Isogeny++: From ideals to modules

2024/05/24 — Quantum Safe Workshop, IBM Research Zurich

Damien Robert

Équipe Canari, Inria Bordeaux Sud-Ouest

From ideals to modules

- Lattices: RingLWE → ModuleLWE
- Codes: Hamming metric → Sum Rank metric
- Isogenies: Ideals → Modules?
  Dimension 1 → Dimension g?

☹ Increasing dimension in isogeny based cryptography is costly…

☺ Dimension 2 already provides a lot of flexibility (Kani…)

- Open question: is it worth it? (Beyond Kani!)

Ideals and isogenies: the oriented case

- $E/k, k = \mathbb{F}_q$, elliptic curve with a primitive orientation by a quadratic imaginary order $R = \mathbb{Z}[\sqrt{-\Delta}] \hookrightarrow \mathrm{End}_k(E)$
- Oriented isogeny: $\phi : E_1 \to E_2$ that commutes with the orientations
- Oriented kernel: K stable by R

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

Example: Frobenius orientation

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

- Invertible ideals I of $R \Leftrightarrow$ oriented horizontal isogenies $\phi_I : E \to E_I$ [Colò-Kohel 2020, Onuki 2020]
- $K = \mathrm{Ker}\,\phi_I = E[I], \quad I = \{\alpha \in R \mid \alpha(K) = 0\}, \quad \deg \phi_I = N(I)$
- $\widetilde{\phi_I} = \phi_{\bar{I}} : E_I \to E$
- $I \simeq J \Leftrightarrow E_I \simeq E_J$

- Special case: p inert in R (can only happen for an orientation on a supersingular curve $E/\mathbb{F}_{p^2}$)
- $\pi_p : E \to E^\sigma$ is not represented by an ideal
- $\rho_R(E)$ representation of R on the k-vector space $T_0(E)$
- an oriented isogeny $\phi : E \to E'$ comes from an ideal iff the representations $\rho_R(E)$ and $\rho_R(E')$ are equivalent.

Ideal and isogenies: the supersingular case

- Deuring correspondance
- maximal orders in $B_{p,\infty}$ = supersingular curves $E/\mathbb{F}_{p^2}$ (up to quadratic twists and Galois conjugates)
- ideals = isogenies; $\deg \phi_I = N(I) := \mathrm{nrd}(I)$

Ideal to isogeny: $I \Leftrightarrow E[I]$

- Easy if $\mathrm{End}(E)$ known, $N(I)$ smooth and $N(I)$-torsion accessible
- Many algorithms to handle the general case: KLPT, Eichler orders, refreshing the torsion, endomorphisms, Clapotis…
- Lots of research effort

☺ SQISign and variants

A general equivalence of category

- E_0/k primitively oriented by R quadratic imaginary ($\mathcal{Z}(R) = R$)
- $E_0/k = \mathbb{F}_{p^2}$ with $R = \mathtt{End}(E_0)$ maximal quaternionic order ($\mathcal{Z}(R) = \mathbb{Z}$)

Theorem

There is an antiequivalence of category between the category of $\mathcal{Z}(R)$-oriented abelian varieties A k-isogenous to E_0^g (with the technical condition $\rho_{\mathcal{Z}(R)}(A) \simeq \oplus_{i=1}^g \rho_{\mathcal{Z}(R)}(E_0)$) and $\mathcal{Z}(R)$-oriented k-morphisms; and the category of finitely presented torsion free (left) R-modules M of rank g and R-module morphisms

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

Alternative approaches to equivalences of category of abelian varieties via lifting to characteristic zero: Deligne, Howe, Marseglia…

Corollary

- *principal polarisation* $\lambda_A : A \to \widehat{A}$ = *a unimodular Hermitian R-form* H_A *on* M_A
- *N-isogeny* $\phi : (A, \lambda_A) \to (B, \lambda_B)$ = *N-similitude* $\Phi : (M_B, H_B) \to (M_A, H_A)$:

$$\Phi^* H_A = N H_B$$

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

The equivalence

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

Definition

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

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

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

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

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

Warmup: ideals

The oriented case:

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

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

- 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 ($R = O_0$):

- 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 $O_R(I)$

N.B.: could use duality to get an equivalence of categories, but contravarience is more practical

Modules to abelian varieties

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

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

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

- $E_0 \to E_0^2, P \mapsto (\alpha P, \beta P)$ 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 $E_0^2 \to E_0, (P, Q) \mapsto uP + vQ$

Module to explicit abelian variety:

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

❦ There are unimodular Hermitian R-modules such that no such N-similitude exist for any N, c.f. the arithmetic obstructions in [Kirschmer, Narbonne, Ritzenthaler, R. 2021]

Abelian variety to module:

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

  Example: a double path $E_I \to E_0$!
- 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). N.B.: Explicit endomorphisms on $E_0 \Leftrightarrow$ abstract endomorphisms.
- $A \hookrightarrow E_0^n \to E_0^m$ gives M_A

Similitudes to isogenies

Module morphism to morphism of abelian varieties:

$$\begin{array}{ccccccc}
R^{m_1} & \longrightarrow & R^{n_1} & \twoheadrightarrow & M_1 & \longrightarrow & 0 \\
\uparrow\vdots & & \uparrow\vdots & & \uparrow & & \\
R^{m_2} & \longrightarrow & R^{n_2} & \twoheadrightarrow & M_2 & \longrightarrow & 0
\end{array}$$

$$\begin{array}{ccccccc}
0 & \longrightarrow & A_1 & \hookrightarrow & E_0^{n_1} & \longrightarrow & E_0^{m_1} \\
 & & \downarrow & & \vdots\downarrow & & \vdots\downarrow \\
0 & \longrightarrow & A_2 & \hookrightarrow & E_0^{n_2} & \longrightarrow & E_0^{m_2}
\end{array}$$

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
- $\phi : A_1 \twoheadrightarrow A_2 \Leftrightarrow (M_2, H/N) \subset (M_1, H)$

  An isogeny is an epimorphism (with finite kernel) so corresponds to a monomorphism (=inclusion) of modules (with finite cokernel)
- $\operatorname{Ker} \phi = A_1[M_2]$
- Equivalence practical if N smooth and the N-torsion on E_0 is accessible
- **Open question for the general case**: ModuleKLPT?

Cryptographic applications?

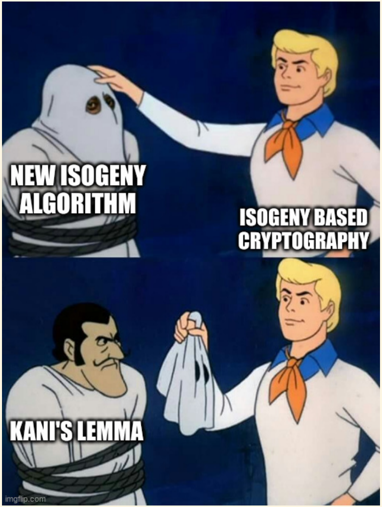
[Page-R. 2023]

- Clapotis: CLass group Action in POlynomial TIme via Sesquilinear forms
- Original motivation for this work: “new” ModuleKLPT algorithm for $M = I \oplus \bar{I} \subset R \oplus R$

Cryptographic applications?

[Page-R. 2023]

- Clapotis: CLass group Action in POlynomial TIme via Sesquilinear forms
- Original motivation for this work: "new" ModuleKLPT algorithm for $M = I \oplus \bar{I} \subset R \oplus R$
- Clapoti: bypass the equivalence of category by just using Kani… again…



Cryptographic applications?

[Page-R. 2023]

- Clapotis: CLass group Action in POlynomial TIme via Sesquilinear forms
- Original motivation for this work: "new" ModuleKLPT algorithm for $M = I \oplus \bar{I} \subset R \oplus R$
- Clapoti: bypass the equivalence of category by just using Kani… again…

Help needed! Any interesting cryptographic application of modules?

Strong assumption: we can extend in dimension g all our algorithmic tools and security assumptions from dimension 1 to dimension g

- ModuleSQISign: Short signatures for oriented isogenies?
- ModuleSIDH: combining torsion noise and oriented commutative group action for key exchange?

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
- $A \simeq E_0^{g-1} \times E_I$
- $\# \mathrm{Cl}(R)$ isomorphism classes of non-polarised R-oriented abelian varieties R-isogenous to E_0^g

- Polarisations add supersingular like graph complexity if $g > 1$ $(\mathrm{End}_R(E_0^g) = M_g(R))$
- Universal group action: $I \cdot (M, H_M) = (IM, H_M/N(I)) \subset (M, H_M)$
- $I \cdot A = A_I := A/A[I]$
- Intuition: multiplication by $[n] \Rightarrow$ multiplication by $[I]$
- Multiple orbits; linked together by oriented isogenies (which are not multiplication by $[I]$)

Example:

- $E_0/\mathbb{F}_p$ supersingular and $g = 2$: graph of supersingular abelian surfaces isogeneous to E_0^2 over $\mathbb{F}_p$ and $\mathbb{F}_p$-rational isogenies
  The graph contains the Weil restriction $W_{\mathbb{F}_{p^2}/\mathbb{F}_p} E$ of supersingular elliptiptic curves over $\mathbb{F}_{p^2}$ (these are neither Jacobians nor product of curves over $\mathbb{F}_p$).
- Conjecture: $\approx p^{3/2}$ nodes
- Universal group action from $\mathrm{Cl}(\mathbb{Z}[\sqrt{-p}])$
- If $\ell = \mathfrak{l}\bar{\mathfrak{l}}$ splits in R, $A[\ell] = A[\mathfrak{l}] \oplus A[\bar{\mathfrak{l}}] \Rightarrow$ action by $\mathfrak{l}$ and $\bar{\mathfrak{l}}$
  $(+\ \ell + 1$ other R-oriented ℓ-isogenies?)

ModuleSQISign: Short signatures for oriented isogenies?

- $\phi_I : E_0 \to E_I$
- Recovering I from (E_0, E_I) ⇔ recovering the module associated to $E_0 \times E_I$
  $E_0 \times E_I$ is doubly oriented!

⇒ SQISign like protocol in dimension 2 (not SQISign2d!)

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

- 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: the commitment should probably not be R-backtracking either

- Needs a generalised ModuleToIsogeny for the response

ModuleSIDH: 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

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

- 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 $\mathrm{Cl}(\mathbb{Z}[\sqrt{-p}])$ in dimension 2
- Size: $p = 4\lambda$ (or 6λ?); $J(A_{a_2})$: $3\log_2(p)$; torsion on deterministic R-basis: $4\log_2(p)$ (or $3\log_2 p$ using pairings?)
  Total: $6\log_2 p = 24\lambda$ (vs $3.5\log_2 p$ for SIDH)

Conclusion: the module equivalence of category

- The module equivalence of category is often more natural than the ideal one: clear distinction of objects and morphisms
- Many algorithmic operations already done in dimension 1 (e.g., double path to E_0) come from the module interpretation
- Unified framework to handle the oriented and supersingular case (still modules, but different rings)

⇒ Can keep track of forgetting the orientation or Weil restrictions purely at the module level

- Generalizes to higher dimension
- Also able to keep track of level structure

  The current methods implicitly use the conductor square and excision to embed level structure information via suborders of conductor divisible by the level, but that's arguably less natural
- New cryptographic protocols?

Torsion free f.p. R-modules

- In both cases: rank 1 torsion free module = ideal

Oriented case (R is a Bass ring)

- $M \simeq I_1 \oplus I_2 \oplus \cdots \oplus I_g$
- $R \subset O(I_1) \subset O(I_2) \subset \cdots \subset O(I_g)$
- $\det M = I_1 \cdot I_2 \cdots \cdot I_g$ invertible R_g-ideal
- The isomorphism class of M only depend on $(R_1, \ldots, R_g)$ and $\det M$

- Example: if all I_j are invertible in R ($\Leftrightarrow O(I_j) = R$),

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

Supersingular case

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

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
- Orthogonal: $M^\sharp = \{v \in V, H(\cdot, v) \subset R\}$

- H induces an isomorphism $M^\sharp \simeq M^\vee, m^\sharp \mapsto H(\cdot, m^\sharp)$
- H is integral on $M^\sharp$ $\Leftrightarrow M^\sharp \subset M$
- We then obtain a polarisation on $M^\vee$: $M^\vee \simeq M^\sharp \subset M$
- This gives a polarisation $\lambda : A \to A^\vee$ with kernel $\mathbb{F}(M/M^\sharp)$
- The polarisation $n\lambda$ corresponds to H/n

- Principal polarisation: $M = M^\sharp$

Non R-backtracking isogenies

Non (partially) backtracking isogeny:

- $\phi : A \to B$ N-isogeny is non partially backtracking (nbt) $\Leftrightarrow$ Ker ϕ of rank g
- $\phi_1 : A_1 \to A_2, \phi_2 : A_2 \to A_3$ nbt, then $\phi_2 \circ \phi_1$ nbt iff Ker $\phi_2 \cap$ Ker $\widetilde{\phi_1} = 0$
- If $\phi_2 \circ \phi_1$ is nbt, ϕ_1, ϕ_2 is nbt
- If $\phi : A \to B$ 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

- $\phi : A \to B$ 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 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 ModuleSQISign:

Lemma

$\phi_1 : A_1 \to A_2, \phi_2 : A_2 \to A_3, \phi_3 : A_3 \to A_4, \phi_4 : A_4 \to A_5$ 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 $\ell \mid \#\,\mathrm{Ker}\,\phi_2 \wedge \#\,\mathrm{Ker}\,\phi_3$, i.e. the ℓ-Sylow of its kernel is of rank g