30−ε Years of Isogeny Group Actions

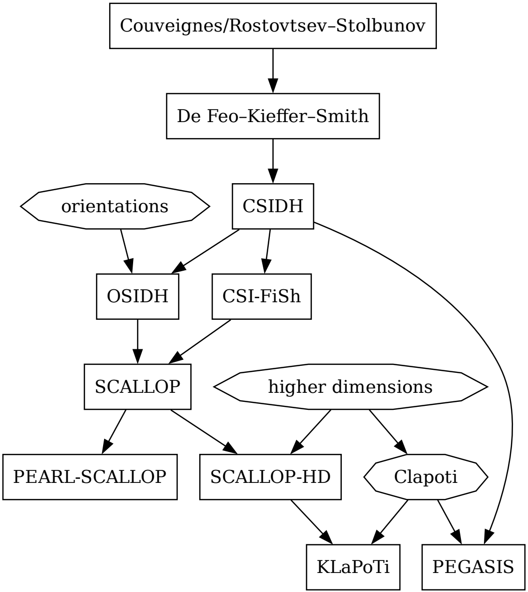
Lorenz Panny

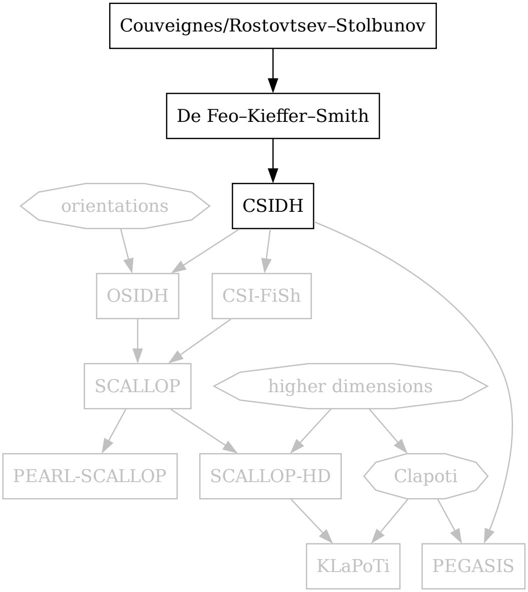
Technische Universität München

Swissogeny Day, Zürich, 20 March 2025

Plan for this talk

- The CSIDH non-interactive key exchange.
- Classical and quantum security.
- Is this an effective group action?
- Oriented elliptic curves and isogenies.
- *Un*restricted effective group actions.


Couveignes/Rostovtsev–Stolbunov
De Feo–Kieffer–Smith
orientations
CSIDH
OSIDH
CSI-FiSh
SCALLOP
higher dimensions
PEARL-SCALLOP
SCALLOP-HD
Clapoti
KLaPoTi
PEGASIS


Couveignes/Rostovtsev–Stolbunov
De Feo–Kieffer–Smith
orientations
CSIDH
OSIDH
CSI-FiSh
SCALLOP
higher dimensions
PEARL-SCALLOP
SCALLOP-HD
Clapoti
KLaPoTi
PEGASIS

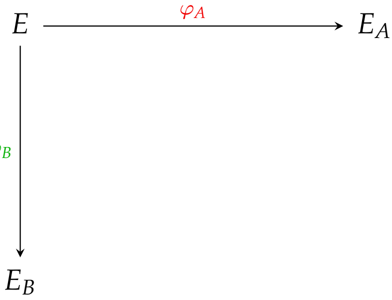
CSIDH [ˈsiːˌsaɪd]

[Castryck–Lange–Martindale–Panny–Renes 2018]

Isogeny-based key exchange: High-level view

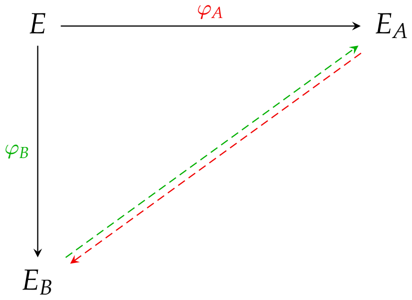
E

Isogeny-based key exchange: High-level view



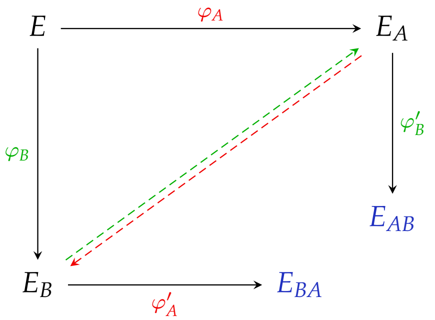
- Alice & Bob pick secret $\varphi_A \colon E \to E_A$ and $\varphi_B \colon E \to E_B$.
  (These isogenies correspond to walking on the isogeny graph.)

Isogeny-based key exchange: High-level view



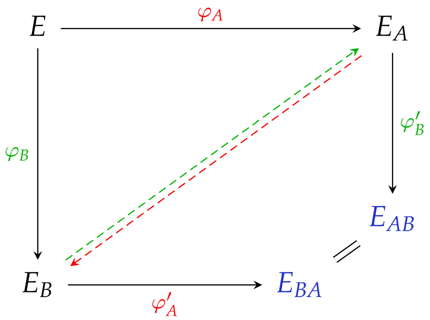
- Alice & Bob pick secret $\varphi_A : E \to E_A$ and $\varphi_B : E \to E_B$.
  (These isogenies correspond to walking on the isogeny graph.)
- Alice and Bob transmit the end curves E_A and E_B.

Isogeny-based key exchange: High-level view



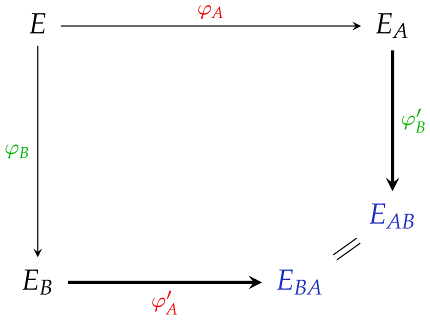
- Alice & Bob pick secret $\varphi_A : E \to E_A$ and $\varphi_B : E \to E_B$.
  (These isogenies correspond to walking on the isogeny graph.)
- Alice and Bob transmit the end curves E_A and E_B.
- Alice somehow finds a "parallel" $\varphi_{A'} : E_B \to E_{BA}$, and
  Bob somehow finds $\varphi_{B'} : E_A \to E_{AB}$,

Isogeny-based key exchange: High-level view

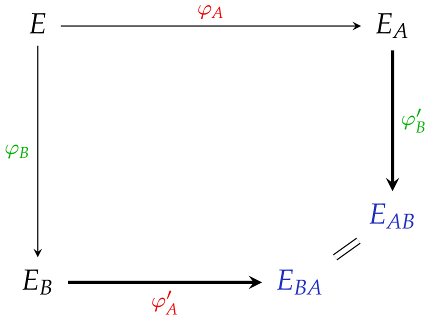


- Alice & Bob pick secret $\varphi_A : E \to E_A$ and $\varphi_B : E \to E_B$.
  (These isogenies correspond to walking on the isogeny graph.)
- Alice and Bob transmit the end curves E_A and E_B.
- Alice <u>somehow</u> finds a "parallel" $\varphi_{A'} : E_B \to E_{BA}$, and
  Bob <u>somehow</u> finds $\varphi_{B'} : E_A \to E_{AB}$, such that $E_{AB} \cong E_{BA}$.

How to find “parallel” isogenies?

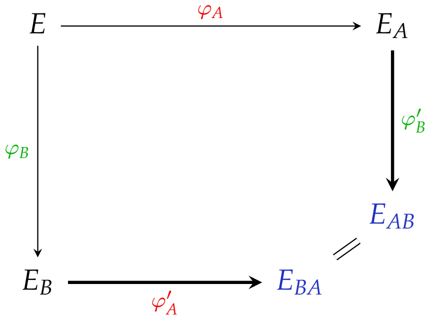


How to find "parallel" isogenies?



CSIDH's solution (earlier: Couveignes, Rostovtsev–Stolbunov):

How to find "parallel" isogenies?



CSIDH's solution (earlier: Couveignes, Rostovtsev–Stolbunov):
Use special isogenies φ_A which can be transported to the curve E_B totally independently of the secret isogeny φ_B.
(Similarly with reversed roles, of course.)

CSIDH in one slide

CSIDH in one slide

- Choose some small odd primes $\ell_1, ..., \ell_n$.
- Make sure $p = 4 \cdot \ell_1 \cdots \ell_n - 1$ is prime.

CSIDH in one slide

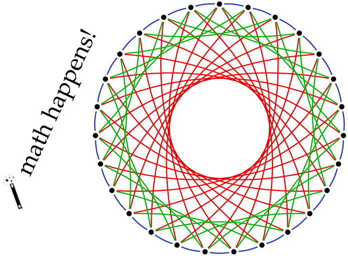
- Choose some small odd primes $\ell_1, \ldots, \ell_n$.
- Make sure $p = 4 \cdot \ell_1 \cdots \ell_n - 1$ is prime.
- Let $X = \{y^2 = x^3 + Ax^2 + x$ supersingular with $A \in \mathbb{F}_p\}$.

CSIDH in one slide

- Choose some small odd primes $\ell_1, ..., \ell_n$.
- Make sure $p = 4 \cdot \ell_1 \cdots \ell_n - 1$ is prime.
- Let $X = \{y^2 = x^3 + Ax^2 + x$ supersingular with $A \in \mathbb{F}_p\}$.
- Look at the $\mathbb{F}_p$-rational isogenies of degrees ℓ_i within X.

CSIDH in one slide

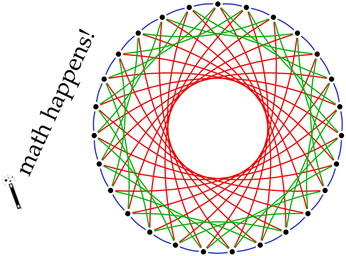
- Choose some small odd primes $\ell_1, \ldots, \ell_n$.
- Make sure $p = 4 \cdot \ell_1 \cdots \ell_n - 1$ is prime.
- Let $X = \{y^2 = x^3 + Ax^2 + x$ supersingular with $A \in \mathbb{F}_p\}$.
- Look at the $\mathbb{F}_p$-rational isogenies of degrees ℓ_i within X.



$p = 419$
$\ell_1 = 3$
$\ell_2 = 5$
$\ell_3 = 7$

CSIDH in one slide

- Choose some small odd primes $\ell_1, ..., \ell_n$.
- Make sure $p = 4 \cdot \ell_1 \cdots \ell_n - 1$ is prime.
- Let $X = \{y^2 = x^3 + Ax^2 + x$ supersingular with $A \in \mathbb{F}_p\}$.
- Look at the $\mathbb{F}_p$-rational isogenies of degrees ℓ_i within X.



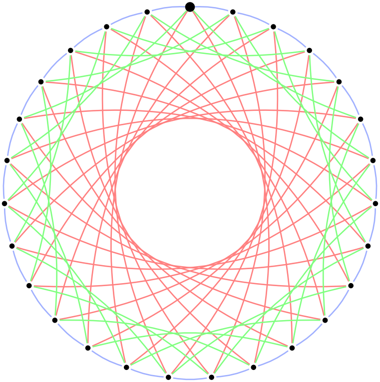
$p = 419$
$\ell_1 = 3$
$\ell_2 = 5$
$\ell_3 = 7$

- Walking “left” and “right” on any ℓ_i-subgraph is efficient.

CSIDH key exchange

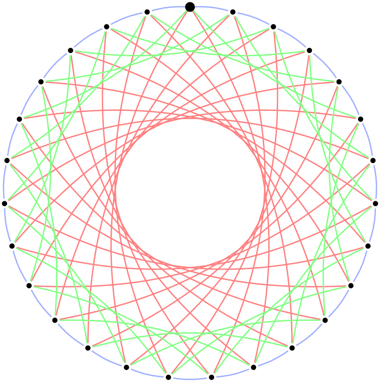
Alice

[+, +, −, −]



Bob

[−, +, −, −]

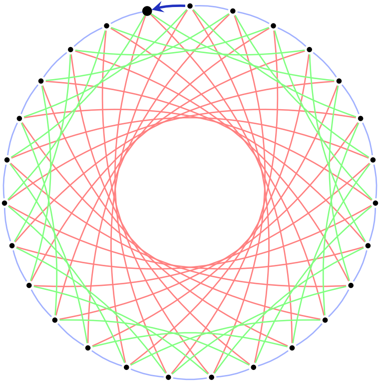


CSIDH key exchange

Alice

[+, +, −, −]

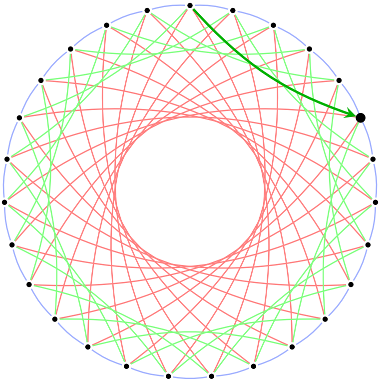
↑



Bob

[−, +, −, −]

↑

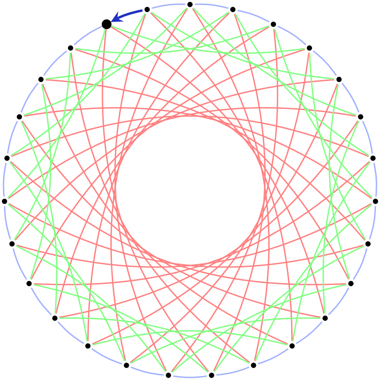


CSIDH key exchange

Alice

[+, +, −, −]

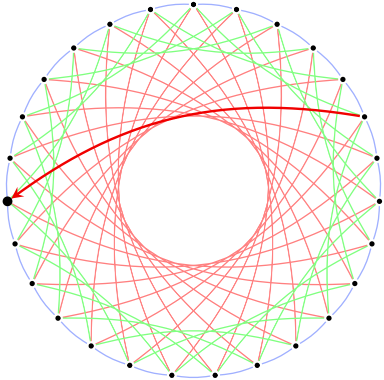
↑



Bob

[−, +, −, −]

↑

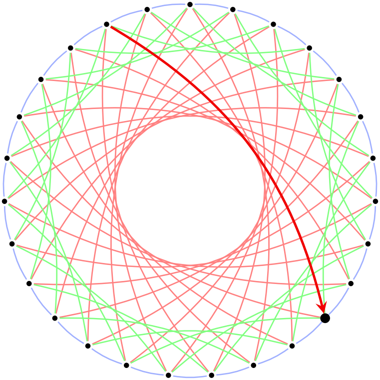


CSIDH key exchange

Alice

[+, +, −, −]

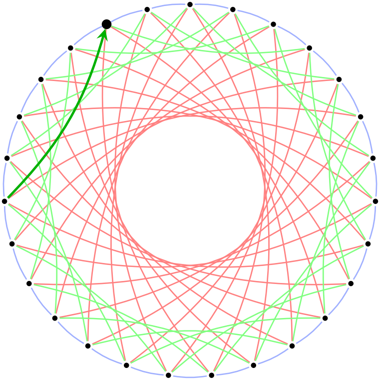
↑



Bob

[−, +, −, −]

↑

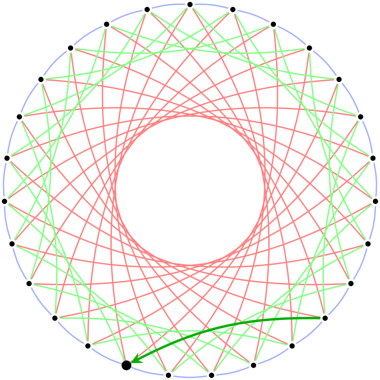


CSIDH key exchange

Alice

[+, +, −, −]

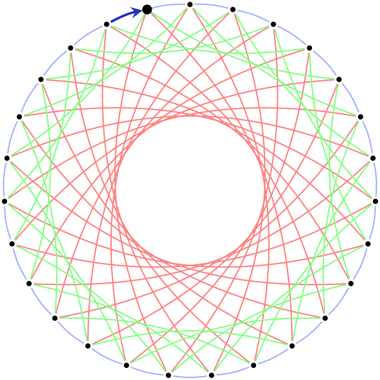
↑



Bob

[−, +, −, −]

↑



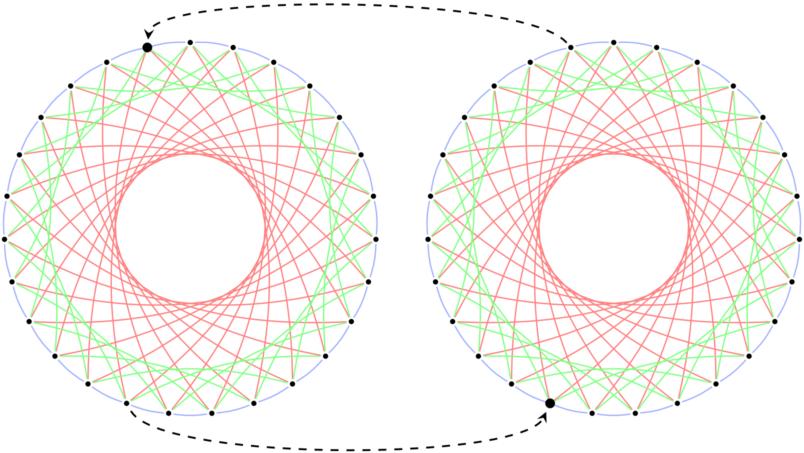
CSIDH key exchange

Alice

[+, +, −, −]

Bob

[−, +, −, −]



CSIDH key exchange

Alice

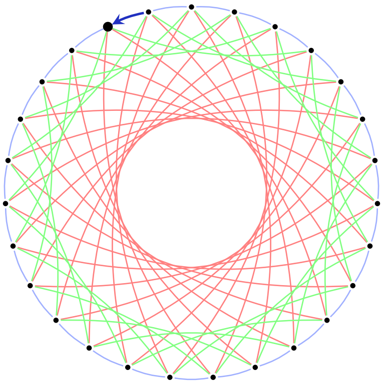
[+, +, −, −]

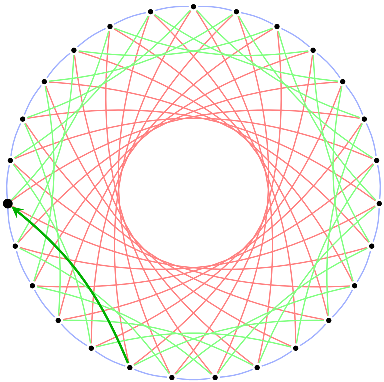
↑

Bob

[−, +, −, −]

↑

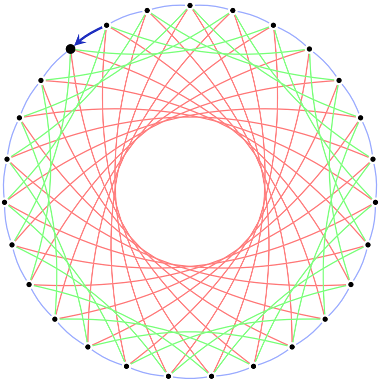




CSIDH key exchange

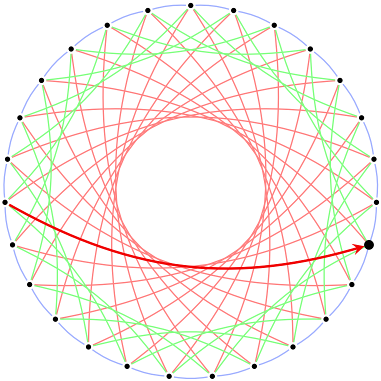
Alice

[+, +, −, −]
↑



Bob

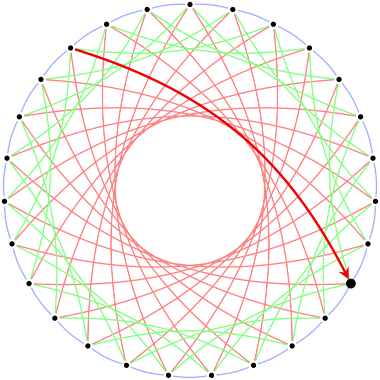
[−, +, −, −]
↑



CSIDH key exchange

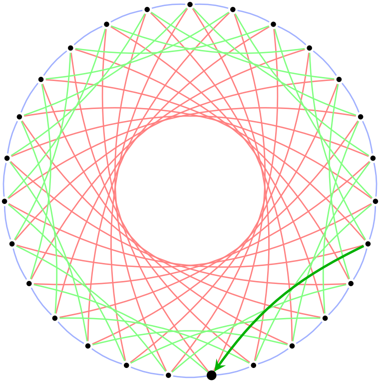
Alice

[+, +, −, −]
↑



Bob

[−, +, −, −]
↑



CSIDH key exchange

Alice

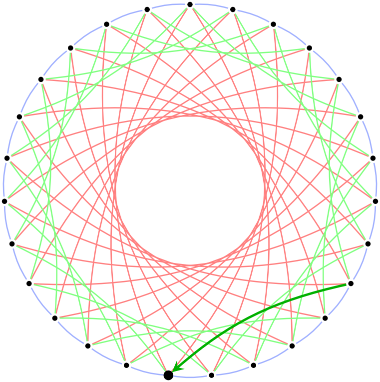
[+, +, −, −]

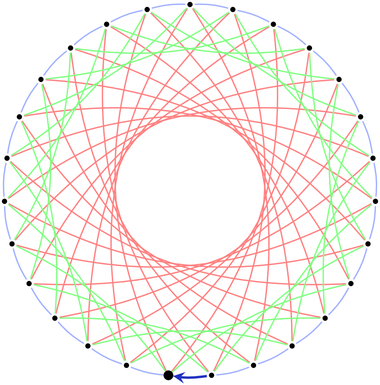
↑

Bob

[−, +, −, −]

↑

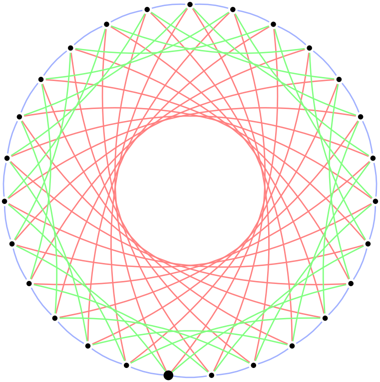




CSIDH key exchange

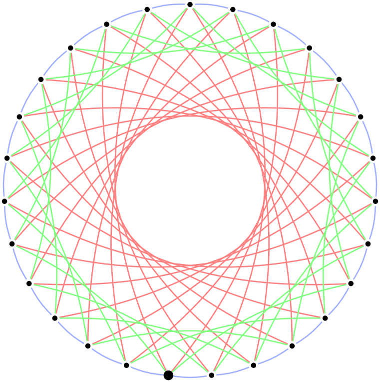
Alice

[+, +, −, −]



Bob

[−, +, −, −]



And... action!

Cycles are compatible: [right then left] = [left then right]

And... action!

Cycles are compatible: [right then left] = [left then right]
$\rightsquigarrow$ only need to keep track of total step counts for each ℓ_i.

Example: [**+**, **+**, **−**, **−**, **−**, **+**, **−**, **−**] just becomes $(+1, \quad 0, -3) \in \mathbb{Z}^3$.

And... action!

Cycles are compatible: [right then left] = [left then right]

$\rightsquigarrow$ only need to keep track of total step counts for each ℓ_i.

Example: [**+**, **+**, **−**, **−**, **−**, **+**, **−**, **−**] just becomes $(+1, \quad 0, -3) \in \mathbb{Z}^3$.

There is a group action of $(\mathbb{Z}^n, +)$ on our set of curves X!

CSIDH via ideals

In CSIDH, the ℓ_i-isogeny kernels are generated by $(x, y) \in E$ with $x \in \mathbb{F}_p$.

CSIDH via ideals

In CSIDH, the ℓ_i-isogeny kernels are generated by $(x, y) \in E$ with $x \in \mathbb{F}_p$. The two cases $y \in \mathbb{F}_p$ and $y \notin \mathbb{F}_p$ correspond precisely to the two $\mathbb{Z}[\pi]$-ideals

$$\mathfrak{l}_i := (\ell_i, \pi - 1)\,;$$
$$\overline{\mathfrak{l}_i} := (\ell_i, \pi + 1)\,,$$

where π is the p-power Frobenius endomorphism ($\pi^2 = [-p]$).

CSIDH via ideals

In CSIDH, the ℓ_i-isogeny kernels are generated by $(x, y) \in E$ with $x \in \mathbb{F}_p$. The two cases $y \in \mathbb{F}_p$ and $y \notin \mathbb{F}_p$ correspond precisely to the two $\mathbb{Z}[\pi]$-ideals

$$\mathfrak{l}_i := (\ell_i, \pi - 1)\,;$$
$$\overline{\mathfrak{l}_i} := (\ell_i, \pi + 1)\,,$$

where π is the p-power Frobenius endomorphism ($\pi^2 = [-p]$).

<u>General picture</u>: The kernels K of rational ℓ_i-isogenies are defined by ideals $\mathfrak{a}$ of $\mathrm{End}_{\mathbb{F}_p}(E)$ via

$$K = \bigcap_{\alpha \in \mathfrak{a}} \ker(\iota(\alpha))\,.$$

CSIDH via ideals

In CSIDH, the ℓ_i-isogeny kernels are generated by $(x, y) \in E$ with $x \in \mathbb{F}_p$. The two cases $y \in \mathbb{F}_p$ and $y \notin \mathbb{F}_p$ correspond precisely to the two $\mathbb{Z}[\pi]$-ideals

$$\mathfrak{l}_i := (\ell_i, \pi - 1)\,;$$
$$\overline{\mathfrak{l}_i} := (\ell_i, \pi + 1)\,,$$

where π is the p-power Frobenius endomorphism ($\pi^2 = [-p]$).

General picture: The kernels K of rational ℓ_i-isogenies are defined by ideals $\mathfrak{a}$ of $\mathrm{End}_{\mathbb{F}_p}(E)$ via

$$K = \bigcap_{\alpha \in \mathfrak{a}} \ker(\iota(\alpha))\,.$$

!! The endomorphisms in $\mathfrak{a}$ “carve out” our kernel subgroup.

The class group

Recall: Group action of $(\mathbb{Z}^n, +)$ on set of curves X.

The class group

Recall: Group action of $(\mathbb{Z}^n, +)$ on set of curves X.

!! The set X is **finite** $\Longrightarrow$ The action is **not free**.

There exist vectors $\underline{v} \in \mathbb{Z}^n \backslash \{0\}$ which act trivially.

The class group

Recall: Group action of $(\mathbb{Z}^n, +)$ on set of curves X.

!! The set X is **finite** $\Longrightarrow$ The action is **not free**.
There exist vectors $\underline{v} \in \mathbb{Z}^n \setminus \{0\}$ which act trivially.
Such $\underline{v}$ form a full-rank subgroup $\Lambda \subseteq \mathbb{Z}^n$, the relation lattice.

The class group

Recall: Group action of $(\mathbb{Z}^n, +)$ on set of curves X.

!! The set X is **finite** $\Longrightarrow$ The action is **not free**.
There exist vectors $\underline{v} \in \mathbb{Z}^n \setminus \{0\}$ which act trivially.
Such $\underline{v}$ form a full-rank subgroup $\Lambda \subseteq \mathbb{Z}^n$, the relation lattice.

We understand the structure: Trivial action $\widehat{=}$ cycle in the graph $\widehat{=}$ endomorphism $\widehat{=}$ principal $\mathbb{Z}[\pi]$-ideal.

The class group

<u>Recall</u>: Group action of $(\mathbb{Z}^n, +)$ on set of curves X.

!! The set X is **finite** $\Longrightarrow$ The action is **not free**.
There exist vectors $\underline{v} \in \mathbb{Z}^n \backslash \{0\}$ which act trivially.
Such $\underline{v}$ form a full-rank subgroup $\Lambda \subseteq \mathbb{Z}^n$, the relation lattice.

We <u>understand the structure</u>: Trivial action $\hat{=}$ cycle in the graph $\hat{=}$ endomorphism $\hat{=}$ principal $\mathbb{Z}[\pi]$-ideal.

The quotient $\mathbb{Z}^n/\Lambda$ is $\cong$ the ideal-class group $\mathrm{cl}(\mathbb{Z}[\sqrt{-p}])$.

(I will talk some more about this later.)

The class group

<u>Recall</u>: Group action of $(\mathbb{Z}^n, +)$ on set of curves X.

!! The set X is **finite** $\Longrightarrow$ The action is **not free**.
There exist vectors $\underline{v} \in \mathbb{Z}^n \setminus \{0\}$ which act trivially.
Such $\underline{v}$ form a full-rank subgroup $\Lambda \subseteq \mathbb{Z}^n$, the relation lattice.

We <u>understand the structure</u>: Trivial action $\widehat{=}$ cycle in the graph $\widehat{=}$ endomorphism $\widehat{=}$ principal $\mathbb{Z}[\pi]$-ideal.

The quotient $\mathbb{Z}^n/\Lambda$ is $\cong$ the ideal-class group $\mathrm{cl}(\mathbb{Z}[\sqrt{-p}])$.

(I will talk some more about this later.)

!! This group characterizes *when two paths lead to the same curve*.

Couveignes/Rostovtsev–Stolbunov/De Feo–Kieffer-Smith

...proposed doing the same thing, but with ordinary curves.

Couveignes/Rostovtsev–Stolbunov/De Feo–Kieffer-Smith

...proposed doing the same thing, but with ordinary curves.

Big problem: No good way to control $\#E(\mathbb{F}_p)$

Couveignes/Rostovtsev–Stolbunov/De Feo–Kieffer-Smith

...proposed doing the same thing, but with ordinary curves.

Big problem: No good way to control $\#E(\mathbb{F}_p)$

$\rightsquigarrow$ Computing the action of $\mathfrak{l}_i$ is much more expensive.

Plan for this talk

- The CSIDH non-interactive key exchange. ✓
- Classical and quantum security.
- Is this an effective group action?
- Oriented elliptic curves and isogenies.
- *Un*restricted effective group actions.

Why no Shor?

Shor's quantum algorithm computes α from g^α in any group in polynomial time.

Why no Shor?

Shor's quantum algorithm computes α from g^α in any group in polynomial time.

Shor computes α from $h = g^\alpha$ by finding the kernel of the map

$$f\colon\ \mathbb{Z}^2 \to G,\ (x, y) \mapsto g^x \cdot h^y\,.$$

Why no Shor?

> Shor's quantum algorithm computes α from g^α in any group in polynomial time.

Shor computes α from $h = g^\alpha$ by finding the kernel of the map

$$f\colon\ \mathbb{Z}^2 \to G,\ (x,y) \mapsto g^x \underset{\uparrow}{\cdot} h^y\,.$$

For group <u>actions</u>, we simply cannot compose $a * s$ and $b * s$!

Security of CSIDH

Core problem:
Given $E, E' \in X$, find a path $E \to E'$ in the isogeny graph.

Security of CSIDH

Core problem:
Given $E, E' \in X$, find a path $E \to E'$ in the isogeny graph.

The size of X is $\#\mathrm{cl}(\mathbb{Z}[\sqrt{-p}]) = 3 \cdot h(-p) \approx \sqrt{p}$.

$\rightsquigarrow$ best known classical attack: meet-in-the-middle, $\tilde{\mathcal{O}}(p^{1/4})$.

Fully exponential: Complexity $\exp\big((\log p)^{1+o(1)}\big)$.

Security of CSIDH

Core problem:
Given $E, E' \in X$, find a path $E \to E'$ in the isogeny graph.

The size of X is $\#\mathrm{cl}(\mathbb{Z}[\sqrt{-p}]) = 3 \cdot h(-p) \approx \sqrt{p}$.

$\rightsquigarrow$ best known classical attack: meet-in-the-middle, $\tilde{\mathcal{O}}(p^{1/4})$.

Fully exponential: Complexity $\exp\big((\log p)^{1+o(1)}\big)$.

Solving abelian hidden shift breaks CSIDH.

$\rightsquigarrow$ non-devastating quantum attack (Kuperberg's algorithm).

Subexponential: Complexity $\exp\big((\log p)^{1/2+o(1)}\big)$.

CSIDH vs. Kuperberg

Kuperberg's algorithm consists of two components:

1. Evaluate the group action many times. (“oracle calls”)
2. Combine the results in a certain way. (“sieving”)

CSIDH vs. Kuperberg

Kuperberg's algorithm consists of two components:

1. Evaluate the group action many times. ("oracle calls")
2. Combine the results in a certain way. ("sieving")

- The algorithm admits many different tradeoffs.
- Oracle calls are expensive.
- The sieving phase has classical *and* quantum operations.

CSIDH vs. Kuperberg

Kuperberg's algorithm consists of two components:

1. Evaluate the group action many times. ("oracle calls")
2. Combine the results in a certain way. ("sieving")

- The algorithm admits many different tradeoffs.
- Oracle calls are expensive.
- The sieving phase has classical *and* quantum operations.
  - $\rightsquigarrow$ **How to compare costs?**
    (Is one qubit operation $\approx$ one bit operation? a hundred? millions?)

CSIDH vs. Kuperberg

Kuperberg's algorithm consists of two components:

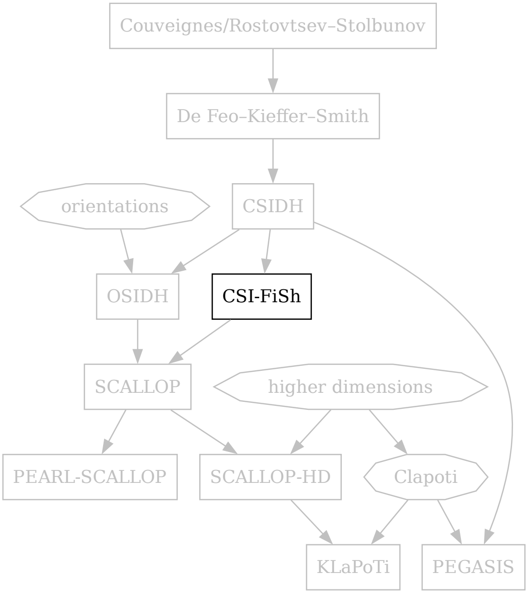
1. Evaluate the group action many times. ("oracle calls")
2. Combine the results in a certain way. ("sieving")

- The algorithm admits many different tradeoffs.
- Oracle calls are expensive.
- The sieving phase has classical *and* quantum operations.
  - $\rightsquigarrow$ **How to compare costs?**
    (Is one qubit operation $\approx$ one bit operation? a hundred? millions?)

$\implies$ Security estimates for CSIDH & friends vary wildly.

Plan for this talk

- The CSIDH non-interactive key exchange. ✓
- Classical and quantum security. ✓
- Is this an effective group action?
- Oriented elliptic curves and isogenies.
- *Un*restricted effective group actions.


Couveignes/Rostovtsev–Stolbunov
De Feo–Kieffer–Smith
orientations
CSIDH
OSIDH
CSI-FiSh
SCALLOP
higher dimensions
PEARL-SCALLOP
SCALLOP-HD
Clapoti
KLaPoTi
PEGASIS

The basic strategy à la C/RS/DKS/CSIDH

- Let $\mathfrak{l}_1, \ldots, \mathfrak{l}_n$ be small prime ideals of $\mathcal{O}$, and suppose $\mathfrak{a}$ is given to us in the form $\mathfrak{a} = \mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n}$.

The basic strategy à la C/RS/DKS/CSIDH

- Let $\mathfrak{l}_1, \ldots, \mathfrak{l}_n$ be small prime ideals of $\mathcal{O}$, and suppose $\mathfrak{a}$ is given to us in the form $\mathfrak{a} = \mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n}$.
- Then $\mathfrak{a}$ can be evaluated as a sequence of $\mathfrak{l}_i$.

The basic strategy à la C/RS/DKS/CSIDH

- Let $\mathfrak{l}_1, ..., \mathfrak{l}_n$ be small prime ideals of $\mathcal{O}$, and suppose $\mathfrak{a}$ is given to us in the form $\mathfrak{a} = \mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n}$.
- Then $\mathfrak{a}$ can be evaluated as a sequence of $\mathfrak{l}_i$.
- Evaluating a single $\mathfrak{l}_i$: Write $\mathfrak{l}_i = (\ell_i, \vartheta - \lambda_i)$. Then the kernel is an order-ℓ_i point P with $\vartheta(P) = [\lambda_i]P$.

The basic strategy à la C/RS/DKS/CSIDH

- Let $\mathfrak{l}_1, \ldots, \mathfrak{l}_n$ be small prime ideals of $\mathcal{O}$, and suppose $\mathfrak{a}$ is given to us in the form $\mathfrak{a} = \mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n}$.
- Then $\mathfrak{a}$ can be evaluated as a sequence of $\mathfrak{l}_i$.

- Evaluating a single $\mathfrak{l}_i$: Write $\mathfrak{l}_i = (\ell_i, \vartheta - \lambda_i)$.
  Then the kernel is an order-ℓ_i point P with $\vartheta(P) = [\lambda_i]P$.
- Optimization: Batch multiple $\mathfrak{l}_i$ together $\rightsquigarrow$ "strategies".

The basic problem with the basic strategy

- Couveignes: This gives a “hard homogeneous space” (weirder name for a one-way commutative group action).

The basic problem with the basic strategy

- Couveignes: This gives a "hard homogeneous space" (weirder name for a one-way commutative group action).
- The CSIDH paper repeats this.

The basic problem with the basic strategy

- Couveignes: This gives a "hard homogeneous space" (weirder name for a one-way commutative group action).
- The CSIDH paper repeats this.

Issue:

- Representing $\mathrm{cl}(\mathcal{O})$ by the group $(\mathbb{Z}^n, +)$ of exponents makes the exponents grow larger with each operation.
  - $\rightsquigarrow$ Cost of evaluating after k operations is $O(\exp(k))$.

The basic problem with the basic strategy

- Couveignes: This gives a "hard homogeneous space" (weirder name for a one-way commutative group action).
- The CSIDH paper repeats this.

Issue:

- Representing $\mathrm{cl}(\mathcal{O})$ by the group $(\mathbb{Z}^n, +)$ of exponents makes the exponents grow larger with each operation.
  - ⇝ Cost of evaluating after k operations is $O(\exp(k))$.
- Representing $\mathrm{cl}(\mathcal{O})$ as reduced ideals allows computing in $\mathrm{cl}(\mathcal{O})$ efficiently, but evaluation becomes superpolynomial.

(A similar approach will be discussed on the following slides.)

The basic problem with the basic strategy

- Couveignes: This gives a "hard homogeneous space" (weirder name for a one-way commutative group action).
- The CSIDH paper repeats this.

<u>Issue:</u>

- Representing $\mathrm{cl}(\mathcal{O})$ by the group $(\mathbb{Z}^n, +)$ of exponents makes the exponents grow larger with each operation.
  $\rightsquigarrow$ Cost of evaluating after k operations is $O(\exp(k))$.
- Representing $\mathrm{cl}(\mathcal{O})$ as reduced ideals allows computing in $\mathrm{cl}(\mathcal{O})$ efficiently, but evaluation becomes superpolynomial.
  (A similar approach will be discussed on the following slides.)

$\rightsquigarrow$ A priori **not** an effective group action when done either way!

The CSI-FiSh approach

...combines exponent vectors with reduction by exploiting the relation lattice of the chosen ideal classes. It works as follows:

The strategy to act by a given, arbitrarily long and ugly exponent vector $\underline{v} \in \mathbb{Z}^d$ consists of the following steps:

1. "Computing the class group": Find a basis of the *relation lattice* $\Lambda \subseteq \mathbb{Z}^d$ with respect to $\mathfrak{l}_1, \ldots, \mathfrak{l}_d$.
   [Classically subexponential-time, quantumly polynomial-time. Precomputation.]
2. "Lattice reduction": Prepare a "good" basis of Λ using a lattice-reduction algorithm such as BKZ.
   [Configurable complexity-quality tradeoff by varying the block size. Precomputation.]
3. "Approximate CVP": Obtain a vector $\underline{w} \in \Lambda$ such that $\|\underline{v} - \underline{w}\|_1$ is "small", using the reduced basis.
   [Polynomial-time, but the quality depends on the quality of step 2.]
4. "Isogeny steps": Evaluate the action of the vector $\underline{v} - \underline{w} \in \mathbb{Z}^d$ as a sequence of $\mathfrak{l}_i$-steps.
   [Complexity depends entirely on the output quality of step 3.]

https://yx7.cc/blah/2023-04-14.html

The CSI-FiSh approach

...combines exponent vectors with reduction by exploiting the relation lattice of the chosen ideal classes. It works as follows:

The strategy to act by a given, arbitrarily long and ugly exponent vector $\underline{v} \in \mathbb{Z}^d$ consists of the following steps:

1. "Computing the class group": Find a basis of the *relation lattice* $\Lambda \subseteq \mathbb{Z}^d$ with respect to $\mathfrak{l}_1, \dots, \mathfrak{l}_d$.
   [Classically subexponential-time, quantumly polynomial-time. Precomputation.]
2. "Lattice reduction": Prepare a "good" basis of Λ using a lattice-reduction algorithm such as BKZ.
   [Configurable complexity-quality tradeoff by varying the block size. Precomputation.]
3. "Approximate CVP": Obtain a vector $\underline{w} \in \Lambda$ such that $\|\underline{v} - \underline{w}\|_1$ is "small", using the reduced basis.
   [Polynomial-time, but the quality depends on the quality of step 2.]
4. "Isogeny steps": Evaluate the action of the vector $\underline{v} - \underline{w} \in \mathbb{Z}^d$ as a sequence of $\mathfrak{l}_i$-steps.
   [Complexity depends entirely on the output quality of step 3.]

https://yx7.cc/blah/2023-04-14.html

The CSI-FiSh paper (2019) does all this in practice for 512-bit p.

The CSI-FiSh approach

...combines exponent vectors with reduction by exploiting the relation lattice of the chosen ideal classes. It works as follows:

The strategy to act by a given, arbitrarily long and ugly exponent vector $\underline{v} \in \mathbb{Z}^d$ consists of the following steps:

1. "Computing the class group": Find a basis of the *relation lattice* $\Lambda \subseteq \mathbb{Z}^d$ with respect to $\mathfrak{l}_1, \dots, \mathfrak{l}_d$.
   [Classically subexponential-time, quantumly polynomial-time. Precomputation.]
2. "Lattice reduction": Prepare a "good" basis of Λ using a lattice-reduction algorithm such as BKZ.
   [Configurable complexity-quality tradeoff by varying the block size. Precomputation.]
3. "Approximate CVP": Obtain a vector $\underline{w} \in \Lambda$ such that $\|\underline{v} - \underline{w}\|_1$ is "small", using the reduced basis.
   [Polynomial-time, but the quality depends on the quality of step 2.]
4. "Isogeny steps": Evaluate the action of the vector $\underline{v} - \underline{w} \in \mathbb{Z}^d$ as a sequence of $\mathfrak{l}_i$-steps.
   [Complexity depends entirely on the output quality of step 3.]

https://yx7.cc/blah/2023-04-14.html

The CSI-FiSh paper (2019) does all this in practice for 512-bit p.

What about asymptotics?

Tradeoff: Lattice part vs. isogeny part

- By increasing the number n of ideals $\mathfrak{l}_i$, we can trade off some "isogeny effort" for "lattice effort".

⇝ Sweet spot: Minimize total cost.

Tradeoff: Lattice part vs. isogeny part

- By increasing the number n of ideals $\mathfrak{l}_i$, we can trade off some "isogeny effort" for "lattice effort".

$\rightsquigarrow$ Sweet spot: Minimize total cost.

CSI-FiSh really isn't polynomial-time

It is fairly well-known that CSIDH[1] in its basic form is merely a *restricted* effective group action $G \times X \to X$: There is a small number of group elements $\mathfrak{l}_1, \ldots, \mathfrak{l}_d \in G$ whose action can be applied to arbitrary elements of X efficiently, but applying other elements (say, large products $\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_d^{e_d}$ of the $\mathfrak{l}_i$) quickly becomes infeasible as the exponents grow.

The only known method to circumvent this issue consists of a folklore strategy first employed in practice by the signature scheme CSI-FiSh. The core of the technique is to rewrite any given group element as a *short* product combination of the $\mathfrak{l}_i$, whose action can then be computed in the usual way much more affordably. (Notice how this is philosophically similar to the role of the square-and-multiply algorithm in discrete-logarithm land!)

The main point of this post is to remark that this approach is **not asymptotically efficient**, even when a quantum computer can be used, contradicting a false belief that appears to be rather common among isogeny aficionados.

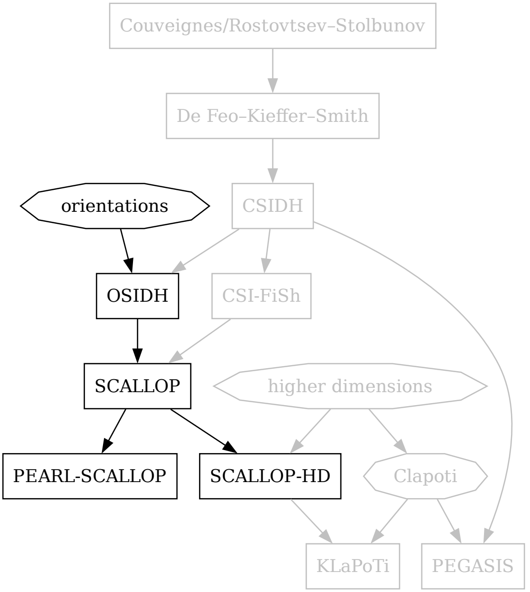
$\rightsquigarrow$

- Classically: Evaluation $L_p[1/2]$. Attack $L_p[1]$.
- Quantumly: Evaluation $L_p[1/3]$. Attack $L_p[1/2]$.

https://yx7.cc/blah/2023-04-14.html

Plan for this talk

- The CSIDH non-interactive key exchange. ✓
- Classical and quantum security. ✓
- Is this an effective group action? ✓
- Oriented elliptic curves and isogenies.
- *Un*restricted effective group actions.


Couveignes/Rostovtsev–Stolbunov
De Feo–Kieffer–Smith
orientations
CSIDH
OSIDH
CSI-FiSh
SCALLOP
higher dimensions
PEARL-SCALLOP
SCALLOP-HD
Clapoti
KLaPoTi
PEGASIS

More endomorphisms

- In CSIDH, we've used kernels of the form $K = E(\mathbb{F}_p)[\ell_i]$, which equals the subgroup defined by the ideal $(\ell_i, \pi - \lambda)$.

More endomorphisms

- In CSIDH, we've used kernels of the form $K = E(\mathbb{F}_p)[\ell_i]$, which equals the subgroup defined by the ideal $(\ell_i, \pi - \lambda)$.
- New idea: Replace π by other endomorphisms.
  (Recall that $\mathrm{End}(E)$ is a rank-4 lattice in the supersingular case $\rightsquigarrow$ plenty of choice.)

More endomorphisms

- In CSIDH, we've used kernels of the form $K = E(\mathbb{F}_p)[\ell_i]$, which equals the subgroup defined by the ideal $(\ell_i, \pi - \lambda)$.
- New idea: Replace π by other endomorphisms.
  (Recall that $\mathrm{End}(E)$ is a rank-4 lattice in the supersingular case $\rightsquigarrow$ plenty of choice.)

Fact: If $\varphi\colon E \to E'$ is an isogeny for which $\ker(\varphi)$ is described in terms of scalars and some endomorphism $\tau \in \mathrm{End}(E)$, then we can usually push τ through φ:

$$\begin{aligned} \mathbb{Z}[\tau] &\longhookrightarrow \mathrm{End}(E') \\ \tau &\longmapsto (\varphi \circ \tau \circ \widehat{\varphi})/\deg(\varphi) \end{aligned}$$

*

Ideals $\leftrightarrow$ kernels

As before with CSIDH, the isogenies for which this works are those defined by (invertible) ideals of the ring $\mathbb{Z}[\tau]$.

Ideals $\leftrightarrow$ kernels

As before with CSIDH, the isogenies for which this works are those defined by (invertible) ideals of the ring $\mathbb{Z}[\tau]$.

Principal ideals (ϑ) correspond to endomorphisms ϑ.

Ideals $\leftrightarrow$ kernels

As before with CSIDH, the isogenies for which this works are those defined by (invertible) ideals of the ring $\mathbb{Z}[\tau]$.

Principal ideals (ϑ) correspond to endomorphisms ϑ.

$\rightsquigarrow$ Connection to the "class set" or class group:

ideals	$\longleftrightarrow$	kernels	$\longleftrightarrow$	isogenies
ideal *classes*	$\longleftrightarrow$	(no name)	$\longleftrightarrow$	isogeny *codomains*

Orientations & oriented curves

Let $\mathcal{O} = \mathbb{Z}[\tau]$ be an imaginary-quadratic order.

(Standard cases: $\tau = \sqrt{-d}$ or $\tau = \frac{1+\sqrt{-d}}{2}$ where $d \in \mathbb{Z}_{\geq 1}$.)

Orientations & oriented curves

Let $\mathcal{O} = \mathbb{Z}[\tau]$ be an imaginary-quadratic order.

(Standard cases: $\tau = \sqrt{-d}$ or $\tau = \frac{1+\sqrt{-d}}{2}$ where $d \in \mathbb{Z}_{\geq 1}$.)

An $\mathcal{O}$-orientation of an elliptic curve E is a ring embedding

$$\iota \colon \mathcal{O} \hookrightarrow \operatorname{End}(E)\,.$$

The pair (E, ι) is then called an $\mathcal{O}$-oriented curve.

Orientations & oriented curves

Let $\mathcal{O} = \mathbb{Z}[\tau]$ be an imaginary-quadratic order.

(Standard cases: $\tau = \sqrt{-d}$ or $\tau = \frac{1+\sqrt{-d}}{2}$ where $d \in \mathbb{Z}_{\geq 1}$.)

An $\mathcal{O}$-orientation of an elliptic curve E is a ring embedding

$$\iota \colon \mathcal{O} \hookrightarrow \mathrm{End}(E)\,.$$

The pair (E, ι) is then called an $\mathcal{O}$-oriented curve.

Example: For $E/\mathbb{F}_p$ supersingular with $p \geq 5$, there are two orientations by $\mathbb{Z}[\sqrt{-p}]$: Mapping $\sqrt{-p}$ either to π or to $-\pi$.

Orientations & oriented curves

Let $\mathcal{O} = \mathbb{Z}[\tau]$ be an imaginary-quadratic order.

(Standard cases: $\tau = \sqrt{-d}$ or $\tau = \frac{1+\sqrt{-d}}{2}$ where $d \in \mathbb{Z}_{\geq 1}$.)

An $\mathcal{O}$-orientation of an elliptic curve E is a ring embedding

$$\iota \colon \mathcal{O} \hookrightarrow \mathrm{End}(E)\,.$$

The pair (E, ι) is then called an $\mathcal{O}$-oriented curve.

Example: For $E/\mathbb{F}_p$ supersingular with $p \geq 5$, there are two orientations by $\mathbb{Z}[\sqrt{-p}]$: Mapping $\sqrt{-p}$ either to π or to $-\pi$.

Example: Any nonscalar endomorphism $\tau \in \mathrm{End}(E) \setminus \mathbb{Z}$ defines an orientation of $\mathcal{O} := \mathbb{Z}[\tau]$ on E.

The oriented class-group action

Onuki 2020 (previously Kohel–Colò 2020 without proof):

Theorem 3.4. *Let K be an imaginary quadratic field such that p does not split in K, and $\mathcal{O}$ an order in K such that p does not divide the conductor of $\mathcal{O}$. Then the ideal class group $\mathcal{C}\ell(\mathcal{O})$ acts freely and transitively on $\rho(\mathcal{E}\ell\ell(\mathcal{O}))$.*

https://arxiv.org/pdf/2002.09894

The oriented class-group action

Theorem 3.4. *Let K be an imaginary quadratic field such that p does not split in K, and $\mathcal{O}$ an order in K such that p does not divide the conductor of $\mathcal{O}$. Then the ideal class group $\mathcal{C}\ell(\mathcal{O})$ acts freely and transitively on $\rho(\mathcal{E}\ell\ell(\mathcal{O}))$.*

$\rho(\mathcal{E}\ell\ell(\mathcal{O}))$: a set of supersingular elliptic curves E over $\mathbb{F}_{p^2}$ with a primitive orientation $\iota\colon \mathcal{O} \hookrightarrow \mathrm{End}(E)$, up to oriented isomorphism.

The oriented class-group action

Theorem 3.4. *Let K be an imaginary quadratic field such that p does not split in K, and $\mathcal{O}$ an order in K such that p does not divide the conductor of $\mathcal{O}$. Then the ideal class group $\mathcal{C}\ell(\mathcal{O})$ acts freely and transitively on $\rho(\mathcal{E}\ell\ell(\mathcal{O}))$.*

$\rho(\mathcal{E}\ell\ell(\mathcal{O}))$: <u>a</u> set of supersingular elliptic curves E over $\mathbb{F}_{p^2}$ with a primitive orientation $\iota\colon \mathcal{O} \hookrightarrow \mathrm{End}(E)$, up to oriented isomorphism.

- $\iota\colon \mathcal{O} \hookrightarrow \mathrm{End}(E)$ is *primitive* if $(\iota(\mathcal{O}) \otimes_{\mathbb{Z}} \mathbb{Q}) \cap \mathrm{End}(E) = \iota(\mathcal{O})$.
- $\alpha\colon (E, \iota) \to (E', \iota')$ is an *oriented* isomorphism if $\alpha \circ \iota = \iota' \circ \alpha$.

The oriented class-group action

Theorem 3.4. *Let K be an imaginary quadratic field such that p does not split in K, and $\mathcal{O}$ an order in K such that p does not divide the conductor of $\mathcal{O}$. Then the ideal class group $\mathcal{C}\ell(\mathcal{O})$ acts freely and transitively on $\rho(\mathcal{E}\ell\ell(\mathcal{O}))$.*

$\rho(\mathcal{E}\ell\ell(\mathcal{O}))$: a set of supersingular elliptic curves E over $\mathbb{F}_{p^2}$ with a primitive orientation $\iota\colon \mathcal{O} \hookrightarrow \mathrm{End}(E)$, up to oriented isomorphism.

- $\iota\colon \mathcal{O} \hookrightarrow \mathrm{End}(E)$ is *primitive* if $(\iota(\mathcal{O}) \otimes_{\mathbb{Z}} \mathbb{Q}) \cap \mathrm{End}(E) = \iota(\mathcal{O})$.
- $\alpha\colon (E, \iota) \to (E', \iota')$ is an *oriented* isomorphism if $\alpha \circ \iota = \iota' \circ \alpha$.

The group action is defined as follows:

$$\mathfrak{a} \star (E, \iota) := \left(E/\mathfrak{a},\ (\phi_{\mathfrak{a}} \circ \iota \circ \widehat{\phi}_{\mathfrak{a}})/\mathrm{norm}(\mathfrak{a})\right)$$

where $\phi_{\mathfrak{a}}\colon E \to E/\mathfrak{a}$ is the isogeny with kernel

$$E[\mathfrak{a}] := \bigcap_{\alpha \in \mathfrak{a}} \ker(\iota(\alpha))\,.$$

(NB: In the cases we care about, we have $\pi_{p^2} = [-p]$, hence all isogenies are $\mathbb{F}_{p^2}$-rational.)

Recap: CSIDH

CSIDH is the special case of orienting by Frobenius.

(That is: Orienting by $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$ via the identification $\sqrt{-p} \mapsto \pi$.)

Recap: CSIDH

CSIDH is the special case of orienting by Frobenius.
(That is: Orienting by $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$ via the identification $\sqrt{-p} \mapsto \pi$.)

Since "finding" π on any $E/\mathbb{F}_p$ is trivial (it is $\pi\colon (x, y) \mapsto (x^p, y^p)$),
it need not be transmitted and we get an action on curves only.

Recap: CSIDH

CSIDH is the special case of orienting by Frobenius.
(That is: Orienting by $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$ via the identification $\sqrt{-p} \mapsto \pi$.)

Since "finding" π on any $E/\mathbb{F}_p$ is trivial (it is $\pi\colon (x, y) \mapsto (x^p, y^p)$),
it need not be transmitted and we get an action on curves only.

Fun fact: Orienting $E/\mathbb{F}_p$ by $\sqrt{-p} \mapsto -\pi$ gives exactly the same picture, but everything is mirrored via quadratic twisting:

$$\{y^2 = x^3 + Ax^2 + x\} \overset{\sim}{\longmapsto} \{y^2 = x^3 - Ax^2 + x\}$$

Representing orientations

To turn the previous theorem into a concrete group action for general $\mathcal{O}$, we need to specify how to encode the pair (E, ι):

Representing orientations

To turn the previous theorem into a concrete group action for general $\mathcal{O}$, we need to specify how to encode the pair (E, ι):

- When $\mathcal{O}$ is represented as $\mathbb{Z}[\tau] := \mathbb{Z}[X]/\mu_\tau(X)$ where μ_τ is the minimal polynomial of τ, an embedding $\iota\colon \mathcal{O} \hookrightarrow \mathrm{End}(E)$ can be specified by the image $\iota(\tau)$.

Representing orientations

To turn the previous theorem into a concrete group action for general $\mathcal{O}$, we need to specify how to encode the pair (E, ι):

- When $\mathcal{O}$ is represented as $\mathbb{Z}[\tau] := \mathbb{Z}[X]/\mu_\tau(X)$ where μ_τ is the minimal polynomial of τ, an embedding $\iota\colon \mathcal{O} \hookrightarrow \mathrm{End}(E)$ can be specified by the image $\iota(\tau)$.

$\rightsquigarrow$ In **practice**, an oriented curve is given as a pair (E, ϑ) with $\vartheta \in \mathrm{End}(E)$, implicitly communicating that $\vartheta = \iota(\tau)$.

Representing orientations

To turn the previous theorem into a concrete group action for general $\mathcal{O}$, we need to specify how to encode the pair (E, ι):

- When $\mathcal{O}$ is represented as $\mathbb{Z}[\tau] := \mathbb{Z}[X]/\mu_\tau(X)$ where μ_τ is the minimal polynomial of τ, an embedding $\iota\colon \mathcal{O} \hookrightarrow \mathrm{End}(E)$ can be specified by the image $\iota(\tau)$.

⇝ In **practice**, an oriented curve is given as a pair (E, ϑ) with $\vartheta \in \mathrm{End}(E)$, implicitly communicating that $\vartheta = \iota(\tau)$.

- There are multiple options for representing such a ϑ.
  Simple example: A deterministically chosen generator point of $\ker(\vartheta)$.
  More complicated: Deterministic HD representation (SCALLOP-HD).

Oriented isogeny group actions: Why?

- Key point: Orientations allow us to decouple the discriminant of $\mathcal{O}$ from the characteristic p.

This is advantageous for at least two reasons (see next part):

Oriented isogeny group actions: Why?

- Key point: Orientations allow us to decouple the discriminant of $\mathcal{O}$ from the characteristic p.

This is advantageous for at least two reasons (see next part):

$\rightsquigarrow$ Can use rings like $\mathcal{O} = \mathbb{Z}[f\sqrt{-d}]$, where computing the relation lattice Λ can be much easier than for general $\mathcal{O}$.

Oriented isogeny group actions: Why?

- Key point: Orientations allow us to decouple the discriminant of $\mathcal{O}$ from the characteristic p.

This is advantageous for at least two reasons (see next part):

⇝ Can use rings like $\mathcal{O} = \mathbb{Z}[f\sqrt{-d}]$, where computing the relation lattice Λ can be much easier than for general $\mathcal{O}$.

⇝ For Clapoti (soon!), we have to solve norm equations that are derived from $\mathcal{O}$ for target values derived from p.

Orientations: Security

!! Not every orientation is equally secure: If $\mathrm{disc}(\mathcal{O})$ has a square factor q^2, the vectorization problem for the $\mathcal{O}$-orientation can be split into smaller chunks by "walking up the q-volcano".

Orientations: Security

!! Not every orientation is equally secure: If $\operatorname{disc}(\mathcal{O})$ has a square factor q^2, the vectorization problem for the $\mathcal{O}$-orientation can be split into smaller chunks by "walking up the q-volcano".

Concretely, this means vectorization for $\mathcal{O}$ reduces to:

Orientations: Security

!! Not every orientation is equally secure: If $\mathrm{disc}(\mathcal{O})$ has a square factor q^2, the vectorization problem for the $\mathcal{O}$-orientation can be split into smaller chunks by "walking up the q-volcano".

Concretely, this means vectorization for $\mathcal{O}$ reduces to:

- Vectorization for the superorder of $\mathcal{O}$ of index q.

  $\rightsquigarrow$ class group shrinks by a factor $\approx q$!

Orientations: Security

!! Not every orientation is equally secure: If $\mathrm{disc}(\mathcal{O})$ has a square factor q^2, the vectorization problem for the $\mathcal{O}$-orientation can be split into smaller chunks by "walking up the q-volcano".

Concretely, this means vectorization for $\mathcal{O}$ reduces to:

- Vectorization for the superorder of $\mathcal{O}$ of index q.
  $\rightsquigarrow$ class group shrinks by a factor $\approx q$!
- Some brute-force search of complexity $\approx q$.

Orientations: Security

!! Not every orientation is equally secure: If $\operatorname{disc}(\mathcal{O})$ has a square factor q^2, the vectorization problem for the $\mathcal{O}$-orientation can be split into smaller chunks by "walking up the q-volcano".

Concretely, this means vectorization for $\mathcal{O}$ reduces to:

- Vectorization for the superorder of $\mathcal{O}$ of index q.
  $\rightsquigarrow$ class group shrinks by a factor $\approx q$!
- Some brute-force search of complexity $\approx q$.

$\rightsquigarrow$ **Complexity** determined by squarefree part of $\operatorname{disc}(\mathcal{O})$, plus the non-smooth square part of $\operatorname{disc}(\mathcal{O})$.

Orientations: Security

!! Not every orientation is equally secure: If $\mathrm{disc}(\mathcal{O})$ has a square factor q^2, the vectorization problem for the $\mathcal{O}$-orientation can be split into smaller chunks by "walking up the q-volcano".

Concretely, this means vectorization for $\mathcal{O}$ reduces to:

- Vectorization for the superorder of $\mathcal{O}$ of index q.
  $\rightsquigarrow$ class group shrinks by a factor $\approx q$!
- Some brute-force search of complexity $\approx q$.

$\rightsquigarrow$ **Complexity** determined by squarefree part of $\mathrm{disc}(\mathcal{O})$, plus the non-smooth square part of $\mathrm{disc}(\mathcal{O})$.

To play around with this, try my CTF challenge "`not_csidh`": `https://hxp.io/blog/96`
(Don't forget to submit your code to SageMath afterwards. :-))

Oriented group actions: Cryptographic instantiations

- **C/RS/DKS**: Oriented by $\mathbb{Z}[\pi]$, using ordinary E.

Oriented group actions: Cryptographic instantiations

- **C/RS/DKS**: Oriented by $\mathbb{Z}[\pi]$, using ordinary E.
- **CSIDH**: Oriented by $\mathbb{Z}[\pi]$, using supersingular $E/\mathbb{F}_p$.

Oriented group actions: Cryptographic instantiations

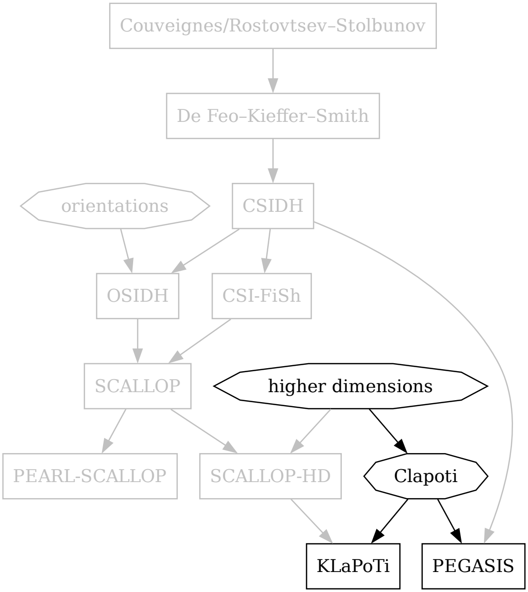
- **C/RS/DKS**: Oriented by $\mathbb{Z}[\pi]$, using ordinary E.
- **CSIDH**: Oriented by $\mathbb{Z}[\pi]$, using supersingular $E/\mathbb{F}_p$.
- **OSIDH**: Oriented by $\mathbb{Z}[\ell^n \iota]$, where ι small endomorphism.

Oriented group actions: Cryptographic instantiations

- **C/RS/DKS**: Oriented by $\mathbb{Z}[\pi]$, using ordinary E.
- **CSIDH**: Oriented by $\mathbb{Z}[\pi]$, using supersingular $E/\mathbb{F}_p$.
- **OSIDH**: Oriented by $\mathbb{Z}[\ell^n \iota]$, where ι small endomorphism.
- **SCALLOP** family: Oriented by $\mathbb{Z}[f\iota]$, where f large prime.

Plan for this talk

- The CSIDH non-interactive key exchange. ✓
- Classical and quantum security. ✓
- Is this an effective group action? ✓
- Oriented elliptic curves and isogenies. ✓
- *Un*restricted effective group actions.


Couveignes/Rostovtsev–Stolbunov
De Feo–Kieffer–Smith
orientations
CSIDH
OSIDH
CSI-FiSh
SCALLOP
higher dimensions
PEARL-SCALLOP
SCALLOP-HD
Clapoti
KLaPoTi
PEGASIS

Clapoti

Even more maritime isogenies??

Noun [edit]

clapotis *m* (*plural* **clapotis**)

1. lapping of water against a surface [synonyms ▲]

Clapoti

Even more maritime isogenies??

Noun [edit]

clapotis *m* (*plural* **clapotis**)

1. lapping of water against a surface [synonyms ▲]

- Page–Robert: A polynomial-time algorithm to evaluate the isogeny group action on arbitrary ideals.

Polynomial-time group action: Clapoti

Idea:

- Find two ideals $\mathfrak{b}$, $\mathfrak{c}$ of coprime norms, both equivalent to $\mathfrak{a}$.
  Let $N := \mathrm{norm}(\mathfrak{b}) + \mathrm{norm}(\mathfrak{c})$.

Polynomial-time group action: Clapoti

Idea:

- Find two ideals $\mathfrak{b}, \mathfrak{c}$ of coprime norms, both equivalent to $\mathfrak{a}$.
  Let $N := \mathrm{norm}(\mathfrak{b}) + \mathrm{norm}(\mathfrak{c})$.

$$\begin{array}{ccc} E & \xrightarrow{\phi_{\mathfrak{b}}} & E_{\mathfrak{a}} \\ {\scriptstyle \phi_{\overline{\mathfrak{c}}}}\downarrow & & \downarrow{\scriptstyle \psi_{\overline{\mathfrak{c}}}} \\ E_{\overline{\mathfrak{a}}} & \xrightarrow[\psi_{\mathfrak{b}}]{} & E \end{array}$$

Polynomial-time group action: Clapoti

Idea:

- Find two ideals $\mathfrak{b}, \mathfrak{c}$ of coprime norms, both equivalent to $\mathfrak{a}$.
  Let $N := \mathrm{norm}(\mathfrak{b}) + \mathrm{norm}(\mathfrak{c})$.

$$\begin{array}{ccc} E & \xrightarrow{\phi_{\mathfrak{b}}} & E_{\mathfrak{a}} \\ {\scriptstyle \phi_{\bar{\mathfrak{c}}}}\downarrow & & \downarrow{\scriptstyle \psi_{\bar{\mathfrak{c}}}} \\ E_{\bar{\mathfrak{a}}} & \xrightarrow[\psi_{\mathfrak{b}}]{} & E \end{array}$$

- Kani: This gives an N-isogeny

$$\begin{aligned} \Phi\colon E \times E &\longrightarrow E_{\mathfrak{a}} \times E_{\bar{\mathfrak{a}}}, \\ (P, Q) &\longmapsto \left(\phi_{\mathfrak{b}}(P) + \widehat{\psi}_{\bar{\mathfrak{c}}}(Q),\ -\phi_{\bar{\mathfrak{c}}}(P) + \widehat{\psi}_{\mathfrak{b}}(Q)\right). \end{aligned}$$

Polynomial-time group action: Clapoti

<u>Idea:</u>

- Find two ideals $\mathfrak{b}, \mathfrak{c}$ of coprime norms, both equivalent to $\mathfrak{a}$.
  Let $N := \mathrm{norm}(\mathfrak{b}) + \mathrm{norm}(\mathfrak{c})$.

$$\begin{array}{ccc} E & \xrightarrow{\phi_{\mathfrak{b}}} & E_{\mathfrak{a}} \\ {\scriptstyle \phi_{\bar{\mathfrak{c}}}}\downarrow & & \downarrow{\scriptstyle \psi_{\bar{\mathfrak{c}}}} \\ E_{\bar{\mathfrak{a}}} & \xrightarrow[\psi_{\mathfrak{b}}]{} & E \end{array}$$

- Kani: This gives an N-isogeny

$$\begin{aligned} \Phi \colon E \times E &\longrightarrow E_{\mathfrak{a}} \times E_{\bar{\mathfrak{a}}}, \\ (P, Q) &\longmapsto \left(\phi_{\mathfrak{b}}(P) + \widehat{\psi}_{\bar{\mathfrak{c}}}(Q),\ -\phi_{\bar{\mathfrak{c}}}(P) + \widehat{\psi}_{\mathfrak{b}}(Q)\right). \end{aligned}$$

- The kernel is $\ker(\Phi) = \left\{\left(\widehat{\phi}_{\mathfrak{b}}(R), \psi_{\bar{\mathfrak{c}}}(R)\right) : R \in E_{\mathfrak{a}}[N]\right\}$.

Polynomial-time group action: Clapoti (in 2D)

- The kernel is $\ker(\Phi) = \left\{ \left(\widehat{\phi_{\mathfrak{b}}}(R), \psi_{\bar{\mathfrak{c}}}(R) \right) : R \in E_{\mathfrak{a}}[N] \right\}$.

Polynomial-time group action: Clapoti (in 2D)

- The kernel is $\ker(\Phi) = \left\{ \left(\widehat{\phi_{\mathfrak{b}}}(R), \psi_{\bar{\mathfrak{c}}}(R) \right) : R \in E_{\mathfrak{a}}[N] \right\}$.
- Issue: Evaluating this formula seems to require a-priori knowledge of $\phi_{\mathfrak{b}}, \psi_{\bar{\mathfrak{c}}}$.

Polynomial-time group action: Clapoti (in 2D)

- The kernel is $\ker(\Phi) = \left\{ \left(\widehat{\phi}_{\mathfrak{b}}(R), \psi_{\overline{\mathfrak{c}}}(R) \right) : R \in E_{\mathfrak{a}}[N] \right\}$.
- Issue: Evaluating this formula seems to require a-priori knowledge of $\phi_{\mathfrak{b}}, \psi_{\overline{\mathfrak{c}}}$.

The kernel is equal to the alternative description

$$\ker(\Phi) = \left\{ \left([\mathrm{norm}(\mathfrak{b})]R, \gamma(R) \right) \mid R \in E[N] \right\}$$

where $\gamma \in \mathrm{End}(E)$ is a generator of the principal ideal $\mathfrak{b}\overline{\mathfrak{c}}$.

Polynomial-time group action: Clapoti (in 2D)

- The kernel is $\ker(\Phi) = \left\{\left(\widehat{\phi}_{\mathfrak{b}}(R), \psi_{\bar{\mathfrak{c}}}(R)\right) : R \in E_{\mathfrak{a}}[N]\right\}$.
- Issue: Evaluating this formula seems to require a-priori knowledge of $\phi_{\mathfrak{b}}, \psi_{\bar{\mathfrak{c}}}$.

The kernel is equal to the alternative description

$$\ker(\Phi) = \left\{\left([\mathrm{norm}(\mathfrak{b})]R, \gamma(R)\right) \mid R \in E[N]\right\}$$

where $\gamma \in \mathrm{End}(E)$ is a generator of the principal ideal $\mathfrak{b}\bar{\mathfrak{c}}$.

$\Longrightarrow$ The isogeny group action can now be computed in polynomial time even for "ugly" input ideals.

Polynomial-time group action: Clapoti (in 2D)

- The kernel is $\ker(\Phi) = \left\{ \left(\widehat{\phi_{\mathfrak{b}}}(R), \psi_{\bar{\mathfrak{c}}}(R) \right) : R \in E_{\mathfrak{a}}[N] \right\}$.
- Issue: Evaluating this formula seems to require a-priori knowledge of $\phi_{\mathfrak{b}}, \psi_{\bar{\mathfrak{c}}}$.

🪄 The kernel is equal to the alternative description

$$\ker(\Phi) = \left\{ \left([\mathrm{norm}(\mathfrak{b})]R, \gamma(R) \right) \mid R \in E[N] \right\}$$

where $\gamma \in \mathrm{End}(E)$ is a generator of the principal ideal $\mathfrak{b}\bar{\mathfrak{c}}$.

$\Longrightarrow$ The isogeny group action can now be computed in polynomial time even for “ugly” input ideals.

$\Longrightarrow$ Isogenies yield true effective group actions, at last!

Effective group actions (2D)

- Ideals equivalent to $\mathfrak{a}$ look like $\mathfrak{a}\overline{\gamma}/\mathrm{norm}(\mathfrak{a})$ where $\gamma \in \mathfrak{a}$.

Effective group actions (2D)

- Ideals equivalent to $\mathfrak{a}$ look like $\mathfrak{a}\overline{\gamma}/\mathrm{norm}(\mathfrak{a})$ where $\gamma \in \mathfrak{a}$.
- The norm equation turns into $N = f(x, y) + f(x, y)$ with $f(x, y) = \mathrm{norm}(x\omega_1 + y\omega_2)/\mathrm{norm}(\mathfrak{a})$ when $\mathfrak{a} = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$.

Effective group actions (2D)

- Ideals equivalent to $\mathfrak{a}$ look like $\mathfrak{a}\overline{\gamma}/\mathrm{norm}(\mathfrak{a})$ where $\gamma \in \mathfrak{a}$.
- The norm equation turns into $N = f(x,y) + f(x,y)$ with $f(x,y) = \mathrm{norm}(x\omega_1 + y\omega_2)/\mathrm{norm}(\mathfrak{a})$ when $\mathfrak{a} = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$.

!! This is the norm form of $\mathcal{I} := \mathfrak{a} + \mathrm{i}\mathfrak{a}$ inside the quaternion order $\mathcal{Q} := \mathcal{O} + \mathrm{i}\mathcal{O}$. (NB: The quaternion algebra here is *not* $\mathrm{End}(E) \otimes \mathbb{Q}$.)

Effective group actions (2D)

- Ideals equivalent to $\mathfrak{a}$ look like $\mathfrak{a}\overline{\gamma}/\mathrm{norm}(\mathfrak{a})$ where $\gamma \in \mathfrak{a}$.
- The norm equation turns into $N = f(x,y) + f(x,y)$ with $f(x,y) = \mathrm{norm}(x\omega_1 + y\omega_2)/\mathrm{norm}(\mathfrak{a})$ when $\mathfrak{a} = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$.

!! This is the norm form of $\mathcal{I} := \mathfrak{a} + \mathrm{i}\mathfrak{a}$ inside the quaternion order $\mathcal{Q} := \mathcal{O} + \mathrm{i}\mathcal{O}$. (NB: The quaternion algebra here is *not* $\mathrm{End}(E) \otimes \mathbb{Q}$.)

⇝ Look for element $\alpha \in \mathfrak{a} + \mathrm{i}\mathfrak{a}$ with $\mathrm{norm}(\alpha) = N \cdot \mathrm{norm}(\mathcal{I})$, split it into $\alpha = \beta + \mathrm{i}\gamma$ with $\beta, \gamma \in \mathcal{O}$.
Then use $\mathfrak{b} := \mathfrak{a}\overline{\beta}/\mathrm{norm}(\mathfrak{a})$ and $\mathfrak{c} := \mathfrak{a}\overline{\gamma}/\mathrm{norm}(\mathfrak{a})$.

Effective group actions (2D)

- Ideals equivalent to $\mathfrak{a}$ look like $\mathfrak{a}\overline{\gamma}/\mathrm{norm}(\mathfrak{a})$ where $\gamma \in \mathfrak{a}$.
- The norm equation turns into $N = f(x,y) + f(x,y)$ with $f(x,y) = \mathrm{norm}(x\omega_1 + y\omega_2)/\mathrm{norm}(\mathfrak{a})$ when $\mathfrak{a} = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$.

!! This is the norm form of $\mathcal{I} := \mathfrak{a} + \mathrm{i}\mathfrak{a}$ inside the quaternion order $\mathcal{Q} := \mathcal{O} + \mathrm{i}\mathcal{O}$. (NB: The quaternion algebra here is *not* $\mathrm{End}(E) \otimes \mathbb{Q}$.)

⇝ Look for element $\alpha \in \mathfrak{a} + \mathrm{i}\mathfrak{a}$ with $\mathrm{norm}(\alpha) = N \cdot \mathrm{norm}(\mathcal{I})$, split it into $\alpha = \beta + \mathrm{i}\gamma$ with $\beta, \gamma \in \mathcal{O}$.
Then use $\mathfrak{b} := \mathfrak{a}\overline{\beta}/\mathrm{norm}(\mathfrak{a})$ and $\mathfrak{c} := \mathfrak{a}\overline{\gamma}/\mathrm{norm}(\mathfrak{a})$.

:) The KLPT algorithm does this for us!

Effective group actions (2D)

- Ideals equivalent to $\mathfrak{a}$ look like $\mathfrak{a}\overline{\gamma}/\mathrm{norm}(\mathfrak{a})$ where $\gamma \in \mathfrak{a}$.
- The norm equation turns into $N = f(x,y) + f(x,y)$ with $f(x,y) = \mathrm{norm}(x\omega_1 + y\omega_2)/\mathrm{norm}(\mathfrak{a})$ when $\mathfrak{a} = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$.

!! This is the norm form of $\mathcal{I} := \mathfrak{a} + \mathrm{i}\mathfrak{a}$ inside the quaternion order $\mathcal{Q} := \mathcal{O} + \mathrm{i}\mathcal{O}$. (NB: The quaternion algebra here is *not* $\mathrm{End}(E) \otimes \mathbb{Q}$.)

⇝ Look for element $\alpha \in \mathfrak{a} + \mathrm{i}\mathfrak{a}$ with $\mathrm{norm}(\alpha) = N \cdot \mathrm{norm}(\mathcal{I})$, split it into $\alpha = \beta + \mathrm{i}\gamma$ with $\beta, \gamma \in \mathcal{O}$.
Then use $\mathfrak{b} := \mathfrak{a}\overline{\beta}/\mathrm{norm}(\mathfrak{a})$ and $\mathfrak{c} := \mathfrak{a}\overline{\gamma}/\mathrm{norm}(\mathfrak{a})$.

:) The KLPT algorithm does this for us!

:(...only for $\mathrm{disc}(\mathcal{O}) = p^{3+\varepsilon}$.

Effective group actions (2D)

- Ideals equivalent to $\mathfrak{a}$ look like $\mathfrak{a}\overline{\gamma}/\mathrm{norm}(\mathfrak{a})$ where $\gamma \in \mathfrak{a}$.
- The norm equation turns into $N = f(x,y) + f(x,y)$ with $f(x,y) = \mathrm{norm}(x\omega_1 + y\omega_2)/\mathrm{norm}(\mathfrak{a})$ when $\mathfrak{a} = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$.

!! This is the norm form of $\mathcal{I} := \mathfrak{a} + \mathrm{i}\mathfrak{a}$ inside the quaternion order $\mathcal{Q} := \mathcal{O} + \mathrm{i}\mathcal{O}$. (NB: The quaternion algebra here is *not* $\mathrm{End}(E) \otimes \mathbb{Q}$.)

⇝ Look for element $\alpha \in \mathfrak{a} + \mathrm{i}\mathfrak{a}$ with $\mathrm{norm}(\alpha) = N \cdot \mathrm{norm}(\mathcal{I})$, split it into $\alpha = \beta + \mathrm{i}\gamma$ with $\beta, \gamma \in \mathcal{O}$.
Then use $\mathfrak{b} := \mathfrak{a}\overline{\beta}/\mathrm{norm}(\mathfrak{a})$ and $\mathfrak{c} := \mathfrak{a}\overline{\gamma}/\mathrm{norm}(\mathfrak{a})$.

:) The KLPT algorithm does this for us!

:(...only for $\mathrm{disc}(\mathcal{O}) = p^{\mathbf{3}+\varepsilon}$.

⇝ KLaPoTi/SCALLOP2D: Practical instantiation of this.
Pretty bad performance for "small" parameters, but finally asymptotically polynomial-time for the first time.

Effective group actions (4D)

Applying Clapoti in $4 > 2$ dimensions is better.

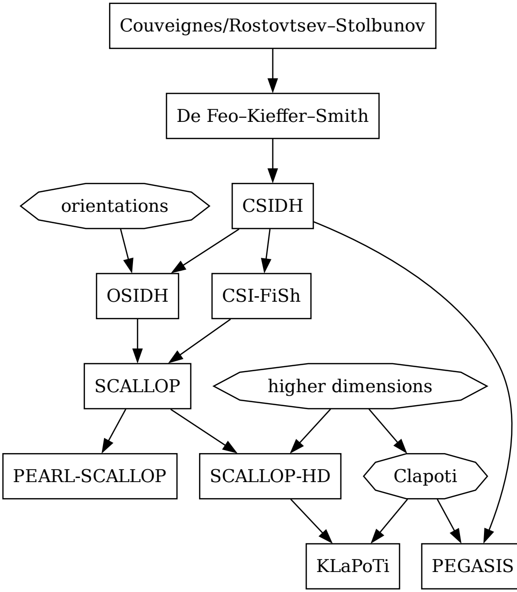
$\rightsquigarrow$ **PEGASIS** $\leftrightsquigarrow$

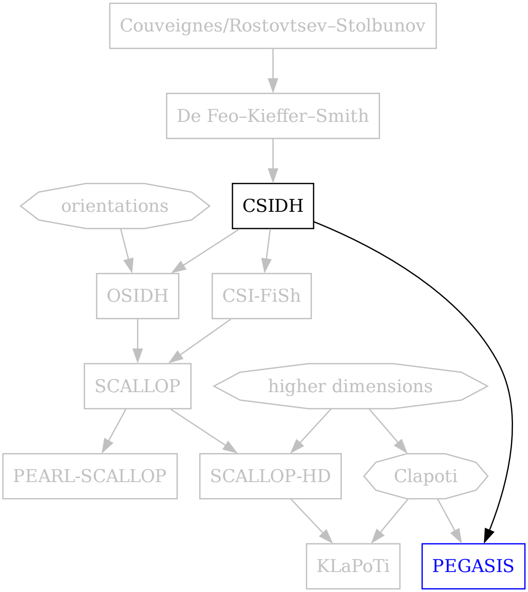
Effective group actions (4D)

Applying Clapoti in $4 > 2$ dimensions is better.

$\rightsquigarrow$ **PEGASIS** $\leftrightsquigarrow$

(See Ryan's talk later today!)


Couveignes/Rostovtsev–Stolbunov
De Feo–Kieffer–Smith
orientations
CSIDH
OSIDH
CSI-FiSh
SCALLOP
higher dimensions
PEARL-SCALLOP
SCALLOP-HD
Clapoti
KLaPoTi
PEGASIS


Couveignes/Rostovtsev–Stolbunov
De Feo–Kieffer–Smith
orientations
CSIDH
OSIDH
CSI-FiSh
SCALLOP
higher dimensions
PEARL-SCALLOP
SCALLOP-HD
Clapoti
KLaPoTi
PEGASIS

Plan for this talk

- The CSIDH non-interactive key exchange. ✓
- Classical and quantum security. ✓
- Is this an effective group action? ✓
- Oriented elliptic curves and isogenies. ✓
- *Un*restricted effective group actions. ✓

Questions!

- Quantum security: How large should $\mathrm{disc}(\mathcal{O})$ be?
  (I think this is the biggest roadblock for CSIDH & friends.)
- Performance: Is PEGASIS universally superior?
  (Can we thank the others for their service and ditch them for good?)
- Protocols: Beyond key exchange?
  (Proposals exist — any of them convincing to practicioners?)

Questions?

(Also feel free to email me: `lorenz@yx7.cc`)