Workshop on the Mathematics of Post-Quantum Cryptography
6th of June 2025

On Cryptographic Group Actions from Isogenies

Ryan Rueger
IBM Research Zurich & Technical University of Munich

Cryptographic Group Actions

Cryptographic Group Actions

(Unrestricted) Cryptographic Group Action

Efficiently Compute gx for all $g \in G$ and $x \in X$

Hard To recover g from (x, gx)

Cryptographic Group Actions

(Unrestricted) Cryptographic Group Action

Efficiently Compute gx for all $g \in G$ and $x \in X$

Hard To recover g from (x, gx)

Restricted Cryptographic Group Action

Efficiently Compute gx for polynomially many $g \in G$ and for all $x \in X$

Hard To recover g from (x, gx)

Cryptographic Group Actions

(Unrestricted) Cryptographic Group Action

Efficiently Compute gx for all $g \in G$ and $x \in X$

Hard To recover g from (x, gx)

Restricted Cryptographic Group Action

Efficiently Compute gx for polynomially many $g \in G$ and for all $x \in X$

Hard To recover g from (x, gx)

(Commutative) Cryptographic Group actions are a powerful construction

Can build many cryptographic primitives

- NIKE, (Threshold) Signatures, SSP-OT, PRF, ...

Elliptic curves

Elliptic curves

Curves

Groups

Elliptic curves

Curves

Base field $k = \mathbb{F}_q$

$E = \left\{(x, y) \in k^{\mathrm{al}} : y^2 = x^3 + ax + b\right\}$

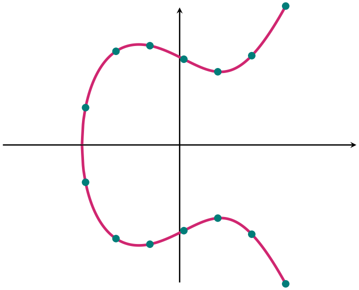
Groups

Elliptic curves

Curves

Base field $k = \mathbb{F}_q$

$$E = \left\{(x, y) \in k^{\text{al}} : y^2 = x^3 + ax + b\right\}$$



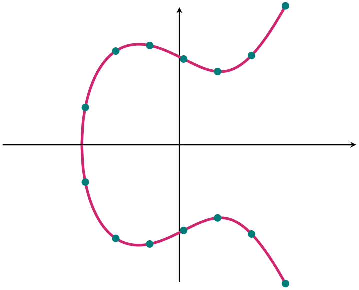
Groups

Elliptic curves

Curves

Base field $k = \mathbb{F}_q$

$E = \left\{(x, y) \in k^{\mathrm{al}} : y^2 = x^3 + ax + b\right\}$



$E(L) = \{(x, y) \in E \mid x, y \in L\}$

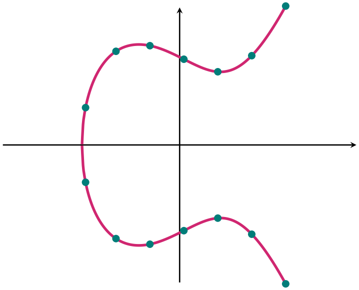
Groups

Elliptic curves

Curves

Base field $k = \mathbb{F}_q$

$$E = \left\{(x, y) \in k^{\mathrm{al}} : y^2 = x^3 + ax + b\right\} \cup \{\mathcal{O}\}$$



$$E(L) = \{(x, y) \in E \mid x, y \in L\}$$

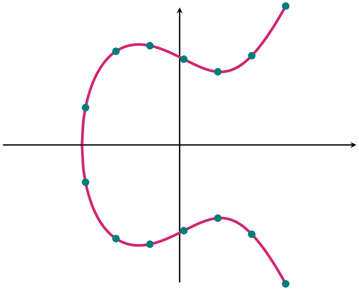
Groups

Elliptic curves

Curves

Base field $k = \mathbb{F}_q$

$$E = \left\{(x,y) \in k^{\mathrm{al}} : y^2 = x^3 + ax + b\right\} \cup \{\mathcal{O}\}$$



$$E(L) = \{(x,y) \in E \mid x,y \in L\}$$

Groups

$$P = (P_x, P_y), Q = (Q_x, Q_y) \in E$$

When $P_x \neq Q_x$

$$(P+Q)_x = \left(\frac{Q_y - P_y}{Q_x - P_x}\right)^2 - P_x - Q_x$$

$$(P+Q)_y = \left(\frac{Q_y - P_y}{Q_x - P_x}\right)(P_x - (P+Q)_x) - P_y$$

When $P_x = Q_x, P_y = Q_y \neq 0$

$$(P+Q)_x = \left(\frac{3P_x^2 + a}{2P_y}\right)^2 - 2P_x$$

$$(P+Q)_y = \left(\frac{3P_x^2 + a}{2P_y}\right)(P_x - (P+Q)_x) - P_y$$

When $P_x = Q_x, P_y = -Q_y$

$$P + Q = \mathcal{O}$$

Isogenies

Isogenies

Morphism of Curves

$$\varphi : E \to E' \quad (x, y) \mapsto \left(\frac{\varphi_1(x,y)}{\varphi_2(x,y)}, \frac{\varphi_3(x,y)}{\varphi_4(x,y)} \right)$$

Isogenies

Morphism of Curves

$$\varphi : E \to E' \quad (x, y) \mapsto \left(\frac{\varphi_1(x, y)}{\varphi_2(x, y)}, \frac{\varphi_3(x, y)}{\varphi_4(x, y)} \right)$$

Morphism of Groups

$$\varphi(P + Q) = \varphi(P) + \varphi(Q)$$
$$\varphi(\mathcal{O}_E) = \mathcal{O}_{E'}$$

Isogenies

Morphism of Curves

$$\varphi : E \to E' \quad (x, y) \mapsto \left(\frac{\varphi_1(x,y)}{\varphi_2(x,y)}, \frac{\varphi_3(x,y)}{\varphi_4(x,y)} \right)$$

Morphism of Groups

$$\varphi(P + Q) = \varphi(P) + \varphi(Q)$$
$$\varphi(\mathcal{O}_E) = \mathcal{O}_{E'}$$

Example Scalar multiplication $E \to E; P \mapsto nP = P + P + \cdots + P$

Isogenies

Morphism of Curves

$$\varphi : E \to E' \quad (x,y) \mapsto \left(\frac{\varphi_1(x,y)}{\varphi_2(x,y)}, \frac{\varphi_3(x,y)}{\varphi_4(x,y)}\right)$$

Morphism of Groups

$$\varphi(P+Q) = \varphi(P) + \varphi(Q)$$

$$\varphi(\mathcal{O}_E) = \mathcal{O}_{E'}$$

Example Scalar multiplication $E \to E; P \mapsto nP = P + P + \cdots + P$

First isomorphism theorem

$$\{G \subseteq E \text{ finite}\} \leftrightsquigarrow \{\text{nonzero isogenies } E \to *\}$$

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

$$\ker(\varphi) \leftarrow\!\shortmid \varphi$$

Isogenies

Morphism of Curves

$$\varphi : E \to E' \quad (x,y) \mapsto \left(\frac{\varphi_1(x,y)}{\varphi_2(x,y)}, \frac{\varphi_3(x,y)}{\varphi_4(x,y)}\right)$$

Morphism of Groups

$$\varphi(P+Q) = \varphi(P) + \varphi(Q)$$
$$\varphi(\mathcal{O}_E) = \mathcal{O}_{E'}$$

Example Scalar multiplication $E \to E; P \mapsto nP = P + P + \cdots + P$

First isomorphism theorem

$$\{G \subseteq E \text{ finite}\} \leftrightsquigarrow \{\text{nonzero isogenies } E \to *\}$$
$$G \mapsto \varphi_G \text{ with } \ker(\varphi_G) = G$$
$$\ker(\varphi) \leftarrow\!\shortmid \varphi$$

Because nonzero isogenies $E \to E'$ are surjective, we write $E' = E/\ker(\varphi)$

Isogeny Problem

Given two isogenous elliptic curves, find an isogeny between them

Cryptography from Isogenies

Isogeny Problem

Given two isogenous elliptic curves, find an isogeny between them

Common isogeny regime

$$\begin{tikzcd}
E_0 \arrow[rr, "\varphi"] & & E \\
\text{Public Parameter} \arrow[u, dashed] & \text{Secret Key} \arrow[u, dashed] & \text{Public Key} \arrow[u, dashed]
\end{tikzcd}$$

Motivating a group action: key exchange

Motivating a group action: key exchange

Alice and Bob pick finite subgroups $A, B \subseteq E_0$

Motivating a group action: key exchange

Alice and Bob pick finite subgroups $A, B \subseteq E_0$

$$\begin{tikzcd} E_0 \arrow[r, "\varphi_A"] \arrow[d, "\varphi_B"'] & E_A = E_0/A \\ E_B = E_0/B & \end{tikzcd}$$

Motivating a group action: key exchange

Alice and Bob pick finite subgroups $A, B \subseteq E_0$

$$\begin{tikzcd}
E_0 \arrow[r, "\varphi_A"] \arrow[d, "\varphi_B"'] & E_A = E_0/A \arrow[d, rightsquigarrow, "???"', "\varphi_{B'}"] \\
E_B = E_0/B \arrow[r, rightsquigarrow, "???", "\varphi_{A'}"'] & E_S
\end{tikzcd}$$

Motivating a group action: key exchange

Alice and Bob pick finite subgroups $A, B \subseteq E_0$

$$\begin{tikzcd} E_0 \arrow[r, "\varphi_A"] \arrow[d, "\varphi_B"'] & E_A = E_0/A \arrow[d, squiggly, "???"', "\varphi_{B'}"] \\ E_B = E_0/B \arrow[r, squiggly, "???", "\varphi_{A'}"'] & E_S \end{tikzcd}$$

Problem How can Bob encode his secret subgroup in Alice's Public Key?

Motivating a group action: key exchange

Alice and Bob pick finite subgroups $A, B \subseteq E_0$

$$\begin{tikzcd} E_0 \arrow[r, "\varphi_A"] \arrow[d, "\varphi_B"'] & E_A = E_0/A \arrow[d, squiggly, "???"', "\varphi_{B'}"] \\ E_B = E_0/B \arrow[r, squiggly, "???", "\varphi_{A'}"'] & E_S \end{tikzcd}$$

Problem How can Bob encode his secret subgroup in Alice's Public Key?

Attempt 1 Alice gives Bob some hints

Motivating a group action: key exchange

Alice and Bob pick finite subgroups $A, B \subseteq E_0$

$$\begin{tikzcd}
E_0 \arrow[r, "\varphi_A"] \arrow[d, "\varphi_B"'] & E_A = E_0/A \arrow[d, rightsquigarrow, "???"', "\varphi_{B'}"] \\
E_B = E_0/B \arrow[r, rightsquigarrow, "???", "\varphi_{A'}"'] & E_S
\end{tikzcd}$$

Problem How can Bob encode his secret subgroup in Alice's Public Key?

Attempt 1 Alice gives Bob some hints

Attempt 2 Global Atlas: Restrict to special subgroups

Motivating a group action: key exchange

Alice and Bob pick finite subgroups $A, B \subseteq E_0$

$$\begin{tikzcd}
E_0 \arrow[r, "\varphi_A"] \arrow[d, "\varphi_B"'] & E_A = E_0/A \arrow[d, squiggly, "???"', "\varphi_{B'}"] \\
E_B = E_0/B \arrow[r, squiggly, "???", "\varphi_{A'}"'] & E_S
\end{tikzcd}$$

Problem How can Bob encode his secret subgroup in Alice's Public Key?

Attempt 1 *Torsion point information* (SIKE, Polynomial time classical attack)

Attempt 2 *Orientations* (CRS, CSIDH, Subexponential Quantum Attack)

The Global Atlas: Orientations

The Global Atlas: Orientations

Consider supersingular $E/\mathbb{F}_p$

The Global Atlas: Orientations

Consider supersingular $E/\mathbb{F}_p$

Recall $E/\mathbb{F}_p$ means $E = \{(x, y) \in k^{\mathrm{al}} : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$ with $a, b \in \mathbb{F}_p$

The Global Atlas: Orientations

Consider supersingular $E/\mathbb{F}_p$

Recall $E/\mathbb{F}_p$ means $E = \{(x, y) \in k^{\mathrm{al}} : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$ with $a, b \in \mathbb{F}_p$

Fact (*Frobenius Endomorphism*) $\pi : E \to E; (x, y) \mapsto (x^p, y^p)$ is an isogeny

The Global Atlas: Orientations

Consider supersingular $E/\mathbb{F}_p$

Recall $E/\mathbb{F}_p$ means $E = \{(x, y) \in k^{\mathrm{al}} : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$ with $a, b \in \mathbb{F}_p$

Fact (*Frobenius Endomorphism*) $\pi : E \to E; (x, y) \mapsto (x^p, y^p)$ is an isogeny

Fact π generates an imaginary quadratic order $\mathbb{Z}[\pi] = \mathbb{Z} + \pi\mathbb{Z} \subseteq \mathrm{End}(E)$

The Global Atlas: Orientations

Consider supersingular $E/\mathbb{F}_p$

Recall $E/\mathbb{F}_p$ means $E = \{(x, y) \in k^{\mathrm{al}} : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$ with $a, b \in \mathbb{F}_p$

Fact (*Frobenius Endomorphism*) $\pi : E \to E; (x, y) \mapsto (x^p, y^p)$ is an isogeny

Fact π generates an imaginary quadratic order $\mathbb{Z}[\pi] = \mathbb{Z} + \pi\mathbb{Z} \subseteq \mathrm{End}(E)$

Insight Independent of the curve!

The Global Atlas: Orientations

Consider supersingular $E/\mathbb{F}_p$

Recall $E/\mathbb{F}_p$ means $E = \{(x, y) \in k^{\text{al}} : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$ with $a, b \in \mathbb{F}_p$

Fact (*Frobenius Endomorphism*) $\pi : E \to E; (x, y) \mapsto (x^p, y^p)$ is an isogeny

Fact π generates an imaginary quadratic order $\mathbb{Z}[\pi] = \mathbb{Z} + \pi\mathbb{Z} \subseteq \text{End}(E)$

Insight Independent of the curve!

Idea Alice and Bob pick secret data from $\mathbb{Z}[\pi]$

The Global Atlas: How to embed information from $\mathbb{Z}[\pi]$

The Global Atlas: How to embed information from $\mathbb{Z}[\pi]$

Alice picks an ideal $I_A \subseteq \mathbb{Z}[\pi]$

The Global Atlas: How to embed information from $\mathbb{Z}[\pi]$

Alice picks an ideal $I_A \subseteq \mathbb{Z}[\pi]$

Fact Every ideal is of the form $I_A = \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z}$

The Global Atlas: How to embed information from $\mathbb{Z}[\pi]$

Alice picks an ideal $I_A \subseteq \mathbb{Z}[\pi]$

Fact Every ideal is of the form $I_A = \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z}$

Given E, she computes

$$A = \bigcap_{\sigma \in I_A} \ker(\sigma : E \to E) = \ker(\alpha_1 : E \to E) \cap \ker(\alpha_1 : E \to E)$$

The Global Atlas: How to embed information from $\mathbb{Z}[\pi]$

Alice picks an ideal $I_A \subseteq \mathbb{Z}[\pi]$

Fact Every ideal is of the form $I_A = \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z}$

Given E, she computes

$$A = \bigcap_{\sigma \in I_A} \ker(\sigma : E \to E) = \ker(\alpha_1 : E \to E) \cap \ker(\alpha_1 : E \to E)$$

Conclusion

We can turn ideals $I_A \subseteq \mathbb{Z}[\pi]$ into isogenies $\varphi_A : E \to E_A$ starting on any curve E

...in particular we can use I_A to go from E to E_A by computing φ_A

The Global Atlas: The Class Group

The Global Atlas: The Class Group

Fact Principal ideals induce endomorphisms $E \to E$

$$I_A = \alpha_1 \mathbb{Z}[\pi] \quad \rightsquigarrow \quad A = \ker(\varphi_A) = \ker(\alpha_1) \quad \rightsquigarrow \quad \varphi_A = \alpha_1 : E \to E = E_A$$

The Global Atlas: The Class Group

Fact Principal ideals induce endomorphisms $E \to E$

$$I_A = \alpha_1 \mathbb{Z}[\pi] \quad \rightsquigarrow \quad A = \ker(\varphi_A) = \ker(\alpha_1) \quad \rightsquigarrow \quad \varphi_A = \alpha_1 : E \to E = E_A$$

Fact I, J ideals, then $E \xrightarrow{\varphi_I} E_I \xrightarrow{\varphi_J} E_{IJ}$ is the same as $E \xrightarrow{\varphi_{IJ}} E_{IJ}$

The Global Atlas: The Class Group

Fact Principal ideals induce endomorphisms $E \to E$

$$I_A = \alpha_1 \mathbb{Z}[\pi] \quad \rightsquigarrow \quad A = \ker(\varphi_A) = \ker(\alpha_1) \quad \rightsquigarrow \quad \varphi_A = \alpha_1 : E \to E = E_A$$

Fact I, J ideals, then $E \xrightarrow{\varphi_I} E_I \xrightarrow{\varphi_J} E_{IJ}$ is the same as $E \xrightarrow{\varphi_{IJ}} E_{IJ}$

Want to form the quotient

$$Q = {}^{\{\text{ideals } I \subseteq \mathbb{Z}[\pi]\}}\Big/_{\{\text{principal ideals } \alpha\mathbb{Z}[\pi] \subseteq \mathbb{Z}[\pi]\}}$$

The Global Atlas: The Class Group

Fact Principal ideals induce endomorphisms $E \to E$

$$I_A = \alpha_1 \mathbb{Z}[\pi] \quad \rightsquigarrow \quad A = \ker(\varphi_A) = \ker(\alpha_1) \quad \rightsquigarrow \quad \varphi_A = \alpha_1 : E \to E = E_A$$

Fact I, J ideals, then $E \xrightarrow{\varphi_I} E_I \xrightarrow{\varphi_J} E_{IJ}$ is the same as $E \xrightarrow{\varphi_{IJ}} E_{IJ}$

Want to form the quotient

$$Q = {}^{\{\text{ideals } I \subseteq \mathbb{Z}[\pi]\}}\big/_{\{\text{principal ideals } \alpha\mathbb{Z}[\pi] \subseteq \mathbb{Z}[\pi]\}}$$

Turns out

- $I \subseteq \mathbb{Z}[\pi]$ ideal then $I\bar{I} = \mathrm{N}(I)\mathbb{Z}[\pi]$ principal
- Q is a multiplicative group, where $\bar{I}$ is the inverse of I
- Q is the Ideal Class Group $\mathrm{Cl}(\mathbb{Z}[\pi])$

The Global Atlas: The Class Group

Fact Principal ideals induce endomorphisms $E \to E$

$$I_A = \alpha_1 \mathbb{Z}[\pi] \quad \rightsquigarrow \quad A = \ker(\varphi_A) = \ker(\alpha_1) \quad \rightsquigarrow \quad \varphi_A = \alpha_1 : E \to E = E_A$$

Fact I, J ideals, then $E \xrightarrow{\varphi_I} E_I \xrightarrow{\varphi_J} E_{IJ}$ is the same as $E \xrightarrow{\varphi_{IJ}} E_{IJ}$

Want to form the quotient

$$Q = {\{\text{ideals } I \subseteq \mathbb{Z}[\pi]\}} \big/ {\{\text{principal ideals } \alpha\mathbb{Z}[\pi] \subseteq \mathbb{Z}[\pi]\}}$$

Turns out

- $I \subseteq \mathbb{Z}[\pi]$ ideal then $I\bar{I} = \mathrm{N}(I)\mathbb{Z}[\pi]$ principal
- Q is a multiplicative group, where $\bar{I}$ is the inverse of I
- Q is the Ideal Class Group $\mathrm{Cl}(\mathbb{Z}[\pi])$

Theorem

$\mathrm{Cl}(\mathbb{Z}[\pi])$ acts regularly on all supersingular elliptic curves defined over $\mathbb{F}_p$

CSIDH: The restricted action

CSIDH: The restricted action

Suppose we want to act by some element $[I]$ in the Ideal Class Group

CSIDH: The restricted action

Suppose we want to act by some element $[\mathcal{I}]$ in the Ideal Class Group

Cost of CSIDH

If $\mathrm{N}(\mathcal{I}) = \prod p_i^{e_i}$ the cost of evaluation is $\widetilde{\Theta}\left(\sum e_i p_i\right)$

CSIDH: The restricted action

Suppose we want to act by some element $[I]$ in the Ideal Class Group

Cost of CSIDH

If $\mathrm{N}(I) = \prod p_i^{e_i}$ the cost of evaluation is $\tilde{\Theta}\left(\sum e_i p_i\right)$

Problem

Try to use 2-dim lattice reduction to find equivalent ideal $[J] = [I]$

...finds J with $\sqrt{p} \approx \mathrm{N}(J) \leq \mathrm{N}(I)$

...this does not help with smoothness

CSIDH: The restricted action

Suppose we want to act by some element $[\mathcal{I}]$ in the Ideal Class Group

Cost of CSIDH

If $\mathrm{N}(\mathcal{I}) = \prod p_i^{e_i}$ the cost of evaluation is $\tilde{\Theta}\left(\sum e_i p_i\right)$

Problem

Try to use 2-dim lattice reduction to find equivalent ideal $[J] = [\mathcal{I}]$

...finds J with $\sqrt{p} \approx \mathrm{N}(J) \leq \mathrm{N}(\mathcal{I})$

...this does not help with smoothness

Solution of CSIDH

Only act by ideals with smooth norm!

These can be decomposed as the action of many small-normed ideals

CSIDH: The restricted action

Suppose we want to act by some element $[\mathcal{I}]$ in the Ideal Class Group

Cost of CSIDH

If $\mathrm{N}(\mathcal{I}) = \prod p_i^{e_i}$ the cost of evaluation is $\tilde{\Theta}\left(\sum e_i p_i\right)$

Problem

Try to use 2-dim lattice reduction to find equivalent ideal $[J] = [\mathcal{I}]$

...finds J with $\sqrt{p} \approx \mathrm{N}(J) \leq \mathrm{N}(\mathcal{I})$

...this does not help with smoothness

Solution of CSIDH

Only act by ideals with smooth norm!

These can be decomposed as the action of many small-normed ideals

Result Practically and asymptotically efficient restricted action

PEGASIS: Unrestricting using Higher-Dimensions

PEGASIS: Practical Effective 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 (To appear at Crypto'25)

First post-quantum commutative unrestricted cryptographic group action that is both asymptotically and practically efficient

Main ingredient: Clapoti

Main ingredient: Clapoti

Theorem (Page-Robert, 2023)

Main ingredient: Clapoti

Theorem (Page-Robert, 2023)

Given

$[I] = [J]$ equivalent ideals, $\quad u = u_1^2 + u_2^2 + \cdots + u_g^2, \quad v = v_1^2 + v_2^2 + \cdots + v_g^2$

Main ingredient: Clapoti

Theorem (Page-Robert, 2023)

Given

$$[\mathcal{I}] = [\mathcal{J}] \text{ equivalent ideals}, \quad u = u_1^2 + u_2^2 + \cdots + u_g^2, \quad v = v_1^2 + v_2^2 + \cdots + v_g^2$$

Let

$$d = u\mathrm{N}(\mathcal{I}) + v\mathrm{N}(\mathcal{J}) = \prod p_i^{e_i} \quad \text{and} \quad k \text{ minimal so } E[d] \subseteq E(\mathbb{F}_{p^k})$$

Main ingredient: Clapoti

Theorem (Page-Robert, 2023)

Given

$$[I] = [J] \text{ equivalent ideals}, \quad u = u_1^2 + u_2^2 + \cdots + u_g^2, \quad v = v_1^2 + v_2^2 + \cdots + v_g^2$$

Let

$$d = u\mathrm{N}(I) + v\mathrm{N}(J) = \prod p_i^{e_i} \quad \text{and} \quad k \text{ minimal so } E[d] \subseteq E(\mathbb{F}_{p^k})$$

There exists an algorithm which computes $\varphi_I : E \to E_I$ in time

$$\tilde{\Theta}\left(k \sum e_i p_i^{2g}\right)$$

Main ingredient: Clapoti

Theorem (Page-Robert, 2023)

Given

$$[I] = [J] \text{ equivalent ideals}, \quad u = u_1^2 + u_2^2 + \cdots + u_g^2, \quad v = v_1^2 + v_2^2 + \cdots + v_g^2$$

Let

$$d = u\mathrm{N}(I) + v\mathrm{N}(J) = \prod p_i^{e_i} \quad \text{and} \quad k \text{ minimal so } E[d] \subseteq E(\mathbb{F}_{p^k})$$

There exists an algorithm which computes $\varphi_I : E \to E_I$ in time

$$\tilde{\Theta}\left(k \sum e_i p_i^{2g}\right)$$

Important Tool for construction isogenies in dimension $2g$

Main ingredient: Clapoti

Theorem (Page-Robert, 2023)

Given

$$[I] = [J] \text{ equivalent ideals}, \quad u = u_1^2 + u_2^2 + \cdots + u_g^2, \quad v = v_1^2 + v_2^2 + \cdots + v_g^2$$

Let

$$d = u\mathrm{N}(I) + v\mathrm{N}(J) = \prod p_i^{e_i} \quad \text{and} \quad k \text{ minimal so } E[d] \subseteq E(\mathbb{F}_{p^k})$$

There exists an algorithm which computes $\varphi_I : E \to E_I$ in time

$$\tilde{\Theta}\left(k \sum e_i p_i^{2g}\right)$$

Important Tool for construction isogenies in dimension $2g$

Goal d as smooth as possible, k as small as possible, g as small as possible

Main ingredient: Clapoti

Theorem (Page-Robert, 2023)

Given

$$[I] = [J] \text{ equivalent ideals}, \quad u = u_1^2 + u_2^2 + \cdots + u_g^2, \quad v = v_1^2 + v_2^2 + \cdots + v_g^2$$

Let

$$d = u\mathrm{N}(I) + v\mathrm{N}(J) = \prod p_i^{e_i} \quad \text{and} \quad k \text{ minimal so } E[d] \subseteq E(\mathbb{F}_{p^k})$$

There exists an algorithm which computes $\varphi_I : E \to E_I$ in time

$$\tilde{\Theta}\left(k \sum e_i p_i^{2g}\right)$$

Important Tool for construction isogenies in dimension $2g$

Goal d as smooth as possible, k as small as possible, g as small as possible

In practice Want $d = 2^n, k = 2, g \leq 2$

Conflicting requirements

$d = 2^n$ (Target solution of $u\mathrm{N}(I) + v\mathrm{N}(J) = d$)

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

...but Minkowski's bound only gives us $[J] = [I]$ with $\mathrm{N}(J) \approx \sqrt{p}$

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

Conflicting requirements

$d = 2^n$ (Target solution of $u\mathrm{N}(I) + v\mathrm{N}(J) = d$)

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

...but Minkowski's bound only gives us $[J] = [I]$ with $\mathrm{N}(J) \approx \sqrt{p}$

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

Conflicting requirements

$d = 2^n$ (Target solution of $u\mathrm{N}(I) + v\mathrm{N}(J) = d$)

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

...but Minkowski's bound only gives us $[J] = [I]$ with $\mathrm{N}(J) \approx \sqrt{p}$

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

$k = 2$ (Extension degree we want for $E[d] \subseteq E(\mathbb{F}_{p^k})$)

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

Conflicting requirements

$d = 2^n$ (Target solution of $u\mathrm{N}(I) + v\mathrm{N}(J) = d$)

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

...but Minkowski's bound only gives us $[J] = [I]$ with $\mathrm{N}(J) \approx \sqrt{p}$

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

$k = 2$ (Extension degree we want for $E[d] \subseteq E(\mathbb{F}_{p^k})$)

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

Core Problem

Even the smallest equivalent ideals are too big

...but not by much

Resolving the tension

Resolving the tension

Idea

Resolving the tension

Idea

Factor ideal into smooth-normed and rough-normed part $I = I_s I_r, J = J_s J_r$

The smooth parts can be computed like in CSIDH

Resolving the tension

Idea

Factor ideal into smooth-normed and rough-normed part $I = I_s I_r, J = J_s J_r$

The smooth parts can be computed like in CSIDH

Problem The ideals I_r, J_r are no longer equivalent

...but they almost are $[\overline{I_r} J_r] = [I_s \overline{J_s}]$ (not trivial, but easy to evaluate)

Resolving the tension

Idea

Factor ideal into smooth-normed and rough-normed part $I = I_s I_r, J = J_s J_r$

The smooth parts can be computed like in CSIDH

Problem The ideals I_r, J_r are no longer equivalent

...but they almost are $[\overline{I_r} J_r] = [I_s \overline{J_s}]$ (not trivial, but easy to evaluate)

Tweak Page-Robert's algorithm

Search for $u, v \geq 0$ such that $d = u\mathrm{N}(I_r) + v\mathrm{N}(J_r) = 2^n$

...works because $\mathrm{N}(I_r), \mathrm{N}(J_r)$ is small enough

Resolving the tension

Idea

Factor ideal into smooth-normed and rough-normed part $I = I_s I_r, J = J_s J_r$

The smooth parts can be computed like in CSIDH

Problem The ideals I_r, J_r are no longer equivalent

...but they almost are $[\overline{I_r} J_r] = [I_s \overline{J_s}]$ (not trivial, but easy to evaluate)

Tweak Page-Robert's algorithm

Search for $u, v \geq 0$ such that $d = u\mathrm{N}(I_r) + v\mathrm{N}(J_r) = 2^n$

...works because $\mathrm{N}(I_r), \mathrm{N}(J_r)$ is small enough

In fact So many solutions u, v that we can find $u = u_1^2 + u_2^2, v = v_1^2 + v_2^2$

...algorithm only needs $(2g = 4)$-dimensional isogeny computation

In fact Using x-only arithmetic, we get away with $k = 1$

Implementation Results

		Lang.	128	256	375	512	1024
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/mathsofpqc25

Ask me anything (I have bonus slides!)

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

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

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

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

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

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

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

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

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

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

Requirements

1. $f \le v_2(p+1) - 3$
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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Requirements

1. $f \leq v_2(p+1) - 3$ 2. $u\mathrm{N}(\mathfrak{b}), v\mathrm{N}(\mathfrak{c})$ coprime 3. $u = \deg_{\mathrm{p}}(\varphi_u), v = \deg_{\mathrm{p}}(\varphi_v)$

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

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

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

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

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

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

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

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

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

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

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

Requirements

1. $f \leq v_2(p+1) - 3$ 2. $u\mathrm{N}(\mathfrak{b}), v\mathrm{N}(\mathfrak{c})$ coprime 3. $u = \deg_{\mathrm{p}}(\varphi_u), v = \deg_{\mathrm{p}}(\varphi_v)$

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 $2^e \,||\, p+1$ 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 $T_{\text{desc}}, T_{\text{horiz},1}, T_{\text{horiz},2}$ points of 2-torsion

Lemma

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

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

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

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