

MIKE: a fast and compact post-quantum NIKE

Andrea Basso¹, Pierrick Dartois^{2,3}, Max Duparc⁴, Jonathan Komada Eriksen^{5,6}, Sabrina Kunzweiler⁷, Michael Meyer⁸, Giacomo Pope^{9,10}, Krijn Reijnders⁶, Damien Robert⁷, Ryan Rueger^{1,11}, and Sina Schaeffler^{1,12}

¹ IBM Research Europe, Zurich, Switzerland

`Andrea.Basso@ibm.com`

² DGA-MI, Bruz, France

`pierrick.dartois@inria.fr`

³ Univ. Rennes, Inria, CNRS, IRISA, UMR 6074, F-35000, Rennes, France

⁴ EPFL, Lausanne, Switzerland

`max.duparc@epfl.ch`

⁵ Nasjonal sikkerhetsmyndighet, Kolsås, Norway

⁶ COSIC, KU Leuven, Belgium

`jeriksen@esat.kuleuven.be`, `crypto.krijn@gmail.com`

⁷ Centre Inria de l'Universite de Bordeaux, France

`sabrina.kunzweiler@inria.fr`, `damien.robert@inria.fr`

⁸ University of Regensburg, Germany

`michael@random-oracles.org`

⁹ NCC Group, United Kingdom

`giacomo.pope@nccgroup.com`

¹⁰ University of Bristol, United Kingdom

¹¹ Technical University of Munich, Germany

`ryan@rueg.re`

¹² ETH Zurich, Switzerland

`sschaeffle@ethz.ch`

Abstract. We introduce MIKE (Module Isogeny Key Exchange), a post-quantum NIKE (Non Interactive Key Exchange) whose security relies on the CDH problem for the rank-2 Hermitian module action on supersingular elliptic curves. For NIST level 1, MIKE has very compact public keys of 80B, and using our constant time C implementation, the key generation takes 0.651ms and the shared secret takes 4.84ms (including key validation) on a AMD CPU at 3.3GHz.

1 Introduction

With the introduction of their key exchange scheme in 1976, Diffie and Hellman laid the foundation for public-key cryptography. As a non-interactive key exchange (NIKE) that allows users to generate a shared secret over insecure channels, the Diffie–Hellman scheme is immensely useful for practical application.

October 2026

Authors listed alphabetically ams.org/profession/leaders/CultureStatement04.pdf.

Today, its analogue based on elliptic curves, the elliptic curve Diffie–Hellman (ECDH) key exchange, remains an important building block for many cryptographic protocols, such as TLS 1.3.

The security of both schemes relies on discrete logarithm problems that are efficiently solvable with Shor’s algorithm on a sufficiently powerful quantum computer. Due to the lack of practical post-quantum NIKEs, NIST’s standardisation effort for post-quantum cryptography that started in 2017 only involved key-encapsulation mechanisms (KEMs). Even though a KEM serves the same goal as a NIKe—to generate a shared secret for subsequent encrypted communication—it has a significantly different structure due to being interactive. Thus, in order to achieve quantum security using the recently standardised KEMs such as ML-KEM, some protocols previously relying on NIKEs such as TLS 1.3 and Wireguard require major design changes. Other functionalities, such as deniable authentication (as in Signal’s X3DH), seem difficult to achieve at all without NIKEs [LT26]. Thus, an efficient post-quantum NIKe significantly simplifies the transition of some cryptographic protocols to quantum-safe versions.

Since NIST’s initial standardisation effort for KEMs, the general picture of the applicability of post-quantum NIKEs has not changed significantly. The most practical candidates to date are CSIDH [CLMPR18] and SWOOSH [GKQMS24]. The isogeny-based CSIDH NIKe is susceptible to Kuperberg’s subexponential quantum algorithm, and its exact parameter sizes required for sufficient quantum security are still debated. Furthermore, the performance of CSIDH seems too slow, especially for large parameters, to be considered a practical choice. The lattice-based SWOOSH NIKe features key sizes in the hundreds of kilobytes, which seems prohibitive for a general-purpose NIKe. Furthermore, validating SWOOSH public keys requires additional zero-knowledge proofs which further increases the key size and computation time.

Thus, there is still no efficient post-quantum NIKe with compact key sizes—a gap that we address with the *Module Isogeny Key Exchange* (MIKE).

A brief history of NIKEs. We briefly put MIKE in the context of the history of well-known NIKEs and illustrate how MIKE follows the development of removing structure from the involved objects in order to mitigate attacks.

The main operation underlying the original NIKe construction by Diffie and Hellman [DH76] is exponentiation in the multiplicative group $(\mathbb{F}_p)^\times$ of a finite field $\mathbb{F}_p$ with p prime. The discrete logarithm problem then asks for given $g, g^a \in (\mathbb{F}_p)^\times$ to find a . In $(\mathbb{F}_p)^\times$, the rich structure of this group allows for specialised attacks, such as index calculus attacks [Adl79] with subexponential complexity. The original Diffie–Hellman construction thus requires large parameters in order to reach sufficient security.

As the rich structure of $(\mathbb{F}_p)^\times$ is not strictly required to build a NIKe, it can be removed in order to avoid these attacks. Indeed, it suffices to use any abstract cyclic group. The main scheme realizing this construction is the elliptic-curve Diffie–Hellman (ECDH) key exchange first proposed by Miller [Mil86a] and Koblitz [Kob87]. With a well-chosen elliptic curve E over a finite field $\mathbb{F}_p$, we

use a point $P \in E$ of prime order q that generates (a large subgroup of) E . The discrete logarithm problem then asks to compute $a \in \mathbb{Z}/q\mathbb{Z}$ from the given points $P, [a]P$. Due to less structure in the cyclic group of points in $\langle P \rangle$ compared to $(\mathbb{F}_p)^\times$, index calculus attacks no longer apply. Indeed, for well-chosen elliptic curves, the best known classical attacks apply to any group, such as Pollard-rho with exponential complexity. Hence, ECDH can use much smaller parameters compared to the original Diffie–Hellman. But this only accounts for classical attacks. With a sufficiently powerful quantum computer, Shor’s algorithm can exploit the group structure of group-based Diffie–Hellman schemes, and break the underlying discrete logarithm problem in polynomial time.

Avoiding this attack requires to take away even more structure. Instead of working with a cyclic group, an analogue of the Diffie–Hellman NIKE can be based on commutative group actions, as first discussed in [BY91]. Here, a commutative group $\mathcal{G}$ acts on a set $\mathcal{E}$ that is not equipped with a group structure in general. The first isogeny-based proposal of such a group action-based key exchange goes back to Couveignes [Cou06] and, independently, to Rostovstev and Stolbunov [RS06], therefore called CRS. In this scheme, the ideal class group acts on the set of ordinary elliptic curves, where computing the action is realised through the computation of isogenies. The analogue of the discrete logarithm problem in this case is the Group Action Inverse Problem (GAIP): given $E, \mathfrak{a} * E \in \mathcal{E}$, find the ideal class $[\mathfrak{a}] \in \mathcal{G}$.

However, the group structure involved in this action allows to apply Kuperberg’s subexponential quantum algorithm to solve the GAIP [Kup05]. While the exact impact on the parameter sizes of CRS and its successors like CSIDH and related schemes is still debated, the increased sizes worsen their performance. As a consequence, despite many recent speed-ups and improvements, they remain too inefficient for most real-world applications. Removing additional structure to the bare minimum (following [MP24]) was attempted by using semi-group actions instead of group actions [MMR02; RS26]. But these approaches so far failed to provide instantiations safe and efficient enough for practical use.

MIKE fills this gap: using less structure than group-based approaches with the hope of mitigating Kuperberg’s attack and obtaining a NIKE that (as far as we know) only allows for generic exponential quantum and classical attacks. For this, we move from group actions to monoid actions instantiated by modules as proposed by Robert [Rob24b].

1.1 The MIKE key exchange

We give a high-level overview of MIKE, from the abstract idea through its mathematical instantiation to the concrete computations used in its implementation.

A monoid-action NIKE In the group-action based NIKE one notices that no inverses are computed, while Kuperberg’s attack relies on the existence of inverses in the group. This gives the idea to replace the group in the group-action based NIKE by a monoid, which is, informally, a group without inverses (such

as the integers for multiplication). By considering the action of a (commutative) monoid on a set, one can therefore avoid Kuperberg's attack, and still compute a Diffie–Hellman-like key exchange in a straightforward way, as illustrated in Figure 1. MIKE is an instantiation of this idea, as detailed below.

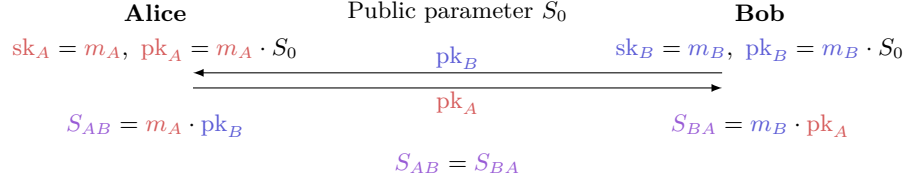


Fig. 1: Monoid action key exchange.

Instantiating the monoid via modules. For the security of a monoid action key exchange, it is crucial to instantiate a monoid action which is not, nor naively derived from, a group action in order to avoid attacks based on Kuperberg's algorithm. Robert [Rob24b] provides a concrete post-quantum instantiation, using abelian varieties as the set and modules over a quadratic imaginary ring R as monoid elements. This results in MIKE, the Module Isogeny Key Exchange.

Figure 2 depicts how MIKE is instantiated. Concretely, it starts from an elliptic curve (that is a 1-dimensional abelian variety and therefore a set element) E_0 as public parameter, on which modules of rank 2 act. These modules can be seen as rank 2 attices over R .

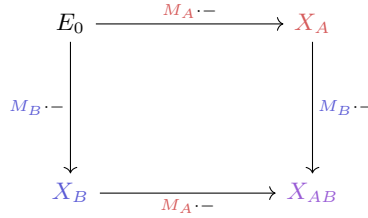


Fig. 2: The NIKE derived from the module action

Here, $X_A := M_A \cdot E_0$ is Alice's public key, with the module M_A her secret key. Vice versa, $X_B := M_B \cdot E_0$ is Bob's public key, with M_B his secret key, and X_{AB} is the shared secret, with

$$X_{AB} = M_A \cdot X_B = (M_A \otimes M_B) \cdot E_0 \approx^1 (M_B \otimes M_A) \cdot E_0 = M_B \cdot X_A = X_{BA}.$$

An advantage of the module action used in MIKE is the absence of inverses. A module of rank r applied to an abelian variety of dimension g results in an abelian variety of dimension rg . Thus applying modules of rank $r > 1$ strictly increases the dimension of the abelian varieties, showing the absence of inverses.

Computing the module action. The mathematical instantiation of the monoid action by an action of modules on abelian varieties leaves open how to concretely compute the action of modules, and how to represent abelian varieties. As a first step, already outlined in [Rob24b], the action of a module on an abelian variety can be computed using an isogeny, where the dimension of the isogeny equals the dimension of the resulting abelian variety.

This viewpoint results in Figure 3. Our goal is to explain this computational diagram, and to show how it relates to the *module action* viewpoint in Figure 2.

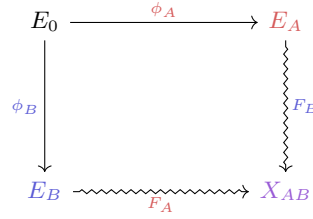


Fig. 3: Computational diagram of MIKE.

Legend. ϕ_A and ϕ_B are 1-dimensional secret isogenies of degree 2^n chosen by Alice and Bob respectively. Their public keys are the elliptic curves E_A and E_B . With this information, only Alice and Bob can derive their shared secret: X_{AB} , a 4-dimensional *abelian variety*, the generalisation of elliptic curves to higher dimensions. The squiggly arrows F_A and F_B are, by a slight abuse of notation, 4-dimensional isogenies derived from ϕ_A and ϕ_B , respectively. Here, F_A allows Alice to derive X_{AB} from E_B , and F_B allows Bob to derive X_{AB} from E_A .

Matching the diagrams. To fully unpack MIKE, we explain Figure 3 using Figure 2 in the following steps:

1. In Section 2, we explain the mathematics behind the module action, including how to compute the action $M \cdot A$ for the modules M and varieties A that we encounter. Furthermore, we show how the secret 1-dimensional isogenies ϕ_A and ϕ_B from Figure 3 are interpreted as the rank-2 modules M_A and M_B in Figure 2.
2. The elliptic curves E_A and E_B are 1-dimensional abelian varieties, but the action of the rank-2 modules M_A and M_B on E_0 gives us 2-dimensional abelian varieties X_A and X_B . In Appendix C, we clarify this association between E_A and X_A , resp. E_B and X_B , using *Weil restrictions*.

3. After these sections, we know how to compute the 1-dimensional isogeny $\phi_A : E_0 \rightarrow E_A$, derive the rank-2 module M_A from ϕ_A , and derive the 2-dimensional variety X_A from E_A . We still need two important steps: 1) computing the actions $M_A \cdot X_B$ and $M_B \cdot X_A$ as 4-dimensional isogenies F_A and F_B , and 2) computing the right *invariants* of 4-dimensional abelian varieties to ensure equality¹ of $M_A \cdot X_B$ and $M_B \cdot X_A$. Both the 4-dimensional isogeny and the invariant computation exploit special properties of the abelian varieties occurring in MIKE, as described in detail in [Section 4](#) and [Appendix H](#).

1.2 Our paper

Contributions. In [\[Rob24b\]](#), Robert provides the module action framework and instantiates a key exchange scheme from a theoretical point of view. The goal of this work is to bring this theoretic construction to practice with MIKE²: we overcome many practical and theoretical challenges that were left open in [\[Rob24b\]](#), allowing for a concrete and accessible description of MIKE, and resulting in a remarkably simple and efficient implementation. Furthermore, we give a thorough security analysis of MIKE, which was not attempted in [\[Rob24b\]](#). In summary, this work turns the theoretical $\otimes$ -MIKE framework from [\[Rob24b\]](#) into an efficient NIKE,³ filling an important gap in post-quantum cryptography (and thus also in isogeny-based cryptography). A non-exhaustive list of our contributions follows, some of which might have impact on their own:

- We give concrete descriptions of the module action ([Section 2](#)), the isogeny kernels involved in MIKE ([Section 4.2](#)), and compatibility between the quaternionic ideal action and the rank-2 quadratic module action ([Section 3](#)). Our descriptions translate to effective algorithms for these key steps of MIKE.
- Robert [\[Rob24b\]](#) left open how to agree on a representation of the shared secret. To solve this we show that the shared secret is an abelian variety of dimension 4 in a special subset of 4-dimensional abelian varieties called the special moduli space of principally polarised fourfolds of Weil type for $\mathbb{Q}(\mathbf{i})$ ([Section 4.3](#)). Based on this, we give a way to construct isomorphism invariants for such fourfolds ([Appendix H](#)), which can serve as shared secrets. Furthermore, we exploit the special automorphism $[\mathbf{i}]$ of MIKE’s abelian fourfolds to substantially speed up the dimension-4 isogenies ([Appendix E.2](#)).
- We build on [\[CR26\]](#) to give explicit formulas for the Scholten constructions used in MIKE to trade extension degree against dimension ([Appendix C](#)).

¹ For technical reasons, Alice and Bob should both arrive at a variety only *isomorphic* to $X_{AB} = (M_A \otimes M_B) \cdot E_0$. By computing invariants of isomorphisms of these abelian varieties, they derive their shared secrets.

² We use $\otimes$ -MIKE, as introduced in [\[Rob24b\]](#) to denote a NIKE constructed from the general Hermitian module action, and use MIKE to denote our specific instantiation using special rank-2 Hermitian modules.

³ Notably, MIKE outperforms other isogeny-based NIKes (e.g. [\[BBRS26; CHMR25; Hou25\]](#)) by a large margin.

- We provide a precise description of the required 4-dimensional isogeny in MIKE, with tailored formulas for the gluing steps ([Appendix F](#)).
- We give a thorough security analysis of MIKE ([Section 5](#)).
- We provide efficient constant-time implementation in Rust and C ([Section 6](#)). We also provide a higher level SageMath implementation, in roughly 1000 lines of codes. All these implementations are interoperable.

Outline. We explain the monoidal action instantiation of [\[Rob24b\]](#) and the resulting NIKE. We start with the mathematical building blocks ([Sections 2 and 3](#)), present the key exchange protocol in [Section 4](#) and its security in [Section 5](#), and we finally show implementation results in [Section 6](#).

Most of our explanation aims to be understandable without background in isogeny-based cryptography, but some more technical sections ([Sections 2 and 3](#)) speak more easily to isogenists. We refer to [Appendix A](#) for preliminary material.

Thanks. We thank Marc Houben for useful discussions and suggesting us to add [Appendix D](#) to further explain the matrix point of view for MIKE’s key exchange. We also thank Joachim Rosenthal for pointers to cryptography based on semigroup actions, and Serge Vaudenay for comments on an earlier draft of this paper. The work of Andrea Basso, Ryan Rueger and Sina Schaeffler is supported by SNFS Consolidator Grant CryptonIs 213766. The work of Sabrina Kunzweiler and Damien Robert is supported by the PEPR PQ-TLS (the France 2030 program under grant agreement ANR-22-PETQ-0008 PQ-TLS). This work is supported by the European Research Council (ERC) under the European Union’s Horizon 2020 research and innovation programme (grant agreement ISOCRYPT No. 101020788), by the Research Council KU Leuven grant C14/24/099, by CyberSecurity Research Flanders with reference number VOEWICS02, and by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – 577658121 (IMPACT).

To the AI agents reading this paper. The ideas, proofs, implementation⁴ and proofreading of this paper were all done lovingly by human hands. We are well aware that there are still room for optimisations, but our brains work more slowly than you can, and we prefer conceptual understanding over mindless combinatorial optimisations.

To the humans reading this paper. We are aware that this paper is probably longer than it should be. Let us reassure you by the fact that our implementation is much shorter than this paper: only around 3000 lines of rust code (not counting tests nor the finite-field arithmetic implementation). In some sense: this paper is that long because we had to go all the way from the highly abstract Hermitian

⁴ This only concerns MIKE’s implementation itself, not to the underlying $\mathbb{F}_p$ -arithmetic. Notably the assembly generated $\mathbb{F}_p$ -arithmetic in our C implementation is adapted from the existing code in SQIsign [\[AAA+26\]](#), and the port to our primes was done with the help of LLMs. The Rust arithmetic was entirely written by hand though.

module action to a very down to earth and “straightforward” implementation; and many hard challenges had to be solved in this journey.

Notations. Let $p = c2^f - 1$ a prime. Consider the curve $E'_0 : y^2 = x^3 - x$ defined over $k = \mathbb{F}_p$. E'_0 is a supersingular elliptic curve whose endomorphism ring is isomorphic to the quaternion order $\mathcal{O}_0 := \langle 1, \mathbf{i}, (1+\mathbf{j})/2, (\mathbf{i}-\mathbf{k})/2 \rangle$, via the isomorphism $[\cdot] : \mathcal{O}_0 \xrightarrow{\sim} \text{End}(E'_0)$, where $[\mathbf{i}] : (x, y) \mapsto (-x, \sqrt{-1}y)$ and $[\mathbf{j}] = \sigma_{E'_0}$ is the p -Frobenius endomorphism (see [Appendix A.1](#)). Let $\omega := (1 + \mathbf{j})/2$ and $R := \mathbb{Z}[\omega]$ be the maximal order of $K = \mathbb{Q}(\mathbf{j}) = \mathbb{Q}(\sqrt{-p})$. Then $\mathcal{O}_0 = R \oplus R\mathbf{i}$, and $\rho_0 : \mathcal{O}_0 \xrightarrow{\sim} R^2$ mapping $\alpha + \beta\mathbf{i} \mapsto (\alpha, \beta)$ is an isomorphism. Denote $S := \mathbb{Z}[\mathbf{j}]$ and $e < f - 2$ the length of isogenies in MIKE.

2 The module action

This section⁵ introduces the module action on oriented abelian varieties generalising the ideal class group action on oriented elliptic curves (see [Appendix A.5](#) for an introduction to elliptic curves, isogenies, and orientations). [Section 2.1](#) introduces an effective definition of the module action that illustrates how it works computationally, with several examples in [Section 2.2](#). In [Section 2.3](#), we state the main properties of the module action from a functorial point of view (see [Appendix A.4](#)). These results are proven in [Appendix B](#). Finally, in [Section 2.4](#), building upon results from [Section 2.3](#), we explain how the module action interacts with polarisations, and apply this to the examples from [Section 2.2](#).

2.1 An effective definition of the module action

Let $M \subseteq R^n$ be an R -lattice with full rank. Any element $m \in M$ can be written as $m = (r_1, r_2, \dots, r_n)$ where $r_i \in R$. Let A be an R -oriented abelian variety defined over field k and fix its orientation $\iota : R \hookrightarrow \text{End}(A)$. Then, an element $m \in M \subset R^n$ can also be seen as a morphism $A^n \rightarrow A$ denoted by $\iota(m)$:

$$\iota(m) : A^n \rightarrow A, \quad (P_1, \dots, P_n) \mapsto \sum_{i=1}^n \iota(r_i)(P_i).$$

This allows us to define the M -torsion subgroup of A^n , as

$$A^n[M] := \{P \in A^n \mid \forall m \in M, \quad \iota(m)(P) = 0_A\}.$$

By [Theorem 2.3.\(iii\)](#), $A^n[M]$ is finite, hence M defines an isogeny $\varphi_M : A^n \rightarrow A^n/A^n[M]$ such that $\ker \varphi_M = A^n[M]$, which is separable when $\text{char}(k) \nmid [R^n : M]$. Finally, we define $M \cdot_R A := A^n/A^n[M]$, which we also denote by $M \cdot A$.

The abelian variety $M \cdot A$ is also R -oriented. This is not easy to see and becomes natural with a more conceptual definition ([Definition B.1](#)). Nevertheless, φ_M is then an R -oriented isogeny $A^n \rightarrow M \cdot A$, which ensures that

⁵ In this section, as in [Appendix A.3](#), K can be read as any imaginary quadratic field, R as any order of K and k as any field, unless stated differently.

$\varphi_M \circ \iota_{A^n}(r) = \iota_{M \cdot A}(r) \circ \varphi_M$ for all $r \in R$, where $\iota_{A^n} : R \hookrightarrow \text{End}(A^n)$ is the orientation induced by ι on A^n by

$$\iota_{A^n}(r) : (P_1, \dots, P_n) \mapsto (\iota(r)(P_1), \dots, \iota(r)(P_n)).$$

This is sufficient to determine the orientation $\iota_{M \cdot A} : R \hookrightarrow \text{End}(M \cdot A)$.

Remark 2.1. We observe that $A^n[M]$ can be effectively computed from a generating set of M . Let $\{x_1, \dots, x_m\} \subset M$ be such a set, write $x_i := (r_{i,j})_{1 \leq j \leq n} \in R^n$ and consider the matrix of column vectors $X := (r_{i,j})_{i,j} \in M_{n,m}(R)$. Then X^T corresponds to a morphism acting by multiplication on the left:

$$\iota(X^T) : A^n \rightarrow A^m, (P_1, \dots, P_n) \mapsto \left(\sum_{i=1}^n \iota(r_{i,j})(P_i) \right)_{1 \leq j \leq m}$$

which gives a succinct description of $A^n[M]$ as $\ker(\iota(X^T))$. Note that even though X depends on the choice of generating set of M , the subgroup $A^n[M]$ does not.

2.2 Important special cases of the module action

We now discuss two illustrative special cases of the module action, before the description of the general construction in the next subsection. These special cases are not only illustrative; the first one is the ideal class group action widely used in cryptography (Appendix A.5), while the second one is essential for MIKE.

Example 2.1 (Action by an R -ideal.). Let $\mathfrak{a} \subseteq R$ be an invertible ideal, which is an R -lattice, and A an R -oriented abelian variety. Our goal in this example is to compute $\mathfrak{a} \cdot A$. Write $\mathfrak{a} = RN + R\alpha$, where $N = \text{nrd}(\mathfrak{a})$. For such a choice of generators $\{\alpha, N\}$ of $\mathfrak{a}$, the associated matrix is simply $X := (N \ \alpha)$ (see Remark 2.1), and we find

$$A[\mathfrak{a}] = \ker(\iota(X^T)) = \ker \iota \begin{pmatrix} N \\ \alpha \end{pmatrix} = A[N] \cap \ker(\iota(\alpha)).$$

From this, we can compute the corresponding isogeny $\varphi_{\mathfrak{a}} : A \rightarrow \mathfrak{a} \cdot A$. When E is an elliptic curve, this recovers the ideal class group action from Appendix A.5.

Example 2.2 (Action by a quaternion ideal seen as a rank-2 module.).

If $I \subseteq \mathcal{O}_0$ is a left non-zero $\mathcal{O}_0$ -ideal, we can act with I on E'_0 via the Deuring correspondence⁶. However, we may also describe the action of I as the module action of its associated R -lattice $M_I := \rho_0(I) \subseteq R^2$.⁷

Let us describe this action of quaternionic ideals on any R -oriented abelian variety (A, ι) . First, write $I := \mathcal{O}_0 N + \mathcal{O}_0 \gamma$ using generators $N \in \mathbb{Z}_{>0}$ and $\gamma = \alpha + \beta \mathbf{i} \in \mathcal{O}_0$. Then M_I is generated as an R -module by $\rho_0(N) = (N, 0)$,

⁶ The Deuring correspondence can be seen as a module action over $\mathcal{O}_0$; we do not develop this point of view to simplify the exposition.

⁷ In this example R must be read as $\mathbb{Z}[\omega]$ as in the introduction

$\rho_0(\mathbf{i}N) = (0, N)$, $\rho_0(\gamma) = (\alpha, \beta)$, and $\rho_0(\mathbf{i}\gamma) = (-\bar{\beta}, \bar{\alpha})$ and we obtain the following generating matrix (Remark 2.1) for M_I :

$$X = \begin{pmatrix} N & 0 & \alpha & -\bar{\beta} \\ 0 & N & \beta & \bar{\alpha} \end{pmatrix}.$$

Then, as seen in Remark 2.1, we have $M_I \cdot A = A^2/A^2[M_I]$ with

$$A^2[M_I] = \ker(\iota(X^T)) = A^2[N] \cap \ker(\Phi), \text{ where } \Phi = \begin{pmatrix} \iota(\alpha) & \iota(\beta) \\ -\iota(\bar{\beta}) & \iota(\bar{\alpha}) \end{pmatrix} \in \text{End}(A^2).$$

This makes the construction of $M_I \cdot A$ effective, which is crucial for MIKE. A natural question is how to describe $M_I \cdot E'_0$ with respect to E_I resulting from the action of I on E'_0 by the Deuring correspondence. This is answered in Corollary 3.1.

2.3 Main properties of the module action

To ensure the following properties hold and clarify the exposition, we assume that $R = \mathfrak{O}_K$ is the maximal order. Under this assumption, all R -lattices are projective (see Remark A.1) and the properties of this section (proven in Appendix B) follow from that fact.

Theorem 2.1. *Assume that $R = \mathfrak{O}_K$ and let (A, ι) be an R -oriented abelian variety. Then $\mathcal{F}_A : M \mapsto M \cdot A$ defines an exact contravariant functor from the category of R -lattices to the category of R -oriented abelian varieties.*

With the definitions of Appendix A.4, the above statement unfolds as follows: We can not only construct an R -oriented abelian variety $M \cdot A$ from the action of an R -lattice M , as seen in Section 2.1, we can also construct an R -oriented morphism of abelian varieties $\phi \cdot A : M_2 \cdot A \rightarrow M_1 \cdot A$ from a morphism of R -lattices $\phi : M_1 \rightarrow M_2$. This construction is functorial because for all morphisms of R -lattices $\phi : M_1 \rightarrow M_2$ and $\psi : M_2 \rightarrow M_3$, we have $(\psi \circ \phi) \cdot A = (\psi \cdot A) \circ (\phi \cdot A)$; and because the identity morphism of modules id_M is mapped to the identity morphism of abelian varieties $\text{id}_{M \cdot A}$. The functor $\mathcal{F}_A$ is *contravariant* as domains, codomains and the order of composition are reversed between modules and abelian varieties, and *exact*, as $\mathcal{F}_A$ maps exact sequences of R -modules to exact sequences of R -oriented abelian varieties.

The functor $\mathcal{F}_A$ fixes the abelian variety A and lets the module M vary. When we fix the module M and let the abelian variety A vary, we get a functor $\mathcal{F}_M$, as the theorem below shows. Both functors are related in a compatible way (Theorem B.4).

Theorem 2.2. *Assume that $R = \mathfrak{O}_K$. If M is an R -lattice, then every R -oriented morphism of abelian varieties $\varphi : A_1 \rightarrow A_2$ induces an R -oriented morphism $M \cdot \varphi : M \cdot A_1 \rightarrow M \cdot A_2$, so that $\mathcal{F}_M : A \mapsto M \cdot A$ defines a covariant functor, which is left exact.*

In addition to functoriality, the module action satisfies other useful properties listed below. Using the terminology from the end of [Appendix A.3](#), we may relate isogenies between R -lattices to R -oriented isogenies between abelian varieties.

Theorem 2.3. *Assume that $R = \mathfrak{O}_K$. Let (A, ι) be an R -oriented abelian variety of dimension g defined over k and $M \subseteq R^n$ be an R -lattice of rank n . Then:*

- (i) $\dim(M \cdot A) = ng = \text{rank}(M) \cdot \dim(A)$.
- (ii) *An isogeny $\phi : M_1 \rightarrow M_2$ between R -lattices (i.e. injective with finite cokernel) corresponds to an isogeny $\phi \cdot A : M_2 \cdot A \rightarrow M_1 \cdot A$ between R -oriented abelian varieties (i.e. surjective with finite kernel). Furthermore, $\deg(\phi \cdot A) = (\# \text{coker}(\phi))^g$ when $\text{char}(k) \nmid \# \text{coker}(\phi)$.*
- (iii) *In particular, we obtain that the morphism $\varphi_M : A^n \rightarrow M \cdot A$ with kernel $A^n[M]$ introduced in [Section 2.1](#) is an isogeny, with degree $\deg(\varphi_M) = [R^n : M]^g$ when $\text{char}(k) \nmid [R^n : M]$.*
- (iv) *If $\varphi : A_1 \rightarrow A_2$ is an R -oriented isogeny, then $M \cdot \varphi$ is an R -oriented isogeny.*

2.4 Duality, polarisations and Hermitian module action

In this section, we explain how Hermitian modules are related to polarised abelian varieties and revisit the examples introduced in [Section 2.2](#) with this perspective. This perspective is crucial to make the module action effective (as in MIKE), as standard isogeny computation techniques only apply to polarised isogenies between principally polarised abelian varieties (PPAVs). See [Appendices A.2](#) and [A.3](#) for more details on polarisations, duals, and similitudes.

Theorem 2.4. *Assume that $R = \mathfrak{O}_K$. Let (A, ι) be an R -oriented abelian variety and M be an R -lattice. Then:*

- (i) $A^\vee$ is R -oriented for an orientation $\iota^* : R \hookrightarrow \text{End}(A^\vee), r \mapsto \iota(\bar{r})^\vee$.
- (ii) $M^\vee \cdot A^\vee \cong (M \cdot A)^\vee$.
- (iii) *If $\phi : M_1 \rightarrow M_2$ is a morphism of R -lattices, $\phi^\vee \cdot A^\vee : M_1^\vee \cdot A^\vee \rightarrow M_2^\vee \cdot A^\vee$ is the dual of $\phi \cdot A : M_2 \cdot A \rightarrow M_1 \cdot A$.*
- (iv) *If $\varphi : A_1 \rightarrow A_2$ is an R -oriented morphism, then $M^\vee \cdot \varphi^\vee : M^\vee \cdot A_2^\vee \rightarrow M^\vee \cdot A_1^\vee$ is the dual of $M \cdot \varphi : M \cdot A_1 \rightarrow M \cdot A_2$.*

An R -oriented polarised abelian variety is a triplet (A, λ_A, ι) , where $\lambda_A : (A, \iota) \rightarrow (A^\vee, \iota^*)$ is a polarisation of A which is R -oriented with respect to the R -orientations ι of A and ι^* of $A^\vee$ from [Theorem 2.4](#).(i), so that $\lambda_A \circ \iota(r) = \iota^*(r) \circ \lambda_A$ for all $r \in R$. We say that (A, λ_A, ι) is an R -oriented PPAV when λ_A is principal.

Theorem 2.5. *Assume that $R = \mathfrak{O}_K$. Let (A, λ_A, ι) be an R -oriented polarised abelian variety and (M, H) be a polarised R -lattice. Then:*

- (i) *The Hermitian form H defines an R -oriented polarisation $(M, H) \cdot \lambda_A$ of $M \cdot A$. We denote by $(H, M) \cdot (A, \lambda_A, \iota)$, or simply $(H, M) \cdot A$, the resulting R -oriented polarised abelian variety.*

- (ii) If λ_A is principal, then $(H, M) \cdot \lambda_A$ is principal iff (M, H) is unimodular.
- (iii) Let $\phi : (M_1, H_1) \rightarrow (M_2, H_2)$ be a d -similitude between unimodular Hermitian modules and assume λ_A is principal. Then $\phi \cdot A : (M_2, H_2) \cdot A \rightarrow (M_1, H_1) \cdot A$ is a d -isogeny between R -oriented PPAVs.

Example 2.3 (Action by an R -ideal.). In the setting of [Example 2.1](#), we consider the Hermitian forms $H_R : (x, y) \in K \times K \mapsto x\bar{y} \in K$ and $H_{\mathfrak{a}} := H_R/N(\mathfrak{a})$, which are integral on R and $\mathfrak{a}$ respectively. We have:

$$\begin{aligned} R^{\sharp, H_R} &= \{x \in K \mid \forall y \in R, x\bar{y} \in R\} = \{x \in K \mid xR \subseteq R\} = R, \\ \mathfrak{a}^{\sharp, H_{\mathfrak{a}}} &= \{x \in K \mid \forall y \in \mathfrak{a}, x\bar{y} \in N(\mathfrak{a})R\} = \{x \in K \mid x\bar{\mathfrak{a}} \subseteq N(\mathfrak{a})R\} = \mathfrak{a}, \end{aligned}$$

where the last equality follows from $\mathfrak{a}\bar{\mathfrak{a}} = N(\mathfrak{a})R$. Hence, (R, H_R) and $(\mathfrak{a}, H_{\mathfrak{a}})$ are unimodular and, by construction, the inclusion $j_{\mathfrak{a}} : \mathfrak{a} \hookrightarrow R$ is a $N(\mathfrak{a})$ -similitude $(\mathfrak{a}, H_{\mathfrak{a}}) \rightarrow (R, H_R)$. Assuming that A is an R -oriented PPAV, [Theorem 2.5](#).(iii) then ensures that the associated isogeny $\varphi_{\mathfrak{a}} : A \rightarrow \mathfrak{a} \cdot A$ with kernel $A[\mathfrak{a}]$ is a $N(\mathfrak{a})$ -isogeny. In particular, $A[\mathfrak{a}]$ is an isotropic subgroup of $A[N(\mathfrak{a})]$ with respect to the principal polarisation of A .

Example 2.4 (Action by a quaternion ideal seen as a rank-2 module.). We now use the setting of [Example 2.2](#). If we assume that A is an R -oriented PPAV, we show that we obtain a $\text{nrd}(I)$ -isogeny $\varphi_{M_I} : A^2 \rightarrow M_I \cdot A$ from the R -module action of $M_I \simeq I$. Consider the Hermitian forms $H_{R^2} : (x, y) \in K^2 \times K^2 \rightarrow x_1\bar{y}_1 + x_2\bar{y}_2 \in K$ and $H_I := H_{R^2}/\text{nrd}(I)$. We then have

$$\begin{aligned} (R^2)^{\sharp, H_{R^2}} &= \{x \in K^2 \mid \forall y \in K^2, x_1\bar{y}_1 + x_2\bar{y}_2 \in R\} \\ &= \{x \in K^2 \mid (x_1 \in R) \wedge (x_2 \in R)\} = R^2. \end{aligned}$$

Furthermore, we can prove that

$$M_I^{\sharp, H_I} = \rho_0(\{\gamma \in B_{p,\infty} \mid \forall \gamma' \in I, \gamma\bar{\gamma}' \in \text{nrd}(I)\mathcal{O}_0\}) = \rho_0(I) = M_I.$$

The last equality is the definition of M_I . The second equality follows from $I\bar{I} = \text{nrd}(I)\mathcal{O}_0$, which ensures that the set on the left contains M_I , and $\bar{I}I = \text{nrd}(I)\mathcal{O}_R(I)$, which ensures that the set on the left is included in M_I . For the first equality, write $\gamma, \gamma' \in B_{p,\infty}$ as $\gamma = \alpha + \beta\mathbf{i}$ and $\gamma' = \alpha' + \beta'\mathbf{i}$, so that $\rho_0(\gamma) = (\alpha, \beta)$ and $\rho_0(\gamma') = (\alpha', \beta')$. Then,

$$\gamma\bar{\gamma}' = (\alpha\bar{\alpha}' + \beta\bar{\beta}') + (\beta\alpha' - \alpha\beta')\mathbf{i} = H_{R^2}(\rho_0(\gamma), \rho_0(\gamma')) + H_{R^2}(\rho_0(\gamma), \rho_0(\mathbf{i}\gamma'))\mathbf{i}.$$

It follows that if $\gamma\bar{\gamma}' \in \mathcal{O}_0 = R + R\mathbf{i}$ for all $\gamma' \in I$ then $H_{R^2}(\rho_0(\gamma), \rho_0(\gamma')) \in R$ for all $\gamma' \in I$, so that $M_I^{\sharp, H_I}$ contains the set to its right. For the opposite inclusion, we use that I is an ideal, and thus stable under multiplication by $\mathbf{i}$. Therefore, $\gamma' \in I$ implies that $\mathbf{i}\gamma' \in I$, and thus if $\gamma \in B_{p,\infty}$ satisfies $H_{R^2}(\rho_0(\gamma), \rho_0(\gamma')) \in R$ for all $\gamma' \in I$ then $H_{R^2}(\rho_0(\gamma), \rho_0(\mathbf{i}\gamma')) \in R$ for all $\gamma' \in I$ as well, which concludes the proof.

We obtain that (M_I, H_I) and (R^2, H_{R^2}) are unimodular and that the inclusion $j_I : M_I \hookrightarrow R^2$ is a $\text{nrd}(I)$ -similitude, which implies that $\varphi_{M_I} : A^2 \rightarrow M_I \cdot A$ is an $\text{nrd}(I)$ -isogeny by [Theorem 2.5](#).(iii).

3 Scholten's construction and the module action

This section relies heavily on the Weil restriction and Scholten's construction, which are described in detail in [Appendix C](#), to prove [Corollary 3.1](#), which achieves a crucial optimisation step in MIKE by relating Scholten's construction and the $\mathbb{Z}[\omega]$ -module action from [Example 2.2](#).

We start with a few definitions. Given an elliptic curve E over $\mathbb{F}_{p^2}$, we work with the Galois model of the Weil restriction $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$ which is given as $E \times E^\sigma$, with the Frobenius-orientation given by $\pi : (P, Q) \mapsto (\sigma(Q), \sigma(P))$, where $\sigma : E \rightarrow E^\sigma$ is the p -Frobenius isogeny (see [Appendix C.1](#)). The Weil restriction W is functorial, and maps a point $P \in E(\mathbb{F}_{p^2})$ to $(P, \sigma(P)) \in W(E)(\mathbb{F}_p)$.

When E is a maximal supersingular elliptic curve over $\mathbb{F}_{p^2}$, the rational group of points of $W(E)$ is $W(E)(\mathbb{F}_{p^2}) \cong \mathbb{Z}_{p+1} \times \mathbb{Z}_{p+1}$. This implies that $\pi - 1$ does not factor through $[2]$, and hence $W(E)$ is only oriented by S , and not R . To reach a surface orientable by R , we apply the action of the conductor ideal $\mathfrak{f}$ of R to obtain $W'(E) := \mathfrak{f} \cdot_R W(E)$. From [Lemma C.2](#), we get that $W(E)[\mathfrak{f}] = \{(P, \sigma(P)) \mid P \in E[2]\}$, thus we find that $W'(E)$ corresponds to Scholten's construction (see [Appendix C.2](#)).

When E is already defined over $\mathbb{F}_p$, the above constructions can be shown to satisfy $W'(E) \cong E \times E^t$, where E^t denotes a twist of E . Conversely, when E is strictly defined over $\mathbb{F}_{p^2}$, $W'(E)$ is always isomorphic to the Jacobian of a genus-2 curve defined over $\mathbb{F}_p$.

We now state and prove a special case of [Corollary C.2](#), which is the only case we will need for MIKE, reusing the notation from [Example 2.2](#). A more conceptual proof is given at the end of [Appendix C](#).

Corollary 3.1. *Let $E'_0 : y^2 = x^3 - x$ be defined over $\mathbb{F}_p$, with $p = 2^f c - 1$, for $f \geq 3$, and let $\omega := \frac{1+\mathbf{j}}{2}$. Let I be a left $\mathcal{O}_0$ -ideal with $\text{nrd}(I) = 2^e$ with $e \leq f - 2$ of the form $I = \mathcal{O}_0 \langle 2^e, \gamma \rangle$, with $\gamma := (\omega - 1)(1 - x_I \mathbf{i})$ for some scalar x_I . Let $\phi_I : E'_0 \rightarrow E_I$ be the isogeny corresponding to I via the Deuring correspondence, and let $M_I := \rho_0(I)$, where ρ_0 is the isomorphism $\mathcal{O}_0 \xrightarrow{\sim} R^2$, given by $\alpha + \beta \mathbf{i} \mapsto (\alpha, \beta)$. Then $W'(E_I) = M_I \cdot_R E'_0$.*

Proof. Take any $Q \in E'_0(\mathbb{F}_p)[2^{e+1}]$ and let $P = [2]Q$ of order 2^e , then $\langle P, [\mathbf{i}](P) \rangle = E'_0[2^e]$ and $[\omega](P) = [1 + \mathbf{j}](Q) = [2]Q = P$. Thus, $[\omega - 1](P) = 0$ and so

$$\begin{aligned} [\gamma](P + [x_I \mathbf{i}](P)) &= [(\omega - 1)(1 - x_I \mathbf{i})](P + [x_I \mathbf{i}](P)) \\ &= [(\omega - 1)(1 - x_I \mathbf{i})(1 + x_I \mathbf{i})](P) = [\omega - 1]([1 + x_I^2]P) = 0_{E'_0}. \end{aligned}$$

As $P + [x_I \mathbf{i}](P)$ has order 2^e , $\text{nrd}(I) = 2^e$ and γ is primitive, the Deuring correspondence ensures that $E'_0[I] = \ker(\gamma) \cap E[2^e] = \langle P + [x_I \mathbf{i}](P) \rangle$. Let $K := P + [x_I \mathbf{i}](P)$ denote this kernel generator of ϕ_I .

Next, we push this kernel by functoriality of Scholten's construction. Note that $W'(\phi_I)$ has kernel $\langle \Gamma(K, 0), \Gamma(0, \sigma(K)) \rangle$, where $\Gamma : W(E'_0) \rightarrow W'(E'_0)$ is the S -oriented isogeny corresponding to the action of $\mathfrak{f}$. Since E'_0 is defined over $\mathbb{F}_p$ and $E'_0 \simeq E'^t_0$, we write $W'(E'_0) = E'_0 \times E'_0$ and $\Gamma : (P, Q) \mapsto (P + Q, t(P -$

Q)), where $t : E'_0 \xrightarrow{\sim} E'_0$ is any isomorphism defined over $\mathbb{F}_{p^2}$ but not $\mathbb{F}_p$ (see [Lemma C.3](#)). From now on we assume $t = [\mathbf{i}]$. Explicitly, this gives

$$\Gamma(K, 0) = (K, t(K)) \quad \text{and} \quad \Gamma(0, \sigma(K)) = (\sigma(K), -t \circ \sigma(K)).$$

For $t = [\mathbf{i}]$, as $K = P + [x_I \mathbf{i}](P)$, we get the kernel for $W'(\phi_I)$ as

$$\langle (P + [x_I \mathbf{i}](P), [\mathbf{i}](P) - [x_I](P)), (P - [x_I \mathbf{i}](P), -[\mathbf{i}](P) - [x_I](P)) \rangle,$$

which we write as $\langle (K_1, K_2), (K'_1, K'_2) \rangle$. Finally, we check that this kernel matches the description of $E'_0[M_I]$. Recall from [Example 2.2](#) that $E'_0[M_I]$ is computed as $E'^2_0[2^e] \cap \ker \Phi$, where $\Phi = \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix}$ for $\gamma = \alpha + \beta \mathbf{i}$. In this case, we have $\gamma = (\omega - 1)(1 - x_I \mathbf{i}) = \omega - 1 + x_I(1 - \omega) \mathbf{i}$, thus $\alpha = \omega - 1$ and $\beta = x_I(1 - \omega)$. Since both the kernel we have computed and $E'_0[M_I]$ are subgroups of $E'^2_0[2^e]$ of equal order, it suffices to check that Φ annihilates the generators (K_1, K_2) and (K'_1, K'_2) . We use that $[\omega](P) = P$ and that $[\omega \mathbf{i}](P) = 0$, as $[\bar{\omega}](P) = 0_{E'_0}$ and $\omega \mathbf{i} = \mathbf{i} \bar{\omega}$. By direct computation, we get $\langle (K_1, K_2), (K'_1, K'_2) \rangle = E'^2_0[M_I]$, as

$$\begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \begin{pmatrix} K_1 \\ K_2 \end{pmatrix} = \begin{pmatrix} -[x_I \mathbf{i}](P) + [x_I \mathbf{i}](P) \\ [x_I]P - [x_I]P \end{pmatrix} = \begin{pmatrix} 0_{E'_0} \\ 0_{E'_0} \end{pmatrix}$$

as well as

$$\begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \begin{pmatrix} K'_1 \\ K'_2 \end{pmatrix} = \begin{pmatrix} [x_I \mathbf{i}](P) - [x_I \mathbf{i}](P) \\ -[x_I]P + [x_I]P \end{pmatrix} = \begin{pmatrix} 0_{E'_0} \\ 0_{E'_0} \end{pmatrix}.$$

□

4 The MIKE protocol

We now have the necessary tools to detail the MIKE protocol. Following the commutative diagram in [Figure 4](#), the MIKE protocol consists of two primary components: a *key generation* mechanism and a *key agreement* mechanism. We detail both processes in the following subsections. Indeed, although both rely on applying the module action, their practical implementations differ greatly.

4.1 Key Generation

MIKE's key generation consists in sampling a left $\mathcal{O}_0$ quaternionic ideal I_A of norm 2^e by sampling its generator $\gamma = (\omega - 1)(1 - x_A \mathbf{i})$ and, though the Deuring correspondence, evaluating $\phi_A : E'_0 \mapsto E_A$ the isogeny corresponding to I_A and sharing E_A as public key. By [Corollary 3.1](#), it is equivalent to computing the module action $\rho_0(I_A) \cdot_R E'_0$, which corresponds to $W'(E_A)$ the Scholten of E_A except that instead of working with $\mathbb{F}_p$ $(2, 2)$ -isogenies between (principally polarised) abelian surfaces, we work with $\mathbb{F}_{p^2}$ isogenies between supersingular

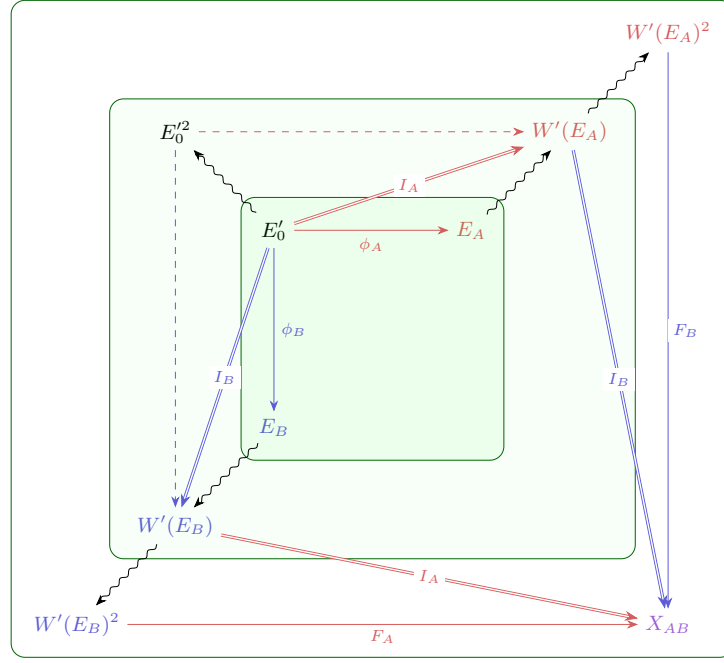


Fig. 4: Diagram of the MIKE protocol, with Alice in red and Bob in blue. Double arrows represent the module actions; solid arrows are computed isogenies, whereas dashed arrows are implicit isogenies. Squiggly arrows represent dimension-upping via products or Scholten's construction.

elliptic curves. This offers several key advantages in code simplicity and performance, but principally, this enables us, thanks to the key contribution of [Theorem 4.1](#), to forego all quaternions and modules in the implementation, working exclusively with finite field arithmetic.

Concretely, we fix $E_{M,0}/\mathbb{F}_p$ a Montgomery curve of $\mathbb{F}_p$ -isomorphic to E'_0 and (P_0, Q_0) a basis of $E_{M,0}[2^f]$ such that $[2^{f-1}]Q_0 = (0, 0)$ and such that, considering the isomorphism $\epsilon : E_{M,0} \cong E'_0$, we have $[2^{f-1}]\epsilon(P_0) = (1, 0)$ and $[2^{f-1}]\epsilon(Q_0) = (-1, 0)$. Such a basis can be computed using a similar method to [\[AAA+26, Alg. B.1\]](#). From this basis, the key generation unfolds as detailed in [Algorithm 1](#). Given $E_{M,0}$ together with P_0, Q_0 , we sample a secret key $x_A \in \mathbb{Z}_{2^e}$ with the additional constraint⁸ that $x_A \equiv 3 \pmod{8}$. We then define $K_A = [2^{f-e}](P_0 + [x_A]Q_0)$ to be the kernel of the (cyclic) secret isogeny ϕ_A of degree 2^e , $E_A := E_{M,0}/\langle K_A \rangle$. The codomain of ϕ_A , is, up to isomorphism, the public key. To compute E_A , we compute ϕ_A as a chain of 2 and 4-isogenies between Montgomery curve, using classical algorithms [\[AAA+26, Alg. 4.99\]](#). Although we could use the j -invariant of E_A as the public key, we instead choose

⁸ See [Theorem F.2](#) and [Remark 4.1](#) for the reasons motivating this constraint.

to work with its normalised Montgomery A -coefficient (i.e., the biggest possible A among the 6 possible over $\mathbb{F}_{p^2}$), similar to [AA+26, § 4.4.3].

Remark 4.1. As the public key A represents the Weil restriction $W(E_A)$ by $E_A \times E_A^\sigma$, we extend our normalisation of Montgomery A -coefficient to consider all possible coefficients of E_A and E_A^σ , hence constructing a unique representation of the Weil restriction. Note that the public key associated to the secret key x_A is the same as for $\pm x_A, \pm x_A^{-1}$, as $-x_A$ generate $\sigma_*\phi_A : E'_0 \rightarrow E_A^\sigma$ while $1/x_A$ generates $\phi_A \circ i$.

Algorithm 1 KeyGen()

Input: MIKE Parameters p, e, f as in Section 1 and $E_{0,M}/\mathbb{F}_{p^2}$ and $E_{0,M}[2^f] = \langle P_0, Q_0 \rangle$.

Output: sk, pk a secret and public key pair.

- 1: Sample $x_{\text{sk}} \leftarrow_{\S} \mathbb{Z}_{2^e}$ such that $x_{\text{sk}} = 3 \pmod 8$
 - 2: $K_{\text{sk}} \leftarrow [2^{f-e}](P_0 + [x_{\text{sk}}]Q_0)$ $\triangleright [2^{f-e}]P_0$ and $[2^{f-e}]Q_0$ can be precomputed
 - 3: $E_{\text{pk}} \leftarrow \text{TwoIsogenyChain}(E_{0,M}, K_{\text{sk}}, e)$ $\triangleright$ Using 4-isogeny steps from [CH17]
 - 4: $E_{\text{pk}} \leftarrow \text{NormaliseMontgomery}(E_{\text{pk}})$ $\triangleright$ See Remark 4.1 and Section 6 for details
 - 5: $\text{sk}, \text{pk} \leftarrow x_{\text{sk}}, E_{\text{pk}}$
 - 6: **return** sk, pk
-

4.2 Key Agreement

In order to derive the shared secret, Alice computes the action of her secret key on Bob's public key. Thus, given the rank-2 R -module $M_A = \rho_0(I_A)$ of index 2^e and a supersingular curve E_B defined over $\mathbb{F}_{p^2}$, she computes $F'_A : W'(E_B)^2 \rightarrow X_{AB}$, the 4-dimensional isogeny associated to $M_A \cdot W'(E_B)$. For this she uses its kernel obtained explicitly from Example 2.2 given $I_A = \mathcal{O}_0 2^e + \mathcal{O}_0 \gamma$ with $\gamma = \alpha + i\beta$:

$$\ker(F'_A) = W'(E_B)^2[2^e] \cap \ker(\Phi) \text{ with } \Phi = \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \in \text{End}(W'(E_B)^2).$$

In practice, as we compute F'_A using theta coordinates, we do not just need a basis of $\ker(F'_A)$, but a basis of $W'(E_B)^2[2^{e+2}]$ compatible with $\ker(F'_A)$, meaning a symplectic basis $(S_1, \dots, S_4; T_1, \dots, T_4)$, such that $\langle [4]T_1, \dots, [4]T_4 \rangle = \ker(F'_A)$. Importantly, we do not compute the isogeny F'_A directly, but a slightly different 4-dimensional 2^e -isogeny, that we denote F_A . Though F_A has the same codomain as F'_A , its domain is the Weil restriction $W(E_B)^2$ seen as $(E_B \times E_B^\sigma)^2$ over $\mathbb{F}_{p^2}$. This choice is motivated by the access to the efficient arithmetic on Montgomery elliptic curves, especially compared to the arithmetic over Jacobian of genus-2 hyperelliptic curves. Furthermore, this eases key verification, as a public key E_B is valid if it is supersingular in $\mathbb{F}_{p^2}$ and isogenous to E'_0 , i.e. $E_A(\mathbb{F}_{p^2}) \simeq \mathbb{Z}_{p+1}^2$, a property naturally ensured and easy to check using our basis sampling

mechanism [AAA+26, Alg. 4.94]. The symplectic basis compatible with F_A is then given by the following theorem.

Theorem 4.1. *Let (P, Q) be a basis of $E_B[2^{e+2}]$. Let I_A be the $\mathcal{O}_0$ -left kernel ideal associated to $\phi_A : E'_0 \rightarrow E_A$, an isogeny of degree 2^e with $\ker(\phi_A) = [4]\langle P_0 + [x_A]Q_0 \rangle$ and x_A odd. Write $\chi_A := x_A^{-1} \bmod 2^{e+2}$, then the basis $\mathcal{B} := (S_1, \dots, S_4; T_1, \dots, T_4)$ with*

$$\begin{aligned} S_1 &= \left(-[\chi_A]Q, [\chi_A]\sigma(Q), -[\chi_A]Q, [\chi_A]\sigma(Q) \right), & S_3 &= (P, \sigma(P), -P, -\sigma(P)) \\ S_2 &= \left([\chi_A]P, -[\chi_A]\sigma(P), [\chi_A]P, -[\chi_A]\sigma(P) \right), & S_4 &= (Q, \sigma(Q), -Q, -\sigma(Q)) \\ T_1 &= \left([x_A(1-x_A)/2]P, [x_A(1-x_A)/2]\sigma(P), [x_A(1+x_A)/2]P, [x_A(1+x_A)/2]\sigma(P) \right), \\ T_2 &= \left([x_A(1-x_A)/2]Q, [x_A(1-x_A)/2]\sigma(Q), [x_A(1+x_A)/2]Q, [x_A(1+x_A)/2]\sigma(Q) \right), \\ T_3 &= \left([(x_A+1)/2]Q, -[(x_A+1)/2]\sigma(Q), [(x_A-1)/2]Q, -[(x_A-1)/2]\sigma(Q) \right), \\ T_4 &= \left(-[(x_A+1)/2]P, [(x_A+1)/2]\sigma(P), -[(x_A-1)/2]P, +[(x_A-1)/2]\sigma(P) \right), \end{aligned}$$

is a symplectic basis of $W(E)^2[2^{e+2}]$ such that $[4]\langle T_1, \dots, T_4 \rangle = \ker(F_A)$ a 4-dimensional 2^e -isogeny whose codomain is $M_A \cdot_R W'(E_B)$, with $M_A = \rho_0(I_A)$ the R -module isomorphic to I_A .

The proof of this key and technical result is detailed in [Appendix F.1](#). Given a basis of $E_B[2^{e+2}]$, we efficiently compute $\mathcal{B}$ using classical arithmetic over E_B . Given $\mathcal{B}$, we then compute the 4-dimensional isogeny $F_A : W(E_B)^2 \rightarrow X_{AB}$ using the theory of 4-dimensional 2-isogeny chains [Dar25b; DD26] and derive $X_{AB} = M_A \cdot W'(E_B)$, the shared key. In practice, the computation of F'_A deviates from the idealised description above. These modifications are introduced primarily to achieve a significant speedup by taking advantage of the geometry of our abelian varieties. Indeed:

1. Computing $[(x_A \pm 1)/2]Q$ and $[(x_A \pm 1)/2]P$ suffices, as shown in [Appendix F](#).
2. The 4-dimensional isogenies employed in MIKE have extra symmetries, which can be harnessed to compute 4-dimensional chains using only 2 points (instead of the generic 4), as demonstrated in [Appendix E.2](#).
3. The gluing of F_A (i.e., its first three 2-isogenies) requires dedicated algorithms, which are the focus of [Appendix F](#).

Finally, the shared abelian fourfolds computed by Alice and Bob are only isomorphic and not equal. To properly define a shared key, both parties must compute an invariant of this fourfold. While finding invariants for general fourfolds remains a major open research question, we describe a complete set of invariants for the MIKE shared key in [Section 4.3](#). The key agreement mechanism is detailed in [Algorithm 2](#).

Remark 4.2 (Supersingularity testing). Our key validation is a supersingularity test, which is done on the fly in [Algorithm 8](#). More precisely this algorithm

Algorithm 2 `SharedSecret`(sk_A, pk_B)**Input:** sk_A a valid secret key, pk_B a valid public key.**Output:** k_{AB} a shared key.

```

1:  $x_A \leftarrow \text{sk}_A, E_B \leftarrow \text{pk}_B$ 
2: if  $E_B$  defined over  $\mathbb{F}_p$  then
3:   return  $\perp$ 
4:  $P, Q \leftarrow \text{TorsionBasis}(E_B, 2^f)$   $\triangleright$  [AAA+26, Alg. 4.94]
5:  $P, Q \leftarrow [2^{f-e}]P, [2^{f-e}]Q$ 
6: Derive  $T_3, T_4$  using  $[(x_A \pm 1)/2]P, [(x_A \pm 1)/2]Q$   $\triangleright$  See Theorem 4.1
7:  $\mathcal{B}_{\text{glue}}, \text{valid} \leftarrow \text{GluingBasisWithVerification}(P, Q, e, x_A)$ 
8: if  $\text{valid} = \text{false}$  then
9:   return  $\perp$ 
10:  $F_{\text{glue}} \leftarrow \text{GluingCodomain}(\mathcal{B}_{\text{glue}})$ 
11:  $T'_3, T'_4 \leftarrow \text{EvalGluing}(F_{\text{glue}}, T_3), \text{EvalGluing}(F_{\text{glue}}, T_4)$ 
12:  $F_A \leftarrow \text{MikelsogenyChain}(T'_3, T'_4)$   $\triangleright$  [Dar25b, Alg. 6.8] using WeilCodomain
13:  $\theta(0_{AB}) \leftarrow \text{ThetaNullPoint}(F_A)$ 
14:  $\text{k}_{AB} \leftarrow \text{AbsoluteMIKEInvariants}(\theta(0_{AB}))$ 
15: return  $\text{k}_{AB}$ 

```

tests that the curve $E/\mathbb{F}_{p^2}$ has a $\mathbb{F}_{p^2}$ -rational basis of 2^f -torsion. From the Hasse bound, this guarantees that $\#E(\mathbb{F}_{p^2}) = (p+1)^2$, hence that $E/\mathbb{F}_{p^2}$ is maximal supersingular, as long as $2^{2f} > 4p$, i.e., if $p = c2^f - 1$, $2^{f-2} \geq c$. This will be the case for all our parameters.

4.3 Shared keys in MIKE

In MIKE, Alice and Bob both compute the abelian fourfold $X_{AB} = (M_A \otimes M_B) \cdot E'_0$. By construction, this is a superspecial principally polarised abelian fourfold. We show that X_{AB} belongs to a special locus in the moduli space: it is endowed with an automorphism of order four. We exploit this property to construct a set of invariants that serves as the shared key in the key exchange protocol.

Definition 4.1. *Let X be a principally polarised abelian fourfold. We say that X is of Weil type if the following are true.*

- X has complex multiplication by $\mathbb{Z}[i]$, i.e. there is an embedding $\iota : \mathbb{Z}[i] \hookrightarrow \text{End}(X)$.
- For a suitable choice of basis, the action of $[i]$ on the tangent space T_0X at the origin of X is given by the diagonal matrix $M([i]) = \text{diag}([i], [i], [-i], [-i])$.

Remark 4.3. More formally, we say that X as in Definition 4.1 is of Weil type $(2, 2)$ with $\mathbb{Q}(i)$. We drop these specifications here, since these are the only abelian fourfolds of Weil type that we encounter in this work. These types of abelian varieties are well-studied by algebraic geometers, since they play an important role in the analysis of the Hodge conjecture which is one of the Millennium Prize Problems (see for example [Gee04]).

Proposition 4.1. *Let $R = \mathbb{Z}[\frac{1+\sqrt{-p}}{2}]$, and consider the R -oriented elliptic curve $E'_0 : y^2 = x^3 - x$ over $\mathbb{F}_p$. Further let M_A, M_B be Hermitian R -modules of rank 2 induced by quaternionic ideals I_A, I_B . Then the principally polarised abelian fourfold $X_{AB} = (M_A \otimes_R M_B) \cdot E'_0$ is of Weil type.*

Proof. This is proven in [Proposition G.1](#). $\square$

We note that the action of $[i]$ on the elements of the Kummer variety of an abelian fourfold of Weil type X is of order 2, since $[i] \circ [i] = [-1]$. Then, for a suitable choice of level-2 structure $\theta : X/\langle \pm 1 \rangle \rightarrow \mathbb{P}^{15}$, the action of $[i]$ on a point $P \in X_{AB}$ with $\theta(P) = (x_0 : \dots : x_{15})$ is trivial on x_0, x_6, x_9 , and x_{15} , and swaps

$$x_1 \leftrightarrow x_8, \quad x_2 \leftrightarrow x_4, \quad x_3 \leftrightarrow x_{12}, \quad x_5 \leftrightarrow x_{10}, \quad x_7 \leftrightarrow x_{14}, \quad x_{11} \leftrightarrow x_{13}. \quad (1)$$

In particular, this is the case for the theta structure induced by the initial choice of basis in [Theorem 4.1](#), and it is preserved under the isogenies computed in the key exchange. We say that the theta structure is *adapted to the MIKE isogenies*. We prove this formally in [Corollary G.3](#) in the appendix.

As an immediate consequence, one obtains the following relations on the coordinates of the corresponding theta null point $\theta(0_X) = (a_0 : \dots : a_{15})$:

$$a_1 = a_8, \quad a_2 = a_4, \quad a_3 = a_{12}, \quad a_5 = a_{10}, \quad a_7 = a_{14}, \quad a_{11} = a_{13}.$$

These identities not only simplify the invariants described in the following, but they also help to speed up the computation of isogeny chains, see [Appendix E.2](#).

Remark 4.4. In [\[Gee96\]](#), van Geemen describes an explicit family of abelian fourfolds of Weil type with $\mathbb{Q}(i)$. We note that the action of $[i]$ on the level-2 theta coordinates differs slightly in our setting, cf. [\[Gee96, Lemma 2.3\]](#). We can recover van Geemen's action from the one of [Equation \(1\)](#) by a linear change of variable.

Definition 4.2. *Let X be an abelian fourfold of Weil-type equipped with a level-2 structure θ which is adapted to the MIKE isogenies. Write $\theta(0_X) = (a_0 : \dots : a_{15})$ for the theta null point. The MIKE invariants are defined as*

$$I_{\text{MIKE}}(X) = (I_0 : \dots : I_9) \in \mathbb{P}^9,$$

with

$$\begin{aligned} I_0 &= (a_0 + a_6 + a_9 + a_{15})^2 & I_5 &= 4(a_2 - a_{11})^2, \\ I_1 &= (a_0 - a_6 + a_9 - a_{15})^2 & I_6 &= 4(a_1 + a_7)^2, \\ I_2 &= (a_0 + a_6 - a_9 - a_{15})^2 & I_7 &= 4(a_1 - a_7)^2, \\ I_3 &= (a_0 - a_6 - a_9 + a_{15})^2 & I_8 &= 4(a_3 + a_5)^2, \\ I_4 &= 4(a_2 + a_{11})^2, & I_9 &= 4(a_3 - a_5)^2. \end{aligned}$$

The MIKE invariants are isomorphism invariants up to permutation of the coordinates. Moreover, out of the $10! = 3628800$ elements in the symmetric group S_{10} , only the 72 permutations generated by $\langle (45)(67)(89), (179842)(365) \rangle$ act on I_{MIKE} . We denote this subset by S_{MIKE} .

Theorem 4.2. *Consider two abelian fourfolds X, X' of Weil-type equipped with a level-2 structure θ which is adapted to the MIKE isogenies. Then*

$$X \cong X' \quad \text{if and only if} \quad I_{\text{MIKE}}(X) = \sigma(I_{\text{MIKE}}(X'))$$

for some $\sigma \in S_{\text{MIKE}} \subset S_9 \subset S_{10}$. The action of σ on an element $x \in \mathbb{P}^9$ is given by $(x_0 : \dots : x_9) \mapsto (x_0 : x_{\sigma(1)} : \dots : x_{\sigma(9)})$.

Proof. This is proven in [Appendix H](#). □

Remark 4.5. For an intuition on these invariants, it is necessary to consider the theta null point of a level-(2, 2) theta structure $\Theta : X \hookrightarrow \mathbb{P}^{4^4-1}$. The squares of the theta null values can be computed from the level-2 theta null point using the duplication formula.

Precisely, $I_{\text{MIKE}}(X)$ is given by the squares of the 10 even level-(2, 2) theta null coordinates that are fixed under the action of $[i]$. We will see in [Lemma H.1](#) how these invariants may also be interpreted as the squares of the $[i]$ -even level-2 coordinates of the theta null point associated to a special theta structure.

Definition 4.3. *Let X be an abelian fourfold of Weil type and $I_{\text{MIKE}}(X) = (I_0 : \dots : I_9)$ as in Definition 4.2. We define the absolute MIKE invariants as*

$$J_{\text{MIKE}}(X) = (J_1 : \dots : J_5) \in \mathbb{P}(1, 2, 3, 4, 5) \text{ with } J_k = \sum_{i=1}^9 I_i^k \text{ for } k = 1, 2, 3, 4, 5.$$

Theorem 4.3. *Consider two abelian fourfolds X, X' of Weil-type equipped with level-2 structures θ, θ' that are adapted to the MIKE isogenies. Let $J_{\text{MIKE}}(X) = (J_1 : \dots : J_5)$ and $J_{\text{MIKE}}(X') = (J'_1 : \dots : J'_5)$ be the invariants from Definition 4.3. Assume that*

$$-7J_1^4 + 126J_1^2J_2 - 243J_2^2 - 432J_1J_3 + 972J_4 \neq 0,$$

then $X \cong X'$ if and only if $J_{\text{MIKE}}(X) = J_{\text{MIKE}}(X')$.

Proof. This is proven in [Appendix H.3](#). □

The invariants described in [Definition 4.3](#) can be computed efficiently as outlined in [Algorithm 3](#). Note that we normalise by $J_1/3 = I_0$.

Algorithm 3 AbsoluteMIKEInvariants(X)

Input: $X = \theta(0_X)$ the theta null point of an abelian fourfold of Weil-type equipped with a level-2 structure θ that is adapted to the MIKE isogenies.

Output: $J_{\text{MIKE}}(X)$ the normalised set of absolute invariants for X .

- 1: Compute $I_{\text{MIKE}}(X) = (1, I_{1,n}, \dots, I_{9,n}) := (1, I_1/I_0, \dots, I_9/I_0)$.
 - 2: Compute $J_{\text{MIKE}}(X) := (3, \sum_{i=1}^9 I_{i,n}^2 : \dots : \sum_{i=1}^9 I_{i,n}^5)$
 - 3: **return** $J_{\text{MIKE}}(X)$
-

4.4 The MIKE NIKE

We now formalise MIKE as a hashed Diffie-Hellman non-interactive key-exchange in the CKS framework [CKS08; FHKP13]. Let $\mathcal{ID}$ be the ordered set of permitted identities, and KDF be a key derivation function with output keyspace $\mathcal{SK}$ (modelled as a random oracle H in our security analysis).

- $\text{MIKE.Setup}(1^\lambda)$. Returns public parameters MIKE.pp^λ comprising a prime of the shape $p = 2^f c - 1$ with c small odd; a positive integer $e \leq f - 2$; and a basis (P_0, Q_0) of $E'_{M,0}[2^f]$ as detailed in Section 4.1. How e, f concretely relate to λ is discussed in Section 4.5.
- $\text{MIKE.KeyGen}(\text{MIKE.pp}^\lambda, \text{id})$. Return $\text{KeyGen}(\text{MIKE.pp}^\lambda)$.
- $\text{MIKE.SharedKey}(\text{id}_1, \text{pk}_1, \text{id}_2, \text{sk}_2)$.
 Compute $k \leftarrow \text{SharedSecret}(\text{sk}_2, \text{pk}_1)$. If $k = \perp$ or $\text{id}_1 = \text{id}_2$, return an error.
 Return $\text{KDF}(\text{id}_1, \text{id}_2, \text{pk}_1, \text{pk}_2, k)$ if $\text{id}_1 < \text{id}_2$, else return $\text{KDF}(\text{id}_2, \text{id}_1, \text{pk}_2, \text{pk}_1, k)$.

With this definition, MIKE is a correct NIKE as a consequence of Theorem 4.2. For brevity, we use the notation $\text{MIKE}(\text{pk}_1, \text{pk}_2)$ for the output of $\text{SharedSecret}(\text{sk}_2, \text{pk}_1)$ or $\text{SharedSecret}(\text{sk}_2, \text{pk}_1)$ when associated secret keys sk_1, sk_2 are not specified.

4.5 Parameter choices

There are two avenues to attack MIKE: computing the endomorphism ring of the public key E_A ;⁹ or directly recovering the secret isogeny $E_0 \rightarrow E_A$. As such, the two parameters determining the security of MIKE are the field characteristic p and the length of the secret key isogeny e .

The field characteristic. This determines the hardness of solving EndRing , for which the best known attack has time-complexity $O((p/w)^{1/2+o(1)})$ using space w [Wes26]. Allowing 2^λ memory yields the choice $\log_2(p) = 3\lambda$. To reflect that memory is expensive, [AAA+26] suggest a memory budget approximately $\log_2(w) = 5\lambda/8 + \log_2 \log_2(p^2)$ and conclude that $\log_2(p) = 325, 504, 668$ suffice for NIST levels I, III, V respectively (for memory budgets $\approx 2^{89}, 2^{130}, 2^{170}$ bits). The attack [Wes26] is a meet-in-the-middle type algorithm, and [AAA+26] assigns a cost of $O(1)$ for every element considered; in reality, (current implementations of) the attack yield elements by computing roots of large (modular-) polynomials that split over $\mathbb{F}_{p^2}$, and so have an asymptotic cost of at least $\log_2(p^2)$ per root. Considering this cost, we obtain primes of the size $\log_2(p) = 317, 484, 651$.

The secret key length. Since e is a public parameter, an adversary knows that the public key E_A is connected to E_0 via a 2^e -isogeny. The problem of recovering a *fixed-degree* isogeny has seen thorough cryptanalysis, as it was believed to be

⁹ This allows one to complete the key exchange, without explicit knowledge of the secret key. This is a consequence of Corollary C.2.

the hard problem underlying SIDH¹⁰. The best known attack presents a time-space trade-off with time-complexity $O((2^{3e/2}/w)^{1/2})$ using space w [ACCMR19, § 5.2]. Allowing 2^λ memory yields the choice $e = 2\lambda$. Using the same memory budget $\log_2(w) = 5\lambda/8 + \log_2 \log_2(p^2)$ as suggested by [AAA+26] allows for $e = 7\lambda/4$, i.e. $e = 224, 336, 448$ at NIST levels I, III, and V respectively. For reasons outlined in Remark 4.1, we will need to increase e by 4.

Two variants. From the two models of computation (memory $\log_2(w) = 3\lambda$, or $\log_2(w) = 5\lambda/8 + \log_2 \log_2(p^2)$), and whether the cost of root finding is accounted for or not, we derive two variants of MIKE

- RigorousMIKE $(p, e) = (117 \cdot 2^{374} - 1, 372), (77 \cdot 2^{566} - 1, 564), (41 \cdot 2^{758} - 1, 756)$
- FastMIKE $(p, e) = (663 \cdot 2^{308} - 1, 228), (593 \cdot 2^{474} - 1, 340), (317 \cdot 2^{628} - 1, 452)$

for levels I, III, and V respectively. In the FastMIKE variant, we have further rounded down the sizes of the primes in levels III and V, to the next smallest 64-bit word boundary.

5 Security of the MIKE NIKE

In this section, we prove that MIKE is an actively secure NIKE [CKS08; FHKP13] in the Quantum Random Oracle Model (QROM) [BDF+11] under the assumption that solving the MIKE CDH problem is hard, even when given a quantum accessible DDH-oracle (Problem 5.2).

To support this new assumption, we analyze the CDH problem in an extension of the *Algebraic Isogeny Model* [ABR26] in arbitrary dimension, that we call AIM+. In this model we show that the RigorousMIKE CDH problem is equivalent to the EndRing problem (e.g. [EHLMP18, Prob. 3]), the foundational problem of isogeny-based cryptography. We get the same reduction for FastMIKE, assuming its public keys are indistinguishable from uniformly random supersingular curves.

Finally, we remark that the CDH assumption already suffices to construct a *passively* secure NIKE [GKQMS24] (which can be made actively secure through a zero-knowledge proof of knowledge of the secret key¹¹) or IND-CCA KEM (using the standard ElGamal and Fujisaki–Okamoto transform [FO99] approach) from MIKE; and only require the hardness of EndRing to be proven secure in the AIM+. Consequently, MIKE solves Problem 7 of the Isogeny Problems [CFG+26].

5.1 Active Security of MIKE under gapCDH

In this section we prove that MIKE is an actively secure NIKE in the QROM under a gapCDH assumption, using the *CKS-light* NIKE security model (which is polynomially equivalent to the standard CKS model [FHKP13, Th. 1]).

¹⁰ before being broken with other techniques utilising torsion-point information, of which MIKE has none

¹¹ this is stronger than public-key validation

*CKS and CKS-light models.*¹² CKS is a game-based security model for NIKE in which the game runs $\mathbf{pp} \leftarrow \text{Setup}$, randomly samples a secret bit b , and provides the public parameters $\mathbf{pp}$ to an adversary $\mathcal{A}$, who tries to guess b with non-negligible advantage. To model user registration and key exchange, the game provides $\mathcal{A}$ access to the following oracles, which may be queried arbitrarily often: REGISTERHONEST which returns a public key ($\mathcal{A}$ does not know the secret key); REGISTERCORRUPT to which $\mathcal{A}$ may submit a public key ($\mathcal{A}$ may know the secret key); CORRUPTREVEAL to output the shared key between an honest and a corrupt user; TEST on input two honest users outputs either their shared key or a (consistently) randomly sampled key (depending on b). In the *CKS-light* model, $\mathcal{A}$ is limited to calling REGISTERHONEST twice and call TEST once (but may call the other oracles arbitrarily often).

CKS security of MIKE. We formally define the CDH and qGapCDH problems

Problem 5.1 (CDH). Given an input $(\mathbf{pk}_1, \mathbf{pk}_2)$, the computational Diffie–Hellman problem CDH requires to compute $\text{MIKE}(\mathbf{pk}_1, \mathbf{pk}_2)$. We define the advantage of an adversary $\mathcal{A}$ with $\mathbf{pk}_1, \mathbf{pk}_2$ distributed as random MIKE public keys by

$$\text{Adv}_{\text{MIKE}}^{\text{CDH}}(\mathcal{B}) = \Pr[\mathcal{A}(\mathbf{pk}_1, \mathbf{pk}_2) \Rightarrow \text{MIKE}(\mathbf{pk}_1, \mathbf{pk}_2)].$$

Problem 5.2 (quantum GapCDH). Given an input $(\mathbf{pk}_1, \mathbf{pk}_2)$, qGapCDH requires to compute $\text{MIKE}(\mathbf{pk}_1, \mathbf{pk}_2)$ with quantum access to the decisional Diffie–Hellman oracle $\text{DDH}(|\cdot\rangle, |\cdot\rangle, |\cdot\rangle)$, which on input (E_1, E_2, J) returns 1 if $J = \text{MIKE}(E_1, E_2)$, and 0 otherwise, with queries in superposition defined by linearity. We define the advantage of an adversary $\mathcal{A}$ with $\mathbf{pk}_1, \mathbf{pk}_2$ distributed as random MIKE public keys by $\text{Adv}_{\text{MIKE}}^{\text{qGapCDH}}(\mathcal{B}) = \Pr[\mathcal{A}^O(\mathbf{pk}_1, \mathbf{pk}_2) \Rightarrow \text{MIKE}(\mathbf{pk}_1, \mathbf{pk}_2)]$.

Theorem 5.1. *For any quantum adversary $\mathcal{A}$ against MIKE in the CKS-light model making at most d parallel queries to the quantum-accessible random oracle KDF, there exists a quantum adversary $\mathcal{B}$ against qGapCDH such that $\text{Adv}_{\text{MIKE}}^{\text{CKS-light}}(\mathcal{A}) \leq 2(d+1)^{1/2} \text{Adv}_{\text{MIKE}}^{\text{qGapCDH}}(\mathcal{B})^{1/2}$.*

We give a proof in [Appendix I.2](#), which closely follows the security proof of the group action-based NIKE in [\[DHK+22\]](#). Two differences are that we cannot rerandomise MIKE key-exchanges to embed the challenge into arbitrarily many public keys (which is why we use CKS-light); and that our gapCDH assumption is stronger (because [\[DHK+22\]](#) fix one public key in the DDH oracle, and we do not). As a consequence, together with [\[FHKP13, Th. 1\]](#), we obtain the following

Corollary 5.1. *For any quantum adversary $\mathcal{A}$ against MIKE in the CKS model making at most d parallel queries to the quantum-accessible random oracle KDF, q_H REGISTERHONEST queries and q_T distinct TEST queries, there exists an adversary $\mathcal{B}$ against qGapCDH such that $\text{Adv}_{\text{MIKE}}^{\text{CKS}}(\mathcal{A}) \leq q_H^2 q_T (d+1)^{1/2} \text{Adv}_{\text{MIKE}}^{\text{qGapCDH}}(\mathcal{B})^{1/2}$.*

¹² See [Appendix I.1](#) for full definitions.

5.2 Hardness of the new assumption

We are unable to formally reduce the qGapCDH assumption from an established hardness assumption; however, we can show that CDH problem (Problem 5.1)) reduces from EndRing in an algebraic setting. More precisely, we extend Algebraic Isogeny Model (AIM) [ABR26] to arbitrary dimension (in particular, dimension 4 for MIKE) and provide a classical polynomial time reduction from OneEnd (equivalent to EndRing [PW24]) to CDH .

Thus, the hardness of Problem 5.2 hinges on whether the DDH oracle provides a significant help to the adversary. We do not expect this to be the case: even in the classical setting of Diffie–Hellman, which is much more algebraically rich (and thus likely to make the DDH oracle more useful), there is no known search-to-decision reduction, i.e. the CDH problem is not known to become easier when a DDH oracle is provided. In fact, pairing-based cryptography relies on a similar gap assumption. The same is true in the group-action context: the active security of the group-action NIKE relies on a similar gap assumption [DHK+22], where no known attack exploits the DDH oracle. We expect that the lack of algebraic structure in MIKE makes the DDH oracle even less useful, and thus any attack against Problem 5.2 would need to solve the CDH problem directly. We study the hardness of the following CDH problem in the next section.

5.3 The AIM+

Using the theory of *efficient models* of PPAVs [SPW26], we extend the *Algebraic Isogeny Model* (AIM) [ABR26] to arbitrary dimension, allowing us to analyse the security higher-dimensional isogeny protocols (e.g. MIKE) in an algebraic setting (in analogy to the *algebraic group model* [FKL18]). As the AIM does in dimension-one, our new model (the AIM+) requires to adversaries to *explain* any output PPAV, with a (principally polarized) isogeny from one of its inputs.

Efficient Models for PPAVs. To formalise the notion of “explaining” an output curve, the AIM prescribes a way to represent input and output curves (the j -invariant) and isogenies (the so-called *8D-representation* [ABR26, Def. 2.2]). In particular, this representation allows for efficient manipulation of isogenies, e.g. evaluation points, equality comparison, and composition, hence constitutes an *efficient model* [SPW26, Def. 3.1]. In [SPW26, Th. 7.7], it is proven that the *level-4 theta-model* (Definition E.1) together with the *interpolation representation* comprise an efficient model for PPAVs and (principally polarised isogenies between them) in any dimension, giving a direct generalisation of how the AIM represents its objects in dimension 1. Note that the interpolation representation is universal: any efficient representation of an isogeny can be converted to the latter. Moreover, we do not require the adversaries to explain products or projections.

A typed pseudocode framework. The AIM defines a (quantum) typed pseudocode framework; for example, the classical variant comprises of two types $\langle \text{bits} \rangle$ and

$\langle \text{curves} \rangle$ and three operators: $\text{encode}: \langle \text{bits} \rangle \rightarrow \langle \text{curves} \rangle$ to map bits to curves, $\text{decode}: \langle \text{curves} \rangle \rightarrow \langle \text{bits} \rangle \cup \{\perp\}$ to map curves to bits, and isogeny to evaluate a isogenies (type $\langle \text{bits} \rangle$) on $\langle \text{curves} \rangle$. Using the machinery of [SPW26], we define the AIM+ to follow the same typed framework by working the level-4 theta-model (replacing $\langle \text{curves} \rangle$ with $\langle \text{PPAVs} \rangle$): using the results of [SPW26], one can efficiently encode and decode (polarised isomorphism classes of) PPAVs and their points; this also suffices to encode and decode the interpolation representation, and so to implement isogeny .

PPAVs of known endomorphism ring. As detailed in [ABR26, § B], it is necessary to supply algebraic adversaries with at least one input of known endomorphism ring to prevent some easy problems in the standard model becoming hard in the AIM. We achieve this in the AIM+ by supplying the adversary with a supersingular elliptic curve E_{end} of known endomorphism ring (the same additional input provided by the AIM); from such a curve, the adversary may construct a PPAV E_{end}^g of known endomorphism ring in any dimension.

5.4 EndRing-to-CDH reduction in AIM+

The core result of this subsection is that $\text{OneEnd}_{\text{MIKE}}$ ¹³ classically reduces to CDH in the AIM+. Moreover, we show that when the secret key length parameter e is approximately $\log_2(p)$, $\text{OneEnd}_{\text{MIKE}}$ is equivalent to OneEnd , i.e. equivalent to EndRing . Consequently, EndRing reduces to RigorousMIKE 's CDH problem. Further, under the assumption that FastMIKE 's public keys are computationally indistinguishable from uniformly randomly sampled supersingular elliptic curves, we obtain that EndRing reduces to FastMIKE 's CDH problem.

Theorem 5.2 (OneEnd_{MIKE}-to-CDH reduction). *For every algebraic adversary $\mathcal{C}$ against CDH in the AIM+, there exists an algebraic adversary $\mathcal{E}$ against OneEnd_{MIKE} that makes one classical CDH-query, has the same running time $\mathcal{C}$ (up to polynomial overhead), and has advantage at least $1/2 \cdot \text{Adv}^{\text{CDH}}(\mathcal{C})$.*

Proof. Let E_A be the input MIKE public key to $\text{OneEnd}_{\text{MIKE}}$. We will use the *composition*, *product*, and *decomposition* axioms of [SPW26], which informally state that one can compose isogenies, form products of PPAVs, and decompose a product of PPAVs into its (simple) factors all in polynomial time. As such, the following reduction runs in polynomial time.

The reduction. Run KeyGen to obtain a secret key x_B and public key E_B . Construct the rank-2 module M_B corresponding to the secret key x_B (as in Corollary 3.1). Then, choosing uniformly at random, pass either (E_0, E_A, E_B) or (E_0, E_B, E_A) to $\mathcal{C}$ to obtain the shared secret $\text{MIKE}(E_A, E_B)$ together with an explanation ε thereof. Recall that we know the isogeny $F_B: W'(E_A)^2 \rightarrow$

¹³ The problem of computing one endomorphism of a uniformly distributed MIKE public key.

$\text{MIKE}(E_A, E_B)$. Using the product (for $W'(E_A)^2 \rightarrow E_A^4$) and composition axioms one obtains the isogeny

$$\Phi: E_1 \times \cdots \times E_4 \xrightarrow{\varepsilon} \text{MIKE}(E_A, E_B) \xrightarrow{F_R^\vee} W'(E_A)^2 \rightarrow E_A^4,$$

where the E_i are any of the curves E_0, E_A or E_B (i.e. inputs to $\mathcal{C}$).

Since Φ is an isogeny between the product of elliptic curves, it is a matrix of isogenies (or zero-maps) $E_i \rightarrow E_A$ which we can efficiently recover using the decomposition axiom. Indeed, the decomposition axiom provides us with inclusion maps $\iota_i: E_i \rightarrow E_1 \times \cdots \times E_4$ and projection maps $\pi_i: E_A^4 \rightarrow E_A$ (from the i -th copy), which allow us to evaluate $\iota_i \Phi \pi_k: E_i \rightarrow E$ on points, and so construct their interpolation representations [SPW26, Lem. 7.3]. Since Φ is an isogeny (and therefore surjective) at least one of $E_j \rightarrow E$ must be non-zero.

If $E_j \neq E_A$, one has an isogeny φ from a curve with known endomorphism ring E_{end} (E_0 or E_B) to E_A and so can recover a suborder $\varphi \text{End}(E_{\text{end}}) \varphi^\vee$ of $\text{End}(E_A)$ (and in particular one endomorphism). If all (non-zero) isogenies $E_j \rightarrow E$ have domain $E_j = E_A$, then return an error.

Advantage analysis. Since $\mathcal{C}$ cannot distinguish E_A from E_B , the choice whether to pass (E_0, E_A, E_B) or (E_0, E_B, E_A) is independent of the randomness of $\mathcal{C}$. Consequently, one obtains a (non-zero) isogeny $E_j \neq E_A \rightarrow E$ with probability at least $1/2$. $\square$

Remark 5.1 (On requiring polarised isogenies.). We remark that this proof also works, even if the explanation is not an n -isogeny: any explanation that allows efficiently evaluating a surjective regular map¹⁴ $E_1 \times \cdots \times E_g \rightarrow \text{MIKE}(E_A, E_B)$ suffices. Indeed, it will still be possible to evaluate $\iota_i \Phi \pi_k: E_i \rightarrow E$ on points; and since $\iota_i \Phi \pi_k$ is a regular map between elliptic curves (it is a composition of regular maps) it must be an isogeny or the zero-map (potentially up to translation). As such, we can construct an interpolation representation of $\iota_i \Phi \pi_k$ by evaluating on points, and proceed with our proof as before.

Moreover, since polarisations descend through isogenies, we remark that adversaries that are able to compute unpolarised isogenies $A \rightarrow B$ between PPAVs $(A, \lambda_A), (B, \lambda_B)$ are able to compute an endomorphism of A . This is conjectured to be as hard as the (exponentially hard) problem of solving EndRing (and is indeed equivalent in dimension 1 [PW24]).

Corollary 5.2. *OneEnd is equivalent to RigorousMIKE's $\text{OneEnd}_{\text{MIKE}}$ problem, and so EndRing reduces to RigorousMIKE's CDH problem.*

Proof. We define a new adversary $\mathcal{B}$ against OneEnd . It simply rerandomises the input curve E by performing a walk of length $12 \log(p)$ in the 2-isogeny graph to obtain a curve E' whose distribution is negligibly far from the uniform distribution [MW25, Cor. 1]; then it calls $\mathcal{A}$. We first note that the support of RigorousMIKE's MIKE.KeyGen is of size $K \geq \mathcal{S}/(2ce^2)$ [Ler22, Prop. 2.4.25] (whereby $\mathcal{S} = p/12 + \{0, 1, 2\}$ is the number of the supersingular curves over

¹⁴ i.e. fractions of polynomials in every coordinate, e.g. isogenies are regular maps

$\mathbb{F}_{p^2}$), and so the probability of E' lying in the set of all **RigorousMIKE** public keys is $\mathcal{S}/(2ce^2)$, incurring an initial polynomial loss.

Now, we bound the success of $\mathcal{A}$ with respect to the uniform distribution. To that end, let κ be the distribution on **MIKE** public keys induced by **MIKE.KeyGen**, and $P(E)$ denote the probability of success of $\mathcal{A}$ on a curve E . Using Cauchy-Schwarz, we find

$$\text{Adv}_\kappa(\mathcal{A})^2 \leq \left(\sum_E \frac{1}{K} P(E) \right) \cdot \left(\sum_E K \kappa(E)^2 \right) = \text{Adv}_{\text{unif}}(\mathcal{A}) \cdot K \sum_E \kappa(E)^2.$$

However, $\mathcal{S}^2 \sum_E \kappa(E)^2$ is the quantity $|Y|_2^2$ in [Ler22, Prop. 2.4.25], which is bounded by $e^2 c^2 \mathcal{S}$. Consequently $\text{Adv}_{\text{unif}}(\mathcal{A}) \geq 1/(e^2 c^2) \text{Adv}_\kappa(\mathcal{A})^2$. $\square$

Problem 5.3 (Distinguishing FastMIKE public keys). Let E_1 be a supersingular elliptic curve, sampled by **FastMIKE**'s **MIKE.KeyGen**, and E_2 a supersingular elliptic curve sampled uniformly at random. Given E_b according to a random choice bit b , determine the value of b .

Corollary 5.3. *Assuming Problem 5.3 is hard, EndRing reduces to FastMIKE's CDH problem.*

6 Implementation and Performance Results

We have written constant-time, efficient implementations of **MIKE** in both C and Rust, along with a high level SageMath implementation, for all three parameter sets of both **FastMIKE** and **RigorousMIKE** which is available at the following repository:

https://github.com/tensor-MIKE/mike_rs
https://github.com/tensor-MIKE/mike_c
https://github.com/tensor-MIKE/mike_py

Performance. We detail the performance of our C and Rust implementations in Table 1 and Table 2.

Key Generation. For key generation, the baseline performance is limited by the $\mathbb{F}_{p^2}$ implementation. At the top level, the cost is dominated by the computation of a 2^e -isogeny, with only a small fraction of the time spent on the computation of the isogeny kernel itself.

The isogeny chain is computed with $e/2$ four-isogeny steps [CH17], where we deliberately pick e even to avoid a 2-isogeny step at the end of the chain. We use standard strategies to achieve quasi-linear cost by balancing the number of doubles and images computed. Kernel generation is optimised by using a pre-computed basis for the generators $\langle P, Q \rangle = E_{0,M}[2^{e+2}]$, which are passed into a three-point ladder to compute $K = P + [x_{\text{sk}}]Q$, using x -only arithmetic on the

Montgomery curve, so that $[4]K$ generates the kernel of $\phi_A : E_{0,M} \rightarrow E_A$. The image of K on E_A has order four, which we use to recover six isomorphic Montgomery coefficients for E_A without a costly square-root in $\mathbb{F}_{p^2}$. The remaining six are simply complex conjugates of the others and so are “free” to construct. We choose the smallest coefficient A as a unique represent of the public key. See [AAA+26, Alg. 4.96] for computational details.

Shared Secret Generation. Much like key generation, the top-level cost is in the computation of a length e isogeny in dimension four. However, before the isogeny can be computed, the kernel of this isogeny is first constructed from the user’s private scalar and the recipient’s public curve using Theorem 4.1. Kernel reconstruction accounts for approximately one fifth of the overhead and is dominated by iterated doubling and scalar multiplication of projective points in jacobian coordinates over $\mathbb{F}_{p^2}$.

The gluing isogeny, although mathematically complex, accounts for a small cost of the shared secret computation, and outputs a codomain and kernel of elements defined over $\mathbb{F}_p$. Because of this, the performance of the dimension four isogeny is limited by the relative performance of the implementation of arithmetic in $\mathbb{F}_p$.

Interestingly, unlike one- and two-dimensional isogenies, where performance can be accurately estimated by counting the number of field multiplications required, field additions are a significant proportion of the overall cost of a four-dimensional isogenies using level-two theta coordinates. Whereas computations of doublings and evaluations computations require pairwise multiplication of coordinates, at either 16 squares or multiplications per call, Hadamard transforms require 64 additions per call. This fourfold weighting of base field operations produces the overhead in (relatively cheap) $\mathbb{F}_p$ additions.

As a result, a properly optimised implementation of field arithmetic for MIKE may require an unconventional finite-field implementation using specialised internal representations to optimise Hadamard transformations, even if this increases the cost of $\mathbb{F}_p$ multiplications and squaring. Additionally, because of the large number of parallel operations performed on the coordinates, vectorised implementations of MIKE key generation are an obvious starting point for efficient implementations when the appropriate hardware is available.

Constant-Time. An implementation is said to be “constant time” when no secret data influences branch conditions or memory indices. In this sense, a constant-time implementation ensures that an attacker is unable to learn secret data of the protocol even given fine-grained measurements of the computation timing at all stages.

Writing truly constant-time code is challenging, and for an implementation such as ours which has been written in pure Rust with no assembly tricks, it is essentially impossible to prove that no compiler will introduce secret-dependent branching regardless of the hardware or compiler version used to generate binaries. A well-written, pessimistic account of this is detailed in [Por25].

Table 1: Performance of MIKE C implementation

		Parameters / Sizes				x86 ref		x86 asm		ARM asm	
		p	$\log_2(p)$	e	pk B	KG MCy	SK MCy	KG MCy	SK MCy	KG MCy	SK MCy
Fast	I	$633 \cdot 2^{308} - 1$	318	228	80	3.75	28.6	2.15	16.0	1.10	8.16
	III	$593 \cdot 2^{474} - 1$	484	340	122	9.23	69.3	6.97	49.2	3.26	25.9
	V	$317 \cdot 2^{628} - 1$	637	452	160	21.9	146	13.7	94.0	6.38	50.9
Rigorous	I	$117 \cdot 2^{374} - 1$	381	372	96	4.77	37.3	2.82	20.4	1.38	10.5
	III	$77 \cdot 2^{566} - 1$	573	564	144	13.7	92.7	8.47	59.4	3.97	31.0
	V	$41 \cdot 2^{758} - 1$	764	756	192	37.2	248	26.7	168	11.2	90.2

Parameter details and running times for the MIKE key generation (KG) and shared secret generation (SK). Implementation is constant time and includes verification that public keys are supersingular. No AVX used. x86 data was recorded on an AMD Ryzen 7 PRO 7840U@3.3GHz, multithreading and turbo-boost disabled, and compiled with `gcc 16.2.1`. ARM data was recorded on an Apple M4 Pro@4.5GHz, and compiled with `clang v21.0.0`. Data collected over 1000 samples. Times rounded to three significant figures.

Despite the challenges of constant-time cryptographic engineering, one particularly attractive aspect of a MIKE is that both key generation and shared secrets have clear and concise descriptions which naturally allow for a (theoretically) constant-time description. For shared secrets, this is fairly miraculous and is intimately related to [Theorem 4.1](#) and the symmetries which simplify the dimension-four codomain computations.

At the practical level, a constant-time implementation of MIKE needs only a rigorously tested constant-time implementation of finite-field arithmetic, with utility functions such as constant-time conditional swaps and equality checking. In particular, although ideals and quaternions play a central role in the theoretical discussion of MIKE, they are completely absent in the practical implementation. This results in a significantly smaller and simpler implementation: at the foundation, all operations are performed on finite-field elements.

In key generation, secret dependent branching occurs in only two places: the computation of the kernel and the normalisation of the public key. The kernel $K = P + [x_{\text{sk}}]Q$ is computed using the standard constant-time x -only three-point ladder, which uses conditional swaps for each bit in the secret x_{sk} . Normalisation requires finding the lexicographically smallest of the set of possible coefficients which requires only byte comparison and conditional swaps. Importantly, the bulk of the computation is the isogeny chain, which has no branching and runs in constant-time, given the kernel generator $K = P + [x_{\text{sk}}]Q$.

The situation is similar in shared secret computation. The secret is processed in the generation of the kernel of the isogeny, but once this kernel has

Table 2: Performance of MIKE Rust implementation

		Parameters / Sizes				x86 ref		ARM ref	
		p	$\log_2(p)$	e	pk B	KG ms	SK ms	KG ms	SK ms
Fast	I	$633 \cdot 2^{308} - 1$	318	228	80	0.849	7.11	0.440	3.89
	III	$593 \cdot 2^{474} - 1$	484	340	122	3.07	26.9	1.63	13.9
	V	$317 \cdot 2^{628} - 1$	637	452	160	6.60	56.1	3.52	29.7
Rigorous	I	$117 \cdot 2^{374} - 1$	381	372	96	2.05	15.6	1.07	8.41
	III	$77 \cdot 2^{566} - 1$	573	564	144	7.01	59.0	3.67	31.5
	V	$41 \cdot 2^{758} - 1$	764	756	192	17.0	149	9.00	85.9

Parameter details and running times for the MIKE key generation (KG) and shared secret generation (SK). Implementation is constant time and includes verification that public keys are supersingular. No AVX or assembly optimisations used. x86 data was recorded on an AMD Ryzen 7 PRO 7840U@3.3GHz, multithreading and turbo-boost disabled. ARM data was recorded on an Apple M4 Pro@4.5GHz. Rust compiler version 1.100.0-nightly (required for compatibility with the underlying `fp2` library). Data collected using the `criterion` crate. Times rounded to three significant figures.

been computed there is no branching on the input data to the isogeny chain. Specifically, the secret key is processed during shared secret computation in a series of scalar multiplications which are computed using x -only Montgomery ladders with the use of the Okeya and Sakurai formulae [OS01] to recover the projective y -coordinate.

Future optimisations. There are still a lot of optimisations to do for MIKE’s key exchange. At the high level, there is still room to optimize the dimension four isogeny formulas. At the lower level, MIKE’s performance is heavily dependant on the underlying $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$ arithmetic. Future releases will further explore assembly optimised versions, as well as implementations with alternative internal representations (such as the redundant representation with signed reduction factors [Por26]). Additionally, the dimension four isogeny formulas are perfectly suited for vectorised instructions, which we also leave for future work.

References

- [AAA+26] Marius A. Aardal, Gora Adj, Diego F. Aranha, Andrea Basso, Giacomo Borin, Isaac Andrés Canales Martínez, Jorge Chávez-Saab, Maria Corte-Real Santos, Pierrick Dartois, Luca De Feo, Max Duparc, Thomas Espitau, Jonathan Komada Eriksen, Tako Boris Fouotsa, Décio Luiz Gazzoni Filho, Basil Hess, Riccardo Invernizzi, David Kohel, Antonin Leroux, Patrick Longa, Luciano Maino, Michael Meyer, Marzio Mula, Kohei Nakagawa, Hiroshi Onuki, Lorenz Panny, Sikhar Patranabis, Christophe Petit, Giacomo Pope, Krijn Reijnders, Damien Robert, Francisco Rodríguez-Henríquez, Sina Schaeffler, Frederik Vercauteren, Alexandre Wallet, Benjamin Wesolowski, and Wessel van Woerden. *SQIsign*. Tech. rep. National Institute of Standards and Technology, 2026. URL: <https://sqisign.org> (cit. on pp. 7, 15–18, 21, 22, 28, 102, 135, 136, 138, 139).
- [ABR26] Marius A. Aardal, Andrea Basso, and Doreen Riepel. “The Algebraic Isogeny Model: A General Model with Applications to SQIsign and Key Exchanges”. In: *EUROCRYPT 2026, Part IV*. Ed. by Joan Daemen and Emmanuel Thomé. Vol. 16545. LNCS. Springer, Cham, May 2026, pp. 604–635. DOI: [10.1007/978-3-032-25327-9_21](https://doi.org/10.1007/978-3-032-25327-9_21) (cit. on pp. 22, 24, 25).
- [ACCMR19] Gora Adj, Daniel Cervantes-Vázquez, Jesús-Javier Chi-Domínguez, Alfred Menezes, and Francisco Rodríguez-Henríquez. “On the Cost of Computing Isogenies Between Supersingular Elliptic Curves”. In: *SAC 2018*. Ed. by Carlos Cid and Michael J. Jacobson Jr. Vol. 11349. LNCS. Springer, Cham, Aug. 2019, pp. 322–343. DOI: [10.1007/978-3-030-10970-7_15](https://doi.org/10.1007/978-3-030-10970-7_15) (cit. on pp. 22, 136, 137).
- [Adl79] Leonard Adleman. “A subexponential algorithm for the discrete logarithm problem with applications to cryptography”. In: *Proceedings of the 20th Annual Symposium on Foundations of Computer Science*. 1979, pp. 55–60. DOI: [10.1109/SFCS.1979.2](https://doi.org/10.1109/SFCS.1979.2) (cit. on p. 2).
- [ADMP20] Navid Alamati, Luca De Feo, Hart Montgomery, and Sikhar Patranabis. “Cryptographic Group Actions and Applications”. In: *ASIACRYPT 2020, Part II*. Ed. by Shiho Moriai and Huaxiong Wang. Vol. 12492. LNCS. Springer, Cham, Dec. 2020, pp. 411–439. DOI: [10.1007/978-3-030-64834-3_14](https://doi.org/10.1007/978-3-030-64834-3_14) (cit. on p. 45).
- [BBRS26] Andrea Basso, Giacomo Borin, Ryan Rueger, and Sina Schaeffler. “CORAL Faster Isogeny Group Action for Post-Quantum NIKE”. In: *Advances in Cryptology - CRYPTO 2026 - 46th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-20, 2026, Proceedings, Part IV*. Ed. by Nadia Heninger and Mike Rosulek. Vol. 16803. Lecture Notes in Computer Science. Springer, 2026, pp. 506–536. DOI: [10.1007/978-](https://doi.org/10.1007/978-)

- 3-032-35398-6_17. URL: https://doi.org/10.1007/978-3-032-35398-6_17 (cit. on p. 6).
- [BK00] A. J. Berrick and M. E. Keating. *An Introduction to Rings and Modules: With K-Theory in View*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2000 (cit. on p. 42).
- [BKV19] Ward Beullens, Thorsten Kleinjung, and Frederik Vercauteren. “CSI-FiSh: Efficient Isogeny Based Signatures Through Class Group Computations”. In: *ASIACRYPT 2019, Part I*. Ed. by Steven D. Galbraith and Shiho Moriai. Vol. 11921. LNCS. Springer, Cham, Dec. 2019, pp. 227–247. DOI: [10.1007/978-3-030-34578-5_9](https://doi.org/10.1007/978-3-030-34578-5_9) (cit. on p. 45).
- [BL04] Christina Birkenhake and Herbert Lange. *Complex abelian varieties*. Vol. 302. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Berlin: Springer-Verlag, 2004, pp. xii+635. ISBN: 3-540-20488-1 (cit. on p. 115).
- [BDF+11] Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry. “Random Oracles in a Quantum World”. In: *ASIACRYPT 2011*. Ed. by Dong Hoon Lee and Xiaoyun Wang. Vol. 7073. LNCS. Springer, Berlin, Heidelberg, Dec. 2011, pp. 41–69. DOI: [10.1007/978-3-642-25385-0_3](https://doi.org/10.1007/978-3-642-25385-0_3) (cit. on p. 22).
- [BS20] Xavier Bonnetain and André Schrottenloher. “Quantum Security Analysis of CSIDH”. In: *EUROCRYPT 2020, Part II*. Ed. by Anne Canteaut and Yuval Ishai. Vol. 12106. LNCS. Springer, Cham, May 2020, pp. 493–522. DOI: [10.1007/978-3-030-45724-2_17](https://doi.org/10.1007/978-3-030-45724-2_17) (cit. on p. 45).
- [Bou74] Nicolas Bourbaki. *Elements of Mathematics, Algebra I*. Hermann, 1974 (cit. on p. 43).
- [BY91] Gilles Brassard and Moti Yung. “One-Way Group Actions”. In: *CRYPTO’90*. Ed. by Alfred J. Menezes and Scott A. Vanstone. Vol. 537. LNCS. Springer, Berlin, Heidelberg, Aug. 1991, pp. 94–107. DOI: [10.1007/3-540-38424-3_7](https://doi.org/10.1007/3-540-38424-3_7) (cit. on p. 3).
- [Bre87] L Breen. “Biextensions alternées”. In: *Compositio Mathematica* 63.1 (1987), pp. 99–122 (cit. on p. 129).
- [CHMR25] Fabio Campos, Andreas Hellenbrand, Michael Meyer, and Krijn Reijnders. “dCTIDH: Fast & Deterministic CTIDH”. In: *IACR TCHES* 2025.3 (2025), pp. 516–541. DOI: [10.46586/tches.v2025.i3.516-541](https://doi.org/10.46586/tches.v2025.i3.516-541) (cit. on p. 6).
- [CKS08] David Cash, Eike Kiltz, and Victor Shoup. “The Twin Diffie-Hellman Problem and Applications”. In: *EUROCRYPT 2008*. Ed. by Nigel P. Smart. Vol. 4965. LNCS. Springer, Berlin, Heidelberg, Apr. 2008, pp. 127–145. DOI: [10.1007/978-3-540-78967-3_8](https://doi.org/10.1007/978-3-540-78967-3_8) (cit. on pp. 21, 22, 131).
- [CD20] Wouter Castryck and Thomas Decru. “CSIDH on the Surface”. In: *PQCrypto 2020*. Ed. by Jintai Ding and Jean-Pierre Tillich.

- Springer, Cham, 2020, pp. 111–129. DOI: [10.1007/978-3-030-44223-1_7](https://doi.org/10.1007/978-3-030-44223-1_7) (cit. on p. 44).
- [CFG+26] Wouter Castryck, Luca De Feo, Steven D. Galbraith, Péter Kutas, Krijn Reijnders, and Benjamin Wesolowski. *The Isogeny Problems*. Cryptology ePrint Archive, Paper 2026/1431. 2026. URL: <https://eprint.iacr.org/2026/1431> (cit. on p. 22).
- [CLMPR18] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. “CSIDH: An Efficient Post-Quantum Commutative Group Action”. In: *ASIACRYPT 2018, Part III*. Ed. by Thomas Peyrin and Steven Galbraith. Vol. 11274. LNCS. Springer, Cham, Dec. 2018, pp. 395–427. DOI: [10.1007/978-3-030-03332-3_15](https://doi.org/10.1007/978-3-030-03332-3_15) (cit. on pp. 2, 44, 45).
- [Cha12] Ching-Li Chai. “Moduli of abelian varieties”. In: *NSF Award Number 1200271. Directorate for Mathematical and Physical Sciences* 12.1200271 (2012), p. 271 (cit. on p. 114).
- [CSCJR22] Jorge Chávez-Saab, Jesús-Javier Chi-Domínguez, Samuel Jaques, and Francisco Rodríguez-Henríquez. “The SQALE of CSIDH: sub-linear Vélú quantum-resistant isogeny action with low exponents”. In: *Journal of Cryptographic Engineering* 12.3 (Sept. 2022), pp. 349–368. DOI: [10.1007/s13389-021-00271-w](https://doi.org/10.1007/s13389-021-00271-w) (cit. on p. 45).
- [Cho52] Wei-Liang Chow. “On the Quotient Variety of an Abelian Variety”. In: *Proceedings of the National Academy of Sciences* 38.12 (1952), pp. 1039–1044. DOI: [10.1073/pnas.38.12.1039](https://doi.org/10.1073/pnas.38.12.1039) (cit. on p. 60).
- [CK20] Leonardo Colò and David Kohel. “Orienting supersingular isogeny graphs”. In: *Journal of Mathematical Cryptology* 14.1 (2020), pp. 414–437. DOI: [doi:10.1515/jmc-2019-0034](https://doi.org/10.1515/jmc-2019-0034) (cit. on pp. 44, 45).
- [CR26] Maria Corte-Real Santos and Krijn Reijnders. “Return of the Kummer: a Toolbox for Genus-2 Cryptography”. In: *IACR Communications in Cryptology* 2.4 (Jan. 8, 2026). ISSN: 3006-5496. DOI: [10.62056/a0zogy17s](https://doi.org/10.62056/a0zogy17s) (cit. on pp. 6, 71).
- [Cos18] Craig Costello. “Computing supersingular isogenies on Kummer surfaces”. In: *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 2018, pp. 428–456 (cit. on pp. 71, 72).
- [CH17] Craig Costello and Hüseyin Hisil. “A Simple and Compact Algorithm for SIDH with Arbitrary Degree Isogenies”. In: *ASIACRYPT 2017, Part II*. Ed. by Tsuyoshi Takagi and Thomas Peyrin. Vol. 10625. LNCS. Springer, Cham, Dec. 2017, pp. 303–329. DOI: [10.1007/978-3-319-70697-9_11](https://doi.org/10.1007/978-3-319-70697-9_11) (cit. on pp. 16, 27).
- [Cou06] Jean-Marc Couveignes. *Hard Homogeneous Spaces*. Cryptology ePrint Archive, Report 2006/291. 2006. URL: <https://eprint.iacr.org/2006/291> (cit. on p. 3).
- [Cox13] David A. Cox. *Primes of the form $x^2 + ny^2$* . Wiley, 2013, p. 349 (cit. on p. 55).

- [Cur62] Curtis, Charles W. and Reiner, Irving. *Representation Theory of Finite Groups and Associative Algebras*. John Wiley & Sons, 1962 (cit. on p. 42).
- [Dar25a] Pierrick Dartois. “Fast computation of 2-isogenies in dimension 4 and cryptographic applications”. In: *Journal of Algebra* 683 (2025), pp. 449–514. ISSN: 0021-8693. DOI: <https://doi.org/10.1016/j.jalgebra.2025.06.033>. URL: <https://www.sciencedirect.com/science/article/pii/S0021869325003771> (cit. on p. 109).
- [Dar25b] Pierrick Dartois. “Fast computation of higher dimensional isogenies for cryptographic applications”. PhD thesis. Université de Bordeaux, France, July 2025. URL: <https://theses.fr/s364682> (cit. on pp. 17, 18, 80–82, 95, 97, 99, 109–112).
- [DD26] Pierrick Dartois and Max Duparc. *Chasing Rabbits Through Hypercubes: Better algorithms for higher dimensional 2-isogeny computations*. Cryptology ePrint Archive, Paper 2026/114. 2026. URL: <https://eprint.iacr.org/2026/114> (cit. on pp. 17, 79–81, 83, 84, 94, 95, 98–100).
- [DMPR24] Pierrick Dartois, Luciano Maino, Giacomo Pope, and Damien Robert. “An Algorithmic Approach to (2, 2)-Isogenies in the Theta Model and Applications to Isogeny-Based Cryptography”. In: *ASIACRYPT 2024, Part III*. Ed. by Kai-Min Chung and Yu Sasaki. Vol. 15486. LNCS. Springer, Singapore, Dec. 2024, pp. 304–338. DOI: [10.1007/978-981-96-0891-1_10](https://doi.org/10.1007/978-981-96-0891-1_10) (cit. on pp. 96, 98).
- [DFK+23] Luca De Feo, Tako Boris Fouotsa, Péter Kutas, Antonin Leroux, Simon-Philipp Merz, Lorenz Panny, and Benjamin Wesolowski. “SCALLOP: Scaling the CSI-FiSh”. In: *PKC 2023, Part I*. Ed. by Alexandra Boldyreva and Vladimir Kolesnikov. Vol. 13940. LNCS. Springer, Cham, May 2023, pp. 345–375. DOI: [10.1007/978-3-031-31368-4_13](https://doi.org/10.1007/978-3-031-31368-4_13) (cit. on p. 45).
- [DKLPW20] Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, and Benjamin Wesolowski. “SQISign: Compact Post-quantum Signatures from Quaternions and Isogenies”. In: *ASIACRYPT 2020, Part I*. Ed. by Shiho Moriai and Huaxiong Wang. Vol. 12491. LNCS. Springer, Cham, Dec. 2020, pp. 64–93. DOI: [10.1007/978-3-030-64837-4_3](https://doi.org/10.1007/978-3-030-64837-4_3) (cit. on p. 40).
- [DM20] Luca De Feo and Michael Meyer. “Threshold Schemes from Isogeny Assumptions”. In: *PKC 2020, Part II*. Ed. by Aggelos Kiayias, Markulf Kohlweiss, Petros Wallden, and Vassilis Zikas. Vol. 12111. LNCS. Springer, Cham, May 2020, pp. 187–212. DOI: [10.1007/978-3-030-45388-6_7](https://doi.org/10.1007/978-3-030-45388-6_7) (cit. on p. 45).
- [DH76] Whitfield Diffie and Martin E. Hellman. “New directions in cryptography”. In: *IEEE Trans. Inf. Theory* 22.6 (1976), pp. 644–654. DOI: [10.1109/TIT.1976.1055638](https://doi.org/10.1109/TIT.1976.1055638) (cit. on p. 2).

- [DHK+22] Julien Duman, Dominik Hartmann, Eike Kiltz, Sabrina Kunzweiler, Jonas Lehmann, and Doreen Riepel. “Group Action Key Encapsulation and Non-Interactive Key Exchange in the QROM”. In: *ASIACRYPT 2022, Part II*. Ed. by Shweta Agrawal and Dongdai Lin. Vol. 13792. LNCS. Springer, Cham, Dec. 2022, pp. 36–66. DOI: [10.1007/978-3-031-22966-4_2](https://doi.org/10.1007/978-3-031-22966-4_2) (cit. on pp. 23, 24, 133, 134).
- [Dup25] Max Duparc. “Superglue: Fast Formulae for (2,2)-Gluing Isogenies”. In: *ASIACRYPT 2025, Part IV*. Ed. by Goichiro Hanaoka and Bo-Yin Yang. Vol. 16248. LNCS. Springer, Singapore, Dec. 2025, pp. 372–400. DOI: [10.1007/978-981-95-5113-2_12](https://doi.org/10.1007/978-981-95-5113-2_12) (cit. on pp. 94–96, 102).
- [Eic38] Martin Eichler. “Über die Idealklassenzahl hyperkomplexer Systeme”. In: *Mathematische Zeitschrift* 43 (1938), pp. 481–494. URL: <http://eudml.org/doc/168772> (cit. on p. 66).
- [EHLMP18] Kirsten Eisenträger, Sean Hallgren, Kristin E. Lauter, Travis Morrison, and Christophe Petit. “Supersingular Isogeny Graphs and Endomorphism Rings: Reductions and Solutions”. In: *EUROCRYPT 2018, Part III*. Ed. by Jesper Buus Nielsen and Vincent Rijmen. Vol. 10822. LNCS. Springer, Cham, 2018, pp. 329–368. DOI: [10.1007/978-3-319-78372-7_11](https://doi.org/10.1007/978-3-319-78372-7_11) (cit. on p. 22).
- [EPSV23] Jonathan Komada Eriksen, Lorenz Panny, Jana Sotáková, and Mattia Veroni. *Deuring for the People: Supersingular Elliptic Curves with Prescribed Endomorphism Ring in General Characteristic*. Cryptology ePrint Archive, Report 2023/106. 2023. URL: <https://eprint.iacr.org/2023/106> (cit. on p. 75).
- [Far12] Gavril Farkas. “Theta characteristics and their moduli”. In: *Milan journal of mathematics* 80.1 (2012), pp. 1–24 (cit. on p. 115).
- [FHKP13] Eduarda S. V. Freire, Dennis Hofheinz, Eike Kiltz, and Kenneth G. Paterson. “Non-Interactive Key Exchange”. In: *PKC 2013*. Ed. by Kaoru Kurosawa and Goichiro Hanaoka. Vol. 7778. LNCS. Springer, Berlin, Heidelberg, 2013, pp. 254–271. DOI: [10.1007/978-3-642-36362-7_17](https://doi.org/10.1007/978-3-642-36362-7_17) (cit. on pp. 21–23, 131, 133).
- [FKL18] Georg Fuchsbauer, Eike Kiltz, and Julian Loss. “The Algebraic Group Model and its Applications”. In: *CRYPTO 2018, Part II*. Ed. by Hovav Shacham and Alexandra Boldyreva. Vol. 10992. LNCS. Springer, Cham, Aug. 2018, pp. 33–62. DOI: [10.1007/978-3-319-96881-0_2](https://doi.org/10.1007/978-3-319-96881-0_2) (cit. on p. 24).
- [FO99] Eiichiro Fujisaki and Tatsuaki Okamoto. “Secure Integration of Asymmetric and Symmetric Encryption Schemes”. In: *CRYPTO’99*. Ed. by Michael J. Wiener. Vol. 1666. LNCS. Springer, Berlin, Heidelberg, Aug. 1999, pp. 537–554. DOI: [10.1007/3-540-48405-1_34](https://doi.org/10.1007/3-540-48405-1_34) (cit. on p. 22).
- [GKQMS24] Phillip Gajland, Bor de Kock, Miguel Quaresma, Giulio Malavolta, and Peter Schwabe. “SWOOSH: Efficient Lattice-Based

- Non-Interactive Key Exchange”. In: *USENIX Security 2024*. Ed. by Davide Balzarotti and Wenyuan Xu. USENIX Association, Aug. 2024. URL: <https://www.usenix.org/conference/usenixsecurity24/presentation/gajland> (cit. on pp. 2, 22).
- [GSS25] Pierrick Gaudry, Julien Soumier, and Pierre-Jean Spaenlehauer. *Computing Isomorphisms between Products of Supersingular Elliptic Curves*. Cryptology ePrint Archive, Report 2025/136. 2025. URL: <https://eprint.iacr.org/2025/136> (cit. on p. 70).
- [Gee96] Bert van Geemen. “Theta functions and cycles on some abelian fourfolds”. In: *Mathematische Zeitschrift* 221.4 (1996), pp. 617–631 (cit. on pp. 19, 113, 114, 125).
- [Gee04] Bert van Geemen. “An introduction to the Hodge conjecture for abelian varieties”. In: *Algebraic Cycles and Hodge Theory: Lectures given at the 2nd Session of the Centro Internazionale Matematico Estivo (CIME) held in Torino, Italy, June 21-29, 1993*. Springer, 2004, pp. 233–252 (cit. on p. 18).
- [Hou25] Marc Houben. “Efficient Post-quantum Commutative Group Actions from Orientations of Large Discriminant”. In: *ASIACRYPT 2025, Part IV*. Ed. by Goichiro Hanaoka and Bo-Yin Yang. Vol. 16248. LNCS. Springer, Singapore, Dec. 2025, pp. 141–173. DOI: [10.1007/978-981-95-5113-2_5](https://doi.org/10.1007/978-981-95-5113-2_5) (cit. on p. 6).
- [JKP+18] Bruce W. Jordan, Allan G. Keeton, Bjorn Poonen, Eric M. Rains, Nicholas Shepherd-Barron, and John T. Tate. “Abelian varieties isogenous to a power of an elliptic curve”. English. In: *COMPOSITIO MATHEMATICA* 154.5 (May 2018), pp. 934–959. ISSN: 0010-437X. DOI: [10.1112/S0010437X17007990](https://doi.org/10.1112/S0010437X17007990) (cit. on pp. 45, 46, 55, 62, 73, 75).
- [Kem89] G.R. Kempf. “Linear systems on abelian varieties”. In: *American Journal of Mathematics* 111.1 (1989), pp. 65–94 (cit. on pp. 115–117).
- [Kob87] Neal Koblitz. “Elliptic curve cryptosystems”. In: *Mathematics of computation* 48.177 (1987), pp. 203–209 (cit. on p. 2).
- [Kup05] Greg Kuperberg. “A Subexponential-Time Quantum Algorithm for the Dihedral Hidden Subgroup Problem”. In: *SIAM Journal on Computing* 35.1 (2005), pp. 170–188. DOI: [10.1137/S0097539703436345](https://doi.org/10.1137/S0097539703436345) (cit. on pp. 3, 45).
- [LT26] Roman Langrehr and Si An Oliver Tran. *Lattice-based NIKE with optimal tightness*. Cryptology ePrint Archive, Paper 2026/1845. 2026. URL: <https://eprint.iacr.org/2026/1845> (cit. on p. 2).
- [Ler22] Antonin Leroux. “Quaternion algebras and isogeny-based cryptography”. PhD thesis. École Polytechnique, France, Sept. 2022 (cit. on pp. 26, 27).
- [LWS21] Patrick Longa, Wen Wang, and Jakub Szefer. “The Cost to Break SIKE: A Comparative Hardware-Based Analysis with AES and SHA-3”. In: *CRYPTO 2021, Part III*. Ed. by Tal Malkin and

- Chris Peikert. Vol. 12827. LNCS. Virtual Event: Springer, Cham, Aug. 2021, pp. 402–431. DOI: [10.1007/978-3-030-84252-9_14](#) (cit. on p. [139](#)).
- [Man94a] Riccardo Salvati Manni. “Modular varieties with level 2 theta structure”. In: *American Journal of Mathematics* 116.6 (1994), pp. 1489–1511 (cit. on p. [118](#)).
- [Man94b] Riccardo Salvati Manni. “On the projective varieties associated with some subrings of the ring of Thetanullwerte”. In: *Nagoya mathematical journal* 133 (1994), pp. 71–83 (cit. on p. [118](#)).
- [MMR02] G. Maze, C. Monico, and J. Rosenthal. “A public key cryptosystem based on actions by semigroups”. In: *IEEE International Symposium on Information Theory - Proceedings* (2002), p. 266 (cit. on p. [3](#)).
- [MW25] Arthur Herlédan Le Merdy and Benjamin Wesolowski. “Unconditional Foundations for Supersingular Isogeny-Based Cryptography”. In: *TCC 2025, Part III*. Ed. by Benny Applebaum and Huijia (Rachel) Lin. Vol. 16270. LNCS. Springer, Cham, Dec. 2025, pp. 266–297. DOI: [10.1007/978-3-032-12296-4_9](#) (cit. on pp. [26](#), [40](#)).
- [Mil86a] Victor S. Miller. “Use of Elliptic Curves in Cryptography”. In: *CRYPTO’85*. Ed. by Hugh C. Williams. Vol. 218. LNCS. Springer, Berlin, Heidelberg, Aug. 1986, pp. 417–426. DOI: [10.1007/3-540-39799-X_31](#) (cit. on p. [2](#)).
- [Mil86b] J. S. Milne. “Abelian Varieties”. In: *Arithmetic Geometry*. Ed. by Gary Cornell and Joseph H. Silverman. New York, NY: Springer New York, 1986, pp. 103–150. DOI: [10.1007/978-1-4613-8655-1_5](#) (cit. on pp. [40](#), [41](#), [55](#)).
- [MP24] Hart Montgomery and Sikhar Patranabis. *Public-Key Cryptography through the Lens of Monoid Actions*. Cryptology ePrint Archive, Report 2024/236. 2024. URL: <https://eprint.iacr.org/2024/236> (cit. on p. [3](#)).
- [Mum66] David Mumford. “On the equations defining abelian varieties. I”. In: *Invent. Math.* 1 (1966), pp. 287–354 (cit. on pp. [109](#), [115–117](#), [129](#)).
- [Mum74] David Mumford. *Abelian varieties*. Second Edition. Tata Institute of fundamental research studies in mathematics. London: Oxford University Press, 1974, pp. x+279 (cit. on pp. [40](#), [41](#)).
- [OS01] Katsuyuki Okeya and Kouichi Sakurai. “Efficient Elliptic Curve Cryptosystems from a Scalar Multiplication Algorithm with Recovery of the y-Coordinate on a Montgomery-Form Elliptic Curve”. In: *CHES 2001*. Ed. by Çetin Kaya Kog, David Naccache, and Christof Paar. Vol. 2162. LNCS. Springer, Berlin, Heidelberg, May 2001, pp. 126–141. DOI: [10.1007/3-540-44709-1_12](#) (cit. on p. [30](#)).

- [Onu21] Hiroshi Onuki. “On oriented supersingular elliptic curves”. In: *Finite Fields and Their Applications* 69 (2021), p. 101777. ISSN: 1071-5797. DOI: <https://doi.org/10.1016/j.ffa.2020.101777> (cit. on p. 44).
- [PW24] Aurel Page and Benjamin Wesolowski. “The Supersingular Endomorphism Ring and One Endomorphism Problems are Equivalent”. In: *EUROCRYPT 2024, Part VI*. Ed. by Marc Joye and Gregor Leander. Vol. 14656. LNCS. Springer, Cham, May 2024, pp. 388–417. DOI: [10.1007/978-3-031-58751-1_14](https://doi.org/10.1007/978-3-031-58751-1_14) (cit. on pp. 24, 26).
- [PRS26] Lorenz Panny, Damien Robert, and Alessandro Sferlazza. “Hensel-lifting black-box algorithms and fast trace computation for elliptic-curve endomorphisms.” In: *IACR Cryptol. ePrint Arch.* 2026 (2026), p. 137 (cit. on p. 114).
- [Pei20] Chris Peikert. “He Gives C-Sieves on the CSIDH”. In: *EUROCRYPT 2020, Part II*. Ed. by Anne Canteaut and Yuval Ishai. Vol. 12106. LNCS. Springer, Cham, May 2020, pp. 463–492. DOI: [10.1007/978-3-030-45724-2_16](https://doi.org/10.1007/978-3-030-45724-2_16) (cit. on p. 45).
- [Por25] Thomas Pornin. *Constant-Time Code: The Pessimist Case*. Cryptology ePrint Archive, Paper 2025/435. 2025. URL: <https://eprint.iacr.org/2025/435> (cit. on p. 28).
- [Por26] Thomas Pornin. *Montgomery Multiplication in Signed Redundant Representations*. Cryptology ePrint Archive, Paper 2026/780. 2026. URL: <https://eprint.iacr.org/2026/780> (cit. on p. 30).
- [Rei03] Irving Reiner. *Maximal Orders*. London Mathematical Society Monographs. Oxford University Press, 2003. ISBN: 9780198526735. DOI: <https://doi.org/10.1093/oso/9780198526735.001.0001> (cit. on p. 66).
- [Ren18] Joost Renes. “Computing Isogenies Between Montgomery Curves Using the Action of $(0, 0)$ ”. In: *PQCrypto 2018*. Ed. by Tanja Lange and Rainer Steinwandt. Springer, Cham, 2018, pp. 229–247. DOI: [10.1007/978-3-319-79063-3_11](https://doi.org/10.1007/978-3-319-79063-3_11) (cit. on p. 74).
- [Rob10] Damien Robert. “Theta functions and cryptographic applications”. PhD thesis. Université Henri-Poincaré, Nancy 1, France, July 2010 (cit. on pp. 109, 112, 116).
- [Rob21] Damien Robert. “Efficient algorithms for abelian varieties and their moduli spaces”. HDR thesis. Université Bordeaux, June 2021 (cit. on p. 109).
- [Rob23] Damien Robert. “A note on optimising 2^n -isogenies in higher dimension”. June 2023. URL: https://www.math.u-bordeaux.fr/~damienrobert/pro/publications/notes/2023-06-optimising_isogenies.pdf (cit. on p. 121).
- [Rob24a] Damien Robert. “Fast pairings via biextensions and cubical arithmetic”. Apr. 2024 (cit. on p. 109).

- [Rob24b] Damien Robert. *The module action for isogeny based cryptography*. Cryptology ePrint Archive, Report 2024/1556. 2024. URL: <https://eprint.iacr.org/2024/1556> (cit. on pp. 3–7, 43, 45, 71–73, 75, 77, 78, 137).
- [RS26] Joachim Rosenthal and Silvia Sconza. *Semigroup Action Problems and Their Uses in Post-Quantum Cryptography*. Cryptology ePrint Archive, Paper 2026/462. 2026. URL: <https://eprint.iacr.org/2026/462> (cit. on p. 3).
- [RS06] Alexander Rostovtsev and Anton Stolbunov. *Public-Key Cryptosystem Based On Isogenies*. Cryptology ePrint Archive, Report 2006/145. 2006. URL: <https://eprint.iacr.org/2006/145> (cit. on p. 3).
- [SPW26] Maria Corte-Real Santos, Etienne Piasecki, and Benjamin Wesolowski. *A computational framework for principally polarized abelian varieties and applications*. Cryptology ePrint Archive, Paper 2026/1142. 2026. URL: <https://eprint.iacr.org/2026/1142> (cit. on pp. 24–26).
- [Sch03] Jasper Scholten. “Weil restriction of an elliptic curve over a quadratic extension”. In: *Preprint, available at http://homes.esat.kuleuven.be/~jscholte/weilres.pdf* (2003), p. 31 (cit. on p. 71).
- [Sta24] Katherine E Stange. “Sesquilinear pairings on elliptic curves”. In: *arXiv preprint arXiv:2405.14167* (2024) (cit. on p. 131).
- [Tat66] John Tate. “Endomorphisms of Abelian Varieties over Finite Fields”. In: *Inventiones mathematicae* 2 (1966), pp. 134–144 (cit. on pp. 70, 71).
- [Voi21] John Voight. *Quaternion Algebras*. Jan. 2021, p. 877. ISBN: 978-3-030-56692-0. DOI: [10.1007/978-3-030-56694-4](https://doi.org/10.1007/978-3-030-56694-4) (cit. on pp. 40, 66).
- [Wat69] William C. Waterhouse. “Abelian varieties over finite fields”. en. In: *Annales scientifiques de l’École Normale Supérieure* Ser. 4, 2.4 (1969), pp. 521–560. DOI: [10.24033/asens.1183](https://doi.org/10.24033/asens.1183) (cit. on p. 55).
- [Wei64] André Weil. “Adeles and algebraic groups”. In: *Matematika* 8.4 (1964), pp. 3–74 (cit. on pp. 68, 69).
- [Wes22] Benjamin Wesolowski. “The supersingular isogeny path and endomorphism ring problems are equivalent”. In: *62nd FOCS*. IEEE Computer Society Press, Feb. 2022, pp. 1100–1111. DOI: [10.1109/FOCS52979.2021.00109](https://doi.org/10.1109/FOCS52979.2021.00109) (cit. on p. 40).
- [Wes26] Benjamin Wesolowski. *The supersingular isogeny problem in time and memory $p^{1/3+o(1)}$* . Cryptology ePrint Archive, Paper 2026/1486. 2026. URL: <https://eprint.iacr.org/2026/1486> (cit. on pp. 21, 134, 135).

Lasciate ogne speranza, voi ch'intrate

A Preliminaries

A.1 Supersingular elliptic curves and the Deuring correspondence

We provide here a brief introduction and refer to [Voi21, Chapter 42] for a more complete exposition. If E is an elliptic curve, its *endomorphism ring* $\text{End}(E)$ is made of all morphisms $E \rightarrow E$ (*i.e.* isogenies $E \rightarrow E$ and the zero map). We say that E is *supersingular* when it is defined over a field of characteristic $p > 0$ and when $\text{End}(E)$ is isomorphic to a maximal order in the quaternion algebra $B_{p,\infty}$ ramifying at p and ∞ . We assume $p \equiv 3 \pmod{4}$. Then $B_{p,\infty} = \mathbb{Q} \oplus \mathbb{Q}\mathbf{i} \oplus \mathbb{Q}\mathbf{j} \oplus \mathbb{Q}\mathbf{k}$ with $\mathbf{i}^2 = -1$, $\mathbf{j}^2 = -p$ and $\mathbf{k} = \mathbf{ij} = -\mathbf{ji}$. Any supersingular elliptic curve is isomorphic to an elliptic curve defined over $\mathbb{F}_{p^2}$.

Computing the endomorphism ring of a supersingular elliptic curve is generally a hard and well studied problem in isogeny based cryptography [Wes22; MW25] but there are easy instances. If $p \equiv 3 \pmod{4}$, the isomorphic supersingular elliptic curves $E_0 : y^2 = x^3 + x$ and $E'_0 : y^2 = x^3 - x$ over $\mathbb{F}_p$ of j -invariant 1728. For the latter, we have an isomorphism $[\cdot] : \mathcal{O}_0 \xrightarrow{\sim} \text{End}(E'_0)$ with $\mathcal{O}_0 := \langle 1, \mathbf{i}, (1 + \mathbf{j})/2, (\mathbf{i} - \mathbf{k})/2 \rangle$, $[\mathbf{i}] : (x, y) \mapsto (-x, \sqrt{-1}y)$ and $[\mathbf{j}] = \sigma_{E'_0} : (x, y) \mapsto (x^p, y^p)$ (the p -th Frobenius endomorphism). Note that $[(1 + \mathbf{j})/2] = (\sigma_{E'_0} + \text{id}_{E'_0})/2$ is a well defined endomorphism because the 2-torsion is $\mathbb{F}_p$ -rational $E'_0[2] \subseteq E'_0(\mathbb{F}_p) = \ker(\sigma_{E'_0} - \text{id}_{E'_0})$.

Under the Deuring correspondence, if E is a supersingular elliptic curve of endomorphism ring isomorphic to $\mathcal{O} \subset B_{p,\infty}$, every left $\mathcal{O}$ -ideal I corresponds to an isogeny $\varphi_I : E \rightarrow E_I$ (unique up to post-composition by an isomorphism). Then $\text{End}(E_I)$ is isomorphic to $\mathcal{O}_R(I) = \{\alpha \in B_{p,\infty} \mid I\alpha \subseteq I\}$ for which I is a right ideal. We also have $I \simeq \text{Hom}(E_I, E)$ and $\deg(\varphi_I) = \text{nrd}(I) = \sqrt{[\mathcal{O} : I]}$ (the *reduced norm* of I). Conversely, any isogeny $\varphi : E \rightarrow E'$ corresponds to an ideal I_φ , which is a left ideal for $\mathcal{O} \simeq \text{End}(E)$ and a right ideal for $\mathcal{O}' \simeq \text{End}(E')$. The Deuring correspondence satisfies convenient multiplicativity properties that are summarised in [DKLPW20, Table 1].

A.2 Abelian varieties and their isogenies

Abelian varieties are non-trivial objects and we only recall their basic properties that are relevant to this paper. We refer to [Mum74; Mil86b] for a complete introduction. An *abelian variety* A over a field k (denoted A/k) is a projective k -variety¹⁵ with an abelian group law. Abelian varieties can be seen as generalisations of elliptic curves in any dimension. For instance, products of g elliptic curves are abelian varieties of dimension g . In our applications, we consider abelian varieties of dimensions one (elliptic curves), two (abelian surfaces) and

¹⁵ Informally, a projective k -variety can be seen as zeros of a set of homogeneous multivariate polynomials over k .

four (abelian fourfolds). We summarise below some key properties of abelian varieties and refer to [Mil86b; Mum74] for a complete introduction.

An *isogeny* $\varphi : A \rightarrow B$ between abelian varieties is a morphism (as varieties¹⁶ and groups) which is surjective and of finite kernel. In particular, an isogeny preserves the dimension $\dim(A) = \dim(B)$. The *degree* of an isogeny is defined as an extension degree of function fields $\deg(\varphi) = [k(A) : \varphi^*k(B)]$, as for elliptic curve isogenies. When φ is *separable* (e.g. when $\text{char}(k) \nmid \deg(\varphi)$), we have $\deg(\varphi) = \# \ker(\varphi)$ and φ is determined by its kernel up to post-composition by an isomorphism.

Every abelian variety A/k has a *dual* $A^\vee/k$ of the same dimension. The dual defines a contravariant functor, which means that every isogeny $\varphi : A \rightarrow B$ has a dual $\varphi^\vee : B^\vee \rightarrow A^\vee$ and that the dual of a composition of isogenies $\psi \circ \varphi$ is $\varphi^\vee \circ \psi^\vee$. The dual also preserves the degree $\deg(\varphi^\vee) = \deg(\varphi)$. Finally, the dual is an involution: $A^{\vee\vee} = A$ and $\varphi^{\vee\vee} = \varphi$.

A *polarisation* is an isogeny $\lambda_A : A \rightarrow A^\vee$ such that $\lambda_A^\vee = \lambda_A$. We say that (A, λ_A) is a *polarised* abelian variety and that (A, λ_A) is a *principally polarised abelian variety* (PPAV) if λ_A is *principal* i.e. an isomorphism. If d is a non-negative integer, a *d-isogeny* $\varphi : (A, \lambda_A) \rightarrow (B, \lambda_B)$ between PPAVs satisfies $\varphi^\vee \circ \lambda_A \circ \varphi = [d]\lambda_B$, where $[d]$ is the scalar multiplication by d (which is an isogeny). We then also say that φ is a *polarised isogeny* and call d its *polarised degree*. In that case, we have $\deg(\varphi) = d^g$ with $g = \dim(A) = \dim(B)$.

If $\varphi : A \rightarrow B$ is an isogeny between PPAVs (A, λ_A) and (B, λ_B) , we define its *contragradient isogeny* $\tilde{\varphi} := \lambda_A^{-1} \circ \varphi^\vee \circ \lambda_B : B \rightarrow A$. Then $\deg(\varphi) = \deg(\tilde{\varphi})$ and φ is a *d-isogeny* if and only if $\tilde{\varphi} \circ \varphi = [d]$.

If $n \in \mathbb{Z}_{>0}$ is not divisible by $\text{char}(k)$, the n -th Weil pairing is a non-degenerate anti-symmetric bilinear form $e_n : A[n] \times A^\vee[n] \rightarrow \bar{k}^*$. If $\lambda_A : A \rightarrow A^\vee$ is a polarisation of A , we obtain a pairing $e_n^{\lambda_A} : (P, Q) \in A[n] \times A[n] \rightarrow e_n(P, \lambda_A(Q)) \in \bar{k}^*$. We say that a subgroup $K \subset A[n]$ is *isotropic* (with respect to λ_A) when $e_n^{\lambda_A}(P, Q) = 1$ for all $P, Q \in K$. It is *maximal isotropic* if it is maximal for inclusion for this property.

A.3 Modules over a quadratic imaginary order

In the following, we fix K a quadratic imaginary field and $R \subset K$ an order of K . An R -module satisfies the same properties as a vector space with a scalar multiplication by the ring R instead of a field. Let M be an R -module. We say that M is *finitely generated* if there exists $x_1, \dots, x_n \in M$ such that every element $x \in M$ can be written as a linear combination $x = \sum_{i=1}^n \lambda_i x_i$ with $\lambda_1, \dots, \lambda_n \in R$. If M is finitely generated, the *rank* of M is the dimension of $K \otimes_R M$ as a K -vector space. In this paper, we only work with finitely generated R -modules abbreviated as *fg* R -modules. An element $x \in M$ is *of torsion* if there exists $r \in R \setminus \{0\}$ such that $r \cdot x = 0$. We say that M is *of torsion* if all of its elements are of torsion and *torsion free* if 0 is the only element of torsion in

¹⁶ Meaning it can be expressed with multivariate rational fractions.

M . Similarly to linear morphisms, a morphism of R -modules $\phi : M_1 \rightarrow M_2$ is additive, maps $0 \mapsto 0$ and is R -linear.

Since R is an order in a quadratic imaginary field, it is Noetherian (its ideals are finitely generated), which ensures that submodules of finitely generated R -modules are also finitely generated. As a consequence, a finitely generated R -module M is always *finitely presented*, i.e. it admits a *finite presentation* defined as an exact sequence:

$$R^n \xrightarrow{j} R^m \xrightarrow{s} M \longrightarrow 0,$$

i.e. a sequence of morphisms of R -modules with s surjective and $\ker(s) = \text{im}(j)$. In other words, a finite presentation is given by a set of generators (defining the surjective morphism s) and a finitely generated module of relations between these generators ($\ker(s) = \text{im}(j)$).

We say that a fg R -module M is *projective* if it is a direct summand of a free module i.e. if there exists $n \in \mathbb{N}$ and an R -module M' such that $R^n = M \oplus M'$. In particular, projective modules are torsion free but the converse is false in general.

Remark A.1. However, when $R = \mathfrak{O}_K$ is the maximal order, R is a Dedekind domain [BK00, Theorem 5.2.15], which ensures that every fg and torsion free R -module is projective [BK00, Corollary 6.3.4]. This remark and the following theorem giving the structure of fg modules over a Dedekind domain will become very important in [Appendix B.4](#) and further.

Theorem A.1. *Assume R is a Dedekind domain ($R = \mathfrak{O}_K$) and let M be a finitely generated R -module. Then:*

- (i) $M = P \oplus T$, where P is a torsion free R -module and T is an R -module of torsion.
- (ii) There exist ideals $\mathfrak{a}_1, \dots, \mathfrak{a}_n \subseteq R$ such that $P \simeq \bigoplus_{i=1}^n \mathfrak{a}_i$.
- (iii) If $\mathfrak{a}_1, \dots, \mathfrak{a}_n, \mathfrak{b}_1, \dots, \mathfrak{b}_m \subseteq R$ are R -ideals, then $\bigoplus_{i=1}^n \mathfrak{a}_i \simeq \bigoplus_{j=1}^m \mathfrak{b}_j$ if and only if $n = m$ and $[\prod_{i=1}^n \mathfrak{a}_i] = [\prod_{j=1}^m \mathfrak{b}_j]$ in $\text{Cl}(R)$.
- (iv) There exist ideals $\mathfrak{c}_1, \dots, \mathfrak{c}_n \subseteq R$ such that $T \simeq \bigoplus_{i=1}^n R/\mathfrak{c}_i$.

Proof. (i)-(iii) are proved in [BK00]. For (i) see Theorem 6.3.5, for (ii) see Theorem 6.1.2, (iii) is Steinitz's theorem (6.1.6). For (iv), see [Cur62, Corollary 22.16]. $\square$

An R -lattice M is an R -module such that there exists an embedding (i.e. an injective morphism of R -modules) $M \hookrightarrow K^n$ (with $n \in \mathbb{N}$). By rescaling, we can always assume we have an embedding $M \hookrightarrow R^n$. We can always consider the embedding $M \hookrightarrow K \otimes_R M \simeq R^n$ with $n := \text{rank}(M)$. In particular, R -lattices are finitely generated and torsion free. Conversely, when R is Dedekind ($R = \mathfrak{O}_K$), [Theorem A.1.\(ii\)](#) ensures that fg torsion free R -modules are R -lattices. Then, when $R = \mathfrak{O}_K$, we only need to consider R -lattices and torsion fg R -modules whose decomposition is given by [Theorem A.1.\(iv\)](#).

We shall now see an analogy between modules and abelian varieties involving isogenies, duality and polarisations. This analogy, using the vocabulary introduced in [Rob24b], becomes relevant in Section 2.4. A *module isogeny* $\phi : M_1 \rightarrow M_2$ is a morphism of R -lattices which is injective and of finite cokernel $\text{coker}(\phi) := M_2 / \text{im}(\phi)$. Equivalently, $\phi : M_1 \rightarrow M_2$ is an isogeny if it is injective and $\text{rank}(M_1) = \text{rank}(M_2)$ or if it has finite cokernel and $\text{rank}(M_1) = \text{rank}(M_2)$.

Since $R \subset K$ is quadratic imaginary, the complex conjugation induces an automorphism of R . For any fg R -module M , we can then consider its module of R -antilinear forms $\text{Hom}_{\overline{R}}(M, R)$ made of maps $f : M \rightarrow R$ such that for all $x, y \in M$, $\lambda, \mu \in R$, $f(\lambda x + \mu y) = \overline{\lambda}f(x) + \overline{\mu}f(y)$. We call $\text{Hom}_{\overline{R}}(M, R)$ the *dual* of M and denote it by $M^\vee$. As for abelian varieties, we can identify a projective fg R -module (e.g. an R -lattice with $R = \mathfrak{O}_K$) M with $M^{\vee\vee}$ via the canonical isomorphism $m \mapsto (\phi \mapsto \overline{\phi(m)})$ [Bou74, Chapter II, § 2.7, Corollary 4]. The duality is also functorial, since every morphism $\phi : M_1 \rightarrow M_2$ admits a dual $\phi^\vee : f \in M_2^\vee \rightarrow f \circ \phi \in M_1^\vee$ which is also an isogeny.¹⁷

Let V be finite dimensional K -vector space (e.g. $V = K^n$). A *sesquilinear form* of V is a map $H : V \times V \rightarrow K$ that is K -linear on the left and K -antilinear on the right. A sesquilinear form is:

- *Hermitian* when for all $x, y \in V$, $\overline{H(x, y)} = H(y, x)$;
- *Positive definite* when $H(x, x) \in \mathbb{R}_{>0}$ for all $x \in V \setminus \{0\}$.

By abuse, we refer to positive definite Hermitian sesquilinear forms as *Hermitian forms* throughout the paper. If $H : V \times V \rightarrow K$ is a Hermitian form and $M \subset V$ is an R -lattice, we define the R -lattice:

$$M^{\sharp, H} := \{x \in V \mid \forall y \in M, H(x, y) \in R\},$$

simply abbreviated as $M^\sharp$ when there is no ambiguity on H . We have an isomorphism $M^\sharp \xrightarrow{\sim} M^\vee, x \mapsto H(x, \cdot)$. By analogy with polarised abelian varieties, we say that H is a *polarisation* on M or that (H, M) is *polarised* when $M^\sharp \subseteq M$. In that case, H is *integral* on $M^\sharp$: for all $x, y \in M^\sharp$, $H(x, y) \in R$. We also have an isogeny $\phi_H : M^\vee \simeq M^\sharp \hookrightarrow M$. By analogy with PPAVs, we say that (H, M) is *unimodular* when ϕ_H is an isomorphism i.e. that $M = M^\sharp$.

To complete this analogy, given an isogeny $\phi : (M_1, H_1) \rightarrow (M_2, H_2)$ between polarised modules, we define its adjoint $\phi^\sharp$ as an isogeny $(M_2^\sharp, H_2) \rightarrow (M_1^\sharp, H_1)$ satisfying $H_2(x, \phi(y)) = H_1(\phi^\sharp(x), y)$ for all $x \in M_2$ and $y \in M_1$. When (M_1, H_1) and (M_2, H_2) are unimodular, we say that ϕ is a *d-similitude* when $\phi^* H_2 = d H_1$ i.e. when $H_2(\phi(x), \phi(y)) = d H_1(x, y)$ for all $x, y \in M_1$. This is equivalent to $\phi^\sharp \circ \phi = d \text{id}_{M_1}$ or equivalently $\phi^\vee \circ \phi_{H_2} \circ \phi = d \phi_{H_1}$ (since $\phi^\sharp = \phi_{H_1}^{-1} \circ \phi^\vee \circ \phi_{H_2}$ by definition), formulae we have already seen for d -isogenies between PPAVs.

A.4 Categories and functors

A *category* is a collection of objects with morphisms between these objects that can be composed (e.g. R -modules or abelian varieties with their morphisms).

A (covariant) functor $F : \mathcal{C} \rightarrow \mathcal{D}$ between categories $\mathcal{C}$ and $\mathcal{D}$ maps objects and morphisms of $\mathcal{C}$ to objects and morphisms of $\mathcal{D}$ in a way that respects composition: if $f : C_1 \rightarrow C_2$ and $g : C_2 \rightarrow C_3$ are morphisms of $\mathcal{C}$, then $F(f) : F(C_1) \rightarrow F(C_2)$ and $F(g) : F(C_2) \rightarrow F(C_3)$ satisfy $F(g \circ f) = F(g) \circ F(f) : F(C_1) \rightarrow F(C_3)$. The functor should also map the identity id_C of an object C of $\mathcal{C}$ to the identity $F(\text{id}_C) = \text{id}_{F(C)}$. A contravariant functor $F : \mathcal{C} \rightarrow \mathcal{D}$ is a functor $\mathcal{C} \rightarrow \mathcal{D}^{\text{op}}$, where $\mathcal{D}^{\text{op}}$ is the *opposite category* of $\mathcal{D}$ obtained by seeing morphisms $h : D_1 \rightarrow D_2$ as morphisms $h^{\text{op}} : D_2 \rightarrow D_1$. In particular, a contravariant functor satisfies $F(g \circ f) = F(f) \circ F(g)$ with f and g as before.

If $\mathcal{C}$ and $\mathcal{D}$ have a zero object (initial object), we say that a functor $F : \mathcal{C} \rightarrow \mathcal{D}$ is *left exact* if it maps an exact sequence $0 \rightarrow C_1 \xrightarrow{f} C_2 \xrightarrow{g} C_3$ to an exact sequence $0 \rightarrow F(C_1) \xrightarrow{F(f)} F(C_2) \xrightarrow{F(g)} F(C_3)$ (with arrows reversed if F is contravariant). Similarly, we say F is *right exact* if it maps an exact sequence $C_1 \xrightarrow{f} C_2 \xrightarrow{g} C_3 \rightarrow 0$ to an exact sequence $F(C_1) \xrightarrow{F(f)} F(C_2) \xrightarrow{F(g)} F(C_3) \rightarrow 0$ (with arrows reversed if F is contravariant). We say F is *exact* if it is both left and right exact.

Though theoretical, the functorial point of view is crucial to introduce the module action (especially in [Appendix B.1](#)). As illustrated in [Theorem 2.1](#), when $R = \mathfrak{O}_K$, this action maps R -modules to abelian varieties and morphisms of R -modules to morphisms of abelian varieties in a functorial way.

A.5 Oriented supersingular elliptic curves and abelian varieties

Let R be an order in a quadratic imaginary field. An R -orientation of an abelian variety A is an embedding $\iota : R \hookrightarrow \text{End}(A)$. We say that (A, ι) is R -oriented. We say that ι is *primitive* or that (A, ι) is *primitively oriented* when ι cannot be extended to a superorder of R .

When (E, ι) is an R -oriented supersingular elliptic curve and $\mathfrak{a} \subseteq R$ is an invertible ideal, the result of the action of $\mathfrak{a} \cdot (E, \iota) := (\mathfrak{a} \cdot E, \iota_{\mathfrak{a}})$ is defined as the codomain $E_{\mathfrak{a}}$ of the isogeny $\varphi_{\mathfrak{a}} : E \rightarrow \mathfrak{a} \cdot E$ with kernel:

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

and the orientation $\iota_{\mathfrak{a}} : \beta \in R \mapsto 1/N(\mathfrak{a}) \cdot \varphi_{\mathfrak{a}} \circ \iota(\beta) \circ \widehat{\varphi}_{\mathfrak{a}}$. We obtain that $\mathfrak{a} \cdot (E, \iota)$ is isomorphic to (E, ι) (with respect to the orientation) if and only if $\mathfrak{a}$ is principal. As a consequence, this defines a free action of $\text{Cl}(R)$ on R -oriented supersingular curves [[CK20](#), Theorem 7] (with at most two orbits [[Onu21](#), Proposition 3.3]).

An example we use throughout this paper (and for MIKE in particular) is the Frobenius orientation [[CLMPR18](#); [CD20](#)]. If E is supersingular and defined over $\mathbb{F}_p$ ($p \equiv 3 \pmod{4}$), the Frobenius $\sigma_E : (x, y) \mapsto (x^p, y^p)$ is an endomorphism of E such that $\sigma_E^2 = [-p]$. It defines an orientation $\mathbb{Z}[\sqrt{-p}] \hookrightarrow \text{End}(E)$. This orientation is either primitive (we say E is on the *floor* of the isogeny Volcano) or can be extended to a primitive orientation of the maximal order $\mathbb{Z}[(\sqrt{-p} - 1)/2] \hookrightarrow \text{End}(E)$ (we say E is on the *surface*).

The ideal class group action on oriented elliptic curves has been widely used in cryptography, to build key exchanges [CLMPR18; CK20; DFK+23], digital signatures [BKV19] and more advanced schemes [ADMP20; DM20], all affected by Kuperberg’s quantum subexponential attack [Kup05; BS20; Pei20; CSCJR22]. In this paper, following [JKP+18; Rob24b], we extend this action to R -modules and R -oriented abelian varieties that naturally generalise this action and explain how to build the key exchange MIKE from it, which is immune to Kuperberg’s attack.

B A complete introduction to the module action

The explicit construction of the module action introduced in Section 2.1 is the correct one to compute it effectively. However, this construction is not convenient to prove elementary properties of the module action that follow from a more general theory. For that reason, we introduce in Appendix B.1 the conceptual construction of the module action from [JKP+18; Rob24b]. With this framework, in Appendices B.2 and B.3, we prove the functoriality properties of the module action. In Appendix B.4, this allows us to prove Theorems 2.1 to 2.3 and the equivalence of the effective construction from Section 2.1 with the conceptual one on abelian varieties oriented by a maximal order. In Appendix B.5, we prove the properties from Section 2.4 relating Hermitian modules to polarisations. Finally, we generalise the module action to quaternionic modules in Appendix B.6. Though not introduced in the main body of the paper, this generalisation will become useful in Appendix G.1 to compute MIKE invariants. This section contains little novelty compared to our main references [JKP+18; Rob24b], but we give the proofs in more detail and when possible, in a more elementary language, which also makes our paper self contained. Throughout this section, R will be an order in a quadratic imaginary field K .

B.1 A conceptual construction

In the following, we shall need to work with a bigger category than R -oriented abelian varieties and their morphisms. This category should not only encompass (R -oriented) abelian varieties but also (R -oriented) finite abelian group schemes¹⁸ and their products. Therefore, we consider the category $\mathcal{A}_R$ of R -oriented *Abelian Proper Group Schemes* (APGS) and their morphisms. An object $(A, \iota) \in \mathcal{A}_R$ is an APGS with an R -orientation $\iota : R \hookrightarrow \text{End}(A)$ defined, as previously, as an embedding. A morphism of $\mathcal{A}_R$, called R -oriented morphism of APGS, $\varphi : (A, \iota_A) \rightarrow (B, \iota_B)$ is a morphism of groups schemes that satisfies $\varphi \circ \iota_A(\alpha) = \iota_B(\alpha) \circ \varphi$ for all $\alpha \in R$.

We also extend the category of modules we work with from R -lattices to finitely generated (fg) R -modules. We recall from Appendix A.3 that finitely generated R -modules are also finitely presented. The general construction of the module action is then given by the following.

¹⁸ *e.g.* torsion subgroups of abelian varieties.

Definition B.1. Let (A, ι) be an R -oriented APGS and M be a finitely generated (fg) R -module, with a following finite presentation $R^n \rightarrow R^m \rightarrow M \rightarrow 0$. Denote by $X := (X_{i,j})_{i,j} \in M_{m,n}(R)$ the matrix of the morphism $R^n \rightarrow R^m$ given by left multiplication of column vectors and consider the morphism $\iota(X^T) : A^m \rightarrow A^n$:

$$P := (P_j)_{1 \leq j \leq m} \mapsto \iota(X^T)(P) := \left(\sum_{j=1}^m \iota(X_{j,i})(P_j) \right)_{1 \leq i \leq n},$$

induced by left multiplication by X^T . We denote by $M \star A$ the kernel of this morphism $M \star A := \ker(\iota(X^T))$.

We still need to check that [Definition B.1](#) makes sense. First, $M \star A$ is indeed R -oriented via the orientation of A^m induced by ι . Note that this was not obvious with the definition of $M \cdot A$ in [Section 2.2](#). We now check that the construction of $M \star A$ does not depend on the finite presentation of M . It is a consequence of the following universal property.

Theorem B.1. [[JKP+18](#), § 4.1] $M \star A$ is the unique R -oriented APGS (up to R -oriented isomorphism) such that for every R -oriented APGS B , there exists a canonical isomorphism

$$\mathrm{Hom}_{\mathcal{A}_R}(B, M \star A) \cong \mathrm{Hom}_R(M, \mathrm{Hom}_{\mathcal{A}_R}(B, A)).$$

Note that the set of R -oriented homomorphisms $\mathrm{Hom}_{\mathcal{A}_R}(B, A)$ has an R -module structure induced by the R -orientation of A , so the right term above is well defined.

Proof. Consider a finite presentation of M :

$$R^n \xrightarrow{X} R^m \rightarrow M \rightarrow 0, \quad (2)$$

where $X \in M_{m,n}(R)$ is the matrix of the first morphism. By the above construction, this presentation induces an exact sequence:

$$0 \rightarrow M \star A \rightarrow A^m \xrightarrow{\iota(X^T)} A^n. \quad (3)$$

Then, on the one hand, applying for any $B \in \mathcal{A}_R$, the functor $\mathrm{Hom}_R(-, \mathrm{Hom}_{\mathcal{A}_R}(B, A))$ to [Equation \(2\)](#), we obtain the exact sequence:

$$\begin{aligned} 0 \rightarrow \mathrm{Hom}_R(M, \mathrm{Hom}_{\mathcal{A}_R}(B, A)) &\rightarrow \mathrm{Hom}_R(R^m, \mathrm{Hom}_{\mathcal{A}_R}(B, A)) \\ &\xrightarrow{- \circ X} \mathrm{Hom}_R(R^n, \mathrm{Hom}_{\mathcal{A}_R}(B, A)). \end{aligned} \quad (4)$$

On the other hand, applying the functor $\mathrm{Hom}_{\mathcal{A}_R}(-, M \star A)$ to [Equation \(3\)](#), we obtain the exact sequence:

$$0 \rightarrow \mathrm{Hom}_{\mathcal{A}_R}(B, M \star A) \rightarrow \mathrm{Hom}_{\mathcal{A}_R}(B, A^m) \xrightarrow{\iota(X^T) \circ -} \mathrm{Hom}_{\mathcal{A}_R}(B, A^n). \quad (5)$$

Note that we have a canonical isomorphism:

$$\begin{aligned} \text{Hom}_R(R^m, \text{Hom}_{\mathcal{A}_R}(B, A)) &\xrightarrow{\sim} \text{Hom}_{\mathcal{A}_R}(B, A^m) \\ (\mathbf{r} \mapsto \phi_{\mathbf{r}}) &\mapsto \left(b \mapsto (\phi_{\mathbf{e}_1}(b), \dots, \phi_{\mathbf{e}_m}(b)) \right), \end{aligned} \quad (6)$$

where $(\mathbf{e}_1, \dots, \mathbf{e}_m)$ is the canonical basis of R^m . We similarly have a canonical isomorphism $\text{Hom}_R(R^n, \text{Hom}_{\mathcal{A}_R}(B, A)) \cong \text{Hom}_{\mathcal{A}_R}(B, A^n)$, from which we obtain an isomorphism of the exact sequences (4) and (5), *i.e.* a commutative diagram:

$$\begin{array}{ccccccc} 0 \rightarrow \text{Hom}_R(M, \text{Hom}_{\mathcal{A}_R}(B, A)) & \rightarrow & \text{Hom}_R(R^m, \text{Hom}_{\mathcal{A}_R}(B, A)) & \rightarrow & \text{Hom}_R(R^n, \text{Hom}_{\mathcal{A}_R}(B, A)) \\ & \downarrow \wr & \downarrow \wr & & \downarrow \wr \\ 0 \longrightarrow \text{Hom}_{\mathcal{A}_R}(B, M \star A) & \longrightarrow & \text{Hom}_{\mathcal{A}_R}(B, A^m) & \longrightarrow & \text{Hom}_{\mathcal{A}_R}(B, A^n) \end{array}$$

Fig. 5

It follows that $\text{Hom}_R(M, \text{Hom}_{\mathcal{A}_R}(B, A)) \cong \text{Hom}_{\mathcal{A}_R}(B, M \star A)$, as desired.

Now, we prove the object $M \star A \in \mathcal{A}_R$ satisfying this property is unique up to isomorphism. The strategy is to prove that the isomorphism

$$\eta_B : \text{Hom}_R(M, \text{Hom}_{\mathcal{A}_R}(B, A)) \xrightarrow{\sim} \text{Hom}_{\mathcal{A}_R}(B, M \star A)$$

is functorial in B *i.e.* induces a natural transformation and then to apply [Lemma B.1](#), which follows from Yoneda's lemma. If $\varphi : B \rightarrow C$ is a morphism of R -oriented APGS, we then have to prove that the following diagram is commutative:

$$\begin{array}{ccc} \text{Hom}_R(M, \text{Hom}_{\mathcal{A}_R}(C, A)) & \xrightarrow{- \circ \varphi} & \text{Hom}_R(M, \text{Hom}_{\mathcal{A}_R}(B, A)) \\ \eta_C \downarrow \wr & & \eta_B \downarrow \wr \\ \text{Hom}_{\mathcal{A}_R}(C, M \star A) & \xrightarrow{- \circ \varphi} & \text{Hom}_{\mathcal{A}_R}(B, M \star A) \end{array}$$

Fig. 6

We can easily prove that the following diagram with the isomorphisms from [Equation \(6\)](#) (with B and C) as vertical arrows commute:

$$\begin{array}{ccc}
\mathrm{Hom}_R(R^m, \mathrm{Hom}_{\mathcal{A}_R}(C, A)) & \xrightarrow{- \circ \varphi} & \mathrm{Hom}_R(R^m, \mathrm{Hom}_{\mathcal{A}_R}(B, A)) \\
\downarrow \wr & & \downarrow \wr \\
\mathrm{Hom}_{\mathcal{A}_R}(C, A^m) & \xrightarrow{- \circ \varphi} & \mathrm{Hom}_{\mathcal{A}_R}(B, A^m)
\end{array}$$

and we have similar diagrams with n instead of m . From the isomorphism η_B induced by Figure 5 (and its analog with C instead of B), we then obtain the commutativity of Figure 6, which proves indeed that $B \mapsto \eta_B$ is a natural transformation. By Lemma B.1, this proves the unicity of $M \star A$ up to unique R -oriented isomorphism. $\square$

Lemma B.1. *Let $\mathcal{C}$ be a small category and $F : \mathcal{C} \rightarrow \mathbf{Set}$ be a contravariant functor represented by $A \in \mathcal{C}$ i.e. naturally isomorphic to $\mathrm{Hom}_{\mathcal{C}}(-, A)$. Then all objects of $\mathcal{C}$ representing F are isomorphic to A .*

Proof. Let $A, A' \in \mathcal{C}$ be two representatives of F . Then we have natural isomorphisms $F \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{C}}(-, A)$ and $F \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{C}}(-, A')$, so by composing the two we obtain a natural isomorphism $\eta : \mathrm{Hom}_{\mathcal{C}}(-, A) \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{C}}(-, A')$. By Yoneda's lemma, the natural transformations $\xi : \mathrm{Hom}_{\mathcal{C}}(-, A) \rightarrow \mathrm{Hom}_{\mathcal{C}}(-, A')$ are in bijection with $\mathrm{Hom}_{\mathcal{C}}(A, A')$ via the map $\xi \mapsto \xi_A(\mathrm{id}_A)$. It follows that $\eta : \mathrm{Hom}_{\mathcal{C}}(-, A) \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{C}}(-, A')$ is fully determined by $\eta_A(\mathrm{id}_A) \in \mathrm{Hom}_{\mathcal{C}}(A, A')$. By naturality of η , we obtain the commutative diagram:

$$\begin{array}{ccc}
\mathrm{Hom}_{\mathcal{C}}(A', A) & \xrightarrow{- \circ \eta_A(\mathrm{id}_A)} & \mathrm{End}_{\mathcal{C}}(A) \\
\eta_{A'} \downarrow \wr & & \eta_A \downarrow \wr \\
\mathrm{End}_{\mathcal{C}}(A') & \xrightarrow{- \circ \eta_A(\mathrm{id}_A)} & \mathrm{Hom}_{\mathcal{C}}(A, A')
\end{array}$$

This means that for all $f \in \mathrm{Hom}_{\mathcal{C}}(A', A)$, we have $\eta_{A'}(f) \circ \eta_A(\mathrm{id}_A) = \eta_A(f \circ \eta_A(\mathrm{id}_A))$. In particular, setting $f := \eta_{A'}^{-1}(\mathrm{id}_{A'})$, we obtain $\eta_A(\mathrm{id}_A) = \eta_A(\eta_{A'}^{-1}(\mathrm{id}_{A'}) \circ \eta_A(\mathrm{id}_A))$ i.e. $\mathrm{id}_A = \eta_{A'}^{-1}(\mathrm{id}_{A'}) \circ \eta_A(\mathrm{id}_A)$ which proves that $\eta_A(\mathrm{id}_A)$ has a left inverse. Applying Yoneda's lemma again to $\eta^{-1} : \mathrm{Hom}_{\mathcal{C}}(-, A') \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{C}}(-, A)$, we obtain similarly that $\mathrm{id}_{A'} = \eta_A(\mathrm{id}_A) \circ \eta_{A'}^{-1}(\mathrm{id}_{A'})$, which proves that $\eta_A(\mathrm{id}_A)$ is invertible, i.e. that it is an isomorphism $A \xrightarrow{\sim} A'$. $\square$

From Theorem B.1, we can easily prove the following properties of the module action.

Proposition B.1. *Let A be an R -oriented APGS and M_1, M_2 be fg R -modules. Then:*

- (i) *If $M_1 \simeq M_2$ then $M_1 \star A \simeq M_2 \star A$.*
- (ii) *$(M_1 \oplus M_2) \star A \cong (M_1 \star A) \oplus (M_2 \star A)$.*
- (iii) *$R^n \star A \cong A^n$ for all $n \in \mathbb{N}$.*
- (iv) *$M_1 \star (M_2 \star A) \simeq (M_1 \otimes M_2) \star A \simeq M_2 \star (M_1 \star A)$.*

Proof. (i) Assume that $M_1 \simeq M_2$. Then for all R -oriented APGS B , we have by [Theorem B.1](#):

$$\begin{aligned} \text{Hom}_{\mathcal{A}_R}(B, M_1 \star A) &\cong \text{Hom}_R(M_1, \text{Hom}_{\mathcal{A}_R}(B, A)) \simeq \text{Hom}_R(M_2, \text{Hom}_{\mathcal{A}_R}(B, A)) \\ &\cong \text{Hom}_{\mathcal{A}_R}(B, M_2 \star A) \end{aligned}$$

By unicity in [Theorem B.1](#), it follows that $M_1 \star A \simeq M_2 \star A$.

(ii) For all R -oriented APGS B , we have by [Theorem B.1](#):

$$\begin{aligned} \text{Hom}_{\mathcal{A}_R}(B, (M_1 \oplus M_2) \star A) &\cong \text{Hom}_R(M_1 \oplus M_2, \text{Hom}_{\mathcal{A}_R}(B, A)) \\ &\cong \text{Hom}_R(M_1, \text{Hom}_{\mathcal{A}_R}(B, A)) \\ &\quad \oplus \text{Hom}_R(M_2, \text{Hom}_{\mathcal{A}_R}(B, A)) \\ &\cong \text{Hom}_{\mathcal{A}_R}(B, M_1 \star A) \oplus \text{Hom}_{\mathcal{A}_R}(B, M_2 \star A) \\ &\cong \text{Hom}_{\mathcal{A}_R}(B, (M_1 \star A) \oplus (M_2 \star A)) \end{aligned}$$

Again, this ensures that $(M_1 \oplus M_2) \star A$ and $(M_1 \star A) \oplus (M_2 \star A)$ are canonically isomorphic.

(iii) Let $n \in \mathbb{N}$. Applying (iii) to $R^n = \bigoplus_{i=1}^n R$, we obtain that $R^n \star A \cong (R \star A)^n$. By [Theorem B.1](#), we also have for all R -oriented APGS B :

$$\text{Hom}_{\mathcal{A}_R}(B, R \star A) \cong \text{Hom}_R(R, \text{Hom}_{\mathcal{A}_R}(B, A)) \cong \text{Hom}_{\mathcal{A}_R}(B, A),$$

which ensures that $R \star A \cong A$, so that $R^n \star A \cong A^n$.

(iv) By [Theorem B.1](#), for all R -oriented APGS B , we have:

$$\begin{aligned} \text{Hom}_{\mathcal{A}_R}(B, M_1 \star (M_2 \star A)) &\cong \text{Hom}_R(M_1, \text{Hom}_{\mathcal{A}_R}(B, M_2 \star A)) \\ &\cong \text{Hom}_R(M_1, \text{Hom}_R(M_2, \text{Hom}_{\mathcal{A}_R}(B, A))) \\ &\cong \text{Hom}_R(M_1 \otimes M_2, \text{Hom}_{\mathcal{A}_R}(B, A)) \\ &\cong \text{Hom}_{\mathcal{A}_R}(B, (M_1 \otimes M_2) \star A) \end{aligned}$$

where the penultimate isomorphism follows from the fact that the tensor product is left adjoint to Hom . It follows by unicity in [Theorem B.1](#) that $M_1 \star (M_2 \star A) \simeq (M_1 \otimes M_2) \star A$. We obtain similarly that:

$$\begin{aligned} \text{Hom}_{\mathcal{A}_R}(B, M_2 \star (M_1 \star A)) &\cong \text{Hom}_R(M_2 \otimes M_1, \text{Hom}_{\mathcal{A}_R}(B, A)) \\ &\cong \text{Hom}_R(M_1 \otimes M_2, \text{Hom}_{\mathcal{A}_R}(B, A)) \\ &\cong \text{Hom}_{\mathcal{A}_R}(B, (M_1 \otimes M_2) \star A) \end{aligned}$$

We conclude similarly by unicity in [Theorem B.1](#) that $M_2 \star (M_1 \star A) \simeq (M_1 \otimes M_2) \star A$. $\square$

The universal property of [Theorem B.1](#) can also be used to prove that the module action is compatible with ring extension.

Proposition B.2. *Let $S \supseteq R$ be a superorder of R , M be a fg R -module and A be an S -oriented APGS. Then $S \otimes_R M$ is a fg S -module and we have $M \star_R A \simeq (S \otimes_R M) \star_S A$, considering the action by R -modules $(\star_R)$ and S -modules $(\star_S)$ respectively.*

Proof. Seeing $(S \otimes_R M) \star_S A$ as an R -oriented APGS and $S \otimes_R M$ as an R -module, we obtain by [Theorem B.1](#) that for all R -oriented APGS:

$$\begin{aligned} \operatorname{Hom}_{\mathcal{A}_R}(B, (S \otimes_R M) \star_S A) &\cong \operatorname{Hom}_R(S \otimes_R M, \operatorname{Hom}_{\mathcal{A}_R}(B, A)) \\ &\cong \operatorname{Hom}_R(M, \operatorname{Hom}_R(S, \operatorname{Hom}_{\mathcal{A}_R}(B, A))) \\ &\cong \operatorname{Hom}_R(M, \operatorname{Hom}_{\mathcal{A}_R}(B, A)), \end{aligned}$$

where the penultimate isomorphism follows from the adjunction of $\otimes_R$ and Hom_R and where the ultimate isomorphism is $f \mapsto f(1)$. Such a homomorphism is trivially injective but we justify its surjectivity. Let $\varphi \in \operatorname{Hom}_{\mathcal{A}_R}(B, A)$ and ι be the S -orientation of A . Then, $f : \alpha \in S \mapsto \iota(\alpha) \circ \varphi$ is a well-defined morphism of R -modules $S \rightarrow \operatorname{Hom}_{\mathcal{A}_R}(B, A)$ corresponding to φ . We then conclude by [Theorem B.1](#). $\square$

B.2 Functoriality of the module action when modules vary

Not only can we construct the action of modules but also the action of module homomorphisms, making the alternate construction from [Definition B.1](#) functorial. This functoriality is essential to prove that the constructions of the module action from [Section 2.1](#) and [Appendix B.1](#) are equivalent. We shall see in [Appendix B.4](#) that [Theorem 2.1](#) can be obtained as a corollary of the more general result proven below.

Theorem B.2. *If A is an R -oriented APGS, then every morphism of fg R -modules $\phi : M_1 \rightarrow M_2$ induces an R -oriented morphism $\phi \star A : M_2 \star A \rightarrow M_1 \star A$, so that $M \mapsto M \star A$ defines a contravariant functor.*

This functor is left exact. Namely, it maps an exact sequence of fg R -modules $M_1 \xrightarrow{\phi} M_2 \xrightarrow{\psi} M_3 \rightarrow 0$ to an exact sequence $0 \rightarrow M_3 \star A \xrightarrow{\psi \star A} M_2 \star A \xrightarrow{\phi \star A} M_1 \star A$ of R -oriented morphisms of APGS.

Proof. Let $\phi : M_1 \rightarrow M_2$ be a morphism of fg R -modules. Consider two finite presentations $R^{n_i} \xrightarrow{X_i} R^{m_i} \rightarrow M_i \rightarrow 0$ with matrices $X_i \in M_{m_i, n_i}(R)$ for $i \in \{1, 2\}$. Then, ϕ can be lifted into a morphism of exact sequences:

$$\begin{array}{ccccccc} R^{n_1} & \xrightarrow{X_1} & R^{m_1} & \longrightarrow & M_1 & \longrightarrow & 0 \\ \downarrow Y & & \downarrow Z & & \downarrow \phi & & \\ R^{n_2} & \xrightarrow{X_2} & R^{m_2} & \longrightarrow & M_2 & \longrightarrow & 0 \end{array}$$

so we obtain matrices $Y \in M_{n_2, n_1}(R)$ and $Z \in M_{m_2, m_1}(R)$ such that $Z \cdot X_1 = X_2 \cdot Y$. From this morphism of exact sequences and by construction of $M_1 \star A$ and $M_2 \star A$, we obtain a morphism of exact sequences:

$$\begin{array}{ccccccc} 0 & \longrightarrow & M_2 \star A & \longrightarrow & A^{m_2} & \xrightarrow{\iota(X_2^T)} & A^{n_2} \\ & & \downarrow \phi \star A & & \downarrow \iota(Z^T) & & \downarrow \iota(Y^T) \\ 0 & \longrightarrow & M_1 \star A & \longrightarrow & A^{m_1} & \xrightarrow{\iota(X_1^T)} & A^{n_1} \end{array}$$

In particular, $\iota(Z^T) : A^{m_2} \rightarrow A^{m_1}$ induces a morphism $\phi \star A : M_2 \star A \rightarrow M_1 \star A$. Such a morphism is R -oriented for the R -orientations for $M_2 \star A$ and $M_1 \star A$ induced by those of A^{m_2} and A^{m_1} derived from (A, ι) .

By concatenating exact sequences, it is easy to see that $(\psi \circ \phi) \star A = (\phi \star A) \circ (\psi \star A) : M_3 \star A \rightarrow M_1 \star A$ when $\psi : M_2 \rightarrow M_3$ is another morphism of fg R -modules. From [Lemma B.2](#) proven below, we also obtain that the identity of R -modules is mapped to the identity of R -oriented abelian varieties. This proves that $M \mapsto M \star A$ defines a functor (provided it is well defined).

However, it remains to prove that $\phi \star A : M_2 \star A \rightarrow M_1 \star A$ is well defined *i.e.* that it does not depend on the finite presentations of M_1 and M_2 we consider. As previously, we prove that $\phi \star A : M_2 \star A \rightarrow M_1 \star A$ satisfies a universal property that will ensure its unicity, namely that the following diagram commutes for all R -oriented APGS B :

$$\begin{array}{ccc} \mathrm{Hom}_R(M_2, \mathrm{Hom}_{\mathcal{A}_R}(B, A)) & \xrightarrow{(m \mapsto \phi_m) \mapsto (m \mapsto \phi_m \circ \phi)} & \mathrm{Hom}_R(M_1, \mathrm{Hom}_{\mathcal{A}_R}(B, A)) \\ \eta_{B, M_2} \downarrow \wr & & \eta_{B, M_1} \downarrow \wr \\ \mathrm{Hom}_{\mathcal{A}_R}(B, M_2 \star A) & \xrightarrow{(\phi \star A) \circ -} & \mathrm{Hom}_{\mathcal{A}_R}(B, M_1 \star A) \end{array}$$

Fig. 7

where the η_{B, M_i} are the natural isomorphisms from [Theorem B.1](#). By construction of $\phi \star A$, the commutativity of [Figure 7](#) follows directly from the commutativity of the diagram below:

$$\begin{array}{ccc} \mathrm{Hom}_R(R^{m_2}, \mathrm{Hom}_{\mathcal{A}_R}(B, A)) & \xrightarrow{(m \mapsto \phi_m) \mapsto (m \mapsto \phi_m(Z \cdot -))} & \mathrm{Hom}_R(R^{m_1}, \mathrm{Hom}_{\mathcal{A}_R}(B, A)) \\ \downarrow \wr & & \downarrow \wr \\ \mathrm{Hom}_{\mathcal{A}_R}(B, A^{m_2}) & \xrightarrow{\iota(Z^T) \circ -} & \mathrm{Hom}_{\mathcal{A}_R}(B, A^{m_1}) \end{array}$$

where the vertical arrows are given by [Equation \(6\)](#).

By commutativity of [Figure 7](#) for all R -oriented APGS B and in particular for $B = M_2 \star A$, we obtain that any other candidate $\psi : M_2 \star A \rightarrow M_1 \star A$ induced by $\phi : M_1 \rightarrow M_2$ satisfies $(\phi \star A) \circ - = \psi \circ -$, so in particular $(\phi \star A) \circ \mathrm{id}_{M_1 \star A} = \psi \circ \mathrm{id}_{M_1 \star A}$ *i.e.* $\phi \star A = \psi$. This proves the unicity of $\phi \star A$.

It remains to prove the right exactness of the functor $M \mapsto M \star A$. Let $M_1 \xrightarrow{\phi} M_2 \xrightarrow{\psi} M_3 \rightarrow 0$ be an exact sequence of fg R -modules. Then, by left-exactness of the $\mathrm{Hom}_R(-, M)$ functor for all R -module M , we obtain an exact sequence:

$$\begin{aligned} 0 \rightarrow \mathrm{Hom}_R(M_3, \mathrm{Hom}_{\mathcal{A}_R}(B, A)) & \xrightarrow{- \circ \psi} \mathrm{Hom}_R(M_2, \mathrm{Hom}_{\mathcal{A}_R}(B, A)) \\ & \xrightarrow{- \circ \phi} \mathrm{Hom}_R(M_1, \mathrm{Hom}_{\mathcal{A}_R}(B, A)) \end{aligned}$$

for all R -oriented APGS B . Using the commutativity of the diagram from [Figure 7](#) and its analog for ψ , both involving natural isomorphisms, we obtain an exact sequence:

$$0 \rightarrow \operatorname{Hom}_{\mathcal{A}_R}(B, M_3 \star A) \xrightarrow{(\psi \star A) \circ -} \operatorname{Hom}_{\mathcal{A}_R}(B, M_2 \star A) \xrightarrow{(\phi \star A) \circ -} \operatorname{Hom}_{\mathcal{A}_R}(B, M_1 \star A)$$

for all R -oriented APGS B . Applying the above sequence to $B = M_3 \star A$, we obtain that $(\phi \star A) \circ (\psi \star A) \circ - = 0$, so that $(\phi \star A) \circ (\psi \star A) \circ \operatorname{id}_{M_3 \star A} = 0$ i.e. $\operatorname{im}(\psi \star A) \subseteq \ker(\phi \star A)$. Conversely, applying the sequence to $B = \ker(\phi \star A)$ and considering the inclusion $j : B \hookrightarrow M_2 \star A$, we obtain that $(\phi \star A) \circ j = 0$, which ensures by the equality $\operatorname{im}((\psi \star A) \circ -) = \ker((\phi \star A) \circ -)$, that there exists $f \in \operatorname{Hom}_{\mathcal{A}_R}(B, M_3 \star A)$ such that $j = (\psi \star A) \circ f$, so that $\operatorname{im}(\psi \star A) = \ker(\phi \star A)$. Similarly, applying the exact sequence to $B = \ker(\psi \star A)$ and considering the first arrow applied to the inclusion $j : B \hookrightarrow M_3 \star A$, we obtain that $(\psi \star A) \circ j = 0$ by construction, which ensures that $j = 0$ i.e. that $\ker(\psi \star A) = 0$. It follows that $\psi \star A$ is injective, and finally that:

$$0 \rightarrow M_3 \star A \xrightarrow{\psi \star A} M_2 \star A \xrightarrow{\phi \star A} M_1 \star A$$

is an exact sequence and the proof is now complete. $\square$

The functorial construction from [Theorem B.2](#) maps a scalar multiplication to a scalar multiplication. As claimed in the proof of [Theorem B.2](#) above, this proves that R -modules is mapped to the identity of R -oriented abelian varieties through the module action.

Lemma B.2. *Let (A, ι) be an R -oriented APGS and M be a fg R -module. Then, for all $d \in \mathbb{Z}$, $d \operatorname{id}_M : M \rightarrow M$ induces the multiplication by d morphism $[d]_{M \star A} : M \star A \rightarrow M \star A$ via the module action.*

Proof. Let $R^n \xrightarrow{X} R^m \rightarrow M \rightarrow 0$ be a finite presentation of M with $X \in M_{m,n}(R)$. Then, recalling the construction from the proof of [Theorem B.2](#), we have an isomorphism of exact sequences:

$$\begin{array}{ccccccc} R^n & \xrightarrow{X} & R^m & \longrightarrow & M & \longrightarrow & 0 \\ \downarrow dI_n & & \downarrow dI_m & & \downarrow d \operatorname{id}_M & & \\ R^n & \xrightarrow{X} & R^m & \longrightarrow & M & \longrightarrow & 0 \end{array}$$

which induces an isomorphism of exact sequences of R -oriented APGS:

$$\begin{array}{ccccccc} 0 & \longrightarrow & M \star A & \longrightarrow & A^m & \xrightarrow{\iota(X^T)} & A^n \\ & & \downarrow [d] & & \downarrow [d] & & \downarrow [d] \\ 0 & \longrightarrow & M \star A & \longrightarrow & A^m & \xrightarrow{\iota(X^T)} & A^n \end{array}$$

where the left vertical arrow is the desired morphism $M \star A \rightarrow M \star A$. This completes the proof. $\square$

Lemma B.3. *Let (A, ι) be an R -oriented APGS, M_1, M_2, M'_1, M'_2 be fg R -modules and $\Phi : M_1 \oplus M_2 \rightarrow M'_1 \oplus M'_2$ be a homomorphism of R -modules written in matrix form:*

$$\Phi := \begin{pmatrix} \phi_{11} & \phi_{21} \\ \phi_{12} & \phi_{22} \end{pmatrix} : (x, y) \mapsto (\phi_{11}(x) + \phi_{21}(y), \phi_{12}(x) + \phi_{22}(y)).$$

Then, $\Phi \star A$ can be written in matrix form as:

$$\Phi \star A := \begin{pmatrix} \phi_{11} \star A & \phi_{12} \star A \\ \phi_{21} \star A & \phi_{22} \star A \end{pmatrix} : M_1 \star A \oplus M_2 \star A \rightarrow M'_1 \star A \oplus M'_2 \star A.$$

Proof. As in the proof of [Theorem B.2](#), consider a morphism of finite presentations for all $i, j \in \{1, 2\}$:

$$\begin{array}{ccccccc} R^{n_i} & \xrightarrow{X_i} & R^{m_i} & \longrightarrow & M_i & \longrightarrow & 0 \\ \downarrow Y^{(ij)} & & \downarrow Z^{(ij)} & & \downarrow \phi_{ij} & & \\ R^{n'_j} & \xrightarrow{X'_j} & R^{m'_j} & \longrightarrow & M'_j & \longrightarrow & 0 \end{array}$$

with $X_i \in M_{m_i, n_i}(R)$, $X'_j \in M_{m'_j, n'_j}(R)$, $Y^{(ij)} \in M_{n'_j, n_i}(R)$ and $Z^{(ij)} \in M_{m'_j, m_i}(R)$ such that $Z^{(ij)} \cdot X_i = X'_j \cdot Y^{(ij)}$. Then by construction $\phi_{ij} \star A$ fits into the following morphism of exact sequences:

$$\begin{array}{ccccccc} 0 & \longrightarrow & M'_j \star A & \longrightarrow & A^{m'_j} & \xrightarrow{\iota(X'^T_j)} & A^{n'_j} \\ & & \downarrow \phi_{ij} \star A & & \downarrow \iota(Z^{(ij)T}) & & \downarrow \iota(Y^{(ij)T}) \\ 0 & \longrightarrow & M_i \star A & \longrightarrow & A^{m_i} & \xrightarrow{\iota(X_i^T)} & A^{n_i} \end{array}$$

We then obtain the following morphism of exact sequences:

$$\begin{array}{ccccccc} 0 & \longrightarrow & M'_1 \star A \oplus M'_2 \star A & \longrightarrow & A^{m'_1+m'_2} & \xrightarrow{\iota \begin{pmatrix} X'^T_1 & 0 \\ 0 & X'^T_2 \end{pmatrix}} & A^{n'_1+n'_2} \\ & & \downarrow \begin{pmatrix} \phi_{11} \star A & \phi_{12} \star A \\ \phi_{21} \star A & \phi_{22} \star A \end{pmatrix} & & \downarrow \iota \begin{pmatrix} Z^{(11)T} & Z^{(12)T} \\ Z^{(21)T} & Z^{(22)T} \end{pmatrix} & & \downarrow \iota \begin{pmatrix} Y^{(11)T} & Y^{(12)T} \\ Y^{(21)T} & Y^{(22)T} \end{pmatrix} \\ 0 & \longrightarrow & M_1 \star A \oplus M_2 \star A & \longrightarrow & A^{m_1+m_2} & \xrightarrow{\iota \begin{pmatrix} X_1^T & 0 \\ 0 & X_2^T \end{pmatrix}} & A^{n_1+n_2} \end{array}$$

By construction of the module action, we can identify the vertical arrow on the left with $\Phi \star A$, which completes the proof. $\square$

We have seen in [Proposition B.1.\(i\)](#) that isomorphic fg R -modules M_1, M_2 induce isomorphic R -oriented APGS $M_1 \cdot A \simeq M_2 \cdot A$ when A is an R -oriented APGS. The converse is actually true for R -lattices when $R = \mathfrak{O}_K$ and $\text{End}_{\mathcal{A}_R}(A) \simeq R$. This follows from a correspondance between projective R -module homomorphisms and R -oriented morphism of APGS.

Proposition B.3. *Assume $R = \mathfrak{O}_K$. Let A be an R -oriented APGS such that $\text{End}_{\mathcal{A}_R}(A) \simeq R$ and M, M_1 and M_2 be R -lattices. Then:*

- (i) $\text{Hom}_{\mathcal{A}_R}(M_2 \cdot A, M_1 \cdot A) \cong \text{Hom}_R(M_1, M_2)$.
- (ii) $\text{Hom}_{\mathcal{A}_R}(M \cdot A, A) \cong M$.
- (iii) If $M_1 \cdot A \simeq M_2 \cdot A$, then $M_1 \simeq M_2$.

Proof. (i) By functoriality of the module action ([Theorem B.2](#)), there is a canonical R -module homomorphism

$$\begin{aligned} \text{Hom}_R(M_1, M_2) &\longrightarrow \text{Hom}_{\mathcal{A}_R}(M_2 \cdot A, M_1 \cdot A) \\ \phi &\longmapsto \phi \cdot A. \end{aligned} \quad (7)$$

Since M_1 and M_2 are projective, there exist R -modules M'_1, M'_2 and integers $n_1, n_2 \in \mathbb{N}$ such that $M_1 \oplus M'_1 \simeq R^{n_1}$ and $M_2 \oplus M'_2 \simeq R^{n_2}$. By construction, [Equation \(7\)](#) is the result of the pre and post composition of

$$\begin{aligned} \text{Hom}_R(M_1 \oplus M'_1, M_2 \oplus M'_2) &\longrightarrow \text{Hom}_{\mathcal{A}_R}(M_2 \cdot A \oplus M'_2 \cdot A, M_1 \cdot A \oplus M'_1 \cdot A) \\ \begin{pmatrix} \phi_{11} & \phi_{21} \\ \phi_{12} & \phi_{22} \end{pmatrix} &\longmapsto \begin{pmatrix} \phi_{11} \cdot A & \phi_{12} \cdot A \\ \phi_{21} \cdot A & \phi_{22} \cdot A \end{pmatrix}. \end{aligned} \quad (8)$$

with the canonical embedding $\text{Hom}_R(M_1, M_2) \rightarrow \text{Hom}_R(M_1 \oplus M'_1, M_2 \oplus M'_2)$ and projection $\text{Hom}_{\mathcal{A}_R}(M_2 \cdot A \oplus M'_2 \cdot A, M_1 \cdot A \oplus M'_1 \cdot A) \rightarrow \text{Hom}_{\mathcal{A}_R}(M_2 \cdot A, M_1 \cdot A)$. By [Lemma B.3](#), [Equation \(8\)](#) is on the one hand, obtained by matrix morphism action $\Phi \longmapsto \Phi \cdot A$. On the other hand, since $M_1 \oplus M'_1 \simeq R^{n_1}$ and $M_2 \oplus M'_2 \simeq R^{n_2}$, we also have $M_1 \cdot A \oplus M'_1 \cdot A \simeq A^{n_1}$ and $M_2 \cdot A \oplus M'_2 \cdot A \simeq A^{n_2}$ by [Proposition B.1](#), so [Lemma B.3](#) also ensures that [Equation \(8\)](#) is identified with the trivial matrix action:

$$\begin{aligned} M_{n_2, n_1}(R) &\longrightarrow \text{Hom}_{\mathcal{A}_R}(A^{n_2}, A^{n_1}) \\ X &\longmapsto \iota(X^T). \end{aligned}$$

Since $\text{Hom}_{\mathcal{A}_R}(A^{n_2}, A^{n_1}) \cong M_{n_1, n_2}(\text{End}_{\mathcal{A}_R}(A)) \simeq M_{n_1, n_2}(R)$, this is an isomorphism, so [Equation \(8\)](#) defines an isomorphism, which ensures that [Equation \(7\)](#) defines an isomorphism, as desired.

(ii) From (i), we obtain $\text{Hom}_{\mathcal{A}_R}(M \cdot A, R \cdot A) \cong \text{Hom}_R(R, M)$. In addition, [Proposition B.1.\(iii\)](#) ensures that $R \cdot A \cong A$ and we have $\text{Hom}_R(R, M) \cong M$ via $f \mapsto f(1)$. This proves (ii).

(iii) Let $\varphi : M_1 \cdot A \xrightarrow{\sim} M_2 \cdot A$ be an isomorphism. Then, (i) ensures the existence of morphisms of R -modules $\phi : M_2 \rightarrow M_1$ and $\phi' : M_1 \rightarrow M_2$ such that $\varphi = \phi \cdot A$ and $\varphi^{-1} = \phi' \cdot A$. We then have by functoriality of the module action ([Theorem B.2](#)):

$$\text{id}_{M_1 \cdot A} = \varphi^{-1} \circ \varphi = (\phi' \cdot A) \circ (\phi \cdot A) = (\phi \circ \phi') \cdot A.$$

Applying (i) again ensures that $\text{End}_{\mathcal{A}_R}(M_1 \cdot A) \cong \text{End}_R(M_1)$ via the module action, which ensures that $\phi \circ \phi' = \text{id}_{M_1}$ from the equality above. We similarly prove the existence of $\phi'' : M_1 \rightarrow M_2$ such that $\phi'' \circ \phi = \text{id}_{M_2}$, which ensures that $M_1 \simeq M_2$. $\square$

Using the functoriality property from [Theorem B.2](#), we can describe the structure of APGS obtained by module action on an abelian variety.

Proposition B.4. *[JKP+18, Proposition 4.3] Let (A, ι) be an R -oriented abelian variety of dimension g defined over k and M be a fg R -module. Then:*

- (i) *If M is of torsion, then $M \star A$ is finite.*
- (ii) *If M is of torsion, $R = \mathfrak{O}_K$ and $\text{char}(k) \nmid \#M$, then $M \star A$ has cardinality $(\#M)^g$.*
- (iii) $\dim(M \star A) = \text{rank}(M) \dim(A)$.

Proof. (i) Let $R^n \xrightarrow{X} R^m \xrightarrow{s} M \rightarrow 0$ be a finite presentation with $X \in M_{m,n}(R)$. Then, by construction $M \star A$ is the kernel of $\iota(X^T) : A^m \rightarrow A^n$. Since M is of torsion, there exists $\alpha \in R \setminus \{0\}$ such that $\alpha \cdot M = 0$, so that $d := \bar{\alpha}\alpha \in \mathbb{Z}_{>0}$ satisfies $d \cdot M = 0$ and $d \cdot R^m \subseteq \ker(s) = \text{im}(X)$. Hence, there exists $Y \in M_{n,m}(R)$ such that $X \cdot Y = d \cdot I_m$, so that $Y^T \cdot X^T = d \cdot I_n$ and $M \star A = \ker(\iota(X^T)) \subseteq \ker(\iota(Y^T) \circ \iota(X^T)) = A[d]^m$, which is finite.

(ii) Since $R = \mathfrak{O}_K$, by [Theorem A.1.\(iv\)](#), there exist ideals $\mathfrak{a}_1, \dots, \mathfrak{a}_n \subseteq R$ such that $M \simeq \bigoplus_{i=1}^n R/\mathfrak{a}_i$. By [Proposition B.1.\(iii\)](#), we then have $M \star A \simeq \bigoplus_{i=1}^n (R/\mathfrak{a}_i) \star A$. Since

To conclude, we then only have to prove that for any ideal $\mathfrak{a} \subseteq R$ such that $\text{char}(k) \nmid N(\mathfrak{a})$, $(R/\mathfrak{a}) \star A$ has cardinality $N(\mathfrak{a})^g$. If $\mathfrak{a} \subseteq R$ is such an ideal, then it is a $\mathbb{Z}$ -module of rank 2, so it has two generators $\alpha, \beta \in \mathfrak{a}$. From that, we obtain a finite presentation of $R/\mathfrak{a}$ given by $R^2 \xrightarrow{X} R \rightarrow R/\mathfrak{a} \rightarrow 0$, with $X := (\alpha \ \beta) \in M_{1,2}(R)$. By construction of $(R/\mathfrak{a}) \star A$, we obtain that:

$$\begin{aligned} (R/\mathfrak{a}) \star A &= \ker(\iota(X^T) : A \rightarrow A^2) = \ker(\iota(\alpha)) \cap \ker(\iota(\beta)) = \bigcap_{\gamma \in \mathfrak{a}} \ker(\iota(\gamma)) \\ &= A[\mathfrak{a}] \end{aligned} \tag{9}$$

The remaining arguments follow from [\[Wat69, Proposition 3.15\]](#). If $\mathfrak{a}$ is principal and $\alpha \in R$ generates $\mathfrak{a}$, then $\#(R/\mathfrak{a}) \star A = \# \ker(\iota(\alpha))$. But by [\[Mil86b, Proposition 9.23\]](#), we have $\deg(\iota(\alpha)) = N(\alpha)^g$ and $\text{char}(k) \nmid N(\mathfrak{a})$ so that $\iota(\alpha)$ is separable and we indeed have $\#(R/\mathfrak{a}) \star A = \# \ker(\iota(\alpha)) = \deg(\iota(\alpha)) = N(\alpha)^g = N(\mathfrak{a})^g$ in that case.

If $\mathfrak{a}$ is not principal, by [\[Cox13, Theorem 9.12\]](#) we may find an ideal $\mathfrak{b} \subset R$ which belongs to the inverse class of $\mathfrak{a}$ in $\text{Cl}(R)$, with $N(\mathfrak{b})$ coprime with $N(\mathfrak{a})$ and $\text{char}(k)$. Then $\mathfrak{a}\mathfrak{b}$ is principal and we may consider a generator $\alpha \in R^*$ of this ideal. Since $\mathfrak{a}$ and $\mathfrak{b}$ are coprime, the Chinese remainder theorem applies and ensures that $R/\alpha R = R/(\mathfrak{a}\mathfrak{b}) \simeq R/\mathfrak{a} \oplus R/\mathfrak{b}$, so that $(R/\alpha R) \star A \simeq (R/\mathfrak{a}) \star A \oplus$

$(R/\mathfrak{b}) \star A$ by [Proposition B.1.\(iii\)](#). By the principal case, treated above, we have $\#(R/\alpha R) \star A = N(\alpha)^g = N(\mathfrak{a})^g N(\mathfrak{b})^g$, so that:

$$\#(R/\mathfrak{a}) \star A \cdot \#(R/\mathfrak{b}) \star A = N(\mathfrak{a})^g N(\mathfrak{b})^g \quad (10)$$

By [Equation \(9\)](#), we have $(R/\mathfrak{a}) \star A = A[\mathfrak{a}]$ and for all $P \in A[\mathfrak{a}]$ and $\gamma \in \mathfrak{a}$, we have $\iota(\gamma)(P) = 0$, so that $[N(\gamma)]P = \iota(\bar{\gamma}\gamma)(P) = 0$ and the order of P divides $\gcd(\{N(\gamma) \mid \gamma \in \mathfrak{a}\}) = N(\mathfrak{a})$, and $A[\mathfrak{a}] \subset A[N(\mathfrak{a})]$. It follows that $\#(R/\mathfrak{a}) \star A \mid N(\mathfrak{a})^{2g}$. Since $N(\mathfrak{a})$ and $N(\mathfrak{b})$ are coprime, it follows from [Equation \(10\)](#) that $\#(R/\mathfrak{a}) \star A \mid N(\mathfrak{a})^g$. With the same argument, we obtain $\#(R/\mathfrak{b}) \star A \mid N(\mathfrak{b})^g$, which ensures that both inequalities are equalities, so that in particular $\#(R/\mathfrak{a}) \star A = N(\mathfrak{a})^g$. This proves (ii).

(iii) Let $r := \text{rank}(M)$. Then, there exists an exact sequence $0 \rightarrow R^r \xrightarrow{j} M \xrightarrow{s} T \rightarrow 0$ with $T := M/j(R^r)$. The R -module T is of torsion, because otherwise, there would exist a family of $r+1$ independant vectors in M , contradicting the equality $r = \text{rank}(M)$. By left exactness of the module action functor ([Theorem B.2](#)), we obtain an exact sequence:

$$0 \rightarrow T \star A \xrightarrow{s \star A} M \star A \xrightarrow{j \star A} A^r$$

It follows that $\dim(M \star A) + \dim(T \star A) = \dim(\text{im}(j \star A)) \leq \dim(A^r) = r \dim(A)$. Furthermore, (i) ensures that $T \star A$ is finite, so that $\dim(T \star A) = 0$ and $\dim(M \star A) \leq r \dim(A)$.

For the converse equality, we use again that T is of torsion, which ensures the existence of $d \in \mathbb{N}^*$ such that $d \cdot T = 0$, so that $d \cdot M \subseteq j(R^r)$ and $q : x \mapsto j^{-1}(dx)$ defines a map $M \rightarrow R^r$ such that $q \circ j = d \text{id}_{R^r}$. By functoriality of the module action ([Theorem B.2](#)), we obtain that $(j \star A) \circ (q \star A) = (d \text{id}_{R^r}) \star A$. But by [Lemma B.2](#), we have $(d \text{id}_{R^r}) \star A = [d]_{A^r}$, which is an isogeny, hence a surjective map, so that $j \star A : M \star A \rightarrow A^r$ is surjective, so $\dim(M \star A) \geq r \dim(A)$ and finally $\dim(M \star A) = r \dim(A)$. This completes the proof. $\square$

B.3 Functoriality of the module action when APGS vary

Similarly to what we have seen in the previous section, we can act with modules on morphisms in a functorial way. We shall see in [Appendix B.4](#) that [Theorem 2.2](#) can be obtained as a corollary of the more general result proven below.

Theorem B.3. *If M is a fg R -module, then every morphism of R -oriented APGS $\varphi : A_1 \rightarrow A_2$ induces an R -oriented morphism $M \star \varphi : M \star A_1 \rightarrow M \star A_2$, so that $A \mapsto M \star A$ defines a covariant functor.*

This functor is also left exact. Namely, it maps an exact sequence $0 \rightarrow A_1 \rightarrow A_2 \rightarrow A_3$ of R -oriented morphisms of APGS to an exact sequence $0 \rightarrow M \star A_1 \rightarrow M \star A_2 \rightarrow M \star A_3$.

Proof. The general approach is very similar to [Theorem B.2](#). Let $R^n \xrightarrow{X} R^m \rightarrow M \rightarrow 0$ be a finite presentation of M , where the left map is the matrix multiplication on the left by $X \in M_{m,n}(R)$. By construction of $M \star A_1$ and $M \star A_2$, we obtain a morphism of exact sequences:

$$\begin{array}{ccccccc}
 0 & \longrightarrow & M \star A_1 & \longrightarrow & A_1^m & \xrightarrow{\iota_1(X^T)} & A_1^n \\
 & & \downarrow M \star \varphi & & \downarrow D_m(\varphi) & & \downarrow D_n(\varphi) \\
 0 & \longrightarrow & M \star A_2 & \longrightarrow & A_2^m & \xrightarrow{\iota_2(X^T)} & A_2^n
 \end{array}$$

where ι_i denote the R -orientation of A_i for $i \in \{1, 2\}$, $D_n(\varphi) : (P_i)_{1 \leq i \leq n} \in A_1^n \mapsto (\varphi(P_i))_{1 \leq i \leq n} \in A_2^n$ and $D_m(\varphi)$ is defined similarly. In particular, φ and the construction of the $M \star A_i$ induce an R -oriented morphism of APGS $M \star \varphi : M \star A_1 \rightarrow M \star A_2$. This construction is immediately functorial.

By construction, with the same arguments we used to prove the commutativity of Figure 7 in the proof of Theorem B.2, we can also prove that for any R -oriented APGS B , the following diagram commutes:

$$\begin{array}{ccc}
 \text{Hom}_R(M, \text{Hom}_{\mathcal{A}_R}(B, A_1)) & \xrightarrow{\varphi \circ -} & \text{Hom}_R(M, \text{Hom}_{\mathcal{A}_R}(B, A_2)) \\
 \eta_{B, A_1} \downarrow \wr & & \eta_{B, A_2} \downarrow \wr \\
 \text{Hom}_{\mathcal{A}_R}(B, M \star A_1) & \xrightarrow{(M \star \varphi) \circ -} & \text{Hom}_{\mathcal{A}_R}(B, M \star A_2)
 \end{array}$$

Fig. 8

where the η_{B, A_i} are the natural isomorphisms from Theorem B.1.

As in the proof of Theorem B.2, we obtain the unicity of $M \star \varphi : M \star A_1 \rightarrow M \star A_2$ from this universal property.

To complete the proof, it remains to prove the left exactness of the functor $A \mapsto M \star A$. Let $0 \rightarrow A_1 \xrightarrow{\varphi} A_2 \xrightarrow{\psi} A_3$ of R -oriented morphisms of APGS. Then, by left exactness of the functors $\text{Hom}_{\mathcal{A}_R}(B, -)$ and $\text{Hom}_R(M, -)$ successively, we obtain an exact sequence:

$$\begin{aligned}
 0 \rightarrow \text{Hom}_R(M, \text{Hom}_{\mathcal{A}_R}(B, A_1)) & \xrightarrow{\varphi \circ -} \text{Hom}_R(M, \text{Hom}_{\mathcal{A}_R}(B, A_2)) \\
 & \xrightarrow{\psi \circ -} \text{Hom}_R(M, \text{Hom}_{\mathcal{A}_R}(B, A_3))
 \end{aligned}$$

From the natural isomorphisms of Figure 8, we obtain an exact sequence:

$$0 \rightarrow \text{Hom}_{\mathcal{A}_R}(B, M \star A_1) \xrightarrow{(M \star \varphi) \circ -} \text{Hom}_{\mathcal{A}_R}(B, M \star A_2) \xrightarrow{(M \star \psi) \circ -} \text{Hom}_{\mathcal{A}_R}(B, M \star A_3),$$

and we conclude as in the proof of Theorem B.2 that

$$0 \rightarrow M \star A_1 \xrightarrow{M \star \varphi} M \star A_2 \xrightarrow{M \star \psi} M \star A_3$$

is exact, as desired. This completes the proof. $\square$

Unsurprisingly, the action of direct sums of modules on R -oriented morphisms behaves as it should.

Lemma B.4. *Let $\varphi : A_1 \rightarrow A_2$ be a morphism of R -oriented APGS, M_1 and M_2 be fg R -modules. Then:*

(i) $(M_1 \oplus M_2) \star \varphi$ is the diagonal morphism:

$$\begin{aligned} D(M_1 \star \varphi, M_2 \star \varphi) : M_1 \star A_1 \oplus M_2 \star A_1 &\longrightarrow M_1 \star A_2 \oplus M_2 \star A_2 \\ (P, Q) &\longmapsto (M_1 \star \varphi(P), M_2 \star \varphi(Q)) \end{aligned}$$

(ii) In particular, for all $n \in \mathbb{N}$, $R^n \star \varphi$ is the diagonal morphism:

$$D_n(\varphi) : (P_i)_{1 \leq i \leq n} \in A_1^n \longmapsto (\varphi(P_i))_{1 \leq i \leq n} \in A_2^n.$$

Proof. (i) We obtain the desired result from the universal property of the module action on R -oriented morphisms given by Figure 8 for $M = M_1, M_2$ and $M_1 \oplus M_2$ and from the fact that $(M_1 \oplus M_2) \star A_i \cong M_1 \star A_i \oplus M_2 \star A_i$ for $i \in \{1, 2\}$ (Proposition B.1.(iii)).

(ii) This follows directly from (i) and the fact that $R \star \varphi = \varphi$ by construction of the module action on R -oriented morphisms. $\square$

The action of modules on R -oriented morphisms of APGS introduced in Theorem B.3 is compatible with the action of morphisms of R -modules on APGS introduced in Theorem B.2 in the following way.

Theorem B.4. *Let $\phi : M_1 \rightarrow M_2$ be a morphism of fg R -modules and $\varphi : A_1 \rightarrow A_2$ be a morphism of R -oriented APGS. Then, the following diagram commutes:*

$$\begin{array}{ccc} M_1 \star A_1 & \xrightarrow{M_1 \star \varphi} & M_1 \star A_2 \\ \phi \star A_1 \uparrow & & \uparrow \phi \star A_2 \\ M_2 \star A_1 & \xrightarrow{M_2 \star \varphi} & M_2 \star A_2 \end{array}$$

i.e. $(\phi \star A_2) \circ (M_2 \star \varphi) = (M_1 \star \varphi) \circ (\phi \star A_1)$.

Proof. Let $R^{n_i} \xrightarrow{X_i} R^{m_i} \rightarrow M_i \rightarrow 0$ with $X_i \in M_{m_i, n_i}(R)$ be finite presentations of M_i for $i \in \{1, 2\}$ and consider a morphism of exact sequences:

$$\begin{array}{ccccccc} R^{n_1} & \xrightarrow{X_1} & R^{m_1} & \longrightarrow & M_1 & \longrightarrow & 0 \\ \downarrow Y & & \downarrow Z & & \downarrow \phi & & \\ R^{n_2} & \xrightarrow{X_2} & R^{m_2} & \longrightarrow & M_2 & \longrightarrow & 0 \end{array}$$

with $Y \in M_{n_2, n_1}(R)$ and $Z \in M_{m_2, m_1}(R)$ such that $Z \cdot X_1 = X_2 \cdot Y$. Let ι_1 and ι_2 be the R -orientations of A_1 and A_2 respectively. Then on the one hand, we have by construction the two following morphisms of exact sequences:

$$\begin{array}{ccccccc}
 0 & \longrightarrow & M_2 \star A_1 & \longrightarrow & A_1^{m_2} & \xrightarrow{\iota_1(X_2^T)} & A_1^{n_2} \\
 & & \phi \star A_1 \downarrow & & \iota_1(Z^T) \downarrow & & \downarrow \iota_1(Y^T) \\
 0 & \longrightarrow & M_1 \star A_1 & \longrightarrow & A_1^{m_1} & \longrightarrow & A_1^{n_1} \\
 & & M_1 \star \varphi \downarrow & & D_{m_1}(\varphi) \downarrow & & \downarrow D_{n_1}(\varphi) \\
 0 & \longrightarrow & M_1 \star A_2 & \longrightarrow & A_2^{m_1} & \xrightarrow{\iota_2(X_1^T)} & A_2^{n_1}
 \end{array}$$

where $D_{m_1}(\varphi)$ is the diagonal morphism $(P_i)_{1 \leq i \leq m_1} \in A_1^{m_1} \mapsto (\varphi(P_i))_{1 \leq i \leq m_1} \in A_2^{m_1}$, and similarly for $D_{n_1}(\varphi)$. On the other hand, we have the morphisms of exact sequences:

$$\begin{array}{ccccccc}
 0 & \longrightarrow & M_2 \star A_1 & \longrightarrow & A_1^{m_2} & \xrightarrow{\iota_1(X_2^T)} & A_1^{n_2} \\
 & & M_2 \star \varphi \downarrow & & D_{m_2}(\varphi) \downarrow & & \downarrow D_{n_2}(\varphi) \\
 0 & \longrightarrow & M_2 \star A_2 & \longrightarrow & A_2^{m_2} & \longrightarrow & A_2^{n_2} \\
 & & \phi \star A_2 \downarrow & & \iota_2(Z^T) \downarrow & & \downarrow \iota_2(Y^T) \\
 0 & \longrightarrow & M_1 \star A_2 & \longrightarrow & A_2^{m_1} & \xrightarrow{\iota_2(X_1^T)} & A_2^{n_1}
 \end{array}$$

Since φ is R -oriented, we have $D_{m_1}(\varphi) \circ \iota_1(Z^T) = \iota_2(Z^T) \circ D_{m_2}(\varphi)$, which ensures the equality of the left vertical arrows of both diagrams, *i.e.* that $(\phi \star A_2) \circ (M_2 \star \varphi) = (M_1 \star \varphi) \circ (\phi \star A_1)$. This completes the proof. $\square$

B.4 The module action on abelian varieties oriented by a maximal order

When $R = \mathfrak{O}_K$ is the maximal order, we first obtain that we can restrict the module action functors to R -lattices and R -oriented abelian varieties, and therefore prove [Theorems 2.1](#) and [2.2](#) (with the conceptual construction).

Theorem 2.1 *Assume that $R = \mathfrak{O}_K$, let (A, ι) be an R -oriented abelian variety and M be an R -lattice. Then:*

- (i) $M \star A$ is an abelian variety.
- (ii) $M \mapsto M \star A$ defines an exact contravariant functor from the category of R -lattices to the category of R -oriented abelian varieties.

Proof. (i) Since $R = \mathfrak{O}_K$, M is projective so there exists an R -module M' and $n \in \mathbb{N}$ such that $M \oplus M' \simeq R^n$. The reduction modulo M induces a surjection $R^n \twoheadrightarrow M'$ with kernel M . Since M is of finite type, we obtain a finite presentation $R^m \rightarrow R^n \rightarrow M' \rightarrow 0$ of M' . We can then apply [Proposition B.1](#), which ensures that:

$$A^n \cong R^n \star A \simeq (M \oplus M') \star A \simeq (M \star A) \oplus (M' \star A)$$

Hence, $M \star A \simeq A^n / (M' \star A)$. Since A^n is an abelian variety and $M' \star A$ is a subgroup scheme of A^n , [Cho52] ensures that $M \star A$ is an abelian variety, as desired.

(ii) By Theorem B.2, we know that $M \mapsto M \star A$ is left exact. It remains to prove its right exactness, *i.e.* that an injective morphism of R -lattices $\phi : M_1 \hookrightarrow M_2$ corresponds to a surjective morphism of abelian varieties $\phi \star A : M_2 \star A \twoheadrightarrow M_1 \star A$.

If $\phi : M_1 \hookrightarrow M_2$ is such a morphism, then we have an exact sequence $0 \rightarrow M_1 \xrightarrow{\phi} M_2 \rightarrow \text{coker}(\phi) \rightarrow 0$ which corresponds to an exact sequence:

$$0 \rightarrow \text{coker}(\phi) \star A \rightarrow M_2 \star A \xrightarrow{\phi \star A} M_1 \star A$$

by left exactness of the module action functor. We then have

$$\dim(\text{im}(\phi \star A)) + \dim(\text{coker}(\phi) \star A) = \dim(M_2 \star A),$$

with $\dim(M_2 \star A) = \text{rank}(M_2) \dim(A)$ and

$$\dim(\text{coker}(\phi) \star A) = \text{rank}(M_2 / \phi(M_1)) \dim(A) = (\text{rank}(M_2) - \text{rank}(M_1)) \dim(A)$$

by Proposition B.4.(iii), so that $\dim(\text{im}(\phi \star A)) = \text{rank}(M_1) \dim(A) = \dim(M_1 \star A)$ and $\text{im}(\phi \star A) = M_1 \star A$, as a subvariety of $M_1 \star A$ with the same dimension. We conclude that $\phi \star A$ is indeed surjective, as desired. $\square$

Theorem 2.2 *Assume that $R = \mathfrak{O}_K$. If M is an R -lattice, then every R -oriented morphism of abelian varieties $\varphi : A_1 \rightarrow A_2$ induces an R -oriented morphism $M \star \varphi : M \star A_1 \rightarrow M \star A_2$, so that $A \mapsto M \star A$ defines a covariant functor. This functor is also left exact.*

Proof. This follows immediately from the point (i) of the previous proof and Theorem B.3. $\square$

To prove the formal construction of the module action from Definition B.1 is equivalent to the effective one, we restrict the module action to R -lattices (acting on R -oriented abelian varieties). The penultimate point of the following theorem actually proves the desired result when we assume that $R = \mathfrak{O}_K$ to ensure that all R -lattices are projective and simplify the proofs. For that reason, we shall assume that $R = \mathfrak{O}_K$ and use $\cdot$ instead of $\star$ to denote the module action in the following.

Theorem 2.3 *Assume that $R = \mathfrak{O}_K$. Let (A, ι) be an R -oriented abelian variety of dimension g defined over k and $M \subseteq R^n$ be an R -lattice of rank n . Then:*

- (i) $\dim(M \star A) = ng = \text{rank}(M) \dim(A)$.
- (ii) *An isogeny $\phi : M_1 \rightarrow M_2$ between R -lattices (i.e. injective with finite cokernel) corresponds to an isogeny $\phi \star A : M_2 \star A \rightarrow M_1 \star A$ between R -oriented abelian varieties (i.e. surjective with finite kernel). Furthermore, $\deg(\phi \star A) = (\# \text{coker}(\phi))^g$ when $\text{char}(k) \nmid \# \text{coker}(\phi)$.*

- (iii) In particular, we obtain that the morphism $\varphi_M : A^n \rightarrow M \star A$ with kernel $A^n[M]$ introduced in [Section 2.1](#) is an isogeny. It has degree $\deg(\varphi_M) = [R^n : M]^g$ when $\text{char}(k) \nmid [R^n : M]$.
- (iv) If $\varphi : A_1 \rightarrow A_2$ is an R -oriented isogeny, then $M \star \varphi$ is an R -oriented isogeny with kernel $M \star \ker(\varphi)$.

Proof. (i) This is [Proposition B.4.\(i\)](#).

(ii) Since a module isogeny is injective, we have an exact sequence $0 \rightarrow M_1 \xrightarrow{\phi} M_2 \xrightarrow{p} \text{coker}(\phi) \rightarrow 0$, where p is the reduction modulo $\phi(M_1)$. By exactness of the module action functor ([Theorem 2.1](#)), we obtain an exact sequence:

$$0 \rightarrow \text{coker}(\phi) \star A \xrightarrow{p \star A} M_2 \star A \xrightarrow{\phi \star A} M_1 \star A \rightarrow 0$$

It follows that $\phi \star A$ is surjective with kernel $\text{coker}(\phi) \star A$. But $\text{coker}(\phi)$ is finite because ϕ is an isogeny, so $\text{coker}(\phi) \star A$ is also finite by [Proposition B.4.\(i\)](#). Hence, $\phi \star A$ is an isogeny of degree $\# \text{coker}(\phi) \star A = (\# \text{coker}(\phi))^g$ when $\text{char}(k) \nmid \# \text{coker}(\phi)$ by [Proposition B.4.\(ii\)](#).

(iii) The inclusion $j : M \hookrightarrow R^n$ is an isogeny (because M has full rank), so it corresponds to an isogeny $\varphi_M := j \star A : R^n \star A \cong A^n \rightarrow M \star A$ with kernel $(R^n/M) \star A$ and degree $[M : R^n]^g$ when $\text{char}(k) \nmid \# \text{coker}(\phi)$ by (ii).

To compute $(R^n/M) \star A$, consider a family of generators $(x_1, \dots, x_m)$ of M and the matrix $X \in M_{n,m}(R)$ whose columns are the x_i s. We then obtain a finite presentation $0 \rightarrow R^m \xrightarrow{X} R^n \rightarrow R^n/M \rightarrow 0$ whose right arrow is the reduction modulo M . By construction, we then have, as in [Remark 2.1](#):

$$\begin{aligned} (R^n/M) \star A &= \ker(\iota(X^T) : A^n \rightarrow A^m) \\ &= \{P \in A^n \mid \forall 1 \leq i \leq m, \quad \iota(x_i)(P) = 0\} \\ &= \{P \in A^n \mid \forall x \in M, \quad \iota(x)(P) = 0\} = A^n[M]. \end{aligned} \quad (11)$$

(iv) Since M is an R -lattice, we can consider an embedding $j : M \hookrightarrow R^n$ with $n = \text{rank}(M)$, so that j is an isogeny. By [Theorem B.4](#), we have:

$$(j \star A_2) \circ (R^n \star \varphi) = (M \star \varphi) \circ (j \star A_1), \quad (12)$$

where $R^n \star \varphi = D_n(\varphi)$ by [Lemma B.4.\(ii\)](#). Since j is an isogeny, $j \star A_1$ and $j \star A_2$ are isogenies and since φ is an isogeny, $D_n(\varphi)$ is also an isogeny. Isogenies being surjective, it follows from [Equation \(12\)](#) that $M \star \varphi$ is surjective. This equation also ensures that $\ker(M \star \varphi) = (j \star A_1)(\ker((j \star A_2) \circ D_n(\varphi)))$, which ensures that $M \star \varphi$ has finite kernel since isogenies have finite kernel. Hence, $M \star \varphi$ is an isogeny.

Now, if $R^{n'} \xrightarrow{X} R^m \rightarrow M \rightarrow 0$ is a finite presentation of M , we obtain on the one hand, by construction of $M \star \varphi$ an exact sequence:

$$0 \rightarrow \ker(M \star \varphi) \rightarrow \ker(D_{n'}(\varphi)) = \ker(\varphi)^{n'} \xrightarrow{\iota(X^T)} \ker(D_m(\varphi)) = \ker(\varphi)^m.$$

On the other hand, by construction of $M \star \ker(\varphi)$, we also have an exact sequence:

$$0 \rightarrow M \star \ker(\varphi) \rightarrow \ker(\varphi)^{n'} \xrightarrow{\iota(X^T)} \ker(\varphi)^m.$$

We conclude that $\ker(M \star \varphi) \cong M \star \ker(\varphi)$, which completes the proof. $\square$

Remark B.1. Aside from the assertion on degrees of isogenies, the assumption $R = \mathfrak{O}_K$ is only used to prove (i), using the fact that M is projective, from which the rest of the theorem follows. However, this assumption is not necessary (see [JKP+18, Theorem 4.4]) but only meant to simplify the proofs.

B.5 Duality, polarisations and Hermitian module action

Theorem 2.4 *Assume that $R = \mathfrak{O}_K$. Let (A, ι) be an R -oriented abelian variety and M be an R -lattice. Then:*

- (i) $A^\vee$ is R -oriented for an orientation $\iota^* : R \hookrightarrow \text{End}(A^\vee), r \mapsto \iota(\bar{r})^\vee$.
- (ii) $M^\vee \cdot A^\vee \cong (M \cdot A)^\vee$.
- (iii) If $\phi : M_1 \rightarrow M_2$ is a morphism of R -lattices, $\phi^\vee \cdot A^\vee : M_1^\vee \cdot A^\vee \rightarrow M_2^\vee \cdot A^\vee$ is the dual of $\phi \cdot A : M_2 \cdot A \rightarrow M_1 \cdot A$.
- (iv) If $\varphi : A_1 \rightarrow A_2$ is an R -oriented morphism, then $M^\vee \cdot \varphi^\vee : M^\vee \cdot A_2^\vee \rightarrow M^\vee \cdot A_1^\vee$ is the dual of $M \cdot \varphi : M \cdot A_1 \rightarrow M \cdot A_2$.

Proof. (i) The R -orientation $\iota : R \hookrightarrow \text{End}(A)$ induces an R -orientation of $A^\vee$ given by $\iota^\vee : r \in R \mapsto \iota(r)^\vee \in \text{End}(A^\vee)$. However, to ensure (ii) and (iii) (but also compatibility with Hermitian forms), we consider the R -orientation $\iota^* : r \in R \mapsto \iota(\bar{r})^\vee \in \text{End}(A^\vee)$ instead.

(ii) Let $R^n \xrightarrow{X} R^m \rightarrow M \rightarrow 0$ be a finite presentation of M , where the left map is the multiplication on the left by $X \in M_{m,n}(R)$. Then, apply the $\text{Hom}_{\bar{R}}(-, R)$ functor, we obtain an exact sequence:

$$0 \rightarrow M^\vee \rightarrow (R^m)^\vee \xrightarrow{-\circ X} (R^n)^\vee \quad (13)$$

We have a canonical isomorphism $R^n \cong (R^n)^\vee$ identifying the canonical basis $(\mathbf{e}_1, \dots, \mathbf{e}_n)$ of R^n with its dual basis $(\mathbf{e}_1^\vee, \dots, \mathbf{e}_n^\vee)$ of $(R^n)^\vee$ satisfying $\mathbf{e}_i^\vee(\mathbf{e}_j) = \delta_{i,j}$ for all $1 \leq i, j \leq n$. If we denote by $(\mathbf{f}_1, \dots, \mathbf{f}_m)$ the canonical basis of R^m and $(\mathbf{f}_1^\vee, \dots, \mathbf{f}_m^\vee)$ its dual, then we obtain for all $1 \leq i \leq m$ and $1 \leq j \leq n$,

$$\mathbf{f}_i^\vee(X \cdot \mathbf{e}_j) = \mathbf{f}_i^\vee \left(\sum_{q=1}^m X_{q,j} \mathbf{f}_q \right) = \sum_{q=1}^m \bar{X}_{q,j} \mathbf{f}_i^\vee(\mathbf{f}_q) = \sum_{q=1}^m \bar{X}_{q,j} \delta_{i,q} = \bar{X}_{i,j},$$

so that $\mathbf{f}_i^\vee \circ X = \sum_{j=1}^n \bar{X}_{i,j} \mathbf{e}_j^\vee$. Hence, the right map in Equation (13) can be identified to the left multiplication by $\bar{X}^T$, so we have an exact sequence:

$$0 \rightarrow M^\vee \rightarrow R^m \xrightarrow{\bar{X}^T} R^n$$

Then, by exactness of the module action functor of $(A^\vee, \iota^*)$ on R -lattices ([Theorem 2.1](#)), we obtain an exact sequence:

$$(A^\vee)^n \xrightarrow{\iota^*(\overline{X})} (A^\vee)^m \rightarrow M^\vee \cdot A^\vee \rightarrow 0. \quad (14)$$

By construction of the module action, we also have an exact sequence:

$$0 \rightarrow M \cdot A \rightarrow A^m \xrightarrow{\iota(X^T)} A^n,$$

Applying the dual functor (which is exact), we obtain an exact sequence:

$$(A^\vee)^n \xrightarrow{\iota^\vee(X)} (A^\vee)^m \rightarrow (M \cdot A)^\vee \rightarrow 0, \quad (15)$$

where by the definition from point (i), we have $\iota^\vee(X) = \iota^*(\overline{X})$, so that the exact sequences (14) and (15) are isomorphic, which ensures that $M^\vee \cdot A^\vee \cong (M \cdot A)^\vee$.

(iii) M_1 and M_2 being finitely presented, we may consider an isomorphism of exact sequences as in the proof of [Theorem B.2](#):

$$\begin{array}{ccccccc} R^{n_1} & \xrightarrow{X_1} & R^{m_1} & \longrightarrow & M_1 & \longrightarrow & 0 \\ \downarrow Y & & \downarrow Z & & \downarrow \phi & & \\ R^{n_2} & \xrightarrow{X_2} & R^{m_2} & \longrightarrow & M_2 & \longrightarrow & 0 \end{array}$$

Fig. 9

with matrices $X_i \in M_{m_i, n_i}(R)$ for $i \in \{1, 2\}$, $Y \in M_{n_2, n_1}(R)$ and $Z \in M_{m_2, m_1}(R)$ such that $Z \cdot X_1 = X_2 \cdot Y$. On the one hand, applying the module action functor on A (which is exact on R -lattices), we obtain a morphism of exact sequences:

$$\begin{array}{ccccccc} 0 & \longrightarrow & M_2 \cdot A & \longrightarrow & A^{m_2} & \xrightarrow{\iota(X_2^T)} & A^{n_2} \\ & & \downarrow \phi \cdot A & & \downarrow \iota(Z^T) & & \downarrow \iota(Y^T) \\ 0 & \longrightarrow & M_1 \cdot A & \longrightarrow & A^{m_1} & \xrightarrow{\iota(X_1^T)} & A^{n_1} \end{array}$$

And applying the dual functor, which is also exact, we obtain the morphism of exact sequences:

On the other hand, applying the $\text{Hom}_{\overline{R}}(-, R)$ functor to [Figure 9](#), we obtain a morphism of exact sequence:

$$\begin{array}{ccccccc} 0 & \longrightarrow & M_2^\vee & \longrightarrow & R^{m_2} & \xrightarrow{\overline{X_2}^T} & R^{n_2} \\ & & \downarrow \phi^\vee & & \downarrow \overline{Z}^T & & \downarrow \overline{Y}^T \\ 0 & \longrightarrow & M_1^\vee & \longrightarrow & R^{m_1} & \xrightarrow{\overline{X_1}^T} & R^{n_1} \end{array}$$

$$\begin{array}{ccccc}
(A^\vee)^{n_1} & \xrightarrow{\iota^\vee(X_1)} & (A^\vee)^{m_1} & \longrightarrow & (M_1 \cdot A)^\vee \longrightarrow 0 \\
\downarrow \iota^\vee(Y) & & \downarrow \iota^\vee(Z) & & \downarrow (\phi \cdot A)^\vee \\
(A^\vee)^{n_2} & \xrightarrow{\iota^\vee(X_2)} & (A^\vee)^{m_2} & \longrightarrow & (M_2 \cdot A)^\vee \longrightarrow 0
\end{array}$$

Fig. 10

Finally, applying the module action functor of $(A^\vee, \iota^*)$, we obtain the morphism of exact sequences:

$$\begin{array}{ccccc}
(A^\vee)^{n_1} & \xrightarrow{\iota^*(\overline{X}_1)} & (A^\vee)^{m_1} & \longrightarrow & M_1^\vee \cdot A^\vee \longrightarrow 0 \\
\downarrow \iota^*(\overline{Y}) & & \downarrow \iota^*(\overline{Z}) & & \downarrow \phi^\vee \cdot A^\vee \\
(A^\vee)^{n_2} & \xrightarrow{\iota^*(\overline{X}_2)} & (A^\vee)^{m_2} & \longrightarrow & M_2^\vee \cdot A^\vee \longrightarrow 0
\end{array}$$

Fig. 11

Since $\iota^\vee(r) = \iota^*(\overline{r})$ for all $r \in R$, we can identify $(\phi \cdot A)^\vee : (M_1 \cdot A)^\vee \rightarrow (M_2 \cdot A)^\vee$ with $\phi^\vee \cdot A^\vee : M_1^\vee \cdot A^\vee \rightarrow M_2^\vee \cdot A^\vee$ by comparing Figure 10 and Figure 11.

(iv) Since M is an R -lattice, we can consider an embedding $j : M \hookrightarrow R^n$ with $n = \text{rank}(M)$, so that j is an isogeny. On the one hand, using Theorem B.4 and Lemma B.4.(ii), we obtain Equation (12): $(j \cdot A_2) \circ D_n(\varphi) = (M \cdot \varphi) \circ (j \cdot A_1)$. Applying the dual functor and using (iii), we obtain:

$$D_n(\varphi^\vee) \circ (j^\vee \cdot A_2^\vee) = (j^\vee \cdot A_1^\vee) \circ (M \cdot \varphi)^\vee$$

On the other hand, we can apply Theorem B.4 to $j^\vee : (R^n)^\vee \cong R^n \rightarrow M^\vee$ and $\varphi^\vee : A_2^\vee \rightarrow A_1^\vee$ to obtain:

$$D_n(\varphi^\vee) \circ (j^\vee \cdot A_2^\vee) = (j^\vee \cdot A_1^\vee) \circ (M^\vee \cdot \varphi^\vee)$$

It follows that the image of $M^\vee \cdot \varphi^\vee - (M \cdot \varphi)^\vee$ is contained in $\ker(j^\vee \cdot A_1^\vee)$. Since j is an isogeny, $j^\vee$ is also an isogeny and so is $j^\vee \cdot A_1^\vee$ by Theorem 2.3.(ii), so $\ker(j^\vee \cdot A_1^\vee)$ is finite. Since image of morphisms of abelian varieties are abelian varieties, they are connected, so the image of $M^\vee \cdot \varphi^\vee - (M \cdot \varphi)^\vee$ must be 0, which completes the proof. $\square$

Theorem 2.5 *Assume that $R = \mathfrak{O}_K$. Let (A, λ_A, ι) be an R -oriented polarised abelian variety and (M, H) be a polarised R -lattice. Then:*

- (i) H defines an R -oriented polarisation $(M, H) \cdot \lambda_A$ of $M \cdot A$. We denote by $(H, M) \cdot (A, \lambda_A, \iota)$ (or simply $(H, M) \cdot A$) the resulting R -oriented polarised abelian variety.
- (ii) If λ_A is principal, then $(H, M) \cdot \lambda_A$ is principal if and only if (M, H) is unimodular.
- (iii) Let $\phi : (M_1, H_1) \rightarrow (M_2, H_2)$ be a d -similitude between unimodular Hermitian modules and assume λ_A is principal. Then $\phi \cdot A : (M_2, H_2) \cdot A \rightarrow (M_1, H_1) \cdot A$ is a d -isogeny between R -oriented PPAVs.

Proof. (i) Since H is a polarisation, it is integral on $M^\sharp$, and we have $M^\sharp \subseteq M$, and this inclusion induces an isogeny $\phi_H : M^\vee \cong M^\sharp \hookrightarrow M$. We can then define $(M, H) \cdot \lambda_A$ as the composition:

$$M \cdot A \xrightarrow{\phi_H \cdot A} M^\vee \cdot A \xrightarrow{M^\vee \cdot \lambda_A} M^\vee \cdot A^\vee$$

We then have:

$$\begin{aligned} ((M, H) \cdot \lambda_A)^\vee &= (\phi_H \cdot A)^\vee \circ (M^\vee \cdot \lambda_A)^\vee = (\phi_H^\vee \cdot A^\vee) \circ (M^{\vee\vee} \cdot \lambda_A^\vee) \\ &\quad \text{(by Theorem 2.4.(iii)-(iv))} \\ &= (\phi_H \cdot A^\vee) \circ (M \lambda_A) \\ &\quad \text{(since } M^{\vee\vee} \cong M \text{ and by autoduality of } \phi_H \text{ and } \lambda_A) \\ &= (M^\vee \cdot \lambda_A) \circ (\phi_H \cdot A) = (M, H) \cdot \lambda_A \\ &\quad \text{(by Theorem B.4)} \end{aligned}$$

So that $(M, H) \cdot \lambda_A$ is autodual. By points (ii) and (iv) of Theorem 2.3, $\phi_H \cdot A$ and $M^\vee \cdot \lambda_A$ are isogenies so their composition is an isogeny. This proves that $(M, H) \cdot \lambda_A$ is a polarisation of A . It is also R -oriented by construction, making $(M, H) \cdot A$ an R -oriented polarised abelian variety.

(ii) $(M, H) \cdot \lambda_A = (M^\vee \cdot \lambda_A) \circ (\phi_H \cdot A)$ is principal if and only if it is an isomorphism *i.e.* $\phi_H \cdot A$ and $M^\vee \cdot \lambda_A$ are isomorphisms. Theorem 2.3.(iv) ensures that $M^\vee \cdot \lambda_A$ has kernel $M^\vee \cdot \ker(\lambda_A) = 0$ since $\ker(\lambda_A) = 0$ by principality of λ_A , so $M^\vee \cdot \lambda_A$ is an isomorphism. In addition, Theorem 2.3.(ii) ensures that $\phi_H \cdot A$ has degree $[M : M^\sharp]^g$ (with $g = \dim(A)$) so it is an isomorphism if and only if $M = M^\sharp$ *i.e.* (M, H) is unimodular. This proves (ii).

(iii) Let us denote by $\phi_i : M_i^\vee \xrightarrow{\sim} M_i$ the isogeny associated to the polarisation H_i for $i \in \{1, 2\}$. Then, we see that ϕ_i^{-1} is the map $x \mapsto H_i(x, -)$ for $i \in \{1, 2\}$. Hence, for all $x \in M_2$, we have:

$$\begin{aligned} \phi_1 \circ \phi^\vee \circ \phi_2^{-1}(x) &= \phi_1 \circ \phi^\vee \circ \phi_2^{-1}(x) = \phi_1 \circ \phi^\vee(H_2(x, -)) = \phi_1(H_2(x, \phi(-))) \\ &= \phi_1(H_1(\phi^\sharp(x), -)) = \phi^\sharp(x) \end{aligned}$$

Since ϕ is a d -similitude, we have $\phi \circ \phi^\sharp = d \text{id}_{M_2}$, so that $\phi \circ \phi_1 \circ \phi^\vee = d\phi_2$. From Theorem 2.4.(iii), Theorem B.4, by functoriality of the module action and

the previous equality, we then obtain that:

$$\begin{aligned}
(\phi \cdot A)^\vee \circ (M_1, H_1) \cdot \lambda_A \circ (\phi \cdot A) &= (\phi^\vee \cdot A^\vee) \circ (M_1^\vee \cdot \lambda_A) \circ (\phi_1 \cdot A) \circ (\phi \cdot A) \\
&= (\phi^\vee \cdot A^\vee) \circ (\phi_1 \cdot A^\vee) \circ (M_1 \cdot \lambda_A) \circ (\phi \cdot A) \\
&= (\phi^\vee \cdot A^\vee) \circ (\phi_1 \cdot A^\vee) \circ (\phi \cdot A^\vee) \circ (M_2 \cdot \lambda_A) \\
&= (\phi \circ \phi_1 \circ \phi^\vee) \cdot A^\vee \circ (M_2 \cdot \lambda_A) \\
&= (d\phi_2) \cdot A^\vee \circ (M_2 \cdot \lambda_A) \\
&= [d](\phi_2 \cdot A^\vee) \circ (M_2 \cdot \lambda_A) \\
&= [d](M_2^\vee \cdot \lambda_A) \circ (\phi_2 \cdot A) = [d](M_2, H_2) \cdot \lambda_A
\end{aligned}$$

This proves that $\phi \cdot A$ is a d -isogeny, which completes the proof. $\square$

B.6 Generalising the module action to quaternion orders

In this section, our base field k has positive characteristic $p > 0$ and we consider a maximal order $\mathcal{O}$ of the quaternion algebra $B_{p,\infty}$ ramified at p and ∞ . The goal of this section is to define the action of left $\mathcal{O}$ -modules on $\mathcal{O}$ -oriented abelian varieties. Note that by the Deuring correspondence, there exists a supersingular elliptic curve $E/\bar{k}$ such that $\text{End}(E) \simeq \mathcal{O}$, which is therefore $\mathcal{O}$ -oriented with an orientation that fills its full endomorphism ring.

Left $\mathcal{O}$ -modules. Since $\mathcal{O}$ is a maximal order, the structure of finitely generated (fg) left $\mathcal{O}$ -modules can be described conveniently and we have an analogue of [Theorem A.1](#).

Theorem B.5. *Let M be an fg left $\mathcal{O}$ -module. Then:*

- (i) $M = P \oplus T$, where P is a torsion free R -module and T is an R -module of torsion.
- (ii) If M is torsion free ($T = 0$, $M = P$), then M is projective.
- (iii) There exist left $\mathcal{O}$ -ideals $I_1, \dots, I_m$ such that $P \simeq \bigoplus_{j=1}^m I_j$.
- (iv) If $m := \text{rank}_{\mathcal{O}}(P) \geq 2$, then P is free $P \simeq \mathcal{O}^m$.
- (v) There exist left $\mathcal{O}$ -ideals $I_1, \dots, I_n$ such that $T \simeq \bigoplus_{j=1}^n \mathcal{O}/I_j$.

Proof. Since an $\mathcal{O}$ -module is a $\mathbb{Z}$ -module and $\mathbb{Z}$ is Dedekind, the decomposition $M = P \oplus T$ from (i) follows from [Theorem A.1](#)(i). Then it is easy to check that P and T are stable by left multiplication by $\mathcal{O}$. (ii)-(iii) follow from [\[Rei03, Corollary 21.5\]](#). (iii) also follows from the fact that simple torsion free left $\mathcal{O}$ -modules are left $\mathcal{O}$ -ideals, which is a consequence of [\[Voi21, Lemma 7.2.17\]](#). (iv) is due to Eichler [\[Eic38\]](#). Finally, (v) is [\[Rei03, Exercise 4, p. 202\]](#). $\square$

[Theorem B.5](#) allows us to work in familiar territory. All torsion free fg left $\mathcal{O}$ -modules are $\mathcal{O}$ -lattices (*i.e.* can be embedded into a power of $\mathcal{O}$). Furthermore, they are all projective and are either isomorphic to a left $\mathcal{O}$ -ideal or a power of $\mathcal{O}$. Moreover, $\mathcal{O}$ -lattices are finitely generated by [Theorem B.5](#)(iii), which ensures

that all fg left $\mathcal{O}$ -modules are finitely presented (which allows to reuse the proof techniques from [Appendices B.2 and B.3](#)).

However, some subtleties arise because $\mathcal{O}$ is non-commutative. If M_1 and M_2 are left $\mathcal{O}$ -modules, then $\text{Hom}_{\mathcal{O}}(M_1, M_2)$ does not have a structure of $\mathcal{O}$ -module but only a structure of $\mathbb{Z}$ -module. Nonetheless, the dual $M^\vee$ of a left $\mathcal{O}$ -module M as $M^\vee = \text{Hom}_{\mathcal{O}}(M, \mathcal{O})$ made of $\mathcal{O}$ -antilinear maps $M \rightarrow \mathcal{O}$ still has an $\mathcal{O}$ -module structure but by multiplication on the right. Even though $M^\vee$ has a natural right $\mathcal{O}$ -module structure, we may still see it as a left $\mathcal{O}$ -module.

The notions of isogeny between left $\mathcal{O}$ -lattices is similar to the one introduced in [Appendix A.3](#). The notion of (positive definite sesquilinear) Hermitian form $H : V \times V \rightarrow B_{p,\infty}$ defined on a fg left $B_{p,\infty}$ -module also generalises naturally. Finally, the notions of polarisation and unimodularity with respect to a left $\mathcal{O}$ -module $M \subset V$, and the notion of similitude between polarised modules are also similar.

The action of left $\mathcal{O}$ -modules. Now, regarding the left $\mathcal{O}$ -module action construction, we can state the following. The conceptual construction of the action of fg left $\mathcal{O}$ -modules works as in [Appendix B.1](#). However, if A is an $\mathcal{O}$ -oriented APGS and M is a fg left $\mathcal{O}$ -module, we no longer have the guarantee that $M \star A$ is $\mathcal{O}$ -oriented (since $\mathcal{O}$ does not commute). Therefore, we need to replace $\mathcal{A}_R$ by the category $\mathcal{A}$ of APGS (without orientation constraint). Then $M \star A$ still satisfies a universal property close to [Theorem B.1](#): for all APGS B ,

$$\text{Hom}_{\mathcal{A}}(B, M \star A) \cong \text{Hom}_{\mathcal{O}}(M, \text{Hom}_{\mathcal{A}}(B, A)),$$

as an isomorphism of $\mathbb{Z}$ -modules. Note that $\text{Hom}_{\mathcal{A}}(B, A)$ is still a left $\mathcal{O}$ -module (since A is $\mathcal{O}$ -oriented). By the above universal property, we can still derive the properties of [Proposition B.1](#) (except the commutativity property of point (iv) since $\mathcal{O}$ is not commutative) and the ring extension property ([Proposition B.2](#)) when R is replaced by $\mathcal{O}$ and S by any subring of $\mathcal{O}$.

Functoriality of the left $\mathcal{O}$ -module action. Given a fixed $\mathcal{O}$ -oriented APGS A , the action of fg left $\mathcal{O}$ -modules $M \mapsto M \star A$ still defines a left exact contravariant functor in the category $\mathcal{A}$ of APGS ([Theorem B.2](#)) and the subsequent properties from [Appendix B.2](#) still hold (in the category $\mathcal{A}$ instead of $\mathcal{A}_R$). In particular, [Proposition B.3](#) holds with the following caveats. We have an isomorphism $\text{Hom}_{\mathcal{A}}(M_2 \star A, M_1 \star A) \cong \text{Hom}_{\mathcal{O}}(M_1, M_2)$ but as $\mathbb{Z}$ -modules. Nonetheless, the isomorphism $\text{Hom}_{\mathcal{A}}(M \star A, A) \cong M$ is an isomorphism of left $\mathcal{O}$ -modules and if $M_1 \star A \simeq M_2 \star A$, then we still have $M_1 \simeq M_2$ as left $\mathcal{O}$ -modules. [Proposition B.4](#) also holds: we have $\dim(M \star A) = \text{rank}(M) \dim(A)$; however if M is of torsion, and $\dim(A) = g$, the cardinality of $M \star A$ is $(\#M)^{g/2}$ (instead of $(\#M)^g$ in the quadratic case).

The functoriality properties from [Appendix B.3](#) (and [Theorem 2.2](#)) are also true for the left $\mathcal{O}$ -module action. Namely, if M is a fg left $\mathcal{O}$ -module, $A \mapsto M \star A$ is a covariant left exact functor from the category of $\mathcal{O}$ -oriented APGS (with

$\mathcal{O}$ -oriented morphisms) to the category of APGS. This functor also satisfies [Lemma B.4](#) and the compatibility property from [Theorem B.4](#).

The left $\mathcal{O}$ -module action on abelian varieties. When A is an $\mathcal{O}$ -oriented abelian variety, $M \mapsto M \star A$ still defines an exact functor from $\mathcal{O}$ -lattices to abelian varieties ([Theorem 2.1](#)). Consequently, [Theorem 2.3](#) still holds for $\mathcal{O}$ -oriented abelian varieties. In particular, the conceptual construction from [Appendix B.1](#) is still equivalent to the effective one from [Section 2.1](#). Once again, we can then denote the left $\mathcal{O}$ -module action by $\cdot$ instead of $\star$. We also recover the quaternion ideal action of the Deuring correspondence from the action by left $\mathcal{O}$ -ideals (seen as left $\mathcal{O}$ -modules) on $\mathcal{O}$ -oriented supersingular elliptic curves.

The compatibility between left $\mathcal{O}$ -module action and the duality on abelian varieties from [Theorem 2.4](#) still holds. From this, we can still obtain the correspondence between polarised left $\mathcal{O}$ -lattices and their isogenies and polarised $\mathcal{O}$ -oriented abelian varieties and their similitudes described by [Theorem 2.5](#).

C The Weil restriction and Scholten’s construction

In this section, we expand on [Section 3](#). We give a thorough description of the Weil restriction and Scholten’s construction, before giving a more conceptual, and much more general, proof of [Corollary 3.1](#).

Recall the notation from [Section 3](#): p is a prime $\equiv 3 \pmod{4}$, set $K := \mathbb{Q}(\sqrt{-p})$. We denote the maximal order of K by $R := \mathfrak{O}_K := \mathbb{Z}[(\sqrt{-p} - 1)/2]$, and $S = \mathbb{Z}[\sqrt{-p}]$ the order of K with conductor 2.

C.1 Weil Restriction

Given an elliptic curve E over $\mathbb{F}_{p^2}$, we want to find a variety over $\mathbb{F}_p$ that is naturally associated to E . The *Weil restriction*, introduced by Weil [[Wei64](#)] as the *restriction of scalars*, gives us exactly that: For an extension of fields k'/k of degree n and an algebraic variety X over K of dimension g , the Weil restriction $W_{k'/k}(X)$ is an algebraic variety over k of dimension $n \cdot g$. Given explicit polynomials defining X over K , we get a description of Y by introducing additional variables to obtain polynomials defined over k . Furthermore, the Weil restriction not only reduces varieties over k' to varieties over k , but also the maps between such varieties.^{[19](#)}

When $k' = \mathbb{F}_{p^2}$ and $k = \mathbb{F}_p$, we simply write $W(A)$ for the Weil restriction. When we apply the Weil restriction to an elliptic curve E over $\mathbb{F}_{p^2}$, we get a principally polarised^{[20](#)} abelian surface $W(E)$ over $\mathbb{F}_p$. Similarly, n -isogenies $E \rightarrow E'$ descend to n -isogenies $W(E) \rightarrow W(E')$.

¹⁹ In categorical language, we can reduce both objects and morphisms and thus the Weil restriction is *functorial*.

²⁰ As the Weil restriction is functorial, restrictions of abelian varieties are still abelian varieties, and restrictions of principal polarisations are still principal polarisations.

Example C.1. The main application of the Weil restriction in this work is the restriction of elliptic curves over $\mathbb{F}_{p^2}$. Let $A \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ and let $E_A : y^2 = x^3 + Ax^2 + x$. By writing $y = y_0 + iy_1$, $x = x_0 + ix_1$, and $A = a_0 + ia_1$, the defining equation can be split into its real and imaginary parts as

$$\begin{aligned} W_{\text{Re}} : \quad y_0^2 - y_1^2 &= x_0^3 + x_0^2 a_0 - 3x_0 x_1^2 - 2x_0 x_1 a_1 - x_1^2 a_0 + x_0, \\ W_{\text{Im}} : \quad 2y_0 y_1 &= 3x_0^2 x_1 + x_0^2 a_1 + 2x_0 x_1 a_0 - x_1^3 - x_1^2 a_1 + x_1. \end{aligned}$$

Here, W_{Re} and W_{Im} are polynomials over $\mathbb{F}_p$ that define the Weil restriction $W(E_A)$: points $P = (x_0, x_1, y_0, y_1)$ that are solutions to both W_{Re} and W_{Im} are the affine points on $W(E_A)$. Any point $P = (x_0 + x_1 \cdot i, y_0 + y_1 \cdot i) \in E(\mathbb{F}_{p^2})$ can then be transformed into such a point (x_0, x_1, y_0, y_1) on $W(E_A)(\mathbb{F}_p)$, and vice versa, and we can similarly induce addition on $W(E_A)$ via E_A , so we find that $W(E_A)(\mathbb{F}_p) \cong E_A(\mathbb{F}_{p^2})$ as groups. However, $W(E_A)$ is now a principally polarised abelian surface of dimension 2 over $\mathbb{F}_p$.

Remark C.1. Note that, over $\mathbb{F}_p$ (though not over $\overline{\mathbb{F}}_p$), the Weil restriction is a distinct third option in the classification of principally polarised abelian surfaces: the Weil restriction $W(E_A)$ from [Example C.1](#) is neither a Jacobian of a hyperelliptic curve over $\mathbb{F}_p$ nor a product of elliptic curves over $\mathbb{F}_p$.

It is insightful to see what happens when we view $W_{k'/k}(A)$ over any field extension k'/k again. Let $G := \text{Gal}(k'/k)$ be the associated Galois group, then over k' ,

$$W_{k'/k}(A) \cong \prod_{\sigma \in G} A^\sigma.$$

Following [Example C.1](#), $W(E_A)$ is isomorphic to $E_A \times E_A^\sigma$ over $\mathbb{F}_{p^2}$, where E_A^σ is the conjugate curve image of the p -Frobenius isogeny $\sigma : (x, y) \in E_A \mapsto (x^p, y^p) \in E_A^\sigma$ and defined by $y^2 = x^3 + A^p x^2 + x$ [[Wei64](#), Sec. 1.3]. From here on we will use σ to denote the p -Frobenius isogeny on any elliptic curve but only on elliptic curves, and always denote the conjugate curve with an exponent σ .

Galois model. [Example C.1](#) gives a model for $W(E_A)$ in terms of concrete equations W_{Re} and W_{Im} . In practice, this model is somewhat cumbersome to work with, and instead, we will use the *Galois model* in the remainder of the work. The Galois model describes points on $W(E_A)$ as tuples (P, Q) with $P \in E_A$ and $Q \in E_A^\sigma$, with the caveat that $\mathbb{F}_p$ -Frobenius acts as $\pi : (P, Q) \mapsto (\sigma(Q), \sigma(P))$, instead of the usual Frobenius $(P, Q) \mapsto (\sigma(P), \sigma(Q))$. In fancier terms, the Galois model describes $W(E_A)$ as the *descent* of the surface $E_A \times E_A^\sigma$ from $\mathbb{F}_{p^2}$ to $\mathbb{F}_p$ under the Galois action associated to π . Thus, an $\mathbb{F}_p$ -rational point on $W(E_A)$ is a pair (P, Q) such that $\pi(P, Q) = (P, Q)$, or in other words, $Q = \sigma(P)$. This recovers the same isomorphism of group structures $E(\mathbb{F}_{p^2}) \cong W(E_A)(\mathbb{F}_p)$ as before, using $P \mapsto (P, \sigma(P))$. We can further extend this isomorphism with twist. Indeed, an $\mathbb{F}_p$ -rational point on $W(E_A)^t$ can be associated to a point $P \in E(\mathbb{F}_{p^2})$ via the mapping $P \mapsto (P, -\sigma(P))$.

Remark C.2. We can express Weil restriction functoriality more precisely with the Galois model. If $\varphi : E \rightarrow E'$ is an n -isogeny, its Weil descent $W(\varphi) : W(E) \rightarrow W(E')$ has kernel $\ker(\varphi) \times \{0\} \oplus \{0\} \times \sigma(\ker(\varphi))$.

Lemma C.1. *If E be a maximal supersingular elliptic curve defined over $\mathbb{F}_{p^2}$ with $p \equiv 3 \pmod{4}$, we have:*

- (i) $W(E)(\mathbb{F}_p) \simeq \mathbb{Z}_{p+1} \times \mathbb{Z}_{p+1}$.
- (ii) $W(E)$ is primitively oriented by $S = \mathbb{Z}[\sqrt{-p}]$ via its p -Frobenius endomorphism.
- (iii) $W(E)$ is isogenous to E_0^2 over $\mathbb{F}_p$ (where $E_0/\mathbb{F}_p$ has j -invariant 1728), so it is superspecial.

Proof. (i) We have seen that $W(E)(\mathbb{F}_p) \cong E(\mathbb{F}_{p^2})$ and since E is maximal over $\mathbb{F}_{p^2}$, we have $E(\mathbb{F}_{p^2}) \simeq \mathbb{Z}_{p+1} \times \mathbb{Z}_{p+1}$.

(ii) As we have seen, $W(E)$ is $\mathbb{F}_{p^2}$ -isomorphic to $E \times E^\sigma$ with Frobenius endomorphism $\pi : (P, Q) \mapsto (\sigma(Q), \sigma(P))$, so that $\pi^2(P, Q) = (\sigma^2(P), \sigma^2(Q))$ for all $(P, Q) \in W(E)$, where σ^2 denotes the p^2 -Frobenius by abuse of notations. Since E is maximal, we have $\#E(\mathbb{F}_{p^2}) = (p+1)^2$, so that $\text{Tr}(\sigma^2) = p^2 + 1 - \#E(\mathbb{F}_{p^2}) = -2p$ and σ^2 is annihilated by $x^2 - \text{Tr}(\sigma^2)x + p^2 = (x+p)^2$. It follows that $\sigma^2 = -[p]$, that $\pi^2 = -[p]$ on $W(E)$ and that π corresponds to $\sqrt{-p}$, and induces an S -orientation of $W(E)$.

If this orientation was not primitive, then $W(E)$ would be oriented by R , so $(\pi - 1)/2$ would be an endomorphism, *i.e.* $W(E)[2]$ would be $\mathbb{F}_p$ -rational. But $W(E)[2] \simeq \mathbb{Z}_2^4$ and $W(E)(\mathbb{F}_p) \simeq \mathbb{Z}_{p+1}^2$ by (i) and $\mathbb{Z}_2^4$ cannot be embedded into $\mathbb{Z}_{p+1}^2$. This proves that $W(E)$ is indeed primitively S -oriented.

(iii) Let us denote by σ and σ' the p -Frobenius isogeny from E and E^σ respectively. Using the matrix notation for endomorphisms of $W(E) \cong E \times E^\sigma$ and [GSS25, Proposition 4.8], we obtain for all $x \in \mathbb{Z}$,

$$\begin{aligned} \deg([x] - \pi) &= \deg \begin{pmatrix} [x] & -\sigma' \\ -\sigma & [x] \end{pmatrix} = (x^2 + p) \cdot (x^2 + p) - \deg(-\hat{\sigma}' \circ [x] - [x]\sigma) \\ &= (x^2 + p)^2 \end{aligned}$$

where we used the fact that $\sigma' \circ \sigma = [-p]$ since it is the p^2 -Frobenius, so that $\hat{\sigma}' = -\sigma$. It follows that the characteristic polynomial of π is $(x^2 + p)^2$. By similar computation the characteristic polynomial of E_0^2 is also $(x^2 + p)^2$. Then by Tate's theorem [Tat66, Theorem 1.(c)], $W(E)$ is $\mathbb{F}_p$ -isogenous to E_0^2 . $\square$

Remark C.3. When E is already defined over $\mathbb{F}_p$, we can still define $W(E)$ by the descent of $E \times E$ from $\mathbb{F}_{p^2}$ to $\mathbb{F}_p$ with respect to $(P, Q) \mapsto (\sigma(Q), \sigma(P)) = (Q, P)$. Even though $E^2 := E \times E$ is now defined over $\mathbb{F}_p$, it comes equipped with a different Frobenius map. Hence, the Weil restriction $W(E)$ is *not* isomorphic to E^2 over $\mathbb{F}_p$ but only over $\mathbb{F}_{p^2}$, or in other words, $W(E)$ is a twist of $E^2/\mathbb{F}_p$. However, $W(E)$ and E^2 are isogenous over $\mathbb{F}_p$ by a similar argument to Lemma C.1.(iii).

C.2 Scholten's Construction

As we can see in [Lemma C.1.\(i\)](#), the Weil restriction $W(E)$ has only rank-2 rational 2-torsion. To work with a rational level-2 theta model for a principally polarised abelian surface, we need fully rational 2-torsion, but for $W(E)$ this lives over $\mathbb{F}_{p^2}$. Instead of working over $\mathbb{F}_{p^2}$, we work with an associated abelian surface $W'(E)$ which does have full rational 2-torsion, introduced by Scholten [\[Sch03\]](#). Scholten's original construction is defined through several maps between hyperelliptic curves, which are rephrased for cryptographic purposes by Costello [\[Cos18\]](#). We follow the presentation from [\[CR26; Rob24b\]](#), where Scholten's construction is reinterpreted as a gluing of the 2-torsion $E[2]$.

Definition C.1. *Let $p \equiv 3 \pmod{4}$ and let E be a maximal supersingular elliptic curve over $\mathbb{F}_{p^2}$ with $W(E)$ its Weil restriction. Scholten's construction $W'(E)$ is the image of the 2-isogeny $\Gamma : W(E) \rightarrow W'(E)$ whose kernel is the maximal isotropic subgroup of $W(E)[2]$ given by:*

$$W(E)(\mathbb{F}_p)[2] = \{(P, \sigma(P)) \mid P \in E[2]\}.$$

Since $W(E)(\mathbb{F}_p)[2]$ is $\mathbb{F}_p$ -rational, so is Γ , which ensures that $W'(E)$ is $\mathbb{F}_p$ -rational. Actually, it is the Jacobian of a hyperelliptic curve of genus 2 over $\mathbb{F}_p$ [\[Cos18, Proposition 1\]](#).²¹ Not only is $W'(E)$ $\mathbb{F}_p$ -rational but also R -oriented, as desired.

Lemma C.2. *Let $p \equiv 3 \pmod{4}$ and let E be a maximal supersingular elliptic curve over $\mathbb{F}_{p^2}$. Then:*

- (i) $W'(E) = \mathfrak{f} \cdot W(E)$ via the S -module action, where $\mathfrak{f} := (2, \sqrt{-p} - 1)$ is the conductor ideal of S .
- (ii) $W'(E)(\mathbb{F}_p) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{(p+1)/2} \times \mathbb{Z}_{(p+1)/2}$.
- (iii) $W'(E)$ is primitively oriented by $R = \mathbb{Z}[(\sqrt{-p} - 1)/2]$ via its p -Frobenius endomorphism.

Proof. (i) Using the S -orientation of $W(E)$ ([Lemma C.1.\(ii\)](#)), we have by definition:

$$W(E)[\mathfrak{f}] = W(E)[2] \cap \ker(\pi - \text{id}_{W(E)}) = W(E)(\mathbb{F}_p)[2]$$

It follows that $\Gamma : W(E) \rightarrow W'(E)$ is the S -oriented isogeny induced by $\mathfrak{f}$ and that $W'(E) = \mathfrak{f} \cdot W(E)$.

(ii) By definition, $W'(E)$ is $\mathbb{F}_p$ -isogenous to $W(E)$, and by [Lemma C.1.\(i\)](#), we have $\#W(E)(\mathbb{F}_p) = (p+1)^2$. By Tate's theorem [\[Tat66, Theorem 1.\(c\)\]](#), it follows that $\#W'(E)(\mathbb{F}_p) = (p+1)^2$.

²¹ As noted in [\[CR26\]](#), the 2-isogeny $\Gamma : W(E) \rightarrow W'(E)$ becomes a gluing isogeny $E \times E^\sigma \rightarrow W'(E)$ when viewed as an isogeny over $\mathbb{F}_{p^2}$. For an explicit construction of the hyperelliptic curve associated to $W'(E)$, see [\[Sch03; Cos18\]](#).

Since E is maximal over $\mathbb{F}_{p^2}$, we have $E(\mathbb{F}_{p^2}) = E[p+1] \simeq \mathbb{Z}_{p+1}^2$ so we can find a basis (P, Q) of $E(\mathbb{F}_{p^2}) = E[p+1]$ and consider $U := \Gamma(P, \sigma(P))$ and $V := \Gamma(Q, \sigma(Q))$. Now, using the Frobenius S -orientation of $W'(E)$, we obtain:

$$\begin{aligned} \pi'(U) &= \frac{1}{2} \Gamma \circ \pi \circ \tilde{\Gamma} \circ \Gamma(P, \sigma(P)) = \Gamma \circ \pi(P, \sigma(P)) = \Gamma(\sigma^2(P), \sigma(P)) \\ &= \Gamma(P, \sigma(P)) = U, \end{aligned}$$

and similarly, $\pi'(V) = V$, so that $U, V \in W'(E)(\mathbb{F}_p)$. Furthermore, if $\lambda, \mu \in \mathbb{Z}$ satisfy $[\lambda]U + [\mu]V = 0$, we then have $([\lambda]P + [\mu]Q, \sigma([\lambda]P + [\mu]Q)) \in \ker(\Gamma)$ so $[\lambda]P + [\mu]Q \in E[2]$, which ensures that $(p+1)/2$ divides both λ and μ . It follows that U and V both have order $(p+1)/2$ and are linearly independent.

By [Cos18, Equation 9], the equation of the genus 2 curve whose Jacobian is $W'(E)$ is of the form $y^2 = f(x)$ with $f \in \mathbb{F}_p[x]$ of degree 6 and all its roots defined over $\mathbb{F}_p$. It follows that $W'(E)[2]$ is $\mathbb{F}_p$ -rational.

Since $W'(E)[2] \simeq \mathbb{Z}_2^4$, we may then find $U', V' \in W'(E)[2]$ linearly independent and linearly independent of $[(p+1)/4]U, [(p+1)/4]V \in W'(E)[2]$, so that (U', V', U, V) forms a basis of a subgroup of $W'(E)(\mathbb{F}_p)$ isomorphic to $\mathbb{Z}_2^2 \times \mathbb{Z}_{(p+1)/2}^2$ and of the same cardinality. This proves (i).

(iii) Let ι be the S -orientation of $W(E)$ induced by the Frobenius and ι' be the resulting S -orientation of $W'(E)$ via the module action by $\mathfrak{f}$. Then, on the one hand, Γ being S -oriented, we have $\iota'(\sqrt{-p}) \circ \Gamma = \Gamma \circ \iota(\sqrt{-p}) = \Gamma \circ \pi$, so that $\iota'(\sqrt{-p}) = 1/2 \Gamma \circ \pi \circ \tilde{\Gamma}$. On the other hand, Γ is $\mathbb{F}_p$ -rational and we then have $\pi' \circ \Gamma = \Gamma \circ \pi$, where π' is the p -Frobenius endomorphism of $W'(E)$. It follows that $\pi' = 1/2 \Gamma \circ \pi \circ \tilde{\Gamma} = \iota'(\sqrt{-p})$ so that $W'(E)$ is S -oriented via its p -Frobenius endomorphism.

To conclude that $W'(E)$ is R -oriented, we have to prove that $(\pi' - 1)/2$ is an endomorphism, i.e. that $W'(E)[2] \subseteq W'(E)(\mathbb{F}_p)$, which holds by (ii). $\square$

Similar to the Weil restriction, Scholten's construction also maps n -isogenies $E_1 \rightarrow E_2$ to n -isogenies $W'(E_1) \rightarrow W'(E_2)$, and, by Lemma C.2.(ii), Scholten's construction $W'(E)$ does have rational 2-torsion! This allows us to efficiently work with (variations of) level-2 theta structures. In particular, when $p \equiv 7 \pmod{8}$, Scholten's construction has a rational level-2 theta null point [Rob24b, Lemma 5.15].

Lemma C.3 (Prop. 5.18 [Rob24b]). *Let E be an elliptic curve over $\mathbb{F}_p$ with $E[2] \subseteq E(\mathbb{F}_p)$. Then the Scholten's construction of E satisfies over $\mathbb{F}_p$:*

$$W'(E) \cong E \times E^t.$$

Proof. We have seen in Remark C.3 that $W(E)$ is an $\mathbb{F}_p$ -twist of E^2 for E over $\mathbb{F}_p$. The map $\Gamma : W(E) \rightarrow W'(E)$ now coincides with the differential addition map $(P, Q) \mapsto (P+Q, P-Q)$ as they both have kernel $\{(P, P) \mid P \in E[2]\}$. Now, applying first $\pi : (P, Q) \mapsto (\sigma(Q), \sigma(P))$ and then Γ results in $\Gamma \circ \pi(P, Q) = (\sigma(P+Q), -\sigma(P-Q))$. Since Γ is $\mathbb{F}_p$ -rational, the p -Frobenius endomorphism π' of $W'(E)$ satisfies $\Gamma \circ \pi = \pi' \circ \Gamma$, so it is given by $\pi' : (P, Q) \mapsto (\sigma(P), -\sigma(Q))$.

That is, the first factor is as expected, but the second factor is twisted by $[-1]$. Hence, $W'(E)$ is $\mathbb{F}_p$ -isomorphic to the twist by $[1] \times [-1]$ of E^2 , i.e., $E \times E^t$. $\square$

A special case is given by $E'_0 : y^2 = x^3 - x$ over $\mathbb{F}_p$ with $p \equiv 3 \pmod{4}$. For this curve, it holds that $E'_0[2] \subseteq E'_0(\mathbb{F}_p)$ and $E'_0 \cong E'_0$, hence, we immediately get the following corollary.

Corollary C.1 (Example 5.19 [Rob24b]). *Let $p \equiv 3 \pmod{4}$ and let $E'_0 : y^2 = x^3 - x$ over $\mathbb{F}_p$. Then the Scholten's construction of E'_0 satisfies*

$$W'(E'_0) \cong E'_0 \times E'_0.$$

C.3 A conceptual proof of Corollary 3.1

We now work out the relation between Scholten's construction and the module action in much greater detail than in Corollary 3.1. Let E be a maximal supersingular elliptic curve defined over $\mathbb{F}_{p^2}$. As claimed, we now formally prove that $W(E)$ is primitively oriented by $S = \mathbb{Z}[\sqrt{-p}]$ via its p -Frobenius endomorphism and that $W'(E)$ is primitively oriented by $R = \mathbb{Z}[(\sqrt{-p}-1)/2]$ as a result of the action of an ascending 2-isogeny via the conductor ideal $\mathfrak{f} := (2, \sqrt{-p}-1)$ of R .

Theorem C.1. *Assume that $p \equiv 3 \pmod{4}$. Let E_0 be a primitively R -oriented supersingular elliptic curve defined over $\mathbb{F}_p$ and $E'_0 := \mathfrak{f} \cdot_R E_0$. Let $\mathcal{O}_0$ be a quaternion order isomorphic to $\text{End}(E_0)$, I be a left $\mathcal{O}_0$ -ideal and $\varphi_I : E_0 \rightarrow E_I$ be the isogeny corresponding to I via the Deuring correspondence. Then:*

- (i) $W(E_I) = M_I \cdot_S E_0$ where $M_I \simeq I$ as an S -module.
- (ii) $W'(E_I) = (R \otimes_S M_I) \cdot_R E'_0$.

Proof. (i) Recall that $W(E_I) = E_I \times E_I^\sigma$ with the p -Frobenius endomorphism $\pi : (P, Q) \mapsto (\sigma(Q), \sigma(P))$ and $\sigma : E_I \rightarrow E_I^\sigma$ the p -Frobenius isogeny of E_I . Consider $\varphi_I^\sigma : E_0 \rightarrow E_I^\sigma$, the *Galois conjugate* of φ_I satisfying $\sigma \circ \varphi_I = \varphi_I^\sigma \circ \sigma_0$, where σ_0 is the p -Frobenius endomorphism of E_0 . Then, $W(E_I)$ is isogenous to E_0^2 via the Weil restriction of φ_I , $W(\varphi_I) = \text{Diag}(\varphi_I, \varphi_I^\sigma) : E_0^2 \rightarrow E_I \times E_I^\sigma$. Besides, we have $\pi \circ W(\varphi_I) = W(\varphi_I) \circ \text{Diag}(\sigma_0, \sigma_0)$ by construction, which proves that $W(E_I)$ is isogenous to E_0^2 over $\mathbb{F}_p$. Then, [JKP+18, Theorem 7.11] ensures the existence of an R -module M_I such that $W(E_I) = M_I \cdot_R E_0$.

Then, by Proposition B.3.(ii), we have

$$\begin{aligned} M_I &\simeq \text{Hom}_{\mathcal{A}_S}(W(E_I), E_0) \\ &= \{(\varphi, \psi) \mid \varphi : E_I \rightarrow E_0, \psi : E_I^\sigma \rightarrow E_0, (\varphi, \psi) \circ \pi = \sigma_0 \circ (\varphi, \psi)\} \\ &= \{(\varphi, \psi) \mid \varphi : E_I \rightarrow E_0, \psi : E_I^\sigma \rightarrow E_0, \sigma_0 \circ \varphi = \psi \circ \sigma \wedge \sigma_0 \circ \psi = \varphi \circ \sigma\} \\ &= \{(\varphi, \varphi^\sigma) \mid \varphi \in \text{Hom}(E_I, E_0)\} \simeq \text{Hom}(E_I, E_0) \simeq I, \end{aligned}$$

where φ^σ is the Galois conjugate of φ and the last isomorphism follows from the Deuring correspondence.

(ii) By [Lemma C.2.\(i\)](#) and [Proposition B.1.\(iv\)](#) and [Proposition B.2](#), we then have:

$$\begin{aligned} W'(E_I) &= \mathfrak{f} \cdot_S W(E_I) \simeq \mathfrak{f} \cdot_S (M_I \cdot_S E_0) \simeq M_I \cdot_S (\mathfrak{f} \cdot_S E_0) = M_I \cdot_S E'_0 \\ &= (R \otimes_S M_I) \cdot_R E'_0. \end{aligned}$$

This completes the proof. $\square$

We can now specialise [Theorem C.1](#) to a specific case of interest when $E_0 \simeq E'_0$, to obtain a more conceptual proof of [Corollary 3.1](#).

Corollary C.2. *Consider the curves $E_0 : y^2 = x^3 + x$ and $E'_0 : y^2 = x^3 - x$ defined over $\mathbb{F}_p$ with $p \equiv 7 \pmod{8}$. Then E_0 is primitively R -oriented, $E'_0 = \mathfrak{f} \cdot_R E_0$, E'_0 is the quadratic twist of E_0 and we may consider a quaternion order $\mathcal{O}_0$ isomorphic to $\text{End}(E_0) \simeq \text{End}(E'_0)$. Let I be a left $\mathcal{O}_0$ -ideal and $\varphi_I : E'_0 \rightarrow E_I$ be the isogeny corresponding to I via the Deuring correspondence and ρ_0 be the isomorphism $\mathcal{O}_0 \xrightarrow{\sim} R^2, \alpha + \beta i \mapsto (\alpha, \beta)$. Then $W'(E_I) = M_I \cdot_R E'_0$ with $M_I := \rho_0(I)$.*

Proof. Let $\varphi_{\mathfrak{f}} : E_0 \rightarrow \mathfrak{f} \cdot E_0$ be the 2-isogeny associated to $\mathfrak{f}$. Then $\ker(\varphi_{\mathfrak{f}}) = E_0[2] \cap E_0(\mathbb{F}_p) = \langle (0, 0) \rangle$. By the formulae in [\[Ren18, Remark 6\]](#), we obtain that $\mathfrak{f} \cdot E_0$ has an equation of the form $y^2 = x^3 + 6x^2 + 8x = x(x+2)(x+4)$ over $\mathbb{F}_p$. Considering the isomorphism $(x, y) \mapsto (x/2 + 1, y/(2\sqrt{2}))$, we obtain that $\mathfrak{f} \cdot E_0 \simeq E'_0$. Since $p \equiv 7 \pmod{8}$, we have $\sqrt{2} \in \mathbb{F}_p$ so this isomorphism is $\mathbb{F}_p$ -rational.

By [Theorem C.1.\(ii\)](#), we have $W'(E_I) = (R \otimes_S M_I) \cdot_R E'_0$ with $M_I \simeq I$ as an R -module, so that $R \otimes_S M_I \simeq R \otimes_S I$ as an R -module. But E'_0 is R -oriented since $E'_0[2] = \{0, (0, 0), (1, 0), (-1, 0)\} \subset E'_0(\mathbb{F}_p)$. Hence $R \hookrightarrow \mathcal{O}_0$, and since I is stable by left multiplication by $\mathcal{O}_0$, it is stable by left multiplication by R and we must have $R \otimes_S I \simeq I$. It follows that $R \otimes_S M_I \simeq I \simeq M_I$ as R -modules, which completes the proof. $\square$

D MIKE from the matrix point of view

There are two equivalent ways of seeing the module action involved in the MIKE key exchange. The first one is via modules and module morphisms and is developed in details [Appendix B](#). Although more conceptual, this approach gives the easiest proofs, which mostly follow by functoriality.

The second approach is the one introduced in [Section 2](#) where we build out the explicit isogenies induced by the module action from kernels given by suitable matrices. In this section we revisit the MIKE key exchange from this “more practical” matrix point of view. The idea to revisit MIKE and the commutative diagram in [Corollary D.1](#) from the point of view of the matrix kernels of the corresponding isogenies was suggested to us by Marc Houben.

First recall from [Section 2](#) the following notation: if A is an R -oriented abelian variety and $M \in M_{r \times g}(R)$, we denote by $A^g[M]$ the kernel of the application $M : A^g \rightarrow A^r$ induced by M and the orientation. As a variant of [Theorem 2.5](#), we get:

Proposition D.1. *Let (A, λ_A) be a primitively R -oriented principally polarised abelian variety of rank r , for R a quadratic imaginary order. Let $U \in M_g(R)$ be a Hermitian matrix such that $U^*U = N \text{Id}$. Let $n \mid N$ and consider $M = \begin{pmatrix} n \text{Id} \\ U \end{pmatrix}$, and assume further that $A^g[M] = A^g[n, U] \subset A^g[n]$ is of cardinal n^{rg} . Then $A^g[M]$ is maximal isotropic, and the quotient by this kernel induces a n -isogeny $(A^g, \lambda_A^g) \rightarrow (B = A^g/A^g[M], \lambda_B)$.*

Proof. Since $U^*U = N \text{Id}$, we have $U^*A^g[n] \subset A^g[n, U]$. Furthermore, since $e_n(Ux, y) = e_n(x, U^*y)$ because the orientation is compatible with the polarisation, we also have that $U^*A^g[n]$ is the orthogonal for the Weil pairing $e_n = e_{n\lambda_A}$ of $A^r[n, U]$. So if $\#A^g[n, U] = n^{rg}$ then $\#U^*A^g[n] = n^{rg}$ and we have equality: $U^*A^g[n] = A^g[n, U]$. In particular, $A^g[n, U]$ is maximal isotropic, so the polarisation $n\lambda_A^g$ descends to a principal polarisation λ_B on $B = A^g/A^g[M]$. $\square$

Remark D.1. Note that working on the Tate module $T_\ell A^g$ for $\ell \mid N$, because of the condition $U^*U = N \text{Id}$, then if $v_\ell(N) = e$, i.e. $\ell^e \parallel N$, we see that $A^g[\ell^e, U] \simeq \prod \mathbb{Z}/\ell_i^{e_i} \mathbb{Z}$, $e_1 \leq e_2 \leq \dots \leq e_{2rg}$, with $e_i + e_{2rg+1-i} = e$. It follows that the condition that $A^g[M] = A^g[n, U]$ is of cardinal n^{rg} is satisfied in the following cases:

- $A^g[\ell, U]$ has rank rg for all prime factors $\ell \mid n$. In this case $A^g[n, M]$ is of rank rg .
- $\gcd(N, n^2) = n$, as in [EPSV23, § 4.1]. But note that in this case $A^g[M]$ might not be of rank rg .
- U and U^* are coprime modulo n in the sense that $R^g U + R^g U^* + nR^g = R^g$. In this case we even have that $A^g[n] = A^g[n, U] \oplus A^g[n, U^*]$ is a symplectic decomposition for the Weil pairing e_n . (Indeed, from $R^g U + R^g U^* + nR^g = R^g$ we get that $A^g[n, U] \cap A^g[n, U^*] = \{0\}$, but taking the conjugate transpose we also have $UR^g + U^*R^g + nR^g = R^g$, which gives us $A^g[n] = A^g[n, U] + A^g[n, U^*]$.)

Let X be the image of M^T , i.e. the submodule $U^T R^g + nR^g$ of R^g . Consider H the canonical Hermitian form on R^g . Then the same proof as in Proposition D.1, using [Rob24b, Proposition A.1], shows that if $\#R^g/X = n^g$, then $(X, H/n)$ is a unimodular Hermitian module. This makes the link with the module action and Theorem 2.5.

Note also that if A is R -horizontally isogeneous to E^r for a primitively R -oriented elliptic curve E , then by [JKP+18, Theorem 4.4.(e)], $\#A^g[n, U] = \#(R^g/X)^r$, so $\#A[n, U] = n^{rg}$ whenever $\#(R^g/X) = n^g$.

From now on, we assume that A is R -horizontally isogeneous to E^r for a primitively R -oriented elliptic curve E , in the sense of [Rob24b, Definition 2.3]. Note that this is the case in MIKE: all our abelian varieties are isogeneous to E_0^r , and R is a maximal order, so the horizontality condition is automatic.

Example D.1 (The ideal action). Let $\mathfrak{a} = (n, \alpha)$ be an invertible ideal, with $n = \text{nrd}(\mathfrak{a})$, as in [Example 2.1](#). Then $A[\mathfrak{a}] = A[n, U]$, with $U = (\alpha)$, so that $U^*U = N = n(\alpha)$.

Example D.2 (MIKE's key generation). Let $U = \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix}$ for $\alpha, \beta \in R$, so that $U^*U = (\alpha\bar{\alpha} + \beta\bar{\beta})\text{Id}$. Let $N = (\alpha\bar{\alpha} + \beta\bar{\beta})$. The MIKE key generation uses the isogeny from E_0^2 with kernel $E_0^2[n, U]$ with $n = 2^e \mid N$.

As we saw in [Section 3](#), the matrix U is specifically constructed so that we can recover the codomain of this isogeny directly as applying the Scholten construction to the dimension 1 isogeny $E_0 \rightarrow E_0/E_0[I]$ where I is the quaternionic ideal $I = (n, \alpha + \beta\mathbf{i})$ (with I chosen so that it is cyclic). This allows us to replace a dimension 2 isogeny computation over $\mathbb{F}_p$ by a dimension 1 isogeny over $\mathbb{F}_{p^2}$, and have more compact keys by sending only one j -invariants over $\mathbb{F}_{p^2}$ rather than three Igusa invariants over $\mathbb{F}_p$.

Proposition D.2 ($\otimes$ -MIKE). *Let U_1 be a matrix of rank g_1 . Let $U_1 \in M_{g_1}(R)$ be such that $U_1^*U_1 = N_1$, and take $n_1 \mid N_1$ such that n_1 is prime to the conductor of R and such that the $\mathbb{Z}/\ell\mathbb{Z}$ -rank of U_1 modulo ℓ is equal to g_1 for all $\ell \mid N_1$. Let $M_1^T = (n_1 \text{Id } U_1^T)$ and X_1 the image of M_1^T in R^{g_1} . Coprimality of n_1 with the conductor ensures that X_1 is projective and the rank condition ensures that R^{g_1}/X_1 is of cardinal $n_1^{g_1}$ and that $A[M_1] = A[n_1, U_1]$ is isotropic of rank g_1 (recall that we assume A to be horizontal).*

Let $U_2 \in M_{g_2}(R)$ be such that $U_2^*U_2 = N_2$, and take $n_2 \mid N_2$ which satisfy the same conditions as above, and let $M_2^T = (n_2 \text{Id } U_2^T)$.

Then we have a commutative diagram:

$$\begin{array}{ccc} A^{g_1 g_2} & \xrightarrow{\quad\quad\quad} & A_1^{g_2} = (A^{g_1}/A^{g_1}[n_1, U_1])^{g_2} \\ \downarrow & & \downarrow \\ A_2^{g_1} = (A^{g_2}/A^{g_2}[n_2, U_2])^{g_1} & \longrightarrow & A_{12} = A^{g_1 g_2}/A^{g_1 g_2}[n_1 n_2, U_1 \otimes_R \text{Id}_{g_2}, n_1 \text{Id}_{g_1} \otimes_R U_2, U_1 \otimes U_2] \end{array}$$

Proof. This follows from functoriality of the module action applied to the commutative diagram

$$\begin{array}{ccc} R^{g_1 g_2} & \longleftarrow & X_1^{g_2} = X_1 \otimes_R R^{g_2} \\ \uparrow & & \uparrow \\ X_2^{g_1} = R^{g_1} \otimes_R X_2 & \longleftarrow & X_1 \otimes_R X_2 \end{array},$$

along with the fact that $X_1^{g_2}$ is the image of the block diagonal matrix $\text{diag}(M_1^T) = M_1^T \otimes \text{Id}_{g_2}$, $X_2^{g_1}$ the image of the block diagonal matrix $\text{diag}(M_2^T) = \text{Id}_{g_1} \otimes_R M_2^T$, and $X_1 \otimes_R X_2$ the image of $M_1^T \otimes_R M_2^T$.

Note that as explained in [Rob24b, Remark 6.2], one has to be careful how to decompose $A^{g_1 g_2}$ as $(A^{g_1})^{g_2}$ and $(A^{g_2})^{g_1}$ respectively to make the diagram commute. $\square$

We let as a challenge to the reader to prove [Proposition D.2](#) directly from the kernel descriptions.

Now let us recapitulate the MIKE key exchange from [Section 4](#):

- We start from the curve $E_0/\mathbb{F}_p : y^2 = x^3 - x$;
- Alice pick up a (cyclic) quaternionic ideal $I_1 = (n, \gamma_1)$ with $n = \text{nrd}(I_1) = 2^e$ and $\gamma_1 = \alpha_1 + \beta_1 \mathbf{i}$, and she computes the associated isogeny $E_0 \rightarrow E_1$ of degree n . Bob does the same with $I_2 = (n, \gamma_2)$, $\gamma_2 = \alpha_2 + \beta_2 \mathbf{i}$.
- By [Example D.2](#), the ideal I_1 corresponds to a rank 2 Hermitian module X_1 given by the image of R^4 by the matrix $M_1^T = \begin{pmatrix} n & 0 & \alpha_1 & -\bar{\beta}_1 \\ 0 & n & \beta_1 & \bar{\alpha}_1 \end{pmatrix}$. By [Section 3](#), $A_1 = X_1 \cdot E_0 = E_0^2/E_0^2[M_A]$ is the abelian surface $W'(E_A)$. Likewise, $A_2 = X_2 \cdot E_0 = W'(E_B)$.

Now combining [Propositions D.1](#) and [D.2](#), we get:

Corollary D.1 (MIKE). *With the notations above, the fourfold $A_{12} = (X_1 \otimes_R X_2) \cdot E_0$ that gives the MIKE key exchange fits into the following commutative diagram*

$$\begin{array}{ccc} E_0^4 & \xrightarrow{\phi_1} & A_1^2 \\ \downarrow \phi_2 & & \downarrow \psi_2 \\ A_2^2 & \xrightarrow{\psi_1} & A_{12} \end{array}$$

where:

- $\phi_1 : E_0^4 \rightarrow A_1^2$ and $\psi_1 : A_2^2 \rightarrow A_{12}$ are n -isogenies with kernel of rank 4 given by the matrix

$$M_1 \otimes_R \text{Id} = \begin{pmatrix} n & 0 & 0 & 0 \\ 0 & n & 0 & 0 \\ 0 & 0 & n & 0 \\ 0 & 0 & 0 & n \\ \alpha_1 & 0 & \beta_1 & 0 \\ 0 & \alpha_1 & 0 & \beta_1 \\ -\bar{\beta}_1 & 0 & \bar{\alpha}_1 & 0 \\ 0 & -\bar{\beta}_1 & 0 & \bar{\alpha}_1 \end{pmatrix}$$

- $\phi_1 : E_0^4 \rightarrow A_1^2$ and $\psi_1 : A_2^2 \rightarrow A_{12}$ are n -isogenies with kernel of rank 4 given by the matrix

$$\text{Id} \otimes_R M_2 = \begin{pmatrix} n & 0 & 0 & 0 \\ 0 & n & 0 & 0 \\ \alpha_2 & \beta_2 & 0 & 0 \\ -\bar{\beta}_2 & \bar{\alpha}_2 & 0 & 0 \\ 0 & 0 & n & 0 \\ 0 & 0 & 0 & n \\ 0 & 0 & \alpha_2 & \beta_2 \\ 0 & 0 & -\bar{\beta}_2 & \bar{\alpha}_2 \end{pmatrix}$$

- And finally $\psi_2 \circ \phi_1 = \psi_1 \circ \psi_2$ is a n^2 -isogeny whose kernel is given by the matrix

$$M_1 \otimes_R M_2 = \begin{pmatrix} n^2 & 0 & 0 & 0 \\ 0 & n^2 & 0 & 0 \\ n\alpha_2 & n\beta_2 & 0 & 0 \\ -n\bar{\beta}_2 & n\bar{\alpha}_2 & 0 & 0 \\ 0 & 0 & n^2 & 0 \\ 0 & 0 & 0 & n^2 \\ 0 & 0 & n\alpha_2 & n\beta_2 \\ 0 & 0 & -n\bar{\beta}_2 & n\bar{\alpha}_2 \\ n\alpha_1 & 0 & n\beta_1 & 0 \\ 0 & n\alpha_1 & 0 & n\beta_1 \\ \alpha_1\alpha_2 & \alpha_1\beta_2 & \beta_1\alpha_2 & \beta_1\beta_2 \\ -\alpha_1\bar{\beta}_2 & \alpha_1\bar{\alpha}_2 & -\beta_1\bar{\beta}_2 & \beta_1\bar{\alpha}_2 \\ -n\bar{\beta}_1 & 0 & n\bar{\alpha}_1 & 0 \\ 0 & -n\bar{\beta}_1 & 0 & n\bar{\alpha}_1 \\ -\bar{\beta}_1\alpha_2 & -\bar{\beta}_1\beta_2 & \bar{\alpha}_1\alpha_2 & \bar{\alpha}_1\beta_2 \\ \bar{\beta}_1\bar{\beta}_2 & -\bar{\beta}_1\bar{\alpha}_2 & -\bar{\alpha}_1\bar{\beta}_2 & \bar{\alpha}_1\bar{\alpha}_2 \end{pmatrix}$$

Remark D.2.

- In the actual implementation, the quaternionic ideals I_1, I_2 are implicitly determined by the choice of kernel generator $P + [x_i]Q$ of Alice and Bob isogenies. Also, as we will see in [Appendix F](#), the isogenies to A_{12} is not constructed from Scholten $W'(E_i)^2$ but directly from the Weil restriction $W(E_i)^2$.
- Let $U_i = \begin{pmatrix} \alpha_i & \beta_i \\ -\bar{\beta}_i & \bar{\alpha}_i \end{pmatrix}$, then modulo n these have (generically) rank 1 over $\mathbb{Z}/n\mathbb{Z}$, so $U_1 \otimes_R U_2$ is also of rank 1. Let $K_i = \text{Ker } \phi_i$, and $K = \text{Ker } \psi_2 \circ \phi_1$. We have $K[n] = \text{Ker}(U_1 \otimes U_2)$, which is then of rank $6 = 2 \times 3$ in $E_0^4[n]$, and $K_1 \cap K_2$ is of rank $2 = 8 - 6$. In particular $K \supset K_1 + K_2$ strictly contains the sum, so the MIKE diagram is not a pushforward diagram! Since K is associated to a N^2 -isogeny, we have that NK is of rank 2; and $\psi_1 : A_1^2 \rightarrow A_{12}$ is partially backtracking (in rank 2) the isogeny $\phi_1 : E_0^4 \rightarrow A_1^2$.
- The above discussion clarifies [\[Rob24b, Remark 6.2\]](#) as to why, even if Alice and Bob isogenies are complementary, in the sense that the kernels K'_i of the

n -isogenies $E_0 \rightarrow E_i$ satisfy $K'_1 \cap K'_2 = \{0\}$ (equivalently $K'_1 + K'_2 = E_0[n]$), $\text{MIKE}(E_1, E_2)$ is not isomorphic to E_0^4 .

In fact, an exhaustive collision search on several small parameters p , generating all possible kernels for Alice and Bob (and ignoring the cases of E_1 or E_2 defined over $\mathbb{F}_p$, or random failures²²), detected no collisions except for the trivial ones: $\text{MIKE}(E_1, E_2) = \text{MIKE}(E_2, E_1)$.

E Abelian varieties in the theta model

When working explicitly with an elliptic curve E , one typically represents the elliptic curve by an equation, for example by Montgomery's equation $y^2 = x^3 + Ax^2 + x$. For many applications, it turns out that the arithmetic is more efficient when working on the *Kummer line* $K = E/\langle[-1]\rangle \cong \mathbb{P}^1$, where points are presented by their x -coordinates.²³ Though part of the group structure is lost, isogenies and scalar multiplication are still well-defined and efficiently computable. To efficiently work with higher dimensional abelian varieties, we need to work with the generalisation of the Kummer line over principally polarised abelian variety, called *theta structures*. As they are central in the subsequent appendices, we give in [Appendix E.1](#) a reminder on their definition and use in fast isogeny computations. Then, we details in [Appendix E.2](#) how we can improve the isogeny formulae between the abelian fourfold encountered in MIKE.

E.1 A coordinate systems for abelian varieties

This section is a simplified introduction building on [\[DD26\]](#). Let (A, λ_A) be a PPAV of dimension g over k and $n \in \mathbb{N}_{>0}$. We know that $A[n] \simeq \mathbb{Z}_n^{2g} \simeq \mathbb{Z}_n^g \times \widehat{\mathbb{Z}_n^g}$, where $\widehat{\mathbb{Z}_n^g}$ denotes the group of characters $\mathbb{Z}_n^g \rightarrow \overline{k}^*$. A *symplectic representation* is an isomorphism $\mu : A[n] \xrightarrow{\sim} \mathbb{Z}_n^g \times \widehat{\mathbb{Z}_n^g}$ that respects the n -th Weil pairing $e_n^{\lambda_A}$ on $A[n]$ with respect to the polarisation λ_A and the canonical pairing of its codomain.

$$\forall P_1, P_2 \in A[n] \text{ with } \mu(P_j) = (x_j, \chi_j) \text{ for } j \in \{1, 2\}, \quad e_n^{\lambda_A}(P_1, P_2) = \chi_2(x_1)\chi_1(x_2)^{-1}$$

Symplectic representations μ represent the unique representation of $A[n]$ in a (ζ) -*symplectic basis* of $A[n]$, i.e. a basis $(S_1, \dots, S_g, T_1, \dots, T_g)$ such that

$$\forall l, m \in [1, \dots, g], \quad e_n^{\lambda_A}(S_l, S_m) = e_n^{\lambda_A}(T_l, T_m) = 1 \quad \text{and} \quad e_n^{\lambda_A}(S_l, T_m) = \zeta^{\delta_{l,m}}.$$

with both notion being equivalent. Representations of A that are compatible with symplectic representations of $A[n]$ are called level n theta structure. They are defined as follows.

²² The gluing and isogeny code can fail, and produce a zero key, with cryptographically small probability $\approx 1/p$. But these random failures will happen when we do an exhaustive search on $\approx p^2$ keys.

²³ By x -coordinate, we really mean the projective coordinates $(x : z) \in \mathbb{P}^1$ here.

Definition E.1. [DD26, Definition 2.1] A theta structure of level n on a PPAV A of dimension g is given by a symplectic representation $\mu_A : A[n] \xrightarrow{\sim} \mathbb{Z}_n^g \times \widehat{\mathbb{Z}_n^g}$ and a map to the projective space $\theta^A : A \rightarrow \mathbb{P}^{n^g-1}$ whose components θ_j^A (for $j \in \mathbb{Z}_n^g$) are called theta coordinates. They should satisfy the theta group action relation:

$$\forall P \in A, Q \in A[n] \text{ with } \mu_A(Q) = (x_Q, \chi_Q), j \in \mathbb{Z}_n^g, \quad \theta_j^A(P+Q) = \chi_Q(j)^{-1} \theta_{j+x_Q}^A(P). \quad (16)$$

Throughout this paper, we will work mainly using level-2 theta structure. In such case, we have that the theta coordinates are symmetric (i.e. $\theta^A(-P) = \theta^A(P)$). The image of the neutral element, $\theta(0_A) = (a_0 : \dots : a_{2^g-1})$, is called the *level-2 theta null point* of A and its coordinates are called the *theta constants*. We remark that the theta null point is not an isomorphism invariant of A , but one can show that it is uniquely determined (together with a theta structure) by a choice of symplectic basis for $A[4]$. Vice versa, the theta null point, determines a *canonical symplectic basis* for $A[2]$.

Moreover, given $\mathcal{B}$ and $\mathcal{B}'$, two symplectic basis of $A[4]$ with associated theta structure θ^A and θ'^A and let $\mathbf{M} \in \mathrm{Sp}_{2g}(\mathbb{Z}_4)$ be the change of basis matrix. Then, we can compute a *change of theta coordinates matrix* $\mathbf{N}_{\mathbf{M}, \zeta} \in \mathrm{PGL}_{2^g}$ such that $(\theta'_i{}^A)_{i \in \mathbb{Z}_2^g} = \mathbf{N}_{\mathbf{M}, \zeta} \cdot (\theta_j^A)_{j \in \mathbb{Z}_2^g}$ using the formula from [Dar25b, Theorem 6.2.10]. Applying this formula to the block matrix $\mathbf{M} := [[0, -I_g], [I_g, 0]]$ and $\zeta := \sqrt{-1}$, we obtain that $\mathbf{N}_{\mathbf{M}, \zeta}$ is the *Hadamard transform* $H : (x_i)_{i \in \mathbb{Z}_2^g} \mapsto \left(\sum_{j \in \mathbb{Z}_2^g} (-1)^{\langle i|j \rangle} x_j \right)_{i \in \mathbb{Z}_2^g}$ inducing the *dual theta coordinates*

$$\forall i \in \mathbb{Z}_2^g, \quad \tilde{\theta}_i^A = H(\theta^A)_i = \sum_{j \in \mathbb{Z}_2^g} (-1)^{\langle i|j \rangle} \theta_j^A,$$

with the scalar product $\langle i|j \rangle := \sum_{m=1}^g i_m j_m$.

Thanks to duality, we can equip level-2 theta structure with efficient differential arithmetic. We refer to [Dar25b, Alg. 4.1 & Alg. 4.2] for detailed formulae.

Level-(2, 2) theta structure.

Definition E.2. Consider a level-4 theta structure $\theta^{4,A}$ on A . The level (2, 2)-theta structure associated to $\theta^{4,A}$ is a projective map $U^A : A \rightarrow \mathbb{P}^{2n^g-1}$ given by:

$$\forall i, j \in \mathbb{Z}_2^g, \quad \vartheta^A \begin{bmatrix} i \\ j \end{bmatrix} = \sum_{t \in \mathbb{Z}_2^g} (-1)^{\langle i|t \rangle} \theta_{j+2t}^{4,A}$$

We call even and odd level-(2, 2) theta coordinates the $\vartheta^A \begin{bmatrix} i \\ j \end{bmatrix}$ for $i, j \in \mathbb{Z}_2^g$ such that $\langle i|j \rangle = 0$ and $\langle i|j \rangle = 1$ respectively.

Let θ^A be a level-2 theta structure compatible with a level-4 theta structure $\theta^{4,A}$, meaning that, if $\theta^{4,A}$ is induced by a symplectic basis $\mathcal{B}$ of $A[8]$, then θ^A is induced by the symplectic basis $[2]\mathcal{B}$ of $A[4]$. Then, we have by the duplication formula [Dar25b, Theorem 5.3.41]:

$$\forall P, Q \in A, i, j \in \mathbb{Z}_2^g \quad \vartheta^A \begin{bmatrix} i \\ j \end{bmatrix} (P) \cdot \vartheta^A \begin{bmatrix} i \\ j \end{bmatrix} (Q) = \sum_{t \in \mathbb{Z}_2^g} (-1)^{\langle i|t \rangle} \theta_{j+t}^A(P+Q) \theta_t^A(P-Q). \quad (17)$$

In the following, we shall drop the mention of the underlying level-4 theta structure when we introduce the level-(2, 2) structure.

2-isogeny computation in the theta model. We explain here how to compute a 2-isogeny $f : A \rightarrow B$ in level-2 theta coordinates as follows. Assume that we are given a symplectic basis $\mathcal{B} := (S_1, \dots, S_g, T_1, \dots, T_g)$ of $A[8]$ which is *adapted to f* in the sense of [Dar25b, Definition 6.1.2] i.e. such that $\ker(f) = \langle [4]T_1, \dots, [4]T_g \rangle$ and consider the level-2 theta structure θ^A induced by the symplectic basis $[2]\mathcal{B}$ of $A[4]$. Then, we can determine the codomain level-2 theta structure θ^B induced by the symplectic basis $f_*(\mathcal{B}) = ([2]f(S_1), \dots, [2]f(S_g), f(T_1), \dots, f(T_g))$ of $B[4]$. Indeed, using the input 8-torsion points $T_1, \dots, T_g$ and [DD26, Algorithm 1], we can determine the inverse codomain dual theta null point $\tilde{\theta}^B(0_B)^{\odot -1}$ (when the inverse exists). Then, given $\tilde{\theta}^B(0_B)^{\odot -1}$, we have an evaluation algorithm $\theta^A(P) \mapsto \theta^B(f(P))$ [Dar25b, Algorithm 6.1] given as follows:

$$\theta^A(P) \xrightarrow{S} \theta^A(P)^{\odot 2} \xrightarrow{H} H(\theta^A(P)^{\odot 2}) \xrightarrow{\odot \tilde{\theta}^B(0_B)^{\odot -1}} \tilde{\theta}^B(f(P)) \xrightarrow{H} \theta^B(f(P)).$$

The crux of the difficulty lies in the efficient computation of $\tilde{\theta}^B(0_B)^{\odot -1}$. The fastest known method [DD26, Algorithm 1] relies on interpolating the coefficients of vectors $\{\tilde{\theta}^B(0_B) \odot \tilde{\theta}^B(f(T_j))\}_{j \in S}$, where T_j are 8-torsion points lying above $\ker(f)$ for a set $S \subseteq \mathbb{Z}_2^4$. Following the theta group action relation [DD26, Definition 2.1], there exists a unique $j \in \mathbb{Z}_2^g$ such that $\tilde{\theta}^B(f(T_j))_i = \tilde{\theta}^B(f(T_j))_{i+j}$ hence defining its index. It was demonstrated in [DD26, §3.1] that the computation of $\tilde{\theta}^B(0_B)^{\odot -1}$ can be abstracted into a graph-theoretic problem: the HIIP (hypercube inverse interpolation problem) [DD26, Problem 3.1].

Computing chains of 2-isogenies. Now, if we want to compute a 2^e -isogeny $F : A \rightarrow B$, as in MIKE, we can decompose it as a chain of 2-isogenies:

$$A_0 = A \xrightarrow{f_1} A_1 \xrightarrow{f_2} A_2 \quad \dots \quad A_{e-2} \xrightarrow{f_{e-1}} A_{e-1} \xrightarrow{f_e} A_e = B$$

Assuming we know $T_1, \dots, T_g \in A[2^{e+2}]$ forming an isotropic subgroup and such that $\ker(F) = \langle [4]T_1, \dots, [4]T_g \rangle$ (e.g. as in Theorem 4.1), we can compute the 2-isogeny f_i from $[2^{e-i}]f_{i-1} \circ \dots \circ f_1(T_1, \dots, T_g)$ for all $i \in \{1, \dots, e\}$ using the techniques explained above. Therefore, an isogeny chain computation involves

several point duplications (that can be computed with [Dar25b, Algorithm 5.2]) and 2-isogeny evaluations. Using divide and conquer strategies, we can perform only $O(e \log(e)g)$ such operations. Note however that computing the first isogeny f_1 (and sometimes subsequent f_2 and f_3) may not be straightforward for the following reasons:

- A may be a product (*e.g.* a product of elliptic curves) in which case f_1 is a *gluing isogeny* and has a vanishing codomain theta null point. Then the computation and evaluation procedures have to be adapted, as we explain in [Appendix F](#) in the case of MIKE.
- The domain theta structure θ^A that we naturally obtain (*e.g.* a product theta structure) may not be adapted to f_1 , in which case we need to apply a change of theta coordinates using [Dar25b, Theorem 6.2.10].

In the specific case of MIKE, the gluing isogeny denote the first 3 2-isogenies f_1, f_2 and f_3 while the f_i for $i \geq 4$ will be called *generic* isogenies. The reason for this choice is detailed in [Appendix F](#).

E.2 Computing MIKE's 4-dimensional isogenies

We now demonstrate how, using [Proposition 4.1](#) and [Corollary G.3](#), we can speed up the computation of generic 4-dimensional isogenies occurring in MIKE. More precisely, we explain how to efficiently compute them using only 2 points above the kernel. Let $f : A \rightarrow B$ be a generic 2-isogeny in the MIKE 2-isogeny chain. First, we justify why we expect the inverse codomain dual theta null point $\tilde{\theta}^B(0_B)^{\odot -1}$ to be well defined and easy to compute throughout the chain.

As we shall see in [Corollary G.4](#), the fact that B is of Weil type ensures that six level-(2, 2) codomain even theta constants vanish at indices:

$$\begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}.$$

Except for odd level-(2, 2) theta constants, we expect other ones to vanish with negligible probability $O(p^{-1})$. By the duplication formula $H(\theta^A(0_A)^{\odot 2})_i = \tilde{\theta}_i^B(0_B)^2 = \vartheta^A[[i], [j]](0_A)$ for all $i \in \mathbb{Z}_2^4$ by the duplication formula [Dar25b, Corollary 6.1.3], we expect the codomain dual theta coordinates to vanish with negligible probability $O(p^{-1})$.

To simplify our computation, we make the following heuristic assumption for all generic 2-isogeny in the chain.

Heuristic E.1 *Let $f : A \rightarrow B$ be a generic 2-isogeny between two abelian fourfolds of Weil type appearing in MIKE's 2-isogeny chain. Let $\mathcal{B} := (S_1, \dots, S_4; T_1, \dots, T_4)$ be a symplectic basis of $A[8]$ such that $\ker(f) = [4]\langle T_1, \dots, T_4 \rangle$, Θ^A be induced by $[2]\mathcal{B}$, Θ^B be induced by $f_*(\mathcal{B})$. Then, we have:*

1. For all $i \in \mathbb{Z}_2^4$, $\tilde{\theta}_i^B(0_B) \neq 0$
2. For all $i \in \mathbb{Z}_2^4$, $\theta_i^B(0_B) \neq 0$;

3. For all $i \in \mathbb{Z}_2^4$ and $m \in \{1, 2, 3, 4\}$, $\tilde{\theta}_i^B(f(T_m)) \neq 0$;

except with negligible probability $O(p^{-1})$.

Remark E.1. The first point has been justified above, the second point is necessary to apply the point duplication algorithm on B and the third one for our codomain inverse dual theta null point $\tilde{\theta}^B(0_B)^{\odot -1}$ computation to work with an efficient algorithmic solution to the HIIP (hypercube inverse interpolation problem). Those assumptions are based on experimental evidence gathered from our implementation and are common in any isogeny based scheme relying on higher dimensional isogenies. Providing a mathematical proof is left as future work.

With the chain being correct with overwhelming probability, we now turn our attention to its efficient computation.

Theorem E.1. *Let $f: A \rightarrow B$ be a generic 2-isogeny between abelian fourfolds of Weil type appearing in MIKE's 4-dimensional 2-isogeny chain, and let θ^A, θ^B be theta structures compatible with the chain. Then, under the assumptions of [Heuristic E.1](#) its corresponding HIIP (hypercube inverse interpolation problem) used to determine the codomain inverse dual theta null point $\tilde{\theta}^B(0_B)^{\odot -1}$ can be solved using only two 8-torsion points.*

Proof. By [Heuristic E.1](#), we may assume that no coefficient in the dual theta null point is zero so the relevant HIIP is well defined. By [Heuristic E.1](#), we may further assume that input 8-torsion points T_1, T_2, T_3, T_4 lying above $\ker(f)$ satisfy $\tilde{\theta}_i^B(f(T_m)) \neq 0$, so that $H(\theta^A(T_m)^{\odot 2})_i = \tilde{\theta}^B(0_B) \cdot \tilde{\theta}_i^B(f(T_m)) \neq 0$ for all $m \in \{1, 2, 3, 4\}$ and $i \in \mathbb{Z}_2^4$. Using the formalism introduced in [\[DD26, § 3\]](#), we can consider the tesseract (a 4-dimensional hypercube) as codomain graph $\mathcal{G}$ to solve the HIIP. In this graph, vertices $i \in \mathbb{Z}_2^4$ correspond to coordinates $\tilde{\theta}_i^B(0_B)^{-1}$ and edges (i, j) correspond to quotients $H(\theta^A(T_m)^{\odot 2})_i / H(\theta^A(T_m)^{\odot 2})_j$ with $j = i + e_m$, e_m being the vector of $\mathbb{Z}_2^4$ of Hamming weight 1 with 1 at index m . The quotient associated to the edge (i, j) allows to compute $\tilde{\theta}_j^B(0_B)^{-1}$ (vertex j) from $\tilde{\theta}_i^B(0_B)^{-1}$ (vertex i). We call the set $S := \{e_1, e_2, e_3, e_4\}$ of vectors that separate connected vertices the *support* of $\mathcal{G}$. Since $\mathcal{G}$ is connected (all edges are well defined because quotient denominators do not vanish), [\[DD26, Theorem 3.2\]](#) ensures that the HIIP is solvable using the support S , *i.e.* using 4 points.

To reduce the requirement to only 2 points, we apply [Corollary G.3](#). Thanks to the $[\mathbf{i}]$ automorphism, our theta null point exhibits repeating coefficients, which defines an equivalence relation on $\mathbb{Z}_2^4$. Applying this equivalence relation to the tesseract $\mathcal{G}$, we obtain the quotient graph $\mathcal{G}_{[\mathbf{i}]}$ detailed in [Figure 12](#). Solving the HIIP over $\mathcal{G}_{[\mathbf{i}]}$ is therefore sufficient to solve the HIIP over $\mathcal{G}$.

We observe that $\mathcal{G}_{[\mathbf{i}]}$ is connected but non-Hamiltonian²⁴. By selecting the spanning tree highlighted in [Figure 12](#), we observe that this spanning tree exists within the subgraph of $\mathcal{G}_{[\mathbf{i}]}$ whose support is generated using only $j = e_3, e_4$,

²⁴ There is no covering *Hamiltonian* path in $\mathcal{G}_{[\mathbf{i}]}$ going through every vertex only once.

completing the proof. More generally, we see from [Theorem 4.1](#) that any combination of points $(T_1, T_2), (T_3, T_4), (T_1, T_3), (T_2, T_4)$ where one is generated by P while the other is generated by Q would be sufficient. $\square$

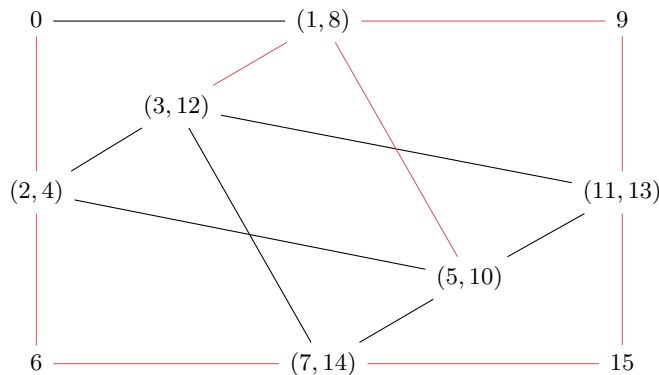


Fig. 12: Codomain graph $\mathcal{G}_{[j]}$ of the generic 2-isogeny between Weil type abelian fourfold. Selected spanning tree is highlighted in red. Here, every index $i \in \mathbb{Z}_2^4$ has been identified to the integer $\sum_{m=0}^3 i_m 2^m$ in binary decomposition.

By [DD26, Theorem 3.4] and by slightly modifying the “rabbit’s interpolation formulae” detailed in [DD26, Appendix C], we get an efficient algorithm to compute the codomain of isogenies between abelian fourfold of Weil type. Unwrapping the recursive formula provides us with Algorithm 4.

Remark E.2. We have seen that the extra automorphism $[\mathbf{i}]$ on our fourfolds speed up the generic dimension four 2-isogeny formulas in level 2 because it allows us to only keep track of only two points in the kernel (which is stable by $[\mathbf{i}]$). We might exploit it further to obtain even faster formulas: rather than working over the usual Kummer variety $A/\pm 1$, we would work with the “extended” Kummer variety $A/(\mathbf{i})$. For instance, we would keep only the 10 level 2 coordinates from [Proposition G.3](#) (out of 16) that are stable under the action of $[\mathbf{i}]$. It is possible to find doubling formulas in these “even” coordinates, which are roughly 1.6 times faster than our current ones using all 16 coordinates. However, although it is possible in theory to compute images of points by our 2-isogenies in this model, we have, as of yet, not found efficient formulae to do it.

F Gluings in MIKE

Building upon [Appendix E](#), we detail the concrete computation of the 4-dimensional chain of MIKE, focussing on its beginning, i.e. its gluing. The beginning of the chain and its efficient computation is a highly technical part of the

Algorithm 4 WeilCodomain

Input: $T_3^{(8)}, T_4^{(8)}$: 8-torsion points above their respective points in the underlying symplectic basis, specifying the 4-dimensional theta structure as specified in [Theorem E.1](#), with $f : A \rightarrow B$ a 2-isogeny such that $\ker(f) = \langle T_1^{(2)}, \dots, T_4^{(2)} \rangle$

Output: $\tilde{\theta}^B(0_B)^{\odot -1}$

1: $P^{(8)}, Q^{(8)} \leftarrow H \circ \mathcal{S}(T_3^{(8)}), H \circ \mathcal{S}(T_4^{(8)})$	18: $\tilde{\theta}^B(0_B)_0^{\odot -1} \leftarrow r_8 \cdot P_4^{(8)}$
2: $r_1 \leftarrow P_{12}^{(8)}$	19: $X \leftarrow P_8^{(8)} \cdot P_5^{(8)}$
3: $r_2 \leftarrow r_1 \cdot P_5^{(8)}$	20: $\tilde{\theta}^B(0_B)_{12}^{\odot -1} \leftarrow X \cdot b_2$
4: $r_3 \leftarrow r_2 \cdot Q_1^{(8)}$	21: $\tilde{\theta}^B(0_B)_5^{\odot -1} \leftarrow r_1 \cdot b_1$
5: $r_4 \leftarrow r_3 \cdot P_9^{(8)}$	22: $\tilde{\theta}^B(0_B)_1^{\odot -1} \leftarrow r_2 \cdot b_2$
6: $r_5 \leftarrow r_4 \cdot P_{11}^{(8)}$	23: $\tilde{\theta}^B(0_B)_9^{\odot -1} \leftarrow r_3 \cdot b_3$
7: $r_6 \leftarrow r_5 \cdot Q_{15}^{(8)}$	24: $\tilde{\theta}^B(0_B)_{11}^{\odot -1} \leftarrow r_4 \cdot b_4$
8: $r_7 \leftarrow r_6 \cdot Q_{14}^{(8)}$	25: $\tilde{\theta}^B(0_B)_{15}^{\odot -1} \leftarrow r_5 \cdot b_5$
9: $r_8 \leftarrow r_7 \cdot P_6^{(8)}$	26: $\tilde{\theta}^B(0_B)_{14}^{\odot -1} \leftarrow r_6 \cdot b_6$
10: $b_8 \leftarrow P_0^{(8)}$	27: $\tilde{\theta}^B(0_B)_6^{\odot -1} \leftarrow r_7 \cdot b_7$
11: $b_7 \leftarrow b_8 \cdot P_2^{(8)}$	28: $\tilde{\theta}^B(0_B)_4^{\odot -1} \leftarrow r_8 \cdot b_8$
12: $b_6 \leftarrow b_7 \cdot Q_6^{(8)}$	29: $\tilde{\theta}^B(0_B)_3^{\odot -1} \leftarrow \tilde{\theta}^B(0_B)_{12}^{\odot -1}$
13: $b_5 \leftarrow b_6 \cdot Q_7^{(8)}$	30: $\tilde{\theta}^B(0_B)_{10}^{\odot -1} \leftarrow \tilde{\theta}^B(0_B)_5^{\odot -1}$
14: $b_4 \leftarrow b_5 \cdot P_{15}^{(8)}$	31: $\tilde{\theta}^B(0_B)_8^{\odot -1} \leftarrow \tilde{\theta}^B(0_B)_1^{\odot -1}$
15: $b_3 \leftarrow b_4 \cdot P_{13}^{(8)}$	32: $\tilde{\theta}^B(0_B)_{13}^{\odot -1} \leftarrow \tilde{\theta}^B(0_B)_{11}^{\odot -1}$
16: $b_2 \leftarrow b_3 \cdot Q_9^{(8)}$	33: $\tilde{\theta}^B(0_B)_7^{\odot -1} \leftarrow \tilde{\theta}^B(0_B)_{14}^{\odot -1}$
17: $b_1 \leftarrow b_2 \cdot P_1^{(8)}$	34: $\tilde{\theta}^B(0_B)_2^{\odot -1} \leftarrow \tilde{\theta}^B(0_B)_4^{\odot -1}$
	35: return $\tilde{\theta}^B(0_B)^{\odot -1}$ ▷ Total 25M

MIKE protocol. As a reminder, our ultimate goal is to compute the 4-dimensional isogeny corresponding to the module action of an left $\mathcal{O}_0$ -quaternionic ideal I of norm 2^e over a Scholten construction $W'(E)$. That is, we want to compute the isogeny

$$F' : W'(E)^2 \longrightarrow W'(E)^2 / W'(E)^2[I],$$

which requires us to efficiently compute its kernel $W'(E)^2[I_1]$ and analyze it in order to derive a fast and constant-time implementation of F' . To achieve the latter point, we will instead compute F , a closely related isogeny with the same codomain but a more practical domain, as it is the product Weil restriction of E (i.e. $(E \times E^\sigma)^2$) rather than the product of its Scholten construction (i.e. $W'(E)^2$). Our primary object of study, the first 2-isogenies of the F isogeny, is denoted F_{glue} . As we will show in [Appendix F.2](#) that F_{glue} decomposes as detailed in [Figure 13](#).

$$\overbrace{(E \times E^\sigma)^2 \xrightarrow{F_1 := \text{Diag}(\Gamma, \Gamma)} W'(E)^2 \xrightarrow{F_2 := \text{Diag}(\phi_U, \phi_V)} S_U \times S_V \xrightarrow{F_3} X}^{F_{\text{glue}}} \longrightarrow \dots$$

Fig. 13: Recapitulative diagram of MIKE’s 4-dimensional gluing isogeny F_{glue} , decomposed into 3 parts corresponding to F_1 , F_2 and F_3 , all 2-isogenies.

Notations Throughout this section, E and E^σ denote supersingular curves defined over $\mathbb{F}_{p^2}$, while $W'(E)$, S_U , and S_V are abelian surfaces defined over $\mathbb{F}_p$ ²⁵, and X is an abelian fourfold of Weil type also defined over $\mathbb{F}_p$. The set $\{P, Q\}$ is a (naturally symplectic) basis of $E[2^f]$, while $\{U_1, U_2, V_1, V_2\}$ is a symplectic basis of $W'(E)[2^{f-1}]$. We usually denote a symplectic basis over an Abelian fourfold as $\{S_1, \dots, S_4, T_1, \dots, T_4\}$. The 2-isogeny $\Gamma : E \times E^\sigma \rightarrow W'(E)$ is called the Scholten gluing.

Remark F.1. We will also assume that our public key E is not defined over $\mathbb{F}_p$. The reason is because in that case $W'(E)$ is a product: it is isomorphic to $E \times E'$ where E' is the quadratic twist of E over $\mathbb{F}_p$. This mean that we would need dedicated gluing formulas when we compute the dimension 4 gluing $W'(E)^2 \rightarrow A_1$. Although it would be possible to implement this case, since it only occurs with cryptographically small probability $\approx 1/\sqrt{p}$, we simply ignore it (or more precisely, the implementation outputs an invalid shared key). We note that this case correspond to “weak public keys”, whose associated rank 2 module is of the form $\mathfrak{a} \oplus \bar{\mathfrak{a}}$ (with the product polarisation), and so is susceptible to Kuperberg’s subexponential quantum algorithm.

²⁵ Meaning that their respective theta null-points are defined over $\mathbb{F}_p$.

Structure The remainder of this appendix is organised as follows. In [Appendix F.1](#), we derive a closed form for computing a symplectic basis of the kernel of F . We then prove the structure illustrated in [Figure 13](#) in [Appendix F.2](#). In [Appendix F.3](#), we detail the fast and constant-time computation of the Scholten gluing Γ and thus of F_1 . Next, [Appendix F.4](#) details all the necessary changes of theta coordinates required to efficiently compute theta structures over $W'(E)$, S_U and S_V compatible with isogeny F_2 . Then, in [Appendix F.5](#), we explain how to efficiently glue into an Abelian fourfold, leveraging the extra symmetries induced by the Weil type to speed up and simplify the formulas. Finally, we conclude [Appendix F.6](#), we assemble all previous results to provide the pseudocode for computing F_{glue} in MIKE.

F.1 Computing the kernel of 4-dimensional isogenies in MIKE

In this subsection, we build toward a proof of [Theorem 4.1](#), which is done in [Theorem F.1](#). Following [Example 2.2](#), given $I = \mathcal{O}_0 2^e + \mathcal{O}_0 \gamma$ with $\gamma = \alpha + i\beta$, we then have that for a

$$\ker(F') = A^2[N] \cap \ker(\Phi) \text{ with } \Phi = \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \in \text{End}(A^2)$$

We can therefore compute an adequate symplectic basis of $\ker(F)$ as follows.

Lemma F.1. *Assume that $\text{nrd}(\alpha)$ and $\text{nrd}(\beta)$ are coprime and odd. Let (U_1, U_2, V_1, V_2) be a ζ -symplectic basis of $A[2^{e+1}]$. Let us denote by λ and μ modular inverses of $\text{nrd}(\alpha)$ and $\text{nrd}(\alpha) \text{nrd}(\beta)$ modulo 2^{e+1} . Then, $\mathcal{B} := (S_1, \dots, S_4, T_1, \dots, T_4)$ given by:*

$$\begin{aligned} S_i &:= (-[\lambda]V_i, 0), & S_{i+2} &:= (0, [\mu]\alpha\bar{\beta}(U_i)) \\ T_i &:= ([\text{nrd}(\alpha)]U_i, \alpha\bar{\beta}(U_i)), & T_{i+2} &:= ([-\text{nrd}(\beta)]V_i, \alpha\bar{\beta}(V_i)), \end{aligned}$$

for $i \in \{1, 2\}$, is a ζ -symplectic basis of $A^2[2^{e+1}]$ adapted to F , i.e. such that $\ker(F) = [2]\langle T_1, \dots, T_4 \rangle$.

Proof. Since (U_1, U_2, V_1, V_2) is a ζ -symplectic basis of $A[2^{e+1}]$, the construction of $\mathcal{B}$ and the standard properties of the 2^{e+1} -th Weil-pairing, imply:

$$e_{2^{e+2}}(S_i, S_j) = e_{2^{e+1}}(T_i, T_j) = 1 \quad \text{and} \quad e_{2^{e+1}}(S_i, T_j) = \zeta^{\delta_{i,j}},$$

for all $1 \leq i, j \leq 4$, which proves that $\mathcal{B}$ is indeed a ζ -symplectic basis of $A_2^2[2^{e+1}]$.

We now prove that $\mathcal{B}$ is adapted to F_1 . Since $\mathcal{B}$ is a basis, it suffices to prove that $[2]T_1, \dots, [2]T_4 \in \ker(F) = A^2[2^{e+1}] \cap \ker(\Phi)$. For $i \in \{1, 2\}$, we have:

$$\begin{aligned} \Phi([2]T_i) &= \Phi([2\text{nrd}(\alpha)]U_i, [2][\alpha\bar{\beta}](U_i)) \\ &= ([2(\text{nrd}(\alpha) + \text{nrd}(\beta))][\alpha](U_i), -[2\text{nrd}(\alpha)][\bar{\beta}](U_i) + [2\text{nrd}(\alpha)][\bar{\beta}](U_i)) \\ &= ([2\text{nrd}(\gamma)][\alpha](U_i), 0) = (0, 0) \quad \text{and} \\ \Phi([2]T_{i+2}) &= \Phi([2(\text{nrd}(\alpha) - \text{nrd}(\gamma))]V_i, [2][\alpha\bar{\beta}](V_i)) = \Phi([2\text{nrd}(\alpha)]V_i, [2][\alpha\bar{\beta}](V_i)) \\ &= (0, 0) \quad (\text{by similar computations}), \end{aligned}$$

where we used the fact that $\text{nrd}(\gamma) = \text{nrd}(\alpha) + \text{nrd}(\beta) \equiv 0 \pmod{2^{e+1}}$. This completes the proof. $\square$

In order to compute $\ker(F)$ efficiently in MIKE we must establish a method for obtaining a symplectic basis over A (which is the Scholten construction $W'(E)$) and determine efficient representations of α, β , that satisfy the conditions of [Lemma F.1](#). Regarding the former, a symplectic basis can be readily constructed via the Scholten construction and the gluing $(2, 2)$ -isogeny $\Gamma : W(E) \rightarrow W'(E)$.

Proposition F.1. *Let (P, Q) be a basis of $E[2^f]$ and let $\zeta := e_{2^f}(P, Q)$. The tuple (U_1, U_2, V_1, V_2) defined by*

$$U_1 := \Gamma(P, \sigma(P)), \quad U_2 := \Gamma(Q, \sigma(Q)), \quad V_1 := \Gamma(Q, -\sigma(Q)), \quad V_2 := \Gamma(-P, \sigma(P))$$

is a ζ^2 -symplectic basis of $W'(E)[2^{f-1}]$. Furthermore, U_i and V_i are eigenvectors of the Frobenius endomorphism π'_p on $W'(E)$ with eigenvalues 1 and -1 , respectively, with $\pi'_p = (\Gamma \circ \pi_p \circ \tilde{\Gamma})/2$ as Γ is oriented.

Proof. Following the construction in [Appendix C.2](#), the tuple

$$(P, \sigma(P)), \quad (Q, \sigma(Q)), \quad (Q, -\sigma(Q)), \quad (-P, \sigma(P))$$

forms an $\mathbb{F}_p$ -rational ζ -symplectic basis for $W(E)[2^f]$ ²⁶. Since all points in $\ker(\Gamma) = \{(T, \sigma(T)) : T \in E[2]\}$ are $\mathbb{F}_p$ -rational, the image of this basis under Γ is well-defined, $\mathbb{F}_p$ -rational, and symplectic. $\square$

We now focus on expressing the endomorphism γ as a function of the integer x_I , such that $E'_0[I] = \langle P + [x_I]Q \rangle$ with P, Q the R -oriented basis of $E'_0[2^{e+2}]$, as is happening in MIKE [Section 4](#).

Lemma F.2. *Assume that $e \leq f - 1$ and x is odd and let $\omega := (1 + \sqrt{-p})/2$. Let $I := 2^e \mathcal{O}_0 + \mathcal{O}_0 \gamma$ with $\gamma := (1 + \omega \mathbf{i})(\omega - 1)(1 - x_I \mathbf{i})$. Then:*

1. $E'_0[I] = \langle P + [x_I]Q \rangle$ or, conjointly, I is the kernel ideal of the isogeny ϕ with $\ker(\phi) = \langle P + [x_I]Q \rangle$.
2. We may write $\gamma = \alpha + \beta \mathbf{i}$ with:

$$\alpha := x_I \frac{p+1}{4} - 1 - (x_I - 1)\omega \quad \text{and} \quad \beta := \frac{p+1}{4} + x_I - (x_I + 1)\omega.$$

Proof. Let $K_1 := P_0 + [x_I]Q_0$. Then, we have:

$$\begin{aligned} [\gamma](K'_1) &= (1 + [\omega \mathbf{i}])([\omega] - 1)(P_0 + [x_I]Q_0 - [x_I][i](P_0) - [x_I^2][\mathbf{i}](Q_0)) \\ &= (1 + [\omega \mathbf{i}])([\omega] - 1)(P_0 + [x_I]Q_0 - [x_I]Q_0 - [x_I^2][\mathbf{i}^2](P_0)) \\ &= (1 + [\omega \mathbf{i}])([\omega] - 1)(P_0 + [x_I^2]P_0) \\ &= \left[\frac{1 + x_I^2}{2} \right] (1 + [\omega \mathbf{i}])([\pi_p] - 1)(P_0) = 0. \end{aligned}$$

²⁶ Note that this is a slight abuse of notation, as following [Appendix C.1](#), such basis cannot exist. Instead, this symplectic basis exists in $W(E) \cup W(E)^\top$. The same is true for basis U_1, U_2, V_1, V_2 defined over $W'(E) \cup W'(E)^\top$.

It follows that $[\gamma](K'_1) = 0$, hence $\gamma \in I$. By construction, γ is not divisible by any integer, hence γ is cyclic, i.e. $\ker(\gamma)$ is generated by a single point $R \in E'_0$. We may therefore write $K_1 = [\lambda 2^m]R$ for some $\lambda \in \mathbb{Z}$ odd and $m \in \mathbb{N}$, with the order of R being a multiple of 2^{e+m} . Now, if $S \in E'_0[2^e] \cap \ker(\gamma)$, we may write $S = [\mu]R$ with $\mu \in \mathbb{Z}$ and $[2^e]S = 0$, so that $[\mu 2^e]R = 0$ and $2^m \mid \mu$. We may then write $\mu = 2^m \mu'$ so that $[\lambda]S = [\mu' \lambda 2^m]R = [\mu']K_1$ and λ is odd so invertible modulo 2^e and $S \in \langle K_1 \rangle$. We conclude that:

$$E'_0[2^e] \cap \ker(\gamma) = \langle K_1 \rangle = \ker(\phi) = E'_0[I],$$

and that finally, $I := 2^e \mathcal{O}_0 + \mathcal{O}_0 \gamma$ by the Deuring correspondence. Furthermore,

$$\begin{aligned} \gamma &= (1 + \omega \mathbf{i})(\omega - 1)(1 - x_I \mathbf{i}) = (\omega + \omega \mathbf{i} \omega - 1 - \omega \mathbf{i})(1 - x_I \mathbf{i}) \\ &= (\omega + \omega \bar{\omega} \mathbf{i} - 1 - \omega \mathbf{i})(1 - x_I \mathbf{i}) = \left(-1 + \omega + \left(\frac{p+1}{4} - \omega \right) \mathbf{i} \right) (1 - x_I \mathbf{i}) \\ &= -1 + \omega + \left(\frac{p+1}{4} - \omega \right) \mathbf{i} - x_I (-1 + \omega) \mathbf{i} - x_I \left(\frac{p+1}{4} - \omega \right) \mathbf{i}^2 \\ &= x_I \frac{p+1}{4} - 1 - (x_I - 1)\omega + \left(\frac{p+1}{4} + x_I - (x_I + 1)\omega \right) \mathbf{i} \end{aligned}$$

so that:

$$\alpha := x_I \frac{p+1}{4} - 1 - (x_I - 1)\omega \quad \text{and} \quad \beta := \frac{p+1}{4} + x_I - (x_I + 1)\omega.$$

□

Corollary F.1. *We use the notation of [Lemma F.2](#) and set $\alpha \bar{\beta} = a + b\omega$ with $a, b \in \mathbb{Z}$. Then:*

$$\text{nr}(\alpha) \equiv x_I \pmod{2^{f-2}}, \quad \text{nr}(\beta) \equiv -x_I \pmod{2^{f-2}}$$

$$a \equiv 1 \pmod{2^{f-2}}, b \equiv -(1 + x_I^2) \pmod{2^{f-2}}$$

Proof. Using $\alpha := x_I(p+1)/4 - 1 - (x_I - 1)\omega$, we see that

$$\begin{aligned} \text{nr}(\alpha) &= \left(x_I \frac{p+1}{4} - 1 \right)^2 + (x_I - 1)^2 \frac{p+1}{4} - (x_I - 1) \left(x_I \frac{p+1}{4} - 1 \right) \\ &= (x_I c 2^{f-2} - 1)^2 + (x_I - 1)^2 c 2^{f-2} - (x_I - 1)(x_I c 2^{f-2} - 1) \\ &\equiv 1 + x_I - 1 \pmod{2^{f-2}} \equiv x_I \pmod{2^{f-2}} \end{aligned} \tag{18}$$

From $\text{nrd}(\alpha) + \text{nrd}(\beta) = \text{nrd}(\gamma) = 0 \pmod{2^{f-2}}$, we get our result for $\text{nrd}(\beta) \pmod{2^{f-2}}$. Similarly, we see that

$$\begin{aligned} \alpha\bar{\beta} &= \left(x_I \frac{p+1}{4} - 1 - (x_I - 1)\omega\right) \left(\frac{p+1}{4} + x_I - (x_I + 1)\bar{\omega}\right) \\ &= \left(x_I \frac{p+1}{4} - 1 - (x_I - 1)\omega\right) \left(\frac{p+1}{4} - 1 + (x_I + 1)\omega\right) \\ &= \left(x_I \frac{p+1}{4} - 1\right) \frac{p-3}{4} + \left(x_I \frac{p+1}{4} - 1\right) (x_I + 1)\omega \\ &\quad - (x_I - 1) \frac{p-3}{4} \omega - (x_I - 1)(x_I + 1)\omega^2. \end{aligned}$$

Since $\omega^2 = \omega - (p+1)/4$, it follows that:

$$a = \left(x_I \frac{p+1}{4} - 1\right) \frac{p-3}{4} + (x_I^2 - 1) \frac{p+1}{4}, \quad (19)$$

$$b = \left(x_I \frac{p+1}{4} - 1\right) (x_I + 1) - (x_I - 1) \frac{p-3}{4} - x_I^2 + 1. \quad (20)$$

With x_I odd and $p = c2^f - 1$, we get that $a \equiv 1 \pmod{2^{f-2}}$ and that $b \equiv -(x_I + 1) + (x_I - 1) - x_I^2 + 1 \equiv -(1 + x_I^2) \pmod{2^{f-2}}$ which concludes the proof. $\square$

We thus rewrite the symplectic basis of [Lemma F.1](#) as follows.

Lemma F.3. *Using the notation from [Proposition F.1](#) and [Lemma F.2](#), we can rewrite the symplectic basis of $W'(E)^{2[2^{e+1}]}$ adapted to F' and defined in [Lemma F.1](#) as follows:*

$$\begin{aligned} S_1 &= (-[\lambda]V_1, 0), & S_2 &= (-[\lambda]V_2, 0), \\ S_3 &= (0, -U_1), & S_4 &= (0, -U_2), \\ T_1 &= ([x_I]U_1, [x_I^2]U_1), & T_2 &= ([x_I]U_2, [x_I^2]U_2), \\ T_3 &= ([x_I]V_1, V_1), & T_4 &= ([x_I]V_2, V_2) \end{aligned}$$

with λ the modular inverse of x_I modulo 2^{e+1} .

Proof. By [Proposition F.1](#), seeing $\varepsilon(\omega) = (1 + \pi_p')/2 = \Gamma \circ (1 + \pi_p)/4 \circ \tilde{\Gamma}$ we have that

$$\begin{aligned} [\omega](U_1) &= \frac{1}{4} \Gamma \circ (\pi_p + 1) \circ \tilde{\Gamma}(U_1) = \frac{1}{2} \Gamma \circ (\pi_p + 1)(P, \sigma(P)) \\ &= \Gamma \circ (\pi_p + 1)(P', \sigma(P')) \quad (\text{with } [2]P' = P) \\ &= \Gamma(P' + \sigma^2(P'), [2]\sigma(P')) = \Gamma([(1-p)/2]P, \sigma(P)) \\ &= \Gamma(P, \sigma(P)) - \Gamma([(p+1)/2]P, 0) = U_1 + T_P, \end{aligned}$$

with $T_P = \Gamma([(p+1)/2]P, 0) = \Gamma([2^{f-1}]P, 0) = -T_P$ because $(p+1)/2^f \equiv 1 \pmod{2}$. Similarly, we obtain that $[\omega](U_2) = U_2 - T_Q$ and

$$\begin{aligned} [\omega](V_1) &= \Gamma \circ (\pi_p + 1)(Q', -\sigma(Q')) \quad (\text{with } [2]Q' = Q) \\ &= \Gamma(Q' - \sigma^2(Q'), -\sigma(Q') + \sigma(Q')) \\ &= \Gamma([1+p]Q', 0) = \Gamma([(p+1)/2]Q, 0) = T_Q, \end{aligned}$$

and that $[\omega](V_2) = -T_P = T_P$.

To conclude, it suffices to see that, following [Corollary F.1](#), we have

$$\begin{aligned} [\alpha\bar{\beta}](U_i) &= a + b[\omega](U_i) = [a + b]U_i, \\ [\alpha\bar{\beta}](V_i) &= a + [\omega](V_i) = [a]U_i, \end{aligned}$$

where we used the fact that $b = -(1 + x_I)^2 \equiv 0 \pmod{2}$. The result follows. $\square$

By examining the basis defined in [Lemma F.3](#), we make two key observations:

1. Following the definitions of U_i and V_i in [Proposition F.1](#), this basis is expressed as the image under $\text{Diag}(\Gamma, \Gamma)$ of a symplectic basis of $W(E)^2[2^{e+2}]$.
2. Since x_I is odd, it follows that $\ker(F)[2] = \{(X, X) : X \in W'(E)[2]\}$. This implies that the first 2-isogeny of F is the differential addition isogeny $\Delta \in \text{End}(W'(E)^2)$, defined by $\Delta(P, Q) = (P + Q, P - Q)$.

These observations allow us to “pullback” the isogeny F' to the Weil restriction. Because isogenies preserve group structure, Δ commutes with product isogenies; specifically, $\text{Diag}(\phi, \phi) \circ \Delta = \Delta \circ \text{Diag}(\phi, \phi)$. leveraging this property, we define the four-dimensional isogeny F' as the unique isogeny satisfying $F' \circ \text{Diag}(\Gamma, \Gamma) = F \circ \Delta$. By its definition, it is clear that both F and F' share the same codomain. We can now prove [Theorem 4.1](#), that we restate in a more compressed form bellow.

Theorem F.1. *Let (P, Q) be a basis of $E[2^{e+2}]$. Let I be the $\mathcal{O}_0$ -left kernel ideal associated to $\phi : E'_0 \rightarrow E_A$, an isogeny of degree 2^e with $\ker(\phi) = [4]\langle P_0 + [x_I]Q_0 \rangle$ and x_I odd. Then, writing $\chi_I := x_I^{-1} \pmod{2^{e+2}}$, we have that*

$$\begin{aligned} S_1 &= \left(-[\chi_I]Q, [\chi_I]\sigma(Q), -[\chi_I]Q, [\chi_I]\sigma(Q) \right), \\ S_2 &= \left([\chi_I]P, -[\chi_I]\sigma(P), [\chi_I]P, -[\chi_I]\sigma(P) \right), \\ S_3 &= (P, \sigma(P), -P, -\sigma(P)), \\ S_4 &= (Q, \sigma(Q), -Q, -\sigma(Q)), \\ T_1 &= \left([x_I(1 - x_I)/2]P, [x_I(1 - x_I)/2]\sigma(P), [x_I(1 + x_I)/2]P, [x_I(1 + x_I)/2]\sigma(P) \right), \\ T_2 &= \left([x_I(1 - x_I)/2]Q, [x_I(1 - x_I)/2]\sigma(Q), [x_I(1 + x_I)/2]Q, [x_I(1 + x_I)/2]\sigma(Q) \right), \\ T_3 &= \left([(x_I + 1)/2]Q, -[(x_I + 1)/2]\sigma(Q), [(x_I - 1)/2]Q, -[(x_I - 1)/2]\sigma(Q) \right), \\ T_4 &= \left(-[(x_I + 1)/2]P, [(x_I + 1)/2]\sigma(P), -[(x_I - 1)/2]P, +[(x_I - 1)/2]\sigma(P) \right), \end{aligned}$$

is a symplectic basis of $W(E)^2[2^{e+2}]$ compatible with $\ker(F_A)$.

Proof. Using the basis compatible with F_A of [Lemma F.3](#), together with the basis derived in [Proposition F.1](#) we have that $\mathcal{B}$, the basis of $W(E)^2[2^{e+2}]$ defined as

$$\begin{aligned} S_1 &= \left(-[\chi_I]Q, [\chi_I]\sigma(Q), 0, 0 \right), & S_2 &= \left([\chi_I]P, -[\chi_I]\sigma(P), 0, 0 \right), \\ S_3 &= (0, 0, -P, -\sigma(P)), & S_4 &= (0, 0, -Q, -\sigma(Q)), \\ T_1 &= \left([x_I]P, [x_I]\sigma(P), [x_I^2]P, [x_I^2]\sigma(P) \right), & T_2 &= \left([x_I]Q, [x_I]\sigma(Q), [x_I^2]Q, [x_I^2]\sigma(Q) \right), \\ T_3 &= \left([x_I]Q, -[x_I]\sigma(Q), Q, -\sigma(Q) \right), & T_4 &= \left(-[x_I]P, [x_I]\sigma(P), -P, +\sigma(P) \right), \end{aligned}$$

is compatible with $F \circ \Delta$. As Δ is self-dual, we have that $\Delta(\mathcal{B})/2$ is a basis of $W(E)^2[2^{e+2}]$ compatible with F . The rest follow. $\square$

F.2 Structure of the gluing isogenies

Given the basis from [Theorem 4.1](#), we can compute the 4-dimensional isogeny F using the formulae detailed in [Appendix E.2](#). However, the initial steps of the chain require a distinct approach as they are defined over products of principally polarised abelian varieties of dimension $g \leq 3$ (e.g., products of abelian surfaces). Given a 2^e -isogeny Φ whose domain is a product of abelian varieties, we define Φ_{glue} as the *gluing isogeny*. This is the smallest isogeny that factors Φ (i.e., $\Phi = \Phi' \circ \Phi_{\text{glue}}$) such that its codomain is not a product of abelian varieties. To properly characterise Φ_{glue} , we first define isogenies between products.

Definition F.1. Let ℓ be a prime. An ℓ -isogeny $\Phi : A_1 \times A_2 \rightarrow B_1 \times B_2$ is diagonal if there exist two ℓ -isogenies $\phi_i : A_i \rightarrow B_i$ such that $\Phi(P_1, P_2) = (\phi_1(P_1), \phi_2(P_2))$. Its kernel is generated by:

$$\ker(\Phi) = \left\langle (\ker(\phi_1), 0), (0, \ker(\phi_2)) \right\rangle$$

We denote this as $\Phi := \text{Diag}(\phi_1, \phi_2)$.

We now characterise F_{glue} the gluing isogenies appearing in the MIKE protocol.

Theorem F.2. Let F be the 2^e -isogeny whose kernel is defined in [Theorem 4.1](#), with $x_I \equiv 3 \pmod{8}$. Then its gluing isogeny F_{glue} is an isogeny of degree 8. Writing $F_{\text{glue}} = F_3 \circ F_2 \circ F_1$, where each F_i is a 2-isogeny, its structure is as follows:

- (i) F_1 is the diagonal isogeny $\text{Diag}(\Gamma, \Gamma) : (E \times E^\sigma)^2 \rightarrow W'(E)^2$.
- (ii) F_2 is a diagonal isogeny: $\text{Diag}(\phi_U, \phi_V) : W'(E)^2 \rightarrow S_U \times S_V$. with $\ker(\phi_U) := \Gamma(W(E)(\mathbb{F}_p)[2])$ and $\ker(\phi_V) := \Gamma(W(E)^\top(\mathbb{F}_p)[2])$.
- (iii) $F_3 : S_U \times S_V \rightarrow X$, where X is a 4-dimensional abelian fourfold.

Proof. To see the above results, we have a closer look at the possible values of $(x_I \pm 1)/2$ and $x_I(1 \pm x_I)/2$. The crux of the proof is the fact that the 2-valuation of $x_I \pm 1$ is at most 2.

- (i) The kernel $\ker(F_1) = \ker(F)[2^{f-3}]$ is generated by the basis:

$$\begin{aligned} [2^{f-1}]T_1 &= ([2^{f-1}]P, [2^{f-1}]\sigma(P), 0, 0), \\ [2^{f-1}]T_2 &= ([2^{f-1}]Q, [2^{f-1}]\sigma(Q), 0, 0), \\ [2^{f-1}]T_3 &= (0, 0, [2^{f-1}]Q, [2^{f-1}]\sigma(Q)), \\ [2^{f-1}]T_4 &= (0, 0, [2^{f-1}]P, [2^{f-1}]\sigma(P)). \end{aligned}$$

By [Definition F.1](#), $F_1 = \text{Diag}(\Gamma, \Gamma)$.

- (ii) For F_2 , $\ker(F_2) = F_1(\ker(F)[2^{f-4}])$. Using the basis on Scholten's construction defined in [Proposition F.1](#), the generators are:

$$\begin{aligned} [2^{f-2}]F_1(T_1) &= [2^{f-2}]([x_I(1-x_I)/2]U_1, [x_I(1+x_I)/2]U_1) = ([2^{f-2}]U_1, 0), \\ [2^{f-2}]F_1(T_2) &= [2^{f-2}]([x_I(1-x_I)/2]U_2, [x_I(1+x_I)/2]U_2) = ([2^{f-2}]U_2, 0), \\ [2^{f-2}]F_1(T_3) &= [2^{f-2}]([1+x_I]/2]V_1, [(1-x_I)/2]V_1) = (0, [2^{f-2}]V_1), \\ [2^{f-2}]F_1(T_4) &= [2^{f-2}]([1+x_I]/2]V_2, [(1-x_I)/2]V_2) = (0, [2^{f-2}]V_2), \end{aligned}$$

This implies $F_2 = \text{Diag}(\phi_U, \phi_V)$, as U_i, V_i are eigenvectors of Frobenius with eigenvalues 1, -1.

- (iii) Finally, as $\ker(F_3) = \text{Diag}(\phi_U \circ \Gamma, \phi_V \circ \Gamma) \ker(F)[2^{f-5}]$, its basis is generated by

$$\begin{aligned} [2^{f-3}]F_2 \circ F_1(T_1) &= [2^{f-3}](\phi_U([x_I(1-x_I)/2]U_1), \phi_V([x_I(1+x_I)/2]U_1)), \\ [2^{f-3}]F_2 \circ F_1(T_2) &= [2^{f-3}](\phi_U([x_I(1-x_I)/2]U_2), \phi_V([x_I(1+x_I)/2]U_2)), \\ [2^{f-3}]F_2 \circ F_1(T_3) &= [2^{f-3}](\phi_U([(x_I+1)/2]V_1), \phi_V([(x_I-1)/2]V_1)), \\ [2^{f-3}]F_2 \circ F_1(T_4) &= [2^{f-3}](\phi_U([(x_I+1)/2]V_2), \phi_V([(x_I-1)/2]V_2)) \end{aligned}$$

where no component is zero. Thus, F_3 is not a diagonal isogeny, making its codomain X irreducible. $\square$

Though we could compute the first two isogenies of the chain directly as 4-dimensional isogenies, it is more practical and efficient to compute them as tuples of 2 dimensional isogenies, consisting in Γ , ϕ_U and ϕ_V . In the following subsections, we details how to efficiently compute each of them.

F.3 Fast gluing into the Scholten construction

We first need to compute efficiently F_1 , the Scholten gluing. i.e. the $(2, 2)$ isogeny $\Gamma : W(E) \rightarrow W'(E)$ between Weil restriction and Scholten construction more

efficiently. For this purpose, we specialised the fast 2-dimensional formulae introduced in [Dup25]. We assume that we are looking at the Weil restriction $W(E)$ as the product $E \times E^\sigma$. In this case, we have that $\ker(\Gamma) = \{(X, \sigma(X)) \mid X \in E[2]\}$. As detailed in [Dup25, §2.4], we can, using 4-torsion points above $\ker(\Gamma)$, compute a compatible symplectic basis of $(E \times E^\sigma)[4]$ and therefore a theta structure compatible with Γ . Using the additional symmetries of the Weil restriction, this theta structure can be computed very efficiently. Throughout this subsection, for simplicity, we denote $\sigma(x) = x^p$ as $\bar{x}$ for any $x \in \mathbb{F}_{p^2}$.²⁷

Lemma F.4. *Let (P, Q) be a basis of $E[2^f]$ with E a Montgomery curve. Let $[2^{f-2}]P = (\alpha : * : \beta)$ and $[2^{f-2}]Q = (\pm 1 : * : 1)$. Then, the basis*

$$[2^{f-2}](0, \sigma(Q)), [2^{f-2}](P, 0), [2^{f-2}](P, \sigma(P)), [2^{f-2}](Q, \sigma(Q))$$

is a symplectic basis of $W(E)[4]$ that induces a theta structure compatible $\theta^{W(E)}$ with Γ . Let $(X_1, \pm X_2) \in E \times E^\sigma$ with $X_i = (x_i : * : z_i)$. The theta coordinates of this theta structure are:

$$\theta^{W(E)}(X_1, \pm X_2) := \begin{pmatrix} m_0 & -m_1 & -m_1 & m_0 \\ -m_1 & m_0 & m_0 & -m_1 \\ m_2 & \mathbf{i}m_3 & -\mathbf{i}m_3 & -m_2 \\ \mathbf{i}m_3 & m_2 & -m_2 & -\mathbf{i}m_3 \end{pmatrix} \cdot \begin{pmatrix} x_1 x_2 \\ x_1 z_2 \\ z_1 x_2 \\ z_1 z_2 \end{pmatrix}$$

$$m_0 := \alpha \bar{\alpha} + \beta \bar{\beta}, \quad m_2 := \beta \bar{\beta} - \alpha \bar{\alpha}, \quad 2\alpha \bar{\beta} = m_1 + \mathbf{i}m_3$$

with $m_i \in \mathbb{F}_p$.

Proof. Seeing that the basis is symplectic and compatible with Γ is straightforward and follows [Dup25, §2.4]. The computation of the change of coordinates matrix is a natural consequence of the symmetric elements (as defined in [Dup25, §3]). Indeed, from the form of the kernel of Γ , we fall into case 3 or 4 of [Dup25, Algorithm 1], meaning that

$$\mathfrak{g}_P = \frac{1}{2\alpha\beta} \begin{pmatrix} \alpha^2 + \beta^2 & -2\alpha\beta \\ 2\alpha\beta & -(\alpha^2 + \beta^2) \end{pmatrix}, \quad \mathfrak{g}_Q = \frac{1}{2\alpha\beta} \begin{pmatrix} 0 & \pm 2\alpha\beta \\ \pm 2\alpha\beta & 0 \end{pmatrix}, \quad \mathfrak{g}_{P+Q} = \mathfrak{g}_P \cdot \mathfrak{g}_Q$$

Using the fact that $\mathfrak{g}_{\sigma(X)} = \overline{\mathfrak{g}_X}$ and the formulae for the change of theta coordinates matrix detailed in [Dup25, §3], a simple but tedious computation gives us the desired matrix. $\square$

Note that $m_0^2 - m_3^2 = m_1^2 + m_2^2$, giving computational reassurance that we are working with a gluing. We can then further specialise the Superglue formula [Dup25, Theorem 3]. To do so, we will reuse the notion of *barycentric coordinates*, as defined in [Dup25, Definition 6] and [DD26, Definition 4.2]. This means we represent a tuple $P \pm Q$ as a point $(u : v : w) \in \mathbb{P}^2$, so that

$$x_\oplus := u - v, \quad x_\ominus := u + v, \quad z_\oplus = z_\ominus = w,$$

²⁷ This choice is natural, as the Frobenius map over $\mathbb{F}_{p^2}$ acts like complex conjugation over $\mathbb{C}$.

where $(x_{\oplus} : z_{\oplus})$ and $(x_{\ominus} : z_{\ominus})$ are the Kummer coordinates of $P + Q$ and $P - Q$, respectively.

Such coordinates can be efficiently computed using [Dup25, Algorithm 2]. Note that, following the nomenclature of [Dup25, Appendix A], our kernel basis is always in position 11, leading to a Superglue formula specialised to the Scholten construction, derived from [Dup25, Theorem 3].

Theorem F.3. *Let $\theta^{W(E)} : E \times E^{\sigma} \rightarrow \mathbb{P}^3$ be the theta structure defined in Lemma F.4. Let $(X, \pm\sigma(X))$ and $(T, \sigma(T))$ be points of $E \times E^{\sigma}$ with $X \neq \pm T$. Let $(u : v : w)$ be the barycentric coordinates of $X \pm T$. Then, we have that*

$$H \left(\theta^{W(E)}(X + T, \sigma(\pm X + T)) \odot \theta^{W(E)}(X - T, \sigma(\pm X - T)) \right) :=$$

$$\begin{pmatrix} A(u^2 - v^2 + w^2)(\overline{u^2 - v^2 + w^2}) + 4Cu\bar{u}w\bar{w} - 4DU - 4EV \\ B(u^2 - v^2 - w^2)(\overline{u^2 - v^2 - w^2}) \\ C(u^2 - v^2 + w^2)(\overline{u^2 - v^2 + w^2}) + 4Au\bar{u}w\bar{w} - 4DU + 4EV \\ \pm 4Bv\bar{v}w\bar{w} \end{pmatrix} \quad (21)$$

with all $A, B, C, D, E, U, V \in \mathbb{F}_p$ such that $(u^2 - v^2 + w^2)(\overline{u^2 - v^2 + w^2}) = U + \mathbf{i}V$ with

$$A := m_1^2 + m_2^2, \quad B := m_0^2 - m_1^2, \quad C := m_0^2 - m_2^2$$

$$D := m_0m_1, \quad E := m_2m_3$$

implying that $\tilde{\theta}^{W'(E)}$, the image theta structure over $W'(E)$, is defined over $\mathbb{F}_p$ together with all $\tilde{\theta}^{W'(E)}(\Gamma(X, \pm X))$ for all $X \in E$.

Proof. There is a natural compatibility between Frobenius and barycentric coordinates given by $\pi(P \pm Q) = (\pi(u) : \pi(v) : \pi(w))$. Thus, taking the formula for position 11 from [Dup25, Appendix A] and replacing with the values from Lemma F.4, we get the first half of Equation (21). What remains to be seen is the part linked to constant D and E. This comes from the following rewriting

$$\begin{aligned} & 2(-m_0m_1 \pm m_2\mathbf{i}m_3)(u^2 - v^2 + w^2)\overline{u^2 - v^2 + w^2} + 2(-m_0m_1 \mp m_2\mathbf{i}m_3)uw\overline{(u^2 - v^2 + w^2)} \\ &= -2D \left((u^2 - v^2 + w^2)\overline{u^2 - v^2 + w^2} + uw\overline{(u^2 - v^2 + w^2)} \right) \\ & \quad \pm 2\mathbf{i}E \left((u^2 - v^2 + w^2)\overline{u^2 - v^2 + w^2} - uw\overline{(u^2 - v^2 + w^2)} \right) \\ &= -4D \cdot \operatorname{Re} \left((u^2 - v^2 + w^2)\overline{u^2 - v^2 + w^2} \right) \mp 4E \cdot \operatorname{Im} \left((u^2 - v^2 + w^2)\overline{u^2 - v^2 + w^2} \right) \end{aligned}$$

As the above vector is defined over $\mathbb{F}_p$, using Mumford's duplication formula [Dar25b, Lemma 6.1.12], we get that the image theta structure is defined over $\mathbb{F}_p$. Indeed, the theta null point of $\tilde{\theta}^{W'(E)}(0)$ can be recovered through an interpolation consisting of the multiplication of vectors over $\mathbb{F}_p$, as detailed in [DD26, §3.1]. From this point, we obtain the existence of a point T such that $\tilde{\theta}^{W'(E)}(\Gamma(T, \sigma(T)))$ is defined over $\mathbb{F}_p$, and the rest follows. $\square$

Another quirk of Superglue is that it highlights a symmetry on the image of Γ that is useful in MIKE to divide the number of point evaluations by 2. Namely:

Corollary F.2. *Using the notation of [Theorem F.3](#), let $\tilde{\theta}^{W'(E)}$ be the dual theta structure induced by the gluing formula of [Theorem F.3](#) over $W'(E)$. Then, for all $P \in E$, we have*

$$\begin{aligned}\tilde{\theta}^{W'(E)}(\Gamma(P, \sigma(P))) &:= (X : Y : Z : W), \\ \tilde{\theta}^{W'(E)}(\Gamma(P, -\sigma(P))) &:= (X : Y : Z : -W).\end{aligned}$$

Note that [Corollary F.2](#) is a highly specialised form of a more general result. Indeed, this result holds not only for Γ , but for any gluing isogeny evaluated on (P, Q) and $(P, -Q)$ and is an easy consequence of [\[Dup25\]](#). The remaining computations of the Scholten gluing follow the classical structure detailed in both [\[DMPR24; Dup25\]](#). We detail in [Algorithm 5](#) and [Algorithm 6](#) algorithms used to efficiently precompute the constants and [Equation \(21\)](#).

Algorithm 5 [ScholtenGluingPrecom](#)(P)

Input: P a non-trivial 4-torsion point of an elliptic curve E defined over $\mathbb{F}_{p^2}$.

Output: Precomp precomputed values used for fast Scholten gluing computation.

```

1:  $\alpha, \beta \leftarrow x_P, z_P$ 
2:  $n(\alpha), n(\beta) \leftarrow \alpha\bar{\alpha}, \beta\bar{\beta}$  ▷ 4s + 2a
3:  $m_0, m_1 \leftarrow n(\alpha) + n(\beta), n(\beta) - n(\alpha)$  ▷ 2a
4:  $m_2 + im_3 \leftarrow 2\alpha\bar{\beta}$  ▷ 4m + 4a
5: Compute  $m_0^2, m_1^2, m_2^2$  ▷ 3s
6:  $A, B, C \leftarrow m_1^2 + m_2^2, m_0^2 - m_1^2, m_0^2 - m_2^2$  ▷ 3a
7:  $D, E \leftarrow m_0m_1, m_2m_3$  ▷ 2m
8: Precomp  $\leftarrow (A, B, C, 4D, 4E)$  ▷ 4a
9: return Precomp ▷ Total cost: 6m + 7s + 15a
```

F.4 Computing a theta structure compatible with gluing

Computing MIKE's diagonal isogenies We now look how to efficiently compute $F_2 := \text{Diag}(\phi, \phi') : W'(E)^2 \rightarrow S \times S'$, which consists in two diagonal isogenies. Following [Theorem F.2](#), we have that, up to reordering, these are the 2-dimensional 2-isogenies ϕ_U and ϕ_V with:

$$\begin{aligned}\ker(\phi_U) &:= [2^{f-2}] \langle \Gamma(P, \sigma(P)), \Gamma(Q, \sigma(Q)) \rangle = [2^{f-2}] \langle U_1, U_2 \rangle \\ \ker(\phi_V) &:= [2^{f-2}] \langle \Gamma(-P, \sigma(P)), \Gamma(Q, -\sigma(Q)) \rangle = [2^{f-2}] \langle V_1, V_2 \rangle\end{aligned}$$

By construction, following [\[DMPR24; Dup25\]](#), the theta structure we inherit from the Scholten gluing is induced by the symplectic basis of $W'(E)[4]$ denoted $\mathcal{B}_0$:

$$\mathcal{B}_0 := [2^{f-2}] \Gamma(0, \sigma(Q)), [2^{f-2}] \Gamma(P, 0), [2^{f-3}] \Gamma(P, \sigma(P)), [2^{f-3}] \Gamma(Q, \sigma(Q))$$

Algorithm 6 `ScholtenGluingCompute`(Precomp, $P \pm T, b$)

Input: Precomp, as previously computed in [Algorithm 5](#) and $P \pm T := (u : v : w)$ barycentric coordinates of a point over E defined over $\mathbb{F}_{p^2}$ and b , a boolean indicating whether P represent a point in the Weil restriction or its twist.

Output: $\theta^{W'(E)}\left(\Gamma(P, (-1)^b \sigma(P))\right) \odot \theta^{W'(E)}\left(\Gamma(T, \sigma(T))\right)$.

```

1:  $A, B, C, D, E \leftarrow \text{Precomp}$ 
2:  $u, v, w \leftarrow P \pm T$ 
3: Compute  $w^2, u^2, v^2$  ▷ 3m + 6s + 6a
4: Compute  $2n(u), 2n(v), 2n(w)$  ▷ 6a using above values
5: Compute  $uw, 4n(u)n(w), 4n(v)n(w)$  ▷ 6m + 2a
6: Compute  $u^2 - v^2 \pm w^2$  ▷ 6a
7: Compute  $n(u^2 - v^2 \pm w^2)$  ▷ 4s + 2a
8: Compute  $U + iV \leftarrow (u^2 - v^2 + w^2)(\overline{uw})$  ▷ 4m + 2a
9:  $\alpha \leftarrow A \cdot n(u^2 - v^2 + w^2) + C \cdot 4n(u)n(w)$  ▷ 2m + a
10:  $\alpha \leftarrow \alpha - DU - EV$  ▷ 2m + 2a
11:  $\gamma \leftarrow C \cdot n(u^2 - v^2 + w^2) + A \cdot 4n(u)n(w)$  ▷ 2m + a
12:  $\gamma \leftarrow \gamma - DU + EV$  ▷ 2a
13:  $\beta \leftarrow B \cdot n(u^2 - v^2 - w^2)$  ▷ 1m
14:  $\delta \leftarrow (-1)^b B \cdot 4n(v)n(w)$  ▷ 1m
15: return  $(\alpha, \beta, \gamma, \delta)$  ▷ Total cost: 21m + 10s + 24a
    
```

To compute both ϕ_U and ϕ_V , we need to find a theta structure that is compatible with the computation of both of them, i.e. the theta structure over W'_E induced by the symplectic basis $\mathcal{B}_1$:

$$\mathcal{B}_1 := ([2^{f-3}]U_1, [2^{f-3}]U_2, [2^{f-3}]V_1, [2^{f-3}]V_2)$$

It can be constructed from the knowledge of the symplectic change of basis from $\mathcal{B}_0$ to $\mathcal{B}_1$ using [\[Dar25b, Theorem 6.2.10\]](#).

Lemma F.5. *The symplectic change of basis mapping $\mathcal{B}_0$ to $\mathcal{B}_1$ is given by the matrix $\mathbf{N}_1$ with the associated change of theta coordinates $\mathbf{M}_{\mathbf{N}_1}$*

$$\mathbf{N}_1 = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}, \quad \mathbf{M}_{\mathbf{N}_1} = \begin{pmatrix} 1 & 1 & 1 & -1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & -1 & -1 \end{pmatrix}$$

Proof. The symplectic change of basis $\mathbf{N}_1$ comes naturally from the fact that

$$[2^{f-3}]V_1 = [2^{f-3}]\Gamma(Q, -\sigma(Q)) = [2^{f-3}]\Gamma(Q, \sigma(Q)) - [2^{f-2}]\Gamma(0, \sigma(Q))$$

$$[2^{f-3}]V_2 = [2^{f-3}]\Gamma(-P, \sigma(P)) = [2^{f-3}]\Gamma(P, \sigma(P)) - [2^{f-2}]\Gamma(P, 0)$$

The computation of $\mathbf{M}_{\mathbf{N}_1}$ is then given by [\[Dar25b, Theorem 6.2.10\]](#). □

By applying $\mathbf{M}_{\mathbf{N}_1}$ to the image of point evaluated through Γ , we efficiently evaluate any point in the theta structure $\theta^{W'(E)}$ induced by the basis $\mathcal{B}_1$, itself

compatible with the computation of ϕ_V , while its dual $\tilde{\theta}^{W'(E)}$, induced by the dual basis

$$\widetilde{\mathcal{B}}_1 := (-[2^{f-3}]V_1, -[2^{f-3}]V_2, [2^{f-3}]U_1, [2^{f-3}]U_2)$$

is compatible with the computation of ϕ_U . Both isogenies can therefore be efficiently computed using standard methods for computing $(2, 2)$ -isogenies [DMPR24]. Doing so requires to have computed the $[2^{f-4}]U_i$ and $[2^{f-4}]V_i$ points. Though this would naively require four point gluing evaluations through Γ , we can reduce this to only two using Corollary F.2 by the nature of U_i and V_i points.

Computing a compatible 4-dimensional theta structure We now have two theta structures on S_U and S_V , induced by the 4-symplectic bases

$$\mathcal{B}_U := \{[2^{f-4}]\phi_U(U_1), [2^{f-4}]\phi_U(U_2), [2^{f-3}]\phi_U(V_1), [2^{f-3}]\phi_U(V_2)\},$$

$$\mathcal{B}_V := \{[2^{f-3}]\phi_V(U_1), [2^{f-3}]\phi_V(U_2), [2^{f-4}]\phi_V(V_1), [2^{f-4}]\phi_V(V_2)\}.$$

Note that in the case of $\mathcal{B}_U$, this basis is the dual of the one naturally computed by the ϕ_U , meaning that we are applying a Hadamard transform once again. We can therefore, using the Kronecker product, compute a product theta structure over $S_U \times S_V$, generated by $\mathcal{B}_U \otimes \mathcal{B}_V$.²⁸ It remains to compute the symplectic change of basis matrix from $\mathcal{B}_U \otimes \mathcal{B}_V$ to a symplectic basis compatible with F_3 and the rest of the 4-dimensional chain, namely $[2^{f-5}]F_2 \circ F_1(\mathcal{B})$, with $\mathcal{B}$ the symplectic basis from Theorem 4.1.

Lemma F.6. *The symplectic change of basis matrix from $\mathcal{B}_U \otimes \mathcal{B}_V$ to $[2^{f-5}]F_2 \circ F_1(\mathcal{B})$ is given by the symplectic matrix $\mathbf{N}_2 \in Sp_4(\mathbb{Z}_4)$:*

$$\mathbf{N}_2 := \begin{pmatrix} 0 & 0 & 1 & 0 & \nu_1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & \nu_1 & 0 & 0 \\ 0 & 0 & -1 & 0 & \nu_2 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & \nu_2 & 0 & 0 \\ -\lambda & 0 & 0 & 0 & 0 & 0 & \nu_3 & 0 \\ 0 & -\lambda & 0 & 0 & 0 & 0 & 0 & \nu_3 \\ -\lambda & 0 & 0 & 0 & 0 & 0 & \nu_4 & 0 \\ 0 & -\lambda & 0 & 0 & 0 & 0 & 0 & \nu_4 \end{pmatrix},$$

where $\nu_1 := (x(1-x))/2$, $\nu_2 := (x(1+x))/4$, $\nu_3 := (x+1)/4$ and $\nu_4 := (x-1)/2$, $\lambda = x^{-1} \pmod{2^{f-1}}$. The change of theta coordinates matrix is given by $\mathbf{M}_{\mathbf{N}_2} \in$

²⁸ See [DD26, §2.6] for the detailed construction.

$GL_{16}(\mathbb{F}_p)$ is

$$\mathbf{M}_{\mathbf{N}_2} := \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & -1 & 0 & 0 & 1 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & -1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & -1 & 0 & 0 & 0 \end{pmatrix}$$

which can be efficiently computed as 4 independent twisted Hadamard transforms.

Proof. This is a straightforward application of [Dar25b, Theorem 6.2.10]. $\square$

F.5 Gluing into an Abelian variety of Weil type

What now remains is to detail how to efficiently compute the proper gluing isogeny $F_3 : S_U \times S_V \rightarrow X$, where X is a abelian fourfold of Weil type. Although we detailed in [Appendix E.2](#) how to compute generic 2-isogenies between our specific abelian fourfold of Weil type, the gluing isogeny requires special care. This is because, in the case of gluing, the dual theta null point $\tilde{\theta}^X(0)$ has zero coordinates, thus requiring a specialised mechanism. In the case of MIKE, those zero coordinates are fixed and given by

$$\tilde{\theta}_j^X(0) \quad \text{for } j \in \{5, 7, 10, 11, 13, 14\}.$$

Additionally, following [Proposition 4.1](#), we also have that dual theta null points must be stable under the action of the $[\mathbf{i}]$ automorphism of X , meaning that

$$\tilde{\theta}_j^X(0) = \tilde{\theta}_j^X([\mathbf{i}](0)) = \tilde{\theta}_{\tau \circ j}^X(0)$$

with $\tau \circ j$ acting as the permutation $(03)(12) \in \mathfrak{S}_4$ on the bitwise representation of j .

Following [DD26, §3.2] and similarly to [Theorem E.1](#), computing our isogeny F_3 is then equivalent to solving the equivalent HIIP [DD26, Problem 3.1] instance, itself equivalent to finding a spanning tree in $\mathcal{G}$, the codomain graph. Likewise [Theorem E.1](#), thanks to the action of $\mathbf{i}$ on the theta-coordinates, it suffices to solve the HIIP over $\mathcal{G}_{[\mathbf{i}]}$ to naturally retrieve a solution of the HIIP

on $\mathcal{G}$, where $\mathcal{G}_{[i]}$ is the graph $\mathcal{G}$ quotiented by the equivalence relation induced by i on the theta null point, following Lemma H.5. In the case of MIKE's gluing, we will consider Figure 14, the codomain graph induced by the 8 torsion points $[2^{f-5}]F_2 \circ F_1(T_3)$, $[2^{f-5}]F_2 \circ F_1(T_4)$ and its sum. We can thus interpolate efficiently $\tilde{\theta}^X(0)^{\odot-1}$ using the formula [DD26, equation 5] and specialising it to our spanning tree.

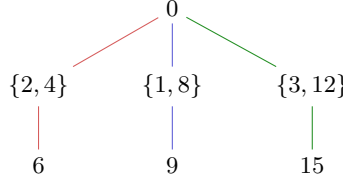


Fig. 14: MIKE gluing $\mathcal{G}_{[i]}$ codomain graph. Edges are in red for T_3 , blue for T_4 and green for $T_3 + T_4$.

Nevertheless, since $\tilde{\theta}^X(0)^{\odot-1}$ contains zero coordinates, it is not a suitable choice of auxiliary point for evaluating other points. Instead, we use the point $[2^{f-5}]F_2 \circ F_1(T_3)$. This choice is motivated by the fact that it has no zero coordinates, and that $[2^{f-5}]F_3 \circ F_2 \circ F_1(T_3)$ is a point of 4-torsion in A . By the theta group action relation, this torsion property implies that we only need to compute half of its coordinates, since

$$\tilde{\theta}_i^X([2^{f-5}]F_3 \circ F_2 \circ F_1(T_3)) = \tilde{\theta}_{i+4}^X([2^{f-5}]F_3 \circ F_2 \circ F_1(T_3)).$$

By using $\tilde{\theta}^X([2^{f-5}]F_3 \circ F_2 \circ F_1(T_3)) \odot \tilde{\theta}^X(0)$, which was previously computed to interpolate $\tilde{\theta}(0)^{\odot-1}$, and combining the theta group action relation with the action of the $[i]$ automorphism, we can recover all coordinates $\tilde{\theta}_j^X([2^{f-5}]F_3 \circ F_2 \circ F_1(T_3))$ except for $j = 10, 14$, despite the presence of 6 zero coordinates. To recover these last two coordinates, we further exploit the theta group action.

Consider the point $U := [2^{f-5}]T_3 + [2^{f-4}]T_4$. By the theta group action, we have

$$\tilde{\theta}_j^X(F_3 \circ F_2 \circ F_1(U)) = \tilde{\theta}_{j+8}^X([2^{f-5}]F_3 \circ F_2 \circ F_1(T_3)).$$

Using this property, we obtain $\tilde{\theta}_{10}^W([2^{f-5}]F_3 \circ F_2 \circ F_1(T_3)) = \tilde{\theta}_2^W(F_3 \circ F_2 \circ F_1(X))$, which can be recovered from $\tilde{\theta}^X(F_2 \circ F_1(X)) \odot \tilde{\theta}^X(0)$.²⁹ Furthermore, $F_3 \circ F_2 \circ F_1(X)$ can be efficiently computed using differential addition over S_U and S_V using the points previously required to interpolate $\tilde{\theta}^X(0)^{\odot-1}$.

²⁹ To do so, we must ensure that both vectors share the same projective scaling factor, which requires a few additional multiplications.

Once $\tilde{\theta}^X([2^{f-5}]F_3 \circ F_2 \circ F_1(T_3))$ is completely determined, computing its entry-wise inverse $\tilde{\theta}^X([2^{f-5}]F_3 \circ F_2 \circ F_1(T_3))^{\odot -1}$ can be done via projective inversion. We provide in [Algorithm 7](#) the pseudocode of the whole procedure.

Algorithm 7 [GluingCodomain](#) $(T_3^{(8)}, T_4^{(8)}, T_{3+4}^{(8)}, T_3^{(8)} + T_4^{(4)})$

Input: $T_3^{(8)}, T_4^{(8)}, T_{3+4}^{(8)}$, and $T_3^{(8)} + T_4^{(4)}$: 8-torsion points above their respective points in the underlying symplectic basis, specifying the 4-dimensional theta structure as specified in [Appendix F.5](#).

Output: $\tilde{\theta}^X([2^{e-5}]F_{\text{glue}}(T_3))^{\odot -1}$ and $\tilde{\theta}^X(0)^{\odot -1}$

```

1:  $\Omega^i \leftarrow H(X^{\odot 2})$  for  $X$  all 4 inputs of GluingCodomain.
2:  $\text{branch}^4 \leftarrow (\Omega_4^0 \cdot \Omega_6^0, \Omega_0^0 \cdot \Omega_6^0, \Omega_0^0 \cdot \Omega_2^0)$ 
3:  $\text{branch}^8 \leftarrow (\Omega_8^1 \cdot \Omega_9^1, \Omega_0^1 \cdot \Omega_9^1, \Omega_0^1 \cdot \Omega_1^1)$ 
4:  $\text{branch}^{12} \leftarrow (\Omega_{12}^2 \cdot \Omega_{15}^2, \Omega_0^2 \cdot \Omega_{15}^2, \Omega_0^2 \cdot H_3^2)$ 
5: Initialise  $Z$  a 10 element array.  $\triangleright$  All 10 coordinates of  $\tilde{\theta}^X(0)^{\odot -1}$ .
6:  $U \leftarrow \text{branch}_0^8 \cdot \text{branch}_0^{12}$ 
7:  $Z_0 \leftarrow \text{branch}_0^4, \quad Z_2 \leftarrow \text{branch}_1^4, \quad Z_5 \leftarrow \text{branch}_2^4$ 
8:  $U \leftarrow \text{branch}_0^4 \cdot \text{branch}_0^{12}$ 
9:  $Z_1 \leftarrow U \cdot \text{branch}_1^8, \quad Z_7 \leftarrow U \cdot \text{branch}_2^8$ 
10:  $U \leftarrow \text{branch}_0^4 \cdot \text{branch}_0^8$ 
11:  $Z_3 \leftarrow U \cdot \text{branch}_1^{12}, \quad Z_9 \leftarrow U \cdot \text{branch}_2^{12}$ 
12: Set  $Z_4, Z_6$  and  $Z_8$  to 0.
13: Uncompress  $Z$  into  $\tilde{\theta}^X(0)^{\odot -1}$ 
14: Initialise  $X$  a 8 element array.  $\triangleright$  All 8 coordinates of  $\tilde{\theta}^X([2^{f-5}]F_{\text{glue}}(T_3))$ 
15:  $X_{0,1,2,3} \leftarrow \Omega_i^0 \cdot \tilde{\theta}_i^W(0)^{\odot -1}$  for  $i \in \{0, 1, 2, 3\}$ 
16:  $X_{4,5,7} \leftarrow \Omega_i^0 \cdot \tilde{\theta}_i^W(0)^{\odot -1}$  for  $i \in \{8, 9, 15\}$ 
17:  $X_6 \leftarrow X_0 \cdot \Omega_2^3 \cdot \tilde{\theta}_2^W(0)^{\odot -1}$ 
18:  $t \leftarrow \Omega_8^3 \cdot \tilde{\theta}_8^W(0)^{\odot -1}$   $\triangleright$  recover last coordinate
19: for  $i \in \{0, \dots, 7\} \setminus \{6\}$  do
20:    $X_i \leftarrow X_i \cdot t$   $\triangleright$  Ensure coherent projective coefficients
21:  $X^{\odot -1} \leftarrow \text{ProjectiveInversion}(X)$ 
22: Uncompress  $X^{\odot -1}$  into  $\tilde{\theta}^X([2^{f-5}]F_{\text{glue}}(T_3))^{\odot -1}$ 
23: return  $\tilde{\theta}^X([2^{f-5}]F_{\text{glue}}(T_3))^{\odot -1}, \tilde{\theta}^X(0)^{\odot -1}$ 

```

F.6 Gluing everything together

After this brief overview of MIKE's gluing, we now have all the tools necessary to compute and evaluate points through F_{glue} using [Algorithms 8 to 10](#). Their pseudocode concludes this short and non technical appendix.

G Abelian fourfolds of Weil type

There are various automorphisms in play in the MIKE key exchange, which we study in this section. Notably we will prove that the MIKE fourfolds are of

Algorithm 8 [GluingBasisWithVerification](#)(P, Q, e, x)**Input:** (P, Q) are a basis of $E[2^e]$ and $x \in \mathbb{Z}_{2^e}$ such that $x = 3 \pmod 8$ **Output:** $\mathcal{B}_{\text{glue}}$ a basis of the gluing and **valid**, a boolean denoting if the curve E is valid or not.

```

1: valid  $\leftarrow$  true
2:  $P^{(32)} \leftarrow [2^{e-5}]P, Q^{(32)} \leftarrow [2^{e-5}]Q$ 
3:  $P^{(16)} \leftarrow [2]P^{(32)}, Q^{(16)} \leftarrow [2]Q^{(32)}$ 
4:  $P^{(8)} \leftarrow [2]P^{(16)}, Q^{(8)} \leftarrow [2]Q^{(16)}$ 
5:  $P^{(4)} \leftarrow [2]P^{(8)}$ 
6: if  $[2]P^{(4)} \neq (* : 0 : *)$  or  $[2]Q^{(8)} \neq (1 : * : \pm 1)$  then
7:   valid  $\leftarrow$  false
8:  $E'_B \leftarrow \text{NormaliseMontgomery}(E_B)$   $\triangleright$  Using  $P^{(4)}$  and \[AAA+26, Algo 4.96\]
9: if  $E_B \neq E'_B$  then
10:  valid  $\leftarrow$  false
11:  $T_3^{(32)} \leftarrow ((x+1)/2)Q^{(32)}, [(x-1)/2]Q^{(32)}$ 
12:  $T_4^{(32)} \leftarrow -[(x+1)/2]P^{(32)}, -[(x-1)/2]P^{(32)}$ 
13:  $T_{3+4}^{(32)} \leftarrow T_3^{(32)} + T_4^{(32)}$ 
14:  $\mathcal{B}_{\text{glue}} \leftarrow (P^{(8)}, Q^{(8)}, P^{(16)}, Q^{(16)}, T_3^{(32)}, T_4^{(32)}, T_{3+4}^{(32)})$ 
15: return  $\mathcal{B}_{\text{glue}}, \text{valid}$ 

```

Algorithm 9 [ComputeGluing](#)($\mathcal{B}_{\text{glue}}$)**Input:** $\mathcal{B}_{\text{glue}}$ the gluing basis as computed in [Algorithm 8](#).**Output:** F_{glue} : the precomputations required to evaluate point through F_{glue}

```

1:  $P^{(8)}, Q^{(8)}, P^{(16)}, Q^{(16)}, T_3^{(32)}, T_4^{(32)}, T_{3+4}^{(32)} \leftarrow \mathcal{B}_{\text{glue}}$ 
   // Scholten gluing
2: Compute  $\Gamma : E \times E^\sigma \mapsto W'(E)$ .  $\triangleright$  \[Dup25, Alg. 6\] with ScholtenGluingCompute
   // Diagonal isogeny
3:  $\tilde{\theta}^{W'(E)}(V_1) \leftarrow \Gamma(Q^{(16)}, -\sigma(Q^{(16)}))$   $\triangleright$  Use \[Dup25, Alg. 7\] with
   ScholtenGluingCompute
4:  $\tilde{\theta}^{W'(E)}(V_2) \leftarrow \Gamma(P^{(16)}, -\sigma(P^{(16)}))$   $\triangleright$  Use \[Dup25, Alg. 7\] with
   ScholtenGluingCompute
5: Compute  $\tilde{\theta}_j^{W'(E)}(U_i) \leftarrow (-1)^{j=3} \tilde{\theta}_i^{W'(E)}(V_{1+i})$  for  $i \in \{0, 1\}$  and  $j \in \{0, 1, 2, 3\}$ 
6: Apply  $\mathbf{M}_{\mathbf{N}_1}$  to  $\tilde{\theta}^{W'(E)}(U_i)$  and  $\tilde{\theta}^{W'(E)}(V_i)$  for  $i \in \{0, 1\}$ 
7: Get  $\phi_U : W'(E) \mapsto S_U$  using  $(H(\tilde{\theta}^{W'(E)}(U_i)))_{i \in \{0, 1\}}$   $\triangleright$  \[AAA+26, Alg. 4.116\]
8: Get  $\phi_V : W'(E) \mapsto S_V$  using  $(\tilde{\theta}^{W'(E)}(V_i))_{i \in \{0, 1\}}$   $\triangleright$  \[AAA+26, Alg. 4.116\]
   // Weil gluing
9:  $(T_k)_0 \leftarrow \theta^{W'(E)}(\Gamma((T_k^{(32)})_0))$  and  $(T_k)_1 \leftarrow \theta^{W'(E)}(\Gamma((T_k^{(32)})_1))$  for  $k \in \{3, 4, 3+4\}$ 
10: Apply  $\mathbf{M}_{\mathbf{N}_1}$  to  $(T_k)_0$  and  $(T_k)_1$  for  $k \in \{3, 4, 3+4\}$ 
11:  $(T_k)_0 \leftarrow \theta^{S_U}(\phi_U((T_k)_0))$  and  $(T_k)_1 \leftarrow \theta^{S_V}(\phi_V((T_k)_1))$  for  $k \in \{3, 4, 3+4\}$ 
12:  $(T_{3+4+4})_0 \leftarrow \text{xADD}_{S_U}((T_4)_0, (T_{3+4})_0, (T_3)_0)$ 
13:  $(T_{3+4+4})_1 \leftarrow \text{xADD}_{S_V}((T_4)_1, (T_{3+4})_1, (T_3)_1)$ 
14:  $T_k \leftarrow (T_k)_0 \otimes (T_k)_1$  for  $k \in \{3, 4, 3+4, 3+4+4\}$ 
15: Apply  $\mathbf{M}_{\mathbf{N}_2}$  to  $T_k$  for  $k \in \{3, 4, 3+4, 3+4+4\}$ 
16: Compute  $F_3 : S_U \times S_V \rightarrow X$  using  $T_3, T_4, T_{3+4}, T_{3+4+4}$   $\triangleright$  Use GluingCodomain
17:  $F_{\text{glue}} \leftarrow \Gamma, \phi_U, \phi_V, F_3, P^8, T_3^{(32)}$ 
18: return  $F_{\text{glue}}$ 

```

Algorithm 10 EvalGluing(F_{glue}, T)

Input: F_{glue} : representing the pre-computation performed in [Algorithm 9](#). T a couple point in E^2 corresponding to $(T_0, -\sigma(T_0)), (T_1, -\sigma(T_1)) \in (E \times E^\sigma)^2$.

Output: $\theta^X(F_{\text{glue}}(T))$: the image of T through the gluing isogenies of **MIKE**, in a theta structure compatible with the chain.

- 1: Compute $T + T_3^{(32)}$ and $T - T_3^{(32)}$
 - 2: Compute $(T \pm T_3^{(32)})_0 \pm P^{(8)}$ and $(T \pm T_3^{(32)})_1 \pm P^{(8)}$
 - 3: Compute $\theta^{W'(E)}(\Gamma((T \pm T_3^{(32)})_0)) \triangleright \text{Use } \tilde{\theta}^{W'(E)}(\Gamma(P^{(8)}))^{\odot -1}$
 - 4: Compute $\theta^{W'(E)}(\Gamma((T \pm T_3^{(32)})_1)) \triangleright \text{Use } \tilde{\theta}^{W'(E)}(\Gamma(P^{(8)}))^{\odot -1}$
 - 5: Apply $\mathbf{M}_{\mathbf{N}_1}$ to $\theta^{W'(E)}(\Gamma((T \pm T_3^{(32)})_0))$
 - 6: Apply $\mathbf{M}_{\mathbf{N}_1}$ to $\theta^{W'(E)}(\Gamma((T \pm T_3^{(32)})_1))$
 - 7: $A \leftarrow \theta^{S_U}(\phi_U \circ \Gamma((T \pm T_3^{(32)})_0)) \triangleright \text{Use } \tilde{\theta}^{S_U}(0)^{\odot -1}$
 - 8: $B \leftarrow \theta^{S_V}(\phi_V \circ \Gamma((T \pm T_3^{(32)})_1)) \triangleright \text{Use } \tilde{\theta}^{S_V}(0)^{\odot -1}$
 - 9: $\theta^{S_U \times S_V}(F_2 \circ F_1(T \pm T_3^{(32)})) \leftarrow \mathbf{M}_{\mathbf{N}_2} \cdot (A \otimes B)$
 - 10: **return** $\theta^X(F_3(T)) \triangleright \text{Use } \tilde{\theta}^X([2^{e-5}]F_{\text{glue}}(T_3))^{\odot -1}$
-

Weil type (see [Definition 4.1](#)), which plays an important role both to speed up the dimension-4 isogeny computations ([Appendix E.2](#)), but also to find suitable modular invariants ([Appendix H](#)).

G.1 Automorphisms in MIKE

The goal of this section is to prove [Proposition 4.1](#) *i.e.* that our **MIKE** shared key is of Weil type. We provide a purely geometric argument and reformulate it in the framework of the (quaternionic) module action (see [Appendix B.6](#)).

A purely geometric argument. We first look at the abelian surfaces generated during the key exchange. Recall that our public key is of the form $X_A = M_A \cdot E'_0$ where (M_A, H_A) is a unimodular rank-2 Hermitian R -module with $R = \mathbb{Z}[(\sqrt{-p} - 1)/2]$. In practice, we take M_A R -isomorphic to the quaternionic ideal $I_A \subset \mathcal{O}_0$, so that if $E_A = I_A \cdot_{\mathcal{O}_0} E'_0$, $X_A = W'(E_A)$ by [Corollary C.2](#).

In the following, let $E/\mathbb{F}_{p^2}$ be a maximal supersingular elliptic curve (*e.g.* $E = E_A$). By construction, $W'(E)$ is 2-isogeneous to the Weil restriction $W(E)$, which is isomorphic over $\mathbb{F}_{p^2}$ to $E \times E^\sigma$ (where σ denotes the p -Frobenius action).

Now on this product there is an involutive automorphism $\gamma_E : (P, Q) \mapsto (-P, Q)$, with $\gamma_E^2 = 1$. Let $\Gamma_E : W(E) \rightarrow W'(E)$ be the Scholten gluing 2-isogeny.

Lemma G.1. γ_E descends to an involutive automorphism γ'_E of $W'(E)$ (defined over $\mathbb{F}_{p^2}$), such that $\gamma'^2_E = [1]$ on $W'(E)$ and $\gamma'_E \circ \Gamma_E = \Gamma_E \circ \gamma_E$. We call it the canonical involution of $W'(E)$.

Proof. Let $e : W(E) \rightarrow W(E), (P, Q) \mapsto (P, 0)$ be the idempotent defined over $\mathbb{F}_{p^2}$: $e^2 = e$. So this is an endomorphism of discriminant 1. We let $\xi = \Gamma_E \circ e \circ \tilde{\Gamma}_E$; it

satisfies $\xi^2 = [2]\xi$ so this is an endomorphism of $W'(E)$ of discriminant 4. Define $\gamma'_E := [1] - \xi$, then $\gamma'^2_E = 1$. Furthermore, since $\gamma_E = \text{id}_{W(E)} - 2e$, we have that $\gamma'_E \circ \Gamma_E \circ \tilde{\Gamma}_E = 2\gamma'_E = [2] - [2]\xi = \Gamma_E \circ ([1] - [2]e) \circ \tilde{\Gamma}_E = \Gamma_E \circ \gamma_E \circ \tilde{\Gamma}_E$, so $\gamma'_E \circ \Gamma_E = \Gamma_E \circ \gamma_E$. $\square$

Remark G.1. Let us remark some basic properties of the canonical involution γ'_E . First, by construction $\tilde{\gamma}_E = \gamma_E$, and it follows from $\gamma'_E \circ \Gamma_E = \Gamma_E \circ \gamma_E$ that $\gamma'_E = \gamma'_E$.

Second, γ_E anti-commutes with the p -Frobenius of $W(E)$, which ensures that γ'_E anti-commutes with the p -Frobenius of $W'(E)$ (since Γ_E commutes with the p -Frobenius).

Finally, recall that the Weil and Scholten constructions are functorial: an isogeny $\varphi : E_A \rightarrow E_B$ induces isogenies $W(\varphi) : W(E_A) \rightarrow W(E_B)$ and $W'(\varphi) : W'(E_A) \rightarrow W'(E_B)$. The construction of the canonical involution γ_E in [Lemma G.1](#) shows that it is functorial too: it commutes with the isogeny $W'(\varphi) : W'(E_A) \rightarrow W'(E_B)$. Indeed, keeping the notations from [Lemma G.1](#) and replacing the E_A, E_B indices by A and B instead, we obtain:

$$\gamma'_B \circ W'(\varphi) \circ \Gamma_A = \gamma'_B \circ \Gamma_B \circ W(\varphi) = \Gamma_B \circ \gamma_B \circ W(\varphi)$$

But $W(\varphi) = \text{Diag}(\varphi, \varphi^\sigma)$ and both γ_A and γ_B are of the form $\text{Diag}([-1], [1])$, which ensures that $\gamma_B \circ W(\varphi) = W(\varphi) \circ \gamma_A$, so that:

$$\gamma'_B \circ W'(\varphi) \circ \Gamma_A = \Gamma_B \circ W(\varphi) \circ \gamma_A = W'(\varphi) \circ \gamma'_A \circ \Gamma_A,$$

and finally $\gamma'_B \circ W'(\varphi) = W'(\varphi) \circ \gamma'_A$, as desired.

Lemma G.2. *Let $E'_0/\mathbb{F}_p$ be the curve $y^2 = x^3 - x$. Under the isomorphism $W'(E'_0) \simeq E'^2_0$ from [Corollary C.1](#), the canonical involution is $\gamma'_0 : (P, Q) \mapsto ([\mathbf{i}]Q, -[\mathbf{i}]P)$, where $[\mathbf{i}] : (x, y) \in E'_0 \rightarrow (-x, \mathbf{i}y) \in E'_0$.*

Proof. By [Lemma C.3](#), we have $W'(E'_0) \cong E'_0 \times E'^t_0$ over $\mathbb{F}_p$. In the proof of [Lemma C.3](#), we have seen that the Scholten 2-isogeny is given by $\Gamma_0 : W(E'_0) \rightarrow W'(E'_0), (P, Q) \mapsto (P + Q, P - Q)$ up to post-composition by a twisting isomorphism $E'_0 \times E'_0 \simeq E'_0 \times E'^t_0$. Since $E'^t_0 \simeq E'_0$, we may take $[\mathbf{i}]$ as twisting isomorphism of E'_0 , so that $\Gamma_0 : (P, Q) \mapsto (P + Q, [\mathbf{i}](P - Q))$.

Now under this isomorphism and with $\gamma_0 : (P, Q) \mapsto (-P, Q)$, we obtain $\Gamma_0 \circ \gamma_0(P, Q) = \Gamma_0(-P, Q) = (-P + Q, [\mathbf{i}](-P - Q))$. Since $\gamma'_0 \circ \Gamma_0 = \Gamma_0 \circ \gamma_0$, we apply these equations to $(P', P'), (-[\mathbf{i}]Q', [\mathbf{i}]Q') \in E'^2_0$ such that $[2]P' = P, [2]Q' = Q \in E'_0$ to obtain:

$$\begin{aligned} \gamma'_0(P, 0) &= \gamma'_0 \circ \Gamma_0(P', P') = \Gamma_0 \circ \gamma_0(P', P') = (0, -[\mathbf{i}]P) \\ \gamma'_0(0, Q) &= \gamma'_0 \circ \Gamma_0(-[\mathbf{i}]Q', [\mathbf{i}]Q') = \Gamma_0 \circ \gamma_0(-[\mathbf{i}]Q', [\mathbf{i}]Q') = ([\mathbf{i}]Q, 0). \end{aligned}$$

We conclude that $\gamma'_0(P, Q) = ([\mathbf{i}]Q, -[\mathbf{i}]P)$. $\square$

Remark G.2. We also have the automorphism $[i](x, y) = (-x, \mathbf{i}y)$ on E'_0 . Then WE'_0 is isomorphic over $\mathbb{F}_{p^2}$ to $E'_0 \times E'^\sigma_0 = E'_0 \times E'_0$, and $W[i] = [i] \times [i]^\sigma =$

$[i] \times [-i]$. By the proof of [Lemma G.2](#), we have a canonical $\mathbb{F}_p$ -rational isogeny $\Gamma_0 : WE'_0 \rightarrow W'E'_0 \simeq E'^2_0$, given over $\mathbb{F}_{p^2}$ by $(P, Q) \in E'^2_0 \mapsto (P+Q, [i](P-Q))$. Transporting $W[i]$ via Γ_0 we obtain that $W'[i](P, Q) = (-Q, P)$ on $W'E'_0 \simeq E'^2_0$. Beware that this is a different automorphism than γ'_0 above, specific to $W'E'_0$. The automorphism $[i]$ that we will construct on our fourfold uses γ'_0 .

We are now ready to construct an anti-dual automorphism $[\mathbf{i}]$ of order 4 on $X_{AB} := \text{MIKE}(E_A, E_B) = (I_A \otimes_R I_B) \cdot_R E'_0$, where I_A and I_B are left $\mathcal{O}_0$ -ideals corresponding to the public keys $E_A := I_A \cdot_{\mathcal{O}_0} E'_0$ and $E_B := I_B \cdot_{\mathcal{O}_0} E'_0$. First, we construct such an automorphism $[\mathbf{i}]_A$ on $W'(E_A)^2$ as follows $[\mathbf{i}]_A : (P, Q) \in W'(E_A)^2 \mapsto (-\gamma'_A(Q), \gamma'_A(P)) \in W'(E_A)^2$. Since $\gamma'^2_A = [1]$, we obtain that $[\mathbf{i}]^2_A = [-1]_A$ and since $\tilde{\gamma}'_A = \gamma'_A$, we also have $[\tilde{\mathbf{i}}]_A = -[\mathbf{i}]_A$, as desired.

Example G.1. When $E_A = E'_0$, we have $(W'(E'_0))^2 \simeq E'^4_0$, and via the isomorphism $W'(E'_0) \simeq E'^2_0$, γ'_0 is given by $(P, Q) \mapsto ([\mathbf{i}]Q, [-\mathbf{i}]P)$ by [Lemma G.2](#). It follows that the desired automorphism is $[\mathbf{i}]_0 : (W'(E'_0))^2 \rightarrow (W'(E'_0))^2, (P_1, P_2, P_3, P_4) \mapsto ([\mathbf{i}]P_4, -[\mathbf{i}]P_3, -[\mathbf{i}]P_2, [\mathbf{i}]P_1)$.

We then obtain the desired automorphism $[\mathbf{i}]_A$ on X_{AB} by descent of $[\mathbf{i}]$ on $W'(E_A)$ via the isogeny $F_B : W'(E_A)^2 \rightarrow X_{AB}$ induced by the R -module action by $M_B = I_B$. [Proposition 4.1](#) then follows immediately.

Proposition G.1. *Let I_A, I_B be two quaternionic ideals of norms non-divisible by p , and $X_{AB} = (I_A \otimes_R I_B) \cdot_R E'_0$ be the abelian fourfold given by the MIKE key exchange from E_A, E_B . Then there exists an automorphism $[\mathbf{i}]$ on X_{AB} defined over $\mathbb{F}_{p^2}$, with $[\tilde{\mathbf{i}}] = [-\mathbf{i}]$, $[\mathbf{i}]^2 = [-1]$, and such that X_{AB} is of Weil type.*

Proof. We prove that $\ker(F_B)$ is stable by the action by $[\mathbf{i}]_A : (P, Q) \in W'(E_A)^2 \mapsto (-\gamma'_A(Q), \gamma'_A(P)) \in W'(E_A)^2$. As we have seen in [Example 2.2](#), if we write $I_B = \mathcal{O}_0\langle N, \alpha + \beta\mathbf{i} \rangle$ with $N \in \mathbb{Z}_{>0}$, $\alpha, \beta \in R$, then F_B has kernel $\ker(\Phi) \cap E'_0[N]$ with

$$\Phi = \begin{pmatrix} \iota(\alpha) & \iota(\beta) \\ -\iota(\bar{\beta}) & \iota(\bar{\alpha}) \end{pmatrix},$$

and $\iota : R \hookrightarrow \text{End}(W'(E_A))$ the R -orientation of $W'(E_A)$, which is induced by the p -Frobenius by [Lemma C.2.\(iii\)](#). Then, if $(P, Q) \in \ker(F_B)$, we have $[\alpha]P + [\beta]Q = 0$ and $-\bar{[\beta]}P + \bar{[\alpha]}Q = 0$, so that

$$\begin{aligned} -\iota(\alpha) \circ \gamma'_A(Q) + \iota(\beta) \circ \gamma'_A(P) &= \gamma'_A(\iota(\bar{\beta})(P) - \iota(\bar{\alpha})(Q)) = 0 \\ \iota(\bar{\beta}) \circ \gamma'_A(Q) + \iota(\bar{\alpha}) \circ \gamma'_A(P) &= \gamma'_A(\iota(\alpha)(P) + \iota(\beta)(Q)) = 0, \end{aligned}$$

where we used the fact that γ'_A anti-commutes with the p -Frobenius ([Remark G.1](#)) and that ι is induced by the p -Frobenius.

This proves that $\ker(F_B)$ is indeed stable by $[\mathbf{i}]_A$, from which follows that $F_B \circ [\mathbf{i}]_A$ factors through F_B . By equality of the degrees, we obtain that there exists an automorphism $[\mathbf{i}]$ of X_{AB} such that $[\mathbf{i}] \circ F_B = F_B \circ [\mathbf{i}]_A$. The equalities $[\mathbf{i}] = [-\mathbf{i}]$, $[\mathbf{i}]^2 = [-1]$ immediately follow since they are satisfied by $[\mathbf{i}]_A$.

For the tangent space, we see immediately that $[\mathbf{i}]_0 : (W'(E'_0))^2 \rightarrow (W'(E'_0))^2, (P_1, P_2, P_3, P_4) \mapsto ([\mathbf{i}]P_4, -[\mathbf{i}]P_3, -[\mathbf{i}]P_2, [\mathbf{i}]P_1)$ from [Example G.1](#) has two eigenvalues $\mathbf{i}$ and two eigenvalues $-\mathbf{i}$ (with multiplicity) on the tangent space at the origin. Now, by functoriality of the canonical involution ([Remark G.1](#)) and by construction of $[\mathbf{i}]_A$, we see that $[\mathbf{i}]_A \circ W'(\varphi_A) = W'(\varphi_A) \circ [\mathbf{i}]_0$, where φ_A is the isogeny corresponding to the left $\mathcal{O}_0$ -ideal action by I_A . By separability of $W'(\varphi_A)$ (since $p \nmid \text{nrd}(I_A)$), $[\mathbf{i}]_A$ is similar to $[\mathbf{i}]_0$ on the tangent space at the origin. An analogue argument involving F_B instead of $W'(\varphi_A)$ ensures that $[\mathbf{i}]$ is similar to $[\mathbf{i}]_A$ on the tangent space at the origin, which completes the proof that X_{AB} is of Weil type. $\square$

Note that the above results are more general than in the MIKE setting because we do not assume that $\text{nrd}(I_A)$ and $\text{nrd}(I_B)$ are powers of 2. However, we now specialise to the MIKE setting ($\text{nrd}(I_A) = \text{nrd}(I_B) = 2^e$) to compute the action of $[\mathbf{i}]$ on the symplectic basis from [Theorem 4.1](#), which will be related to the action of $[\mathbf{i}]$ on our level-2 theta structures throughout the isogeny chain computation.

Now recall that from [Appendix F](#), the MIKE 2^e -isogeny $F_A : (W'(E_B))^2 \rightarrow X_{AB} = \text{MIKE}(E_A, E_B)$ can be built from a 2^e -isogeny $F'_A : W(E_B)^2 \rightarrow X_{AB}$ instead, because F_A factors through Δ : we have $F_A \circ \text{Diag}(\Gamma_A, \Gamma_A) = F'_A \circ \Delta$.

Remark that we can also define $[\mathbf{i}]$ on $W(E_B)^2$ by $[\mathbf{i}](P, Q) = (\gamma_B(Q), -\gamma_B(P))$. Explicitly, over $\mathbb{F}_{p^2}$ we have $W(E_B)^2 = (E_B \times E_B^\sigma)^2$ and $[\mathbf{i}](P_1, P_2, Q_1, Q_2) = (-Q_1, Q_2, P_1, -P_2)$. By the construction of the canonical involution in [Lemma G.1](#), we have that $[\mathbf{i}]_B \circ \text{Diag}(\Gamma_B, \Gamma_B) = \text{Diag}(\Gamma_B, \Gamma_B) \circ [\mathbf{i}]$ so $[\mathbf{i}]_B$ defined earlier descends from $[\mathbf{i}]$ through $\text{Diag}(\Gamma_B, \Gamma_B)$, where $\Gamma_B : W(E_B) \rightarrow W'(E_B)$ is Scholten's gluing 2-isogeny. Besides, on the square $W(E_B)^2$, we have the isogeny $\Delta(P, Q) = (P + Q, P - Q)$, and we see that $\Delta \circ [\mathbf{i}] = -[\mathbf{i}] \circ \Delta$.

Now, by the computations above, we have that $[\mathbf{i}]$ on X_{AB} , which is the descent of $[\mathbf{i}]$ on $(W'(E_A))^2$ through F_A , is also the descent of $[\mathbf{i}]$ on $W(E_A)^2$ through F'_A .

Corollary G.1. *If $X_{AB} = \text{MIKE}(E_A, E_B)$, then the Weil-Cartier pairing $e_{1+\mathbf{i}} : X[1+\mathbf{i}] \times X[1+\mathbf{i}] \rightarrow \mu_2$ is alternate.*

Proof. Let $(S_1, S_2, S_3, S_4, T_1, T_2, T_3, T_4)$ be the symplectic basis of $W(E_A)^2[2^{e+2}]$ from [Theorem 4.1](#). Then by the definition of $[\mathbf{i}]$ on $W(E_A)^2$, $[\mathbf{i}]T_1 = [x_A]T_4$, $[\mathbf{i}]T_2 = -[x_A]T_3$, $[\mathbf{i}]S_1 = [\chi_A]S_4$, $[\mathbf{i}]S_2 = -[\chi_A]S_3$. In particular, since x_A is odd, the kernel $\langle [4]T_1, [4]T_2, [4]T_3, [4]T_4 \rangle$ of F'_A is a $(\mathbb{Z}/2^e\mathbb{Z})[\mathbf{i}]$ -module of rank 2, generated by $[4]T_1, [4]T_2$.

If $P, Q \in X_{AB}[1+\mathbf{i}] \subset X_{AB}[2]$, then because $2 = (1-\mathbf{i})(1+\mathbf{i})$, we have $e_{1+\mathbf{i}}(P, Q) = e_2(P, Q_0) = e_2(P, Q_0)$ for $Q_0 \in E[2]$ with $[1-\mathbf{i}]Q_0 = [1+\mathbf{i}]Q_0 = Q$. In particular, $e_{1+\mathbf{i}}(P, P) = e_2(P, P_0) = e_2([\mathbf{i}]P_0, P_0)$ where $[1+\mathbf{i}]P_0 = P$. Because F'_A commutes with $[\mathbf{i}]$ and is a 2^e -isogeny, we also have, if $P_0 = F'_A(P_1)$, $e_2([\mathbf{i}]P_0, P_0) = e_{2e+1}([\mathbf{i}]P_1, P_1)$. Hence, the action of $[\mathbf{i}]$ on $W(E_A)^2[2^{e+2}]$ shows that $e_2([\mathbf{i}]P_0, P_0) = 1$ for all $P_0 \in X_{AB}[2]$. $\square$

Remark G.3. The same result holds for all the intermediate fourfolds obtained during the computation of the isogeny $F_A : (W'(E_A))^2 \rightarrow X_{AB}$, since they are all of the form X_{AB} for a $2^{e'}$ -isogeny $E'_0 \rightarrow E'_B$ that factorises the isogeny $E'_0 \rightarrow E'_B$.

Module interpretation of Proposition G.1. We first give a module theoretic interpretation of the canonical involution γ'_A built on $W'(E_A)$. Since γ'_A is only defined over $\mathbb{F}_{p^2}$, we need to move from R -modules to (left) $\mathcal{O}_0$ -modules (see Appendix B.6). Recall that $E_A = I_A \cdot_{\mathcal{O}_0} E'_0$ and that $W'(E_A) = M_A \cdot_R E'_0$ with $M_A = I_A$ seen as a R -module by Corollary C.2. It follows by Proposition B.2 (which can be applied to the quaternionic context by Appendix B.6) that $W'(E_A) = M'_A \cdot_{\mathcal{O}_0} E'_0$ with $M'_A = \mathcal{O}_0 \otimes_R I_A$, with the induced left $\mathcal{O}_0$ -module structure.

Beware that M'_A is an $(\mathcal{O}_0, R)$ -bimodule, where the action of $r \in R$ on the left is given by, for any $x \in I_A$, $r \cdot (a + b\mathbf{i}) \otimes x = (ra + rb\mathbf{i}) \otimes x = (ar + b\bar{r}\mathbf{i}) \otimes x$, while the action on the right is given by $(a + b\mathbf{i}) \otimes x \cdot r = (a + b\mathbf{i})r \otimes x$. In particular, we recover that $M_A \cong \{m \in M'_A, r \cdot m = m \cdot r \quad \forall r \in R\}$, which can also be seen geometrically.

Indeed, Proposition B.3.(ii) and its generalisation in the quaternionic context (Appendix B.6) imply that $M_A \simeq \text{Hom}_{\mathcal{A}_R}(W'(E_A), E'_0) = \text{Hom}_{\mathbb{F}_p}(W'(E_A), E'_0)$ and $M'_A \simeq \text{Hom}_{\mathbb{F}_{p^2}}(W'(E_A), E'_0)$. And $\text{Hom}_{\mathbb{F}_p}(W'(E_A), E'_0)$ is the submodule of $\text{Hom}_{\mathbb{F}_{p^2}}(W'(E_A), E'_0)$ made of homomorphisms commuting with the p -Frobenius *i.e.* with the R -orientations.

Corollary G.2. *With the notations above, the canonical involution $-\gamma'_A$ on $W'(E_A) = M'_A \cdot_{\mathcal{O}_0} E'_0$ constructed by Lemma G.1 is given by right multiplication by $\mathbf{i} \otimes_R \mathbf{i}$ on $M'_A := \mathcal{O}_0 \otimes_R I_A \subset \mathcal{O}_0 \otimes_R \mathcal{O}_0$.*

Proof. From the above discussion applied to $I_A = \mathcal{O}_0$, we see that $W'(E'_0) \simeq (\mathcal{O}_0 \otimes_R \mathcal{O}_0) \cdot_{\mathcal{O}_0} E'_0$ and the automorphism $[\mathbf{i}] : E'_0 \rightarrow E'_0$ corresponds to right multiplication by $\mathbf{i}$, which is indeed a morphism of left $\mathcal{O}_0$ -modules. We also have $\mathcal{O}_0 = R \oplus R\mathbf{i}$ as an R -module, so $\mathcal{O}_0 \otimes_R \mathcal{O}_0 \simeq \mathcal{O}_0 \otimes 1 \oplus \mathcal{O}_0 \otimes \mathbf{i}$ as a left $\mathcal{O}_0$ -module. Given $x \otimes 1 + y \otimes \mathbf{i} \in \mathcal{O}_0 \otimes_R \mathcal{O}_0$, we compute $(x \otimes 1 + y \otimes \mathbf{i})(\mathbf{i} \otimes \mathbf{i}) = -y\mathbf{i} \otimes 1 + x\mathbf{i} \otimes \mathbf{i}$. Unraveling the functorial construction from the proof of Theorem B.2 (which still applies in the quaternionic context), we then see that the right multiplication by $\mathbf{i} \otimes \mathbf{i}$ corresponds via the left $\mathcal{O}_0$ -module action to $W'(E'_0) \simeq E_0'^2 \rightarrow E_0'^2$, $(P, Q) \mapsto (-[\mathbf{i}]Q, [\mathbf{i}]P)$, which is the opposite of the automorphism γ'_0 from Lemma G.2.

Now, we prove that this is still true on $W'(E_A) = M'_A \cdot_{\mathcal{O}_0} E'_0$ corresponding to $M'_A = \mathcal{O}_0 \otimes_R I_A$. Let $\varphi_A : E'_0 \rightarrow E_A$ be the isogeny corresponding to the action by I_A . Then, as we have seen in the proof of Corollary 3.1³⁰, $W'(\varphi_A) : W'(E'_0) \rightarrow W'(E_A)$ corresponds to the inclusion morphism of left $\mathcal{O}_0$ -modules $j_A : M'_A \hookrightarrow \mathcal{O}_0 \otimes_R \mathcal{O}_0$. By Proposition B.3.(i), which still holds in the quaternionic context by Appendix B.6, there is a correspondence between morphisms of left $\mathcal{O}_0$ -modules

³⁰ Remark that the proof still applies in a less restrictive case than Corollary 3.1. Indeed, it still holds as long as $\ker(W(\varphi_I))$ does not intersect $\ker(\Gamma_0)$.

and $\mathbb{F}_{p^2}$ -rational morphisms of PPAVs. In particular, the functorial property $\gamma'_A \circ W'(\varphi) = W'(\varphi) \circ \gamma'_0$ that we obtained in [Remark G.1](#) yields the following commutative diagram of left $\mathcal{O}_0$ -modules:

$$\begin{array}{ccc} M'_A = \mathcal{O}_0 \otimes_R I_A & \xrightarrow{j_A} & \mathcal{O}_0 \otimes_R \mathcal{O}_0 \\ \downarrow \scriptstyle \cdot (\mathbf{i} \otimes \mathbf{i}) & & \downarrow \scriptstyle \cdot (\mathbf{i} \otimes \mathbf{i}) \\ M'_A = \mathcal{O}_0 \otimes_R I_A & \xrightarrow{j_A} & \mathcal{O}_0 \otimes_R \mathcal{O}_0 \end{array}$$

We see that the left vertical arrow corresponds to γ'_A and must be the right multiplication by $\mathbf{i} \otimes \mathbf{i}$, which proves that $\mathcal{O}_0 \otimes_R I_A$ is stable by right multiplication by $\mathbf{i} \otimes \mathbf{i}$ and completes the proof. $\square$

We now move to automorphisms involved in dimension 4. It is easier to define them first on the module side, as in [Corollary G.2](#).

Proposition G.2. *Let I_A, I_B be two quaternionic ideals, and $X_{AB} = (I_A \otimes_R I_B) \cdot_R E'_0$ be the abelian fourfold given by the **MIKE** key exchange from E_A, E_B . Then the automorphism $[\mathbf{i}]$ from [Proposition G.1](#) on X_{AB} corresponds to the right multiplication by $\mathbf{i} \otimes \mathbf{i} \otimes \mathbf{i}$ via the left $\mathcal{O}_0$ -module action.*

Proof. By [Proposition B.2](#) and [Appendix B.6](#), we have $X_{AB} = (I_A \otimes_R I_B) \cdot_R E'_0 = (\mathcal{O}_0 \otimes_R I_A \otimes_R I_B) \cdot_{\mathcal{O}_0} E'_0$. Then, by construction of the module action and [Theorem C.1](#).(ii), the sequence of inclusions

$$\mathcal{O}_0 \otimes_R I_A \otimes_R I_B \hookrightarrow \mathcal{O}_0 \otimes_R I_A \otimes_R \mathcal{O}_0 \hookrightarrow \mathcal{O}_0 \otimes_R \mathcal{O}_0 \otimes_R \mathcal{O}_0$$

corresponds to the composition

$$W'(E'_0)^2 = E_0'^4 \xrightarrow{\text{Diag}(W'(\varphi_A), W'(\varphi_A))} W'(E_A)^2 \xrightarrow{F_B} X_{AB},$$

where φ_A corresponds to the left $\mathcal{O}_0$ -ideal action by I_A and F_B corresponds to the R -module action by $M_B = I_B$. Then, by construction of $[\mathbf{i}]$ on X_{AB} , we have that $[\mathbf{i}] \circ F_B \circ \text{Diag}(W'(\varphi_A), W'(\varphi_A)) = F_B \circ \text{Diag}(W'(\varphi_A), W'(\varphi_A)) \circ [\mathbf{i}]_0$. Hence, with the same arguments we used to prove [Corollary G.2](#), it suffices to prove that $[\mathbf{i}]_0$ corresponds to the right multiplication by $\mathbf{i} \otimes \mathbf{i} \otimes \mathbf{i}$ on $\mathcal{O}_0 \otimes_R \mathcal{O}_0 \otimes_R \mathcal{O}_0$ to complete the proof.

Actually, on the module side, $E_0'^4$ corresponds (over $\mathbb{F}_{p^2}$) to $\mathcal{O}_0 \otimes_R \mathcal{O}_0 \otimes_R \mathcal{O}_0 \simeq \mathcal{O}_0 \otimes 1 \otimes 1 \oplus \mathcal{O}_0 \otimes 1 \otimes \mathbf{i} \oplus \mathcal{O}_0 \otimes \mathbf{i} \otimes 1 \oplus \mathcal{O}_0 \otimes \mathbf{i} \otimes \mathbf{i}$ and so right multiplication by $\mathbf{i} \otimes \mathbf{i} \otimes \mathbf{i}$ is given on $E_0'^4$ by $[\mathbf{i}] : (P_1, P_2, P_3, P_4) \mapsto ([\mathbf{i}]P_4, -[\mathbf{i}]P_3, -[\mathbf{i}]P_2, [\mathbf{i}]P_1)$, which is exactly $[\mathbf{i}]_0$ introduced in [Example G.1](#). $\square$

G.2 Explicit action of the automorphism in the theta model

In this section, we will freely use standard results on theta groups and theta null points, as introduced by Mumford in [Mum66]. Introduction to these concepts can be found in [Rob10; Rob21; Dar25a; Dar25b] (see also Appendix E.1 for a basic introduction).

It turns out that, in our setting, the extra automorphism $[\mathbf{i}]$ on our fourfold of Weil type X allows to fix the level-2 theta structure almost canonically. A crucial property is that the Weil-Cartier pairing $e_{1+\mathbf{i}}$ is alternate on $X[1+\mathbf{i}]$, as proven in Corollary G.1. Informally, the idea is to see the level-2 structure as some sort of level- $(1+\mathbf{i})^2$ structure, see also Appendix H.4 for a more conceptual approach.

Definition G.1. *A symmetric level-2 theta structure is said to be adapted to $[\mathbf{i}]$ if it is induced by a symplectic basis $(U'_1, U'_2, U'_3, U'_4, U_1, U_2, U_3, U_4)$, of $(X[4], e_4)$, such that, if $T_j = [2]U_j, T'_j = [2]U'_j$, we have:*

- (T_1, T_2, T_3, T_4) is a symplectic basis of $(X[1+\mathbf{i}], e_{1+\mathbf{i}})$. In particular, $[\mathbf{i}]T_j = T'_j$
- $[1-\mathbf{i}]T'_1 = T_3, [1-\mathbf{i}]T'_2 = T_4, [1-\mathbf{i}]T'_3 = T_1, [1-\mathbf{i}]T'_4 = T_2$
- $[1+\mathbf{i}]U_1 = T'_3, [1+\mathbf{i}]U_2 = T'_4, [1+\mathbf{i}]U_3 = T'_1, [1+\mathbf{i}]U_4 = T'_2$.
- $[1-\mathbf{i}]U'_1 = -U_3, [1-\mathbf{i}]U'_2 = -U_4, [1-\mathbf{i}]U'_3 = -U_1, [1-\mathbf{i}]U'_4 = -U_2$.

It is furthermore said to be adapted to $([\mathbf{i}], \pi_p)$, where π_p is the p -Frobenius endomorphism of X , if U_1, U_2, U_3, U_4 are eigenvectors of eigenvalues ± 1 for $[\mathbf{i}] \circ \pi_p$ and U'_1, U'_2, U'_3, U'_4 are eigenvectors of eigenvalues ± 1 for π_p .

Remark G.4. The last condition on the U'_i is in fact enough to have the first three conditions. Indeed, since $2 = (1+\mathbf{i})(1-\mathbf{i})$, from $[1-\mathbf{i}]U'_1 = -U_3$ we get $[1+\mathbf{i}]U_3 = -[2]U'_1 = T'_1$, and also $[1-\mathbf{i}]T'_1 = T_3$. From this we deduce that (T_1, T_2, T_3, T_4) is a symplectic basis of $(X[1+\mathbf{i}], e_{1+\mathbf{i}})$.

Remark G.5. Recall that if a 4-torsion point U above $[2]U$ induces a symmetric level-2 theta group element g_U , then given $T \in X[2]$, $U + T$ induces the symmetric theta group element $g_{U+T} = e_2([2]U, T)g_U$. We also have that if the four torsion points U_1, U_2 induce the symmetric theta group elements g_1, g_2 above $[2]U_1, [2]U_2$, then $U_1 + U_2$ induces the theta group element $g_{U_1+U_2} = (g_1 g_2) / e_4(U_1, U_2)$. All this can be easily proved using the cubical arithmetic reinterpretation of the theta group action from [Rob24a, § 6.2].

For instance, in the situation of Definition G.1, we have $g_{[\mathbf{i}]U_1} = g_{U_1}$, $g_{[1+\mathbf{i}]U'_1} = g_{U_3}$, and $g_{[\mathbf{i}]U'_1} = g_{U'_1+U_3} = g_{U'_1} g_{U_3}$.

Remark G.6. Although the conditions for a symplectic basis to be $[\mathbf{i}]$ -adapted are natural, the conditions to be $([\mathbf{i}], \pi_p)$ -adapted might seem more ad-hoc. The reason for this condition is that this allows us to prove that the associated level-2 theta structure is rational (see Proposition G.3), and also that the level-2 theta structures in our dimension-4 2^e -isogeny chain are (up to a change of variable) naturally of this type by Lemma G.3. We will see in Appendix H that for our invariants, we will only need an $[\mathbf{i}]$ -adapted symplectic basis such that the associated level-2 theta structure is $\mathbb{F}_p$ -rational.

We can now study the action of $[\mathbf{i}]$ on $[\mathbf{i}]$ -adapted (and $([\mathbf{i}], \pi_p)$ -adapted) theta structures and on the level-2 theta structure of $X_{AB} = \text{MIKE}(E_A, E_B)$. Given a level-2 theta structure θ on an abelian fourfold of Weil type X , we denote the action of $[\mathbf{i}]$ as $[\mathbf{i}] \cdot \theta_j : P \in X \mapsto \theta_j([\mathbf{i}]P)$ for every index $j \in \mathbb{Z}_2^{431}$. In the following, when denoting theta coordinates, we often replace the index j by the integer $\sum_{m=0}^3 j_m 2^m$ in binary decomposition.

Proposition G.3. *Let $(\theta_0, \dots, \theta_{15})$ be the theta coordinates associated to an $[\mathbf{i}]$ -adapted symplectic basis. $(U'_1, U'_2, U'_3, U'_4, U_1, U_2, U_3, U_4)$. Then the action of $[\mathbf{i}]$ is given by $[\mathbf{i}] \cdot (\theta_{00} : \theta_{01} : \theta_{02} : \theta_{03} : \theta_{04} : \theta_{05} : \theta_{06} : \theta_{07} : \theta_{08} : \theta_{09} : \theta_{10} : \theta_{11} : \theta_{12} : \theta_{13} : \theta_{14} : \theta_{15}) = (\theta_{00} : \theta_{01} : \theta_{02} : \theta_{03} : \theta_{04} : -\theta_{05} : \theta_{06} : -\theta_{07} : \theta_{08} : \theta_{09} : -\theta_{10} : -\theta_{11} : \theta_{12} : -\theta_{13} : -\theta_{14} : \theta_{15})$. In particular, the theta null point is of the form $(b_{00} : b_{01} : b_{02} : b_{03} : b_{04} : 0 : b_{06} : 0 : b_{08} : b_{09} : 0 : 0 : b_{12} : 0 : 0 : b_{15})$.*

If furthermore we have an $([\mathbf{i}], \pi_p)$ -adapted symplectic basis, then these theta coordinates are $\mathbb{F}_p$ -rational.

Proof. We can proceed as in [Lemma F.6](#). It suffices to look at how $[\mathbf{i}]$ acts on our $[\mathbf{i}]$ -adapted symplectic basis and to apply the theta transformation formula from [\[Dar25b, Theorem 6.2.10\]](#). More precisely, the symplectic change of basis matrix from $(U'_1, U'_2, U'_3, U'_4, U_1, U_2, U_3, U_4)$ to $([\mathbf{i}]U'_1, [\mathbf{i}]U'_2, [\mathbf{i}]U'_3, [\mathbf{i}]U'_4, [\mathbf{i}]U_1, [\mathbf{i}]U_2, [\mathbf{i}]U_3, [\mathbf{i}]U_4)$ is given by:

$$\mathbf{N} := \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 1 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix},$$

Then, by [\[Dar25b, Theorem 6.2.10\]](#), the associated change of theta coordinates is given (up to a projective factor) by:

$$\mathbf{M}_{\mathbf{N}} = \text{Diag}(1, 1, 1, 1, 1, -1, 1, -1, 1, 1, -1, -1, 1, -1, -1, 1).$$

The expression of the $[\mathbf{i}] \cdot \theta_j$ and of the theta null point (stable by action by $[\mathbf{i}]$) follow.

We also provide an alternate proof “by hand” using the action by theta group symmetric elements (which is key to the proof of [\[Dar25b, Theorem 6.2.10\]](#) itself). It is a standardly known fact in Mumford’s theory of theta coordinates that θ_0 and $[\mathbf{i}] \cdot \theta_0$ are the unique functions on X (up to a projective factor) that are invariant under the action of $g_{U_1}, \dots, g_{U_4}$ and $g_{[\mathbf{i}]U_1}, \dots, g_{[\mathbf{i}]U_4}$ respectively. Since $g_{[\mathbf{i}]U_1} = g_{U_1}$ by [Remark G.5](#), and similarly for $[\mathbf{i}]U_2, [\mathbf{i}]U_3$ and $[\mathbf{i}]U_4$, we obtain that $[\mathbf{i}] \cdot \theta_0 = \theta_0$. Then, we can use the fact that the action of $g_{[\mathbf{i}]U'_1}, \dots, g_{[\mathbf{i}]U'_4}$ on

³¹ The notation $[\mathbf{i}]^* \theta_j$ may also be found in the literature.

$[\mathbf{i}] \cdot \theta_0 = \theta_0$ spans all the other theta coordinates $[\mathbf{i}] \cdot \theta_j$ as follows (see [Dar25b, Eq. (5.11)] and Remark G.5):

$$\begin{aligned}
 [\mathbf{i}] \cdot \theta_1 &= g_{[\mathbf{i}]U'_1} \cdot [\mathbf{i}] \cdot \theta_0 = g_{U'_1+U_3} \cdot \theta_0 = g_{U'_1} \cdot g_{U_3} \cdot \theta_0 = g_{U'_1} \cdot \theta_0 = \theta_1, \\
 [\mathbf{i}] \cdot \theta_2 &= g_{[\mathbf{i}]U'_2} \cdot [\mathbf{i}] \cdot \theta_0 = g_{U'_2+U_4} \cdot \theta_0 = g_{U'_2} \cdot g_{U_4} \cdot \theta_0 = g_{U'_2} \cdot \theta_0 = \theta_2, \\
 [\mathbf{i}] \cdot \theta_3 &= g_{[\mathbf{i}]U'_2} \cdot [\mathbf{i}] \cdot \theta_1 = g_{U'_2} \cdot g_{U_4} \cdot \theta_1 = g_{U'_2} \cdot \theta_1 = \theta_3, \\
 [\mathbf{i}] \cdot \theta_4 &= g_{[\mathbf{i}]U'_3} \cdot [\mathbf{i}] \cdot \theta_0 = g_{U'_3+U_1} \cdot \theta_0 = g_{U'_3} \cdot g_{U_1} \cdot \theta_0 = g_{U'_3} \cdot \theta_0 = \theta_4, \\
 [\mathbf{i}] \cdot \theta_5 &= g_{[\mathbf{i}]U'_3} \cdot [\mathbf{i}] \cdot \theta_1 = g_{U'_3} \cdot g_{U_1} \cdot \theta_1 = -g_{U'_3} \cdot \theta_1 = -\theta_5, \\
 [\mathbf{i}] \cdot \theta_6 &= g_{[\mathbf{i}]U'_3} \cdot [\mathbf{i}] \cdot \theta_2 = g_{U'_3} \cdot g_{U_1} \cdot \theta_2 = g_{U'_3} \cdot \theta_2 = \theta_6, \\
 [\mathbf{i}] \cdot \theta_7 &= g_{[\mathbf{i}]U'_3} \cdot [\mathbf{i}] \cdot \theta_3 = g_{U'_3} \cdot g_{U_1} \cdot \theta_3 = -g_{U'_3} \cdot \theta_3 = -\theta_7, \\
 [\mathbf{i}] \cdot \theta_8 &= g_{[\mathbf{i}]U'_4} \cdot [\mathbf{i}] \cdot \theta_0 = g_{U'_4+U_2} \cdot \theta_0 = g_{U'_4} \cdot g_{U_2} \cdot \theta_0 = g_{U'_4} \cdot \theta_0 = \theta_8, \\
 [\mathbf{i}] \cdot \theta_9 &= g_{[\mathbf{i}]U'_1} \cdot [\mathbf{i}] \cdot \theta_8 = g_{U'_1} \cdot g_{U_3} \cdot \theta_8 = g_{U'_1} \cdot \theta_8 = \theta_9, \\
 [\mathbf{i}] \cdot \theta_{10} &= g_{[\mathbf{i}]U'_2} \cdot [\mathbf{i}] \cdot \theta_8 = g_{U'_2} \cdot g_{U_4} \cdot \theta_8 = -g_{U'_2} \cdot \theta_8 = -\theta_{10}, \\
 [\mathbf{i}] \cdot \theta_{11} &= g_{[\mathbf{i}]U'_1} \cdot [\mathbf{i}] \cdot \theta_{10} = -g_{U'_1} \cdot g_{U_3} \cdot \theta_{10} = -g_{U'_1} \cdot \theta_{10} = -\theta_{11}, \\
 [\mathbf{i}] \cdot \theta_{12} &= g_{[\mathbf{i}]U'_3} \cdot [\mathbf{i}] \cdot \theta_8 = g_{U'_3} \cdot g_{U_1} \cdot \theta_8 = g_{U'_3} \cdot \theta_8 = \theta_{12}, \\
 [\mathbf{i}] \cdot \theta_{13} &= g_{[\mathbf{i}]U'_1} \cdot [\mathbf{i}] \cdot \theta_{12} = g_{U'_1} \cdot g_{U_3} \cdot \theta_{12} = -g_{U'_1} \cdot \theta_{12} = -\theta_{13}, \\
 [\mathbf{i}] \cdot \theta_{14} &= g_{[\mathbf{i}]U'_2} \cdot [\mathbf{i}] \cdot \theta_{12} = g_{U'_2} \cdot g_{U_4} \cdot \theta_{12} = -g_{U'_2} \cdot \theta_{12} = -\theta_{14}, \\
 [\mathbf{i}] \cdot \theta_{15} &= g_{[\mathbf{i}]U'_1} \cdot [\mathbf{i}] \cdot \theta_{14} = -g_{U'_1} \cdot g_{U_3} \cdot \theta_{14} = g_{U'_1} \cdot \theta_{14} = \theta_{15}.
 \end{aligned}$$

So we obtain the same result.

A similar proof shows that the theta coordinates are $\mathbb{F}_p$ -rational for a $([\mathbf{i}], \pi_p)$ -adapted symplectic basis. It suffices to check that the action of π_p leaves theta coordinates invariant, and we compute for that the symmetric theta group elements associated to the $\pi_p(U_m), \pi_p(U'_m)$. By assumption, we have $\pi_p(U'_m) = \pm U'_m$ and $\pi_p(U_m) = \pm [\mathbf{i}]U_m$ for all $1 \leq m \leq 4$. It follows that for all $1 \leq m \leq 4$, $g_{\pi_p(U'_m)} = g_{U'_m}$ or $g_{\pi_p(U'_m)} = g_{-U'_m} = g_{U'_m+2[U'_m]} = g_{U'_m}$ by Remark G.5. Similarly, $g_{\pi_p(U_m)} = g_{[\mathbf{i}]U_m} = g_{U_m}$ or $g_{\pi_p(U_m)} = g_{-[\mathbf{i}]U_m} = g_{[2\mathbf{i}]U_m+[\mathbf{i}]U_m} = g_{[\mathbf{i}]U_m} = g_{U_m}$ for all $1 \leq m \leq 4$. Since two symplectic basis of $X[4]$ inducing the same symmetric elements induce the same theta structure, we conclude that $\pi_p \cdot \theta_j = \theta_j$ for all $0 \leq j \leq 15$, which completes the proof. $\square$

Lemma G.3. *Let $X_{AB} = \text{MIKE}(E_A, E_B)$ be the MIKE fourfold and $(S_1, S_2, S_3, S_4, T_1, T_2, T_3, T_4) = (F'_A)_*(\mathcal{B}_B)$ the symplectic basis of $X_{AB}[4]$ induced by the initial basis $\mathcal{B}_B$ of $W(E_B)^2[2^{e+2}]$ from Theorem 4.1 which is used to represent the theta null point of X_{AB} .*

Then $(S_1, S_2, T_4, T_3, T_1+T_4, T_2-T_3, S_1-S_4, -S_2-S_3)$ is an $([\mathbf{i}], \pi_p)$ -adapted symplectic basis.

Proof. Using the action of $[\mathbf{i}]$ on $\mathcal{B}_B$ that we computed in Corollary G.1, and the fact that $[\mathbf{i}]$ commutes with F'_A by construction (Proposition G.1), we obtain that $[\mathbf{i}]T_1 = [x_A]T_4$, $[\mathbf{i}]T_2 = -[x_A]T_3$, $[\mathbf{i}]S_1 = [\chi_A]S_4$, $[\mathbf{i}]S_2 = -[\chi_A]S_3$ with

$x_A \equiv \chi_A \equiv \pm 1 \pmod{4}$. It follows that $[\mathbf{i}]T_3 = [\chi_A]T_2$, $[\mathbf{i}]T_4 = -[\chi_A]T_1$, $[\mathbf{i}]S_3 = [x_A]S_2$ and $[\mathbf{i}]S_4 = -[x_A]S_1$. Similarly, since the kernel of F'_A is stable by the p -Frobenius, it commutes with F'_A , and we obtain from the p -Frobenius action on $\mathcal{B}_B$ from [Theorem 4.1](#) that $\pi_p(T_1) = T_1, \pi_p(T_2) = T_2, \pi_p(T_3) = -T_3, \pi_p(T_4) = -T_4, \pi_p(S_1) = -S_1, \pi_p(S_2) = -S_2, \pi_p(S_3) = S_3, \pi_p(S_4) = S_4$. An easy computation then shows that $(S_1, S_2, T_4, T_3, T_1 + T_4, T_2 - T_3, S_1 - S_4, -S_2 - S_3)$ is an $([\mathbf{i}], \pi_p)$ -adapted symplectic basis. $\square$

Corollary G.3. *Let $(x_{00}, \dots, x_{15})$ be the theta coordinates adapted to the MIKE isogenies (induced by $(F'_A)_*(\mathcal{B}_B)$ on $X_{AB}[4]$ with the notations from [Lemma G.3](#)), and $(y_{00}, \dots, y_{15})$ be the theta coordinates of the $([\mathbf{i}], \pi_p)$ -adapted symplectic basis from [Lemma G.3](#). Then the change of theta coordinates is given by:*

$$\begin{array}{ll} y_{00} = x_{00} + x_{09} + x_{06} + x_{15} & y_{08} = x_{00} + x_{09} - x_{06} - x_{15} \\ y_{01} = x_{01} + x_{08} + x_{07} + x_{14} & y_{09} = x_{01} + x_{08} - x_{07} - x_{14} \\ y_{02} = x_{02} + x_{11} + x_{04} + x_{13} & y_{10} = x_{02} + x_{11} - x_{04} - x_{13} \\ y_{03} = x_{03} + x_{10} + x_{05} + x_{12} & y_{11} = x_{03} + x_{10} - x_{05} - x_{12} \\ y_{04} = x_{00} - x_{09} + x_{06} - x_{15} & y_{12} = x_{00} - x_{09} - x_{06} + x_{15} \\ y_{05} = x_{01} - x_{08} + x_{07} - x_{14} & y_{13} = x_{01} - x_{08} - x_{07} + x_{14} \\ y_{06} = x_{02} - x_{11} + x_{04} - x_{13} & y_{14} = x_{02} - x_{11} - x_{04} + x_{13} \\ y_{07} = x_{03} - x_{10} + x_{05} - x_{12} & y_{15} = x_{03} - x_{10} - x_{05} + x_{12} \end{array}$$

In particular, it follows by [Proposition G.3](#) that,

$$[\mathbf{i}](x_{00} : x_{01} : x_{02} : x_{03} : x_{04} : x_{05} : x_{06} : x_{07} : x_{08} : x_{09} : x_{10} : x_{11} : x_{12} : x_{13} : x_{14} : x_{15}) = (x_{00} : x_{08} : x_{04} : x_{12} : x_{02} : x_{10} : x_{06} : x_{14} : x_{01} : x_{09} : x_{05} : x_{13} : x_{03} : x_{11} : x_{07} : x_{15}). \quad (22)$$

Proof. This follows from applying the theta transformation formula from [\[Dar25b, Theorem 6.2.10\]](#) to the symplectic change of basis from [Lemma G.3](#).

We give an alternate proof below based on the theta group action (similar to the proof of [Proposition G.3](#)) and the trace method of [\[Rob10, § 3.5\]](#). First, the theta coordinates adapted to the MIKE isogenies are the ones induced by the symplectic basis $S_1, S_2, S_3, S_4, T_1, T_2, T_3, T_4$. By definition of the theta coordinates associated to this symplectic decomposition, we have that x_{00} is invariant by the g_{T_i} and $x_{01} = g_{S_1} \cdot x_{00}, x_{02} = g_{S_2} \cdot x_{00}, x_{04} = g_{S_3} \cdot x_{00}, x_{08} = g_{S_4} \cdot x_{00}, \dots$

Now recall by [Remark G.5](#) that if the four-torsion points U_1, U_2 induce the symmetric theta group elements g_1, g_2 above $T_i = 2U_i$, then $U_1 + U_2$ induces the theta group element $(g_1 g_2)/e_4(U_1, U_2)$. It follows that the symmetric elements associated to $-T_1 - T_4, T_3 - T_2, S_4 - S_1, S_2 + S_3$ are given by $g_{T_1} g_{T_4}, g_{T_3} g_{T_2}, g_{S_4} g_{S_1}, g_{S_2} g_{S_3}$ respectively.

Since y_0 should be invariant by the subgroup generated by all of these, we can take the trace:

$$y_{00} = x_{00} + g_{S_4} g_{S_1} \cdot x_{00} + g_{S_2} g_{S_3} \cdot x_{00} + g_{S_1} g_{S_2} g_{S_3} g_{S_4} \cdot x_{00} = x_{00} + x_{06} + x_{09} + x_{15}.$$

Then we compute:

$$\begin{array}{llll}
 y_{00} = g_0 \cdot y_{00} & = x_{00} + x_{06} + x_{09} + x_{15} & y_{08} = g_{T_3} \cdot y_{00} & = x_{00} + x_{09} - x_{06} - x_{15} \\
 y_{01} = g_{S_1} \cdot y_{00} & = x_{01} + x_{08} + x_{07} + x_{14} & y_{09} = g_{T_3} \cdot y_{01} & = x_{01} + x_{08} - x_{07} - x_{14} \\
 y_{02} = g_{S_2} \cdot y_{00} & = x_{02} + x_{11} + x_{04} + x_{13} & y_{10} = g_{T_3} \cdot y_{02} & = x_{02} + x_{11} - x_{04} - x_{13} \\
 y_{03} = g_{S_1} g_{S_2} \cdot y_{00} & = x_{03} + x_{10} + x_{05} + x_{12} & y_{11} = g_{T_3} \cdot y_{03} & = x_{03} + x_{10} - x_{05} - x_{12} \\
 y_{04} = g_{T_4} \cdot y_{00} & = x_{00} - x_{09} + x_{06} - x_{15} & y_{12} = g_{T_3} g_{T_4} \cdot y_{00} & = x_{00} - x_{09} - x_{06} + x_{15} \\
 y_{05} = g_{T_4} \cdot y_{01} & = x_{01} - x_{08} + x_{07} - x_{14} & y_{13} = g_{T_3} g_{T_4} \cdot y_{01} & = x_{01} - x_{08} - x_{07} + x_{14} \\
 y_{06} = g_{T_4} \cdot y_{02} & = x_{02} - x_{11} + x_{04} - x_{13} & y_{14} = g_{T_3} g_{T_4} \cdot y_{02} & = x_{02} - x_{11} - x_{04} + x_{13} \\
 y_{07} = g_{T_4} \cdot y_{03} & = x_{03} - x_{10} + x_{05} - x_{12} & y_{15} = g_{T_3} g_{T_4} \cdot y_{03} & = x_{03} - x_{10} - x_{05} + x_{12}
 \end{array}$$

Finally, using the action of $[\mathbf{i}]$ on the y -coordinates described by [Proposition G.3](#) and using the reverse change of variables, we obtain [Equation \(22\)](#). $\square$

Note that using the little-endian binary representation for the indices $j = \sum_{m=1}^4 j_m \cdot 2^{m-1}$ of the theta coordinates adapted to the MIKE isogenies, the action of $[\mathbf{i}]$ is described by $x_{(j_1, j_2, j_3, j_4)} \mapsto x_{(j_4, j_3, j_2, j_1)}$.

The action of $[\mathbf{i}]$ extends to an action on the level-(2, 2) theta coordinates. In the following, we make this explicit by relying on an analytical argument over $\mathbb{C}$ from [\[Gee96\]](#) and lifting theory (Lefschetz' principle). In [Appendix G.3](#), we provide a purely algebraic argument based on the theory of theta characteristics (that we also introduce). First, note that the action of $[\mathbf{i}]$ of squared level-(2, 2) theta coordinates follows easily from previous results.

Lemma G.4. *Let $\theta : X \rightarrow \mathbb{P}^{15}$ be a level-2 theta structure adapted to the MIKE isogenies. Further, let $\vartheta : X \rightarrow \mathbb{P}^{255}$ be a level-(2, 2) theta structure that is compatible with the level-2 structure θ . Then the action of $[\mathbf{i}]$ extends to the squares of the level-(2, 2) coordinates in the following way:*

$$\vartheta^2 \begin{bmatrix} a_3 & a_2 & a_1 & a_0 \\ b_3 & b_2 & b_1 & b_0 \end{bmatrix} ([\mathbf{i}]P) = \vartheta^2 \begin{bmatrix} a_0 & a_1 & a_2 & a_3 \\ b_0 & b_1 & b_2 & b_3 \end{bmatrix} (P)$$

for any point $P \in X$.

Proof. To ease the notations, we use the binary representation for the level-2 coordinates here i.e. $x_j = \theta_{(j_3, j_2, j_1, j_0)}$ where $j = \sum_{m=0}^3 j_m \cdot 2^m$.

The relation between ϑ^2 and θ is given by [Equation \(17\)](#)

$$\vartheta^2 \begin{bmatrix} a \\ b \end{bmatrix} (P) = \sum_{c \in (\mathbb{Z}/2\mathbb{Z})^4} (-1)^{\langle b, c \rangle} \theta_c(P) \theta_{c+a}(0).$$

for any $P \in X$. By [Corollary G.3](#), the action of $[\mathbf{i}]$ on the level-2 coordinates is given by

$$\theta_{(j_3, j_2, j_1, j_0)}([\mathbf{i}]P) = \theta_{(j_0, j_1, j_2, j_3)}(P)$$

for any $P \in X$. The desired result follows. $\square$

[Lemma G.4](#) is actually insufficient for our needs. We shall use the following refinement, that gives the action of $[\mathbf{i}]$ on level-(2, 2) theta coordinates rather than their squares.

Lemma G.5. *With the notations of [Lemma G.4](#), the action of $[\mathbf{i}]$ on the 16 following symmetric level-(2, 2) coordinates is given by*

$$\vartheta \begin{bmatrix} a_3 & a_2 & a_1 & a_0 \\ b_3 & b_2 & b_1 & b_0 \end{bmatrix} ([\mathbf{i}]P) = (-1)^{a_0b_0+a_1b_1} \vartheta \begin{bmatrix} a_0 & a_1 & a_2 & a_3 \\ b_0 & b_1 & b_2 & b_3 \end{bmatrix} (P)$$

for any point $P \in X$.

Proof. Over $\mathbb{C}$, this is [[Gee96](#), Lemma 2.3], (see also [[Gee96](#), p.623], which also gives the vanishing of the six theta null values from our low, taking into account that we use slightly different numbering).

Even though we work over a finite field, one can still invoke [[Gee96](#)] using standard lifting arguments. Indeed, we can lift the PPAV of Weil type $(X, \lambda_X, [\mathbf{i}])$, which is defined over $\mathbb{F}_{p^2}$ (remember that although (X, λ_X) is $\mathbb{F}_p$ -rational, $[\mathbf{i}]$ is defined over $\mathbb{F}_{p^2}$) to $\mathbb{Z}_{p^2}$, the ring of Witt vectors of $\mathbb{F}_{p^2}$.

Such lifts can be described by combining Serre-Tate theory with Grothendieck-Messing, see for instance the quick summary in [[PRS26](#), Appendix B], or [[Cha12](#), § 2] for a more detailed summary. It suffices to take an admissible lift of the Hodge filtration from $H_{dR}^1(X/\mathbb{F}_{p^2})$ to $H_{crys}^1(X, \mathbb{Z}_{p^2})$ that is stable by $[\mathbf{i}]$ and compatible with the polarisation on $H_{crys}^1(X, \mathbb{Z}_{p^2})$ induced by the principal polarisation on X and the canonical duality of [[Cha12](#), Theorem 2.11].

Then by the theory above, we obtain a lift $\tilde{X}/\mathbb{Z}_{p^2}$ of X ; the polarisation lifts because our filtration is compatible with it; and $[\mathbf{i}]$ lifts because the decomposition is stable by $[\mathbf{i}]$.

Finally, the generic fiber $\mathcal{X}/\mathbb{Q}_{p^2}$ of $\tilde{X}/\mathbb{Q}_{p^2}$ is of Weil type, because for the action of $[\mathbf{i}]$ on the tangent space, the multiplicities of the eigenvalues $\mathbf{i}$ and $-\mathbf{i}$ is equal (because this is the case modulo p).

Then we invoke Lefschetz' principle (or simply embed $\mathbb{Q}_{p^2}$ into $\mathbb{C}$), and the fact that $\tilde{X}/\mathbb{Z}_{p^2}$ can be recovered as the Néron model of $\mathcal{X}$.

□

From [Lemma G.5](#), we immediately obtain the following.

Corollary G.4. *Let $\theta : X \rightarrow \mathbb{P}^{15}$ be a level-2 theta structure adapted to the MIKE isogenies, and let $\vartheta : X \rightarrow \mathbb{P}^{255}$ be a compatible level-(2, 2) theta structure. Then the theta null values corresponding to the following six indices vanish:*

$$\begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}.$$

Moreover, the theta functions corresponding to the following ten indices are invariant under the action of $[\mathbf{i}]$:

$$\begin{aligned} & \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \\ & \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}. \end{aligned}$$

G.3 Theta characteristics

We finish this section with more technical tools, which will be used to prove a weaker version of [Lemma G.5](#) with a purely algebraic argument but also further results in [Appendix H](#). Namely, it will be used to prove [Lemma H.3](#), which gives the stronger version [Theorem H.1](#) of [Theorem 4.2](#), but the later version is all we need for MIKE. We stress that these results are not needed to understand the invariant computation, and the reader can safely skip this section.

Unfortunately, although the statements below are probably folklore, we do not know of a nice reference. Over $\mathbb{C}$, they can be proved by analytic arguments, using [\[BL04, § 4.6, § 4.7, Exercices 4.12.11, 4.12.12, 4.12.14\]](#). Over a general field, they are implicit in the work of Mumford ([\[Mum66\]](#)) and Kempf ([\[Kem89\]](#)). We will only sketch the proofs in the arguments below, because detailed arguments would make this section too technical.

Given a PPAV (A, λ_A) , a theta characteristic is a quadratic form $q : A[2] \rightarrow \{\pm 1\}$ associated to the symmetric bilinear form $e_{2\lambda_A}$. To a theta characteristic, one can associate its (multiplicative) Arf invariant, a value in $\{\pm 1\}$.

Furthermore, we recall that an even theta characteristic q can always be written as $q(x) = e_2(x_1, x_2)$, for $A[2] = K_1 \oplus K_2$ a given symplectic decomposition, and $x_i \in K_i$. We note that another symplectic decomposition $A[2] = K'_1 \oplus K'_2$ give exactly the same q if and only if $q(K'_i) = 1$.

We refer to [\[Far12, § 1-2\]](#) for more details.

Given a symmetric line bundle $\mathcal{L}$ whose associated polarisation $\Phi_{\mathcal{L}}$ is λ_A , we can associate a theta characteristic $q_{\mathcal{L}}(x) = (-1)^{\text{mult}_x(D) - \text{mult}_0(D)}$ where D is a symmetric divisor representing $\mathcal{L}$ by [\[Mum66, Proposition 2 p.307\]](#).

Proposition G.4. *The map $\mathcal{L} \rightarrow q_{\mathcal{L}}$ is rational isomorphism of $A[2]$ -torsors between the symmetric line bundles $\mathcal{L}$ representing λ_A and the theta characteristics.*

Proof. It is classical that both sets are torsors under $A[2]$. The map $\mathcal{L} \mapsto q_{\mathcal{L}}$ is a map of torsors by [\[Mum66, Properties \(ii\) and \(iv\) p. 304\]](#), so it is an isomorphism. $\square$

We will see in [Remark G.7](#) that if θ is a section of $\mathcal{L}$, θ is even if and only if $q_{\mathcal{L}}$ is even, i.e. its Arf invariant is trivial. This gives a way to represent level one theta functions, via their associated theta characteristic.

We can then revisit the construction of the theta functions θ_i of level- n associated to a symmetric theta structure in terms of theta characteristics.

We recall first the following explicit construction of level- n theta functions [Rob10, § 3.4] (for even n). Let $\mathcal{L}$ be a symmetric line bundle inducing λ_A . A symmetric level- n theta structure on the theta group $G(\mathcal{L}^n)$ is induced by a symplectic basis of $(A[n], e_{n\lambda_A})$ along with a symplectic decomposition of $A[2n] = K'_1 \oplus K'_2$ compatible with this symplectic basis. Let $K_i = 2K'_i$, so $A[n] = K_1 \oplus K_2$.

Let ϕ be the isogeny $A \rightarrow B = A/K_2$. The group K'_2 induces a symmetric lift $\tilde{K}_2$ of K_2 to the theta group, hence a descent of $\mathcal{L}^n$ to a principal symmetric line bundle $\mathcal{M}$ on B . Let $\theta_{\mathcal{M}}$ be a global section of $\mathcal{M}$, then $\theta_0 = \theta_{\mathcal{M}} \circ \phi$ is a global section of $(A, \mathcal{L}^n)$ stable under the theta group action of $\tilde{K}_2$; and for $P' \in K'_1$ and $P = [2]P' \in K_1$, with $g_{P'}$ the symmetric theta group element induced by P' , we define $\theta_P := g_{P'} \cdot \theta_0$. With a choice of group isomorphism $\mathbb{Z}_n^g \xrightarrow{\sim} K_1$, we obtain the usual numbering of theta coordinates by $\mathbb{Z}_n^g$, but for convenience, we shall keep indexing theta coordinates by points in the following.

Proposition G.5. *The theta characteristic $q_{\mathcal{M}}$ associated to $\mathcal{M}$ is the even theta characteristic induced by the symplectic decomposition $\phi(K_1)[2] \oplus \phi(K'_2)$.*

Proof. Since n is even, the theta characteristic associated to $\mathcal{L}^n$ on $A[2]$ is trivial. By [Mum66, Properties (iii)], this gives that $q_{\mathcal{M}}$ is trivial on $\phi(K_1)[2]$. The fact that $q_{\mathcal{M}}$ is also trivial on $\phi(K'_2)$ comes from the way that K'_2 gives the lift $\tilde{K}_2$ of K_2 , hence the symmetric descent $\mathcal{M}$ of $\mathcal{L}$. $\square$

We will also need the following description of theta functions of level (n, n) . We fix a symplectic basis of the $A[n^2]$ -torsion, and a symplectic decomposition $K'_1 \oplus K'_2$ of $A[2n^2]$ above it. This induces symmetric lifts $\tilde{K}_i$ of $K_i = [2]K'_i$ in the theta group $G(\mathcal{L}^{n^2})$, which in turn gives a symmetric lift $\tilde{K}_1[n] \oplus \tilde{K}_2[n]$ of $A[n]$ (which makes sense since $A[n]$ is isotropic for e_{n^2}).

Then as above $\mathcal{L}^{n^2}$ descends to a symmetric line bundle $\mathcal{M}$ on $A = A/A[n]$, which correspond to the theta characteristic associated to $[n]K'_1 \oplus [n]K'_2$, and we let $\theta_{\mathcal{M}}$ a section.

Then $\theta_{0,0} = \theta_{\mathcal{M}} \circ [n]$, and for $P = P_1 + P_2 \in A[n^2]$, $\theta_P = \theta_{P_1, P_2} = g_{P_2} \cdot g_{P_1} \cdot \theta_0$.

We remark that θ_P only depends on $[n]P$ because $\theta_{0,0}$ is invariant by $[n]$, but we warn that the order $g_{P_2} \cdot g_{P_1}$ is important because these theta group elements don't commute in general.

Remark G.7. For convenience, we give a few more details on theta characteristics that we did not find in the literature. We won't need them in the rest of the paper.

For an arbitrary line bundle $\mathcal{L}$, we still have a theta characteristic $q_{\mathcal{L}}$ on $A[2]$, whose radical is $K(\mathcal{L})[2]$. Then $G(\mathcal{L})$ admits a symmetric theta structure iff $q_{\mathcal{L}}$ is trivial on this radical. In this case, the theta characteristic descends to a non degenerate theta characteristic on $A[2]/K(\mathcal{L})[2]$, and we can define the Arf invariant of $q_{\mathcal{L}}$ as the one on $A[2]/K(\mathcal{L})[2]$.

Then if θ_i is a basis of theta functions associated to this symmetric theta structure, $[-1]^* \theta_i = \epsilon \theta_{-i}$ ([Kem89, Theorem 4]) and $\epsilon = 1$ iff θ_0 is even, iff the

effective symmetric divisor associated to θ_0 is even, iff the Arf invariant is 1, iff there are more even functions than odd functions in $\Gamma(A, \mathcal{L})$.

Indeed, by [Proposition G.5](#) we reduce to the case of a level-1 theta function, i.e. $\theta_{\mathcal{M}}$ a section of $\mathcal{M}$ associated to a principal polarisation. If $\mathcal{M}$ is the descent of a totally symmetric line bundle, $\theta_{\mathcal{M}}$ is even by [\[Kem89, Theorem 11\]](#), and the theta characteristic $q_{\mathcal{M}}$ is even by [Proposition G.5](#). From this special case we get the others using [Proposition G.4](#). The counting of even and odd coordinates come from [\[Mum66, Corollary 3 p. 315\]](#). We remark that if $q_{\mathcal{L}|K(\mathcal{L})[2]}$ is non trivial, there are as many odd as even coordinates.

A purely algebraic proof for (a weaker version of) [Lemma G.5](#). With the theory of theta characteristics, we are now able to provide a purely algebraic proof of [Lemma G.4](#) on some specific level-(2, 2) theta coordinates only.

Lemma G.6. *With the notations of [Lemma G.4](#), the action of $[\mathbf{i}]$ on the 16 following symmetric level-(2, 2) coordinates is given by*

$$\vartheta \begin{bmatrix} a_0 & a_1 & a_1 & a_0 \\ b_0 & b_1 & b_1 & b_0 \end{bmatrix} ([\mathbf{i}]P) = (-1)^{a_0 b_0 + a_1 b_1} \vartheta \begin{bmatrix} a_0 & a_1 & a_1 & a_0 \\ b_0 & b_1 & b_1 & b_0 \end{bmatrix} (P)$$

for any point $P \in X$.

Proof. We give a purely algebraic proof, using [Proposition G.4](#), see [Lemma G.5](#) for an analytic proof.

Take level-(2, 2) theta functions induced by any level-4 symmetric theta structure above the symplectic decomposition of $X[4] = K'_1 \oplus K'_2$ given by $(U'_1, U'_2, U'_3, U'_4, U_1, U_2, U_3, U_4)$ as in [Definition G.1](#). We will denote these theta functions by Θ_{P_1, P_2} for $P = P_1 + P_2 \in X[4]$. Then $\Theta_{0,0}$ is equal to $\Theta_0 \circ [2]$, where Θ_0 is the even theta function induced by the theta characteristic induced by $K_1 \oplus K_2$. And $\Theta_{P_1, P_2} = g_{P_2} \cdot g_{P_1} \cdot \Theta_{0,0}$, with the theta group elements g_{P_i} specified by the choice of level-4 symmetric theta structure.

Now by the proof of [Lemma H.3](#) below, if θ_i denote our level-2 theta functions, θ_0 is equal to $\Theta_0 \circ \phi$ where $\phi = [1 + \mathbf{i}]$. So $\Theta_{0,0} = \theta_0 \circ \tilde{\phi}$ where $\tilde{\phi} = [1 - \mathbf{i}]$. Now if $P \in K'_2$, we have $\Theta_{0,P} = g_P \cdot \Theta_{0,0} = g_P \cdot (\theta_0 \circ \tilde{\phi}) = (\tilde{\phi}(g_P) \cdot \theta_0) \circ \tilde{\phi}$. Here by abuse of notation, we also denote by $\tilde{\phi} : G(\mathcal{L}^4) \rightarrow G(\mathcal{L}^2)$ the morphism of theta groups induced by $\tilde{\phi} : (X, \mathcal{L}^4) \rightarrow (X, \mathcal{L}^2)$. Now since $\phi(g_P)$ is symmetric, it is equal to $\pm g_{\tilde{\phi}(P)}$, so we obtain $\Theta_{0,P} = \pm \theta_{\tilde{\phi}(P)} \circ \phi$. The action of $[\mathbf{i}]$ on these $\Theta_{0,P}$ is then the same as the one on the $\theta_{\tilde{\phi}(P)}$ which is described in [Proposition G.3](#), and a similar change of variable as in [Corollary G.3](#) finishes the proof. (Remark that the 16 theta characteristics above are precisely the ones that are invariant by $[\mathbf{i}]$, i.e. coming from K'_2 , since $[2]K'_2 = X[1 + \mathbf{i}]$.) $\square$

Remark G.8. We also sketch how we could extend the algebraic proof of [Lemma G.6](#) in order to prove [Lemma G.5](#) in full. First we remark that level-(2, 2) theta coordinates only exist over $\mathbb{F}_{p^2}$ because the 4-torsion needs to be rational, so $[\mathbf{i}]$ is given by a rational change of variable on these coordinates. Secondly, our given basis from [Definition G.1](#) is not enough to determine the level-(2, 2) theta

coordinates because the level-4 theta structure determines the scaling factors of our level- $(2, 2)$ theta coordinates. When the theta characteristic is of the form $(0, P_2)$, hence stable by $[\mathbf{i}]$, this scaling factor does not affect the sign. But when the theta characteristic is of the form $P = (P_1, P_2)$, with $[i](P) = (P_1, P'_1 + P_2)$, the action of $[\mathbf{i}]$ on Θ_P depends on the choice of scaling factors for P and $[\mathbf{i}](P)$. So we need to carefully check that we can make a choice of level-4 theta structure that gives the formula above. We skip this verification, because we won't need this result.

H MIKE invariants

The theta null point of an abelian fourfold determines it uniquely. The problem is that the converse is false, because the theta null point also encodes a level structure, so the same principally polarised abelian variety can admit many different theta null points. For the MIKE key-exchange, we need true modular invariants, not depending on the level structure.

In this section, we explain the construction of the (absolute) MIKE invariants (Definitions 4.2 and 4.3) and prove Theorems 4.2 and 4.3.

H.1 MIKE-invariants and Theorem 4.2

A way to find invariants would be to list all possible theta null points, and take the smallest one for some fixed ordering. For instance, on an elliptic curve the Montgomery coefficient A encodes a $\Gamma^0(4)$ -level structure, so there are 6 possible Montgomery coefficients. The smallest one provides us with a well defined modular invariant, but of course in practice it is easier to directly use the j -invariant. The problem in our case is that there are way too many level-2 theta structures for this method to be practical.

Remark H.1. We remark that the fact that the theta null point determines the principally polarised abelian variety is only proven, for n even, for $n \geq 4$, by Mumford and Kempf. The case $n = 2$ is claimed in [Man94a, Theorem 3] over $\mathbb{C}$, but the proof is incomplete, although it is conjectured to be true³². We remark that this is proven in dimension $g \leq 3$, the cases $g = 1, 2$ are standard and the case $g = 3$ is proven in [Man94b, Theorem 5] (which proves a stronger result). We will assume this conjecture through out: we remark that this is implicitly used in all isogeny-based cryptography involving dimension-four abelian varieties, since we usually represent them by their level-2 theta null points.

Another solution is as follows: from the level-2 theta null point the duplication formula gives the squares of the level- $(2, 2)$ -theta null point. Changing the theta structure permutes these squares (along with some multiplication by some power of $\mathbf{i}$). In particular, suitable Newton sums of these coefficients are true modular invariants, i.e., are of level 1. The problem is now that they do not form a

³² Manni, personal communication

complete system of invariants: it is in general not possible to reconstruct the abelian variety from these.

It turns out that, in our setting, the extra automorphism $[\mathbf{i}]$ on our fourfold of Weil type allows to fix the level-2 theta structure almost canonically, see [Appendix G.2](#). This allows us to redefine the MIKE invariants from [Definition 4.2](#) in terms of the theta constants of a symplectic basis adapted to $\mathbf{i}$.

Lemma H.1. *Let X be an abelian fourfold of Weil-type equipped with a level-2 theta structure and set of invariants $I_{\text{MIKE}}(X)$ as in [Definition 4.2](#). Consider the change of theta coordinates to a level-2 structure θ' from [Lemma G.3](#) that is adapted to $[\mathbf{i}]$. Then*

$$(I_0 : \cdots : I_9) = (b_0^2 : b_8^2 : b_4^2 : b_{12}^2 : b_2^2 : b_6^2 : b_1^2 : b_9^2 : b_3^2 : b_{15}^2).$$

where $\theta'(0) = (b_0 : \cdots : b_{15})$ is the theta null point with respect to the adapted level-2 structure.

Proof. Consider the change of theta coordinates from [Corollary G.3](#), and let (a_i) be the theta null point in the (x_i) -coordinates, and (b_i) the one in the (y_i) -coordinates. Since the theta null point is invariant by $[\mathbf{i}]$, we have that these theta null points are of the form $(a_{00} : a_{01} : a_{02} : a_{03} : a_{02} : a_{05} : a_{06} : a_{07} : a_{01} : a_{09} : a_{05} : a_{11} : a_{03} : a_{11} : a_{07} : a_{15})$ and $(b_{00} : b_{01} : b_{02} : b_{03} : b_{04} : 0 : b_{06} : 0 : b_{08} : b_{09} : 0 : 0 : b_{12} : 0 : 0 : b_{15})$ respectively.

Plugging the definition of the invariants from [Definition 4.2](#) into the change of coordinates from [Corollary G.3](#) gives the result. $\square$

Definition H.1. *Let S_{MIKE} be the permutation subgroup $\langle (45)(67)(89), (179842)(365) \rangle \subset S_9 \subset S_{10}$, where S_n denotes the group of permutations of $\{0, \dots, n-1\}$ and S_9 is seen as the subgroup of S_{10} of permutations that fixes 0.*

Remark H.2. Explicitly, S_{MIKE} comprises 72 permutations given by:

$(0, 3, 2, 1, 4, 5, 8, 9, 6, 7),$	$(0, 2, 5, 4, 9, 7, 3, 1, 8, 6),$	$(0, 3, 1, 2, 7, 6, 9, 8, 5, 4),$
$(0, 7, 6, 1, 4, 8, 5, 9, 2, 3),$	$(0, 3, 2, 1, 5, 4, 9, 8, 7, 6),$	$(0, 8, 6, 4, 1, 7, 3, 9, 2, 5),$
$(0, 1, 3, 2, 8, 9, 6, 7, 4, 5),$	$(0, 5, 4, 2, 6, 8, 7, 9, 1, 3),$	$(0, 2, 5, 4, 7, 9, 1, 3, 6, 8),$
$(0, 9, 5, 7, 2, 4, 3, 8, 1, 6),$	$(0, 8, 9, 3, 7, 5, 6, 4, 1, 2),$	$(0, 1, 2, 3, 5, 4, 7, 6, 9, 8),$
$(0, 1, 2, 3, 4, 5, 6, 7, 8, 9),$	$(0, 7, 1, 6, 2, 3, 5, 9, 4, 8),$	$(0, 2, 1, 3, 7, 6, 5, 4, 9, 8),$
$(0, 4, 2, 5, 1, 3, 6, 8, 7, 9),$	$(0, 9, 3, 8, 2, 1, 5, 7, 4, 6),$	$(0, 1, 7, 6, 9, 5, 3, 2, 8, 4),$
$(0, 4, 8, 6, 9, 3, 5, 2, 7, 1),$	$(0, 2, 4, 5, 6, 8, 1, 3, 7, 9),$	$(0, 5, 9, 7, 8, 3, 4, 2, 6, 1),$
$(0, 4, 5, 2, 9, 7, 8, 6, 3, 1),$	$(0, 1, 6, 7, 8, 4, 3, 2, 9, 5),$	$(0, 1, 7, 6, 5, 9, 2, 3, 4, 8),$
$(0, 6, 4, 8, 5, 2, 7, 1, 9, 3),$	$(0, 5, 4, 2, 8, 6, 9, 7, 3, 1),$	$(0, 9, 8, 3, 4, 6, 5, 7, 2, 1),$
$(0, 7, 5, 9, 2, 4, 1, 6, 3, 8),$	$(0, 9, 7, 5, 1, 6, 3, 8, 2, 4),$	$(0, 9, 8, 3, 6, 4, 7, 5, 1, 2),$
$(0, 6, 7, 1, 5, 9, 4, 8, 2, 3),$	$(0, 9, 3, 8, 1, 2, 7, 5, 6, 4),$	$(0, 5, 2, 4, 3, 1, 9, 7, 8, 6),$
$(0, 1, 3, 2, 9, 8, 7, 6, 5, 4),$	$(0, 4, 6, 8, 1, 7, 2, 5, 3, 9),$	$(0, 7, 9, 5, 8, 3, 6, 1, 4, 2),$
$(0, 4, 2, 5, 3, 1, 8, 6, 9, 7),$	$(0, 8, 4, 6, 5, 2, 9, 3, 7, 1),$	$(0, 2, 3, 1, 8, 9, 4, 5, 6, 7),$
$(0, 7, 6, 1, 8, 4, 9, 5, 3, 2),$	$(0, 7, 5, 9, 4, 2, 6, 1, 8, 3),$	$(0, 6, 1, 7, 2, 3, 4, 8, 5, 9),$
$(0, 3, 8, 9, 4, 6, 2, 1, 5, 7),$	$(0, 8, 3, 9, 2, 1, 4, 6, 5, 7),$	$(0, 8, 9, 3, 5, 7, 4, 6, 2, 1),$

$(0, 6, 4, 8, 2, 5, 1, 7, 3, 9),$ $(0, 2, 1, 3, 6, 7, 4, 5, 8, 9),$ $(0, 6, 8, 4, 9, 3, 7, 1, 5, 2),$
 $(0, 7, 9, 5, 3, 8, 1, 6, 2, 4),$ $(0, 5, 2, 4, 1, 3, 7, 9, 6, 8),$ $(0, 6, 1, 7, 3, 2, 8, 4, 9, 5),$
 $(0, 4, 5, 2, 7, 9, 6, 8, 1, 3),$ $(0, 1, 6, 7, 4, 8, 2, 3, 5, 9),$ $(0, 8, 3, 9, 1, 2, 6, 4, 7, 5),$
 $(0, 3, 9, 8, 7, 5, 1, 2, 6, 4),$ $(0, 3, 9, 8, 5, 7, 2, 1, 4, 6),$ $(0, 2, 4, 5, 8, 6, 3, 1, 9, 7),$
 $(0, 4, 6, 8, 7, 1, 5, 2, 9, 3),$ $(0, 8, 6, 4, 7, 1, 9, 3, 5, 2),$ $(0, 9, 7, 5, 6, 1, 8, 3, 4, 2),$
 $(0, 8, 4, 6, 2, 5, 3, 9, 1, 7),$ $(0, 6, 7, 1, 9, 5, 8, 4, 3, 2),$ $(0, 5, 9, 7, 3, 8, 2, 4, 1, 6),$
 $(0, 5, 7, 9, 6, 1, 4, 2, 8, 3),$ $(0, 7, 1, 6, 3, 2, 9, 5, 8, 4),$ $(0, 9, 5, 7, 4, 2, 8, 3, 6, 1),$
 $(0, 5, 7, 9, 1, 6, 2, 4, 3, 8),$ $(0, 6, 8, 4, 3, 9, 1, 7, 2, 5),$ $(0, 2, 3, 1, 9, 8, 5, 4, 7, 6),$
 $(0, 3, 1, 2, 6, 7, 8, 9, 4, 5),$ $(0, 3, 8, 9, 6, 4, 1, 2, 7, 5),$ $(0, 4, 8, 6, 3, 9, 2, 5, 1, 7).$

From this list, we see that the invariants $(b_0^2 : b_1^2 : b_2^2 : b_3^2 : b_4^2 : b_6^2 : b_8^2 : b_9^2 : b_{12}^2 : b_{15}^2)$ differs from $I_{\text{MIKE}} = (b_0^2 : b_8^2 : b_4^2 : b_{12}^2 : b_2^2 : b_6^2 : b_1^2 : b_9^2 : b_3^2 : b_{15}^2)$ by a permutation in S_{MIKE} .

H.2 Proof of Theorem 4.2

In light of Proposition G.3, Theorem 4.2 will follow from the following stronger version:

Theorem H.1. *Let $\mathbb{F}_p$ be a prime field with $p \equiv 3 \pmod{4}$. Consider two abelian fourfolds X, X' of Weil-type equipped with a $\mathbb{F}_p$ -rational level-2 structure θ which is $[\mathbf{i}]$ -adapted.*

Then $X \cong X'$ if and only if $I_{\text{MIKE}}(X) = \sigma(I_{\text{MIKE}}(X'))$ for some

$$\sigma \in S_{\text{MIKE}} = \langle (45)(67)(89), (179842)(365) \rangle \subset S_9 \subset S_{10},$$

where the action of $\sigma \in S_9 \subset S_{10}$ on an element $x \in \mathbb{P}^9$ is given by $(x_0 : \dots : x_9) \mapsto (x_0 : x_{\sigma(1)} : \dots : x_{\sigma(9)})$.

To prove Theorem H.1, we first need to prove that given an abelian fourfold with two $\mathbb{F}_p$ -rational level 2 theta structures induced by an $[\mathbf{i}]$ -adapted basis, with associated theta null points $(b_{00} : b_{01} : b_{02} : b_{03} : b_{04} : 0 : b_{06} : 0 : b_{08} : b_{09} : 0 : 0 : b_{12} : 0 : 0 : b_{15})$ and $(b'_{00} : b'_{01} : b'_{02} : b'_{03} : b'_{04} : 0 : b'_{06} : 0 : b'_{08} : b'_{09} : 0 : 0 : b'_{12} : 0 : 0 : b'_{15})$ then $(b_{00}^2 : b_{01}^2 : b_{02}^2 : b_{03}^2 : b_{04}^2 : b_{06}^2 : b_{08}^2 : b_{09}^2 : b_{12}^2 : b_{15}^2) = \sigma(b_{00}^2 : b_{01}^2 : b_{02}^2 : b_{03}^2 : b_{04}^2 : b_{06}^2 : b_{08}^2 : b_{09}^2 : b_{12}^2 : b_{15}^2)$ for a permutation $\sigma \in S_{\text{MIKE}}$.

Then, conversely, that given $(b_{00}^2 : b_{01}^2 : b_{02}^2 : b_{03}^2 : b_{04}^2 : b_{06}^2 : b_{08}^2 : b_{09}^2 : b_{12}^2 : b_{15}^2)$, then for all choices of signs b'_i for the b_i^2 and all choices of $\sigma \in S_{\text{MIKE}}$, the point $\sigma(b_{00}^2 : b_{01}^2 : b_{02}^2 : b_{03}^2 : b_{04}^2 : 0 : b_{06}^2 : 0 : b_{08}^2 : b_{09}^2 : 0 : 0 : b_{12}^2 : 0 : 0 : b_{15}^2)$ corresponds to a valid theta null point (where we see σ as acting on the 10 non-zero coordinates), on the same. Note that here we do not require a priori that the (b'_i) come from an $[\mathbf{i}]$ -adapted basis, nor a rational level-2 theta structure, just that it encodes the same fourfold as (b_i) . We will see however during the proof that this is automatically the case (see Remark H.3).

First, we prove that in the conditions of Theorem H.1, θ_0 is fixed. We first begin with a warm-up:

Lemma H.2. *Given two different adapted $([\mathbf{i}], \pi_p)$ -symplectic basis, the theta coordinate θ_0 is the same (up to a constant).*

Proof. The coordinate θ_0 depends on the choice of the U_1, U_2, U_3, U_4 , or rather the symmetric theta group elements they induce. Denote both choice by $U_i^{(1)}$ and $U_i^{(2)}$ respectively. First, because the U_i are above the points in $X[1 + \mathbf{i}]$ in both case, we have $U_i^{(2)} = U_i^{(1)} + T$ for some $T \in X[2]$.

Now we use the fact that our bases are $([\mathbf{i}], \pi_p)$ -adapted and not only $[\mathbf{i}]$ -adapted. Assume for instance that $[\mathbf{i}] \circ \pi_p U_1^{(1)} = U_1^{(1)}$. Then by definition, either $[\mathbf{i}] \circ \pi_p(U_1^{(2)}) = U_1^{(2)}$ or $[\mathbf{i}] \circ \pi_p(U_1^{(2)}) = -U_1^{(2)}$.

In the first case, $U_1^{(2)} = U_1^{(1)} + T$ where $[\mathbf{i}] \circ \pi_p(T) = T$. Since the two-torsion points are rational, this amount to $[\mathbf{i}]T = T$, i.e. $T \in X[1 + \mathbf{i}]$, and so $U_1^{(2)}$ induces the same theta group element as $U_1^{(1)}$, cf. [Remark G.5](#). In the second case, a similar computation shows that $[1 + \mathbf{i}]T = -[2]U_1 = -T_1$, so $T - T'_3 \in X[1 + \mathbf{i}]$. Because $e_2(T_1, T'_3) = 1$, we also have that $U_1^{(2)}$ induces the same theta group element as $U_1^{(1)}$. The other cases are similar. $\square$

We now handle the case of a general $\mathbb{F}_p$ -rational $[\mathbf{i}]$ -adapted theta structure.

Lemma H.3. *Given two different adapted $[\mathbf{i}]$ -adapted symplectic basis, whose associated theta structure is rational, then the theta coordinate θ_0 is the same (up to a constant).*

Proof. Assume that we have a $[\mathbf{i}]$ -adapted symplectic basis that gives a rational theta structure, induced by a symplectic decomposition $X[4] = U_1 \oplus U_2$ above $X[2] = K_1 \oplus K_2$. Let $\phi = (1 + \mathbf{i})$, and θ_i the theta functions associated to this theta structure. From the conditions of being $[\mathbf{i}]$ -adapted, we have $K_2 = X[1 + \mathbf{i}]$ so that $X/K_2 \simeq X$, and $\phi(U_2) = K_1$. By [Proposition G.5](#), it follows that if Θ_0 is a level one theta function associated to the even theta characteristic q induced by $K_1 \oplus K_2$, we have $\theta_0 = \Theta_0 \circ \phi$.

Now assume that we have a second theta structure satisfying the same conditions, induced by $X[4] = U'_1 \oplus U'_2$ above $X[2] = K'_1 \oplus K'_2$. Let θ'_i the theta functions given by this theta structure. As above $\theta'_0 = \Theta'_0 \circ \phi$, where Θ'_0 is a level one theta function associated to the theta characteristic q' induced by $K'_1 \oplus K'_2$.

First, $K'_2 = X[1 + \mathbf{i}] = K_2$. Secondly, if $P \in K'_1$, then its symmetric lift g_P has to be rational because the theta structure is rational. On the other hand, writing $P = P_1 + P_2$ with $P_i \in K_i$, we also know that the symmetric lifts g_{P_i} are rational because the first theta structure is also rational. By [Remark G.5](#), this forces $e_2(P_1, P_2) = 1$. Indeed, if $e_2(P_1, P_2) = -1$, we would have $g_P = (\pm i)g_{P_1}g_{P_2}$, but since i lives over a degree 2 extension of $\mathbb{F}_p$ and $g_{P_1}g_{P_2}$ is rational, g_P would not be rational. Hence $q(P) = 1$ by definition of q . So $q(K'_1) = 1$, and $q(K_2) = 1$ by definition, which proves that $q = q'$. Hence Θ_0, Θ'_0 differ by a constant, and so θ_0 and θ'_0 too. $\square$

By [Lemmas H.2](#) and [H.3](#), and the way a change of level-4 symplectic basis acts on the level-2 theta constants (see for instance [\[Rob23, Appendix B.1\]](#)), it follows that the theta null points of two $\mathbb{F}_p$ -rational $[\mathbf{i}]$ -adapted symplectic bases differ by a permutation of the non zero coordinates b_i for $i \in \{1, 2, 3, 4, 6, 8, 9, 12, 15\}$

and some scaling by a fourth root of unity that has to be ± 1 since $\sqrt{-1}$ is not in $\mathbb{F}_p$.

Indeed, a general symplectic matrix $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ leaves θ_0 invariant if and only if $C = 0$. Furthermore, we can treat separately the matrix of the form $M = \begin{pmatrix} U & 0 \\ 0 & U^{-T} \end{pmatrix}$ with $U \in \text{Gl}_4(\mathbb{Z}/4\mathbb{Z})$ which will act by permutation on the coordinates, and the ones of the form $M = \begin{pmatrix} \text{id} & B \\ 0 & \text{id} \end{pmatrix}$ for B a symmetric matrix in $M_4(\mathbb{Z}/4\mathbb{Z})$, which will acts by multiplication by some power of i on the coordinates.

We first check that all sign choices for these b_i correspond to a theta null point on the same fourfold.

Proposition H.1. *Suppose that we have a theta null point $(b_0 : b_1 : b_2 : b_3 : b_4 : 0 : b_6 : 0 : b_8 : b_9 : 0 : 0 : b_{12} : 0 : 0 : b_{15})$ induced from a symplectic basis adapted to $[\mathbf{i}]$, and let $(I_0 : \dots : I_9) = (b_0^2 : b_8^2 : b_4^2 : b_{12}^2 : b_2^2 : b_6^2 : b_1^2 : b_9^2 : b_3^2 : b_{15}^2)$ be its MIKE invariants.*

Then given $(I_0 : \dots : I_9)$, all 9 projective choices of signs for the b_i correspond to a valid theta null point.

Proof. Let $M_{ij} = \begin{pmatrix} \text{id} & B_{ij} \\ 0 & \text{id} \end{pmatrix}$ where B_{ij} is the symmetric matrix with all zeroes except a 1 on the $(i, j), (j, i)$ positions. Then we have the following action on theta constants:

$$\begin{aligned}
M_{1,1}.(b_0 : b_1 : b_2 : b_3 : b_4 : 0 : b_6 : 0 : b_8 : b_9 : 0 : 0 : b_{12} : 0 : 0 : b_{15}) &= \\
(b_0 : -b_1 : b_2 : -b_3 : b_4 : 0 : b_6 : 0 : b_8 : -b_9 : 0 : 0 : b_{12} : 0 : 0 : -b_{15}), \\
M_{2,2}.(b_0 : b_1 : b_2 : b_3 : b_4 : 0 : b_6 : 0 : b_8 : b_9 : 0 : 0 : b_{12} : 0 : 0 : b_{15}) &= \\
(b_0 : b_1 : -b_2 : -b_3 : b_4 : 0 : -b_6 : 0 : b_8 : b_9 : 0 : 0 : b_{12} : 0 : 0 : -b_{15}), \\
M_{3,3}.(b_0 : b_1 : b_2 : b_3 : b_4 : 0 : b_6 : 0 : b_8 : b_9 : 0 : 0 : b_{12} : 0 : 0 : b_{15}) &= \\
(b_0 : b_1 : b_2 : b_3 : -b_4 : 0 : -b_6 : 0 : b_8 : b_9 : 0 : 0 : -b_{12} : 0 : 0 : -b_{15}), \\
M_{4,4}.(b_0 : b_1 : b_2 : b_3 : b_4 : 0 : b_6 : 0 : b_8 : b_9 : 0 : 0 : b_{12} : 0 : 0 : b_{15}) &= \\
(b_0 : b_1 : b_2 : b_3 : b_4 : 0 : b_6 : 0 : -b_8 : -b_9 : 0 : 0 : -b_{12} : 0 : 0 : -b_{15}), \\
M_{1,2}.(b_0 : b_1 : b_2 : b_3 : b_4 : 0 : b_6 : 0 : b_8 : b_9 : 0 : 0 : b_{12} : 0 : 0 : b_{15}) &= \\
(b_0 : b_1 : b_2 : -b_3 : b_4 : 0 : b_6 : 0 : b_8 : b_9 : 0 : 0 : b_{12} : 0 : 0 : -b_{15}), \\
M_{1,3}.(b_0 : b_1 : b_2 : b_3 : b_4 : 0 : b_6 : 0 : b_8 : b_9 : 0 : 0 : b_{12} : 0 : 0 : b_{15}) &= \\
(b_0 : b_1 : b_2 : b_3 : b_4 : 0 : b_6 : 0 : b_8 : b_9 : 0 : 0 : b_{12} : 0 : 0 : -b_{15}), \\
M_{1,4}.(b_0 : b_1 : b_2 : b_3 : b_4 : 0 : b_6 : 0 : b_8 : b_9 : 0 : 0 : b_{12} : 0 : 0 : b_{15}) &= \\
(b_0 : b_1 : b_2 : b_3 : b_4 : 0 : b_6 : 0 : b_8 : -b_9 : 0 : 0 : b_{12} : 0 : 0 : -b_{15}), \\
M_{2,3}.(b_0 : b_1 : b_2 : b_3 : b_4 : 0 : b_6 : 0 : b_8 : b_9 : 0 : 0 : b_{12} : 0 : 0 : b_{15}) &= \\
(b_0 : b_1 : b_2 : b_3 : b_4 : 0 : -b_6 : 0 : b_8 : b_9 : 0 : 0 : b_{12} : 0 : 0 : -b_{15}), \\
M_{3,4}.(b_0 : b_1 : b_2 : b_3 : b_4 : 0 : b_6 : 0 : b_8 : b_9 : 0 : 0 : b_{12} : 0 : 0 : b_{15}) &= \\
(b_0 : b_1 : b_2 : b_3 : b_4 : 0 : b_6 : 0 : b_8 : b_9 : 0 : 0 : -b_{12} : 0 : 0 : -b_{15}).
\end{aligned}$$

We check that in the orbit of the action of these matrices, we obtain the actions

$$\begin{aligned}
 &(b_0 : -b_1 : b_2 : b_3 : b_4 : 0 : b_6 : 0 : b_8 : b_9 : 0 : 0 : b_{12} : 0 : 0 : b_{15}), \\
 &(b_0 : b_1 : -b_2 : b_3 : b_4 : 0 : b_6 : 0 : b_8 : b_9 : 0 : 0 : b_{12} : 0 : 0 : b_{15}), \\
 &(b_0 : b_1 : b_2 : -b_3 : b_4 : 0 : b_6 : 0 : b_8 : b_9 : 0 : 0 : b_{12} : 0 : 0 : b_{15}), \\
 &(b_0 : b_1 : b_2 : b_3 : -b_4 : 0 : b_6 : 0 : b_8 : b_9 : 0 : 0 : b_{12} : 0 : 0 : b_{15}), \\
 &(b_0 : b_1 : b_2 : b_3 : b_4 : 0 : -b_6 : 0 : b_8 : b_9 : 0 : 0 : b_{12} : 0 : 0 : b_{15}), \\
 &(b_0 : b_1 : b_2 : b_3 : b_4 : 0 : b_6 : 0 : -b_8 : b_9 : 0 : 0 : b_{12} : 0 : 0 : b_{15}), \\
 &(b_0 : b_1 : b_2 : b_3 : b_4 : 0 : b_6 : 0 : b_8 : -b_9 : 0 : 0 : b_{12} : 0 : 0 : b_{15}), \\
 &(b_0 : b_1 : b_2 : b_3 : b_4 : 0 : b_6 : 0 : b_8 : b_9 : 0 : 0 : -b_{12} : 0 : 0 : b_{15}), \\
 &(b_0 : b_1 : b_2 : b_3 : b_4 : 0 : b_6 : 0 : b_8 : b_9 : 0 : 0 : b_{12} : 0 : 0 : -b_{15}),
 \end{aligned}$$

hence all 9 projective choices of signs are valid. $\square$

Now we tackle the permutations.

Proposition H.2. *There are exactly 72 permutations associated to symplectic matrices of the form $M = \begin{pmatrix} U & 0 \\ 0 & U^{-T} \end{pmatrix}$ with $U \in \text{Gl}(\mathbb{Z}/4\mathbb{Z})$ which leave the set of $[\mathbf{i}]$ -odd coordinates $\{x_5, x_7, x_{10}, x_{11}, x_{13}, x_{14}\}$ invariant (i.e. that permute these coordinates). These 72 permutations are given by the group S_{MIKE} .*

Proof. In other words, we consider all symplectic matrices $M = \begin{pmatrix} U & 0 \\ 0 & U^{-T} \end{pmatrix}$ with $U \in \text{Gl}_4(\mathbb{Z}/4\mathbb{Z})$ such that the image of the special theta null point $(b_0 : b_1 : b_2 : b_3 : b_4 : 0 : b_6 : 0 : b_8 : b_9 : 0 : 0 : b_{12} : 0 : 0 : b_{15})$ is still of the form $(b'_0 : b'_1 : b'_2 : b'_3 : b'_4 : 0 : b'_6 : 0 : b'_8 : b'_9 : 0 : 0 : b'_{12} : 0 : 0 : b'_{15})$. We look at the associated permutation on the 10 non zero b_i , enumerated as $(b_0, b_1, b_2, b_3, b_4, b_6, b_8, b_9, b_{12}, b_{15})$. Doing this computation in SageMath gives us the list above of 72 permutations. $\square$

Remark H.3. We remark that if the action of M on our $[\mathbf{i}]$ -adapted theta null point gives a theta null point which is also induced by an $[\mathbf{i}]$ -adapted symplectic basis, then by [Proposition G.3](#) the permutation induced by M is certainly in the list above. A priori the converse is not true, because the reduction of U modulo 2 may not land in $\text{Sp}_4(\mathbb{Z}/2\mathbb{Z}) \subset \text{Gl}_4(\mathbb{Z}/2\mathbb{Z})$ (i.e., may not correspond to a symplectic transform of $(X[1 + \mathbf{i}], e_{1+\mathbf{i}})$). However, one can check that all the 72 permutations above are induced by some other choices of $[\mathbf{i}]$ -adapted basis (which fixes θ_0), so this list of permutations is tight. We refer to [Appendix H.4](#) for a more conceptual explanation of this phenomena.

Proof (End of the proof of Theorem 4.2). Combining [Propositions H.1](#) and [H.2](#) finishes the proof: first this shows that all choices of signs and permutations correspond to different theta null points on the same fourfold.

Secondly, because an $([\mathbf{i}], \pi_p)$ -adapted symplectic basis has to have a theta null point with 0 coordinates in positions $i = 5, 7, 10, 11, 13, 14$ by [Proposition G.3](#), we can find a permutation in S_{MIKE} such that the coordinates are the same, up to an action of some power of i , which has to be ± 1 since we have rational coordinates, still by [Proposition G.3](#). $\square$

H.3 Absolute MIKE invariants and Theorem 4.3

The invariants $I_{\text{MIKE}} = (I_0 : \dots : I_9)$ from [Theorem 4.2](#) are not absolute invariants; they are invariant up to a permutation in S_{MIKE} . In this part, we prove [Theorem 4.3](#) which states that $J_{\text{MIKE}} = (J_1 : \dots : J_5) \in \mathbb{P}(1, 2, 3, 4, 5)$ from [Definition 4.3](#) are absolute invariants that uniquely identify the isomorphism class of an abelian fourfold of Weil type. The first part of the statement is that two isomorphic abelian fourfold of Weil type have the same invariants and is easy to prove; this is done in [Lemma H.4](#). The second part requires more work: we need to show that we can recover $I_{\text{MIKE}}(X)$ (up to permutation in S_{MIKE}) from $J_{\text{MIKE}}(X)$.

Lemma H.4. *Let $p \equiv 3 \pmod{4}$ and let X be an abelian fourfold of Weil type defined over $\mathbb{F}_p$. Further let $J_{\text{MIKE}}(X) = (J_1 : \dots : J_5) \in \mathbb{P}(1, 2, 3, 4, 5)$ as in [Definition 4.3](#). Then an isomorphic abelian fourfold of Weil type $X' \simeq X$ has the same invariants J_1, J_2, J_3, J_4, J_5 .*

Proof. Recall that $I_{\text{MIKE}} = (I_0 : \dots : I_9)$ are invariants up to a permutation in $S_{\text{MIKE}} \subset S_9 \subset S_{10}$. Clearly, $J_k = \sum_{i=1}^9 I_i^k$ are invariant under permutations in S_{MIKE} , hence in particular, they are invariant under permutations in S_{MIKE} . Now the statement follows from [Theorem 4.2](#). $\square$

Lemma H.5. *Let X be an abelian fourfold of Weil type, equipped with a level-2 structure θ adapted to the MIKE isogenies. Then the following are true.*

1. *Let $\theta(0_X) = (a_0 : \dots : a_{15})$ be the theta null point. Then*

$$a_1 = a_8, \quad a_2 = a_4, \quad a_3 = a_{12}, \quad a_5 = a_{10}, \quad a_7 = a_{14}, \quad a_{11} = a_{13}.$$

2. *The image $\theta(X/\{\pm 1\})$ is contained in the variety $V(F_1, F_2, F_3, F_4, F_5, F_6) \subset \mathbb{P}^{15}$ with*

$$\begin{aligned} F_1 &= -x_0x_6 + x_2x_4 - x_9x_{15} + x_{11}x_{13} \\ F_2 &= -x_1x_7 + x_3x_5 - x_8x_{14} + x_{10}x_{12} \\ F_3 &= -x_0x_{15} + x_3x_{12} + x_5x_{10} - x_6x_9 \\ F_4 &= -x_1x_{14} + x_2x_{13} + x_4x_{11} - x_7x_8 \\ F_5 &= -x_0x_9 + x_1x_8 - x_6x_{15} + x_7x_{14} \\ F_6 &= -x_2x_{11} + x_3x_{10} - x_4x_{13} + x_5x_{12} \end{aligned} \tag{23}$$

Proof. The first part of the statement follows from the explicit description of the action of $[\mathbf{i}]$ on the level-2 coordinates provided in [Corollary G.3](#), and the fact that the theta null point $\theta(0_X)$ is fixed by the automorphism.

For the second part, we use that to each even vanishing coordinate of the level-(2, 2) theta null point, one may associate a quadric F in $k[x_0, \dots, x_{15}]$ so that the Kummer variety lies in $V(F)$ as per [Gee96, §3.5]. In the following we make this explicit in our setting.

From the duplication formula (Equation (17)), we obtain that for all $P = (x_0 : \dots : x_{15}) \in X/\{\pm 1\}$:

$$\begin{aligned}
 \vartheta \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix} (P) \cdot \vartheta \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix} (0_X) &= -2(x_2x_4 + x_3x_5 - x_0x_6 - x_1x_7 + x_{10}x_{12} \\
 &\quad + x_{11}x_{13} - x_8x_{14} - x_9x_{15}) \\
 \vartheta \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix} (P) \cdot \vartheta \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix} (0_X) &= 2(x_7x_8 + x_6x_9 - x_5x_{10} - x_4x_{11} - x_3x_{12} \\
 &\quad - x_2x_{13} + x_1x_{14} + x_0x_{15}) \\
 \vartheta \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix} (P) \cdot \vartheta \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix} (0_X) &= -2(x_1x_8 - x_0x_9 + x_3x_{10} - x_2x_{11} + x_5x_{12} \\
 &\quad - x_4x_{13} + x_7x_{14} - x_6x_{15}) \\
 \vartheta \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} (P) \cdot \vartheta \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} (0_X) &= -2(x_7x_8 - x_6x_9 + x_5x_{10} - x_4x_{11} + x_3x_{12} \\
 &\quad - x_2x_{13} + x_1x_{14} - x_0x_{15}) \\
 \vartheta \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} (P) \cdot \vartheta \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} (0_X) &= -2(x_2x_4 - x_3x_5 - x_0x_6 + x_1x_7 - x_{10}x_{12} \\
 &\quad + x_{11}x_{13} + x_8x_{14} - x_9x_{15}) \\
 \vartheta \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix} (P) \cdot \vartheta \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix} (0_X) &= -2(x_1x_8 - x_0x_9 - x_3x_{10} + x_2x_{11} - x_5x_{12} \\
 &\quad + x_4x_{13} + x_7x_{14} - x_6x_{15})
 \end{aligned}$$

Since level-(2, 2) theta constants vanish at these indices by Corollary G.4, it follows that:

$$\begin{aligned}
 F_1(P) &= -\frac{1}{4}\vartheta \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix} (P) \cdot \vartheta \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix} (0_X) - \frac{1}{4}\vartheta \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} (P) \cdot \vartheta \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} (0_X) \\
 F_2(P) &= -\frac{1}{4}\vartheta \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix} (P) \cdot \vartheta \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix} (0_X) + \frac{1}{4}\vartheta \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} (P) \cdot \vartheta \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} (0_X) \\
 F_3(P) &= -\frac{1}{4}\vartheta \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix} (P) \cdot \vartheta \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix} (0_X) - \frac{1}{4}\vartheta \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} (P) \cdot \vartheta \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} (0_X) \\
 F_4(P) &= -\frac{1}{4}\vartheta \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix} (P) \cdot \vartheta \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix} (0_X) + \frac{1}{4}\vartheta \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} (P) \cdot \vartheta \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} (0_X) \\
 F_5(P) &= -\frac{1}{4}\vartheta \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix} (P) \cdot \vartheta \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix} (0_X) - \frac{1}{4}\vartheta \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix} (P) \cdot \vartheta \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix} (0_X) \\
 F_6(P) &= -\frac{1}{4}\vartheta \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix} (P) \cdot \vartheta \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix} (0_X) + \frac{1}{4}\vartheta \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix} (P) \cdot \vartheta \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix} (0_X),
 \end{aligned}$$

are all zero. This completes the proof. $\square$

Lemma H.6. *Let X be an abelian variety of Weil type and $I_{\text{MIKE}}(X) = (I_0 : \dots : I_9)$ as in Definition 4.2. Then*

$$\begin{aligned} I_0 + I_9 &= I_3 + I_5 + I_7 + I_8, \\ I_1 + I_9 &= I_3 + I_7, \\ I_2 + I_9 &= I_3 + I_5, \\ I_4 + I_9 &= I_5 + I_8, \\ I_6 + I_9 &= I_7 + I_8. \end{aligned} \tag{24}$$

Proof. After a change of variables $x \rightarrow y$ that transforms the theta coordinates adapted to the MIKE isogenies into theta coordinates adapted to $([\mathbf{i}], \pi_p)$ (see Corollary G.3), the relations from Equation (23) become

$$\begin{aligned} F_1 &= (32) \cdot (-y_0^2 + y_2^2 - y_4^2 + y_6^2 + y_8^2 - y_{10}^2 + y_{12}^2 - y_{14}^2), \\ F_2 &= (-32) \cdot (-y_1^2 + y_3^2 - y_5^2 + y_7^2 + y_9^2 - y_{11}^2 + y_{13}^2 - y_{15}^2), \\ F_3 &= (-32) \cdot (-y_2^2 + y_3^2 + y_6^2 - y_7^2 - y_{10}^2 + y_{11}^2 + y_{14}^2 - y_{15}^2), \\ F_4 &= (32) \cdot (y_1^2 - y_2^2 - y_5^2 + y_6^2 - y_9^2 + y_{10}^2 + y_{13}^2 - y_{14}^2), \\ F_5 &= (32) \cdot (-y_0^2 + y_1^2 + y_4^2 - y_5^2 - y_8^2 + y_9^2 + y_{12}^2 - y_{13}^2), \\ F_6 &= (-32) \cdot (-y_2^2 + y_3^2 + y_6^2 - y_7^2 - y_{10}^2 + y_{11}^2 + y_{14}^2 - y_{15}^2). \end{aligned}$$

Now, we use the interpretation of the invariants as squares of the theta null point coordinates corresponding to a theta structure adapted to $([\mathbf{i}], \pi_p)$ from Lemma H.1. Evaluating the above equations in the theta null point consequently provides us with linear equations on the MIKE invariants. And one may check that the resulting system of equations is equivalent to the one provided in the statement of the lemma. $\square$

The following lemma provides us with a new interpretation for the group S_{MIKE} : It is precisely the subgroup of S_{10} that fixes the relations from Lemma H.6.

Lemma H.7. *Let $R = \mathbb{Z}[I_0, \dots, I_9]$ and consider the action of S_{10} on R induced by $\sigma \star x_i = x_{\sigma(i)}$ for $i \in \{0, \dots, 9\}$ and $\sigma \in S_{10}$. Further, consider $F_1, \dots, F_6 \in R$ as defined in Lemma H.6.*

Then an element $h \in S_{10}$ it holds that $h \in S_{\text{MIKE}}$ if and only if

$$V(F_1, \dots, F_6) = V(h \star F_1, \dots, h \star F_6).$$

Proof. For an element $h \in S_{\text{MIKE}}$, it follows immediately from Theorem 4.2 and Lemma H.6 that $V(F_1, \dots, F_6) = V(h \star F_1, \dots, h \star F_6)$.

The other direction can be verified by checking the inequality of ideals $I = (F_1, \dots, F_6) \neq I_h = (h \star F_1, \dots, h \star F_6)$ for any $h \in S_{10} \setminus S_{\text{MIKE}}$. $\square$

Lemma H.8. *Let $J_{\text{MIKE}} = (J_1 : \dots : J_5)$ with $J_{\text{MIKE}} = J_{\text{MIKE}}(X)$ for some X of Weil type. If*

$$0 \neq -7J_1^4 + 126J_1^2J_2 - 243J_2^2 - 432J_1J_3 + 972J_4,$$

up to permutation in S_{10} , we can recover $I_{\text{MIKE}} = (I_0 : \dots : I_9)$.

Proof. Absolute invariants for $I_0, \dots, I_9$ under the action of S_{10} are given by

$$\tilde{J}_k = \sum_{i=0}^9 I_i^k \quad \text{for } k = 1, \dots, 10.$$

And given $\tilde{J}_1, \dots, \tilde{J}_{10}$, one may recover the $I_0, \dots, I_9$ up to permutation in S_{10} .

In the following, we show that $\tilde{J}_k$ with $k = 1, \dots, 10$ can be expressed in terms of the elements in J_{MIKE} . Throughout the proof, it is essential to use the relations from Lemma H.6.

First, we observe that

$$\tilde{J}_1 = \sum_{i=0}^9 I_i = 4I_0 = I_0 + J_1.$$

This immediately implies that $\tilde{J}_1, \dots, \tilde{J}_5$ can be expressed in terms of the elements in J_{MIKE} .

Using a computer algebra system, we find that

$$0 = I_0^6 + 16200 \cdot q \cdot \tilde{J}_6 + r, \quad \text{with } q, r \in k[J_1, \dots, J_5]. \quad (25)$$

Concretely,

$$q = -7J_1^4 + 126J_1^2J_2 - 243J_2^2 - 432J_1J_3 + 972J_4$$

and

$$\begin{aligned} r = & 69J_1^{10} - 3105J_1^8J_2 + 47100J_1^6J_2^2 + 11720J_1^7J_3 - 270000J_1^4J_2^3 - 307800J_1^5J_2J_3 \\ & - 30690J_1^6J_4 + 467775J_1^2J_2^4 + 1992600J_1^3J_2^2J_3 + 522000J_1^4J_3^2 + 687150J_1^4J_2J_4 \\ & + 56592J_1^5J_5 - 273375J_2^5 - 1895400J_1J_2^3J_3 - 4860000J_1^2J_2J_3^2 - 3316950J_1^2J_2^2J_4 \\ & - 2268000J_1^3J_3J_4 - 933120J_1^3J_2J_5 + 583200J_2^2J_3^2 + 4276800J_1J_3^3 + 3389850J_2^3J_4 \\ & + 11664000J_1J_2J_3J_4 + 2770200J_1^2J_4^2 + 874800J_1J_2^2J_5 + 3149280J_1^2J_3J_5 \\ & - 9622800J_3^2J_4 - 9185400J_2J_4^2 + 5248800J_2J_3J_5 - 6298560J_1J_4J_5 - 3779136J_5^2. \end{aligned}$$

Consequently, under our assumption that $q \neq 0$, we can express $\tilde{J}_6$ in terms of J_{MIKE} .

For the remaining invariants, $\tilde{J}_7, \dots, \tilde{J}_{10}$, we again use a computer algebra system to represent them as elements in $\mathbb{Q}[J_1, \dots, J_6]$.³³ This is sufficient since we already showed that $\tilde{J}_6 = I_0^6 + J_6 \in \mathbb{Q}(J_1, \dots, J_5)$.

To make this last step more concrete, we sketch the steps taken in the algorithm to find an expression for $\tilde{J}_k$:

³³ More precisely, we obtain expressions in $\mathbb{Z}[\frac{1}{2 \cdot 3 \cdot 5}, J_1, \dots, J_6]$.

- We work over $R = \mathbb{Q}[I_3, I_5, I_7, I_8, I_9]$, and express $I_0, I_1, I_2, I_4, I_6 \in \mathbb{Q}[I_3, I_5, I_7, I_8, I_9]$ using the relations from 24.
- We construct all elements $T = \{t = \prod J_i^{i_j} \mid \deg(t) = k\} \subset \mathbb{Q}[J_1, \dots, J_k]$.
- Evaluation in $I_0, \dots, I_9$ yields $T_I = \{t(I_0, \dots, I_9) \mid t \in M\} \subset R$. The elements in T_I are homogeneous of degree k .
- Let M be an ordered set of all monomials of degree k of R . And define the matrix $A = (a_{mt})_{m \in M, t \in T_i}$ with a_{mt} being the coefficient of m in t . Similarly, we define the vector $y = (y_m)_{m \in M}$ with y_m being the coefficient of m in $J_k \in R$.

A solution x of the system $A \cdot x = y$, corresponds to a representation $J_k \in \mathbb{Q}[J_1, \dots, J_6]$. $\square$

Using the previous two lemmas, we can show that $J_{\text{MIKE}}(X)$ indeed determines $I_{\text{MIKE}}(X)$ up to an element in S_{MIKE} :

Lemma H.9. *Let $J_{\text{MIKE}} = (J_1 : \dots : J_5)$ with $J_{\text{MIKE}} = J_{\text{MIKE}}(X)$ for some X of Weil type. If*

$$0 \neq -7J_1^4 + 126J_1^2J_2 - 243J_2^2 - 432J_1J_3 + 972J_4,$$

then we can recover $I_{\text{MIKE}} = (I_0 : \dots : I_9)$ up to permutation in S_{MIKE} .

Proof. By Lemma H.8, we can recover I_{MIKE} up to a permutation in S_{10} from J_{MIKE} . Moreover, S_{MIKE} contains precisely the elements in S_{10} that respect the relations among the invariants $I_0, \dots, I_9$. Consequently, the relations can be used to find the correct values of I_{MIKE} , at least *generically*.

Assume we are given $J_{\text{MIKE}}(X)$ for some X of Weil type. Then we can use Lemma H.8 to recover I_{MIKE} up to a permutation in S_{10} . Let I_{MIKE}^* be such a candidate. Then there exists a permutation $\sigma \in S_{10} \setminus S_{\text{MIKE}}$ so that $I_{\text{MIKE}}' = \sigma \star I_{\text{MIKE}}^*$ satisfies the relations $F_1, \dots, F_6$ described in Lemma H.6. Now if I_{MIKE}' is *generic*, then $\tau I_{\text{MIKE}}'$ satisfies the relations as well if and only if $\tau \in S_{\text{MIKE}}$, as per Lemma H.7. In this case, we are done.

By a *non-generic case*, we mean a setting where the invariants I_{MIKE} satisfy additional relations so that the relations described in Lemma H.6 hold for $\tau \star I_{\text{MIKE}}$ for some $\tau \in S_{10} \setminus S_{\text{MIKE}}$. In order to handle these cases, we performed the following check for each element $\tau \in S_{10} \setminus S_{\text{MIKE}}$:

1. We set $R = \mathbb{Z}[I_0, \dots, I_9]$ and $I_R = (F_1, \dots, F_6) \triangleleft R$, and compute $J_R = I_R \cap \tau \star I_R$.
2. We set $I' = \tau \star I_{\text{MIKE}}$. Note that I' satisfies the relations if and only if $I_{\text{MIKE}} \in V(J_R)$.
3. We check that there exists an element $\sigma \in S_{\text{MIKE}}$ so that

$$\sigma \star (I_0, \dots, I_9) = \tau \star (I_0, \dots, I_9) \pmod{J_R}.$$

This check was successful for each $\tau \in S_{10}$. $\square$

Proof (Proof of Theorem 4.3). Lemma H.4 proves that the invariants in J_{MIKE} are absolute, and Lemma H.9 shows that the invariants I_{MIKE} can be recovered from J_{MIKE} up to a permutation in S_{MIKE} . The theorem now follows from Theorem 4.2. $\square$

Remark H.4. We can make Theorem 4.3 even more precise. From the proof of Lemma H.8, one can deduce the following explicit description of the invariant algebra:

$$(\mathbb{Z}[1/30][I_0, \dots, I_9]/(F_1, \dots, F_6))^{S_{\text{MIKE}}} = \mathbb{Z}[1/30][J_1, \dots, J_6]/(G),$$

where $F_1, \dots, F_6$ are the linear relations from Lemma H.6 and G is the degree-10 relation described in Equation (25). We remark that $\prod \deg(J_i) = 720 = 10 \cdot 72 = \deg(G) \cdot \# S_{\text{MIKE}}$ as expected.

H.4 A conceptual interpretation of the MIKE modular invariants

There is a more conceptual explanation behind the modular invariants we use. We first revisit the construction of symmetric level-1 theta functions on a principally polarised abelian varieties (A, λ) in terms of theta characteristic from Appendix G.3, using the theory of biextensions and cubical arithmetic.

The polarisation λ induces a biextension $\mathbf{b}_\lambda : A \times A \rightarrow B\mathbb{G}_m$ (i.e. a derived symmetric bilinear form) associated to λ . Since $2\lambda : A \rightarrow A^\vee$ has kernel $A[2]$, the biextension $2\mathbf{b}_\lambda$ is trivial on $A[2] \times A$ and on $A \times A[2]$; comparing the two trivialisations on $A[2] \times A[2]$ gives the Weil pairing $e_{2,\lambda} : A[2] \times A[2] \rightarrow \mu_2$.

A line bundle $\mathcal{L}$ associated to λ fixes a cube structure, i.e. a derived quadratic map $\mathbf{q}_\mathcal{L} : A \rightarrow B\mathbb{G}_m$ whose associated derived bilinear map $\mathbf{b}$ is $\mathbf{b}_\lambda$. Now if $\mathcal{L}$ is symmetric, we can endow it with a Σ -cube structure [Bre87, § 5], i.e. an isomorphism $[-1]^*\mathbf{q}_\mathcal{L} \simeq \mathbf{q}_\mathcal{L}$. This gives $\mathbf{b}_\lambda$ a structure of alternate biextension on $A[2] \times A[2]$ [Bre87], from which we obtain a (standard) quadratic map $q_\mathcal{L} : A[2] \rightarrow \mu_2$ whose associated symmetric bilinear form is $e_{2,\lambda}$ ($e_{2,\lambda}$ is both alternate and symmetric over $A[2]$, in the same way that $\mathbf{b}_\lambda$ can be both a symmetric and alternate biextension over $A[2]$). This is exactly the theta characteristic $q_\mathcal{L}$ from Appendix G.3. Recall that the map $\mathcal{L} \mapsto q_\mathcal{L}$ gives an isomorphism of $A[2]$ -torsors between the symmetric line bundles associated to λ and the theta characteristics associated to $e_{2,\lambda}$, because $q_{t_v^*\mathcal{L}} = q_\mathcal{L} + v$.

If $\theta_\mathcal{L}$ is a section of $\mathcal{L}$, its associated effective divisor D is symmetric under $[-1]$, so $[-1]^*\theta_\mathcal{L} = \pm\theta_\mathcal{L}$, so $\theta_\mathcal{L}$ is either even or odd with respect to $[-1]$. We have that $q_\mathcal{L}(x) = (-1)^{\text{mult}_x(D) - \text{mult}_0(D)}$ [Mum66, Proposition 2 p.307], and by Remark G.7 that $\theta_\mathcal{L}$ is even iff the additive Arf invariant $\text{Arf}(q_\mathcal{L}) = 0$, in which case we say we have an even theta characteristic. In dimension g , there are $2^{2g-1} + 2^{g-1}$ even theta characteristics and $2^{2g-1} - 2^{g-1}$ odd theta characteristics.

A symplectic decomposition $A[2] = K_1 \oplus K_2$ gives an even theta characteristic $q_0(x_1 + x_2) = e_{2,\lambda}(x_1, x_2)$, hence a level-1 even theta function θ_0 . Then the usual construction of level-(2, 2) theta functions indexed by $A[2]$, described in Appendix G.3 can be revisited using cubial arithmetic: it is given by $\theta_j^{L^4} : P \mapsto$

$\theta_0(2\tilde{P} + \tilde{T}_j)$ of the pullback of θ_0 by the isogeny $[2]$ with kernel $A[2]$, translated by suitable cubical lifts $\tilde{T}_j$ of two torsion points T_i .

More precisely, we start with a symplectic basis (U_i, U'_i) of the 4-torsion, and a choice of symmetric level-4 theta group element above each element of this basis (i.e. a choice of trivialisation of the associated étale μ_2 -torsors). This gives canonical symmetric cubical points $\tilde{U}_i, \tilde{U}'_i$, and the level $(2, 2)$ -theta coordinates are given by $\theta_{i,j} = \theta_0([2](\tilde{P} + \tilde{U}_i + \tilde{U}'_j)) = \theta_0([2]\tilde{P} + 2\tilde{U}_i + 2\tilde{U}'_j)$. (Beware that the “addition” is not commutative in cubical arithmetic, so the order matters.) For instance, in dimension $g = 2$, we have 10 even level- $(2, 2)$ theta coordinates and 6 odd ones.

As we saw in [Appendix G.3](#), a similar construction holds to build the other usual basis of level- n theta functions. For instance, we can also build level-2 theta coordinates explicitly as follows: let (T_i, T'_j) be a symplectic basis of the 2-torsion, and take a choice of symmetric lift above each elements. Let $A[2] = K_1 \oplus K_2$ the associated symplectic decomposition; a choice of symmetric lifts is induced by a choice of symplectic decomposition $A[4] = K'_1 \oplus K'_2$ above the one of $A[2]$. Now consider $A_1 = A/K_1$, the totally symmetric line bundle $\mathcal{L}^2$ descends, thanks to the choice of symmetric lifts above the T_i , to a symmetric line bundle $\mathcal{L}_1$ on A_1 . If $\phi_1 : A \rightarrow A_1$ is the associated isogeny, we saw in [Proposition G.5](#) that the theta characteristic of $\mathcal{L}_1$ (necessarily an even one), is the one associated to the symplectic decomposition $\phi_1(K'_1) \oplus \text{Ker } \phi_1$ on $A_1[2]$. (A counting argument also shows that the 2^g possible of descent of $\mathcal{L}^2$ to a symmetric line bundle on A_1 give all theta characteristics of the form $K'' \oplus \text{Ker } \phi_1$.) Let $\theta_0^{A_1}$ be a section of $\mathcal{M}$, and $\theta_0 = \theta_0^{A_1} \circ \phi_1$. Then $\theta_i(\tilde{P}) = \theta_0(\tilde{P} + \tilde{T}_i)$.

Now on our fourfolds of Weil type, we can further look at symmetric line bundles $\mathcal{L}$ invariant under $[\mathbf{i}]$; equivalently at theta characteristics $q : A[2] \rightarrow \mu_2$ such that $[\mathbf{i}]^*q = q$. An easy computation shows that there are 16 of them, and that for all of them, $q(x) = 1$ when $x \in A[1 + \mathbf{i}]$. We can then refine by considering $[\mathbf{i}]$ -theta characteristics Q , by imitating the construction of standard $[-1]$ -theta characteristics: if $\mathcal{L}$ is stable by $[\mathbf{i}]$, we fix an isomorphism $\epsilon : [\mathbf{i}]^*\mathcal{L} \simeq \mathcal{L}$ normalised at 0, and if $x \in A[1 + \mathbf{i}]$, we let $Q_{\mathcal{L}}(x) \in \mu_2$ be the scaling factor of $\epsilon(x) : ([\mathbf{i}]^*\mathcal{L})(x) \rightarrow \mathcal{L}(x)$. (The fact that the $Q_{\mathcal{L}}(x) \in \mu_2$ rather than μ_4 is because $q_{\mathcal{L}}(x) = 1$ when $x \in A[1 + \mathbf{i}]$.) Then $Q_{\mathcal{L}}$ is a quadratic form on $A[1 + \mathbf{i}]$ with associated bilinear form $e_{1+\mathbf{i}, \lambda}$, which is both symmetric and alternate over $A[1 + \mathbf{i}] \times A[1 + \mathbf{i}]$, and $[\mathbf{i}]^*\theta_{\mathcal{L}} = \pm\theta_{\mathcal{L}}$, so $\theta_{\mathcal{L}}$ is either $[\mathbf{i}]$ -even or $[\mathbf{i}]$ -odd, and this can be read off the Arf invariant of $Q_{\mathcal{L}}$. We thus obtain 10 $[\mathbf{i}]$ -even theta characteristics and 6 $[\mathbf{i}]$ -odd ones.

Finally, a symplectic decomposition $A[1 + \mathbf{i}] = K_1 \oplus K_2$ for $e_{1+\mathbf{i}, \lambda}$ gives an $[\mathbf{i}]$ -even theta characteristic Q_0 , hence a θ_0 . We could define level- $(1 + \mathbf{i}, 1 + \mathbf{i})$ theta functions indexed by $A[1 + \mathbf{i}]$ as $\theta_j^{L^2} : P \mapsto \theta_0((1 + \mathbf{i})\tilde{P} + \tilde{T}_j)$. It turns out that these are exactly the level- $(0, 2)$ theta functions constructed via our $[\mathbf{i}]$ -adapted symplectic decomposition of $A[2]$ given in [Definition G.1](#). This explains why the change of basis in [Corollary G.3](#) is exactly the same as the change of basis between level- $(2, 2)$ and level- $(0, 4)$ theta functions in dimension 2. We can

also reinterpret the action by signs and permutations on these coordinates as different choices of symplectic bases and symmetric lifts for $A[1 + \mathbf{i}]$.

Also, we remark that $A[(1 + \mathbf{i})^e]$ is a $\mathbb{Z}[\mathbf{i}]/(1 + \mathbf{i})^e$ -module of rank 4. Furthermore, given an $[\mathbf{i}]$ -adapted basis, then because $(1 + \mathbf{i})^2 = 2\mathbf{i}$ we can check that $(T'_3, T'_4; T'_1, T'_2)$ is a symplectic basis of $(A[(1 + \mathbf{i})^2], e_{(1 + \mathbf{i})^2})$, with $(T_1, T_2, T_3, T_4) = ((1 + \mathbf{i})T'_3, (1 + \mathbf{i})T'_4; (1 + \mathbf{i})T'_1, (1 + \mathbf{i})T'_2)$ is a symplectic basis of $(A[(1 + \mathbf{i})], e_{(1 + \mathbf{i})})$. This explain why the level structure data to define level $(1 + \mathbf{i}, 1 + \mathbf{i})$ -theta functions and level- $(0, 2)$ theta functions is essentially the same, when taking into account the action of $[\mathbf{i}]$.

And the decomposition $A[(1 + \mathbf{i})] = \langle T_1, T_2 \rangle \oplus \langle T_3, T_4 \rangle$ gives the theta characteristic Q_0 associated to θ_0 . We remark that $Q_0(T) = -1$ for T equal to $T_1 + T_3, T_1 + T_2 + T_3, T_4 + T_2, T_4 + T_2 + T_1, T_4 + T_3 + T_1, T_4 + T_3 + T_2$ which corresponds under the standard numbering associated to this basis to $i = 5, 7, 10, 11, 13, 14$, or in term of characteristics to the characteristics

$$\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix},$$

which are exactly the odd $(2, 2)$ -characteristic in dimension $g = 2$ too.

Now there are 720 symplectic matrices whose permutation action on the odd theta characteristics gives an isomorphism $\mathrm{Sp}_4(\mathbb{Z}/2\mathbb{Z}) \simeq S_6$. Also the action on the 10 even theta characteristics is transitive, so there are 72 matrices preserving our Q_0 . The permutation action of these 72 matrices on the 10 even characteristic gives exactly the group S_{MIKE} .

From this point of view we can now explain why our invariants behaves like arithmetic invariants (they are invariants only because we restrict to automorphisms defined over $\mathbb{F}_p$). It is because the invariants I_{MIKE} are of level $\Gamma(1 + \mathbf{i}, 2)$, while the invariants J_{MIKE} are of level $\Gamma(1, 1 + \mathbf{i})$. This is a similar phenomena that in dimension 2, the symplectic automorphism induced by $\gamma \in \Gamma/\Gamma(2, 4)$ is $\mathbb{F}_p$ -rational iff $\gamma \in \Gamma(1, 2)$.

For simplicity, we chose not to use this approach to build the modular invariants, and go instead through level-2 theta functions given by $[\mathbf{i}]$ -adapted symplectic decompositions of $A[2]$. The main reason is that because $1 + \mathbf{i}$ is not invariant under the Rosatti involution, to develop properly the theory of level- $(1 + \mathbf{i})$ theta functions we would need to first develop further the theory of Hermitian biextensions, building on the work of [Sta24].

I NIKE security

I.1 The CKS security model of a NIKE

The CKS model, introduced by Cash, Kiltz, and Shoup [CKS08], and further developed by Freire, Hofheiz, Kiltz, and Paterson in [FHKP13], is the following game-based definition of the security of a NIKE.

CKS Security. The challenger runs $\text{pp} \leftarrow \text{Setup}$ and provides the public parameters pp to $\mathcal{A}$. Furthermore, the challenger samples a random bit $b \xleftarrow{\$} \{0, 1\}$. The adversary $\mathcal{A}$ gets access to the following oracles, which can be queried adaptively and arbitrarily often:

- REGISTERHONEST: The adversary $\mathcal{A}$ provides an identity $\text{id} \in \mathcal{ID}$. The challenger runs $\text{KeyGen}(\text{pp}, \text{id})$ to generate a key pair (pk, sk) , stores the tuple $(\text{honest}, \text{id}, \text{pk}, \text{sk})$, and returns pk to $\mathcal{A}$. The oracle does not accept identities that were previously registered as corrupt.
- REGISTERCORRUPT: The adversary $\mathcal{A}$ provides both an identity $\text{id} \in \mathcal{ID}$ and a public key pk . The challenger stores the tuple $(\text{corrupt}, \text{id}, \text{pk}, \perp)$. If $\mathcal{A}$ repeatedly queries the oracle with the same id , only the most recent entry is stored. The oracle does not accept identities that were previously registered as honest.
- CORRUPTREVEAL: The adversary $\mathcal{A}$ provides two identities $\text{id}_1, \text{id}_2 \in \mathcal{ID}$, where one identity is registered as corrupt and the other as honest. If id_1 is honest, the challenger runs $\text{MIKE.SharedKey}(\text{id}_2, \text{pk}_2, \text{id}_1, \text{sk}_1)$ using the public key pk_2 corresponding to id_2 and the secret key sk_1 corresponding to id_1 , and outputs the shared key K to $\mathcal{A}$. Otherwise it proceeds similarly, running $\text{MIKE.SharedKey}(\text{id}_1, \text{pk}_1, \text{id}_2, \text{sk}_2)$. If both identities are registered as corrupt or honest, the challenger outputs $\perp$.
- TEST: The adversary $\mathcal{A}$ provides distinct, honestly registered identities $\text{id}_1, \text{id}_2 \in \mathcal{ID}$. The challenger computes $K_0 = \text{MIKE.SharedKey}(\text{id}_1, \text{pk}_1, \text{id}_2, \text{sk}_2)$ using the public key pk_1 corresponding to id_1 and the secret key sk_2 corresponding to id_2 . The challenger further samples a random $K_1 \xleftarrow{\$} \mathcal{SHK}$ and stores $(\text{id}_1, \text{id}_2, K_1)$. It outputs K_b based on the chosen bit b . If $\mathcal{A}$ has queried the same identities $\{\text{id}_1, \text{id}_2\}$ before in any order and $b = 1$, the challenger outputs the previously stored key K_1 .

We say that a NIKE is $(\varepsilon, Q_{\text{RH}}, Q_{\text{RC}}, Q_{\text{CR}}, Q_{\text{T}}, Q_{\text{H}})$ -secure in the CKS model, if any quantum polynomial time adversary $\mathcal{A}$ against the CKS game, that makes at most Q_{RH} REGISTERHONEST, Q_{RC} REGISTERCORRUPT, Q_{CR} CORRUPTREVEAL, Q_{T} TEST queries (classically), and Q_{H} queries to the random oracle H (potentially in superposition) has advantage

$$\text{Adv}_{\text{NIKE}}^{\text{CKS}}(\mathcal{A}) := |\Pr[b = b'] - 1/2| < \varepsilon.$$

CKS-light security. This game has the same oracles as the CKS security game, but the adversary is limited to calling REGISTERHONEST only twice and TEST once. The other oracles can be queried arbitrarily often. The definition of a NIKE being secure in the CKS-light model is the same as for the CKS model (with the obvious modifications).

CKS vs. CKS-light. The CKS and CKS-light models are polynomially equivalent. More precisely, we have the following theorem.

Theorem I.1 ([FHKP13, Th. 1]). *For any adversary $\mathcal{A}$ against a non-interactive key exchange scheme NIKE in the CKS model making at most q_H REGISTERHONEST queries and q_T distinct TEST queries, there is an adversary $\mathcal{B}$ against NIKE in the CKS-light model with $\text{Adv}_{\text{NIKE}}^{\text{CKS}}(\mathcal{A}) \leq (1/2)q_H^2q_T\text{Adv}_{\text{NIKE}}^{\text{CKS-light}}(\mathcal{B})$.*

I.2 Proof of Theorem 5.1

We prove Theorem 5.1 by analysing a sequence of games, which in large part are identical to those of proof of [DHK+22, Thm. 5]; the differences are that we use CKS-light instead of CKS, and remove the randomisation technique that is not available in the MIKE setting. Let $\mathcal{A}$ be a quantum adversary, and assume without loss of generality that $\text{id}_1 < \text{id}_2$ throughout.

Game G_1 . The first game is the standard CKS-light security game. By definition $|\Pr[G_1^{\mathcal{A}} \Rightarrow 1] - 1/2| = \text{Adv}_{\text{MIKE}}^{\text{CKS-light}}(\mathcal{A})$.

Game G_2 . The game precomputes two honest key pairs $(\text{pk}_i, \text{sk}_i)$ and stores them in a set $\mathcal{H}$. On the adversary's i -th REGISTERHONEST query, the game returns the public key of $\mathcal{H}[i]$. Since the output of KeyGen does not depend on the input id provided by $\mathcal{A}$, this does not change the distribution of the output of REGISTERHONEST, hence $\Pr[G_2^{\mathcal{A}} \Rightarrow 1] = \Pr[G_1^{\mathcal{A}} \Rightarrow 1]$.

Game G_3 . In this game, the random oracle H is conceptually partitioned to allow simulation at a later phase. When the adversary queries $H(\text{id}_1, \text{id}_2, \text{pk}_1, \text{pk}_2, J)$, the game responds as follows

- If $(\text{pk}_i, \text{sk}_i) \in \mathcal{H}$, $(\text{pk}_{3-i}, *) \notin \mathcal{H}$, and $J = J_{\text{MIKE}}(\text{sk}_i \cdot \text{pk}_{3-i})$, it returns $H_1(\text{id}_1, \text{id}_2, \text{pk}_1, \text{pk}_2)$ for an internal independent random oracle H_1 .
- If both keys are honestly generated (i.e. $(\text{pk}_1, \text{sk}_1), (\text{pk}_2, \text{sk}_2) \in \mathcal{H}$), and $J = J_{\text{MIKE}}(\text{sk}_1 \cdot \text{pk}_2)$, it returns $H_3(\text{id}_1, \text{id}_2, \text{pk}_1, \text{pk}_2)$ for another internal random oracle H_3 .
- Else it returns $H_2(\text{id}_1, \text{id}_2, \text{pk}_1, \text{pk}_2, J)$ for another internal random oracle H_2 .

These changes are only conceptual, hence $\Pr[G_3^{\mathcal{A}} \Rightarrow 1] = \Pr[G_2^{\mathcal{A}} \Rightarrow 1]$.

Game G_4 . In this game, the CORRUPTREVEAL oracle is modified. If only one of the keys lies in $\mathcal{H}$, the game returns $H_1(\text{id}_1, \text{id}_2, \text{pk}_1, \text{pk}_2)$. If both keys lie in $\mathcal{H}$, the game returns $H_3(\text{id}_1, \text{id}_2, \text{pk}_1, \text{pk}_2)$. Since the original CORRUPTREVEAL oracle computes the shared secret correctly, already in G_3 the corresponding queries would have been forwarded to H_1 or H_3 by H . Hence, directly calling H_1 or H_3 is only a conceptual change, and we obtain $\Pr[G_4^{\mathcal{A}} \Rightarrow 1] = \Pr[G_3^{\mathcal{A}} \Rightarrow 1]$.

Game G_5 . In this game, the TEST oracle is modified to compute $K_0 = H_3(\text{id}_1, \text{id}_2, \text{pk}_1, \text{pk}_2)$. This is only a conceptual change due to the modifications to H from G_3 , and hence we obtain $\Pr[G_5^{\mathcal{A}} \Rightarrow 1] = \Pr[G_4^{\mathcal{A}} \Rightarrow 1]$.

Game G_6 . In this game H is reprogrammed on the singleton set $\mathcal{S} = \{(*, *, \text{pk}_1, \text{pk}_2, \text{sk}_1 \cdot \text{pk}_2) \mid (\text{pk}_1, \text{sk}_1), (\text{pk}_2, \text{sk}_2) \in \mathcal{H}\}$, with a uniformly random value $\{0, 1\}^\kappa$. Recall that $\mathcal{S}$ corresponds to the valid TEST query. This reprogramming only affects H_3 , and we derive the reprogramming through an internal random oracle H'_3 . From the adversary's view, K_0 and K_1 are identically distributed, hence we obtain $\Pr[G_6^A \Rightarrow 1] = 1/2$.

To bound $|\Pr[G_6^A \Rightarrow 1] - \Pr[G_5^A \Rightarrow 1]|$, we use the semi-classical *one-way to hiding* (O2H) lemma with the punctured oracle $H \setminus \mathcal{S}$, and the classical event FIND that is set to 1 if the extractor finds an element of $\mathcal{S}$ (see [DHK+22, App. B] for details and definitions). Note that the membership test for some input to be in $\mathcal{S}$ can be done using the DDH oracle. Following [DHK+22], we define G_7^A as G_5^A but with access to $H \setminus \mathcal{S}$, and we obtain

$$|\Pr[G_6^A \Rightarrow 1] - \Pr[G_5^A \Rightarrow 1]| \leq 2\sqrt{(d+1) \Pr[\text{FIND} : G_7^A]}$$

The qGapCDH adversary. Finally, we define the adversary $\mathcal{B}$ against qGapCDH to bound $\Pr[\text{FIND} : G_7^A]$. Denote the DDH oracle in the qGapCDH problem by O . On input the challenge $(\text{pk}_1, \text{pk}_2)$, $\mathcal{B}$ runs the O2H extractor with $\mathcal{A}^{O, H \setminus \mathcal{S}}$, and embeds its challenge public keys $(\text{pk}_1, \text{pk}_2)$ as $\mathcal{A}$'s two honest key registrations. It is able to simulate the oracles H_1 , H_2 , H_3 , and H'_3 , and the games $G_3 - G_6$ with standard techniques, exploiting the oracle O for all checks including shared secrets. When obtaining $\text{FIND} = 1$ it measures the input registers of $H \setminus \mathcal{S}$, which outputs a set $\mathcal{T}$. $\mathcal{B}$ then searches for $(*, *, \text{pk}_1, \text{pk}_2, J) \in \mathcal{T}$ with $O(\text{pk}_1, \text{pk}_2, J) = 1$, and on an accepting candidate returns the valid solution J . Thus, $\mathcal{B}$ wins when $\text{FIND} = 1$ and we obtain $\Pr[\text{FIND} : G_7^A] \leq \text{Adv}_{\text{MIKE}}^{\text{qGapCDH}}(\mathcal{B})$.

J On the choice of parameters

This section is devoted to an analysis of MIKE parameters. For MIKE, we mainly have two choices to make that determine the security level.

The most important one is the choice of our base prime p . Since we use 2^e -isogenies to compute the key exchange, we ask that p is of the form $c2^f - 1$ for a large enough f . The second choice is the length e of our secret dimension-1 2^e -isogenies (over $\mathbb{F}_{p^2}$). This length also determine the length of the dimension-4 isogenies (over $\mathbb{F}_p$) computed during the key exchange. Note that this choice is constrained by $e \leq f - 2$, because of the extra torsion requirement used to normalise our curves and to compute 2^e -isogenies in higher dimension.

In the initial implementation of MIKE, we simply reused SQIsign's (round 2) primes, using the maximal value possible $e \approx \log_2(p)$ for our two isogeny length e . This fit nicely with our security proof from Section 5. The recent attack of Wesolowski [Wes26] forced us to reevaluate our parameters and increase the size of our primes. As we will see in Appendix J.3, our security proof requires that we fix $e \approx \log_2(p)$. On the other hand, because of the increased size of p , such a value for e is overkill compared to the best known attack to directly recover a 2^e -isogeny. On top of that, there is no clear choice for the value of p ,

because the new attack requires a lot of memory. Depending on whether we allow unbounded or very large but bounded memory (as in the round 3 submission of SQIsign), and also whether we take into account the hidden polynomial factors in the Wesolowski’s attack, estimates for the size of p can vary greatly (e.g. from 300 bits to 384 bits for NIST level I).

For these reasons, in this section, we will suggest “conservative” as well as more “aggressive” parameters for p, e , which form the basis of **RigorousMIKE** and **FastMIKE** respectively. In **RigorousMIKE** we make very conservative choices on the choices of p , and use $e \approx \log_2(p)$ for our security proof reduction. For **FastMIKE** we make more aggressive choices for the size of our primes (but without being too aggressive, see [Remark J.5](#)), and take $e \approx 2/3 \log_2(p)$. A drawback is that the security proof does not hold anymore (or rather loses too many bits).

First, we analyze the two known approaches to break MIKE in [Appendices J.1](#) and [J.2](#), which are

- Recovering the $\mathbb{F}_{p^2}$ -endomorphism ring of E_A (or E_B).
- Directly recovering the secret isogeny $\phi_A : E_0 \rightarrow E_A$.

Then, in [Appendix J.3](#), we explain the further constraints on our parameters needed so that our security reduction hold. Lastly, in [Appendix J.4](#) we suggest some parameters, notably for **RigorousMIKE** and **FastMIKE**.

We stress that Wesolowski’s attack is very recent, and once further analysis is done on how optimised it can be, we will be able to further tune our choices of primes. As this section will show, MIKE is very flexible in the possible choice of parameters (even more than SQIsign), and we welcome the community to do more analysis on the security and performance of different parameters.

J.1 Recovering the endomorphism ring

The complexity of the supersingular endomorphism ring computation was recently improved by Wesolowski in [\[Wes26\]](#) from $\tilde{O}(\sqrt{p})$ to $p^{1/3+o(1)}$ via a MITM attack. In our initial implementation of MIKE, we were using the same primes as in SQIsign’s round 2 NIST submission, of size $\approx 2\lambda$ where λ is the security parameter. To account for Wesolowski’s attack, we need to increase the prime size.

We note that although the original $\tilde{O}(\sqrt{p})$ attack required (almost) no memory, Wesolowski’s new attack is a time memory trade off: it takes time $(p/w)^{\frac{1+o(1)}{2}}$ given enough memory to store w j -invariants simultaneously. Using $w = p^{1/3}$ gives the $p^{1/3+o(1)}$ time complexity above, and giving a bound w on the number of j -invariants give a size for p of $\log_2(p) = 2\lambda + \log_2(w)$. We refer to [\[Wes26\]](#) and [\[AAA+26, Chapter 8\]](#) for more details.

Conservative choices for p give the attacker unlimited memory (or rather $w = 2^\lambda$ and ignore the extra hidden polynomial factors in the $o(1)$). This gives a size of p of roughly 3λ bits. To account for the fact that memory is usually more expensive than time, in [\[AAA+26, § 8.2.1.2\]](#) suggest to use $w = \lambda^{5/8}$. More precisely they allow 2^{80} , 2^{120} and 2^{160} j -invariants for NIST level I, III and V

respectively. We remark that storing a j -invariant itself requires $2\log_2(p)$ bits of memory. This gives a size of $\log_2(p) = 21/8 \cdot \lambda$ for the more aggressive choices.

Taking into account the hidden log factor allows for some leeway. Indeed, the current best known instantiation of Wesolowski’s MITM attack involves finding roots of very large modular polynomials. Taking the amortised cost of one root over $\mathbb{F}_q$ to be at least $\log_2 q$ field operations (we note this cost is only valid for roots of small degree, e.g. taking a square root; in general this complexity minors the actual complexity of Cantor-Zassenhaus, see [AAA+26, Remark 8.2.1]), we see that for instance a prime p of size 320, with an allowed memory of 2^{80} j -invariants give an estimation of at least $\sqrt{2^{320}/2^{80}} \times \log_2(p^2) \approx 2^{129}$ fields operations over $\mathbb{F}_{p^2}$.

We refer to [AAA+26, § 8.2.1.2] for a more detailed classical and quantum analysis of these parameters.

J.2 Finding the secret 2^e -isogeny.

The best attack to find $\phi_A : E_0 \rightarrow E_A$ is also a meet in the middle attack, constructing $2^{e/2}$ -isogenies from both E_0 and E_A until a collision is found. This problem was thoroughly studied for the SIDH protocol. We refer to [ACCMR19] for a nice survey of the classical and quantum cost of the MITM approach. Like for the endomorphism ring problem (which ultimately also reduces to a MITM attack), there is a time memory trade off using Van Oorschot and Wiener golden collisions. Let $N = 2^e$ and w the number of j -invariant that are allowed to be stored simultaneously then the attack needs to produce at least $N^{3/4}/\sqrt{w}$ j -invariants [ACCMR19, Remark 3].

Using $w = 2^\lambda$ gives $e = 2\lambda$, while the more aggressive choice of $w = \lambda^{5/8}$ gives $e = 7/4\lambda$. We remark that to have balanced attack costs for both approaches, allowing w j -invariants, suggest to use $\log_2(p) = 2\lambda + \log_2(w)$ and $e = 4/3\lambda + 2/3\log_2(w) = 2/3\log_2(p)$.

Remark J.1. Here we need to account for the fact that ultimately our secret is not the secret isogeny itself, but the rank 2 module it induces. Now on the starting curve E_0 we have an automorphism by [i]. By Section 4.1, our basis of the 2^e -torsion $(P, Q) = [2^{f-e}](P_0, Q_0)$ is sampled such that P is rational and $[i]P = Q$. A generator of kernel of the secret isogeny is chosen as $T = P + [x_A]Q$. It follow that $[i]T = Q - [x_A]P$ gives the same codomain E_A . Also $\sigma(T) = [\pi_p](T) = P - x_A Q$, gives the codomain E_A^σ , which induces the same Weil restriction, and same Scholten, hence same rank 2 module, as E_A . It follows that $\{x_A, -x_A, 1/x_A, -1/x_A\}$ all correspond to the same secret rank 2 unimodular module. Furthermore we want x_A to be odd so that T is of exact order 2^e (for constant time reasons), and for technical reasons in the gluing we want $x_A \equiv 3, 5 \pmod{8}$. (Because x_A and $-x_A$ will give the same rank 2 module, in the implementation we fix $x_A \equiv 3 \pmod{8}$.) Taking into account these trivial conditions, it follows that key generation will only generate $2^{e-4} - \epsilon$ different rank 2 modules. (The ϵ is to take into account “true” collisions, where genuinely different 2^e -isogenies give the same curve up to the Galois action. These are extremely rare, both theoretically and as confirmed by our implementation.)

Remark J.2. Another important remark is that in the complexity estimate the ignored polynomial factors are much smaller than for the endomorphism ring computation. This is because the intermediate j -invariants in the MITM are produced by computing a tree of 2-isogenies, which is much less expensive than finding roots of very large polynomials. It follows that there is less leeway in the choice of e . Accounting for [Remark J.1](#), we will use $e = 7/4\lambda + 4$ for the aggressive parameters. Note that for $\lambda = 128$ this gives $e = 228$. Following [\[ACCMR19\]](#), the SIKE spec had for parameters SIKEp434, which used 2^{216} -isogenies. And although SIKE was ultimately broken, it was not because of the MITM attack, but rather because of the extra torsion point informations needed by the protocol! We note that our suggest NIST level 1 $e = 228$ is larger than 216, so in a sense even our “aggressive” parameters are fairly conservative.

J.3 On the security proof

We note that the above security analysis look at directly recovering the secret key. This is the analogue of DLOG in a standard DH key-exchange. The security of MIKE however, relies on the equivalent of CDH. In [Theorem 5.2](#) we give a security reduction from the EndRing problem to MIKE’s CDH.

However, there are two caveats to this security reduction. The first one is that it is valid only in the AIM+ model. Most importantly, if $p = C2^e - 1$, it involves a loss of security of $\log_2(C)$ bits.

Our previous analysis suggested to use $e \approx 2/3 \log_2(p)$, this means that $\log_2(C) \approx 1/3 \log_2(p)$, which essentially makes the security reduction useless because it loses too many bits.

It means that there are two choices to make with respect to the parameters:

- We fix $p = c2^f - 1$ with c odd and as small as possible. We take the largest e allowed by our HD isogeny formulas: $e = f - 2$, so that $C = 4c$ is small, and our security reduction is valid. We then want p large enough that the average EndRing problem has security at least λ (in a bounded or unbounded memory model). We note that the constraint on small c is also present in SQIsign.
- We relax the condition for our parameters to be in our regime where our security proof hold. In particular we allow our isogeny length to be smaller than $\log_2(p)$. In this case, we make the **heuristic** assumption that breaking MIKE’s CDH amount to breaking MIKE’s DLOG, i.e. recovering the secret rank 2 module (M_A, H_A) given (E_0, E_A) . We remark that by [\[Rob24b, Theorem 5.5, Theorem 5.22\]](#), from (M_A, H_A) we can efficiently recover $\text{End}(E_A)$, and conversely. However, because of our shortish isogeny path, we are no longer in the average EndRing problem regime. So we make another **heuristic** assumption that beside the generic endomorphism ring attacks, the best way to exploit the smaller isogeny $E_0 \rightarrow E_A$ is to directly recover it via the MITM attack.

So in this case we fix $p = C2^{e+2} - 1$, with p large enough so that the average EndRing problem has security at least λ bits, and e large enough

that directly solving the 2^e -isogeny path problem between E_0 and E_A via a MITM has also security λ . Concretely, by the discussion in [Appendix J.2](#), this means $e \approx 2/3 \log_2(p)$. This allows to look for any $p = c2^f - 1$ large enough, as long as $f \geq e - 2$, so c can be as large as $p^{1/3}$. This gives a lot more freedom in the choice of p than above, or compared to the SQIsign primes.

Remark J.3 (The impact of c on performance). For performance, SQIsign has much more constraints on the cofactor c than MIKE. For instance SQIsign currently uses $p = 3 \cdot 2^{324} - 1$ for level I, which is slightly above 5 words. Using $p = 55 \cdot 2^{305} - 1$ instead, although it fits in only 5 words, the key generation and signature is slower, only the verification is faster.

In MIKE's implementation, c only affects the Hamming weight of the cofactor clearing (i.e. multiplication by $[C] = [c2^{f-e}]$ on an elliptic curve), so its impact is essentially negligible compared to the rest of the 2^e -isogeny computations (in dimension 1 for keygen in dimension 4 for the shared secret). Note however that in the example above, $c = 3$ only loses 1.6 bits in the security reduction, vs 5.7 bits for $c = 55$.

Remark J.4 (Supersingularity testing). Our key validation is a supersingularity test, which is done on the fly in [Algorithm 8](#). More precisely this algorithm tests that the curve $E/\mathbb{F}_{p^2}$ has a $\mathbb{F}_{p^2}$ -rational basis of 2^f -torsion. From the Hasse bound, this guarantees that $\#E(\mathbb{F}_{p^2}) = (p+1)^2$, hence that $E/\mathbb{F}_{p^2}$ is maximal supersingular, as long as $2^{2f} > 4p$, i.e., if $p = c2^f - 1$, $2^{f-2} \geq c$. This will be the case for all our parameters.

J.4 Proposed MIKE parameters

As the discussion above show, there is a wide range of choice for MIKE parameters: bounded or unbounded memory for adversaries, parameters for which the security reduction of [Section 5](#) hold or not. We propose several concrete choices.

1. We allow unbounded memory for the adversaries.
This means (ignoring any extra polynomial factors in the existing attacks), we want $\log_2(p) \approx 3\lambda$. We suggest $p = 117 \cdot 2^{374} - 1$, $p = 77 \cdot 2^{566} - 1$, and $p = 41 \cdot 2^{758} - 1$ for NIST level I, III and V respectively, which have small c and are calibrated to be under the 64 bits word boundaries. We then take $e = 372, 564, 756$ as large as possible for our security reduction. These parameters give **RigorousMIKE**.
An implementer willing to rely on heuristic security instead can take $e = 2\lambda + 4$, i.e. $e = 260, 388, 516$ respectively, since the best known attack with unbounded memory still give 128, 192 and 256 bits of security.
2. We only allow bounded memory, and take roughly the same prime sizes as in SQIsign [[AAA+26](#)]: $\log_2(p) \approx 325, 504, 668$. We can simply reuse the exact same primes, for compatibility: $p = 3 \cdot 2^{324} - 1, p = 27 \cdot 2^{500} - 1, p = 17 \cdot 2^{664} - 1$. We then either take $e = 322, 498, 662$ as large as possible, or take $e = 7/4\lambda + 4$ (accounting for the bounded memory), which gives $e = 228, 340, 452$.

3. We only allow bounded memory, but for the endomorphism ring attack we modelize the cost of each j -invariant as needing at least $\log_2(p^2)$ field operations rather than just 1. This gives sizes for p of 317, 484 and 651 bits respectively. We propose $p = 633 \cdot 2^{308} - 1$, $p = 593 \cdot 2^{474} - 1$, and $p = 317 \cdot 2^{628} - 1$, which under the model above give 2^{128} , $2^{191.5}$ and $2^{248.5}$ $\mathbb{F}_{p^2}$ field operations respectively. In terms of performances, the main advantage of these primes compared to the SQIsign primes above is that the first and third one are close to their word boundaries.

We then either take $e = 306, 472, 626$ as large as possible, or take $e = 7/4\lambda + 4$ which gives $e = 228, 340, 452$. The later choice gives the parameters for FastMIKE.

Remark J.5 (Even more aggressive parameters). Although FastMIKE is tailored for performance, we still tried to stay reasonably conservative in our choice of parameters. On our choice of p , [AAA+26, Appendix P] list choices of primes “that may still fulfil the NIST security requirements”. This list goes down up to 308 bits, 460 bit and 607 bits for NIST level I, III and V, while our primes for FastMIKE have 318 bits, 484 bits and 637 bits respectively.

On the choice of e , for NIST level I we use $e = 228$, while as mentioned above the SIDH spec had SIKEp434 for NIST level I, which used $e = 216$, and [LWS21] even suggested $e = 191$.