The module action for isogeny based cryptography

Damien Robert

The module action for isogeny based cryptography

DAMIEN ROBERT

Abstract. We extend the usual ideal action on oriented elliptic curves to a (Hermitian) module action on oriented (polarised) abelian varieties. Oriented abelian varieties are naturally enriched in R-modules, and our module action comes from the canonical power object construction on categories enriched in a closed symmetric monoidal category. In particular our action is canonical and gives a fully fledged symmetric monoidal action. Furthermore, we give algorithms to compute this action in practice, generalising the usual algorithms in rank 1.

The action allows us to unify in the same framework, on the one hand isogeny based cryptography based on ordinary or oriented elliptic curves, and on the other hand the one based on supersingular elliptic curves defined over $\mathbb{F}_{p^2}$. In particular, from our point of view, supersingular elliptic curves over $\mathbb{F}_p$ are given by a rank 1 module action, while (the Weil restriction) of those defined over $\mathbb{F}_{p^2}$ are given by a rank 2 module action. As a consequence, rank 2 module action inversion is at least as hard as the supersingular isogeny path problem.

We thus propose to use Hermitian modules as an avatar of a cryptographic symmetric monoidal action framework. This generalizes the more standard cryptographic group action framework, and still allows for a NIKE (Non Interactive Key Exchange). The main advantage of our action is that, presumably, Kuperberg's algorithm does not apply. Compared to CSIDH, this allows for more compact keys and much better scaling properties.

In practice, we propose the key exchange scheme $\otimes$-MIKE (Tensor Module Isogeny Key Exchange). Alice and Bob start from a supersingular elliptic curve $E_0/\mathbb{F}_p$ and both compute an isogeny over $\mathbb{F}_{p^2}$. They each send the j-invariant of their curve. Crucially, unlike SIDH, no torsion information at all is required. Their common secret, given by the module action, is then a dimension 4 principally polarised abelian variety. We obtain a very compact post-quantum NIKE: only 64B for NIST level 1 security.

1. Introduction

The ideal group action on elliptic curve was first introduced for cryptography in [Cou06]), and revisited in [RS06; DKS18]: this is the CRS key exchange. The first efficient instantiation was CSIDH [CLMPR18]. In particular, CSIDH-512 use supersingular elliptic curves over $\mathbb{F}_p$, with p of 512 bits. The key exchange uses the j-invariant, which only takes 64B.

Unfortunately, ulterior analysis [BS20; Pei20] cast in doubt the NIST-1 security of CSIDH-512. Current recommandations for p range between 2000b and 5000b, greatly increasing the size of the CSIDH key exchange. Due to the subexponential attacks on group actions given by Kuperberg's algorithm [Kup05], higher security parameters need even larger keys.

1.1. Contributions.

The purpose of this article is as follows:

(1) We introduce the symmetric monoidal action framework, which generalizes the more standard group action framework. Since we don't have a group anymore, the action is less flexible, but it is still possible to do a standard Diffie-Hellman like key exchange, hence use it as a NIKE (and so as a PKE as usual). On the other hand, the lack of a group is also a strength from a security perspective, since presumably Kuperberg's algorithm does not apply anymore (see Remark 3.4).

(2) We instantiate this framework in the context of isogeny based cryptography on R-oriented elliptic curves and abelian varieties, for R a quadratic imaginary order (or more generally a CM order). Our action will be given by projective unimodular Hermitian R-modules.

Date: October 18, 2024.
Key words and phrases. Keywords: isogenies, module action.
Funded by ANR Ciao (ANR-19-CE48-0008).

Given two R-oriented abelian varieties A, B, the set of R-morphisms $\mathrm{Hom}_R(A,B)$ has naturally a R-module structure: we will be working with a category enriched in R-modules. The category of R-modules is closed symmetric monoidal for the tensor product $\otimes_R$, and is even a tensor category. From these properties, one can define a power object $\mathcal{HOM}_R(M,A)$ canonically, whenever it exists as an abelian variety; we then define $M \cdot A$ as $\mathcal{HOM}_R(M,A)$. (There is also a copower object $M \otimes_R A$.) The main results of this paper, are first that the power object does exist when M is projective[1] (this is well known to specialists, see Section 1.2), secondly that we can incorporate polarisations by looking at Hermitian forms, and finally that we can compute this action in practice.

(3) We show how, via the Weil restriction, the isogeny path problem for supersingular elliptic curves over $\mathbb{F}_{p^2}$ reduces to solving the module action inversion problem for rank 2 modules over $R = \mathbb{Z}[\sqrt{-p}]$. By contrast, rank 1 projective modules are precisely (isomorphism classes of) invertible ideals, which form the Picard group of R (precisely the group used in the CSIDH action), and so the rank 1 module inversion is susceptible to Kuperberg's algorithm. This point of view allows on one hand to both unify the oriented isogeny path problem and the supersingular isogeny path problem as two instances of module inversion, and on the other hand to interpret the different complexity of the best algorithms available to solve these problems as coming from the rank of the modules involved.

(4) We introduce $\otimes$-MIKE (Tensor Module Isogeny Key Exchange) a novel NIKE. The setup is similar to SIDH: we start from an elliptic curve $E_0/\mathbb{F}_p$, and Alice and Bob computes isogenies over $\mathbb{F}_{p^2}$: $E_0 \to E_A$ and $E_0 \to E_B$ respectively. They send $j(E_A) \in \mathbb{F}_{p^2}$ and $j(E_B) \in \mathbb{F}_{p^2}$. Upon receiving $j(E_B)$, Alice acts on its Weil restriction $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_B)$ by the module M_A encoded by the isogeny $E_0 \to E_A$ (or more precisely, such that $M_A \cdot E_0 = W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_A)$) and constructs $M_A \cdot W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_B) = M_A \cdot M_B \cdot E_0 = (M_A \otimes_R M_B) \cdot E_0$, which is a dimension 4 principally polarised abelian variety. Bob obtains the same variety, up to isomorphism over $\mathbb{F}_p$. The key exchange requires only the j-invariants which live over $\mathbb{F}_{p^2}$. This is a crucial difference compared to SIDH [JD11; DJP14], which relied on computing the pushforward of Alice and Bob isogenies as a common key, and needed additional torsion point information for this computation, which led to its downfall [CD23; MMPPW23; Rob23]. We argue that this module action, rather than the pushforward, is the correct generalisation of the ideal action for a key exchange involving supersingular curves over $\mathbb{F}_{p^2}$.

The security of our key exchange relies on the module action CDH problem. Under the heuristic assumption that the best attack against action-CDH is the module action inversion, which we have seen is at least as hard as the supersingular isogeny path problem, we can take our parameters as follows. For a security level of λ, we need to use p of size $\approx 2\lambda$, and so $j(E_A)$ will be of size $\approx 4\lambda$. In particular, for NIST level 1, the key exchange takes 64B, as with the original CSIDH-512 parameters, and for NIST level 5 the key exchange takes 128B.

We stress that there is currently no implementation of $\otimes$-MIKE, even in a high level language. We will thus refrain, except briefly in the conclusion in Section 7, to comment on the efficiency of the key exchange, as this will only be speculative.

Remark 1.1. In a prior version of this paper, the author foolishly claimed that Alice and Bob could use isogenies of the same degree 2^n for $\otimes$-MIKE. On further thoughts, this is probably a very bad idea: if the dimension 2 isogenies are represented by two 2^n-submodules M_1, M_2 of R^2 respectively, as explained in Remark 6.2 there are many cases where there is a full cancellation in the tensor product $M_1 \otimes_R M_2 \simeq R^4$ (as unimodular Hermitian modules), which make action-CDH trivial to break in these cases. Pending further examination of this cancellation phenomena (could we guaranty dimension 2 isogeny choices such that there are still enough isomorphism classes of the unimodular modules $M_1 \otimes_R M_2$ with respect to the security parameter?), it seems prudent to stick to isogenies of coprime degrees for Alice and Bob. Unfortunately, this impacts the performance of MIKE.

[1] We can relax in some cases the projectivity condition, see Theorem 4.17

1.2. **History.** Using power and copower objects to study abelian varieties has a long history. We will see that if R is a ring, M a left (resp. right) finitely presented (f.p.) R-module and A an abelian variety oriented by R, the power $\mathcal{HOM}_R(M, A)$ and copower $M \otimes_R A$ objects of A under M exist as proper commutative group schemes.

These constructions have notably been used by Serre in his 1985 course on rational points on curves over finite fields (see [SHOR20] for a modern edition). Earlier references are [Gir68, § 1; Wat69, Appendix], which credit Serre and Tate for this construction. In that course, Serre mainly uses the copower object construction $M \otimes_R E$ on elliptic curves, the main advantage is that the copower is automatically an abelian variety, since it is built as a cokernel.

In this article, we will use the power object construction $\mathcal{HOM}_R(M, A)$ on abelian varieties instead. The power object is built as a kernel, so is just a proper group scheme in general (the kernel of a morphism of abelian varieties may not be connected). But, when M is projective, as explained by Serre already, it is easy to see that $\mathcal{HOM}_R(M, A)$ is an abelian variety (see Section 4.2). The main advantage of the power object construction, is that it behaves better when applied to torsion modules: $\mathcal{HOM}_R(R/n, A) = A[n]$ while $R/n \otimes_R A = 0$.

So the power and copower construction on abelian varieties have a long history, and we only make a modest pedagogical contribution in their presentations. We first remark that in the case that R is commutative, then the power object $A' = \mathcal{HOM}_R(M, A)$ has a natural R-orientation (we warn that A' may just be a group scheme), and likewise for the copower object (this would not work for R non commutative). This means that we can apply the power/copower object construction on A' again, and so on. In other words, we see $\mathcal{HOM}_R(\cdot, \cdot)$ as a functor on M and on A, and so we can restate the power/copower construction as a symmetric monoidal action from the category of R-modules to the category of R-oriented proper commutative group schemes. The copower construction gives a covariant action, while the power construction a contravariant action. We hope that the analogy with the more well known group action will render the construction more palatable to a wider cryptographic audience. In this article we will use the contravariant power construction, and so will denote $M \cdot A := \mathcal{HOM}_R(M, A)$. If M is projective and A abelian, $M \cdot A$ is an abelian variety.

Our focus in this paper are in the algorithmic aspects. We continue a line of work initiated in [KNRR21] for the Frobenius orientation, and continued in [PR23a] for arbitrary orientations, where we gave algorithms to compute the power objects on elliptic curves, and extend these algorithms to general abelian varieties (but, for ease of exposition, mainly for a imaginary quadratic orientation R). For this, we make use of the full modern toolbox of isogenies and their efficient representations (for which we refer to the survey [Rob24b]). For these algorithmic aspects, we need to work with polarised abelian varieties. As explained by Serre already, the natural pendant of polarisations on the module side is given by positive definite Hermitian forms. We will give algorithms in Section 4.5 for translating a n-similitude between unimodular Hermitian modules to its corresponding n-isogeny.

The natural cryptographic application of a symmetric monoidal action is a Diffie-Hellman like key exchange (exactly as in group actions). For efficiency reasons we start with an elliptic curve E_0 as a base point. So it makes sense to study the power object construction in more detail on E_0 and its orbit under the monoidal action. This study has already been done in [JKP+18] (for the Frobenius orientation, and extended in [PR23a] for an arbitrary orientation, and we remark that Serre had already proved a covariant equivalence using the copower construction in the case that R is maximal). The authors of [JKP+18] show that the action is particularly well behaved. Namely, if E_0 is primitively oriented by a imaginary quadratic order R, then $\mathcal{HOM}_R(M, E_0)$ is an abelian variety (and not just a group scheme) whenever M is torsion free, and if $\mathfrak{Ab}_{E_0,R}$ denotes the orbit of E_0 under torsion free f.p. R-modules (a different definition is given in Definition 4.15, but Theorem 4.9 shows that these definitions are equivalent), then $M \mapsto M \cdot E_0$ is an antiequivalence of category between torsion free f.p. modules and $\mathfrak{Ab}_{E_0,R}$. This antiequivalence of category is very powerful, and we explored some applications in our talk [Rob24a]. Many other equivalence of categories between abelian varieties over finite fields and "linear algebra data" have been constructed through the years, see [Wat69; Del69; How95; Kan11; Yu12; CS15; CS23; BKM23; BKM24] for some examples.

In this article, we will use it to extend the range of applications of our monoidal action: namely if $A \in \mathfrak{Ab}_{E_0,R}$ and M just torsion free, we give a criteria in Theorem 4.17 for when $M \cdot A$ is still an abelian variety. This extra generality can be useful: for instance if R is not maximal and $R \subset S$, then the going up isogeny $E_0 \to E_S$ is given by the action of the conductor ideal $\mathfrak{f}_{S/R}$ on E_0. This conductor ideal is not a projective R-module. However, for the key exchange $\otimes$-MIKE, we only need to use the rank 2 projective module action, so the reader may skip the more general torsion free case.

Moving on from algorithms to cryptographic applications, our symmetric monoidal action framework is a natural generalisation of the group action framework, first introduced in 1997 by Couveignes [Cou06], using the action of invertible ideals on elliptic curves. Indeed, our action use (projective) modules on oriented abelian varieties. In Section 3.2, we stress that the advantage of the monoidal point of view is not really moving from a (commutative) group to a (commutative) monoid, but that it allows us to handle morphisms, and action by morphisms on objects (or other morphisms). The ideal class group action on elliptic curve is already better understood via the monoidal framework, because an ideal can also act on an oriented isogeny (via the obvious commutative diagram), or a morphism between ideals act on an elliptic curve. Many constructions in isogeny based cryptography implicitly use this morphism action. Although we do not have a killer application of this point of view (i.e., putting objects and morphisms on the same footing), we hope it can help clarify existing constructions. Our own application of the module key exchange $\otimes$-MIKE, on the surface only use the object action, by modules on abelian varieties. But as explained in Section 4.5, to compute $M \cdot A$ in practice, one solution is to find a nice similitude $R^g \to M$ and act by this similitude to get a nice isogeny $R^g \cdot A \simeq A^g \to M \cdot A$, so we actually act by a morphism on A under the hood. This was already true for computing the ideal action: when computing $I \cdot E_0$, the choice of a nice (e.g. smooth) equivalent ideal $J \sim I$ can be reframed as a choice of a nice similitude $I \hookrightarrow R$, from which we can compute the isogeny $E_0 \to I \cdot E_0$ via its kernel, and recover the codomain $I \cdot E_0$.

Finally, it has already been remarked several times in the literature that, although by contrast to oriented isogenies, there is no apparent group action involved in supersingular isogeny cryptography, there are hidden actions involved in the supersingular isogeny path problem.

For instance, to solve a N-isogeny path problem between E_0 and E, [KMPW21; KP23, § 5.3] describe an action from $\mathrm{PGL}_2(\mathbb{Z}/N\mathbb{Z})$ (via, if $K = \mathrm{Ker}\,\phi : E_0 \to E$, $\alpha \cdot E_0 = E_0/\alpha(K)$), which can be computed if enough point images for the isogeny ϕ are known. But it is not known how to compute this action without this information.

Another example, much closer to the ideal inversion problem for CRS/CSIDH, is the uber isogeny problem, first introduced in [DDF+21] (see also [Wes22a]). The R-Uber isogeny problem is, given an R-oriented elliptic curve E_0 and an R-orientable E, to find an ideal $\mathfrak{a} \subset R$ such that $E = \mathfrak{a} \cdot E_0$. In [DDF+21, Proposition 5.10], it is shown how the supersingular path problem between E_0 and E reduces to the R-Uber problem, for R an order of large enough conductor ℓ^e for a suitable small ℓ. The main reason that quantum attacks based on malleability oracle (namely, the hidden shift problem), do not apply for R-Uber, is that since the orientation on E is unknown, it is not possible to compute the actions of R-ideals on E. To make the orientation effective would involve to find a suitable endomorphism α on E (such that $R = \mathbb{Z}[\alpha]$), but even just finding a random (non trivial) endomorphism on a random supersingular curve is a hard problem [PW24].

As mentioned in Section 1.1, we have a new reduction, via the Weil restriction, between the supersingular isogeny path problem and the rank 2 R-module inversion problem, with $R = \mathbb{Z}[\sqrt{-p}]$. Namely, if E_0 is defined over $\mathbb{F}_p$ (and primitively oriented by the Frobenius), then given $(E_0, W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E))$, the module inversion problem requires to find the rank 2 unimodular module such that $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E) = M \cdot E_0$ (we remark that M is projective, see Section 5). From M, we can recover the ideal $I = \mathrm{Hom}_{\mathbb{F}_{p^2}}(E, E_0)$, see Theorem 5.5. Taking the Weil restriction solves the orientation problem of Uber-isogeny: we have the natural Frobenius orientation on $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$, and we can act by modules both on E_0 and on $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$. On the other hand, we now have a dimension 2 abelian variety, so we need to solve inversion for a rank 2 module rather than an ideal. Still, this is probably the reduction that gives the closest analogy

between solving the CRS/CSIDH path problem and solving the supersingular isogeny problem, the only difference between the two problems being the rank of the modules involved.

1.3. **Terminology.** By $\mathrm{End}(E)$ we mean the endomorphism ring over the algebraic closure, and by $\mathrm{End}_{\mathbb{F}_q}(E)$ the subring of endomorphisms defined over $\mathbb{F}_q$.

When we say that $E/\mathbb{F}_{p^2}$ is a supersingular curve, we will always mean a supersingular curve that has maximal endomorphism ring (i.e. its endomorphism ring over $\mathbb{F}_{p^2}$ is a quaternion algebra, i.e. $\mathrm{End}(E) = \mathrm{End}_{\mathbb{F}_{p^2}}(E)$). Such a curve is either maximal or minimal (i.e. $\#E = (p+1)^2$ or $\#E = (p-1)^2$, equivalently $[\pi_{p^2}] = -p$ or $[\pi_{p^2}] = p$), and any (arbitrary) supersingular curve defined over $\mathbb{F}_{p^2}$ has a twist which is a maximal curve. We will often restrict to maximal supersingular curves because if $E/\mathbb{F}_p$ is supersingular, $E/\mathbb{F}_{p^2}$ is maximal, but all results apply just as well to their quadratic twists, the minimal supersingular curves.

By supersingular isogeny based cryptography, or simply "the supersingular case" we mean isogeny based cryptography on maximal supersingular curves over $\mathbb{F}_{p^2}$.

By the "oriented case", we mean either a maximal curve E with an orientation by a quadratic imaginary order R, or an ordinary curve. In the ordinary case, the orientation will always be the one induced by the Frobenius (often the saturation of $\mathbb{Z}[\pi]$ in $\mathrm{End}(E) = \mathrm{End}_{\mathbb{F}_q}(E)$). When we speak of an oriented supersingular curve $E/\mathbb{F}_p$, we also implicitely mean the orientation induced by the Frobenius, and that $\pi_p^2 = [-p]$, which is automatic if $p > 3$.

We say that a supersingular abelian variety $A/\mathbb{F}_p$ is "standard" if it is an abelian variety such that $\pi_A^2 = -p$, or equivalently by Tate's isogeny theorem, A is isogeneous over $\mathbb{F}_p$ to E_0^g, $E_0/\mathbb{F}_p$ a (standard) supersingular elliptic curve. Such an A is superspecial by [Yu12, Lemma 2.2]. If E_0 is primitively oriented by the Frobenius (i.e. $R = \mathbb{Z}[\pi]$ is saturated in $\mathrm{End}_{\mathbb{F}_p}(E_0)$), then A is standard iff it belongs to $\mathfrak{Ab}_{E_0,R}$.

Likewise, if $E_0/\mathbb{F}_{p^2}$ is a maximal supersingular elliptic curve, then an abelian variety $A/\mathbb{F}_{p^2}$ of dimension g is isogeneous to E_0^g iff it is maximal, i.e. $\#A = (p+1)^{2g}$ (or equivalently by [JKP+18, Proposition 5.1] $\pi_A = -p$, or $A(\mathbb{F}_{p^2}) = (\mathbb{Z}/(p+1)\mathbb{Z})^{2g}$). Then it is also superspecial by combining [JKP+18, Theorem 5.3 and Theorem 3.3.(c)].

We will often denote our quadratic imaginary orders by R or S and quaternion orders by $\mathfrak{O}$.

1.4. **Outline.** In Section 2 we recall some results on Hermitian R-modules, for R a quadratic imaginary order. In Section 3 we describe symmetric monoidal actions, recall the power object construction, and use it to give a symmetric monoidal action from the category of f.p. R-modules on R-oriented objects in any abelian category (for R a commutative ring). In Section 4 we specialize the above construction to the abelian category of commutative proper group schemes over a field, and look at the properties of this action on abelian varieties. We also explain how to compute the action in practice. In Section 5 we recast the supersingular isogeny path problem as a rank 2 module inversion problem. Finally in Section 6 we describe our new NIKE: $\otimes$-MIKE.

We mainly work with Hermitian R-modules, for R a quadratic imaginary order. In Appendix A we extend some of the theory to Gorenstein orders, for which we have good biduality isomorphisms. We also look at the general (non projective) module action on a general abelian variety in Appendix B.

We provide two paths to the module action. The first one deals with action by projective R-modules on an arbitrary R-oriented abelian variety, this is done in Sections 3, 4.1 and 4.2.

In Sections 4.3 and 4.4, we refine this action in the special case where $A \in \mathfrak{Ab}_{E_0,R}$ is in the orbit (by the module action!) of a primitively oriented elliptic curve: we explain when a torsion free module action on A still gives an abelian variety. The reader who is only interested in actions by projective modules can skip these sections.

On the other hand, for the reader who is mainly interested in the special case where A is in the orbit of an elliptic curve rather than an arbitrary abelian variety (this is the case we need in Section 6.2), we have written Sections 4.3 and 4.4 to be essentially self contained from Sections 3, 4.1 and 4.2. Admitting the antiequivalence of category from Theorem 4.9 in Section 4.3 as a black box, we rederive in Theorem 4.17 the module action in a self contained manner. This allows the reader to skip the very general machinery of Section 3. This come at the cost of some redundancy between Theorems 4.7, 4.11 and 4.21.

1.5. **Thanks.** This article is a natural follow up of [KNRR21], which was the outcome of a project initially started in 2011 with Christophe Ritzenthaler. It is thanks to him that I learnt about Serre's Hermitian module construction. We thank Aurel Page for useful discussions on Morita contexts between $R = \mathrm{End}_{\mathbb{F}_p}(E)$ and $\mathfrak{O}_0 = \mathrm{End}_{\mathbb{F}_{p^2}}(E)$ for a supersingular elliptic curve $E/\mathbb{F}_p$. Our article [PR23a] was also the first one that considered the module point of view (not yet reframed as a module action) for isogeny based cryptography. We thank Dajano Tossici for useful discussions on group schemes and fppf sheafs. We thank Benjamin Wesolowski for various security discussions related to the module action, Peter Kutas and Lorenz Panny for discussions on Kuperberg's algorithm, and Luca De Feo for suggesting the name MIKE. This article is meant to accompany my talk [Rob24a] at the Leuven isogeny days 5, we thank the participants of this workshop for their encouragements.

2. Hermitian modules and similitudes

In Section 2.1 we recall the basic theory of Hermitian modules, and in Section 2.2 we look at similitudes.

2.1. **Hermitian modules.** In this article, R will be a quadratic imaginary order of discriminant Δ_R, and $K = R \otimes_{\mathbb{Z}} \mathbb{Q}$ its field of fractions. If O_R is its maximal order, and $R \subset S \subset O_K$, we denote by $f_{S/R} = [S : R]$ the conductor of R relative to S, and $\mathfrak{f}_{S/R} = f_{S/R}S \subset R$ the conductor ideal. We have $\sqrt{\Delta_R} = f_{S/R}\sqrt{\Delta_S}$, and $R = \mathbb{Z} + f_{S/R}S$. We let f_R be the absolute conductor of R, i.e. the conductor in its maximal order O_K.

We extend the norm map on integral ideals $N_R(I) = [R : I]$ multiplicatively, for instance, because $N_R(\mathfrak{f}_{S/R}) = f$, we have $N_R(S) = 1/f$, since $S = 1/f\mathfrak{f}_{S/R}$.

All our modules will be of finite type (hence of finite presentation). If M is a torsion free module, its R-rank g is the dimension of $V = M \otimes_R K$ as a K-vector space. Since M is torsion free, M injects into V. Conversely, a R-lattice $M \subset V$ is a R-submodule M of V of rank the dimension of V/K.

Lemma 2.1 (Module isogenies)**.** *Let $\psi : M_2 \to M_1$ be a morphism of torsion free f.p. R-modules. The following are equivalent:*

- *ψ is a monomorphism with finite cokernel $M_1/\psi(M_2)$*
- *ψ is a monomorphism and M_1 and M_2 have the same rank*
- *ψ has finite cokernel and M_1 and M_2 have the same rank*

If these conditions are satisfied, we say that ψ is a (module) isogeny, of cokernel $M_1/\psi(M_2)$ and degree $\#M_1/\psi(M_2)$.

If $\psi : M_2 \subset M_1$ is an isogeny, we have an exact sequence $0 \to M_1^\vee \to M_2^\vee \to \mathrm{Ext}^1_R(M_1/M_2, R) \to 0$ so $\psi^\vee : M_1^\vee \to M_2^\vee$ is an isogeny with cokernel $\mathrm{Ext}^1_R(M_1/M_2, R) \simeq \mathrm{Hom}_R(M_1/M_2, K/R)$ and same degree as ψ (see Appendix A).

We remark also that a f.t. R-module is finite iff it is of torsion, iff it is of N-torsion for some $N \in \mathbb{Z}$.

Lemma 2.2. *Let M be a f.p. torsion free R-module of rank g. Then there is a decomposition $M = I_1 \oplus I_2 \oplus \cdots I_g$, such that $O(I_1) \subset O(I_2) \subset \cdot \subset O(I_g)$ (hence I_i is invertible in $O(I_i) = \{x \in K, xI_i \subset I_i\}$). Furthermore, the isomorphism class of M only depend on the $O(I_i)$ and on the class of $I_1 \cdot I_2 \ldots I_g$ which is an invertible $O(I_g)$ ideal.*

In particular, if $M \subset V$ is a R-lattice, it admits a pseudo-basis $M = I_1x_1 \oplus I_2x_2 \oplus \cdots \oplus I_gx_g$ where $(x_1, \ldots, x_g)$ is a basis of V/K.

Proof. This follows from the fact that a quadratic ring is a Bass order, see [JKP+18, Thorem 3.2], and [Bas63; LW85] for much more details. □

Definition 2.3. If M is as above, we define its conductor relative to R as $f_{M/R} = f_{O(I_g)/R}$, which we also call its vertical gap or conductor gap (we will see the link with isogeny volcanoes in Example 4.16). In particular, the flat locus of M is the open $U(f_{M/R})$ defined by $f_{M/R}$. We say that M is horizontal if $f_{M/R} = 1$, this is equivalent to M being projective.

When we speak of an Hermitian R-module (M, H_M), M will always be assumed to be f.p. torsion free.

Definition 2.4 (Hermitian modules)**.** Let M be a f.p. torsion free R-module.

- The dual $M^\vee$ is the R-module $\mathrm{Hom}_{\overline{R}}(M, R)$ of R-antilinear forms. We have a canonical biduality isomorphism $M \simeq M^{\vee\vee} : m \mapsto (\psi \mapsto \overline{\psi(m)})$. (See [KNRR21, p. 6], or Remark 2.5 below, or Appendix A for a more general statement).
- A sesquilinear form $H : M \times M \to R$ is a bilinear map which is R-linear on the left side and R-antilinear on the second side. Equivalently, $\phi_H : M \to M^\vee : x \mapsto H(x, \cdot)$ is a morphism.
- An Hermitian form $H : M \times M \to R$ is a sesquilinear form which satisfy the symmetry condition: $H(x, y) = \overline{H(y, x)}$. Equivalently, $\phi_H : M \to M^\vee$ is autodual via the biduality isomorphism from above.
- An Hermitian form H on M is non degenerate when $\phi_H : M \to M^\vee$ is a monomorphism, i.e. an isogeny by Lemma 2.2. By the symmetry condition, non degeneracy on the left is equivalent to the one on the right.
- An Hermitian form H is positive definite if $H(x, x) > 0$ for all x in M; it is then non degenerate.
- An unimodular positive definite Hermitian module (M, H) is a module M with a Hermitian form H which is positive definite and such that $\phi_H : M \to M^\vee$ is an isomorphism.
- An Hermitian form H on M induces an Hermitian form $H_K = H \otimes_R K$ on $V = M \otimes_R K$, which is positive definite iff H is.
- Given an Hermitian form $H_K : V \times V \to K$ on V, we define the R-orthogonal of a R-lattice $M \subset V$ as $M^\sharp = \{x \in V \mid H(x, y) \in R \quad \forall y \in M\}$. If H_K is non degenerate, it induces an isomorphism $M^\sharp \simeq M^\vee, x \mapsto H_K(x, \cdot)$. So by biduality, $M^{\sharp\sharp} = M$
- We say that a non degenerate Hermitian form $H_K : V \times V \to K$ is integral on a R-lattice $M \subset V$ if $M \subset M^\sharp$, this is equivalent to the fact that H_K restrict to an Hermitian form $H_M : M \times M \to R$ on M. Then $\phi_{H_M} : M \to M^\vee$ is given by $M \hookrightarrow M^\sharp \simeq M^\vee$. In that case, (M, H_M) is unimodular iff $M^\sharp = M$.
- Let ψ be a vector space isomorphism $\psi : (V_1, H_1) \to (V_2, H_2)$ between two non degenerate Hermitian vector spaces: here we do not require $\psi^* H_1 = H_2$.

  Then ψ induces an isogeny of modules $\psi : M_1 \to M_2$ for any lattice $M_1 \subset V_1, M_2 \subset H_2$ such that $\psi(M_1) \subset M_2$.

  Furthermore, if $\psi^\sharp$ denote the adjoint of ψ, so that $H_2(x_1, \psi(y_1)) = H_1(\psi^\sharp(x_1), y_1)$, we have $\psi^\sharp(M_2^\sharp) \subset M_1^\sharp$, and $\psi^\sharp : M_2^\sharp \to M_1^\sharp$ coincides with the dual isogeny $\psi^\vee$ under the isomorphism $M_i^\sharp \simeq M_i^\vee$ above. We call $\psi^\sharp$ the adjoint isogeny (or also the dual isogeny by abuse of notation).

  If M_1, M_2 are unimodular, via $M_1 = M_1^\sharp$ and $M_2 = M_2^\sharp$, we can also identify the adjoint isogeny $M_2^\sharp \to M_1^\sharp$ with an isogeny $M_2 \to M_1$ which we call the contragredient isogeny $\tilde{\psi}$.

Remark 2.5.

- If M is an integral sublattice of a non degenerate Hermitian space (V, H_K), and $M = \sum_{i=1}^g I_i x_i$ is a pseudo-basis, then if $x_i^\sharp \in V$ is the dual basis of $(x_1, \dots, x_g)$, $M^\sharp = \sum \overline{(R : I_i)} x_i^\sharp$.

  We have $(R : I) = \overline{I}/N(I)$, from this it follows that $M^{\sharp\sharp} = M$.
- If H_K is positive definite, $H_Q := \mathrm{Tr}_{K/\mathbb{Q}}(H_K)$ is a symmetric bilinear form, positive definite, so (M, H_Q) can be seen as a rank $2g$ $\mathbb{Z}$-lattice.
- A very important fact about Hermitian modules is that if we have an orthogonal decomposition

  $$(M, H_M) = (M_1, H_{M_1}) \oplus_\perp (M_2, H_{M_2}) \oplus_\perp \cdots$$

  with the (M_i, H_{M_i}) indecomposable (we call this a full orthogonal decomposition), the (M_i, H_{M_i}) are uniquely determined (up to permutation) [KNRR21, Lemma 2.9]. This is in stark contrast with modules: if I, J are two non equivalent invertible ideals of R, then $I \oplus I^{-1} \simeq J \oplus J^{-1}$. If $\mathfrak{O}$ is a maximal order in a quaternion algebra, we even have $I_1 \oplus I_2 \simeq J_1 \oplus J_2$ for any integral ideals I_1, I_2, J_1, J_2 of $\mathfrak{O}$.

When we have an Hermitian form, it induces "pairings":

Proposition 2.6 (Orthogonality)**.** *Let (V, H_K) be a non degenerate hermitian vector space.*

- *If $M_2 \subset M_1$ is a sublattice (i.e. an isogeny), $M_2^\sharp \supset M_1^\sharp$ is the "dual isogeny", and the "Weil-Cartier" pairing $H \mod R : M_1/M_2 \times M_2^\sharp/M_1^\sharp \to K/R$ is non degenerate.*
  In particular, we have that $\#M_1/M_2 = \#M_2^\sharp/M_1^\sharp$.
- *Given a lattice $M \subset V$, "the Weil pairing", $H_K \mod n : M/nM \times M^\sharp/nM^\sharp \to R/nR$, is non degenerate.*

Proof. The Weil-Cartier pairing $M_1/M_2 \times M_2^\sharp/M_1^\sharp \to K/R$ is well defined by definition of the R-orthogonal. It is non degenerate on both side because $M_2 = M_2^{\sharp\sharp}$.

The Weil pairing is given by, up to rescaling, the special case of the multiplication by n: $nM \subset M$ has for "dual isogeny" $M^\sharp \subset (nM)^\sharp = 1/nM^\sharp$. □

For simplicity, unless explicitly stated otherwise, by assumption all our Hermitian modules M will come from a positive definite Hermitian form H, and we will just say unimodular instead of positive definite unimodular Hermitian.

Lemma 2.7. *Let M_1, M_2 be two f.p. torsion free R-modules whose relative conductor gap are coprime: $f_{M_1/R} \wedge f_{M_2/R} = 1$. Then $M_1 \otimes_R M_2$ and $\mathrm{Hom}_R(M_1, M_2)$ are torsion free, and $\mathrm{Tor}_R^1(M_1, M_2) = 0$. We call M_1 and M_2 Tor-independant.*

Proof. Under our hypothesis, at each prime $\mathfrak{p}$ of R, either $M_{1,\mathfrak{p}}$ or $M_{2,\mathfrak{p}}$ is free. The results follow by localisation. □

Example 2.8.

- (R, H_R) with $H_R(x, y) = x\overline{y}$ is a unimodular Hermitian module, it induces $H_K(x, y) = x\overline{y}$ on K.
- If (M_1, H_1) and (M_2, H_2) are (unimodular) Hermitian modules, then their direct sum $(M_1 \oplus M_2, H_1 \oplus H_2)$ is also a (unimodular) Hermitian module and, if M_1 and M_2 are Tor-independant, their tensor product $(M_1 \otimes_R M_2, H_1 \otimes_R H_2)$ is too[2].
- In particular, (R^g, H_R^g) is unimodular.
- If $I \subset K$ is a fractional R-ideal, then its R-orthonal under H_K is given by $I^\sharp = I/N_R(I)$. So $(I, H_R/N_R(I))$ is unimodular. This is always the Hermitian form we will use when considering ideals as unimodular Hermitian rank 1 modules.

2.2. **Similitudes.** Our main result will be an action of Hermitian modules on (certain) R-oriented polarised abelian varieties. An n-similitude will induce a n-isogeny. We will use an antiequivalence of category, so for us a polarised abelian variety will correspond to a lattice M in a positive definite vector space $(V/K, H_K)$, such that H_K is integral on $M^\sharp$, i.e. $M^\sharp \subset M$. We call H_K cointegral on M, or by analogy with abelian varieties, a polarisation on M. And the degree of this polarisation is defined to be $\#M/M^\sharp$.

Definition 2.9 (Similitudes and polarised isogenies)**.** Assume M f.p. torsion free.

- A polarisation on M is a (non degenerate) Hermitian form H on $V = M \otimes_R \mathbb{Q}$ such that $M^\sharp \subset M$
- A polarised isogeny $\psi : (M_2, H_2) \to (M_1, H_1)$ between two polarised modules is an isogeny $M_2 \hookrightarrow M_1$ such that $\psi^* H_1 = H_2$, where $(\psi^* H_1)(x, y) = H_1(\psi(x), \psi(y))$. Equivalently, $\psi^\sharp = \psi^{-1}$ where $\psi^\sharp$ is the adjoint isogeny.
- A n-similitude (or n-isogeny) $\psi : (M_2, H_2) \to (M_1, H_1)$ between two polarised Hermitian modules is a polarised isogeny $\psi : (M_2, nH_2) \to (M_1, H_1)$ of Hermitian modules, i.e., $\psi^* H_1 = nH_2$.
  We will always assume that a n-similitude is between unimodular Hermitian modules, in which case ψ is a n-similitude iff $\tilde{\psi} \circ \psi = [n]$ iff $\psi \circ \tilde{\psi} = [n]$, and the contragredient isogeny $\tilde{\psi} : (M_1, H_1) \to (M_2, H_2)$ is a n-similitude.

Lemma 2.10 (Isotropic kernels)**.** *Let H be a positive definite Hermitian form on V of dimension g, and M_1 a polarised lattice of V: $M_1^\sharp \subset M_1$.*

[2]Recall that (M_i, H_i) is unimodular iff the induced map $M_i \to M_i^\vee$ is an isomorphism; in which case the tensor product $M_1 \otimes_R M_2 \to M_1^\vee \otimes_R M_2^\vee$ is too

- *Any polarised submodule $M_2 \subset M_1$ gives a polarised isogeny $(M_2, H) \to (M_1, H)$, with dual isogeny $(M_1^\sharp, H) \to (M_2^\sharp, H)$, both induced by the natural inclusions $M_1^\sharp \subset M_2^\sharp \subset M_2 \subset M_1$. We call $\psi : M_2 \hookrightarrow M_1$ a polarised isogeny for H, and define its degree as $\#M_1/M_2$. By Proposition 2.6, this is also the degree of the adjoint isogeny $\psi^\sharp : M_1^\sharp \to M_2^\sharp$.*
- *There is a bijection between polarised isogenies for H and isotropic submodules for the non degenerate form $H \mod R : M_1/M_1^\sharp \times M_1/M_1^\sharp \to K/R$ induced by H. The bijection is, to $M_2^\sharp$ such that $M_1^\sharp \subset M_2^\sharp \subset M_2$, we associate $M_2^\sharp/M_1^\sharp$. We remark that its orthogonal for $H \mod R$ is given by $M_2/M_1^\sharp$.*

  If d_i is the degree of the polarisation $M_i \to M_i^\sharp$, and d the degree of the isogeny $\psi : M_2 \to M_1$, we have $d_1 = d_2 d^2$, since $M_1^\sharp \to M_1$ can be written as the composition of the adjoint isogeny $\tilde{\psi} : M_1^\sharp \to M_2^\sharp$, which has the same degree as ψ, the polarisation $M_2^\sharp \to M_2$ and the isogeny $\psi : M_2 \to M_1$.
- *If (M_1, H) is unimodular, then the R-orthogonal of M_1 for $\frac{1}{n}H$ is $M_1^{\sharp,n} = nM_1$, and so n-similitudes corresponds to modules $M_2 \subset M_1$ such that $M_1^{\sharp,n} = nM_1 \subset M_2^{\sharp,n} \subset M_2 \subset M_1$. Notice that in a n-similitude with M_1 unimodular, every element in M_1/M_2 is of n-torsion.*

  Since $M_2^{\sharp,n} = nM_2^\sharp$ (where we recall that $M_2^{\sharp,n}$ is the R-orthogonal of M_2 for $\frac{1}{n}H$), the condition becomes $nM_1 \subset nM_2^\sharp \subset M_2 \subset M_1$.

  These submodules $M_2^\sharp$ are are in bijection with isotropic submodules for the non degenerate form, "the Weil pairing", $M_1/nM_1 \times M_1/nM_1 \to \frac{1}{n}R/R$. And (M_2, H) is unimodular iff this isotropic submodule is maximal, iff $\#M_1/M_2 = n^g$, iff $M_2 = nM_2^\sharp$.

Proof. Immediate by Proposition 2.6. □

As mentioned above, because we will have in Section 4 an antiequivalence of category between Hermitian modules and polarised abelian varieties, the concepts from isogenies between abelian varieties translate to an Hermitian version. As a first example, to build a ℓ^m-similitude $M' \hookrightarrow M$, we can use a "path" $M' = M_m \subset M_{m-1} \subset ... \subset M = M_0$ using Lemma 2.10.

Example 2.11. Having an Hermitian form (or its associated quadratic form $q_H(x) = H(x, x)$) on a module gives a way to measure the "size" of a submodule. For instance for an n-similitude $M_2 \to M_1$ of torsion free rank g modules, $\#M_1/M_2 = n^g$. And a monomorphism $M_2 \hookrightarrow M_1$ of unimodular modules with the same quadratic form has to be an isomorphism.

Example 2.12 (Kani's construction for Hermitian modules)**.** An Hermitian module isogeny diamond is given by a commutative diagram of isogenies

$$\begin{array}{ccc} M_0 & \xrightarrow{\psi_1} & M_1 \\ \downarrow{\scriptstyle \psi_2} & & \downarrow{\scriptstyle \psi_2'} \\ M_1 & \xrightarrow{\psi_1'} & M_{12} \end{array}$$

where $\psi_1 : (M_0, H_0) \to (M_1, H_1), \psi_1' : (M_2, H_2) \to (M_{12}, H_{12})$ are n_1-similitudes and $\psi_2 : (M_0, H_0) \to (M_2, H_2), \psi_2' : (M_1, H_2) \to (M_{12}, H_{12})$ are n_2-similitudes.

Then $\Psi = \begin{pmatrix} \psi_1 & \tilde{\psi'}_1 \\ -\psi_2 & \tilde{\psi'}_2 \end{pmatrix} : (M_0 \oplus M_{12}, H_0 \oplus H_{12}) \to (M_1 \oplus M_2, H_1 \oplus H_2)$ is a $n_1 + n_2$-similitude.

Similarly, if (M, H_M) is unimodular, there is always a n-similitude on (M^4, H_M^4) (resp. on (M^2, H_M^2) if $n = x\overline{x} + y\overline{y}$, $x, y \in R$; resp. on (M, H_M) if $n = x\overline{x}$, $x \in R$).

We refer to [KNRR21, § 2] for algorithms to enumerate unimodular modules of rank g, and to [Kir16] for more details.

Of particular importance to us will be [KNRR21, Theorem 2.16], which gives precise conditions on when, given a unimodular Hermitian module (M, H_M) of rank g, we can find a n-similitude $(R^g, H_R^g) \to (M, H_M)$ (eventually with n asked to be coprime to some integer f).

There are essentially two obstructions: first, there can be no n-similitude at all. This only can happen when g is even, so an easy fix is to instead look for a similitude $(R^{g+1}, H_R^{g+1}) \to (M \oplus R, H_M \oplus H_R)$.

The second obstruction happens when we try to find a n-similitude prime to some integer f, then a necessary condition is that f is coprime to the conductor gap $f_{M/R}$ of M [KNRR21, Theorem 2.16.(3).(a)]. Conversely, if g is odd, and f is coprime to $2f_{M/R}$, then we can find a n-similitude $(R^g, H_R^g) \to (M, H_M)$ with n coprime to f, see [KNRR21, Theorem 2.16.(3)] (which gives more refined conditions, including the case g even).

In light of these results, we make the:

Heuristic 2.13. *Let (M, H_M) be a unimodular* projective *Hermitian module of rank g, and f an integer. Then there exists a small m such that we can find two n_i-similitudes $(R^{g+m}, H_R^{g+m}) \to (M \oplus R^m, H_M \oplus H_R^m)$ with $n_1 \wedge n_2 = 2^u$ for u small, and n_1, n_2 of medium size. Here by medium we mean that n_1, n_2 are bounded polynomially in term of Δ_R, g and the discriminant of H_M, and by small m, u we mean that $2^m, 2^u$ should be medium.*

Proof. Since M is projective, there are no conductor gap obstruction. We can find a first n_1-similitude (eventually replacing M by $M \times R$, so with $m = 1$). Then by [KNRR21, Theorem 2.16.(3)] we can find another n_2-similitude with n_2 coprime to the odd part of n_1, so $n_1 \wedge n_2$ is a power of two. However, this result only gives an existence result, not a bound on the size of n_i constructed (nor on the power of two we obtain). We expect that a careful analysis of the proof will give such a bound, but for now we leave that as an heuristic. □

We stress that this heuristic is not needed to define our module action, it will be only needed to show that the action is effective in all cases. But what we will do usually is apply the action to unimodular modules specifically constructed from a nice n-similitude from (R^g, H_R^g). In particular, we won't need to use the heuristic to compute $\otimes$-MIKE.

3. Symmetric monoidal actions

In Section 3.1 we briefly review symmetric monoidal categories and their action, and study their cryptographic relevance in Section 3.2. In Section 3.3, we introduce the power object construction, and we show in Section 3.4 that power objects exist in R-oriented abelian categories, and then in Section 3.5 that the power object construction simplifies for projective modules.

3.1. Symmetric monoidal categories and actions.

Let $(\mathfrak{C}, \otimes, 1)$ be a symmetric monoidal category. This can be seen as a categorification of the concept of commutative monoid; we refer to the nlab [nLa24c] for the precise definition.

For us the main example will be the category of R-modules, with R a commutative ring, with the usual module tensor product as the (symmetric) monoidal tensor product. This is a very nice category: it is a Grothendieck abelian category, hence is complete and cocomplete, so form a cosmos; it is closed, and $(R - \mathrm{mod}, \oplus, \otimes)$ form a tensor category (a categorification of the notion of rigs).

If $\mathfrak{D}$ is another category, a symmetric monoidal action is a categorification of the notion of action, i.e. it is a functor $\cdot : \mathfrak{C} \times \mathfrak{D} \to \mathfrak{D}$, which respect the "obvious coherence conditions". Equivalently, an action is given by a monoidal functor from $\mathfrak{C} \to \mathrm{End}(\mathfrak{D})$. For simplicity, we will only work with strict categories and functors, in order to keep track of as few coherence conditions as possible. The category $\mathfrak{D}$ endowed with the monoidal action from $\mathfrak{C}$ is also called an actegory or (left) $\mathfrak{C}$-module category.

Example 3.1. Let $(M, +, 0)$ be a commutative monoid acting on a set X. Then we can see M as a monoidal category with its set of object equal to M, trivial morphisms, and $+$ as the monoidal tensor product. Likewise, we can consider X as a category with trivial morphisms. The action of M on X then gives a symmetric monoidal action from M seen as a symmetric monoidal category to X seen as a category.

Note that, as a categorification of the usual notion of action on a set, in our case we have an action on morphisms (subject to the obvious coherence conditions), not only on objects. In particular, a morphism $d_1 \to d_2$ in $\mathfrak{D}$ induces $c \cdot d_1 \to c \cdot d_2$, and likewise a morphism $c_1 \to c_2$ in $\mathfrak{C}$ induces $c_1 \cdot d \to c_2 \cdot d$, and one of the coherence condition is that given $c_1 \to c_2$ and $d_1 \to d_2$, the two ways to construct $c_1 \cdot d_1 \to c_2 \cdot d_2$ should coincide.

3.2. **Symmetric monoidal actions for cryptography.** If G is a commutative group acting on a set X, there is the well known generalisation of Diffie-Helmann key exchange given as follows: we fix a base point $x_0 \in X$, Alice and Bob takes secret $a, b \in G$ and publish $a \cdot x_0$ and $b \cdot x_0$ respectively. Their common secret is $(ab) \cdot x_0 = a \cdot (b \cdot x_0)$.

We have the notion of action inversion, action-CDH, action-DDH (by decreasing order of difficulty), and the security of the key exchange rely on action ddh.

All these concept translate immediately for a symmetric monoidal action of $\mathfrak{C}$ on $\mathfrak{D}$: if a, b are objects in $\mathfrak{C}$ and x_0 an object in $\mathfrak{D}$, the common secret is $(a \otimes b) \cdot x_0 = a \cdot (b \cdot x_0) \simeq (b \otimes a) \cdot x_0 = b \cdot (a \cdot x_0)$, where the isomorphism comes from the canonical symmetric morphism $(a \otimes b) \simeq (b \otimes a)$ in $\mathfrak{C}$ (this is where using strict actions simplify our life).

Since a commutative group (or monoid) action is a special case of symmetric monoidal action by Example 3.1, the monoidal framework is more general. The point we want to make here, is not going from groups to monoids; it is that by going from set to categories, we can act on morphisms and not only on objects.

More precisely, we can act by objects on objects, but also by objects on morphisms, by morphisms on objects, and even by morphisms on morphisms; all these, except the first one, give morphisms. In fact the first three actions are special cases of the morphism on morphism action, where we identify an object a with its identity morphism Id_a.

As an example, let us consider one of the usual example of cryptographic group action in the literature: namely the action of the group $\mathrm{Pic}(R)$ of invertible R-ideals on R-oriented elliptic curves.

We argue that we should consider the invertible ideals not as a group, but as the symmetric monoidal category of rank 1 projective modules over R (this is a subcategory of the more general category we will consider later in Section 4). Likewise, oriented elliptic curves form a natural category, with morphisms the R-oriented isogenies (and 0). It is easy to see that the usual ideal action is actually (contravariantly) compatible with these morphisms, hence form a symmetric monoidal *contravariant* action (we will generalise this to modules and abelian varieties in Section 4). But this extra data cannot be encapsulated under the framework of group actions.

Example 3.2 (Monoidal action for cryptography)**.**

- As an example, the SiGamal [MOT20] construction relies on not only constructing a common elliptic curve $\mathfrak{ab}E_0$ starting from E_0 and two invertible integral ideals $\mathfrak{a}, \mathfrak{b}$, but also on constructing a common isogeny $E_0 \to \mathfrak{ab}E_0$. From our point of view, this corresponds to looking at the action not only of the object $\mathfrak{a}$, but also of the canonical morphism $\mathfrak{a} \to R$ corresponding to the natural inclusion, which gives (by contravariance) an isogeny $E_0 \to \mathfrak{a}E_0$. Hence the SiGamal construction fits easily into our monoidal action framework.
- As a related example, in the monoidal action framework, we can do a key exchange on morphisms rather than objects. We start with a base morphism $\phi_0 : x_0 \to y_0 \in \mathfrak{D}$, Alice and Bob select secret morphisms $\psi_1 : a_1 \to b_1 \in \mathfrak{C}$ and $\psi_2 : a_2 \to b_2 \in \mathfrak{C}$, they send $\psi_1 \cdot \phi_0 : a_1 \cdot x_0 \to b_1 \cdot y_0$ and $\psi_2 \cdot \phi_0 : a_2 \cdot x_0 \to b_2 \cdot y_0$ respectively, and the common secret is $(\psi_1 \otimes \psi_2) \cdot \phi_0 = \psi_1 \cdot \psi_2 \cdot \phi_0 : (a_1 \otimes a_2) \cdot x_0 \to (b_1 \otimes b_2) \cdot y_0$. The Diffie-Helmann key exhange on objects is the special case where the morphisms are given by identity morphisms.
- We could also imagine a signature scheme, as follows. Assume that it is hard to compute morphisms in $\mathfrak{D}$ between two given objects; then Alice has for secret key such a morphism $\phi : x \to y$, and for public key the domain and codomain x, y. Bob challenges with an element $b \in \mathfrak{C}$, and Alice responds to the challenge with $b \cdot \phi : b \cdot x \to b \cdot y$, since Bob can compute $b \cdot x$ and $b \cdot y$, he can check that the morphism is between the correct domain and codomain. Of course, a difficulty in instantiating such a scheme, is that $b \cdot \phi$ should not provide information on

ϕ. In particular, such a scheme cannot work for in the group action framework, where applying b^{-1} gives back ϕ.

The SQISign signature scheme [DKLPW20] has some similarity. The problem is that even using a rank 2 module action would not hide the isogeny path enough, so SQISign works differently than the method outlined above. Anticipating Section 5.2 to go from a supersingular isogeny path to a rank 2 module action (via the Weil restriction), SQISign can be reinterpreted in term of module action as follows: the public key is $M \cdot E_0$, and the secret the rank 2 unimodular module M. There is first a public commitment $M' \cdot E_0$, with M' another secret rank 2 unimodular module, which is then transformed by the challenger into a commitment $M'' \cdot E_0$, via an isogeny path $M' \cdot E_0 \to M'' \cdot E_0$. The challenger knows the isogeny path, but not M', so M'' is only known by the prover. The prover then responds by an isogeny between $M \cdot E_0$ and $M'' \cdot E_0$, which he can build thanks to the knowledge of the modules.

Remark 3.3 (The module action vs the ideal action for cryptography)**.**

- Invertible ideals form a group, this is very convenient for cryptography. By contrast, projective modules of rank > 1 are not invertible, hence we only have a monoid.
- Each action by a projective module of rank g multiplies the dimension by g. Hence, even in rank $g = 2$, we can only act by very few modules before the dimension explodes.
- It follows that the module action is a lot less flexible than the ideal action. However, for security, this drawbacks turn into advantages, preventing Kuperberg's algorithm to apply directly.

We give a list of reasons why we expect Kuperberg's algorithm to not apply:

Remark 3.4 (Kuperberg's algorithm for the module action)**.**

- First, we have a monoid, rather than a group.
- Secondly, the monoid is not finite, nor even finitely generated (a projective module of rank a prime number ℓ can only be written as a tensor product of another module of rank ℓ and an ideal)
- And finally, each action increases the dimension, so the action acts on an infinite set.

3.3. **The power and copower object construction.** Recall that a closed symmetric monoidal category $\mathfrak{C}$ is a symmetric monoidal category that has an internal Hom $\mathcal{HOM}_{\mathfrak{C}}(c_1, c_2)$, defined as an adjoint of $\otimes$: $\mathrm{Hom}_{\mathfrak{C}}(c, \mathcal{HOM}_{\mathfrak{C}}(c_1, c_2)) = \mathrm{Hom}_{\mathfrak{C}}(c \otimes c_1, c_2)$.

Assume now that $\mathfrak{C}$ is closed symmetric monoidal, and let $\mathfrak{D}$ be a category enriched in $\mathfrak{C}$, which means that we see the hom objects $\mathrm{Hom}_{\mathfrak{D}}(d_1, d_2)$ as living in $\mathfrak{C}$ rather than in Set.

Definition 3.5. Given $c \in \mathfrak{C}$ and $d \in \mathfrak{D}$, the power object $\mathcal{HOM}_{\mathfrak{C}}(c, d) \in \mathfrak{D}$, is the unique object, if it exists, such that $\mathrm{Hom}_{\mathfrak{D}}(d', \mathcal{HOM}_{\mathfrak{C}}(c, d)) = \mathrm{Hom}_{\mathfrak{C}}(c, \mathrm{Hom}_{\mathfrak{D}}(d', d))$ for all $d' \in \mathfrak{D}$. In other words, $\mathcal{HOM}_{\mathfrak{C}}(c, d)$ is defined as a presheaf on $\mathfrak{D}$, and we say that the power object exist whenever this presheaf is representable.

The copower object $c \otimes_{\mathfrak{C}} d$, if it exists, corresponds to the dual notion (i.e. is a power object in the opposed category of $\mathfrak{D}$): $\mathrm{Hom}_{\mathfrak{D}}(c \otimes_{\mathfrak{C}} d, d') = \mathrm{Hom}_{\mathfrak{C}}(c, \mathrm{Hom}_{\mathfrak{D}}(d, d'))$ for all $d' \in \mathfrak{D}$.

If the power (resp. copower) object construction exists for all $c \in \mathfrak{C}, d \in \mathfrak{D}$, then by general abstract nonsense, $c \cdot d = \mathcal{HOM}_{\mathfrak{C}}(c, d)$ gives a contravariant symmetric monoidal action (resp. $c \cdot d = c \otimes_{\mathfrak{C}} d$ gives a covariant symmetric monoidal action).

Essentially all monoidal actions are of this type. First, for all $d \in \mathfrak{D}$ the functor $\mathfrak{C} \to \mathfrak{D}, c \mapsto c \otimes_{\mathfrak{C}} d$ coming from the copower construction has for right adjoint the functor $\mathfrak{D} \to \mathfrak{C}, d' \mapsto \mathrm{Hom}_{\mathfrak{D}}(d, d')$ by construction. But conversely, has soon as we have a monoidal action such that the functors $\cdot d$ have a right adjoint for all $d \in \mathfrak{D}$, then these right adjoints provide a natural enrichment in $\mathfrak{C}$ for $\mathfrak{D}$ such that the action is the copower action. More generally, if we have a monoidal action, it gives an enrichment in the category of presheaves on $\mathfrak{C}$ and the action comes from the copower construction there [nLa24a].

3.4. **Power objects in an abelian category.** Let $\mathcal{A}$ be an abelian category, $A \in \mathcal{A}$ an object of $\mathcal{A}$, and assume that we have an orientation by a ring R (not assumed commutative yet), i.e. a morphism $R \to \mathrm{End}_{\mathcal{A}}(A)$.

Then for $B \in \mathcal{A}$, $\mathrm{Hom}_{\mathcal{A}}(B, A)$ has a natural structure of left R-module. For M a left R-module, we can then define as in Section 3.3 a power object $\mathcal{HOM}_R(M, A) \in \mathcal{A}$ if the presheaf $X \in \mathcal{A} \mapsto \mathrm{Hom}_R(M, \mathrm{Hom}_{\mathcal{A}}(X, A))$ is representable in $\mathcal{A}$.

Theorem 3.6. *If $A \in \mathcal{A}$ is R-oriented, and if M is a f.p. R-module, the power object $\mathcal{HOM}_R(M, A)$ exist in $\mathcal{A}$: $\mathrm{Hom}_{\mathcal{A}}(X, \mathcal{HOM}_R(M, A)) = \mathrm{Hom}_R(M, \mathrm{Hom}_{\mathcal{A}}(X, A))$ for all $X \in \mathcal{A}$. The contravariant functor $\mathcal{HOM}_R(\cdot, A)$ is functorial and right exact.*

Proof. This is proven in [JKP+18, § 4.1], using a construction of Serre and Tate. □

The properties of Theorem 3.6 are enough to reverse engineer the black box construction of $\mathcal{HOM}_R(\cdot, A)$. First $\mathcal{HOM}_R(R, A) = A$ because both represent the presheaf $\mathrm{Hom}_{\mathcal{A}}(\cdot, A)$ on $\mathcal{A}$. Likewise, it is clear from its functorial definition, that $\mathcal{HOM}_R(\cdot, A)$ commutes with direct sums. Now, by right exactness, for an arbitrary f.p. module M, taking a presentation $R^m \to R^n \to M \to 0$ gives by contravariance an exact sequence $0 \to \mathcal{HOM}_R(M, A) \to A^n \to A^m$. The map $\psi : R^m \to R^n$ is represented by right multiplication by a matrix $X \in \mathrm{Mat}_{m \times n}(R)$, and the same matrix acts by left multiplication to define a morphism $A^n \to A^m$, which is precisely $\phi = \mathcal{HOM}_R(\psi, A)$. The exact sequence above shows that $\mathcal{HOM}_R(M, A) = \mathrm{Ker}\, \phi$. It is not obvious from the construction that this object does not depends on the choice of presentation, but this follows from its functorial property.

Theorem 3.6 is not enough to define a symmetric monoidal action, because there is no reason for $\mathcal{HOM}_R(M, A)$ to be R-oriented. However, things work out well when we assume further that R is *commutative*.

Theorem 3.7. *Let R be a commutative ring, and $\mathcal{A}_R$ be the R-oriented category of $\mathcal{A}$: objects are given by (A, i_A) with $A \in \mathcal{A}_R$ and $i_A : R \to \mathrm{End}_{\mathcal{A}}(A)$ an R-orientation, and morphisms $(A, i_A) \to (B, i_B)$ are morphisms $A \to B$ in $\mathcal{A}$ respecting the orientations on A and B. We will denote these oriented morphisms by $\mathrm{Hom}_{\mathcal{A}_R}(A, B)$ or even $\mathrm{Hom}_R(A, B)$, dropping the orientations i_A, i_B from the notation by simplicity. Given such an oriented morphism, its kernel and cokernel have a canonical orientation, induced by the ones on A and B respectively and the functorial definitions of the kernel and cokernel. So $\mathcal{A}_R$ is an abelian category, naturally enriched in R-modules.*

Given a f.p. R-module M, and $(A, i_A) \in \mathcal{A}_R$, the power object $\mathcal{HOM}_R(M, A)$ from Theorem 3.6 has a natural R-orientation so lives in $\mathcal{A}_R$, and it gives the power object in this enriched category: $\mathrm{Hom}_{\mathcal{A}_R}(X, \mathcal{HOM}_R(M, A)) = \mathrm{Hom}_R(M, \mathrm{Hom}_{\mathcal{A}_R}(X, A))$ for all $X \in \mathcal{A}_R$. In particular, we obtain a symmetric monoidal contravariant action from f.p. R-module to R-oriented objects in $\mathcal{A}$, which we denote by $M \cdot A = \mathcal{HOM}_R(M, A)$.

The functor $\mathcal{HOM}_R(\cdot, \cdot) : R - \mathrm{modules} \times \mathcal{A}_R \to \mathcal{A}_r$ is right exact on the left (by contravariance, this means it sends a right exact sequence to a left exact sequence) and left exact on the right (by covariance, this means it sends a left exact sequence to a left exact sequence), and it commutes with direct sums (on the left and on the right).

We note that in the categorical point of view on "stuff, structure and properties" [nLa24b], the category $\mathcal{A}_R$ of R-oriented objects o $\mathcal{A}$ correspond to an extra *structure*.

Proof. Recall the construction of $\mathcal{HOM}_R(M, A) \in \mathcal{A}$ from Theorem 3.6. Taking a presentation $R^m \to R^n \to M$, given by a matrix $X \in \mathrm{Mat}_{n \times m}$ acting on the left (this time we see R^m and R^n as column vectors), then its transpose X^T acts on the left to give a morphism $A^n \to A^m$ via the orientation, and $\mathcal{HOM}_R(M, A)$ is defined as the kernel of this morphism: $0 \to \mathcal{HOM}_R(M, A) \to A^n \to A^m$ is exact. Since $A^n \to A^m$ respects the R-orientation (because R is commutative!), $\mathcal{HOM}_R(M, A)$ has a natural R-orientation too.

Now, given another oriented element $X \in \mathcal{A}_R$, since $\mathrm{Hom}_R(X, \cdot)$ is right exact, we have an exact sequence $0 \to \mathrm{Hom}_{\mathcal{A}_R}(X, \mathcal{HOM}_R(M, A)) \to \mathrm{Hom}_{\mathcal{A}_R}(X, A)^n \to \mathrm{Hom}_{\mathcal{A}_R}(X, A)^m$. On the other hand, $\mathrm{Hom}_{\mathcal{A}_R}(X, A)$ is a R-module, and applying $\mathrm{Hom}_R(\cdot, \mathrm{Hom}_R(X, A))$ to the right exact sequence $R^m \to R^n \to M \to 0$ gives a left exact sequence $0 \to \mathrm{Hom}_R(M, \mathrm{Hom}_{\mathcal{A}_R}(X, A)) \to \mathrm{Hom}_{\mathcal{A}_R}(X, A)^n \to \mathrm{Hom}_{\mathcal{A}_R}(X, A)^m$. Comparing the two exact sequences, we get that $\mathrm{Hom}_{\mathcal{A}_R}(X, \mathcal{HOM}_R(M, A)) =$

$\mathrm{Hom}_R(M, \mathrm{Hom}_{\mathcal{A}_R}(X, A))$, as needed. (This is the same proof as in [JKP+18, § 4]: the same reasoning as above using $\mathrm{Hom}_{\mathcal{A}}(X, \cdot)$ rather than $\mathrm{Hom}_{\mathcal{A}_R}(X, \cdot)$ shows that $\mathrm{Hom}_R(M, A)$ is also the power object in $\mathcal{A}$ when forgetting its natural R-orientation.)

The exactness properties follow from the functorial definition and the exactness property of the Hom functor in R-modules and $\mathfrak{Ab}_R$. □

Example 3.8. $M \cdot N \cdot A = (M \otimes_R N) \cdot A = N \cdot M \cdot A$.

It will be useful to change orientations.

Proposition 3.9. *With the notations of Theorem 3.7, suppose that $R \subset S \subset \mathrm{End}_{\mathfrak{Ab}}(A)$, where S is not assumed to be commutative. If we see S as a right R-module, then to a f.p. R-module M we can associate the left S module $S \otimes_R M$. Then we have $\mathrm{Hom}_R(M, A) = \mathrm{Hom}_S(S \otimes_R M, A)$.*

Proof. Recall that $\mathrm{Hom}_R(M, A)$ the power object in $\mathfrak{Ab}_R$ with its natural orientation, but forgetting its orientation it is also the power object in $\mathfrak{Ab}$. The result follows by functoriality from the tensor/hom adjunction on modules: $\mathrm{Hom}_{\mathfrak{Ab}}(X, \mathrm{Hom}_R(M, A)) = \mathrm{Hom}_R(M, \mathrm{Hom}_{\mathfrak{Ab}}(X, A)) = \mathrm{Hom}_S(S \otimes_R M, \mathrm{Hom}_{\mathfrak{Ab}}(X, A)) = \mathrm{Hom}_{\mathfrak{Ab}}(X, \mathrm{Hom}_{\mathfrak{Ab}}(S \otimes_R M, A))$.

This can also be seen from the explicit construction: if $R^m \to R^n \to M \to 0$ is a presentation of M, given by a matrix F, then $S^m \to S^n \to S \otimes_R M \to S$ is a presentation of $S \otimes_R M$ as a S-module, given by the same matrix F. □

The functorial properties of the action come from the power object construction, but it will be useful to give an explicit construction in order to compute the actions in practice. The proof of Theorem 3.7 gives an explicit construction of $M \cdot A$ as an object. We can extend this construction to morphisms as follows:

Proposition 3.10. *Let $\psi : M_2 \to M_1$ be a morphism of f.p. R-module, and take presentations $R^{m_2} \to R^{n_2} \to M_2 \to 0$ and $R^{m_1} \to R^{n_1} \to M_1 \to 0$. Since R is projective, ψ lifts to form a commutative diagram:*

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

If $A \in \mathcal{A}_R$, $A_1 = M_1 \cdot A$ and $A_2 = M_2 \cdot A$, the diagram above induces by the action a commutative diagram:

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

There is a unique dotted arrow making the diagram commutative, this is $\phi : A_1 \to A_2 = \psi \cdot A : M_1 \cdot A \to M_2 \cdot A$.

Proposition 3.11. *Let $\phi : A_1 \to A_2$ be an oriented morphism of objects in $\mathcal{A}_R$, and M a f.p. R-module. Take a presentation $R^m \to R^n \to M \to 0$, and consider the commutative diagram:*

$$\begin{array}{ccccccc} 0 & \longrightarrow & M \cdot A_1 & \hookrightarrow & A_1^n & \longrightarrow & A_1^m \\ & & \vdots & & \downarrow & & \downarrow \\ 0 & \longrightarrow & M \cdot A_2 & \hookrightarrow & A_2^n & \longrightarrow & A_2^m \end{array}$$

where the vertical arrows $A_1^n \to A_2^n$ are given by the diagonal of ϕ.

Then there is a unique dotted arrow making the diagram commutative, this is $M \cdot \phi : M \cdot A_1 \to M \cdot A_2$.

3.5. **Power objects from projective modules.** Let R be a commutative ring. Finitely presented projective modules are given by the Cauchy completion Proj_R (i.e. the free completion under absolute colimits) of the R-linear category BR with one object R. Now a functor F from BR to an abelian category is precisely a R-oriented object $X \in \mathcal{A}_R$, and since $\mathcal{A}_R$ is Cauchy complete, this functor extends naturally to the Cauchy completion of BR, hence to projective modules. More precisely, we can extend this functor covariantly or contravariantly, since R is commutative we cannot see the difference on BR. Since we are mostly interested in the contravariant action given by the power object construction, we will use the contravariant extension. Let us denote this contravariant functor by $F_X : \mathrm{Proj}_R \to \mathcal{A}_R$.

In practice, Proj_R is given by the Karoubi envelope (i.e. splitting the idempotents) of the free completion of BR under direct sums. This is just a fancy way of saying that a f.p. projective module M is a direct summand of a free module: $R^n = M \oplus M'$. Let $p : R^n \twoheadrightarrow M$ be the projector: M is the image of p and M' its kernel. In an abelian category, since kernels and cokernels exist, all idempotents splits. Since $F_X(R^n) = X^n$, we define $F_X(M)$ as the split object in $\mathcal{A}_R$ given by the idempotent $F_X(p) : X^n \to X^n$: $F_X(M)$ is the kernel of $F_X(p)$ and $F_X(M')$ its image (we reverse the order because we use the contravariant version of F_X).

Theorem 3.12. *With the notations above, if M is projective, then $F_X(M) = \mathcal{HOM}_R(M, X) = M \cdot X$ is the power object.*

Assume furthermore that $\mathrm{End}_R(X) = R$. Then F_X is fully faithful: if M_1 and M_2 are projective, then $\mathrm{Hom}_{\mathcal{A}}(M_2 \cdot X, M_1 \cdot X) = \mathrm{Hom}_R(M_1, M_2)$. In particular, the action $M \cdot X$ by projective module is free on $\mathcal{A}_R$.

Proof. Write $R^n = M \oplus M'$, and let $p : R^n \to R^n$ be the idempotent associated to M. Then p induces an idempotent on $\mathrm{Hom}_R(R^n, \mathrm{Hom}_{\mathcal{A}}(Y, X))$ which corresponds to the decomposition $\mathrm{Hom}_R(R^n, \mathrm{Hom}_{\mathcal{A}}(Y, X)) = \mathrm{Hom}_R(M, \mathrm{Hom}_{\mathcal{A}}(Y, X)) \oplus \mathrm{Hom}_R(M, \mathrm{Hom}_{\mathcal{A}}(Y, X))$. And $F_X(p)$ is an idempotent on X^n, which induces the decomposition $X^n = F_X(M) \oplus F_X(M')$, hence we also have an idempotent on $\mathrm{Hom}_{\mathcal{A}}(Y, X^n)$ (note that this reverse the order from before!) which induces the decomposition $\mathrm{Hom}_{\mathcal{A}}(Y, X^n) = \mathrm{Hom}_{\mathcal{A}}(Y, F_X(M)) \oplus \mathrm{Hom}_{\mathcal{A}}(Y, F_X(M'))$. But $\mathrm{Hom}_R(R^n, \mathrm{Hom}_{\mathcal{A}}(Y, X)) = \mathrm{Hom}_{\mathcal{A}}(Y, X)^n = \mathrm{Hom}_{\mathcal{A}}(Y, X)^n$ canonically, and this identification is compatible with our idempotents by functoriality. If follows that $\mathrm{Hom}_{\mathcal{A}}(Y, F_X(M)) = \mathrm{Hom}_R(M, \mathrm{Hom}_{\mathcal{A}}(Y, X))$, hence $F_X(M) = \mathcal{HOM}_R(M, X)$.

For the second statement, we have a map $\mathrm{Hom}_R(M_1, M_2) \to \mathrm{Hom}_{\mathcal{A}}(M_2 \cdot X, M_1 \cdot X)$ by functoriality. Writing $R^{n_1} = M_1 \oplus M_1'$, $R^{n_2} = M_2 \oplus M_2'$, and using the fact that $\mathrm{Hom}_R(R^{n_1}, R^{n_2}) = R^{n_1 n_2} = \mathrm{Hom}_R(X^{n_2}, X^{n_1}) = \mathrm{Hom}_R(X, X)^{n_1 n_2} = R^{n_1 n_2}$ under our assumption that $\mathrm{End}_R(X) = R$, we obtain that the map above is a bijection.

If two projective modules M_1, M_2 induce isomorphic objects $M_1 \cdot X, M_2 \cdot X$ in $\mathcal{A}_R$ (so with isomorphisms compatible with the orientation), then since the action is fully faithul isomorphisms reflect, and we have an isomorphism $M_1 \simeq M_2$ of R-modules.

□

4. The module action on oriented abelian varieties

In Section 4.1, we specialize the construction from Section 3.4 to the case of commutative proper group schemes, to obtain an action on oriented abelian varieties (which gives a group scheme in general). In Section 4.2 we look at the action from a projective module. In Section 4.3, we look at this action on primitively oriented elliptic curves, then in Section 4.4 we extend its properties to a subcategory of oriented abelian varieties. Finally in Section 4.5, we focus on computing this action in practice.

4.1. **The module action on commutative proper group schemes.** Let k be a field. Since commutative proper k-group schemes $\mathfrak{GroupSchemes}$ form an abelian category (see [JKP+18, § 4.2]), we can apply Theorem 3.7 to get a canonical symmetric monoidal action via the power object construction on R-oriented commutative proper group schemes, for R a commutative ring.

We will apply this action to oriented abelian varieties, in the case that R is a quadratic imaginary order. We denote by $\mathfrak{Ab}$ the category of abelian varieties, this is a subcategory of $\mathfrak{GroupSchemes}$, and $\mathfrak{Ab}_R$ is a subcategory of $\mathfrak{GroupSchemes}_R$. We recall that an abelian variety over k is a smooth proper group scheme A/k. The commutativity condition is then automatic. Equivalently, A/k is an abelian

variety whenever it is a proper group scheme, which is geometrically connected (equivalently, since 0_A is k-rational point, A/k is connected over k) and geometrically reduced (equivalently A is geometrically reduced at 0_A). If k is perfect, then this result also holds using "reduced" instead of "geometrically reduced". From now on, we will assume that k is perfect to avoid pathologies; in practice for our applications $k = \mathbb{F}_q$ will be a finite field.

In general, if A is an R-oriented abelian variety and M an arbitrary f.p. module, then $M \cdot A := \mathcal{HOM}_R(M, A) \in \mathfrak{GroupSchemes}_R$ is not an abelian variety, just a commutative proper group scheme.

For instance, the construction of Theorem 3.7 shows that $R/n \cdot A = A[n]$. We will see that the action behaves well when M is a f.p. projective R-module, in particular $M \cdot A$ is an abelian variety.

When R is a quadratic imaginary order, and A is isogeneous to a power of a primitively oriented elliptic curve E_0, in Theorem 4.17 we will give a criteria for when $M \cdot A$ is still an abelian variety, for M not necessarily projective. In Theorem 4.21 we explain how to extend the action to an action of Hermitian R-modules to keep track of polarisations.

The following lemma gives an alternative construction of $M \cdot X$ by describing its functor of points explicitly:

Lemma 4.1. *Let X be an R-oriented proper k-group scheme and M be a f.p. R-module. Let k' be a k-algebra, then $X(k')$ has a natural action from R. Then $(M \cdot X)(k') \simeq \mathrm{Hom}_R(M, X(k'))$.*

Proof. This is [JKP+18, Proposition 4.2]. □

Proposition 4.2. *Assume that R is a (not necessarily commutative) domain, f.p. as a $\mathbb{Z}$-module. If X is an R-oriented commutative proper group scheme, and M a f.p. R-module, then $M \cdot X = \mathcal{HOM}_R(M, X)$ is a commutative proper group scheme of dimension $\operatorname{rank} M \cdot \dim A$. In particular, if M is of torsion (i.e. is finite as a set), $\mathcal{HOM}_R(M, X)$ is a finite scheme.*

Proof. We know that $\mathcal{HOM}_R(M, X)$ is a proper group scheme by Theorem 3.7. If $X = A$ is an abelian variety, its dimension is given by [JKP+18, Proposition 4.3].

For a general proper reduced group scheme X, we let X^0 be its connected component at 0, this is an abelian variety of the same dimension as X, and X/X^0 is the finite group of components. The module action is right exact, so we have $0 \to M \cdot X^0 \to M \cdot X$. If N is the degree of X/X^0, then $[N] : X \to X$ factor through X^0, hence $M \cdot [N] : M \cdot X \to M \cdot X$ factor through $M \cdot X^{(0)}$, so the quotient $M \cdot X / M \cdot X^{(0)}$ is finite. It follows that $M \cdot X$ has the same dimension as $M \cdot X^{(0)}$, and we can apply the previous result.

For the general case, we consider $X^{red} \subset X$. The group $M \cdot X$ is constructed as the kernel of a matrix $X^n \to X^m$, and $M \cdot X^{red}$ is constructed as the kernel of the same matrix $X^{red,n} \to X^{m,red}$. But, if $\phi : X \to Y$ is a morphism of group, which induces $\phi^{red} : X^{red} \to Y^{red}$, then[3] $(\operatorname{Ker} \phi)^{red} \subset (\operatorname{Ker} \phi^{red}) \subset \operatorname{Ker} \phi$, so $(\operatorname{Ker} \phi)^{red} = (\operatorname{Ker} \phi^{red})^{red}$. So in particular, $M \cdot X^{red}$ has the same dimension as $M \cdot X$. □

To avoid repeating too many times the condition that ensures that an action still gives an abelian variety, or that the action of an isogeny on an isogeny is still an isogeny, we give the following definition.

Definition 4.3. Given an oriented abelian variety A and a f.p. torsion free module M, we say that M is compatible with A if $M \cdot A$ is still an abelian variety. Given an isogeny $\psi : M_2 \hookrightarrow M_1$, and an isogeny $\phi : A_1 \twoheadrightarrow A_2$, we say that ψ is compatible with ϕ if $\phi \cdot \psi : M_1 \cdot A_1 \to M_2 \cdot A_2$ is still an isogeny of abelian varieties (in particular, we require that $M_i \cdot A_i$ is an abelian variety). We say that ψ is compatible with A if ψ is compatible with $\mathrm{Id}_A : A \to A$, in that case the kernel is given by $M_1/M_2 \cdot A$ by right exactness. And similarly for the compatibility of M with $\phi : A_1 \to A_2$.

We will see in Theorem 4.5 that a projective module is always compatible with an oriented abelian variety.

Corollary 4.4. *If A is an oriented abelian variety, and $\psi : M_2 \hookrightarrow M_1$ is a monomorphism, with each M_i compatible with A, then $\psi \cdot A : M_1 \cdot A \twoheadrightarrow M_2 \cdot A$ is an epimorphism with kernel $(M_1/M_2) \cdot A$. In particular, if furthermore $M_2 \hookrightarrow M_1$ is an isogeny, then $\psi \cdot A$ is an isogeny.*

[3] I thank Dajano Tossici for this argument.

If $\phi : A_1 \twoheadrightarrow A_2$ is an oriented epimorphism with kernel U, and M is compatible with each A_i, then $M \cdot \phi : M \cdot A_1 \twoheadrightarrow M \cdot A_2$ is an epimorphism with kernel $M \cdot U$. In particular, if ϕ is furthermore an isogeny, $M \cdot \phi$ is an isogeny.

With the notations of Definition 4.3, for an isogeny ψ to be compatible with ϕ, it suffices that each M_i is compatible with each A_j.

Proof. We use a similar argument as in the proof of [JKP+18, Theorem 4.4.b].

If $M_2 \hookrightarrow M_1$, then from the exact sequence $M_2 \to M_1 \to M_1/M_2 \to 0$, we obtain $0 \to M_1/M_2 \cdot A \to M_1 \cdot A \to M_2 \cdot A$. Since M_1, M_2 are compatible with A, $M_1 \cdot A$ and $M_2 \cdot A$ are abelian varieties, so the image B of $M_1 \cdot A$ in $M_2 \cdot A$ is an abelian variety. By Proposition 4.2, the dimension of B is given by $\dim A(\operatorname{rank} M_1 - \operatorname{rank}(M_1/M_2)) = \dim A \operatorname{rank} M_2 = \dim M_2 \cdot A$, so $\dim B = \dim M_2 \cdot A$, hence $B = M_2 \cdot A$.

If $M_2 \hookrightarrow M_1$ is an isogeny, then $\operatorname{rank} M_2 = \operatorname{rank} M_1$, so $\dim M_1 \cdot A = \dim M_2 \cdot A$, so $M_1 \cdot X \twoheadrightarrow M_2 \cdot X$ is an isogeny. An alternative argument is that $M_2 \hookrightarrow M_1$ is an isogeny iff M_1/M_2 is a finite set, so equivalently of rank 0, but then the kernel of $M_1 \cdot X \twoheadrightarrow M_2 \cdot X$ is of dimension 0 by Proposition 4.2, hence is finite.

A similar argument works for $\phi : A_1 \twoheadrightarrow A_2$: we have an exact sequence $0 \to U \to A_1 \to A_2 \to 0$, hence a left exact sequence $0 \to M \cdot U \to M \cdot A_1 \to M \cdot A_2$. By assumption, each $M \cdot A_i$ is an abelian variety, so the image of $M \cdot A_1$ in $M \cdot A_2$ is an abelian variety of dimension $\operatorname{rank} M(\dim A_1 - \dim U) = \operatorname{rank} M \dim A_2 = \dim M \cdot A_2$. Likewise for an isogeny ϕ.

Combining these two cases, we obtain that ψ is compatible with ϕ whenever each M_i is compatible with each A_j. □

4.2. **The projective module action on abelian varieties.** Let R be a commutative ring and A/k be an R-oriented abelian variety. As explained in Section 3.5, the power object action $M \cdot A$ from a projective module is given by a split idempotent $A^n \to A^n$, which greatly simplifies the study of this action.

Theorem 4.5. *If $A \in \mathfrak{Ab}_R$ is an oriented abelian variety, and M is a f.p. projective module, then $M \cdot A$ is still an abelian variety. And we have a canonical isomorphism $(M \cdot A)^\vee \simeq M^\vee \cdot A^\vee$.*

If $\psi : M_2 \hookrightarrow M_1$ is an isogeny between projective modules, $\psi \cdot A$ is an isogeny, and the dual module isogeny $\tilde{\psi} : M_1^\vee \to M_2^\vee$ gives the dual isogeny $\tilde{\psi} \cdot A^\vee : M_2^\vee \cdot A^\vee \to M_1^\vee \cdot A^\vee$.

Proof. If $R^n = M \oplus M'$, then by Theorem 3.12, $A^n = M \cdot A \oplus M' \cdot A$, hence $M \cdot A$ is a quotient of A^n, so is an abelian variety.

If A is R-oriented, duality gives an R-orientation on the dual $A^\vee$ of A, if $i : R \to \operatorname{End}(A)$, we define $i^\vee : R \to \operatorname{End}(A)$ via $i^\vee(r) = \widehat{i(r)}$. and if $F : A^n \to A^m$ is a matrix of elements in R, then $F^\vee : A^{\vee,m} \to A^{\vee,n}$ is given by the transpose matrix $F^\vee = F^T$. If the projective module M is given by splitting the idempotent p on R^n, then $M^\vee$ is given by splitting the idempotent $p^\vee$ on $R^{\vee,n} = R^n$, so $M^\vee \cdot A^\vee$ is given by splitting the idempotent $p^\vee \cdot A^\vee$ on $A^{\vee,n}$. On the other hand, $M \cdot A$ is given by splitting the idempotent $p \cdot A$: $A^n = M \cdot A \oplus M' \cdot A$, hence by duality we get the splitting idempotent $(p \cdot A)^\vee : A^{\vee,n} = (M \cdot A)^\vee \oplus (M' \cdot A)^\vee$. Since $(p \cdot A)^\vee = p^\vee \cdot A^\vee$ from our matrix computation above, we get that $(M \cdot A)^\vee = M^\vee \cdot A^\vee$.

The statement on duality also follows from splitting the idempotent and the fact that the dual endomorphism of an endomorphism of A^g given by a matrix of elements in R is given by the transpose matrix. The fact that $\psi \cdot A$ is an isogeny is a consequence of Corollary 4.4 and the fact that projective modules are compatible with abelian varieties. □

We can incorporate polarisations in our action by considering Hermitian modules. Let us first recall the definition.

Definition 4.6. A polarisation $\lambda : A \to A^\vee$ is an autodual morphism. Equivalently, by [Mum70, Theorem 2 p.188], a polarisation is a morphism $\lambda = \Phi_{\mathcal{L}}$ induced by a line bundle.

The polarisation is said to be non degenerate if λ is an isogeny, and to be positive if $\mathcal{L}$ is ample, it is then automatically non degenerate. A principal polarisation is a positive polarisation which is an isomorphism.

We restrict to the case that R is a commutative domain. Let (A, λ_A) be a principally polarised R-oriented abelian variety. To get meaningful results, we need to assume that R is stable under the Rosatti involution on A, which we will denote by $\bar{\cdot}$. Replacing R by its image in $\mathrm{End}(A)$ if needed, we can also assume that $R \to \mathrm{End}(A)$ is a monomorphism. Then by [Mum70, § 21], $K = R \otimes_Q$ is either a totally real field, in which case $\bar{\cdot}$ is the identity, or K is a CM field, in which case $\bar{\cdot}$ is the canonical Galois involution of K over its totally real subfield K_0. By abuse of terminology, we call R a "CM order" in both cases, including the totally real case.

In practice, we will look at the case where R is quadratic imaginary, but the notions introduced in Section 2 still make sense for the more general CM case. In particular, if M is torsion free, we can also define $M^\vee = \mathrm{Hom}_{\overline{R}}(M, R)$, and we still have the duality morphism $M \simeq (M^\vee)^\vee, m \mapsto (\psi \mapsto \overline{\psi(m)})$. This is an isomorphism if M is projective. In particular, an autodual morphism $\psi : M \to M^\vee$, meaning that $\psi = M \to M^{\vee\vee} \xrightarrow{\psi^\vee} M^\vee$ is the same thing as an integral Hermitian form H_M on M. We say that an Hermitian form H on $V = M \otimes_R K$ is positive definite whenever the $H(x, x)$ are totally positive for all x (since H is Hermitian, $H(x, x) \in K$ is stable by the involution, so is in the totally real subfield K_0). And we say that (M, H_M) is unimodular if H is definite positive on V and $M^\sharp = M$.

Theorem 4.7. *Let (A, λ_A) be a principally polarised abelian variety, and $(R, \bar{\cdot})$ a CM order as above.*

Let (M, H_M) be a projective module with a non degenerate Hermitian polarisation H_M (we recall that this means that H_M is an Hermitian form integral on $M^\sharp$). Then we have an autodual isogeny $(M, H_M) \cdot \lambda_A : M \cdot A \to (M \cdot A)^\vee$. This autodual isogeny is induced by a line bundle (i.e. is a polarisation) iff H_M is definite positive, and it gives a principal polarisation on $M \cdot A$ iff (M, H_M) is furthermore unimodular.

Let $\psi : M_2 \hookrightarrow M_1$ be an isogeny of projective R-modules, and $\phi = \psi \cdot A : M_1 \cdot A \to M_2 \cdot A$ be the induced isogeny of oriented abelian varieties. Then the dual module isogeny $M_1^\vee \to M_2^\vee$ gives the dual isogeny $M_2^\vee \cdot A^\vee \to M_1^\vee \cdot A^\vee$, and the contragredient isogeny $\tilde{\phi}$ corresponds to the action of the adjoint of ψ: $\tilde{\psi} : (M_1, H_1) \to (M_2, H_2)$. In particular, a n-similitude $(M_2, H_2) \to (M_1, H_1)$ between unimodular projective modules induces a n-isogeny $M \cdot A_1 \to M \cdot A_2$.

Proof. We follow the line of arguments from [KNRR21]. These arguments are essentially the same as the ones given by Serre in his course [SHOR20] and in his appendix to [LS01].

By definition of the Rosatti involution, we have that λ_A is an R-oriented anti-isomorphism, for the canonical orientation induced on $A^\vee$ from the one on A: if $i : R \to \mathrm{End}(A)$, we have $\lambda_A \circ i(\overline{r}) = \widehat{i(r)} \circ \lambda_A$. To get a R-oriented isomorphism, we need to change the orientation on $A^\vee$: we define $i^\vee(r) = \widehat{i(\overline{r})}$. Now the same statement as in Theorem 4.5 still hold, provided that we use $M^\vee = \mathrm{Hom}_{\overline{R}}(M, R)$ instead of $\mathrm{Hom}_R(M, R)$. In particular, this time, to an morphism $\gamma : A^n \to A^m$ given by a matrix F of elements in R, then the dual morphism $A^{\vee,m} \to A^{n,\vee}$ is given by the conjugate transpose: $F^* = \overline{F^T}$. (A restatement of this discussion is as follows: if $M^* = \mathrm{Hom}_R(M, R)$ is the standard dual, we have $(M \cdot A)^\vee = M^* \cdot A^\vee = M^\vee \cdot A$.)

Now, a polarisation H_M on M is an integral Hermitian form on $M^\sharp \simeq M^\vee$, and since H_M is assumed to be non degenerate on $M \otimes_R K$, we have that $H_M : M^\vee \simeq M^\sharp \to M$ is an isogeny. By Theorem 4.5, the action gives an isogeny $M \cdot A \to M^\vee \cdot A \simeq M^\vee \cdot A^\vee \simeq (M \cdot A)^\vee$, where the last isomorphism comes from Theorem 4.5, and the one before from the fact that λ_A is an oriented isomorphism. Since H_M is Hermitian, $M^\vee \to M$ is autodual, hence the corresponding isogeny $M \cdot A \to (M \cdot A)^\vee$ is also autodual, since everything has been set up to be compatible with duality on both sides.

It remains to prove that this isogeny is induced by an ample line bundle iff H_M is positive definite. Since M is of rank g, we have an isogeny $M \to R^g$, hence an isogeny $A^g \to M \cdot A$. By [KNRR21, Lemma 3.5], the question reduces to whether the induced isogeny $A^g \to A^{\vee,g}$ comes from an ample line bundle, so we can assume that $M = R^g$ is free. On A^g, we have the product polarisation as a principal polarisation. The other polarisation are given by totally positive elements in $NS(A^g)$ which correspond to totally positive symmetric elements in $\mathrm{End}(A^g)$ [Mum70, Proof of Theorem 6 p.208–210]. We also have a canonical product polarisation (R^g, H_R^g) on R^g, and the other positive definite Hermitian forms are also given by totally positive symmetric elements in $\mathrm{End}_R(R^g) = M_g(R) \subset \mathrm{End}_R(A^g)$, by the same

arguments as for abelian varieties. The result follows. See also the argument by Serre at the end of [LS01, p. 26] for an alternative proof when R is quadratic imaginary.

The last statement on the dual and contragredient isogeny follows from our matrix computation. □

If we have an orientation $(R, \bar{\cdot}) \subset \mathrm{End}(A)$ (where $\bar{\cdot}$ is induced by the Rosatti involution), Theorem 4.7 still apply to give an action of polarised Hermitian projective left R-modules on (A, λ_A), since [Mum70, Proof of Theorem 6 p.208–210] also gives the general non commutative case.

4.3. **The module action on primitively oriented elliptic curves.** The module action on an elliptic curve with a primitive orientation by E_0 is particularly well behaved, we can act by an arbitrary torsion free f.p. R-module M and still get an abelian variety (even for non projective M), and we will obtain an antiequivalence of category. This is reminiscent of having a principal homogeneous space (aka a torsor) for a group action.

We remark that if R is an orientation on $E_0/\mathbb{F}_q$, with R a quadratic imaginary order, then the Rosatti involution on E_0 always leave R stable (and induces the complex conjugation on it), and the condition $\mathrm{End}_R(A) = R$ from Theorem 3.12 is equivalent to R being a primitive orientation. Hence we already knew that the action from projective modules on E_0 was fully faithful, but by the antiequivalence of Theorem 4.9, this still hold true for torsion free modules.

We first define precisely the exact subcategory of oriented abelian variety which will give an antiequivalence with modules via the module action on E_0. We fix $E_0/\mathbb{F}_q$ be an elliptic curve, primitively oriented by R. More precisely, we have two cases: $E_0/\mathbb{F}_q$ is an ordinary curve, and $R = \mathrm{End}_{\mathbb{F}_q}(E_0)$ is the natural orientation induced by the Frobenius, or $E_0/\mathbb{F}_{p^2}$ is a maximal supersingular curve, and R is a primitive orientation inside $\mathfrak{O}_0 = \mathrm{End}(E_0) = \mathrm{End}_{\mathbb{F}_{p^2}}(E_0)$. In the first case p is split in R, while in the second case p is either ramified or inert; the conductor of R is always prime to p.

An important special case for us will be $E_0/\mathbb{F}_p$ a rational supersingular curve, and $R = \mathrm{End}_{\mathbb{F}_p}(E_0)$, which is a quadratic order, and the orientation induced by the Frobenius like the ordinary case. This is the setting of CSIDH.

Definition 4.8. We let $\mathfrak{Ab}_{E_0,R}$ be the subcategory of R-oriented abelian varieties $A \in \mathfrak{Ab}_R$, with A R-isogeneous to E_0^g (over its base field).

In the case that p is inert in R, we require furthermore that the action of R on the tangent space of A is isomorphic to the action of R on the tangent space of E_0^g.

We will always assume that the orientation on our abelian varieties is effective. This is notably the case for the Frobenius orientation (via isogeny division to handle general endomorphisms).

We remark that the orientation on $A \in \mathfrak{Ab}_{E_0,R}$ needs not be primitive in our definition. For instance, in the CSIDH case of $E_0/\mathbb{F}_p$ supersingular, if we take E_0 at the bottom of the 2-isogeny volcano, i.e. such that $\mathrm{End}_{\mathbb{F}_p}(E_0) = \mathbb{Z}[\pi] = \mathbb{Z}[\sqrt{-p}]$, then $\mathfrak{Ab}_{E_0,R}$ consists of all supersingular abelian varieties defined over $\mathbb{F}_p$ isogeneous to a power of E_0 so in particular it contains the elliptic curves at the top of the volcano, which are oriented by the full maximal order.

Theorem 4.9. *The contravariant action $M \mapsto M \cdot E_0$ from R-modules to proper group scheme is exact and faithful. It induces an antiequivalence of category between torsion free f.p. R-modules and abelian varieties in $\mathfrak{Ab}_{E_0,R}$, whose inverse is given by $A \in \mathfrak{Ab}_{E_0,R} \mapsto \mathrm{Hom}_R(A, E_0)$.*

Proof. This was proven (except for the faithfulness which is implicit) in [JKP+18] for the Frobenius orientation, and extended in [PR23a] to the case of an arbitrary orientation. The faithfullness follows from the fact that $\mathfrak{F}$ reflect 0, i.e., $\mathfrak{F}(M) = 0$ iff $M = 0$. (Indeed, if $\mathfrak{F}(M) = 0$ then M has to be of rank 0, so of torsion, and $1 = \deg \mathfrak{F}(M) = \#M$ implies that $M = 0$).

Unfortunately, [PR23a] is not yet public, the article has been in limbo since the publication of [PR23b]. We hope to publish it soonish. Meanwhile, for Section 6, we only need the case of E_0 supersingular over $\mathbb{F}_p$, so the Frobenius orientation, which as mentionned is already proven in [JKP+18]. As an alternative, since we only act by projective modules in Section 6, it suffices to apply Theorems 4.5 and 4.7. □

Example 4.10.

- If $M = \mathfrak{a}$ is given by an inversible ideal, we will see in Corollary 4.25 that the action $\mathfrak{a} \cdot E_0$ corresponds to the usual ideal action from $\mathrm{Pic}(R)$.
- If $A = M \cdot E_0$, then by Lenstra's theorem [Len96], $A[n](\overline{k})$ is isomorphic as a R-module to M/nM for n prime to p (a similar result should hold on the p-torsion taking the Dieudonné module instead).
- If M is torsion of degree n, then $M \cdot E_0$ is a finite group scheme of degree n [JKP+18, Theorem 4.4.(e)]. In particular, if $\psi : M_2 \hookrightarrow M_1$ is an isogeny of degree $d = \#M_1/M_2$, $\phi = \psi \cdot E_0 : A_1 \to A_2$ is an isogeny of degree d.
- Since the action on E_0 is exact, a monomorphism $M_2 \hookrightarrow M_1$ induces an epimorphism $M_1 \cdot E_0 \twoheadrightarrow M_2 \cdot E_0$, and this epimorphism has finite kernel (i.e., is an isogeny) iff the cokernel M_1/M_2 is finite (as a set). So monomorphisms with finite cokernel correspond to isogenies.
- By Lemma 2.2, it follows that every abelian variety A in $\mathfrak{Ab}_{E_0,R}$ is isomorphic as an *unpolarised variety* to a product of elliptic curves in $\mathfrak{Ab}_{E_0,R}$: $A = \prod(\mathfrak{a}_i \cdot E_0)$. So in the unpolarised setting, the module action brings nothing compared to the ideal action. The real interest of the module action comes from how it acts on polarisations.

We can keep track of polarisations exactly as in Theorem 4.7:

Theorem 4.11. *Let $A \in \mathfrak{Ab}_{E_0,R}$, A can thus be written as $A = M \cdot E_0$ for some torsion free R-module M. Then $A^\vee = M^\vee \cdot E_0$, a symmetric morphism $\phi : A \to A^\vee$ (equivalently a morphism induced by a line bundle $\mathcal{L}$ on A) respecting the orientation corresponds to an Hermitian R-form H_M on $M^\vee$, ϕ is an isogeny (i.e. $\mathcal{L}$ is non degenerate) iff H_M is non degenerate, and ϕ is a polarisation (i.e. $\mathcal{L}$ is an ample line bundle) iff H_M is positive definite.*

Finally, a principally polarised abelian variety $(A, \lambda_A) \in \mathfrak{Ab}_{E_0,R}$ corresponds to a unimodular positive definite Hermitian module (M, H_M).

Proof. This is proven in [KNRR21] in the ordinary case and [PR23a] in the general case. As explained in the proof of Theorem 4.7, the argument is essentially the same as in the appendix by J.-P. Serre in [LS01]. The explicit construction of H_M from λ_A follows from unraveling the definitions. □

Remark 4.12 (The Hermitian form associated to the module of morphisms)**.** Given (A, λ_A) a polarised abelian variety in $\mathfrak{Ab}_{E_0,R}$, we can recover (M, H_M) as follows. First $M = \mathrm{Hom}_R(A, E_0)$ is the module of oriented morphisms to E_0. Next, since $A^\vee = M^\vee \cdot A$, two elements $x, y \in M^\vee$, seen as morphisms $R \to M^\vee$, induces morphisms $x \cdot E_0, y \cdot E_0 : A^\vee \to E_0$. Then the dual of $y \cdot E_0$ (which is equal to $y^\vee \cdot E_0$) gives a morphism $E_0 \to A$ (using the canonical polarisation on E_0). The composition $x \cdot E_0 \circ \lambda_A \circ y^\vee \cdot E_0$ gives an oriented morphism $\gamma : E_0 \to E_0$, which belongs in R since R is a primitive orientation on E_0. We then have $H_M(x, y) = \gamma$.

The module antiequivalence of category from Theorem 4.9 is a powerful tool which was used in [PR23a] to compute class group actions in polynomial time (before we found an alternative way in [PR23b] bypassing the equivalence). It is instructive to translate concepts from the elliptic curve and abelian variety side to the module side and vice versa. For instance, torsion modules can be used to handle level structure, and non invertible ideals to handle ascending isogenies. We refer to the talk [Rob24a] for many examples.

An important thing to note is that despite the notation $\mathfrak{Ab}_{E_0,R}$ does not depends too much on E_0: any other base point $E_0' \in \mathfrak{Ab}_{E_0,R}$ (i.e. another primitively oriented curve isogeneous to E_0) will give the same category.

Lemma 4.13. *Let $E_0' \in \mathfrak{Ab}_{E_0,R}$ be another primitively R-oriented elliptic curve. Let $I = \mathrm{Hom}_R(E_0', E_0)$, this is an invertible ideal. Then $M \cdot E_0' = M \cdot I \cdot E_0 = (M \otimes_R I)E_0$ and if $A \in \mathfrak{Ab}_{E_0,R}$, $\mathrm{Hom}(A, E_0) = I\,\mathrm{Hom}(A, E_0')$.*

Remark 4.14 (Internal monoidal structure)**.** Working in $\mathfrak{Ab}_{E_0,R}$, every abelian variety is of the form $A = M \cdot E_0$, so we can define $A_1 \otimes_{E_0} A_2$ as $(M_1 \otimes_R M_2) \cdot E_0$ where $A_i = M_i \cdot E_0$ (as long as the module tensor product is torsion free).

This gives a nice monoidal structure on $\mathfrak{Ab}_{E_0,R}$, which unfortunately is not effective (effectivity is equivalent to solving the action-CDH problem from E_0, see Section 6). Otherwise this would have been very useful for cryptographic protocols!

To reformulate: this tensor product is effective only if we know one of the two modules. To reformulate again: the monoidal action is effective, but the monoidal structure it induces on $\mathfrak{Ab}_{E_0,R}$ is not. Also the action does not depend on the base point E_0 while the tensor product $\otimes_{E_0}$ does. Note the similarity with a principal homogeneous group action from G on X, which can induce non effective group structures on X once we fix a base point $x_0 \in X$.

4.4. **The module action on abelian varieties isogeneous to a power of a primitively oriented elliptic curve.** For efficiency reason, in our cryptographic applications of the projective module action from Section 4.2, we will often restrict the action to the orbit of a (primitively oriented) elliptic curve E_0. Choosing E_0 as a base point for a module key exchange, for instance, allows to reduce the dimension of the abelian varieties involved. Now, thanks to Section 4.3, we can actually define the action in greater generality than from just projective modules (compared to the general case in Section 4.2).

First we need a definition:

Definition 4.15. Let $A \in \mathfrak{Ab}_{E_0,R}$, so that $A = M_A \cdot E_0$ for some torsion free module $M_A = \mathrm{Hom}_R(A, E_0)$. Then we define the conductor or vertical gap of A relative to R as the conductor of M_A relative to R; it does not depend on the choice of base point E_0 by Lemma 4.13. We say that A is horizontal if the vertical gap is one, i.e. if M_A is projective.

If M is a torsion free f.p. R-module, we say that it is Tor-independant with A whenever M and M_A are Tor-independant, i.e. have coprime relative conductors.

This notion of vertical gap corresponds to the one we can expect from isogeny volcanoes:

Example 4.16. Let I be an ideal in R (not necessarily invertible). Then $\mathrm{End}_R(I \cdot E_0) = \mathrm{End}_R(I) = O(I)$ is the order associated to I. In particular, if $I = \mathfrak{f}$ is the conductor ideal relative to S, then $\mathfrak{f} \subset R$ induces the going up isogeny $E_0 \to I \cdot E_0$, and $I \cdot E_0$ is at height $f = N_R(\mathfrak{f})$ with respect to the isogeny volcano.

A similar example hold for an abelian variety in $\mathfrak{Ab}_{E_0,R}$, since it is isomorphic (as an unpolarised) abelian variety to a product of elliptic curves $A = \prod_{i=1}^{g} E_i$, with the vertical gap of E_i dividing the one of E_{i+1}. The vertical gap of A is then the vertical of the highest one E_g.

Theorem 4.17. *Let $A \in \mathfrak{Ab}_{E_0,R}$ and M a torsion free f.p. R-module. If M and A are* Tor*-independant, i.e. the conductor of A and M relative to R are coprime to each other, then M is compatible with A: the power object $M \cdot A := \mathcal{HOM}_R(M, A)$ is in $\mathfrak{Ab}_{E_0,R}$, and in particular is still an abelian variety. The copower object $M \otimes_R A$ also exist in $\mathfrak{Ab}_{E_0,R}$.*

Proof. By Theorem 4.9, A comes from a module M_A: $A = M_A \cdot E_0$, and $M \cdot A = (M \otimes_R M_A) \cdot E_0$. Now under our assumptions, $M_A \otimes_R M$ is torsion free, so its action on E_0 gives an abelian variety by Theorem 4.9.

We remark that we can use Theorem 4.9 directly to construct the power object $M \cdot A$ without refering to Section 3.4: since we have an antiequivalence of categories, a power object will correspond to the copower object $M_A \otimes_R M$ in R-modules, and a copower object to the power object $\mathrm{Hom}(M, M_A)$ in R-modules. Under our assumptions, these modules are torsion free by Lemma 2.7, so they give abelian varieties. □

Remark 4.18 (On the notation)**.** We warn the reader that there is an unfortunate clash of notation where our $\mathcal{HOM}_R(M, A)$ was denoted by $M \otimes_R A$ in [Rob24a]. The reason for that notation is due to the construction of the object $\mathcal{HOM}_R(M, A)$ as $(M \otimes M_A) \cdot E_0$: it corresponds to the copower object in the category opposed to $\mathfrak{Ab}_{E_0,R}$. In this article, since we work over $\mathfrak{Ab}_{E_0,R}$ and not its opposed category we prefer to use the admittedly more correct notation $\mathcal{HOM}_R(M, A)$, which makes it clear we have a contravariant symmetric monoidal action. Of course, we could also use the copower construction from Theorem 4.17 to have a covariant action, but from my experience the contravariant one behaves better in many way, in particular with respect to level structure (see Section 1.2).

Example 4.19.

- If M is projective, it is of relative conductor 1, so $M \cdot A := \mathcal{HOM}_R(M, A)$ is an abelian variety for any $A \in \mathfrak{Ab}_{E_0,R}$ (which we already knew from Theorem 4.5).
- Since E_0 is of relative conductor 1, $M \cdot E_0 = \mathcal{HOM}_R(M, E_0)$ is an abelian variety for any torsion free f.p. module M, as we had already seen in Theorem 4.9. More generally, if $A \in \mathfrak{Ab}_{E_0,R}$ is horizontal, $M \cdot A$ is an abelian variety for any torsion free f.p. module M.

Example 4.20 (Categorical constructions)**.** Because we have an antiequivalence of category, categorical constructions on one side are mapped into their coequivalent on the other side.

For instance, a direct sum is mapped to a direct sum (because it is both a product and a coproduct), and a module pullback $M_1 \times_M M_2$ correspond to a pushforward on the abelian variety side. In particular, if $M_1 \hookrightarrow M$, $M_2 \hookrightarrow M$ are two modules isogenies, corresponding to the abelian variety isogenies $A \to A_1, A \to A_2$, where $A = M \cdot E_0, A_i = M_i \cdot E_0$, then the pushforward isogeny $A \to A_{12}$ with kernel $K_1 + K_2$ correspond to the module isogeny $M_1 \cap M_2 \hookrightarrow M$, while the isogeny $A \to A'_{12}$ with kernel $K_1 \cap K_2$ corresponds to the module isogeny $M_1 + M_2 \hookrightarrow M$.

Like usual, we are really interested in polarised abelian varieties. The nice thing about having a monoidal action, is that it handles morphism, hence in particular polarisations, for free: let $\lambda_A : A \to A^\vee$ be a symmetric morphism in $\mathfrak{Ab}_{E_0,R}$, and $\Phi_H : M \to M^\vee$ be the application induced by an Hermitian form, then by functoriality we have a morphism $M \cdot A \to M^\vee \cdot A^\vee$, which has to be symmetric by the functorial properties of our action (we can also check this directly using the construction in Theorem 4.17). We denote the corresponding morphism $H \cdot \lambda_A$.

Specialising this to ppavs, we have:

Theorem 4.21. *Let $A \in \mathfrak{Ab}_{E_0,R}$, and suppose that M is compatible with A. (for instance M is projective or A is horizontal), then $M^\vee$ is compatible with $A^\vee$, and $M^\vee \cdot A^\vee = (M \cdot A)^\vee$.*

If λ_A is a polarisation on A which lives in $\mathfrak{Ab}_{E_0,R}$, and H_M a positive definite Hermitian form on $M^\vee$, then $H_M \cdot \lambda_A$ is a polarisation on $M \cdot A$. In particular, if λ_A is principal and H_M unimodular on M, then $(M \cdot A, H_M \cdot \lambda_A)$ is a ppav.

Given a principal polarisation λ_A as above on A, assume that $\psi : (M_2, H_2) \to (M_1, H_1)$ is a n-similitude with the M_i compatibles with A. Then $\phi = \psi \cdot A : (M_1 \cdot A, H_1 \cdot \lambda_A) \to (M_2 \cdot A, H_2 \cdot \lambda_A)$ is a n-isogeny, which we will often denote simply by $M_2 \cdot A \to M_1 \cdot A$. Furthermore the contragredient isogeny $\tilde{\phi}$ corresponds to the action of the adjoint of ψ: $\tilde{\psi} : (M_1, H_1) \to (M_2, H_2)$.

Proof. Let $M_A = \mathrm{Hom}_R(A, E_0)$. Then by the coprimality of the vertical gaps, and the fact that M and $M^\vee$ have the same relative conductors, we have $M_A^\vee \otimes_R M^\vee \simeq (M_A \otimes_R M)^\vee$, hence the first statement follows.

The rest is immediate from the construction of Theorem 4.17, and the fact that the tensor product of two positive definite Hermitian forms (resp. unimodular modules) is positive definite (resp. unimodular), so in particular the polarisation is compatible with the Hermitian form.

For the statement on the similitude, we first note that $M_1 \cdot A \to M_2 \cdot A$ is an isogeny by Corollary 4.4. And since $\psi^* H_1 = nH_2$, this remains true when tensoring with M_A, hence $M \cdot A \to N \cdot A$ is a n-isogeny. The last statement follows because all the constructions are compatible with the duality. □

Example 4.22 (The ideal vs the module point of view for oriented elliptic curves)**.** In the ideal point of view, an ideal class $[I]$ encodes an isomorphism class E of an elliptic curve isogeneous to E_0, and a choice of integral ideal $I \subset R$ in the class encodes an isogeny $E_0 \to E$.

Given two elliptic curves E_1, E_2 represented by (invertible) ideals I_1, I_2 respectively, isogenies $E_1 \to E_2$ are represented by integral ideals J equivalent to $I = I_2 I_1^{-1}$. Since $I^{-1} = \overline{I}/N(I)$, taking $x \in I$ gives such an ideal via $J := I\overline{x}/N(I) \sim I$, we remark that the corresponding isogeny is of degree $N(J) = N(x)/N(I)$.

In the module point of view, an ideal I also represent an elliptic curve $E_I = I \cdot E_0$. There is a unique principal polarisation (0_E) on an elliptic curve, on the module size this corresponds to the fact that there is a unique (canonical) unimodular form $H_I = H_R/N(I)$ on I, i.e. $H_I(x, y) = x\overline{y}/N(I)$. One could look at multiples $n(0_E)$ of this principal polarisation; this amount to replacing H_I by H_I/n.

Now this time an isogeny $E_1 \to E_2$ corresponds to a similitude $(I_2, H_2) \to (I_1, H_1)$. If $z \in I^{-1}$, we can build such a map by taking $\psi_z : r \mapsto zr$; this is a $N := N(z)N(I_2)/N(I_1)$-similitude Now, writing $z = \overline{x}/N(I)$, we get that $N = N(x)/N(I)$, as is consistent with the ideal point of view.

It is thus quite straightforward to move between the two point of views. In several aspect, the module point of view is nicer; first morphisms corresponds to morphisms of modules (rather than to objects). But the main advantage is as follow: from the module point of view, specifying an integral ideal I not only specify a module but also a canonical map $I \hookrightarrow R$ (via the inclusion). On the elliptic curve side, this means that an ideal corresponds to both an elliptic curve *and* a specific isogeny $E_0 \to E$. For many constructions on elliptic curves we do not need to fix such a specific isogeny from the base curve E_0; in that sense the ideal representation is less functorial than the module one because it impose our constructions to be compatible with that spurious isogeny choice. In the "stuff, structure and properties" categorical parlance, the ideal point of view corresponds to an extra *stuff* compared to the module point of view.

Remark 4.23 (Going up in orientation)**.** Let $R \subset S$, and E_0' an elliptic curve isogeneous to E_0 and primitively oriented by S. If A is an abelian variety oriented by R, then there is a unique S-orientation compatible with the one given by R, if it exists. Indeed, if $s : A \to A$ is an endomorphism corresponding to $s \in S$, then for some multiple $ns \in R$, so $ns : A \to A$ is the endomorphism corresponding to $ns \in R$, which uniquely determine s by division. This also gives a way to test if an orientation extends, via the efficient isogeny division algorithm of [Rob22b]. (From the module point of view, this corresponds to the fact that a R-linear map $M \to M$ on a torsion free module extends in at most one way to a S-linear map.)

In other words, in the "stuff, structure and properties" categorical parlance, in the category of R-oriented abelian varieties being S oriented (in a way compatible with the R-orientation) is just a *property*.

If A is S-oriented, when we have a f.p. R-module M, then $M_S = M \otimes_R S$ is a f.p. S-module. We can consider two actions: $M \cdot A$ in R-oriented proper group schemes, or $M_S \cdot A$ in S-oriented proper group schemes; these give the same schemes by Proposition 3.9.

In particular, the abelian varieties that are given by a S-module action (or as we have just seen R-module action) from E_0' are S-oriented, and conversely an S-oriented abelian variety in $\mathfrak{Ab}_{E_0,R}$ is R-isogeneous to E_0' by hypothesis, so is S-isogeneous to it, and so is of the form $M \cdot E_0'$ for a torsion free S-module.

This explains the Tor-independant condition for $M \cdot E_0'$ to still be an abelian variety: $M \cdot E_0' = (M \otimes_R S) \cdot E_0'$, and we want $M \otimes_R S$ to still be torsion free for the action to give an abelian variety.

Now let $\mathfrak{f}$ be the conductor of R in S, and assume that $E_0' = \mathfrak{f} \cdot E_0$ is given by the going up isogeny. Let $A = M' \cdot_S E_0'$ with M' a torsion free S-module, then as we have seen above, we also have $A = M \cdot_R E_0'$ for any M such that $M' = M \otimes_R S$. But we also have $M \cdot_R E_0' = M \cdot_R S \cdot_R E_0 = (M \otimes_R S) \cdot_R E_0 = M' \cdot_R E_0$. In other words: $\mathrm{Hom}_S(M \otimes_R S, E_0') = \mathrm{Hom}_R(M, E_0') = \mathrm{Hom}_R(M, \mathrm{Hom}_R(S, E_0)) = \mathrm{Hom}_R(M \otimes_R S, E_0)$, for a module M Tor-independant with S, as expected by functoriality.

Now for the Hermitian form, one needs to be a bit careful because the S-Hermitian form on $M \otimes_R S$ (seen as a S-module) induced from H_M is given by extension of scalar $H(s_1 \otimes_R m1, s_2 \otimes_R m_2) = s_1\overline{s_2}H_M(m_1, m_2) = H_K(s_1, s_2)H_M(m_1, m_2)$, while the R-Hermitian form on $M \otimes_R S$ (seen as a R-module) is given by $H_M \otimes_R H_S$, with $H_S = fH_K$ when S is seen as a unimodular R-module, where $f = [S : R]$. Note also that $M_S = M \otimes_R S$ is isomorphic to $M_S' = M \otimes_R \mathfrak{f}$ as a S-module, but in the latter isomorphism we have $H_S' = H_M \otimes_R H_{\mathfrak{f}} = H_M/f$.

Similarly, if $A = M_A' \cdot_S E_0'$ and $B = M_B' \cdot_S E_0'$, with $M_A' = \mathrm{Hom}_S(A, E_0') = \mathrm{Hom}_R(A, E_0)$, we have $\mathrm{Hom}_S(A, B) = \mathrm{Hom}_S(M_B', M_A') = \mathrm{Hom}_R(M_B', M_A') = \mathrm{Hom}_R(A, B)$.

Our final remark is that we can also use the conductor square and Milnor exision to give a refined correspondance between projective modules over R and S, see [Rob24b, Appendix D].

4.5. **Computing the module action.** Since our action comes from the canonical power object construction, it is purely functorial, hence every natural way one can think to actually compute it works! We will see that the natural generalisation of the known algorithms to compute the ideal action (via the kernel, or via Clapotis [PR23a; PR23b]) work equally as well for the module action.

4.5.1. *The kernel approach.* From the module point of view, the ideal action works as follows. An integral ideal $\mathfrak{a} \subset R$ corresponds to a $N(\mathfrak{a})$-similitude $i : (\mathfrak{a}, H_R/N(\mathfrak{a})) \to (R, H_R)$, for the inclusion map $\mathfrak{a} \to R$, where $H_R/N(\mathfrak{a})$ is the canonical Hermitian form making $\mathfrak{a}$ a unimodular module. If E is R-oriented, we can look at the kernel $E[i(\mathfrak{a})]$, which is the intersection of the kernels of the image by i of the generators of $\mathfrak{a}$. This kernel is of degree $N(\mathfrak{a})$, and the quotient $E/E[i(\mathfrak{a})]$ gives $\mathfrak{a} \cdot E$. We can look at different maps $i' : \mathfrak{a} \to R$; for instance if $\mathfrak{a}$ is inversible and $z \in \mathfrak{a}^{-1} = \overline{\mathfrak{a}}/N(\mathfrak{a})$, then $i_z : \mathfrak{a} \to R, x \mapsto xz$ is such a map. It is a $N(z)N(\mathfrak{a})$-similitude, and we can still define $\mathfrak{a} \cdot E$ as the quotient of E by $E[i_z(\mathfrak{a})]$. We remark that the codomain is the same, but the isogenies $E \to \mathfrak{a}E$ are different in both construction. From the ideal point of view, we usually present this alternative isogeny as follows: $i_z(\mathfrak{a}) = \mathfrak{a}' \subset R$ is an integral ideal equivalent to $\mathfrak{a}$, of norm $N(z)N(\mathfrak{a})$, and $E[i_z(\mathfrak{a})] = E[\mathfrak{a}']$. Writing $z = \overline{x}/N(\mathfrak{a})$ for some $x \in \mathfrak{a}$, we remark that $N(z)N(\mathfrak{a}) = N(x)/N(\mathfrak{a})$.

All these results are a particular case of the kernel associated to the module action (which shows that our module action generalize the usual ideal action).

If M is a module, an element $m \in M$ corresponds to a map $R \to M$, hence induces a morphism $m : M \cdot A \to A$. We say that the module module orientation $M \cdot A$ is effective when we can evaluate this map for every m. (This is a generalisation of the notion of orientation by a ring: if $r \in R$ we ask to be able to evaluate the map $r : R \cdot A = A \to A$). Equivalently, since we suppose our ring orientations are always effective, it suffices to be able to evaluate the map $M \cdot A \to A^n$ associated to $R^n \twoheadrightarrow M$ as in the proof of Theorem 3.7.

We recall Definition 4.3 for the definition of compatible isogenies, and Corollary 4.4 for an easy criterion.

Proposition 4.24. *Let $M_2 \hookrightarrow M_1$ be an isogeny, i.e. M_2 is a sublattice of M_1, i.e. it has the same rank as M_1, i.e. M_1/M_2 is of torsion. Let $A \in \mathfrak{Ab}_R$ compatible with this isogeny. By assumption, the corresponding morphism $\phi : M_1 \cdot A \to M_2 \cdot A$ is an isogeny. The kernel of this isogeny is given by $(M_1/M_2) \cdot A = (M_1 \cdot A)[M_2]$, the intersection of the kernels of all the morphisms $m : M_1 \cdot A \to A$, for $m \in M_2$, and conversely, if $m \in M_1$ is zero on this kernel, then m belongs in M_2.*

Proof. Taking generators $(m_1, \dots, m_{n_2})$ of M_2, we get a presentation $R^{m_2} \to R^{n_2} \to M_2 \to 0$. Now, looking at the diagram in Proposition 3.11, we have a map $M_2 \cdot A \to A^{n_2}$ given by the generators, and by functoriality the map $M_1 \cdot A \to A^{n_1} \to A^{n_2}$ given by the commutative diagram corresponds precisely to the map $R^{n_2} \to M_2 \to M_1$ (i.e. we see the m_i as elements of M_1, i.e. as morphisms $M_1 \cdot A \to A$).

Now the kernel of $M_1 \cdot A \to M_2 \cdot A$ is the kernel of $M_1 \cdot A \to A^{n_2}$, which is precisely the definition of $(M_1 \cdot A)[M_2]$.

Conversely, if $m : M_1 \cdot A \to A$ is zero on the kernel, then m descends to $M_2 \cdot A$, hence m belongs to M_2. □

From the module point of view, when $A = E_0$, we can restate Proposition 4.24 as follows: given the isogeny $\phi : A_1 \to A_2$, the map $M_2 = \mathrm{Hom}_R(A_2, E_0) \to M_1 = \mathrm{Hom}_R(A_1, E_0)$ is given by $\phi' \mapsto \phi' \circ \phi$. An element $m \in M_1$ belong to the image of M_2 through this map iff $m \cdot E_0 : A_1 \to E_0$ factors through A_2, i.e., is 0 on $\mathrm{Ker}\,\phi$.

Note that if $r \in R$, the morphism $r \cdot A : A \to A$ it induces is precisely the one given by the orientation. From Proposition 4.24, we get:

Corollary 4.25. *Let I be an ideal of R, it induces a $N(I)$-similitude $(I, H_R/N(I)) \to (R, H_R)$. Assume that this similitude is compatible with A (e.g. A is horizontal). Then the corresponding isogeny $A \to I \cdot A$ as for kernel $(R/I) \cdot A = A[I] = \{x \in A \mid \gamma(x) = 0 \quad \forall \gamma \in I\}$. In particular, we recover the usual ideal action, extended to abelian varieties.*

Example 4.26 (Double orientations)**.** Let $A \in \mathfrak{Ab}_R$, then A is already R-oriented. Assume that we have another orientation $S \subset \mathrm{End}_R(A)$, with S another quadratic order (different from R to avoid trivial cases). Since we assume that S gives R-oriented morphisms on A, we have that S and R commute in $\mathrm{End}(A)$: we say that A is doubly oriented by R and S. On A, we can look at the action of invertible ideals of R or ideals of S, furthermore, if $I \subset S$ is an ideal of S, then $A[I]$ is stable by R because R commutes with S, hence $A/A[I]$ is still doubly oriented.

More generally, due to the way the S-module action on A is computed, via kernels of matrix of elements of S acting on A, we see that $M \cdot A$ is still R-oriented for a S-module M (on top of being S-oriented), and similarly a S-isogeny $M_2 \to M_1$ gives both a S-oriented and a R-oriented isogeny $M_1 \cdot A \to M_2 \cdot A$. One can reformulate that by saying that we look at $R \otimes_{\mathbb{Z}} S$ orientations, and $M_R \otimes_{\mathbb{Z}} M_S$ module actions.

As an example, let $E_0/\mathbb{F}_p$ be a supersingular curve, which its natural orientation by the Frobenius, i.e. $R = \mathbb{Z}[\sqrt{-p}]$ (which we will assume is primitive) and take a S-orientation on $E_0'/\mathbb{F}_{p^2}$. Then $A = W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_0')$ is both R and S oriented, and we can act by $\mathrm{Pic}(R)$ and $\mathrm{Pic}(S)$ on it.

Corollary 4.27. *Let (A, λ_A) be a ppav in $\mathfrak{Ab}_R$, and $\psi : (M_2, H_2) \to (M_1, H_1)$ be a n-similitude compatible with A. If $M_1 \cdot A$ has its module orientation effective, n is smooth, and the n-torsion on $M_1 \cdot A$ is accessible, then we can effectively compute the n-isogeny $\phi : M_1 \cdot A \to M_2 \cdot A$.*

Proof. We know that the kernel of ϕ lives in $(M_1 \cdot A)[n]$ and by Proposition 4.24, it is given by the intersection of the kernels of the morphisms $m_i : M_1 \cdot A \to A$, for generators $m_1, \dots, m_u$ of $\psi(N) \subset M$. By assumption we can compute the m_i, and recover the kernels by some DLPs. Once we have the kernels, we can apply an isogeny algorithm to compute the isogeny. □

Corollary 4.28. *If (M, H_M) is unimodular of rank g, and we can find a n-similitude $(R^g, H_R^g) \to (M, H_M)$ compatible with a ppav (A, λ_A), with n smooth and the n-torsion on A accessible, then we can compute $(M, H_M) \cdot (A, \lambda_A)$ efficiently.*

Proof. By contragredience we have a n-similitude $(M, H_M) \to (R^g, H_R^g)$, and we certainly have an effective module orientation on $(R^g, H_R^g) \cdot (A, \lambda_A) = (A^g, \lambda_A^g)$ where λ_A^g is the product polarisation: to an element $m \in R^g$, given as a column of elements in R, the corresponding morphism $m : A^g \to A$ corresponds to the morphisms induced by the line vector m^T and the orientation on A. Hence we can apply Corollary 4.27. □

Remark 4.29 (Computing the action iteratively)**.**

- In the context of Proposition 4.24, assume that we have an efficient representation of the n-isogeny $\phi : M_1 \cdot A \to M_2 \cdot A$. To iterate the construction, we still need to descend the effective module orientation on $M_1 \cdot A$ to $M_2 \cdot A$. If $m \in M_2$, then $m : M_2 \cdot A \to A$ corresponds, by functoriality, when seen as $\psi(m) \in M_1$ to $M_1 \cdot A \to A$ given by $M_1 \cdot A \to M_2 \cdot A \to A$, which we know how to evaluate by assumption. So we know how to evaluate m on a point $P \in M_2 \cdot A$ as long as we can compute a preimage P' under ϕ. Since $\tilde{\phi}$ has an efficient representation, this solves the problem when P is of order prime to n.

  An alternative, if $m \in M_2$ fits into the image of a u-similitude $(R^g, H_R^g) \to (M_2, H_2)$, is to compute the corresponding u-isogeny isogeny $\psi' : M_2 \cdot A \to A^g$. Indeed, $\psi' \circ \psi$ is a nu-similitude $M_1 \cdot A \to A^g$, for which we have an efficient representation because we can evaluate it on points by our assumption on the effectiveness of the module orientation on $M_1 \cdot A$, and since we can also evaluate ψ on enough nice points, we have an efficient representation of ψ'. (Alternatively, we invoke the isogeny division algorithm, see [Rob24b], but this amount to the same thing). We can do similar tricks with a u-similitude $(R^{g+g'}, H_R^{g+g'}) \to (M_2 \times R^{g'}, H_2 \oplus H_R^{g'})$.

  Finally, we can also build a double path $A^g \to N \cdot A$ a la Clapotis (see Proposition 4.30), using Heuristic 2.13.
- Conversely, suppose that we have an explicit n-isogeny $\phi : M_1 \cdot A \to A'$, and we know that A' comes from a module action $A' = M_2 \cdot A$ (this is automatic by Theorem 4.9 if $A = E_0$ is a primitively oriented elliptic curve), and we want to recover M_2 as a submodule of M_1. Then we know that $nM_1 \subset M_2 \subset M_1$ is isotropic, and by Proposition 4.24 we can use the kernel of ϕ to test which elements of M_1 belong to M_2. This is efficient if n is smooth and the n-torsion accessible.

  If n is smooth but the n-torsion is not accessible, we can try to split ϕ into smaller isogenies, and recover M_2 iteratively, using the previous item to descend the effective module orientation on each intermediate codomain. This works well if we are sure that the intermediate isogenies correspond to a submodule action; this should be the case if the kernel of the big isogeny is of

rank g, because we then have a canonical filtration of the kernel (given by $K \cap (M_1 \cdot A)[n']$), hence of the submodule (given by $M_2 + n' M_1$).

4.5.2. *The Clapoti(s) approach.*

Proposition 4.30. *Suppose that we have a n_1 and a n_2 similitude, with n_1 coprime to n_2, between two unimodular Hermitian modules $(M_2, H_2) \to (M_1, H_1)$, and that we know $M \cdot A$ and its module action. Then the two corresponding isogenies $M_1 \cdot A \to M_2 \cdot A$ are efficiently computable.*

Proof. Taking the contragredient of the n_2-similitude, we have a $n_1 n_2$-similitude $\psi : (M_1, H_1) \to (M_1, H_1)$, which split as $M_1 \to M_2 \to M_1$, a n_2-similitude followed by a n_1-similitude, or as $M_1 \to M_2' \to M_1$, a n_1-similitude followed by a n_2-similitude. We have $M_2' = \psi(M_1) + n_2 M_1 \subset M_1$. Assume first that $n_1 + n_2$ is powersmooth. The Kani construction gives us a (n_1+n_2)-similitude $(M_2, H_2) \oplus (M_2', H_2') \to (M_1^2, H_1^2)$, which we can compute by Corollary 4.27, because the module orientation is effective on $M_1^2 \cdot A = (M_1 \cdot A)^2$, since it is on $M_1 \cdot A$. The corresponding (n_1+n_2)-isogeny $(M_1 \cdot A)^2 \to (M_2 \cdot A) \oplus (M_2' \cdot A)$ allows us to recover both $M_2 \cdot A$ and the two n_i-isogenies $(M_1 \cdot A) \to (M_2 \cdot A)$ (remember that a product polarisation allows to recover the individual abelian varieties, this is similar to the fact that a decomposition of an Hermitian module into an orthogonal sum of indecomposable modules is unique). For the general case, pad n_1, n_2 by u, v such that $un_1 + vn_2$ is powersmooth, replacing A by A^4 if necessary, as usual. □

Example 4.31. Given a unimodular Hermitian module (M, H_M), if we can find two n_1, n_2 similitudes $(R^g, H_R^g) \to (M, H_M)$ with $n_1 \wedge n_2 = 1$, then we obtain a $n_1 n_2$-endomorphism $A^g \to A^g$ (given by a matrix of elements in R), and splitting this endomorphism (see [Rob24b]) gives the n_1-isogeny $(A^g, \lambda_A^g) \to (M \cdot A, H_M \cdot \lambda_A)$.

4.5.3. *Acting on an isogeny.* In Sections 4.5.1 and 4.5.2, we have seen how to translate in practice an Hermitian n-similitude $M_2 \to M_1$ into an n-isogeny $M_1 \cdot A \to M_2 \cdot A$, provided that the M_1-module orientation on $M_1 \cdot A$ was effective. This gave a way to compute $M \cdot A$ by finding a nice similitude $M \to R^g$.

But given an Hermitian unimodular module M, and a n-isogeny $\phi : A_1 \to A_2$ between ppavs in $\mathfrak{Ab}_{E_0,R}$, we can also look at the action $M \cdot \phi : M \cdot A_1 \to M \cdot A_2$. We will assume that the module orientation on $M \cdot A_1$ is effective. We will provide two algorithms to construct $M \cdot \phi$, the first one can be used when n is smooth and the n-torsion is accessible, while the second one only assume that ϕ has an efficient representation (see [Rob24b]).

Combining both type of actions, we can act by a n-similitude on a m-isogeny.

Proposition 4.32. *Let $\phi : A_1 \to A_2$ be a n-isogeny between ppavs in $\mathfrak{Ab}_R$ with kernel K. Let M be a R-module compatible with ϕ. Then $\operatorname{Ker} M \cdot \phi : M \cdot A_1 \to M \cdot A_2$ is given by $\{x \in M \cdot A_1 \mid m(x) \in K \quad \forall m \in M : M \cdot A_1 \to A_1\}$. In particular, if M is unimodular and we know $M \cdot A_1$ and the module action of M on A_1, n is smooth and the n-torsion on $M \cdot A_1$ is accessible, we can compute the n-isogeny $M \cdot \phi$ efficiently via its kernel.*

Proof. Take a surjection $R^n \twoheadrightarrow M$ and consider the commutative diagram induced by functoriality:

$$\begin{array}{ccc} A_1^n & \xrightarrow{\operatorname{diag}(\phi)} & A_2^n \\ \uparrow & & \uparrow \\ M \cdot A_1 & \xrightarrow{M \cdot \phi} & M \cdot A_2 \end{array}$$

The commutativity shows that $\operatorname{Ker} M \cdot \phi = \{x \in M \cdot A_1 \mid m(x) \in K \quad \forall m \in M : M \cdot A_1 \to A_1\}$. □

Proposition 4.33. *With the notations of Proposition 4.32, assume that we have an efficient representation of $\phi : A_1 \to A_2$, and that we also know both $M \cdot A_1$ and $M \cdot A_2$ and the module action of M on them. Then we can recover an efficient representation of $M \cdot \phi$.*

Proof. Since we know an efficient representation of ϕ, we can evaluate $\phi(P)$ on points of ℓ-torsion in A_1 for small ℓ. By assumption, we can also evaluate the maps $M \cdot A_1 \hookrightarrow A_1^n$ and $M \cdot A_2 \hookrightarrow A_2^n$ from the proof of Proposition 4.32. The commutative diagram in this proof shows that we can recover the image of $M \cdot \phi$ on ℓ-torsion points in $M \cdot A_1$. This is enough to have an efficient representation of $M \cdot \phi$ by [Rob22a; Rob24b]. □

4.5.4. *Module kernels and kernel modules.* Let $A_1 = M_1 \cdot A$ be an M_1-oriented abelian variety. To a submodule $M_2 \subset M_1$, we can associate the (oriented) "module kernel" $A_1[M_2]$. Conversely, to a (oriented) kernel $K \subset A_1$, we can associate the kernel module $M(K) = \{m \in M_1 \mid m(K) = 0\}$. These two maps give a Galoisian adjunction, hence a bijection between kernel modules and module kernels (this is a special case of the fact that an adjunction gives an equivalence on the subcategories where the monad unit and comonad units respectively are isomorphisms).

Whenever the action by submodules is (well defined and) reflect isomorphisms, every submodule is a kernel module. This is the case for instance if $A \in \mathfrak{Ab}_{E_0,R}$.

Conversely, if a kernel $K \subset A_1$ is a module kernel $K = A_1[M_2]$, then $A_2 \coloneqq A_1/K = M_2 \cdot A$, is in the image of A by the module action (recall that we assume that we restrict to submodules that are compatible with A, so A_1/K is indeed equal to $M_2 \cdot A$ rather than just equal to its connected component). Conversely, if $A_2 \coloneqq A_1/K$ is given by a (torsion free) module action $A_2 = M' \cdot A$, and the module action on A is full, then the morphism $A_1 \to A_2$ comes from a morphism $i : M' \to M_1$, which has to be a monomorphism (since both modules are torsion free of rank g, if the map was not a monomorphism the cokernel would be of codimension > 0, contradicting the fact that K is finite), and so K is the module kernel associate to $M_2 = i(M') \subset M_1$.

5. Supersingular elliptic curves and the module action

In Section 5.4, section we study the link between the supersingular isogeny path problem and specific instances of rank 2 module action inversion. This relationship goes through the Weil restriction, which we study from the module point of view in Section 5.2.

5.1. **The supersingular equivalence of category.**

Theorem 5.1. *Let E_0 be a maximal supersingular curve E_0 with endomorphism ring $\mathfrak{O}_0$. Then the functor the functor $A \mapsto \mathrm{Hom}_{\mathbb{F}_{p^2}}(A, E_0)$ is an antiequivalence between the category of maximal supersingular abelian varieties over $\mathbb{F}_{p^2}$ and f.p. torsion free left $\mathfrak{O}_0$-modules, the inverse functor being given by the power object construction $M \to \mathcal{HOM}_{\mathfrak{O}_0}(M, E_0)$.*

A principal polarisation on $A = M \cdot E_0$ is represented by an $\mathfrak{O}_0$-integral unimodular positive definite Hermitian form H_M on M. (The sesquilinear condition on H_M is $H_M(\alpha x, y) = \alpha H_M(x, y)$, $H_M(x, \alpha y) = H_M(x, y)\overline{\alpha}$).

Proof. The first statement comes from [JKP+18], and the second follows by the same arguments as in Section 4. □

In particular, if $M = \mathrm{Hom}_{\mathbb{F}_{p^2}}(E, E_0)$, this left $\mathfrak{O}_0$-module has a canonical unimodular polarisation H_M given by $H_M(\phi_1, \phi_2) = \phi_1\tilde{\phi_2} \in \mathcal{O}_0$. Now if $\phi : E_0 \to E$ is an isogeny, we have an isomorphism $M \to I \subset \mathfrak{O}_0, m \mapsto m \circ \phi$. Since $\deg \phi = N(I)$, the reduced norm of I, we see that the polarisation on I becomes $H_I(x, y) = x\overline{y}/N(I)$.

Like in the oriented case, even in rank 1 we will prefer working with modules rather than ideal, for the same reasons as in Example 4.22. Indeed, going from the module to ideal point of view require a choice of monomorphism $M \hookrightarrow \mathfrak{O}_0$, which correspond to a choice of isogeny $E_0 \to E$.

Proposition 5.2. *Let E_0 be as above, and suppose that E_0 admits a primitive orientation by a quadratic imaginary ring R. Let M be a R-module, $\mathfrak{O}_0 \otimes_R M$ is then a $(\mathfrak{O}_0, R)$-bimodule, and $\mathcal{HOM}_R(M, E_0) \simeq \mathcal{HOM}_{\mathfrak{O}_0}(\mathfrak{O}_0 \otimes_R M, E_0)$ (where the isomorphism forgets the R orientation on $\mathcal{HOM}_R(M, E_0)$).*

Proof. This is a special case of Proposition 3.9. □

Remark 5.3 (Supersingular morphisms vs oriented morphisms)**.** From the module point of view, we can reframe Proposition 5.2 as follows. By the antiequivalence of category of Theorem 5.1, if $A = M_{\mathfrak{O}} E_0$ is a maximal supersingular abelian variety, an R-orientation on A corresponds to an R-orientation on $M_{\mathfrak{O}}$, i.e. an inclusion $R \to \mathrm{End}_{\mathfrak{O}_0}(M_{\mathfrak{O}})$. Since $M_{\mathfrak{O}}$ is a $(\mathfrak{O}_0, \mathrm{End}_{\mathfrak{O}_0}(M_{\mathfrak{O}})^{op})$-bimodule, this amount to a choice of $(\mathfrak{O}_0, R)$-bimodule *structure* on the $\mathfrak{O}_0$-left module M. Oriented morphisms are the morphisms of left $\mathfrak{O}_0$-module that also commute with the right R-action (we call these the elements that commute with the orientation).

By the equivalence of categories, we also have $A = M \cdot E_0$ for a R-module M, where $M = \mathrm{Hom}_R(M \cdot E_0, E_0)$ if M is an R-module, and likewise $M_{\mathfrak{O}} = \mathrm{Hom}_{\mathbb{F}_{p^2}}(M \cdot E_0, E_0)$ if $M_{\mathfrak{O}}$ is an $\mathfrak{O}_0$-module. Hence, if $A = M \cdot E_0$, Proposition 5.2 gives the following relationship between $M_{\mathfrak{O}} = \mathrm{Hom}_{\mathbb{F}_{p^2}}(A, E_0)$ and $M = \mathrm{Hom}_R(A, E_0)$:

- $M_{\mathfrak{O}} = \mathfrak{O}_0 \otimes_R M$
- Conversely, since by definition $\mathrm{Hom}_R(A, B)$ is the submodule of $\mathrm{Hom}(A, B)$ that commutes with the orientation, M is the R-submodule of $M_{\mathfrak{O}}$ that commutes with the R-orientation on A and E_0. (Which, if $R = \mathbb{Z}[\alpha]$, we represent on the module side as endomorphisms $i(\alpha)$ on $M_{\mathfrak{O}}$ and $\mathfrak{O}_0$ respectively).

A morphism ϕ in $\mathrm{Hom}_{\mathbb{F}_{p^2}}(A, E_0)$ does not necessarily preserve the R-orientation (it does iff it is in the submodule $M \subset M_{\mathfrak{O}}$). By the module interpretation of orientation above, we can reformulate these relationship as follows: if (the torsion free) $M_{\mathfrak{O}}$ has a $(\mathfrak{O}_0, R)$-bimodule structure, and M is the submodule of elements that commute with the R-orientation, then $M_{\mathfrak{O}} \simeq \mathfrak{O}_0 \otimes_R M$.

We make two remarks here. The first is that the equality $M_{\mathfrak{O}} = \mathfrak{O}_0 \otimes_R M$ on the Hom modules could also have been obtained without the full power of the equivalence of category. One just need to know that the Hom modules are unimodular with respect to their canonical associated polarisations. Then we have a map $\mathfrak{O}_0 \otimes_R M \to \mathrm{Hom}_{\mathbb{F}_{p^2}}(A, E_0)$ obtained by composing an oriented morphisms with an arbitrary endomorphism of E_0. This map is a monomorphism because the modules are torsion free. But the quadratic forms on $\mathrm{Hom}_{\mathbb{F}_{p^2}}(A, E_0)$ and on its submodule $M = \mathrm{Hom}_R(A, E_0)$ are the same by construction (to $\phi : A \to E_0$ we associate $\phi \circ \tilde{\phi}$, seen as an element in $\mathbb{Z}$). By Example 2.11, the inclusion has to be a bijection.

The second remark is as follows. Assume that $E = \mathfrak{a} \cdot E_0$ for an R-ideal $\mathfrak{a}$, and that we know both $\mathfrak{O}_0 = \mathrm{End}(E_0)$, $\mathfrak{O} = \mathrm{End}(E)$ and their R-orientation. Then we can easily construct the supersingular module $M_{\mathfrak{O}} = \mathrm{Hom}_{\mathbb{F}_{p^2}}(E, E_0)$ (say as the connecting ideal between $\mathfrak{O}$ and $\mathfrak{O}_0$). This is an $(\mathfrak{O}_0, \mathfrak{O})$-bimodule, and so inherit a $(\mathfrak{O}_0, R)$-bimodule from the orientation on $\mathfrak{O}$. Thus we recover the isomorphism class of $\mathfrak{a}$ as a R-module as the submodule of elements m such that the right action of $r \in R$ on m coincide with its left action (via $R \subset \mathfrak{O}_0$) for all $r \in R$.

We see how the module point of view both simplify and generalizes some of the arguments in [CPV20; Wes22a; EL24, § 4.1].

5.2. **Weil's restriction from the module point of view.** Recall that the Weil restriction $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$ of an elliptic curve is defined functorially by $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)(T) = E(T \otimes_{\mathbb{F}_p} \mathbb{F}_{p^2})$ for a $\mathbb{F}_p$-algebra T (or even an scheme $T/\operatorname{Spec} \mathbb{F}_p$). The Weil restriction $W_{k'/k}(A)$ of an abelian variety A over a separable extension k'/k of degree n exist (and is of dimension ng if A is of dimension g). It is functorial, hence the Weil restriction of a ppav also has a principal polarisation, and the Weil restriction of a n-isogeny is a n-isogeny (because the Weil restriction behaves as expected on duals, polarisations, and the Weil restriction of $[n]$ is $[n]$).

In our case, $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$ is defined as the descent of the abelian surface $E \times E^\sigma$ from $\mathbb{F}_{p^2}$ to $\mathbb{F}_p$ (here we denote by σ the Galois action of the small Frobenius π_p), under the Galois action $(P_1, P_2) \mapsto (\sigma(P_2), \sigma(P_1))$. In particular, if $E/\mathbb{F}_p$ is an elliptic curve defined over $\mathbb{F}_p$, then $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)/\mathbb{F}_p$ is a twist of $E^2/\mathbb{F}_p$: it becomes isomorphic to it only over $\mathbb{F}_{p^2}$ in general. From the definition above, we see that it is the twist which corresponds to the cocycle that sends σ to the permutation automorphism $(P, Q) \mapsto (Q, P)$.

In particular, on $E^2(\mathbb{F}_{p^2})$, while the standard Frobenius from $E^2/\mathbb{F}_p$ is $(P,Q)\mapsto(\sigma(P),\sigma(Q))$, the one induced by $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)/\mathbb{F}_p$ is $(P,Q)\mapsto(\sigma(Q),\sigma(P))$.

If $E/\mathbb{F}_p$ is supersingular, it has $(p+1)$ points over $\mathbb{F}_p$, so $E^2(\mathbb{F}_p)$ has $(p+1)^2$ points, while $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)(\mathbb{F}_p)\simeq E(\mathbb{F}_{p^2})$ also has $(p+1)^2$ points. In particular, $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$ is isogeneous to E_0^2, and $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$ belongs to our category $\mathfrak{Ab}_{E_0,R}$, so is of the form $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)=(M,H_M)\cdot E_0$. More generally, if $A/\mathbb{F}_{p^2}$ is a maximal supersingular abelian variety of dimension g, the Frobenius endomorphism on $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(A)/\mathbb{F}_p$ satisfy $\pi^2=-p$, hence $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(A)$ is standard supersingular, so is isogeneous to E_0^{2g}.

Remark 5.4 (The Galois action of the Frobenius)**.** If $A/\mathbb{F}_{p^2}$ is an abelian variety, we call σ the associated Galois action by the small Frobenius π_p, it sends a point $P\in A$ to a point P^σ on A^σ. One needs to be careful that although σ is actually an isogeny $\sigma=\pi_A$ (that acts on coordinates by raising them to the power p), its inverse σ^{-1} is not (because it involves p-th roots so is not algebraic). Only $[p]\sigma^{-1}$ is an isogeny, given by the Verschiebung. By abuse of notation, we may denote σ^{-1} by π_A^{-1}. We also have a map $\mathrm{Hom}_{\mathbb{F}_{p^2}}(A_1,A_2)\to\mathrm{Hom}_{\mathbb{F}_{p^2}}(A_1^\sigma,A_2^\sigma)$ given by conjugation $\psi\mapsto\sigma\circ\psi\circ\sigma^{-1}$.

Theorem 5.5. *Let $E_0/\mathbb{F}_p$ be primitively oriented by $R=\mathbb{Z}[\sqrt{-p}]$. Let $(M_\mathfrak{O},H_\mathfrak{O})=\mathrm{Hom}_{\mathbb{F}_{p^2}}(E,E_0)$, and $(M_R,H_R)=\mathrm{Hom}_{\mathbb{F}_p}(W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E),E_0)$, so that $E=(M_\mathfrak{O},H_\mathfrak{O})\cdot E_0$ and $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)=(M_R,H_R)\cdot E_0$ by the antiequivalence of categories. Then $\mathfrak{O}_0\otimes_R(M_R,H_R)=(M_\mathfrak{O},H_\mathfrak{O})\oplus(M_\mathfrak{O}^\sigma,H_\mathfrak{O}^\sigma)$, where $M_\mathfrak{O}^\sigma$ is the given by the Galois conjugation by σ, i.e. $M_\mathfrak{O}^\sigma=\pi_{E_0}M_\mathfrak{O}\pi_E^{-1}$.*

So from M_R we recover $M_\mathfrak{O}$ by unicity of the orthogonal decomposition (it is crucial to have the polarisation H_R here), and conversely given $M_\mathfrak{O}$ we can recover M_R as the set of elements of $M_\mathfrak{O}\oplus M_\mathfrak{O}^\sigma$ commuting with the following Galois action: $\sigma\cdot(\alpha,\beta)=(\beta^\sigma,\alpha^\sigma)$, and H_R as the descent of $H_\mathfrak{O}\oplus H_\mathfrak{O}^\sigma$.

This unimodular module (M_R,H_R) is isomorphic to $(M_\mathfrak{O},H'_\mathfrak{O})$ where $H'_\mathfrak{O}(x,y)=H_\mathfrak{O}(x,y)+\pi H_\mathfrak{O}(x,y)\pi^{-1}\in R$, and $\pi=\pi_{E_0}\in\mathfrak{O}_0$.

Proof. We have $M_R=\mathrm{Hom}_{\mathbb{F}_p}(W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E),E_0)$, $M_\mathfrak{O}=\mathrm{Hom}_{\mathbb{F}_{p^2}}(E,E_0)$, and $\mathfrak{O}_0\otimes_R M_R=\mathrm{Hom}_{\mathbb{F}_{p^2}}(W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E),E_0)$ by Proposition 5.2.

By Galois, $\mathrm{Hom}_{\mathbb{F}_p}(W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E),E_0)$ is the submodule of $\mathrm{Hom}_{\mathbb{F}_{p^2}}(W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E),E_0)$ commuting with the Frobenius action. But over $\mathbb{F}_{p^2}$, $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)=E\times E^\sigma$, so $\mathfrak{O}_0\otimes_R M_R=\mathrm{Hom}_{\mathbb{F}_{p^2}}(W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E),E_0)=\mathrm{Hom}_{\mathbb{F}_{p^2}}(E,E_0)\oplus\mathrm{Hom}_{\mathbb{F}_{p^2}}(E^\sigma E_0)\simeq\mathrm{Hom}_{\mathbb{F}_{p^2}}(E,E_0)\oplus\mathrm{Hom}_{\mathbb{F}_{p^2}}(E^\sigma E_0^\sigma)=M_\mathfrak{O}\oplus M_\mathfrak{O}^\sigma$ (this is an orthogonal direct sum).

This allows to find $M_\mathfrak{O}$ from M_R by linear algebra. Conversely, from $M_\mathfrak{O}$, we can find M_R as the elements of $\mathrm{Hom}_{\mathbb{F}_{p^2}}(W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E),E_0)$ that commute with the Galois action. On the left, σ acts by multiplication by π_{E_0}. On the other hand on the right, because of the way $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$ is descended from $E\times E^\sigma$, the Galois action on $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$ is given by $\sigma\cdot(\alpha,\beta)=(\beta\pi_E^{-1},\alpha\pi_E^{-1})$ under the identification $\mathrm{Hom}_{\mathbb{F}_{p^2}}(W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E),E_0)=\mathrm{Hom}_{\mathbb{F}_{p^2}}(E,E_0)\oplus\mathrm{Hom}_{\mathbb{F}_{p^2}}(E^\sigma E_0)$. It follows that (α,β) is invariant under conjugation by σ iff $\beta=\pi_{E_0}\alpha\pi_E^{-1}$).

So $\alpha\mapsto(\alpha,\pi_{E_0}\alpha\pi_E^{-1})$ gives an isomorphism $M_\mathfrak{O}\simeq M_R$ (where we consider $M_\mathfrak{O}$ as an R-module). The polarisation is given by $H'_\mathfrak{O}(\alpha_1,\alpha_2)=H_\mathfrak{O}(\alpha_1,\alpha_2)+H_\mathfrak{O}^\sigma(\pi_{E_0}\alpha_1\pi_E^{-1},\pi_{E_0}\alpha_2\pi_E^{-1})=\alpha_1\tilde{\alpha_2}+\pi_{E_0}\alpha_1\pi_E^{-1}\pi_{E_0}\tilde{\alpha_2}\pi_E^{-1}=\alpha_1\tilde{\alpha_2}+\pi_{E_0}\alpha_1\tilde{\alpha_2}\pi_{E_0}^{-1}$. □

Remark 5.6 (Quadratic forms)**.** When juggling with polarisations between $\mathfrak{O}_0$-modules and R-modules, it is convenient to work with the associated quadratic form $q_H(x)=H(x,x)$. Indeed, $q_H(x+\alpha y)=q_H(x)+\alpha\overline{\alpha}q_H(y)+H(x,y)\overline{\alpha}+\alpha\overline{H(x,y)}$, so we can recover H from q_H by linear algebra, using $\alpha=1$ and then α any non integer.

From this point of view, Theorem 5.5 shows that from the module point of view, the Weil restriction is simply the forgetting morphism $M_\mathfrak{O}\mid R$, with associated quadratic form $q'=2q_{M_\mathfrak{O}}$ (this factor 2 is important to go from a unimodular $\mathfrak{O}_0$ module to a unimodular R-module, because $\Delta_R=-4p$ while $\Delta_{\mathfrak{O}_0}=-p$).

Remark 5.7 (The weil restriction of a maximal supersingular abelian variety)**.** The exact same argument as in Theorem 5.5 work for a general maximal supersingular abelian variety $A/\mathbb{F}_{p^2}$: if $(M_{\mathfrak{O}}, H_{\mathfrak{O}}) = \mathrm{Hom}_{\mathbb{F}_{p^2}}(A, E_0)$, and $(M_R, H_R) = \mathrm{Hom}_{\mathbb{F}_p}(W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(A), E_0)$, then $\mathfrak{O}_0 \otimes_R (M_R, H_R) = (M_{\mathfrak{O}}, H_{\mathfrak{O}}) \oplus (M_{\mathfrak{O}}^\sigma, H_{\mathfrak{O}}^\sigma)$. So $(M_{\mathfrak{O}})$ can be recovered from M_R (at least if A is simple), and conversely M_R is the appropriate descent of $M_{\mathfrak{O}} \oplus M_{\mathfrak{O}}^\sigma$ by the Galois action.

Remark 5.8 (The dimension 2 supersingular graph over $\mathbb{F}_p$)**.** As in Theorem 5.5, for E_1, E_2 supersingular over $\mathbb{F}_{p^2}$, we have $\mathrm{Hom}_{\mathbb{F}_p}(W_{\mathbb{F}_{p^2}/\mathbb{F}_p}E_1, W_{\mathbb{F}_{p^2}/\mathbb{F}_p}E_2) = \mathrm{Hom}_{\mathbb{F}_{p^2}}(W_{\mathbb{F}_{p^2}/\mathbb{F}_p}E_1 \times_{\mathbb{F}_p} \mathbb{F}_{p^2}, E_2) = \mathrm{Hom}_{\mathbb{F}_{p^2}}(E_1 \times E_1^\sigma, E_2) = \mathrm{Hom}_{\mathbb{F}_{p^2}}(E_1, E_2) \oplus \mathrm{Hom}_{\mathbb{F}_{p^2}}(E_1^\sigma, E_2)$.

So the $\mathbb{F}_p$-isogeny graph in dimension 2 contains, via the Weil restriction, the supersingular $\mathbb{F}_{p^2}$-isogeny graph in dimension 1, modulo the identifications of E with E^σ.

Remark 5.9 (Other descents)**.** Assume that E is defined over $\mathbb{F}_p$. Then $E \times E^\sigma/\mathbb{F}_{p^2}$ has for descent $E \times E$ over $\mathbb{F}_p$; this is a twist of $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$. Let $M'_R = \mathrm{Hom}_{\mathbb{F}_p}(E^2, E_0) = I_E^2$ where $I_E = \mathrm{Hom}_{\mathbb{F}_p}(E, E_0)$. This is an R-module which is not isomorphic with $M_R = \mathrm{Hom}_{\mathbb{F}_p}(W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E), E_0)$ in general. But since both abelian surfaces give $E \times E^\sigma$ over $\mathbb{F}_{p^2}$, we have that $M_{\mathfrak{O}} = \mathfrak{O}_0 \otimes_R M'_R$ too: $M_{\mathfrak{O}}$ can have different non isomorphic descent to a R-module. Here it is important to keep track of the Galois action on $M_{\mathfrak{O}} \oplus M_{\mathfrak{O}}^\sigma$ to compute the correct descent.

In our case, σ acts by π_{E_0} on the left and by π_E (diagonally) on the right. The invariant elements of $M_{\mathfrak{O}} \oplus M_{\mathfrak{O}}^\sigma$ are precisely given by $I_E \oplus I_E^\sigma \simeq I_E^2$ as expected.

Remark 5.10 (Twists from the module point of view)**.** As illustrated by Remark 5.9, the Galois action is important to get the correct module descent corresponding on different $\mathbb{F}_p$-forms of a supersingular abelian variety $A/\mathbb{F}_{p^2}$.

Let $G = \mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p) = \langle\sigma\rangle \simeq \mathbb{Z}/2\mathbb{Z}$. As explained by Milne in [Mil72, § 2], we can consider actions by $R[G]$-modules to build twists, and $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(A)$ is precisely given by the action $R[G] \cdot A$.

We could probably extend the R-module action to a Galoisian module action (i.e. acting by $R[G]$-modules), by looking at the category of abelian varieties over $\mathbb{F}_{p^2}$ with a descent datum. If $A/\mathbb{F}_p$ is an R-oriented abelian variety, which we see as an abelian variety A over $\mathbb{F}_{p^2}$ along with its associated descent data ξ to $\mathbb{F}_p$, then if χ is the non trivial quadratic character on G, and R_χ the free rank 1 R-module where G acts by χ (i.e. $\sigma(r) = \overline{r}$), we would have $R_\chi \cdot A = (A, -\xi) = A^t$ (by abuse of notation where we represent the descent data via the descended abelian variety). Then we would have $I \otimes_{R[G]} R_\chi \cdot A = I \cdot (A, -\xi) = \overline{I} \cdot A^t = R_\chi \otimes_{R[G]} I \cdot A = R_\chi \cdot (I \cdot A) = (I \cdot A)^t$ which extends [CPV20, Lemma 5].

We leave these investigations for future work, because we won't need it with our choices of parameters for MIKE.

5.3. Scholten's construction from the module point of view.

Lemma 5.11. *Let $E_0/\mathbb{F}_p$ be a supersingular curve with primitive Frobenius orientation, and let $A = M \cdot E_0$. Then M is projective iff $A[2](\mathbb{F}_p) \simeq (\mathbb{Z}/2\mathbb{Z})^g$.*

Proof. Let us assume first that $p \equiv 3 \mod 4$, so that $R = \mathbb{Z}[\sqrt{-p}]$ is not maximal. It has conductor 2, let O_R be its maximal order.

Let $M = \oplus \mathfrak{a}_i$, then $A[2]$ is isomorphic as a R-module to $M/2M$. If $O(\mathfrak{a}) = R$, then $\mathfrak{a}/2\mathfrak{a} \simeq R/2R$, and $\mathrm{Ker}\,\pi - 1 \simeq \mathbb{Z}/2\mathbb{Z}$ on $\mathfrak{a} \cdot E_0$, while if $O(\mathfrak{a}) = S$, then $\mathfrak{a}/2\mathfrak{a} \simeq S/2S$, and $\mathrm{Ker}\,\pi - 1 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ on $\mathfrak{a} \cdot E_0$. So we can read of from the Galois structure of $A[2]$ if M is projective over R or not. More precisely, M is a direct sum of g modules $\mathfrak{a}_i$, and each $\mathfrak{a}_i$ is invertible either in R or in O_R. Let m be the number of modules invertible in R. Then $A[2](\mathbb{F}_p) \simeq (\mathbb{Z}/2\mathbb{Z})^m \times (\mathbb{Z}/2\mathbb{Z})^{2(g-m)}$.

If $p \equiv 1 \mod 4$, $R = O_R$, and in this case M is automatically projective, and $A[2](\mathbb{F}_p)$ always equal to $(\mathbb{Z}/2\mathbb{Z})^g$. □

If $p \equiv 3 \mod R$, the proof shows that the R orientation of $A = M \cdot E_0$ extend to an O_R-orientation iff $A[2] = (\mathbb{Z}/2\mathbb{Z})^{2g}$. This can be checked directly: the R orientation extend to an O_R-orientation iff

$(1+\pi)/2$ is well defined on A, iff $1+\pi = 0$ on $A[2]$. But this is equivalent to $\pi = 1$ on $A[2]$, i.e. all the 2-torsion is rational.

If $E_0' = \mathfrak{f}E_0$, then a standard supersinguliar abelian variety over $\mathbb{F}_p$ is horizontal to $E_0^m \times {E_0'}^{g-m}$, the varieties with $m = g$ being at the bottom, and the ones with $m = 0$ at the top. One can change level through cyclic isogenies of degree 2, and go from the bottom to the top by applying the action of $\mathfrak{f}$.

Corollary 5.12. *The Weil restriction $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(A)$ of a maximal supersingular abelian variety $A/\mathbb{F}_{p^2}$ is given by a projective module action: $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(A) = M \cdot E_0$, with M a projective R-module.*

Proof. We have $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(A)[2](\mathbb{F}_p) = A[2](\mathbb{F}_{p^2}) = (\mathbb{Z}/2\mathbb{Z})^g$, so we can apply Lemma 5.11. □

It is quite hard to work with Weil restrictions: over $\mathbb{F}_p$ they are not Jacobians nor product of elliptic curves in general, and since their 2-torsion is not fully rational by Corollary 5.12, their level 2 theta constants are not defined over $\mathbb{F}_p$. The best thing is probably to work on $E \times E^\sigma$ over $\mathbb{F}_{p^2}$ and keep track of the descent data, but this involves doing arithmetic over $\mathbb{F}_{p^2}$ rather than $\mathbb{F}_p$.

Fortunately, if $p \equiv 3 \mod 4$, Scholten's construction [Sch03] solves these problems. This construction was used in cryptography in [Cos18; CR24]. In this section, we reinterpret that construction from the module point of view.

In [CR24], the authors reinterpret Scholten's construction as a gluing on the 2-torsion of $E \times E^\sigma$. Although it is not stated explicitly in that paper, that gluing is given by the kernel $K = \{(T, \sigma(T)) \subset E \times E^\sigma, \quad \forall T \in E[2]\}$. Indeed, the points in that kernel are rational for the Frobenius induced by the Weil restriction: $\sigma_{\mathrm{WEIL}(E)}(T, \sigma(T)) = (\sigma^2(T), \sigma(T)) = (T, \sigma(T))$, so in particular the kernel K itself descends to a rational kernel on $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$. Scholten's construction is then $W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E) := W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)/K$.

Proposition 5.13. *Let $p \equiv 3 \mod 4$, $R = \mathbb{Z}[\sqrt{-p}]$, O_R be its maximal order, and $\mathfrak{f}$ the conductor ideal (this is on O_R-ideal of norm 2). Let E_0 be primitively oriented by R, and $E_0' = \mathfrak{f} \cdot E_0$ the curve above E_0 in the 2-isogeny volcano.*

Let $E/\mathbb{F}_{p^2}$ be a maximal supersingular curve. Then Scholten's construction is given by $\mathfrak{f} \cdot W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$.

Proof. We have $\mathfrak{f} = (2, 1+\pi)$, and $\mathfrak{f} \cdot W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$ is given by the codomain of the isogeny with kernel $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)[\mathfrak{f}] = W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)[1+\pi]$. But on $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$ seen as $E \times E^\sigma$ over $\mathbb{F}_{p^2}$, π acts by $\pi(P, Q) = (\pi(Q), \pi(P))$, and so this kernel is precisely the kernel $\{(T, \sigma(T)\}$ of Scholten's gluing isogeny. □

Remark 5.14. If $p \equiv 1 \mod 4$, the action by the ideal $\mathfrak{f} = (2, 1+\pi)$ on $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$ still gives Scholten's construction $W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$, by the same proof as in Proposition 5.13. But this time R is already maximal, so $\mathfrak{f}$ is invertible rather than a conductor ideal, and the resulting isogeny is an horizontal one rather than an ascending isogeny. In particular, the action does not change the Galois properties of the 2-torsion, so is less interesting in that case for our purposes.

More generally, we define Scholten's construction on a maximal supersingular $A/\mathbb{F}_{p^2}$ as $W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(A) = \mathfrak{f} \cdot W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(A)$. By Corollary 5.12, $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(A) = M \cdot E_0$ with M a projective module, so the action of $\mathfrak{f}$ on A is well defined, and we have $W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(A) = \mathfrak{f} \cdot M \cdot E_0 = M \cdot E_0' = (M \otimes_R O_R) \cdot_{O_R} E_0'$ by Remark 4.23.

One important consequence of Proposition 5.13 is that the Scholten construction $W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}$ is functorial (as composition of two functors), in particular it sends n-isogenies to n-isogenies.

In particular:

Lemma 5.15. *Assume that $p \equiv 3 \mod 4$. Scholten's construction $W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(A)$ is naturally O_R-oriented, so is O_R-isogeneous to E_0', and in particular it has its full 2-torsion rational, and it even has a rational level 2 theta null point rational if $p \equiv 7 \mod 8$.*

Proof. By the above discussion, $W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(A)$ comes from an O_R-module action from E_0', so it is naturally O_R oriented and has its 2-torsion fully rational (see the discussion after the proof of Lemma 5.11).

It remains to check that it has a rational level 2 theta null point. If 2 splits in O_R (so $p \equiv 7 \mod 8$), the decomposition $(2) = \mathfrak{p}_2\overline{\mathfrak{p}}_2$ gives a symplectic decomposition $B[4] = B[\mathfrak{p}_2^2] \oplus B[\overline{\mathfrak{p}}_2^2]$ for any O_R-oriented abelian variety, so in particular for $W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(A)$.

This is sufficient for $W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(A)$ to have a rational theta null point (and likewise for E'_0). □

Remark 5.16 (The case $p \equiv 3 \mod 8$)**.** Whenever $p \equiv 3 \mod 4$, then E'_0 has a rational twisted theta null point (the twisted theta model is equal to the squared theta model up to the Hadamard transform, and is birationally equivalent over the base field to the Montgomery model with full rational two torsion when $g = 1$). Since there is always an isogeny of odd degree between E'_0 and another supersingular curve E, then there is also one between $W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E'_0)$ and $W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$ by functoriality. But $W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E'_0) = (E'_0) \times (E'_0)^t$ as we will see in Proposition 5.18 has rational twisted theta null point, and the odd degree isogeny preserve the Galois property on the 4-torsion, so $W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$ also have a rational twisted theta null point.

Lemma 5.15 was our motivation to work with Scholten's construction rather than the Weil restriction directly for ⊗-MIKE: we will be able to work with rational theta null points over $\mathbb{F}_p$.

We can nom combine Theorem 5.5 with Remark 4.23 to go from ideals to modules for Scholten's construction:

Proposition 5.17. *With the notations above, let $\mathfrak{O}_0 = \mathrm{End}(E_0)$, $\mathfrak{O}'_0 = \mathrm{End}(E'_0)$, $A/\mathbb{F}_{p^2}$ be a maximal supersingular abelian variety, and $(M_{\mathfrak{O}'}, H_{\mathfrak{O}'}) = \mathrm{Hom}_{\mathbb{F}_{p^2}}(A, E'_0)$. Then $W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(A) = (M_{\mathfrak{O}'}, H'_{\mathfrak{O}'}) \cdot_{O_R} E'_0$, with $M_{\mathfrak{O}'}$ seen as a O_R-module, and $H'_{\mathfrak{O}}$ the Hermitian O_R form on $M_{\mathfrak{O}'}$ having the same quadratic form as the one given by $H_{\mathfrak{O}'}$.*

In other words, while the Weil restriction corresponded to forgetting the $\mathfrak{O}_0$ structure on I when $A = I \cdot E_0$ (only keeping the R-structure), Scholten's construction corresponds to forgetting the $\mathfrak{O}'_0$ structure on I' when $A = I' \cdot E'_0$ (only keeping the O_R structure).

Proof. We have $E'_0 = \mathfrak{f} \cdot_R E_0$, so by Proposition 3.9, $E'_0 = (\mathfrak{O}_0 \otimes_R \mathfrak{f}) \cdot_{\mathfrak{O}_0} E_0$, hence $\mathrm{Hom}_{\mathbb{F}_{p^2}}(E'_0, E_0) = \mathfrak{O}_0 \otimes_R \mathfrak{f}$.

Let $I_0 = \mathfrak{O}_0 \otimes_R \mathfrak{f}$ to simplify the notations, this is a left $\mathfrak{O}_0$-module. We have $\mathfrak{O}'_0 = \mathrm{Hom}_{\mathfrak{O}_0}(I_0, I_0) = I_0^\vee \otimes_{\mathfrak{O}_0} I_0$, and I_0 is a right $\mathfrak{O}'_0$-module. For our I_0, $\mathfrak{O}'_0 = \mathfrak{f} \otimes_R \mathfrak{O}_0 \otimes_R \mathfrak{f}$ as a O_R-module because $\mathfrak{f}$ is self dual.

Likewise, if $M_{\mathfrak{O}} = \mathrm{Hom}_{\mathbb{F}_{p^2}}(A, E_0)$, we have $M_{\mathfrak{O}'} = \mathrm{Hom}_{\mathbb{F}'_{p^2}}(A, E'_0) = I_0^\vee \otimes_{\mathfrak{O}_0} M_{\mathfrak{O}}$.

Now by Theorem 5.5, $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(A) = M \cdot_R E_0$, with $M = M_{\mathfrak{O}}$ seen as a R-module. So by Proposition 5.13, $W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(A) = \mathfrak{f} \cdot W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(A) = M' \cdot E_0$ with $M' = \mathfrak{f} \otimes_R M$. We thus have $W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(A) = M \otimes_R \mathfrak{f} \cdot E_0 = M \cdot E'_0 = (M \otimes_R \mathfrak{f}) \cdot_{O_R} E'_0$, where the last equality comes by Remark 4.23. In other words, $W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(A) = M' \cdot_{O_R} E'_0$.

But as a O_R-module, we also have $M_{\mathfrak{O}'} = \mathfrak{f} \otimes_R \mathfrak{O}_0 \otimes_{\mathfrak{O}_0} M_{\mathfrak{O}} = \mathfrak{f} \otimes_R M_{\mathfrak{O}} = M'$.

Now, for the polarisation, since E_0 and E'_0 are linked by a 2-isogeny, the $\mathfrak{O}$-Hermitian form on $M_{\mathfrak{O}'}$ and $M_{\mathfrak{O}}$ and the R-Hermitian form on M' and M differ by a factor 2 (via the appropriate pullback). But the quadratic form on M is twice the quadratic form on $M_{\mathfrak{O}}$ by Theorem 5.5, on the other hand the quadratic form on M' seen as a S-module is half the quadratic form on M' seen as a R-module by the discussion in Remark 4.23. This means that the pullback of it on M is equal to H_M, whose quadratic form is twice the one induced by $H_{M_{\mathfrak{O}}}$ so corresponds to the pullback of $M_{\mathfrak{O}'}$. In other words, the quadratic form induced on M' is precisely the one from $M_{\mathfrak{O}'}$. □

We finish this section by a discussion on $W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$ when $E/\mathbb{F}_p$ is rational.

Proposition 5.18. *Let $E/\mathbb{F}_p$ be a rational supersingular curve, with its 2-torsion rational (so E is horizontal to E'_0), and $A = W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$. Then $A \simeq E \times E^t$, where E^t is the quadratic twist of E.*

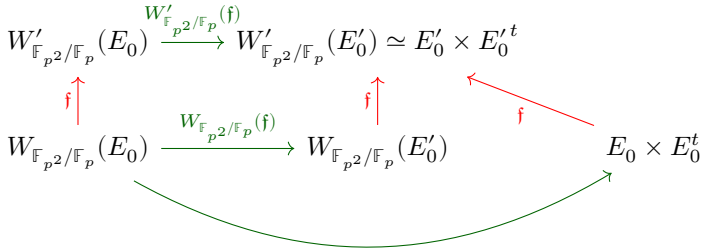

FIGURE 1. Isogeny diagram for the Weil restriction and Scholten's construction. All varieties are either horizontal to E_0 or horizontal to E'_0, horizontal isogenies are in green and ascending isogenies in red.

Proof. We give two proofs, the first one purely algebraic, and the second one via the module equivalence of category and Proposition 5.17.

We work over $\mathbb{F}_{p^2}$ and keep track of the descend giving the various twists. Scholten's construction is given by the quotient of $E \times E^\sigma$ by the kernel $K = \{(T, \sigma(T)), \quad \forall T \in E[2]\}$. But with our hypothesis, $E^\sigma = E$ and $\sigma(T) = T$, hence the kernel is simply $K = \{(T, T), \quad \forall T \in E[2]\}$. Let $\Phi : E^2 \to E^2, (P, Q) \mapsto (P + Q, P - Q)$, this Φ has the same kernel K, the diagonal of $E[2]$ in E^2, ence $E^2/K \simeq E^2$ over $\mathbb{F}_{p^2}$.

Now if we descend Φ to $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$, the codomain will be a twist of E^2 over $\mathbb{F}_p$. We can find it by keeping track of the Galois action, the one on the Weil restriction is given by $\sigma(P, Q) = (\pi(Q), \pi(P))$, and applying F to this we get $(\pi(P + Q), -\pi(P - Q))$. So on the codomain the Galois action is the usual one on the first factor so corresponds to E, but the twisted one (by -1) on the second factor. This twist by -1 corresponds to the quadratic twist E^t of E.

From the module point of view, $W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E) = M \cdot E'_0$, where $M = \mathrm{Hom}_{\mathbb{F}_{p^2}}(E, E'_0)$ by Proposition 5.17. Let $\alpha_E : E \to E'_t$ be the twisting isomorphism over $\mathbb{F}_{p^2}$. Then $M = \mathrm{Hom}_{\mathbb{F}_p}(E, E'_0) \oplus \mathrm{Hom}_{\mathbb{F}_p}(E^t, E'_0)\alpha$. Let $M_\kappa = \{m \in M, \pi_{E'_0} m \pi_E^{-1} = \kappa m\}$, we have $\mathrm{Hom}_{\mathbb{F}_p}(E, E'_0) = M_1$, $\mathrm{Hom}_{\mathbb{F}_p}(E^t, E'_0)\alpha = M_{-1}$, so they have trivial intersection (and they are actually orthogonal by [CPV20, Lemma 11]). Furthermore, the members of the left and on the right are both unimodular modules for the same quadratic form by Proposition 5.17, so the inclusion has to be an equality. □

Note that by Theorem 5.5, when $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E) = M \cdot E_0$, we have $M = \mathrm{Hom}_{\mathbb{F}_{p^2}}(E, E_0)$ as a R-module but this time the quadratic form is twice the natural one on $\mathrm{Hom}_{\mathbb{F}_{p^2}}(E, E_0)$, so in that case $\mathrm{Hom}_{\mathbb{F}_p}(E, E'_0) \oplus \mathrm{Hom}_{\mathbb{F}_p}(E^t, E'_0)\alpha \subset M$ is of index 4. In particular, we should expect a degree 4 isogeny $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_0) \to E_0 \times E_0^t$. This is indeed a particular case of [Mil72, Proposition 7], and more concretely the same argument as above for E'_0 shows that the map $W_{\mathbb{F}_{p^2}/\mathbb{F}_p} E_0 \to E_0 \times E_0^t$ is the descent of the map $F/\mathbb{F}_{p^2} : E_0^2 \to E_0^2, (P, Q) \mapsto (P + Q, P - Q)$ to $\mathbb{F}_p$ (the difference with the case above is that this time $E_0 \times E_0^t$ is not isomorphic to $W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_0)$ since they are on different horizontal levels).

In summary, we have the following commutative diagram in Figure 1.

Example 5.19. Let $p \equiv 3 \mod 4$ and let $E_0 : y^2 = x^3 + x/\mathbb{F}_p$. It is primitively oriented by R, and it is 2-isogeneous to its quartic twist $E'_0 : y^2 = x^3 - x/\mathbb{F}_p$. We have $E'_0 = \mathfrak{f} \cdot E_0$.

We have $E_0(\mathbb{F}_p) = \mathbb{Z}/(p + 1)\mathbb{Z}$ while $E'_0(\mathbb{F}_p) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/(p + 1)/2\mathbb{Z}$. The endomorphism $1 + \pi_p$ is not trivial on $E_0[2]$, because it only has half of its two torsion rational, while it is trivial on $E'_0[2]$, so $(1 + \pi_p)/2$ only exist as an endomorphism over E'_0.

Now this curve has j-invariant $j(E_0) = 1728$, which means it plays shenanigans with twists. Indeed, $\mathrm{Aut}(E_0) = \mu_R = \langle i \rangle$ over $\overline{\mathbb{F}}_p$, but the automorphism i is not rational over $\mathbb{F}_p$.

Twists over $\mathbb{F}_p$ are represented by étale μ_4-torsors, hence by $H^1(G,\mu_4) \simeq \mu_4/(\sigma-1)$ where $G = \mathrm{Gal}(\mathbb{F}_p)$. Here we have $\sigma(i)/i = -1$, so the twists induced by the cocycles giving value 1 and -1 on σ differ by a coboundary, hence are actually isomorphic over $\mathbb{F}_p$. (For an elementary proof, see [CPV20, Lemma 1].) In other words, $E_0^t \simeq E_0^t$ and $E_0'^t \simeq E_0'$, there are only two twists of E_0 over $\mathbb{F}_p$ (but there are indeed 4 twists over $\mathbb{F}_{p^2}$; E_0' which is now a quadratic twist of E_0, and two new quartic twists).

In particular, by Proposition 5.18, $W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_0') \simeq (E_0')^2$.

We known also that $\mathrm{End}(E_0) = \langle 1, i, (i+\pi)/2, (1+i\pi)/2\rangle$, this contains $R \oplus Ri$ but is not equal to it, as we can check with the discriminants (the index is 4, and $\mathrm{End}(E_0) = R + R(i+j)/2$). On the other hand $\mathrm{End}(E_0')$ is $O_R \oplus O_R i$, since both have reduced discriminant $-p$. By Proposition 5.17, this gives another proof that $W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_0') \simeq (E_0')^2$, since this is isomorphic to O_R^2 as an O_R-module.

5.4. **The supersingular isogeny path problem and module action inversion.** In this section, we reduce the supersingular isogeny path problem to inverting a rank 2 module action, for $R = \mathbb{Z}[\sqrt{-p}]$.

Fix $E_0/\mathbb{F}_p$ a supersingular curve, with primitive orientation by R, and let $\mathfrak{O}_0$ be its full endomorphism ring, a quaternion order. Given a supersingular (maximal) curve $E/\mathbb{F}_{p^2}$, the supersingular isogeny path problem for E consist in computing an isogeny $E_0 \to E$.

This essentially reduces to computing the right $\mathfrak{O}_0$ ideal $I = \mathrm{Hom}_{\mathbb{F}_{p^2}}(E, E_0)$: from the ideal we can use the quaternionic version of Clapotis as in [BDD+24] to obtain an efficient representation of a path $E \to E_0$. Conversely (we won't need this converse), if we have an efficient representation of a smooth isogeny $\phi : E_0 \to E$, we can compute I by splitting ϕ into smaller isogenies, computing the intermediate ideals, and descending the action (e.g. via Clapotis again). This is similar to Remark 4.29, which was inspired by this supersingular case. If ϕ is an arbitrary efficient isogeny, we can invoke [CII+23] to recover the ideal in quantum polynomial time.

We refer to [Wes22b; PW24; Wes24] for more details and other reductions on this problem.

Let us now state the module inversion problem:

Definition 5.20 (Module inversion)**.** Given (an explicit representation of the ppavs) $(A, \lambda_A), (M \cdot A, H_M \cdot \lambda_A)$, recover a description of the unimodular Hermitian module (M, H_M).

Like in the supersingular case, we could ask for variants of this problem where we ask to recover the effective orientation of M on $M \cdot A$, or if we just want to recover partial informations on M, e.g one element $M \cdot A \to A$ corresponding to $m \in M$. We could also ask for the relationship, given $M \cdot E_0$, between knowing $\mathrm{End}_R(M \cdot E_0)$ and knowing M (in rank > 1), and so on. We leave it for future work to study the relationship between these variants (which is now well understood in the supersingular case).

Example 5.21. If $(A, \lambda_A) = (M, H_M) \cdot (E_0, \lambda_{E_0})$, then $M = \mathrm{Hom}_R(A, E_0)$, and the Hermitian form H_M is given as follows: for m_1, m_2 which we interpret as morphisms $A \to E_0$, then $\tilde{m_2} m_1$ gives a R-endomorphism of E_0, hence an element of R, which is $H_M(m_1, m_2)$. This is a special case of Theorem 4.11.

Let $E_0' = \mathfrak{f} E_0$ as in Section 5.3. By the commutative diagram in Figure 1, provided we know a path from E_0 to its quadratic twist E_0^t (which is easy if $\mathfrak{O}_0$ is known, see [CPV20; Wes22a]), then finding a path to E_0^2, $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_0)$, $W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_0)$, $W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_0')$, ...is essentially equivalent.

Let E be a (maximal) supersingular elliptic curve. If we find an isogeny path $\phi : E_0 \to E$, then we obtain an isogeny $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\phi) : W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_0) \to W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$. Conversely, if we have some path $\Phi : W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_0) \to W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$ over $\mathbb{F}_p$, then over $\mathbb{F}_{p^2}$, we get $\Phi : {E_0}^2 \to E \times E^\sigma$. Now Φ is given by a matrix of isogenies, and at least one of the isogeny $E_0 \to E$ or $E_0 \to E^\sigma$ in this matrix is non trivial. It follows that, composing with π_p if necessary, we obtain a non trivial isogeny $E_0 \to E$. We see that the path problem between E_0 and E and the one between $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_0)$ and $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$ are essentially equivalent.

Our main theorem, which refines this observation, is:

Theorem 5.22. *Assume that we know $\mathfrak{O}_0 = \mathrm{End}(E_0)$. Then the isogeny path problem $E_0 \to E$ reduces to the rank 2 module inversion problem on $E_0, W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$.*

Proof. From E we can compute its Weil restriction $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$. Let $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E) = (M, H_M) \cdot E_0$. In Theorem 5.5, we have shown that the knowledge of $I = \mathrm{Hom}_{\mathbb{F}_{p^2}}(E, E_0)$ is equivalent to the knowledge of (M, H_M). Since the isogeny path reduces to finding I, the result follows. □

Remark 5.23. We make several *heurisitic* remarks on the security of the rank 2 module inversion.

- We focus on the subcategory of $\mathfrak{Ab}_{E_0,R}$ given by abelian surfaces: that is supersingular abelian surfaces over $\mathbb{F}_p$ isogeneous to E_0^g over $\mathbb{F}_p$. We conjecture that there are $\approx p^{3/2}$ such abelian surfaces, and that the ℓ-isogeny graphs are expander.
- A more refined version of the conjecture above is that a combining the Weil restriction of supersingular curves over $\mathbb{F}_{p^2}$ with the inversible ideal actions (i.e. action by rank 1 modules) give most of the surfaces. We do not expect to get all of them, first because both Weil restriction and invertible ideal actions only give horizontal abelian surfaces (see Lemma 5.11). And secondly because, forgetting polarisations, looking at the action of ideals on $E_0^2 = W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_0)$, $\mathfrak{a} \cdot E_0^2 \simeq E_0 \times \mathfrak{a}^2 \cdot E_0$, so the action of the Picard group on E_0^2 misses the unpolarised abelian varieties of the form $E_0 \times \mathfrak{b}E_0$, with $\mathfrak{b}$ not a square in the Picard group, hence we only get a proportion of $1/\#\operatorname{Pic}(R)[2]$ of unpolarised abelian surfaces when looking at the action on E_0^2.

  However, we do conjecture that if $A = W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$ is a Weil restriction, then acting by an invertible ideal does not give another Weil restriction (unless E is already defined over $\mathbb{F}_p$). We remark that there are $\approx p$ Weil restriction of supersingular curves, and $\approx \sqrt{p}$ invertible ideals, which is coherent with our $\approx p^{3/2}$ supersingular abelian surfaces in $\mathbb{F}_p$ isogeneous to E_0^2 above.
- Under the expander assumption, we have a worst case to average case reduction, namely the average rank 2 module inversion is hard if the worst case is hard. Indeed, if the average case was easy, if $A = M \cdot E_0$ is an abelian surface, we can take random smooth isogenies until we hit an easy case $A' = M' \cdot E_0$: with the expander property we are quickly uniformly distributed. From M' and our path $A \to A'$, we recover M using Remark 4.29. In particular, by Theorem 5.22, under the expander assumption, the average case of rank 2 module inversion is at least as hard as the supersingular isogeny path problem.
- The best currently known algorithm to solve the supersingular isogeny path problem is in $\widetilde{O}(\sqrt{p})$. An heuristic version is given in [DG16], taking a random path until hitting a supersingular curve over $\mathbb{F}_p$ (which happens with probability $\approx 1/\sqrt{p}$), and a proven algorithm is given in [PW24]. We expect the general module inversion problem in rank 2 to be of the same complexity: using an heuristic algorithm similar to [DG16]: we take a random path until we find an abelian surface A' which is isomorphic to a product (with the product polarisations), and reduce to a rank 1 problem: the Hermitian module corresponding to A' is an orthogonal direct sum of ideals. Then we propagate the module inversion on A' back to our original A via our smooth path.

  Heuristically, it takes $\widetilde{O}(\sqrt{p})$ to reach a product. The rank 1 problem can then be solved in heuristic $\widetilde{O}(p^{1/4})$ time by [DG16] (for a rigorous argument see [MS24]), or in subexponential quantum time, so the first step is dominant. We could also search for a Weil restriction, which we also expect to hit in time $\widetilde{O}(\sqrt{p})$, and reduce to the supersingular isogeny path problem, which can be solved in $\widetilde{O}(\sqrt{p})$.

  So we see that, unless a better algorithm is found for the supersingular isogeny path problem, we do not gain security by considering supersingular abelian surfaces over $\mathbb{F}_p$ which are not Weil restrictions.

We finish this section by a discussion on variants of module inversion vs path finding, with a list of open questions. To simplify notations, by the Weil restriction case we mean that $A = W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$ is the Weil restriction of a supersingular elliptic curve $E/\mathbb{F}_{p^2}$ and we are trying to solve the Hermitian module inversion problem $A = (M, H_M) \cdot E_0$ from some primitively $\mathbb{Z}[\pi]$-oriented supersingular curve $E_0/\mathbb{F}_p$. We will assume that we have chosen a E_0 with known endomorphism ring $\mathfrak{O}_0$, this can always be done efficiently under GRH.

Remark 5.24 (Variants of module inversion)**.**

- Let $A \in \mathfrak{Ab}_{E_0,R}$ be a ppav, and M a rank g unimodular Hermitian module. If we know M, and we can build nice similitude $R^g \to M$, then we can build an effective isogeny path $A^g \to M \cdot A$. Under Heuristic 2.13, using Section 4.5.2, we can always build effective isogeny paths $A^{g+r} \to M \cdot A \times A^r$.
- Conversely, given a smooth isogeny path $A^g \to M \cdot A$, can we recover M? If the isogeny $A^g \to M \cdot A$ is of small degree, then we can certainly compute its kernel, and recover M from that kernel using Proposition 4.24. Otherwise, if the isogeny is smooth, we can proceed as in Remark 4.29 (this also uses Heuristic 2.13), splitting the path into small chunks, and reconstructing M iteratively.
- In the Weil restriction case, we have seen in the discussion above Theorem 5.22 that to give an effective path $E_0^2 \to W_{\mathbb{F}_{p^2}/\mathbb{F}_p} E$ is essentially the same as to give an effective path $E_0 \to E$ (we assume we have already constructed an effective path $E_0 \to E_0^t$). And Theorem 5.5 shows that, if we know $\mathrm{End}(E_0)$, knowing $\mathrm{Hom}_{\mathbb{F}_{p^2}}(E, E_0)$ abstractly is equivalent to knowing (M, H_M) abstractly.
- Suppose that we have an efficient representation of an isogeny path $A^g \to M \cdot A$. Can we recover M? By the discussion above, we see that the article [CII+23] gives a quantum polynomial time algorithm in the Weil restriction case.
- How much does the knowledge of $\mathrm{End}_R(M \cdot A_0)$ helps in recovering M? If $A_0 = E_0$ is a primitively oriented elliptic curve and M is an invertible ideal, then $\mathrm{End}_R(M \cdot E_0) = R$, so we already know the R-endomorphism ring, so this information is vacuous in that case (and we remark that we also have a subexponential algorithm to recover M by Kuperberg).

  On the other hand, using once again the Weil restriction case, $A = W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$ the Weil restriction of a supersingular elliptic curve over $\mathbb{F}_{p^2}$, then $\mathrm{End}_R(A) = \mathrm{Hom}_{\mathbb{F}_p}(W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E), W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)) = \mathrm{Hom}_{\mathbb{F}_{p^2}}(E \oplus E^\sigma, E) = \mathrm{End}(E) \oplus \mathfrak{p}$, where $\mathfrak{p}$ is the unique bilateral of $\mathrm{End}(E)$ of reduced norm p: $p = \mathfrak{p}^2$ in $\mathrm{End}(E)$ (we warn that the multiplicative structure on $\mathrm{End}_R(A)$ is not the one inherited from the cartesian product). So from $\mathrm{End}(E)$ we recover $\mathrm{End}_R(A)$. Conversely, if we know $\mathrm{End}_R(A)$ not only abstractly but as effective endomorphisms of A, working over $\mathbb{F}_{p^2}$ where $A = E \times E^\sigma$ and projecting back to E, we recover $\mathrm{End}(E)$. We conjecture that this is still true if we only know $\mathrm{End}_R(A)$ abstractly, as long as we know how to evaluate the Rosatti involution. But from the knowledge of $\mathrm{End}(E)$, we can recover the ideal $I = \mathrm{Hom}_{\mathbb{F}_{p^2}}(E, E_0)$, hence the module M such that $A = M \cdot E_0$ by Theorem 5.22. So in this special case, module inversion reduces to the effective variant of computing the R-endomorphism ring of $A = \mathrm{Weil}(E)$, which is essentially equivalent to computing the full endomorphism ring of E. (And for the supersingular curve E the effective and non effective variants are equivalent, see [EHLMP18; Wes22b]).
- Recall the notion of double orientation from Example 4.26. In the Weil restriction case, a double orientation on $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$ essentially amount to an orientation on E.

  We remark that, given an orientation on E', computing the full endomorphism ring on E' only takes quantum subexponential time [MW23]. By Theorem 5.22, finding the rank 2 module M such that $A = M \cdot E_0$ then also only takes quantum subexponential time.

  We leave it as an open question, whether for an arbitrary doubly oriented supersingular abelian surface $A/\mathbb{F}_p$, so which admit an extra orientation on top of the one given by R, the module inversion problem $A = M \cdot E_0$ can be solved in quantum subexponential time. The above discussion gives a positive answer in the special case where A is a Weil restriction.

6. ⊗-MIKE: Tensor Module Isogeny Key Exchange

In this section, we bring together the action from Section 4 and the cryptographic applications of Section 3: in Section 6.1 we describe a very general version of ⊗-MIKE. Then in Section 6.2, we incorporate the results of Section 5 to instantiate ⊗-MIKE on supersingular elliptic curves.

6.1. The Hermitian module key exchange.

Let (A_0, λ_{A_0}) be a ppav in $\mathfrak{Ab}_R$. We can use the unimodular action from projective modules to build a key exchange as follows (dropping the polarisations for simplicity):

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

If A_0 is of dimension g_0, M_1, M_2 of rank g_1, g_2, then the common key is of dimension $g_0 g_1 g_2$. We will also denote $A_{12} = (M_1 \otimes_R M_2) \cdot A_0$ as $A_1 \otimes_{A_0} A_2$, this explain the name $\otimes$-MIKE. We remark that if $A_0 \in \mathfrak{Ab}_{E_0,R}$, we can relax the projectivity condition on M_i to M_i torsion free, as long as $M_{12} \coloneqq M_1 \otimes_R M_2$ is still torsion free, and M_1, M_2, M_{12} are compatibles with A_0.

One way to choose (M_1, H_1) is for Alice to compute a smooth n_1-similitude $(M_1, H_1) \to (R^{g_1}, H_R^{g_1})$, with the n-torsion accessible, for instance by doing an Hermitian path of small similitudes. Then we can apply Section 4.5.1 to compute the action by (M_1, H_1) efficiently: she first computes A_1 in dimension $g_0 g_1$, publish it, then compute $A_{12} = M_1 \cdot A_2$ in dimension $g_0 g_1 g_2$ from the A_2 of Bob.

We thus have a smooth n_1-isogeny $A_0^{g_1} \to A_1 = M_1 \cdot A_0$ and a smooth n_2-isogeny $A_0^{g_2} \to A_2 = M_2 \cdot A_0$, and the key exchange fits into the following commutative diagram:

$$\begin{array}{ccc} A_0^{g_1 g_2} & \longrightarrow & A_1^{g_2} \\ \downarrow & & \downarrow \\ A_2^{g_1} & \longrightarrow & A_{12} \end{array}$$

where $A_0^{g_1 g_2} \to A_1^{g_2}$ is the n_1-isogeny induced by $A_0^{g_1} \to A_1$, and $A_1^{g_2} \to A_{12}$ is a n_2-isogeny. On the module side, this diagram corresponds to

$$\begin{array}{ccc} R^{g_1} \otimes_R R^{g_2} & \longrightarrow & M_1 \otimes_R R^{g_2} \\ \downarrow & & \downarrow \\ R^{g_1} \otimes_R M_2 & \longrightarrow & M_1 \otimes_R M_2 \end{array}$$

We note that if the isogenies $A_0^{g_1} \to A_1$ and $A_0^{g_2} \to A_2$ have coprime degree, the diagram above is a pushforward. The key point of working with modules over the *commutative* ring R is that the codomain A_{12} does not depend on the paths chosen, like in CSIDH (and contrary to SIDH). Also, unlike CSIDH, the path $A_0^{g_1 g_2} \to A_1^{g_2}$ will not come from an ideal action (in general, unless M_1 is taken to be $(R^{g_1}, H_R) \otimes_R (I_1, H_{I_1})$).

An alternative approach is to use the Clapoti(s) method Section 4.5.2, this allows to relax the smoothness condition on n_1, at the cost of doubling (at least) the dimension of each of these computations.

Remark 6.1. We can reformulate the way we compute the MIKE key exchange as follows: we exploit the functoriality of the action, so that to compute $M \cdot A$ we need to:

- Find a unimodular module M' such that we know how to efficiently compute $M' \cdot A$ and its associated module orientation.
- Find a nice similitude between M' and M.

The computation above is the special case where we take $M' = R^g$.

Finally, we remark that we can convert this NIKE into a PKE using the Elgamal approach. In fact the monoidal action, since it also acts on isogenies, allow us to use an approach similar to SiGamal, using the image of a point, too (see Section 3.2).

6.2. **Instantiation on supersingular elliptic curves.** In order to have an efficient module key exchange, we will start on $A_0 = E_0$ an elliptic curve, typically use a supersingular elliptic curve $E_0/\mathbb{F}_p$ (on the bottom of the 2-volcano) to have a good control on its torsion, as in CSIDH, and act by rank 2 module (to prevent Kuperberg), We will select a prime of the form $u2^e - 1$ with e large, in order to use 2^e-similitudes in higher dimension. So in that case A_1, A_2 are supersingular abelian surfaces over $\mathbb{F}_p$, and A_{12} is of dimension 4. The key exchange takes $3 \log p$ bit to send the Igusa invariants $J(A_i)$.

By Remark 5.23, using Weil restrictions of elliptic curves for A_1 and A_2 (i.e. acting by the projective modules corresponding to Weil restrictions, as in Theorem 5.5), does not give a worse security for the module inversion problem (given the current best algorithms), so we might as well use a supersingular isogeny path $E_0 \to E_1$ for Alice to encode our rank 2 module. We convert this path to an $\mathfrak{O}_0$-ideal, which in turn we convert to an unimodular rank 2 module using Theorem 5.5.

In practice, to simplify the computation of the common key, we will use Scholten's construction rather than the Weil restriction. We will reuse the notations of Example 5.19, assume $p \equiv 3 \mod 4$, then $W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E'_0) = E'_0 \times {E'_0}^t$. And we further specialize to the usual curve $E_0 : y^2 = x^3 + x$, so $E'_0 : y^2 = x^3 - x$ and $W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E'_0) = (E'_0)^2$ by Example 5.19.

With these simplifications, we obtain $\otimes$-MIKE, where the common key is a ppav of dimension 4:

$$\begin{array}{ccc} E'_0 & \longrightarrow & E_1 \\ \downarrow & & \wr \\ E_2 & \rightsquigarrow & W'_{\mathbb{F}_{p^2}/\mathbb{F}_p} E_1 \otimes_{E'_0} W'_{\mathbb{F}_{p^2}/\mathbb{F}_p} E_2 \end{array}$$

We note that while $W_{\mathbb{F}_{p^2}/\mathbb{F}_p} E_i$ is horizontal with E_0, $W'_{\mathbb{F}_{p^2}/\mathbb{F}_p} E_i$ is horizontal with E'_0, so it make sense to make the tensor product over E'_0, and work with O_R-modules rather than R-modules.

Remark 6.2 (On the (un)security of taking isogenies of non coprime degree for Alice and Bob)**.** The $\otimes$-MIKE key exchange gives the following commutative dimension 4 diagram:

$$\begin{array}{ccc} {E'_0}^4 & \longrightarrow & W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_1)^2 \\ \downarrow & & \downarrow \\ W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_2)^2 & \longrightarrow & W'_{\mathbb{F}_{p^2}/\mathbb{F}_p} E_1 \otimes_{E'_0} W'_{\mathbb{F}_{p^2}/\mathbb{F}_p} E_2 \end{array}$$

Now, if we take (say) 2^e-isogenies $E'_0 \to E_i$ on both Alice and Bob's side, then with good probability they have disjoint kernels. Their Weil restriction will still have disjoint kernels, and this is also the case in Scholten's construction ${E'_0}^2 \to W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_i)$: they have disjoint kernels K_1, K_2. Thus, the diagonal 2^e-isogenies ${E'_0}^4 \to W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_i)^2$ will also have disjoint kernels K'_1, K'_2, of degree 2^{4e}, with $K'_i = K_i \times K_i$. From the commutative diagram, the 2^{2e}-isogeny ${E'_0}^4 \to A_{12} := W'_{\mathbb{F}_{p^2}/\mathbb{F}_p} E_1 \otimes_{E'_0} W'_{\mathbb{F}_{p^2}/\mathbb{F}_p} E_2$ factors through the quotient by $K'_1 + K'_2$. So its kernel K' contains $K'_1 + K'_2$, and since both side have degrees 2^{8e} (because $K'_1 \cap K'_2 = 0$), we have equality. Furthermore, the kernels K'_i live in the 2^e-torsion, so $K' = K'_1 + K'_2 = {E'_0}^4[2^e]$, and $A_{12} = {E'_0}^4$.

From the module side what happens is as follows. We take two 2^e-submodules M_1, M_2 of O_R^2, where we call a unimodular M_i a 2^e-submodule of M when the map $M_i \to M$ is a 2^e-isogeny. The assumption of the two dimension 2 isogenies having disjoint kernels translate on the module side to the condition $M = M_1 + M_2$, where $M = O_R^2$. In particular, we have $M/2^eM = M_1/2^eM \oplus M_2/2^eM$ (which corresponds to the condition $A[2^e] = K_1 \oplus K_2$ where $A = {E'_0}^2$). And the same reasoning as in the diagram above shows that $M_1 \otimes_{O_R} M_2 = (M_1 \otimes_{O_R} O_R^2) \cap (O_R^2 \otimes_{O_R} M_2)$ via the natural injection $M_1 \otimes_{O_R} M_2 \hookrightarrow O_R^2 \otimes_{O_R} O_R^2$, but since $(M_1 \otimes_{O_R} O_R^2) + (O_R^2 \otimes_{O_R} M_2) = O_R^4$, we have $M_1 \otimes_{O_R} M_2 = 2^e O_R^4 \simeq O_R^4$.

In other words, there is a complete cancellation in the key exchange whenever the isogenies have the same degree and disjoint kernels. So for security it seems best to impose them to have coprime degrees.

Since we have not yet implemented the protocol, we might as well describe a version focused on security in this section. We will give some trade offs towards efficiency later in Remark 6.3. For maximum security, we would like E_1, E_2 to be statically uniform. This can be done by using the Clapotis version of the IdealToIsogeny algorithm, as in [BDD+24]; concretely Alice converts an uniformly sample ideal representing the isogeny $E'_0 \to E_1$ by splitting an appropriate endomorphism (or even isogeny), using a dimension 2 isogeny. For simplicity we describe the endomorphism version: given an ideal I we sample two ideals I_1, I_2 of coprime norm d_1, d_2, such that $ud_1 + vd_2 = 2^e$, and $u = u_1^2 + u_2^2$, $v = v_1^2 + v_2^2$, and we split an

endomorphism $\gamma \in \mathfrak{O}_0'$ of reduce norm uvd_1d_2. We will reinterpret γ as an endomorphism of $W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_0')$, i.e. as an element of $M_2(O_R) = \mathrm{End}_{O_R}(O_R^2)$. When Alice receive Bob's supersingular j-invariant $j(E_2)$, she uses the same element $\gamma \in M_2(O_R)$ as an endomorphism of A_2^2 where $A_2 = W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_2)$, using the fact that A_2 is O_R-oriented, which she then splits using a 8-dimensional isogeny to obtain the dimension four abelian variety A_{12}.

Remark 6.3 (Improving the efficiency)**.** In the current description of the protocol, the second step of the key exchange requires a dimension 8 2^e-isogeny over $\mathbb{F}_p$, which is very slow (we can estimate it as being roughly 32× slower than a dimension 4 2^e-isogeny; a factor 2 for the rank of the kernels involved, and a factor 16 for the number of theta coordinates in level 2 (from 16 to 256). We describe some potential improvements:

- Alice could compute a dimension 1 2^e-isogeny $E_0' \to E_1$ over $\mathbb{F}_{p^2}$. Upon receiving Bob's supersingular curve, she then only needs to compute a dimension 4 2^e-isogeny $A_2^2 \to A_{12}$ over $\mathbb{F}_p$, which will be much faster than computing a dimension 8 isogeny. The corresponding algorithm is described in Algorithm 6.1. In the algorithm, we use 2^e-isogenies for $E_0' \to E_i$, but we could relax to 2^n-isogenies with $n \leq e$.

  Bob cannot do the same thing though, because of Remark 6.2. In this variant, the efficiency is asymmetric, and one side can compute the common key much faster than the other side (for instance we could have "fast" encryption but slow decryption).

  We will focus on this version of ⊗-MIKE for the rest of this section.
- Alice could compute a dimension 1 2^e-isogeny $E_0' \to E_1$ over $\mathbb{F}_{p^2}$ as above, and Bob a 3^f-isogeny $E_0' \to E_2$ over $\mathbb{F}_{p^2}$, as in SIDH. For the second step, Bob can compute a dimension 4 3^f-isogeny. In that variant we need to select $p = u2^e3^f - 1$, with $2^e \approx 3^f \approx 2\lambda$, so $p \approx 4\lambda$ and the j-invariants which live in $\mathbb{F}_{p^2}$ will be of size $\approx 8\lambda$. This double the key size compared to the previous variant.

Theorem 6.4. *Assume that we know $\mathfrak{O}_0 = \mathrm{End}(E_0)$. Assume that the rank 2 module action-CDH from Weil restriction of supersingular curves is as hard as the inversion. Assume that the isogeny path problem on E_1, E_2 is as hard as for a uniformly sampled supersingular curve E, and that the best attack against this problem is in $\widetilde{O}(\sqrt{p})$.*

Then for λ bits of security for ⊗-MIKE, we need to select p with size 2λ. The key exchange which outputs the j-invariant of the E_i then takes 4λ bits for each E_i.

Proof. By assumption action-CDH is as hard as action-inversion, which by Theorem 5.22 is at least as hard as the supersingular isogeny path problem on E_1 or E_2.

We note that since $2^e \approx p$, there are $\approx p$ possible different 2^e-isogenies for Alice starting from E_0' over $\mathbb{F}_{p^2}$, so the assumption on the isogeny path problem between E_0' and E_1 being as hard as for a random supersingular curve is not made immediately vacuous by a meet in the middle collision. □

Remark 6.5 (On the efficiency for Alice's side)**.** Computing 2^e-isogenies $E_0' \to E_1$ over $\mathbb{F}_{p^2}$ has been thoroughly optimised for SIDH. Also it is not hard to convert a 2^e-ideal I_1 in $\mathfrak{O}_0'$ to the kernel of $E_0' \to E_1$, and Proposition 5.13 explains how to convert this ideal to the module (M_1, H_1) corresponding to $W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}E_1 = (M_1, H_1) \cdot (E_0')^2$. Since $W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_0') = (E_0')^2$, the 2^e-isogeny $E_0' \to E_i$ induces a 2^e-isogeny $(E_0')^2 \to W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_i)$, hence we have a 2^e-similitude $(M_1, H_1) \hookrightarrow (O_R^2, H_R^2)$.

The main difficulty for Alice's side of the key exchange will be computing the 2^e-isogeny $A_2 \times A_2 \to A_{12} = W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}E_1 \otimes_{E_0'} W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}E_2 = (M_1, H_1) \cdot A_2$ in dimension 4. Converting the module to a kernel is described in Section 4.5.1, and we are helped that the orientation is given by the Frobenius, so is easy to compute.

There is very promising work by Dartois in [Dar24] for 2^e isogenies in dimension 4 in the theta model, building on [DMPR24] for dimension 2. For now Dartois only has a Sage implementation, and is working on a lower level optimised implementation. Only when this implementation is finished will we be able to give concrete timings for ⊗-MIKE.

***Input*:** The supersingular curve $E_0'/\mathbb{F}_p : y^2 = x^3 - x$, primitively oriented by O_R, with $p = u \cdot 2^e - 1$. .
***Output*:** The common secret $J(A_{12})$ in the $\otimes$-MIKE key exchange from Alice's point of view

- As a precomputation step, we compute a basis (P, Q) of $E_0'[2^e]$ and how generators of of $\mathfrak{O}_0'$ act on this basis.
- Alice selects a random kernel $K = \langle uP + vQ\rangle$ of degree 2^e, along with its corresponding ideal I. For instance, she selects $I_1 = (2^e, \alpha)$ with α of reduced norm $2^e o$, o odd, and computes $K = \langle \overline{\alpha} P\rangle$ (assuming $\overline{\alpha}P$ has full order, otherwise switch to $K = \langle \overline{\alpha} Q\rangle$).
- She computes $E_1 = E/K$, and send $j(E_1)$ to Bob.
- By Proposition 5.13, the $\mathfrak{O}_0'$-ideal 2^e-similitude $\Psi : I_1 \hookrightarrow \mathfrak{O}_0'$ gives (by forgetting the $\mathfrak{O}_0'$-orientation), a unimodular O_R-module 2^e-similitude $\psi : M_1 \hookrightarrow O_R^2$.
- She receives $j(E_2)$ from Bob, and selects a model for E_2.
- She computes the Scholten construction $A_2 = W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_2)$
- She computes the kernel $K' = (A_2^2)[M_1]$, where the action of $m_1 \in M_1$ on A_2^2 is given by, if $\psi(m_1) = (\gamma_1, \gamma_2)$, $(P_1, P_2) \in A_2^2 \mapsto \gamma_1 P_1 + \gamma_2 P_2 \in A_2$, where $\gamma_i P_1$ is computed via the Frobenius orientation.
- She computes the quotient $A_{12} = (A_2^2)/K'$
- She output $J(A_{12})$ where J are dimension 4 modular invariants.

Algorithm 6.1 The $\otimes$-MIKE key exchange on Alice's side

We remark that the dimension 4 isogeny is defined over $\mathbb{F}_p$. And thanks to Lemma 5.15, there is a level 2 theta null point of $W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_i)$ defined over $\mathbb{F}_p$ when $p \equiv 7 \mod 8$ (whereas this is never the case for $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_i)$, this was one of our motivation to switch from the Weil restriction to Scholten's construction in the key exchange). We will also benefit from all the optimisations made in [CR24] (building on [Cos18]). Scholten's construction is given by an action of a non inversible ideal, this was one of our motivation for looking at non projective module actions.

For efficiency reasons, it will also be helpful to use 2^{e-2}-isogenies rather than 2^e-isogenies, the extra available torsion allows the theta algorithm to work without needing any square roots, and also to evaluate the action of O_R (since $\mathbb{Z}[\pi]$ is only of index 2 in O_R).

Due to the conjectured quantum exponential security of $\otimes$-MIKE, it will scale better than CSIDH. Another advantage is that we only need 2^e-isogenies, while scaling CSIDH require using isogenies of larger and larger degree. And a dimension 4 2^u-isogeny, while quite a bit slower than a dimension 1 2^u-isogeny, will be faster than a dimension 1 ℓ-isogeny for $\ell \approx 2^u$ large enough, even with `sqrtVelu` [BDLS20] or radical isogenies [CDV20].

Of course the main drawback is that we have only discussed Alice's side here, while in Bob's side he needs to compute a dimension 8 2^e-isogeny over $\mathbb{F}_p$ to complete the second part of the key exchange, which will be much more expansive (and annoying to implement) than Alice's dimension 4 counterpart.

Remark 6.6 (On the knowledge of $\mathrm{End}(E_0)$)**.** We remark that for Alice's side, we do not need to know the full endomorphism ring $\mathfrak{O}_0 = \mathrm{End}(E_0)$ for $\otimes$-MIKE. We might as well take a 2^e-isogeny $M \hookrightarrow R^2$ and compute the 2^e-isogeny $E_0^2 \to M \cdot E_0$ in dimension 2.

We could also take a random 2^e-isogeny $E_0 \to E_1$ over $\mathbb{F}_{p^2}$, take its Weil restriction, and recover the module M via Remark 4.29, using pairings and DLPs.

But knowing $\mathfrak{O}_0$ allows us to start with an ideal $I \subset \mathfrak{O}_0$ of reduced norm 2^e rather than a module, or to recover the ideal I from the 2^e-path $E_0 \to E_1$ in dimension 1 rather than in dimension 2. Furthermore, it is used in the security reduction from Theorem 6.4. Lastly, this is needed in Bob's side (unless we are in the variant where Bob computes a 3^f-isogeny).

There is a key subtlety in using the Weil restriction from a random $E_0/\mathbb{F}_p$. The n-isogeny $E_0 \to E$ over $\mathbb{F}_{p^2}$ gives a n-isogeny $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_0) \to W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$ over $\mathbb{F}_p$. But $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_0)$ is a twist of E_0^2, and there is no reason that the module W such that $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_0) = W \cdot E_0$ admit a nice similitude from R^2

(i.e. that there is a nice isogeny $E_0^2 \to W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_0)$). This means that if $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E) = M \cdot E_0$, then to compute $M \cdot A$ for $A/\mathbb{F}_p$ using Remark 6.1, we would need to first compute an effective orientation on $W \cdot A$. If E_0 is the special curve $y^2 = x^3 - x$ (and using $W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}$ rather than $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}$), we are saved because $W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_0) = E_0^2$, so $W = R^2$! This is similar to what happens in CSIDH (see [CPV20]): there is no reason to expect to have a nice ideal I linking $E/\mathbb{F}_p$ and $E^t/\mathbb{F}_p$, except when $E = E_0$ is the special curve!

What we could do instead starting on a non special $E_0/\mathbb{F}_p$, is to exploit the fact that $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_0)$ is always given by the Galoisian module action $R[G] \cdot E_0$ (see Remark 5.10). So we could instead use the construction of Remark 6.1, working with Galoisian modules rather than R-modules, and computing the corresponding kernel in $R[G] \cdot A = W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(A)$, via the isomorphism $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(A) \simeq A^g$ over $\mathbb{F}_{p^2}$, and taking into account the twisted Galois actions we have when descending this isomorphism to $\mathbb{F}_p$.

As mentioned in the remark above, we leave these Galoisian action considerations for future work, especially since there is little incentive to start with a random base curve $E_0/\mathbb{F}_p$ rather than our special curve. Indeed, the endomorphism ring computation of E_0 is only quantum subexponential in that case anyway, so an attack relying on knowing the full endomorphism ring of the starting curve would still work up to an extra subexponential work. To get a quantum exponential gap for the endomorphism ring computation, we would need to start with $E_0/\mathbb{F}_{p^2}$, or rather with $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_0)/\mathbb{F}_p$, but then our base point lives in dimension 2 and when we act by rank 2 module, the common key would then be in dimension 8, and so potentially (depending on the variants used), require a dimension 16 isogeny computation…

Remark 6.7 (Modular invariants)**.** One key technical difficulty that we have swept under the rug so far, is that to get a common key, Alice and Bob need to fix invariants for the common dimension 4 codomain A_{12} that does not depend on the isomorphism class. Theta constants are not good enough because they depend on a level structure. A solution is to take all equivalent level 2 theta null points under the action of $\Gamma/\Gamma(2,4)$, and use the smallest one for the lexicographic order. This takes $O(1)$ (this only depends on the dimension $g = 4$, not on the security parameter), but this hides a large constant and would be ineffective.

The best solution would be to use a full set of modular invariants, constructed from a level 2 theta null point, which will be the output of the isogeny computation. I don't know if such a set is already given in the literature.

It is easy to build invariants as suitable symmetric polynomials in the theta constants (the difficulty is to be sure we have a full set), so maybe a solution would be to use only partial invariants. This could worsen the security through.

Remark 6.8 (On the security)**.** Although we now have good signatures algorithms, like SQISign2d [BDD+24] whose security properties (essentially) reduce to the supersingular isogeny path problem, this is not the case key exchange schemes or public key encryption based on supersingular isogenies.

⊗-MIKE is a first step towards this direction, since it requires to publish neither torsion point, nor partial information on the endomorphism rings of E_1, E_2. There are still several gaps compared to a full security reduction though:

- The most important one is the gap between module action-CDH and module action-inversion. We know that module action inversion is harder than both CDH and the supersingular isogeny path problem by Theorem 5.22, but this gives no information on how action-CDH relates to the isogeny path problem.
- Secondly, on Alice's side, taking 2^e-isogenies with $2^e \approx p$ is not quite long enough to get statically uniform random curves E_i in the supersingular graph: even through the graph is Ramanujan, to get a provable uniform bound of $O(p^{-1/2})$ the path would need to be of degree $\approx p^2$ [DLRW24, Proposition 29].

  A solution is for Alice to do as Bob, i.e., to instead sample a uniform random ideal $I_1 \subset \mathfrak{O}_0$ (of large enough norm), and use Clapotis as in [BDD+24] to compute $E_1 = I_1 \cdot E_0$, via a

dimension 2 isogeny. The drawback is then that her dimension 4 common secret A_{12} then needs to be computed through a dimension 8 isogeny too.
- Finally, if we don't use full modular invariants for A_{12} (see Remark 6.7), then we have a weak variant of the CDH problem (where several different abelian varieties of dimension 4 could solve the CDH problem, as long as they have the same partial modular invariants). As mentioned in Remark 6.7, a solution is to use normalised theta constants under the action of $\Gamma/\Gamma(2,4)$.

With these adaptations, we get a more inefficient scheme (but still polynomial time with respect to the security parameter), especially on Alice's side, whose security reduces to the action-CDH problem for (the Weil restriction of) random supersingular elliptic curves.

Remark 6.9 (Higher dimensional CRS/CSIDH)**.** It is folklore that the CRS key exchange can be extended to higher dimension: take a CM abelian variety $A/\mathbb{F}_q$, and act on it by the Shimura class group. (This is a special case of Theorem 4.7, see Section 7). In the special case that $A = E$ is an elliptic curve, the CM field is a quadratic field, and the Shimura class group is the standard class group.

Our module action, although it also involves higher dimensional abelian varieties, goes in a somewhat orthogonal direction: rather than acting by ideals in an order of higher rank than 2, we act by modules of rank > 1 over the same quadratic ring R as the usual ideal action. Notably, we can still act on elliptic curves, but the result will be an abelian variety of dimension > 1.

Remark 6.10 (Relationship with SIDH)**.** The main difference with the SIDH key exchange, is that SIDH used the pushforward of the isogenies $E'_0 \to E_i$ as a common secret key E_{12}. This required to publish extra torsion information, since E_{12} depends on the exact path taken from $E_0 \to E_i$, and not only on the codomains.

By contrast, in ⊗-MIKE the common dimension 4 abelian variety A_{12} depends only on E_1 and E_2.

We remark that in the CSIDH group action, when acting by ideals of coprime degrees I_1, I_2, the common curve $E_{12} = I_1 I_2 \cdot E'_0$ is also the pushforward of $E'_0 \to E_1$ by $E'_0 \to E_2$. But this is specific to the rank 1 case, in general the pushforward approach yields very different results from the module action approach, and we argue that the later is the more natural generalisation of the CSIDH key exchange.

There is still a link between the two approaches: let E_{12} be the SIDH pushforward, and A_{12} be the MIKE common key. Then $W'_{\mathbb{F}_{p^2}/\mathbb{F}_p} E_{12}$ is the pushforward of ${E'_0}^2 \to W'_{\mathbb{F}_{p^2}/\mathbb{F}_p} E_1$ and ${E'_0}^2 \to W'_{\mathbb{F}_{p^2}/\mathbb{F}_p} E_2$.

Let M_1, M_2 be the unimodular modules such that $M_i \cdot E'_0 = W'_{\mathbb{F}_{p^2}/\mathbb{F}_p} E_i$. We can see, using the path $E_0 \to E_i$, the M_i as submodules of O_R^2. Then by Example 4.20, $W_{\mathbb{F}_{p^2}/\mathbb{F}_p} E_{12} = (M_1 \cap M_2) \cdot E_0$, where the intersection is taken in R^2 (hence depends on the paths!). Now there is an injection $M_1 \cap M_2 \hookrightarrow M_1 \otimes_R M_2$, which gives a quotient $A_{12} \to W'_{\mathbb{F}_{p^2}/\mathbb{F}_p} E_{12}$. So in some sense, A_{12} contains all possible SIDH key exchanges with codomains E_1, E_2; the corresponding quotients depending on the exact paths.

7. Conclusion

The projective module action on abelian varieties is a powerful tool. Although it has been used in number theory for a long time (see Section 1.2), it had not really been used for isogeny based cryptography until recently (see [PR23a] and this current work).

The fact that it gives an antiequivalence when applied to a base elliptic curve E_0 (see Theorem 4.9) allows to reformulate many questions in term of modules. We refer to [Rob24a] for some examples: level structure, going up and down isogenies, sesquilinear pairings (as introduced in [Sta24]), (un)forgetting orientations, non principal polarisations… Beside ⊗-MIKE, in that talk we also mention some other potential cryptographic applications of the module action.

In this paper, for simplicity we have mainly looked at the case where R is an imaginary quadratic order. But we formulated Section 4.2 in the general case, and in particular Theorem 4.7 is given for R an order in a CM field or totally real field (see also Appendix A to go further). Notably, we can act by a projective R-module M, endowed with a positive definite Hermitian form H, where in that case the positive definite condition is that $H(x,x)$ is totally positive for all $x \in M$. Notably, assuming R maximal for simplicity, we can reinterpret the Shimura class group as given by the isomorphism equivalence class of projective unimodular Hermitian R-modules, and group law given by the tensor

product. These Hermitian CM modules have been thoroughly studied by Shimura. Whenever R is Gorenstein, orthogonality behaves well, see Appendix A. Of course, the action itself is only a small part of the beautiful theory of complex multiplication, the main result being Shimura's reciprocity law!

I am optimistic about the potential performance of $\otimes$-MIKE on Alice's side. Of course we really need an implementation, but, thanks to the awesome work of the younger generation of isogenists (see Remark 6.5), what would have seemed hopelessly inefficient a few years ago (a 2^n-isogeny in dimension 4) is not scary anymore. Unfortunately, I am more pessimistic on Bob's side (at least in the version that involves a dimension 8-isogeny on his side). Maybe there is hope, using the Galoisian R-modules action from Remark 5.10 rather than just the R-modules action, to choose parameters for the key exchange so that the second step also comes from a Weil restriction (like in the first step), which would allow us to work with varieties of half the dimension (but over $\mathbb{F}_{p^2}$ rather than $\mathbb{F}_p$).

We hope that the module action will find many other cryptographic applications, beside $\otimes$-MIKE and the ones mentioned in [Rob24a].

Appendix A. Biduality for a Gorenstein order

Let $K/\mathbb{Q}$ be a number field, with an involution $x \mapsto \overline{x}$, and $R \subset O_K$ an order stable by $\bar{\cdot}$. In view of Section 4.2, we are mainly thinking about K a CM field here.

Let (V, H) be a non degenerate K-Hermitian vector space. If $M \subset V$ is a R-lattice (which means that $M \otimes_R \mathbb{Q} = V$), then as in Section 2 we define the R-orthogonal $M^\sharp = \{v \in V : H(m, v) \in R\}$ The literature on Hermitian forms often specialize to the case $R = O_K$, where it is easy to show using pseudo-basis, as in Remark 2.5, that $M^{\sharp\sharp} = M$.

By [Bas63, Theorem 6.2], (see also [Vas68, p.1 and Theorem A.1]), since $\operatorname{Spec} R$ is of dimension 1, R is Gorenstein iff every torsion free R-modules M is reflexive, meaning that the biduality morphism $M \to M^{\vee\vee}$ is an isomorphism.

In particular, this implies that if R is Gorenstein, then for our lattice $M \subset V$ as above, $M^{\sharp\sharp} = M$. For convenience, we give a self contained proof of this fact (using the fact that R is an order simplify some of the arguments from the more general case cited above).

Proposition A.1. *With the notations above, assume furthermore that R is a Gorenstein order. Let $M_2 \subset M_1 \subset V$ be two lattices. Then $M_1^\sharp \subset M_2^\sharp$ and $\#M_1/M_2 = \#M_2^\sharp/M_1^\sharp$. In particular $M^{\sharp\sharp} = M$.*

We remark that this proposition is a particular case of [Bas63, Theorem 6.3.3].

Proof. Step 1: We first prove that the second statement is a corollary of the first. If $M \subset M^\sharp$, then $M \subset M^{\sharp\sharp} \subset M^\sharp$, but $\#M^\sharp/M = \#M^\sharp/M^{\sharp\sharp}$ so we have equality. For a general M, we can scale it to $M' = nM$ so that $M' \subset M'^\sharp$. We have $M'^\sharp = 1/nM^\sharp$, so $M'^{\sharp\sharp} = nM^{\sharp\sharp}$. Since $M'^{\sharp\sharp} = M'$, we get that $M^{\sharp\sharp} = M$.

Step 2: we have $M^\sharp \simeq M^\vee := \operatorname{Hom}_{\overline{R}}(M, R)$, via $m^\sharp \in M^\sharp \mapsto H(m^\sharp, \cdot)$. Indeed, this map is an injection since H is non degenerate, and on the other hand $\operatorname{Hom}_{\overline{R}}(M, R) \subset \operatorname{Hom}_{\overline{R}}(M, K) = \operatorname{Hom}_{\overline{K}}(M \otimes_R K, K) = \operatorname{Hom}_{\overline{K}}(V, K) \simeq V$, where the last isomorphism also comes from the non degeneracy of H. So every element in $\operatorname{Hom}_{\overline{R}}(M, R)$ is represented by some $v \in V$, which has to be in $M^\sharp$ be definition.

We also note that $\operatorname{Hom}_{\overline{R}}(M, R)$ is R-antisomorphic to $\operatorname{Hom}_R(M, R)$, so in particular is isomorphic to it as an abelian group. So we reduce to studying duality of modules.

Step 3: We remark first that duality behaves differently between a torsion R-module T, where $\operatorname{Hom}_R(T, R) = 0$ and we want to define its dual as $\operatorname{Hom}_R(T, K/R)$, and torsion free R-modules.

If M is a f.p. R-module, from the exact sequence $0 \to R \to K \to K/R \to 0$ we obtain $0 \to \operatorname{Hom}_R(M, R) \to \operatorname{Hom}_R(M, K) \to \operatorname{Hom}_R(M, K/R) \to \operatorname{Ext}^1_R(M, R) \to \operatorname{Ext}^1_R(M, K) = 0$ where the last equality comes from the fact that K is an injective R-module (by [Bas63, Theorem 6.2], we remark that K/R is also an injective R-module). If M is torsion free, $\operatorname{Hom}(M, K/R) = 0$, so $\operatorname{Ext}^1_R(M, R) = 0$. On the other hand, if $M = T$ is torsion, then $\operatorname{Hom}(T, K) = 0$, so $\operatorname{Hom}(T, K/R) \simeq \operatorname{Ext}^1_R(T, R)$.

Using Ext^1 for duality on torsion modules behaves well with quotients of torsion-free modules. Assume that $T = M_1/M_2$, M_1, M_2 torsion free. From the exact sequence $0 \to M_2 \to M_1 \to M_1/M_2 \to 0$, we get

$0 \to \mathrm{Hom}(M_1/M_2, R) = 0 \to \mathrm{Hom}_R(M_1, R) \to \mathrm{Hom}_R(M_2, R) \to \mathrm{Ext}^1(M_1/M_2, R) \to \mathrm{Ext}^1(M_1, R) = 0$, from which we get that $\mathrm{Hom}_R(M_1/M_2, K/R) \simeq \mathrm{Ext}^1_R(M_1/M_2, R) \simeq \mathrm{Hom}_R(M_2, R)/\mathrm{Hom}_R(M_1, R)$ is anti-isomorphic to $M_2^\vee/M_1^\vee \simeq M_2^\sharp/M_1^\sharp$.

Step 4: It remains to show that, for a torsion module T like $T = M_1/M_2$, then $\#\mathrm{Hom}_R(T, K/R) = \#T$.

Since $K/\mathbb{Q}$ is separable, the trace map: $\mathrm{Tr} : K \times K \to \mathbb{Q}$ is non degenerate, and we definite the trace dual R^* as the $\mathbb{Z}$-orthogonal of R for the trace.

From $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$ we get $0 \to \mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Z}) \to \mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Q}) \to \mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Q}/\mathbb{Z}) \to \mathrm{Ext}^1_{\mathbb{Z}}(R, \mathbb{Z}) = 0$ where the last equality comes from the fact that R is torsion free, so projective as a $\mathbb{Z}$-module. Since the trace is non degenerate, we have $\mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Z}) \simeq R^*$, and $\mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Q}) \simeq K$; these are isomorphisms as R-modules. So $\mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Q}/\mathbb{Z}) \simeq K/R^*$.

Step 5: If M is a R-module, $\mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z}) \simeq \mathrm{Hom}_R(M, \mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Q}/\mathbb{Z}))$ by the tensor/hom adjunction, so $\mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z}) \simeq \mathrm{Hom}_R(M, K/R^*)$. If $M = T$ is torsion, by Pontryagin duality we have $\#T = \#\mathrm{Hom}_{\mathbb{Z}}(T, \mathbb{Q}/\mathbb{Z})$.

Step 6: We have reduced to showing that $\#\mathrm{Hom}_R(T, K/R^*) = \#\mathrm{Hom}_R(T, K/R)$ for a torsion module.

This is where we need that R is Gorenstein: the Gorenstein condition (this is one of many equivalent definition, see [Bas63]) is that the dualizing complex is invertible; for our order R this equivalent to R^* being invertible. But then, if $n = \#T$, we have $R^*/nR^* \simeq R/nR$ (by localisation), hence we have an isomorphism of R-modules: $\mathrm{Hom}_R(T, K/R^*) \simeq \mathrm{Hom}_R(T, R^*/nR^*) \simeq \mathrm{Hom}_R(T, R/nR) \simeq \mathrm{Hom}_R(T, K/R)$. We can finally conclude that if T is a torsion module, $\#\mathrm{Hom}(T, K/R) = \#T$. □

Example A.2. If K is a CM field, so K is quadratic imaginary over K_0 totally real, then if R contains the maximal order O_{K_0} of K_0, it is Gorenstein (because its singularities are of nodal types), and even Bass (because its orverorder contains O_{K_0} too so are Gorenstein).

Appendix B. The general module action

In this section, we let $(R, \bar{\cdot}) \subset \mathrm{End}_k(A)$ be an orientation by a domain (hence a "CM order") on an abelian variety A/k, and look at the module action for modules which are not necessarily projective.

As explained in [Wat69], since the functor $M \mapsto \mathcal{HOM}_R(M, A)$ maps right exact sequences to left exact sequences, we can consider the derived functors $\mathcal{EXT}^i_R(M, A)$. Concretly, we can take a free (or projective) resolution of M, apply $\mathcal{HOM}_R(\cdot, A)$ to this resolution, and take the cohomology to obtain the $\mathcal{EXT}^i_R(M, A)$.

It is convenient, for these sort of cohomological considerations, to use the fact that $\mathfrak{GroupSchemes}$ embeds into the category of fppf-sheafs (because the group scheme quotient is the fppf quotient, see [DA70; Ryd13, Corollary 2.17]). So we can reinterpret these $\mathcal{EXT}$ functors as standard $\mathcal{Ext}$ functors on (R-oriented) fppf sheafs, and apply the general topos cohomological framework from algebraic geometry:

Proposition B.1. *Working on the category of fppf R-modules over the base field k, (i.e. fppf sheafs that have a R-module structure), and embedding A as a fppf-sheaf via its functor of points, and seeing the R-module M as a locally constant fppf sheaf, then the group scheme $\mathcal{EXT}^i_R(M, A)$ seen as a fppf sheaf is equal to $\mathcal{Ext}^i_R(M, A)$.*

Proof. The following argument was obtained thanks to help from Dajano Tossici. By definition, given two fppf R-modules $\mathcal{F}, \mathcal{G}$, the functor $\mathcal{Ext}^i_R(\mathcal{F}, \mathcal{G})$ is the derived functor of the hom sheaf $\mathcal{Hom}_{R,fppf}(\mathcal{F}, \mathcal{G})$.

But the group scheme $\mathcal{EXT}^i_R(M, A)$ is also defined as a derived functor of $\mathcal{HOM}_R(M, A)$. It thus suffices to check that via our embeddings these are the same functors. Taking S a k-algebra, we have $\mathcal{Hom}_{R,fppf}(\mathcal{F}, \mathcal{G})(S) = \mathrm{Hom}_R(\mathcal{F}_S, \mathcal{G}_S)$, hence $\mathcal{Hom}_{R,fppf}(M, A)(S) = \mathrm{Hom}_R(M, A(S))$ since M_S is the constant sheaf over S. But by Lemma 4.1, we also have $\mathcal{HOM}_R(M, A)(S) = \mathrm{Hom}_R(M, A(S))$. □

From the general cohomological machinery, it follows that we can also compute $\mathcal{EXT}^i_R(M, A)$ by taking an injective resolution of A (in fppf sheafs) and applying the functor $\mathcal{Hom}_{R,fppf}(M, \cdot)$ and taking the cohomology; the resulting fppf sheaf $\mathcal{Ext}^i_R(M, A)$ is representable by the group scheme $\mathcal{EXT}^i_R(M, A)$.

We can use the $\mathcal{EXT}^1_R$ functor to measure the obstruction to surjectivity: if $M_2 \hookrightarrow M_1$ is a monomorphism, by the usual long exact sequence in cohmology we have

$$0 \to \mathcal{HOM}_R(M_1/M_2, A) \to \mathcal{HOM}_R(M_1, A) \to \mathcal{HOM}_R(M_2, A) \to \mathcal{EXT}^1_R(M_1/M_2, A) \to \mathcal{EXT}^1_R(M_1, A) \to \mathcal{EXT}^1_R(M_2, A)$$

and so the map $M_1 \cdot A \to M_1 \cdot A$ is surjective if $\mathcal{EXT}^1_R(M_1/M_2, A) = 0$.

In general, if $M_2 \hookrightarrow M_1$ is an isogeny, the kernel $K = \mathcal{HOM}_R(M_1/M_2, A)$ is precisely given by $A_1[M_2]$, where $A_1 = M_1 \cdot A$, by the same argument as in Proposition 4.24. But the quotient $A_2 = A_1/K$, which is an abelian variety, is only the connected component of $M_2 \cdot A$ (because the quotient $(M_2 \cdot A)/A_2$ is a subgroup of $\mathcal{EXT}^1_R(M_1/M_2)$, which is finite because it is of torsion, since M_1/M_2 is of torsion). If M_1 is projective, $\mathcal{EXT}^1_R(M_1, A) = 0$, so $\mathcal{EXT}^1_R(M_1/M_2, A)$ is precisely the quotient of $M_2 \cdot A$ by its connected component A_2, hence M_2 is compatible with A iff $\mathcal{EXT}^1_R(M_1, A) = 0$.

From this discussion, we see that a module M is compatible with A iff for any isogeny $M \hookrightarrow R^g$ we have $\mathcal{EXT}^1_R(R^g/M, A) = 0$. And Theorem 4.9 shows that for a primitively oriented elliptic curve E_0, $\mathcal{EXT}^1_R(M, E_0) = 0$ for any f.p. module M (because the module action on E_0 is exact), hence E_0 behaves as an injective R-module.

Theorem B.2. *Assume that we are given a R-orientation on A as above, such that $\mathrm{End}_R(A) = R$. Assume furthermore that R is Gorenstein. Let M be compatible with A, and assume that $M^* = \mathrm{Hom}_R(M, R)$ is compatible with $A^\vee$.*

Then $\mathrm{Hom}_R(M \cdot A, A) = M$, and if M_2 is another module compatible with A, and we let $M_1 = M$, then $\mathrm{Hom}_R(M_1 \cdot A, M_2 \cdot A) = \mathrm{Hom}_R(M_2, M_1)$.

We conjecture that in the conditions of Theorem B.2 (in particular, R is Gorenstein), then if M is compatible with A, then M^* is automatically compatible with $A^\vee$.

Proof. We first prove that under the hypothesis, $(M \cdot A)^\vee \simeq M^* \cdot A^\vee$, this is a similar argument as in Theorem 4.5. Taking a presentation $R^m \to R^n \to M \to 0$, we have $0 \to M \cdot A \to A^n \to A^m$, and taking the dual abelian varieties, $A^{\vee m} \to A^{\vee n} \to (M \cdot A)^\vee \to 0$.

On the other hand, taking dual modules we have $0 \to M^* \to R^n \to R^m$, hence acting on $A^\vee$, $A^{\vee m} \to A^{\vee n} \to M^* \cdot A^\vee$. In these sequences, both maps $A^{\vee m} \to A^{\vee n}$ are the same. Now since M^* is compatible with $A^\vee$, $M^* \cdot A^\vee$ is an abelian variety of dimension rg where r is the rank of M and g the dimension of A by Proposition 4.2. But the image of $A^{\vee m} \to A^{\vee n}$ is of dimension rg, so it has to be all of $M^* \cdot A^\vee$.

Now we compute $\mathrm{Hom}_R(M \cdot A, A) = \mathrm{Hom}_R(A^\vee, (M \cdot A)^\vee) = \mathrm{Hom}_R(A^\vee, M^* \cdot A^\vee) = \mathrm{Hom}_R(M^*, \mathrm{Hom}_R(A^\vee, A^\vee)) = \mathrm{Hom}_R(M^*, \mathrm{Hom}_R(A, A)) = \mathrm{Hom}_R(M^*, R) \simeq M$ where in the second to last equality we have used the hypothesis that $R = \mathrm{End}_R(A)$, and in the last equality we have used the biduality isomorphism from Appendix A.

We also have $\mathrm{Hom}_R(M_1 \cdot A, M_2 \cdot A) = \mathrm{Hom}_R(M_2, \mathrm{Hom}_R(M_1 \cdot A, A)) = \mathrm{Hom}_R(M_2, M_1)$. □

References

[Bas63] H. Bass. "On the ubiquity of Gorenstein rings". In: *Mathematische Zeitschrift* 82.1 (1963), pp. 8–28 (cit. on pp. 6, 43, 44).

[BDD+24] A. Basso, L. De Feo, P. Dartois, A. Leroux, L. Maino, G. Pope, D. Robert, and B. Wesolowski. "SQIsign2D-West: The Fast, the Small, and the Safer". Accepted for publication at Asiacrypt 2024. Aug. 2024. URL: http://www.normalesup.org/~robert/pro/publications/articles/sqisign2d.pdf. eprint: 2024/760. (Cit. on pp. 34, 38, 41).

[BKM23] J. Bergström, V. Karemaker, and S. Marseglia. "Polarizations of abelian varieties over finite fields via canonical liftings". In: *International Mathematics Research Notices* 2023.4 (2023), pp. 3194–3248 (cit. on p. 3).

[BKM24] J. Bergström, V. Karemaker, and S. Marseglia. "Abelian varieties over finite fields with commutative endomorphism algebra: theory and algorithms". In: *arXiv preprint arXiv:2409.08865* (2024) (cit. on p. 3).

[BDLS20] D. Bernstein, L. De Feo, A. Leroux, and B. Smith. "Faster computation of isogenies of large prime degree". In: *Algorithmic Number Theory Symposium (ANTS XIV)*. Vol. 4. 1. Mathematical Sciences Publishers, 2020, pp. 39–55. arXiv: 2003.10118. URL: https://msp.org/obs/2020/4/p04.xhtml (cit. on p. 40).

[BS20] X. Bonnetain and A. Schrottenloher. "Quantum security analysis of CSIDH". In: *Advances in Cryptology–EUROCRYPT 2020: 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10–14, 2020, Proceedings, Part II 30*. Springer. 2020, pp. 493–522 (cit. on p. 1).

[CD23] W. Castryck and T. Decru. "An efficient key recovery attack on SIDH". In: Springer-Verlag (Eurocrypt 2023), Apr. 2023, pp. 423–447. DOI: 10.1007/978-3-031-30589-4_15 (cit. on p. 2).

[CDV20] W. Castryck, T. Decru, and F. Vercauteren. "Radical isogenies". In: *International Conference on the Theory and Application of Cryptology and Information Security (Asiacrypt)*. Lecture Notes in Computer Sciencie 12492. Springer. 2020, pp. 493–519 (cit. on p. 40).

[CLMPR18] W. Castryck, T. Lange, C. Martindale, L. Panny, and J. Renes. "CSIDH: an efficient post-quantum commutative group action". In: *International Conference on the Theory and Application of Cryptology and Information Security (Asiacrypt 2018)*. Springer. 2018, pp. 395–427 (cit. on p. 1).

[CPV20] W. Castryck, L. Panny, and F. Vercauteren. "Rational isogenies from irrational endomorphisms". In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2020, pp. 523–548 (cit. on pp. 28, 30, 33, 34, 41).

[CS15] T. Centeleghe and J. Stix. "Categories of abelian varieties over finite fields, I: Abelian varieties over p". In: *Algebra & Number Theory* 9.1 (2015), pp. 225–265 (cit. on p. 3).

[CS23] T. G. Centeleghe and J. Stix. "Categories of abelian varieties over finite fields II: Abelian varieties over F q and Morita equivalence". In: *Israel Journal of Mathematics* 257.1 (2023), pp. 103–170 (cit. on p. 3).

[CII+23] M. Chen, M. Imran, G. Ivanyos, P. Kutas, A. Leroux, and C. Petit. "Hidden stabilizers, the isogeny to endomorphism ring problem and the cryptanalysis of pSIDH". In: *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 2023, pp. 99–130 (cit. on pp. 34, 36).

[CR24] M. Corte-Real Santos and K. Reijnders. *Return of the Kummer: a toolbox for genus 2 cryptography*. Cryptology ePrint Archive, Paper 2024/948. 2024. URL: https://eprint.iacr.org/2024/948 (cit. on pp. 31, 40).

[Cos18] C. Costello. "Computing supersingular isogenies on Kummer surfaces". In: *Advances in Cryptology–ASIACRYPT 2018: 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2–6, 2018, Proceedings, Part III 24*. Springer. 2018, pp. 428–456 (cit. on pp. 31, 40).

[Cou06] J. M. Couveignes. "Hard Homogeneous Spaces." In: *IACR Cryptology ePrint Archive* 2006 (2006), p. 291 (cit. on pp. 1, 4).

[Dar24] P. Dartois. "Fast computation of 2-isogenies in dimension 4 with the theta model and cryptographic applications". 2024 (cit. on p. 39).

[DLRW24] P. Dartois, A. Leroux, D. Robert, and B. Wesolowski. "SQISignHD: New Dimensions in Cryptography". In: Lecture Notes in Computer Science 14651 (May 2024). Ed. by M. Joye and G. Leander, pp. 3–32. DOI: 10.1007/978-3-031-58716-0_1. URL: http://www.normalesup.org/~robert/pro/publications/articles/SQISignHD.pdf. eprint: 2023/436, HAL: hal-04056062v1, artifact: https://artifacts.iacr.org/tches/2022/a11. (Cit. on p. 41).

[DMPR24] P. Dartois, L. Maino, G. Pope, and D. Robert. "An Algorithmic Approach to (2, 2)-isogenies in the Theta Model and Applications to Isogeny-based Cryptography". Accepted for publication at Asiacrypt 2024. Aug. 2024. URL: http://www.normalesup.org/

~robert/pro/publications/articles/_2_2__isogenies_in_the_theta_model.pdf. eprint: 2023/1747. (Cit. on p. 39).

[DDF+21] L. De Feo, C. Delpech de Saint Guilhem, T. B. Fouotsa, P. Kutas, A. Leroux, C. Petit, J. Silva, and B. Wesolowski. "Séta: Supersingular encryption from torsion attacks". In: *International Conference on the Theory and Application of Cryptology and Information Security (Asiacrypt 2021)*. Springer. 2021, pp. 249–278 (cit. on p. 4).

[DJP14] L. De Feo, D. Jao, and J. Plût. "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies". In: *Journal of Mathematical Cryptology* 8.3 (2014), pp. 209–247 (cit. on p. 2).

[DKS18] L. De Feo, J. Kieffer, and B. Smith. "Towards practical key exchange from ordinary isogeny graphs". In: *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 2018, pp. 365–394. arXiv: 1809.07543 (cit. on p. 1).

[DKLPW20] L. De Feo, D. Kohel, A. Leroux, C. Petit, and B. Wesolowski. "SQISign: compact post-quantum signatures from quaternions and isogenies". In: *International Conference on the Theory and Application of Cryptology and Information Security (Asiacrypt 2020)*. Springer. 2020, pp. 64–93 (cit. on p. 12).

[DG16] C. Delfs and S. D. Galbraith. "Computing isogenies between supersingular elliptic curves over Fp". In: *Designs, Codes and Cryptography* 78 (2016), pp. 425–440 (cit. on p. 35).

[Del69] P. Deligne. "Variétés abéliennes ordinaires sur un corps fini". In: *Inventiones Mathematicae* 8.3 (1969), pp. 238–243 (cit. on p. 3).

[DA70] M. Demazure and M. Artin. *Schémas en groupes (SGA3)*. Springer Berlin, Heidelberg, New York, 1970 (cit. on p. 44).

[EHLMP18] K. Eisenträger, S. Hallgren, K. Lauter, T. Morrison, and C. Petit. "Supersingular isogeny graphs and endomorphism rings: reductions and solutions". In: *Advances in Cryptology–EUROCRYPT 2018: 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29-May 3, 2018 Proceedings, Part III 37*. Springer. 2018, pp. 329–368 (cit. on p. 36).

[EL24] J. K. Eriksen and A. Leroux. "Computing orientations from the endomorphism ring of supersingular curves and applications". In: *Cryptology ePrint Archive* (2024) (cit. on p. 28).

[Gir68] J. Giraud. "Remarque sur une formule de Shimura-Taniyama". In: *Inventiones mathematicae* 5.3 (1968), pp. 231–236 (cit. on p. 3).

[How95] E. Howe. "Principally polarized ordinary abelian varieties over finite fields". In: *American Mathematical Society* 347.7 (1995) (cit. on p. 3).

[JD11] D. Jao and L. De Feo. "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies". In: *International Workshop on Post-Quantum Cryptography (PQCrypto 2011)*. Springer. 2011, pp. 19–34 (cit. on p. 2).

[JKP+18] B. W. Jordan, A. G. Keeton, B. Poonen, E. M. Rains, N. Shepherd-Barron, and J. T. Tate. "Abelian varieties isogenous to a power of an elliptic curve". In: *Compositio Mathematica* 154.5 (2018), pp. 934–959 (cit. on pp. 3, 5, 6, 13–17, 19, 20, 27).

[Kan11] E. Kani. "Products of CM elliptic curves". In: *Collectanea mathematica* 62.3 (2011), pp. 297–339 (cit. on p. 3).

[Kir16] M. Kirschmer. "Definite quadratic and hermitian forms with small class number". In: *Habilitation, RWTH Aachen University* (2016) (cit. on p. 9).

[KNRR21] M. Kirschmer, F. Narbonne, C. Ritzenthaler, and D. Robert. "Spanning the isogeny class of a power of an elliptic curve". In: *Mathematics of Computation* 91.333 (Sept. 2021), pp. 401–449. DOI: 10.1090/mcom/3672. arXiv: 2004.08315. URL: http://www.normalesup.org/~robert/pro/publications/articles/algebraic_obstruction.pdf. HAL: hal-02554714. (Cit. on pp. 3, 6, 7, 9, 10, 18, 20).

[Kup05] G. Kuperberg. "A subexponential-time quantum algorithm for the dihedral hidden subgroup problem". In: *SIAM Journal on Computing* 35.1 (2005), pp. 170–188 (cit. on p. 1).

[KMPW21] P. Kutas, S.-P. Merz, C. Petit, and C. Weitkämper. "One-way functions and malleability oracles: Hidden shift attacks on isogeny-based protocols". In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2021, pp. 242–271 (cit. on p. 4).

[KP23] P. Kutas and C. Petit. "Torsion point attacks on 'SIDH-like'cryptosystems". In: *IET Information Security* 17.2 (2023), pp. 161–170 (cit. on p. 4).

[LS01] K. Lauter and J.-P. Serre. "The maximum or minimum number of rational points on curves of genus three over finite fields". In: *arXiv preprint math/0104086* (2001) (cit. on pp. 18–20).

[Len96] H. Lenstra Jr. "Complex multiplication structure of elliptic curves". In: *journal of number theory* 56.2 (1996), pp. 227–241 (cit. on p. 20).

[LW85] L. S. Levy and R. Wiegand. "Dedekind-like behavior of rings with 2-generate ideals". In: *Journal of Pure and Applied Algebra* 37 (1985), pp. 41–58 (cit. on p. 6).

[MS24] J. Macula and K. E. Stange. "Extending class group action attacks via sesquilinear pairings". In: *arXiv preprint arXiv:2406.10440* (2024) (cit. on p. 35).

[MMPPW23] L. Maino, C. Martindale, L. Panny, G. Pope, and B. Wesolowski. "A direct key recovery attack on SIDH". In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2023, pp. 448–471 (cit. on p. 2).

[MW23] A. H. L. Merdy and B. Wesolowski. "The supersingular endomorphism ring problem given one endomorphism". In: *arXiv preprint arXiv:2309.11912* (2023) (cit. on p. 36).

[Mil72] J. S. Milne. "On the arithmetic of abelian varieties". In: (1972) (cit. on pp. 30, 33).

[MOT20] T. Moriya, H. Onuki, and T. Takagi. "SiGamal: a supersingular isogeny-based PKE and its application to a PRF". In: *Advances in Cryptology–ASIACRYPT 2020: 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7–11, 2020, Proceedings, Part II 26*. Springer. 2020, pp. 551–580 (cit. on p. 11).

[Mum70] D. Mumford. *Abelian varieties*. Tata Institute of Fundamental Research Studies in Mathematics, No. 5. Published for the Tata Institute of Fundamental Research, Bombay, 1970, pp. viii+242 (cit. on pp. 17–19).

[nLa24a] nLab authors. *action of a monoidal category*. Revision 30. Sept. 2024. URL: https://ncatlab.org/nlab/show/action+of+a+monoidal+category (cit. on p. 12).

[nLa24b] nLab authors. *stuff, structure, property*. Oct. 2024. URL: https://ncatlab.org/nlab/show/stuff%2C+structure%2C+property (cit. on p. 13).

[nLa24c] nLab authors. *symmetric monoidal category*. Revision 54. Sept. 2024. URL: https://ncatlab.org/nlab/show/symmetric+monoidal+category (cit. on p. 10).

[PR23a] A. Page and D. Robert. "Clapotis: Evaluating the isogeny class group action in polynomial time". Nov. 2023. URL: http://www.normalesup.org/~robert/pro/publications/articles/group_action.pdf. In preparation. (Cit. on pp. 3, 6, 19, 20, 23, 42).

[PR23b] A. Page and D. Robert. "Introducing Clapoti(s): Evaluating the isogeny class group action in polynomial time". Nov. 2023. URL: http://www.normalesup.org/~robert/pro/publications/articles/clapotis.pdf. eprint: 2023/1766. (Cit. on pp. 19, 20, 23).

[PW24] A. Page and B. Wesolowski. "The supersingular endomorphism ring and one endomorphism problems are equivalent". In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2024, pp. 388–417 (cit. on pp. 4, 34, 35).

[Pei20] C. Peikert. "He gives C-sieves on the CSIDH". In: *Annual international conference on the theory and applications of cryptographic techniques*. Springer. 2020, pp. 463–492 (cit. on p. 1).

[Rob22a] D. Robert. "Evaluating isogenies in polylogarithmic time". Aug. 2022. URL: http://www.normalesup.org/~robert/pro/publications/articles/polylog_isogenies.pdf. eprint: 2022/1068, HAL: hal-03943970. (Cit. on p. 27).

[Rob22b] D. Robert. "Some applications of higher dimensional isogenies to elliptic curves (overview of results)". Dec. 2022. URL: http://www.normalesup.org/~robert/pro/publications/articles/isogenies_applications.pdf. eprint: 2022/1704, HAL: hal-03943973. (Cit. on p. 23).

[Rob23] D. Robert. "Breaking SIDH in polynomial time". In: *Eurocrypt 2023* (Apr. 2023). Ed. by C. Hazay and M. Stam, pp. 472–503. DOI: 10.1007/978-3-031-30589-4_17. URL: http://www.normalesup.org/~robert/pro/publications/articles/breaking_sidh.pdf. eprint: 2022/1038, HAL: hal-03943959, Slides: 2023-04-Eurocrypt.pdf (15 min, Eurocrypt 2023, April 2023, Lyon, France). (Cit. on p. 2).

[Rob24a] D. Robert. "From ideals to modules for isogeny based cryptography". Leuven isogeny days 5, Leuven. Sept. 2024. URL: http://www.normalesup.org/~robert/pro/publications/slides/2024-09-Leuven.pdf (cit. on pp. 3, 6, 20, 21, 42, 43).

[Rob24b] D. Robert. "On the efficient representation of isogenies (a survey)". June 2024. URL: http://www.normalesup.org/~robert/pro/publications/articles/isogeny_survey.pdf. eprint: 2024/1071. (Cit. on pp. 3, 23, 25–27).

[RS06] A. Rostovtsev and A. Stolbunov. "Public-key cryptosystem based on isogenies". In: *International Association for Cryptologic Research. Cryptology ePrint Archive* (2006). eprint: http://eprint.iacr.org/2006/145 (cit. on p. 1).

[Ryd13] D. Rydh. "Existence and properties of geometric quotients". In: *Journal of Algebraic Geometry* 22.4 (May 13, 2013), pp. 629–669. ISSN: 1056-3911, 1534-7486. DOI: 10.1090/S1056-3911-2013-00615-3. arXiv: 0708.3333 (cit. on p. 44).

[Sch03] J. Scholten. "Weil restriction of an elliptic curve over a quadratic extension". In: *Preprint, available at http://homes. esat. kuleuven. be/~ jscholte/weilres. pdf* (2003) (cit. on p. 31).

[SHOR20] J.-P. Serre, E. W. Howe, J. Oesterle, and C. Ritzenthaler. *Rational points on curves over finite fields*. Société mathématique de France, 2020 (cit. on pp. 3, 18).

[Sta24] K. E. Stange. "Sesquilinear pairings on elliptic curves". In: *arXiv preprint arXiv:2405.14167* (2024) (cit. on p. 42).

[Vas68] W. V. Vasconcelos. "Reflexive modules over Gorenstein rings". In: *Proceedings of the American Mathematical Society* 19.6 (1968), pp. 1349–1355 (cit. on p. 43).

[Wat69] W. Waterhouse. "Abelian varieties over finite fields". In: *Ann. Sci. Ecole Norm. Sup* 2.4 (1969), pp. 521–560 (cit. on pp. 3, 44).

[Wes22a] B. Wesolowski. "Orientations and the supersingular endomorphism ring problem". In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2022, pp. 345–371 (cit. on pp. 4, 28, 34).

[Wes22b] B. Wesolowski. "The supersingular isogeny path and endomorphism ring problems are equivalent". In: *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*. IEEE. 2022, pp. 1100–1111 (cit. on pp. 34, 36).

[Wes24] B. Wesolowski. "Random Walks in Number-theoretic Cryptology". HDR. Aug. 2024. URL: https://www.bweso.com/hdr.pdf (cit. on p. 34).

[Yu12] C.-F. Yu. "Superspecial abelian varieties over finite prime fields". In: *Journal of Pure and Applied Algebra* 216.6 (2012), pp. 1418–1427 (cit. on pp. 3, 5).

INRIA Bordeaux–Sud-Ouest, 200 avenue de la Vieille Tour, 33405 Talence Cedex FRANCE
Email address: damien.robert@inria.fr
URL: http://www.normalesup.org/~robert/

Institut de Mathématiques de Bordeaux, 351 cours de la liberation, 33405 Talence cedex FRANCE