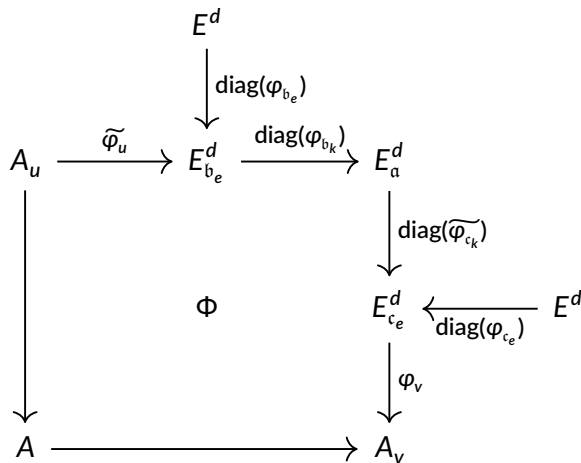
easier to solve because  $N(\mathfrak{b}_k)N(\mathfrak{c}_k) \leq N(\mathfrak{b})N(\mathfrak{c})$

## Solvability of the norm equation: The diagram



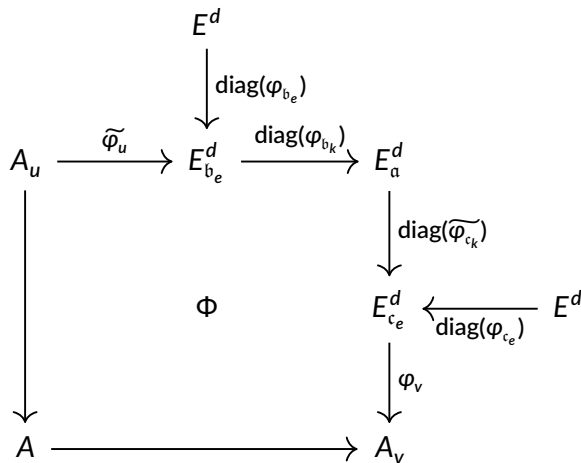


## Solvability of the norm equation: The diagram



Norm equation  $\deg_p(\Phi) = uN(b_k) + vN(c_k) \stackrel{!}{=} 2^f$

## Solvability of the norm equation: The diagram



Norm equation  $\deg_p(\Phi) = uN(b_k) + vN(c_k) \stackrel{!}{=} 2^f$

$$\ker(\Phi) = \left\{ (N(a)\varphi_u(y), \varphi_v \text{diag}(\widetilde{\varphi}_{c_k} \varphi_{b_k})(y) \mid y \in E_{b_e}^d[2^f] \right\} \quad \text{and} \quad \widetilde{\varphi}_{c_k} \varphi_{b_k} = \frac{1}{N(b_e)N(c_e)} \widetilde{\varphi}_{b_e} \varphi_{c_e}$$

# Constructing isogenies of prescribed degree

The isogenies  $\phi_u, \phi_v$

# Constructing isogenies of prescribed degree

The isogenies  $\phi_u, \phi_v$

Dimension 1  $\rightsquigarrow$  Dimension 2 Kani-isogeny  $\Phi$

Requires knowledge of the endomorphism ring (SQISign2D)

# Constructing isogenies of prescribed degree

The isogenies  $\phi_u, \phi_v$

Dimension 1  $\rightsquigarrow$  Dimension 2 Kani-isogeny  $\Phi$

Requires knowledge of the endomorphism ring (SQISign2D)

Dimension 2  $\rightsquigarrow$  Dimension 4 Kani-isogeny  $\Phi$

Sums of squares (or QFESTA-style splitting using 4-dimensional isogenies)

# Constructing isogenies of prescribed degree

The isogenies  $\phi_u, \phi_v$

Dimension 1  $\rightsquigarrow$  Dimension 2 Kani-isogeny  $\Phi$

Requires knowledge of the endomorphism ring (SQISign2D)

Dimension 2  $\rightsquigarrow$  Dimension 4 Kani-isogeny  $\Phi$

Sums of squares (or QFESTA-style splitting using 4-dimensional isogenies)

Dimension 4  $\rightsquigarrow$  Dimension 8 Kani-isogeny  $\Phi$

Zahrin's trick

# Constructing isogenies of prescribed degree

In dimension 2 with sum of two squares

# Constructing isogenies of prescribed degree

In dimension 2 with sum of two squares

$$\text{With } u = x_u^2 + y_u^2 \quad \varphi_u = \begin{pmatrix} x_u & y_u \\ -y_u & x_u \end{pmatrix} : E^2 \rightarrow E^2 \quad \text{has } \deg_p(\varphi_u) = u$$



# Constructing isogenies of prescribed degree

In dimension 2 with sum of two squares

$$\text{With } u = x_u^2 + y_u^2 \quad \varphi_u = \begin{pmatrix} x_u & y_u \\ -y_u & x_u \end{pmatrix} : E^2 \rightarrow E^2 \quad \text{has } \deg_p(\varphi_u) = u$$

**Theorem**  $u = p_1^{k_1} \cdots p_n^{k_n} = x_u^2 + y_u^2$  if and only if  $k_i$  even when  $p_i \equiv 3 \pmod{4}$

# Constructing isogenies of prescribed degree

In dimension 2 with sum of two squares

$$\text{With } u = x_u^2 + y_u^2 \quad \varphi_u = \begin{pmatrix} x_u & y_u \\ -y_u & x_u \end{pmatrix} : E^2 \rightarrow E^2 \quad \text{has } \deg_p(\varphi_u) = u$$

**Theorem**  $u = p_1^{k_1} \cdots p_n^{k_n} = x_u^2 + y_u^2$  if and only if  $k_i$  even when  $p_i \equiv 3 \pmod{4}$

**Idea**

Factor out (with multiplicity 1) small primes  $r_i \equiv 3 \pmod{4}$  that are split in  $\mathcal{O}$

# Constructing isogenies of prescribed degree

In dimension 2 with sum of two squares

$$\text{With } u = x_u^2 + y_u^2 \quad \varphi_u = \begin{pmatrix} x_u & y_u \\ -y_u & x_u \end{pmatrix} : E^2 \rightarrow E^2 \quad \text{has } \deg_p(\varphi_u) = u$$

**Theorem**  $u = p_1^{k_1} \cdots p_n^{k_n} = x_u^2 + y_u^2$  if and only if  $k_i$  even when  $p_i \equiv 3 \pmod{4}$

**Idea**

Factor out (with multiplicity 1) small primes  $r_i \equiv 3 \pmod{4}$  that are split in  $\mathcal{O}$

Perform this part as chain of Elkies  $r_i$ -isogenies  $\varphi_{u,r_i}$

# Constructing isogenies of prescribed degree

In dimension 2 with sum of two squares

$$\text{With } u = x_u^2 + y_u^2 \quad \varphi_u = \begin{pmatrix} x_u & y_u \\ -y_u & x_u \end{pmatrix} : E^2 \rightarrow E^2 \quad \text{has } \deg_p(\varphi_u) = u$$

**Theorem**  $u = p_1^{k_1} \cdots p_n^{k_n} = x_u^2 + y_u^2$  if and only if  $k_i$  even when  $p_i \equiv 3 \pmod{4}$

**Idea**

Factor out (with multiplicity 1) small primes  $r_i \equiv 3 \pmod{4}$  that are split in  $\mathcal{O}$

Perform this part as chain of Elkies  $r_i$ -isogenies  $\varphi_{u,r_i}$

If  $u = g_u(x_u^2 + y_u^2)$  with  $g_u$  product of “bad primes”  $r_i \equiv 3 \pmod{4}$  then

$$\varphi_u = \begin{pmatrix} \varphi_{u,r_1} \cdots \varphi_{u,r_l} & 0 \\ 0 & \varphi_{u,r_1} \cdots \varphi_{u,r_l} \end{pmatrix} \begin{pmatrix} x_u & y_u \\ -y_u & x_u \end{pmatrix} : E^2 \rightarrow E_u^2$$

has  $\deg_p(\Phi) = g_u(x_u^2 + y_u^2) = u$

## Rerandomisation

If we cannot solve the norm equation for  $[\alpha]$  we can rerandomise

## Rerandomisation

If we cannot solve the norm equation for  $[\alpha]$  we can rerandomise  
Pick small ideal  $[I]$  and compute  $[\alpha I] \cdot ([I]^{-1}E)$

## Rerandomisation

If we cannot solve the norm equation for  $[a]$  we can rerandomise

Pick small ideal  $[l]$  and compute  $[al] \cdot ([l]^{-1}E)$

Let's look at some data ...

# Our algorithm

## What we implemented



# Our algorithm

What we implemented

## Step 1: Finding UV

Do (easy) Lagrange lattice reduction on the input ideal  $\alpha$

# Our algorithm

## What we implemented

### Step 1: Finding UV

Do (easy) Lagrange lattice reduction on the input ideal  $\alpha$

Iterate small equivalent representatives

# Our algorithm

## What we implemented

### Step 1: Finding UV

Do (easy) Lagrange lattice reduction on the input ideal  $\mathfrak{a}$

Iterate small equivalent representatives

Factor out all small ideals up to a small bound  $\mathfrak{b} = \mathfrak{b}_e \mathfrak{b}_k$

# Our algorithm

## What we implemented

### Step 1: Finding UV

Do (easy) Lagrange lattice reduction on the input ideal  $\mathfrak{a}$

Iterate small equivalent representatives

Factor out all small ideals up to a small bound  $\mathfrak{b} = \mathfrak{b}_e \mathfrak{b}_k$

Sort by norm of the non-smooth part  $\mathfrak{b}_k$

# Our algorithm

## What we implemented

### Step 1: Finding UV

Do (easy) Lagrange lattice reduction on the input ideal  $\alpha$

Iterate small equivalent representatives

Factor out all small ideals up to a small bound  $\mathfrak{b} = \mathfrak{b}_e \mathfrak{b}_k$

Sort by norm of the non-smooth part  $\mathfrak{b}_k$

Try to solve the norm equation for the non-smooth part  $\mathfrak{b}_k, c_k$

# Our algorithm

## What we implemented

### Step 1: Finding UV

Do (easy) Lagrange lattice reduction on the input ideal  $\alpha$

Iterate small equivalent representatives

Factor out all small ideals up to a small bound  $\mathfrak{b} = \mathfrak{b}_e \mathfrak{b}_k$

Sort by norm of the non-smooth part  $\mathfrak{b}_k$

Try to solve the norm equation for the non-smooth part  $\mathfrak{b}_k, c_k$

### Step 2: Computing $\ker(\Phi)$

# Our algorithm

## What we implemented

### Step 1: Finding UV

Do (easy) Lagrange lattice reduction on the input ideal  $\mathfrak{a}$

Iterate small equivalent representatives

Factor out all small ideals up to a small bound  $\mathfrak{b} = \mathfrak{b}_e \mathfrak{b}_k$

Sort by norm of the non-smooth part  $\mathfrak{b}_k$

Try to solve the norm equation for the non-smooth part  $\mathfrak{b}_k, c_k$

### Step 2: Computing $\ker(\Phi)$

Evaluate the isogeny  $\varphi_{b_e}$

# Our algorithm

## What we implemented

### Step 1: Finding UV

Do (easy) Lagrange lattice reduction on the input ideal  $\mathfrak{a}$

Iterate small equivalent representatives

Factor out all small ideals up to a small bound  $\mathfrak{b} = \mathfrak{b}_e \mathfrak{b}_k$

Sort by norm of the non-smooth part  $\mathfrak{b}_k$

Try to solve the norm equation for the non-smooth part  $\mathfrak{b}_k, \mathfrak{c}_k$

### Step 2: Computing $\ker(\Phi)$

Evaluate the isogeny  $\varphi_{\mathfrak{b}_e}$

Evaluate the isogeny  $\widetilde{\varphi_{\mathfrak{c}_k}} \varphi_{\mathfrak{b}_k} = \widetilde{\varphi_{\mathfrak{b}_e}} \varphi_{\mathfrak{c}_e} / N(\mathfrak{b}_e)N(\mathfrak{c}_e)$



# Our algorithm

## What we implemented

### Step 1: Finding UV

Do (easy) Lagrange lattice reduction on the input ideal  $\mathfrak{a}$

Iterate small equivalent representatives

Factor out all small ideals up to a small bound  $\mathfrak{b} = \mathfrak{b}_e \mathfrak{b}_k$

Sort by norm of the non-smooth part  $\mathfrak{b}_k$

Try to solve the norm equation for the non-smooth part  $\mathfrak{b}_k, \mathfrak{c}_k$

### Step 2: Computing $\ker(\Phi)$

Evaluate the isogeny  $\varphi_{\mathfrak{b}_e}$

Evaluate the isogeny  $\widetilde{\varphi}_{\mathfrak{c}_k} \varphi_{\mathfrak{b}_k} = \widetilde{\varphi}_{\mathfrak{b}_e} \varphi_{\mathfrak{c}_e} / N(\mathfrak{b}_e) N(\mathfrak{c}_e)$

### Step 3: Compute the 4d-isogeny

# Our algorithm

## What we implemented

### Step 1: Finding UV

Do (easy) Lagrange lattice reduction on the input ideal  $\alpha$

Iterate small equivalent representatives

Factor out all small ideals up to a small bound  $\mathfrak{b} = \mathfrak{b}_e \mathfrak{b}_k$

Sort by norm of the non-smooth part  $\mathfrak{b}_k$

Try to solve the norm equation for the non-smooth part  $\mathfrak{b}_k, \mathfrak{c}_k$

### Step 2: Computing $\ker(\Phi)$

Evaluate the isogeny  $\varphi_{\mathfrak{b}_e}$

Evaluate the isogeny  $\widetilde{\varphi}_{\mathfrak{c}_k} \varphi_{\mathfrak{b}_k} = \widetilde{\varphi}_{\mathfrak{b}_e} \varphi_{\mathfrak{c}_e} / N(\mathfrak{b}_e)N(\mathfrak{c}_e)$

### Step 3: Compute the 4d-isogeny

Pass the kernel to 4d-library

# Our algorithm

## What we implemented

### Step 1: Finding UV

Do (easy) Lagrange lattice reduction on the input ideal  $\alpha$

Iterate small equivalent representatives

Factor out all small ideals up to a small bound  $\mathfrak{b} = \mathfrak{b}_e \mathfrak{b}_k$

Sort by norm of the non-smooth part  $\mathfrak{b}_k$

Try to solve the norm equation for the non-smooth part  $\mathfrak{b}_k, \mathfrak{c}_k$

### Step 2: Computing $\ker(\Phi)$

Evaluate the isogeny  $\varphi_{\mathfrak{b}_e}$

Evaluate the isogeny  $\widetilde{\varphi}_{\mathfrak{c}_k} \varphi_{\mathfrak{b}_k} = \widetilde{\varphi}_{\mathfrak{b}_e} \varphi_{\mathfrak{c}_e} / N(\mathfrak{b}_e)N(\mathfrak{c}_e)$

### Step 3: Compute the 4d-isogeny

Pass the kernel to 4d-library

Solve the twisting problem

## Timings of the steps

Parameter	Step 1	Step 2	Step 3	Tot. Time
500	0.097s	0.48s	0.96s	1.53s
1000	0.21s	1.16s	2.84s	4.21s
1500	1.19s	2.85s	6.49s	10.5s
2000	1.68s	8.34s	11.3s	21.3s
4000	15.6s	52.8s	53.5s	122s

**Table:** SageMath 10.5 timings on Intel Core i5-1235U at 4.0 GHz, in wall-clock time.

# Constructing isogenies of prescribed degree

In dimension 2 with QFESTA splitting via 4-dimensional isogeny

# Constructing isogenies of prescribed degree

In dimension 2 with QFESTA splitting via 4-dimensional isogeny

Consider  $\gamma_1 = x_1 + y_1\sqrt{\Delta}$  and  $\gamma_2 = x_2 + y_2\sqrt{\Delta}$  in  $\mathcal{O} = \mathbb{Z} + \sqrt{\Delta}\mathbb{Z}$

# Constructing isogenies of prescribed degree

In dimension 2 with QFESTA splitting via 4-dimensional isogeny

Consider  $\gamma_1 = x_1 + y_1\sqrt{\Delta}$  and  $\gamma_2 = x_2 + y_2\sqrt{\Delta}$  in  $\mathcal{O} = \mathbb{Z} + \sqrt{\Delta}\mathbb{Z}$

Then

$$\gamma = \begin{pmatrix} \gamma_1 & \overline{\gamma_1} \\ -\gamma_2 & \overline{\gamma_2} \end{pmatrix} : E^2 \rightarrow E^2 \quad \text{has} \quad \deg_p(\gamma) = (x_1^2 + x_2^2) + \Delta(y_1^2 + y_2^2)$$

# Constructing isogenies of prescribed degree

In dimension 2 with QFESTA splitting via 4-dimensional isogeny

Consider  $\gamma_1 = x_1 + y_1\sqrt{\Delta}$  and  $\gamma_2 = x_2 + y_2\sqrt{\Delta}$  in  $\mathcal{O} = \mathbb{Z} + \sqrt{\Delta}\mathbb{Z}$

Then

$$\gamma = \begin{pmatrix} \gamma_1 & \overline{\gamma_1} \\ -\gamma_2 & \overline{\gamma_2} \end{pmatrix} : E^2 \rightarrow E^2 \quad \text{has} \quad \deg_p(\gamma) = (x_1^2 + x_2^2) + \Delta(y_1^2 + y_2^2)$$

**Idea** If  $N \gg |\Delta|$  then  $m = N - |\Delta|(y_1^2 + y_2^2) \geq 0$  often enough that we find  $m = x_1^2 + x_2^2$  as sum of squares



# Constructing isogenies of prescribed degree

In dimension 2 with QFESTA splitting via 4-dimensional isogeny

Consider  $\gamma_1 = x_1 + y_1\sqrt{\Delta}$  and  $\gamma_2 = x_2 + y_2\sqrt{\Delta}$  in  $\mathcal{O} = \mathbb{Z} + \sqrt{\Delta}\mathbb{Z}$

Then

$$\gamma = \begin{pmatrix} \gamma_1 & \overline{\gamma_1} \\ -\gamma_2 & \overline{\gamma_2} \end{pmatrix} : E^2 \rightarrow E^2 \quad \text{has} \quad \deg_p(\gamma) = (x_1^2 + x_2^2) + \Delta(y_1^2 + y_2^2)$$

**Idea** If  $N \gg |\Delta|$  then  $m = N - |\Delta|(y_1^2 + y_2^2) \geq 0$  often enough that we find  $m = x_1^2 + x_2^2$  as sum of squares

**Heuristic** If  $N \gg |\Delta|$ , we can find endomorphism of  $E^2$  with polarised degree  $N$

# Constructing isogenies of prescribed degree

In dimension 2 with QFESTA splitting via 4-dimensional isogeny

# Constructing isogenies of prescribed degree

In dimension 2 with QFESTA splitting via 4-dimensional isogeny

Moreover

Let  $\deg_p(\gamma) = N_1 N_2$  with  $N_i$  coprime

# Constructing isogenies of prescribed degree

In dimension 2 with QFESTA splitting via 4-dimensional isogeny

Moreover

Let  $\deg_p(\gamma) = N_1 N_2$  with  $N_i$  coprime

Then  $\gamma = \mu_1 \mu_2 = \nu_2 \nu_1$  with  $\deg_p(\mu_1) = N_1$  and  $\deg_p(\nu_1) = N_2$

# Constructing isogenies of prescribed degree

In dimension 2 with QFESTA splitting via 4-dimensional isogeny

Moreover

Let  $\deg_p(\gamma) = N_1 N_2$  with  $N_i$  coprime

Then  $\gamma = \mu_1 \mu_2 = \nu_2 \nu_1$  with  $\deg_p(\mu_1) = N_1$  and  $\deg_p(\nu_1) = N_2$

Then the 4-dimensional isogeny

$$\Gamma = \begin{pmatrix} \mu_1 & \widetilde{\mu}_2 \\ -\nu_1 & \widetilde{\nu}_2 \end{pmatrix}$$

has polarised degree  $N = N_1 + N_2$  and kernel  $\{(\deg_p(\mu_1)x, \gamma(x)) \mid x \in E^2[N]\}$

# Constructing isogenies of prescribed degree

In dimension 2 with QFESTA splitting via 4-dimensional isogeny

Moreover

Let  $\deg_p(\gamma) = N_1 N_2$  with  $N_i$  coprime

Then  $\gamma = \mu_1 \mu_2 = \nu_2 \nu_1$  with  $\deg_p(\mu_1) = N_1$  and  $\deg_p(\nu_1) = N_2$

Then the 4-dimensional isogeny

$$\Gamma = \begin{pmatrix} \mu_1 & \widetilde{\mu}_2 \\ -\nu_1 & \widetilde{\nu}_2 \end{pmatrix}$$

has polarised degree  $N = N_1 + N_2$  and kernel  $\{(\deg_p(\mu_1)x, \gamma(x)) \mid x \in E^2[N]\}$

Idea (Specific to Frobenius orientation)

# Constructing isogenies of prescribed degree

In dimension 2 with QFESTA splitting via 4-dimensional isogeny

Moreover

Let  $\deg_p(\gamma) = N_1 N_2$  with  $N_i$  coprime

Then  $\gamma = \mu_1 \mu_2 = \nu_2 \nu_1$  with  $\deg_p(\mu_1) = N_1$  and  $\deg_p(\nu_1) = N_2$

Then the 4-dimensional isogeny

$$\Gamma = \begin{pmatrix} \mu_1 & \widetilde{\mu}_2 \\ -\nu_1 & \widetilde{\nu}_2 \end{pmatrix}$$

has polarised degree  $N = N_1 + N_2$  and kernel  $\{(\deg_p(\mu_1)x, \gamma(x)) \mid x \in E^2[N]\}$

Idea (Specific to Frobenius orientation)

Our  $u \approx \sqrt{\Delta} = \sqrt{p}$

Set  $N = u(2^e - u) \gg |\Delta| = p$  to get 4-dimensional isogeny  $\Gamma$  of degree  $2^e$

Obtain  $u$ -isogeny  $\mu_i : E^2 \rightarrow A_u$  as component of  $\Gamma$

## Improved timings

Parameter	Step 1	Step 2	Total time	N. Rerand.
2000	0.49 s	3.83 s	4.32 s	0.70
4000	3.25 s	22.8 s	26.0 s	1.25

**Table:** Step 1 and Step 2 when solving the norm equation with single sum of squares, in wall-clock seconds.



Thank you!

Paper <https://eprint.iacr.org/2025/401>

Implementation <https://github.com/pegasis4d>

Slides <https://rueg.re/pegasis-tum>

## Working over $F_p$ : Fast basis sampling

Let  $p \equiv 7 \pmod{8}$  and  $E/F_p$  oriented by  $\mathbb{Z}[(\sqrt{-p} + 1)/2]$

## Working over $F_p$ : Fast basis sampling

Let  $p \equiv 7 \pmod{8}$  and  $E/F_p$  oriented by  $\mathbb{Z}[(\sqrt{-p} + 1)/2]$

Then for  $2^e \parallel p + 1$  we have

$$E[2^e] \cong \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2^{e-1}\mathbb{Z}$$

Let  $T_{\text{desc}}, T_{\text{horiz},1}, T_{\text{horiz},2}$  points of 2-torsion

### Lemma

Let  $E : y^2 = g(x)$

An element  $x_p$  in  $F_p$  lifts to  $P = (x_p, y_p)$

- (i) on  $E$  with  $\text{ord}(P) = 2^{e-1}$  iff  $x_p - x(T_{\text{desc},1})$  a non-zero non-square  
(and  $g(x_p)$  non-zero square)
- (ii) on  $E^t$  with  $\text{ord}(P) = 2^{e-1}$  iff  $x_p - x(T_{\text{desc},2})$  non-zero square  
(and  $g(x_p)$  a non-zero non-square)