MaGIC Workshop on Group Actions in Cryptography, Borgo Lanciano, 7th of May 2026

CORAL
Faster Isogeny Group Action For Post-Quantum NIKE

Joint with Andrea Basso, Giacomo Borin, and Sina Schaeffler

Ryan Rueger
IBM Research Zurich & Technical University of Munich

Recall

Recall

Slogan Class-groups act on elliptic curves (a.k.a *Complex Multiplication*)

Recall

Slogan Class-groups act on elliptic curves (a.k.a *Complex Multiplication*)

Elliptic Curves

Not important in this talk

Recall

Slogan Class-groups act on elliptic curves (a.k.a *Complex Multiplication*)

Elliptic Curves

Not important in this talk

Class-groups

Recall

Slogan Class-groups act on elliptic curves (a.k.a *Complex Multiplication*)

Elliptic Curves

Not important in this talk

Class-groups

Let $K = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic number field ($d > 0$ squarefree)

Recall

Slogan Class-groups act on elliptic curves (a.k.a *Complex Multiplication*)

Elliptic Curves

Not important in this talk

Class-groups

Let $K = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic number field ($d > 0$ squarefree)

Let $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$ be an order of K (Think $\mathcal{O} = \mathcal{O}_K$ ring of integers if you like)

Recall

Slogan Class-groups act on elliptic curves (a.k.a *Complex Multiplication*)

Elliptic Curves

Not important in this talk

Class-groups

Let $K = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic number field ($d > 0$ squarefree)

Let $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$ be an order of K (Think $\mathcal{O} = \mathcal{O}_K$ ring of integers if you like)

We say two $\mathcal{O}$-ideals $\mathfrak{a}, \mathfrak{b}$ are equivalent $\mathfrak{a} \sim \mathfrak{b}$ if $\mathfrak{a}\overline{\mathfrak{b}}$ is principal ($\mathfrak{a}\overline{\mathfrak{b}} = \gamma\mathcal{O}$)

Recall

Slogan Class-groups act on elliptic curves (a.k.a *Complex Multiplication*)

Elliptic Curves

Not important in this talk

Class-groups

Let $K = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic number field ($d > 0$ squarefree)

Let $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$ be an order of K (Think $\mathcal{O} = \mathcal{O}_K$ ring of integers if you like)

We say two $\mathcal{O}$-ideals $\mathfrak{a}, \mathfrak{b}$ are equivalent $\mathfrak{a} \sim \mathfrak{b}$ if $\mathfrak{a}\overline{\mathfrak{b}}$ is principal ($\mathfrak{a}\overline{\mathfrak{b}} = \gamma\mathcal{O}$)

The class-group is the set of all ideals modulo equivalence

$$\mathrm{Cl}(\mathcal{O}) = \{\mathfrak{a} \subseteq \mathcal{O} \text{ ideal}\}_{/\sim}$$

Recall

Slogan Class-groups act on elliptic curves (a.k.a *Complex Multiplication*)

Elliptic Curves

Not important in this talk

Class-groups

Let $K = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic number field ($d > 0$ squarefree)

Let $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$ be an order of K (Think $\mathcal{O} = \mathcal{O}_K$ ring of integers if you like)

We say two $\mathcal{O}$-ideals $\mathfrak{a}, \mathfrak{b}$ are equivalent $\mathfrak{a} \sim \mathfrak{b}$ if $\mathfrak{a}\overline{\mathfrak{b}}$ is principal ($\mathfrak{a}\overline{\mathfrak{b}} = \gamma\mathcal{O}$)

The class-group is the set of all ideals modulo equivalence

$$\mathrm{Cl}(\mathcal{O}) = \{\mathfrak{a} \subseteq \mathcal{O} \text{ ideal}\}_{/\sim}$$

Denote class of ideal $\mathfrak{c}$ in $\mathrm{Cl}(\mathcal{O})$ by $[\mathfrak{c}]$ (*i.e.* $[\mathfrak{c}] = [\mathfrak{d}] \iff \mathfrak{c} \sim \mathfrak{d} \iff \mathfrak{c}\overline{\mathfrak{d}}$ is principal)

Recall

Slogan Class-groups act on elliptic curves (a.k.a *Complex Multiplication*)

Elliptic Curves

Not important in this talk

Class-groups

Let $K = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic number field ($d > 0$ squarefree)

Let $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$ be an order of K (Think $\mathcal{O} = \mathcal{O}_K$ ring of integers if you like)

We say two $\mathcal{O}$-ideals $\mathfrak{a}, \mathfrak{b}$ are equivalent $\mathfrak{a} \sim \mathfrak{b}$ if $\mathfrak{a}\overline{\mathfrak{b}}$ is principal ($\mathfrak{a}\overline{\mathfrak{b}} = \gamma\mathcal{O}$)

The class-group is the set of all ideals modulo equivalence

$$\mathrm{Cl}(\mathcal{O}) = \{\mathfrak{a} \subseteq \mathcal{O} \text{ ideal}\}_{/\sim}$$

Denote class of ideal $\mathfrak{c}$ in $\mathrm{Cl}(\mathcal{O})$ by $[\mathfrak{c}]$ (*i.e.* $[\mathfrak{c}] = [\mathfrak{d}] \iff \mathfrak{c} \sim \mathfrak{d} \iff \mathfrak{c}\overline{\mathfrak{d}}$ is principal)

Cryptography

Recall

Slogan Class-groups act on elliptic curves (a.k.a *Complex Multiplication*)

Elliptic Curves

Not important in this talk

Class-groups

Let $K = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic number field ($d > 0$ squarefree)

Let $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$ be an order of K (Think $\mathcal{O} = \mathcal{O}_K$ ring of integers if you like)

We say two $\mathcal{O}$-ideals $\mathfrak{a}, \mathfrak{b}$ are equivalent $\mathfrak{a} \sim \mathfrak{b}$ if $\mathfrak{a}\overline{\mathfrak{b}}$ is principal ($\mathfrak{a}\overline{\mathfrak{b}} = \gamma\mathcal{O}$)

The class-group is the set of all ideals modulo equivalence

$$\mathrm{Cl}(\mathcal{O}) = \{\mathfrak{a} \subseteq \mathcal{O} \text{ ideal}\}_{/\sim}$$

Denote class of ideal $\mathfrak{c}$ in $\mathrm{Cl}(\mathcal{O})$ by $[\mathfrak{c}]$ (*i.e.* $[\mathfrak{c}] = [\mathfrak{d}] \iff \mathfrak{c} \sim \mathfrak{d} \iff \mathfrak{c}\overline{\mathfrak{d}}$ is principal)

Cryptography

Classical Security (128 bits) Need $\Delta_{\mathcal{O}} = f^2 d \geq 2^{512}$ (For Meet-In-The-Middle)

Recall

Slogan Class-groups act on elliptic curves (a.k.a *Complex Multiplication*)

Elliptic Curves

Not important in this talk

Class-groups

Let $K = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic number field ($d > 0$ squarefree)

Let $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$ be an order of K (Think $\mathcal{O} = \mathcal{O}_K$ ring of integers if you like)

We say two $\mathcal{O}$-ideals $\mathfrak{a}, \mathfrak{b}$ are equivalent $\mathfrak{a} \sim \mathfrak{b}$ if $\mathfrak{a}\overline{\mathfrak{b}}$ is principal ($\mathfrak{a}\overline{\mathfrak{b}} = \gamma\mathcal{O}$)

The class-group is the set of all ideals modulo equivalence

$$\mathrm{Cl}(\mathcal{O}) = \{\mathfrak{a} \subseteq \mathcal{O} \text{ ideal}\}_{/\sim}$$

Denote class of ideal $\mathfrak{c}$ in $\mathrm{Cl}(\mathcal{O})$ by $[\mathfrak{c}]$ (*i.e.* $[\mathfrak{c}] = [\mathfrak{d}] \iff \mathfrak{c} \sim \mathfrak{d} \iff \mathfrak{c}\overline{\mathfrak{d}}$ is principal)

Cryptography

Classical Security (128 bits) Need $\Delta_{\mathcal{O}} = f^2 d \geq 2^{512}$ (For Meet-In-The-Middle)

Quantum Security (NIST 1) Need $\Delta_{\mathcal{O}} = f^2 d \geq 2^{???}$ (For Kuperberg)

Recall

Slogan Class-groups act on elliptic curves (a.k.a *Complex Multiplication*)

Elliptic Curves

Not important in this talk

Class-groups

Let $K = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic number field ($d > 0$ squarefree)

Let $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$ be an order of K (Think $\mathcal{O} = \mathcal{O}_K$ ring of integers if you like)

We say two $\mathcal{O}$-ideals $\mathfrak{a}, \mathfrak{b}$ are equivalent $\mathfrak{a} \sim \mathfrak{b}$ if $\mathfrak{a}\overline{\mathfrak{b}}$ is principal ($\mathfrak{a}\overline{\mathfrak{b}} = \gamma\mathcal{O}$)

The class-group is the set of all ideals modulo equivalence

$$\mathrm{Cl}(\mathcal{O}) = \{\mathfrak{a} \subseteq \mathcal{O} \text{ ideal}\}_{/\sim}$$

Denote class of ideal $\mathfrak{c}$ in $\mathrm{Cl}(\mathcal{O})$ by $[\mathfrak{c}]$ (*i.e.* $[\mathfrak{c}] = [\mathfrak{d}] \iff \mathfrak{c} \sim \mathfrak{d} \iff \mathfrak{c}\overline{\mathfrak{d}}$ is principal)

Cryptography

Classical Security (128 bits) Need $\Delta_{\mathcal{O}} = f^2 d \geq 2^{512}$ (For Meet-In-The-Middle)

Quantum Security (NIST 1) Need $\Delta_{\mathcal{O}} = f^2 d \geq 2^{???}$ (For Kuperberg)

Notoriously difficult to estimate

Recall

Slogan Class-groups act on elliptic curves (a.k.a *Complex Multiplication*)

Elliptic Curves

Not important in this talk

Class-groups

Let $K = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic number field ($d > 0$ squarefree)

Let $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$ be an order of K (Think $\mathcal{O} = \mathcal{O}_K$ ring of integers if you like)

We say two $\mathcal{O}$-ideals $\mathfrak{a}, \mathfrak{b}$ are equivalent $\mathfrak{a} \sim \mathfrak{b}$ if $\mathfrak{a}\bar{\mathfrak{b}}$ is principal ($\mathfrak{a}\bar{\mathfrak{b}} = \gamma\mathcal{O}$)

The class-group is the set of all ideals modulo equivalence

$$\mathrm{Cl}(\mathcal{O}) = \{\mathfrak{a} \subseteq \mathcal{O} \text{ ideal}\}_{/\sim}$$

Denote class of ideal $\mathfrak{c}$ in $\mathrm{Cl}(\mathcal{O})$ by $[\mathfrak{c}]$ (*i.e.* $[\mathfrak{c}] = [\mathfrak{d}] \iff \mathfrak{c} \sim \mathfrak{d} \iff \mathfrak{c}\bar{\mathfrak{d}}$ is principal)

Cryptography

Classical Security (128 bits) Need $\Delta_\mathcal{O} = f^2 d \geq 2^{512}$ (For Meet-In-The-Middle)

Quantum Security (NIST 1) Need $\Delta_\mathcal{O} = f^2 d \geq 2^{???}$ (For Kuperberg)

Notoriously difficult to estimate

Summary: $\Delta_\mathcal{O} \approx 2^{512}$ 🪦 $\Delta_\mathcal{O} \approx 2^{1024}$ 😟 $\Delta_\mathcal{O} \approx 2^{2048}$ 😊 $\Delta_\mathcal{O} \approx 2^{4096}$ 🤩 (Very Scientific!!1!)

Unrestricted Isogeny Class-Group Actions

Unrestricted Isogeny Class-Group Actions

Recall

Evaluating the action of $[\mathfrak{c}] \in \mathrm{Cl}(\mathcal{O})$ requires computing an isogeny of degree $\mathrm{N}(\mathfrak{c})$

Unrestricted Isogeny Class-Group Actions

Recall

Evaluating the action of $[\mathfrak{c}] \in \mathrm{Cl}(\mathcal{O})$ requires computing an isogeny of degree $\mathrm{N}(\mathfrak{c})$

Evaluating isogenies of non-smooth degree is difficult (cannot break into small chunks)

Unrestricted Isogeny Class-Group Actions

Recall

Evaluating the action of $[\mathfrak{c}] \in \mathrm{Cl}(\mathcal{O})$ requires computing an isogeny of degree $\mathrm{N}(\mathfrak{c})$

Evaluating isogenies of non-smooth degree is difficult (cannot break into small chunks)

Need to find "good representative" of the class $[\mathfrak{c}]$ we want to evaluate

Unrestricted Isogeny Class-Group Actions

Recall

Evaluating the action of $[\mathfrak{c}] \in \mathrm{Cl}(\mathcal{O})$ requires computing an isogeny of degree $\mathrm{N}(\mathfrak{c})$

Evaluating isogenies of non-smooth degree is difficult (cannot break into small chunks)

Need to find "good representative" of the class $[\mathfrak{c}]$ we want to evaluate

Solutions Evaluate the action of a given class $[\mathfrak{c}]$ by...

Unrestricted Isogeny Class-Group Actions

Recall

Evaluating the action of $[\mathfrak{c}] \in \mathrm{Cl}(\mathcal{O})$ requires computing an isogeny of degree $\mathrm{N}(\mathfrak{c})$

Evaluating isogenies of non-smooth degree is difficult (cannot break into small chunks)

Need to find "good representative" of the class $[\mathfrak{c}]$ we want to evaluate

Solutions Evaluate the action of a given class $[\mathfrak{c}]$ by...

CSI-FiSH (Dimension 1)

Find equivalent ideal $\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n} \sim \mathfrak{c}$ of smooth norm

Requires computing the structure $\mathrm{Cl}(\mathcal{O}) \cong \mathbb{Z}^n/\Lambda$ (Superpolynomial: Limited to $\Delta_{\mathcal{O}} \approx 2^{500}$ 🪦)

Unrestricted Isogeny Class-Group Actions

Recall

Evaluating the action of $[\mathfrak{c}] \in \mathrm{Cl}(\mathcal{O})$ requires computing an isogeny of degree $\mathrm{N}(\mathfrak{c})$

Evaluating isogenies of non-smooth degree is difficult (cannot break into small chunks)

Need to find "good representative" of the class $[\mathfrak{c}]$ we want to evaluate

Solutions Evaluate the action of a given class $[\mathfrak{c}]$ by...

CSI-FiSH (Dimension 1)

Find equivalent ideal $\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n} \sim \mathfrak{c}$ of smooth norm

Requires computing the structure $\mathrm{Cl}(\mathcal{O}) \cong \mathbb{Z}^n/\Lambda$ (Superpolynomial: Limited to $\Delta_{\mathcal{O}} \approx 2^{500}$ 🪦)

KLaPoTi (Dimension 2)

Unrestricted Isogeny Class-Group Actions

Recall

Evaluating the action of $[\mathfrak{c}] \in \mathrm{Cl}(\mathcal{O})$ requires computing an isogeny of degree $\mathrm{N}(\mathfrak{c})$

Evaluating isogenies of non-smooth degree is difficult (cannot break into small chunks)

Need to find "good representative" of the class $[\mathfrak{c}]$ we want to evaluate

Solutions Evaluate the action of a given class $[\mathfrak{c}]$ by...

CSI-FiSH (Dimension 1)

Find equivalent ideal $\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n} \sim \mathfrak{c}$ of smooth norm

Requires computing the structure $\mathrm{Cl}(\mathcal{O}) \cong \mathbb{Z}^n/\Lambda$ (Superpolynomial: Limited to $\Delta_\mathcal{O} \approx 2^{500}$ 🪦)

KLaPoTi (Dimension 2)

Find equivalent $\mathfrak{a}, \mathfrak{b} \sim \mathfrak{c}$ such that $\mathrm{N}(\mathfrak{a}) + \mathrm{N}(\mathfrak{b}) = 2^e$

Requires $e \approx \log(\Delta_\mathcal{O})^3$ (Expensive arithmetic, cannot use Frobenius-orientation, can have $\Delta_\mathcal{O} \approx 2^{4096}$ 😍)

Unrestricted Isogeny Class-Group Actions

Recall

Evaluating the action of $[\mathfrak{c}] \in \mathrm{Cl}(\mathcal{O})$ requires computing an isogeny of degree $\mathrm{N}(\mathfrak{c})$

Evaluating isogenies of non-smooth degree is difficult (cannot break into small chunks)

Need to find "good representative" of the class $[\mathfrak{c}]$ we want to evaluate

Solutions Evaluate the action of a given class $[\mathfrak{c}]$ by...

CSI-FiSH (Dimension 1)

Find equivalent ideal $\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n} \sim \mathfrak{c}$ of smooth norm

Requires computing the structure $\mathrm{Cl}(\mathcal{O}) \cong \mathbb{Z}^n/\Lambda$ (Superpolynomial: Limited to $\Delta_\mathcal{O} \approx 2^{500}$ 🪦)

KLaPoTi (Dimension 2)

Find equivalent $\mathfrak{a}, \mathfrak{b} \sim \mathfrak{c}$ such that $\mathrm{N}(\mathfrak{a}) + \mathrm{N}(\mathfrak{b}) = 2^e$

Requires $e \approx \log(\Delta_\mathcal{O})^3$ (Expensive arithmetic, cannot use Frobenius-orientation, can have $\Delta_\mathcal{O} \approx 2^{4096}$ 🤩)

qt-PEGASIS (Dimension 4)

Unrestricted Isogeny Class-Group Actions

Recall

Evaluating the action of $[\mathfrak{c}] \in \mathrm{Cl}(\mathcal{O})$ requires computing an isogeny of degree $\mathrm{N}(\mathfrak{c})$

Evaluating isogenies of non-smooth degree is difficult (cannot break into small chunks)

Need to find "good representative" of the class $[\mathfrak{c}]$ we want to evaluate

Solutions Evaluate the action of a given class $[\mathfrak{c}]$ by...

CSI-FiSH (Dimension 1)

Find equivalent ideal $\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n} \sim \mathfrak{c}$ of smooth norm

Requires computing the structure $\mathrm{Cl}(\mathcal{O}) \cong \mathbb{Z}^n/\Lambda$ (Superpolynomial: Limited to $\Delta_\mathcal{O} \approx 2^{500}$ 🪦)

KLaPoTi (Dimension 2)

Find equivalent $\mathfrak{a}, \mathfrak{b} \sim \mathfrak{c}$ such that $\mathrm{N}(\mathfrak{a}) + \mathrm{N}(\mathfrak{b}) = 2^e$

Requires $e \approx \log(\Delta_\mathcal{O})^3$ (Expensive arithmetic, cannot use Frobenius-orientation, can have $\Delta_\mathcal{O} \approx 2^{4096}$ 🤩)

qt-PEGASIS (Dimension 4)

Find equivalent $\mathfrak{a}, \mathfrak{b}, \mathfrak{d}, \mathfrak{e} \sim \mathfrak{c}$ such that $\mathrm{N}(\mathfrak{a}) + \mathrm{N}(\mathfrak{b}) + \mathrm{N}(\mathfrak{d}) + \mathrm{N}(\mathfrak{e}) = 2^e$

Requires computing isogenies in dimension 4 (Cost exponential in dimension, Can have $\Delta_\mathcal{O} \approx 2^{4096}$ 🤩)

Unrestricted Isogeny Class-Group Actions

Recall

Evaluating the action of $[\mathfrak{c}] \in \mathrm{Cl}(\mathcal{O})$ requires computing an isogeny of degree $\mathrm{N}(\mathfrak{c})$

Evaluating isogenies of non-smooth degree is difficult (cannot break into small chunks)

Need to find "good representative" of the class $[\mathfrak{c}]$ we want to evaluate

Solutions Evaluate the action of a given class $[\mathfrak{c}]$ by...

CSI-FiSH (Dimension 1)

Find equivalent ideal $\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n} \sim \mathfrak{c}$ of smooth norm

Requires computing the structure $\mathrm{Cl}(\mathcal{O}) \cong \mathbb{Z}^n/\Lambda$ (Superpolynomial: Limited to $\Delta_\mathcal{O} \approx 2^{500}$ 🪦)

KLaPoTi (Dimension 2)

Find equivalent $\mathfrak{a}, \mathfrak{b} \sim \mathfrak{c}$ such that $\mathrm{N}(\mathfrak{a}) + \mathrm{N}(\mathfrak{b}) = 2^e$

Requires $e \approx \log(\Delta_\mathcal{O})^3$ (Expensive arithmetic, cannot use Frobenius-orientation, can have $\Delta_\mathcal{O} \approx 2^{4096}$ 🤩)

qt-PEGASIS (Dimension 4)

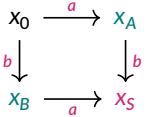
Find equivalent $\mathfrak{a}, \mathfrak{b}, \mathfrak{d}, \mathfrak{e} \sim \mathfrak{c}$ such that $\mathrm{N}(\mathfrak{a}) + \mathrm{N}(\mathfrak{b}) + \mathrm{N}(\mathfrak{d}) + \mathrm{N}(\mathfrak{e}) = 2^e$

Requires computing isogenies in dimension 4 (Cost exponential in dimension, Can have $\Delta_\mathcal{O} \approx 2^{4096}$ 🤩)

Do we need this for Key Exchange?

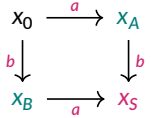
Do we need this for Key Exchange?

Recall Alice samples secret a in $\mathrm{Cl}(\mathcal{O})$, Bob samples secret b in $\mathrm{Cl}(\mathcal{O})$



Do we need this for Key Exchange?

Recall Alice samples secret a in $\mathrm{Cl}(\mathcal{O})$, Bob samples secret b in $\mathrm{Cl}(\mathcal{O})$

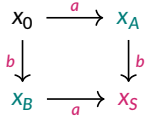


Conclusion We don't need an unrestricted action

Just need exponentially-sized key-space $\mathcal{K} \subseteq \mathrm{Cl}(\mathcal{O})$ from which we can efficiently sample

Do we need this for Key Exchange?

Recall Alice samples secret a in $\mathrm{Cl}(\mathcal{O})$, Bob samples secret b in $\mathrm{Cl}(\mathcal{O})$



Conclusion We don't need an unrestricted action

Just need exponentially-sized key-space $\mathcal{K} \subseteq \mathrm{Cl}(\mathcal{O})$ from which we can efficiently sample

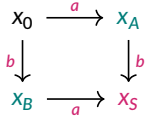
Slogan

Because they sample their own ideals, they can construct an ideal in "smooth" representation

...instead of computing a "smooth" representation of a given class

Do we need this for Key Exchange?

Recall Alice samples secret a in $\mathrm{Cl}(\mathcal{O})$, Bob samples secret b in $\mathrm{Cl}(\mathcal{O})$



Conclusion We don't need an unrestricted action

Just need exponentially-sized key-space $\mathcal{K} \subseteq \mathrm{Cl}(\mathcal{O})$ from which we can efficiently sample

Slogan

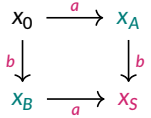
Because they sample their own ideals, they can construct an ideal in "smooth" representation

...instead of computing a "smooth" representation of a given class

Quantum Security?

Do we need this for Key Exchange?

Recall Alice samples secret a in $\mathrm{Cl}(\mathcal{O})$, Bob samples secret b in $\mathrm{Cl}(\mathcal{O})$



Conclusion We don't need an unrestricted action

Just need exponentially-sized key-space $\mathcal{K} \subseteq \mathrm{Cl}(\mathcal{O})$ from which we can efficiently sample

Slogan

Because they sample their own ideals, they can construct an ideal in "smooth" representation

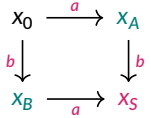
...instead of computing a "smooth" representation of a given class

Quantum Security?

Classical We need $|\mathcal{K}| \geq 2^{\lambda}$ to protect against brute-force search ($\geq 2^{2\lambda}$ if meet-in-the-middle applies)

Do we need this for Key Exchange?

Recall Alice samples secret a in $\mathrm{Cl}(\mathcal{O})$, Bob samples secret b in $\mathrm{Cl}(\mathcal{O})$



Conclusion We don't need an unrestricted action

Just need exponentially-sized key-space $\mathcal{K} \subseteq \mathrm{Cl}(\mathcal{O})$ from which we can efficiently sample

Slogan

Because they sample their own ideals, they can construct an ideal in "smooth" representation

...instead of computing a "smooth" representation of a given class

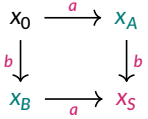
Quantum Security?

Classical We need $|\mathcal{K}| \geq 2^\lambda$ to protect against brute-force search ($\geq 2^{2\lambda}$ if meet-in-the-middle applies)

Quantum Best attacks have complexity in $L_{1/2}(\Delta_\mathcal{O})$ (Must attack the entire class group! [CSCJR22, Sec. 4])

Do we need this for Key Exchange?

Recall Alice samples secret a in $\mathrm{Cl}(\mathcal{O})$, Bob samples secret b in $\mathrm{Cl}(\mathcal{O})$



Conclusion We don't need an unrestricted action

Just need exponentially-sized key-space $\mathcal{K} \subseteq \mathrm{Cl}(\mathcal{O})$ from which we can efficiently sample

Slogan

Because they sample their own ideals, they can construct an ideal in "smooth" representation

...instead of computing a "smooth" representation of a given class

Quantum Security?

Classical We need $|\mathcal{K}| \geq 2^{\lambda}$ to protect against brute-force search ($\geq 2^{2\lambda}$ if meet-in-the-middle applies)

Quantum Best attacks have complexity in $L_{1/2}(\Delta_{\mathcal{O}})$ (Must attack the entire class group! [CSCJR22, Sec. 4])

Strategy Large Discriminant and "Small" Key-space (*e.g.* $\Delta_{\mathcal{O}} = 2^{4096}, |\mathcal{K}| = 2^{128}$)

Constructing “Smooth” Ideals

Constructing “Smooth” Ideals

CSI-FiSH (Dimension 1)

Constructing “Smooth” Ideals

CSI-FiSH (Dimension 1)

Find equivalent ideal $\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n} \sim \mathfrak{c}$ of smooth norm

Requires computing the structure $\mathrm{Cl}(\mathcal{O}) \cong \mathbb{Z}^n/\Lambda$ (Superpolynomial: Limited to $\Delta_{\mathcal{O}} \approx 2^{500}$ 🔔)

Constructing “Smooth” Ideals

CSI-FiSH (Dimension 1)

Find equivalent ideal $\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n} \sim \mathfrak{c}$ of smooth norm

Requires computing the structure $\mathrm{Cl}(\mathcal{O}) \cong \mathbb{Z}^n/\Lambda$ (Superpolynomial: Limited to $\Delta_{\mathcal{O}} \approx 2^{500}$ 🔔)

Instead...

Constructing “Smooth” Ideals

CSI-FiSH (Dimension 1)

Find equivalent ideal $\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n} \sim \mathfrak{c}$ of smooth norm

Requires computing the structure $\mathrm{Cl}(\mathcal{O}) \cong \mathbb{Z}^n/\Lambda$ (Superpolynomial: Limited to $\Delta_{\mathcal{O}} \approx 2^{500}$ 🔔)

Instead…

CSIDH (Dimension 1)

Constructing “Smooth” Ideals

CSI-FiSH (Dimension 1)

- Find equivalent ideal $\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n} \sim \mathfrak{c}$ of smooth norm
- Requires computing the structure $\mathrm{Cl}(\mathcal{O}) \cong \mathbb{Z}^n/\Lambda$ (Superpolynomial: Limited to $\Delta_\mathcal{O} \approx 2^{500}$ 🔔)

Instead...

CSIDH (Dimension 1)

- Write down $\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n}$ of smooth norm (Do not care which class)
- Requires no knowledge of the class-group (Can have $\Delta_\mathcal{O} \approx 2^{4096}$ 🤩)
- $\approx 6\times$ Faster than qt-PEGASIS

Constructing “Smooth” Ideals

CSI-FiSH (Dimension 1)

- Find equivalent ideal $\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n} \sim \mathfrak{c}$ of smooth norm
- Requires computing the structure $\mathrm{Cl}(\mathcal{O}) \cong \mathbb{Z}^n/\Lambda$ (Superpolynomial: Limited to $\Delta_\mathcal{O} \approx 2^{500}$ 🪦)

Instead...

CSIDH (Dimension 1)

- Write down $\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n}$ of smooth norm (Do not care which class)
- Requires no knowledge of the class-group (Can have $\Delta_\mathcal{O} \approx 2^{4096}$ 🤩)
- $\approx 6\times$ Faster than qt-PEGASIS

Idea Combine CSIDH and qt-PEGASIS in protocols

Constructing “Smooth” Ideals

CSI-FiSH (Dimension 1)

Find equivalent ideal $\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n} \sim \mathfrak{c}$ of smooth norm

Requires computing the structure $\mathrm{Cl}(\mathcal{O}) \cong \mathbb{Z}^n/\Lambda$ (Superpolynomial: Limited to $\Delta_\mathcal{O} \approx 2^{500}$ 🪦)

Instead...

CSIDH (Dimension 1)

Write down $\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n}$ of smooth norm (Do not care which class)

Requires no knowledge of the class-group (Can have $\Delta_\mathcal{O} \approx 2^{4096}$ 🤩)

$\approx 6\times$ Faster than qt-PEGASIS

Idea Combine CSIDH and qt-PEGASIS in protocols

When Alice can evaluate the action of a self-sampled group element: use CSIDH

Constructing “Smooth” Ideals

CSI-FiSH (Dimension 1)

- Find equivalent ideal $\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n} \sim \mathfrak{c}$ of smooth norm
- Requires computing the structure $\mathrm{Cl}(\mathcal{O}) \cong \mathbb{Z}^n/\Lambda$ (Superpolynomial: Limited to $\Delta_\mathcal{O} \approx 2^{500}$ 🪦)

Instead...

CSIDH (Dimension 1)

- Write down $\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n}$ of smooth norm (Do not care which class)
- Requires no knowledge of the class-group (Can have $\Delta_\mathcal{O} \approx 2^{4096}$ 🤩)
- $\approx 6\times$ Faster than qt-PEGASIS

Idea Combine CSIDH and qt-PEGASIS in protocols

- When Alice can evaluate the action of a self-sampled group element: use CSIDH
- When Alice must evaluate the action a specific element: use qt-PEGASIS

Constructing “Smooth” Ideals

CSI-FiSH (Dimension 1)

- Find equivalent ideal $\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n} \sim \mathfrak{c}$ of smooth norm
- Requires computing the structure $\mathrm{Cl}(\mathcal{O}) \cong \mathbb{Z}^n/\Lambda$ (Superpolynomial: Limited to $\Delta_\mathcal{O} \approx 2^{500}$ 🪦)

Instead...

CSIDH (Dimension 1)

- Write down $\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n}$ of smooth norm (Do not care which class)
- Requires no knowledge of the class-group (Can have $\Delta_\mathcal{O} \approx 2^{4096}$ 🤩)
- $\approx 6\times$ Faster than qt-PEGASIS

Idea Combine CSIDH and qt-PEGASIS in protocols

- When Alice can evaluate the action of a self-sampled group element: use CSIDH
- When Alice must evaluate the action a specific element: use qt-PEGASIS

Problem

- Base prime characteristic for CSIDH must shape $p + 1 = \ell_1 \cdots \ell_n$
- Base prime characteristic for qt-PEGASIS must shape $p + 1 = c2^f$

Constructing “Smooth” Ideals

Constructing “Smooth” Ideals

KLaPoTi (Dimension 2)

Find equivalent $\mathfrak{a} \sim \mathfrak{b} \sim \mathfrak{c}$ such that $\mathrm{N}(\mathfrak{a}) + \mathrm{N}(\mathfrak{b}) = 2^e$

Requires $e \approx \log(\Delta_{\mathcal{O}})^3$ (Expensive arithmetic, cannot use Frobenius-orientation)

Constructing “Smooth” Ideals

KLaPoTi (Dimension 2)

Find equivalent $\mathfrak{a} \sim \mathfrak{b} \sim \mathfrak{c}$ such that $N(\mathfrak{a}) + N(\mathfrak{b}) = 2^e$

Requires $e \approx \log(\Delta_{\mathcal{O}})^3$ (Expensive arithmetic, cannot use Frobenius-orientation)

Instead…

Constructing “Smooth” Ideals

KLaPoTi (Dimension 2)

Find equivalent $\mathfrak{a} \sim \mathfrak{b} \sim \mathfrak{c}$ such that $\mathrm{N}(\mathfrak{a}) + \mathrm{N}(\mathfrak{b}) = 2^e$

Requires $e \approx \log(\Delta_{\mathcal{O}})^3$ (Expensive arithmetic, cannot use Frobenius-orientation)

Instead…

CORAL (Dimension 2)

Constructing “Smooth” Ideals

KLaPoTi (Dimension 2)

Find equivalent $\mathfrak{a} \sim \mathfrak{b} \sim \mathfrak{c}$ such that $\mathrm{N}(\mathfrak{a}) + \mathrm{N}(\mathfrak{b}) = 2^e$

Requires $e \approx \log(\Delta_{\mathcal{O}})^3$ (Expensive arithmetic, cannot use Frobenius-orientation)

Instead…

CORAL (Dimension 2)

Find equivalent $\mathfrak{a} \sim \mathfrak{b}$ such that $\mathrm{N}(\mathfrak{a}) + \mathrm{N}(\mathfrak{b}) = 2^e$ (Do not care which class)

Constructing “Smooth” Ideals

KLaPoTi (Dimension 2)

Find equivalent $\mathfrak{a} \sim \mathfrak{b} \sim \mathfrak{c}$ such that $\mathrm{N}(\mathfrak{a}) + \mathrm{N}(\mathfrak{b}) = 2^e$

Requires $e \approx \log(\Delta_{\mathcal{O}})^3$ (Expensive arithmetic, cannot use Frobenius-orientation)

Instead…

CORAL (Dimension 2)

Find equivalent $\mathfrak{a} \sim \mathfrak{b}$ such that $\mathrm{N}(\mathfrak{a}) + \mathrm{N}(\mathfrak{b}) = 2^e$ (Do not care which class)

Requires $e \approx \log(\Delta_{\mathcal{O}})/2 + \lambda$ (Faster arithmetic, can use Frobenius orientation, with short HD chains)

Constructing “Smooth” Ideals

KLaPoTi (Dimension 2)

Find equivalent $\mathfrak{a} \sim \mathfrak{b} \sim \mathfrak{c}$ such that $\mathrm{N}(\mathfrak{a}) + \mathrm{N}(\mathfrak{b}) = 2^e$

Requires $e \approx \log(\Delta_{\mathcal{O}})^3$ (Expensive arithmetic, cannot use Frobenius-orientation)

Instead…

CORAL (Dimension 2)

Find equivalent $\mathfrak{a} \sim \mathfrak{b}$ such that $\mathrm{N}(\mathfrak{a}) + \mathrm{N}(\mathfrak{b}) = 2^e$ (Do not care which class)

Requires $e \approx \log(\Delta_{\mathcal{O}})/2 + \lambda$ (Faster arithmetic, can use Frobenius orientation, with short HD chains)

Can we combine CORAL and PEGASIS?

Constructing “Smooth” Ideals

KLaPoTi (Dimension 2)

Find equivalent $\mathfrak{a} \sim \mathfrak{b} \sim \mathfrak{c}$ such that $N(\mathfrak{a}) + N(\mathfrak{b}) = 2^e$

Requires $e \approx \log(\Delta_{\mathcal{O}})^3$ (Expensive arithmetic, cannot use Frobenius-orientation)

Instead...

CORAL (Dimension 2)

Find equivalent $\mathfrak{a} \sim \mathfrak{b}$ such that $N(\mathfrak{a}) + N(\mathfrak{b}) = 2^e$ (Do not care which class)

Requires $e \approx \log(\Delta_{\mathcal{O}})/2 + \lambda$ (Faster arithmetic, can use Frobenius orientation, with short HD chains)

Can we combine CORAL and PEGASIS?

Yes their base prime is the same!

The most efficient instantiation of CORAL uses exactly the same parameters as qt-PEGASIS

Sampling $\mathfrak{a} \sim \mathfrak{b}$ such that $\mathrm{N}(\mathfrak{a}) + \mathrm{N}(\mathfrak{b}) = 2^e$

Specialise to $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$ (Frobenius Orientation, Same as qt-PEGASIS)

Sampling $\mathfrak{a} \sim \mathfrak{b}$ such that $\mathrm{N}(\mathfrak{a}) + \mathrm{N}(\mathfrak{b}) = 2^e$

Specialise to $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$ (Frobenius Orientation, Same as qt-PEGASIS)

Note

When $\mathfrak{a} \sim \mathfrak{b}$ are $\mathcal{O}$-ideals with $\mathrm{N}(\mathfrak{a}) + \mathrm{N}(\mathfrak{b}) = 2^e$, then $\mathfrak{a}\overline{\mathfrak{b}} = \gamma\mathcal{O}$ with $\mathrm{N}(\gamma) = \mathrm{N}(\mathfrak{a})\mathrm{N}(\mathfrak{b}) = q(2^e - q)$

Sampling $\mathfrak{a} \sim \mathfrak{b}$ such that $\mathrm{N}(\mathfrak{a}) + \mathrm{N}(\mathfrak{b}) = 2^e$

Specialise to $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$ (Frobenius Orientation, Same as qt-PEGASIS)

Note

When $\mathfrak{a} \sim \mathfrak{b}$ are $\mathcal{O}$-ideals with $\mathrm{N}(\mathfrak{a}) + \mathrm{N}(\mathfrak{b}) = 2^e$, then $\mathfrak{a}\overline{\mathfrak{b}} = \gamma\mathcal{O}$ with $\mathrm{N}(\gamma) = \mathrm{N}(\mathfrak{a})\mathrm{N}(\mathfrak{b}) = q(2^e - q)$

Conversely When γ in $\mathcal{O}$ has norm $q(2^e - q)$, then

$$\mathfrak{a} = (q, \gamma)\mathcal{O} \quad \mathfrak{b} = (2^e - q, \overline{\gamma})\mathcal{O} \quad \text{satisfy} \quad \mathrm{N}(\mathfrak{a}) = q, \mathrm{N}(\mathfrak{b}) = 2^e - q \quad \text{so} \quad \mathrm{N}(\mathfrak{a}) + \mathrm{N}(\mathfrak{b}) = 2^e$$

Sampling $\mathfrak{a} \sim \mathfrak{b}$ such that $N(\mathfrak{a}) + N(\mathfrak{b}) = 2^e$

Specialise to $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$ (Frobenius Orientation, Same as qt-PEGASIS)

Note

When $\mathfrak{a} \sim \mathfrak{b}$ are $\mathcal{O}$-ideals with $N(\mathfrak{a}) + N(\mathfrak{b}) = 2^e$, then $\mathfrak{a}\overline{\mathfrak{b}} = \gamma\mathcal{O}$ with $N(\gamma) = N(\mathfrak{a})N(\mathfrak{b}) = q(2^e - q)$

Conversely When γ in $\mathcal{O}$ has norm $q(2^e - q)$, then

$$\mathfrak{a} = (q, \gamma)\mathcal{O} \quad \mathfrak{b} = (2^e - q, \overline{\gamma})\mathcal{O} \quad \text{satisfy} \quad N(\mathfrak{a}) = q, N(\mathfrak{b}) = 2^e - q \quad \text{so} \quad N(\mathfrak{a}) + N(\mathfrak{b}) = 2^e$$

Reduces problem of finding "good" pair $\mathfrak{a}, \mathfrak{b}$ to finding "good" γ

Sampling $\mathfrak{a} \sim \mathfrak{b}$ such that $\mathrm{N}(\mathfrak{a}) + \mathrm{N}(\mathfrak{b}) = 2^e$

Specialise to $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$ (Frobenius Orientation, Same as qt-PEGASIS)

Note

When $\mathfrak{a} \sim \mathfrak{b}$ are $\mathcal{O}$-ideals with $\mathrm{N}(\mathfrak{a}) + \mathrm{N}(\mathfrak{b}) = 2^e$, then $\mathfrak{a}\overline{\mathfrak{b}} = \gamma\mathcal{O}$ with $\mathrm{N}(\gamma) = \mathrm{N}(\mathfrak{a})\mathrm{N}(\mathfrak{b}) = q(2^e - q)$

Conversely When γ in $\mathcal{O}$ has norm $q(2^e - q)$, then

$$\mathfrak{a} = (q, \gamma)\mathcal{O} \quad \mathfrak{b} = (2^e - q, \overline{\gamma})\mathcal{O} \quad \text{satisfy} \quad \mathrm{N}(\mathfrak{a}) = q, \mathrm{N}(\mathfrak{b}) = 2^e - q \quad \text{so} \quad \mathrm{N}(\mathfrak{a}) + \mathrm{N}(\mathfrak{b}) = 2^e$$

Reduces problem of finding "good" pair $\mathfrak{a}, \mathfrak{b}$ to finding "good" γ

Note

$$\mathrm{N}(\gamma) = \mathrm{N}(x + y\sqrt{-p}) = x^2 - py^2 = q(2^e - q) = (2^{e-1} - a)(2^{e-1} + a) = 2^{2(e-1)} - a^2$$

Sampling $\mathfrak{a} \sim \mathfrak{b}$ such that $N(\mathfrak{a}) + N(\mathfrak{b}) = 2^e$

Specialise to $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$ (Frobenius Orientation, Same as qt-PEGASIS)

Note

When $\mathfrak{a} \sim \mathfrak{b}$ are $\mathcal{O}$-ideals with $N(\mathfrak{a}) + N(\mathfrak{b}) = 2^e$, then $\mathfrak{a}\overline{\mathfrak{b}} = \gamma\mathcal{O}$ with $N(\gamma) = N(\mathfrak{a})N(\mathfrak{b}) = q(2^e - q)$

Conversely When γ in $\mathcal{O}$ has norm $q(2^e - q)$, then

$$\mathfrak{a} = (q, \gamma)\mathcal{O} \quad \mathfrak{b} = (2^e - q, \overline{\gamma})\mathcal{O} \quad \text{satisfy} \quad N(\mathfrak{a}) = q, N(\mathfrak{b}) = 2^e - q \quad \text{so} \quad N(\mathfrak{a}) + N(\mathfrak{b}) = 2^e$$

Reduces problem of finding "good" pair $\mathfrak{a}, \mathfrak{b}$ to finding "good" γ

Note

$$N(\gamma) = N(x + y\sqrt{-p}) = x^2 - py^2 = q(2^e - q) = (2^{e-1} - a)(2^{e-1} + a) = 2^{2(e-1)} - a^2$$

which becomes the norm equation

$$2^{2(e-1)} - y^2 p = x^2 + a^2$$

Sampling $\mathfrak{a} \sim \mathfrak{b}$ such that $N(\mathfrak{a}) + N(\mathfrak{b}) = 2^e$

Specialise to $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$ (Frobenius Orientation, Same as qt-PEGASIS)

Note

When $\mathfrak{a} \sim \mathfrak{b}$ are $\mathcal{O}$-ideals with $N(\mathfrak{a}) + N(\mathfrak{b}) = 2^e$, then $\mathfrak{a}\overline{\mathfrak{b}} = \gamma\mathcal{O}$ with $N(\gamma) = N(\mathfrak{a})N(\mathfrak{b}) = q(2^e - q)$

Conversely When γ in $\mathcal{O}$ has norm $q(2^e - q)$, then

$$\mathfrak{a} = (q, \gamma)\mathcal{O} \quad \mathfrak{b} = (2^e - q, \overline{\gamma})\mathcal{O} \quad \text{satisfy} \quad N(\mathfrak{a}) = q, N(\mathfrak{b}) = 2^e - q \quad \text{so} \quad N(\mathfrak{a}) + N(\mathfrak{b}) = 2^e$$

Reduces problem of finding "good" pair $\mathfrak{a}, \mathfrak{b}$ to finding "good" γ

Note

$$N(\gamma) = N(x + y\sqrt{-p}) = x^2 - py^2 = q(2^e - q) = (2^{e-1} - a)(2^{e-1} + a) = 2^{2(e-1)} - a^2$$

which becomes the norm equation

$$2^{2(e-1)} - y^2 p = x^2 + a^2$$

which we can solve "efficiently" in practice (by isogeny standards)

Distribution in the Class Group

and how big does $N(a) + N(b) = 2^e$ have to be?

Distribution in the Class Group

and how big does $N(\mathfrak{a}) + N(\mathfrak{b}) = 2^e$ have to be?

Recall $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$ has $\Delta_{\mathcal{O}} = p$, so need $p \geq 2^{2048}$ for quantum security

Want Key-space of size 2^λ

Distribution in the Class Group

and how big does $N(a) + N(b) = 2^e$ have to be?

Recall $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$ has $\Delta_{\mathcal{O}} = p$, so need $p \geq 2^{2048}$ for quantum security

Want Key-space of size 2^λ

Strategy To solve $2^{2(e-1)} - y^2 p = x^2 + a^2$

Distribution in the Class Group

and how big does $N(a) + N(b) = 2^e$ have to be?

Recall $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$ has $\Delta_{\mathcal{O}} = p$, so need $p \geq 2^{2048}$ for quantum security

Want Key-space of size 2^λ

Strategy To solve $2^{2(e-1)} - y^2 p = x^2 + a^2$

Pick random y until $\mathcal{L}_y = 2^{2(e-1)} - y^2 p$ can be decomposed into sum of two squares $x^2 + a^2$

Distribution in the Class Group

and how big does $N(a) + N(b) = 2^e$ have to be?

Recall $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$ has $\Delta_{\mathcal{O}} = p$, so need $p \geq 2^{2048}$ for quantum security

Want Key-space of size 2^λ

Strategy To solve $2^{2(e-1)} - y^2 p = x^2 + a^2$

Pick random y until $\mathcal{L}_y = 2^{2(e-1)} - y^2 p$ can be decomposed into sum of two squares $x^2 + a^2$

...which is easy when $\mathcal{L}_y$ can be factored

Distribution in the Class Group

and how big does $N(\mathfrak{a}) + N(\mathfrak{b}) = 2^e$ have to be?

Recall $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$ has $\Delta_{\mathcal{O}} = p$, so need $p \geq 2^{2048}$ for quantum security

Want Key-space of size 2^λ

Strategy To solve $2^{2(e-1)} - y^2 p = x^2 + a^2$

- Pick random y until $\mathcal{L}_y = 2^{2(e-1)} - y^2 p$ can be decomposed into sum of two squares $x^2 + a^2$
- ...which is easy when $\mathcal{L}_y$ can be factored
- ...in particular when $\mathcal{L}_y$ is prime (In practice, $p \equiv 3 \pmod 4$)

Distribution in the Class Group

and how big does $N(a) + N(b) = 2^e$ have to be?

Recall $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$ has $\Delta_{\mathcal{O}} = p$, so need $p \geq 2^{2048}$ for quantum security

Want Key-space of size 2^λ

Strategy To solve $2^{2(e-1)} - y^2 p = x^2 + a^2$

- Pick random y until $\mathcal{L}_y = 2^{2(e-1)} - y^2 p$ can be decomposed into sum of two squares $x^2 + a^2$
- ...which is easy when $\mathcal{L}_y$ can be factored
- ...in particular when $\mathcal{L}_y$ is prime (In practice, $p \equiv 3 \pmod 4$)
- ...which has "probability" $1/2e$ (Prime Number Theorem)

Distribution in the Class Group

and how big does $N(a) + N(b) = 2^e$ have to be?

Recall $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$ has $\Delta_{\mathcal{O}} = p$, so need $p \geq 2^{2048}$ for quantum security

Want Key-space of size 2^λ

Strategy To solve $2^{2(e-1)} - y^2 p = x^2 + a^2$

- Pick random y until $\mathcal{L}_y = 2^{2(e-1)} - y^2 p$ can be decomposed into sum of two squares $x^2 + a^2$
- ...which is easy when $\mathcal{L}_y$ can be factored
- ...in particular when $\mathcal{L}_y$ is prime (In practice, $p \equiv 3 \pmod 4$)
- ...which has "probability" $1/2e$ (Prime Number Theorem)

Need at least 2^λ choices for y, so $2^e p^{-1/2}/2e \geq 2^\lambda$

Distribution in the Class Group

and how big does $\mathsf{N}(\mathfrak{a}) + \mathsf{N}(\mathfrak{b}) = 2^e$ have to be?

Recall $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$ has $\Delta_{\mathcal{O}} = p$, so need $p \geq 2^{2048}$ for quantum security

Want Key-space of size 2^λ

Strategy To solve $2^{2(e-1)} - y^2 p = x^2 + a^2$

- Pick random y until $\mathcal{L}_y = 2^{2(e-1)} - y^2 p$ can be decomposed into sum of two squares $x^2 + a^2$
- ...which is easy when $\mathcal{L}_y$ can be factored
- ...in particular when $\mathcal{L}_y$ is prime (In practice, $p \equiv 3 \pmod 4$)
- ...which has "probability" $1/2e$ (Prime Number Theorem)

Need at least 2^λ choices for y, so $2^e p^{-1/2}/2e \geq 2^\lambda \rightsquigarrow e \approx \log(p)/2 + \lambda + \varepsilon$

Distribution in the Class Group

and how big does $\mathsf{N}(\mathfrak{a}) + \mathsf{N}(\mathfrak{b}) = 2^e$ have to be?

Recall $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$ has $\Delta_{\mathcal{O}} = p$, so need $p \geq 2^{2048}$ for quantum security

Want Key-space of size 2^λ

Strategy To solve $2^{2(e-1)} - y^2 p = x^2 + a^2$

Pick random y until $\mathcal{L}_y = 2^{2(e-1)} - y^2 p$ can be decomposed into sum of two squares $x^2 + a^2$

...which is easy when $\mathcal{L}_y$ can be factored

...in particular when $\mathcal{L}_y$ is prime (In practice, $p \equiv 3 \pmod 4$)

...which has "probability" $1/2e$ (Prime Number Theorem)

Need at least 2^λ choices for y, so $2^e p^{-1/2}/2e \geq 2^\lambda \rightsquigarrow e \approx \log(p)/2 + \lambda + \varepsilon$

Under heuristics

1) $2^{e-1} + a$, $2^{e-1} - a$ behave like random integers

2) The events that $2^{e-1} + a$, $2^{e-1} - a$ are represented by a given class $[\mathfrak{c}]$ are independent

one can prove that the distribution of resulting classes $[(2^{e-1} - a, x + y\sqrt{-p})\mathcal{O}]$ is uniform

Distribution in the Class Group

and how big does $\mathsf{N}(\mathfrak{a}) + \mathsf{N}(\mathfrak{b}) = 2^e$ have to be?

Recall $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$ has $\Delta_{\mathcal{O}} = p$, so need $p \geq 2^{2048}$ for quantum security

Want Key-space of size 2^λ

Strategy To solve $2^{2(e-1)} - y^2 p = x^2 + a^2$

Pick random y until $\mathcal{L}_y = 2^{2(e-1)} - y^2 p$ can be decomposed into sum of two squares $x^2 + a^2$

...which is easy when $\mathcal{L}_y$ can be factored

...in particular when $\mathcal{L}_y$ is prime (In practice, $p \equiv 3 \pmod 4$)

...which has "probability" $1/2e$ (Prime Number Theorem)

Need at least 2^λ choices for y, so $2^e p^{-1/2}/2e \geq 2^\lambda \rightsquigarrow e \approx \log(p)/2 + \lambda + \varepsilon$

Under heuristics

1) $2^{e-1} + a$, $2^{e-1} - a$ behave like random integers

2) The events that $2^{e-1} + a$, $2^{e-1} - a$ are represented by a given class $[\mathfrak{c}]$ are independent

one can prove that the distribution of resulting classes $[(2^{e-1} - a, x + y\sqrt{-p})\mathcal{O}]$ is uniform

Experimental data supports both $e \approx \log(p)/2 + \lambda + \varepsilon$ and uniformity

Comparison of selected isogeny-based group-action evaluations

			Time (ms)			
			$\approx \log(\Delta_{\mathcal{O}})$			
	Name	Lang.	512	1024	2048	4096
Unrestricted	KLaPoTi [PPS25]	Rust	2 360	17 500	138 000	
	PEGASIS [DEF+25]	Sage	1 900	5 290	21 300	121 000
	qt-PEGASIS [DEIV25]	Sage	1 200	3 250	11 800	58 000
	qt-PEGASIS [DD26]	C	73.6	419	2 940	22 000
Restricted	CSIDH [CLM+18]	C/asm	26.5	529		
	SQALE [CSCJR22]	C/asm	66.7	240	1 300	7 710
	dCTIDH [CHMR25]	C/asm			400	
	CSIDH-LDO [ZLL+26]	C/AVX			408	696
	OSIDH-LD [WLLZ26]	C/AVX				754
	CORAL	C	6.99	36.5	240	1 780
	CORAL	C/asm	4.43			

Benchmarks exclusively measure the isogeny computation; excluding norm equation solving, public key compression, or public key validation where applicable. Using variants `AVX-512IFMA-8w_r7` and `AVX-512IFMA-8w8w_r13` for CSIDH-LDO2000 and CSIDH-LDO4000 respectively. The dCTIDH variant used is $m = 6, \ell = 194$. The SQALE variant used is "MCR". `asm` denotes use of assembly-optimized arithmetic. AVX denotes use of platform-specific *Advanced Vector Extensions*. Data for CORAL and CSIDH collected over 1000 samples. Data for other algorithms collected over 100 samples. All benchmarks measured with AMD Ryzen 7 PRO 7840U@3.3GHz, boost and hyperthreading disabled. Times rounded to three significant figures.

Comparison of selected post-quantum NIKEs

Scheme	Lang.	Actively secure	|pk| (B)	KeyGen (ms)	SharedKey (ms)
Swoosh [GdKQ+24]	Rust Jasmin `asm`	No‡	221184	38.2	2.53
dCTIDH2047 [CHMR25]	C/`asm`	Yes	256	3840	479†
CSIDH-LDO2000 [ZLL+26]	C/AVX	No*	320§	439	427
CORAL2032-1155	C	Yes	256	594	240
CSIDH-LDO4000 [ZLL+26]	C/AVX	No*	576§	784	761
OSIDH-LD4000 [WLLZ26]	C/AVX	No*	576§	844	754
CORAL4092-2185	C	Yes	512	5480	1 780

Using variants `AVX-512IFMA-8w_r7` and `AVX-512IFMA-8w8w_r13` for CSIDH-LDO2000 and CSIDH-LDO4000 respectively. CSIDH-LDO variants include compression (KeyGen) and decompression (SharedKey). †With improved public key validation as described in [PRR+25, Tab. 4]. *Does not include public-key validation necessary to make the protocol actively secure. At time of writing, practically efficient public-key validation is still in progress [Hou25, Sec. 7]. §Using best possible theoretical approximation $2\log(p) + \log(\mathrm{Disc}(\mathcal{O}))$ bits for public-key sizes, not implemented sizes (here $r = 7$ (resp. 13) for 2048-bit (resp. 4096-bit) discriminant). ‡Whilst the full Swoosh protocol can be made actively secure though applying proofs-of-knowledge, the current (benchmarked) implementation does not include these; nor does the reported public-key size include the additional 89 KB space required for these proofs. `asm` denotes an implementation with assembly-optimized arithmetic. Data collected from 500 key exchanges (*i.e.* 1000 KeyGen and SharedKey calls). All benchmarks measured with AMD Ryzen 7 PRO 7840U@3.3GHz, boost and hyperthreading disabled. Times rounded to three significant figures.

Applications

CORAL can be used to accelerate some group-action protocols

Recall CORAL computes same action as PEGASIS

Applications

CORAL can be used to accelerate some group-action protocols

Recall CORAL computes same action as PEGASIS

...and can be employed whenever the action of a self-sampled ideal must be

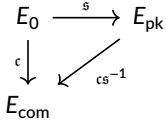
Applications

CORAL can be used to accelerate some group-action protocols

Recall CORAL computes same action as PEGASIS

...and can be employed whenever the action of a self-sampled ideal must be

Example 1-bit identification scheme (core of CSI-FiSh Signature)



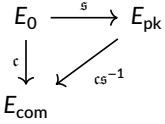
Applications

CORAL can be used to accelerate some group-action protocols

Recall CORAL computes same action as PEGASIS

...and can be employed whenever the action of a self-sampled ideal must be

Example 1-bit identification scheme (core of CSI-FiSh Signature)



Can compute both the commitment isogeny $\mathfrak{c}$ and keygen $\mathfrak{s}$ using CORAL

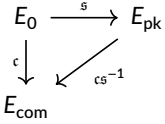
Applications

CORAL can be used to accelerate some group-action protocols

Recall CORAL computes same action as PEGASIS

...and can be employed whenever the action of a self-sampled ideal must be

Example 1-bit identification scheme (core of CSI-FiSh Signature)



Can compute both the commitment isogeny $\mathfrak{c}$ and keygen $\mathfrak{s}$ using CORAL

Can compute $\mathfrak{c}\mathfrak{s}^{-1}$ using qt-PEGASIS

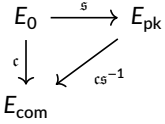
Applications

CORAL can be used to accelerate some group-action protocols

Recall CORAL computes same action as PEGASIS

...and can be employed whenever the action of a self-sampled ideal must be

Example 1-bit identification scheme (core of CSI-FiSh Signature)



Can compute both the commitment isogeny $\mathfrak{c}$ and keygen $\mathfrak{s}$ using CORAL

Can compute $\mathfrak{c}\mathfrak{s}^{-1}$ using qt-PEGASIS

Ongoing work

Can also compute 2-dim representation of $\mathfrak{c}\mathfrak{s}^{-1}$ to allow for 2-dimensional verification

Outlook

Outlook

Security

- Better understanding of distribution (In particular the implied constants in heuristics used)
- Full constant-time implementation

Outlook

Security

- Better understanding of distribution (In particular the implied constants in heuristics used)
- Full constant-time implementation

Outlook

Security

- Better understanding of distribution (In particular the implied constants in heuristics used)
- Full constant-time implementation

Implementation

- Working fully over $\mathbb{F}_p$, using more symmetric formulae [DD26]
- Integrating assembly-optimised arithmetic (or AVX-accelerations)
- Cleaner diagonal isogenies (Currently needs expensive switching of models)

Outlook

Security

- Better understanding of distribution (In particular the implied constants in heuristics used)
- Full constant-time implementation

Implementation

- Working fully over $\mathbb{F}_p$, using more symmetric formulae [DD26]
- Integrating assembly-optimised arithmetic (or AVX-accelerations)
- Cleaner diagonal isogenies (Currently needs expensive switching of models)

Applications

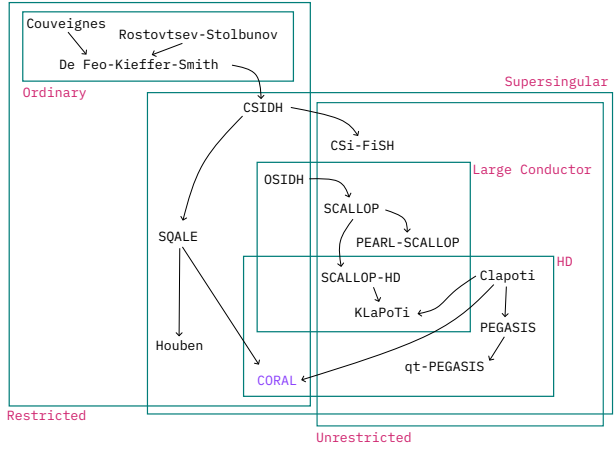
- Which protocols can we accelerate with CORAL? (*e.g.* for NIST's Threshold Call)

Thank you

CORAL to appear at Crypto'26

Paper will be on ePrint soon...

https://rueg.re/magic26



References I

[CHMR25] Fabio Campos, Andreas Hellenbrand, Michael Meyer, and Krijn Reijnders.
dCTIDH: Fast & deterministic CTIDH.
IACR TCHES, 2025(3):516–541, 2025.
doi:10.46586/tches.v2025.i3.516-541.

[CLM+18] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes.
CSIDH: An efficient post-quantum commutative group action.
In Thomas Peyrin and Steven Galbraith, editors, *ASIACRYPT 2018, Part III*, volume 11274 of *LNCS*, pages 395–427. Springer, Cham, December 2018.
doi:10.1007/978-3-030-03332-3_15.

[CSCJR22] Jorge Chávez-Saab, Jesús-Javier Chi-Domínguez, Samuel Jaques, and Francisco Rodríguez-Henríquez.
The SQALE of CSIDH: sublinear Vélu quantum-resistant isogeny action with low exponents.
Journal of Cryptographic Engineering, 12(3):349–368, September 2022.
doi:10.1007/s13389-021-00271-w.

[DD26] Pierrick Dartois and Max Duparc.
Chasing rabbits through hypercubes: better algorithms for higher dimensional 2-isogeny computations.
Cryptology ePrint Archive, Paper 2026/114, 2026.
URL: https://eprint.iacr.org/2026/114.

[DEF+25] Pierrick Dartois, Jonathan Komada Eriksen, Tako Boris Fouotsa, Arthur Herlédan Le Merdy, Riccardo Invernizzi, Damien Robert, Ryan Rueger, Frederik Vercauteren, and Benjamin Wesolowski.
PEGASIS: Practical effective class group action using 4-dimensional isogenies.
In Yael Tauman Kalai and Seny F. Kamara, editors, *CRYPTO 2025, Part I*, volume 16000 of *LNCS*, pages 67–99. Springer, Cham, August 2025.
doi:10.1007/978-3-032-01855-7_3.

[DEIV25] Pierrick Dartois, Jonathan Komada Eriksen, Riccardo Invernizzi, and Frederik Vercauteren.
qt-pegasis: Simpler and faster effective class group actions.
Cryptology ePrint Archive, Report 2025/1859, 2025.
URL: https://eprint.iacr.org/2025/1859.

References II

[GdKQ+24] Phillip Gajland, Bor de Kock, Miguel Quaresma, Giulio Malavolta, and Peter Schwabe.
SWOOSH: Efficient lattice-based non-interactive key exchange.
In Davide Balzarotti and Wenyuan Xu, editors, *USENIX Security 2024*. USENIX Association, August 2024.
URL: https://www.usenix.org/conference/usenixsecurity24/presentation/gajland.

[Hou25] Marc Houben.
Efficient post-quantum commutative group actions from orientations of large discriminant.
In Goichiro Hanaoka and Bo-Yin Yang, editors, *ASIACRYPT 2025, Part IV*, volume 16248 of *LNCS*, pages 141–173. Springer, Singapore, December 2025.
doi:10.1007/978-981-95-5113-2_5.

[PPS25] Lorenz Panny, Christophe Petit, and Miha Stopar.
KLaPoTi: An asymptotically efficient isogeny group action from 2-dimensional isogenies.
CiC, 2(3):5, 2025.
doi:10.62056/ahp2wakrz.

[PRR+25] Giacomo Pope, Krijn Reijnders, Damien Robert, Alessandro Sferlazza, and Benjamin Smith.
Simpler and faster pairings from the montgomery ladder.
CiC, 2(2):29, 2025.
doi:10.62056/ah2i893y6.

[WLLZ26] Weize Wang, Yi-Fu Lai, Kaizhan Lin, and Yunlei Zhao.
Efficient and parallel implementation of isogeny-based deterministic group actions.
Cryptology ePrint Archive, Paper 2026/627, 2026.
URL: https://eprint.iacr.org/2026/627.

[ZLL+26] Yuhao Zheng, Jianming Lin, Yutong Liang, Yanzhen Ren, Huixin Zhang, and Chang-An Zhao.
Compressed key exchange protocol from orientations of large discriminant using AVX-512.
Cryptology ePrint Archive, Paper 2026/679, 2026.
URL: https://eprint.iacr.org/2026/679.