Computing the Isogeny Class-Group Action on Ordinary Elliptic Curves by going into higher dimensions

Ryan Rueger

rueg.re/icga

July 2024

Outline

Cryptographic Group Actions

Motivation Diffie-Hellman key exchange is not post-quantum

Cryptographic Group Actions

Motivation Diffie-Hellman key exchange is not post-quantum

Closer Look

Cryptographic Group Actions

Motivation Diffie-Hellman key exchange is not post-quantum

Closer Look $G = \langle g_0 \rangle$ order p

Cryptographic Group Actions

Motivation Diffie-Hellman key exchange is not post-quantum

Closer Look $G = \langle g_0 \rangle$ order p

(i) Sample $a, b \xleftarrow{\$} \mathbb{Z}/p\mathbb{Z} - \{0\} \cong (\mathbb{Z}/p\mathbb{Z})^\times$

Cryptographic Group Actions

Motivation Diffie-Hellman key exchange is not post-quantum

Closer Look $G = \langle g_0 \rangle$ order p

(i) Sample $a, b \xleftarrow{\$} \mathbb{Z}/p\mathbb{Z} - \{0\} \cong (\mathbb{Z}/p\mathbb{Z})^{\times}$

(ii) Publish g_0^a, g_0^b

Cryptographic Group Actions

Motivation Diffie-Hellman key exchange is not post-quantum

Closer Look $G = \langle g_0 \rangle$ order p

(i) Sample $a, b \xleftarrow{\$} \mathbb{Z}/p\mathbb{Z} - \{0\} \cong (\mathbb{Z}/p\mathbb{Z})^\times$

(ii) Publish g_0^a, g_0^b

(iii) Recover $k = g_0^{ab} = (g_0^a)^b = (g_0^b)^a$

Cryptographic Group Actions

Motivation Diffie-Hellman key exchange is not post-quantum

Closer Look $G = \langle g_0 \rangle$ order p

(i) Sample $a, b \xleftarrow{\$} \mathbb{Z}/p\mathbb{Z} - \{0\} \cong (\mathbb{Z}/p\mathbb{Z})^\times$

(ii) Publish g_0^a, g_0^b

(iii) Recover $k = g_0^{ab} = (g_0^a)^b = (g_0^b)^a$

Insight This exponentiation is a group action! $\left(\mathbb{Z}/p\mathbb{Z}\right)^\times \times G \to G; (e, g) \mapsto g^e$

Cryptographic Group Actions

Motivation Diffie-Hellman key exchange is not post-quantum

Closer Look $G = \langle g_0 \rangle$ order p

(i) Sample $a, b \xleftarrow{\$} \mathbb{Z}/p\mathbb{Z} - \{0\} \cong (\mathbb{Z}/p\mathbb{Z})^{\times}$

(ii) Publish g_0^a, g_0^b

(iii) Recover $k = g_0^{ab} = (g_0^a)^b = (g_0^b)^a$

Insight This exponentiation is a group action! $\left(\mathbb{Z}/p\mathbb{Z}\right)^{\times} \times G \to G; (e, g) \mapsto g^e$

Recall (Group action) H a group, X a set

$$H \times X \to X \qquad (h, x) \mapsto h \cdot x$$

Cryptographic Group Actions

Motivation Diffie-Hellman key exchange is not post-quantum

Closer Look $G = \langle g_0 \rangle$ order p

(i) Sample $a, b \overset{\$}{\leftarrow} \mathbb{Z}/p\mathbb{Z} - \{0\} \cong (\mathbb{Z}/p\mathbb{Z})^{\times}$

(ii) Publish g_0^a, g_0^b

(iii) Recover $k = g_0^{ab} = (g_0^a)^b = (g_0^b)^a$

Insight This exponentiation is a group action! $\left(\mathbb{Z}/p\mathbb{Z}\right)^{\times} \times G \to G; (e, g) \mapsto g^e$

Recall (Group action) H a group, X a set

$$H \times X \to X \qquad (h, x) \mapsto h \cdot x$$

(i) $1_H \cdot x = x$

Cryptographic Group Actions

Motivation Diffie-Hellman key exchange is not post-quantum

Closer Look $G = \langle g_0 \rangle$ order p

(i) Sample $a, b \xleftarrow{\$} \mathbb{Z}/p\mathbb{Z} - \{0\} \cong (\mathbb{Z}/p\mathbb{Z})^\times$

(ii) Publish g_0^a, g_0^b

(iii) Recover $k = g_0^{ab} = (g_0^a)^b = (g_0^b)^a$

Insight This exponentiation is a group action! $(\mathbb{Z}/p\mathbb{Z})^\times \times G \to G; (e, g) \mapsto g^e$

Recall (Group action) H a group, X a set

$$H \times X \to X \qquad (h, x) \mapsto h \cdot x$$

(i) $1_H \cdot x = x$ (Exponentiation: $g^1 = g$)

Cryptographic Group Actions

Motivation Diffie-Hellman key exchange is not post-quantum

Closer Look $G = \langle g_0 \rangle$ order p

(i) Sample $a, b \overset{\$}{\leftarrow} \mathbb{Z}/p\mathbb{Z} - \{0\} \cong (\mathbb{Z}/p\mathbb{Z})^\times$

(ii) Publish g_0^a, g_0^b

(iii) Recover $k = g_0^{ab} = (g_0^a)^b = (g_0^b)^a$

Insight This exponentiation is a group action! $(\mathbb{Z}/p\mathbb{Z})^\times \times G \to G; (e, g) \mapsto g^e$

Recall (Group action) H a group, X a set

$$H \times X \to X \qquad (h, x) \mapsto h \cdot x$$

(i) $1_H \cdot x = x$ (Exponentiation: $g^1 = g$)

(ii) $h_2 \cdot (h_1 \cdot x) = (h_2 h_1) \cdot x$

Cryptographic Group Actions

Motivation Diffie-Hellman key exchange is not post-quantum

Closer Look $G = \langle g_0 \rangle$ order p

(i) Sample $a, b \xleftarrow{\$} \mathbb{Z}/p\mathbb{Z} - \{0\} \cong (\mathbb{Z}/p\mathbb{Z})^{\times}$

(ii) Publish g_0^a, g_0^b

(iii) Recover $k = g_0^{ab} = (g_0^a)^b = (g_0^b)^a$

Insight This exponentiation is a group action! $(\mathbb{Z}/p\mathbb{Z})^{\times} \times G \to G; (e, g) \mapsto g^e$

Recall (Group action) H a group, X a set

$$H \times X \to X \qquad (h, x) \mapsto h \cdot x$$

(i) $1_H \cdot x = x$ (Exponentiation: $g^1 = g$)

(ii) $h_2 \cdot (h_1 \cdot x) = (h_2 h_1) \cdot x$ (Exponentiation: $(g^a)^b = g^{ab}$)

Cryptography from group actions

Rephrase NIKE from group action

Setup: $H \times X \longrightarrow X$ group action, H commutative, $x_0 \in X$

Cryptography from group actions

Rephrase NIKE from group action

Setup: $H \times X \to X$ group action, H commutative, $x_0 \in X$

(i) Sample $a, b \overset{\$}{\leftarrow} H$

Cryptography from group actions

Rephrase NIKE from group action

Setup: $H \times X \longrightarrow X$ group action, H commutative, $x_0 \in X$

(i) Sample $a, b \xleftarrow{\$} H$

(ii) Publish $a \cdot x_0, b \cdot x_0$

Cryptography from group actions

Rephrase NIKE from group action

Setup: $H \times X \longrightarrow X$ group action, H commutative, $x_0 \in X$

(i) Sample $a, b \overset{\$}{\leftarrow} H$

(ii) Publish $a \cdot x_0, b \cdot x_0$

(iii) Recover $k = (ab) \cdot x_0 = b \cdot (a \cdot x_0) = a \cdot (b \cdot x_0)$

Cryptography from group actions

Rephrase NIKE from group action

Setup: $H \times X \to X$ group action, H commutative, $x_0 \in X$

(i) Sample $a, b \xleftarrow{\$} H$

(ii) Publish $a \cdot x_0, b \cdot x_0$

(iii) Recover $k = (ab) \cdot x_0 = b \cdot (a \cdot x_0) = a \cdot (b \cdot x_0)$

Cryptographic Group Action if it is hard to If it is hard to

(i) (“DLP”) Recover a from $(x, a \cdot x)$

Cryptography from group actions

Rephrase NIKE from group action

Setup: $H \times X \to X$ group action, H commutative, $x_0 \in X$

(i) Sample $a, b \overset{\$}{\leftarrow} H$

(ii) Publish $a \cdot x_0, b \cdot x_0$

(iii) Recover $k = (ab) \cdot x_0 = b \cdot (a \cdot x_0) = a \cdot (b \cdot x_0)$

Cryptographic Group Action if it is hard to If it is hard to

(i) ("DLP") Recover a from $(x, a \cdot x)$

(ii) ("CDHP") Recover $k = (ab) \cdot x$ from $(x, a \cdot x, b \cdot x)$

Cryptography from group actions

Rephrase NIKE from group action

Setup: $H \times X \to X$ group action, H commutative, $x_0 \in X$

(i) Sample $a, b \overset{\$}{\leftarrow} H$

(ii) Publish $a \cdot x_0, b \cdot x_0$

(iii) Recover $k = (ab) \cdot x_0 = b \cdot (a \cdot x_0) = a \cdot (b \cdot x_0)$

Cryptographic Group Action if it is hard to If it is hard to

(i) ("DLP") Recover a from $(x, a \cdot x)$

(ii) ("CDHP") Recover $k = (ab) \cdot x$ from $(x, a \cdot x, b \cdot x)$

Note These are equivalently hard problems on a quantum computer [GPSV18, MZ22, GLM24]

Cryptographic Group Actions

Conclusion CGAs generalise exponentiation and we get a NIKE

Cryptographic Group Actions

Conclusion CGAs generalise exponentiation and we get a NIKE

...but also

Public Key Encryption [CLM$^+$18]

Signatures [DFG18, BKV19]

Threshold Signatures [DFM19]

Oblivious Transfer [DdSGOPS18]

+ more (Smooth & Projective Hashing, Dual-Mode PKE, SSP-OT, Naor-Reingold PRF) [ADFMP20]

Cryptographic Group Actions

Conclusion CGAs generalise exponentiation and we get a NIKE

...but also

Public Key Encryption [CLM+18]

Signatures [DFG18, BKV19]

Threshold Signatures [DFM19]

Oblivious Transfer [DdSGOPS18]

+ more (Smooth & Projective Hashing, Dual-Mode PKE, SSP-OT, Naor-Reingold PRF) [ADFMP20]

Since: e.g. Oblivious Pseudorandom Functions [DdSGP23]

Cryptographic Group Actions

Conclusion CGAs generalise exponentiation and we get a NIKE

...but also

Public Key Encryption [CLM⁺18]

Signatures [DFG18, BKV19]

Threshold Signatures [DFM19]

Oblivious Transfer [DdSGOPS18]

+ more (Smooth & Projective Hashing, Dual-Mode PKE, SSP-OT, Naor-Reingold PRF) [ADFMP20]

Since: e.g. Oblivious Pseudorandom Functions [DdSGP23]

Naturally arising CGA from isogenies: *Isogeny Class-Group Action* [Cou97, RS06]

Attacks on CGAs

$H \times X \to X$, H commutative

Classical [GHS01]

Complexity $O\left(\sqrt{|H|}\right)$

Attacks on CGAs

$H \times X \to X$, H commutative

Classical [GHS01]

Complexity $O\left(\sqrt{|H|}\right)$

Quantum [Kup10, CJS10]

Complexity $O\left(\exp\left(\sqrt{\log(|H|)}\right)\right)$

Elliptic curves and Isogenies

Elliptic curves and Isogenies

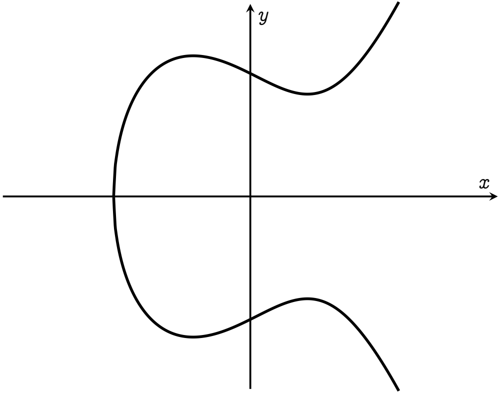
Elliptic curves are algebraic groups

Elliptic curves and Isogenies

Elliptic curves are algebraic groups

Algebraic

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



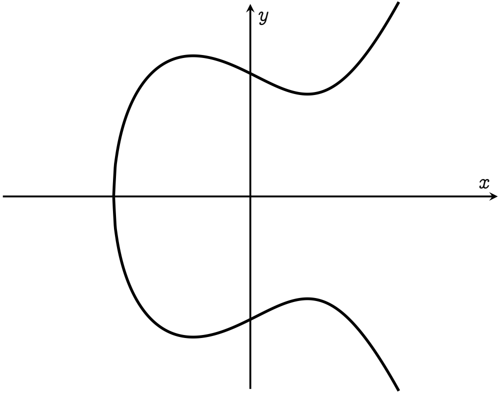
Elliptic curves and Isogenies

Elliptic curves are algebraic groups

Algebraic

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

Slogan *“Described by polynomials”*



Elliptic curves and Isogenies

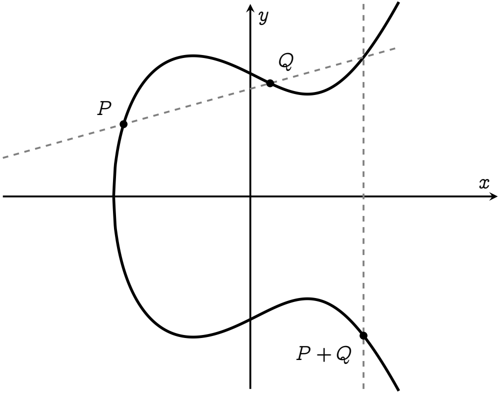
Elliptic curves are algebraic groups

Algebraic

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

Slogan *“Described by polynomials”*

Groups



Elliptic curves and Isogenies

Isogenies are morphisms of algebraic groups

Elliptic curves and Isogenies

Isogenies are morphisms of algebraic groups

Slogan *"Isogenies preserve geometric and group structure"*

Elliptic curves and Isogenies

Isogenies are morphisms of algebraic groups

Slogan *"Isogenies preserve geometric and group structure"*

Example Scalar multiplication

$$[N]_E \colon E \to E \qquad P \mapsto NP = \underbrace{P + \cdots + P}_{N \text{ times}}$$

Elliptic curves and Isogenies

Lemma Every isogeny $\varphi\colon E \to E'$ has a *reverse* $\widetilde{\varphi} : E' \to E$

Elliptic curves and Isogenies

Lemma Every isogeny $\varphi\colon E \to E'$ has a *reverse* $\widetilde{\varphi} : E' \to E$

$$\widetilde{\varphi} \circ \varphi = [d]_E \qquad \varphi \circ \widetilde{\varphi} = [d]_{E'} \qquad d = \deg(\varphi)$$

Elliptic curves and Isogenies

Lemma Every isogeny $\varphi\colon E \to E'$ has a *reverse* $\widetilde{\varphi} : E' \to E$

$$\widetilde{\varphi} \circ \varphi = [d]_E \qquad \varphi \circ \widetilde{\varphi} = [d]_{E'} \qquad d = \deg(\varphi)$$

Naïve Evaluating an isogeny of degree d costs $O(d)$

Elliptic curves and Isogenies

Lemma Every isogeny $\varphi\colon E \to E'$ has a *reverse* $\widetilde{\varphi} : E' \to E$

$$\widetilde{\varphi} \circ \varphi = [d]_E \qquad \varphi \circ \widetilde{\varphi} = [d]_{E'} \qquad d = \deg(\varphi)$$

Naïve Evaluating an isogeny of degree d costs $O(d)$

Lemma $\deg(\varphi\psi) = \deg(\varphi)\deg(\psi)$

Elliptic curves and Isogenies

Lemma Every isogeny $\varphi\colon E \to E'$ has a *reverse* $\widetilde{\varphi}: E' \to E$

$$\widetilde{\varphi} \circ \varphi = [d]_E \qquad \varphi \circ \widetilde{\varphi} = [d]_{E'} \qquad d = \deg(\varphi)$$

Naïve Evaluating an isogeny of degree d costs $O(d)$

Lemma $\deg(\varphi\psi) = \deg(\varphi)\deg(\psi)$ and when $\deg(\varphi) = p_m \cdots p_1$

$$\begin{tikzcd}
E \arrow[rrrr, "\varphi"] \arrow[dr, bend right, "\varphi_1"'] & & & & E' \\
& E_1 \arrow[r, "\varphi_2"'] & \cdots \arrow[r, "\varphi_{n-1}"'] & E_{m-1} \arrow[ur, bend right, "\varphi_m"'] &
\end{tikzcd}$$

$$\deg(\varphi_i) = p_i$$

Elliptic curves and Isogenies

Lemma Every isogeny $\varphi\colon E \to E'$ has a *reverse* $\widetilde{\varphi}\colon E' \to E$

$$\widetilde{\varphi} \circ \varphi = [d]_E \qquad \varphi \circ \widetilde{\varphi} = [d]_{E'} \qquad d = \deg(\varphi)$$

Naïve Evaluating an isogeny of degree d costs $O(d)$

Lemma $\deg(\varphi\psi) = \deg(\varphi)\deg(\psi)$ and when $\deg(\varphi) = p_m \cdots p_1$

$$\begin{tikzcd}
E \arrow[rrrr, "\varphi"] \arrow[dr, bend right, "\varphi_1"'] & & & & E' \\
& E_1 \arrow[r, "\varphi_2"'] & \cdots \arrow[r, "\varphi_{n-1}"'] & E_{m-1} \arrow[ur, bend right, "\varphi_m"'] &
\end{tikzcd}$$

$$\deg(\varphi_i) = p_i$$

Better If all $p_i \leq B$ cost of evaluating is $O(B\log(d))$

Elliptic curves and Isogenies

Lemma Every isogeny $\varphi\colon E \to E'$ has a *reverse* $\widetilde{\varphi}\colon E' \to E$

$$\widetilde{\varphi} \circ \varphi = [d]_E \qquad \varphi \circ \widetilde{\varphi} = [d]_{E'} \qquad d = \deg(\varphi)$$

Naïve Evaluating an isogeny of degree d costs $O(d)$

Lemma $\deg(\varphi\psi) = \deg(\varphi)\deg(\psi)$ and when $\deg(\varphi) = p_m \cdots p_1$

$$\begin{tikzcd}
E \arrow[rrrr, "\varphi"] \arrow[dr, bend right, "\varphi_1"'] & & & & E' \\
& E_1 \arrow[r, "\varphi_2"'] & \cdots \arrow[r, "\varphi_{n-1}"'] & E_{m-1} \arrow[ur, bend right, "\varphi_m"'] &
\end{tikzcd}$$

$$\deg(\varphi_i) = p_i$$

Better If all $p_i \leq B$ cost of evaluating is $O(B\log(d))$

Slogan *"Isogenies of smooth degree are easy to compute"*

Towards an action: The Endomorphism Ring

Towards an action: The Endomorphism Ring

Definition *Endomorphism Ring*

$$\mathrm{End}(E) = \{\varphi\colon E \to E \mid \varphi \text{ an isogeny}\}$$

Towards an action: The Endomorphism Ring

Definition *Endomorphism Ring*

$$\mathrm{End}(E) = \{\varphi\colon E \to E \mid \varphi \text{ an isogeny}\}$$

$$(\varphi + \omega)(P) \overset{\text{def.}}{=} \varphi(P) + \omega(P)$$

$$(\varphi\omega)(P) \overset{\text{def.}}{=} (\varphi \circ \omega)(P)$$

Towards an action: The Endomorphism Ring

Definition *Endomorphism Ring*

$$\mathrm{End}(E) = \{\varphi \colon E \to E \mid \varphi \text{ an isogeny}\}$$

$$(\varphi + \omega)(P) \overset{\text{def.}}{=} \varphi(P) + \omega(P)$$

$$(\varphi\omega)(P) \overset{\text{def.}}{=} (\varphi \circ \omega)(P)$$

Example Scalar multiplication $[N]_E$ is an endomorphism $E \to E$

Towards an action: Classifying the Endomorphism Rings

Towards an action: Classifying the Endomorphism Rings

Theorem (Deuring) $\mathrm{End}(E)$ isomorphic (as ring) to

(i) $\mathbb{Z}$

Towards an action: Classifying the Endomorphism Rings

Theorem (Deuring) End(E) isomorphic (as ring) to

(i) $\mathbb{Z}$

(ii) Rank-2 lattice $\mathbb{Z} + \sigma\mathbb{Z} \subseteq$ imaginary quadratic field

Towards an action: Classifying the Endomorphism Rings

Theorem (Deuring) End(E) isomorphic (as ring) to

(i) $\mathbb{Z}$

(ii) Rank-2 lattice $\mathbb{Z} + \sigma\mathbb{Z} \subseteq$ imaginary quadratic field
Commutative

Towards an action: Classifying the Endomorphism Rings

Theorem (Deuring) End(E) isomorphic (as ring) to

(i) $\mathbb{Z}$

(ii) Rank-2 lattice $\mathbb{Z} + \sigma\mathbb{Z} \subseteq$ imaginary quadratic field

Commutative

Ordinary

Towards an action: Classifying the Endomorphism Rings

Theorem (Deuring) End(E) isomorphic (as ring) to

(i) $\mathbb{Z}$

(ii) Rank-2 lattice $\mathbb{Z} + \sigma\mathbb{Z} \subseteq$ imaginary quadratic field

Commutative

Ordinary

(iv) Rank-4 lattice $\mathbb{Z} + \sigma\mathbb{Z} + \omega\mathbb{Z} + \zeta\mathbb{Z} \subseteq$ quaternion algebra

Towards an action: Classifying the Endomorphism Rings

Theorem (Deuring) End(E) isomorphic (as ring) to

(i) $\mathbb{Z}$

(ii) Rank-2 lattice $\mathbb{Z} + \sigma\mathbb{Z} \subseteq$ imaginary quadratic field

Commutative

Ordinary

(iv) Rank-4 lattice $\mathbb{Z} + \sigma\mathbb{Z} + \omega\mathbb{Z} + \zeta\mathbb{Z} \subseteq$ quaternion algebra

Non-commutative

Towards an action: Classifying the Endomorphism Rings

Theorem (Deuring) End(E) isomorphic (as ring) to

(i) $\mathbb{Z}$

(ii) Rank-2 lattice $\mathbb{Z} + \sigma\mathbb{Z} \subseteq$ imaginary quadratic field

Commutative

Ordinary

(iv) Rank-4 lattice $\mathbb{Z} + \sigma\mathbb{Z} + \omega\mathbb{Z} + \zeta\mathbb{Z} \subseteq$ quaternion algebra

Non-commutative

Supersingular

Towards an action: Classifying the Endomorphism Rings

Theorem (Deuring) End(E) isomorphic (as ring) to

(i) $\mathbb{Z}$

(ii) Rank-2 lattice $\mathbb{Z} + \sigma\mathbb{Z} \subseteq$ imaginary quadratic field

Commutative

Ordinary

(iv) Rank-4 lattice $\mathbb{Z} + \sigma\mathbb{Z} + \omega\mathbb{Z} + \zeta\mathbb{Z} \subseteq$ quaternion algebra

Non-commutative

Supersingular

We are interested in the ordinary case

Towards an action: Visualising the Endomorphism Ring

Towards an action: Visualising the Endomorphism Ring

Imaginary Quadratic Fields

Towards an action: Visualising the Endomorphism Ring

Imaginary Quadratic Fields

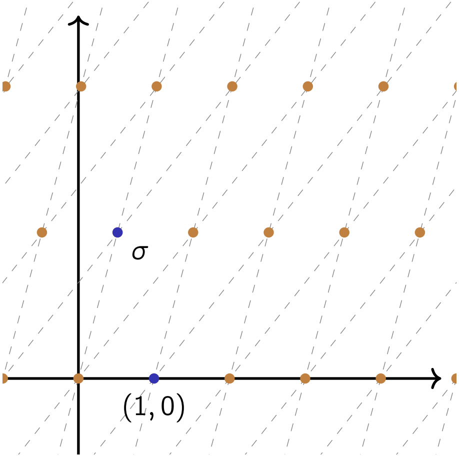
$\mathbb{Q}(\sqrt{D}) \subseteq \mathbb{C} \quad D < 0 \in \mathbb{Z}$

Towards an action: Visualising the Endomorphism Ring

Imaginary Quadratic Fields

$\mathbb{Q}(\sqrt{D}) \subseteq \mathbb{C} \quad D < 0 \in \mathbb{Z}$

$\mathrm{End}(E) \cong 1\mathbb{Z} + \sigma\mathbb{Z}$



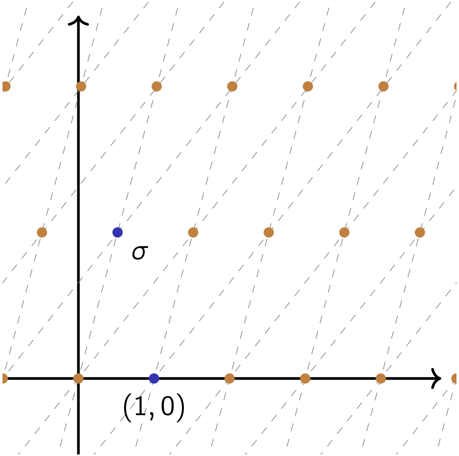
Towards an action: Visualising the Endomorphism Ring

Imaginary Quadratic Fields

$\mathbb{Q}(\sqrt{D}) \subseteq \mathbb{C} \quad D < 0 \in \mathbb{Z}$

$\mathrm{End}(E) \cong 1\mathbb{Z} + \sigma\mathbb{Z}$

Lattice + Ring = *Order* $\rightsquigarrow \mathrm{End}(E) \cong \mathcal{O}$



Isogeny Class-Group Action

Isogeny Class-Group Action

Correspondence Ideal $I \subseteq \mathcal{O} \cong \mathrm{End}(E) \rightsquigarrow$ Isogeny $I\colon E \longrightarrow E_I$

Isogeny Class-Group Action

Correspondence Ideal $I \subseteq \mathcal{O} \cong \mathrm{End}(E) \rightsquigarrow$ Isogeny $I\colon E \to E_I$

Definition Ideal Class Group and its Action

$$\mathrm{Cl}(\mathcal{O}) = \left\{ \text{Classes } [I] \text{ of ideals } I \subseteq \mathcal{O} \quad \text{s.t.} \quad \begin{array}{l} \text{(i)}\ \ \mathrm{End}(E_I) \cong \mathrm{End}(E) \cong \mathcal{O} \\ \text{(ii)}\ [I] = [J] \iff E_I \cong E_J \end{array} \right\}$$

Isogeny Class-Group Action

Correspondence Ideal $I \subseteq \mathcal{O} \cong \mathrm{End}(E) \rightsquigarrow$ Isogeny $I\colon E \to E_I$

Definition Ideal Class Group and its Action

$$\mathrm{Cl}(\mathcal{O}) = \left\{ \text{Classes } [I] \text{ of ideals } I \subseteq \mathcal{O} \quad \text{s.t.} \quad \begin{array}{l} \text{(i) } \mathrm{End}(E_I) \cong \mathrm{End}(E) \cong \mathcal{O} \\ \text{(ii) } [I] = [J] \iff E_I \cong E_J \end{array} \right\}$$

Group law: $[I][J] = [IJ]$, $[\mathcal{O}]$ is the neutral element and $[I]^{-1} = [\bar{I}]$

Isogeny Class-Group Action

Correspondence Ideal $I \subseteq \mathcal{O} \cong \mathrm{End}(E) \rightsquigarrow$ Isogeny $I\colon E \to E_I$

Definition Ideal Class Group and its Action

$$\mathrm{Cl}(\mathcal{O}) = \left\{ \text{Classes } [I] \text{ of ideals } I \subseteq \mathcal{O} \quad \text{s.t.} \quad \begin{array}{l} \text{(i)}\;\; \mathrm{End}(E_I) \cong \mathrm{End}(E) \cong \mathcal{O} \\ \text{(ii)}\; [I] = [J] \iff E_I \cong E_J \end{array} \right\}$$

Group law: $[I][J] = [IJ]$, $[\mathcal{O}]$ is the neutral element and $[I]^{-1} = [\bar{I}]$

Acts on

$$\mathrm{Ell}(\mathcal{O}) = \{\text{Isomorphism classes } [E] \text{ of elliptic curves } E \text{ s.t. } \mathrm{End}(E) \cong \mathcal{O}\}$$

Isogeny Class-Group Action

Correspondence Ideal $I \subseteq \mathcal{O} \cong \mathrm{End}(E) \rightsquigarrow$ Isogeny $I\colon E \longrightarrow E_I$

Definition Ideal Class Group and its Action

$$\mathrm{Cl}(\mathcal{O}) = \left\{ \text{Classes } [I] \text{ of ideals } I \subseteq \mathcal{O} \quad \text{s.t.} \quad \begin{array}{l} \text{(i)}\ \ \mathrm{End}(E_I) \cong \mathrm{End}(E) \cong \mathcal{O} \\ \text{(ii)}\ [I] = [J] \iff E_I \cong E_J \end{array} \right\}$$

Group law: $[I][J] = [IJ]$, $[\mathcal{O}]$ is the neutral element and $[I]^{-1} = [\bar{I}]$

Acts on

$$\mathrm{Ell}(\mathcal{O}) = \{\text{Isomorphism classes } [E] \text{ of elliptic curves } E \text{ s.t. } \mathrm{End}(E) \cong \mathcal{O}\}$$

via

$$\mathrm{Cl}(\mathcal{O}) \times \mathrm{Ell}(\mathcal{O}) \to \mathrm{Ell}(\mathcal{O}) \qquad ([I],[E]) \mapsto [I]\cdot[E] = [E_I]$$

Computing this isogeny class-group action

Computing this isogeny class-group action

Naïve

Computing this isogeny class-group action

Naïve

Input: $[I] \in \mathrm{Cl}(\mathcal{O})$ and $[E] \in \mathrm{Ell}(\mathcal{O})$

Output: $[I] \cdot [E] = [E_I]$

Computing this isogeny class-group action

Naïve

Input: $[I] \in \mathrm{Cl}(\mathcal{O})$ and $[E] \in \mathrm{Ell}(\mathcal{O})$

Output: $[I] \cdot [E] = [E_I]$

(i) Choose representative $J \subseteq \mathcal{O}$ so that $[J] = [I]$

Computing this isogeny class-group action

Naïve

Input: $[I] \in \mathrm{Cl}(\mathcal{O})$ and $[E] \in \mathrm{Ell}(\mathcal{O})$

Output: $[I] \cdot [E] = [E_I]$

(i) Choose representative $J \subseteq \mathcal{O}$ so that $[J] = [I]$

(ii) Construct isogeny $J \colon E \to E_J$

Computing this isogeny class-group action

Naïve

Input: $[I] \in \mathrm{Cl}(\mathcal{O})$ and $[E] \in \mathrm{Ell}(\mathcal{O})$

Output: $[I] \cdot [E] = [E_I]$

(i) Choose representative $J \subseteq \mathcal{O}$ so that $[J] = [I]$

(ii) Construct isogeny $J \colon E \to E_J$

(iii) Evaluate the isogeny $J \colon E \to E_J$ to obtain equation for E_J

Computing this isogeny class-group action

Naïve

Input: $[I] \in \mathrm{Cl}(\mathcal{O})$ and $[E] \in \mathrm{Ell}(\mathcal{O})$

Output: $[I] \cdot [E] = [E_I]$

(i) Choose representative $J \subseteq \mathcal{O}$ so that $[J] = [I]$

(ii) Construct isogeny $J \colon E \to E_J$

(iii) Evaluate the isogeny $J \colon E \to E_J$ to obtain equation for E_J

(iv) Return $[E_J] = [E_I]$

Computing this isogeny class-group action

Naïve

Input: $[I] \in \mathrm{Cl}(\mathcal{O})$ and $[E] \in \mathrm{Ell}(\mathcal{O})$

Output: $[I] \cdot [E] = [E_I]$

(i) Choose representative $J \subseteq \mathcal{O}$ so that $[J] = [I]$

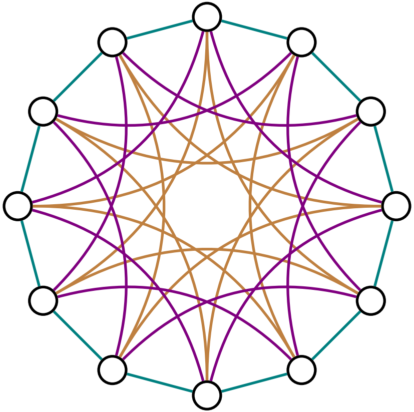
(ii) Construct isogeny $J \colon E \to E_J$

(iii) Evaluate the isogeny $J \colon E \to E_J$ to obtain equation for E_J

(iv) Return $[E_J] = [E_I]$

Problem $J \colon E \to E_J$ might have large non-smooth degree

Computing this isogeny class-group action



Higher dimensional methods: Abelian Varieties

Higher dimensional methods: Abelian Varieties

Recall Elliptic curves are algebraic groups

Higher dimensional methods: Abelian Varieties

Recall Elliptic curves are algebraic groups

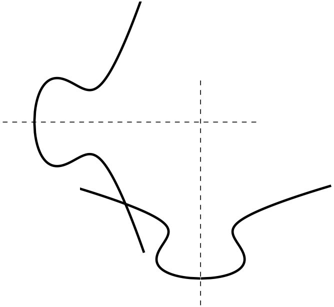
…$E \times E$ also group

Higher dimensional methods: Abelian Varieties

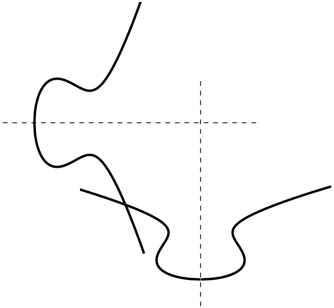
Recall Elliptic curves are algebraic groups

...$E \times E$ also group

...$E \times E$ also algebraic



Higher dimensional methods: Abelian Varieties



Recall Elliptic curves are algebraic groups

…$E \times E$ also group

…$E \times E$ also algebraic

…but $E \times E$ is not an Elliptic curve

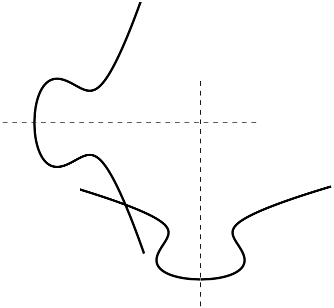
Higher dimensional methods: Abelian Varieties

Recall Elliptic curves are algebraic groups

...$E \times E$ also group

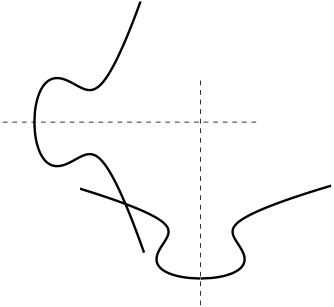
...$E \times E$ also algebraic

...but $E \times E$ is not an Elliptic curve



Resolution

Higher dimensional methods: Abelian Varieties



Recall Elliptic curves are algebraic groups

…$E \times E$ also group

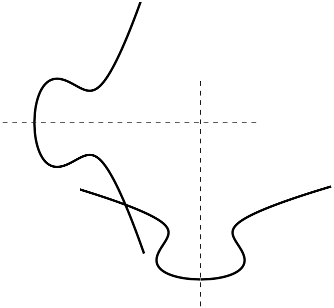
…$E \times E$ also algebraic

…but $E \times E$ is not an Elliptic curve

Resolution

Products of elliptic curves are *Abelian varieties*

Higher dimensional methods: Abelian Varieties



Recall Elliptic curves are algebraic groups

…$E \times E$ also group

…$E \times E$ also algebraic

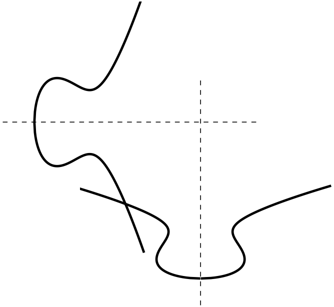
…but $E \times E$ is not an Elliptic curve

Resolution

Products of elliptic curves are *Abelian varieties*

Isogenies between Abelian varieties are morphisms of algebraic groups

Higher dimensional methods: Abelian Varieties



Recall Elliptic curves are algebraic groups

...$E \times E$ also group

...$E \times E$ also algebraic

...but $E \times E$ is not an Elliptic curve

Resolution

Products of elliptic curves are *Abelian varieties*

Isogenies between Abelian varieties are morphisms of algebraic groups

Example Scalar multiplication $[N]_A \colon A \to A; P \mapsto NP = P + \cdots + P$

Abelian Varieties: Features of isogenies

Lemma

For all isogenies

$$\varphi\colon E_1 \times \cdots \times E_n \to E_1' \times \cdots \times E_n'$$

the reverse map exists

$$\widetilde{\varphi}\colon E_1' \times \cdots \times E_n' \to E_1 \times \cdots \times E_n$$

Abelian Varieties: Features of isogenies

Lemma

For all isogenies

$$\varphi\colon E_1 \times \cdots \times E_n \to E_1' \times \cdots \times E_n'$$

the reverse map exists

$$\widetilde{\varphi}\colon E_1' \times \cdots \times E_n' \to E_1 \times \cdots \times E_n$$

Caution However it must not necessarily satisfy

$$\widetilde{\varphi} \circ \varphi = [d]_{E_1 \times \cdots \times E_n} \qquad \varphi \circ \widetilde{\varphi} = [d]_{E_1' \times \cdots \times E_n'}$$

Abelian Varieties: Features of isogenies

Lemma

For all isogenies

$$\varphi\colon E_1 \times \cdots \times E_n \to E'_1 \times \cdots \times E'_n$$

the reverse map exists

$$\widetilde{\varphi}\colon E'_1 \times \cdots \times E'_n \to E_1 \times \cdots \times E_n$$

Caution However it must not necessarily satisfy

$$\widetilde{\varphi} \circ \varphi = [d]_{E_1 \times \cdots \times E_n} \qquad \varphi \circ \widetilde{\varphi} = [d]_{E'_1 \times \cdots \times E'_n}$$

When it *does*, we say that φ has *degree d*

Abelian Varieties: Features of isogenies

Lemma

For all isogenies

$$\varphi\colon E_1 \times \cdots \times E_n \to E'_1 \times \cdots \times E'_n$$

the reverse map exists

$$\widetilde{\varphi}\colon E'_1 \times \cdots \times E'_n \to E_1 \times \cdots \times E_n$$

Caution However it must not necessarily satisfy

$$\widetilde{\varphi} \circ \varphi = [d]_{E_1\times\cdots\times E_n} \qquad \varphi \circ \widetilde{\varphi} = [d]_{E'_1\times\cdots\times E'_n}$$

When it *does*, we say that φ has *degree d*

Naïve Evaluating an isogeny of degree d costs $O(d)$

Abelian Varieties: Features of isogenies

Abelian Varieties: Features of isogenies

Lemma $\deg(\varphi\psi) = \deg(\varphi)\deg(\psi)$

Abelian Varieties: Features of isogenies

Lemma $\deg(\varphi\psi) = \deg(\varphi)\deg(\psi)$ and when $\deg(\varphi) = p_m \cdots p_1$

$$\begin{tikzcd}
E_1 \times \cdots \times E_n \arrow[rrrr, "\varphi"] \arrow[dr, bend right, "\varphi_1"'] & & & & E'_1 \times \cdots \times E'_n \\
& A_1 \arrow[r, "\varphi_2"'] & \cdots \arrow[r, "\varphi_{n-1}"'] & A_{m-1} \arrow[ur, bend right, "\varphi_m"'] &
\end{tikzcd}$$

$\deg(\varphi_i) = p_i$

Abelian Varieties: Features of isogenies

Lemma $\deg(\varphi\psi) = \deg(\varphi)\deg(\psi)$ and when $\deg(\varphi) = p_m \cdots p_1$

$$\begin{tikzcd}
E_1 \times \cdots \times E_n \arrow[rrrr, "\varphi"] \arrow[dr, bend right, "\varphi_1"'] & & & & E_1' \times \cdots \times E_n' \\
& A_1 \arrow[r, "\varphi_2"'] & \cdots \arrow[r, "\varphi_{n-1}"'] & A_{m-1} \arrow[ur, bend right, "\varphi_m"'] &
\end{tikzcd}$$

$\deg(\varphi_i) = p_i$

Better If all $p_i \leq B$ cost of evaluating is $O(B\log(d))$

Abelian Varieties: Features of isogenies

Lemma $\deg(\varphi\psi) = \deg(\varphi)\deg(\psi)$ and when $\deg(\varphi) = p_m \cdots p_1$

$$\begin{tikzcd}
E_1 \times \cdots \times E_n \arrow[rrrr, "\varphi"] \arrow[dr, bend right, "\varphi_1"'] & & & & E_1' \times \cdots \times E_n' \\
& A_1 \arrow[r, "\varphi_2"'] & \cdots \arrow[r, "\varphi_{n-1}"'] & A_{m-1} \arrow[ur, bend right, "\varphi_m"'] &
\end{tikzcd}$$

$\deg(\varphi_i) = p_i$

Better If all $p_i \leq B$ cost of evaluating is $O(B \log(d))$

Slogan *"Isogenies of smooth degree are easy to compute"*

Abelian Varieties: Features of isogenies

Lemma $\deg(\varphi\psi) = \deg(\varphi)\deg(\psi)$ and when $\deg(\varphi) = p_m \cdots p_1$

$$\begin{tikzcd}
E_1 \times \cdots \times E_n \arrow[rrrr, "\varphi"] \arrow[dr, bend right, "\varphi_1"'] & & & & E_1' \times \cdots \times E_n' \\
& A_1 \arrow[r, "\varphi_2"'] & \cdots \arrow[r, "\varphi_{n-1}"'] & A_{m-1} \arrow[ur, bend right, "\varphi_m"'] &
\end{tikzcd}$$

$\deg(\varphi_i) = p_i$

Better If all $p_i \leq B$ cost of evaluating is $O(B\log(d))$

Slogan *"Isogenies of smooth degree are easy to compute"*

Caution A_i generic Abelian Variety (not necessarily $E_1'' \times \cdots \times E_n''$)

Abelian Varieties: Features of isogenies

Lemma $\deg(\varphi\psi) = \deg(\varphi)\deg(\psi)$ and when $\deg(\varphi) = p_m \cdots p_1$

$$\begin{tikzcd}
E_1 \times \cdots \times E_n \arrow[rrrr, "\varphi"] \arrow[dr, bend right, "\varphi_1"'] & & & & E'_1 \times \cdots \times E'_n \\
& A_1 \arrow[r, "\varphi_2"'] & \cdots \arrow[r, "\varphi_{n-1}"'] & A_{m-1} \arrow[ur, bend right, "\varphi_m"'] &
\end{tikzcd}$$

$\deg(\varphi_i) = p_i$

Better If all $p_i \leq B$ cost of evaluating is $O(B\log(d))$

Slogan *"Isogenies of smooth degree are easy to compute"*

Caution A_i generic Abelian Variety (not necessarily $E''_1 \times \cdots \times E''_n$)

Evaluating φ_i requires heavy machinery: *Mumford's Theta Coordinates*

Going into higher dimensions: Kani's Lemma

Lemma (Kani)

From a commuting square of isogenies between elliptic curves

$$\begin{tikzcd} E_1 \arrow[r, "g_1"] \arrow[d, "h_1"'] & E_3 \arrow[d, "g_2"] \\ E_4 \arrow[r, "h_2"'] & E_2 \end{tikzcd}$$

$$d_1 = \deg(g_1) = \deg(h_2)$$
$$d_2 = \deg(h_1) = \deg(g_2)$$

Going into higher dimensions: Kani's Lemma

Lemma (Kani)

From a commuting square of isogenies between elliptic curves

$$\begin{tikzcd} E_1 \arrow[r, "g_1"] \arrow[d, "h_1"'] & E_3 \arrow[d, "g_2"] \\ E_4 \arrow[r, "h_2"'] & E_2 \end{tikzcd}$$

$$d_1 = \deg(g_1) = \deg(h_2)$$
$$d_2 = \deg(h_1) = \deg(g_2)$$

we get the *Kani isogeny*

$$K = \begin{pmatrix} g_1 & \widetilde{g_2} \\ -h_1 & \widetilde{h_2} \end{pmatrix} : E_1 \times E_2 \to E_3 \times E_4$$

Going into higher dimensions: Kani's Lemma

Lemma (Kani)

From a commuting square of isogenies between elliptic curves

$$\begin{tikzcd} E_1 \arrow[r, "g_1"] \arrow[d, "h_1"'] & E_3 \arrow[d, "g_2"] \\ E_4 \arrow[r, "h_2"'] & E_2 \end{tikzcd}$$

$$d_1 = \deg(g_1) = \deg(h_2)$$
$$d_2 = \deg(h_1) = \deg(g_2)$$

we get the *Kani isogeny*

$$K = \begin{pmatrix} g_1 & \widetilde{g_2} \\ -h_1 & \widetilde{h_2} \end{pmatrix} : E_1 \times E_2 \to E_3 \times E_4$$

of degree

$$\deg(K) = d_1 + d_2$$

Going into higher dimensions: Kani's Lemma

Lemma (Kani)

From a commuting square of isogenies between powers of elliptic curves

$$\begin{tikzcd} E_1^n \arrow[r, "g_1"] \arrow[d, "h_1"'] & E_3^n \arrow[d, "g_2"] \\ E_4^n \arrow[r, "h_2"'] & E_2^n \end{tikzcd}$$

$$d_1 = \deg(g_1) = \deg(h_2)$$
$$d_2 = \deg(h_1) = \deg(g_2)$$

we get the *Kani isogeny*

$$K = \begin{pmatrix} g_1 & \widetilde{g_2} \\ -h_1 & \widetilde{h_2} \end{pmatrix} : E_1^n \times E_2^n \to E_3^n \times E_4^n$$

of degree

$$\deg(K) = d_1 + d_2$$

Going into higher dimensions: Kani's Lemma

Lemma (Kani)

From a commuting square of isogenies between general Abelian varieties

$$\begin{tikzcd} A_1 \arrow[r, "g_1"] \arrow[d, "h_1"'] & A_3 \arrow[d, "g_2"] \\ A_4 \arrow[r, "h_2"'] & A_2 \end{tikzcd}$$

$$d_1 = \deg(g_1) = \deg(h_2)$$
$$d_2 = \deg(h_1) = \deg(g_2)$$

we get the *Kani isogeny*

$$K = \begin{pmatrix} g_1 & \widetilde{g_2} \\ -h_1 & \widetilde{h_2} \end{pmatrix} : A_1 \times A_2 \to A_3 \times A_4$$

of degree

$$\deg(K) = d_1 + d_2$$

Going into higher dimensions: Kani's Lemma

Interpretation Kani's Lemma

$$\begin{tikzcd} E_1 \arrow[r, "g_1"] \arrow[d, "h_1"'] & E_3 \arrow[d, "g_2"] \\ E_4 \arrow[r, "h_2"'] & E_2 \end{tikzcd} \quad \rightsquigarrow \quad K = \begin{pmatrix} g_1 & \widetilde{g_2} \\ -h_1 & \widetilde{h_2} \end{pmatrix} : E_1 \times E_2 \to E_3 \times E_4$$

Going into higher dimensions: Kani's Lemma

Interpretation Kani's Lemma

$$\begin{tikzcd} E_1 \arrow[r, "g_1"] \arrow[d, "h_1"'] & E_3 \arrow[d, "g_2"] \\ E_4 \arrow[r, "h_2"'] & E_2 \end{tikzcd} \quad \rightsquigarrow \quad K = \begin{pmatrix} g_1 & \widetilde{g_2} \\ -h_1 & \widetilde{h_2} \end{pmatrix} : E_1 \times E_2 \to E_3 \times E_4$$

Slogan *"Isogenies of dimension* 1 *have been embedded into dimension* 2*"*

Going into higher dimensions: Kani's Lemma

Interpretation Kani's Lemma

$$\begin{tikzcd} E_1 \arrow[r, "g_1"] \arrow[d, "h_1"'] & E_3 \arrow[d, "g_2"] \\ E_4 \arrow[r, "h_2"'] & E_2 \end{tikzcd} \rightsquigarrow \quad K = \begin{pmatrix} g_1 & \widetilde{g_2} \\ -h_1 & \widetilde{h_2} \end{pmatrix} : E_1 \times E_2 \to E_3 \times E_4$$

Slogan *"Isogenies of dimension* 1 *have been embedded into dimension* 2*"*

Idea $\deg(K) = d_1 + d_2$

If g_i, h_i so that $\deg(K) = d_1 + d_2 = \deg(g_1) + \deg(h_1)$ is smooth

Going into higher dimensions: Kani's Lemma

Interpretation Kani's Lemma

$$\begin{tikzcd} E_1 \arrow[r, "g_1"] \arrow[d, "h_1"'] & E_3 \arrow[d, "g_2"] \\ E_4 \arrow[r, "h_2"'] & E_2 \end{tikzcd} \quad \rightsquigarrow \quad K = \begin{pmatrix} g_1 & \widetilde{g_2} \\ -h_1 & \widetilde{h_2} \end{pmatrix} : E_1 \times E_2 \to E_3 \times E_4$$

Slogan *"Isogenies of dimension* 1 *have been embedded into dimension* 2*"*

Idea $\deg(K) = d_1 + d_2$

If g_i, h_i so that $\deg(K) = d_1 + d_2 = \deg(g_1) + \deg(h_1)$ is smooth

...we can evaluate K easily!

Going into higher dimensions: Kani's Lemma

Interpretation Kani's Lemma

$$\begin{tikzcd} E_1 \arrow[r, "g_1"] \arrow[d, "h_1"'] & E_3 \arrow[d, "g_2"] \\ E_4 \arrow[r, "h_2"'] & E_2 \end{tikzcd} \quad \rightsquigarrow \quad K = \begin{pmatrix} g_1 & \widetilde{g_2} \\ -h_1 & \widetilde{h_2} \end{pmatrix} : E_1 \times E_2 \to E_3 \times E_4$$

Slogan *"Isogenies of dimension* 1 *have been embedded into dimension* 2*"*

Idea $\deg(K) = d_1 + d_2$

If g_i, h_i so that $\deg(K) = d_1 + d_2 = \deg(g_1) + \deg(h_1)$ is smooth

...we can evaluate K easily!

...then recover g_i, h_i by evaluating K

Going into higher dimensions: Kani's Lemma

Interpretation Kani's Lemma

$$\begin{tikzcd} E_1 \arrow[r, "g_1"] \arrow[d, "h_1"'] & E_3 \arrow[d, "g_2"] \\ E_4 \arrow[r, "h_2"'] & E_2 \end{tikzcd} \quad \rightsquigarrow \quad K = \begin{pmatrix} g_1 & \widetilde{g_2} \\ -h_1 & \widetilde{h_2} \end{pmatrix} : E_1 \times E_2 \to E_3 \times E_4$$

Slogan *"Isogenies of dimension* 1 *have been embedded into dimension* 2*"*

Idea $\deg(K) = d_1 + d_2$

If g_i, h_i so that $\deg(K) = d_1 + d_2 = \deg(g_1) + \deg(h_1)$ is smooth

...we can evaluate K easily!

...then recover g_i, h_i by evaluating K e.g.

$$\begin{pmatrix} g_1 & \widetilde{g_2} \\ -h_1 & \widetilde{h_2} \end{pmatrix} \begin{pmatrix} P \\ 0 \end{pmatrix} = \begin{pmatrix} g_1(P) \\ -h_1(P) \end{pmatrix} \quad \rightsquigarrow \quad g_1(P)$$

Clapoti [PR23]

Clapoti [PR23]

Recall

Clapoti [PR23]

Recall

(i) $\mathrm{End}(E) \cong \mathcal{O} \subseteq \mathbb{Q}(\sqrt{D})$

Clapoti [PR23]

Recall

(i) $\mathrm{End}(E) \cong \mathcal{O} \subseteq \mathbb{Q}(\sqrt{D})$

(ii) $I \subseteq \mathcal{O}$ ideal $\rightsquigarrow I\colon E \to E_I$ isogeny

Clapoti [PR23]

Recall

(i) $\mathrm{End}(E) \cong \mathcal{O} \subseteq \mathbb{Q}(\sqrt{D})$

(ii) $I \subseteq \mathcal{O}$ ideal $\rightsquigarrow I\colon E \to E_I$ isogeny

(iii) $[I] \cdot [E] \to [E_I]$ is a group action

$$[I] \cdot ([J] \cdot [E]) = [I][J] \cdot [E] = [IJ] \cdot [E] = [JI] \cdot [E] = [J][I] \cdot [E] = [J] \cdot ([I] \cdot [E])$$

Clapoti [PR23]

Recall

(i) $\mathrm{End}(E) \cong \mathcal{O} \subseteq \mathbb{Q}(\sqrt{D})$

(ii) $I \subseteq \mathcal{O}$ ideal $\rightsquigarrow I\colon E \to E_I$ isogeny

(iii) $[I] \cdot [E] \to [E_I]$ is a group action

$$[I] \cdot ([J] \cdot [E]) = [I][J] \cdot [E] = [IJ] \cdot [E] = [JI] \cdot [E] = [J][I] \cdot [E] = [J] \cdot ([I] \cdot [E])$$

in a diagram

$$\begin{tikzcd}
{[E]} \arrow[r, "{[I]}"] \arrow[d, "{[J]}"'] & {[E_I]} \arrow[d, "{[J]}"] \\
{[E_J]} \arrow[r, "{[I]}"'] & {[E_{IJ}]}
\end{tikzcd}$$

Clapoti [PR23]

Recall

(i) $\mathrm{End}(E) \cong \mathcal{O} \subseteq \mathbb{Q}(\sqrt{D})$

(ii) $I \subseteq \mathcal{O}$ ideal $\rightsquigarrow$ $I\colon E \to E_I$ isogeny

(iii) $[I] \cdot [E] \to [E_I]$ is a group action

$$[I] \cdot ([J] \cdot [E]) = [I][J] \cdot [E] = [IJ] \cdot [E] = [JI] \cdot [E] = [J][I] \cdot [E] = [J] \cdot ([I] \cdot [E])$$

in a diagram

$$\begin{tikzcd} {[E]} \arrow[r, "{[I]}"] \arrow[d, "{[J]}"'] & {[E_I]} \arrow[d, "{[J]}"] \\ {[E_J]} \arrow[r, "{[I]}"'] & {[E_{IJ}]} \end{tikzcd}$$

$$\rightsquigarrow$$

$$\begin{tikzcd} E \arrow[r, "I"] \arrow[d, "J"'] & E_I \arrow[d, "J"] \\ E_J \arrow[r, "I"'] & E' \cong E_{IJ} \end{tikzcd}$$

Clapoti [PR23]

Recall $[I]^{-1} = [\bar{I}]$.

Clapoti [PR23]

Recall $[I]^{-1} = [\bar{I}]$. So if $[J] = [I]$ then $[\bar{J}] = [J]^{-1} = [I]^{-1}$

Clapoti [PR23]

Recall $[I]^{-1} = [\bar{I}]$. So if $[J] = [I]$ then $[\bar{J}] = [J]^{-1} = [I]^{-1}$

$$\begin{tikzcd}
{[E]} \arrow[r, "{[I]}"] \arrow[d, "{[\bar{J}]}"'] & {[E_I]} \arrow[d, "{[\bar{J}]}"] \\
{[E_{\bar{J}}]} \arrow[r, "{[I]}"'] & {[E]}
\end{tikzcd}$$

Clapoti [PR23]

Recall $[I]^{-1} = [\bar{I}]$. So if $[J] = [I]$ then $[\bar{J}] = [J]^{-1} = [I]^{-1}$

$$\begin{tikzcd}
{[E]} \arrow[r, "{[I]}"] \arrow[d, "{[\bar{J}]}"'] & {[E_I]} \arrow[d, "{[\bar{J}]}"] \\
{[E_{\bar{J}}]} \arrow[r, "{[I]}"'] & {[E]}
\end{tikzcd}
\rightsquigarrow
\begin{tikzcd}
E \arrow[r, "I"] \arrow[d, "\bar{J}"'] & E_I \arrow[d, "\bar{J}"] \\
E_{\bar{J}} \arrow[r, "I"'] & E \cong E_{I\bar{J}}
\end{tikzcd}$$

Clapoti [PR23]

Recall $[I]^{-1} = [\bar{I}]$. So if $[J] = [I]$ then $[\bar{J}] = [J]^{-1} = [I]^{-1}$

$$\begin{tikzcd}
{[E]} \arrow[r, "{[I]}"] \arrow[d, "{[\bar{J}]}"'] & {[E_I]} \arrow[d, "{[\bar{J}]}"] & & E \arrow[r, "I"] \arrow[d, "\bar{J}"'] & E_I \arrow[d, "\bar{J}"] \\
{[E_{\bar{J}}]} \arrow[r, "{[I]}"'] & {[E]} \arrow[r, phantom, "\rightsquigarrow"] & {} & E_{\bar{J}} \arrow[r, "I"'] & E \cong E_{I\bar{J}}
\end{tikzcd}$$

Clapoti [PR23]

Recall $[I]^{-1} = [\bar{I}]$. So if $[J] = [I]$ then $[\bar{J}] = [J]^{-1} = [I]^{-1}$

$$\begin{tikzcd}
{[E]} \arrow[r, "{[I]}"] \arrow[d, "{[\bar{J}]}"'] & {[E_I]} \arrow[d, "{[\bar{J}]}"] \\
{[E_{\bar{J}}]} \arrow[r, "{[I]}"'] & {[E]}
\end{tikzcd}
\rightsquigarrow
\begin{tikzcd}
E \arrow[r, "I"] \arrow[d, "\bar{J}"'] & E_I \arrow[d, "\bar{J}"] \\
E_{\bar{J}} \arrow[r, "I"'] & E \cong E_{I\bar{J}}
\end{tikzcd}$$

(i) Square commutes

Clapoti [PR23]

Recall $[I]^{-1} = [\bar{I}]$. So if $[J] = [I]$ then $[\bar{J}] = [J]^{-1} = [I]^{-1}$

$$\begin{tikzcd}
{[E]} \arrow[r, "{[I]}"] \arrow[dd, "{[\bar{J}]}"'] & {[E_I]} \arrow[dd, "{[\bar{J}]}"] & & E \arrow[r, "I"] \arrow[dd, "\bar{J}"'] & E_I \arrow[dd, "\bar{J}"] \\
& & \rightsquigarrow & & \\
{[E_{\bar{J}}]} \arrow[r, "{[I]}"'] & {[E]} & & E_{\bar{J}} \arrow[r, "I"'] & E \cong E_{I\bar{J}}
\end{tikzcd}$$

(i) Square commutes

(ii) Horizontal degree $\deg(I)$

Clapoti [PR23]

Recall $[I]^{-1} = [\bar{I}]$. So if $[J] = [I]$ then $[\bar{J}] = [J]^{-1} = [I]^{-1}$

$$\begin{tikzcd}
{[E]} \arrow[r, "{[I]}"] \arrow[dd, "{[\bar{J}]}"'] & {[E_I]} \arrow[dd, "{[\bar{J}]}"] & & & E \arrow[r, "I"] \arrow[dd, "\bar{J}"'] & E_I \arrow[dd, "\bar{J}"] \\
& & {} \arrow[r, rightsquigarrow] & {} & & \\
{[E_{\bar{J}}]} \arrow[r, "{[I]}"'] & {[E]} & & & E_{\bar{J}} \arrow[r, "I"'] & E \cong E_{I\bar{J}}
\end{tikzcd}$$

(i) Square commutes

(ii) Horizontal degree $\deg(I)$

(iii) Vertical degree $\deg(\bar{J})$

Clapoti [PR23]

Recall $[I]^{-1} = [\bar{I}]$. So if $[J] = [I]$ then $[\bar{J}] = [J]^{-1} = [I]^{-1}$

$$\begin{tikzcd}
{[E]} \arrow[r, "{[I]}"] \arrow[d, "{[\bar{J}]}"'] & {[E_I]} \arrow[d, "{[\bar{J}]}"] \\
{[E_{\bar{J}}]} \arrow[r, "{[I]}"'] & {[E]}
\end{tikzcd}
\quad \rightsquigarrow \quad
\begin{tikzcd}
E \arrow[r, "I"] \arrow[d, "\bar{J}"'] & E_I \arrow[d, "\bar{J}"] \\
E_{\bar{J}} \arrow[r, "I"'] & E \cong E_{I\bar{J}}
\end{tikzcd}$$

(i) Square commutes

(ii) Horizontal degree $\deg(I)$

(iii) Vertical degree $\deg(\bar{J}) = \deg(J)$

Clapoti [PR23]

Recall $[I]^{-1} = [\bar{I}]$. So if $[J] = [I]$ then $[\bar{J}] = [J]^{-1} = [I]^{-1}$

$$\begin{tikzcd}
{[E]} \arrow[r, "{[I]}"] \arrow[dd, "{[\bar{J}]}"'] & {[E_I]} \arrow[dd, "{[\bar{J}]}"] & & E \arrow[r, "I"] \arrow[dd, "\bar{J}"'] & E_I \arrow[dd, "\bar{J}"] \\
& & \rightsquigarrow & & \\
{[E_{\bar{J}}]} \arrow[r, "{[I]}"'] & {[E]} & & E_{\bar{J}} \arrow[r, "I"'] & E \cong E_{I\bar{J}}
\end{tikzcd}$$

(i) Square commutes

(ii) Horizontal degree $\deg(I)$

(iii) Vertical degree $\deg(\bar{J}) = \deg(J)$

Conclusion This is a Kani-square!

Clapoti [PR23]

Recall $[I]^{-1} = [\bar{I}]$. So if $[J] = [I]$ then $[\bar{J}] = [J]^{-1} = [I]^{-1}$

$$\begin{tikzcd}
{[E]} \arrow[r, "{[I]}"] \arrow[d, "{[\bar{J}]}"'] & {[E_I]} \arrow[d, "{[\bar{J}]}"] \\
{[E_{\bar{J}}]} \arrow[r, "{[I]}"'] & {[E]}
\end{tikzcd}
\rightsquigarrow
\begin{tikzcd}
E \arrow[r, "I"] \arrow[d, "\bar{J}"'] & E_I \arrow[d, "\bar{J}"] \\
E_{\bar{J}} \arrow[r, "I"'] & E \cong E_{I\bar{J}}
\end{tikzcd}$$

(i) Square commutes

(ii) Horizontal degree $\deg(I)$

(iii) Vertical degree $\deg(\bar{J}) = \deg(J)$

Conclusion This is a Kani-square!

Kani-map K has degree $N = \deg(I) + \deg(J)$

Clapoti [PR23]

Problem $N = \deg(I) + \deg(J)$ might not be smooth

Clapoti [PR23]

Problem $N = \deg(I) + \deg(J)$ might not be smooth

Idea

$\alpha, \beta \in \mathcal{O} \cong \mathrm{End}(E)$

$$\begin{tikzcd}
E \arrow[r, "\alpha"] \arrow[d, "\beta"'] & E \arrow[r, "I"] & E_I \arrow[d, "\beta"] \\
E \arrow[d, "\bar{J}"'] & E \arrow[r, "I"] \arrow[d, "\bar{J}"'] & E_I \arrow[d, "\bar{J}"] \\
E_{\bar{J}} \arrow[r, "\alpha"'] & E_{\bar{J}} \arrow[r, "I"'] & E
\end{tikzcd}$$

Again a Kani-square!

Clapoti [PR23]

Problem $N = \deg(I) + \deg(J)$ might not be smooth

Idea

$\alpha, \beta \in \mathcal{O} \cong \mathrm{End}(E)$

$$\begin{tikzcd}
E \arrow[r, "\alpha"] \arrow[d, "\beta"'] & E \arrow[r, "I"] & E_I \arrow[d, "\beta"] \\
E \arrow[d, "\bar{J}"'] & E \arrow[r, "I"] \arrow[d, "\bar{J}"'] & E_I \arrow[d, "\bar{J}"] \\
E_{\bar{J}} \arrow[r, "\alpha"'] & E_{\bar{J}} \arrow[r, "I"'] & E
\end{tikzcd}$$

Again a Kani-square!

Induced Kani-map degree $N = \deg(\alpha I) + \deg(\beta J) = \deg(\alpha)\deg(I) + \deg(\beta)\deg(J)$

Clapoti [PR23]

Problem $N = \deg(I) + \deg(J)$ might not be smooth

Idea

$\alpha, \beta \in \mathcal{O} \cong \mathrm{End}(E)$

$$\begin{tikzcd}
E \arrow[r, "\alpha"] \arrow[d, "\beta"'] & E \arrow[r, "I"] & E_I \arrow[d, "\beta"] \\
E \arrow[d, "\bar{J}"'] & E \arrow[r, "I"] \arrow[d, "\bar{J}"'] & E_I \arrow[d, "\bar{J}"] \\
E_{\bar{J}} \arrow[r, "\alpha"'] & E_{\bar{J}} \arrow[r, "I"'] & E
\end{tikzcd}$$

Again a Kani-square!

Induced Kani-map degree $N = \deg(\alpha I) + \deg(\beta J) = \deg(\alpha)\deg(I) + \deg(\beta)\deg(J)$

Slogan *"Composing with endomorphisms gives us wiggle room"*

Clapoti [PR23]

Extend this idea

Clapoti [PR23]

Extend this idea

Idea Endomorphism $E^2 \longrightarrow E^2$

$$\alpha = \begin{pmatrix} a_1 & a_2 \\ -a_2 & a_1 \end{pmatrix} : E^2 \longrightarrow E^2 \qquad\qquad a_1, a_2 \in \mathbb{Z}$$

has

$$\deg(\alpha) = a_1^2 + a_2^2$$

Clapoti [PR23]

Extend this idea

Idea Endomorphism $E^4 \to E^4$

$$\alpha = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ -a_2 & a_1 & a_4 & -a_3 \\ -a_3 & -a_4 & a_1 & a_2 \\ -a_4 & a_3 & -a_2 & a_1 \end{pmatrix} : E^4 \to E^4 \qquad a_1, a_2, a_3, a_4 \in \mathbb{Z}$$

has

$$\deg(\alpha) = a_1^2 + a_2^2 + a_3^2 + a_4^2$$

Clapoti [PR23]

Extend this idea

Idea Endomorphism $E^4 \to E^4$

$$\alpha = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ -a_2 & a_1 & a_4 & -a_3 \\ -a_3 & -a_4 & a_1 & a_2 \\ -a_4 & a_3 & -a_2 & a_1 \end{pmatrix} : E^4 \to E^4 \qquad a_1, a_2, a_3, a_4 \in \mathbb{Z}$$

has

$$\deg(\alpha) = a_1^2 + a_2^2 + a_3^2 + a_4^2$$

Theorem (Jacobi) Every positive integer is the sum of four squares

Clapoti [PR23]

Conclusion For any smooth N and ideals I, J find $\alpha, \beta \in \mathrm{Mat}_{4\times 4}(\mathbb{Z})$ so that

$$N = \deg(\alpha)\deg(I) + \deg(\beta)\deg(J)$$

Clapoti [PR23]

Conclusion For any smooth N and ideals I, J find $\alpha, \beta \in \mathrm{Mat}_{4\times 4}(\mathbb{Z})$ so that

$$N = \deg(\alpha)\deg(I) + \deg(\beta)\deg(J)$$

Then get diagram

$$\begin{tikzcd}
E^4 \arrow[r, "\alpha"] \arrow[d, swap, "\beta"] & E^4 \arrow[r, "I^{(4)}"] & E_I^4 \arrow[d, "\beta"] \\
E^4 \arrow[d, swap, "\bar{J}^{(4)}"] & E^4 \arrow[r, "I^{(4)}"] \arrow[d, swap, "\bar{J}^{(4)}"] & E_I^4 \arrow[d, "\bar{J}^{(4)}"] \\
E_{\bar{J}}^4 \arrow[r, swap, "\alpha"] & E_{\bar{J}}^4 \arrow[r, swap, "I^{(4)}"] & E^4
\end{tikzcd}$$

where

$$I^{(4)} = \begin{pmatrix} I & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & I \end{pmatrix} : E^4 \to E_I^4$$

Clapoti [PR23]

Conclusion For any smooth N and ideals I, J find $\alpha, \beta \in \mathrm{Mat}_{4\times 4}(\mathbb{Z})$ so that

$$N = \deg(\alpha)\deg(I) + \deg(\beta)\deg(J)$$

Then get diagram

$$\begin{tikzcd}
E^4 \arrow[r, "\alpha"] \arrow[d, "\beta"'] & E^4 \arrow[r, "I^{(4)}"] & E_I^4 \arrow[d, "\beta"] \\
E^4 \arrow[d, "\bar{J}^{(4)}"'] & E^4 \arrow[r, "I^{(4)}"] \arrow[d, "\bar{J}^{(4)}"'] & E_I^4 \arrow[d, "\bar{J}^{(4)}"] \\
E_{\bar{J}}^4 \arrow[r, "\alpha"'] & E_{\bar{J}}^4 \arrow[r, "I^{(4)}"'] & E^4
\end{tikzcd}$$

where

$$I^{(4)} = \begin{pmatrix} I & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & I \end{pmatrix} : E^4 \to E_I^4$$

Again a Kani-square!

Clapoti [PR23]

Conclusion For any smooth N and ideals I, J find $\alpha, \beta \in \mathrm{Mat}_{4\times 4}(\mathbb{Z})$ so that

$$N = \deg(\alpha)\deg(I) + \deg(\beta)\deg(J)$$

Then get diagram

$$\begin{tikzcd}
E^4 \arrow[r, "\alpha"] \arrow[d, "\beta"'] & E^4 \arrow[r, "I^{(4)}"] & E_I^4 \arrow[d, "\beta"] \\
E^4 \arrow[d, "\bar{J}^{(4)}"'] & E^4 \arrow[r, "I^{(4)}"] \arrow[d, "\bar{J}^{(4)}"'] & E_I^4 \arrow[d, "\bar{J}^{(4)}"] \\
E_{\bar{J}}^4 \arrow[r, "\alpha"'] & E_{\bar{J}}^4 \arrow[r, "I^{(4)}"'] & E^4
\end{tikzcd}$$

where
$$I^{(4)} = \begin{pmatrix} I & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & I \end{pmatrix} : E^4 \to E_I^4$$

Again a Kani-square!

Induced Kani-map has degree $N = \deg(\alpha)\deg(I) + \deg(\beta)\deg(J)$ smooth!

Clapoti Summary

Input: Ideal class $[H] \in \mathrm{Cl}(\mathcal{O})$, Curve class $[E] \in \mathrm{Ell}(\mathcal{O})$

Output: $[E_H]$

1. Find $I, J \subseteq \mathcal{O}$ such that: (i) $[I] = [J] = [H]$

Clapoti Summary

Input: Ideal class $[H] \in \mathrm{Cl}(\mathcal{O})$, Curve class $[E] \in \mathrm{Ell}(\mathcal{O})$

Output: $[E_H]$

1. Find $I, J \subseteq \mathcal{O}$ such that: (i) $[I] = [J] = [H]$ (ii) $\deg(I)$ prime to $\deg(J)$

Clapoti Summary

Input: Ideal class $[H] \in \mathrm{Cl}(\mathcal{O})$, Curve class $[E] \in \mathrm{Ell}(\mathcal{O})$

Output: $[E_H]$

1. Find $I, J \subseteq \mathcal{O}$ such that: (i) $[I] = [J] = [H]$ (ii) $\deg(I)$ prime to $\deg(J)$
2. Find a, b so that $N = a \deg(I) + b \deg(J)$ is smooth

Clapoti Summary

Input: Ideal class $[H] \in \mathrm{Cl}(\mathcal{O})$, Curve class $[E] \in \mathrm{Ell}(\mathcal{O})$

Output: $[E_H]$

1. Find $I, J \subseteq \mathcal{O}$ such that: (i) $[I] = [J] = [H]$ (ii) $\deg(I)$ prime to $\deg(J)$
2. Find a, b so that $N = a\deg(I) + b\deg(J)$ is smooth
3. Compute a_1, a_2, a_3, a_4 such that $a = a_1^2 + a_2^2 + a_3^2 + a_4^2$ (same for b)

Clapoti Summary

Input: Ideal class $[H] \in \mathrm{Cl}(\mathcal{O})$, Curve class $[E] \in \mathrm{Ell}(\mathcal{O})$

Output: $[E_H]$

1. Find $I, J \subseteq \mathcal{O}$ such that: (i) $[I] = [J] = [H]$ (ii) $\deg(I)$ prime to $\deg(J)$
2. Find a, b so that $N = a\deg(I) + b\deg(J)$ is smooth
3. Compute a_1, a_2, a_3, a_4 such that $a = a_1^2 + a_2^2 + a_3^2 + a_4^2$ (same for b)
4. Write down the matrices α, β

Clapoti Summary

Input: Ideal class $[H] \in \mathrm{Cl}(\mathcal{O})$, Curve class $[E] \in \mathrm{Ell}(\mathcal{O})$

Output: $[E_H]$

1. Find $I, J \subseteq \mathcal{O}$ such that: (i) $[I] = [J] = [H]$ (ii) $\deg(I)$ prime to $\deg(J)$
2. Find a, b so that $N = a\deg(I) + b\deg(J)$ is smooth
3. Compute a_1, a_2, a_3, a_4 such that $a = a_1^2 + a_2^2 + a_3^2 + a_4^2$ (same for b)
4. Write down the matrices α, β
5. Construct $K\colon E^{(4)} \times E^{(4)} \to E_I^{(4)} \times E_{\bar{J}}^{(4)}$ from Kani-square

Clapoti Summary

Input: Ideal class $[H] \in \mathrm{Cl}(\mathcal{O})$, Curve class $[E] \in \mathrm{Ell}(\mathcal{O})$

Output: $[E_H]$

1. Find $I, J \subseteq \mathcal{O}$ such that: (i) $[I] = [J] = [H]$ (ii) $\deg(I)$ prime to $\deg(J)$
2. Find a, b so that $N = a\deg(I) + b\deg(J)$ is smooth
3. Compute a_1, a_2, a_3, a_4 such that $a = a_1^2 + a_2^2 + a_3^2 + a_4^2$ (same for b)
4. Write down the matrices α, β
5. Construct $K\colon E^{(4)} \times E^{(4)} \to E_I^{(4)} \times E_{\bar{J}}^{(4)}$ from Kani-square
6. Compute K to recover equations for $E_I^{(4)} \times E_{\bar{J}}^{(4)} \rightsquigarrow$ get equation for $E_I \cong E_H$

Clapoti Summary

Input: Ideal class $[H] \in \mathrm{Cl}(\mathcal{O})$, Curve class $[E] \in \mathrm{Ell}(\mathcal{O})$

Output: $[E_H]$

1. Find $I, J \subseteq \mathcal{O}$ such that: (i) $[I] = [J] = [H]$ (ii) $\deg(I)$ prime to $\deg(J)$
2. Find a, b so that $N = a\deg(I) + b\deg(J)$ is smooth
3. Compute a_1, a_2, a_3, a_4 such that $a = a_1^2 + a_2^2 + a_3^2 + a_4^2$ (same for b)
4. Write down the matrices α, β
5. Construct $K \colon E^{(4)} \times E^{(4)} \to E_I^{(4)} \times E_{\bar{J}}^{(4)}$ from Kani-square
6. Compute K to recover equations for $E_I^{(4)} \times E_{\bar{J}}^{(4)}$ $\rightsquigarrow$ get equation for $E_I \cong E_H$
7. Return $[E_H]$

Clapoti Summary

Input: Ideal class $[H] \in \mathrm{Cl}(\mathcal{O})$, Curve class $[E] \in \mathrm{Ell}(\mathcal{O})$

Output: $[E_H]$

1. Find $I, J \subseteq \mathcal{O}$ such that: (i) $[I] = [J] = [H]$ (ii) $\deg(I)$ prime to $\deg(J)$
2. Find a, b so that $N = a \deg(I) + b \deg(J)$ is smooth
3. Compute a_1, a_2, a_3, a_4 such that $a = a_1^2 + a_2^2 + a_3^2 + a_4^2$ (same for b)
4. Write down the matrices α, β
5. Construct $K \colon E^{(4)} \times E^{(4)} \to E_I^{(4)} \times E_{\bar{J}}^{(4)}$ from Kani-square
6. Compute K to recover equations for $E_I^{(4)} \times E_{\bar{J}}^{(4)} \rightsquigarrow$ get equation for $E_I \cong E_H$
7. Return $[E_H]$

Fact Polynomial time in $|\mathrm{Cl}(\mathcal{O})|$, no pre-computation!

Comparison of dimensions

Method		Dimension
Direct evaluation	Only if $\deg(I)$ is smooth	1
Use endomorphisms of E	$K = E \times E \to E_I \times E_{\overline{J}}$	2
Use endomorphisms of E^2	$K = E^2 \times E^2 \to E_I^2 \times E_{\overline{J}}^2$	4
Use endomorphisms of E^4	$K = E^4 \times E^4 \to E_I^4 \times E_{\overline{J}}^4$	8

$$\begin{tikzcd} E \arrow[r, "I"] & E_I \end{tikzcd}$$

$$\begin{tikzcd} E \arrow[r, "\alpha I"] \arrow[d, "\beta J"'] & E_I \arrow[d, "\beta J"] \\ E_{\overline{J}} \arrow[r, "\alpha I"'] & E \end{tikzcd}$$

$$\begin{tikzcd} E^2 \arrow[r, "\alpha I^{(2)}"] \arrow[d, "\beta J^{(2)}"'] & E_I^2 \arrow[d, "\beta J^{(2)}"] \\ E_{\overline{J}}^2 \arrow[r, "\alpha I^{(2)}"'] & E^2 \end{tikzcd}$$

$$\begin{tikzcd} E^4 \arrow[r, "\alpha I^{(4)}"] \arrow[d, "\beta J^{(4)}"'] & E_I^4 \arrow[d, "\beta J^{(4)}"] \\ E_{\overline{J}}^4 \arrow[r, "\alpha I^{(4)}"'] & E^4 \end{tikzcd}$$

Computing higher-dimensional isogenies in practice

Computing higher-dimensional isogenies in practice

Recall Factoring isogenies

$$\begin{tikzcd}
E_1 \times \cdots \times E_n \arrow[rrrr, "\varphi"] \arrow[dr, bend right, "\varphi_1"'] & & & & E'_1 \times \cdots \times E'_n \\
& A_1 \arrow[r, "\varphi_2"'] & \cdots \arrow[r, "\varphi_{m-1}"'] & A_{m-1} \arrow[ur, bend right, "\varphi_m"'] &
\end{tikzcd}$$

Computing higher-dimensional isogenies in practice

Recall Factoring isogenies

$$\begin{tikzcd}
E_1 \times \cdots \times E_n \arrow[rrrr, "\varphi"] \arrow[dr, bend right, "\varphi_1"'] & & & & E_1' \times \cdots \times E_n' \\
& A_1 \arrow[r, "\varphi_2"'] & \cdots \arrow[r, "\varphi_{m-1}"'] & A_{m-1} \arrow[ur, bend right, "\varphi_m"'] &
\end{tikzcd}$$

Mathematically Computing φ_i requires time exponential in n

Computing higher-dimensional isogenies in practice

Recall Factoring isogenies

$$\begin{tikzcd}
E_1 \times \cdots \times E_n \arrow[rrrr, "\varphi"] \arrow[dr, bend right, "\varphi_1"'] & & & & E'_1 \times \cdots \times E'_n \\
& A_1 \arrow[r, "\varphi_2"'] & \cdots \arrow[r, "\varphi_{m-1}"'] & A_{m-1} \arrow[ur, bend right, "\varphi_m"'] &
\end{tikzcd}$$

Mathematically Computing φ_i requires time exponential in n

Practically Right now, only have implementation of

$$\varphi \colon E_1 \times E_2 \to E'_1 \times E'_2 \qquad \deg(\varphi) = 2^m$$

due to [DMPR23]

Computing higher-dimensional isogenies in practice

Recall Factoring isogenies

$$\begin{tikzcd}
E_1 \times \cdots \times E_n \arrow[rrrr, "\varphi"] \arrow[dr, bend right, "\varphi_1"'] & & & & E_1' \times \cdots \times E_n' \\
& A_1 \arrow[r, "\varphi_2"'] & \cdots \arrow[r, "\varphi_{m-1}"'] & A_{m-1} \arrow[ur, bend right, "\varphi_m"'] &
\end{tikzcd}$$

Mathematically Computing φ_i requires time exponential in n

Practically Right now, only have implementation of

$$\varphi\colon E_1 \times E_2 \to E_1' \times E_2' \qquad\qquad \deg(\varphi) = 2^m$$

due to [DMPR23]

Caveat This 2d-library requires very special group structure on E

Ordinary curves with special group structure

Folklore *CM Method*

Ordinary curves with special group structure

Folklore *CM Method*

Naïve Sage implementation

$\mathbb{Z}/2^{512}\mathbb{Z} \times \mathbb{Z}/2^{512}\mathbb{Z} \subseteq E(F_q)$ in $\sim$ 30 minutes, $\left|E(F_q)\right| \sim$ 1024 bits

$\mathbb{Z}/2^{1024}\mathbb{Z} \times \mathbb{Z}/2^{1024}\mathbb{Z} \subseteq E(F_q)$ in $\sim$ 28 hours, $\left|E(F_q)\right| \sim$ 2048 bits

Ordinary curves with special group structure

Folklore *CM Method*

Naïve Sage implementation

$\mathbb{Z}/2^{512}\mathbb{Z} \times \mathbb{Z}/2^{512}\mathbb{Z} \subseteq E(F_q)$ in $\sim$ 30 minutes, $\left|E(F_q)\right| \sim$ 1024 bits

$\mathbb{Z}/2^{1024}\mathbb{Z} \times \mathbb{Z}/2^{1024}\mathbb{Z} \subseteq E(F_q)$ in $\sim$ 28 hours, $\left|E(F_q)\right| \sim$ 2048 bits

Limitation

Ordinary curves with special group structure

Folklore *CM Method*

Naïve Sage implementation

$\mathbb{Z}/2^{512}\mathbb{Z} \times \mathbb{Z}/2^{512}\mathbb{Z} \subseteq E(F_q)$ in $\sim$ 30 minutes, $\left|E(F_q)\right| \sim$ 1024 bits

$\mathbb{Z}/2^{1024}\mathbb{Z} \times \mathbb{Z}/2^{1024}\mathbb{Z} \subseteq E(F_q)$ in $\sim$ 28 hours, $\left|E(F_q)\right| \sim$ 2048 bits

Limitation

Only works for small class-groups

Best method [Sut12]

$$O\left(\left|\sqrt{\mathrm{Cl}(\mathcal{O})}\right| \log\left(\left|\sqrt{\mathrm{Cl}(\mathcal{O})}\right|\right)\right)$$

Ordinary curves with special group structure

Folklore *CM Method*

Naïve Sage implementation

$\mathbb{Z}/2^{512}\mathbb{Z} \times \mathbb{Z}/2^{512}\mathbb{Z} \subseteq E(F_q)$ in $\sim$ 30 minutes, $\left|E(F_q)\right| \sim$ 1024 bits

$\mathbb{Z}/2^{1024}\mathbb{Z} \times \mathbb{Z}/2^{1024}\mathbb{Z} \subseteq E(F_q)$ in $\sim$ 28 hours, $\left|E(F_q)\right| \sim$ 2048 bits

Limitation

Only works for small class-groups

Best method [Sut12]

$$O\left(\left|\sqrt{\mathrm{Cl}(\mathcal{O})}\right| \log\left(\left|\sqrt{\mathrm{Cl}(\mathcal{O})}\right|\right)\right)$$

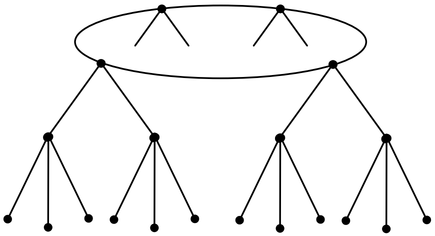
Does not scale

Ordinary curves with special group structure: Larger Class Group

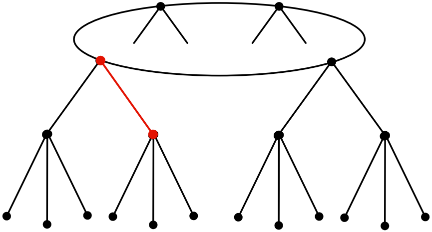
Ordinary curves with special group structure: Larger Class Group

Idea

Walk down the ℓ-isogeny volcano



Ordinary curves with special group structure: Larger Class Group



Idea

Walk down the ℓ-isogeny volcano

Start: $\mathrm{End}(E) \cong \mathcal{O}$

After n ℓ-steps: $\mathrm{End}(E_{\ell^n}) \cong \mathcal{O}_{\ell^n} \subseteq \mathcal{O}$

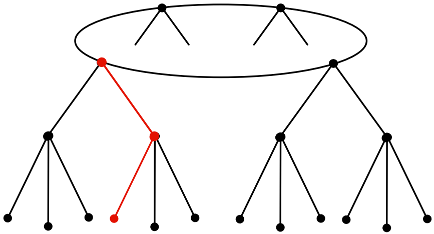
Ordinary curves with special group structure: Larger Class Group

Idea

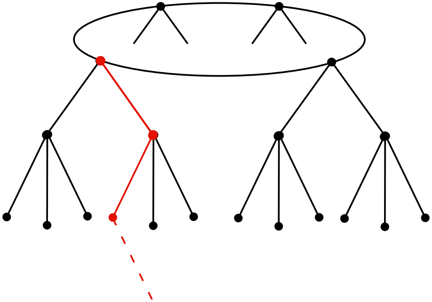
Walk down the ℓ-isogeny volcano

Start: $\mathrm{End}(E) \cong \mathcal{O}$

After n ℓ-steps: $\mathrm{End}(E_{\ell^n}) \cong \mathcal{O}_{\ell^n} \subseteq \mathcal{O}$



Ordinary curves with special group structure: Larger Class Group



Idea

Walk down the ℓ-isogeny volcano

Start: $\mathrm{End}(E) \cong \mathcal{O}$

After n ℓ-steps: $\mathrm{End}(E_{\ell^n}) \cong \mathcal{O}_{\ell^n} \subseteq \mathcal{O}$

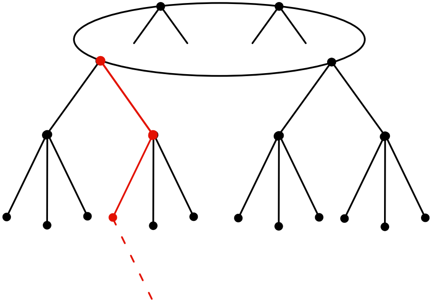
Ordinary curves with special group structure: Larger Class Group

Idea

Walk down the ℓ-isogeny volcano

Start: $\mathrm{End}(E) \cong \mathcal{O}$

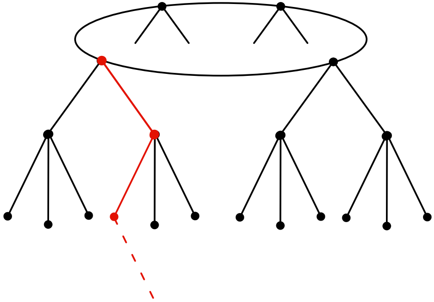
After n ℓ-steps: $\mathrm{End}(E_{\ell^n}) \cong \mathcal{O}_{\ell^n} \subseteq \mathcal{O}$



Lemma

$$|\mathrm{Cl}(\mathcal{O}_{\ell^n})| = |\mathrm{Cl}(\mathcal{O})|\, \ell^n \left(1 - \left(\left(\frac{\ell}{D}\right)\right)\frac{1}{\ell}\right) \sim \ell^n$$

Ordinary curves with special group structure: Larger Class Group



Idea

Walk down the ℓ-isogeny volcano

Start: $\mathrm{End}(E) \cong \mathcal{O}$

After n ℓ-steps: $\mathrm{End}(E_{\ell^n}) \cong \mathcal{O}_{\ell^n} \subseteq \mathcal{O}$

Lemma

$$|\mathrm{Cl}(\mathcal{O}_{\ell^n})| = |\mathrm{Cl}(\mathcal{O})|\, \ell^n \left(1 - \left(\left(\frac{\ell}{D}\right)\right) \frac{1}{\ell}\right) \sim \ell^n$$

Note This is not secure! [DDF21]

Clapoti: In two dimensions on ordinary curves

Clapoti: In two dimensions on ordinary curves

Find ordinary E using CM Method and volcano walking

Clapoti: In two dimensions on ordinary curves

Find ordinary E using CM Method and volcano walking

Input: Ideal class $[H] \in \mathrm{Cl}(\mathcal{O})$, Curve class $[E] \in \mathrm{Ell}(\mathcal{O})$

Output: $[E_H]$

Clapoti: In two dimensions on ordinary curves

Find ordinary E using CM Method and volcano walking

Input: Ideal class $[H] \in \mathrm{Cl}(\mathcal{O})$, Curve class $[E] \in \mathrm{Ell}(\mathcal{O})$

Output: $[E_H]$

1. Find $I, J \subseteq \mathcal{O}$ such that

Clapoti: In two dimensions on ordinary curves

Find ordinary E using CM Method and volcano walking

Input: Ideal class $[H] \in \mathrm{Cl}(\mathcal{O})$, Curve class $[E] \in \mathrm{Ell}(\mathcal{O})$

Output: $[E_H]$

1. Find $I, J \subseteq \mathcal{O}$ such that
   (i) $[I] = [J] = [H]$

Clapoti: In two dimensions on ordinary curves

Find ordinary E using CM Method and volcano walking

Input: Ideal class $[H] \in \mathrm{Cl}(\mathcal{O})$, Curve class $[E] \in \mathrm{Ell}(\mathcal{O})$

Output: $[E_H]$

1. Find $I, J \subseteq \mathcal{O}$ such that
   - (i) $[I] = [J] = [H]$
   - (ii) $\deg(I)$ prime to $\deg(J) = \deg(\overline{J})$

Clapoti: In two dimensions on ordinary curves

Find ordinary E using CM Method and volcano walking

Input: Ideal class $[H] \in \mathrm{Cl}(\mathcal{O})$, Curve class $[E] \in \mathrm{Ell}(\mathcal{O})$

Output: $[E_H]$

1. Find $I, J \subseteq \mathcal{O}$ such that
   (i) $[I] = [J] = [H]$
   (ii) $\deg(I)$ prime to $\deg(J) = \deg(\overline{J})$
   (iii) there exist endomorphisms $\alpha, \beta \in \mathcal{O}$ so that
   $$\deg(\alpha)\deg(I) + \deg(\beta)\deg(J) = N = 2^n$$

Clapoti: In two dimensions on ordinary curves

Find ordinary E using CM Method and volcano walking

Input: Ideal class $[H] \in \mathrm{Cl}(\mathcal{O})$, Curve class $[E] \in \mathrm{Ell}(\mathcal{O})$

Output: $[E_H]$

1. Find $I, J \subseteq \mathcal{O}$ such that
   - (i) $[I] = [J] = [H]$
   - (ii) $\deg(I)$ prime to $\deg(J) = \deg(\overline{J})$
   - (iii) there exist endomorphisms $\alpha, \beta \in \mathcal{O}$ so that
$$\deg(\alpha)\deg(I) + \deg(\beta)\deg(J) = N = 2^n$$
2. Compute kernel of K. Depends on $\alpha, \beta, I\overline{J}$

Clapoti: In two dimensions on ordinary curves

Find ordinary E using CM Method and volcano walking

Input: Ideal class $[H] \in \mathrm{Cl}(\mathcal{O})$, Curve class $[E] \in \mathrm{Ell}(\mathcal{O})$

Output: $[E_H]$

1. Find $I, J \subseteq \mathcal{O}$ such that
   (i) $[I] = [J] = [H]$
   (ii) $\deg(I)$ prime to $\deg(J) = \deg(\overline{J})$
   (iii) there exist endomorphisms $\alpha, \beta \in \mathcal{O}$ so that

$$\deg(\alpha)\deg(I) + \deg(\beta)\deg(J) = N = 2^n$$

2. Compute kernel of K. Depends on $\alpha, \beta, I\overline{J}$
3. Pass $\ker(K)$ to the 2d-library [DMPR23] to obtain an equation for E_I

Clapoti: In two dimensions on ordinary curves

Find ordinary E using CM Method and volcano walking

Input: Ideal class $[H] \in \mathrm{Cl}(\mathcal{O})$, Curve class $[E] \in \mathrm{Ell}(\mathcal{O})$

Output: $[E_H]$

1. Find $I, J \subseteq \mathcal{O}$ such that
   - (i) $[I] = [J] = [H]$
   - (ii) $\deg(I)$ prime to $\deg(J) = \deg(\overline{J})$
   - (iii) there exist endomorphisms $\alpha, \beta \in \mathcal{O}$ so that

$$N = \deg(\alpha)\deg(I) + \deg(\beta)\deg(J) = 2^n$$

2. Compute kernel of Kani-map K. Depends on $\alpha, \beta, I\overline{J}$
3. Pass $\ker(K)$ to the 2d-library [DMPR23] to obtain an equation for E_I

Solving degree equations

1.(iii) Finding endomorphisms $\alpha, \beta \in \mathcal{O}$ so that

$$N = \deg(\alpha)\deg(I) + \deg(\beta)\deg(J) = 2^n$$

Solving degree equations

1.(iii) Finding endomorphisms $\alpha, \beta \in \mathcal{O}$ so that

$$N = \deg(\alpha)\deg(I) + \deg(\beta)\deg(J) = 2^n$$

Lemma $\alpha = x + y\sigma \in \mathcal{O} = \mathbb{Z} + \sigma\mathbb{Z}$

$$\deg(\alpha) = x^2 + A_\sigma xy + B_\sigma y^2 \qquad A_\sigma, B_\sigma \in \mathbb{Z} \qquad A_\sigma, B_\sigma \sim \sqrt{|\mathrm{Cl}(\mathcal{O})|}$$

Solving degree equations

1.(iii) Finding endomorphisms $\alpha, \beta \in \mathcal{O}$ so that

$$N = \deg(\alpha)\deg(I) + \deg(\beta)\deg(J) = 2^n$$

Lemma $\alpha = x + y\sigma \in \mathcal{O} = \mathbb{Z} + \sigma\mathbb{Z}$

$$\deg(\alpha) = x^2 + A_\sigma xy + B_\sigma y^2 \qquad A_\sigma, B_\sigma \in \mathbb{Z} \qquad A_\sigma, B_\sigma \sim \sqrt{|\mathrm{Cl}(\mathcal{O})|}$$

Case $(y = 0)$ we can only obtain squares

Solving degree equations

1.(iii) Finding endomorphisms $\alpha, \beta \in \mathcal{O}$ so that

$$N = \deg(\alpha)\deg(I) + \deg(\beta)\deg(J) = 2^n$$

Lemma $\alpha = x + y\sigma \in \mathcal{O} = \mathbb{Z} + \sigma\mathbb{Z}$

$$\deg(\alpha) = x^2 + A_\sigma xy + B_\sigma y^2 \qquad A_\sigma, B_\sigma \in \mathbb{Z} \qquad A_\sigma, B_\sigma \sim \sqrt{|\mathrm{Cl}(\mathcal{O})|}$$

Case $(y = 0)$ we can only obtain squares

Case $(y \neq 0)$ numbers represented by $\deg(\alpha)$ explode with $|\mathrm{Cl}(\mathcal{O})|$

Calling the 2-dimensional isogeny library

$$\begin{tikzcd}
E_1 \times \cdots \times E_n \arrow[rrrr, "\varphi"] \arrow[dr, bend right, "\varphi_1"'] & & & & E'_1 \times \cdots \times E'_n \\
& E''_1 \times \cdots E''_n \arrow[r, "\varphi_2"'] & \cdots \arrow[r, "\varphi_{m-1}"'] & A_{m-1} \arrow[ur, bend right, "\varphi_m"'] &
\end{tikzcd}$$

Conclusion

It appears efficient isogeny class-group evaluation on ordinary elliptic curves is infeasible with current technology

Conclusion

It appears efficient isogeny class-group evaluation on ordinary elliptic curves is infeasible with current technology

Nevertheless ...

Conclusion

It appears efficient isogeny class-group evaluation on ordinary elliptic curves is infeasible with current technology

Nevertheless ...

Implementations

(i) CM Method

(ii) Ideals of endomorphism rings + rudimentary class group computation $\sim 2^{13}$

(iii) Finding matching endomorphisms $\sim 2^{10}$

(iv) Translation from endomorphisms to isogenies

(v) Computing the Kani-kernel

Outlook

Outlook

Curve finding

Difficult problem

Removing the requirement of special group structure

Pair finding

More precise lattice sampling techniques (α in $\mathbb{Z} + \sigma\mathbb{Z}$)

Better 2-dimensional heuristics a la SQISign-2D-West [BDDF$^+$24]

Higher-dimensional isogenies

Higher higher-dimensional isogeny-libraries

Thank you!

References

[PR23] *Introducing Clapoti(s): Evaluating the isogeny class group action in polynomial time*. Aurel Page and Damien Robert (2023). From eprint.iacr.org/2023/1766.

[DFM19] *Threshold Schemes from Isogeny Assumptions*. Luca De Feo and Michael Meyer (2019). From eprint.iacr.org/2019/1288.pdf.

[DFG18] *SeaSign: Compact isogeny signatures from class group actions*. Luca De Feo and Steven D. Galbraith (2018). From eprint.iacr.org/2018/824.

[BKV19] *CSI-FiSh: Efficient Isogeny based Signatures through Class Group Computations*. Ward Beullens, Thorsten Kleinjung, and Frederik Vercauteren (2019). From eprint.iacr.org/2019/498.

[CLM⁺18] *CSIDH: An Efficient Post-Quantum Commutative Group Action*. Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes (2018). From eprint.iacr.org/2018/383.

References

[DdSGOPS18] *Semi-Commutative Masking: A Framework for Isogeny-based Protocols, with an Application to Fully Secure Two-Round Isogeny-based OT.* Cyprien Delpech de Saint Guilhem, Emmanuela Orsini, Christophe Petit, and Nigel P. Smart (2018). From eprint.iacr.org/2018/648.pdf.

[DdSGP23] *New proof systems and an OPRF from CSIDH*. Cyprien Delpech de Saint Guilhem and Robi Pederson (2023). From https://eprint.iacr.org/2023/1614.pdf.

[DFFK$^+$23] *SCALLOP: scaling the CSI-FiSh*. Luca De Feo, Tako Boris Fouotsa, Péter Kutas, Antonin Leroux, Simon-Philipp Merz, Lorenz Panny, and Benjamin Wesolowski (2023). From eprint.iacr.org/2023/058.

[CLP23] *SCALLOP-HD: group action from 2-dimensional isogenies*. Mingjie Chen, Antonin Leroux, and Lorenz Panny (2023). From eprint.iacr.org/2023/1488.

References

[GPSV18] *Quantum Equivalence of the DLP and CDHP for Group Actions*. Steven Galbraith, Lorenz Panny, Benjamin Smith, and Frederik Vercauteren (2018). From eprint.iacr.org/2018/1199.

[MZ22] *Full Quantum Equivalence of Group Action DLog and CDH, and More.* Hart Montgomery and Mark Zhandry (2022). From eprint.iacr.org/2022/1135.

[GLM24] *A Simpler and More Efficient Reduction of DLog to CDH for Abelian Group Actions*. Steven Galbraith, Yi-Fu Lai, and Hart Montgomery (2024). From eprint.iacr.org/2024/191.

[DDF21] *On the security of OSIDH*. Pierrick Dartois and Luca De Feo (2021). From eprint.iacr.org/2021/1681.

[Sut12] *Accelerating the CM method.* Andrew Sutherland (2012). From arxiv.org/pdf/1009.1082.

References

[DMPR23] *An Algorithmic Approach to* $(2,2)$*-isogenies in the Theta Model and Applications to Isogeny-based Cryptography*. Pierrick Dartois, Luciano Maino, Giacomo Pope, and Damien Robert (2023). From eprint.iacr.org/2023/1747.

[DFKS18] *Towards practical key exchange from ordinary isogeny graphs*. Luca De Feo, Jean Kieffer, and Benjamin Smith (2018). From eprint.iacr.org/2018/485.

[GHS01] *Extending the GHS Weil descent attack*. Steven G. Galbraith, Florian Hess, and Nigel P. Smart (2001). From eprint.iacr.org/2001/054.

[CJS10] *Constructing elliptic curve isogenies in quantum subexponential time*. Andrew M. Childs, David Jao, and Vladimir Soukharev (2010). From arxiv.org/abs/1012.4019. The original version is from December 2010. In April 2018 there was a revision.

References

[ADFMP20] *Cryptographic Group Actions and Applications*. Navid Alamati, Luca De Feo, Hart Montgomery, and Sikhar Patranabis (2020). From eprint.iacr.org/2020/1188.

[Cou97] *Hard Homogeneous Spaces*. Jean-Marc Couveignes (1997). From eprint.iacr.org/2006/291.

[RS06] *Public-key Cryptosystem Based on Isogenies*. Alexander Rostovstev and Anton Stolbunov (2006). From eprint.iacr.org/2006/145.

[BDDF$^+$24] *SQIsign2D-West: The Fast, the Small, and the Safer*. Andrea Basso, Pierrick Dartois, Luca De Feo, Antonin Leroux, Luciano Maino, Giacomo Pope, Damien Robert, and Benjamin Wesolowski (2024). From eprint.iacr.org/2024/760.

[Kup10] *A subexponential-time quantum algorithm for the dihedral hidden subgroup problem*. Greg Kuperberg (2010). From arxiv.org/abs/quant-ph/0302112.