

From ideals to modules for isogeny based cryptography

2024/09/13 — Leuven Isogeny Days 5

Damien Robert

Équipe Canari, Inria Bordeaux Sud-Ouest



université
de BORDEAUX

Inria

Why modules? (1)

Noisy linear algebra:

- Lattices: RingLWE \rightarrow ModuleLWE
- Codes: Hamming metric \rightarrow Sum Rank metric

Isogenies:

- Ideals \rightarrow Modules?
- Dimension 1 \rightarrow Dimension g ?
- Ideal equivalence of category \rightarrow module equivalence of category
- ☹ Increasing dimension in isogeny based cryptography is costly...

🌀🌀🌀 Work in progress! 🌀🌀🌀

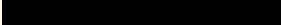
Why modules? (2)

- Kani: moving to dimension 2 (or 4) provided many new powerful algorithms
- So far only exploit isogenies between products of elliptic curves
- Hence still working via (representations of) dimension 1 isogenies
- Goal: exploit the full dimension 2 isogeny graph (or higher)

Why modules? (3)

- Abelian varieties are “scary” (even more than elliptic curves)
- Cryptographers need **abstractions**
- Example: LWE for lattice based cryptography
- **Good abstractions** in dimension 1: Deuring correspondance, class group actions
- But cannot incorporate Kani

This talk: new abstractions for higher dimensional isogenies

- Module correspondance
- ⇒ Isogeny based cryptography = **one way functor** from a **symmetric monoidal** category!
- In fact, this is a special type of one way functor, we actually have:
 (see later!)

Why modules? (4)

- Full (oriented) isogeny graph of E_0^g
- Ascending and descending isogenies
- Level structures
- Pairings
- (Un)forgetting orientations

Outline

1 Ideals

2 Modules

3 Applications to isogeny based cryptography

4 Advanced topics for modules

- Level structures
- Some isogeny constructions from the module point of view
- Ascending and descending isogenies: the conductor square and excision
- (Un)forgetting orientations via comonadic descent
- Non principal polarisations
- Sesquilinear Weil pairings
- Non R -backtracking isogenies

Table of Contents

1 Ideals

2 Modules

3 Applications to isogeny based cryptography

4 Advanced topics for modules

- Level structures
- Some isogeny constructions from the module point of view
- Ascending and descending isogenies: the conductor square and excision
- (Un)forgetting orientations via comonadic descent
- Non principal polarisations
- Sesquilinear Weil pairings
- Non R -backtracking isogenies

Ideals and isogenies: the oriented case

- $E_0/k, k = \mathbb{F}_{q^r}$ elliptic curve with a primitive orientation by a quadratic imaginary order $R = \mathbb{Z}[\sqrt{-\Delta}] \hookrightarrow \text{End}_k(E_0)$
- **Oriented isogeny:** $\phi : E_1 \rightarrow E_2$ that commutes with the orientations
- **Oriented kernel:** K stable by R

Unique R -orientation compatible on E/K with the quotient isogeny $E \rightarrow E/K$, and the isogeny is horizontal or ascending

Example: Frobenius orientation

- E_0/k with non trivial π_k -action: ordinary curves, supersingular curves over \mathbb{F}_p
- π_k -oriented isogenies = rational isogenies.

Kernels, isogenies, and ideals

- $I \mapsto \phi_I : E_0 \rightarrow E_I$ oriented isogeny with kernel $E_0[I] = \{P \in E_0(\bar{k}), \alpha(P) = 0 \forall \alpha \in I\}$
- $K \mapsto \mathfrak{I}(K) := \{\alpha \in R \mid \alpha(K) = 0\}$
- $I \rightarrow E_0[I] \Leftrightarrow K \mapsto \mathfrak{I}(K)$: bijections¹ between R -stable kernels and integral ideals I of R
- **Ideals \Leftrightarrow oriented isogenies**
- $I \sim J \Leftrightarrow E_I \simeq E_J$

¹At least in the separable case: $E_0[\pi_p]$ is not represented by an ideal if p inert in R

Class group actions

- $E_I := E_0/E_0[I]$ primitively oriented by $O(I) := \{\alpha \in R \otimes_{\mathbb{Z}} \mathbb{Q} \mid \alpha I \subset I\}$
- I is invertible $\Leftrightarrow O(I) = R \Leftrightarrow$ the isogeny is horizontal
- $\text{Pic}(R) := \{[I], I \text{ invertible ideal}\}$
- Invertible ideals I of $R \Leftrightarrow$ oriented horizontal isogenies $\phi_I : E \rightarrow E_I$
[Colò-Kohel 2020, Onuki 2020]
- $\widetilde{\phi}_I = \phi_{\bar{I}} : E_I \rightarrow E$
- Special case: p inert in R (can only happen for an orientation on a supersingular curve E/\mathbb{F}_{p^2})
- $\pi_p : E \rightarrow E^\sigma$ is not represented by an ideal
- An oriented isogeny $\phi : E \rightarrow E'$ comes from an ideal iff the representations $\rho_R(E)$ and $\rho_R(E')$ are equivalent, $\rho_R(E)$ representation of R on the k -vector space $T_0(E)$

Group action:

- $\text{Pic}(R) \curvearrowright \{E \text{ primitively } R\text{-oriented}\}$
- $[I] \cdot E \mapsto E_I$
- Free and transitive action (if p ramified or split; two orbits if p inert in R)
- $E[\mathfrak{m}](\bar{k}) \simeq R/\mathfrak{m}R$ as R -modules [Lenstra 1996] ($p \nmid \mathfrak{m} = 1$)
- Generalised class group action (ray class groups modulo \mathfrak{m}) to incorporate \mathfrak{m} -level structure [ACELV 2024]

Ideal and isogenies: the supersingular case

- **Deuring correspondance**
- Maximal orders O in $B_{p,\infty}$ = supersingular curves E/\mathbb{F}_{p^2} (up to quadratic twists and Galois conjugates)
- $I \mapsto E_0[I], K \mapsto \mathfrak{I}(K)$: bijection between kernels and left O_0 -ideals ($O_0 = \text{End}(E_0)$)
- **ideals \Leftrightarrow isogenies**
- $\text{End}(E_I) = O_R(I)$ the right order of I ; $\deg \phi_I = N(I) := \text{nrd}(I)$

Ideal to isogeny: $I \Leftrightarrow E_0 \rightarrow E_I := E_0/E[I]$

- Easy if $\text{End}(E_0)$ known, $N(I)$ smooth and $N(I)$ -torsion accessible
- Many **smoothening** algorithms to handle the general case: KLPT, Eichler orders, refreshing the torsion, endomorphisms, Clapoti(s) (= smoothening in higher dimension)...
- Lots of research effort
- 😊 SQISign and variants

Table of Contents

1 Ideals

2 Modules

3 Applications to isogeny based cryptography

4 Advanced topics for modules

- Level structures
- Some isogeny constructions from the module point of view
- Ascending and descending isogenies: the conductor square and excision
- (Un)forgetting orientations via comonadic descent
- Non principal polarisations
- Sesquilinear Weil pairings
- Non R -backtracking isogenies

A general equivalence of category

- **Oriented case:** E_0/k primitively oriented by $\mathcal{R} = R$ quadratic imaginary ($Z(\mathcal{R}) = R$)
- **Supersingular case:** $E_0/k = \mathbb{F}_{p^2}$ with $\mathcal{R} = O_0 = \text{End}(E_0)$ maximal quaternionic order ($Z(\mathcal{R}) = \mathbb{Z}$)

Theorem (Module antiequivalence of category)

There is an **antiequivalence of category** between the category of $Z(\mathcal{R})$ -oriented abelian varieties ^a A k -isogenous to E_0^g and $Z(\mathcal{R})$ -oriented k -morphisms; and the category of finitely presented torsion free (right) \mathcal{R} -modules M of rank g and \mathcal{R} -module morphisms

^awith the technical condition $\rho_{Z(\mathcal{R})}(A) \simeq \bigoplus_{i=1}^g \rho_{Z(\mathcal{R})}(E_0)$

[Waterhouse 1969], [Kani 2011], [Jordan, Keeton, Poonen, Rains, Shepherd-Barron, Tate 2018],
[Kirschmer, Narbonne, Ritzenthaler, R. 2021], [Page-R. 2023]

Alternative approaches to equivalences of category of abelian varieties via lifting to characteristic zero: [Deligne, Howe, Centeleghe-Stix, Marseglia]...

Example

- **Oriented case:** classify R -oriented isogenies
- ⇒ Frobenius orientation: all rational isogenies at level “above” E_0 in the volcano
- **Supersingular case:** classify all isogenies

The equivalence

Serre's generalised Ext and Tor functors: $\mathcal{F}(M) := \text{Ext}_{\mathcal{R}}^1(M, E_0)$ E_0 "compact projective generator"

Definition

If $\mathcal{R}^m \rightarrow \mathcal{R}^n \rightarrow M \rightarrow 0$ is a presentation of a \mathcal{R} -module M , with corresponding matrix Φ , $\mathcal{F}(M) := \text{Ext}_{\mathcal{R}}^1(M, E_0)$ is the kernel of the morphism $E_0^n \rightarrow E_0^m$ given by Φ^T and the \mathcal{R} -orientation:

$$0 \rightarrow \mathcal{F}(M) \rightarrow E_0^n \rightarrow E_0^m$$

\mathcal{F} is a faithful contravariant exact functor from f.p. \mathcal{R} -modules to proper group schemes over k

- Ideals: $\mathcal{F}(\mathcal{R}/I) \simeq E_0[I]$, $\mathcal{F}(I) \simeq E_0/E_0[I]$
- Abelian varieties: If M is torsion free of rank g , $A = \mathcal{F}(M)$ is an abelian variety of rank g
- Duality: $A^\vee \simeq \mathcal{F}(M^\vee)$, $M^\vee := \text{Hom}_{\overline{\mathcal{R}}}(M, \mathcal{R})$
- Torsion: $A[n] \simeq \mathcal{F}(M/nM) = \text{Ext}_{\mathcal{R}}^1(M/nM, E_0) \simeq \text{Ext}_{\mathcal{R}}^1(M, E_0[n])$
- Rational points: $A(k') \simeq \text{Hom}_{\mathcal{R}}(M, E_0(k'))$, k' a k -algebra

Inverse map: $A \mapsto \text{Hom}_{Z(\mathcal{R})}(A, E_0)$: module of (oriented) morphisms from A to E_0

Duality and polarisations

$$\phi : A_1 \rightarrow A_2 \Leftrightarrow \psi : M_2 \rightarrow M_1$$

- Recall $M^\vee = \text{Hom}_{\overline{R}}(M, R)$ ($M^\vee \simeq \text{Hom}_R(M, R)$ as a \mathbb{Z} -module)
- **Duality:** $\hat{\phi} : \hat{A}_2 \rightarrow \hat{A}_1 \Leftrightarrow \psi^\vee : M_1^\vee \rightarrow M_2^\vee, \gamma \mapsto (v \mapsto \gamma \circ \psi(v))$
- **Double duality:** $M \simeq M^{\vee\vee}, m \mapsto (\phi \mapsto \overline{\phi(m)})$
- **Polarisation:** autodual isogeny $\lambda_A : A \rightarrow A^\vee$ induced by an ample line bundle

Corollary (Principal polarisations)

- *Principal polarisation* $\lambda_A : A \rightarrow \hat{A} \Leftrightarrow$ a unimodular Hermitian R -form H_A on M_A
- *N-isogeny* $\phi : (A_1, \lambda_{A_1}) \rightarrow (A_2, \lambda_{A_2}) = N$ -similitude $\Phi : (M_2, H_2) \rightarrow (M_1, H_1)$:

$$\Phi^* H_1 = N H_2$$

[Kirschmer, Narbonne, Ritzenthaler, R. 2021] (Project started in 2011 with Christophe!)

Definition (Hermitian forms)

- Hermitian R -form = R -sesquilinear positive definite
- R -sesquilinear: $H : M \times M \rightarrow R, H(\alpha x, y) = H(x, \bar{\alpha} y) = \alpha H(x, y)$
- Positive definite: $H(x, x) \in \mathbb{Z}^{>0}, \quad \forall x \neq 0 \in M$
- Unimodular: $H : M \simeq M^\vee, m \mapsto H(m, \cdot)$
 $\Leftrightarrow M^\# := \{v \in M \otimes \mathbb{Q}, H(m, v) \in R \quad \forall m \in R\} = M$

Warmup: ideals

The oriented case: ($\mathcal{R} = R$)

- $\mathcal{F}(R) = E_0$, so $\phi_I : E_0 \rightarrow E_I$ corresponds to $I \hookrightarrow R$
- Canonical unimodular Hermitian form on I :

$$H_I(x, y) = \frac{x\bar{y}}{N(I)}$$

- The inclusion $(I, H_I) \subset (R, H_R)$ is a $N(I)$ -similitude
- Handles ascending isogenies: I not invertible (the R -orientation needs not be primitive on E_I)

The supersingular case ($\mathcal{R} = O_0$):

- Maximal orders \Leftrightarrow left O_0 -ideals
- To an order O we associated a connecting (O_0, O) -ideal
- To a left O_0 -ideal I we associate the right order $O_R(I)$
- Original version of Deuring's correspondance (see [Voight, Leroux]): $I = \text{Hom}(E_0, E_I)$

Note that we use an antiequivalence, so for us $I = \text{Hom}(E_I, E_0)$ and I is a right O_0 -ideal. We could apply duality to get an equivalence of categories, but contravariance is more practical for level structures

From now on: focus on the oriented case (almost all results also hold in the supersingular case).

Warmup: ideals (2)

$\phi : E_{I_1} \rightarrow E_{I_2}, \quad I_1, I_2 \text{ invertible}$

- Ideal point of view: $\phi \Leftrightarrow$ some integral ideal J equivalent to $I = I_2 I_1^{-1}$
- $I^{-1} = \bar{I}/N(I)$ so if $x \in I, J := I\bar{x}/N(I) \sim I; \quad N(J) = N(x)/N(I)$
- Module point of view: $\phi \Leftrightarrow \psi : (I_2, H_R/N(I_2)) \rightarrow (I_1, H_R/N(I_1))$
- If $z \in I^{-1}: \psi_z : r \mapsto zr$ is a $N := N(z)N(I_2)/N(I_1)$ -similitude
- $z = \bar{x}/N(I), N = N(x)/N(I)$
- If I integral: canonical isogeny via $z = 1 \in R \subset I^{-1}$

Duality:

- $I^\vee \simeq I$ via H_I , so $I^\vee \simeq I/N(I)$ via $x \in I/N(I) \mapsto (y \in I \mapsto x\bar{y})$
- $\hat{\phi} \Leftrightarrow \psi^\vee = \psi_{\bar{z}} : I_1/N(I_1) \rightarrow I_2/N(I_2)$
- Contragredient isogeny $\tilde{\phi} \Leftrightarrow \tilde{\psi} : I_1 \rightarrow I_2, \tilde{\psi} = \psi_{\bar{z}N(I)}$

Extend $N := N_R$ to fractional ideals

Proposition (Contragredient = Adjoint)

If $\phi : (A_1, \lambda_1) \rightarrow (A_2, \lambda_2) \Leftrightarrow \psi : (M_2, H_2) \rightarrow (M_1, H_1), \tilde{\phi} \Leftrightarrow \tilde{\psi}$, where $\tilde{\psi} = \psi^* : M_1 \rightarrow M_2$ is the adjoint: $H_1(\psi(x), y) = H_2(x, \psi^*(y))$

Similitudes to isogenies

Module morphism to morphism of abelian varieties:

$$\begin{array}{ccccccc}
 R^{m_1} & \longrightarrow & R^{n_1} & \twoheadrightarrow & M_1 & \longrightarrow & 0 \\
 \uparrow \vdots & & \uparrow \vdots & & \uparrow & & \\
 R^{m_2} & \longrightarrow & R^{n_2} & \twoheadrightarrow & M_2 & \longrightarrow & 0
 \end{array}
 \quad \Leftrightarrow \quad
 \begin{array}{ccccccc}
 0 & \longrightarrow & A_1 & \hookrightarrow & E_0^{n_1} & \longrightarrow & E_0^{m_1} \\
 & & \downarrow & & \vdots & & \vdots \\
 0 & \longrightarrow & A_2 & \hookrightarrow & E_0^{n_2} & \longrightarrow & E_0^{m_2}
 \end{array}$$

R^n is a projective module, so we can lift module maps. The commutative diagram allows to find the kernel of $A_1 \rightarrow A_2$.

- N -similitudes $\Leftrightarrow N$ -isogenies
- $\phi : A_1 \rightarrow A_2 \Leftrightarrow (M_2, H/N) \subset (M_1, H)$
Isogeny = epimorphism (with finite kernel) \Leftrightarrow monomorphism (=inclusion) of modules (with finite cokernel)
- $\text{Ker } \phi = A_1[M_2] \subset A_1[N]$ (Recall $M_1 = \text{Hom}(A_1, E_0)$)

$$A_1[M_2] := \{P \in A_1(\bar{k}), \phi(P) = 0_{E_0} \forall \phi \in M_2\}$$

- $\text{Ker } \phi \simeq \mathcal{F}(M_1/M_2)$ so $\deg \phi = \#M_1/M_2$ (R commutative)
- Equivalence **practical** if N **smooth**, the N -torsion on E_0 is **accessible**, and the action of M_1 on A_1 is **effective**

Similitudes to isogenies: the general case

- Find a smooth similitude $(M_2, H_2) \rightarrow (M_1, H_1)$
- Clapoti(s): it suffice to build two N_1, N_2 -similitudes with $N_1 \wedge N_2 = 1$ (or small)
- There are unimodular Hermitian R -modules (M, H_M) such that no N -similitude $R^g \hookrightarrow M$ exist for any N , c.f. the arithmetic obstructions in [Kirschmer, Narbonne, Ritzenthaler, R. 2021]
- Solution: look at $R^{g+1} \hookrightarrow M \times R$
- Conductor gap: a N -isogeny $E_0^g \rightarrow E \times A$ (with the product polarisations) inducing a non trivial isogeny $E_0 \rightarrow E$ satisfy

$$f_{E/E_0} \mid N$$

Isogeny to similitude:

- $\phi : A_1 \rightarrow A_2$ a N -isogeny of kernel K
- $A_1 = \mathcal{F}(M_1)$ with effective action
- $M_2 := \{\gamma \in M_1, \gamma(K) = 0\}, H_2 = H_1/N$
Needs efficient DLPs in $A_1[N]$ to compute M_2
- The action of M_2 on A_1 descends to an effective action on A_2
(via isogeny division, at least in nice cases)

Modules to abelian varieties

- $R^m \rightarrow R^n \rightarrow M \rightarrow 0$ presentation of M
- $0 \rightarrow A \hookrightarrow E_0^n \rightarrow E_0^m$ co-presentation of $A = \mathcal{F}(M)$

Example: $I = (\alpha, \beta)$, with syzygys of rank 1: $u\alpha + v\beta = 0$

$$R \xrightarrow{(u,v)^T} R^2 \xrightarrow{(\alpha,\beta)} I \subset R \quad \Leftrightarrow \quad E_0 \twoheadrightarrow E_I \hookrightarrow E_0^2 \rightarrow E_0$$

- $E_0 \rightarrow E_0^2, P \mapsto (\alpha P, \beta P)$ has kernel $E_0[I]$, so the image is isomorphic to E_I
- $E_I \hookrightarrow E_0^2$ is also given by the kernel of $E_0^2 \rightarrow E_0, (P, Q) \mapsto uP + vQ$

Module to explicit abelian variety:

- Try to find a nice N -similitude $(M, H_M) \hookrightarrow (R^g, \oplus_{i=1}^g H_R)$
- Convert to $E_0^g \twoheadrightarrow A_M$

Abelian variety to module:

- Find n morphisms $\phi_i : A \rightarrow E_0$ whose kernels intersect trivially

Example: a double path $E_I \rightarrow E_0$!

- Find the R -lattice of relations on the ϕ_i

Find relations by testing on points of smooth order. Each relation reduces the tentative module M_A . Use the principal polarisation on A as a stop criterion (pairings).

- $A \hookrightarrow E_0^n \rightarrow E_0^m$ gives M_A

Table of Contents

1 Ideals

2 Modules

3 Applications to isogeny based cryptography

4 Advanced topics for modules

- Level structures
- Some isogeny constructions from the module point of view
- Ascending and descending isogenies: the conductor square and excision
- (Un)forgetting orientations via comonadic descent
- Non principal polarisations
- Sesquilinear Weil pairings
- Non R -backtracking isogenies

Cryptographic applications?

- **Clapotis**: Class group Action in Polynomial Time via Sesquilinear forms [Page-R. 2023]
- **Original motivation**: “new” Module-KLPT algorithm for $M = I \oplus \bar{I} \subset R \oplus R$
Via an algebraic embedding $B^\times \subset \mathrm{GU}_2$ to reduce to quaternionic KLPT

Cryptographic applications?

- **Clapotis**: Class group Action in Polynomial Time via Sesquilinear forms [Page-R. 2023]
- **Original motivation**: “new” Module-KLPT algorithm for $M = I \oplus \bar{I} \subset R \oplus R$
Via an algebraic embedding $B^\times \subset \mathrm{GU}_2$ to reduce to quaternionic KLPT
- **Clapoti**: bypass the module equivalence of category by just using Kani... again...

Meme: Culprit

- New isogeny algorithm
- Isogeny based cryptography
- Kani’s lemma

Cryptographic applications!


Help needed! Any other interesting cryptographic application of modules?

Hypothesis: we can extend all our **algorithmic tools** and **security assumptions** from dimension 1 to dimension g .

Security assumption: **Module-Inversion**. Given A , it is hard to recover (some?) module information

$$M = \text{Hom}_R(A, E_0).$$

This talk: three (potential) examples:

- **SQISurf**: **short signatures** for **oriented isogenies** (dimension 2)
Philosophy: apply supersingular tools to oriented isogenies via dimension 2
- **Noisy-CSIDH**: Module Isogeny Key Exchange. Combining **torsion noise** and oriented **commutative group action** for **key exchange** (dimension 1 and 2)
Philosophy: combine supersingular-like graph properties with commutative group actions
- **⊗-MIKE**: Module Isogeny Key Exchange². Higher dimensional version of CSIDH; Supersingular key exchange **without any torsion information** (dimension 1, 2 and 4)
New tool! **Tensor product** of abelian varieties and 



Work in progress!



²Name courtesy of Luca De Feo

The isogeny graph of oriented isogenies in higher dimension

- M torsion free of rank g : $M \simeq R^{g-1} \oplus I$ Assume R maximal for simplicity
- $A \simeq E_0^{g-1} \times E_I$
- $\# \text{Cl}(R)$ isomorphism classes of **non-polarised** R -oriented abelian varieties R -isogenous to E_0^g
- **Polarisations** add supersingular like graph complexity if $g > 1$ ($\text{End}_R(E_0^g) = M_g(R)$)
- **Universal group action**: $I \cdot (M, H_M) = (IM, H_M/N(I)) \subset (M, H_M)$ (I invertible)
- $I \cdot A = A_I := A/A[I]$
- **Intuition**: multiplication by $[n] \Rightarrow$ multiplication by $[I]$
- **Multiple orbits**; linked together by oriented isogenies (which are not multiplication by $[I]$)

Example: rational supersingular abelian surfaces

- E_0/\mathbb{F}_p supersingular, $R = \text{End}_{\mathbb{F}_p}(E) = \mathbb{Z}[\sqrt{-p}]$ (or its maximal order)
- $g = 2$: graph of supersingular abelian surfaces isogeneous to E_0^2 over \mathbb{F}_p and \mathbb{F}_p -rational isogenies
- Universal group action from $\text{Cl}(R)$
- Conjecture: $\approx p^{3/2}$ nodes ($\approx \#\text{supersingular curves} \times \#\text{Cl}(R)$)
- If $\ell = \bar{\ell}$ splits in R , $A[\ell] = A[\ell] \oplus A[\bar{\ell}] \Rightarrow$ action by ℓ and $\bar{\ell}$ and $\ell + 1$ (?) other oriented ℓ -isogenies.

Weil's restriction of supersingular elliptic curves

E_0/\mathbb{F}_p supersingular, $R = \text{End}_{\mathbb{F}_p}(E) = \mathbb{Z}[\sqrt{-p}]$ (or its maximal order)

- If E_i/\mathbb{F}_{p^2} , Weil restriction $W_{\mathbb{F}_{p^2}/\mathbb{F}_p} E_i$ is a p.p. abelian surface over \mathbb{F}_p (which is neither a Jacobian or product of curves over \mathbb{F}_p). And the Weil restriction of an N -isogeny $\phi/\mathbb{F}_{p^2} : E_1 \rightarrow E_2$, is an \mathbb{F}_p -rational isogeny between rational the abelian surfaces $A_1 \rightarrow A_2, A_i = W_{\mathbb{F}_{p^2}/\mathbb{F}_p} E_i$

\Rightarrow If E_i is isogeneous to E_0 , A_i is isogeneous to $E_0^2 = W_{\mathbb{F}_{p^2}/\mathbb{F}_p} E_0$

- $\text{Hom}_{\mathbb{F}_p}(W_{\mathbb{F}_{p^2}/\mathbb{F}_p} E_1, W_{\mathbb{F}_{p^2}/\mathbb{F}_p} E_2) = \text{Hom}_{\mathbb{F}_{p^2}}(W_{\mathbb{F}_{p^2}/\mathbb{F}_p} E_1 \otimes_{\mathbb{F}_p} \mathbb{F}_{p^2}, E_2) =$
 $\text{Hom}_{\mathbb{F}_{p^2}}(E_1 \oplus E_1^\sigma, E_2) = \text{Hom}_{\mathbb{F}_{p^2}}(E_1, E_2) \oplus \text{Hom}_{\mathbb{F}_{p^2}}(E_1, E_2)^\sigma$

- So the dimension 2 supersingular graph over \mathbb{F}_p contains, via the Weil restriction, the supersingular graph of elliptic curves over \mathbb{F}_{p^2} (with E collapsed with E^σ)

\Rightarrow Convenient way to obtain \mathbb{F}_p -rational isogenies in dimension 2

\Rightarrow Module-Inversion in dimension 2 (heuristically) at least as hard as the supersingular isogeny path problem.

From $M = \text{Hom}_{\mathbb{F}_p}(W_{\mathbb{F}_{p^2}/\mathbb{F}_p} E, E_0)$, we recover a rational N -isogeny $E_0^2 \rightarrow W_{\mathbb{F}_{p^2}/\mathbb{F}_p} E$, which gives over \mathbb{F}_{p^2} an isogeny $E_0^2 \rightarrow E \times E^\sigma$ from which we extract an isogeny $E_0 \rightarrow E$.

- Weil restriction from the module point of view: If $\phi/\mathbb{F}_{p^2} : E_1 \rightarrow E_2$ is represented by $\psi/O_0 : I_2 \rightarrow I_1$, see § 4 for how to find the module representation $\Psi/R : M_2 \rightarrow M_1$ of $W_{\mathbb{F}_{p^2}/\mathbb{F}_p} \phi$

SQISurf: Short signatures for oriented isogenies on abelian surfaces

- $\phi_I : E_0 \rightarrow E_I$
- Recovering I from $(E_0, E_I) \Leftrightarrow$ recovering the module $R \oplus I$ associated to $E_0 \times E_I$
Quantum subexponential via [Kuperberg]. N.B.: $E_0 \times E_I$ is doubly oriented via $(P, Q) \mapsto (P, -Q)$!

\Rightarrow SQISign like protocol in dimension 2 (not SQISign2d!)

$$\begin{array}{ccc} E_0 \times E_0 & \xrightarrow{\phi_{sec}} & E_0 \times E_I \\ \downarrow \phi_{com} & & \downarrow \phi_{chl} \\ A & \xleftarrow{\phi_{resp}} & B \end{array}$$

- Soundness: check that the response is not R -backtracking through the challenge
We want an R -endomorphism on $E_0 \times E_I$ which does not come from R !
- ZK: depends on how we compute the response
- Needs a generalised ModuleToIsogeny for the response

Noisy-CSIDH Noisy group action key exchange

- Commutative group action on a supersingular like graph
- ⇒ Mask the torsion in a SIDH-like key exchange by using this commutative group action (like M-SIDH but using $[I]$ rather than $[n]$)
- ⇒ Hide the commutative group action in a CSIDH-like key exchange by adding a SIDH-like torsion exchange

$$\begin{array}{ccccc}
 A_0 & \xrightarrow{\phi_a} & A_{a_1} & \xrightarrow{[a]} & (A_{a_2}, [a] \circ \phi_a(A_0[N_B])) \\
 \downarrow \phi_b & & \downarrow \phi'_b & & \downarrow \phi''_b \\
 A_{b_1} & \xrightarrow{\phi'_a} & A_{a_1, b_1} & \xrightarrow{[a]} & A_{a_2, b_1} \\
 \downarrow [b] & & \downarrow [b] & & \downarrow [b] \\
 (A_{b_2}, [b] \circ \phi_b(A_0[N_A])) & \xrightarrow{\phi''_a} & A_{a_1, b_2} & \xrightarrow{[a]} & A_{a_2, b_2}
 \end{array}$$

- ϕ_a : oriented N_A -isogeny; ϕ_b : oriented N_B -isogeny
- Speed up trick: do a standard SIDH key exchange over \mathbb{F}_{p^2} , take Weil restriction to \mathbb{F}_p , apply group action of $\text{Cl}(\mathbb{Z}[\sqrt{-p}])$ in dimension 2
- Size: $p = 4\lambda$; $J(A_{a_2})$: $3 \log_2(p)$; torsion on deterministic R -basis: $4 \log_2(p)$ (or $3 \log_2 p$ using pairings?)
Total: $6 \log_2 p = 24\lambda$ (vs $3.5 \log_2 p = 14\lambda$ for SIDH)

Direct sums and pushforwards

$$(A_1, \lambda_1) \Leftrightarrow (M_1, H_1) \text{ and } (A_2, \lambda_2) \Leftrightarrow (M_2, H_2)$$

Product polarisations: $(A_1 \times A_2, \lambda_1 \times \lambda_2) \Leftrightarrow (M_1 \oplus M_2, H_1 \oplus H_2)$

Pushforwards:

- If $\phi_1 : A_0 \rightarrow A_1$ and $\phi_2 : A_0 \rightarrow A_2$ correspond to $\psi_1 : M_1 \rightarrow M$ and $\psi_2 : M \rightarrow M_2$, their **pushforward** A_{12} corresponds to the **fiber product** $M_1 \times_M M_2$
- If $\phi_1 : A_0 \twoheadrightarrow A_1$, $\phi_2 : A_0 \twoheadrightarrow A_2$ are isogenies, $\psi_1 : M_1 \hookrightarrow M$, $\psi_2 : M_2 \hookrightarrow M$ are **monomorphisms**, and the fiber product $M_1 \times_M M_2$ is just the **intersection** $M_1 \cap M_2 \subset M$

$$\begin{array}{ccc}
 A_0 & \twoheadrightarrow & A_1 \\
 \downarrow & & \downarrow \\
 A_2 & \twoheadrightarrow & A_{12}
 \end{array}
 \quad \Leftrightarrow \quad
 \begin{array}{ccc}
 M & \longleftarrow & M_1 \\
 \uparrow & & \uparrow \\
 M_2 & \longleftarrow & M_1 \cap M_2
 \end{array}$$

- $\phi_1 : A_0 \rightarrow A_1, K_1 = \text{Ker } \phi_1 = \mathcal{F}(M/M_1) = A_0[M_1]$
- $\phi_2 : A_0 \rightarrow A_2, K_2 = \text{Ker } \phi_2 = \mathcal{F}(M/M_2) = A_0[M_2]$
- $\phi_{12} : A_0 \rightarrow A_{12}, K_{12} = K_1 + K_2 = \mathcal{F}(M/M_1 \cap M_2) = A_0[M_1 \cap M_2]$

Tensor product of abelian varieties

Assumptions: R commutative, M_1, M_2 R -modules with $f_{M_1} \wedge f_{M_2} = 1$.

(Ex: M_1 or M_2 projective. N.B: if M_1, M_2 projectives, $M_1 \otimes_R M_2$ is too)

Definition ((Co)tensor product)

Under our assumptions, $M_1 \otimes_R M_2$ is torsion free and we define $A_1 \otimes_{E_0} A_2$ as $\mathcal{F}(M_1 \otimes_R M_2)$

- $(M_1 \otimes_R M_2)^\vee \simeq M_1^\vee \otimes_R M_2^\vee$
 - So $H_1 \otimes_R H_2$ is unimodular Hermitian if H_1, H_2 are
 - And if $\psi_1 : M_1 \rightarrow M'_1$ is a N_1 -similitude and $\psi_2 : M_2 \rightarrow M'_2$ is a N_2 -similitude, $\psi_1 \otimes_R \psi_2 : M_1 \otimes_R M_2 \rightarrow M'_1 \otimes_R M'_2$ is a $N_1 N_2$ -similitude
 - Tensor product of isogenies: $\phi_1 \otimes_{E_0} \phi_2 : A'_1 \otimes_{E_0} A'_2 \rightarrow A_1 \otimes_{E_0} A_2$
- ☹ • \otimes_{E_0} • is **not effective**

Example

- $E_0 \otimes_{E_0} A \simeq A$
- $E_I \otimes_{E_0} A \simeq I \cdot A$ if I invertible ideal

Symmetric monoidal actions

Definition (The module monoidal (co)-action)

- If M is a **projective** module, the action by M is $M \cdot A = M \otimes_R A := \mathcal{F}(M) \otimes_{E_0} A$.
- If $\phi : A_1 \rightarrow A_2$ is a N -isogeny, $M \otimes_R \phi : M \otimes_R A_1 \rightarrow M \otimes_R A_2$ is a N -isogeny.
- If $\psi : M_2 \hookrightarrow M_1$ is a N -similitude, $\psi \otimes_R A : M_1 \otimes_R A \rightarrow M_2 \otimes_R A$ is a N -isogeny.

Theorem (Effectivity of the symmetric monoidal action)

The **symmetric monoidal action** $M \cdot A = M \otimes_R A$ from **projective** R -modules to **abelian varieties** corresponds to the **canonical copower action construction** on categories enriched in a closed monoidal category^a (in particular it does not depend on the base point E_0).

It is **effective**.

^aThis is just a fancy way of saying that $\text{Hom}_R(M \otimes_R A_1, A_2) = \text{Hom}_R(M, \text{Hom}_R(A_2, A_1))$.

Group action analogy: If $G \curvearrowright X$ (principal homogeneous space), fixing a point $x_0 \in X$ transfers the group structure of G on X . But the group multiplication may only be effective on G .

Group action framework: one way function $G \rightarrow X$ with some compatibility with the group structure.

In our case, \otimes is only effective on the module side, not the abelian side, but we can still transfer partially the monoidal structure via the monoidal action.

Symmetric monoidal actions for key exchange

Example (The action by ideals)

- $M \cdot E_0 = M \otimes_R E_0 \simeq A_M = \mathcal{F}(M)$
- $I \otimes_R M \simeq IM$ when I is invertible (or simply $f_I \wedge f_M = 1$), so $I \cdot A := I \otimes_R A$ recovers the usual CSIDH action

Proposition (CSIDH as a tensor product)

if I_1, I_2 invertible, $I_1 \otimes I_2 \simeq I_1 I_2$, so \otimes gives the CSIDH key exchange:

$$\begin{array}{ccc} E_0 & \xrightarrow{\quad\quad\quad} & E_{I_1} = I_1 \cdot E_0 \\ \downarrow & & \downarrow \\ E_{I_2} = I_2 \cdot E_0 & \longrightarrow & E_{I_1 \otimes I_2} \simeq E_{I_1} \otimes_{E_0} E_{I_2} = I_1 I_2 \cdot E_0 \end{array}$$

- If $N(I_1) \wedge N(I_2) = 1$, the diagram above is also a **pushforward** because $I_1 I_2 = I_1 \cap I_2$
- Monoidal action on **rank 1** projective modules = **class group action**
- ☹ **Subexponential** quantum attacks (Kuperberg)

Symmetric monoidal actions for key exchange

Proposition (Higher dimensional CSIDH via the monoidal action)

$$\begin{array}{ccc} A_0 & \rightsquigarrow & A_1 = M_1 \cdot A_0 \\ \Downarrow & & \Downarrow \\ A_2 = M_2 \cdot A_0 & \rightsquigarrow & A_{12} = (M_1 \otimes_R M_2) \cdot A_0 \end{array}$$

If $\dim A_0 = g_0$, $\text{rank } M_1 = g_1$, $\text{rank } M_2 = g_2$, then $\dim A_{12} = g_0 g_1 g_2$.

Example (Monoidal action by rank 2 modules: $A_0 = E_0$, $g_1 = g_2 = 2$)

M_i projective module of rank 2 $\Leftrightarrow E_0^2 \twoheadrightarrow A_i$ a path:

$$\begin{array}{ccc} E_0^2 & \longrightarrow & A_1 \\ \downarrow & & \Downarrow \\ A_2 & \rightsquigarrow & A_1 \otimes_{E_0} A_2 \end{array}$$

Common secret: the dimension 4 abelian variety $A_1 \otimes_{E_0} A_2$

Symmetric monoidal actions for key exchange

Proposition (Higher dimensional CSIDH via the monoidal action)

$$\begin{array}{ccc} A_0 & \rightsquigarrow & A_1 = M_1 \cdot A_0 \\ \Downarrow & & \Downarrow \\ A_2 = M_2 \cdot A_0 & \rightsquigarrow & A_{12} = (M_1 \otimes_R M_2) \cdot A_0 \end{array}$$

If $\dim A_0 = g_0$, $\text{rank } M_1 = g_1$, $\text{rank } M_2 = g_2$, then $\dim A_{12} = g_0 g_1 g_2$.

☹ Acting by rank g projective modules increase the dimension if $g > 1$

😊 Protects (hopefully!) from Kuperberg

- **Security:** Action-DDH \leq Action-CDH \leq Action-Inversion

- Action-Inversion \approx Module-Inversion

Indeed, if $M = \text{Hom}_R(A, E_0)$, then $M \cdot E_0 = \mathcal{F}(M)$

Recall that, thanks to Weil's restriction, Module-Inversion on supersingular abelian surfaces over \mathbb{F}_p is at least as hard as solving the supersingular isogeny path problem over \mathbb{F}_{p^2}

- Action-CDH: **Hope** for exponential quantum security when $g > 1$

Computing the symmetric monoidal action

M_1 projective of rank g , $A_1 = M_1 \cdot E_0$

We want to compute $M_1 \cdot A_2$ for an R -oriented A_2 (with effective orientation)

General idea: look at how we construct $A_1 = M_1 \cdot E_0$ from E_0 , and apply the same recipe replacing E_0 by A_2 .

The smooth case:

- Suppose we can construct a smooth similitude $R^g \subset M_1$ (by duality, this is equivalent to constructing a smooth isogeny $E_0^g \rightarrow A_1$), this gives us a smooth similitude $A_2^g \rightarrow M_1 \otimes_R A_2$
- Via the orientation, we can transpose the kernel of $E_0^g \rightarrow A_1$ to the kernel of $A_2^g \rightarrow M_1 \otimes_R A_2$. The codomain gives us $M_1 \otimes_R A_2$
- Similar to the usual way the CSIDH action is computed

The general case:

- If instead A_1 is computed via Clapoti(s), splitting an appropriate endomorphism on $E_0^{g_1}$
- Then we can compute $M_1 \cdot A_2$ by splitting an appropriate endomorphism on $A_2^{g_1}$
- ☹ Needs to work in dimension $2g_1g_2$

Computing the symmetric monoidal action: the smooth case

$$R^g \longleftarrow M_1 \quad \Leftrightarrow \quad E_0^g \longrightarrow A_1$$

$$M_2^g \longleftarrow M_1 \otimes_R M_2 \quad A_2^g \longrightarrow A_1 \otimes_{E_0} A_2 = M_1 \cdot A_2$$

Proposition (Computing projective tensor products: the smooth case)

If $E_0^g \twoheadrightarrow A_1 \Leftrightarrow M_1 \hookrightarrow R^g$, we can compute $A_1 \otimes_{E_0} A_2$ as the quotient of $A_2^g = E_0^g \otimes_{E_0} A_2$ given by the kernel $K \subset A_2^g$ induced by $M_1 \otimes M_2 \hookrightarrow R^g \otimes M_2$: if M_1 is generated by (m_1, \dots, m_n) , and $m_i = (\alpha_{i1}, \dots, \alpha_{ig}) \in R^g$, then $K = A_2^g[m_1 \otimes M_2, \dots, m_n \otimes M_2]$ and

$$A_2^g[m_i \otimes M_2] = \text{Ker } A_2^g \xrightarrow{(\alpha_{ij})} A_2$$

Corollary (Computing the action in practice)

- If A_1 is the quotient of E_0^g by $E_0^g[m_1, \dots, m_n]$, where $E_0^g[m_i] = \text{Ker}(E_0^g \rightarrow E_0, (P_1, \dots, P_g) \mapsto \sum \alpha_{ij} P_j)$
- Then $A_1 \otimes_{E_0} A_2$ is the quotient of A_2^g by $A_2^g[m_1 \otimes M_2, \dots, m_n \otimes M_2]$, where $A_2^g[m_i \otimes M_2] = \text{Ker}(A_2^g \rightarrow A_2, (P_1, \dots, P_g) \mapsto \sum \alpha_{ij} P_j)$
- And if $E_0^g \twoheadrightarrow A_1$ is a N -isogeny, $A_2^g \twoheadrightarrow A_1 \otimes_{E_0} A_2$ is a N -isogeny

Computing the symmetric monoidal action: the smooth case

Commutative diagram:

$$\begin{array}{ccc}
 R^{\mathcal{G}^1} \otimes_R R^{\mathcal{G}^2} & \longleftarrow & M_1 \otimes_R R^{\mathcal{G}^2} \\
 \uparrow & & \uparrow \\
 R^{\mathcal{G}^1} \otimes_R M_2 & \longleftarrow & M_1 \otimes_R M_2
 \end{array}
 \quad \Leftrightarrow \quad
 \begin{array}{ccc}
 E_0^{\mathcal{G}^1} \otimes_{E_0} E_0^{\mathcal{G}^2} \simeq E_0^{\mathcal{G}^1 \mathcal{G}^2} & \longrightarrow & A_1 \otimes_{E_0} E_0^{\mathcal{G}^2} \simeq A_1^{\mathcal{G}^2} \\
 \downarrow & & \downarrow \\
 E_0^{\mathcal{G}^1} \otimes_{E_0} A_2 \simeq A_2^{\mathcal{G}^1} & \longrightarrow & A_1 \otimes_{E_0} A_2
 \end{array}$$

Pairing analogy: \otimes_{E_0} = categorified bilinear map

Assume we don't know how to compute $e(P_1, P_2)$ for general P_1, P_2 , but we know $e(P_0, P_2)$. Then if $P_1 = mP_0$, we can compute $e(P_1, P_2) = e(P_0, P_2)^m$

Here we use that $E_0^{\mathcal{G}} \otimes_{E_0} A_2 \simeq A_2^{\mathcal{G}}$ and our known path $E_0^{\mathcal{G}} \rightarrow A_1$.

Monoidal actions for isogenies

- $M'_1 \hookrightarrow M_1 \hookrightarrow R^{\mathcal{G}} \Leftrightarrow A_2^{\mathcal{G}} \twoheadrightarrow M_1 \otimes_R A_2 \twoheadrightarrow M'_1 \otimes_R A_2 \Rightarrow$ recover it via the **isogeny factorisation**: $A_2^{\mathcal{G}}[M_1 \otimes_R M_2] \subset A_2^{\mathcal{G}}[M'_1 \otimes_R M_2]$
- If $A_2 \rightarrow A'_2$, then we recover $M_1 \otimes_R A_2 \rightarrow M_1 \otimes_R A'_2$ via **isogeny division**:

$$\begin{array}{ccc}
 A_2^{\mathcal{G}} & \longrightarrow & M_1 \otimes_R A_2 \\
 \downarrow & & \downarrow \\
 A_2'^{\mathcal{G}} & \longrightarrow & M_1 \otimes_R A_2'
 \end{array}$$

Computing the symmetric monoidal action: the general case

$$E_0^g \longrightarrow A_1 \longrightarrow E_0^g$$

$$A_2^g \longrightarrow A_1 \otimes_{E_0} A_2 \longrightarrow A_2^g$$

Proposition (Computing projective tensor products: the general case)

Assume A_1 is constructed from E_1 via Clapoti(s), i.e. constructing a N_1 and N_2 -similitude $R^g \hookrightarrow M_1$, and then splitting the induced $N_1 N_2$ -endomorphism $\gamma : E_0^g \rightarrow E_0^g$. So γ is given by an explicit matrix in $M_g(R)$.

Then $\gamma \otimes_{E_0} \text{Id}_{A_2}$ is the same matrix acting as an endomorphism $A_2^g \rightarrow A_2^g$ via the R -orientation, and splitting this $N_1 N_2$ -endomorphism gives $A_1 \otimes_{E_0} A_2$.

$$\begin{array}{ccc}
 E_0 & \longrightarrow & E_1 \\
 \downarrow & & \downarrow \\
 E_2 & \rightsquigarrow & W_{\mathbb{F}_p^2/\mathbb{F}_p} E_1 \otimes_{E_0} W_{\mathbb{F}_p^2/\mathbb{F}_p} E_2
 \end{array}$$

- Start with our good old friend E_0/\mathbb{F}_p **supersingular** (with p e.g. the SQISign2d prime)
- Alice and Bob compute (**smooth or not**) isogenies over \mathbb{F}_{p^2} : $E_0 \rightarrow E_1, E_0 \rightarrow E_2$ (no need for coprime degrees!)
- They send $j(E_1), j(E_2)$: **no torsion information!**
- **Validation**: check that E_i is supersingular
- The **common key** is the **dimension 4** ppav $A_{12} := W_{\mathbb{F}_p^2/\mathbb{F}_p} E_1 \otimes_{E_0} W_{\mathbb{F}_p^2/\mathbb{F}_p} E_2$

Alice can compute it by converting her isogeny $E_0 \rightarrow E_1$ to the module map representing $E_0^2 = W_{\mathbb{F}_p^2/\mathbb{F}_p} E_0 \rightarrow W_{\mathbb{F}_p^2/\mathbb{F}_p} E_1$ and then applying the tensor product construction to $W_{\mathbb{F}_p^2/\mathbb{F}_p} E_2$.

The smooth case requires a **dimension 4 isogeny**, and the non smooth case requires splitting a dimension 4 endomorphism, so a **dimension 8 isogeny**...

- **Size**: $p = 2\lambda, j(E_i) = 2 \log_2(p) = 4\lambda$: 64B. **Very compact!**
- **NIKE**. PKE a la ElGamal/SiGamal

🧐 Need good **dimension 4 modular invariants** to represent A_{12} (e.g. suitable symmetric polynomials in the theta constants?)

🧐 **Security?** Action-CDH on supersingular abelian surfaces coming from the Weil restriction of elliptic curves

$$\begin{array}{ccc}
 E_0 & \longrightarrow & E_1 \\
 \downarrow & & \downarrow \\
 E_2 & \rightsquigarrow & W_{\mathbb{F}_p^2/\mathbb{F}_p} E_1 \otimes_{E_0} W_{\mathbb{F}_p^2/\mathbb{F}_p} E_2
 \end{array}$$

Example of parameters:

- $p = u2^e - 1$. Ex: $p = 5 \cdot 2^{248} - 1$.
- Alice and Bob each compute a 2^e -isogeny from E_0 over \mathbb{F}_{p^2}
- Then the **common key** then requires computing a 2^e -isogeny in dimension 4 over \mathbb{F}_p
- Unfortunately, for the dimension 4 isogeny, the **theta null point** will only be defined over \mathbb{F}_{p^2} , so our known isogeny formulas will require to work over \mathbb{F}_{p^2} for the dimension 4 isogeny too
- Open problem: adapt the **theta formulas** to work over \mathbb{F}_p

Table of Contents

1 Ideals

2 Modules

3 Applications to isogeny based cryptography

4 Advanced topics for modules

- Level structures
- Some isogeny constructions from the module point of view
- Ascending and descending isogenies: the conductor square and excision
- (Un)forgetting orientations via comonadic descent
- Non principal polarisations
- Sesquilinear Weil pairings
- Non R -backtracking isogenies

4 Advanced topics for modules

■ Level structures

- Some isogeny constructions from the module point of view
- Ascending and descending isogenies: the conductor square and excision
- (Un)forgetting orientations via comonadic descent
- Non principal polarisations
- Sesquilinear Weil pairings
- Non R -backtracking isogenies

Torsion free f.p. R -modules

- In both cases: rank 1 torsion free modules = ideals

Oriented case (R is a Bass ring)

- $M \simeq I_1 \oplus I_2 \oplus \cdots \oplus I_g$
- $R \subset O(I_1) \subset O(I_2) \subset \cdots \subset O(I_g)$
- $\det M = I_1 \cdot I_2 \cdots I_g$ invertible R_g -ideal
- **Conductor** of M : $f_M := [R_g : R]$
N.B.: M is projective over $\text{Spec } R[1/f_M]$
- The **isomorphism class** of M only depend on (R_1, \dots, R_g) and $\det M$
- Example: if all I_j are invertible in R ($\Leftrightarrow O(I_j) = R$),

$$M \simeq R^{g-1} \oplus I_1 \cdot I_2 \cdots I_g$$

Supersingular case

- $M \simeq R^g$ if $g > 1$

Level structure

- $M \twoheadrightarrow M/\mathfrak{a}$ induces $A[\mathfrak{a}] \hookrightarrow A$
- $\psi : M_2 \rightarrow M_1 \Leftrightarrow \phi : A_1 \rightarrow A_2$
- $\psi \bmod \mathfrak{a} : M_2/\mathfrak{a}M_2 \rightarrow M_1/\mathfrak{a}M_1 \Leftrightarrow A_1[\mathfrak{a}] \rightarrow A_2[\mathfrak{a}]$ $A[\mathfrak{a}](\bar{k}) \simeq \operatorname{Hom}_{\mathbb{Z}\mathcal{R}}(M/\mathfrak{a}, E_0(\bar{k}))$

Oriented case:

- $A_M[\mathfrak{a}](\bar{k}) \simeq M/\mathfrak{a}M$ as R -modules (if \mathfrak{a} prime to p)
- The Dieudonné module of $A_M[p^m]$ inherits a R -module structure which is isomorphic to M/p^mM (?)
- If M torsion R -module, $\deg \mathcal{F}(M) = \#M$

Differentials (oriented case)

- If $A = \mathcal{F}(M)$, $\mathrm{Lie}(A) = \mathrm{Hom}_R(M, \mathrm{Lie}(E_0)) = \mathrm{Hom}_{R/p}(M/p, \mathrm{Lie}(E_0))$
- Action on **tangent space**: $\psi : M_2 \rightarrow M_1 \Leftrightarrow \phi : A_1 \rightarrow M_2$. Then $d\phi : \mathrm{Lie}(A_1) \rightarrow \mathrm{Lie}(A_2) = \mathrm{Hom}_R(M_1, \mathrm{Lie}(E_0)) \rightarrow \mathrm{Hom}_R(M_2, \mathrm{Lie}(E_0))$
- Since $\Omega^1 A/k = \mathrm{Hom}_k(\mathrm{Lie}(A), k)$, by duality, we get: $\phi^* : \Omega^1 A_2 \rightarrow \Omega^1 A_1$

- If E elliptic curve, choice of **short Weierstrass equation** \Leftrightarrow choice of **global differential** ω_E (via $y^2 = x^3 + ax + b \mapsto \omega_E = dx/y$)
- Fixing an equation of E_0 fixes ω_{E_0}
Equivalently, fixing an element in $\mathrm{Lie}(E_0)$ since $\mathrm{Lie}(E_0) = \mathrm{Hom}(\Omega^1(E_0), k)$ is of dimension 1 over k
- Propagating this choice through our isogenies $\mathcal{F}(I \hookrightarrow R)$ fix equations for E_I (**normalised isogenies**).
- This allows to **keep track of equations** of E (and not work up to isomorphisms)
- Two normalised isogenies $\phi_1, \phi_2 : E_0 \rightarrow E_I$ **induce the same equation** on E_I iff $\psi_1, \psi_2 : I \rightarrow R$ induce the same map $\mathrm{Lie}(E_0) \rightarrow \mathrm{Lie}(E_I)$, so in particular if $\phi_1 \equiv \phi_2 \pmod p$

- **“Differentials = p -level structure”**: recall that $\mathbb{D}(A[p]) = H_{DR}^1(A)$ and that the Frobenius filtration on $A[p]$ corresponds to the Hodge filtration on $H_{DR}^1(A)$ (up to a Frobenius twist)
- So **differentials** are a convenient way to **keep track of p -level structure**

Torsion modules

Proposition (Finite group schemes represented by modules)

A finite group scheme X is induced by a torsion module M iff X is R -embeddable: $X \hookrightarrow A$ ($A = \mathcal{F}(M_A)$), equivalently $X \hookrightarrow E_0^8$

Proof.

Since X is finite, $A \rightarrow B := A/X$ is an isogeny. By the antiequivalence this is represented by a module map $M_B \hookrightarrow M_A$ and we let $M_X = M_A/M_B$. Since \mathcal{F} is exact, $X = \mathcal{F}(M_X)$.

N.B.: M_X encodes both X and an isomorphism class of R -embedding to an abelian variety, we will implicitly work with this class. □

Proposition (Maps induced by modules)

A morphism $X \rightarrow Y$ is induced by a module map $M_Y \rightarrow M_X$ iff there exist embeddings $X \hookrightarrow A_X$, $Y \hookrightarrow A_Y$ such that $X \rightarrow Y$ lifts to $A_X \rightarrow A_Y$ iff for any embeddings $X \hookrightarrow A_X$, $Y \hookrightarrow A_Y$, with $A_Y = \mathcal{F}(M_Y)$ and M_{A_Y} projective, $X \rightarrow Y$ lifts to $A_X \rightarrow A_Y$

Proof.

If $X \rightarrow Y$ lifts, then $A_X \rightarrow A_Y$ is induced by $M_{A_Y} \rightarrow M_{A_X}$. M_X is a quotient of M_{A_X} and M_Y a quotient of M_{A_Y} . The map $M_{A_Y} \rightarrow M_{A_X} \rightarrow M_X$ factors through $M_Y \rightarrow M_X$ since the image of X is in Y and \mathcal{F} is exact. Finally, if $X \rightarrow Y$ is induced by $M_Y \rightarrow M_X$, the map $M_{A_Y} \rightarrow M_Y \rightarrow M_X$ lifts to $M_{A_Y} \rightarrow M_{A_X}$ when M_{A_Y} is projective. □

4 Advanced topics for modules

- Level structures
- Some isogeny constructions from the module point of view
- Ascending and descending isogenies: the conductor square and excision
- (Un)forgetting orientations via comonadic descent
- Non principal polarisations
- Sesquilinear Weil pairings
- Non R -backtracking isogenies

Kani's lemma from the module point of view

$$\begin{array}{ccc} M_0 & \xrightarrow{\psi_1} & M_1 \\ \downarrow \psi_2 & & \downarrow \psi'_2 \\ M_2 & \xrightarrow{\psi'_1} & M_{12} \end{array}$$

- $\psi_1 : (M_0, H_0) \rightarrow (M_1, H_1), \psi'_1 : (M_2, H_2) \rightarrow (M_{12}, H_{12}) : N_1$ -similitudes
- $\psi_2 : (M_0, H_0) \rightarrow (M_2, H_2), \psi'_2 : (M_1, H_1) \rightarrow (M_{12}, H_{12}) : N_2$ -similitudes
- Then $\Psi = \begin{pmatrix} \psi_1 & \hat{\psi}'_1 \\ -\psi_2 & \hat{\psi}'_2 \end{pmatrix} : (M_0 \oplus M_{12}, H_0 \oplus H_{12}) \rightarrow (M_1 \oplus M_2, H_1 \oplus H_2)$ is a $N_1 + N_2$ -similitude
- Bonus: if the module action is effective, we can recover the kernel of $\Phi = \mathcal{F}(\Psi)$ even if $N_1 \wedge N_2 \neq 1$

SIDH from the module point of view

- E_0/\mathbb{F}_{p^2} supersingular, $O_0 = \text{End}(E_0)$
- I_A, I_B left O_0 -ideals of reduced norms N_A, N_B , $N_A \wedge N_B = 1$
- SIDH:

$$\begin{array}{ccc}
 O_0 & \longleftarrow & I_A \\
 \uparrow & & \uparrow \\
 I_B & \longleftarrow & I_A \cap I_B
 \end{array}
 \quad \Leftrightarrow \quad
 \begin{array}{ccc}
 E_0 & \longrightarrow & E_A \\
 \downarrow & & \downarrow \\
 E_B & \longrightarrow & E_{AB}
 \end{array}$$

- Bob publish (the image by \mathcal{F}) of $I_B/N_A \rightarrow O_0/N_A$
- Alice intersect this with I_A to find $I_A \cap I_B/N_A \rightarrow I_A/N_A$ and recover (the image by \mathcal{F}) of $I_A \cap I_B \rightarrow I_B$

More precisely:

- Alice knows $I_A/N_A \rightarrow O_0/N_A$, i.e., $E_0[N_A] \rightarrow E_A[N_A]$
- Pushing this through Bob's isomorphism $E_0[N_A] \simeq E_B[N_A]$ she obtains $I_A/N_A \rightarrow I_B/N_A$, i.e. $E_B[N_A] \rightarrow E_A[N_A]$
- This factors through $(I_A \cap I_B)/N_A$, i.e. through $E_{AB}[N_A]$, so the kernel of the map above gives the kernel of $E_B \rightarrow E_{AB}$

$$\begin{array}{ccc}
 E_0[N_A] & \longrightarrow & E_A[N_A] \\
 \downarrow \wr & & \downarrow \wr \\
 E_B[N_A] & \longrightarrow & E_{AB}[N_A]
 \end{array}$$

SIGamal from the module point of view

$$\begin{array}{ccc} (E_0, P_0) & \longrightarrow & (E_{I_1}, P_1) \\ \downarrow & & \downarrow \\ (E_{I_2}, P_2) & \longrightarrow & (E_{12}, P_{12}) \end{array}$$

- Fix a point $P_0 \in E_0[N]$
- $\psi : I/N \rightarrow R/N \Leftrightarrow E_0[N] \rightarrow E_I[N]$, and this gives a point $P \in E_I[N]$ as the image $\phi(P_0)$
- We can then keep track of various **point images**
- We can also keep track of **equations** through **differentials**

4 Advanced topics for modules

- Level structures
- Some isogeny constructions from the module point of view
- **Ascending and descending isogenies: the conductor square and excision**
- (Un)forgetting orientations via comonadic descent
- Non principal polarisations
- Sesquilinear Weil pairings
- Non R -backtracking isogenies

Ascending and descending isogenies

- $R \subset S$ of conductor f : $R = \mathbb{Z} + fS, f = [S : R], \mathfrak{f} = fS$
- $E_0 \rightarrow E_S$ canonical ascending isogeny of degree f
- $(\mathfrak{f}, H_R/f) \subset (R, H_R) \subset (S, f \times H_R) \Leftrightarrow E_S \rightarrow E_0 \rightarrow E_S \quad (N_R(S) = 1/f)$
- Kernel of ascending isogeny: $E_0[\mathfrak{f}] = E_0[f, \sqrt{\Delta_R}]$
- $R/\mathfrak{f} \hookrightarrow S/\mathfrak{f}$ induces $E_S[f] \rightarrow E_0[\mathfrak{f}]$
- $S = \text{Hom}(E_S, E_0)$ via $E_S \xrightarrow{\alpha} E_S \rightarrow E_0$
- Kernel of descending isogeny: $E_S[R] \subset E_S[f]$, induced by $S/\mathfrak{f} \rightarrow S/R$
- $\sqrt{\Delta_R} = f\sqrt{\Delta_S}$: $E_0 \rightarrow E_S \xrightarrow{\sqrt{\Delta_S}} E_S \rightarrow E_0$
- If $\alpha \in S, \alpha^{-1} : \alpha R \cap R \rightarrow S$ gives another descending isogeny $E_S \rightarrow E_\alpha$

$$\begin{array}{ccc}
 S & \xleftarrow{\alpha} & S \\
 \uparrow & & \uparrow \alpha^{-1} \\
 R & \xleftarrow{\quad} & \alpha R \cap R
 \end{array}
 \quad \Leftrightarrow \quad
 \begin{array}{ccc}
 E_S & \xrightarrow{\alpha} & E_S \\
 \downarrow & & \downarrow \\
 E_0 & \longrightarrow & E_\alpha
 \end{array}$$

Conductor square

$$\begin{array}{ccc} R & \longrightarrow & S \\ \downarrow & & \downarrow \\ R/\mathfrak{f} & \longrightarrow & S/\mathfrak{f} \end{array}$$

- **Excision:** $\mathrm{Spec} R = \mathrm{Spec} S \coprod_{\mathrm{Spec} S/\mathfrak{f}} \mathrm{Spec} R/\mathfrak{f}$
- [Milnor]: M projective on $R \Leftrightarrow M_S$ projective on $S + M_f$ projective on $R/\mathfrak{f} +$ an isomorphism $M_S/\mathfrak{f} \simeq M_f \otimes_{R/\mathfrak{f}} S/\mathfrak{f}$
- Invertible ideal $I_R \Leftrightarrow$ invertible ideal $I_S + S/\mathfrak{f} \simeq I_S/\mathfrak{f}$

Isogeny interpretation:

- $I_R \subset R$ invertible $\Leftrightarrow E_0 \rightarrow E_{I_R}, I_S \subset S$ invertible $\Leftrightarrow E_S \rightarrow E_{I_S}$:

$$\begin{array}{ccc} E_S & \longrightarrow & E_{I_S} \\ \downarrow & & \downarrow \\ E_0 & \longrightarrow & E_{I_R} \end{array}$$

- Isomorphism $I_S/\mathfrak{f} \simeq S/\mathfrak{f} \Leftrightarrow$ isomorphism $E_S[f] \simeq E_{I_S}[f]$
- Encodes the descending isogeny $E_{I_S} \rightarrow E_{I_R}$ as the image of $E_S[R]$ in E_{I_S}
- Since $S/R \simeq R/\mathfrak{f}$ as R -modules, an isomorphism $S/\mathfrak{f} \simeq I_S/\mathfrak{f}$ is the same as a surjection $I_S/\mathfrak{f} \twoheadrightarrow R/\mathfrak{f}$ which extends (via the base change $\cdot \otimes_R S$) to an iso $I_S/\mathfrak{f} \simeq S/\mathfrak{f}$
- This corresponds to $E_0[f] \hookrightarrow E_{I_S}[f]$ (i.e., a cyclic R -stable kernel K in $E_{I_S}[f]$) such that the action of S on K spans the whole of $E_{I_S}[f]$.

4 Advanced topics for modules

- Level structures
- Some isogeny constructions from the module point of view
- Ascending and descending isogenies: the conductor square and excision
- (Un)forgetting orientations via comonadic descent
- Non principal polarisations
- Sesquilinear Weil pairings
- Non R -backtracking isogenies

Forgetting orientations

- E_0 (primitively) R -oriented, $O_0 = \text{End}(E_0)$
- $M \mapsto M' := M \otimes_R O_0$ corresponds to **forgetting the orientation** (M torsion free):
$$\text{Ext}_R^1(M, E_0) \simeq \text{Ext}_{O_0}^1(M', E_0) \text{ as abelian varieties}$$
- Conversely for an O_0 -module M' , an R -orientation on $A_{M'}$ corresponds to finding an R -module M such that $M' = M \otimes_R O_0$
- This is a question of **non commutative descent**, a special case of **comonadic descent**
- A morphism $A_{M'_1} \rightarrow A_{M'_2}$ of R -oriented abelian varieties is **oriented** iff the map $M'_2 \rightarrow M'_1$ **descends** to $M_2 \rightarrow M_1$

Weil's restriction from the module point of view

- E_0/\mathbb{F}_p supersingular with Frobenius orientation, $R = \text{End}_{\mathbb{F}_p}(E_0)$, $O_0 = \text{End}_{\mathbb{F}_{p^2}}(E_0)$
- **Weil's restriction:** $A/\mathbb{F}_{p^2} \mapsto W_{\mathbb{F}_{p^2}/\mathbb{F}_p} A/\mathbb{F}_p$
- If $A \Leftrightarrow M/O_0$, then $W_{\mathbb{F}_{p^2}/\mathbb{F}_p} A$ is represented by the module
$$M' = \text{Hom}_{\mathbb{F}_{p^2}}(W_{\mathbb{F}_{p^2}/\mathbb{F}_p} A, E_0) = \text{Hom}_{\mathbb{F}_{p^2}}(A \oplus A^\sigma, E_0) = \text{Hom}_{\mathbb{F}_{p^2}}(A, E_0) \oplus \text{Hom}_{\mathbb{F}_{p^2}}(A, E_0)^\sigma = M \oplus M^\sigma$$
- Since $A \oplus A^\sigma$ descends to $W_{\mathbb{F}_{p^2}/\mathbb{F}_p} A$ over \mathbb{F}_p , it is represented by a canonical R -module N such that: $M' = M \oplus M^\sigma = N \otimes_R O_0$ (by our result on forgetting the orientation).
- The Frobenius Galois action σ acts on the left and right on $M \oplus M^\sigma$
- Unraveling³ the Morita equivalence between R and O_0 , we get that N is the submodule where these two actions commute
- Abelian variety interpretation: on the supersingular side, $M' = \text{Hom}_{\mathbb{F}_{p^2}}(W_{\mathbb{F}_{p^2}/\mathbb{F}_p} A, E_0)$ while on the oriented side, $N = \text{Hom}_{\mathbb{F}_p}(W_{\mathbb{F}_{p^2}/\mathbb{F}_p} A, E_0)$
- This is indeed the submodule of rational morphisms in $\text{Hom}_{\mathbb{F}_{p^2}}(W_{\mathbb{F}_{p^2}/\mathbb{F}_p} A, E_0)$, i.e., which commute with σ

³With help by Aurel Page!

Various other module constructions

Base change adjunction:

- $M \mapsto M' = M \otimes_R O_0$ has for adjoint $N' \mapsto \text{Hom}_R(R, N')$:

$$\text{Hom}_{O_0}(M \otimes_R O_0, N') = \text{Hom}_R(M, \text{Hom}_R(R, N'))$$

- This sends an abelian variety A' of dimension g to an R -oriented abelian variety A of dimension $2g$ (Not clear how to get a polarisation on A from one on A')
- If X R -oriented, $\text{Hom}(A', X) \simeq \text{Hom}_R(A, X)$

Internal Hom:

- If R commutative, like our (co)tensor product construction $A_1 \otimes_{E_0} A_2$, we can define an **internal (co)hom** construction $\text{Hom}_{E_0}(A_1, A_2)$
- If $A_1 = M_1 \cdot E_0$ and $A_2 = M_2 \cdot E_0$, with M_1, M_2 projective, then $\text{Hom}_{E_0}(A_1, A_2) := \text{Hom}_R(M_2, M_1) \cdot E_0$
- The $\otimes_R \dashv \text{Hom}_R$ adjunction induces a $\text{Hom}_{E_0} \dashv \otimes_{E_0}$ adjunction
- Can we exploit this in isogeny based cryptography?

Change of base point:

- E'_0 **another** primitively R -oriented curve isogeneous to E_0
- If $I := \text{Hom}_R(E'_0, E_0) = I$, I is invertible
- If $\text{Hom}_R(A, E_0) = M$, then $\text{Hom}_R(A, E'_0) = I^{-1}M$
- So $M \mapsto I^{-1}M$ encodes the **change of base point** $E_0 \rightsquigarrow E'_0$ in the antiequivalences of category

4 Advanced topics for modules

- Level structures
- Some isogeny constructions from the module point of view
- Ascending and descending isogenies: the conductor square and excision
- (Un)forgetting orientations via comonadic descent
- **Non principal polarisations**
- Sesquilinear Weil pairings
- Non R -backtracking isogenies

Non principal polarisations

- M torsion free, $V = M \otimes_{\mathbb{Z}} \mathbb{Q}, K = R \otimes_{\mathbb{Z}} \mathbb{Q}$
- H K -hermitian form on V
- R -orthogonal: $M^{\#} := \{v \in V, H(\cdot, v) \subset R\}$
- H induces an isomorphism $M^{\#} \simeq M^{\vee}, m^{\#} \mapsto H(\cdot, m^{\#})$
- H is integral on $M^{\#} \Leftrightarrow M^{\#} \subset M$
- We then obtain a polarisation on $M^{\vee}: M^{\vee} \simeq M^{\#} \subset M$
- This gives a polarisation $\lambda : A \rightarrow A^{\vee}$ with kernel $\mathcal{F}(M/M^{\#})$
- The polarisation $n\lambda$ corresponds to H/n
- Principal polarisation: $M = M^{\#}$

Classifying polarisations

- (M, H_M) principally polarised
- Example: $M = \oplus I_i, H_M = \oplus H_{I_i}$
- **Rosatti involution**: $\alpha \in \text{End}_R(M) \mapsto \alpha^\dagger$ (the adjoint morphism)

Proposition (Polarisations as totally real positive endomorphisms)

All other polarisations on M are of the form

$$H_\alpha(\cdot, \cdot) := H_M(\alpha \cdot, \cdot)$$

for $\alpha \in \text{End}_R(M)$ such that

- α is *real*: $\alpha^\dagger = \alpha$
- α is *totally positive*: H_α is positive definite

And H_α is principal iff α is invertible.

Isotropic kernels and N -isogenies

- (M_1, H_{M_1}) unimodular R -Hermitian, $V = M_1 \otimes_{\mathbb{Z}} \mathbb{Q}$
- $M_2 \subset M_1$ induces a N -similitude iff $M_2^{\#} = NM_2$
- Indeed in this case H_{M_1}/N is unimodular on M_2

- We have $\#M_1/M_2 = \#M_2^{\#}/M_1^{\#}$. In fact, if M_1 is projective,

$$M_2^{\#}/M_1^{\#} \simeq M_2^{\vee}/M_1^{\vee} \simeq \text{Ext}_R^1(M_1/M_2, R) \simeq \text{Hom}_R(M_1/M_2, \text{Frac}(R)/R)$$

- So (for R commutative), $M_2 \subset M_1$ induces a N -similitude iff $H_{M_1} \bmod N = 0$ on $M_2 \times M_2$, and $\#M_1/M_2 = N^g$
- This corresponds to $A_1[M_2]$ being isotropic of degree N^g , i.e. $A_1[M_2]$ being maximal isotropic

4 Advanced topics for modules

- Level structures
- Some isogeny constructions from the module point of view
- Ascending and descending isogenies: the conductor square and excision
- (Un)forgetting orientations via comonadic descent
- Non principal polarisations
- **Sesquilinear Weil pairings**
- Non R -backtracking isogenies

Sesquilinear Weil pairing

- Polarisation $\lambda : A \rightarrow A^\vee \Leftrightarrow M^\vee \rightarrow M$ induced by H on M^\vee ($A = \mathcal{F}(M)$)

- H induces:

$$H \bmod N : M^\vee/N \times M^\vee/N \rightarrow R/N$$

- $M^\vee/N \simeq \operatorname{Hom}_{\overline{R}/N}(M/N, R/N)$, if $N \wedge f_M = 1$

Because the flat locus of M contains $\operatorname{Spec} R/N$

- $x, y \in M^\vee/N$ thus correspond to $x, y : E_0[N] \rightarrow A[N]$

- Fix a point $P_0 \in E_0[N]$, then $x(P_0), y(P_0) \in A[N]$, $N \wedge f_R = 1$

- Sesquilinear pairing [Stange 2024]: $P \mapsto e_{W,N}^{\otimes R}(P_0, P) = e_{W,N}^{\otimes R}(P_0, \alpha(P_0)) = e_{W,N}^{\otimes R}(P_0, P_0)^\alpha$
induces an isomorphism $R/NR \simeq E_0[N](\bar{k}) \simeq \mu_N^{\otimes R}$

- $e_{W,N\lambda}^{\otimes R}(x(P_0), y(P_0)) \in \mu_N^{\otimes R}$ corresponds via this isomorphism to $H(x, y) \in R/N$

- N -sesquilinear pairings \Leftrightarrow Hermitian forms modulo N

4 Advanced topics for modules

- Level structures
- Some isogeny constructions from the module point of view
- Ascending and descending isogenies: the conductor square and excision
- (Un)forgetting orientations via comonadic descent
- Non principal polarisations
- Sesquilinear Weil pairings
- Non R -backtracking isogenies

Non R -backtracking isogenies

Non (partially) backtracking isogeny:

- $\phi : A \rightarrow B$ N -isogeny is non partially backtracking (nbt) $\Leftrightarrow \text{Ker } \phi$ of rank g
- $\phi_1 : A_1 \rightarrow A_2, \phi_2 : A_2 \rightarrow A_3$ nbt, then $\phi_2 \circ \phi_1$ nbt iff $\text{Ker } \phi_2 \cap \widetilde{\text{Ker } \phi_1} = 0$
- If $\phi_2 \circ \phi_1$ is nbt, ϕ_1, ϕ_2 is nbt
- If $\phi : A \rightarrow B$ nbt N -isogeny, and $N = \prod \ell_i$, ϕ uniquely decomposes as $\phi = \prod \phi_i$, with ϕ_i a ℓ_i -isogeny

Non R -backtracking isogeny: Assume all degrees prime to the conductor of R

- $\phi : A \rightarrow B$ is non R -backtracking iff it is nbt and does not come from the action of an ideal I
- If ϕ is nbt but comes from I , $\phi = \phi_2 \circ \phi_1$, then ϕ_i comes from I_i
- If ϕ nbt, it suffices to check that some subgroup $\text{Ker } \phi[\ell^e]$ is not induced by an ideal to know that ϕ is not R -backtracking

Combined with the following lemma, this gives a way to check that the response is not R -backtracking through the challenge for SQISurf:

Lemma

$\phi_1 : A_1 \rightarrow A_2, \phi_2 : A_2 \rightarrow A_3, \phi_3 : A_3 \rightarrow A_4, \phi_4 : A_4 \rightarrow A_5$ such that $\phi_2 \circ \phi_1, \phi_3 \circ \phi_2$ and $\phi_4 \circ \phi_3$ are nbt. Then $\phi_4 \circ \phi_3 \circ \phi_2 \circ \phi_1$ is ℓ -nbt for each $\ell \mid \# \text{Ker } \phi_2 \wedge \# \text{Ker } \phi_3$, i.e. the ℓ -Sylow of its kernel is of rank g

Conclusion: the module equivalence of category

- **Module equivalence of category**: more natural than the ideal one.
Clear distinction of **objects** and **morphisms**
 - Many algorithmic operations in dimension 1 (e.g., double path to E_0) come from the module interpretation
 - Generalizes to higher dimension
 - Keep track of level structure and sesquilinear pairings
 - Unified framework to handle oriented and supersingular case (still modules, but different rings)
- ⇒ Forgetting the orientation or Weil restrictions purely at the module level

- **New cryptographic protocols?**
- Exploit further the **tensor category** structure on $(R - \text{mod}, \oplus, \otimes)$, the internal (co)hom structure $\text{Hom}_{E_0}(A_1, A_2)$ and the $\text{Hom}_{E_0} \dashv \otimes_{E_0}$ adjunction?

The symmetric monoidal action framework

Theorem (Base point free version of the antiequivalence of category)

There is a *faithful effective symmetric monoidal (co)-action* (given by the canonical *copower* construction) from *projective R -modules to abelian varieties R -isogeneous to a product of R -oriented elliptic curves*. It extends to an action of *Hermitian projective modules to polarised abelian varieties*.

If E_0 is any primitively oriented curve, the action is *free* with image abelian varieties “horizontally” isogeneous to E_0^g (meaning that $\text{Hom}_R(A, E_0)$ is projective) and with the same R/pR representation on their tangent space as for E_0^g .

- Let R be the maximal order of $\mathbb{Z}[\sqrt{-p}]$, E_0/\mathbb{F}_p be any curve R -oriented, and $O_0 = \text{End}(E_0)$. Via Weil’s restriction, we can recast the *supersingular isogeny path problem* $E_0 \rightarrow E/\mathbb{F}_{p^2}$ to a *rank 2 module action inversion* between E_0 and $W_{\mathbb{F}_{p^2}/\mathbb{F}_p} E$.
- Conversely, abelian surfaces that are Weil restriction corresponds to R -modules M of rank 2 such that $M \otimes_R O_0 = M' \oplus M'^\sigma$ for a right O_0 -ideal M' , with the decomposition induced by the polarisation
- We can extend the action to incorporate *level structure* (which we represent as a morphism M/nM to some explicit torsion module)
- We could probably *reformulate most of supersingular isogeny based cryptography* in terms of this monoidal action. This somewhat unify the oriented and supersingular case, the difference between the two being whether we apply rank 1 or rank 2 module actions.

The symmetric monoidal action from

Theorem (Base point free)

There is a faithful effective

from projective K

extends to an action

If E_0 is any

isogeneous

their tangent

We can act on supersingular
abelian varieties over \mathbb{F}_p by
Hermitian $\mathbb{Z}[\sqrt{-p}]$ -modules!

Supersingular curves over
 \mathbb{F}_p are given by an action
of rank 1 from E_0 while the
ones over \mathbb{F}_{p^2} are given
by an action of rank 2!

- Let

- V

- K

- E_0

- Co

- the

- pola

- E_0

- E_0

- We can

- M/nM to

- We could proba

- this monoidal action

- between the two being w

power construction)

elliptic curves. It

"

station on

E_0)

to a

E_0)

to a

2 such

by the

orphism

why in terms of

the difference

the action is