SIAM Conference on Algebraic Geometry, 8th of July 2025

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 Isogeny Class Group Action using 4-dimensional Supersingular Isogenies

Practically Efficient Isogeny Class Group Action
using 4-dimensional Supersingular Isogenies

Practically Efficient Isogeny Class Group Action using 4-dimensional Supersingular Isogenies

Practically Efficient Isogeny Class Group Action using 4-dimensional Supersingular Isogenies

Practically Efficient Isogeny Class Group Action using 4-dimensional Supersingular Isogenies

Cryptographic Group Actions

Easy to compute gx for all $g \in G$ and $x \in X$, but hard to recover g from (x, gx)

Cryptographic Group Actions

Easy to compute gx for all $g \in G$ and $x \in X$, but hard to recover g from (x, gx)

Example Commutative group gives Non-Interactive Key-Exchange

Cryptographic Group Actions

Easy to compute gx for all $g \in G$ and $x \in X$, but hard to recover g from (x, gx)

Example Commutative group gives Non-Interactive Key-Exchange

$$\begin{tikzcd} x \arrow[r, "g_A"] \arrow[d, "g_B"'] & x_A = g_A x \\ x_B = g_B x & \end{tikzcd}$$

Cryptographic Group Actions

Easy to compute gx for all $g \in G$ and $x \in X$, but hard to recover g from (x, gx)

Example Commutative group gives Non-Interactive Key-Exchange

$$\begin{tikzcd}
x \arrow[r, "g_A"] \arrow[d, "g_B"'] & x_A = g_A x \arrow[d, "g_B"] \\
x_B = g_B x \arrow[r, "g_A"'] & g_A g_B x = g_B g_A x
\end{tikzcd}$$

Cryptographic Group Actions

Easy to compute gx for all $g \in G$ and $x \in X$, but hard to recover g from (x, gx)

Example Commutative group gives Non-Interactive Key-Exchange

$$\begin{tikzcd}
x \arrow[r, "g_A"] \arrow[d, "g_B"'] & x_A = g_A x \arrow[d, "g_B"] \\
x_B = g_B x \arrow[r, "g_A"'] & g_A g_B x = g_B g_A x
\end{tikzcd}$$

Quantum resistance

Best known generic (quantum) algorithm to invert the action is subexponential

Cryptographic Group Actions

Easy to compute gx for all $g \in G$ and $x \in X$, but hard to recover g from (x, gx)

Example Commutative group gives Non-Interactive Key-Exchange

$$\begin{tikzcd} x \arrow[r, "g_A"] \arrow[d, "g_B"'] & x_A = g_A x \arrow[d, "g_B"] \\ x_B = g_B x \arrow[r, "g_A"'] & g_A g_B x = g_B g_A x \end{tikzcd}$$

Quantum resistance

Best known generic (quantum) algorithm to invert the action is subexponential

Isogeny class-group action only known commutative, quantum resistant cryptographic group action

Abelian Varieties & Isogenies

Abelian Varieties & Isogenies

Abelian Variety (Formal)

Abelian Varieties & Isogenies

Abelian Variety (Formal)

Group scheme over a field

Abelian Varieties & Isogenies

Abelian Variety (Formal)

Group scheme over a field with one property from each set

(i) projective, proper
(ii) geometrically irreducible, irreducible, geometrically connected, connected
(iii) smooth, geometrically reduced

Abelian Varieties & Isogenies

Abelian Variety (Formal)

Group scheme over a field with one property from each set

(i) projective, proper
(ii) geometrically irreducible, irreducible, geometrically connected, connected
(iii) smooth, geometrically reduced

Abelian Variety (Informal) Variety + Group Law

Abelian Varieties & Isogenies

Abelian Variety (Formal)

Group scheme over a field with one property from each set

(i) projective, proper

(ii) geometrically irreducible, irreducible, geometrically connected, connected

(iii) smooth, geometrically reduced

Abelian Variety (Informal) Variety + Group Law

Fact Elliptic curves are exactly 1-dim Abelian Varieties

Abelian Varieties & Isogenies

Abelian Variety (Formal)

Group scheme over a field with one property from each set

(i) projective, proper
(ii) geometrically irreducible, irreducible, geometrically connected, connected
(iii) smooth, geometrically reduced

Abelian Variety (Informal) Variety + Group Law

Fact Elliptic curves are exactly 1-dim Abelian Varieties

Isogeny Surjective morphism of Abelian Varieties

Abelian Varieties & Isogenies

Abelian Variety (Formal)

Group scheme over a field with one property from each set

(i) projective, proper
(ii) geometrically irreducible, irreducible, geometrically connected, connected
(iii) smooth, geometrically reduced

Abelian Variety (Informal) Variety + Group Law

Fact Elliptic curves are exactly 1-dim Abelian Varieties

Isogeny Surjective morphism of Abelian Varieties

First isomorphism theorem

$$\{G \subseteq A \text{ finite}\} \leftrightsquigarrow \{\text{separable isogenies } A \to *\} / \{\text{iso}\}$$

$$G \mapsto \varphi_G \text{ with } \ker(\varphi_G) = G \quad (\deg(\varphi_G) = \#G)$$

$$\ker(\varphi) \mapsfrom \varphi$$

The isogeny class-group action

Let $\mathcal{O}$ be an order inside an imaginary quadratic number field

The isogeny class-group action

Let $\mathcal{O}$ be an order inside an imaginary quadratic number field

An $\mathcal{O}$-*orientation* on a curve E is an injective ring morphism $\iota_E : \mathcal{O} \to \mathrm{End}(E)$

The isogeny class-group action

Let $\mathcal{O}$ be an order inside an imaginary quadratic number field

An $\mathcal{O}$-*orientation* on a curve E is an injective ring morphism $\iota_E : \mathcal{O} \to \mathrm{End}(E)$

Theorem $\mathrm{Cl}(\mathcal{O})$ acts on isomorphism classes of oriented elliptic curves E

The isogeny class-group action

Let $\mathcal{O}$ be an order inside an imaginary quadratic number field

An $\mathcal{O}$-*orientation* on a curve E is an injective ring morphism $\iota_E : \mathcal{O} \to \mathrm{End}(E)$

Theorem $\mathrm{Cl}(\mathcal{O})$ acts on isomorphism classes of oriented elliptic curves E

Construction Act by $[\mathcal{A}]$ in $\mathrm{Cl}(\mathcal{O})$. Let $[\mathfrak{a}] = [\mathcal{A}]$ with $\mathfrak{a} \subseteq \mathcal{O}$ integral

$$G_{\mathfrak{a}} = \bigcap_{\sigma \in \mathfrak{a}} \ker(\iota_E(\sigma)) \qquad \rightsquigarrow \qquad \varphi_{\mathfrak{a}} : E \to E_{\mathfrak{a}} \quad \text{with} \quad \ker(\varphi_{\mathfrak{a}}) = G_{\mathfrak{a}}$$

The isogeny class-group action

Let $\mathcal{O}$ be an order inside an imaginary quadratic number field

An $\mathcal{O}$-*orientation* on a curve E is an injective ring morphism $\iota_E : \mathcal{O} \to \mathrm{End}(E)$

Theorem $\mathrm{Cl}(\mathcal{O})$ acts on isomorphism classes of oriented elliptic curves E

Construction Act by $[\mathcal{A}]$ in $\mathrm{Cl}(\mathcal{O})$. Let $[\mathfrak{a}] = [\mathcal{A}]$ with $\mathfrak{a} \subseteq \mathcal{O}$ integral

$$G_{\mathfrak{a}} = \bigcap_{\sigma \in \mathfrak{a}} \ker(\iota_E(\sigma)) \qquad \rightsquigarrow \qquad \varphi_{\mathfrak{a}} : E \to E_{\mathfrak{a}} \quad \text{with} \quad \ker(\varphi_{\mathfrak{a}}) = G_{\mathfrak{a}}$$

Define $[\mathcal{A}] \cdot E = [\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

The isogeny class-group action

Let $\mathcal{O}$ be an order inside an imaginary quadratic number field

An $\mathcal{O}$-*orientation* on a curve E is an injective ring morphism $\iota_E : \mathcal{O} \to \mathrm{End}(E)$

Theorem $\mathrm{Cl}(\mathcal{O})$ acts on isomorphism classes of oriented elliptic curves E

Construction Act by $[\mathcal{A}]$ in $\mathrm{Cl}(\mathcal{O})$. Let $[\mathfrak{a}] = [\mathcal{A}]$ with $\mathfrak{a} \subseteq \mathcal{O}$ integral

$$G_{\mathfrak{a}} = \bigcap_{\sigma \in \mathfrak{a}} \ker(\iota_E(\sigma)) \qquad \rightsquigarrow \qquad \varphi_{\mathfrak{a}} : E \to E_{\mathfrak{a}} \quad \text{with} \quad \ker(\varphi_{\mathfrak{a}}) = G_{\mathfrak{a}}$$

Define $[\mathcal{A}] \cdot E = [\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Lemma $\deg(\varphi_{\mathfrak{a}}) = \mathrm{N}(\mathfrak{a})$

The isogeny class-group action

Let $\mathcal{O}$ be an order inside an imaginary quadratic number field

An $\mathcal{O}$-*orientation* on a curve E is an injective ring morphism $\iota_E : \mathcal{O} \to \mathrm{End}(E)$

Theorem $\mathrm{Cl}(\mathcal{O})$ acts on isomorphism classes of oriented elliptic curves E

Construction Act by $[\mathcal{A}]$ in $\mathrm{Cl}(\mathcal{O})$. Let $[\mathfrak{a}] = [\mathcal{A}]$ with $\mathfrak{a} \subseteq \mathcal{O}$ integral

$$G_{\mathfrak{a}} = \bigcap_{\sigma \in \mathfrak{a}} \ker(\iota_E(\sigma)) \qquad \rightsquigarrow \qquad \varphi_{\mathfrak{a}} : E \to E_{\mathfrak{a}} \quad \text{with} \quad \ker(\varphi_{\mathfrak{a}}) = G_{\mathfrak{a}}$$

Define $[\mathcal{A}] \cdot E = [\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Lemma $\deg(\varphi_{\mathfrak{a}}) = \mathrm{N}(\mathfrak{a})$

Example (CSIDH) $E/\mathbb{F}_p$ supersingular, $\iota_E : \mathbb{Z}[\sqrt{-p}] \to \mathrm{End}(E); \sqrt{-p} \mapsto \pi$

The isogeny class-group action

Let $\mathcal{O}$ be an order inside an imaginary quadratic number field

An $\mathcal{O}$-*orientation* on a curve E is an injective ring morphism $\iota_E : \mathcal{O} \to \mathrm{End}(E)$

Theorem $\mathrm{Cl}(\mathcal{O})$ acts on isomorphism classes of oriented elliptic curves E

Construction Act by $[\mathcal{A}]$ in $\mathrm{Cl}(\mathcal{O})$. Let $[\mathfrak{a}] = [\mathcal{A}]$ with $\mathfrak{a} \subseteq \mathcal{O}$ integral

$$G_{\mathfrak{a}} = \bigcap_{\sigma \in \mathfrak{a}} \ker(\iota_E(\sigma)) \quad \rightsquigarrow \quad \varphi_{\mathfrak{a}} : E \to E_{\mathfrak{a}} \quad \text{with} \quad \ker(\varphi_{\mathfrak{a}}) = G_{\mathfrak{a}}$$

Define $[\mathcal{A}] \cdot E = [\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Lemma $\deg(\varphi_{\mathfrak{a}}) = \mathrm{N}(\mathfrak{a})$

Example (CSIDH) $E/\mathbb{F}_p$ supersingular, $\iota_E : \mathbb{Z}[\sqrt{-p}] \to \mathrm{End}(E); \sqrt{-p} \mapsto \pi$

Theorem

The action on oriented supersingular elliptic curves is free and has at most 2 orbits

The Ideal2Isogeny Construction

The Ideal2Isogeny Construction

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

The Ideal2Isogeny Construction

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Let $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$

The Ideal2Isogeny Construction

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Let $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$

Assume $\mathrm{N}(\mathfrak{b}), \mathrm{N}(\mathfrak{c})$ coprime

The Ideal2Isogeny Construction

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Let $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$

Assume $\mathrm{N}(\mathfrak{b}), \mathrm{N}(\mathfrak{c})$ coprime

$$\begin{tikzcd} E \arrow[r, "\varphi_{\mathfrak{b}}"] & E_{\mathfrak{a}} \arrow[d, "\widetilde{\varphi_{\mathfrak{c}}}"] \\ & E \end{tikzcd}$$

The Ideal2Isogeny Construction

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Let $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$

Assume $\mathrm{N}(\mathfrak{b}), \mathrm{N}(\mathfrak{c})$ coprime

$$\begin{tikzcd}
E \arrow[r, "\varphi_{\mathfrak{b}}"] \arrow[d] & E_{\mathfrak{a}} \arrow[d, "\widetilde{\varphi_{\mathfrak{c}}}"] \\
E' \arrow[r] & E
\end{tikzcd}$$

The Ideal2Isogeny Construction

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Let $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$

Assume $\mathrm{N}(\mathfrak{b}), \mathrm{N}(\mathfrak{c})$ coprime

$$\begin{tikzcd}
E \arrow[r, "\varphi_{\mathfrak{b}}"] \arrow[d] \arrow[dr, phantom, "\Phi"] & E_{\mathfrak{a}} \arrow[d, "\widetilde{\varphi_{\mathfrak{c}}}"] \\
E' \arrow[r] & E
\end{tikzcd}$$

The Ideal2Isogeny Construction

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Let $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$

Assume $\mathrm{N}(\mathfrak{b}), \mathrm{N}(\mathfrak{c})$ coprime

$$\begin{tikzcd}
E \arrow[r, "\varphi_{\mathfrak{b}}"] \arrow[d] \arrow[dr, phantom, "\Phi"] & E_{\mathfrak{a}} \arrow[d, "\widetilde{\varphi_{\mathfrak{c}}}"] \\
E' \arrow[r] & E
\end{tikzcd}$$

$$\Phi : E \times E \to E_{\mathfrak{a}} \times E'$$

$$\begin{aligned}
\ker(\Phi) &= \left\{ \left(\mathrm{N}(\mathfrak{b})x, \widetilde{\varphi_{\mathfrak{c}}}\varphi_{\mathfrak{b}}(x) \right) \mid x \in E[\deg_p(\Phi)] \right\} \\
&= \left\{ \left(\mathrm{N}(\mathfrak{b})x, \varphi_{\bar{\mathfrak{c}}\mathfrak{b}}(x) \right) \mid x \in E[\deg_p(\Phi)] \right\}
\end{aligned}$$

The Ideal2Isogeny Construction

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Let $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$

Assume $\mathrm{N}(\mathfrak{b}), \mathrm{N}(\mathfrak{c})$ coprime

$$\begin{tikzcd}
E \arrow[r, "\varphi_{\mathfrak{b}}"] \arrow[d] \arrow[dr, phantom, "\Phi"] & E_{\mathfrak{a}} \arrow[d, "\widetilde{\varphi_{\mathfrak{c}}}"] \\
E' \arrow[r] & E
\end{tikzcd}$$

$$\Phi : E \times E \to E_{\mathfrak{a}} \times E'$$

$$\begin{aligned}
\ker(\Phi) &= \left\{ \left(\mathrm{N}(\mathfrak{b})x, \widetilde{\varphi_{\mathfrak{c}}}\varphi_{\mathfrak{b}}(x)\right) \mid x \in E[\deg_{\mathrm{p}}(\Phi)] \right\} \\
&= \left\{ \left(\mathrm{N}(\mathfrak{b})x, \varphi_{\bar{\mathfrak{c}}\mathfrak{b}}(x)\right) \mid x \in E[\deg_{\mathrm{p}}(\Phi)] \right\}
\end{aligned}$$

Norm equation $\deg_{\mathrm{p}}(\Phi) = \mathrm{N}(\mathfrak{b}) + \mathrm{N}(\mathfrak{c}) \stackrel{!}{=} 2^f$

The Ideal2Isogeny Construction

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Let $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$

Assume $\mathrm{N}(\mathfrak{b}), \mathrm{N}(\mathfrak{c})$ coprime

$$\begin{tikzcd}
E \arrow[r, "\varphi_{\mathfrak{b}}"] \arrow[d] \arrow[dr, phantom, "\Phi"] & E_{\mathfrak{a}} \arrow[d, "\widetilde{\varphi}_{\mathfrak{c}}"] \\
E' \arrow[r] & E
\end{tikzcd}$$

$$\Phi : E \times E \to E_{\mathfrak{a}} \times E'$$

$$\begin{aligned}
\ker(\Phi) &= \left\{ \left(\mathrm{N}(\mathfrak{b})x, \widetilde{\varphi}_{\mathfrak{c}} \varphi_{\mathfrak{b}}(x) \right) \mid x \in E[\deg_{\mathrm{p}}(\Phi)] \right\} \\
&= \left\{ \left(\mathrm{N}(\mathfrak{b})x, \varphi_{\bar{\mathfrak{c}}\mathfrak{b}}(x) \right) \mid x \in E[\deg_{\mathrm{p}}(\Phi)] \right\}
\end{aligned}$$

Norm equation $\deg_{\mathrm{p}}(\Phi) = \mathrm{N}(\mathfrak{b}) + \mathrm{N}(\mathfrak{c}) \overset{!}{=} 2^f$

Strategy Find $\mathfrak{a}, \mathfrak{b}$ equivalent ideals such that

1. $E[2^f]$ is $\mathbb{F}_{p^2}$-rational
2. $\mathrm{N}(\mathfrak{b}), \mathrm{N}(\mathfrak{c})$ coprime

The Ideal2Isogeny Construction: Iteration #2

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

The Ideal2Isogeny Construction: Iteration #2

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Let $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$

The Ideal2Isogeny Construction: Iteration #2

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Let $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$, $\varphi_u : E \to E_u$, $\varphi_v : E \to E_v$

The Ideal2Isogeny Construction: Iteration #2

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Let $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$, $\varphi_u : E \to E_u$, $\varphi_v : E \to E_v$

Assume $u\mathrm{N}(\mathfrak{b}), v\mathrm{N}(\mathfrak{c})$ coprime

The Ideal2Isogeny Construction: Iteration #2

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Let $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$, $\varphi_u : E \to E_u$, $\varphi_v : E \to E_v$

Assume $u\mathrm{N}(\mathfrak{b}), v\mathrm{N}(\mathfrak{c})$ coprime

$$\begin{tikzcd}
E_u \arrow[r, "\widetilde{\varphi_u}"] & E \arrow[r, "\varphi_{\mathfrak{b}}"] & E_{\mathfrak{a}} \arrow[d, "\widetilde{\varphi_{\mathfrak{c}}}"] \\
 & & E \arrow[d, "\varphi_v"] \\
 & & E_v
\end{tikzcd}$$

The Ideal2Isogeny Construction: Iteration #2

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Let $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$, $\varphi_u : E \to E_u$, $\varphi_v : E \to E_v$

Assume $u\mathrm{N}(\mathfrak{b}), v\mathrm{N}(\mathfrak{c})$ coprime

$$\begin{tikzcd}
E_u \arrow[r, "\widetilde{\varphi_u}"] \arrow[dd] & E \arrow[r, "\varphi_{\mathfrak{b}}"] & E_{\mathfrak{a}} \arrow[d, "\widetilde{\varphi_{\mathfrak{c}}}"] \\
 & & E \arrow[d, "\varphi_v"] \\
E' \arrow[rr] & & E_v
\end{tikzcd}$$

The Ideal2Isogeny Construction: Iteration #2

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Let $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$, $\varphi_u : E \to E_u$, $\varphi_v : E \to E_v$

Assume $u\mathrm{N}(\mathfrak{b}), v\mathrm{N}(\mathfrak{c})$ coprime

$$\begin{tikzcd}
E_u \arrow[r, "\widetilde{\varphi}_u"] \arrow[dd] & E \arrow[r, "\varphi_{\mathfrak{b}}"] & E_{\mathfrak{a}} \arrow[d, "\widetilde{\varphi}_{\mathfrak{c}}"] \\
 & \Phi & E \arrow[d, "\varphi_v"] \\
E' \arrow[rr] & & E_v
\end{tikzcd}$$

The Ideal2Isogeny Construction: Iteration #2

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Let $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$, $\varphi_u : E \to E_u$, $\varphi_v : E \to E_v$

Assume $u\mathrm{N}(\mathfrak{b}), v\mathrm{N}(\mathfrak{c})$ coprime

$$
\begin{tikzcd}
E_u \arrow[r, "\widetilde{\varphi_u}"] \arrow[dd] & E \arrow[r, "\varphi_{\mathfrak{b}}"] & E_{\mathfrak{a}} \arrow[d, "\widetilde{\varphi_{\mathfrak{c}}}"] \\
& \Phi & E \arrow[d, "\varphi_v"] \\
E' \arrow[rr] & & E_v
\end{tikzcd}
$$

$$\Phi : E_u \times E_v \to E_{\mathfrak{a}} \times E'$$

$$
\begin{aligned}
&\ker(\Phi) \\
&= \left\{ \left(u\mathrm{N}(\mathfrak{b})x, \varphi_v \widetilde{\varphi_{\mathfrak{c}}} \varphi_{\mathfrak{b}} \widetilde{\varphi_u}(x)\right) \mid x \in E_u[\deg_{\mathrm{p}}(\Phi)] \right\} \\
&= \left\{ \left(u\mathrm{N}(\mathfrak{b})x, \varphi_v \varphi_{\bar{\mathfrak{c}}\mathfrak{b}} \widetilde{\varphi_u}(x)\right) \mid x \in E_u[\deg_{\mathrm{p}}(\Phi)] \right\}
\end{aligned}
$$

The Ideal2Isogeny Construction: Iteration #2

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Let $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$, $\varphi_u : E \to E_u$, $\varphi_v : E \to E_v$

Assume $u\mathrm{N}(\mathfrak{b}), v\mathrm{N}(\mathfrak{c})$ coprime

$$\begin{tikzcd}
E_u \arrow[r, "\widetilde{\varphi}_u"] \arrow[dd] & E \arrow[r, "\varphi_{\mathfrak{b}}"] & E_{\mathfrak{a}} \arrow[d, "\widetilde{\varphi}_{\mathfrak{c}}"] \\
 & \Phi & E \arrow[d, "\varphi_v"] \\
E' \arrow[rr] & & E_v
\end{tikzcd}$$

$$\Phi : E_u \times E_v \to E_{\mathfrak{a}} \times E'$$

$$\ker(\Phi)$$

$$= \left\{ \left(u\mathrm{N}(\mathfrak{b})x, \varphi_v \widetilde{\varphi}_{\mathfrak{c}} \varphi_{\mathfrak{b}} \widetilde{\varphi}_u(x) \right) \mid x \in E_u[\deg_{\mathrm{p}}(\Phi)] \right\}$$

$$= \left\{ \left(u\mathrm{N}(\mathfrak{b})x, \varphi_v \varphi_{\bar{\mathfrak{c}}\mathfrak{b}} \widetilde{\varphi}_u(x) \right) \mid x \in E_u[\deg_{\mathrm{p}}(\Phi)] \right\}$$

Norm equation $\deg_{\mathrm{p}}(\Phi) = u\mathrm{N}(\mathfrak{b}) + v\mathrm{N}(\mathfrak{c}) \overset{!}{=} 2^f$

The Ideal2Isogeny Construction: Iteration #2

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Let $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$, $\varphi_u : E \to E_u$, $\varphi_v : E \to E_v$

Assume $u\mathrm{N}(\mathfrak{b}), v\mathrm{N}(\mathfrak{c})$ coprime

$$
\begin{tikzcd}
E_u \arrow[r, "\widetilde{\varphi_u}"] \arrow[dd] & E \arrow[r, "\varphi_{\mathfrak{b}}"] & E_{\mathfrak{a}} \arrow[d, "\widetilde{\varphi_{\mathfrak{c}}}"] \\
 & \Phi & E \arrow[d, "\varphi_v"] \\
E' \arrow[rr] & & E_v
\end{tikzcd}
$$

$$\Phi : E_u \times E_v \to E_{\mathfrak{a}} \times E'$$

$$
\begin{aligned}
&\ker(\Phi) \\
&= \left\{ \left(u\mathrm{N}(\mathfrak{b})x, \varphi_v \widetilde{\varphi_{\mathfrak{c}}} \varphi_{\mathfrak{b}} \widetilde{\varphi_u}(x) \right) \mid x \in E_u[\deg_{\mathrm{p}}(\Phi)] \right\} \\
&= \left\{ \left(u\mathrm{N}(\mathfrak{b})x, \varphi_v \varphi_{\bar{\mathfrak{c}}\mathfrak{b}} \widetilde{\varphi_u}(x) \right) \mid x \in E_u[\deg_{\mathrm{p}}(\Phi)] \right\}
\end{aligned}
$$

Norm equation $\deg_{\mathrm{p}}(\Phi) = u\mathrm{N}(\mathfrak{b}) + v\mathrm{N}(\mathfrak{c}) \stackrel{!}{=} 2^f$

Strategy Find $\mathfrak{a}, \mathfrak{b}$ equivalent ideals and φ_u, φ_v such that

1. $E[2^f]$ is $\mathbb{F}_{p^2}$-rational 2. $u\mathrm{N}(\mathfrak{b}), v\mathrm{N}(\mathfrak{c})$ coprime 3. Can compute φ_u, φ_v

The Ideal2Isogeny Construction: Iteration #3

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

The Ideal2Isogeny Construction: Iteration #3

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Let $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$

The Ideal2Isogeny Construction: Iteration #3

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Let $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$, $\varphi_u : E^d \to A_u$, $\varphi_v : E^d \to A_v$

The Ideal2Isogeny Construction: Iteration #3

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Let $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$, $\varphi_u : E^d \to A_u$, $\varphi_v : E^d \to A_v$

Assume $u\mathrm{N}(\mathfrak{b}), v\mathrm{N}(\mathfrak{c})$ coprime

The Ideal2Isogeny Construction: Iteration #3

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Let $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$, $\varphi_u : E^d \to A_u$, $\varphi_v : E^d \to A_v$

Assume $u\mathrm{N}(\mathfrak{b}), v\mathrm{N}(\mathfrak{c})$ coprime

$$\begin{tikzcd}
A_u \arrow[r, "\widetilde{\varphi_u}"] & E^d \arrow[r, "\mathrm{diag}(\varphi_{\mathfrak{b}})"] & E_{\mathfrak{a}}^d \arrow[d, "\mathrm{diag}(\widetilde{\varphi_{\mathfrak{c}}})"] \\
 & & E^d \arrow[d, "\varphi_v"] \\
 & & A_v
\end{tikzcd}$$

The Ideal2Isogeny Construction: Iteration #3

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Let $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$, $\varphi_u : E^d \to A_u$, $\varphi_v : E^d \to A_v$

Assume $u\mathrm{N}(\mathfrak{b}), v\mathrm{N}(\mathfrak{c})$ coprime

$$\begin{tikzcd}
A_u \arrow[r, "\widetilde{\varphi_u}"] \arrow[ddd] & E^d \arrow[r, "\mathrm{diag}(\varphi_{\mathfrak{b}})"] & E_{\mathfrak{a}}^d \arrow[d, "\mathrm{diag}(\widetilde{\varphi_{\mathfrak{c}}})"] \\
 & & E^d \arrow[dd, "\varphi_v"] \\
 & & \\
A \arrow[rr] & & A_v
\end{tikzcd}$$

The Ideal2Isogeny Construction: Iteration #3

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Let $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$, $\varphi_u : E^d \to A_u$, $\varphi_v : E^d \to A_v$

Assume $u\mathrm{N}(\mathfrak{b}), v\mathrm{N}(\mathfrak{c})$ coprime

$$\begin{tikzcd}
A_u \arrow[r, "\widetilde{\varphi_u}"] \arrow[dd] & E^d \arrow[r, "\mathrm{diag}(\varphi_{\mathfrak{b}})"] & E^d_{\mathfrak{a}} \arrow[d, "\mathrm{diag}(\widetilde{\varphi_{\mathfrak{c}}})"] \\
 & \Phi & E^d \arrow[d, "\varphi_v"] \\
A \arrow[rr] & & A_v
\end{tikzcd}$$

$$\Phi : A_u \times A_v \to E^d_{\mathfrak{a}} \times A$$

$$\begin{aligned}
&\ker(\Phi) \\
&= \left\{ \left(u\mathrm{N}(\mathfrak{b})x, \varphi_v \mathrm{diag}(\widetilde{\varphi_{\mathfrak{c}}}\varphi_{\mathfrak{b}})\widetilde{\varphi_u}(x) \right) \mid x \in A_u[\deg_{\mathrm{p}}(\Phi)] \right\} \\
&= \left\{ \left(u\mathrm{N}(\mathfrak{b})x, \varphi_v \mathrm{diag}(\varphi_{\bar{\mathfrak{c}}\mathfrak{b}})\widetilde{\varphi_u}(x) \right) \mid x \in A_u[\deg_{\mathrm{p}}(\Phi)] \right\}
\end{aligned}$$

The Ideal2Isogeny Construction: Iteration #3

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Let $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$, $\varphi_u : E^d \to A_u$, $\varphi_v : E^d \to A_v$

Assume $u\mathrm{N}(\mathfrak{b}), v\mathrm{N}(\mathfrak{c})$ coprime

$$\begin{tikzcd}
A_u \arrow[r, "\widetilde{\varphi_u}"] \arrow[dd] & E^d \arrow[r, "\mathrm{diag}(\varphi_{\mathfrak{b}})"] & E^d_{\mathfrak{a}} \arrow[d, "\mathrm{diag}(\widetilde{\varphi_{\mathfrak{c}}})"] \\
 & \Phi & E^d \arrow[d, "\varphi_v"] \\
A \arrow[rr] & & A_v
\end{tikzcd}$$

$$\Phi : A_u \times A_v \to E^d_{\mathfrak{a}} \times A$$

$$\begin{aligned}
&\ker(\Phi) \\
&= \left\{ \left(u\mathrm{N}(\mathfrak{b})x, \varphi_v \mathrm{diag}(\widetilde{\varphi_{\mathfrak{c}}}\varphi_{\mathfrak{b}})\widetilde{\varphi_u}(x) \right) \mid x \in A_u[\deg_{\mathrm{p}}(\Phi)] \right\} \\
&= \left\{ \left(u\mathrm{N}(\mathfrak{b})x, \varphi_v \mathrm{diag}(\varphi_{\bar{\mathfrak{c}}\mathfrak{b}})\widetilde{\varphi_u}(x) \right) \mid x \in A_u[\deg_{\mathrm{p}}(\Phi)] \right\}
\end{aligned}$$

Norm equation $\deg_{\mathrm{p}}(\Phi) = u\mathrm{N}(\mathfrak{b}) + v\mathrm{N}(\mathfrak{c}) \stackrel{!}{=} 2^f$

The Ideal2Isogeny Construction: Iteration #3

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Let $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$, $\varphi_u : E^d \to A_u$, $\varphi_v : E^d \to A_v$

Assume $u\mathrm{N}(\mathfrak{b}), v\mathrm{N}(\mathfrak{c})$ coprime

$$\begin{tikzcd}
A_u \arrow[r, "\widetilde{\varphi_u}"] \arrow[dd] & E^d \arrow[r, "\mathrm{diag}(\varphi_{\mathfrak{b}})"] & E^d_{\mathfrak{a}} \arrow[d, "\mathrm{diag}(\widetilde{\varphi_{\mathfrak{c}}})"] \\
 & \Phi & E^d \arrow[d, "\varphi_v"] \\
A \arrow[rr] & & A_v
\end{tikzcd}$$

$$\Phi : A_u \times A_v \to E^d_{\mathfrak{a}} \times A$$

$$\begin{aligned}
&\ker(\Phi) \\
&= \left\{ \left(u\mathrm{N}(\mathfrak{b})x, \varphi_v \mathrm{diag}(\widetilde{\varphi_{\mathfrak{c}}}\varphi_{\mathfrak{b}})\widetilde{\varphi_u}(x) \right) \mid x \in A_u[\deg_{\mathrm{p}}(\Phi)] \right\} \\
&= \left\{ \left(u\mathrm{N}(\mathfrak{b})x, \varphi_v \mathrm{diag}(\varphi_{\bar{\mathfrak{c}}\mathfrak{b}})\widetilde{\varphi_u}(x) \right) \mid x \in A_u[\deg_{\mathrm{p}}(\Phi)] \right\}
\end{aligned}$$

Norm equation $\deg_{\mathrm{p}}(\Phi) = u\mathrm{N}(\mathfrak{b}) + v\mathrm{N}(\mathfrak{c}) \stackrel{!}{=} 2^f$

Strategy Find $\mathfrak{a}, \mathfrak{b}$ equivalent ideals and φ_u, φ_v such that

1. $E[2^f]$ is $\mathbb{F}_{p^2}$-rational 2. $u\mathrm{N}(\mathfrak{b}), v\mathrm{N}(\mathfrak{c})$ coprime 3. Can compute φ_u, φ_v

Solvability of the norm equation: Conflict

$\deg_p(\Phi) = 2^f$ (Target solution of $u\mathrm{N}(I) + v\mathrm{N}(J) = 2^f$)

Solvability of the norm equation: Conflict

$\deg_p(\Phi) = 2^f$ (Target solution of $u\mathrm{N}(I) + v\mathrm{N}(J) = 2^f$)

Guaranteed solutions for $u\mathrm{N}(\mathfrak{b}) + v\mathrm{N}(\mathfrak{c}) = 2^n$ when $2^n \geq \mathrm{N}(\mathfrak{b})\mathrm{N}(\mathfrak{c})$ (Coin Problem)

Solvability of the norm equation: Conflict

$\deg_{\mathrm{p}}(\Phi) = 2^f$ (Target solution of $u\mathrm{N}(I) + v\mathrm{N}(J) = 2^f$)

Guaranteed solutions for $u\mathrm{N}(\mathfrak{b}) + v\mathrm{N}(\mathfrak{c}) = 2^n$ when $2^n \geq \mathrm{N}(\mathfrak{b})\mathrm{N}(\mathfrak{c})$ (Coin Problem)

...but Minkowski's bound only gives us $\mathfrak{b}, \mathfrak{c}$ with $\mathrm{N}(\mathfrak{b}), \mathrm{N}(\mathfrak{c}) \approx \sqrt{\mathrm{Disc}(\mathcal{O})} = \sqrt{p}$

Solvability of the norm equation: Conflict

$\deg_p(\Phi) = 2^f$ (Target solution of $u\mathrm{N}(I) + v\mathrm{N}(J) = 2^f$)

Guaranteed solutions for $u\mathrm{N}(\mathfrak{b}) + v\mathrm{N}(\mathfrak{c}) = 2^n$ when $2^n \geq \mathrm{N}(\mathfrak{b})\mathrm{N}(\mathfrak{c})$ (Coin Problem)

...but Minkowski's bound only gives us $\mathfrak{b}, \mathfrak{c}$ with $\mathrm{N}(\mathfrak{b}), \mathrm{N}(\mathfrak{c}) \approx \sqrt{\mathrm{Disc}(\mathcal{O})} = \sqrt{p}$

...empirical example when $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$ we can only find $\mathfrak{b}, \mathfrak{c}$ with $p \leq \mathrm{N}(\mathfrak{b})\mathrm{N}(\mathfrak{c}) \leq 2p$

Solvability of the norm equation: Conflict

$\deg_p(\Phi) = 2^f$ (Target solution of $u\mathrm{N}(I) + v\mathrm{N}(J) = 2^f$)

Guaranteed solutions for $u\mathrm{N}(\mathfrak{b}) + v\mathrm{N}(\mathfrak{c}) = 2^n$ when $2^n \geq \mathrm{N}(\mathfrak{b})\mathrm{N}(\mathfrak{c})$ (Coin Problem)

...but Minkowski's bound only gives us $\mathfrak{b}, \mathfrak{c}$ with $\mathrm{N}(\mathfrak{b}), \mathrm{N}(\mathfrak{c}) \approx \sqrt{\mathrm{Disc}(\mathcal{O})} = \sqrt{p}$

...empirical example when $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$ we can only find $\mathfrak{b}, \mathfrak{c}$ with $p \leq \mathrm{N}(\mathfrak{b})\mathrm{N}(\mathfrak{c}) \leq 2p$

...so $p \leq 2^n$

Solvability of the norm equation: Conflict

$\deg_p(\Phi) = 2^f$ (Target solution of $u\mathrm{N}(I) + v\mathrm{N}(J) = 2^f$)

Guaranteed solutions for $u\mathrm{N}(\mathfrak{b}) + v\mathrm{N}(\mathfrak{c}) = 2^n$ when $2^n \geq \mathrm{N}(\mathfrak{b})\mathrm{N}(\mathfrak{c})$ (Coin Problem)

...but Minkowski's bound only gives us $\mathfrak{b}, \mathfrak{c}$ with $\mathrm{N}(\mathfrak{b}), \mathrm{N}(\mathfrak{c}) \approx \sqrt{\mathrm{Disc}(\mathcal{O})} = \sqrt{p}$

...empirical example when $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$ we can only find $\mathfrak{b}, \mathfrak{c}$ with $p \leq \mathrm{N}(\mathfrak{b})\mathrm{N}(\mathfrak{c}) \leq 2p$

...so $p \leq 2^n = 2^{\lceil \log_2(p) \rceil}$

Solvability of the norm equation: Conflict

$\deg_{\mathrm{p}}(\Phi) = 2^f$ (Target solution of $u\mathrm{N}(I) + v\mathrm{N}(J) = 2^f$)

Guaranteed solutions for $u\mathrm{N}(\mathfrak{b}) + v\mathrm{N}(\mathfrak{c}) = 2^n$ when $2^n \geq \mathrm{N}(\mathfrak{b})\mathrm{N}(\mathfrak{c})$ (Coin Problem)

...but Minkowski's bound only gives us $\mathfrak{b}, \mathfrak{c}$ with $\mathrm{N}(\mathfrak{b}), \mathrm{N}(\mathfrak{c}) \approx \sqrt{\mathrm{Disc}(\mathcal{O})} = \sqrt{p}$

...empirical example when $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$ we can only find $\mathfrak{b}, \mathfrak{c}$ with $p \leq \mathrm{N}(\mathfrak{b})\mathrm{N}(\mathfrak{c}) \leq 2p$

...so $p \leq 2^n = 2^{\lceil \log_2(p) \rceil}$

Rationality of kernel (Want $E[\deg_{\mathrm{p}}(\Phi)] \subseteq E(\mathbb{F}_{p^2})$)

Solvability of the norm equation: Conflict

$\deg_{\mathrm{p}}(\Phi) = 2^f$ (Target solution of $u\mathrm{N}(I) + v\mathrm{N}(J) = 2^f$)

Guaranteed solutions for $u\mathrm{N}(\mathfrak{b}) + v\mathrm{N}(\mathfrak{c}) = 2^n$ when $2^n \geq \mathrm{N}(\mathfrak{b})\mathrm{N}(\mathfrak{c})$ (Coin Problem)

...but Minkowski's bound only gives us $\mathfrak{b}, \mathfrak{c}$ with $\mathrm{N}(\mathfrak{b}), \mathrm{N}(\mathfrak{c}) \approx \sqrt{\mathrm{Disc}(\mathcal{O})} = \sqrt{p}$

...empirical example when $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$ we can only find $\mathfrak{b}, \mathfrak{c}$ with $p \leq \mathrm{N}(\mathfrak{b})\mathrm{N}(\mathfrak{c}) \leq 2p$

...so $p \leq 2^n = 2^{\lceil \log_2(p) \rceil}$

Rationality of kernel (Want $E[\deg_{\mathrm{p}}(\Phi)] \subseteq E(\mathbb{F}_{p^2})$)

E supersingular, so $\#E(\mathbb{F}_{p^2}) = (p+1)^2$ (Need supersingularity!)

Solvability of the norm equation: Conflict

$\deg_{\mathrm{p}}(\Phi) = 2^f$ (Target solution of $u\mathrm{N}(I) + v\mathrm{N}(J) = 2^f$)

Guaranteed solutions for $u\mathrm{N}(\mathfrak{b}) + v\mathrm{N}(\mathfrak{c}) = 2^n$ when $2^n \geq \mathrm{N}(\mathfrak{b})\mathrm{N}(\mathfrak{c})$ (Coin Problem)

...but Minkowski's bound only gives us $\mathfrak{b}, \mathfrak{c}$ with $\mathrm{N}(\mathfrak{b}), \mathrm{N}(\mathfrak{c}) \approx \sqrt{\mathrm{Disc}(\mathcal{O})} = \sqrt{p}$

...empirical example when $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$ we can only find $\mathfrak{b}, \mathfrak{c}$ with $p \leq \mathrm{N}(\mathfrak{b})\mathrm{N}(\mathfrak{c}) \leq 2p$

...so $p \leq 2^n = 2^{\lceil \log_2(p) \rceil}$

Rationality of kernel (Want $E[\deg_{\mathrm{p}}(\Phi)] \subseteq E(\mathbb{F}_{p^2})$)

E supersingular, so $\#E(\mathbb{F}_{p^2}) = (p+1)^2$ (Need supersingularity!)

...if $E[2^n] \subseteq E(\mathbb{F}_{p^2})$, then 2^n must divide $p+1$ (because $\#E[2^n] = 2^{2n}$)

Solvability of the norm equation: Conflict

$\deg_p(\Phi) = 2^f$ (Target solution of $u\mathrm{N}(I) + v\mathrm{N}(J) = 2^f$)

Guaranteed solutions for $u\mathrm{N}(\mathfrak{b}) + v\mathrm{N}(\mathfrak{c}) = 2^n$ when $2^n \geq \mathrm{N}(\mathfrak{b})\mathrm{N}(\mathfrak{c})$ (Coin Problem)

...but Minkowski's bound only gives us $\mathfrak{b}, \mathfrak{c}$ with $\mathrm{N}(\mathfrak{b}), \mathrm{N}(\mathfrak{c}) \approx \sqrt{\mathrm{Disc}(\mathcal{O})} = \sqrt{p}$

...empirical example when $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$ we can only find $\mathfrak{b}, \mathfrak{c}$ with $p \leq \mathrm{N}(\mathfrak{b})\mathrm{N}(\mathfrak{c}) \leq 2p$

...so $p \leq 2^n = 2^{\lceil \log_2(p) \rceil}$

Rationality of kernel (Want $E[\deg_p(\Phi)] \subseteq E(\mathbb{F}_{p^2})$)

E supersingular, so $\#E(\mathbb{F}_{p^2}) = (p+1)^2$ (Need supersingularity!)

...if $E[2^n] \subseteq E(\mathbb{F}_{p^2})$, then 2^n must divide $p+1$ (because $\#E[2^n] = 2^{2n}$)

...in particular $2^n = 2^{\lfloor \log_2(p) \rfloor - \varepsilon} < p$

Solvability of the norm equation: Conflict

$\deg_p(\Phi) = 2^f$ (Target solution of $u\mathrm{N}(I) + v\mathrm{N}(J) = 2^f$)

Guaranteed solutions for $u\mathrm{N}(\mathfrak{b}) + v\mathrm{N}(\mathfrak{c}) = 2^n$ when $2^n \geq \mathrm{N}(\mathfrak{b})\mathrm{N}(\mathfrak{c})$ (Coin Problem)

...but Minkowski's bound only gives us $\mathfrak{b}, \mathfrak{c}$ with $\mathrm{N}(\mathfrak{b}), \mathrm{N}(\mathfrak{c}) \approx \sqrt{\mathrm{Disc}(\mathcal{O})} = \sqrt{p}$

...empirical example when $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$ we can only find $\mathfrak{b}, \mathfrak{c}$ with $p \leq \mathrm{N}(\mathfrak{b})\mathrm{N}(\mathfrak{c}) \leq 2p$

...so $p \leq 2^n = 2^{\lceil \log_2(p) \rceil}$

Rationality of kernel (Want $E[\deg_p(\Phi)] \subseteq E(\mathbb{F}_{p^2})$)

E supersingular, so $\#E(\mathbb{F}_{p^2}) = (p+1)^2$ (Need supersingularity!)

...if $E[2^n] \subseteq E(\mathbb{F}_{p^2})$, then 2^n must divide $p+1$ (because $\#E[2^n] = 2^{2n}$)

...in particular $2^n = 2^{\lceil \log_2(p) \rceil - \varepsilon} < p$

Core Problem

Even the smallest equivalent ideals are too big...but not by much

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”

Compute easy part first

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"

Compute easy part first and hope we can find a diagram with norm-equation

$$u\mathrm{N}(\mathfrak{b}_k) + v\mathrm{N}(\mathfrak{c}_k) = 2^f$$

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”

Compute easy part first and hope we can find a diagram with norm-equation

$$u\mathrm{N}(\mathfrak{b}_k) + v\mathrm{N}(\mathfrak{c}_k) = 2^f$$

Maybe then $\mathrm{N}(\mathfrak{b}_k)\mathrm{N}(\mathfrak{c}_k) \leq 2^f$, guaranteeing $u, v \geq 0$ solution

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"

Compute easy part first and hope we can find a diagram with norm-equation

$$u\mathrm{N}(\mathfrak{b}_k) + v\mathrm{N}(\mathfrak{c}_k) = 2^f$$

Maybe then $\mathrm{N}(\mathfrak{b}_k)\mathrm{N}(\mathfrak{c}_k) \leq 2^f$, guaranteeing $u, v \geq 0$ solution

"Easy" In practice

Ensure $\mathrm{N}(\mathfrak{b}_e), \mathrm{N}(\mathfrak{c}_e)$ 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”

Compute easy part first and hope we can find a diagram with norm-equation

$$u\mathrm{N}(\mathfrak{b}_k) + v\mathrm{N}(\mathfrak{c}_k) = 2^f$$

Maybe then $\mathrm{N}(\mathfrak{b}_k)\mathrm{N}(\mathfrak{c}_k) \leq 2^f$, guaranteeing $u, v \geq 0$ solution

“Easy” In practice

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

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

Compute $[\mathfrak{b}_e] \cdot E$ with successive Elkies isogenies

Solvability of the norm equation: The diagram

$$
\begin{tikzcd}
 & E^d \arrow[d, "\operatorname{diag}(\varphi_{\mathfrak{b}_e})"] & & \\
A_u \arrow[r, "\widetilde{\varphi_u}"] \arrow[dd] & E^d_{\mathfrak{b}_e} \arrow[r, "\operatorname{diag}(\varphi_{\mathfrak{b}_k})"] & E^d_{\mathfrak{a}} \arrow[d, "\operatorname{diag}(\widetilde{\varphi_{\mathfrak{c}_k}})"] & \\
 & & E^d_{\mathfrak{c}_e} \arrow[d, "\varphi_v"] & E^d \arrow[l, "\operatorname{diag}(\varphi_{\mathfrak{c}_e})"'] \\
A \arrow[rr] & & A_v &
\end{tikzcd}
$$

Solvability of the norm equation: The diagram

$$
\begin{tikzcd}
 & E^d \arrow[d, "\mathrm{diag}(\varphi_{\mathfrak{b}_e})"] & & \\
A_u \arrow[r, "\widetilde{\varphi}_u"] \arrow[dd] \arrow[ddrr, phantom, "\Phi"] & E^d_{\mathfrak{b}_e} \arrow[r, "\mathrm{diag}(\varphi_{\mathfrak{b}_k})"] & E^d_{\mathfrak{a}} \arrow[d, "\mathrm{diag}(\widetilde{\varphi_{\mathfrak{c}_k}})"] & \\
 & & E^d_{\mathfrak{c}_e} \arrow[d, "\varphi_v"] & E^d \arrow[l, "\mathrm{diag}(\varphi_{\mathfrak{c}_e})"'] \\
A \arrow[rr] & & A_v &
\end{tikzcd}
$$

Solvability of the norm equation: The diagram

$$\begin{tikzcd}
 & E^d \arrow[d, "\operatorname{diag}(\varphi_{\mathfrak{b}_e})"] & & \\
A_u \arrow[r, "\widetilde{\varphi_u}"] \arrow[dd] & E^d_{\mathfrak{b}_e} \arrow[r, "\operatorname{diag}(\varphi_{\mathfrak{b}_k})"] & E^d_{\mathfrak{a}} \arrow[d, "\operatorname{diag}(\widetilde{\varphi_{\mathfrak{c}_k}})"] & \\
 & \Phi & E^d_{\mathfrak{c}_e} \arrow[d, "\varphi_v"] & E^d \arrow[l, "\operatorname{diag}(\varphi_{\mathfrak{c}_e})"'] \\
A \arrow[rr] & & A_v &
\end{tikzcd}$$

Norm equation $\deg_{\mathrm{p}}(\Phi) = u\mathrm{N}(\mathfrak{b}_k) + v\mathrm{N}(\mathfrak{c}_k) \overset{!}{=} 2^f$

Solvability of the norm equation: The diagram

$$\begin{tikzcd}
 & E^d \arrow[d, "\mathrm{diag}(\varphi_{\mathfrak{b}_e})"] & & \\
A_u \arrow[r, "\widetilde{\varphi_u}"] \arrow[dd] \arrow[ddrr, phantom, "\Phi"] & E^d_{\mathfrak{b}_e} \arrow[r, "\mathrm{diag}(\varphi_{\mathfrak{b}_k})"] & E^d_{\mathfrak{a}} \arrow[d, "\mathrm{diag}(\widetilde{\varphi_{\mathfrak{c}_k}})"] & \\
 & & E^d_{\mathfrak{c}_e} \arrow[d, "\varphi_v"] & E^d \arrow[l, "\mathrm{diag}(\varphi_{\mathfrak{c}_e})"'] \\
A \arrow[rr] & & A_v &
\end{tikzcd}$$

Norm equation $\deg_{\mathrm{p}}(\Phi) = u\mathrm{N}(\mathfrak{b}_k) + v\mathrm{N}(\mathfrak{c}_k) \overset{!}{=} 2^f$

$$\ker(\Phi) = \left\{(u\mathrm{N}(\mathfrak{b}_e)x, \varphi_v \mathrm{diag}(\widetilde{\varphi_{\mathfrak{c}_k}}\varphi_{\mathfrak{b}_k})\widetilde{\varphi_u}(x)) \mid x \in A_u[2^f]\right\} \quad \text{and} \quad \widetilde{\varphi_{\mathfrak{c}_k}}\varphi_{\mathfrak{b}_k} = \frac{1}{\mathrm{N}(\mathfrak{b}_e)\mathrm{N}(\mathfrak{c}_e)}\varphi_{\mathfrak{c}_e}\varphi_{\bar{\mathfrak{c}}\mathfrak{b}}\widetilde{\varphi_{\mathfrak{b}_e}}$$

Solvability of the norm equation: The diagram

$$
\begin{tikzcd}
 & E^d \arrow[d, "\operatorname{diag}(\varphi_{\mathfrak{b}_e})"] & & \\
A_u \arrow[r, "\widetilde{\varphi}_u"] \arrow[dd] \arrow[ddrr, phantom, "\Phi"] & E^d_{\mathfrak{b}_e} \arrow[r, "\operatorname{diag}(\varphi_{\mathfrak{b}_k})"] & E^d_{\mathfrak{a}} \arrow[d, "\operatorname{diag}(\widetilde{\varphi_{\mathfrak{c}_k}})"] & \\
 & & E^d_{\mathfrak{c}_e} \arrow[d, "\varphi_v"] & E^d \arrow[l, "\operatorname{diag}(\varphi_{\mathfrak{c}_e})"'] \\
A \arrow[rr] & & A_v &
\end{tikzcd}
$$

$$\varphi_{\bar{\mathfrak{c}}\mathfrak{b}} = \widetilde{\varphi}_{\mathfrak{c}}\varphi_{\mathfrak{b}} = \widetilde{\varphi_{\mathfrak{c}_e}}\,\widetilde{\varphi_{\mathfrak{c}_k}}\,\varphi_{\mathfrak{b}_k}\varphi_{\mathfrak{b}_e}$$

Norm equation $\deg_{\mathrm{p}}(\Phi) = u\mathrm{N}(\mathfrak{b}_k) + v\mathrm{N}(\mathfrak{c}_k) \overset{!}{=} 2^f$

$$\ker(\Phi) = \left\{(u\mathrm{N}(\mathfrak{b}_e)x, \varphi_v \operatorname{diag}(\widetilde{\varphi_{\mathfrak{c}_k}}\varphi_{\mathfrak{b}_k})\widetilde{\varphi}_u(x)) \mid x \in A_u[2^f]\right\} \quad \text{and} \quad \widetilde{\varphi_{\mathfrak{c}_k}}\varphi_{\mathfrak{b}_k} \overset{(*)}{=} \frac{1}{\mathrm{N}(\mathfrak{b}_e)\mathrm{N}(\mathfrak{c}_e)}\varphi_{\mathfrak{c}_e}\varphi_{\bar{\mathfrak{c}}\mathfrak{b}}\widetilde{\varphi_{\mathfrak{b}_e}}$$

Constructing isogenies of prescribed degree

The isogenies φ_u, φ_v

Constructing isogenies of prescribed degree

The isogenies φ_u, φ_v

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

Requires knowledge of the endomorphism ring (SQISign2D)

Constructing isogenies of prescribed degree

The isogenies φ_u, φ_v

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

Requires knowledge of the endomorphism ring (SQISign2D)

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

Sums of squares

Constructing isogenies of prescribed degree

The isogenies φ_u, φ_v

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

Requires knowledge of the endomorphism ring (SQISign2D)

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

Sums of squares

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

Zahrin's trick

An algorithm for solving the norm equation

Input: $\mathfrak{a} \subset \mathcal{O}$, $p = c2^e - 1$, Set of small split primes $\mathfrak{B}$

Output: Return $\mathfrak{b}_e, \mathfrak{b}_k, \mathfrak{c}_e, \mathfrak{c}_k, \varphi_u, \varphi_v$ such that $u\mathrm{N}(\mathfrak{b}_k) + v\mathrm{N}(\mathfrak{c}_k) = 2^f \leq 2^{e-3}$

An algorithm for solving the norm equation

Input: $\mathfrak{a} \subset \mathcal{O}$, $p = c2^e - 1$, Set of small split primes $\mathfrak{B}$

Output: Return $\mathfrak{b}_e, \mathfrak{b}_k, \mathfrak{c}_e, \mathfrak{c}_k, \varphi_u, \varphi_v$ such that $u\mathrm{N}(\mathfrak{b}_k) + v\mathrm{N}(\mathfrak{c}_k) = 2^f \leq 2^{e-3}$

1. Perform lattice reduction on $\mathfrak{a}$ to obtain small basis b_1, b_2

An algorithm for solving the norm equation

Input: $\mathfrak{a} \subset \mathcal{O}$, $p = c2^e - 1$, Set of small split primes $\mathfrak{B}$

Output: Return $\mathfrak{b}_e, \mathfrak{b}_k, \mathfrak{c}_e, \mathfrak{c}_k, \varphi_u, \varphi_v$ such that $u\mathrm{N}(\mathfrak{b}_k) + v\mathrm{N}(\mathfrak{c}_k) = 2^f \leq 2^{e-3}$

1. Perform lattice reduction on $\mathfrak{a}$ to obtain small basis b_1, b_2
2. Use b_1, b_2 to iterate over small ideals $\mathrm{N}(\mathfrak{b})$ equivalent to $\mathfrak{a}$

An algorithm for solving the norm equation

Input: $\mathfrak{a} \subset \mathcal{O}$, $p = c2^e - 1$, Set of small split primes $\mathfrak{B}$

Output: Return $\mathfrak{b}_e, \mathfrak{b}_k, \mathfrak{c}_e, \mathfrak{c}_k, \varphi_u, \varphi_v$ such that $u\mathrm{N}(\mathfrak{b}_k) + v\mathrm{N}(\mathfrak{c}_k) = 2^f \leq 2^{e-3}$

1. Perform lattice reduction on $\mathfrak{a}$ to obtain small basis b_1, b_2
2. Use b_1, b_2 to iterate over small ideals $\mathrm{N}(\mathfrak{b})$ equivalent to $\mathfrak{a}$
3. Factor the ideals $\mathfrak{b} = \mathfrak{b}_e\mathfrak{b}_k$ so that $\mathrm{N}(\mathfrak{b}_e)$ is a product of primes in $\mathfrak{B}$

An algorithm for solving the norm equation

Input: $\mathfrak{a} \subset \mathcal{O}$, $p = c2^e - 1$, Set of small split primes $\mathfrak{B}$

Output: Return $\mathfrak{b}_e, \mathfrak{b}_k, \mathfrak{c}_e, \mathfrak{c}_k, \varphi_u, \varphi_v$ such that $u\mathrm{N}(\mathfrak{b}_k) + v\mathrm{N}(\mathfrak{c}_k) = 2^f \leq 2^{e-3}$

1. Perform lattice reduction on $\mathfrak{a}$ to obtain small basis b_1, b_2
2. Use b_1, b_2 to iterate over small ideals $\mathrm{N}(\mathfrak{b})$ equivalent to $\mathfrak{a}$
3. Factor the ideals $\mathfrak{b} = \mathfrak{b}_e\mathfrak{b}_k$ so that $\mathrm{N}(\mathfrak{b}_e)$ is a product of primes in $\mathfrak{B}$
4. Choosing pairs $\mathfrak{b} = \mathfrak{b}_e\mathfrak{b}_k, \mathfrak{c} = \mathfrak{c}_e\mathfrak{c}_k$, try to solve $u\mathrm{N}(\mathfrak{b}_k) + v\mathrm{N}(\mathfrak{c}_k) = 2^f < 2^{e-3}$

An algorithm for solving the norm equation

Input: $\mathfrak{a} \subset \mathcal{O}$, $p = c2^e - 1$, Set of small split primes $\mathfrak{B}$

Output: Return $\mathfrak{b}_e, \mathfrak{b}_k, \mathfrak{c}_e, \mathfrak{c}_k, \varphi_u, \varphi_v$ such that $u\mathrm{N}(\mathfrak{b}_k) + v\mathrm{N}(\mathfrak{c}_k) = 2^f \leq 2^{e-3}$

1. Perform lattice reduction on $\mathfrak{a}$ to obtain small basis b_1, b_2
2. Use b_1, b_2 to iterate over small ideals $\mathrm{N}(\mathfrak{b})$ equivalent to $\mathfrak{a}$
3. Factor the ideals $\mathfrak{b} = \mathfrak{b}_e \mathfrak{b}_k$ so that $\mathrm{N}(\mathfrak{b}_e)$ is a product of primes in $\mathfrak{B}$
4. Choosing pairs $\mathfrak{b} = \mathfrak{b}_e \mathfrak{b}_k, \mathfrak{c} = \mathfrak{c}_e \mathfrak{c}_k$, try to solve $u\mathrm{N}(\mathfrak{b}_k) + v\mathrm{N}(\mathfrak{c}_k) = 2^f < 2^{e-3}$
5. Construct φ_u, φ_v as sums-of-squares $(x, y; -y, x)$ matrices (plus some Elkies isogenies)

An algorithm for solving the norm equation

Input: $\mathfrak{a} \subset \mathcal{O}$, $p = c2^e - 1$, Set of small split primes $\mathfrak{B}$

Output: Return $\mathfrak{b}_e, \mathfrak{b}_k, \mathfrak{c}_e, \mathfrak{c}_k, \varphi_u, \varphi_v$ such that $u\mathrm{N}(\mathfrak{b}_k) + v\mathrm{N}(\mathfrak{c}_k) = 2^f \leq 2^{e-3}$

1. Perform lattice reduction on $\mathfrak{a}$ to obtain small basis b_1, b_2
2. Use b_1, b_2 to iterate over small ideals $\mathrm{N}(\mathfrak{b})$ equivalent to $\mathfrak{a}$
3. Factor the ideals $\mathfrak{b} = \mathfrak{b}_e \mathfrak{b}_k$ so that $\mathrm{N}(\mathfrak{b}_e)$ is a product of primes in $\mathfrak{B}$
4. Choosing pairs $\mathfrak{b} = \mathfrak{b}_e \mathfrak{b}_k, \mathfrak{c} = \mathfrak{c}_e \mathfrak{c}_k$, try to solve $u\mathrm{N}(\mathfrak{b}_k) + v\mathrm{N}(\mathfrak{c}_k) = 2^f < 2^{e-3}$
5. Construct φ_u, φ_v as sums-of-squares $(x, y; -y, x)$ matrices (plus some Elkies isogenies)
6. Return $\mathfrak{b}_e, \mathfrak{b}_k, \varphi_u, \varphi_v$

Some data for the solvability of the norm equation

	Avg	Med	Min	Max
Time:	37.137	24.506	0.968	542.416
Rerandomisations:	0.499	0	0	11
$\log(2^f = u\mathrm{N}(\mathfrak{b}_k) + v\mathrm{N}(\mathfrak{c}_k))$	4076.080	4077	4058	4081
UV solutions tried:	38952.563	19701	10	548118
3-Elkies steps for $\varphi_{\mathfrak{b}_e}, \varphi_{\mathfrak{c}_e}$:	4.950	4	0	17
7-Elkies steps for $\varphi_{\mathfrak{b}_e}, \varphi_{\mathfrak{c}_e}$:	2.658	2	0	9
11-Elkies steps for $\varphi_{\mathfrak{b}_e}, \varphi_{\mathfrak{c}_e}$:	2.010	2	0	9
17-Elkies steps for $\varphi_{\mathfrak{b}_e}, \varphi_{\mathfrak{c}_e}$:	1.691	1	0	7
19-Elkies steps for $\varphi_{\mathfrak{b}_e}, \varphi_{\mathfrak{c}_e}$:	1.567	1	0	6
3-Elkies steps for φ_u, φ_v:	0.496	0	0	1
7-Elkies steps for φ_u, φ_v:	0.259	0	0	1
11-Elkies steps for φ_u, φ_v:	0.160	0	0	1
17-Elkies steps for φ_u, φ_v:	0.000	0	0	0
19-Elkies steps for φ_u, φ_v:	0.106	0	0	1

Table: Times, rerandomisations and elkies steps required for $p = 63 \cdot 2^{4084} - 1$.

Implementation Results

This all works!

		Lang.	500	1000	1500	2000	4000
Restricted	CSIDH*	C	40ms				
	SQALE*	C					5.75s**
	dCTIDH*	C				350ms**	
Unrestricted	SCALLOP*	C++	35s	750s			
	SCALLOP-HD*	Sage	88s	1140s			
	PEARL-SCALLOP*	C++	30s	58s	710s		
	KLaPoTi	Sage	207s				
		Rust	1.95s				
	PEGASIS	Sage	1.53s	4.21s	10.5s	21.3s	121s

Table: *Measured on different hardware, **Converted from cycles to time @4GHz.

Thank you for your attention

PEGASIS Paper https://eprint.iacr.org/2025/401 (To appear at Crypto'25)

PEGASIS Implementation https://github.com/pegasis4d

Slides https://rueg.re/siam25

Ask me anything (I have bonus slides!)

Higher dimensional isogenies

A *Principally Polarised Abelian Variety* is an Abelian variety A together with an isomorphism $\lambda_A : A \xrightarrow{\sim} A^\vee$

Higher dimensional isogenies

A *Principally Polarised Abelian Variety* is an Abelian variety A together with an isomorphism $\lambda_A : A \xrightarrow{\sim} A^\vee$ (which is induced by an ample divisor)

PPAVs vs Elliptic Curves

A, B *Principally Polarised Abelian Varieties*	E, E' Elliptic curves
	$\varphi : E \to E'$ isogeny

Higher dimensional isogenies

A *Principally Polarised Abelian Variety* is an Abelian variety A together with an isomorphism $\lambda_A : A \xrightarrow{\sim} A^\vee$ (which is induced by an ample divisor)

PPAVs vs Elliptic Curves

A, B *Principally Polarised Abelian Varieties*	E, E' Elliptic curves
$f : A \to B$ *isogeny*	$\varphi : E \to E'$ isogeny
	$\hat{\varphi} = \tilde{\varphi} : E' \to E$ dual

Higher dimensional isogenies

A *Principally Polarised Abelian Variety* is an Abelian variety A together with an isomorphism $\lambda_A : A \xrightarrow{\sim} A^\vee$ (which is induced by an ample divisor)

PPAVs vs Elliptic Curves

A, B *Principally Polarised Abelian Varieties*

$f : A \to B$ *isogeny*

$\tilde{f} = \lambda_B^{-1} f^\vee \lambda_A : B \to A$ *polarised dual*

E, E' Elliptic curves

$\varphi : E \to E'$ isogeny

$\hat{\varphi} = \tilde{\varphi} : E' \to E$ dual

(They all are)

Higher dimensional isogenies

A *Principally Polarised Abelian Variety* is an Abelian variety A together with an isomorphism $\lambda_A : A \xrightarrow{\sim} A^\vee$ (which is induced by an ample divisor)

PPAVs vs Elliptic Curves

A, B *Principally Polarised Abelian Varieties*

$f : A \to B$ *isogeny*

$\tilde{f} = \lambda_B^{-1} f^\vee \lambda_A : B \to A$ *polarised dual*

f is *polarised isogeny* if $\tilde{f} f = [d]_A$

E, E' Elliptic curves

$\varphi : E \to E'$ isogeny

$\hat{\varphi} = \tilde{\varphi} : E' \to E$ dual

(They all are)

$\deg_p(\varphi) = \deg(\varphi)$

Higher dimensional isogenies

A *Principally Polarised Abelian Variety* is an Abelian variety A together with an isomorphism $\lambda_A : A \xrightarrow{\sim} A^\vee$ (which is induced by an ample divisor)

PPAVs vs Elliptic Curves

A, B *Principally Polarised Abelian Varieties*	E, E' Elliptic curves
$f : A \to B$ *isogeny*	$\varphi : E \to E'$ isogeny
$\tilde{f} = \lambda_B^{-1} f^\vee \lambda_A : B \to A$ *polarised dual*	$\hat{\varphi} = \tilde{\varphi} : E' \to E$ dual
f is *polarised isogeny* if $\tilde{f} f = [d]_A$	(They all are)
...it has *polarised degree* $\deg_{\mathrm{p}}(f) = d$	$\deg_{\mathrm{p}}(\varphi) = \deg(\varphi)$

Higher dimensional isogenies

A *Principally Polarised Abelian Variety* is an Abelian variety A together with an isomorphism $\lambda_A : A \xrightarrow{\sim} A^\vee$ (which is induced by an ample divisor)

PPAVs vs Elliptic Curves

A, B *Principally Polarised Abelian Varieties*	E, E' Elliptic curves
$f : A \to B$ *isogeny*	$\varphi : E \to E'$ isogeny
$\tilde{f} = \lambda_B^{-1} f^\vee \lambda_A : B \to A$ *polarised dual*	$\hat{\varphi} = \tilde{\varphi} : E' \to E$ dual
f is *polarised isogeny* if $\tilde{f} f = [d]_A$	(They all are)
...it has *polarised degree* $\deg_{\mathrm{p}}(f) = d$	$\deg_{\mathrm{p}}(\varphi) = \deg(\varphi)$

Example

$\mathrm{diag}_d(f) : A^d \to B^d$ is polarised (if f is) and $\deg_{\mathrm{p}}(\mathrm{diag}_d(f)) = \deg_{\mathrm{p}}(f)$

Example

$\Phi = (x, y; -y, x)$ in $\mathrm{Mat}_{2\times 2}(\mathbb{Z})$ is polarised on A^2 with $\deg_{\mathrm{p}}(\Phi) = x^2 + y^2$

Kani's Lemma

A_i, B_j PPAVs over k, $\varphi_{ij} : A_i \to B_j$ polarised isogenies, $\mathrm{char}(k) \nmid \deg_{\mathrm{p}}(\varphi_{ij})$

Kani's Lemma

A_i, B_j PPAVs over k, $\varphi_{ij} : A_i \to B_j$ polarised isogenies, $\mathrm{char}(k) \nmid \deg_p(\varphi_{ij})$

$$\Phi = \begin{pmatrix} \varphi_{11} & \varphi_{21} \\ \varphi_{12} & \varphi_{22} \end{pmatrix} : A_1 \times A_2 \to B_1 \times B_2$$

is a polarised isogeny

$\iff$

$$\begin{tikzcd} A_1 \arrow[r, "\varphi_{11}"] \arrow[d, "-\varphi_{12}"'] & B_1 \arrow[d, "\widetilde{\varphi_{21}}"] \\ B_2 \arrow[r, "\widetilde{\varphi_{22}}"'] & A_2 \end{tikzcd}$$

$\deg_p(\varphi_{11}) = \deg_p(\varphi_{22})$

$\deg_p(\varphi_{12}) = \deg_p(\varphi_{21})$

Kani's Lemma

A_i, B_j PPAVs over k, $\varphi_{ij} : A_i \to B_j$ polarised isogenies, $\mathrm{char}(k) \nmid \deg_p(\varphi_{ij})$

$$\Phi = \begin{pmatrix} \varphi_{11} & \varphi_{21} \\ \varphi_{12} & \varphi_{22} \end{pmatrix} : A_1 \times A_2 \to B_1 \times B_2$$

is a polarised isogeny

$\Longleftrightarrow$

$$\begin{tikzcd} A_1 \arrow[r, "\varphi_{11}"] \arrow[d, "-\varphi_{12}"'] & B_1 \arrow[d, "\widetilde{\varphi_{21}}"] \\ B_2 \arrow[r, "\widetilde{\varphi_{22}}"'] & A_2 \end{tikzcd}$$

$$\deg_p(\varphi_{11}) = \deg_p(\varphi_{22})$$
$$\deg_p(\varphi_{12}) = \deg_p(\varphi_{21})$$

Then $\deg_p(\Phi) = \deg_p(\varphi_{11}) + \deg_p(\varphi_{21})$

Kani's Lemma

A_i, B_j PPAVs over k, $\varphi_{ij} : A_i \to B_j$ polarised isogenies, $\mathrm{char}(k) \nmid \deg_p(\varphi_{ij})$

$$\Phi = \begin{pmatrix} \varphi_{11} & \varphi_{21} \\ \varphi_{12} & \varphi_{22} \end{pmatrix} : A_1 \times A_2 \to B_1 \times B_2$$

is a polarised isogeny

$\iff$

$$\begin{tikzcd} A_1 \arrow[r, "\varphi_{11}"] \arrow[d, "-\varphi_{12}"'] & B_1 \arrow[d, "\widetilde{\varphi_{21}}"] \\ B_2 \arrow[r, "\widetilde{\varphi_{22}}"'] & A_2 \end{tikzcd}$$

$\deg_p(\varphi_{11}) = \deg_p(\varphi_{22})$

$\deg_p(\varphi_{12}) = \deg_p(\varphi_{21})$

Then $\deg_p(\Phi) = \deg_p(\varphi_{11}) + \deg_p(\varphi_{21})$

If additionally $\deg_p(\varphi_{11}), \deg_p(\varphi_{21})$ coprime and $\mathrm{char}(k) \nmid \deg_p(\Phi)$ then

$$\ker(\Phi) = \left\{ \left(\deg_p(\varphi_{11}) x, \widetilde{\varphi_{21}} \varphi_{11}(x) \right) \mid x \in A_1[\deg_p(\Phi)] \right\} \subseteq A_1 \times A_2$$

An Algorithm for constructing isogenies

of prescribed degree in dimension 2

Input: Integer u, Bound B, Set of small split primes $\mathcal{S}$

Output: Isogeny φ_u with degree u

An Algorithm for constructing isogenies

of prescribed degree in dimension 2

Input: Integer u, Bound B, Set of small split primes $\mathcal{S}$

Output: Isogeny φ_u with degree u

1. Attempt factorisation of u with trial divisions up to B

An Algorithm for constructing isogenies

of prescribed degree in dimension 2

Input: Integer u, Bound B, Set of small split primes $\mathcal{S}$

Output: Isogeny φ_u with degree u

1. Attempt factorisation of u with trial divisions up to B
2. Reject if prime $p_i \equiv 3 \pmod 4$, $p_i \notin \mathcal{S}$ divides u with odd multiplicity

An Algorithm for constructing isogenies

of prescribed degree in dimension 2

Input: Integer u, Bound B, Set of small split primes $\mathcal{S}$

Output: Isogeny φ_u with degree u

1. Attempt factorisation of u with trial divisions up to B
2. Reject if prime $p_i \equiv 3 \pmod 4$, $p_i \notin \mathcal{S}$ divides u with odd multiplicity
3. Let g_u product of primes $p_i \equiv 3 \pmod 4$ and $p_i \in \mathcal{S}$ that divide u with odd multiplicity

An Algorithm for constructing isogenies

of prescribed degree in dimension 2

Input: Integer u, Bound B, Set of small split primes $\mathcal{S}$

Output: Isogeny φ_u with degree u

1. Attempt factorisation of u with trial divisions up to B
2. Reject if prime $p_i \equiv 3 \pmod 4$, $p_i \notin \mathcal{S}$ divides u with odd multiplicity
3. Let g_u product of primes $p_i \equiv 3 \pmod 4$ and $p_i \in \mathcal{S}$ that divide u with odd multiplicity
4. Then $u/g_u = x_u^2 + y_u^2$.

An Algorithm for constructing isogenies

of prescribed degree in dimension 2

Input: Integer u, Bound B, Set of small split primes $\mathcal{S}$

Output: Isogeny φ_u with degree u

1. Attempt factorisation of u with trial divisions up to B
2. Reject if prime $p_i \equiv 3 \pmod 4$, $p_i \notin \mathcal{S}$ divides u with odd multiplicity
3. Let g_u product of primes $p_i \equiv 3 \pmod 4$ and $p_i \in \mathcal{S}$ that divide u with odd multiplicity
4. Then $u/g_u = x_u^2 + y_u^2$.
5. Let ψ_u be isogeny of degree g_u, computed by sequence of p_i-isogenies using Elkies' algorithm

An Algorithm for constructing isogenies

of prescribed degree in dimension 2

Input: Integer u, Bound B, Set of small split primes $\mathcal{S}$

Output: Isogeny φ_u with degree u

1. Attempt factorisation of u with trial divisions up to B
2. Reject if prime $p_i \equiv 3 \pmod 4$, $p_i \notin \mathcal{S}$ divides u with odd multiplicity
3. Let g_u product of primes $p_i \equiv 3 \pmod 4$ and $p_i \in \mathcal{S}$ that divide u with odd multiplicity
4. Then $u/g_u = x_u^2 + y_u^2$.
5. Let ψ_u be isogeny of degree g_u, computed by sequence of p_i-isogenies using Elkies' algorithm
6. Return

$$\varphi_u = \begin{pmatrix} \psi_u & 0 \\ 0 & \psi_u \end{pmatrix} \begin{pmatrix} x_u & y_u \\ -y_u & x_u \end{pmatrix}$$

Working over F_p: Fast basis sampling

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

Working over F_p: Fast basis sampling

Let $p \equiv 7 \pmod 8$ and E/F_p oriented by $\mathbb{Z}\left[\left(\sqrt{-p}+1\right)/2\right]$
Then for $2^e \,||\, p+1$ we have

$$E[2^e](F_p) \cong {}^{\mathbb{Z}}\!/_{2\mathbb{Z}} + {}^{\mathbb{Z}}\!/_{2^{e-1}\mathbb{Z}}$$

Working over F_p: Fast basis sampling

Let $p \equiv 7 \pmod 8$ and E/F_p oriented by $\mathbb{Z}\left[\left(\sqrt{-p}+1\right)/2\right]$
Then for $2^e \mid\mid p+1$ we have

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

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

Working over F_p: Fast basis sampling

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

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

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

Let $T_{\mathrm{desc}}, T_{\mathrm{horiz},1}, T_{\mathrm{horiz},2}$ 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 $\mathrm{ord}(P) = 2^{e-1}$ iff $x(p) - x(T_{\mathrm{desc},1})$ a non-zero non-square (and $g(x_p)$ non-zero square)

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

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

$$\gamma = \begin{pmatrix} \gamma_1 & \overline{\gamma_1} \\ -\gamma_2 & \overline{\gamma_2} \end{pmatrix} : E^2 \to E^2 \qquad \text{has} \qquad \deg_{\mathrm{p}}(\gamma) = (x_1^2 + x_2^2) + \Delta(y_1^2 + y_2^2)$$

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

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

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

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

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 $\deg_{\mathrm{p}}(\gamma) = N_1 N_2$ with N_i coprime

Constructing isogenies of prescribed degree

In dimension 2 with QFESTA splitting via 4-dimensional isogeny

Moreover

Let $\deg_{\mathrm{p}}(\gamma) = N_1 N_2$ with N_i coprime

Then $\gamma = \mu_1\mu_2 = \nu_2\nu_1$ with $\deg_{\mathrm{p}}(\mu_1) = N_1$ and $\deg_{\mathrm{p}}(\nu_1) = N_2$

Constructing isogenies of prescribed degree

In dimension 2 with QFESTA splitting via 4-dimensional isogeny

Moreover

Let $\deg_{\mathrm{p}}(\gamma) = N_1 N_2$ with N_i coprime

Then $\gamma = \mu_1 \mu_2 = \nu_2 \nu_1$ with $\deg_{\mathrm{p}}(\mu_1) = N_1$ and $\deg_{\mathrm{p}}(\nu_1) = N_2$

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 $\left\{ (\deg_{\mathrm{p}}(\mu_1) x, \gamma(x)) \mid x \in E^2[N] \right\}$

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 $\left\{(\deg_p(\mu_1)x, \gamma(x)) \mid x \in E^2[N]\right\}$

Idea (Specific to Frobenius orientation)

Constructing isogenies of prescribed degree

In dimension 2 with QFESTA splitting via 4-dimensional isogeny

Moreover

Let $\deg_{\mathrm{p}}(\gamma) = N_1 N_2$ with N_i coprime

Then $\gamma = \mu_1\mu_2 = \nu_2\nu_1$ with $\deg_{\mathrm{p}}(\mu_1) = N_1$ and $\deg_{\mathrm{p}}(\nu_1) = N_2$

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 $\left\{(\deg_{\mathrm{p}}(\mu_1)x, \gamma(x)) \mid x \in E^2[N]\right\}$

Idea (Specific to Frobenius orientation)

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

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

Obtain u-isogeny $\mu_i : E^2 \to A_u$ as component of Γ