Isogeny graphs of abelian varieties and applications to M-SIDH

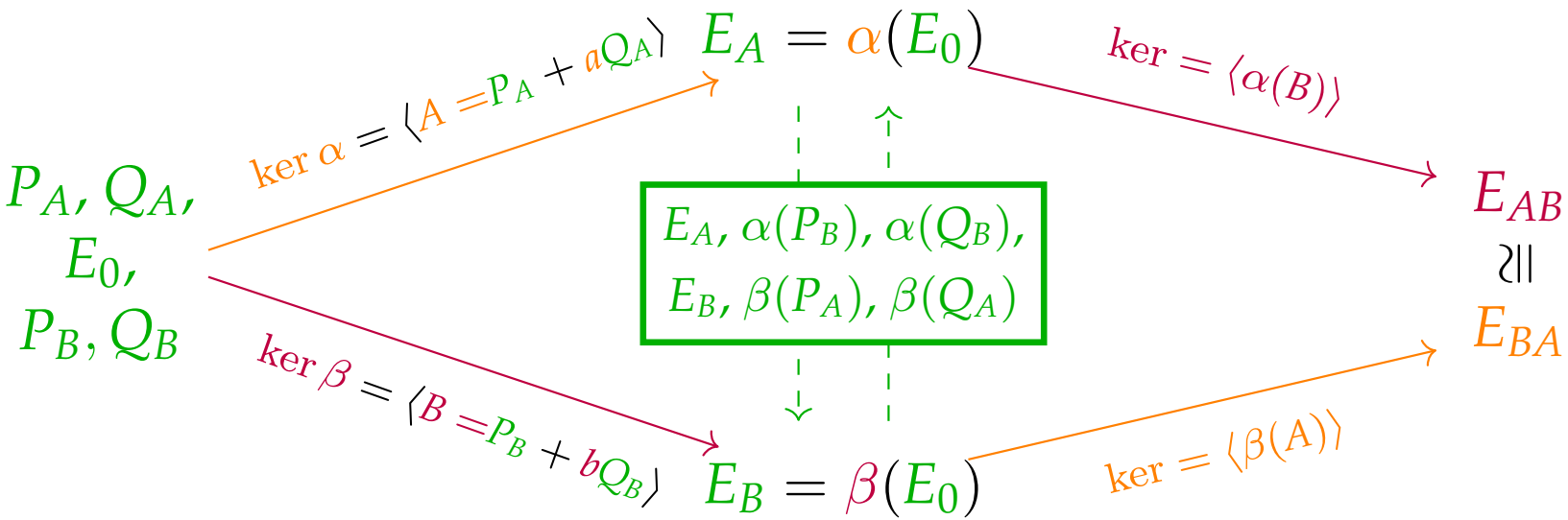
Chloe Martindale
www.martindale.info
University of Bristol

What is this about?

- What is M-SIDH?
- Can we apply SIDH attack methods to M-SIDH?
  - Mostly representing discussions w/ Basso, Cottaar, Fouotsa, Laflamme, Minko, Mocanu, Mokrani, Pedersen, Santos, Stange, Wesolowski
- Theoretical and computational barriers re: isogenies of abelian varieties.
- What do we know?
  - Includes discussions w/ Brooks, Ionica, Jetchev, Milio, Robert, Streng, Vuille, Wesolowski
- Other applications of pushing barriers?

M-SIDH Fouotsa, Moriya, Petit '22

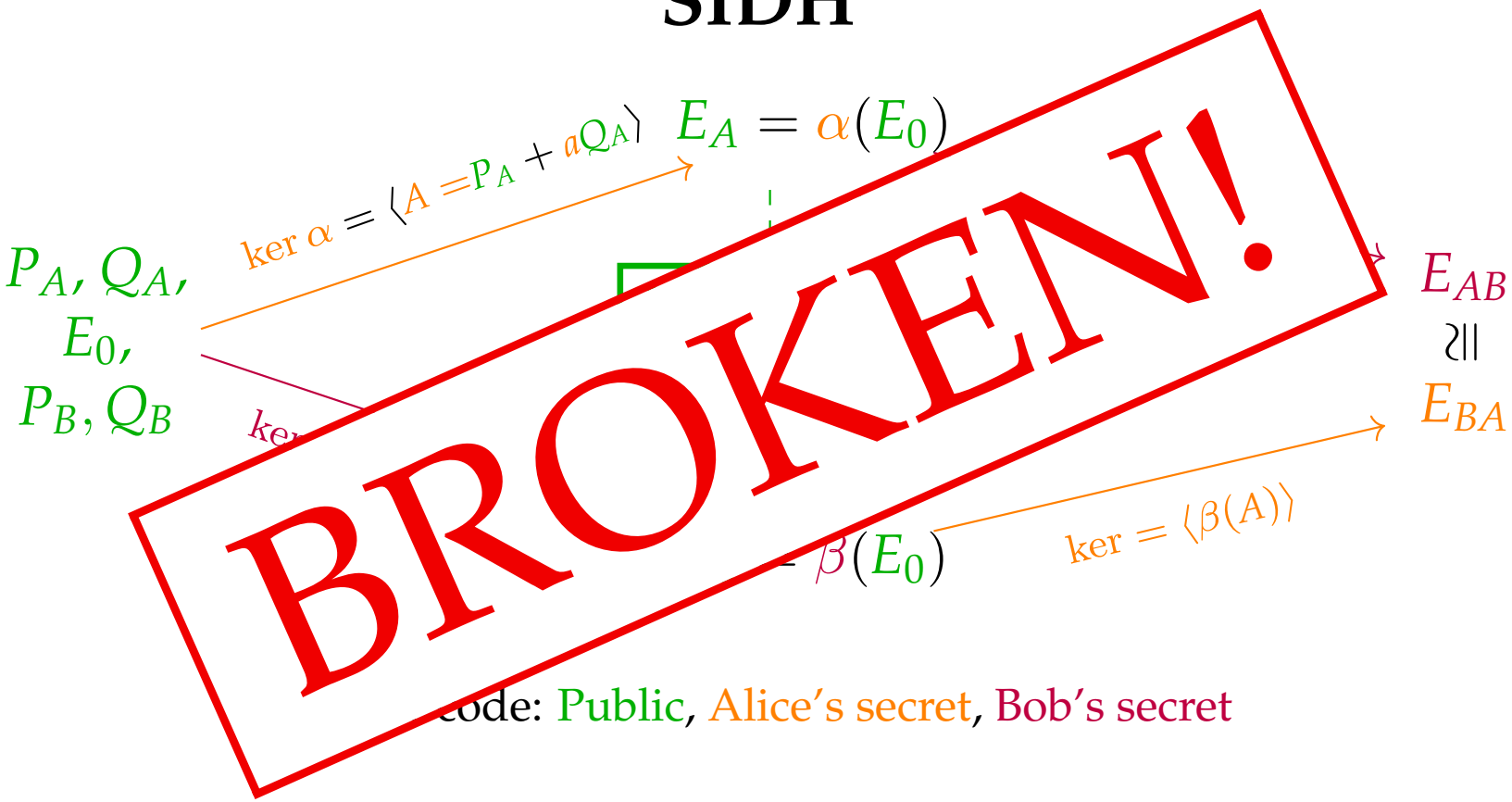
SIDH



Colour code: Public, Alice's secret, Bob's secret

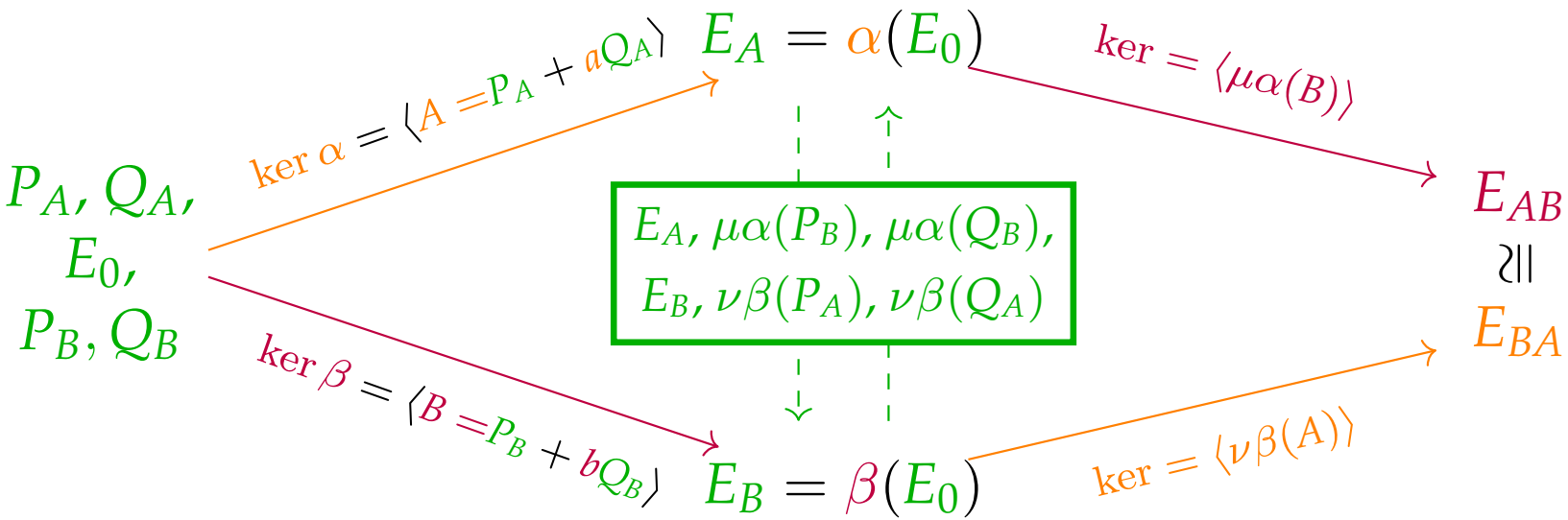
M-SIDH Fouotsa, Moriya, Petit '22

SIDH



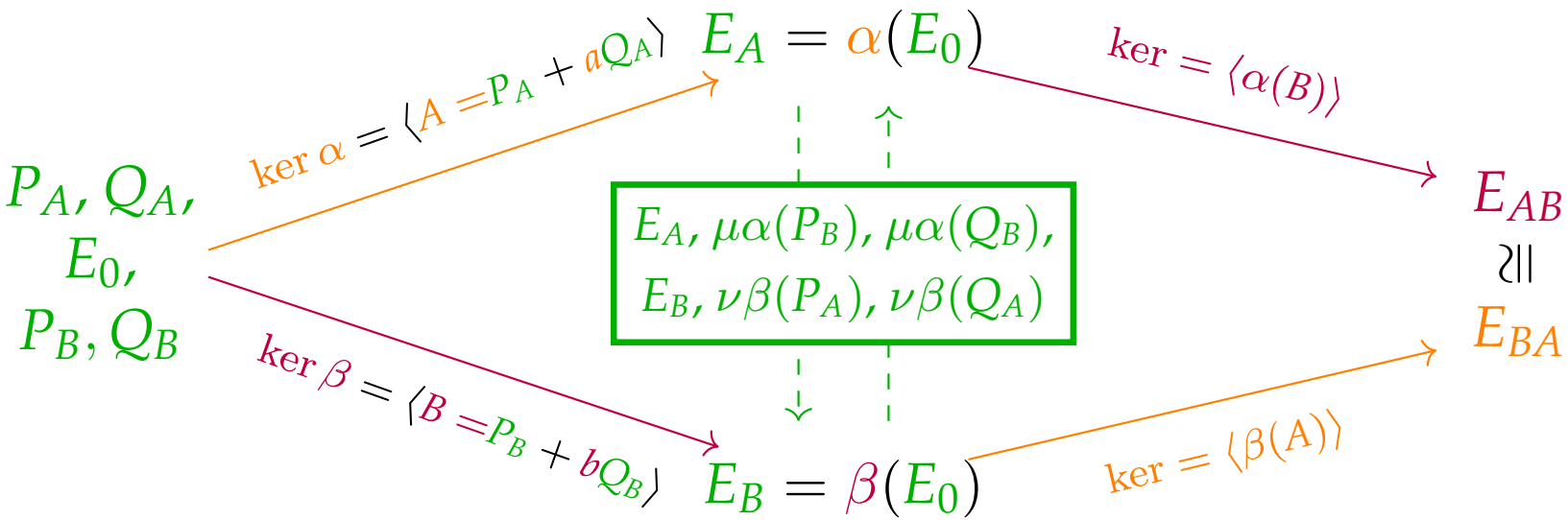
code: Public, Alice's secret, Bob's secret

M-SIDH



Colour code: Public, Alice's secret, Bob's secret

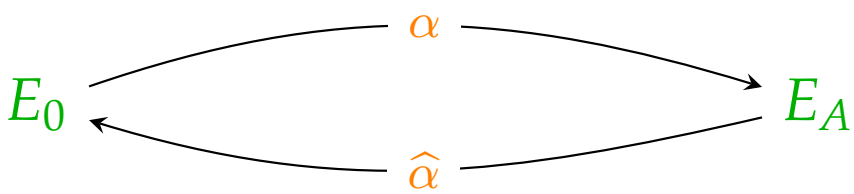
M-SIDH



Colour code: Public, Alice's secret, Bob's secret

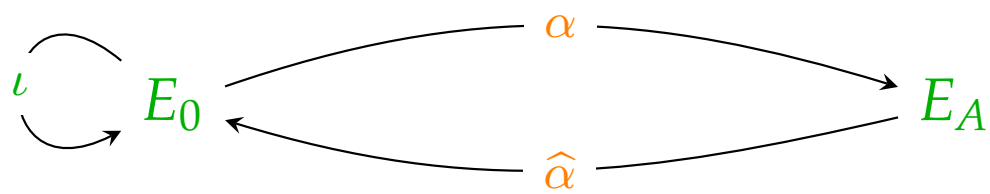
Petit vs. SIDH: torsion points to isogenies

Finding the secret isogeny α of known degree, given $\alpha|_{E_0[B]}$.



Petit vs. SIDH: torsion points to isogenies

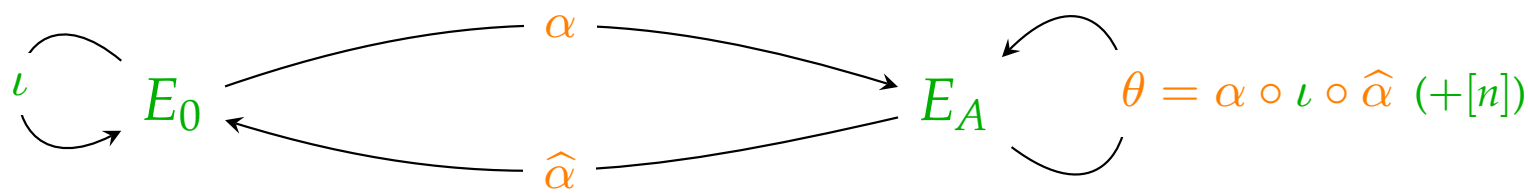
Finding the secret isogeny α of known degree, given $\alpha|_{E_0[B]}$.



1. Restriction # 1: Assume we can choose $\iota : E_0 \to E_0$.

Petit vs. SIDH: torsion points to isogenies

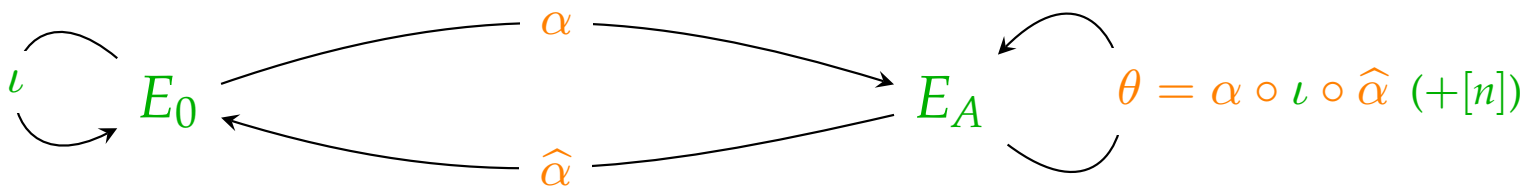
Finding the secret isogeny α of known degree, given $\alpha|_{E_0[B]}$.



1. Restriction # 1: Assume we can choose $\iota : E_0 \to E_0$.
2. Know $\alpha|_{E_0[B]}$ (and $\widehat{\alpha}|_{E_A[B]}$) from public torsion points.

Petit vs. SIDH: torsion points to isogenies

Finding the secret isogeny α of known degree, given $\alpha|_{E_0[B]}$.

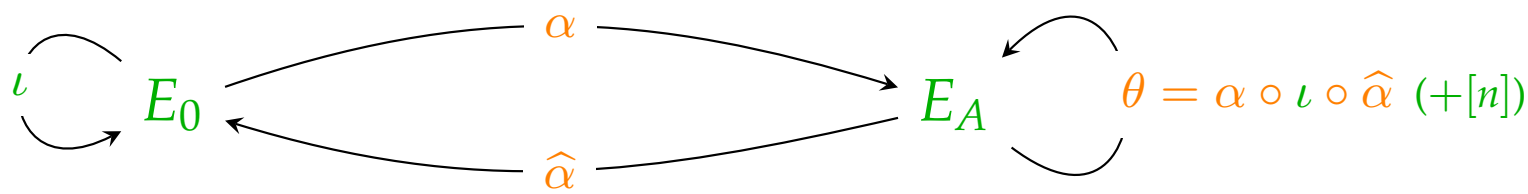


1. Restriction # 1: Assume we can choose $\iota : E_0 \to E_0$.
2. Know $\alpha|_{E_0[B]}$ (and $\widehat{\alpha}|_{E_A[B]}$) from public torsion points.
3. Restriction # 2: $\deg(\theta) = \epsilon B^2$.

$$(1) + (2) + (3) \rightsquigarrow \alpha.$$

Petit vs. SIDH: torsion points to isogenies

Finding the secret isogeny α of known degree, given $\alpha|_{E_0[B]}$.



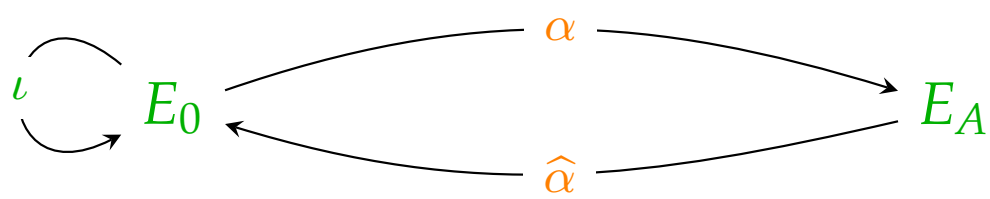
1. Restriction # 1: Assume we can choose $\iota : E_0 \to E_0$.
2. Know $\alpha|_{E_0[B]}$ (and $\widehat{\alpha}|_{E_A[B]}$) from public torsion points.
3. Restriction # 2: $\deg(\theta) = \epsilon B^2$.

$$(1) + (2) + (3) \rightsquigarrow \alpha.$$

Restriction # 2 $\Rightarrow B > \deg(\alpha)^2$. Problem!

Kani vs. SIDH: torsion points to isogenies

Finding the secret isogeny α of known degree, given $\alpha|_{E_0[B]}$.



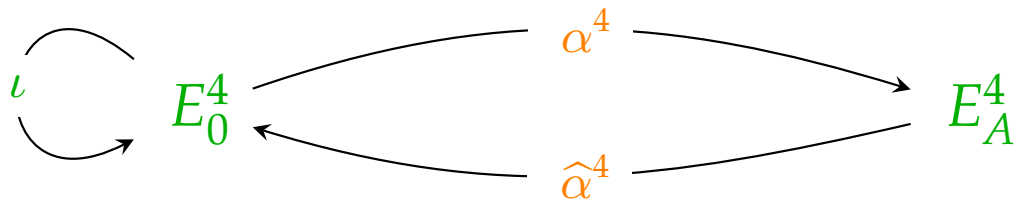
1. Restriction # 1: Assume we can choose $\iota : E_0 \to E_0$.
2. Know $\alpha|_{E_0[B]}$ (and $\widehat{\alpha}|_{E_A[B]}$) from public torsion points.
3. Restriction # 2: ι a $(B - \deg(\alpha))$-isogeny.

$$(1) + (2) + (3) \rightsquigarrow \alpha.$$

Restriction # 2 $\Rightarrow B > \deg(\alpha)$. ~~Problem!~~

Robert vs. SIDH: torsion points to isogenies

Finding the secret isogeny α of known degree, given $\alpha|_{E_0[B]}$.



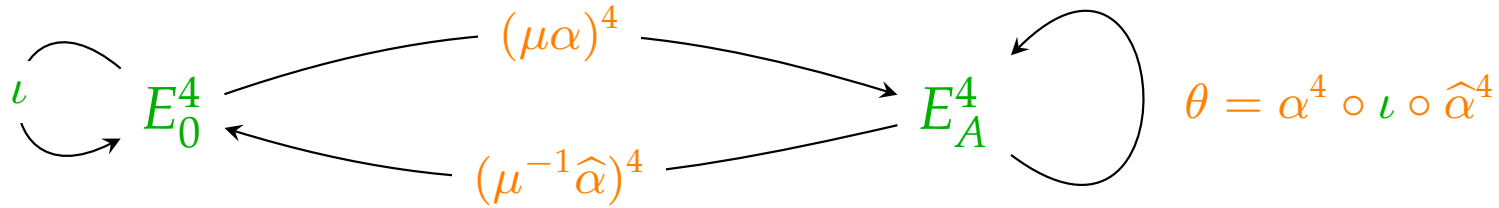
1. ~~Restriction # 1: Assume~~ we can choose $\iota : E_0^4 \to E_0^4$.
2. Know $\alpha|_{E_0[B]}$ (and $\widehat{\alpha}|_{E_A[B]}$) from public torsion points.
3. Restriction # 2: ι a $(B - \deg(\alpha))$-isogeny.

$$(1) + (2) + (3) \rightsquigarrow \alpha.$$

Restriction # 2 $\Rightarrow B > \deg(\alpha)$. ~~Problem!~~

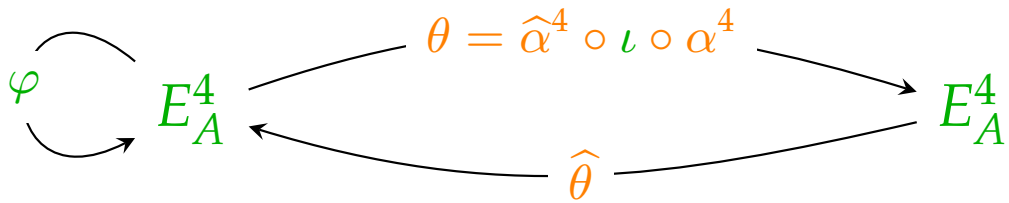
Kani+ vs. M-SIDH: masked points to isogenies

Finding the secret isogeny α of known degree, given $\mu\alpha|_{E_0[B]}$.



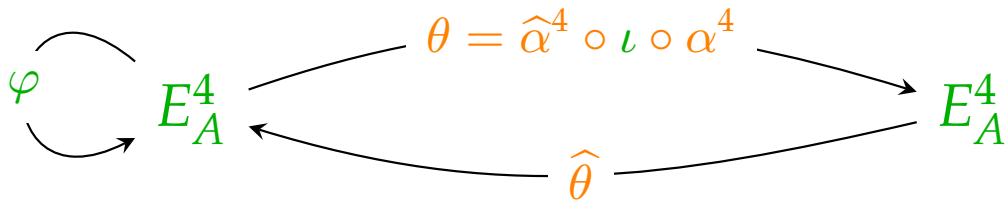
Kani+ vs. M-SIDH: masked points to isogenies

Finding the secret isogeny α of known degree, given $\mu\alpha|_{E_0[B]}$.



Kani+ vs. M-SIDH: masked points to isogenies

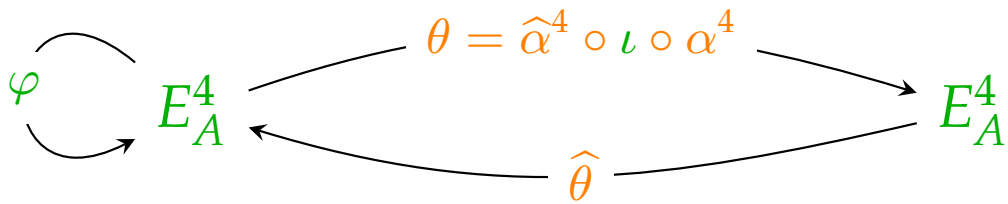
Finding the secret isogeny α of known degree, given $\mu\alpha|_{E_0[B]}$.



1. Restriction # 1: assume we can choose $\iota \in \mathrm{End}(E_0^4)$ that doesn't commute with α^4.

Kani+ vs. M-SIDH: masked points to isogenies

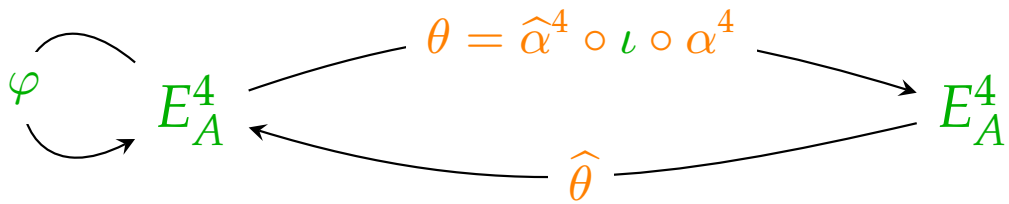
Finding the secret isogeny α of known degree, given $\mu\alpha|_{E_0[B]}$.



1. Restriction # 1: assume we can choose $\iota \in \mathrm{End}(E_0^4)$ that doesn't commute with α^4.
2. We can choose $\varphi : E_A^4 \to E_A^4$.

Kani+ vs. M-SIDH: masked points to isogenies

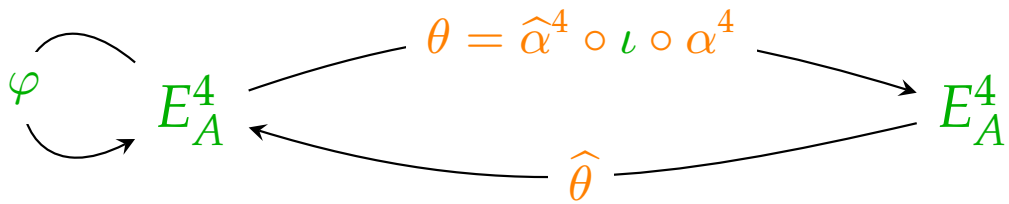
Finding the secret isogeny α of known degree, given $\mu\alpha|_{E_0[B]}$.



1. Restriction # 1: assume we can choose $\iota \in \mathrm{End}(E_0^4)$ that doesn't commute with α^4.
2. We can choose $\varphi : E_A^4 \to E_A^4$.
3. Know $\theta|_{E_A[B]}$ (and $\widehat{\theta}|_{E_A[B]}$) from public torsion points.

Kani+ vs. M-SIDH: masked points to isogenies

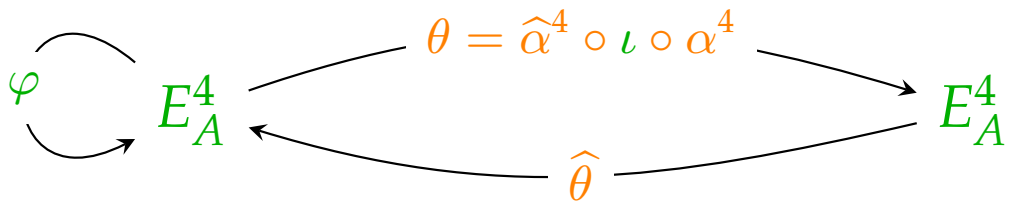
Finding the secret isogeny α of known degree, given $\mu\alpha|_{E_0[B]}$.



1. Restriction # 1: assume we can choose $\iota \in \mathrm{End}(E_0^4)$ that doesn't commute with α^4.
2. We can choose $\varphi : E_A^4 \to E_A^4$.
3. Know $\theta|_{E_A[B]}$ (and $\widehat{\theta}|_{E_A[B]}$) from public torsion points.
4. Restriction # 2: $B > A\sqrt{\deg \iota}$.

Kani+ vs. M-SIDH: masked points to isogenies

Finding the secret isogeny α of known degree, given $\mu\alpha|_{E_0[B]}$.



1. Restriction # 1: assume we can choose $\iota \in \mathrm{End}(E_0^4)$ that doesn't commute with α^4.
2. We can choose $\varphi : E_A^4 \to E_A^4$.
3. Know $\theta|_{E_A[B]}$ (and $\widehat{\theta}|_{E_A[B]}$) from public torsion points.
4. Restriction # 2: $B > A\sqrt{\deg \iota}$.

$$(1) + (2) + (3) + (4) \rightsquigarrow \alpha.$$

Barriers to breaking M-SIDH

Problem: Attack needs small, nontrivial, known $\iota \in \mathrm{End}(E_0^4)$.

Barriers to breaking M-SIDH

Problem: Attack needs small, nontrivial, known $\iota \in \mathrm{End}(E_0^4)$.

$\rightsquigarrow$ Questions:

- How many dim 4 varieties have small nontrivial endomorphisms?

Barriers to breaking M-SIDH

Problem: Attack needs small, nontrivial, known $\iota \in \mathrm{End}(E_0^4)$.

$\rightsquigarrow$ Questions:

- How many dim 4 varieties have small nontrivial endomorphisms?
- Increase dimension again $\rightsquigarrow$ more small endomorphisms?

Barriers to breaking M-SIDH

Problem: Attack needs small, nontrivial, known $\iota \in \mathrm{End}(E_0^4)$.

$\rightsquigarrow$ Questions:

- How many dim 4 varieties have small nontrivial endomorphisms?
- Increase dimension again $\rightsquigarrow$ more small endomorphisms?
- Non-principal polarizations?

Barriers to breaking M-SIDH

Problem: Attack needs small, nontrivial, known $\iota \in \mathrm{End}(E_0^4)$.

$\rightsquigarrow$ Questions:

- How many dim 4 varieties have small nontrivial endomorphisms?
- Increase dimension again $\rightsquigarrow$ more small endomorphisms?
- Non-principal polarizations?
- Isogeny computation feasible as dimension grows?

What is known: endomorphism rings

- All varieties A so far were isogenous to E^g, with E supersingular.

What is known: endomorphism rings

- All varieties A so far were isogenous to E^g, with E supersingular.
  That makes A supersingular.

What is known: endomorphism rings

- All varieties A so far were isogenous to E^g, with E supersingular.
  That makes A supersingular.
- E supersingular $\Leftrightarrow \mathrm{End}(E) \otimes \mathbb{Q} \cong B_{p,\infty}$, a quaternion algebra.

What is known: endomorphism rings

- All varieties A so far were isogenous to E^g, with E supersingular.
  That makes A supersingular.
- E supersingular $\Leftrightarrow \mathrm{End}(E) \otimes \mathbb{Q} \cong B_{p,\infty}$, a quaternion algebra.
- A of dim g supersingular $\Leftrightarrow \mathrm{End}(A) \otimes \mathbb{Q} \cong \mathrm{Mat}_{g\times g}(B_{p,\infty})$.

What is known: endomorphism rings

- All varieties A so far were isogenous to E^g, with E supersingular.
  That makes A supersingular.
- E supersingular $\Leftrightarrow \mathrm{End}(E) \otimes \mathbb{Q} \cong B_{p,\infty}$, a quaternion algebra.
- A of dim g supersingular $\Leftrightarrow \mathrm{End}(A) \otimes \mathbb{Q} \cong \mathrm{Mat}_{g\times g}(B_{p,\infty})$.
  Warning: ignores polarizations.

What is known: endomorphism rings

- All varieties A so far were isogenous to E^g, with E supersingular.
  That makes A supersingular.
- E supersingular $\Leftrightarrow \mathrm{End}(E) \otimes \mathbb{Q} \cong B_{p,\infty}$, a quaternion algebra.
- A of dim g supersingular $\Leftrightarrow \mathrm{End}(A) \otimes \mathbb{Q} \cong \mathrm{Mat}_{g\times g}(B_{p,\infty})$.
  Warning: ignores polarizations.

Let $A = E^g$. The principally polarized endomorphisms of A are

$$\{M \in \mathrm{Mat}_{g\times g}(\mathrm{End}(E)) : M^t M \in \mathbb{Z}I\}.$$

What is known: endomorphism rings

- All varieties A so far were isogenous to E^g, with E supersingular.
  That makes A supersingular.
- E supersingular $\Leftrightarrow \mathrm{End}(E) \otimes \mathbb{Q} \cong B_{p,\infty}$, a quaternion algebra.
- A of dim g supersingular $\Leftrightarrow \mathrm{End}(A) \otimes \mathbb{Q} \cong \mathrm{Mat}_{g\times g}(B_{p,\infty})$.
  Warning: ignores polarizations.

Let $A = E^g$. The principally polarized endomorphisms of A are

$$\{M \in \mathrm{Mat}_{g\times g}(\mathrm{End}(E)) : M^t M \in \mathbb{Z}I\}.$$

Example: when $g = 2$

$$M = \begin{pmatrix} a & -\iota \\ \widehat{\iota} & b \end{pmatrix},$$

with $a, b \in \mathbb{Z}$ and $\iota \in \mathrm{End}(E) \subseteq B_{p,\infty}$.

Barriers to breaking M-SIDH

Recall:

Problem: Attack needs small, nontrivial, known $\iota \in \mathrm{End}(E_0^4)$.

$\rightsquigarrow$ Questions:

- How many dim 4 varieties have small nontrivial endomorphisms?
- Increase dimension again $\rightsquigarrow$ more small endomorphisms?

What is known: endomorphism (sub)rings

Idea # 1: orient by small, nontrivial $\iota \in \mathrm{End}(E_0^g)$. (c.f. Colò-Kohel)

What is known: endomorphism (sub)rings

Idea # 1: orient by small, nontrivial $\iota \in \mathrm{End}(E_0^g)$. (c.f. Colò-Kohel)

- Does there exist ι such that many supersingular dim g $\mathrm{End}(A) \supseteq \mathbb{Z}[\iota, \bar{\iota}]$?

What is known: endomorphism (sub)rings

Idea # 1: orient by small, nontrivial $\iota \in \mathrm{End}(E_0^g)$. (c.f. Colò-Kohel)

- Does there exist ι such that many supersingular dim g $\mathrm{End}(A) \supseteq \mathbb{Z}[\iota, \bar{\iota}]$?
  i.e. such that the isogeny subgraph oriented by $\iota, \bar{\iota}$ is large?

What is known: endomorphism (sub)rings

Idea # 1: orient by small, nontrivial $\iota \in \mathrm{End}(E_0^g)$. (c.f. Colò-Kohel)

- Does there exist ι such that many supersingular dim g $\mathrm{End}(A) \supseteq \mathbb{Z}[\iota, \bar{\iota}]$?
  i.e. such that the isogeny subgraph oriented by $\iota, \bar{\iota}$ is large?
- Now: What are these isogeny subgraphs?

What is known: isogenies in g dimensions

Recall:

Definition

$f : E \to E'$ an isogeny of elliptic curves $/\mathbb{F}_{p^n}$. $p \neq \ell$ prime.

If $\ker(f) \cong \mathbb{Z}/\ell\mathbb{Z}$, we call f an ℓ-isogeny.

If f an ℓ-isogeny, then $f^\vee \circ f = [\ell]$.

What is known: isogenies in g dimensions

Definition

$f : A \to A'$ an isogeny of g-dimensional principally polarized abelian varieties $/\mathbb{F}_{p^n}$. $p \neq \ell$ prime.

If $\ker(f) \cong \underbrace{\mathbb{Z}/\ell\mathbb{Z} \times \cdots \times \mathbb{Z}/\ell\mathbb{Z}}_{g \text{ times}}$ and $f^\vee \circ f = [\ell]$ and f respects polarizations we call f an ℓ-isogeny or $(\ell, \ldots, \ell)$-isogeny.

What is known: isogenies in g dimensions

Definition

$f : A \to A'$ an isogeny of g-dimensional principally polarized abelian varieties $/\mathbb{F}_{p^n}$. $p \neq \ell$ prime.

If $\ker(f) \cong \underbrace{\mathbb{Z}/\ell\mathbb{Z} \times \cdots \times \mathbb{Z}/\ell\mathbb{Z}}_{g \text{ times}}$ and $f^\vee \circ f = [\ell]$ and f respects polarizations we call f an ℓ-isogeny or $(\ell, \ldots, \ell)$-isogeny.

$\deg(f) = \ell^g \rightsquigarrow$

Question: isogenies of degree ℓ when $g > 1$?

What is known: isogenies in g dimensions

Example: The Jacobian $\mathrm{Jac}(C)$ of $C/\mathbb{F}_{17} : y^2 = x^6 + 2x + 1$.
$\mu = \frac{5+\sqrt{5}}{2} \in \mathrm{End}(\mathrm{Jac}(C))$.

What is known: isogenies in g dimensions

Example: The Jacobian $\mathrm{Jac}(C)$ of $C/\mathbb{F}_{17} : y^2 = x^6 + 2x + 1$.
$\mu = \frac{5+\sqrt{5}}{2} \in \mathrm{End}(\mathrm{Jac}(C))$.

- The kernel of a $(5,5)$-isogeny from $\mathrm{Jac}(C)$ is isomorphic to $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ and is generated by

$$P \in \mathrm{Jac}(C)[5] \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}.$$

What is known: isogenies in g dimensions

Example: The Jacobian $\mathrm{Jac}(C)$ of $C/\mathbb{F}_{17} : y^2 = x^6 + 2x + 1$.
$\mu = \frac{5+\sqrt{5}}{2} \in \mathrm{End}(\mathrm{Jac}(C))$.

- The kernel of a $(5,5)$-isogeny from $\mathrm{Jac}(C)$ is isomorphic to $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ and is generated by

$$P \in \mathrm{Jac}(C)[5] \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}.$$

- The kernel of a cyclic μ-isogeny f from $\mathrm{Jac}(C)$ is isomorphic to $\mathbb{Z}/5\mathbb{Z}$ (hence is cyclic!) and is generated by

$$P \in \mathrm{Jac}(C)[\mu] \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}.$$

What is known: isogenies in g dimensions

Example: The Jacobian $\mathrm{Jac}(C)$ of $C/\mathbb{F}_{17} : y^2 = x^6 + 2x + 1$.
$\mu = \frac{5+\sqrt{5}}{2} \in \mathrm{End}(\mathrm{Jac}(C))$.

- The kernel of a $(5,5)$-isogeny from $\mathrm{Jac}(C)$ is isomorphic to $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ and is generated by

$$P \in \mathrm{Jac}(C)[5] \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}.$$

- The kernel of a cyclic μ-isogeny f from $\mathrm{Jac}(C)$ is isomorphic to $\mathbb{Z}/5\mathbb{Z}$ (hence is cyclic!) and is generated by

$$P \in \mathrm{Jac}(C)[\mu] \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}.$$

- This isogeny satisfies $f^\vee \circ f = [\mu]$ (up to polarisation-isomorphisms).

What is known: isogenies in g dimensions

Example: The Jacobian $\mathrm{Jac}(C)$ of $C/\mathbb{F}_{17} : y^2 = x^6 + 2x + 1$.
$\mu = \frac{5+\sqrt{5}}{2} \in \mathrm{End}(\mathrm{Jac}(C))$.

- The kernel of a $(5,5)$-isogeny from $\mathrm{Jac}(C)$ is isomorphic to $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ and is generated by

$$P \in \mathrm{Jac}(C)[5] \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}.$$

- The kernel of a cyclic μ-isogeny f from $\mathrm{Jac}(C)$ is isomorphic to $\mathbb{Z}/5\mathbb{Z}$ (hence is cyclic!) and is generated by

$$P \in \mathrm{Jac}(C)[\mu] \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}.$$

- This isogeny satisfies $f^\vee \circ f = [\mu]$ (up to polarisation-isomorphisms).

Do these isogenies always exist?

What is known: isogenies in g dimensions

- Let $A/\mathbb{F}_q$ be a g-dimensional principally polarised abelian variety, let $\iota \in \mathrm{End}(A)$ such that $\mathbb{Q}(\iota)$ is a degree $2g$ CM-field K

What is known: isogenies in g dimensions

- Let $A/\mathbb{F}_q$ be a g-dimensional principally polarised abelian variety, let $\iota \in \mathrm{End}(A)$ such that $\mathbb{Q}(\iota)$ is a degree $2g$ CM-field K

  (an imaginary quadratic extension of a totally real number field K_0).

What is known: isogenies in g dimensions

- Let $A/\mathbb{F}_q$ be a g-dimensional principally polarised abelian variety, let $\iota \in \mathrm{End}(A)$ such that $\mathbb{Q}(\iota)$ is a degree $2g$ CM-field K

  (an imaginary quadratic extension of a totally real number field K_0).

- Write $\mathcal{O}_{K_0}$ for the ring of integers of K_0. If:
  1. $\mu \in \mathcal{O}_{K_0}$ is a prime element and is totally positive (all embeddings are positive), $\mathrm{Norm}_{K_0/\mathbb{Q}}(\mu) = \ell$, and

What is known: isogenies in g dimensions

- Let $A/\mathbb{F}_q$ be a g-dimensional principally polarised abelian variety, let $\iota \in \mathrm{End}(A)$ such that $\mathbb{Q}(\iota)$ is a degree $2g$ CM-field K

  (an imaginary quadratic extension of a totally real number field K_0).

- Write $\mathcal{O}_{K_0}$ for the ring of integers of K_0. If:
  1. $\mu \in \mathcal{O}_{K_0}$ is a prime element and is totally positive (all embeddings are positive), $\mathrm{Norm}_{K_0/\mathbb{Q}}(\mu) = \ell$, and
  2. $\mathcal{O}_{K_0} \subseteq \mathrm{End}(A)$,

What is known: isogenies in g dimensions

- Let $A/\mathbb{F}_q$ be a g-dimensional principally polarised abelian variety, let $\iota \in \mathrm{End}(A)$ such that $\mathbb{Q}(\iota)$ is a degree $2g$ CM-field K

  (an imaginary quadratic extension of a totally real number field K_0).

- Write $\mathcal{O}_{K_0}$ for the ring of integers of K_0. If:
  1. $\mu \in \mathcal{O}_{K_0}$ is a prime element and is totally positive (all embeddings are positive), $\mathrm{Norm}_{K_0/\mathbb{Q}}(\mu) = \ell$, and
  2. $\mathcal{O}_{K_0} \subseteq \mathrm{End}(A)$,

  then $P \in A[\mu]$, $\mathrm{ord}(P) = \ell$
  $\rightsquigarrow$ cyclic isogeny f with $\ker(f) = \langle P \rangle$

Barriers to breaking M-SIDH

Recall:

- Problem: M-SIDH Attack needs small, nontrivial, known $\iota \in \mathrm{End}(E_0^4)$.
- Idea # 1: orient by small, nontrivial, known $\iota \in \mathrm{End}(E_0^g)$.

Barriers to breaking M-SIDH

Recall:

- Problem: M-SIDH Attack needs small, nontrivial, known $\iota \in \mathrm{End}(E_0^4)$.
- Idea # 1: orient by small, nontrivial, known $\iota \in \mathrm{End}(E_0^g)$.
- What are the oriented isogeny graphs of abelian varieties A with $\iota \in \mathrm{End}(A)$?

What is known*: oriented isogeny subgraphs

Recall:
An ℓ-isogeny graph of elliptic curves $/k$ has:

- Vertices: Elliptic curves E/k (up to isomorphism).
- Edges: An edge $E - E'$ represents an ℓ-isogeny $E \to E'$ and its dual (up to isomorphism).

What is known*: oriented isogeny subgraphs

An $(\ell, \ldots, \ell)$-isogeny (resp. cyclic μ-isogeny) graph of abelian varieties $/k$ satisfying property P [1] has:

- Vertices: Abelian varieties A/k satisying P (up to P-preserving-isomorphism).
- Edges: An edge $A - A'$ represents an P-preserving $(\ell, \ldots, \ell)$-isogeny (resp. cyclic μ-isogeny) $A \to A'$ and its dual (up to P-preserving-isomorphism).

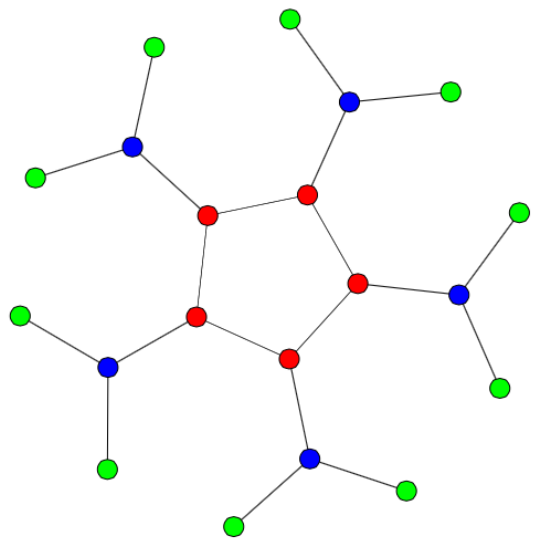
[1] This property should include that abelian varieties are isomorphic to their duals

What is known*: oriented isogeny subgraphs

Recall:

Theorem ([K96])

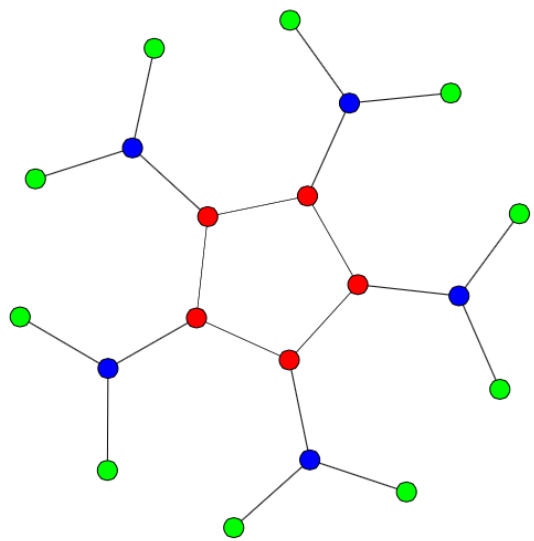
Let $E/\mathbb{F}_q$ be an ordinary elliptic curve such that $j(E) \neq 0, 1728$, and let $p \neq \ell \in \mathbb{Z}$ be a prime. Then the connected component of the ℓ-isogeny graph containing E is a volcano.



What is known*: oriented isogeny subgraphs

Theorem ([BJW17]* / [M18]*)

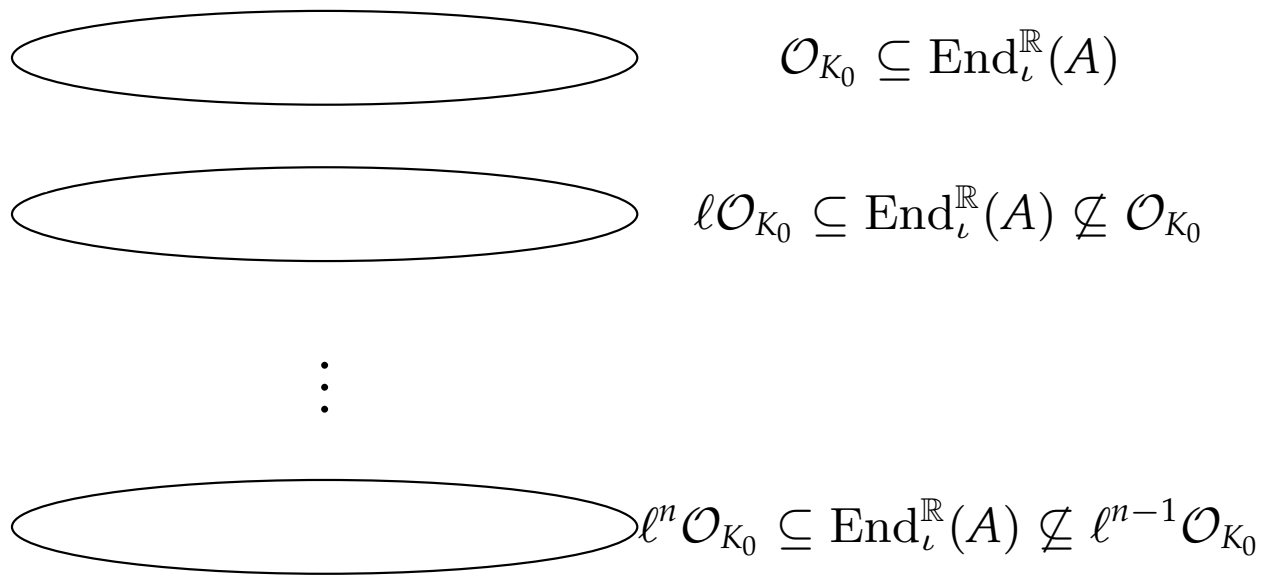
Let $A/\mathbb{F}_q$ be a principally polarised abelian variety, ι, μ as before (modulo technical conditions) If $\mathcal{O}_{K_0} \subseteq \mathrm{End}(A)$, then the connected component of the ι-oriented cyclic μ-isogeny graph containing A is a volcano.



What is known*: oriented isogeny subgraphs

Connected component of ι-oriented $(\ell, \ldots, \ell)$-isogeny graph of a principally polarised abelian variety over $\mathbb{F}_q$:

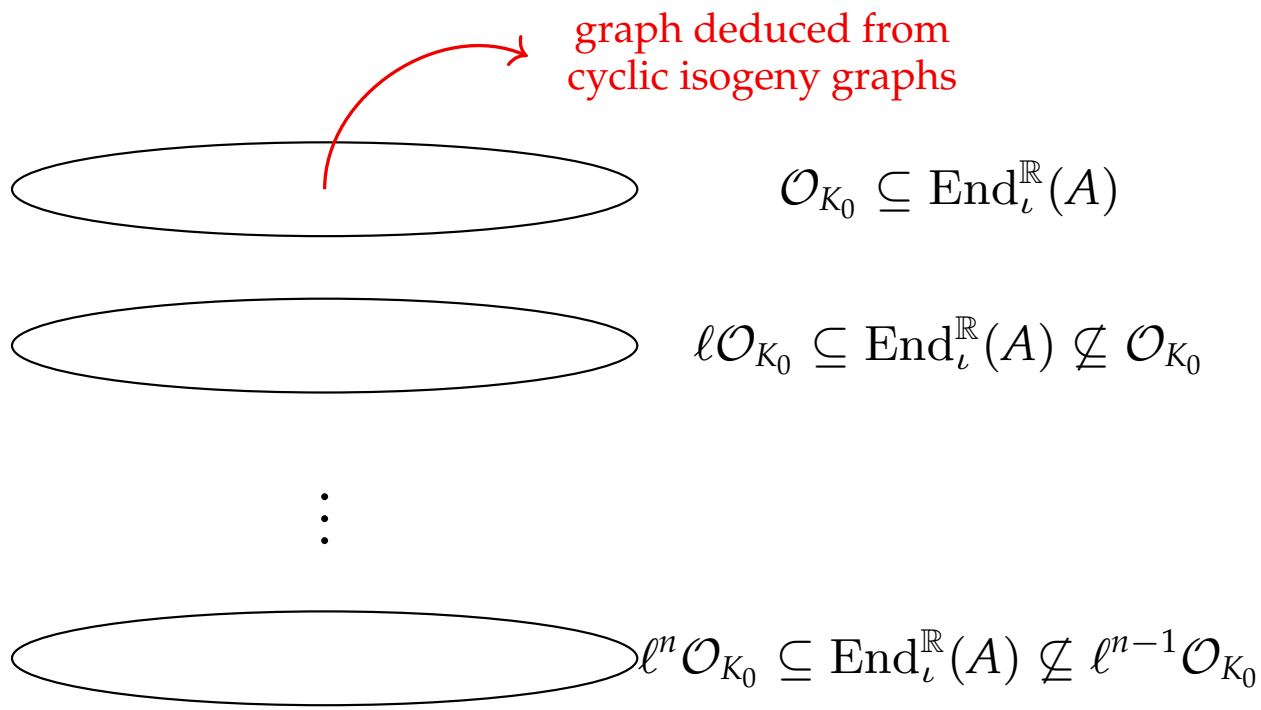
$\mathrm{End}_\iota^{\mathbb{R}}(A)$ is the real part of $\mathrm{End}(A) \cap \mathbb{Q}(\iota)$.



What is known*: oriented isogeny subgraphs

Connected component of ι-oriented $(\ell, \ldots, \ell)$-isogeny graph of a principally polarised abelian variety over $\mathbb{F}_q$:

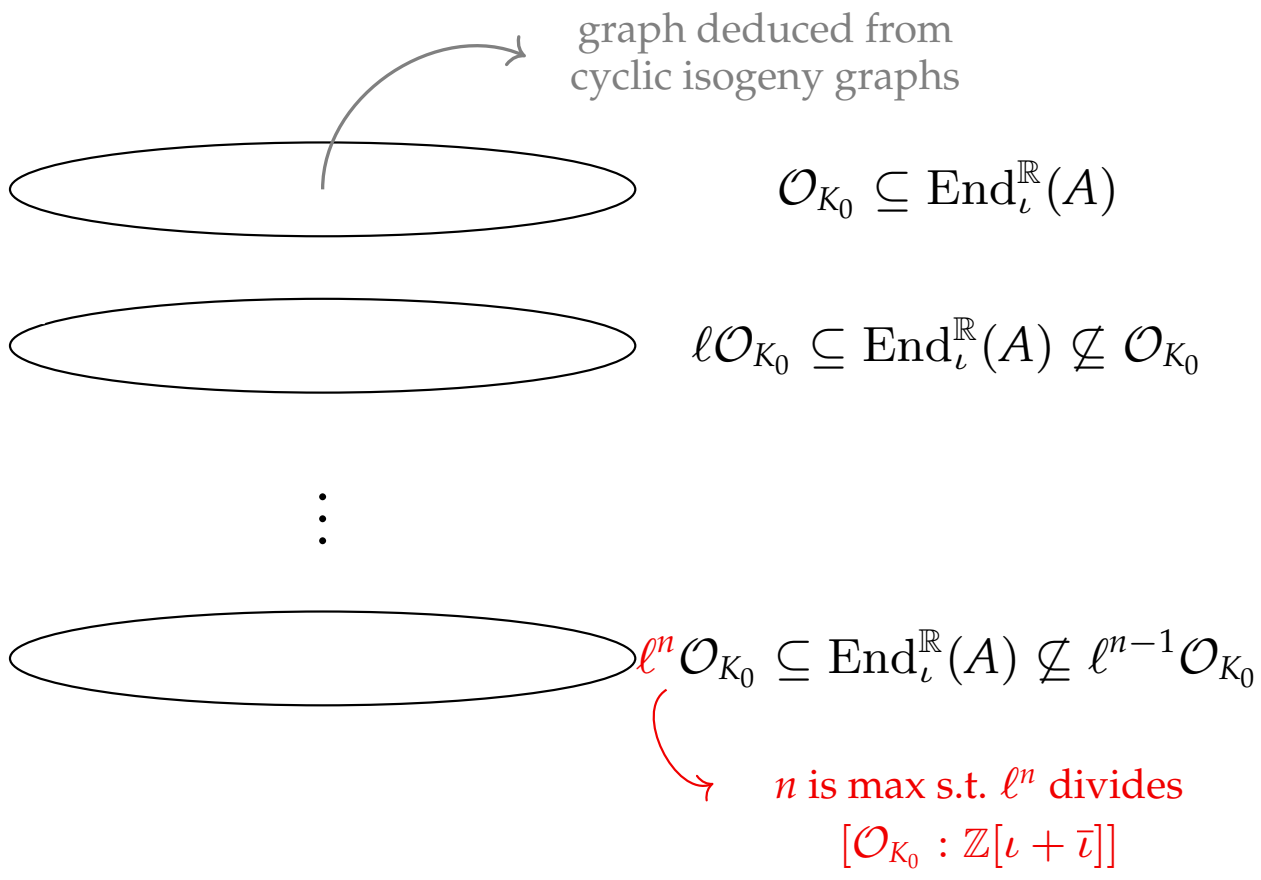
$\mathrm{End}_\iota^{\mathbb{R}}(A)$ is the real part of $\mathrm{End}(A) \cap \mathbb{Q}(\iota)$.



What is known*: oriented isogeny subgraphs

Connected component of ι-oriented $(\ell, \ldots, \ell)$-isogeny graph of a principally polarised abelian variety over $\mathbb{F}_q$:

$\mathrm{End}_\iota^{\mathbb{R}}(A)$ is the real part of $\mathrm{End}(A) \cap \mathbb{Q}(\iota)$.

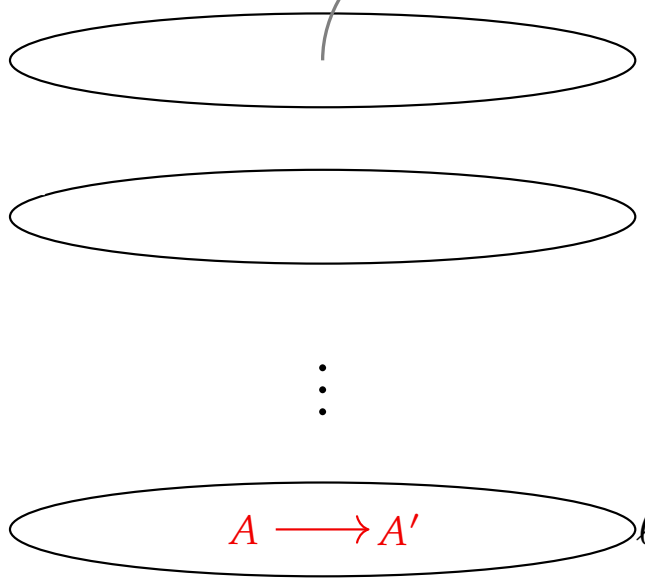


What is known*: oriented isogeny subgraphs

Connected component of ι-oriented $(\ell, \ldots, \ell)$-isogeny graph of a principally polarised abelian variety over $\mathbb{F}_q$:

$\mathrm{End}_\iota^{\mathbb{R}}(A)$ is the real part of $\mathrm{End}(A) \cap \mathbb{Q}(\iota)$.

graph deduced from cyclic isogeny graphs



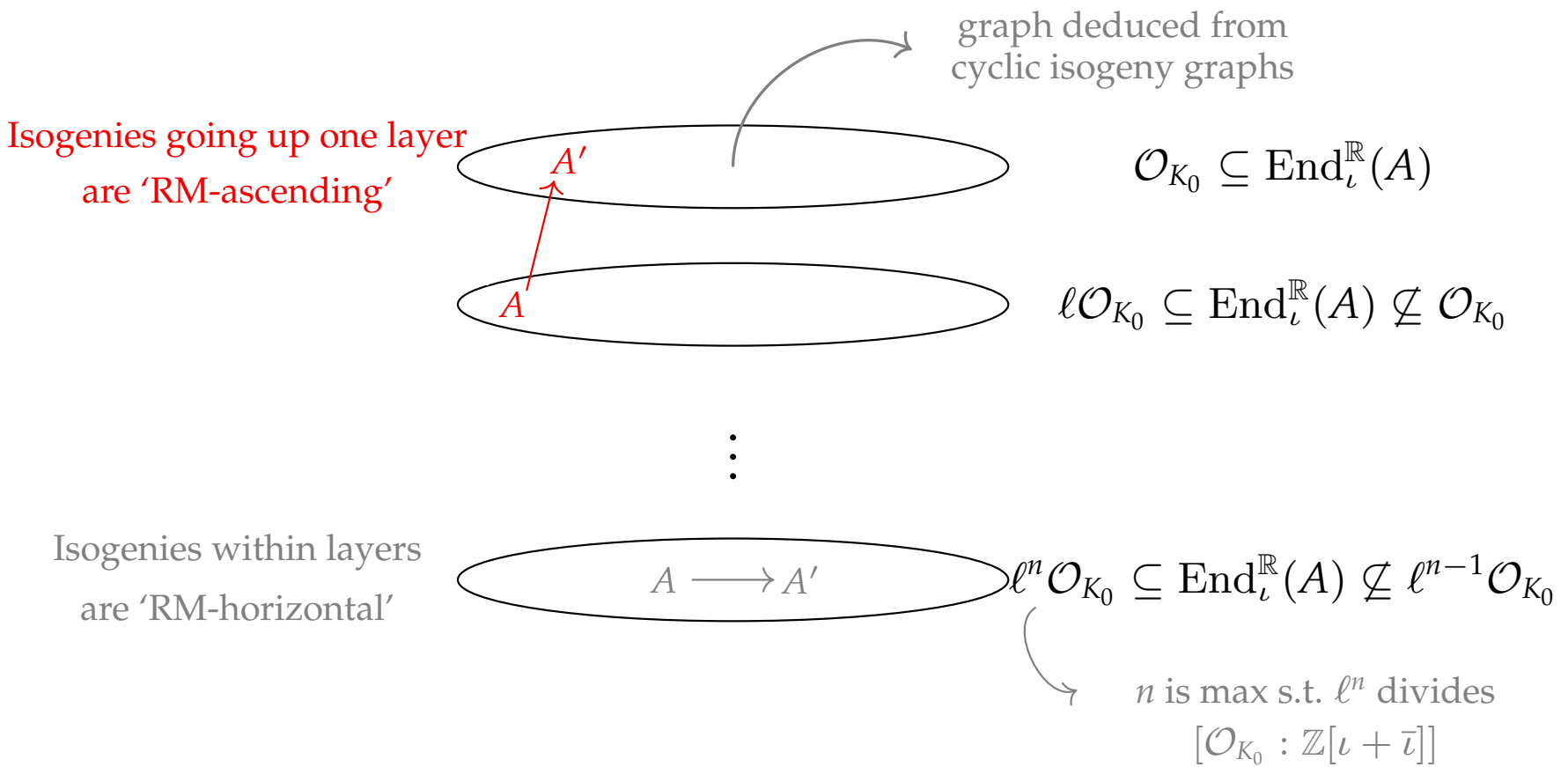
Isogenies within layers are 'RM-horizontal'

n is max s.t. ℓ^n divides $[\mathcal{O}_{K_0} : \mathbb{Z}[\iota + \bar{\iota}]]$

What is known*: oriented isogeny subgraphs

Connected component of ι-oriented $(\ell, \ldots, \ell)$-isogeny graph of a principally polarised abelian variety over $\mathbb{F}_q$:

$\mathrm{End}_\iota^{\mathbb{R}}(A)$ is the real part of $\mathrm{End}(A) \cap \mathbb{Q}(\iota)$.



What is known*: oriented isogeny subgraphs

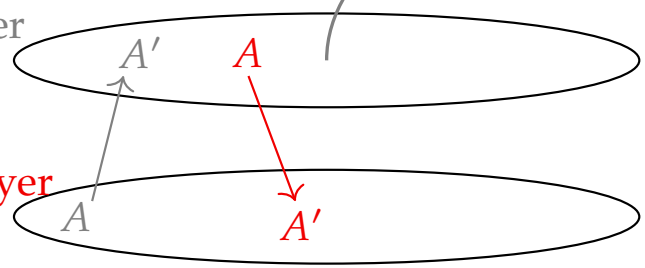
Connected component of ι-oriented $(\ell, \ldots, \ell)$-isogeny graph of a principally polarised abelian variety over $\mathbb{F}_q$:

$\mathrm{End}_\iota^{\mathbb{R}}(A)$ is the real part of $\mathrm{End}(A) \cap \mathbb{Q}(\iota)$.

graph deduced from cyclic isogeny graphs

Isogenies going up one layer are 'RM-ascending'

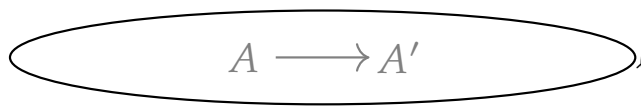
Isogenies going down one layer are 'RM-descending'



$\mathcal{O}_{K_0} \subseteq \mathrm{End}_\iota^{\mathbb{R}}(A)$

$\ell\mathcal{O}_{K_0} \subseteq \mathrm{End}_\iota^{\mathbb{R}}(A) \not\subseteq \mathcal{O}_{K_0}$

Isogenies within layers are 'RM-horizontal'



$\ell^n\mathcal{O}_{K_0} \subseteq \mathrm{End}_\iota^{\mathbb{R}}(A) \not\subseteq \ell^{n-1}\mathcal{O}_{K_0}$

n is max s.t. ℓ^n divides $[\mathcal{O}_{K_0} : \mathbb{Z}[\iota + \bar{\iota}]]$

What is known*: oriented isogeny subgraphs

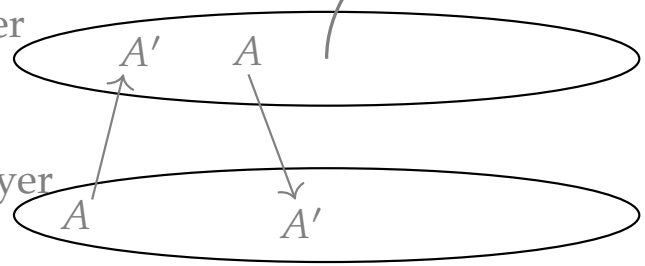
Connected component of ι-oriented $(\ell, \ldots, \ell)$-isogeny graph of a principally polarised abelian variety over $\mathbb{F}_q$:

$\mathrm{End}_\iota^{\mathbb{R}}(A)$ is the real part of $\mathrm{End}(A) \cap \mathbb{Q}(\iota)$.

graph deduced from cyclic isogeny graphs

Isogenies going up one layer are 'RM-ascending'

Isogenies going down one layer are 'RM-descending'

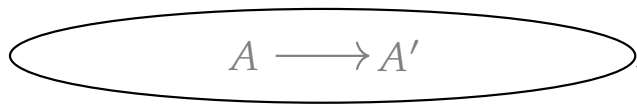


$\mathcal{O}_{K_0} \subseteq \mathrm{End}_\iota^{\mathbb{R}}(A)$

$\ell\mathcal{O}_{K_0} \subseteq \mathrm{End}_\iota^{\mathbb{R}}(A) \not\subseteq \mathcal{O}_{K_0}$

$\vdots$

Isogenies within layers are 'RM-horizontal'



$\ell^n\mathcal{O}_{K_0} \subseteq \mathrm{End}_\iota^{\mathbb{R}}(A) \not\subseteq \ell^{n-1}\mathcal{O}_{K_0}$

n is max s.t. ℓ^n divides $[\mathcal{O}_{K_0} : \mathbb{Z}[\iota + \bar{\iota}]]$

There is a unique RM-ascending ℓ-isogeny from every vertex not on the top layer.

What is known*: oriented isogeny subgraphs

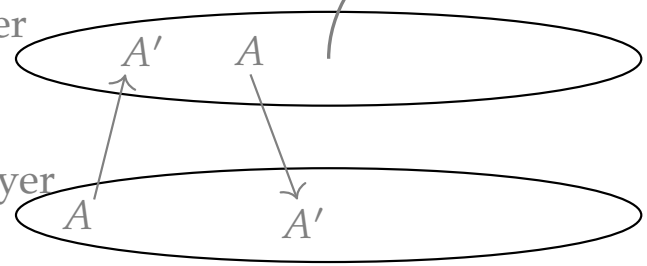
Connected component of ι-oriented $(\ell, \ldots, \ell)$-isogeny graph of a principally polarised abelian variety over $\mathbb{F}_q$:

$\mathrm{End}_\iota^{\mathbb{R}}(A)$ is the real part of $\mathrm{End}(A) \cap \mathbb{Q}(\iota)$.

graph deduced from cyclic isogeny graphs

Isogenies going up one layer are 'RM-ascending'

Isogenies going down one layer are 'RM-descending'

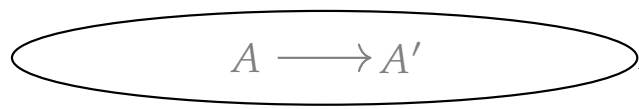


$\mathcal{O}_{K_0} \subseteq \mathrm{End}_\iota^{\mathbb{R}}(A)$

$\ell\mathcal{O}_{K_0} \subseteq \mathrm{End}_\iota^{\mathbb{R}}(A) \not\subseteq \mathcal{O}_{K_0}$

$\vdots$

Isogenies within layers are 'RM-horizontal'



$\ell^n\mathcal{O}_{K_0} \subseteq \mathrm{End}_\iota^{\mathbb{R}}(A) \not\subseteq \ell^{n-1}\mathcal{O}_{K_0}$

n is max s.t. ℓ^n divides $[\mathcal{O}_{K_0} : \mathbb{Z}[\iota + \bar{\iota}]]$

There is a unique RM-ascending ℓ-isogeny from every vertex not on the top layer.

The known meets the unknown

Recall Problem: M-SIDH Attack needs small, nontrivial, known $\iota \in \mathrm{End}(E_0^4)$.

- Idea # 1: orient by small, nontrivial, known $\iota \in \mathrm{End}(E_0^g)$. Does there exist ι such that the oriented isogeny subgraph is large?

The known meets the unknown

Recall Problem: M-SIDH Attack needs small, nontrivial, known $\iota \in \mathrm{End}(E_0^4)$.

- Idea # 1: orient by small, nontrivial, known $\iota \in \mathrm{End}(E_0^g)$. Does there exist ι such that the oriented isogeny subgraph is large?
  - Expectation: no (based on $g = 1$). But no known proof.

The known meets the unknown

Recall Problem: M-SIDH Attack needs small, nontrivial, known $\iota \in \mathrm{End}(E_0^4)$.

- Idea # 1: orient by small, nontrivial, known $\iota \in \mathrm{End}(E_0^g)$. Does there exist ι such that the oriented isogeny subgraph is large?
  - Expectation: no (based on $g = 1$). But no known proof.
  - Computing $(\ell, \ldots, \ell)$-isogenies for $g > 2$ very hard.

The known meets the unknown

Recall Problem: M-SIDH Attack needs small, nontrivial, known $\iota \in \mathrm{End}(E_0^4)$.

- Idea # 1: orient by small, nontrivial, known $\iota \in \mathrm{End}(E_0^g)$. Does there exist ι such that the oriented isogeny subgraph is large?
  - Expectation: no (based on $g = 1$). But no known proof.
  - Computing $(\ell, \ldots, \ell)$-isogenies for $g > 2$ very hard. Degree $= \ell^g$ so restricted to small dimension.

The known meets the unknown

Recall Problem: M-SIDH Attack needs small, nontrivial, known $\iota \in \mathrm{End}(E_0^4)$.

- Idea # 1: orient by small, nontrivial, known $\iota \in \mathrm{End}(E_0^g)$. Does there exist ι such that the oriented isogeny subgraph is large?
  - Expectation: no (based on $g = 1$). But no known proof.
  - Computing $(\ell, \ldots, \ell)$-isogenies for $g > 2$ very hard. Degree $= \ell^g$ so restricted to small dimension.
  - No working implementation of cyclic isogenies.

The known meets the unknown

Recall Problem: M-SIDH Attack needs small, nontrivial, known $\iota \in \mathrm{End}(E_0^4)$.

- Idea # 1: orient by small, nontrivial, known $\iota \in \mathrm{End}(E_0^g)$. Does there exist ι such that the oriented isogeny subgraph is large?
  - Expectation: no (based on $g = 1$). But no known proof.
  - Computing $(\ell, \ldots, \ell)$-isogenies for $g > 2$ very hard. Degree $= \ell^g$ so restricted to small dimension.
  - No working implementation of cyclic isogenies. But degree ℓ so more scalable?

The known meets the unknown

Recall Problem: M-SIDH Attack needs small, nontrivial, known $\iota \in \mathrm{End}(E_0^4)$.

- Idea # 1: orient by small, nontrivial, known $\iota \in \mathrm{End}(E_0^g)$. Does there exist ι such that the oriented isogeny subgraph is large?
  - Expectation: no (based on $g = 1$). But no known proof.
  - Computing $(\ell, \ldots, \ell)$-isogenies for $g > 2$ very hard. Degree $= \ell^g$ so restricted to small dimension.
  - No working implementation of cyclic isogenies. But degree ℓ so more scalable?
- Idea # 2: use nonprincipal endomorphisms.
  - No existing literature on computation.

Summary

- Lollipop + Kani applies to M-SIDH but needs small, nontrivial $\iota \in \mathrm{End}(E_0^g)$.

Summary

- Lollipop + Kani applies to M-SIDH but needs small, nontrivial $\iota \in \mathrm{End}(E_0^g)$.
- Most promising direction to removing this condition: nonprincipal polarizations.

Summary

- Lollipop + Kani applies to M-SIDH but needs small, nontrivial $\iota \in \mathrm{End}(E_0^g)$.
- Most promising direction to removing this condition: nonprincipal polarizations.
- Even theory currently out of reach.

Summary

- Lollipop + Kani applies to M-SIDH but needs small, nontrivial $\iota \in \mathrm{End}(E_0^g)$.
- Most promising direction to removing this condition: nonprincipal polarizations.
- Even theory currently out of reach.
- Some theory known about isogeny graphs in higher dimensions. Higher dimensions $\rightsquigarrow$ more isogeny subgraphs to exploit.

Summary

- Lollipop + Kani applies to M-SIDH but needs small, nontrivial $\iota \in \mathrm{End}(E_0^g)$.
- Most promising direction to removing this condition: nonprincipal polarizations.
- Even theory currently out of reach.
- Some theory known about isogeny graphs in higher dimensions. Higher dimensions $\rightsquigarrow$ more isogeny subgraphs to exploit.
  Potential application: easier isogeny problem?

Thank you!