FAST COMPUTATION OF 2-ISOGENIES IN DIMENSION 4 AND CRYPTOGRAPHIC APPLICATIONS

PIERRICK DARTOIS

Abstract. Dimension 4 isogenies have first been introduced in cryptography for the cryptanalysis of Supersingular Isogeny Diffie-Hellman (SIDH) and have been used constructively in several schemes, including SQIsignHD, a derivative of SQIsign isogeny based signature scheme. Unlike in dimensions 2 and 3, we can no longer rely on the Jacobian model and its derivatives to compute isogenies. In dimension 4 (and higher), we can only use theta-models. Previous works by Romain Cosset, David Lubicz and Damien Robert have focused on the computation of ℓ-isogenies in theta-models of level n coprime to ℓ (which requires to use n^g coordinates in dimension g). For cryptographic applications, we need to compute chains of 2-isogenies, requiring to use $\geq 3^g$ coordinates in dimension g with state of the art algorithms.

In this paper, we present algorithms to compute chains of 2-isogenies between abelian varieties of dimension $g \geq 1$ with theta-coordinates of level $n = 2$, generalizing a previous work by Pierrick Dartois, Luciano Maino, Giacomo Pope and Damien Robert in dimension $g = 2$. We propose an implementation of these algorithms in dimension $g = 4$ to compute endomorphisms of elliptic curve products derived from Kani's lemma with applications to SQIsignHD and SIDH cryptanalysis. We are now able to run a complete key recovery attack on SIDH when the endomorphism ring of the starting curve is unknown within a few seconds on a laptop for all NIST SIKE parameters.

1. Introduction

Higher dimensional isogenies have become a popular and widely used tool in cryptography since they were introduced to attack the Supersingular Isogeny Diffie-Hellman (SIDH) key exchange [22–24]. The attacks against SIDH used a result due to Kani [26, proof of Theorem 2.3], abusively called Kani's lemma, to "embed" a (presumably secret) isogeny φ between elliptic curves into an isogeny F between elliptic products of dimension $2, 4$ or 8. This higher dimensional isogeny F could be computed in polynomial time given images of φ on some torsion points, that were given in SIDH. The ability to evaluate F could be used to evaluate φ everywhere, leading to a full key recovery.

With this new method involving higher dimensional isogenies, we are now able to evaluate an isogeny everywhere given its images on torsion points. This allows in particular to evaluate non-smooth degree isogenies efficiently [32], which could not be done with previous state of the art techniques. After its cryptanalytic use against SIDH, Kani's lemma has been leveraged for several constructive applications in cryptography: among others, the public-key encryption schemes FESTA [27] and its improvement QFESTA [28], SQIsignHD [5] followed by [6–9] improving the digital signature NIST candidate SQIsign [4], SCALLOP-HD [29] improving

2020 *Mathematics Subject Classification.* 14K02; 14Q15; 11T71.

the SCALLOP group action [30], a key encapsulation mechanism IS-CUBE [31] and a verifiable random function DeuringVRF [21]. From an algorithmic point of view, Kani's lemma offers a way to make the Deuring correspondence between ideals of an elliptic curve endomorphism ring and isogenies defined on this elliptic curve effective for ideals of non-smooth norms [25]. This effective way to translate ideals into isogenies has been leveraged in SQIsignHD and follow-up works [5–7, 9], DeuringVRF [21] and also in the group action setting [29] where an orientation of elliptic curves is fixed.

1.1. **Previous works.** In the works of W. Castryck, T. Decru, L. Maino, C. Martindale, L. Panny, G. Pope and B. Wesolowski against SIDH [23, 24], dimension 2 isogenies were used which constrained the attack. When the endomorphism ring of the starting curve is unknown, a subexponential search for parameter tweaks and a subexponential auxiliary 1-dimensional isogeny computation were necessary. In [22, § 2, 4], D. Robert proved that using dimension 4 or 8 isogenies would relax these constraints and make the attack polynomial. Unlike 2-dimensional attacks[1], Robert's 4-dimensional attack has not been implemented yet.

Finding fast higher dimensional isogeny formulas was not crucial to cryptanalytic applications but has become relevant to constructive applications. Most applications use 2-dimensional isogenies and some of them use 4-dimensional isogenies [5, 21]. In dimension 2, state of the art techniques using Richelot isogenies [33, 34] became the bottleneck of these cryptographic protocols, making them impractical. Recently, efficient formulas using theta coordinates have been introduced to compute 2-dimensional 2 and 3-isogenies [1, 2].

While still useful in practice, especially for SQIsignHD [5], 4-dimensional isogenies have been the focus of very little attention. Algorithmic efforts have been made to compute ℓ-isogenies between abelian varieties of any dimension in the Theta model [35–37]. The state of the art technique [37] enables to compute ℓ-isogenies between abelian varieties of dimension g with theta-coordinates of level n coprime to ℓ in time $O((n\ell)^g)$. In particular, we can compute 2-isogenies using n^g theta-coordinates of level n with $n \geq 3$. Generalizing this method to level $n = \ell = 2$ is essential to reduce complexity. This has been done and implemented in dimension 2 [1], leading to very fast computations. The algorithmic approach of [1] was based on formulas valid in any dimension introduced in a note by Damien Robert [18, Chapter 7]. However, no proof was provided for these formulas.

1.2. **Our contribution.** In this paper, we generalize the algorithms of [1] to compute 2-isogenies in any dimension g with level 2 theta-coordinates. We provide proofs for the formulas introduced in [18, Chapter 7]. We also introduce and prove formulas to change theta-coordinates required for isogeny computations. Finally, we provide an implementation of 4-dimensional 2-isogenies with applications to SQIsignHD[2] and SIDH torsion point attacks with a random starting curve [22] along with implementation details that were missing in the original SQIsignHD paper [5, Appendix F].

[1]See `https://github.com/Breaking-SIDH/direct-attack` and `https://github.com/GiacomoPope/Castryck-Decru-SageMath`

[2]This implementation can be found here `https://github.com/Pierrick-Dartois/SQISignHD-lib`.

Section 2 recalls foundational notions on polarized abelian varieties and theta functions, following the approach of Mumford [15]. Section 3 introduces a formula to compute new theta-coordinates associated to a change of symmetric theta-structure. In Section 4, we provide formulas and an algorithmic approach to compute chains of 2-isogenies in any dimension g. In Section 5, we apply this approach to the computation of 4-dimensional 2^e-isogenies between elliptic products derived from Kani's lemma, e.g. in the context of SQIsignHD and SIDH torsion attacks. Our SIDH attacks run in a few seconds on a laptop for all NIST SIKE parameters. Appendix B and Appendix C give implementation details, focusing on how to compute the necessary changes of theta-coordinates in this context. Finally, Appendix E explains how optimal divide an conquer strategies can be adapted to compute chains of 4-dimensional isogenies.

2. Preliminaries on the Theta model

2.1. **Polarized abelian varieties.** In the following, k is an algebraically closed field of characteristic $\mathrm{char}(k) \neq 2$ and A is an abelian variety of dimension g defined over k. Abelian varieties are projective connected group varieties. By rigidity, their group structure is always abelian [3, Corollary 2.4]. In particular, elliptic curves are abelian varieties of dimension 1.

An *isogeny* between abelian varieties is a group variety homomorphism (homomorphism of varieties respecting the group law) which is surjective and has finite kernel. In particular, if $f : A \longrightarrow B$ is an isogeny, then A and B have the same dimension. As in dimension 1, in higher dimension, we can compute f with the knowledge of $\ker(f)$. This will be the goal of this paper.

A *line bundle* $\mathcal{L}$ over A is a locally free sheaf of $\mathcal{O}_A$-modules of rank 1. This means that $\mathcal{L}$ is locally isomorphic to the sheaf of regular functions $\mathcal{O}_A$ of A. Isomorphism classes of line bundles on A form a group denoted by $\mathrm{Pic}(A)$ [13, Chapter 7, p. 178]. Line bundles can be seen as divisors, since there is a group isomorphism between $\mathrm{Pic}(A)$ and equivalence classes of divisors modulo principal divisors [14, Proposition II.6.15]. We denote by $\mathrm{Pic}^0(A)$ the subgroup of line bundles invariant by translation:

$$\mathrm{Pic}^0(A) = \{[\mathcal{L}] \mid \forall a \in A(k), \quad t_a^*\mathcal{L} \cong \mathcal{L}\}.$$

$\mathrm{Pic}^0(A)$ identifies with the group of k-rational points $\widehat{A}(k)$ of the *dual abelian variety* $\widehat{A}$. If $\mathcal{L}$ is a line bundle on A generated by global sections $s_1, \cdots, s_n \in \Gamma(A, \mathcal{L})$ *i.e.* when $s_{1,x}, \cdots, s_{n,x}$ generate the stalk $\mathcal{L}_x$ for all $x \in A$, these global sections define a morphism of k-varieties $A \longrightarrow \mathbb{P}_k^{n-1}$ [14, Theorem II.7.1]. We say that $\mathcal{L}$ is *very ample* when it induces such a map $A \longrightarrow \mathbb{P}_k^{n-1}$ which is a closed immersion and that $\mathcal{L}$ is *ample* when one of its powers is very ample. Abelian varieties are projective [3, Theorem 7.1] so (very) ample line bundles always exist on A.

Given a line bundle $\mathcal{L}$ on A, one defines a group homomorphism $\varphi_{\mathcal{L}} : A(k) \longrightarrow \mathrm{Pic}(A), a \longmapsto [t_a^*\mathcal{L} \otimes \mathcal{L}^{-1}]$. As a consequence of the theorem of the square [3, Theorem 6.7], this homomorphism maps into $\mathrm{Pic}^0(A)$ [3, Proposition 10.1]. When $\mathcal{L}$ is ample, $\varphi_{\mathcal{L}}$ has finite kernel. In that case, $\varphi_{\mathcal{L}}$ defines an isogeny $A \longrightarrow \widehat{A}$, which is called a *polarization* of A. We say that $(A, \varphi_{\mathcal{L}})$ or $(A, \mathcal{L})$ is a *polarized abelian variety*. Intuitively, a polarization on A might be seen as a way to orient A. We can derive models from them (*eg.* the Theta model). We say that $\mathcal{L}$ or $\varphi_{\mathcal{L}}$ is *separable* when $\mathrm{char}(k) \nmid \deg(\varphi_{\mathcal{L}})$. **Throughout this paper, we shall assume that line bunldes are ample and separable.**

We say that a polarization $\varphi_{\mathcal{L}}$ is *principal* and that $(A, \mathcal{L})$ is a *principally polarised abelian variety (PPAV)* when $\varphi_{\mathcal{L}}$ is an isomorphism $A \xrightarrow{\sim} \widehat{A}$. All elliptic curves are principally polarized but this is not the case of all abelian varieties. If $(A, \mathcal{L}_0)$ and $(B, \mathcal{M}_0)$ are PPAVs and $f : A \longrightarrow B$ is an isogeny and $d \in \mathbb{N}^*$, we say that f is *d-isogeny* when $\widehat{f} \circ \varphi_{\mathcal{M}_0} \circ f = [d] \circ \varphi_{\mathcal{L}_0}$ *i.e.* $\widetilde{f} \circ f = [d]$, where $\widetilde{f} := \varphi_{\mathcal{L}_0}^{-1} \circ \widehat{f} \circ \varphi_{\mathcal{M}_0}$. By abuse, we shall call $\widetilde{f}$ the dual of f (instead of $\widehat{f}$). If $\mathcal{L}$ and $\mathcal{M}$ are polarisations on A and B respectively, we say that f is a *polarised isogeny* from $(A, \mathcal{L})$ to $(B, \mathcal{M})$ and denote $f : (A, \mathcal{L}) \longrightarrow (B, \mathcal{M})$ when $\widehat{f} \circ \varphi_{\mathcal{M}} \circ f = \varphi_{\mathcal{L}}$. If $\mathcal{L} = \mathcal{L}_0^d$ and $\mathcal{M} = \mathcal{M}_0$, then f is a d-isogeny if and only if it is a polarised isogeny $(A, \mathcal{L}) \longrightarrow (B, \mathcal{M})$. Indeed, we have $\varphi_{\mathcal{L}} = \varphi_{\mathcal{L}_0^d} = [d] \circ \varphi_{\mathcal{L}_0}$ by the theorem of the square [3, Theorem 6.7].

2.2. **The Theta group.** Let $\mathcal{L}$ be an ample and separable line bundle on A and $K(\mathcal{L}) := \{x \in A(k) \mid t_x^* \mathcal{L} \cong \mathcal{L}\}$ be the kernel of $\varphi_{\mathcal{L}}$. The *theta-group* of $\mathcal{L}$, denoted by $G(\mathcal{L})$ is made of pairs (x, ϕ_x), where $x \in K(\mathcal{L})$ and ϕ_x is an isomorphism $\mathcal{L} \xrightarrow{\sim} t_x^* \mathcal{L}$ (which always exists by the definition of $K(\mathcal{L})$). $G(\mathcal{L})$ is indeed a group for the group law given by $(x, \phi_x) \cdot (y, \phi_y) := (x+y, t_x^* \phi_y \circ \phi_x)$ for all $(x, \phi_x), (y, \phi_y) \in G(\mathcal{L})$, where $t_x^* \phi_y \circ \phi_x$ is the map:

$$\mathcal{L} \xrightarrow{\phi_x} t_x^* \mathcal{L} \xrightarrow{t_x^* \phi_y} t_x^*(t_y^* \mathcal{L}) = t_{x+y}^* \mathcal{L},$$

t_x being the translation by x.

There is an exact sequence:

$$1 \longrightarrow k^* \longrightarrow G(\mathcal{L}) \longrightarrow K(\mathcal{L}) \longrightarrow 0,$$

where the first arrow is $\lambda \longmapsto (0, \lambda \, \mathrm{id}_{\mathcal{L}})$ and the last arrow is the *forgetful map* $\rho_{\mathcal{L}} : (x, \phi_x) \longmapsto x$.

$G(\mathcal{L})$ is not abelian. To measure the commutativity defect of two elements, we introduce the *commutator pairing* $e_{\mathcal{L}} : K(\mathcal{L}) \times K(\mathcal{L}) \longrightarrow k^*$, given for all $x, y \in K(\mathcal{L})$ by $e_{\mathcal{L}}(x, y) := \widetilde{x} \cdot \widetilde{y} \cdot \widetilde{x}^{-1} \cdot \widetilde{y}^{-1}$, where $\widetilde{x}$ and $\widetilde{y}$ are respectively lifts of x and y in $G(\mathcal{L})$. By the above exact sequence, this quantity $e_{\mathcal{L}}(x, y)$ defines a scalar in k^* and does not depend on the lifts $\widetilde{x}$ and $\widetilde{y}$ of x and y. The commutator pairing is bilinear, skew-symmetric and non-degenerate [15, Theorem 1].

An isogeny between polarised abelian varieties $f : (A, \mathcal{L}) \longrightarrow (B, \mathcal{M})$ satisfies $f^* \mathcal{M} \cong \mathcal{L}$. Then, it is easy to check that $K(\mathcal{L})$ contains $K := \ker(f)$. Besides, K can be lifted in $G(\mathcal{L})$ as follows. Given an isomorphism $\alpha : f^* \mathcal{M} \xrightarrow{\sim} \mathcal{L}$, we define $\widetilde{K} := \{(x, t_x^* \alpha \circ \alpha^{-1}) \mid x \in K\} \subset G(\mathcal{L})$. The forgetful map induces an isomorphism $\widetilde{K} \xrightarrow{\sim} K$. We say that $\widetilde{K}$ is a *level subgroup* lying above K. In particular, $\widetilde{K}$ is abelian so $e_{\mathcal{L}}$ is trivial on K. We say that K is *isotropic*. Conversely, it can be proved that a subgroup $K \subseteq K(\mathcal{L})$ admits a level subgroup lying above it if and only if K is isotropic. There is a one to one correspondence between level subgroups $\widetilde{K}$ in $G(\mathcal{L})$ and pairs (f, α) as above [15, Proposition 1, p. 291].

2.3. **Theta structures.** The commutator pairing being non-degenerate, it can be proved that $K(\mathcal{L})$ admits a *symplectic decomposition*, namely there exists maximal isotropic subgroups $K_1(\mathcal{L})$ and $K_2(\mathcal{L})$ such that $K(\mathcal{L}) = K_1(\mathcal{L}) \oplus K_2(\mathcal{L})$ and such that $e_{\mathcal{L}}$ induces an isomorphism $K_2(\mathcal{L}) \cong \widehat{K_1}(\mathcal{L}) := \mathrm{Hom}(K_1(\mathcal{L}), k^*)$. By the finite abelian groups structure theorem, there exists a unique tuple of integers

$\delta = (d_1, \cdots, d_r)$ such that $d_1 | \cdots | d_r$ and $K_1(\mathcal{L}) \cong K_1(\delta)$ and $K_2(\mathcal{L}) \cong K_2(\delta)$, where:

$$K_1(\delta) := \prod_{i=1}^{r} \mathbb{Z}/d_i\mathbb{Z} \quad \text{and} \quad K_2(\delta) := \widehat{K}_1(\delta) = \mathrm{Hom}(K_1(\delta), k^*).$$

We say that $\mathcal{L}$ is *of type* δ. It follows that $K(\mathcal{L}) \subseteq A[d_r]$, with $A[d_r] \cong (\mathbb{Z}/d_r\mathbb{Z})^f$ and $f \leq 2g = 2\dim(A)$ by [3, Remarks 8.4 and 8.5]. Hence, we can assume that $r = g$ without loss of generality.

Let $K(\delta) := K_1(\delta) \times K_2(\delta)$. As $K(\mathcal{L})$, $K(\delta)$ can be equipped with a non-degenerate skew-symmetric pairing $e_\delta : K(\delta) \times K(\delta) \longrightarrow k^*$, given by:

$$\forall (x, \chi), (x', \chi') \in K(\delta), \quad e_\delta((x, \chi), (x', \chi')) = \chi'(x)\chi(x)^{-1}.$$

$K(\mathcal{L})$ is not only isomorphic to $K(\delta)$. Actually, there exists a *symplectic isomorphism* $\sigma : K(\mathcal{L}) \xrightarrow{\sim} K(\delta)$ mapping $K_i(\mathcal{L})$ to $K_i(\delta)$ and such that $e_\delta(\sigma(x), \sigma(y)) = e_{\mathcal{L}}(x, y)$ for all $x, y \in K(\mathcal{L})$.

We define the *Heisenberg group* as $\mathcal{H}(\delta) := k^* \times K(\delta)$, with the following non abelian group law:

$$(\alpha, x, \chi) \cdot (\beta, x', \chi') := (\alpha\beta\chi'(x), x + x', \chi\chi'),$$

for all $(\alpha, x, \chi), (\beta, x', \chi') \in k^* \times K_1(\delta) \times K_2(\delta)$. As for $G(\mathcal{L})$, there is an exact sequence:

$$1 \longrightarrow k^* \longrightarrow \mathcal{H}(\delta) \longrightarrow K(\delta) \longrightarrow 0.$$

If $\mathcal{L}$ is of type δ, a *theta-structure* is an isomorphism $\Theta_{\mathcal{L}} : \mathcal{H}(\delta) \xrightarrow{\sim} G(\mathcal{L})$ inducing an isomorphism of exact sequences:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & k^* & \longrightarrow & \mathcal{H}(\delta) & \longrightarrow & K(\delta) & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle \Theta_{\mathcal{L}}} & & \downarrow{\scriptstyle \overline{\Theta}_{\mathcal{L}}} & & \\ 1 & \longrightarrow & k^* & \longrightarrow & G(\mathcal{L}) & \longrightarrow & K(\mathcal{L}) & \longrightarrow & 0 \end{array}$$

Such theta structures always exist and are in bijection with triples $(\overline{\Theta}_{\mathcal{L}}, s_1, s_2)$, where $\overline{\Theta}_{\mathcal{L}}$ is a symplectic isomorphism $K(\delta) \xrightarrow{\sim} K(\mathcal{L})$ and s_i are sections $K_i(\mathcal{L}) \xrightarrow{\sim} \widetilde{K}_i(\mathcal{L})$, the $\widetilde{K}_i(\mathcal{L}) \subset G(\mathcal{L})$ being level subgroups lying above $K_i(\mathcal{L})$ for $i \in \{1, 2\}$. Note that the $K_i(\mathcal{L})$ are fully determined by $\overline{\Theta}_{\mathcal{L}}$ via the formula $K_i(\mathcal{L}) = \overline{\Theta}_{\mathcal{L}}(K_i(\delta))$. In the following, we denote $K_i(\overline{\Theta}_{\mathcal{L}})$ or $K_i(\Theta_{\mathcal{L}})$ instead of $K_i(\mathcal{L})$ and $\widetilde{K}_i(\Theta_{\mathcal{L}})$ instead of $\widetilde{K}_i(\mathcal{L})$ to stress this dependence.

2.4. **Theta functions.** The Heisenberg group $\mathcal{H}(\delta)$ acts on the space $V(\delta)$ of functions $K_1(\delta) \longrightarrow k$ as follows:

$$\forall f \in V(\delta), (\alpha, x, \chi) \in \mathcal{H}(\delta), \quad (\alpha, x, \chi) \cdot f : y \longmapsto \alpha\chi(y)^{-1} f(y - x). \tag{1}$$

This action defines the only irreducible representation of $\mathcal{H}(\delta)$ on which k^* acts naturally [15, Proposition 3, p. 295]. Similarly, the theta-group $G(\mathcal{L})$ acts on the ring of global sections $\Gamma(A, \mathcal{L})$ as follows:

$$\forall s \in \Gamma(A, \mathcal{L}), (x, \phi_x) \in G(\mathcal{L}), \quad (x, \phi_x) \cdot s = t^*_{-x}(\phi_x(s)).$$

When $\mathcal{L}$ is of type δ, this representation is irreducible [15, Theorem 2, p. 297] and naturally isomorphic to $V(\delta)$. Hence, there is an isomorphism $\beta : V(\delta) \xrightarrow{\sim} \Gamma(A, \mathcal{L})$

respecting the group actions of $\mathcal{H}(\delta)$ and $G(\mathcal{L})$, namely such that:

$$\forall v \in V(\delta), h \in \mathcal{H}(\delta), \quad \beta(h \cdot v) = \Theta_{\mathcal{L}}(h) \cdot \beta(v). \tag{2}$$

As a consequence of Schur's lemma [16, Lemma XVIII.5.9], β is unique up to scalar multiplication. Consider the basis of $V(\delta)$ given by Kronecker functions $(\delta_i)_{i \in K_1(\delta)}$ and the basis of $\Gamma(A, \mathcal{L})$ given by $\theta_i^{\mathcal{L}} := \beta(\delta_i)$ for all $i \in K_1(\delta)$. We call this basis $(\theta_i^{\mathcal{L}})_{i \in K_1(\delta)}$ the basis of *theta functions* associated to $\Theta_{\mathcal{L}}$ or the basis of $\Theta_{\mathcal{L}}$-*coordinates*. It is defined up to multiplication by a scalar in k^*.

When $\mathcal{L}$ is generated by global sections, theta functions define a map $A \longrightarrow \mathbb{P}_k^{d-1}$ [14, Theorem II.7.1],where $d := \prod_{i=1}^g d_i$ and $\delta := (d_1, \cdots, d_g)$, so they give a way to represent the polarised abelian variety $(A, \mathcal{L})$ in the projective space. When $d_g \geq 3$, $\mathcal{L}$ is generated by global sections and the induced map $A \longrightarrow \mathbb{P}_k^{d-1}$ is a closed immersion [39, p. 163]. When $2|\delta$, $\mathcal{L}$ is also generated by global sections [39, p. 60] but the theta functions only define a closed immersion of the Kummer variety $A/\pm \hookrightarrow \mathbb{P}_k^{d-1}$ under the assumption that $(A, \mathcal{L})$ is not a product of polarised abelian varieties and that $\mathcal{L}$ is *totally symmetric*, as we shall see in Section 2.9 [40, Theorem 4.8.1].

When we work with a polarization $\mathcal{L}$ of type δ, we obtain $d = \prod_{i=1}^g d_i$ theta coordinates to represent points. In practice, to minimize computational complexity, we assume $\delta = \underline{2} := (2, \cdots, 2)$ to obtain 2^g theta-coordinates only. In that case, we say that $\Theta_{\mathcal{L}}$ is a theta-structure of *level 2*. We work on the Kummer variety so points are represented up to sign.

Theta functions are convenient because we can easily compute the action of the theta-group on these functions. The theta group action can be leveraged to derive arithmetic formulas (including differential addition, doubling, isogeny computation, change of basis).

2.5. **The Theta-null point.** As we have seen previously, we may see theta-functions as projective coordinates. The *theta-null point* is the projective point $(\theta_i^{\mathcal{L}}(0))_{i \in K_1(\delta)}$. In [17, p. 51], Robert proves that the theta-null point determines the sections $s_i : K_i(\Theta_{\mathcal{L}}) \xrightarrow{\sim} \widetilde{K}_i(\Theta_{\mathcal{L}})$ induced by the theta-structure $\Theta_{\mathcal{L}}$[3]. When $4|\delta$, the theta-null point even determines the symplectic isomorphism $\overline{\Theta}_{\mathcal{L}} : K(\delta) \xrightarrow{\sim} K(\mathcal{L})$, so the whole theta structure. When $2|\delta$, $\overline{\Theta}_{\mathcal{L}}$ is only determined up to signs.

In practice, this means that if $x = \overline{\Theta}_{\mathcal{L}}(j, \chi) \in K(\mathcal{L})$, then we have:

$$(\theta_i^{\mathcal{L}}(x))_{i \in K_1(\delta)} = (\Theta_{\mathcal{L}}(1, j, \chi) \cdot \theta_i^{\mathcal{L}}(0))_i = (\chi(i+j)^{-1} \cdot \theta_{i+j}^{\mathcal{L}}(0))_i, \tag{3}$$

where the first equality is proved in [17, p. 51] and the last follows from (1). More generally, the theta-group action can be used to translate any point $y \in A(k)$ by a point of $K(\mathcal{L})$:

$$(\theta_i^{\mathcal{L}}(x+y))_{i \in K_1(\delta)} = (\Theta_{\mathcal{L}}(1, j, \chi) \cdot \theta_i^{\mathcal{L}}(y))_i = (\chi(i+j)^{-1} \cdot \theta_{i+j}^{\mathcal{L}}(y))_i. \tag{4}$$

2.6. **The product Theta structure.** Let $(A_1, \mathcal{L}_1), \cdots, (A_r, \mathcal{L}_r)$ be polarised abelian varieties, $A := \prod_{i=1}^r A_i$ and $\mathcal{L} := \bigotimes_{i=1}^r \pi_i^* \mathcal{L}_i$, where $\pi_i : A \longrightarrow A_i$ is the projection for all $i \in [\![1 \ ; \ r]\!]$. Then $(A, \mathcal{L})$ is an abelian variety equipped with the *product polarization*. We have natural isomorphisms $K(\mathcal{L}) \cong \bigoplus_{i=1}^r K(\mathcal{L}_i)$ and

$$G(\mathcal{L}) \cong \prod_{i=1}^r G(\mathcal{L}_i) / \{(\lambda_1, \cdots, \lambda_r) \in k^* \mid \lambda_1 \cdots \lambda_r = 1\}.$$

[3]Provided it is not identically zero, which is always the case in practice.

Let $\delta^{(i)}$ be the type of $\mathcal{L}_i$ for all $i \in [\![1\ ;\ r]\!]$ and $\delta := \delta^{(1)} \vee \cdots \vee \delta^{(r)}$ be the concatenation of the $\delta^{(i)}$. Then, we also have:

$$\mathcal{H}(\delta) \cong \prod_{i=1}^{r} \mathcal{H}(\delta^{(i)})/\{(\lambda_1, \cdots, \lambda_r) \in k^* \mid \lambda_1 \cdots \lambda_r = 1\}.$$

If $\Theta_{\mathcal{L}_1}, \cdots, \Theta_{\mathcal{L}_r}$ are theta-structures on $G(\mathcal{L}_1), \cdots, G(\mathcal{L}_r)$ respectively, the *product theta-structure* $\Theta_{\mathcal{L}} := \prod_{i=1}^{r} \Theta_{\mathcal{L}_i}$ is the isomorphism $\mathcal{H}(\delta) \xrightarrow{\sim} G(\mathcal{L})$ induced by $(h_1, \cdots, h_r) \longmapsto (\Theta_{\mathcal{L}_1}(h_1), \cdots, \Theta_{\mathcal{L}_r}(h_r))$. This theta-structure induces a natural symplectic decomposition of $K(\mathcal{L}) = K_1(\Theta_{\mathcal{L}}) \oplus K_2(\Theta_{\mathcal{L}})$, where $K_i(\Theta_{\mathcal{L}}) := \prod_{j=1}^{r} K_i(\Theta_{\mathcal{L}_j})$ for $i \in \{1, 2\}$.

Lemma 1. [17, p. 70] *For all* $i := (i_1, \cdots, i_r) \in K_1(\delta^{(1)}) \times \cdots \times K_1(\delta^{(r)})$,

$$\theta_i^{\mathcal{L}} = \bigotimes_{j=1}^{r} \pi_j^* \theta_{i_j}^{\mathcal{L}_j}.$$

Proof. With the notations of Section 2.4, we have $V(\delta) \cong \bigoplus_{j=1}^{r} V(\delta^{(j)})$ and $\Gamma(A, \mathcal{L}) = \bigoplus_{j=1}^{r} \pi_j^* \Gamma(A_j, \mathcal{L}_j)$. For all $j \in [\![1\ ;\ r]\!]$, let $\beta_j : V(\delta^{(j)}) \xrightarrow{\sim} \Gamma(A_j, \mathcal{L}_j)$ be an isomorphism satisfying (2) for $\Theta_{\mathcal{L}_j}$. Then, the isomorphism $\beta : V(\delta) \xrightarrow{\sim} \Gamma(A, \mathcal{L})$, $v_1 \otimes \cdots \otimes v_r \longmapsto \pi_1^* \beta_1(v_1) \otimes \cdots \otimes \pi_r^* \beta_r(v_r)$ also satisfies (2) for the product theta-structure $\Theta_{\mathcal{L}}$. The result follows. □

Our goal is to work with a product of elliptic curves. By Lemma 1, we just have to multiply theta coordinates of elliptic curves to obtain theta coordinates on the product. However, a question remains: how can we translate elliptic curves Montgomery coordinates into theta coordinates?

2.7. **From Montgomery to Theta coordinates in level 2.** In [18, Chapter 7, Appendix A], formulas were introduced to convert Montgomery coordinates into level 2 theta-coordinates and vice versa. Let E be an elliptic curve in the Montgomery model and (T_1', T_2') be a basis of $E[4]$ such that $T_2' := (-1 : 1)$. Let us write $T_1' := (r : s)$. Then, we may define a level 2 theta-structure on E with theta-null point $(a : b) := (r + s : r - s)$. The conversion map from Montgomery to theta coordinates is then $(x : z) \longmapsto (a(x - z) : b(x + z))$. Conversely, if $(a : b)$ is the theta-null point, the conversion map from theta to Montgomery coordinates is $(\theta_0, \theta_1) \longmapsto (a\theta_1 + b\theta_0 : a\theta_1 - b\theta_0)$.

We see here is that a basis of the 4-torsion can determine a theta-structure of level 2. This is a consequence of a general result for symmetric theta-structures (Theorem 5.(ii)).

2.8. **The isogeny theorem.** Here we explain how to compute isogenies with theta coordinates. Let $f : (A, \mathcal{L}) \longrightarrow (B, \mathcal{M})$ be an isogeny between polarised abelian varieties. Let δ and $\delta_{\mathcal{M}}$ be respectively the types of $\mathcal{L}$ and $\mathcal{M}$. We want to express the $f^*\theta_i^{\mathcal{M}}$ for all $i \in K_1(\delta_{\mathcal{M}})$ (seen as functions $x \longmapsto \theta_i^{\mathcal{M}}(f(x))$) in the basis $(\theta_j^{\mathcal{L}})_{j \in K_1(\delta)}$ (seen as functions $x \longmapsto \theta_j^{\mathcal{L}}(x)$).

We begin by choosing *compatible* theta-structures on $G(\mathcal{L})$ and $G(\mathcal{M})$ determining these theta functions. Let $K := \ker(f)$. Assume that $K \subseteq K(\mathcal{L})$ is isotropic, let $\widetilde{K}$ be a level subgroup lying over K and $Z(\widetilde{K})$ be the centralizer of $\widetilde{K}$ in $G(\mathcal{L})$. Then, the isomorphism $\alpha : f^*\mathcal{M} \xrightarrow{\sim} \mathcal{L}$ associated to $\widetilde{K}$ by [15, Proposition 1, p. 291] induces a surjective map $\alpha_f : Z(\widetilde{K}) \twoheadrightarrow G(\mathcal{M})$ of kernel $\widetilde{K}$ [15, Proposition

2, p. 291]. For $i \in \{1,2\}$, let $\widetilde{K}_i(\Theta_{\mathcal{L}})$ (respectively $\widetilde{K}_i(\Theta_{\mathcal{M}})$) be the level subgroups lying above $K_i(\Theta_{\mathcal{L}})$ (respectively $K_i(\Theta_{\mathcal{M}})$) induced by the theta-structure (as we saw in Section 2.3).

Definition 2. We say that two theta-structures $\Theta_{\mathcal{L}}$ and $\Theta_{\mathcal{M}}$ on $G(\mathcal{L})$ and $G(\mathcal{M})$ respectively are *compatible* when: **(i)** $\widetilde{K} = (\widetilde{K} \cap \widetilde{K}_1(\Theta_{\mathcal{L}})) \oplus (\widetilde{K} \cap \widetilde{K}_2(\Theta_{\mathcal{L}}))$ and **(ii)** α_f maps $Z(\widetilde{K}) \cap \widetilde{K}_i(\Theta_{\mathcal{L}})$ to $\widetilde{K}_i(\Theta_{\mathcal{M}})$ for $i \in \{1,2\}$.

Let $K^{\perp} = \{x \in K(\mathcal{L}) \mid \forall y \in K, \quad e_{\mathcal{L}}(x,y) = 1\}$ and let us write $K := K_1 \oplus K_2$ and $K^{\perp} := K^{\perp,1} \oplus K^{\perp,2}$, with $K_i, K^{\perp,i} \subseteq K_i(\Theta_{\mathcal{L}})$ for $i \in \{1,2\}$. Then, if we fix a theta-structure $\Theta_{\mathcal{L}}$ on $G(\mathcal{L})$, there is a one to one correspondence between theta-structures $\Theta_{\mathcal{M}}$ on $G(\mathcal{M})$ compatible with $\Theta_{\mathcal{L}}$ and isomorphisms $\sigma : K^{\perp,1}/K_1 \xrightarrow{\sim} K_1(\delta_{\mathcal{M}})$ [17, Proposition 3.6.2]. In [15, Theorem 4, p. 302], Mumford proved the following theorem to compute isogenies with theta coordinates, which has been reformulated by Robert [17, Theorem 3.6.4].

Theorem 3. *Let $\Theta_{\mathcal{L}}$ and $\Theta_{\mathcal{M}}$ be compatible theta-structures on $G(\mathcal{L})$ and $G(\mathcal{M})$ respectively and let $\sigma : K^{\perp,1}/K_1 \xrightarrow{\sim} K_1(\delta_{\mathcal{M}})$ be the isomorphism induced by $\Theta_{\mathcal{M}}$. Then, there exists $\lambda \in k^*$ such that for all $i \in K_1(\delta_{\mathcal{M}})$,*

$$f^*\theta_i^{\mathcal{M}} = \lambda \sum_{j \in \overline{\Theta}_{\mathcal{L}}^{-1}(\sigma^{-1}(\{i\}))} \theta_j^{\mathcal{L}}. \tag{5}$$

When $K \subseteq K_2(\Theta_{\mathcal{L}})$, there is always only one index j in the sum of Equation (5) and the isogeny is simpler to compute. In this paper, we always work in that case. When $K \not\subseteq K_2(\Theta_{\mathcal{L}})$, we may do a change of basis between theta-structures. This is explained in the section 3.

2.9. **Symmetric Theta structures.** A line bundle $\mathcal{L}$ on A is *symmetric* when $[-1]^*\mathcal{L} \cong \mathcal{L}$. It is *totally symmetric* when there exists a symmetric line bundle $\mathcal{M}$ such that $\mathcal{L} \cong \mathcal{M}^2$. By [15, Proposition 1, p. 305], $\mathcal{L}$ is totally symmetric if and only if it descends to a line bundle $\mathcal{N}$ on the Kummer variety $K_A := A/\pm$ via the projection $\pi : A \longrightarrow K_A$ *i.e.* such that $\mathcal{L} \cong \pi^*\mathcal{N}$.

Let $\mathcal{L}$ be a symmetric line bundle of type δ. In [15, p. 308], Mumford defines δ_{-1}, an automorphism of $G(\mathcal{L})$ making the following diagram commute:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & k^* & \longrightarrow & G(\mathcal{L}) & \xrightarrow{\rho_{\mathcal{L}}} & K(\mathcal{L}) & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle \delta_{-1}} & & \downarrow{\scriptstyle [-1]} & & \\ 1 & \longrightarrow & k^* & \longrightarrow & G(\mathcal{L}) & \xrightarrow{\rho_{\mathcal{L}}} & K(\mathcal{L}) & \longrightarrow & 0 \end{array}$$

He also defines an Heisenberg group analogue $D_{-1} \in \mathrm{Aut}(\mathcal{H}(\delta))$. We say that a theta structure $\Theta_{\mathcal{L}}$ on $G(\mathcal{L})$ is *symmetric* when $\Theta_{\mathcal{L}} \circ D_{-1} = \delta_{-1} \circ \Theta_{\mathcal{L}}$. We say that an element $g \in G(\mathcal{L})$ is *symmetric* when $\delta_{-1}(g) = g^{-1}$. A theta-structure $\Theta_{\mathcal{L}}$ is symmetric if and only if its induced level subgroups $\widetilde{K}_i(\Theta_{\mathcal{L}})$ are symmetric *i.e.* made of symmetric elements [17, Proposition 4.2.9].

Let $f : A \longrightarrow B$ be an isogeny of kernel K. Let $\mathcal{L}$ be a symmetric line bundle on A. Then, there exists a symmetric line bundle $\mathcal{M}$ on B such that $f^*\mathcal{M} \cong \mathcal{L}$ if and only if there is a symmetric level subgroups $\widetilde{K}$ lying above K [17, Proposition 4.2.12]. Assuming $\mathcal{M}$ exists, if $\Theta_{\mathcal{L}}$ is a symmetric theta structure on $G(\mathcal{L})$, then any theta-structure $\Theta_{\mathcal{M}}$ on $G(\mathcal{M})$ which is compatible with $\Theta_{\mathcal{L}}$ in the sense of

Definition 2, is automatically symmetric [17, Remark 4.2.15]. This property is very convenient to compute isogeny chains, because we can obtain a symmetric theta-structure on the codomain from a symmetric theta structure on the domain.

Now, we assume that $\mathcal{L}$ is totally symmetric. We explain compatibility conditions between theta structures on $G(\mathcal{L})$ and $G(\mathcal{L}^2)$. Note that $K(\mathcal{L}^2) = [2]^{-1}K(\mathcal{L})$ [15, Proposition 4, p. 310], so that $K(\mathcal{L}) \subset K(\mathcal{L}^2)$. In [15, pp. 309-310], Mumford defines group homomorphisms ε_2 and η_2 between $G(\mathcal{L})$ and $G(\mathcal{L}^2)$ making the following diagrams commute:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & k^* & \longrightarrow & G(\mathcal{L}) & \xrightarrow{\rho_{\mathcal{L}}} & K(\mathcal{L}) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \lambda\mapsto\lambda^2} & & \downarrow{\scriptstyle \varepsilon_2} & & \downarrow & & \\
1 & \longrightarrow & k^* & \longrightarrow & G(\mathcal{L}^2) & \xrightarrow{\rho_{\mathcal{L}^2}} & K(\mathcal{L}^2) & \longrightarrow & 0
\end{array}$$

$$\begin{array}{ccccccccc}
1 & \longrightarrow & k^* & \longrightarrow & G(\mathcal{L}^2) & \xrightarrow{\rho_{\mathcal{L}^2}} & K(\mathcal{L}^2) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \lambda\mapsto\lambda^2} & & \downarrow{\scriptstyle \eta_2} & & \downarrow{\scriptstyle [2]} & & \\
1 & \longrightarrow & k^* & \longrightarrow & G(\mathcal{L}) & \xrightarrow{\rho_{\mathcal{L}}} & K(\mathcal{L}) & \longrightarrow & 0
\end{array}$$

In [15, p. 316], he also defines their Heisenberg analogues $E_2 : \mathcal{H}(\delta) \longrightarrow \mathcal{H}(2\delta)$ and $H_2 : \mathcal{H}(2\delta) \longrightarrow \mathcal{H}(\delta)$.

Definition 4. We say that theta-structures $\Theta_{\mathcal{L}}$ and $\Theta_{\mathcal{L}^2}$ on $G(\mathcal{L})$ and $G(\mathcal{L}^2)$ respectively are *compatible* when $\Theta_{\mathcal{L}^2} \circ E_2 = \varepsilon_2 \circ \Theta_{\mathcal{L}}$ and $\Theta_{\mathcal{L}} \circ H_2 = \eta_2 \circ \Theta_{\mathcal{L}^2}$. We also say that $(\Theta_{\mathcal{L}}, \Theta_{\mathcal{L}^2})$ is a *pair of symmetric theta-structures* (for $(\mathcal{L}, \mathcal{L}^2)$).

Theorem 5.

(i) Every symmetric theta-structure $\Theta_{\mathcal{L}^2}$ on $G(\mathcal{L}^2)$ induces a unique symmetric theta-structure $\Theta_{\mathcal{L}}$ on $G(\mathcal{L})$ that is compatible with $\Theta_{\mathcal{L}^2}$.

(ii) The resulting theta-structure $\Theta_{\mathcal{L}}$ on $G(\mathcal{L})$ only depends on the symplectic isomorphism $\overline{\Theta}_{\mathcal{L}^2} : K(2\delta) \xrightarrow{\sim} K(\mathcal{L}^2)$.

(iii) Every symmetric theta-structure on $G(\mathcal{L})$ is induced by a symmetric theta-structure on $G(\mathcal{L}^2)$, or equivalently, by a symplectic isomorphism $K(2\delta) \xrightarrow{\sim} K(\mathcal{L}^2)$.

Proof. (i) is [15, Remark 1, p. 317], (ii) is [15, Remark 3, p. 319] and (iii) is [15, Remark 4, p. 319]. □

2.10. **Addition and duplication formulas.** Let $\mathcal{L}$ be a totally symmetric line bundle of type δ on A. Let $(\Theta_{\mathcal{L}}, \Theta_{\mathcal{L}^2})$ be a pair of symmetric theta-structures for $(\mathcal{L}, \mathcal{L}^2)$. Then, by [17, Corollary 4.3.7], we have for all $x, y \in A(k)$, and all $i, j \in K_1(\delta)$,

$$\theta_i^{\mathcal{L}}(x+y)\theta_j^{\mathcal{L}}(x-y) = \sum_{\substack{u,v \in K_1(2\delta) \\ u+v=2i \\ u-v=2j}} \theta_u^{\mathcal{L}^2}(x)\theta_v^{\mathcal{L}^2}(y). \tag{6}$$

We have an injective map $(\mathbb{Z}/2\mathbb{Z})^g \hookrightarrow K_1(2\delta)$, mapping $t := (t_1, \cdots, t_g)$ to $t\delta = (t_1 d_1, \cdots, t_g d_g)$. We can then define the following change of variables: for all

$\chi \in (\widehat{\mathbb{Z}/2\mathbb{Z}})^g$ and $i \in K_1(2\delta)$,

$$U^{\mathcal{L}^2}_{\chi,i} := \sum_{t\in(\mathbb{Z}/2\mathbb{Z})^g} \chi(t)\theta^{\mathcal{L}^2}_{i+t\delta}. \tag{7}$$

Using this change of variable, we can rewrite and revert Equation (6):

Theorem 6. [17, Theorem 4.4.3] *Let $x, y \in A(k)$. Then there exists $\lambda_1, \lambda_2 \in k^*$ such that for all $i, j \in K_1(2\delta)$ such that $i \equiv j \mod 2$ and $\chi \in (\widehat{\mathbb{Z}/2\mathbb{Z}})^g$, we have:*

$$\theta^{\mathcal{L}}_{(i+j)/2}(x+y)\theta^{\mathcal{L}}_{(i-j)/2}(x-y) = \lambda_1 \sum_{\chi\in(\widehat{\mathbb{Z}/2\mathbb{Z}})^g} U^{\mathcal{L}^2}_{\chi,i}(x)U^{\mathcal{L}^2}_{\chi,j}(y) \tag{8}$$

$$U^{\mathcal{L}^2}_{\chi,i}(x)U^{\mathcal{L}^2}_{\chi,j}(y) = \lambda_2 \sum_{t\in(\mathbb{Z}/2\mathbb{Z})^g} \chi(t)\theta^{\mathcal{L}}_{(i+j+t\delta)/2}(x+y)\theta^{\mathcal{L}}_{(i-j+t\delta)/2}(x-y). \tag{9}$$

These formulas can be used to compute differential addition. Knowing the coordinates $\theta^{\mathcal{L}}_i(x), \theta^{\mathcal{L}}_i(y)$ and $\theta^{\mathcal{L}}_i(x-y)$, we can obtain the $\theta^{\mathcal{L}}_i(x+y)$ [17, Algorithm 4.4.10]. In particular, for doubling ($x = y$), $(\theta^{\mathcal{L}}_i(x-y))_i = (\theta^{\mathcal{L}}_i(0))_i$ is the *theta-null point*, so we only need to know the $\theta^{\mathcal{L}}_i(x)$, provided the theta-null point has been precomputed (see Algorithm 8).

2.11. **Heisenberg group automorphisms.** We denote by $\mathrm{Aut}_{k^*}(\mathcal{H}(\delta))$ the group of automorphisms of $\mathcal{H}(\delta)$ fixing k^*. Every such automorphism $\psi \in \mathrm{Aut}_{k^*}(\mathcal{H}(\delta))$ induces a symplectic isomorphism $\overline{\psi} \in \mathrm{Sp}(K(\delta))$, and by [17, Proposition 3.5.1], we have an exact sequence:

$$0 \longrightarrow K(\delta) \longrightarrow \mathrm{Aut}_{k^*}(\mathcal{H}(\delta)) \longrightarrow \mathrm{Sp}(K(\delta)) \longrightarrow 1.$$

Every $\psi \in \mathrm{Aut}_{k^*}(\mathcal{H}(\delta))$, can be written explicitly as

$$\psi(\alpha, x, \chi) := (\alpha\xi(x,\chi), \overline{\psi}(x,\chi)) \tag{10}$$

for all $(\alpha, x, \chi) \in \mathcal{H}(\delta)$, where $\overline{\psi} \in \mathrm{Sp}(K(\delta))$ is the induced symplectic isomorphism and $\xi : K(\delta) \longrightarrow k^*$ is a *semi-character*, satisfying the following property:

$$\xi(x_1 + x_2, \chi_1 \cdot \chi_2) = \frac{\xi(x_1,\chi_2)\xi(x_2,\chi_2)\overline{\psi}_2(x_2,\chi_2)(\overline{\psi}_1(x_1,\chi_1))}{\chi_2(x_1)}$$

for all $(x_1, \chi_1), (x_2, \chi_2) \in K(\delta)$ [17, Remark 3.5.2]. If $\mathcal{L}$ has type δ, then $\mathrm{Aut}_{k^*}(\mathcal{H}(\delta))$ acts faithfully and transitively on the set of theta-structures on $G(\mathcal{L})$ by right-composition [17, p. 52].

Now, what happens if we restrict to symmetric theta-structures? An automorphism $\psi \in \mathrm{Aut}_{k^*}(\mathcal{H}(\delta))$ is *symmetric* if $\psi \circ D_{-1} = D_{-1} \circ \psi$ (where D_{-1} has been defined in Section 2.9). We denote by $\mathrm{Aut}^0_{k^*}(\mathcal{H}(\delta))$ the subgroup of symmetric automorphisms. Let $\mathcal{L}$ be a totally symmetric theta structure of type δ. Then, as previously, $\mathrm{Aut}^0_{k^*}(\mathcal{H}(\delta))$ acts faithfully and transitively on the set of symmetric theta structures on $G(\mathcal{L})$. By [17, p. 67], we also have an exact sequence:

$$0 \longrightarrow K(\delta)[2] \longrightarrow \mathrm{Aut}^0_{k^*}(\mathcal{H}(\delta)) \longrightarrow \mathrm{Sp}(K(\delta)) \longrightarrow 1.$$

Lemma 7. *Let $\psi \in \mathrm{Aut}_{k^*}(\mathcal{H}(\delta))$ and $\overline{\psi}$, ξ as in Equation (10). Then ψ is symmetric if and only if*

$$\forall (x,\chi) \in K(\delta), \quad \xi(x,\chi)^2 = \chi(x)^{-1}\overline{\psi}_2(x,\chi)(\overline{\psi}_1(x,\chi)). \tag{11}$$

Proof. Let $(\alpha, x, \chi) \in \mathcal{H}(\delta)$. Then, by the definition of D_{-1} [15, p. 316], we have $D_{-1}(\alpha, x, \chi) = (\alpha, -x, \chi^{-1}) = \alpha^2/\chi(x)(\alpha, x, \chi)^{-1}$, so that:

$$\psi \circ D_{-1}(\alpha, x, \chi) = \psi\left(\frac{\alpha^2}{\chi(x)}(\alpha, x, \chi)^{-1}\right) = \frac{\alpha^2}{\chi(x)}\psi(\alpha, x, \chi)^{-1}$$

$$\text{and} \qquad D_{-1} \circ \psi(\alpha, x, \chi) = \frac{\alpha^2 \xi(x, \chi)^2}{\overline{\psi}_2(x, \chi)(\overline{\psi}_1(x, \chi))}\psi(\alpha, x, \chi)^{-1}$$

The result follows. □

2.12. **Action of Heisenberg automorphisms on Theta functions.** Let $\mathcal{L}$ be a line bundle of type δ on A, $\Theta_{\mathcal{L}}$ be a theta-structure on $G(\mathcal{L})$, $\psi \in \mathrm{Aut}_{k^*}(\mathcal{H}(\delta))$ and $\Theta'_{\mathcal{L}} := \Theta_{\mathcal{L}} \circ \psi$. The group actions introduced in Section 2.4 give a way to compute the change of basis matrix between theta-functions $(\theta_i)_{i \in K_1(\delta)}$ and $(\theta'_i)_{i \in K_1(\delta)}$ associated to $\Theta_{\mathcal{L}}$ and $\Theta'_{\mathcal{L}}$ respectively.

By the definition of the theta-group action (1), we have:

$$\delta_i = (1, i, 1) \cdot \delta_0 \quad \text{and} \quad (1, 0, \chi) \cdot \delta_0 = \delta_0 \tag{12}$$

for all $i \in K_1(\delta)$ and $\chi \in K_2(\delta)$, where the δ_i are the Kronecker functions. It follows that the action of the level subgroup $\widetilde{K}_2(\Theta'_{\mathcal{L}})$ associated to $\Theta'_{\mathcal{L}}$ stabilizes $\theta'^{\mathcal{L}}_0$. Besides, $T_i := \sum_{j \in K_2(\delta)} \Theta_{\mathcal{L}} \circ \psi(1, 0, j) \cdot \theta_i$ is stable under the action of $\widetilde{K}_2(\Theta'_{\mathcal{L}})$ for all $i \in K_1(\delta)$. But this level subgroup is maximal (since $K_2(\Theta_{\mathcal{L}})$ is maximal isotropic in $K(\mathcal{L})$), so [15, Proposition 3, p. 295] ensures that the subspace of $V(\delta)$ stabilized by $\widetilde{K}_2(\Theta'_{\mathcal{L}})$ has dimension 1. The following result follows:

Proposition 8. [17, p. 53] *There exists $i_0 \in K_1(\delta)$ and $\lambda \in k^*$ such that:*

$$\theta'_0 = \lambda \sum_{j \in K_2(\delta)} \Theta_{\mathcal{L}}(\delta) \circ \psi(1, 0, j) \cdot \theta_{i_0}.$$

Once we found θ'_0, we can obtain θ'_i for all $i \in K_1(\delta)$, by the formula $\theta'_i = \Theta_{\mathcal{L}} \circ \psi(1, i, 1) \cdot \theta'_0$ derived from Equation (12).

3. Change of basis formulas

In this section, we derive explicit change of basis formulas from Proposition 8 in the case of symmetric theta structures. Given a totally symmetric line bundle $\mathcal{L}$ of type δ on an abelian variety A and a symmetric theta-structure $\Theta_{\mathcal{L}}$ on $G(\mathcal{L})$, we know that $\Theta_{\mathcal{L}}$ is completely determined by a symplectic isomorphism $\overline{\Theta}_{\mathcal{L}^2} : K(2\delta) \xrightarrow{\sim} K(\mathcal{L}^2)$ by Theorem 5. Our change of basis formula (Theorem 12) only depends on the symplectic isomorphism of $\mathrm{Sp}(K(2\delta))$ induced by the change of basis. This formula was already known to Igusa [19, Theorem V.2] and Cosset [20, Proposition 3.1.24] but was proved in the analytic setting of complex theta functions. Our proof only uses the algebraic setting of [15]. In this setting, we obtain more convenient formulas to implement for isogeny computations over finite fields.

3.1. **Action of Heisenberg automorphisms on pairs of symmetric theta structures.** Throughout this section, we fix a totally symmetric line bundle $\mathcal{L}$ of type $\delta := (d_1, \cdots, d_g)$ on an abelian variety A. We study the action of $\mathrm{Aut}_{k^*}(\mathcal{H}(2\delta))$ on pairs of symmetric theta structures $(\Theta_{\mathcal{L}}, \Theta_{\mathcal{L}^2})$ for $(\mathcal{L}, \mathcal{L}^2)$.

First, we give more details on the maps E_2 and H_2 introduced in Section 2.9 and defined in [15, p. 316]. We have a natural embedding $K_1(\delta) \hookrightarrow K_1(2\delta)$ via the multiplication by 2 map and conversely, we have a natural surjective map $K_1(2\delta) \twoheadrightarrow K_1(\delta)$ mapping $x := (x_1 \mod 2d_1, \cdots, x_g \mod 2d_g)$ to $\overline{x} := (x_1 \mod d_1, \cdots, x_g \mod d_g)$. Looking at the dual, we also have a natural embedding $K_2(\delta) \hookrightarrow K_2(2\delta)$ mapping every $\chi \in K_2(\delta)$ to $2 \star \chi : x \in K_1(2\delta) \longmapsto \chi(\overline{x}) \in k^*$ and a surjective map $K_2(2\delta) \twoheadrightarrow K_2(\delta)$ mapping every $\chi \in K_2(2\delta)$ to $\overline{\chi} : x \in K_1(\delta) \longmapsto \chi(2x) \in k^*$. Then $E_2 : \mathcal{H}(\delta) \longrightarrow \mathcal{H}(2\delta)$ and $H_2 : \mathcal{H}(2\delta) \longrightarrow \mathcal{H}(\delta)$ are given by:

$$\forall (\alpha, x, \chi) \in \mathcal{H}(\delta), \quad E_2(\alpha, x, \chi) := (\alpha^2, 2x, 2 \star \chi),$$

$$\forall (\alpha, x, \chi) \in \mathcal{H}(2\delta), \quad H_2(\alpha, x, \chi) := (\alpha^2, \overline{x}, \overline{\chi}).$$

Let $\overline{E}_2 : K(\delta) \longrightarrow K(2\delta)$ and $\overline{H}_2 : K(2\delta) \longrightarrow K(\delta)$ be the homomorphisms induced by E_2 and H_2 respectively. We also define $D_n : \mathcal{H}(\delta) \longrightarrow \mathcal{H}(\delta)$ by $D_n(\alpha, x, \chi) := (\alpha^{n^2}, nx, \chi^n)$ for all $(\alpha, x, \chi) \in \mathcal{H}(\delta)$ and $n \in \mathbb{Z}$.

Lemma 9. [15, p. 316] *Assume that $2|\delta$. Then:*

(i) $\ker(H_2) = \{h \in \mathcal{H}(2\delta) \mid h^2 = 1\}$.
(ii) $E_2 \circ D_{-1}^{\mathcal{H}(\delta)} = D_{-1}^{\mathcal{H}(2\delta)} \circ E_2$ *and* $H_2 \circ D_{-1}^{\mathcal{H}(2\delta)} = D_{-1}^{\mathcal{H}(\delta)} \circ H_2$ *(where the exponents indicate the group of definition).*
(iii) $E_2 \circ H_2 = D_2^{\mathcal{H}(2\delta)}$ *and* $H_2 \circ E_2 = D_2^{\mathcal{H}(\delta)}$.
(iv) For all $h \in \mathcal{H}(\delta)$, $D_n(h) = h^{n(n+1)/2} D_{-1}(h)^{n(n-1)/2}$.

Proposition 10. *Assume that $2|\delta$. Then:*

(i) For all $\psi \in \mathrm{Aut}^0(\mathcal{H}(2\delta))$, *there exists a unique* $\psi' \in \mathrm{Aut}^0(\mathcal{H}(\delta))$ *such that* $\psi' \circ H_2 = H_2 \circ \psi$ *and* $\psi \circ E_2 = E_2 \circ \psi'$.
(ii) Let $\overline{\psi}, \overline{\psi}', \xi, \xi'$ *be respectively the symplectic automorphisms and semi-characters associated to* ψ *and* ψ' *as in Equation (10). Then, we have* $\overline{\psi}' \circ \overline{H}_2 = \overline{H}_2 \circ \overline{\psi}$, $\overline{E}_2 \circ \overline{\psi}' = \overline{\psi} \circ \overline{E}_2$ *and:*

$$\forall (x, \chi) \in K(2\delta), \quad \xi'(\overline{x}, \overline{\chi}) = \chi(x)^{-1} \overline{\psi}_2(x, \chi)(\overline{\psi}_1(x, \chi)).$$

(iii) Let $(\Theta_{\mathcal{L}}, \Theta_{\mathcal{L}^2})$ *and* $(\Theta'_{\mathcal{L}}, \Theta'_{\mathcal{L}^2})$ *be two pairs of symmetric theta-structures for* $(\mathcal{L}, \mathcal{L}^2)$. *Then, there exists* $\psi \in \mathrm{Aut}^0(\mathcal{H}(2\delta))$ *such that* $\Theta'_{\mathcal{L}^2} = \Theta_{\mathcal{L}^2} \circ \psi$ *and* $\Theta'_{\mathcal{L}} = \Theta_{\mathcal{L}} \circ \psi'$, *where* $\psi' \in \mathrm{Aut}^0(\mathcal{H}(\delta))$ *is induced by* ψ.

Proof. **(i)** Since $2|\delta$, Lemma 9.(i) ensures that $\ker(H_2) = \mathcal{H}(2\delta)[2]$, so that $\ker(H_2 \circ \psi) = \mathcal{H}(2\delta)[2] = \ker(H_2)$ as well since ψ is an automorphism. Hence, $H_2 \circ \psi$ factors through H_2 and this defines an automorphism $\psi' : \mathcal{H}(\delta) \xrightarrow{\sim} \mathcal{H}(\delta)$ such that $\psi' \circ H_2 = H_2 \circ \psi$. This automorphism ψ' is trivial on k^* because ψ is and H_2 acts as $\lambda \longmapsto \lambda^2$. Besides, ψ' is symmetric by Lemma 9.(ii) and since H_2 is surjective, so $\psi' \in \mathrm{Aut}^0(\mathcal{H}(2\delta))$. The uniqueness is a consequence of the surjectivity of H_2.

We now prove that $\psi \circ E_2 = E_2 \circ \psi'$. By surjectivity of H_2, it suffices to prove that $\psi \circ E_2 \circ H_2 = E_2 \circ \psi' \circ H_2$ *i.e.* that $\psi \circ D_2 = D_2 \circ \psi$ since $\psi' \circ H_2 = H_2 \circ \psi$ and $E_2 \circ H_2 = D_2$ by Lemma 9.(iii). Let $h \in \mathcal{H}(2\delta)$. Then, $D_2(h) = h^3 D_{-1}(h)$ by Lemma 9.(iv) and:

$$\psi \circ D_2(h) = \psi(h^3 D_{-1}(h)) = \psi(h)^3 \psi \circ D_{-1}(h) = \psi(h)^3 D_{-1} \circ \psi(h) = D_2 \circ \psi(h)$$

The result follows.

(ii) Let $(\alpha, x, \chi) \in \mathcal{H}(2\delta)$. The equalities $\overline{\psi}' \circ \overline{H}_2 = \overline{H}_2 \circ \overline{\psi}$ and $\overline{E}_2 \circ \overline{\psi}' = \overline{\psi} \circ \overline{E}_2$ immediately follow from $\psi' \circ H_2 = H_2 \circ \psi$ and $\psi \circ E_2 = E_2 \circ \psi'$. By Lemma 7:

$$\xi'(\overline{x}, \overline{\chi}) = \xi(x, \chi)^2 = \chi(x)^{-1}\overline{\psi}_2(x, \chi)(\overline{\psi}_1(x, \chi)).$$

The result follows.

(iii) Let $\psi := \Theta_{\mathcal{L}^2}^{-1} \circ \Theta'_{\mathcal{L}^2}$. Then, $\Theta_{\mathcal{L}^2}$ and $\Theta'_{\mathcal{L}^2}$ being symmetric, we have:

$$\psi \circ D_{-1} = \Theta_{\mathcal{L}^2}^{-1} \circ \Theta'_{\mathcal{L}^2} \circ D_{-1} = \Theta_{\mathcal{L}^2}^{-1} \circ \gamma_{-1} \circ \Theta'_{\mathcal{L}^2} = D_{-1} \circ \Theta_{\mathcal{L}^2}^{-1} \circ \Theta'_{\mathcal{L}^2} = D_{-1} \circ \psi,$$

so $\psi \in \mathrm{Aut}^0(\mathcal{H}(2\delta))$. Besides by compatibility of the pairs $(\Theta_{\mathcal{L}}, \Theta_{\mathcal{L}^2})$ and $(\Theta'_{\mathcal{L}}, \Theta'_{\mathcal{L}^2})$:

$$\Theta'_{\mathcal{L}} \circ H_2 = \eta_2 \circ \Theta'_{\mathcal{L}^2} = \eta_2 \circ \Theta_{\mathcal{L}^2} \circ \psi = \Theta_{\mathcal{L}} \circ H_2 \circ \psi = \Theta_{\mathcal{L}} \circ \psi' \circ H_2,$$

so that $\Theta'_{\mathcal{L}} = \Theta_{\mathcal{L}} \circ \psi'$ since H_2 is surjective. This completes the proof. □

3.2. **Change of basis of symmetric theta structures.** Let $\delta := (d_1, \cdots, d_g)$ with $d_1 | \cdots | d_g$ and $\zeta \in k^*$ be a d_g-th primitive root of unity. Let us fix a canonical symplectic basis of $K(\delta)$ as follows. For $i \in [\![1\ ;\ g]\!]$, let e_i be the vector of $K_1(\delta)$ with 1 at index i and 0 everywhere else. For all $l \in [\![1\ ;\ g]\!]$, let $\chi_l \in K_2(\delta)$ be the character such that $\chi_l(e_m) = \zeta^{d_g/d_l \delta_{l,m}}$ for all $l \in [\![1\ ;\ g]\!]$. Then $K_1(\delta)$ can be canonically identified with $K_2(\delta)$ via the map $i \in K_1(\delta) \longmapsto \chi^i := \prod_{l=1}^g \chi_l^{i_l}$. We then have

$$\forall i, j \in K_1(\delta), \quad \chi^i(j) = \zeta^{\langle i|j\rangle} \quad \text{with} \quad \langle i|j\rangle := \sum_{l=1}^{g} \frac{d_g}{d_l} i_l j_l.$$

Such a basis is called a *ζ-canonical symplectic basis.*

Lemma 11. *Let $\sigma : K(\delta) \xrightarrow{\sim} K(\delta)$ be an automorphism of $K(\delta)$ and M be its matrix in the ζ-canonical symplectic basis $(e_1, \cdots, e_g, \chi_1, \cdots, \chi_g)$. Then σ is symplectic if and only if*

$${}^tM \cdot J_\Delta \cdot M \equiv J_\Delta \mod d_g, \qquad \textit{where} \qquad J_\Delta := \begin{pmatrix} 0 & \Delta \\ -\Delta & 0 \end{pmatrix}$$

and $\Delta := \mathrm{Diag}(d_g/d_1, \cdots, d_g/d_{g-1}, 1)$.

If we write

$$M := \begin{pmatrix} A & C \\ B & D \end{pmatrix},$$

this is equivalent to ${}^tB\Delta A \equiv {}^tA\Delta B$, ${}^tD\Delta C \equiv {}^tC\Delta D$ and ${}^tA\Delta D - {}^tB\Delta C \equiv \Delta$ modulo d_g.

Proof. Let $l, m \in [\![1\ ;\ g]\!]$. Then

$$\begin{aligned} e_\delta(\sigma(e_l, 1), \sigma(e_m, 1)) &= e_\delta((Ae_l, \chi^{Be_l}), (Ae_m, \chi^{Be_m})) = \chi^{Be_j}(Ae_l)\chi^{-Be_l}(Ae_m) \\ &= \zeta^{\langle Ae_l|Be_m\rangle - \langle Be_l|Ae_m\rangle} = \zeta^{{}^te_l({}^tA\Delta B - {}^tB\Delta A)e_m} \end{aligned}$$

and $e_\delta((e_l, 1), (e_m, 1)) = 1$. Besides

$$\begin{aligned} e_\delta(\sigma(0, \chi_l), \sigma(0, \chi_m)) &= e_\delta((Ce_l, \chi^{De_l}), (Ce_m, \chi^{De_m})) = \chi^{De_m}(Ce_l)\chi^{-De_l}(Ce_m) \\ &= \zeta^{\langle Ce_l|De_m\rangle - \langle De_l|Ce_m\rangle} = \zeta^{{}^te_l({}^tC\Delta D - e_m - {}^tD\Delta C)e_m} \end{aligned}$$

and $e_\delta((0, \chi_l), (0, \chi_m)) = 1$. Finally

$$\begin{aligned} e_\delta(\sigma(e_l, 1), \sigma(0, \chi_m)) &= e_\delta((Ae_l, \chi^{Be_l}), (Ce_m, \chi^{De_m})) = \chi^{De_m}(Ae_l)\chi^{-Be_l}(Ce_m) \\ &= \zeta^{\langle Ae_l|De_m\rangle - \langle Be_l|Ce_m\rangle} = \zeta^{{}^te_l({}^tA\Delta D - e_m - {}^tB\Delta C)e_m} \end{aligned}$$

and $e_\delta((e_l,1),(0,\chi_m)) = \zeta^{d_g/d_l\delta_{l,m}}$. Hence, σ is symplectic if and only if ${}^tB\Delta A \equiv {}^tA\Delta B$, ${}^tD\Delta C \equiv {}^tC\Delta B$ and ${}^tA\Delta D - {}^tB\Delta C \equiv \Delta$ modulo d_g. The result immediately follows. □

We now finally prove an explicit change of basis formula between symmetric Theta structures $\Theta_{\mathcal{L}}$ and $\Theta'_{\mathcal{L}}$. This formula provides a *change of coordinates matrix* from $\Theta_{\mathcal{L}}$ to $\Theta'_{\mathcal{L}}$. In the rest of the paper, **we shall only consider symmetric Theta structures** (and simply mention them as Theta structures) in order to be able to use the following theorem.

Theorem 12 (Symplectic change of basis)**.** *Let $\Theta_{\mathcal{L}^2}$ be a symmetric theta-structure on $G(\mathcal{L}^2)$ and $\Theta_{\mathcal{L}}$ be the induced compatible theta-structure on $G(\mathcal{L})$. Let $\psi \in \mathrm{Aut}^0(\mathcal{H}(2\delta))$ and $\psi' \in \mathrm{Aut}^0(\mathcal{H}(\delta))$ be the induced symmetric automorphism (following Proposition 10.(i)). Let ζ be a primitive $2d_g$-th root of unitiy and*

$$M := \begin{pmatrix} A & C \\ B & D \end{pmatrix}$$

be the matrix of $\overline{\psi} \in \mathrm{Sp}(K(2\delta))$ in the ζ-canonical symplectic basis. Let $(\theta_i^{\mathcal{L}})_{i\in K_1(\delta)}$ and $(\theta'^{\mathcal{L}}_i)_{i\in K_1(\delta)}$ be respectively the $\Theta_{\mathcal{L}}$ and $\Theta'_{\mathcal{L}}$-coordinates (where $\Theta'_{\mathcal{L}} := \Theta_{\mathcal{L}} \circ \psi'$). Then, there exists $i_0 \in K_1(\delta)$ and $\lambda \in k^*$ such that for all $i \in K_1(\delta)$,

$$\theta'^{\mathcal{L}}_i = \lambda \sum_{j\in K_1(\delta)} \zeta^{\langle i|j\rangle - \langle Ai+Cj+2i_0|Bi+Dj\rangle}\theta^{\mathcal{L}}_{Ai+Cj+i_0}.$$

We can choose any value of $i_0 \in K_1(\delta)$ such that

$$\sum_{j\in K_1(\delta)} \zeta^{-\langle Cj+2i_0|Dj\rangle}\theta^{\mathcal{L}}_{i_0+Cj} \neq 0.$$

Proof. By Proposition 8, there exists $i_0 \in K_1(\delta)$ and $\lambda \in k^*$ such that $\theta'^{\mathcal{L}}_0 = \lambda T_{i_0}$, where

$$T_{i_0} := \sum_{j\in K_2(\delta)} \Theta_{\mathcal{L}} \circ \psi'(1,0,j)\cdot\theta^{\mathcal{L}}_{i_0}$$

is non-zero.

As explained before, we can identify $K_1(\delta)$ with $K_2(\delta)$ via the map $j \longmapsto \chi^j$, where $\chi^j(i) := \zeta^{2\langle i|j\rangle}$ for all $i,j \in K_1(\delta)$ (ζ^2 being a primitive d_g-th root of unity). Similarly, we identify $K_1(2\delta)$ with $K_2(2\delta)$ via the map $j \longmapsto \widetilde{\chi}^j$, where $\widetilde{\chi}^j(i) = \zeta^{\langle i|j\rangle}$ for all $i,j \in K_1(2\delta)$. Now, by Proposition 10, we can express ψ' as follows: for all $i,j \in K_1(\delta)$, we have:

$$\psi'(1,i,\chi^j) = \left(\widetilde{\chi}^{j'}(i')^{-1}\overline{\psi}_2(i',\widetilde{\chi}^{j'})(\overline{\psi}_1(i',\widetilde{\chi}^{j'})), \overline{\psi}_1(i',\widetilde{\chi}^{j'}), \overline{\psi}_2(i',\widetilde{\chi}^{j'})\right),$$

with $i',j' \in K_1(2\delta)$ such that $\overline{i'} = i$ and $\overline{j'} = j$. It follows that for all $(i,j) \in K_1(\delta)$,

$$\begin{aligned}\psi'(1,i,\chi^j) &= \left(\zeta^{-\langle i'|j'\rangle}\widetilde{\chi}^{Bi'+Dj'}(Ai'+Cj'), \overline{Ai'+Cj'}, \overline{\widetilde{\chi}^{Bi'+Dj'}}\right)\\ &= (\zeta^{-\langle i'|j'\rangle+\langle Bi'+Dj'|Ai'+Cj'\rangle}, Ai+Cj, \chi^{Bi+Dj})\\ &= (\zeta^{-\langle i|j\rangle+\langle Bi+Dj|Ai+Cj\rangle}, Ai+Cj, \chi^{Bi+Dj})\end{aligned}$$

For the last equality, we can easily check that $-\langle i'|j'\rangle + \langle Bi' + Dj'|Ai' + Cj'\rangle$ only depends on the values of i' and j' modulo d_g. Consequently,

$$\begin{aligned} T_{i_0} &= \sum_{j\in K_1(\delta)} \zeta^{\langle Dj|Cj\rangle}\chi^{Dj}(Cj+i_0)^{-1}\theta^{\mathcal{L}}_{Cj+i_0} \\ &= \sum_{j\in K_1(\delta)} \zeta^{\langle Dj|Cj\rangle}\zeta^{-2\langle Cj+i_0|Dj\rangle}\theta^{\mathcal{L}}_{Cj+i_0} \\ &= \sum_{j\in K_1(\delta)} \zeta^{-\langle Cj+2i_0|Dj\rangle}\theta^{\mathcal{L}}_{Cj+i_0} \end{aligned}$$

And, if $T_{i_0} \neq 0$, we have for all $i \in K_1(\delta)$,

$$\begin{aligned} \theta'^{\mathcal{L}}_i &= \Theta'_{\mathcal{L}}(1,i,1)\cdot\theta'^{\mathcal{L}}_0 = \lambda\Theta_{\mathcal{L}}\circ\psi(1,i,1)\cdot T_{i_0} \\ &= \lambda\sum_{j\in K_1(\delta)} \zeta^{-\langle Cj+2i_0|Dj\rangle}\Theta_{\mathcal{L}}\circ\psi(1,i,1)\cdot\theta^{\mathcal{L}}_{Cj+i_0} \\ &= \lambda\sum_{j\in K_1(\delta)} \zeta^{-\langle Cj+2i_0|Dj\rangle}\zeta^{\langle Bi|Ai\rangle}\chi^{Bi}(Ai+Cj+i_0)^{-1}\theta^{\mathcal{L}}_{Ai+Cj+i_0} \\ &= \lambda\sum_{j\in K_1(\delta)} \zeta^{-\langle Cj+2i_0|Dj\rangle}\zeta^{\langle Bi|Ai\rangle}\zeta^{-2\langle Bi|Ai+Cj+i_0\rangle}\theta^{\mathcal{L}}_{Ai+Cj+i_0} \\ &= \lambda\sum_{j\in K_1(\delta)} \zeta^{-\langle Cj+2i_0|Dj\rangle}\zeta^{-\langle Bi|Ai+2Cj+2i_0\rangle}\theta^{\mathcal{L}}_{Ai+Cj+i_0} \\ &= \lambda\sum_{j\in K_1(\delta)} \zeta^{-\langle Cj+2i_0|Bi+Dj\rangle-\langle Bi|Ai+Cj\rangle}\theta^{\mathcal{L}}_{Ai+Cj+i_0} \\ &= \lambda\sum_{j\in K_1(\delta)} \zeta^{-\langle Ai+Cj+2i_0|Bi+Dj\rangle+\langle Ai|Bi+Dj\rangle-\langle Bi|Ai+Cj\rangle}\theta^{\mathcal{L}}_{Ai+Cj+i_0} \\ &= \lambda\sum_{j\in K_1(\delta)} \zeta^{-\langle Ai+Cj+2i_0|Bi+Dj\rangle+\langle Ai|Dj\rangle-\langle Bi|Cj\rangle}\theta^{\mathcal{L}}_{Ai+Cj+i_0} \\ &= \lambda\sum_{j\in K_1(\delta)} \zeta^{-\langle Ai+Cj+2i_0|Bi+Dj\rangle+{}^t i({}^tA\Delta D-{}^tB\Delta C)j}\theta^{\mathcal{L}}_{Ai+Cj+i_0} \\ &= \lambda\sum_{j\in K_1(\delta)} \zeta^{-\langle Ai+Cj+2i_0|Bi+Dj\rangle+{}^t i\Delta j}\theta^{\mathcal{L}}_{Ai+Cj+i_0} \\ &= \lambda\sum_{j\in K_1(\delta)} \zeta^{-\langle Ai+Cj+2i_0|Bi+Dj\rangle+\langle i|j\rangle}\theta^{\mathcal{L}}_{Ai+Cj+i_0} \end{aligned}$$

This completes the proof. □

4. An algorithm to compute 2^e-isogenies with level 2 Theta coordinates

In this section, we explain how to compute a 2^e-isogeny $F : \mathcal{A} \longrightarrow \mathcal{B}$ between principally polarised abelian varieties abelian varieties (PPAV) of any dimension g with the Theta model of level 2. As in dimension 1, we compute F as a chain of 2-isogenies. In Section 4.1, we give an overview of this isogeny chain computation given an isotropic subgroup $K'' \subset \mathcal{A}[2^{e+2}]$ such that $\ker(F) = [4]K''$. In Section 4.2, we give a generic algorithm to compute a 2-isogeny in the Theta model of level 2 and we adapt this algorithm in Section 4.3 to the case of *gluing isogenies*, namely

isogenies defined over products of abelian varieties (*eg.* elliptic products, as in SQIsignHD) whose codomain is not isomorphic to a product of abelian varieties. Finally, we explain how to compute the dual of a 2-isogeny in Section 4.4.

4.1. **Algorithmic overview of a 2^e-isogeny computation.** Let $F : \mathcal{A} \longrightarrow \mathcal{B}$ be a 2^e-isogeny between PPAV with kernel $K \subset \mathcal{A}[2^e]$ of rank g. This means that K is a free $(\mathbb{Z}/2^e\mathbb{Z})$-module of rank g. Then, we can decompose F as a chain of 2-isogenies $F := f_e \circ \cdots \circ f_1$, with $\ker(f_i) = [2^{e-i}]f_{i-1} \circ \cdots \circ f_1(K)$ for all $i \in [\![1\ ;\ e]\!]$ [5, Lemma 51].

In the following, we say that we *compute* F when we compute all the 2-isogenies f_i which form a *chain representation* of F. As we shall see in Section 4.2, we can easily evaluate f_i once we know the dual theta-null point of its codomain (Algorithm 1). Hence, we shall *represent* the f_i with this data: *computing* f_i means computing the dual theta-null point of its codomain. In addition to a list of dual theta-null points (representing the f_i), the representation of F may include relevant change of basis matrices of theta-coordinates to ensure we can apply f_1 and compose the f_i in compatible theta-coordinates. This way, once we have computed (a chain representation of) F, we can evaluate it easily on points.

To compute the 2-isogeny $f_i : A_i \longrightarrow A_{i+1}$, one needs to know an isotropic subgroup $K_i'' \subset A_i[8]$ such that $[4]K_i'' = \ker(f_i)$. Otherwise, we would have to compute square roots, and guess signs which is more costly (see Remark 18). To simplify the isogeny theorem formula (see Theorem 3 and Lemma 13), we also need to make sure that the level 2 Theta-structure $\Theta_{\mathcal{L}_i}$ on $(A_i, \mathcal{L}_i)$ satisfies $K_2(\Theta_{\mathcal{L}_i}) = \ker(f_i)$.

To ensure these conditions for all $i \in [\![1\ ;\ e]\!]$, we proceed as follows. We assume that we know an isotropic subgroup $K'' \subset \mathcal{A}[2^{e+2}]$ such that $K = [4]K''$. To compute f_1, we first make sure the level 2 Theta structure $\Theta_{\mathcal{L}_1}$ on $(\mathcal{A}, \mathcal{L}_1)$ satisfies $K_2(\Theta_{\mathcal{L}_1}) = [2^{e+1}]K''$ (where, for instance, $\mathcal{L}_1 = \mathcal{L}_0^2$ and $\mathcal{L}_0$ is the principal polarization). Consider a totally symmetric level 2 Theta structure $\Theta_{\mathcal{L}_1}$ on $\mathcal{A}$ that is naturally given to us (*eg.* the product Theta structure on a product of elliptic curves). By Theorem 5.(ii), $\Theta_{\mathcal{L}_1}$ is completely determined by a symplectic basis $\mathscr{B}$ of $\mathcal{A}[4]$. We compute a symplectic matrix $M \in \mathrm{Sp}_{2g}(\mathbb{Z}/4\mathbb{Z})$ mapping $\mathscr{B}$ to a symplectic basis $\mathscr{C} := (S_1', \cdots, S_g', T_1', \cdots, T_g')$ of $\mathcal{A}[4]$ such that $(T_1', \cdots, T_g')$ is a basis of $[2^e]K''$. Let $\Theta'_{\mathcal{L}_1}$ be the Theta structure induced by the action of M on $\Theta_{\mathcal{L}_1}$. By Theorem 12, we know how to compute the new Theta coordinates associated to $\Theta'_{\mathcal{L}_1}$ and we now have $K_2(\Theta'_{\mathcal{L}_1}) = [2^{e+1}]K''$ by construction. We can then compute f_1 with the algorithms of Sections 4.2 and 4.3.

By [5, Theorem 56], $([2]f_1(S_1'), \cdots, [2]f_1(S_g'), f_1(T_1'), \cdots, f_1(T_g'))$ is a symplectic basis of $A_2[2]$, so we easily obtain a level 2 Theta structure on $(A_2, \mathcal{L}_2, \Theta_{\mathcal{L}_2})$ such that $K_2(\Theta_{\mathcal{L}_2}) = \ker(f_2) = \langle f_1(T_1'), \cdots, f_1(T_g')\rangle$ (see Section 4.2). Hence, once we have evaluated $[2^{e-2}]f_1(K'')$, we can compute f_2 without computing a change of basis. The same applies for all $i \geq 2$: we can compute f_i given $K_i'' := [2^{e-i}]f_{i-1} \circ \cdots \circ f_1(K'')$, without computing a change of basis.

As in dimension 1, the K_i'' are the leaves of a computation tree whose nodes are basis of rank g isotropic subgroups (with K'' as root node), left edges are doublings and right edges are evaluations by the f_i (see Fig. 1). Evaluating this tree can be done in quasi-linear time $O(e\log(e))$ with optimal strategies depending on the relative cost of evaluation and doublings. We refer Appendix E for a detailed

explanation on how these strategies are obtained and used to compute 2^e-isogenies (see Algorithm 20 in particular).

4.2. **Generic algorithm to compute a 2-isogeny in dimension g.** Let $(A, \mathcal{L}_0)$ and $(B, \mathcal{M}_0)$ be to PPAVs and $\mathcal{L} := \mathcal{L}_0^2$ and $\mathcal{M} := \mathcal{M}_0^2$. Both $\mathcal{L}$ and $\mathcal{M}$ are totally symmetric line bundles of level 2. Let $f : A \longrightarrow B$ be a 2-isogeny with respect to the principal polarizations $\varphi_{\mathcal{L}_0}$ and $\varphi_{\mathcal{M}_0}$. Then f is also an isogeny of polarised abelian varieties with respect to $\varphi_{\mathcal{L}^2}$ and $\varphi_{\mathcal{M}}$.

Let $K := \ker(f)$. In the following, we assume that $K = K_2(\Theta_{\mathcal{L}})$. Let $(T_1, \cdots, T_g)$ be a basis of K and $\mathscr{B}'' := (S_1'', \cdots, S_g'', T_1'', \cdots, T_g'')$ be a symplectic basis of $K(\mathcal{L}^4) = A[8]$ with respect to an 8-th root of unity $\zeta_8 \in k^*$ such that $[4]T_k'' = T_k$ for all $k \in [\![1\ ;\ g]\!]$. Then $\mathscr{B}''$ induces a symmetric theta-structure $\Theta_{\mathcal{L}^2}$ on $G(\mathcal{L}^2)$ by Theorem 5. Besides, $\mathscr{C} := ([2]f(S_1''), \cdots, [2]f(S_g''), f(T_1''), \cdots, f(T_g''))$ is a ζ_8^2-symplectic basis of $B[4]$ which induces a theta-structure $\Theta_{\mathcal{M}}$ on $G(\mathcal{M})$ which is compatible with $\Theta_{\mathcal{L}^2}$ by [5, Theorem 56]. $\Theta_{\mathcal{M}}$ is also symmetric by [17, Remark 4.2.15].

Lemma 13. *With this choice of theta-structure $\Theta_{\mathcal{M}}$, we have for all $i \in (\mathbb{Z}/2\mathbb{Z})^g$,*

$$f^*\theta_i^{\mathcal{M}} = \theta_{2i}^{\mathcal{L}^2}.$$

Proof. In $K(\mathcal{L}^2) = [2]^{-1}K(\mathcal{L})$, we have $K^{\perp} = [2]K_1(\Theta_{\mathcal{L}^2}) \oplus K_2(\Theta_{\mathcal{L}^2}) = K_1(\Theta_{\mathcal{L}}) \oplus K_2(\Theta_{\mathcal{L}^2})$, so that $K^{\perp,1} = K_1(\Theta_{\mathcal{L}})$ and $K_1 = \{0\}$. Taking the notations of Theorem 3 (applied to $\Theta_{\mathcal{L}^2}$ and $\Theta_{\mathcal{M}}$), we get that $\Theta_{\mathcal{M}}$ is determined by an isomorphism $\sigma : K_1(\Theta_{\mathcal{L}}) \xrightarrow{\sim} (\mathbb{Z}/2\mathbb{Z})^g$. By the definition of $\Theta_{\mathcal{M}}$ with respect to $\Theta_{\mathcal{L}^2}$ and σ [15, Theorem 4, p. 302], we get that:

$$\forall i \in (\mathbb{Z}/2\mathbb{Z})^g, \quad \overline{\Theta}_{\mathcal{M}}(i, 1) = f(\sigma^{-1}(i)).$$

Hence, with our choice of theta-structure $\Theta_{\mathcal{M}}$, we get that for all $l \in [\![1\ ;\ g]\!]$, $\sigma([4]S_l'') = e_l$, where $e_l \in (\mathbb{Z}/2\mathbb{Z})^g$ is the vector with component 1 at index l and 0 elsewhere. Besides, for all $l \in [\![1\ ;\ g]\!]$, $\overline{\Theta}_{\mathcal{L}^2}^{-1}([2]S_l'') = e_l \in K_1(\underline{4})$ so $\overline{\Theta}_{\mathcal{L}^2}^{-1} \circ \sigma^{-1}$ is the map $i \in (\mathbb{Z}/2\mathbb{Z})^g \longmapsto 2i \in (\mathbb{Z}/4\mathbb{Z})^g$. The result follows. □

By the above lemma, to compute the $\theta_i^{\mathcal{M}}(f(x))$, we have to compute the $\theta_{2i}^{\mathcal{L}^2}(x)$ knowing the $\theta_i^{\mathcal{L}}(x)$. We may use the duplication formulas introduced in Section 2.10 for that.

Notation 14. We introduce two operators on $k^{(\mathbb{Z}/2\mathbb{Z})^g}$:

- the *Hadamard* operator $H : (x_i)_{i \in (\mathbb{Z}/2\mathbb{Z})^g} \longmapsto \left(\sum_{i \in (\mathbb{Z}/2\mathbb{Z})^g} (-1)^{\langle i|j \rangle} x_i\right)_{j \in (\mathbb{Z}/2\mathbb{Z})^g}$;
- the *squaring* operator $S : (x_i)_{i \in (\mathbb{Z}/2\mathbb{Z})^g} \longmapsto (x_i^2)_{i \in (\mathbb{Z}/2\mathbb{Z})^g}$.

We also denote by $\star$ the component-wise product on $k^{(\mathbb{Z}/2\mathbb{Z})^g}$. Note that $H \circ H = 2^g\,\mathrm{id}$, so H is an involution up to a projective factor.

For all $l \in [\![1\ ;\ g]\!]$, we denote by $\chi_l \in \widehat{(\mathbb{Z}/2\mathbb{Z})^g}$ the character $i \longmapsto (-1)^{i_l}$. The χ_l form a basis of $\widehat{(\mathbb{Z}/2\mathbb{Z})^g}$ since every character $\chi \in \widehat{(\mathbb{Z}/2\mathbb{Z})^g}$ can be written as $\chi = \chi^j$ for a unique $j \in (\mathbb{Z}/2\mathbb{Z})^g$, where $\chi^j := \prod_{l=1}^g \chi_l^{j_l} : i \longmapsto (-1)^{\langle i|j \rangle}$. Using this canonical isomorphism between $(\mathbb{Z}/2\mathbb{Z})^g$ and $\widehat{(\mathbb{Z}/2\mathbb{Z})^g}$, we can index dual theta points by characters. In particular, we may write $(U_{\chi,0}^{\mathcal{M}}(x))_{\chi} = H((\theta_i^{\mathcal{M}}(x))_i)$.

Proposition 15. [1, Equation (3)] *Let $x \in A(k)$ and $(\theta_i^{\mathcal{M}}(0_B))_{i\in(\mathbb{Z}/2\mathbb{Z})^g}$ be the theta-null point of $(B, \mathcal{M}, \Theta_{\mathcal{M}})$. Then, we have (up to a projective constant):*

$$H((\theta_i^{\mathcal{M}}(f(x)))_i) \star H((\theta_i^{\mathcal{M}}(0_B))_i) = H \circ S((\theta_i^{\mathcal{L}}(x))_i). \tag{13}$$

Proof. Equation (9) ensures that (up to a projective constant), we have for all $\chi \in \widehat{(\mathbb{Z}/2\mathbb{Z})^g}$,

$$U^{\mathcal{L}^2}_{\chi,0}(x)U^{\mathcal{L}^2}_{\chi,0}(0_A) = \sum_{t\in(\mathbb{Z}/2\mathbb{Z})^g} \chi(t)\theta_t^{\mathcal{L}}(x)^2,$$

so that $(U^{\mathcal{L}^2}_{\chi,0}(x))_\chi \star (U^{\mathcal{L}^2}_{\chi,0}(0_A))_\chi = H \circ S((\theta_i^{\mathcal{L}}(x))_i)$. Besides, Equation (7) and Lemma 13, ensure that $(U^{\mathcal{L}^2}_{\chi,0}(x))_\chi = H((\theta^{\mathcal{L}^2}_{2i}(x))_i) = H((\theta_i^{\mathcal{M}}(f(x))_i)$, up to a projective constant. Finally, we also have $(U^{\mathcal{L}^2}_{\chi,0}(0_A))_\chi = H((\theta_i^{\mathcal{M}}(f(0_A))_i) = H((\theta_i^{\mathcal{M}}(0_B))_i)$. The result follows. □

Using the formula (13), we easily obtain an algorithm to evaluate f when the codomain theta-null point (or its dual) is known. This is a simple generalization of [1, Algorithm 6]. This algorithm only works when the dual theta constants of B do not vanish. We treat the vanishing case in the next section.

Algorithm 1: Generic isogeny evaluation algorithm.

Data: A theta point $(\theta_i^{\mathcal{L}}(x))_i$ of A and the dual theta-null point $H((\theta_i^{\mathcal{M}}(0_B))_i)$ of B with non-vanishing coordinates.
Result: $(\theta_i^{\mathcal{L}}(f(x)))_i$.
1 Precompute $C_j \longleftarrow 1/H((\theta_i^{\mathcal{M}}(0_B))_i)_j$ for all $j \in (\mathbb{Z}/2\mathbb{Z})^g$;
2 Compute $(Z_j)_j \longleftarrow H \circ S((\theta_i^{\mathcal{L}}(x))_i)$;
3 Compute $(Y_j)_j \longleftarrow (C_j \cdot Z_j)_j$;
4 **return** $H((Y_j)_j)$;

We now explain how to compute the dual theta-null point of B. Let $\mathcal{B} := (S'_1, \cdots, S'_g, T'_1, \cdots, T'_g)$ be a symplectic basis of $K(\mathcal{L}^2)$ adapted to the decomposition $K(\mathcal{L}^2) = K_1(\Theta_{\mathcal{L}^2}) \oplus K_2(\Theta_{\mathcal{L}^2})$. Let $\zeta_4 \in k$ such that $\zeta_4^2 = -1$ and $e_4(S'_l, T'_m) = \zeta_4^{\delta_{l,m}}$ for all $l, m \in [\![1\ ;\ g]\!]$. Then, $([2]T'_1, \cdots, [2]T'_g)$ is a basis of $[2]K_2(\Theta_{\mathcal{L}^2}) = K_2(\Theta_{\mathcal{L}}) = K$. Besides, $\mathcal{B}$ determines a symplectic isomorphism $\overline{\Theta}_{\mathcal{L}^2} : K(\underline{4}) \xrightarrow{\sim} K(\mathcal{L}^2)$ mapping the ζ_4-canonical symplectic basis of $K(\underline{4})$ (as defined in Section 3.2) to $\mathcal{B}$. By Theorem 5.(ii), $\overline{\Theta}_{\mathcal{L}^2}$ determines the symmetric theta-structure $\Theta_{\mathcal{L}}$ on $G(\mathcal{L})$. Via this isomorphism $\overline{\Theta}_{\mathcal{L}^2}$, for all $l \in [\![1\ ;\ g]\!]$, the character $\chi'_l : j \longmapsto \zeta_4^{j_l}$ corresponds to T'_l, so the character $\chi_l = {\chi'_l}^2 : j \longmapsto (-1)^{j_l}$ corresponds to $T_l := [2]T'_l$.

Lemma 16. *Let T''_l such that $[2]T''_l = T'_l$ for all $l \in [\![1\ ;\ g]\!]$. Then for all $l \in [\![1\ ;\ g]\!]$ and $\chi \in \widehat{(\mathbb{Z}/2\mathbb{Z})^g}$,*

$$U^{\mathcal{M}}_{\chi\chi_l,0}(0_B) \cdot H \circ S((\theta_i^{\mathcal{L}}(T''_l))_i)_\chi = U^{\mathcal{M}}_{\chi,0}(0_B) \cdot H \circ S((\theta_i^{\mathcal{L}}(T''_l))_i)_{\chi\chi_l}. \tag{14}$$

Proof. Let $l \in [\![1\ ;\ g]\!]$ and $\chi \in \widehat{(\mathbb{Z}/2\mathbb{Z})^g}$. Then, by (13), we get that

$$U^{\mathcal{M}}_{\chi,0}(0_B) \cdot U^{\mathcal{M}}_{\chi,0}(f(T''_l)) = H \circ S((\theta_i^{\mathcal{L}}(T''_l))_i)_\chi. \tag{15}$$

Since $[4]T''_l = T_l \in K$, $f(T''_l)$ has order 4 so $f(T''_l) \equiv f(T''_l) + [2]f(T''_l)$ in the Kummer variety $A/\pm$ and $\theta_i^{\mathcal{L}}(f(T''_l)) = \theta_i^{\mathcal{L}}(f(T''_l) + [2]f(T''_l))$ for all $i \in (\mathbb{Z}/2\mathbb{Z})^g$.

Besides, $\Theta_{\mathcal{L}^2}$ and $\Theta_{\mathcal{M}}$ are compatible so $[2]f(T_l'') \in K_2(\Theta_{\mathcal{M}})$ since $[2]T_l'' = T_l' \in K_2(\Theta_{\mathcal{L}^2})$. Assuming we have made the canonical choice of theta-structure $\Theta_{\mathcal{M}}$, the symplectic isomorphism $\overline{\Theta}_{\mathcal{M}} : K(\underline{2}) \xrightarrow{\sim} K(\mathcal{M})$ maps χ_l to $[2]f(T_l'')$ [5, Theorem 56]. Hence, equation (4) ensures that:

$$\forall i \in (\mathbb{Z}/2\mathbb{Z})^g, \quad \theta_i^{\mathcal{L}}(f(T_l'')) = \theta_i^{\mathcal{L}}(f(T_l'') + [2]f(T_l'')) = \chi_l(i)^{-1}\theta_i^{\mathcal{L}}(f(T_l'')),$$

so that,

$$\begin{aligned} U_{\chi,0}^{\mathcal{M}}(f(T_l'')) &= \sum_{t\in(\mathbb{Z}/2\mathbb{Z})^g} \chi(t)\theta_t^{\mathcal{M}}(f(T_l'')) = \sum_{t\in(\mathbb{Z}/2\mathbb{Z})^g} \chi(t)\chi_l(t)^{-1}\theta_t^{\mathcal{M}}(f(T_l'')) \\ &= U_{\chi\chi_l^{-1},0}^{\mathcal{M}}(f(T_l'')) = U_{\chi\chi_l,0}^{\mathcal{M}}(f(T_l'')), \end{aligned}$$

since $\chi_l^{-1} = \chi_l$. Combining this with (15), we finally obtain (14). □

Given a basis of 8-torsion points $(T_1'', \cdots, T_g'')$ lying above the basis of K, as in Lemma 16, we can compute the dual theta-null point $(U_{\chi,0}^{\mathcal{M}}(0_B))_\chi$ of B with Equation (14). First, we select $\chi^0 \in (\widehat{\mathbb{Z}/2\mathbb{Z}})^g$ and $l \in [\![1\ ;\ g]\!]$ such that $H \circ S((\theta_i^{\mathcal{M}}(T_l''))_i)_{\chi^0} \neq 0$ (so that $U_{\chi^0,0}^{\mathcal{M}}(0_B) \neq 0$ by (15)), and then we compute $U_{\chi^0\chi_l,0}^{\mathcal{M}}(0_B)/U_{\chi^0,0}^{\mathcal{M}}(0_B) = H \circ S((\theta_i^{\mathcal{L}}(T_l''))_i)_{\chi^0\chi_l}/H \circ S((\theta_i^{\mathcal{L}}(T_l''))_i)_{\chi^0}$. Then, taking $\chi := \chi^0\chi_l$, we find $l' \in [\![1\ ;\ g]\!]$ such that $H \circ S((\theta_i^{\mathcal{L}}(T_{l'}''))_i)_\chi \neq 0$ and obtain $U_{\chi\chi_{l'},0}^{\mathcal{M}}(0_B)/U_{\chi,0}^{\mathcal{M}}(0_B)$. Multiplying this by the previous quotient, we can get $U_{\chi\chi_{l'},0}^{\mathcal{M}}(0_B)/U_{\chi^0,0}^{\mathcal{M}}(0_B)$. We repeat the same procedure until we have covered all indices in $\chi \in (\widehat{\mathbb{Z}/2\mathbb{Z}})^g$, so we are finally able to compute $(U_{\chi,0}^{\mathcal{M}}(0_B)/U_{\chi^0,0}^{\mathcal{M}}(0_B))_\chi$.

To perform this computation, we fill in a computation tree whose nodes are characters of $(\widehat{\mathbb{Z}/2\mathbb{Z}})^g$ related to each other by multiplication by a χ_l for $l \in [\![1\ ;\ g]\!]$. Each edge between a parent χ and a child $\chi\chi_l$ stores the value $U_{\chi\chi_l,0}^{\mathcal{M}}(0_B)/U_{\chi,0}^{\mathcal{M}}(0_B)$. The tree filling algorithm is summarized in Algorithm 2. The full algorithm computing the codomain dual theta-null point is Algorithm 4, generalizing [1, Algorithm 5].

Remark 17. Algorithm 4 does not always terminate when some theta-constants $U_{\chi,0}^{\mathcal{M}}(0_B)$ vanish. This can happen when we compute a gluing isogeny (see Section 4.3). In this case, we may need more than g points to fill in the tree. This is not a problem because (14) generalizes to sums of T_l'' and products of χ_l.

Remark 18 (Codomain computation without 8-torsion points)**.** When the 8-torsion points $T_1'', \cdots, T_g''$ are not known but only a 2-torsion basis of the kernel is known, we can still compute the codomain of f. Using (13), we get that $S \circ H((\theta_i^{\mathcal{M}}(0_B))_i) = H \circ S((\theta_i^{\mathcal{L}}(0_A))_i)$, so we can compute the codomain theta null-point $(\theta_i^{\mathcal{M}}(0_B))_i$ with $2^g - 1$ square root computations and choices of signs (projectively). This method is not only more costly but also not sufficient to determine $(\theta_i^{\mathcal{M}}(0_B))_i$ in general because all sign choices may not be valid.

As Robert did in [18, Chapter 7, Appendix B.2], we can prove that we can make at least $g(g+1)/2$ arbitrary sign choices among $2^g - 1$. Indeed, we may act on a symplectic basis of $B[4]$ inducing the theta-structure $\Theta_{\mathcal{M}}$ via the symplectic matrix:

$$M := \begin{pmatrix} I_g & 0 \\ B & I_g \end{pmatrix} \in \mathrm{Sp}_{2g}(\mathbb{Z}/4\mathbb{Z}),$$

which fixes $K_2(\mathcal{M}^2)$. By Theorem 12, the new resulting theta-coordinates are ${\theta'}_i^{\mathcal{M}} = \zeta^{-\langle i|Bi\rangle}\theta_i^{\mathcal{M}}$ for all $i \in (\mathbb{Z}/2\mathbb{Z})^g$ (up to a projective factor), where $\zeta^2 = -1$.

Algorithm 2: Tree filling algorithm for the codomain dual theta-null point computation.

Data: Theta-coordinates $\theta_i^{\mathcal{L}}$ of 8-torsion points $T_1'', \cdots, T_g''$ such that $K = \langle [4]T_1'', \cdots, [4]T_g'' \rangle$.
Result: Full computation tree $\mathcal{T}$ as described above.

Initialize the computation tree $\mathcal{T} \longleftarrow \emptyset$;
while $\mathcal{T}$ *does not cover* $(\widehat{\mathbb{Z}/2\mathbb{Z}})^g$ **do**
  Select $\chi^0 \in (\widehat{\mathbb{Z}/2\mathbb{Z}})^g$ and initialize $\mathcal{T}$ at root χ^0;
  while *all terminal nodes of* $\mathcal{T}$ *are not not marked as leaves* **do**
    for *every terminal node* χ *of* $\mathcal{T}$ *not marked as a leaf* **do**
      $leaf \longleftarrow$ True;
      for $l = 1$ **to** g **do**
        if $\chi\chi_l \notin \mathcal{T}$ *and* $H \circ S((\theta_i^{\mathcal{L}}(T_l''))_i)_{\chi\chi_l} \neq 0$ **then**
          $E(\chi, \chi\chi_l) \longleftarrow H \circ S((\theta_i^{\mathcal{L}}(T_l''))_i)_{\chi\chi_l} / H \circ S((\theta_i^{\mathcal{L}}(T_l''))_i)_{\chi}$;
          Add $\chi\chi_l$ as the child of χ in $\mathcal{T}$ and store $E(\chi, \chi\chi_l)$ on the edge;
          $leaf \longleftarrow$ False;
        end
      end
      if $leaf$ **then**
        Mark χ as a leaf;
      end
    end
  end
end
return $\mathcal{T}$;

Algorithm 3: Tree evaluation recursive algorithm.

Data: A computation tree $\mathcal{T}$ as above and a root value u.
Result: $(U_{\chi,0}^{\mathcal{M}}(0_B))_{\chi \in \mathcal{T}}$.

Let χ^0 be the root of $\mathcal{T}$. Set $U_{\chi^0,0}^{\mathcal{M}}(0_B) \longleftarrow u$;
if $\mathcal{T} = \{\chi^0\}$ **then**
  return u;
else
  for *every child* χ *of* χ^0 **do**
    Let $U_{\chi,0}^{\mathcal{M}}(0_B) \longleftarrow E(\chi^0, \chi) \cdot u$;
    Recurse on subtree $\mathcal{T}_\chi$ with root χ and root value $U_{\chi,0}^{\mathcal{M}}(0_B)$;
  end
  return all the computed values $(U_{\chi,0}^{\mathcal{M}}(0_B))_{\chi \in \mathcal{T}}$;
end

Algorithm 4: Codomain dual theta-null point computation algorithm.

Data: Theta-coordinates $\theta_i^{\mathcal{L}}$ of 8-torsion points $T_1'', \cdots, T_g''$ such that $K = \langle [4]T_1'', \cdots, [4]T_g'' \rangle$.

Result: $(U^{\mathcal{M}}_{\chi,0}(0_B))_{\chi \in (\widehat{\mathbb{Z}/2\mathbb{Z}})^g}$.

1 Call Algorithm 2 to get a computation tree $\mathcal{T}$;

2 Call Algorithm 3 on $\mathcal{T}$ with root value $U^{\mathcal{M}}_{\chi^0,0}(0_B) = 1$ to compute $(U^{\mathcal{M}}_{\chi,0}(0_B))_{\chi \in (\widehat{\mathbb{Z}/2\mathbb{Z}})^g}$;

3 **return** $(U^{\mathcal{M}}_{\chi,0}(0_B))_{\chi \in (\widehat{\mathbb{Z}/2\mathbb{Z}})^g}$;

Since M is symplectic, we have ${}^tB = B$ by Lemma 11 so we have $g(g+1)/2$ values to choose. We have:

$$\forall i \in (\mathbb{Z}/2\mathbb{Z})^g, \quad \langle i|Bi\rangle = \sum_{k=1}^{g} i_k^2 B_{k,k} + 2 \sum_{1 \le k < l \le g} i_k i_l B_{k,l},$$

so the $\langle i|Bi\rangle$ are determined by the $B_{k,k}$ and the $B_{k,l} \mod 2$. For all $k \in [\![1\ ;\ g]\!]$ and $l \in [\![k+1\ ;\ g]\!]$, we may fix $B_{k,k} \in \{0, 2\}$ and $B_{k,l} \in \{0, 1\}$ and obtain ${\theta'}^{\mathcal{M}}_{e_k} = (-1)^{-B_{k,k}/2}\theta^{\mathcal{M}}_{e_k}$, ${\theta'}^{\mathcal{M}}_{e_k+e_l} = (-1)^{-(B_{k,k}+B_{l,l}+2B_{k,l})/2}\theta^{\mathcal{M}}_{e_k+e_l}$ and ${\theta'}^{\mathcal{M}}_{i} = \pm\theta^{\mathcal{M}}_i$ for all $i \in (\mathbb{Z}/2\mathbb{Z})^g$. This amounts to choosing $g(g+2)/2$ signs among $2^g - 1$ and fixing the others.

In dimension $g = 2$, it was already remarked in [1, § 4.2] that all $g(g+1)/2 = 3 = 2^g - 1$ arbitrary sign choices are valid. This is no longer true in dimension $g > 2$. In dimension $g = 3$, only 6 among 7 sign choices determine the last one with an explicit formula [41]. In dimension $g \ge 4$, we have no such explicit formulas so the theta null-point is harder to guess.

4.3. **Gluing isogenies.** In the previous section, we have seen how to compute 2-isogenies when none of the dual theta-coordinates $(U^{\mathcal{M}}_{\chi,0}(0_B))_\chi$ vanish. In this section, we treat the vanishing case which is frequent when we want to compute a *gluing isogeny*, namely isogenies defined over a product of abelian varieties whose codomain is not isomorphic to a product of abelian varieties $f : A_1 \times A_2 \longrightarrow B$. There is a heuristic explanation of this phenomenon. The level 2 Theta coordinates that we use represent points on the Kummer abelian variety, so up to a sign ambiguity. On a product of Kummer varieties $A_1/\pm \times A_2/\pm$ we have two sign ambiguities and on $B/\pm$, only one so we need additional information to evaluate f and remove one sign ambiguity. This additional information will be provided by point translates.

Assuming we have already computed the dual theta-constants $U^{\mathcal{M}}_{\chi,0}(0_B)$ (which may vanish), we immediately see that Algorithm 1 may no longer be used (to avoid divisions by zero). However, in order to evaluate $x \in A(k)$, we may still use (13) with translates of x. Let $T_1', \cdots, T_g'$ be points such that $\langle [2]T_1', \cdots, [2]T_g' \rangle = K$ as in the previous section. Then, for all $l \in [\![1\ ;\ g]\!]$ and $\chi \in (\widehat{\mathbb{Z}/2\mathbb{Z}})^g$, we have:

$$U^{\mathcal{M}}_{\chi,0}(f(x + T_l')) \cdot U^{\mathcal{M}}_{\chi,0}(0_B) = H \circ S((\theta_i^{\mathcal{L}}(x + T_l'))_i)_\chi. \tag{16}$$

As we have seen in the proof of Lemma 16, the Theta structure $\overline{\Theta}_{\mathcal{M}}$ maps $f(T_l')$ to χ_l so there exists a projective constant $\lambda_l \in k^*$ such that $U^{\mathcal{M}}_{\chi,0}(f(x + T_l')) =$

$\lambda_l U^{\mathcal{M}}_{\chi\chi_l,0}(f(x))$ for all $\chi \in (\widehat{\mathbb{Z}/2\mathbb{Z}})^g$. It follows by (13) and (16) that for all $l \in [\![1\ ;\ g]\!]$ and $\chi \in (\widehat{\mathbb{Z}/2\mathbb{Z}})^g$, we have:

$$\lambda_l \cdot H \circ S((\theta^{\mathcal{L}}_i(x))_i)_{\chi\chi_l} \cdot U^{\mathcal{M}}_{\chi,0}(0_B) = H \circ S((\theta^{\mathcal{L}}_i(x+T'_l))_i)_\chi \cdot U^{\mathcal{M}}_{\chi\chi_l,0}(0_B), \tag{17}$$

so we can compute the λ_l once we know the coordinates of x and the $x+T'_l$ (and 0_B). Since $\chi_l^2 = 1$, we also obtain by (13) that for all $l \in [\![1\ ;\ g]\!]$, we have:

$$\forall \chi \in (\widehat{\mathbb{Z}/2\mathbb{Z}})^g, \quad \lambda_l \cdot U^{\mathcal{M}}_{\chi,0}(f(x)) \cdot U^{\mathcal{M}}_{\chi\chi_l,0}(0_B) = H \circ S((\theta^{\mathcal{L}}_i(x+T'_l))_i)_{\chi\chi_l}. \tag{18}$$

Hence, to compute $U^{\mathcal{M}}_{\chi,0}(f(x))$, we may use (13) when $U^{\mathcal{M}}_{\chi,0}(0_B) \neq 0$ and otherwise, find $l \in [\![1\ ;\ g]\!]$ such that $U^{\mathcal{M}}_{\chi\chi_l,0}(0_B) \neq 0$ and use (18). We summarize the evaluation procedure in Algorithm 5.

Remark 19. In practice, we do not need to use all the translates $x+T'_l$ to compute the coordinates of $f(x)$. When $g = 2$ and $f : E_1 \times E_2 \longrightarrow B$ is a gluing of elliptic curves, one point (T'_1) is sufficient [1, Algorithm 8]. When $g = 4$ and $f : A_1 \times A_2 \longrightarrow B$ is a gluing of abelian surfaces, two points (T'_1 and T'_2) are sufficient.

Remark 20. Computing the $x + T'_l$ with the Theta model may not be easy since we also need to know the $x - T'_l$ to apply differential addition formulas (Theorem 6). This is not an issue when we work on elliptic curve products because we can use standard arithmetic. In practice, we compute chains of 2-isogenies starting from an elliptic curve product so we can always perform the additions of preimages of the points on this elliptic curve product and then push the result through several 2-isogenies.

The evaluation procedure of a gluing isogeny differs significantly from the generic one. However, the codomain theta-null point computation is very similar. As in the previous section, let $T''_1, \cdots, T''_g$ be 8-torsion points such that $T'_l = [2]T''_l$ for all $l \in [\![1\ ;\ g]\!]$ ($K = \langle [4]T''_1, \cdots, [4]T''_g \rangle$). For all multi-index $j \in (\mathbb{Z}/2\mathbb{Z})^g$, we denote $T''_j := \sum_{k=1}^g [j_k]T''_k$ and recall that $\chi^j := \prod_{i=1}^g \chi_k^{j_k}$. Then, (14) is still valid for multi-indices: for all $j \in (\mathbb{Z}/2\mathbb{Z})^g$ and $\chi \in (\widehat{\mathbb{Z}/2\mathbb{Z}})^g$,

$$U^{\mathcal{M}}_{\chi\chi^j,0}(0_B) \cdot H \circ S((\theta^{\mathcal{M}}_i(T''_j))_i)_\chi = U^{\mathcal{M}}_{\chi,0}(0_B) \cdot H \circ S((\theta^{\mathcal{M}}_i(T''_j))_i)_{\chi\chi^j}.$$

Using the above equation, we may obtain the dual theta constants $U^{\mathcal{M}}_{\chi,0}(0_B)$ from the theta-coordinates of (sums of) the $T''_1, \cdots, T''_g$ with tree filling algorithms as in the generic case (see Algorithms 2, 3 and 4).

Remark 21. For $g = 2$, when we glue a product of elliptic curves, only two points T''_1, T''_2 (and no sum of points) are needed [1, Algorithm 7]. For $g = 4$, in practice, when we glue two abelian surfaces only one point $T''_1 + T''_2$, in addition to $T''_1, \cdots, T''_4$ is needed for the codomain computation. As mentioned in Remark 20, when we compute a chain of 2-isogenies starting from an elliptic product, sums of preimages of the $T''_1, \cdots, T''_g$ may be computed on the domain and then pushed through several 2-isogenies.

4.4. **Computing dual isogenies.** Once we have computed a 2-isogeny $f : (A, \mathcal{L}^2) \longrightarrow (B, \mathcal{M})$ as in Sections 4.2 and 4.3, it is then easy to compute its dual $\widetilde{f} : B \longrightarrow A$ with the data we already have. By the following lemma, we only have to precompute the inverse theta-constants $(1/\theta^{\mathcal{L}}_i(0_A))_i$ to be able to evaluate $\widetilde{f}$. Up to Hadamard transforms, the formulas are similar to those of Section 4.2.

Algorithm 5: Gluing isogeny evaluation algorithm.

Data: 4-torsion points $T'_1, \cdots, T'_g$ such that $K = \langle [2]T'_1, \cdots, [4]T'_g \rangle$, a subset of indices $L \subseteq [\![1\ ;\ g]\!]$, theta points of A $(\theta_i^{\mathcal{L}}(x))_i$ and $(\theta_i^{\mathcal{L}}(x+T'_l))_i$ for all $l \in L$ and the dual theta-null point $(U^{\mathcal{M}}_{\chi,0}(0_B))_\chi$ of B.

Result: $(\theta_i^{\mathcal{L}}(f(x)))_i$.

Precompute $C_\chi \longleftarrow 1/U^{\mathcal{M}}_{\chi,0}(0_B)$ for all $\chi \in \widehat{(\mathbb{Z}/2\mathbb{Z})^g}$ such that $U^{\mathcal{M}}_{\chi,0}(0_B) \neq 0$;
Compute $H \circ S((\theta_i^{\mathcal{L}}(x))_i)$ and $H \circ S((\theta_i^{\mathcal{L}}(x+T'_l))_i)$ for all $l \in L$;
for $l \in L$ **do**
  Find $\chi \in \widehat{(\mathbb{Z}/2\mathbb{Z})^g}$ such that $H \circ S((\theta_i^{\mathcal{L}}(x+T'_l))_i)_\chi \cdot U^{\mathcal{M}}_{\chi\chi_l,0}(0_B) \neq 0$;
  $\lambda_l^{-1} \longleftarrow H \circ S((\theta_i^{\mathcal{L}}(x))_i)_{\chi\chi_l} \cdot U^{\mathcal{M}}_{\chi,0}(0_B) / (H \circ S((\theta_i^{\mathcal{L}}(x+T'_l))_i)_\chi \cdot U^{\mathcal{M}}_{\chi\chi_l,0}(0_B))$;
end
for $\chi \in \widehat{(\mathbb{Z}/2\mathbb{Z})^g}$ **do**
  if $U^{\mathcal{M}}_{\chi,0}(0_B) \neq 0$ **then**
    $U^{\mathcal{M}}_{\chi,0}(f(x)) \longleftarrow C_\chi \cdot H \circ S((\theta_i^{\mathcal{L}}(x))_i)_\chi$;
  else
    Find $l \in L$ such that $U^{\mathcal{M}}_{\chi\chi_l,0}(0_B) \neq 0$;
    $U^{\mathcal{M}}_{\chi,0}(f(x)) \longleftarrow \lambda_l^{-1} C_{\chi\chi_l} \cdot H \circ S((\theta_i^{\mathcal{L}}(x+T'_l))_i)_{\chi\chi_l}$;
  end
end
return $H((U^{\mathcal{M}}_{\chi,0}(f(x)))_\chi)$;

Lemma 22. *Let $f : (A, \mathcal{L}^2) \longrightarrow (B, \mathcal{M})$ be a 2-isogeny. As in Section 4.2, let $(\Theta_{\mathcal{L}}, \Theta_{\mathcal{L}^2})$ be a pair of symmetric theta-structures for $(\mathcal{L}, \mathcal{L}^2)$ such that $\ker(f) = K_2(\Theta_{\mathcal{L}})$ and $\Theta_{\mathcal{M}}$ be a theta-structure on $G(\mathcal{M})$ compatible with $\Theta_{\mathcal{L}^2}$ with respect to f. Then:*

(i) $\widetilde{f}$ is a polarised abelian variety $(B, \mathcal{M}^2) \longrightarrow (A, \mathcal{L})$ of kernel $\ker(\widetilde{f}) = K_1(\Theta_{\mathcal{M}})$.

(ii) We have for all $y \in B(k)$,

$$(\theta_i^{\mathcal{L}}(\widetilde{f}(y)))_i \star (\theta_i^{\mathcal{L}}(0_A))_i = H \circ S((U^{\mathcal{M}}_{\chi,0}(y))_\chi),$$

up to a projective constant.

Proof. **(i)** Recall that $\mathcal{L} = \mathcal{L}_0^2$ and $\mathcal{M} = \mathcal{M}_0^2$ where $\varphi_{\mathcal{L}_0}$ and $\varphi_{\mathcal{M}_0}$ are principal polarizations. Since f is a 2-isogeny, we have $f \circ \widetilde{f} = [2]$, where $\widetilde{f} = \varphi_{\mathcal{L}_0}^{-1} \circ \widehat{f} \circ \varphi_{\mathcal{M}_0}$. Hence, $\widehat{\widetilde{f}} = \widehat{\varphi_{\mathcal{M}_0}} \circ f \circ \widehat{\varphi_{\mathcal{L}_0}^{-1}}$ but $\widehat{\varphi_{\mathcal{M}_0}} = \varphi_{\mathcal{M}_0}$ and $\widehat{\varphi_{\mathcal{L}_0}^{-1}} = \varphi_{\mathcal{L}_0}^{-1}$, so that $\widehat{\widetilde{f}} = \varphi_{\mathcal{M}_0} \circ f \circ \varphi_{\mathcal{L}_0}^{-1}$. It follows that:

$$[2] = f \circ \widetilde{f} = \varphi_{\mathcal{M}_0}^{-1} \circ \widehat{\widetilde{f}} \circ \varphi_{\mathcal{L}_0} \circ \widetilde{f},$$

and $\widehat{\widetilde{f}} \circ \varphi_{\mathcal{L}_0} \circ \widetilde{f} = [2]\varphi_{\mathcal{M}_0}$. Since $\mathcal{L} = \mathcal{L}_0^2$ and $\mathcal{M} = \mathcal{M}_0^2$, we have $\varphi_{\mathcal{L}} = [2] \circ \varphi_{\mathcal{L}_0}$ and $\varphi_{\mathcal{M}^2} = [4] \circ \varphi_{\mathcal{L}_0}$ by the theorem of the square [3, Theorem 6.7]. We conclude that $\widehat{\widetilde{f}} \circ \varphi_{\mathcal{L}} \circ \widetilde{f} = \varphi_{\mathcal{M}^2}$ so $\widetilde{f}$ is a polarised abelian variety $(A, \mathcal{L}^2) \longrightarrow (B, \mathcal{M})$.

Besides, $f(A[2]) \subseteq \ker(\widetilde{f})$ since $\widetilde{f} \circ f = [2]$ and $\widetilde{f}$ is separable since $\mathrm{char}(k)$ is odd so $\#\ker(\widetilde{f}) = \deg(\widetilde{f}) = \deg(f) = 2^g$. We also have $f(A[2]) = f(K_1(\Theta_{\mathcal{L}})) = K_1(\Theta_{\mathcal{M}})$ by construction and $\#K_1(\Theta_{\mathcal{M}}) = 2^g$ so the inclusion $f(A[2]) \subseteq \ker(\widetilde{f})$ is an equality, which proves (i).

(ii) Consider the symplectic basis $\mathscr{B}'' = (S_1'', \cdots, S_g'', T_1'', \cdots, T_g'')$ of $K(\mathcal{L}^2) = A[8]$ introduced in Section 4.2 to define $\Theta_{\mathcal{L}^2}$ and a symplectic basis $\mathscr{B}''' = (S_1''', \cdots, S_g''', T_1''', \cdots, T_g''')$ of $K(\mathcal{L}^4) = A[16]$ such that $S_l'' = [2]S_l'''$ and $T_l'' = [2]T_l'''$ for all $l \in [\![1\ ;\ g]\!]$. By Theorem 5.(ii), $\mathscr{B}'''$ induces a symmetric Theta-structure $\Theta_{\mathcal{L}^4}$ on $G(\mathcal{L}^4)$. In addition, by Theorem 5.(i), $\Theta_{\mathcal{L}^4}$ induces a symmetric Theta-structure $\Theta'_{\mathcal{L}^2}$ on $G(\mathcal{L}^2)$ and by Theorem 5.(ii), $\Theta'_{\mathcal{L}^2}$ is determined by $[2]\mathscr{B}''' = \mathscr{B}''$ so $\Theta'_{\mathcal{L}^2} = \Theta_{\mathcal{L}^2}$ and $\Theta_{\mathcal{L}^4}$ is compatible with $\Theta_{\mathcal{L}^2}$. Then, one can prove exactly as in [5, Theorem 56], that $\mathscr{C}' = (f(S_1''), \cdots, f(S_g''), f(T_1'''), \cdots, f(T_g'''))$ is a symplectic basis of $B[8]$ which induces a symmetric theta-structure $\Theta_{\mathcal{M}^2}$ on $G(\mathcal{M}^2)$ which is compatible with $\Theta_{\mathcal{L}^4}$ with respect to f. Since $\mathscr{C} = [2]\mathscr{C}'$ is the symplectic basis determining $\Theta_{\mathcal{M}}$, we can conclude by Theorem 5 that $\Theta_{\mathcal{M}^2}$ is compatible with $\Theta_{\mathcal{M}}$.

Let $\zeta_8 := e_{16}(S_1'', T_1'')$ and $\psi \in \mathrm{Aut}^0(\mathcal{H}(\underline{8}))$ such that $\overline{\psi}$ has matrix

$$M_\psi := \begin{pmatrix} 0 & -I_g \\ I_g & 0 \end{pmatrix} \in \mathrm{Sp}(K(\underline{8})),$$

in the ζ_8-canonical symplectic basis. Let $\psi' \in \mathrm{Aut}^0(\mathcal{H}(\underline{4}))$ be the symmetric Heisenberg automorphism induced by ψ (Proposition 10.(i)). Let $\Theta'_{\mathcal{M}^2} := \Theta_{\mathcal{M}^2} \circ \psi$, $\Theta'_{\mathcal{M}} := \Theta_{\mathcal{M}} \circ \psi'$ and $\Theta'_{\mathcal{L}} := \Theta_{\mathcal{L}} \circ \psi'$. Then, by Theorem 12, the $\Theta'_{\mathcal{M}}$-coordinates are the dual of the $\Theta_{\mathcal{M}}$-coordinates (obtained after a Hadamard transform) and similarly for the $\Theta'_{\mathcal{L}}$ and $\Theta_{\mathcal{L}}$-coordinates. Besides, $M_\psi \cdot \mathscr{C}' = (-f(T_1'''), \cdots, -f(T_g'''), f(S_1''), \cdots, f(S_g''))$ induces $\Theta'_{\mathcal{M}^2}$ and $M_\psi \cdot \mathscr{B} = (-T_1', \cdots, -T_g', S_1', \cdots, S_g')$ induces $\Theta'_{\mathcal{L}}$. Hence, [5, Theorem 56] ensures that $\Theta'_{\mathcal{M}^2}$ and $\Theta'_{\mathcal{L}}$ are compatible with respect to $\widetilde{f}$. We also have $\ker(\widetilde{f}) = K_1(\Theta_{\mathcal{L}}) = K_2(\Theta'_{\mathcal{L}})$ by (i). We conclude by Proposition 15 that for all $y \in B(k)$,

$$H(U^{\mathcal{L}}_{\chi,0}(\widetilde{f}(y)))_\chi) \star H((U^{\mathcal{L}}_{\chi,0}(0_A))_\chi) = H \circ S((U^{\mathcal{M}}_{\chi,0}(y))_\chi),$$

up to a projective constant, $U^{\mathcal{L}}_{\chi,0}$ and $U^{\mathcal{M}}_{\chi,0}$ being the $\Theta'_{\mathcal{L}}$ and $\Theta'_{\mathcal{M}}$-coordinates respectively. Since $H((U^{\mathcal{L}}_{\chi,0}(x))_\chi) = (\theta^{\mathcal{L}}_i(x))_i$ for all $x \in A(k)$, this completes the proof. □

4.5. **Complexity.** In Table 1, we give some operation counts for 2-isogeny computations. Unlike what we have assumed so far, in practice, the base field k that we use is not algebraically closed. All operations take place in the field of definition of torsion points used to compute isogenies (that we also denote by k). We denote by M, S, I and a the cost (in bit operations) of multiplication, squaring, inversion and addition/subtraction over k. In general, inversions are much more costly than multiplications so we compute them by batch. This enables to replace nI by $3(n-1)M + I$ as explained in Appendix D.1. We can even work projectively and remove the inversion[4]. While additions are much less costly than multiplications, Hadamard transforms require a lot of them, which can impact concrete performance. For that reason, we propose in Appendix D.2 a recursive method to compute Hadamard transforms which reduces their cost from $2^{2g}a$ to $g2^g a$.

5. Cryptographic applications

In this section, we apply the algorithms presented in Section 4 to compute a 4 dimensional 2^e-isogeny between elliptic curve products. The main applications

[4]This optimisation is not implemented in our dimension 4 code.

TABLE 1. Cost of algorithms involved in 2-isogeny computations. Here, $L \subseteq [\![1\ ;\ g]\!]$ is the subset given on entry of Algorithm 5. $\#L = 2$ for $g = 4$ (Remark 19). Inversions in parenthesis could be removed by working purely projectively.

		Dimension g	Dimension 4
Doubling	Precomp.	$(I) + 3(2^{g+1} - 1)M + 2^g S + g2^{g+1}a$	$(I) + 62M + 16S + 128a$
Algorithm 8	Main	$2^{g+1}M + 2^{g+1}S + g2^{g+1}a$	$32M + 32S + 128a$
Codomain (Algorithm 4)		$(I) + (2^g + 3g - 4)M + g2^g S + g^2 2^g a$	$(I) + 24M + 64S + 256a$
Evaluation	Precomp.	$(I) + 3(2^g - 1)M$	$(I) + 45M$
Algorithm 1	Main	$2^g M + 2^g S + g2^{g+1}a$	$16M + 16S + 128a$
Evaluation	Precomp.	$\leq (I) + 3(2^g - 1)M$	$\leq (I) + 45M$
(gluing)	Main	$\leq (I) + (2^{g+1} + 5\#L - 1)M +$	$\leq (I) + 41M + 48S$
Algorithm 5		$(\#L + 1)2^g S + (\#L + 2)g2^g a$	$+256a$

we have in mind is the verification procedure in SQIsignHD [5] and SIDH torsion attacks [22] but this could also be applied to other cryptographic constructions [21], or more generally, an improvement of the Deuring correspondence [25, Remark 2.9]. In [5, Appendix F], algorithms for the verification procedure were briefly presented but they differ significantly from the real implementation[5] relying on the ideas of Section 4 and do not include several optimizations and implementation details presented here.

Recall that in SQIsignHD, we compute the 2^e-isogeny given by Kani's lemma [26] as follows:

$$F := \begin{pmatrix} \alpha_1 & \widetilde{\Sigma} \\ -\Sigma & \widetilde{\alpha}_2 \end{pmatrix} \in \mathrm{End}(E_1^2 \times E_2^2), \tag{19}$$

where $\Sigma := \mathrm{Diag}(\sigma, \sigma) : E_1^2 \longrightarrow E_2^2$ with $\sigma : E_1 \longrightarrow E_2$ a q-isogeny and for $i \in \{1, 2\}$,

$$\alpha_i := \begin{pmatrix} a_1 & a_2 \\ -a_2 & a_1 \end{pmatrix} \in \mathrm{End}(E_i^2),$$

with $a_1, a_2 \in \mathbb{Z}$ such that $a_1^2 + a_2^2 + q = 2^e$. Input data a_1, a_2 is given along with a basis (P_1, P_2) of $E_1[2^f]$ (where $f \geq e/2 + 2$) and its image $(\sigma(P_1), \sigma(P_2))$. We have to compute F and evaluate it on some points. We shall keep those notations in the following.

5.1. **Gluing isogenies.** As explained previously, F will be computed as a chain of 2-isogenies. Our goal here is to determine where gluing isogenies appear in the chain in order to optimize our computations (because gluing isogenies are computed differently than generic ones and more expensive).

Since q is odd, either one of the a_1 or a_2 must be even. Without loss of generality, we can assume that a_2 is even (so that a_1 is odd). Then, we have:

Lemma 23. *Assume that $2|a_2$ and let $m := v_2(a_2)$ be its 2-adic valuation. Then $F := G \circ f_{m+1} \circ f_m \circ \cdots \circ f_1$, with*

$$E_1^2 \times E_2^2 \xrightarrow{f_1} A_1^2 \quad \cdots \quad A_{m-1}^2 \xrightarrow{f_m} A_m^2 \xrightarrow{f_{m+1}} B,$$

[5]This implementation can be found here `https://github.com/Pierrick-Dartois/SQISignHD-lib`.

a chain of 2*-isogenies, where the* A_i *are abelian surfaces and* B *is an abelian variety of dimension 4. For all* $i \in [\![2\ ;\ m]\!]$, $f_i := (\varphi_i, \varphi_i)$, *with* $\varphi_i : A_{i-1} \longrightarrow A_i$ *and* $f_1 : (R_1, S_1, R_2, S_2) \longmapsto (\varphi_1(R_1, R_2), \varphi_1(S_1, S_2))$, *with* $\varphi_1 : E_1 \times E_2 \longrightarrow A_1$. *Besides,*

$$\ker(\varphi_m \circ \cdots \circ \varphi_1) = \{([a_1]P, \sigma(P)) \mid P \in E_1[2^m]\}.$$

Proof. Kani's lemma [26] ensures that

$$\ker(F) = \{([a_1]P - [a_2]Q, [a_2]P + [a_1]Q, \sigma(P), \sigma(Q)) \mid P, Q \in E_1[2^e]\}.$$

Let $f_1, \cdots, f_{m+1}$ be the $m+1$ first elements of the 2-isogeny chain F. Then, since $a_2 \equiv 0 \mod 2^m$, we have

$$\ker(f_m \circ \cdots \circ f_1) = [2^{e-m}] \ker(F) = K_1 \oplus K_2,$$

where $K_1 := \{([a_1]P, 0, \sigma(P), 0) \mid P \in E_1[2^m]\}$ and $K_2 := \{(0, [a_1]P, 0, \sigma(P)) \mid P \in E_1[2^m]\}$. This proves the chain $f_m \circ \cdots \circ f_1$ has the desired form. This completes the proof. □

The above lemma indicates we should compute the first $m := v_2(a_2)$ isogenies of the chain in dimension 2 and treat f_{m+1} as a gluing isogeny. This is how we proceed in the following.

5.2. **Computing a 4 dimensional endomorphism derived from Kani's lemma with full available torsion.** In this paragraph, we assume we can access to 2^{e+2}-torsion points of supersingular elliptic curves. This way, we can compute at once the isogeny $F \in \mathrm{End}(E_1^2 \times E_2^2)$ as a chain of 2-isogenies. Using the notations of Lemma 23, we propose the following strategy:

(1) We compute the first $m = v_2(a_2)$ isogenies by computing the 2-isogeny chain $\Phi := \varphi_m \circ \cdots \circ \varphi_1$ in dimension 2. Our implementation of this step relies on [1].
(2) We then compute the isogeny $f_{m+1} : A_m^2 \longrightarrow B$ assuming it is a gluing isogeny, so using Algorithm 4 with 5 points on entry instead of 4 (Remark 21).
(3) We can compute a maximal isotropic subgroup $K'' \subset B[2^{e-m+1}]$ such that $[4]K'' = \ker(G)$ and we can finally compute the 2^{e-m-1}-isogeny $G : B \longrightarrow E_1^2 \times E_2^2$.
(4) We compute a change of theta-coordinates to express image points by G in $(x : z)$-Montgomery coordinates on $E_1^2 \times E_2^2$.

Prior to the computation of (gluing) isogenies φ_1 and f_{m+1}, we have to compute changes of theta-coordinates. These changes of basis are described in full detail in Appendices B.1 and B.2. Since m can be significantly bigger than 1 in some cases, the computation of Φ in step 1 above uses optimal strategies that can be computed as in dimension 1 [10, 12].

However, for the computation of $G := f_e \circ \cdots \circ f_{m+2}$ in step 3 the optimal strategy has to satisfy several constraints:

- First, we select a strategy of depth $e-m$ instead of $e-m-1$ that integrates the first $m+1$ isogenies $f_{m+1} \circ \cdots \circ f_1$ as one "first step" (more costly than a regular isogeny evaluation). Indeed, if we started the strategy at f_{m+2}, we would need to compute $[2^{e-m-2}]K''$ to obtain f_{m+2}. Doubling $e-m-2$ times a basis of K'' may be more costly than reusing some point doublings we already have computed on $E_1^2 \times E_2^2$ to compute the first m isogenies and pushing them through $f_{m+1} \circ \cdots \circ f_1$.

- Second, the strategy should not contain any doubling on the codomain B of f_{m+1}. Indeed, B may have zero dual theta constants as we have seen in Section 4.3, which dramatically increases the cost of doublings.
- Third, the strategy should not contain any doubling on the domain of f_{e-m}, for the same reason. Indeed, Lemma 23 also applies to $\widetilde{F}$ so $\widetilde{f}_{e-m}$ may be a gluing isogeny and its dual theta constants may vanish.

We refer to Appendix E.2 for the construction of such optimal strategies.

Algorithm 6 summarizes steps 1-3 above to compute F as a 2-isogeny chain. The output is used in Algorithm 7 to evaluate F on a point. The evaluation procedure requires a change of Theta coordinates on the codomain $E_1^2 \times E_2^2$ to recover the product Theta structure (step 4) as explained in Appendix B.3. Points can then be converted into $(x : z)$-Montgomery coordinates with Algorithm 12.

5.3. **Cutting the endomorphism computation in two.** In this paragraph, we explain how to compute $F \in \mathrm{End}(E_1^2 \times E_2^2)$ as defined in (19) when we cannot access the 2^{e+2}-torsion of elliptic curves but only "half" of it. Namely, we can access the $2^{e'+2}$-torsion with $e' \geq e/2$. We follow the approach of [5, § 4.4]: we write $F := F_2 \circ F_1$ where F_i is a 2^{e_i}-isogeny with $e_i \leq e'$ for $i \in \{1, 2\}$ and $e = e_1 + e_2$. We compute F_1 and $\widetilde{F}_2$ whose kernels are respectively:

$$\ker(F_1) = \{([a_1]P - [a_2]Q, [a_2]P + [a_1]Q, \sigma(P), \sigma(Q)) \mid P, Q \in E_1[2^{e_1}]\}$$

$$\ker(\widetilde{F}_2) = \{([a_1]P + [a_2]Q, -[a_2]P + [a_1]Q, -\sigma(P), -\sigma(Q)) \mid P, Q \in E_1[2^{e_2}]\}.$$

And we compute the dual $F_2 = \widetilde{\widetilde{F}}_2$ to obtain $F = F_2 \circ F_1$.

Since $\ker(F_1) = \ker(F)[2^{e_1}]$ and $\ker(\widetilde{F}_2) = \ker(\widetilde{F})[2^{e_2}]$, Lemma 23 applies to F_1 and an analogue of Lemma 23 applies to $\widetilde{F}_2$ (see Lemma 28), so we may assume $e_1, e_2 \geq m$. Then the computation of F_1 and $\widetilde{F}_2$ starts by a chain of m isogenies of dimension 2 and a gluing isogeny in dimension 4.

Unlike previously, we do not expect any splitting in the chains of 2-isogenies representing F_1 and $\widetilde{F}_2$ (except in very rare cases). However, we expect to be able to recover the same codomain $\mathcal{C}$ for F_1 and $\widetilde{F}_2$, or more exactly, to identify the theta-structures on $\mathcal{C}$ induced by F_1 and $\widetilde{F}_2$. This identification is not automatic and depends on the choice of theta-structures (*i.e.* of symplectic basis of the $2^{e'}$-torsion) that we make on $E_1^2 \times E_2^2$ prior to the computation of F_1 and $\widetilde{F}_2$. We explain how to make this choice in Appendix C.2. This choice also affects the change of theta-coordinates that we perform to compute the $(m+1)$-th gluing isogenies in the 2-isogeny chains F_1 and $\widetilde{F}_2$. This is explained in Appendix C.2.2.

To compute the dual $F_2 = \widetilde{\widetilde{F}}_2$, we only have to compute the dual isogeny of every 2-isogeny intervening in the chain $\widetilde{F}_2$. This can be done easily by Lemma 22. However, note that Lemma 23 also applies to $\widetilde{F}_2$. As a consequence, the first m isogenies of the chain $\widetilde{F}_2$ are computed in dimension 2 and the $(m+1)$-th isogeny is a gluing isogeny $g_{m+1} : A'^2_m \longrightarrow B'$. After the computation of $\widetilde{g}_{m+1}$, the product theta-structure on the codomain A'^2_m has to be recovered before computing the dual of the m 2-dimensional 2-isogenies. This is explained in Appendix C.3. We refer to Algorithm 13 in Appendix C for a detailed overview of the computation of F with half available torsion and to Algorithm 14 for its evaluation.

Algorithm 6: Computation of a 4 dimensional endomorphism derived from Kani's lemma with full available torsion.

Data: a_1, a_2, q such that a_2 is even, q is odd and $a_1^2 + a_2^2 + q = 2^e$, two supersingular elliptic curves E_1 and E_2 defined over $\mathbb{F}_{p^2}$, (P_1'', Q_1'') a basis of $E_1[2^{e+2}]$, $(\sigma(P_1''), \sigma(Q_1''))$ for some q-isogeny $\sigma : E_1 \longrightarrow E_2$.

Result: A chain representation of the isogeny $F \in \mathrm{End}(E_1^2 \times E_2^2)$ given by (19).

$m \longleftarrow v_2(a_2)$, $r \longleftarrow 1/q \mod 4$, $\mu \longleftarrow 1/a_1 \mod 2^{e+2}$;

(Pre)compute an optimal strategy S with m leaves [11, Algorithm 60];

(Pre)compute an optimal strategy S' with $e - m$ leaves with constraints at the beginning and m steps before the end (see Appendix E.2);

/* Step 1: First m isogenies in dimension 2 */

$c \longleftarrow e - m - 1$, $P_1', Q_1', P_2', R_2' \longleftarrow [2^c]P_1'', [2^c]Q_1'', [2^c]\sigma(P_1''), [2^c]\sigma(Q_1'')$;

$P_1, Q_1, P_2, Q_2 \longleftarrow [2^{m+1}]P_1', [2^{m+1}]Q_1', [2^{m+1}]P_2', [r2^{m+1}]R_2'$;

$\zeta_4 \longleftarrow e_4(P_1, Q_1)$;

$T_1, T_2 \longleftarrow [2]([a_1]P_1' - [a_2]Q_1', P_2'), [2]([a_2]P_1' + [a_1]Q_1', R_2')$;

For $i \in \{1, 2\}$, compute a basis (α_i, β_i) of $E_i[4]$ such that $\beta_i = (-1 : 1)$ in $(x : z)$-Montgomery coordinates and $e_4(\alpha_i, \beta_i) = \zeta_4$;

Compute the change of basis matrices M_i from (α_i, β_i) to (P_i, Q_i) for $i \in \{1, 2\}$;

Find a Theta structure $\Theta'_{\mathcal{L}}$ on $(E_1 \times E_2, \mathcal{L})$ such that $K_2(\Theta'_{\mathcal{L}}) = [2^{m+1}]\langle T_1, T_2\rangle$ and compute the change of coordinates matrix N_{12} from $(x : z)$ to $\Theta'_{\mathcal{L}}$ (using Algorithm 9 with input $a_1, a_2, q, (\alpha_i : \beta_i), M_i, \zeta_4$);

$(\theta'^{\mathcal{L}}_j(T_i))_j \longleftarrow N_{12} \cdot {}^t(x_1(T_i)x_2(T_i), x_1(T_i)z_2(T_i), z_1(T_i)x_2(T_i), z_1(T_i)z_2(T_i))$ for $i \in \{1, 2\}$;

Use the coordinates $(\theta'^{\mathcal{L}}_j(T_i))_j$ and strategy S to compute a 2-dimensional 2-isogeny chain $\Phi := \varphi_m \circ \cdots \circ \varphi_1$ of kernel $\ker(\Phi) = [4]\langle T_1, T_2\rangle$ (see [1]);

/* Step 2: Gluing isogeny f_{m+1} in dimension 4 */

$V_1 \longleftarrow (\Phi([a_1]P_1', P_2'), \Phi([a_2]P_1', 0))$;

$V_2 \longleftarrow (\Phi([a_1]Q_1', R_2'), \Phi([a_2]Q_1', 0))$;

$V_3 \longleftarrow (\Phi(-[a_2]P_1', 0), \Phi([a_1]P_1', P_2'))$;

$V_4 \longleftarrow (\Phi(-[a_2]Q_1', 0), \Phi([a_1]Q_1', R_2'))$;

$V_5 \longleftarrow (\Phi([a_1](P_1' + Q_1'), P_2' + R_2'), \Phi([a_2](P_1' + Q_1'), 0)) = V_1 + V_2$;

Let $\Theta_{\mathcal{L}_m}$ be the level 2 Theta-structure on the codomain $(A_m, \mathcal{L}_m)$ of Φ and $\Theta_{\mathcal{M}_m} := \Theta_{\mathcal{L}_m} \times \Theta_{\mathcal{L}_m}$;

Find a Theta structure $\Theta'_{\mathcal{M}_m}$ on $(A_m^2, \mathcal{M}_m)$ such that $K_2(\Theta'_{\mathcal{M}_m}) = [4]\langle V_1, \cdots, V_4\rangle$ and compute the change of basis matrix N_{24} from $\Theta_{\mathcal{M}_m}$ to $\Theta'_{\mathcal{M}_m}$-coordinates (using Algorithm 10 with input a_1, a_2, q, m, ζ_4);

$(\theta'^{\mathcal{M}_m}_j(V_i))_j \longleftarrow N_{24} \cdot (\theta^{\mathcal{M}_m}_j(V_i))_j$ for $i \in [\![1\ ;\ 5]\!]$;

Using the $(\theta'^{\mathcal{M}_m}_j(V_i))_j$ for $i \in [\![1\ ;\ 5]\!]$, compute f_{m+1} of kernel $[4]\langle V_1, \cdots, V_4\rangle$ (Algorithm 4 and Remark 21);

/* Step 3: Last $e-m-1$ isogenies in dimension 4 */
$V_1' \longleftarrow f_{m+1}(\Phi([a_1]P_1'' - [\mu]P_1, \sigma(P_1'')), \Phi([a_2]P_1'', 0))$;
$V_2' \longleftarrow f_{m+1}(\Phi([a_1]Q_1'', \sigma(Q_1'')), \Phi([a_2]Q_1'', 0))$;
$V_3' \longleftarrow f_{m+1}(\Phi(-[a_2]P_1'', 0), \Phi([a_1]P_1'', \sigma(P_1'')))$;
$V_4' \longleftarrow f_{m+1}(\Phi(-[a_2]Q_1'', 0), \Phi([a_1]Q_1'' - [\mu]Q_1, \sigma(Q_1'')))$;
Use Algorithm 21 with input $V_1', \cdots, V_4'$ and strategy S' to compute a 4-dimensional 2-isogeny chain $f_e \circ \cdots \circ f_{m+2}$ of kernel $[4]\langle V_1', \cdots, V_4'\rangle$;
/* Step 4: Splitting change of Theta coordinates */
Let $\Theta_{\mathcal{L}_0} := \Theta_{\mathcal{L}_1} \times \Theta_{\mathcal{L}_1} \times \Theta_{\mathcal{L}_2} \times \Theta_{\mathcal{L}_2}$ be the product Theta structure on $(E_1^2 \times E_2^2, \mathcal{L}_0)$ induced by the (α_i, β_i) $(i \in \{1,2\})$;
Let $\Theta'_{\mathcal{L}_0}$ be the (non-product) level 2 Theta structure on $(E_1^2 \times E_2^2, \mathcal{L}_0)$ generated when computing f_e;
Compute the change of basis matrix N_{41} from $\Theta'_{\mathcal{L}_0}$ to $\Theta_{\mathcal{L}_0}$-coordinates (using Algorithm 11 with input $a_1, a_2, q, m, M_1, M_2, \zeta_4$);
return $N_{12}, \varphi_1, \cdots, \varphi_m, N_{24}, f_{m+1}, \cdots, f_e, N_{41}, (\alpha_1, \beta_1), (\alpha_2, \beta_2)$;

Algorithm 7: Evaluation of a 4 dimensional endomorphism derived from Kani's lemma with full available torsion given its representation.

Data: A chain C outputted by Algorithm 6 representing $F \in \mathrm{End}(E_1^2 \times E_2^2)$ given by (19), and a point $Q \in E_1^2 \times E_2^2$.
Result: The Montgomery $(x:z)$-coordinates of $F(Q)$.
Parse C as $N_{12}, \varphi_1, \cdots, \varphi_m, N_{24}, f_{m+1}, \cdots, f_e, N_{41}, (\alpha_1, \beta_1), (\alpha_2, \beta_2)$;
$v \longleftarrow {}^t(x(Q_1)x(Q_3), x(Q_1)z(Q_3), z(Q_1)x(Q_3), z(Q_1)z(Q_3))$;
$(\theta'^{\mathcal{L}}_i(Q_1, Q_3))_i \longleftarrow N_{12} \cdot v$;
$(\theta_i^{\mathcal{L}_m}(R_1))_i \longleftarrow \varphi_m \circ \cdots \circ \varphi_1((\theta'^{\mathcal{L}}_i(Q_1, Q_3))_i)$;
$w \longleftarrow {}^t(x(Q_2)x(Q_4), x(Q_2)z(Q_4), z(Q_2)x(Q_4), z(Q_2)z(Q_4))$;
$(\theta'^{\mathcal{L}}_i(Q_2, Q_4))_i \longleftarrow N_{12} \cdot w$;
$(\theta_i^{\mathcal{L}_m}(R_2))_i \longleftarrow \varphi_m \circ \cdots \circ \varphi_1((\theta'^{\mathcal{L}}_i(Q_1, Q_3))_i)$;
$\theta^{\mathcal{M}_m}_{i_1,i_2}(R) \longleftarrow \theta^{\mathcal{L}_m}_{i_1}(R_1) \cdot \theta^{\mathcal{L}_m}_{i_2}(R_2)$ for $i_1, i_2 \in (\mathbb{Z}/2\mathbb{Z})^2$;
$(\theta'^{\mathcal{M}_m}_i(R))_i \longleftarrow N_{24} \cdot (\theta_i^{\mathcal{M}_m}(R))_i$;
$(\theta'^{\mathcal{L}_0}_i(S))_i \longleftarrow f_e \circ \cdots \circ f_{m+1}((\theta'^{\mathcal{M}_m}_i(R))_i)$;
$(\theta_i^{\mathcal{L}_0}(S))_i \longleftarrow N_{41} \cdot (\theta'^{\mathcal{L}_0}_i(S))_i$;
Use Algorithm 12 with input $(\theta_i^{\mathcal{L}_0}(S))_i$ and (α_i, β_i) for $i \in \{1,2\}$ to obtain $(x_1(F(Q)) : z_1(F(Q))), \cdots, (x_4(F(Q)) : z_4(F(Q)))$;
return $(x_1(F(Q)) : z_1(F(Q))), \cdots, (x_4(F(Q)) : z_4(F(Q)))$;

5.4. **Performance.** The computation and evaluation algorithms of F defined in Eq. (19) have been implemented in Python/Sagemath for the needs of SQIsignHD. This computation has been tested on various parameters on random supersingular elliptic curves E_1 defined over finite fields $\mathbb{F}_{p^2}$ of characteristic p between 30 and 378 bits. Primes are of the form $p = c \cdot 2^f \ell^{f'} - 1$ with $\ell = 3$ or 7, $f \geq e+2$ and c small. The isogeny $\sigma : E_1 \longrightarrow E_2$ "embedded" in $F \in \mathrm{End}(E_1^2 \times E_2^2)$ in

dimension 4 as defined in Eq. (19) is always a random cyclic isogeny of degree $q|\ell^{f'}$ and integers $a_1, a_2 \in \mathbb{Z}$ such that $q + a_1^2 + a_2^2 = 2^e$ are precomputed. In SQIsignHD verification, q is not smooth and may vary and a_1, a_2 are computed at runtime, however we have chosen $q|\ell^{f'}$ here to be able to verify that point images of F are correct. For every set of parameters, we compared the computation and evaluation of a 2^e-isogeny $F \in \mathrm{End}(E_1^2 \times E_2^2)$ in dimension 4 as defined in Eq. (19) with the computation and evaluation of a cyclic 2^e-isogeny in dimension 1 with domain E_1 (using x-only arithmetic code due to Giacomo Pope[6]). To compute F, both full torsion algorithms (Algorithms 6 and 7) and half torsion algorithms (Algorithms 13 and 14) were tested[7]. Computations were repeated 100 times and averaged.

Results are displayed in Tables 2 and 3. We found that computing a 2^e-isogeny in dimension 4 is $16 - 18$ times more costly than in dimension 1 over a large base field $\mathbb{F}_{p^2}$, with a slight advantage to the half torsion algorithms (due to the quasilinear complexity of an isogeny chain computation). Timings for evaluation are ≈ 20 times faster in dimensions 1 than in dimension 4. This suggests that our algorithmic approach is promising and can be made cryptographically relevant with a low level implementation (e.g. in C or Rust).

TABLE 2. Comparison of timings (in ms) for 2^e-isogeny computations in dimension 4 with full available torsion (Algorithm 6), half available torsion (Algorithm 13) and in dimension 1 with G. Pope's code for various parameters in Python/Sagemath on a 2,7 GHz Intel Core i5 CPU.

				Dimension 4		Dimension 1
e	$\log_2(p)$	p	$\deg(\sigma)$	Full tors.	Half tors.	G. Pope
16	33	$2^{19} \cdot 3^9 - 1$	3^9	139	164	6
32	55	$2^{34} \cdot 3^{13} - 1$	3^{13}	366	384	12
64	121	$11 \cdot 2^{68} \cdot 3^{31} - 1$	3^{31}	741	695	37
64	125	$5 \cdot 2^{66} \cdot 3^{36} - 1$	3^{35}	678	674	36
128	254	$2^{131} \cdot 3^{78} - 1$	3^{75}	1519	1428	83
128	261	$5^2 \cdot 2^{131} \cdot 3^{79} - 1$	3^{79}	1586	1484	87
192	365	$2^{199} \cdot 3^{105} - 1$	3^{105}	2447	2320	137
192	371	$239 \cdot 2^{194} \cdot 3^{107} - 1$	3^{107}	2459	2309	137
17	30	$3 \cdot 2^{20} \cdot 7^3 - 1$	7^3	142	168	6
17	35	$2^{21} \cdot 7^5 - 1$	7^5	131	164	6
33	52	$3^2 \cdot 2^{35} \cdot 7^5 - 1$	7^5	256	261	12
33	71	$2^{37} \cdot 7^{12} - 1$	7^{11}	352	351	18
65	110	$109 \cdot 2^{67} \cdot 7^{13} - 1$	7^{13}	691	685	37
65	137	$5 \cdot 2^{70} \cdot 7^{23} - 1$	7^{23}	723	708	39
129	249	$261 \cdot 2^{131} \cdot 7^{39} - 1$	7^{39}	1559	1449	86
129	257	$15 \cdot 2^{132} \cdot 7^{43} - 1$	7^{43}	1612	1517	91
193	359	$3^2 \cdot 2^{196} \cdot 7^{57} - 1$	7^{57}	2499	2354	137
193	378	$97 \cdot 2^{195} \cdot 7^{63} - 1$	7^{63}	2488	2370	142

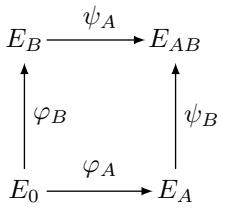
[6] `https://github.com/GiacomoPope/KummerIsogeny`

[7] The 2^{e+2}-torsion is always available but we only used "half" of it to test Algorithms 13 and 14.

TABLE 3. Comparison of timings (in ms) for 2^e-isogeny evaluations in dimension 4 with full available torsion (Algorithm 7), half available torsion (Algorithm 14) and in dimension 1 with G. Pope's code for various parameters in Python/Sagemath on a 2,7 GHz Intel Core i5 CPU.

				Dimension 4		Dimension 1
e	$\log_2(p)$	p	$\deg(\sigma)$	Full tors.	Half tors.	G. Pope
16	33	$2^{19} \cdot 3^9 - 1$	3^9	7.1	6.8	0.6
32	55	$2^{34} \cdot 3^{13} - 1$	3^{13}	14.2	13.9	0.8
64	121	$11 \cdot 2^{68} \cdot 3^{31} - 1$	3^{31}	27.5	26.8	1.8
64	125	$5 \cdot 2^{66} \cdot 3^{36} - 1$	3^{35}	25.9	26.1	1.8
128	254	$2^{131} \cdot 3^{78} - 1$	3^{75}	59.3	59.4	3.5
128	261	$5^2 \cdot 2^{131} \cdot 3^{79} - 1$	3^{79}	64.1	64.2	3.7
192	365	$2^{199} \cdot 3^{105} - 1$	3^{105}	107.7	109.9	5.4
192	371	$239 \cdot 2^{194} \cdot 3^{107} - 1$	3^{107}	106.6	106.9	5.4
17	30	$3 \cdot 2^{20} \cdot 7^3 - 1$	7^3	7.1	6.9	0.6
17	35	$2^{21} \cdot 7^5 - 1$	7^5	7.2	6.9	0.6
33	52	$3^2 \cdot 2^{35} \cdot 7^5 - 1$	7^5	10.0	9.7	0.8
33	71	$2^{37} \cdot 7^{12} - 1$	7^{11}	15.9	15.5	1.2
65	110	$109 \cdot 2^{67} \cdot 7^{13} - 1$	7^{13}	26.4	26.3	1.8
65	137	$5 \cdot 2^{70} \cdot 7^{23} - 1$	7^{23}	29.0	28.8	1.9
129	249	$261 \cdot 2^{131} \cdot 7^{39} - 1$	7^{39}	60.2	59.3	3.6
129	257	$15 \cdot 2^{132} \cdot 7^{43} - 1$	7^{43}	66.3	65.2	3.8
193	359	$3^2 \cdot 2^{196} \cdot 7^{57} - 1$	7^{57}	108.5	107.4	5.4
193	378	$97 \cdot 2^{195} \cdot 7^{63} - 1$	7^{63}	108.1	108.9	5.6

5.5. **Application to SIDH attacks.** In SIDH, Alice and Bob are given a starting supersingular elliptic curve E_0 defined over $\mathbb{F}_{p^2}$ where p is a prime of the form $p = 2^{e_2}3^{e_3} - 1$ along with two basis (P_A, Q_A) and (P_B, Q_B) of $E_0[2^{e_2}]$ and $E_0[3^{e_3}]$ respectively. Alice and Bob sample secret integers $s_A \in \mathbb{Z}/2^{e_2}\mathbb{Z}$ and $s_B \in \mathbb{Z}/3^{e_3}\mathbb{Z}$ respectively. Then Alice computes a 2^{e_2}-isogeny $\varphi_A : E_0 \longrightarrow E_A$ of kernel $\ker(\varphi_A) = \langle P_A + [s_A]Q_A \rangle$ and Bob computes a 3^{e_3}-isogeny $\varphi_B : E_0 \longrightarrow E_B$ of kernel $\ker(\varphi_B) = \langle P_B + [s_B]Q_B \rangle$. Alice sends $(E_A, \varphi_A(P_B), \varphi_A(Q_B))$ to Bob and Bob sends $(E_B, \varphi_B(P_A), \varphi_B(Q_A))$ to Alice. Alice can then compute $\psi_A := [\varphi_B]_*\varphi_A : E_B \longrightarrow E_{BA}$ of kernel $\ker(\psi_A) = \langle \varphi_B(P_A) + [s_A]\varphi_B(Q_A) \rangle$ and Bob computes $\psi_B := [\varphi_A]_*\varphi_B : E_A \longrightarrow E_{AB}$ of kernel $\ker(\psi_B) = \langle \varphi_A(P_B) + [s_B]\varphi_A(Q_B) \rangle$. Then, they share knowledge of a secret elliptic curve $E_{AB} \cong E_{BA}$.



However, given $(E_B, \varphi_B(P_A), \varphi_B(Q_A))$, an attacker is able to recover φ_B (hence s_B) in polynomial time. Knowing s_B, they can then compute ψ_B and find the secret E_{AB}. To compute φ_B, the attacker embeds φ_B into a dimension 4 isogeny:

$$F_B := \begin{pmatrix} \alpha_0 & \widetilde{\Phi}_B \\ -\Phi_B & \widetilde{\alpha}_B \end{pmatrix} \in \mathrm{End}(E_0^2 \times E_B^2),$$

where $\Phi_B := \mathrm{Diag}(\varphi_B, \varphi_B) : E_0^2 \longrightarrow E_B^2$ and for $i = 0, B$,

$$\alpha_i := \begin{pmatrix} a_1 & a_2 \\ -a_2 & a_1 \end{pmatrix} \in \mathrm{End}(E_i^2),$$

with $a_1, a_2 \in \mathbb{Z}$ such that $a_1^2 + a_2^2 + 3^{e_3} = 2^e$ and $\lceil e/2 \rceil + 2 \leq e_2$. Knowing the 2^{e_2}-torsion point images $\varphi_B(P_A)$ and $\varphi_B(Q_A)$, the attacker can compute $F_B = F_2 \circ F_1$ in two parts as in Section 5.3.

The parameters a_1, a_2 and e such that $a_1^2 + a_2^2 + 3^{e_3} = 2^e$ are precomputed before the attack. In practice, we increment e until $2^e - 3^{e_3}$ is easy to factor in the form $\alpha^2 \beta N$, where α is smooth, β is smooth and all its prime factors are congruent to 1 mod 4 and N is a big prime congruent to 1 mod 4. Then $2^e - 3^{e_3}$ can be easily decomposed as a sum of two squares using Cornacchia's algorithm [38]. This procedure terminates and outputs a small value of e (satisfying $\lceil e/2 \rceil + 2 \leq e_2$) only when e_3 is odd. When e_3 is even (as in SIKE p610), we look for a_1, a_2 and e such that $a_1^2 + a_2^2 + 3^{e_3+1} = 2^e$ and embed $\varphi' \circ \varphi_B$ instead of φ_B in dimension 4, where $\varphi' : E_B \longrightarrow E'_B$ is a random 3-isogeny. The parameter search took less than 1 s on a laptop even for the biggest prime (SIKE p751).

We performed our attack 100 times on all SIKE NIST primes (p434, p503, p610 and p751) with starting elliptic curves E_0 sampled at random in the supersingular isogeny graph with an isogeny walk from the elliptic curve of j-invariant 1728. Timings and parameters are displayed in Table 4. This attack runs in less than 15 s on a laptop for SIKE p751. This significantly improves previous attack implementations using 2-dimensional isogenies. The implementation by W. Castryck, T. Decru, G. Pope and R. Oudompheng[8] only worked with a special starting curve of known endomorphism ring and broke SIKE p751 in 1 h. The implementation by L. Maino, L. Panny, G. Pope and B. Wesolowski[9] worked with any starting curve but only for small parameters.

TABLE 4. Timings (in s) and parameters of the complete SIDH key recovery attack with a random starting curve in Python/Sagemath for various NIST SIKE primes on a 2,7 GHz Intel Core i5 CPU.

SIKE prime	e_2	e_3	e	Attack timing (s)
p434	216	137	225	3.82
p503	250	159	290	5.47
p610	305	192	407	8.61
p751	372	239	589	14.02

[8] `https://github.com/GiacomoPope/Castryck-Decru-SageMath`
[9] `https://github.com/Breaking-SIDH/direct-attack`

References

[1] Pierrick Dartois and Luciano Maino and Giacomo Pope and Damien Robert, *An Algorithmic Approach to* $(2,2)$*-isogenies in the Theta Model and Applications to Isogeny-based Cryptography*, 2023. `https://eprint.iacr.org/2023/1747`.

[2] Maria Corte-Real Santos and Craig Costello and Benjamin Smith, *Efficient (3,3)-isogenies on fast Kummer surfaces*, 2024. `https://eprint.iacr.org/2024/144`.

[3] J. S. Milne, *Abelian Varieties*, Springer New York, New York, NY, 1986.

[4] Luca De Feo and David Kohel and Antonin Leroux and Christophe Petit and Benjamin Wesolowski, *SQISign: Compact Post-quantum Signatures from Quaternions and Isogenies* (Shiho Moriai and Huaxiong Wang, ed.), Springer International Publishing, Cham, 2020.

[5] Pierrick Dartois and Antonin Leroux and Damien Robert and Benjamin Wesolowski, *SQIsignHD: New Dimensions in Cryptography* (Marc Joye and Gregor Leander, ed.), Springer Nature Switzerland, Cham, 2024.

[6] Andrea Basso and Luca De Feo and Pierrick Dartois and Antonin Leroux and Luciano Maino and Giacomo Pope and Damien Robert and Benjamin Wesolowski, *SQIsign2D-West: The Fast, the Small, and the Safer*, 2024. `https://eprint.iacr.org/2024/760`.

[7] Kohei Nakagawa and Hiroshi Onuki, *SQIsign2D-East: A New Signature Scheme Using 2-dimensional Isogenies*, 2024. `https://eprint.iacr.org/2024/771`.

[8] Hiroshi Onuki and Kohei Nakagawa, *Ideal-to-isogeny algorithm using 2-dimensional isogenies and its application to SQIsign*, 2024. `https://eprint.iacr.org/2024/778`.

[9] Max Duparc and Tako Boris Fouotsa, *SQIPrime: A dimension 2 variant of SQISignHD with non-smooth challenge isogenies*, 2024. `https://eprint.iacr.org/2024/773`.

[10] David Jao and Luca De Feo, *Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies* (Bo-Yin Yang, ed.), Springer Berlin Heidelberg, Berlin, Heidelberg, 2011.

[11] David Jao and Reza Azarderakhsh and Matthew Campagna and Craig Costello and Luca De Feo and Basil Hess and Amir Jalali and Brian Koziel and Brian LaMacchia and Patrick Longa and Michael Naehrig and Joost Renes and Vladimir Soukharev and David Urbanik and Geovandro Pereira and Koray Karabina and Aaron Hutchinson, *Supersingular Isogeny Key Encapsulation*, 2022.

[12] Jesus-Javier Chi-Dominguez and Amalia Pizarro-Madariaga and Edgardo Riquelme, *Computing Isogenies of Power-Smooth Degrees Between PPAVs*, 2023. `https://eprint.iacr.org/2023/508`.

[13] Ulrich Görtz and Torsten Wedhorn, *Algebraic Geometry I Schemes with examples and exercises*, Vieweg Teubner, Wiesbaden, Germany, 2010. Advanced lectures in mathematics.

[14] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

[15] David Mumford, *On the equations defining abelian varieties 1*, Inventiones mathematicae **1** (1966/12/01), no. 4, 287-354, DOI 10.1007/BF01389737.

[16] Serge Lang, *Algebra*, Springer, 2004.

[17] Damien Robert, *Theta functions and cryptographic applications*, Université Henri-Poincarré, Nancy 1, France, 2010.

[18] Damien Robert, *A note on optimising* 2^n*-isogenies in higher dimension*, 2024. `https://eprint.iacr.org/2024/406`.

[19] Jun-Ichi Igusa, *Theta functions*, Springer-Verlag, New York, 1972. Die Grundlehren der mathematischen Wissenschaften, Band 194.

[20] Romain Cosset, *Applications des fonctions thêta à la cryptographie sur courbes hyperelliptiques*, Université Henri-Poincarré, Nancy 1, France, 2011.

[21] Antonin Leroux, *Verifiable random function from the Deuring correspondence and higher dimensional isogenies*, 2023. `https://eprint.iacr.org/2023/1251`.

[22] Damien Robert, *Breaking SIDH in Polynomial Time* (Carmit Hazay and Martijn Stam, ed.), Springer Nature Switzerland, Cham, 2023.

[23] Wouter and Decru Castryck Thomas, *An Efficient Key Recovery Attack On SIDH*, Springer-Verlag, Berlin, Heidelberg, 2023.

[24] Luciano Maino and Chloe Martindale and Lorenz Panny and Giacomo Pope and Benjamin Wesolowski, *A Direct Key Recovery Attack on SIDH*, Springer-Verlag, 2023.

[25] Aurel Page and Damien Robert, *Introducing Clapoti(s): Evaluating the isogeny class group action in polynomial time*, 2023. https://eprint.iacr.org/2023/1766.
[26] Ernst Kani, *The number of curves of genus two with elliptic differentials*, Journal für die reine und angewandte Mathematik **1997** (1997), no. 485, 93–122, DOI 10.1515/crll.1997.485.93.
[27] Andrea Basso and Luciano Maino and Giacomo Pope, *FESTA: Fast Encryption from Supersingular Torsion Attacks* (Jian Guo and Ron Steinfeld, ed.), Springer Nature Singapore, Singapore, 2023.
[28] Kohei Nakagawa and Hiroshi Onuki, *QFESTA: Efficient Algorithms and Parameters for FESTA using Quaternion Algebras*, 2023. https://eprint.iacr.org/2023/1468.
[29] Mingjie Chen and Antonin Leroux and Lorenz Panny, *SCALLOP-HD: Group Action from 2-Dimensional Isogenies* (Qiang Tang and Vanessa Teague, ed.), Springer Nature Switzerland, Cham, 2024.
[30] Luca De Feo and Tako Boris Fouotsa and Péter Kutas and Antonin Leroux and Simon-Philipp Merz and Lorenz Panny and Benjamin Wesolowski, *SCALLOP: Scaling the CSI-FiSh* (Alexandra Boldyreva and Vladimir Kolesnikov, ed.), Springer Nature Switzerland, Cham, 2023.
[31] Tomoki Moriya, *IS-CUBE: An isogeny-based compact KEM using a boxed SIDH diagram*, 2023. https://eprint.iacr.org/2023/1506.
[32] Damien Robert, *Evaluating isogenies in polylogarithmic time*, 2022. https://eprint.iacr.org/2022/1068.
[33] Benjamin Smith, *Explicit Endomorphisms and Correspondences*, The University of Sydney, 2005.
[34] Takashima Katsuyuki and Yoshida Reo, *An algorithm for computing a sequence of Richelot isogenies*, Bulletin of the Korean Mathematical Society **46** (2009), no. 4, 789-802.
[35] David Lubicz and Damien Robert, *Computing isogenies between abelian varieties*, Compositio Mathematica **148** (2012), no. 5, 1483–1515, DOI 10.1112/S0010437X12000243.
[36] ———, *Computing separable isogenies in quasi-optimal time*, LMS Journal of Computation and Mathematics **18** (2015), no. 1, 198–216, DOI 10.1112/S146115701400045X.
[37] ———, *Fast change of level and applications to isogenies*, Research in Number Theory **9** (2022), no. 7, 7, DOI 10.1007/s40993-022-00407-9.
[38] Giuseppe Cornacchia, *Su di un metodo per la risoluzione in numeri interi dell'equazione* $\sum_{h=0}^{n} C_h x^{n-h} y^h = P$, Giornale di matematiche di Battaglini **46** (1908), 33–90.
[39] David Mumford, *Abelian varieties*, Oxford University Press, London, 1974. Second Edition. Tata Institute of fundamental research studies in mathematics.
[40] Christina Birkenhake and Herbert Lange, *Complex Abelian Varieties*, Springer Berlin Heidelberg, Berlin, Heidelberg, 2004.
[41] Sabrina Kunzweiler and Luciano Maino and Tomoki Moriya and Chrstophe Petit and Giacomo Pope and Damien Robert and Miha Stopar and Yan Bo Ti, *Radical isogenies in the theta model and applications to cryptographic hash functions*, 2024. Unpublished.

Appendix A. Doubling algorithm

Let $\Theta_{\mathcal{L}}$ be a level 2 theta-structure on a polarised abelian variety $(A, \mathcal{L})$. We explain here how to compute $(\theta_i^{\mathcal{L}}(2x))_i$ when $(\theta_i^{\mathcal{L}}(x))_i$ is given using the formulas of Theorem 6. This is described in Algorithm 8, which is derived from [17, Algorithm 4.4.10]. Algorithm 8 requires that:

$$\forall i \in (\mathbb{Z}/2\mathbb{Z})^g, \quad \theta_i^{\mathcal{L}}(0_A) \neq 0 \quad \text{and} \quad \forall \chi \in (\widehat{\mathbb{Z}/2\mathbb{Z}})^g, \quad U_{\chi,0}^{\mathcal{L}^2}(0_A) \neq 0. \tag{20}$$

In practice, this condition is satisfied except when A is a product of abelian varieties of smaller dimension. In that case, we can either:

- Work with a product theta-structure and compute the doubling in every component of A (e.g. with elliptic curve arithmetic on product of elliptic curves).
- Compute random change of coordinates (using Theorem 12) until (20) is satisfied. This option is generally avoided because it is costly.
- Still use the formulas Theorem 6 in a different way than in Algorithm 8, which is also costly.

Algorithm 8: Generic doubling algorithm.

Data: A theta point $(\theta_i^{\mathcal{L}}(x))_i$ of A and the dual theta-null point $(U_{\chi,0}^{\mathcal{L}}(0_A))_\chi$ of A with non-vanishing coordinates.

Result: $(\theta_i^{\mathcal{L}}(2x))_i$.

Precompute $\theta_i^{\mathcal{L}}(0_A)^{-1} \longleftarrow H((U_{\chi,0}^{\mathcal{L}}(0_A))_\chi)_i$ for all $i \in (\mathbb{Z}/2\mathbb{Z})^g$;

Precompute $U_{\chi,0}^{\mathcal{L}^2}(0_A)^{-2} \longleftarrow 1/H \circ S((\theta_i^{\mathcal{L}}(0_A))_i)_\chi$ for all $\chi \in (\widehat{\mathbb{Z}/2\mathbb{Z}})^g$;

$(Z_\chi)_\chi \longleftarrow H \circ S \circ H((\theta_i^{\mathcal{L}}(x))_i)$;

$(Y_\chi)_\chi \longleftarrow (U_{\chi,0}^{\mathcal{L}^2}(0_A)^{-2} \cdot Z_\chi)_\chi$;

$(X_i)_i \longleftarrow H((Y_\chi)_\chi)$;

$(W_i)_i \longleftarrow (\theta_i^{\mathcal{L}}(0_A)^{-1} \cdot X_i)_i$;

return $(W_i)_i$;

Appendix B. Explicit change of basis computations for 4 dimensional isogenies derived from Kani's lemma with full available torsion

Throughout this section, we keep the notations of Section 5. We assume we have full available torsion $(E_1^2 \times E_2^2)[2^{e+2}]$ to compute $F \in \mathrm{End}(E_1^2 \times E_2^2)$ as defined in Eq. (19).

B.1. **Change of basis in dimension 2.** In this paragraph, we explain how to perform the change of basis prior to the computation of the first (gluing) 2 dimensional 2-isogeny φ_1 (see Lemma 23).

For $i \in \{1,2\}$, consider a basis (α_i, β_i) of $E_i[4]$ such that $\beta_i = (-1:1)$ in Montgomery $(x:z)$-coordinates and the associated level 2 Theta structure $\Theta_{\mathcal{L}_i}$ on $(E_i, \mathcal{L}_i)$. We assume that $e_4(U_1, V_1) = e_4(U_2, V_2)$ and we denote by ζ_4 this quantity. Let $\mathcal{L} := \pi_1^*\mathcal{L}_1 \otimes \pi_2^*\mathcal{L}_2$, where the π_i are the projections $E_1 \times E_2 \longrightarrow E_i$ and consider the product Theta structure $\Theta_{\mathcal{L}} := \Theta_{\mathcal{L}_1} \times \Theta_{\mathcal{L}_2}$. Then, $\Theta_{\mathcal{L}}$ is associated to the ζ_4-symplectic basis of $(E_1 \times E_2)[4]$: $\mathscr{B}_0 := ((\alpha_1, 0), (0, \alpha_2), (\beta_1, 0), (0, \beta_2))$ (see Section 2.6).

Lemma 24. *Let (P_1, Q_1) be a basis of $E_1[4]$ such that $e_4(P_1, Q_1) = \zeta_4$ and $(P_2, Q_2) := (\sigma(P_1), [r]\sigma(Q_1))$, where $rq \equiv 1 \mod 4$. Let M_i be the change of basis matrices (in columns convention) from (α_i, β_i) to (P_i, Q_i) for $i \in \{1,2\}$.*

Let μ be a modular inverse of a_1 modulo 4. Consider $\mathscr{B}_1$ given by:

$$((0, -P_2), ([\mu]P_1, [\mu a_2]P_2), ([a_1]P_1 - [a_2]Q_1, P_2), ([a_2]P_1 + [a_1]Q_1, [q]Q_2)).$$

Then $\mathscr{B}_1$ is a ζ_4-symplectic basis of $(E_1 \times E_2)[4]$ which induces a level 2 Theta structure $\Theta'_{\mathcal{L}}$ on $E_1 \times E_2$ such that $K_2(\Theta'_{\mathcal{L}}) = \ker(\varphi_1)$.

Besides, the change of basis matrix (in columns convention) from $\mathscr{B}_0$ to $\mathscr{B}_1$ is $M := M_l \cdot M_r$, where:

$$M_l := \begin{pmatrix} M_{1,1,1} & 0 & M_{1,1,2} & 0 \\ 0 & M_{2,1,1} & 0 & M_{2,1,2} \\ M_{1,2,1} & 0 & M_{1,2,2} & 0 \\ 0 & M_{2,2,1} & 0 & M_{2,2,2} \end{pmatrix} \quad \textit{and} \quad M_r := \begin{pmatrix} 0 & \mu & a_1 & a_2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & -a_2 & a_1 \\ -1 & \mu a_2 & 0 & q \end{pmatrix}$$

Proof. The left factor M_l is the change of basis matrix from $\mathscr{B}_0$ to the ζ_4-symplectic basis $\mathscr{B}'_0 := ((P_1, 0), (0, P_2), (Q_1, 0), (0, Q_2))$. The right factor M_r is the change of basis matrix from $\mathscr{B}'_0$ to $\mathscr{B}_1$. Since $\mathscr{B}_0$ and $\mathscr{B}'_0$ are both ζ_4-symplectic basis by construction, we have $M_l \in \mathrm{Sp}_4(\mathbb{Z}/4\mathbb{Z})$. Besides, we easily check that $M_r \in \mathrm{Sp}_4(\mathbb{Z}/4\mathbb{Z})$ by decomposing M_r into 2×2-blocks:

$$M_r = \begin{pmatrix} A & C \\ B & D \end{pmatrix}$$

and verifying that ${}^tBA \equiv {}^tAB$, ${}^tDC \equiv {}^tCD$ and ${}^tAD - {}^tBC \equiv I_2 \mod 4$, as in Lemma 11. Hence, the change of basis matrix from $\mathscr{B}_0$ to $\mathscr{B}_1$ $M = M_l \cdot M_r$ belongs to $\mathrm{Sp}_4(\mathbb{Z}/4\mathbb{Z})$ and $\mathscr{B}_1$ is a ζ_4-symplectic basis.

Since $2|a_2$, we have:

$$[2]\langle \mathscr{B}_{1,3}, \mathscr{B}_{1,4} \rangle = [2]\langle ([a_1]P_1, \sigma(P_1)), ([a_1]Q_1, \sigma(Q_1)) \rangle = \ker(\varphi_1),$$

so the level 2 Theta-structure $\Theta'_{\mathcal{L}}$ associated to $\mathscr{B}_1$ by Theorem 5.(ii) satisfies $K_2(\Theta'_{\mathcal{L}}) = \ker(\varphi_1)$. □

If we want to compute the $\Theta'_{\mathcal{L}}$-coordinates of a point $(R_1, R_2) \in E_1 \times E_2$ expressed in Montgomery $(x : z)$-coordinates, we first have to translate $(x(R_i) : z(R_i))$ into $(\theta_0^{\mathcal{L}_i}(R_i) : \theta_1^{\mathcal{L}_i}(R_i))$ for $i \in \{1, 2\}$, using the formulas of Section 2.7, then we compute the product $\Theta_{\mathcal{L}}$-coordinates $\theta^{\mathcal{L}}_{i,j}(R_1, R_2) = \theta_i^{\mathcal{L}_1}(R_1) \cdot \theta_j^{\mathcal{L}_2}(R_2)$ for all $i, j \in \mathbb{Z}/2\mathbb{Z}$ (by Lemma 1) and then act on $(\theta^{\mathcal{L}}_{i,j}(R_1, R_2))_{i,j}$ with the change of basis matrix N from $\Theta_{\mathcal{L}}$ to $\Theta'_{\mathcal{L}}$-coordinates obtained by Lemma 24 and Theorem 12. Assuming N has been precomputed, each conversion of $(x : z)$-coordinates into $\Theta'_{\mathcal{L}}$-coordinates costs 2×2 multiplication to translate $(x : z)$ into $\Theta_{\mathcal{L}_i}$-coordinates, 4 multiplications to compute the product $\Theta_{\mathcal{L}}$-coordinates and 16 multiplication to apply the matrix N, for a total of 24 multiplications.

Instead, we can translate directly $(x : z)$-coordinates to $\Theta'_{\mathcal{L}}$-coordinates without intermediate $\Theta_{\mathcal{L}_i}$-coordinates computation. We first compute the product $(x : z)$-coordinates $(x(R_1)x(R_2) : x(R_1)z(R_2) : z(R_1)x(R_2) : z(R_1)z(R_2))$. Then, we act with the *change of ccordinates matrix from* $(x : z)$ *to* $\Theta'_{\mathcal{L}}$ $N'' := N \cdot N'$, where N' translates product $(x : z)$-coordinates into $\Theta_{\mathcal{L}}$-coordinates and is given by:

$$N' := \begin{pmatrix} a_1a_2 & -a_1a_2 & -a_1a_2 & a_1a_2 \\ b_1a_2 & -b_1a_2 & b_1a_2 & -b_1a_2 \\ a_1b_2 & a_1b_2 & -a_1b_2 & -a_1b_2 \\ b_1b_2 & b_1b_2 & b_1b_2 & b_1b_2 \end{pmatrix},$$

with $(a_i : b_i)$ the theta-null point of $(E_i, \mathcal{L}_i, \Theta_{\mathcal{L}_i})$ for $i \in \{1, 2\}$. Assuming N'' has been precomputed, translating $(x : z)$-coordinates to $\Theta'_{\mathcal{L}}$-coordinates costs 20 multiplications, saving 4 multiplications compared to the previous method. The precomputation of the product $N'' = N \cdot N'$ is not too costly compared to the computation of N alone since the product $N \cdot N'$ can be computed with 16 multiplications only instead of 64 (see Algorithm 9).

B.2. **Change of basis in dimension 4 with full available torsion.** In this paragraph, we explain how to perform the change of basis prior to the computation of the first (gluing) 4 dimensional 2-isogeny $f_{m+1} : A_m^2 \longrightarrow B$ (see Lemma 23) when we can access the 2^{e+2}-torsion of E_1. We first determine the product Theta structure $\Theta_{\mathcal{M}_m}$ on $(A_m^2, \mathcal{M}_m)$ and then explain how to compute a new Theta structure such that $K_2(\Theta'_{\mathcal{M}_m}) = \ker(f_{m+1})$.

B.2.1. *Computing the Theta structure induced by the 2-dimensional chain.* After the computation of $\Phi := \varphi_m \circ \cdots \circ \varphi_1 : E_1 \times E_2 \longrightarrow A_m$, we obtain a level 2 Theta structure $\Theta_{\mathcal{L}_m}$ on the polarised abelian surface $(A_m, \mathcal{L}_m)$. This Theta structure $\Theta_{\mathcal{L}_m}$ is induced by the symplectic basis of $A_m[4]$ given by

$$\mathscr{C}_1 := ([2^m]\Phi(S_1), [2^m]\Phi(S_2), \Phi(T_1), \Phi(T_2)),$$

where $\widetilde{\mathscr{B}}_1 := (S_1, S_2, T_1, T_2)$ is a symplectic basis of $(E_1 \times E_2)[2^{m+2}]$ such that:

(i) $[2^m]\widetilde{\mathscr{B}}_1$ is the basis $\mathscr{B}_1$ of Lemma 24;
(ii) For all $i \in [\![1\ ;\ m]\!]$, the 8-torsion points $[2^{m-i-1}]\varphi_{i-1} \circ \cdots \circ \varphi_1(T_j)$ where $j \in \{1, 2\}$ lye above $\ker(\varphi_i)$ and have been used to compute φ_i (on entry of [1, Algorithm 5 or 7] or Algorithm 4).

To satisfy point (ii) above, it is sufficient that $\widetilde{\mathscr{B}}_1$ satisfies the following:

(ii)' $\langle T_1, T_2\rangle$ is a maximal isotropic subgroup of $(E_1 \times E_2)[2^{m+2}]$ such that:

$$\langle [4]T_1, [4]T_2\rangle = \ker(\Phi) = \{([a_1]P, \sigma(P)) \mid P \in E_1[2^m]\}.$$

Algorithm 9: Change of basis in dimension 2.

Data: Integer parameters a_1, a_2, q, the basis (α_i, β_i) of $E_i[4]$, the change of basis matrices M_i from (α_i, β_i) to (P_i, Q_i) (as defined in Lemma 24 for $i \in \{1, 2\}$) and the Weil pairing $\zeta_4 = e_4(P_1, Q_1)$.

Result: A change of coordinates matrix from $(x : z)$ to $\Theta'_{\mathcal{L}}$, where $\Theta'_{\mathcal{L}}$ is the Theta structure induced by $\mathscr{B}_1$ (as defined in Lemma 24) satisfying $K_2(\Theta'_{\mathcal{L}}) = \ker(\varphi_1)$.

$\mu \longleftarrow 1/a_1 \mod 4$;
Using a_1, a_2, μ, compute the matrix M_r of Lemma 24;
Using M_1 and M_2, compute the matrix M_l of Lemma 24;
$M \longleftarrow M_l \cdot M_r$;
Let $\Theta_{\mathcal{L}} = \Theta_{\mathcal{L}_1} \times \Theta_{\mathcal{L}_2}$ be the product theta-structure of $E_1 \times E_2$ induced by (α_1, β_1) and (α_2, β_2);
Using the formulas of Theorem 12 with M and ζ_4 compute the change of basis matrix N from $\Theta_{\mathcal{L}}$ to $\Theta'_{\mathcal{L}}$-coordinates;
$a_i \longleftarrow x(\alpha_i) + z(\alpha_i)$, $b_i \longleftarrow x(\alpha_i) - z(\alpha_i)$ for $i \in \{1, 2\}$;
$c_1, c_2, c_3, c_4 \longleftarrow a_1a_2, b_1a_2, a_1b_2, b_1b_2$;
$N'_{i,j} \longleftarrow N_{i,j} \cdot c_j$ for all $i, j \in [\![1\ ;\ 4]\!]$;
for $i = 1$ **to** 4 **do**
    $N''_{i,1} \longleftarrow N'_{i,1} + N'_{i,2} + N'_{i,3} + N'_{i,4}$;
    $N''_{i,2} \longleftarrow -N'_{i,1} - N'_{i,2} + N'_{i,3} + N'_{i,4}$;
    $N''_{i,3} \longleftarrow -N'_{i,1} + N'_{i,2} - N'_{i,3} + N'_{i,4}$;
    $N''_{i,4} \longleftarrow N'_{i,1} - N'_{i,2} - N'_{i,3} + N'_{i,4}$;
end
return N'';

Lemma 25. *Let (P'_1, Q'_1) be a basis of $E_1[2^{m+2}]$ such that $P_1 = [2^m]P'_1$ and $Q_1 = [2^m]Q'_1$, where (P_1, Q_1) is the basis of $E_1[4]$ of Lemma 24. Let $\zeta := e_{2^{m+2}}(P'_1, Q'_1)$. Consider $\widetilde{\mathscr{B}}_1 := (S_1, S_2, T_1, T_2)$, with:*

$$S_1 := ([2^{m+1}]Q'_1, [a]\sigma(P'_1) + [b]\sigma(Q'_1)), \quad S_2 := ([\mu]P'_1, [c]\sigma(P'_1) + [d]\sigma(Q'_1)),$$
$$T_1 := ([a_1]P'_1 - [a_2]Q'_1, \sigma(P'_1)) \quad \text{and} \quad T_2 := ([a_2]P'_1 + [a_1]Q'_1, \sigma(Q'_1)),$$

$a \equiv 2^{m+1}a_2/q$, $b \equiv -(1 + 2^{m+1}a_1)/q$, $\mu \equiv (1 - 2^{m+1}q)/a_1$, $d \equiv -\mu a_2/q \mod 2^{m+2}$ and $c = 2^{m+1}$. Then $\widetilde{\mathscr{B}}_1$ is a ζ-symplectic basis of $(E_1 \times E_2)[2^{m+2}]$ satisfying (i) and (ii)'.

Proof. Let r be the modular inverse of q modulo 2^{m+2}, $P'_2 := \sigma(P_1)$ and $Q'_2 := [r]\sigma(Q'_1)$. Consider the ζ-symplectic basis of $(E_1 \times E_2)[2^{m+2}]$ given by $\widetilde{\mathscr{B}}_0 := ((P'_1, 0), (0, P'_1), (Q'_1, 0), (0, Q'_2))$. Then, the change of basis matrix from $\widetilde{\mathscr{B}}_0$ to $\widetilde{\mathscr{B}}_1$ is:

$$M := \begin{pmatrix} 0 & \mu & a_1 & a_2 \\ a & c & 1 & 0 \\ 2^{m+1} & 0 & -a_2 & a_1 \\ bq & dq & 0 & q \end{pmatrix}$$

As in the proof of Lemma 24, we easily check that $M \in \mathrm{Sp}_4(\mathbb{Z}/2^{m+2}\mathbb{Z})$, which proves that $\widetilde{\mathscr{B}}_1$ is a ζ-symplectic basis of $(E_1 \times E_2)[2^{m+2}]$.

We also see that the reduction of M modulo 4 is the matrix M_r introduced in the proof of Lemma 24, which is the change of basis matrix from $\mathscr{B}'_0$ to $\mathscr{B}_1$. Besides, $[2^m]\widetilde{\mathscr{B}}_0 = \mathscr{B}'_0$ so we obtain $[2^m]\widetilde{\mathscr{B}}_1 = \mathscr{B}_1$, which proves (i).

Finally, since $2^m | a_2$, we see that:

$$\begin{aligned}\langle [4]T_1, [4]T_2\rangle &= \langle ([4a_1]P'_1, \sigma([4]P'_1)), ([4a_1]Q'_1, \sigma([4]Q'_1))\rangle \\ &= \{([a_1]P, \sigma(P)) \mid P \in E_1[2^m]\} = \ker(\Phi),\end{aligned}$$

which proves (ii)' and completes the proof. □

B.2.2. *Computing the change of Theta structure before the 4-dimensional gluing.* Consider the product $(A_m^2, \mathcal{M}_m)$ with $\mathcal{M}_m := \pi_1^*\mathcal{L}_m \otimes \pi_2^*\mathcal{L}_m$, where the π_i are the projections $A_m^2 \longrightarrow A_m$ on the i-th component and the product Theta structure $\Theta_{\mathcal{M}_m} := \Theta_{\mathcal{L}_m} \times \Theta_{\mathcal{L}_m}$. Then $\Theta_{\mathcal{M}_m}$ is associated to the 4-torsion symplectic basis:

$$\begin{aligned}\mathscr{C}_1 \times \mathscr{C}_1 := (&([2^m]\Phi(S_1), 0), ([2^m]\Phi(S_2), 0), (0, [2^m]\Phi(S_1)), (0, [2^m]\Phi(S_2)), \\ &(\Phi(T_1), 0), (\Phi(T_2), 0), (0, \Phi(T_1)), (0, \Phi(T_2)))\end{aligned}$$

We want to compute a Theta structure $\Theta'_{\mathcal{M}_m}$ on $(A_m^2, \mathcal{M}_m)$ such that $K_2(\Theta'_{\mathcal{M}_m}) = \ker(f_{m+1})$. In order to do that, we compute a change of basis from $\mathscr{C}_1 \times \mathscr{C}_1$ to a symplectic basis $\mathscr{C} := (U_1, \cdots, U_4, V_1, \cdots, V_4)$ such that:

$$V_1 = (\Phi([a_1]P'_1, \sigma(P'_1)), \Phi([a_2]P'_1, 0)), \quad V_2 = (\Phi([a_1]Q'_1, \sigma(Q'_1)), \Phi([a_2]Q'_1, 0)),$$

$$V_3 = (\Phi(-[a_2]P'_1, 0), \Phi([a_1]P'_1, \sigma(P'_1))), \quad V_4 = (\Phi(-[a_2]Q'_1, 0), \Phi([a_1]Q'_1, \sigma(Q'_1))),$$

so that $\langle V_1, \cdots, V_4\rangle = [2^{e-m}]f_m \circ \cdots \circ f_1(K'')$. Any symplectic complement $(U_1, \cdots, U_4)$ of $(V_1, \cdots, V_4)$ is acceptable. When we cannot access the full 2^{e+2}-torsion, we may choose a different basis $\mathscr{C}$ because we have to satisfy more constraints. Here, to compute $\mathscr{C}$ we first compute the matrix of $(V_1, \cdots, V_4)$ in the basis $\mathscr{C}_1 \times \mathscr{C}_1$ and complete it to obtain a symplectic matrix of $\mathrm{Sp}_8(\mathbb{Z}/4\mathbb{Z})$ (which can be done with easy linear algebra over $\mathbb{Z}/4\mathbb{Z}$).

Lemma 26. *The matrix of $(V_1, \cdots, V_4)$ in $\mathscr{C}_1 \times \mathscr{C}_1$ is:*

$$\begin{pmatrix} -a_1a_2/2^m & a_2^2/2^m & a_2^2/2^m & a_1a_2/2^m \\ -a_2^2/2^m & -a_1a_2/2^m & -a_1a_2/2^m & a_2^2/2^m \\ -a_2^2/2^m & -a_1a_2/2^m & -a_1a_2/2^m & a_2^2/2^m \\ a_1a_2/2^m & -a_2^2/2^m & -a_2^2/2^m & -a_1a_2/2^m \\ 1 & 0 & 0 & 0 \\ \mu a_2 & 1 & 0 & -\mu a_2 \\ 0 & 0 & 1 & 0 \\ 0 & \mu a_2 & \mu a_2 & 1 \end{pmatrix},$$

where μ has been defined in Lemma 25.

Proof. Let $W_1 := \Phi([a_1]P'_1, \sigma(P'_1))$, $W_2 := \Phi([a_1]Q'_1, \sigma(Q'_1))$, $W_3 := \Phi([a_2]P'_1, 0)$ and $W_4 := \Phi([a_2]Q'_1, 0)$. To conclude, it suffices to compute the matrix of $(W_1, \cdots, W_4)$ in $\mathscr{C}_1$. Let us write:

$$W_j := \sum_{i=1}^{2}[c_{i,j}2^m]\Phi(S_i) + \sum_{i=1}^{2}[d_{i,j}]\Phi(T_i)$$

for all $j \in [\![1\ ;\ 4]\!]$. Then, we have for all $i \in \{1, 2\}$ and $j \in [\![1\ ;\ 4]\!]$,

$$e_4(W_j, [2^m]\Phi(S_i)) = e_4([2^m]\Phi(S_i), \Phi(T_i))^{-d_{i,j}} = \zeta_4^{-d_{i,j}}$$

$$\text{and} \quad e_4(W_j, \Phi(T_i)) = e_4([2^m]\Phi(S_i), \Phi(T_i))^{c_{i,j}} = \zeta_4^{c_{i,j}},$$

where $\zeta_4 = \zeta^{2^m} = e_{2^{m+2}}(P_1', Q_1')^{2^m}$. Hence, we can obtain the coefficients $c_{i,j}$ and $d_{i,j}$ that we are looking for by computing Weil pairings.

We have:

$$\begin{aligned}
e_4(W_1, [2^m]\Phi(S_1)) &= e_4(\Phi([a_1]P_1', \sigma(P_1')), [2^m]\Phi(S_1)) \\
&= e_4(([a_1]P_1', \sigma(P_1')), [2^m]\widetilde{\Phi} \circ \Phi(S_1)) \quad \text{[3, Lemma 16.2.(a)]} \\
&= e_4(([a_1]P_1', \sigma(P_1')), [2^{2m}]S_1) \\
&= e_4([2^m]([a_1]P_1', \sigma(P_1')), [2^m]S_1) \\
&= e_{2^{m+2}}(([a_1]P_1', \sigma(P_1')), S_1)^{2^m} \quad \text{[3, Lemma 16.1]} \\
&= e_{2^{m+2}}(([a_1]P_1', \sigma(P_1')), ([2^{m+1}]Q_1', [a]\sigma(P_1') + [b]\sigma(Q_1')))^{2^m} \\
&= e_{2^{m+2}}(P_1', Q_1')^{2^m(a_1 2^{m+1} + bq)} = \zeta_4^{a_1 2^{m+1} + bq} = \zeta_4^{bq} = \zeta_4^{-1},
\end{aligned}$$

so that $d_{1,1} = 1$. Similarly, we obtain:

$$\begin{aligned}
e_4(W_1, [2^m]\Phi(S_2)) &= e_{2^{m+2}}(([a_1]P_1', \sigma(P_1')), S_2)^{2^m} \\
&= e_{2^{m+2}}(([a_1]P_1', \sigma(P_1')), ([\mu]P_1', [c]\sigma(P_1') + [d]\sigma(Q_1')))^{2^m} \\
&= e_{2^{m+2}}(P_1', Q_1')^{2^m dq} = \zeta_4^{dq} = \zeta_4^{-\mu a_2},
\end{aligned}$$

$$\begin{aligned}
e_4(W_1, \Phi(T_1)) &= e_4(\Phi([a_1]P_1', \sigma(P_1')), \Phi([a_1]P_1' - [a_2]Q_1', \sigma(P_1'))) \\
&= e_4(\Phi([a_1]P_1', \sigma(P_1')), \Phi(-[a_2]Q_1', 0)) \\
&\quad \times e_4(\Phi([a_1]P_1', \sigma(P_1')), \Phi([a_1]P_1', \sigma(P_1'))) \\
&= e_4(\Phi([a_1]P_1', \sigma(P_1')), \Phi(-[a_2]Q_1', 0)) \\
&= e_4(\Phi([a_1]P_1', \sigma(P_1')), [2^m]\Phi(-[a_2/2^m]Q_1', 0)) \\
&= e_{2^{m+2}}(([a_1]P_1', \sigma(P_1')), (-[a_2/2^m]Q_1', 0))^{2^m} \\
&= e_{2^{m+2}}(P_1', Q_1')^{-a_1 a_2} = \zeta^{-a_1 a_2} = \zeta_4^{-a_1 a_2/2^m},
\end{aligned}$$

so that $d_{2,1} = \mu a_2$ and $c_{1,1} = -a_1 a_2/2^m$. Let $W_1' \in A_m[2^{m+2}]$ and $T_2' \in (E_1 \times E_2)[2^{2m+2}]$ such that $[2^m]W_1' = W_1$ and $[2^m]T_2' = T_2$. Then:

$$\begin{aligned}
e_4(W_1, \Phi(T_2)) &= e_4([2^m]W_1', [2^m]\Phi(T_2')) = e_{2^{m+2}}(W_1', \Phi(T_2'))^{2^m} \\
&= e_{2^{m+2}}([2^m]W_1', \Phi(T_2')) = e_{2^{m+2}}(\Phi([a_1]P_1', \sigma(P_1')), \Phi(T_2')) \\
&= e_{2^{m+2}}(([a_1]P_1', \sigma(P_1')), \widetilde{\Phi} \circ \Phi(T_2')) \\
&= e_{2^{m+2}}(([a_1]P_1', \sigma(P_1')), [2^m]T_2') \\
&= e_{2^{m+2}}(([a_1]P_1', \sigma(P_1')), ([a_2]P_1' + [a_1]Q_1', \sigma(Q_1'))) \\
&= e_{2^{m+2}}(P_1', Q_1')^{a_1^2 + q} = \zeta^{2^e - a_2^2} = \zeta^{-a_2^2} = \zeta_4^{-a_2^2/2^m},
\end{aligned}$$

so that $c_{2,1} = -a_2^2/2^m$. It follows that:

$$W_1 = -\left[\frac{a_1 a_2}{2^m}\right][2^m]\Phi(S_1) - \left[\frac{a_2^2}{2^m}\right][2^m]\Phi(S_2) + \Phi(T_1) + [\mu a_2]\Phi(T_2).$$

Similarly, we obtain the coordinates of W_2, W_3 and W_4 to finally get the matrix of $(W_1, \cdots, W_4)$ in $\mathscr{C}_1$:

$$\begin{pmatrix} -a_1a_2/2^m & a_2^2 & -a_2^2/2^m & -a_1a_2/2^m \\ -a_2^2/2^m & -a_1a_2/2^m & a_1a_2/2^m & -a_2^2/2^m \\ 1 & 0 & 0 & 0 \\ \mu a_2 & 1 & 0 & \mu a_2 \end{pmatrix}.$$

Since $V_1 = (W_1, W_3)$, $V_2 = (W_2, W_4)$, $V_3 = (-W_3, W_1)$ and $V_4 = (-W_4, W_2)$, we easily obtain the matrix of $(V_1, \cdots, V_4)$ in $\mathscr{C}_1 \times \mathscr{C}_1$. □

We summarize the change of basis computation prior to the gluing $f_{m+1} : A_m^2 \longrightarrow B$ in Algorithm 10.

Algorithm 10: Change of basis in dimension 4 (full torsion case).

Data: Integer parameters $a_1, a_2, q, m = v_2(a_2)$ and the Weil pairing $\zeta_4 = e_4(P_1, Q_1) = e_{2^{m+2}}(P_1', Q_1')^{2^m}$.

Result: A change of basis matrix from $\Theta_{\mathcal{M}_m}$ to $\Theta'_{\mathcal{M}_m}$-coordinates, where $\Theta_{\mathcal{M}_m}$ is the level 2 product Theta structure on $(A_m^2, \mathcal{M}_m)$ and $\Theta'_{\mathcal{M}_m}$ satisfies $K_2(\Theta'_{\mathcal{M}_m}) = \ker(f_{m+1})$.

$\mu \longleftarrow (1 - 2^{m+1}q)/a_1 \mod 2^{m+2}$;

Using μ, compute the matrix M of Lemma 26;

Decompose M in 4×4-blocks $M := \begin{pmatrix} C \\ D \end{pmatrix}$;

Find $A, B \in M_4(\mathbb{Z}/4\mathbb{Z})$ such that ${}^tBA = {}^tAB$, ${}^tDC = {}^tCD$ and ${}^tAD - {}^tBC = I_4$;

$M' \longleftarrow \begin{pmatrix} A & C \\ B & D \end{pmatrix}$;

Let $\Theta'_{\mathcal{M}_m}$ be the Theta structure given by the action of M' on $\Theta_{\mathcal{M}_m}$;

Using Theorem 12, compute the change of basis matrix N from $\Theta_{\mathcal{M}_m}$ to $\Theta'_{\mathcal{M}_m}$-coordinates;

return N;

B.3. **Recovering the product Theta structure on the codomain with full available torsion.** When we can access the full 2^{e+2}-torsion and compute $F \in \mathrm{End}(E_1^2 \times E_2^2)$ as a 2-isogeny chain at once, we have to recover the product Theta structure on the codomain $E_1^2 \times E_2^2$ at the end in order to be able to evaluate F in Montgomery coordinates.

Once we have computed the whole 2-isogeny chain F, the level 2 Theta structure $\Theta'_{\mathcal{L}_0}$ naturally induced on the codomain $(E_1^2 \times E_2^2, \mathcal{L}_0)$ is associated to the symplectic 4-torsion basis:

$$\mathscr{D} := ([2^{e-m}]H(U_1'), \cdots, [2^{e-m}]H(U_4'), H(V_1'), \cdots, H(V_4')), \tag{21}$$

where $H := f_e \circ \cdots \circ f_{m+1}$, so that $F := H \circ f_m \circ \cdots \circ f_1$ and $\widetilde{\mathscr{C}_1} := (U_1', \cdots, U_4', V_1', \cdots, V_4')$ is a symplectic basis of $A_m^2[2^{e-m+2}]$ such that:

(i) $[2^{e-m}]\widetilde{\mathscr{C}}$ is the basis $\mathscr{C}$ of $A_m^2[4]$ introduced in Appendix B.2.

(ii) For all $i \in [\![m+1\ ;\ e]\!]$, the 8-torsion points $[2^{e-i-1}]f_{i-1} \circ \cdots \circ f_{m+1}(V'_j)$ where $j \in [\![1\ ;\ 4]\!]$ lye above $\ker(f_i)$ and have been used to compute f_i on entry of Algorithm 4.

As in Appendix B.2, to satisfy point (ii) above, it is sufficient that $\widetilde{\mathscr{C}}$ satisfies the following:

(ii)' $\langle V'_1, \cdots, V'_4\rangle$ is a maximal isotropic subgroup of $A^2_m[2^{e-m+2}]$ such that $\langle [4]V'_1, \cdots, [4]V'_4\rangle = \ker(H)$.

In the following lemma, we give an explicit construction of $\mathscr{D}$ induced by a basis $\widetilde{\mathscr{C}}$ satisfying (i) and (ii)'.

Lemma 27. *Let:*

- (P_1, Q_1) *and* $(P_2, Q_2) := (\sigma(P_1), [r]\sigma(Q_1))$ *be the* ζ_4*-symplectic basis of* $E_1[4]$ *and* $E_2[4]$ *introduced in Lemma 24.*
- $\mathscr{B}'_0 \times \mathscr{B}'_0$ *be the* ζ_4*-symplectic basis of* $(E_1^2 \times E_2^2)[4]$ *given by:*

$$\begin{aligned}\mathscr{B}'_0 \times \mathscr{B}'_0 := ((P_1,0,0,0),(0,P_1,0,0),(0,0,P_2,0),(0,0,0,P_2),\\ (Q_1,0,0,0),(0,Q_1,0,0),(0,0,Q_2,0),(0,0,0,Q_2)).\end{aligned}$$

- $\mathscr{D}'$ *be the basis:*

$$\begin{aligned}\mathscr{D}' := ([2^{e-m}]H(\Phi(S_1),0),[2^{e-m}]H(\Phi(S_2),0),[2^{e-m}]H(0,\Phi(S_1)),[2^{e-m}]H(0,\Phi(S_2)),\\ H(\Phi(T_1),0),H(\Phi(T_2),0),H(0,\Phi(T_1)),H(0,\Phi(T_2))),\end{aligned}$$

  with S_1, S_2, T_1, T_2 *as in Lemma 25.*
- $M_{\mathscr{B}'_0\times\mathscr{B}'_0,\mathscr{D}'}$ *be the change of basis matrix from* $\mathscr{B}'_0 \times \mathscr{B}'_0$ *to* $\mathscr{D}'$.
- $M_{\mathscr{C}_1\times\mathscr{C}_1,\mathscr{C}}$ *be the change of basis matrix from* $\mathscr{C}_1 \times \mathscr{C}_1$ *to* $\mathscr{C}$ *(introduced in Appendix B.2) decomposed into two* 8×4 *blocks* $M_{\mathscr{C}_1\times\mathscr{C}_1,\mathscr{C}} := (L_{\mathscr{C}_1\times\mathscr{C}_1,\mathscr{C}}|R_{\mathscr{C}_1\times\mathscr{C}_1,\mathscr{C}})$.

Then, there exists a symplectic basis of $A_m[2^{e-m+2}]$, $\widetilde{\mathscr{C}} := (U'_1, \cdots, U'_4, V'_1, \cdots, V'_4)$ *satisfying conditions (i) and (ii)' such that the change of basis matrix from* $\mathscr{B}'_0 \times \mathscr{B}'_0$ *to the basis* $\mathscr{D}$ *related to* $\widetilde{\mathscr{C}}$ *by (21) is given by:*

$$M_{\mathscr{B}'_0\times\mathscr{B}'_0,\mathscr{D}} = (M_{\mathscr{B}'_0\times\mathscr{B}'_0,\mathscr{D}'} \cdot L_{\mathscr{C}_1\times\mathscr{C}_1,\mathscr{C}}|R_{\mathscr{B}'_0\times\mathscr{B}'_0,\mathscr{D}}),$$

with $M_{\mathscr{B}'_0\times\mathscr{B}'_0,\mathscr{D}'}$, *the matrix:*

$$\begin{pmatrix}
0 & 1 & 0 & \mu a_2 & (a_1^2+q)/2^m & a_1a_2/2^m & a_1a_2/2^m & a_2^2/2^m\\
0 & -\mu a_2 & 0 & 1 & -a_1a_2/2^m & -a_2^2/2^m & (a_1^2+q)/2^m & a_1a_2/2^m\\
0 & -\mu & 0 & 0 & 0 & -a_2/2^m & -a_2/2^m & 0\\
0 & 0 & 0 & -\mu & a_2/2^m & 0 & 0 & -a2/2^m\\
-1 & -\mu a_2 & 0 & 0 & -a_1a_2/2^m & (a_1^2+q)/2^m & -a_2^2/2^m & a_1a_2/2^m\\
0 & 0 & -1 & -\mu a_2 & a_2^2/2^m & -a_1a_2/2^m & -a_1a_2/2^m & (a_1^2+q)/2^m\\
-a_1 & -\mu a_1a_2 & a_2 & \mu a_2^2 & a_2q/2^m & 0 & 0 & -a_2q/2^m\\
-a_2 & -\mu a_2^2 & -a_1 & -\mu a_1a_2 & 0 & a_2q/2^m & a_2q/2^m & 0
\end{pmatrix}$$

and:

$$R_{\mathscr{B}'_0\times\mathscr{B}'_0,\mathscr{D}} := \begin{pmatrix} 0 & 0 & 0 & 0 \\ \mu a_2 & 0 & 1 & 0 \\ \mu & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -\mu a_2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \mu q \end{pmatrix},$$

where $\mu \equiv 1/a_1 \mod 4$.

Proof. Let (P_1'', Q_1'') be a basis of $E_1[2^{e+2}]$ such that $[2^{e-m}]P_1'' = P_1'$ and $[2^{e-m}]Q_1'' = Q_1'$, where (P_1', Q_1') has been introduced in Lemma 25, so that $[2^e]P_1'' = P_1$ and $[2^e]Q_1'' = Q_1$. Then, we may choose:

$$V_1' = (\Phi([a_1]P_1'' - [\mu]P_1, \sigma(P_1'')), \Phi([a_2]P_1'', 0)),$$

$$V_2' = (\Phi([a_1]Q_1'', \sigma(Q_1'')), \Phi([a_2]Q_1'', 0)),$$

$$V_3' = (\Phi(-[a_2]P_1'', 0), \Phi([a_1]P_1'', \sigma(P_1''))),$$

$$V_4' = (\Phi(-[a_2]Q_1'', 0), \Phi([a_1]Q_1'' - [\mu]Q_1, \sigma(Q_1''))),$$

and the U_i' in a symplectic complement, so that $[2^{e-m}]U_i' = U_i$ for all $i \in [\![1\ ;\ 4]\!]$ and (i) is satisfied. By construction of the V_i', we have $\langle [4]V_1', \cdots, [4]V_4' \rangle = \ker(H)$ and we can also easily check that $e_{2^{e-m+2}}(V_i', V_j') = 1$ for all $i, j \in [\![1\ ;\ 4]\!]$. Hence, (ii)' is also satisfied.

Besides, we have:

$$H(V_1') = F([a_1]P_1'' - [\mu]P_1, [a_2]P_1'', \sigma(P_1''), 0) = (0, [\mu a_2]P_1, [\mu]\sigma(P_1), 0)$$

$$H(V_2') = F([a_1]Q_1'', [a_2]Q_1'', \sigma(Q_1''), 0) = (Q_1, 0, 0, 0)$$

$$H(V_3') = F(-[a_2]P_1'', [a_1]P_1'', 0, \sigma(P_1'')) = (0, P_1, 0, 0)$$

$$H(V_4') = F(-[a_2]Q_1'', [a_1]Q_1'' - [\mu]Q_1, 0, \sigma(P_1'')) = (-[\mu a_2]Q_1, 0, 0, [\mu]Q_1).$$

The expression of $R_{\mathscr{B}'_0\times\mathscr{B}'_0,\mathscr{D}}$ follows.

Let us write $M_{\mathscr{C}_1\times\mathscr{C}_1,\mathscr{C}} := (M_{i,j})_{1\le i,j\le 8}$, $M_{\mathscr{B}'_0\times\mathscr{B}'_0,\mathscr{D}'} := (M'_{i,j})_{1\le i,j\le 8}$ and $\mathscr{B}'_0 \times \mathscr{B}'_0 := (x_1, \cdots, x_8)$. We have chosen $\widetilde{\mathscr{C}}$ such that for all $j \in [\![1\ ;\ 4]\!]$,

$$\begin{aligned}[2^{e-m}]U_j' = U_j = \sum_{i=1}^{2}[M_{i,j}]([2^m]\Phi(S_i), 0) + \sum_{i=1}^{2}[M_{i+2,j}](0, [2^m]\Phi(S_i)) \\ + \sum_{i=1}^{2}[M_{i+4,j}](\Phi(T_i), 0) + \sum_{i=1}^{2}[M_{i+6,j}](0, \Phi(T_i))\end{aligned}$$

Hence,

$$\begin{aligned}[2^{e-m}]H(U'_j) &= \sum_{i=1}^{2}[M_{i,j}]H([2^m]\Phi(S_i),0) + \sum_{i=1}^{2}[M_{i+2,j}]H(0,[2^m]\Phi(S_i)) \\ &\quad + \sum_{i=1}^{2}[M_{i+4,j}]H(\Phi(T_i),0) + \sum_{i=1}^{2}[M_{i+6,j}]H(0,\Phi(T_i)) \\ &= \sum_{i=1}^{8}[M_{i,j}]\mathscr{D}'_i = \sum_{i=1}^{8}[M_{i,j}]\sum_{k=1}^{8}[M'_{k,i}]x_k \\ &= \sum_{k=1}^{8}\left[\sum_{i=1}^{8}M'_{k,i}M_{i,j}\right]x_k = \sum_{k=1}^{8}[(M_{\mathscr{B}'_0\times\mathscr{B}'_0,\mathscr{D}'}\cdot L_{\mathscr{C}_1\times\mathscr{C}_1,\mathscr{C}})_{k,j}]x_k\end{aligned}$$

The expression of $M_{\mathscr{B}'_0\times\mathscr{B}'_0,\mathscr{D}}$ follows.

Finally, to obtain the expression of $M_{\mathscr{B}'_0\times\mathscr{B}'_0,\mathscr{D}'}$ it suffices to evaluate F on several points, given that F is determined by H and Φ and given the expression of S_1, S_2, T_1, T_2 in Lemma 25. □

Algorithm 11: Splitting change of Theta coordinates (from dimension 4 to 1).

Data: Integer parameters $a_1, a_2, q, m = v_2(a_2)$, the left 4×8 block $L_{\mathscr{C}_1\times\mathscr{C}_1,\mathscr{C}}$ of the change of basis matrix from $\mathscr{C}_1\times\mathscr{C}_1$ to $\mathscr{C}$ (as defined in Appendix B.2), the change of basis matrices M_i from (α_i,β_i) to (P_i,Q_i) (as defined in Lemma 24 for $i\in\{1,2\}$) and the Weil pairing $\zeta_4 = e_4(P_1,Q_1)$.

Result: A change of basis matrix from $\Theta'_{\mathcal{L}_0}$ to $\Theta_{\mathcal{L}_0}$-coordinates, where $\Theta'_{\mathcal{L}_0}$ is the Theta structure induced by $\mathscr{D}$ (21) on $(E_1^2\times E_2^2,\mathcal{L}_0)$ and $\Theta_{\mathcal{L}_0}$ is the product Theta structure on $(E_1^2\times E_2^2,\mathcal{L}_0)$ induced by (α_i,β_i) $(i\in\{1,2\})$.

$\mu \longleftarrow 1/a_1 \mod 4$;

Using μ, a_1, a_2, q, m, compute the matrices $M_{\mathscr{B}'_0\times\mathscr{B}'_0,\mathscr{D}'}$ and $R_{\mathscr{B}'_0\times\mathscr{B}'_0,\mathscr{D}}$ of Lemma 27;

$M_{\mathscr{B}'_0\times\mathscr{B}'_0,\mathscr{D}} \longleftarrow (M_{\mathscr{B}'_0\times\mathscr{B}'_0,\mathscr{D}'}\cdot L_{\mathscr{C}_1\times\mathscr{C}_1,\mathscr{C}} | R_{\mathscr{B}'_0\times\mathscr{B}'_0,\mathscr{D}})$;

$M_0 \longleftarrow$

$$\begin{pmatrix} M_{1,1,1} & 0 & 0 & 0 & M_{1,1,2} & 0 & 0 & 0 \\ 0 & M_{1,1,1} & 0 & 0 & 0 & M_{1,1,2} & 0 & 0 \\ 0 & 0 & M_{2,1,1} & 0 & 0 & 0 & M_{2,1,2} & 0 \\ 0 & 0 & 0 & M_{2,1,1} & 0 & 0 & 0 & M_{2,1,2} \\ M_{1,2,1} & 0 & 0 & 0 & M_{1,2,2} & 0 & 0 & 0 \\ 0 & M_{1,2,1} & 0 & 0 & 0 & M_{1,2,2} & 0 & 0 \\ 0 & 0 & M_{2,2,1} & 0 & 0 & 0 & M_{2,2,2} & 0 \\ 0 & 0 & 0 & M_{2,2,1} & 0 & 0 & 0 & M_{2,2,2} \end{pmatrix};$$

$M \longleftarrow (M_0\cdot M_{\mathscr{B}'_0\times\mathscr{B}'_0,\mathscr{D}})^{-1}$;

Apply the formulas of Theorem 12 to M and ζ_4 to compute a change of basis matrix N from $\Theta'_{\mathcal{L}_0}$ to $\Theta_{\mathcal{L}_0}$-coordinates;

return N;

Algorithm 12: Product Theta coordinates to Montgomery coordinates (in dimension 4).

Data: Product $\Theta_{\mathcal{L}_0}$-coordinates $(\theta_i^{\mathcal{L}_0}(Q))_i$ of a point $Q \in E_1^2 \times E_2^2$, where $\Theta_{\mathcal{L}_0}$ is the product Theta structure on $(E_1^2 \times E_2^2, \mathcal{L}_0)$ induced by (α_k, β_k) (as defined in Lemma 24 for $k \in \{1,2\}$), and the Montgomery $(x:z)$-coordinates of α_k for $k \in \{1,2\}$.

Result: Montgomery $(x:z)$-coordinates of Q.

Parse $\alpha_k := (r_k : s_k)$ in Montgomery $(x:z)$-coordinates for $k \in \{1,2\}$;
$a_k, b_k \longleftarrow r_k + s_k, r_k - s_k$ for $k \in \{1,2\}$;
for $j = 1$ **to** 4 **do**
  if $\exists\, i \in (\mathbb{Z}/2\mathbb{Z})^4,\ i_j = 1 \wedge \theta_i^{\mathcal{L}_0}(Q) \neq 0$ **then**
    Find such $i \in (\mathbb{Z}/2\mathbb{Z})^4$;
    Let $i' \in (\mathbb{Z}/2\mathbb{Z})^4$ such that $i'_l = i_l$ if $l \neq j$ and $i'_j = 0$;
    $\theta_0(Q_j) \longleftarrow \theta_{i'}^{\mathcal{L}_0}(Q)/\theta_i^{\mathcal{L}_0}(Q)$, $\theta_1(Q_j) \longleftarrow 1$;
  else
    $\theta_0(Q_j) \longleftarrow 1$, $\theta_1(Q_j) \longleftarrow 0$;
  end
  $x(Q_j), z(Q_j) \longleftarrow a_{\lceil j/2 \rceil}\theta_1(Q_j) + b_{\lceil j/2 \rceil}\theta_0(Q_j), a_{\lceil j/2 \rceil}\theta_1(Q_j) - b_{\lceil j/2 \rceil}\theta_0(Q_j)$;
end
return $(x(Q_1) : z(Q_1)), \cdots, (x(Q_4) : z(Q_4))$;

From Lemma 27, we derive Algorithm 11 to compute the the change of basis matrix from the Theta coordinates associated to the Theta structure $\Theta'_{\mathcal{L}_0}$ induced by $\mathscr{D}$ to the product $\Theta_{\mathcal{L}_0}$-coordinates on $E_1^2 \times E_2^2$.

Then, we can evaluate F in $(x:z)$-Montgomery coordinates. If $P \in E_1^2 \times E_2^2$ and if we have computed the $\Theta'_{\mathcal{L}_0}$-coordinates $(\theta_i'^{\mathcal{L}_0}(F(P))))_i$, then we apply the change of basis matrix of Theta coordinates N outputted by Algorithm 11 to obtain the product $\Theta_{\mathcal{L}_0}$-coordinates $(\theta_i^{\mathcal{L}_0}(F(P))))_i$. Then, Algorithm 12 transforms these coordinates into the $(x:z)$-Montgomery coordinates of $F(P)$.

The underlying idea of Algorithm 12 is the following. Let $Q := F(P)$, Then, we may write $Q := (Q_1, \cdots, Q_4)$ and by Lemma 1, $\theta_i^{\mathcal{L}_0}(x) = \prod_{j=1}^4 \theta_{i_j}(Q_j)$ for all $i := (i_1, \cdots, i_4) \in (\mathbb{Z}/2\mathbb{Z})^4$, where the Theta coordinates $\theta_{i_j}(Q_j)$ are the level 2 Theta coordinates of $E_{\lceil j/2 \rceil}$ (induced by the basis $(\alpha_{\lceil j/2 \rceil}, \beta_{\lceil j/2 \rceil})$ from Lemma 24). Assuming $\theta_1(Q_j) \neq 0$, then we can find $i \in (\mathbb{Z}/2\mathbb{Z})^4$ such that $i_j = 1$ and $\theta_i^{\mathcal{L}_0}(Q_j) \neq 0$ and we have $\theta_0(Q_j)/\theta_1(Q_j) = \theta_{i'}^{\mathcal{L}_0}(Q)/\theta_i^{\mathcal{L}_0}(Q)$, where $i' \in (\mathbb{Z}/2\mathbb{Z})^4$ satisfies $i'_l = i_l$ for all $l \neq j$ and $i'_j = 0$. This way, we can compute $(\theta_0(Q_j) : \theta_1(Q_j))$ for all $j \in [\![1\ ;\ 4]\!]$. If we denote by (a_k, b_k) the Theta-null point of E_k for $k \in \{1,2\}$, we can then write $Q_j := (a_{\lceil j/2 \rceil}\theta_1(Q_j) + b_{\lceil j/2 \rceil}\theta_0(Q_j) : a_{\lceil j/2 \rceil}\theta_1(Q_j) - b_{\lceil j/2 \rceil}\theta_0(Q_j))$ in Montgomery $(x:z)$-coordinates for all $j \in [\![1\ ;\ 4]\!]$.

Appendix C. Computing 4 dimensional isogenies derived from Kani's lemma with half available torsion

Throughout this section, we keep the notations of Section 5. Unlike in Appendix B, we assume that all the 2^{e+2}-torsion is not available. Namely, we can access the $2^{e'+2}$-torsion with $e' \geq e/2$. We proceed as explained in Section 5.3 to compute F in two parts $F_1 : E_1^2 \times E_2^2 \longrightarrow \mathcal{C}$ and $\widetilde{F}_2 : E_1^2 \times E_2^2 \longrightarrow \mathcal{C}$ such that $F = F_2 \circ F_1$, F_1 being a 2^{e_1}-isogeny and F_2 being a 2^{e_2}-isogeny with $e = e_1 + e_2$ and $m \leq e_1, e_2 \leq e'$.

Since $\ker(F_1) = \ker(F)[2^{e_1}]$ and $\ker(\widetilde{F}_2) = \ker(\widetilde{F})[2^{e_2}]$, Lemma 23 applies to F_1 and an analogue of Lemma 23 applies to $\widetilde{F}_2$.

Lemma 28. *Assume that $2|a_2$ and let $m := v_2(a_2)$ be its 2-adic valuation. Then $\widetilde{F}_2 = g_{e_2} \circ \cdots \circ g_1$, with*

$$E_1^2 \times E_2^2 \xrightarrow{g_1} {A'}_1^2 \quad \cdots \quad {A'}_{m-1}^2 \xrightarrow{g_m} {A'}_m^2 \xrightarrow{g_{m+1}} B',$$

a chain of 2-isogenies, where the A'_i are abelian surfaces and B' is an abelian variety of dimension 4. For all $i \in [\![2\ ;\ m]\!]$, $g_i := (\psi_i, \psi_i)$, with $\psi_i : A'_{i-1} \longrightarrow A'_i$ and $g_1 : (R_1, S_1, R_2, S_2) \longmapsto (\psi_1(R_1, R_2), \psi_1(S_1, S_2))$, with $\psi_1 : E_1 \times E_2 \longrightarrow A'_1$. Besides,

$$\ker(\psi_m \circ \cdots \circ \psi_1) = \{([a_1]P, -\sigma(P)) \mid P \in E_1[2^m]\}.$$

Proof. We proceed as in the proof of Lemma 23. We have:

$$\ker(\widetilde{F}) = \{([a_1]P + [a_2]Q, -[a_2]P + [a_1]Q, -\sigma(P), -\sigma(Q)) \mid P, Q \in E_1[2^e]\}.$$

Let $g_1, \cdots, g_{m+1}$ be the $m+1$ first elements of the 2-isogeny chain $\widetilde{F}$. Then, since $a_2 \equiv 0 \mod 2^m$, we have

$$\ker(g_m \circ \cdots \circ g_1) = [2^{e-m}] \ker(\widetilde{F}) = K_1 \oplus K_2,$$

where $K_1 := \{([a_1]P, 0, -\sigma(P), 0) \mid P \in E_1[2^m]\}$ and $K_2 := \{(0, [a_1]P, 0, -\sigma(P)) \mid P \in E_1[2^m]\}$. This proves the chain $g_m \circ \cdots \circ g_1$ has the desired form. □

Hence, we can compute $\widetilde{F}_2$ exactly as we would compute F_1 (or F with the full torsion available). We give a detailed algorithmic overview of the computation of F in Algorithm 13.

C.1. Change of basis in dimension 2 with half available torsion.

By Lemma 28, we can compute $\widetilde{F}_2$ exactly as we would compute F_1 (or F with the full torsion available). We start by computing a chain of m 2-isogenies $\psi_1, \cdots, \psi_m$ in dimension 2. To compute ψ_1, we have to compute a theta-structure $\Theta'_{\mathcal{L}}$ satisfying $K_2(\Theta'_{\mathcal{L}}) = \ker(\psi_1)$. $\Theta'_{\mathcal{L}}$ is induced by the symplectic basis:

$$((0, P_2), ([\mu]P_1, -[\mu a_2]P_2), ([a_1]P_1 + [a_2]Q_1, -P_2), (-[a_2]P_1 + [a_1]Q_1, -[q]Q_2)).$$

where (P_1, Q_1) is a basis of $E_1[4]$ and $(P_2, Q_2) := (\sigma(P_1), [r]\sigma(Q_1))$, with $rq \equiv 1 \mod 4$ and $\mu a_1 \equiv 1 \mod 4$. Hence, the change of coordinates matrix from $(x : z)$ to $\Theta'_{\mathcal{L}}$ can be computed with Algorithm 9 where the matrix M_r in Lemma 24 is replaced by:

$$M_r := \begin{pmatrix} 0 & \mu & a_1 & -a_2 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & a_2 & a_1 \\ 1 & -\mu a_2 & 0 & -q \end{pmatrix}.$$

Algorithm 13: Computation of a 4 dimensional endomorphism derived from Kani's lemma with half available torsion.

Data: a_1, a_2, q such that a_2 is even, q is odd and $a_1^2 + a_2^2 + q = 2^e$, two supersingular elliptic curves E_1 and E_2 defined over $\mathbb{F}_{p^2}$, (P_1'', Q_1'') a basis of $E_1[2^{e'+2}]$ with $e' \geq e/2$, $(\sigma(P_1''), \sigma(Q_1''))$ for some q-isogeny $\sigma : E_1 \longrightarrow E_2$ and two 4-torsion basis (α_i, β_i) of E_i for $i \in \{1, 2\}$.

Result: A chain representation of the isogeny $F \in \mathrm{End}(E_1^2 \times E_2^2)$ given by (19).

$m \longleftarrow v_2(a_2)$, $e_1 \longleftarrow \lceil e/2 \rceil$ and $e_2 \longleftarrow e - e_1$, $r \longleftarrow 1/q \mod 2^{e'+2}$, $\mu \longleftarrow 1/a_1 \mod 2^{e'+2}$;

(Pre)compute an optimal strategy S with m leaves [11, Algorithm 60];

(Pre)compute optimal strategies S_i ($i \in \{1, 2\}$) with $e_i - m$ leaves with constraints at the beginning and m steps before the end (see Appendix E.2);

/* Step 1: Two symplectic basis inducing dual theta-structures on $\mathcal{C}$ */

$\mathscr{B}_0 \longleftarrow ((P_1'', 0, 0, 0), (0, P_1'', 0, 0), (0, 0, \sigma(P_1''), 0), (0, 0, 0, \sigma(P_1'')), (Q_1'', 0, 0, 0), (0, Q_1'', 0, 0), (0, 0, [r]\sigma(Q_1''), 0), (0, 0, 0, [r]\sigma(Q_1''))$;

Compute symplectic basis of $(E_1^2 \times E_2^2)[2^{e'+2}]$, $\mathscr{B}_1$ and $\mathscr{B}_2$ satisfying the conditions of Lemma 29 and the symplectic change of basis matrices M_1 and M_2 from $\mathscr{B}_0$ to $\mathscr{B}_1$ and $\mathscr{B}_2$ using Algorithm 15;

/* Step 2.a: First m isogenies of F_1 in dimension 2 */

$c \longleftarrow e' - m$, $P_1', Q_1', P_2', R_2' \longleftarrow [2^c]P_1'', [2^c]Q_1'', [2^c]\sigma(P_1''), [2^c]\sigma(Q_1'')$;

$P_1, Q_1, P_2, Q_2 \longleftarrow [2^m]P_1', [2^m]Q_1', [2^m]P_2', [r2^m]R_2'$;

$\zeta_4 \longleftarrow e_4(P_1, Q_1)$;

$T_1, T_2 \longleftarrow [2]([a_1]P_1' - [a_2]Q_1', P_2'), [2]([a_2]P_1' + [a_1]Q_1', R_2')$;

For $i \in \{1, 2\}$, compute a basis (α_i, β_i) of $E_i[4]$ such that $\beta_i = (-1 : 1)$ in $(x : z)$-Montgomery coordinates and $e_4(\alpha_i, \beta_i) = \zeta_4$;

Compute the change of basis matrices M_i from (α_i, β_i) to (P_i, Q_i) for $i \in \{1, 2\}$;

Find a Theta structure $\Theta'_{\mathcal{L}}$ on $(E_1 \times E_2, \mathcal{L})$ such that $K_2(\Theta'_{\mathcal{L}}) = [2^{m+1}]\langle T_1, T_2\rangle$ and compute the change of basis matrix N_{12} from $(x : z)$ to $\Theta'_{\mathcal{L}}$-coordinates (using Algorithm 9 with input $a_1, a_2, q, (\alpha_i : \beta_i), M_i, \zeta_4$);

$({\theta'}_j^{\mathcal{L}}(T_i))_j \longleftarrow N_{12} \cdot {}^t(x_1(T_i)x_2(T_i), x_1(T_i)z_2(T_i), z_1(T_i)x_2(T_i), z_1(T_i)z_2(T_i))$ for $i \in \{1, 2\}$;

Use the coordinates $({\theta'}_j^{\mathcal{L}}(T_i))_j$ and strategy S to compute a 2-dimensional 2-isogeny chain $\Phi := \varphi_m \circ \cdots \circ \varphi_1$ of kernel $\ker(\Phi) = [4]\langle T_1, T_2\rangle$ (see [1]);

/* Step 2.b: Gluing isogeny f_{m+1} of F_1 in dimension 4 */

Parse $X_1, \cdots, X_4, Y_1, \cdots, Y_4 \longleftarrow \mathscr{B}_1$ and let $G : (P_1, \cdots, P_4) \longmapsto (\Phi(P_1, P_3), \Phi(P_2, P_4))$;

Compute $Y_i' \longleftarrow [2^{e'-m-1}]G(Y_i)$ for all $i \in [\![1\ ;\ 4]\!]$ and $Y_5' \longleftarrow [2^{e'-m-1}]G(Y_1 + Y_2)$;

Let $\Theta_{\mathcal{L}_m}$ be the level 2 Theta-structure on the codomain $(A_m, \mathcal{L}_m)$ of Φ and $\Theta_{\mathcal{M}_m} := \Theta_{\mathcal{L}_m} \times \Theta_{\mathcal{L}_m}$;

Find a Theta structure $\Theta'_{\mathcal{M}_m}$ on $(A_m^2, \mathcal{M}_m)$ such that $K_2(\Theta'_{\mathcal{M}_m}) = [4]\langle Y'_1, \cdots, Y'_4\rangle$ and compute the change of coordinates matrix N_{24} from $\Theta_{\mathcal{M}_m}$ to $\Theta'_{\mathcal{M}_m}$ (using Lemma 30 and Theorem 12);
$(\theta'^{\mathcal{M}_m}_j(Y'_i))_j \longleftarrow N_{24} \cdot (\theta^{\mathcal{M}_m}_j(Y'_i))_j$ for $i \in [\![1\ ;\ 5]\!]$;
Using the $(\theta'^{\mathcal{M}_m}_j(Y'_i))_j$ for $i \in [\![1\ ;\ 5]\!]$, compute f_{m+1} of kernel $[4]\langle Y'_1, \cdots, Y'_4\rangle$ (Algorithm 4 and Remark 21);
/* Step 2.c: Last $e_1 - m - 1$ isogenies of F_1 in dimension 4 */
$Y''_i \longleftarrow [2^{e'-e_1}]f_{m+1} \circ G(Y_i)$ for all $i \in [\![1\ ;\ 4]\!]$;
Use Algorithm 21 with input $Y''_1, \cdots, Y''_4$ and strategy S_1 to compute a 4-dimensional 2-isogeny chain $f_{e_1} \circ \cdots \circ f_{m+2}$ of kernel $[4]\langle Y''_1, \cdots, Y''_4\rangle$;
/* Step 3.a: First m isogenies of $\widetilde{F}_2$ in dimension 2 */
$\widetilde{T}_1, \widetilde{T}_2 \longleftarrow [2]([a_1]P'_1 + [a_2]Q'_1, -P'_2), [2](-[a_2]P'_1 + [a_1]Q'_1, -R'_2)$;
Find a Theta structure $\Theta''_{\mathcal{L}}$ on $(E_1 \times E_2, \mathcal{L})$ such that $K_2(\Theta''_{\mathcal{L}}) = [2^m]\langle \widetilde{T}_1, \widetilde{T}_2\rangle$ and compute the change of coordinates matrix $\widetilde{N}_{12}$ from $(x : z)$ to $\Theta''_{\mathcal{L}}$ (using Algorithm 9 with the matrix M_r of Appendix C.1);
$(\theta''^{\mathcal{L}}_j(\widetilde{T}_i))_j \longleftarrow \widetilde{N}_{12} \cdot {}^t(x_1(\widetilde{T}_i)x_2(\widetilde{T}_i), x_1(\widetilde{T}_i)z_2(\widetilde{T}_i), z_1(\widetilde{T}_i)x_2(\widetilde{T}_i), z_1(\widetilde{T}_i)z_2(\widetilde{T}_i))$ for $i \in \{1, 2\}$;
Use the coordinates $(\theta''^{\mathcal{L}}_j(\widetilde{T}_i))_j$ and strategy S to compute a 2-dimensional 2-isogeny chain $\Psi := \psi_m \circ \cdots \circ \psi_1$ of kernel $\ker(\Psi) = [4]\langle \widetilde{T}_1, \widetilde{T}_2\rangle$ (see [1]);
/* Step 3.b: Gluing isogeny g_{m+1} of $\widetilde{F}_2$ in dimension 4 */
Parse $U_1, \cdots, U_4, V_1, \cdots, V_4 \longleftarrow \mathscr{B}_1$ and let $H : (P_1, \cdots, P_4) \longmapsto (\Psi(P_1, P_3), \Psi(P_2, P_4))$;
Compute $V'_i \longleftarrow [2^{e'-m-1}]H(V_i)$ for all $i \in [\![1\ ;\ 4]\!]$ and $V'_5 \longleftarrow [2^{e'-m-1}]H(V_1 + V_2)$;
Let $\Theta_{\mathcal{L}'_m}$ be the level 2 Theta-structure on the codomain $(A'_m, \mathcal{L}'_m)$ of Ψ and $\Theta_{\mathcal{M}'_m} := \Theta_{\mathcal{L}'_m} \times \Theta_{\mathcal{L}'_m}$;
Find a Theta structure $\Theta'_{\mathcal{M}'_m}$ on $(A'^2_m, \mathcal{M}'_m)$ such that $K_2(\Theta'_{\mathcal{M}'_m}) = [4]\langle V'_1, \cdots, V'_4\rangle$ and compute the change of basis matrix $\widetilde{N}_{24}$ from $\Theta_{\mathcal{M}'_m}$ to $\Theta'_{\mathcal{M}'_m}$-coordinates (using Lemma 31 and Theorem 12);
$(\theta'^{\mathcal{M}'_m}_j(V'_i))_j \longleftarrow \widetilde{N}_{24} \cdot (\theta^{\mathcal{M}'_m}_j(V'_i))_j$ for $i \in [\![1\ ;\ 5]\!]$;
Using the $(\theta'^{\mathcal{M}'_m}_j(V'_i))_j$ for $i \in [\![1\ ;\ 5]\!]$, compute g_{m+1} of kernel $[4]\langle V'_1, \cdots, V'_4\rangle$ (Algorithm 4 and Remark 21);
/* Step 3.c: Last $e_2 - m - 1$ isogenies of $\widetilde{F}_2$ in dimension 4 */
$V''_i \longleftarrow [2^{e'-e_1}]g_{m+1} \circ H(V_i)$ for all $i \in [\![1\ ;\ 4]\!]$;
Use Algorithm 21 with input $V''_1, \cdots, V''_4$ and strategy S_2 to compute a 4-dimensional 2-isogeny chain $g_{e_2} \circ \cdots \circ g_{m+2}$ of kernel $[4]\langle V''_1, \cdots, V''_4\rangle$;
/* Step 4: Computing $F_2 = \widetilde{\widetilde{F}}_2$ */
Compute $\widetilde{\psi}_1, \cdots, \widetilde{\psi}_m, \widetilde{g}_1, \cdots, \widetilde{g}_{e_2}$ using Lemma 22;
return $\varphi_1, \cdots, \varphi_m, f_1, \cdots, f_{e_1}, \widetilde{\psi}_1, \cdots, \widetilde{\psi}_m, \widetilde{g}_1, \cdots, \widetilde{g}_{e_2}, N_{12}, N_{24}, \widetilde{N}_{24}^{-1}, \widetilde{N}_{12}^{-1}$;

Algorithm 14: Evaluation of a 4 dimensional endomorphism derived from Kani's lemma with half available torsion given its representation.

Data: A chain C outputted by Algorithm 13 representing $F \in \mathrm{End}(E_1^2 \times E_2^2)$ given by (19), and a point $Q \in E_1^2 \times E_2^2$.
Result: The Montgomery $(x:z)$-coordinates of $F(Q)$.

Parse C as $\varphi_1, \cdots, \varphi_m, f_1, \cdots, f_{e_1}, \widetilde{\psi}_1, \cdots, \widetilde{\psi}_m, \widetilde{g}_1, \cdots, \widetilde{g}_{e_2}, N_{12}, N_{24}, \widetilde{N}_{24}^{-1}, \widetilde{N}_{12}^{-1}$;
$v \longleftarrow {}^t(x(Q_1)x(Q_3), x(Q_1)z(Q_3), z(Q_1)x(Q_3), z(Q_1)z(Q_3))$;
$(\theta'^{\mathcal{L}}_i(Q_1, Q_3))_i \longleftarrow N_{12} \cdot v$;
$(\theta_i^{\mathcal{L}_m}(R_1))_i \longleftarrow \varphi_m \circ \cdots \circ \varphi_1((\theta'^{\mathcal{L}}_i(Q_1, Q_3))_i)$;
$w \longleftarrow {}^t(x(Q_2)x(Q_4), x(Q_2)z(Q_4), z(Q_2)x(Q_4), z(Q_2)z(Q_4))$;
$(\theta'^{\mathcal{L}}_i(Q_2, Q_4))_i \longleftarrow N_{12} \cdot w$;
$(\theta_i^{\mathcal{L}_m}(R_2))_i \longleftarrow \varphi_m \circ \cdots \circ \varphi_1((\theta'^{\mathcal{L}}_i(Q_1, Q_3))_i)$;
$\theta^{\mathcal{M}_m}_{i_1,i_2}(R) \longleftarrow \theta^{\mathcal{L}_m}_{i_1}(R_1) \cdot \theta^{\mathcal{L}_m}_{i_2}(R_2)$ for $i_1, i_2 \in (\mathbb{Z}/2\mathbb{Z})^2$;
$(\theta'^{\mathcal{M}_m}_i(R))_i \longleftarrow N_{24} \cdot (\theta^{\mathcal{M}_m}_i(R))_i$;
$(\theta'^{\mathcal{M}'_m}_i(S_1, S_2))_i \longleftarrow \widetilde{g}_{m+1} \circ \cdots \circ \widetilde{g}_{e_2} \circ f_{e_1} \circ \cdots \circ f_{m+1}((\theta'^{\mathcal{M}_m}_i(R))_i)$;
$(\theta^{\mathcal{M}'_m}_i(S_1, S_2))_i \longleftarrow \widetilde{N}_{24}^{-1} \cdot (\theta'^{\mathcal{M}'_m}_i(S))_i$;
Use Algorithm 16 with input $(\theta^{\mathcal{M}'_m}_{i,j}(S_1, S_2))_{i,j \in (\mathbb{Z}/2\mathbb{Z})^2}$ to obtain $(\theta^{\mathcal{L}'_m}_i(S_1))_{i \in (\mathbb{Z}/2\mathbb{Z})^2}$ and $(\theta^{\mathcal{L}'_m}_i(S_2))_{i \in (\mathbb{Z}/2\mathbb{Z})^2}$;
$(\theta''^{\mathcal{L}}_j(T_i))_j \longleftarrow \widetilde{\psi}_1 \circ \cdots \circ \widetilde{\psi}_m((\theta^{\mathcal{L}'_m}_j(S_i))_j)$ for all $i \in \{1, 2\}$;
$(x_1(F(Q))x_3(F(Q)), x_1(F(Q))z_3(F(Q)), z_1(F(Q))x_3(F(Q)), z_1(F(Q))z_3(F(Q))) \longleftarrow \widetilde{N}_{12}^{-1} \cdot (\theta''^{\mathcal{L}}_j(T_1))_j$;
$(x_2(F(Q))x_4(F(Q)), x_2(F(Q))z_4(F(Q)), z_2(F(Q))x_4(F(Q)), z_2(F(Q))z_4(F(Q))) \longleftarrow \widetilde{N}_{12}^{-1} \cdot (\theta''^{\mathcal{L}}_j(T_2))_j$;
Use Algorithm 17 to recover $(x_1(F(Q)) : z_1(F(Q))), \cdots, (x_4(F(Q)) : z_4(F(Q)))$;
return $(x_1(F(Q)) : z_1(F(Q))), \cdots, (x_4(F(Q)) : z_4(F(Q)))$;

C.2. **Change of basis in dimension 4 with half available torsion.**

C.2.1. *Finding two symplectic basis inducing dual theta-structures on $\mathcal{C}$.* Our goal is to find symplectic basis of $(E_1^2 \times E_2^2)[2^{e'+2}]$ inducing via F_1 and $\widetilde{F}_2$ the same level 2 theta-structure on their common codomain $\mathcal{C}$ (up to a Hadamard transform). This is explained in the following lemma:

Lemma 29. [5, Corollary 58] *Consider two ζ-symplectic basis of $(E_1^2 \times E_2^2)[2^{e'+2}]$, $(X_1, \cdots, X_4, Y_1, \cdots, Y_4)$ and $(U_1, \cdots, U_4, V_1, \cdots, V_4)$ such that:*

(i) $\ker(F_1) = [c_1]\langle Y_1, \cdots, Y_4\rangle$ *and* $\ker(\tilde{F}_2) = [c_2]\langle V_1, \cdots, V_4\rangle$*;*
(ii) $[c_2]F(X_l) = -[c_2]V_l$ *and* $[c_1]\widetilde{F}(U_l) = [c_1]Y_l$ *for all* $l \in [\![1\ ;\ 4]\!]$*;*

where $c_i := 2^{e'+2-e_i}$ for $i \in \{1, 2\}$. Then the symplectic basis of $\mathcal{C}[4]$:

$$\mathscr{B}_1 := ([2^{e'}]F_1(X_1), \cdots, [2^{e'}]F_1(X_4), [c_1]F_1(Y_1), \cdots, [c_1]F_1(Y_4))$$

$$\mathscr{B}_2 := ([2^{e'}]\widetilde{F}_2(U_1), \cdots, [2^{e'}]\widetilde{F}_2(U_4), [c_2]\widetilde{F}_2(V_1), \cdots, [c_2]\widetilde{F}_2(V_4))$$

induced by F_1 and $\widetilde{F}_2$ respectively are related by the standard symplectic matrix $\mathscr{B}_2 = J \cdot \mathscr{B}_1$, with:

$$J := \begin{pmatrix} 0 & -I_4 \\ I_4 & 0 \end{pmatrix} \in \mathrm{Sp}_8(\mathbb{Z}/4\mathbb{Z}).$$

In particular, the theta-coordinates induced by F_1 and $\widetilde{F}_2$ on $\mathcal{C}$ are the dual of each other i.e. *related by a Hadamard transform.*

To find symplectic basis $\mathscr{B}_1 := (X_1, \cdots, X_4, Y_1, \cdots, Y_4)$ and $\mathscr{B}_2 := (U_1, \cdots, U_4, V_1, \cdots, V_4)$ of $(E_1^2 \times E_2^2)[2^{e'+2}]$ as in Lemma 29, the idea is to compute a basis of $\ker(F_1)$, find a symplectic complement $(X_1, \cdots, X_4)$, evaluate $F(X_1), \cdots, F(X_4)$, find a symplectic complement $(U_1, \cdots, U_4)$, and finally evaluate $\widetilde{F}(U_1), \cdots, \widetilde{F}(U_4)$. We then set $V_l := -F(X_l)$ and $Y_l := \widetilde{F}(U_l)$ for all $l \in [\![1\ ;\ 4]\!]$. Evaluating F and $\widetilde{F}$ can be easily done with the knowledge of $\sigma(E_1[2^{e'+2}])$, q, a_1 and a_2. All these operations can be done with linear algebra computations over $\mathbb{Z}/2^{e'+2}\mathbb{Z}$. We summarize them in Algorithm 15.

C.2.2. *Change of basis before the $(m+1)$-th isogeny computation (gluing).* Let $m = v_2(a_2)$. When we compute F_1, we start by computing the m first 2-isogenies of the chain in dimension 2 as we do in the full available torsion case. We also use Algorithm 9 introduced in Appendix B.1 to compute the change of theta structure prior to the computation of the first 2-dimensional isogeny $\varphi_1 : E_1 \times E_2 \longrightarrow A_1$. Hence, after the computation of the 2-isogeny chain $\Phi := \varphi_m \circ \cdots \circ \varphi_1 : E_1 \times E_2 \longrightarrow A_m$ (using the notations of Lemma 23 applied to F_1) we obtain the level 2 product theta structure Θ_{mM_m} on $(A_m^2, \mathcal{M}_m)$ induced by the symplectic basis of $A_m^2[4]$:

$$\begin{aligned}\mathscr{C}_1 \times \mathscr{C}_1 := ((&[2^m]\Phi(S_1), 0), ([2^m]\Phi(S_2), 0), (0, [2^m]\Phi(S_1)), (0, [2^m]\Phi(S_2)),\\ &(\Phi(T_1), 0), (\Phi(T_2), 0), (0, \Phi(T_1)), (0, \Phi(T_2)))\end{aligned}$$

introduced in Appendix B.2.2 (with S_1, S_2, T_1, T_2 defined in Lemma 25).

However, this product theta-structure Θ_m is not suitable to compute $f_{m+1} : A_m^2 \longrightarrow B$ and subsequent isogenies of the chain, since $K_2(\Theta_{\mathcal{L}}) \neq \ker(f_{m+1})$. The isogeny f_{m+1} is computed with the theta-structure $\Theta'_{\mathcal{M}_m}$ induced by the following symplectic basis of $A_m^2[4]$:

$$\begin{aligned}\mathscr{C} := ([2^{e'}]f_m \circ \cdots \circ f_1(X_1), \cdots, &[2^{e'}]f_m \circ \cdots \circ f_1(X_4), [2^{e'-m}]f_m \circ \cdots \circ f_1(Y_1),\\ &\cdots, [2^{e'-m}]f_m \circ \cdots \circ f_1(Y_4))\end{aligned}$$

where $\mathscr{B}_1 := (X_1, \cdots, X_4, Y_1, \cdots, Y_4)$ is an output of Algorithm 15. We then have to compute the change of basis between $\Theta_{\mathcal{M}_m}$ and $\Theta'_{\mathcal{M}_m}$. This can be done with the following lemma:

Lemma 30. *Let $\begin{pmatrix} A & C \\ B & D \end{pmatrix} \in \mathrm{Sp}_8(\mathbb{Z}/2^{e'+2}\mathbb{Z})$ be the basis change matrix from $\mathscr{B}_0$ to $\mathscr{B}_1$, where $\mathscr{B}_0$ has been defined on Line 2 of Algorithm 15. Then change of basis*

Algorithm 15: Two basis of $(E_1^2 \times E_2^2)[2^{e'+2}]$ inducing dual theta-structures on $\mathcal{C}$.

Data: a_1, a_2, q such that a_2 is even, q is odd and $a_1^2 + a_2^2 + q = 2^e$, two supersingular elliptic curves E_1 and E_2 defined over $\mathbb{F}_{p^2}$, (P_1'', Q_1'') a basis of $E_1[2^{e'+2}]$, $(\sigma(P_1''), \sigma(Q_1''))$ for some q-isogeny $\sigma : E_1 \longrightarrow E_2$.

Result: Two ζ-symplectic basis of $(E_1^2 \times E_2^2)[2^{e'+2}]$, $\mathscr{B}_1$ and $\mathscr{B}_2$ satisfying the conditions of Lemma 29, with $\zeta := e_{2^{e'+2}}(P_1'', Q_1'')$ and the symplectic change of basis matrices from $\mathscr{B}_0$ defined on Line 2 to $\mathscr{B}_1$ and $\mathscr{B}_2$.

1 $r \longleftarrow 1/q \mod 2^{e'+2}$;

2 $\mathscr{B}_0 \longleftarrow ((P_1'', 0, 0, 0), (0, P_1'', 0, 0), (0, 0, \sigma(P_1''), 0), (0, 0, 0, \sigma(P_1'')), (Q_1'', 0, 0, 0), (0, Q_1'', 0, 0), (0, 0, [r]\sigma(Q_1''), 0), (0, 0, 0, [r]\sigma(Q_1''))$;

3 $C_1 \longleftarrow \begin{pmatrix} a_1 & 0 & -a_2 & 0 \\ a_2 & 0 & a_1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ and $D_1 \longleftarrow \begin{pmatrix} 0 & a_1 & 0 & -a_2 \\ 0 & a_2 & 0 & a_1 \\ 0 & q & 0 & 0 \\ 0 & 0 & 0 & q \end{pmatrix}$;

4 Find $A_1, B_1 \in M_4(\mathbb{Z}/2^{e'+2}\mathbb{Z})$ satisfying ${}^tB_1A_1 \equiv {}^tA_1B_1$, ${}^tD_1C_1 \equiv {}^tC_1D_1$, ${}^tA_1D_1 - {}^tB_1C_1 \equiv I_4 \mod 2^{e'+2}$, so that $\begin{pmatrix} A_1 & C_1 \\ B_1 & D_1 \end{pmatrix} \in \mathrm{Sp}_8(\mathbb{Z}/2^{e'+2}\mathbb{Z})$;

5 $E_1 \longleftarrow \begin{pmatrix} a_1 & a_2 & q & 0 \\ -a_2 & a_1 & 0 & q \\ -1 & 0 & a_1 & -a_2 \\ 0 & -1 & a_2 & a_1 \end{pmatrix}$ and $E_2 \longleftarrow \begin{pmatrix} a_1 & a_2 & 1 & 0 \\ -a_2 & a_1 & 0 & 1 \\ -q & 0 & a_1 & -a_2 \\ 0 & -q & a_2 & a_1 \end{pmatrix}$;

6 $M_F \longleftarrow \mathrm{Diag}(E_1, E_2)$;

7 $\begin{pmatrix} C_2 \\ D_2 \end{pmatrix} \longleftarrow M_F \cdot \begin{pmatrix} A_1 \\ B_1 \end{pmatrix}$;

8 Find $C_2, D_2 \in M_4(\mathbb{Z}/2^{e'+2}\mathbb{Z})$ satisfying ${}^tB_2A_2 \equiv {}^tA_2B_2$, ${}^tD_2C_2 \equiv {}^tC_2D_2$, ${}^tA_2D_2 - {}^tB_2C_2 \equiv I_4 \mod 2^{e'+2}$;

9 $M_2 \longleftarrow \begin{pmatrix} A_1 & C_1 \\ B_1 & D_1 \end{pmatrix} \in \mathrm{Sp}_8(\mathbb{Z}/2^{e'+2}\mathbb{Z})$;

10 $E_3 \longleftarrow \begin{pmatrix} a_1 & -a_2 & -q & 0 \\ a_2 & a_1 & 0 & -q \\ 1 & 0 & a_1 & a_2 \\ 0 & 1 & -a_2 & a_1 \end{pmatrix}$ and $E_4 \longleftarrow \begin{pmatrix} a_1 & -a_2 & -1 & 0 \\ a_2 & a_1 & 0 & -1 \\ q & 0 & a_1 & a_2 \\ 0 & q & -a_2 & a_1 \end{pmatrix}$;

11 $M_{\tilde{F}} \longleftarrow \mathrm{Diag}(E_3, E_4)$;

12 $\begin{pmatrix} C_1' \\ D_1' \end{pmatrix} \longleftarrow M_{\tilde{F}} \cdot \begin{pmatrix} A_2 \\ B_2 \end{pmatrix}$;

13 $M_1' \longleftarrow \begin{pmatrix} A_1 & -C_1' \\ B_1 & -D_1' \end{pmatrix} \in \mathrm{Sp}_8(\mathbb{Z}/2^{e'+2}\mathbb{Z})$;

14 $\mathscr{B}_1 \longleftarrow M_1' \cdot \mathscr{B}_0$ and $\mathscr{B}_2 \longleftarrow M_2 \cdot \mathscr{B}_0$;

15 **return** $\mathscr{B}_1, \mathscr{B}_2, M_1', M_2$;

matrix from $\mathscr{C}_1 \times \mathscr{C}_1$ to $\mathscr{C}$ is:

$$\left(\begin{array}{c|c} -a_1 \cdot B_1 - a_2 \cdot A_1 - B_3 & (-a_1 \cdot D_1 - a_2 \cdot C_1 - D_3)/2^m \\ a_1 \cdot A_1 - a_2 \cdot B_1 + q \cdot A_3 & (a_1 \cdot C_1 - a_2 \cdot D_1 + q \cdot C_3)/2^m \\ -a_1 \cdot B_2 - a_2 \cdot A_2 - B_4 & (-a_1 \cdot D_2 - a_2 \cdot C_2 - D_4)/2^m \\ a_1 \cdot A_2 - a_2 \cdot B_2 + q \cdot A_4 & (a_1 \cdot C_2 - a_2 \cdot D_2 + q \cdot C_4)/2^m \\ \hline 2^m \cdot A_3 & C_3 \\ 2^m(\mu \cdot B_1 + \mu a_2 \cdot A_3) & \mu \cdot D_1 + \mu a_2 \cdot C_3 \\ 2^m \cdot A_4 & C_4 \\ 2^m(\mu \cdot B_2 + \mu a_2 \cdot A_4) & \mu \cdot D_2 + \mu a_2 \cdot C_4 \end{array}\right),$$

where $\mu \equiv 1/a_1 \mod 4$ and the A_i, B_i, C_i, D_i are the i-th lines of A, B, C, D respectively.

Proof. The basis change matrix can be computed via 4-th Weil pairings as in the proof of Lemma 26. □

The same method applies for the computation of $\widetilde{F}_2$. Using notations introduced in Appendix C.1, the product theta-structure we obtain on A'^2_m is induced by the symplectic basis of $A'^2_m[4]$:

$$\begin{aligned}\mathscr{C}_2 \times \mathscr{C}_2 := ((&[2^m]\Psi(S_1), 0), ([2^m]\Psi(S_2), 0), (0, [2^m]\Psi(S_1)), (0, [2^m]\Psi(S_2)), \\ &(\Psi(T_1), 0), (\Psi(T_2), 0), (0, \Psi(T_1)), (0, \Psi(T_2)))\end{aligned}$$

with $\Psi := \psi_m \circ \cdots \circ \psi_1$,

$$S_1 := ([2^{m+1}]Q'_1, [a]\sigma(P'_1) + [b]\sigma(Q'_1)), \quad S_2 := ([\mu]P'_1, [c]\sigma(P'_1) + [d]\sigma(Q'_1)),$$

$$T_1 := ([a_1]P'_1 + [a_2]Q'_1, -\sigma(P'_1)) \quad \text{and} \quad T_2 := (-[a_2]P'_1 + [a_1]Q'_1, -\sigma(Q'_1)),$$

$P'_1 = [2^{e'-m}]P''_1$, $Q'_1 = [2^{e'-m}]Q''_1$ (where (P''_1, Q''_1) is the input basis of Algorithm 15), $a \equiv 2^{m+1}a_2/q$, $b \equiv -(1 + 2^{m+1}a_1)/q$, $\mu \equiv (1 - 2^{m+1}q)/a_1$, $d \equiv -\mu a_2/q \mod 2^{m+2}$ and $c = 2^{m+1}$.

Lemma 31. *Let $\begin{pmatrix} A & C \\ B & D \end{pmatrix} \in \mathrm{Sp}_8(\mathbb{Z}/2^{e'+2}\mathbb{Z})$ be the basis change matrix from $\mathscr{B}_0$ to $\mathscr{B}_2$, where $\mathscr{B}_0$ has been defined on Line 2 of Algorithm 15. Then change of basis matrix from $\mathscr{C}_2 \times \mathscr{C}_2$ to $\widetilde{\mathscr{C}}$ is:*

$$\left(\begin{array}{c|c} -a_1 \cdot B_1 + a_2 \cdot A_1 + B_3 & (-a_1 \cdot D_1 + a_2 \cdot C_1 + D_3)/2^m \\ a_1 \cdot A_1 + a_2 \cdot B_1 - q \cdot A_3 & (a_1 \cdot C_1 + a_2 \cdot D_1 - q \cdot C_3)/2^m \\ -a_1 \cdot B_2 + a_2 \cdot A_2 + B_4 & (-a_1 \cdot D_2 + a_2 \cdot C_2 + D_4)/2^m \\ a_1 \cdot A_2 + a_2 \cdot B_2 - q \cdot A_4 & (a_1 \cdot C_2 + a_2 \cdot D_2 - q \cdot C_4)/2^m \\ \hline -2^m \cdot A_3 & -C_3 \\ 2^m(\mu \cdot B_1 + \mu a_2 \cdot A_3) & \mu \cdot D_1 + \mu a_2 \cdot C_3 \\ -2^m \cdot A_4 & -C_4 \\ 2^m(\mu \cdot B_2 + \mu a_2 \cdot A_4) & \mu \cdot D_2 + \mu a_2 \cdot C_4 \end{array}\right),$$

where $\mu \equiv 1/a_1 \mod 4$ and the A_i, B_i, C_i, D_i are the i-th lines of A, B, C, D respectively.

C.3. **Recovering the product theta structure on an intermediate product of abelian surfaces.** When computing the "second part" $\widetilde{F}_2$ of F, we also have to compute a chain of 2-isogenies ψ_i in dimension 2 of length $m = v_2(a_2)$ and a gluing isogeny $g_{m+1} : {A'}^2_m \longrightarrow B'$ (Lemma 23). To recover $F_2 = \widetilde{\widetilde{F}}_2$, we compute the dual of every isogeny in the chain. In particular, we compute $\widetilde{g}_{m+1} : B' \longrightarrow {A'}^2_m$ and $\widetilde{\varphi}_i$ for all $i \in [\![1\ ;\ m]\!]$. To be able to evaluate the composition $\widetilde{g}_m \circ \widetilde{g}_{m+1} = (\widetilde{\psi}_m \times \widetilde{\psi}_m) \circ \widetilde{g}_{m+1}$, we need to convert the theta-coordinates of images of $\widetilde{g}_{m+1}$ for a non-product theta-structure $\Theta'_{\mathcal{M}'_m}$ on $({A'}^2_m, \mathcal{M}'_m)$ into product theta-coordinates (for $\Theta_{\mathcal{M}'_m} = \Theta_{\mathcal{L}'_m} \times \Theta_{\mathcal{L}'_m}$). To translate $\Theta'_{\mathcal{M}'_m}$-coordinates into $\Theta_{\mathcal{M}'_m}$-coordinates, we can simply act by the inverse of the change of basis matrix from $\Theta_{\mathcal{M}'_m}$ to $\Theta'_{\mathcal{M}'_m}$-coordinates that has been computed to obtain the gluing isogeny g_{m+1} (using Lemma 31 and Theorem 12).

We then need to split the $\Theta_{\mathcal{M}'_m}$-coordinates on $({A'}^2_m, \mathcal{M}'_m)$ into couples of $\Theta_{\mathcal{L}'_m}$-coordinates on $(A'_m, \mathcal{L}'_m)$. Our approach is similar to Appendix B.3. Let $x, y \in A'_m$. Given $(\theta_{i,j}^{\mathcal{M}'_m}(x,y))_{(i,j)\in(\mathbb{Z}/2\mathbb{Z})^4}$, we want to compute $(\theta_i^{\mathcal{L}'_m}(x))_{i\in(\mathbb{Z}/2\mathbb{Z})^2}$ and $(\theta_i^{\mathcal{L}'_m}(y))_{i\in(\mathbb{Z}/2\mathbb{Z})^2}$ up to a projective constant. By Lemma 1, we have for all $i, j \in (\mathbb{Z}/2\mathbb{Z})^2$, $\theta_{i,j}^{\mathcal{M}'_m}(x,y) = \theta_i^{\mathcal{L}'_m}(x) \cdot \theta_j^{\mathcal{L}'_m}(y)$. Hence we can start by finding $i_0, j_0 \in (\mathbb{Z}/2\mathbb{Z})^2$ such that $\theta_{i_0,j_0}^{\mathcal{M}'_m}(x,y) \neq 0$ and then compute $\theta_{i,j_0}^{\mathcal{M}'_m}(x,y)/\theta_{i_0,j_0}^{\mathcal{M}'_m}(x,y) = \theta_i^{\mathcal{L}'_m}(x)/\theta_{i_0}^{\mathcal{L}'_m}(x)$ and $\theta_{i_0,j}^{\mathcal{M}'_m}(x,y)/\theta_{i_0,j_0}^{\mathcal{M}'_m}(x,y) = \theta_j^{\mathcal{L}'_m}(y)/\theta_{j_0}^{\mathcal{L}'_m}(y)$ for all $i, j \in (\mathbb{Z}/2\mathbb{Z})^2$. This is explained in Algorithm 16.

Algorithm 16: Splitting Product Theta coordinates (from dimension 4 to dimension 2).

Data: Product $\Theta_{\mathcal{M}'_m}$-coordinates $(\theta_{i,j}^{\mathcal{M}'_m}(x,y))_{i,j\in(\mathbb{Z}/2\mathbb{Z})^2}$ of $(x,y) \in {A'}^2_m$.

Result: The $\Theta_{\mathcal{L}'_m}$-coordinates $(\theta_i^{\mathcal{L}'_m}(x))_{i\in(\mathbb{Z}/2\mathbb{Z})^2}$ and $(\theta_i^{\mathcal{L}'_m}(x))_{i\in(\mathbb{Z}/2\mathbb{Z})^2}$.

Find $i_0, j_0 \in (\mathbb{Z}/2\mathbb{Z})^2$ such that $\theta_{i_0,j_0}^{\mathcal{M}'_m}(x,y) \neq 0$;

$x_{i_0} \longleftarrow 1$, $y_{j_0} \longleftarrow 1$;

Compute $x_i \longleftarrow \theta_{i,j_0}^{\mathcal{M}'_m}(x,y)/\theta_{i_0,j_0}^{\mathcal{M}'_m}(x,y)$ for all $i \in (\mathbb{Z}/2\mathbb{Z})^2 \setminus \{i_0\}$;

Compute $y_j \longleftarrow \theta_{i_0,j}^{\mathcal{M}'_m}(x,y)/\theta_{i_0,j_0}^{\mathcal{M}'_m}(x,y)$ for all $j \in (\mathbb{Z}/2\mathbb{Z})^2 \setminus \{j_0\}$;

return $(x_i)_{i\in(\mathbb{Z}/2\mathbb{Z})^2}, (y_j)_{j\in(\mathbb{Z}/2\mathbb{Z})^2}$;

C.4. **Recovering the product theta structure in dimension 2.** When we evaluate $F = F_2 \circ F_1$, the last isogeny of the chain to be evaluated is the 2-dimensional splitting isogeny $\widetilde{\psi}_1 : A'_1 \longrightarrow E_1 \times E_2$. The resulting image points are expressed in non-product $\Theta''_{\mathcal{L}}$-coordinates. We have to translate these points into $(x : z)$-Montgomery coordinates. Given $\Theta''_{\mathcal{L}}$-coordinates $({\theta''}_i^{\mathcal{L}}(R_1, R_2))_i$ of a point $(R_1, R_2) \in E_1 \times E_2$, we can apply the inverse of the change of coordinates matrix from $(x : z)$ to $\Theta''_{\mathcal{L}}$ computed in Appendix C.1. We then obtain $(x(R_1)x(R_2) : x(R_1)z(R_2) : z(R_1)x(R_2) : z(R_1)z(R_2))$. If $z(R_1)z(R_2) \neq 0$, we can then compute $(x(R_1)/z(R_1) : 1)$ and $(x(R_2)/z(R_2) : 1)$ as follows: $x(R_1)/z(R_1) = x(R_1)z(R_2)/z(R_1)z(R_2)$ and $x(R_2)/z(R_2) = z(R_1)x(R_2)/z(R_1)z(R_2)$. Otherwise, we have $R_1 = 0$ or $R_2 = 0$ and we can also recover the Montgomery $(x : z)$-coordinates (with the convention $(x(0) : z(0)) = (1 : 0)$). We refer to Algorithm 17

for the complete conversion procedure of $\Theta''_{\mathcal{L}}$-coordinates into Montgomery $(x:z)$-coordinates.

Algorithm 17: Splitting non product theta coordinates (from dimension 2 to dimension 1).

Data: $\Theta''_{\mathcal{L}}$-coordinates $({\theta''}^{\mathcal{L}}_i(R))_{i\in(\mathbb{Z}/2\mathbb{Z})^2}$ of a point $R := (R_1, R_2) \in E_1 \times E_2$ and the inverse of the change of coordinates matrix N^{-1} from $(x:z)$ to $\Theta''_{\mathcal{L}}$.

Result: Montgomery $(x:z)$-coordinates $(x(R_1):z(R_1)), (x(R_2):z(R_2))$.

$(x(R_1)x(R_2) : x(R_1)z(R_2) : z(R_1)x(R_2) : z(R_1)z(R_2)) \longleftarrow N^{-1} \cdot ({\theta''}^{\mathcal{L}}_i(R))_i$;
if $z(R_1)z(R_2) \neq 0$ **then**
  $t \longleftarrow 1/(z(R_1)z(R_2))$;
  $x_1 \longleftarrow x(R_1)z(R_2) \cdot t$;
  $x_2 \longleftarrow z(R_1)x(R_2) \cdot t$;
  return $(x_1:1), (x_2:1)$;
else if $z(R_1)x(R_2) = 0$ *and* $x(R_1)z(R_2) \neq 0$ **then**
  $t \longleftarrow 1/(x(R_1)z(R_2))$;
  $x_2 \longleftarrow x(R_1)x(R_2) \cdot t$;
  return $(1:0), (x_2:1)$;
else if $z(R_1)x(R_2) \neq 0$ *and* $x(R_1)z(R_2) = 0$ **then**
  $t \longleftarrow 1/(z(R_1)x(R_2))$;
  $x_1 \longleftarrow x(R_1)x(R_2) \cdot t$;
  return $(x_1:1), (1:0)$;
else
  return $(1:0), (1:0)$;

Appendix D. Basic arithmetic optimisations

D.1. **Batch inversion.** Let k be a base field in which we want to invert several elements. In general inversions are much more costly than multiplications over k (e.g. when k is a finite field). In Algorithm 18, we present how to invert n elements with only one inversion at the expense of $3(n-1)$ multiplications.

Algorithm 18: Batch inversion.

Data: $a_1, \cdots, a_n \in k^*$.
Result: $1/a_1, \cdots, 1/a_n$.

1 $b_1 \longleftarrow a_0$ **for** $i = 2$ **to** n **do**
2 $\quad b_i \longleftarrow b_{i-1} \cdot a_i$; // $b_i = a_1 \cdots a_i$
3 **end**
4 $c_1 \longleftarrow 1/b_n$;
5 **for** $i = 2$ **to** n **do**
6 $\quad c_i \longleftarrow c_{i-1} \cdot a_{n-i+2}$; // $c_i = 1/(a_1 \cdots a_{n-i+1})$
7 **end**
8 $d_1 \longleftarrow c_n$;
9 **for** $i = 2$ **to** n **do**
10 $\quad d_i \longleftarrow c_{n-i+1} \cdot b_{i-1}$; // $d_i = 1/(a_1 \cdots a_i) \cdot (a_1 \cdots a_{i-1}) = 1/a_i$
11 **end**
12 **return** $d_1, \cdots, d_n$;

If we are willing to work projectively and obtain $\lambda/a_1, \cdots, \lambda/a_n$ with $\lambda \in k^*$ a projective constant when $a_1, \cdots, a_n \in k^*$ are given, we can simply remove the inversion on Line 4 ($c_1 \longleftarrow 1$) and compute $3(n-1)$ multiplications only. Though considered and recommended, this optimization is not implemented in our dimension 4 code.

D.2. **Recursive Hadamard transform.** For all $g \in \mathbb{N}^*$, let H_g be the Hadamard transform over $k^{(\mathbb{Z}/2\mathbb{Z})^g}$:

$$H_g : (x_i)_{i \in (\mathbb{Z}/2\mathbb{Z})^g} \longmapsto \left(\sum_{i \in (\mathbb{Z}/2\mathbb{Z})^g} (-1)^{\langle i|j \rangle} x_i \right)_{j \in (\mathbb{Z}/2\mathbb{Z})^g}.$$

A naive evaluation of H_g would cost 2^{2g} additions/subtractions which can become costly. Instead, we propose a recursive method to compute H_g. We notice that for all $g \geq 2$ and $(x, y) \in (k^{(\mathbb{Z}/2\mathbb{Z})^{g-1}})^2$:

$$H_g(x, y) = \left(H_1(H_{g-1}(x)_{(j_1, \cdots, j_{g-1})}, H_{g-1}(y)_{(j_1, \cdots, j_{g-1})}))_{j_g} \right)_{j \in (\mathbb{Z}/2\mathbb{Z})^g},$$

where:

$$\forall x \in k^{\mathbb{Z}/2\mathbb{Z}}, \quad H_1(x_0, x_1) = (x_0 + x_1, x_0 - x_1).$$

We can then apply Algorithm 19 to evaluate H_g with only $g \cdot 2^g$ additions/subtractions. For $g = 4$, this decreases the complexity from 256 to 64 additions/subtractions.

Algorithm 19: Recursive Hadamard transform.

Data: $(x_i)_{i\in(\mathbb{Z}/2\mathbb{Z})^g} \in k^{(\mathbb{Z}/2\mathbb{Z})^g}$.
Result: $H((x_i)_{i\in(\mathbb{Z}/2\mathbb{Z})^g})$.

```
if g = 1 then
    return (x_0 + x_1, x_0 - x_1);
else
    x, y ⟵ (x_{i,0})_{i∈(Z/2Z)^{g-1}}, (x_{i,1})_{i∈(Z/2Z)^{g-1}};
    z, t ⟵ H_{g-1}(x), H_{g-1}(y) ;                    // Recursive calls
    for j ∈ (Z/2Z)^g do
        u_j ⟵ z_{(j_1,···,j_{g-1})} + (-1)^{j_g} t_{(j_1,···,j_{g-1})};
    end
    return (u_j)_{j∈(Z/2Z)^g};
end
```

Appendix E. Optimal strategies for isogenies derived from Kani's lemma

E.1. **Definition of optimal strategies.** Let us assume we want to compute a 2^e-isogeny $F : \mathcal{A} \longrightarrow \mathcal{B}$ (in dimension g), decomposed as a chain of 2-isogenies:

$$A_1 = \mathcal{A} \xrightarrow{f_1} A_2 \quad \cdots \quad A_e \xrightarrow{f_e} A_{e+1} = \mathcal{B},$$

and that we are given a basis $\mathscr{B}_{K''}$ of a maximal isotropic subgroup $K'' \subseteq \mathcal{A}[2^{e+2}]$ such that $\ker(F) = [4]K''$. For all $i \in [\![1\ ;\ e]\!]$, we need to know $\mathscr{B}_{i-1,e-i} := [2^{e-i}]f_{i-1} \circ \cdots \circ f_1(\mathscr{B}_{K''})$ in order to compute f_i (using Algorithm 4).

Hence, computing F reduces to computing the leaves $\mathscr{B}_{i-1,e-i}$ of the binary computation tree whose:

- vertices are the basis $\mathscr{B}_{i,j} := [2^j]f_i \circ \cdots \circ f_1(\mathscr{B}_{K''})$ for all $i, j \in \mathbb{N}$ such that $i + j \leq e - 1$;
- left edges are doublings $\mathscr{B}_{i,j-1} \xrightarrow{[2]} \mathscr{B}_{i,j}$;
- right edges are 2-isogeny evaluations $\mathscr{B}_{i-1,j} \xrightarrow{f_i} \mathscr{B}_{i,j}$.

Such a tree is displayed in Fig. 1 for $e = 5$[10]. The computation tree can only be evaluated depth first and left first since the leaf $\mathscr{B}_{i-1,e-i}$ has to be computed prior to any evaluation by f_i. However, evaluating all the vertices $\mathscr{B}_{i,j}$ would be a waste of computational resources leading to a quadratic complexity $O(e^2)$. Optimal strategies consist in navigating the computation tree depth first and left first with a minimal number of doublings and evaluations to evaluate the leaves $\mathscr{B}_{i-1,e-i}$.

As in [10], we can represent the computation tree as a *discrete equilateral triangle* T_e formed by points of the unit triangular equilateral lattice delimited by the x axis and the straight lines $y = \sqrt{3}x$ and $y = \sqrt{3}(e - 1 - x)$:

$$T_e := \left\{ \left(r + \frac{s}{2}, \frac{s\sqrt{3}}{2} \right) \middle| \ r, s \in \mathbb{N}, \quad r + s \leq e - 1 \right\}$$

In T_e, *edges* are unit segments connecting two points of T_e. A *left edge* is a segment of positive slope and a *right edge* is a segment of negative slope. Edges are oriented

[10] This tree is inspired from [5, Figure 2].

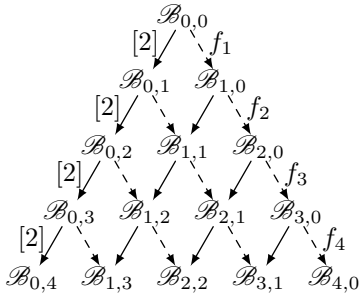


FIGURE 1. Computational structure of the 2^e isogeny F with $e = 5$.

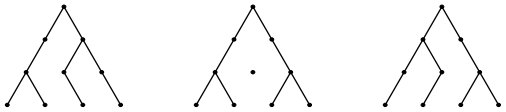


FIGURE 2. Three strategies of depth 3 sharing the same tree topology. The middle one is canonical.

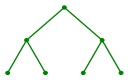


FIGURE 3. Tree topology of the strategies on the left.

in the direction of decreasing y coordinates. This defines an oriented graph structure on T_e. Vertices on $x, y \in T_e$ are ordered $x \to y$ if there exists a path from x to y. On a subgraph of T_e, the *root* is the initial points and *leaves* are final points.

Definition 32. A *strategy* S of T_e is a subgraph of T_e having a unique root. In the following, we only consider strategies that are:

(1) *full*, meaning that S contains all leaves of T_e.
(2) *well-formed*, meaning that there is only one path going through interior point of S and no leaf in S distinct from the leaves of T_e.

Such a (full and well formed) strategy of T_e is also called a *strategy of depth* $e-1$. We denote $|S| = e$ its number of leaves.

To compare strategies, we fix a measure $(\alpha, \beta) \in \mathbb{R}_+^2$ on them, where α is the cost of a left edge (accounting for doubling cost) and β is the cost of a right edge (accounting for evaluation cost). Given such a measure, an *optimal strategy* of depth $e-1$ is a strategy of T_e with minimal cost.

We define the *tree topology* of a strategy S of depth $e-1$ as the binary tree with e leaves obtained by forgetting internal vertices of out degree less than two and keeping the same connectivity structure. Conversely, to any binary tree T with e leaves we associate a *canonical strategy* S_T of depth $e-1$ recursively as follows. If $e = 1$, we take $S_T := T_1$. If $e \geq 2$, we consider the left and right branches T' and T'' of T respectively and consider the canonical strategies $S' := S_{T'}$ and $S_{T''}$ associated to them. Let S'' be the translate of $S_{T''}$ by $|S'|$ to the right. Let r' and r'' be the roots of S' and S'' in T_e respectively and r be the root of T_e. Then the shortest paths rr' and rr'' from r to r' and r'' respectively are respectively made of left edges only and right edges only. We can then consider the strategy $S_T := rr' \cup rr'' \cup S' \cup S''$.

The following result has been proved in [10]:

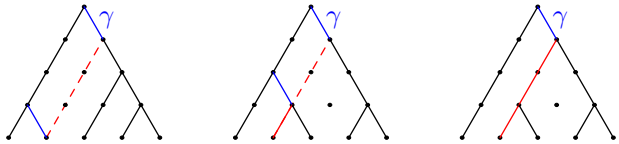


FIGURE 4. Three strategies of depth 4 with the new measure μ'. Only the left one respects the constraint at the beginning, unlike the others.

Lemma 33. [10, Lemma 4.3] *The canonical strategy is minimal, with respect to any measure, among all the strategies sharing the same tree topology.*

It follows that we can restrict to canonical strategies to find optimal strategies in the following. If S is a canonical strategy, we can consider its left and right branches S' and S'' as follows. If S has i leaves to the left of its root, we define $S' := S \cap T_i$ and $S'' := S \cap ((i,0) + T_{|S|-i})$.

Lemma 34. [10, Lemma 4.5] *Let S be an optimal (canonical) strategy and let S' and S'' be its left and right branches respectively. Then, S' and S'' translated by $-|S'|$ are optimal strategies of $T_{|S'|}$ and $T_{|S''|}$ respectively.*

Proof. The proof is very natural. By [10, Lemma 4.3], we know that S is a canonical strategy, so S' and S'' are well defined. If S' were not optimal, then by substituting an optimal strategy for S' inside S, we obtain a strategy with measure lower than $\mu(S)$. Contradiction. The same argument holds for S''. □

As pointed out in [10], this suggests a dynamic programming approach to compute optimal strategies. For $e = 1$, the only optimal strategy is trivially $S = T_1$. Now, if we assume that we have computed optimal strategies $S_1, \cdots, S_{e-1}$ of $T_1, \cdots, T_{e-1}$ of respective measures $\mu(S_1), \cdots, \mu(S_{e-1})$, then the optimal strategy S_e will have left branch S_i and right branch S_{e-i} where:

$$i := \underset{1 \leq j \leq e-1}{\operatorname{argmin}} (\mu(S_j) + \mu(S_{e-j}) + (e-j)\alpha + j\beta).$$

E.2. **Constrained optimal strategies for isogenies derived from Kani's lemma.**

E.2.1. *Constraint at the beginning.* Suppose we want to compute a 2^e-isogeny $F \in \mathrm{End}(E_1^2 \times E_2^2)$ derived from Kani's lemma as in (19) but we cannot access to 2^{e+2}-torsion points. Then, we divide the computation of $F := F_2 \circ F_1$ in two by computing F_1 and $\widetilde{F_2}$ as explained in Section 5.3. Assume we want to compute the 2^{e_1}-isogeny F_1. Since Lemma 23 applies to F_1, we look for an optimal strategy of depth $e_1 - m$ (with $m = v_2(a_2)$) for a measure different from the previous one and satisfying a constraint at the beginning.

The new measure μ' is parametrized by $(\alpha, \beta, \gamma) \in \mathbb{R}_+^3$ where α is the cost of a left edge (accounting for doubling cost), β is the cost of a right edge not starting from the root (accounting for a generic evaluation cost) and γ is the cost of a right edge starting from the root (accounting for the evaluation by $f_{m+1} \circ \cdots \circ f_1$ with the notations of Lemma 23). In addition, we want a strategy with no left edge on the line $y = \sqrt{3}(x-1)$ in order to avoid doublings on the codomain B of f_{m+1}. Such an optimal strategy (for the new measure μ') is called an optimal strategy *with constraint at the beginning.*

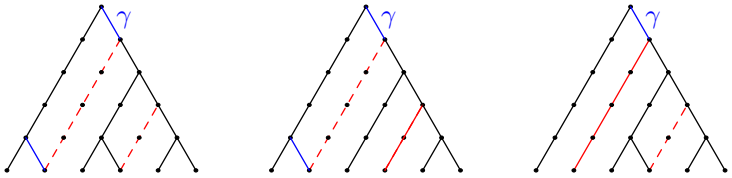


FIGURE 5. Three strategies of depth 5. Only the left one respects the constraints at the beginning and 2 steps before the end. The middle one respects the constraint at the beginning and the right one respects the constraint 2 steps before the end.

[10, Lemma 4.3] generalizes to strategies with constraint at the beginning for the measure μ', so we can restrict to canonical strategies. Indeed, the two key ingredients used in the proof of [10, Lemma 4.3] still hold. First, if there is a path from x to y in T_e (we denote $x \to y$), then all paths going from x to y have the same measure $\mu'(xy)$. Second, if $x \to y$, $y \to y'$ and $y \to y''$, then $\mu'(xy) + \mu'(yy') + \mu'(yy'') \leq \mu'(xy') + \mu'(xy'')$. Hence, we can also generalize [10, Lemma 4.5].

Lemma 35. *Let S be a (canonical) optimal strategy with constraint at the beginning such that $|S| \geq 2$ and let S' and S'' be its left and right branches respectively. Then, $|S'| \geq 2$, S' is an optimal strategy of $T_{|S'|}$ for μ' with constraint at the beginning and S'' translated by $-|S'|$ is an optimal strategy of $T_{|S''|}$ for μ (without constraint at the beginning).*

Hence, a dynamic programming approach is still valid here. Assuming we have computed optimal strategies of $T_1, \cdots, T_{n-1}$ with constraint at the beginning $S'_1, \cdots, S'_{n-1}$ and without constraint at the beginning $S_1, \cdots, S_{n-1}$ respectively, we can compute an optimal strategy with constraint at the beginning S'_n of T_n with left branch S'_i and right branch S_{n-i}, where $i \geq 2$ is given by:

$$i := \underset{2 \leq j \leq n-1}{\operatorname{argmin}} (\mu'(S'_j) + \mu(S_{n-j}) + (n-j)\alpha + (j-1)\beta + \gamma),$$

μ is the measure introduced in Appendix E.1 parametrized by (α, β) and μ' is the new measure parametrized by (α, β, γ).

E.2.2. *Constraints at the beginning and the end.* Now, suppose we want to compute a 2^e-isogeny $F \in \mathrm{End}(E_1^2 \times E_2^2)$ derived from Kani's lemma as in (19) with access to 2^{e+2}-torsion points this time. As explained in Section 5.2, we compute an optimal strategy of depth $|S| = e - m$ for the new measure μ' we just introduced satisfying the following constraints:

- There is no left edge on the line $y = \sqrt{3}(x-1)$ (in order to avoid doublings on the codomain of f_{m+1});
- There is no left edge on the line $y = \sqrt{3}(x - (|S| - 1 - m))$ (in order to avoid doublings on the domain of f_{e-m}).

Such a strategy is called an optimal strategy *with constraints at the beginning and m steps before the end*. An optimal strategy of depth $n > m+1$ for the measure μ introduced in Appendix E.1 satisfying only the last constraint (and not necessarily the first one) is called an optimal strategy *with constraint m steps before the end* (see Fig. 5).

We can generalize again [10, Lemma 4.3] to this case and obtain that optimal strategies with constraints at the beginning and m steps before the end are canonical. Hence, we obtain the following generalization of [10, Lemma 4.5].

Lemma 36. *Let S be an optimal strategy with constraint at the beginning and m steps before the end (with $|S| \geq m+1$). Let S' and S'' be respectively the left and right branches of S. Then $|S'| \geq 2$ and one of these cases hold:*

(i) $|S'| \leq |S| - m - 2$, S' is an optimal strategy for μ' with constraint at the beginning and S'' translated by $-|S'|$ is an optimal strategy for μ with constraint m steps before the end.

(ii) $|S'| = |S| - m$, S' is an optimal strategy for μ' with constraint at the beginning and S'' translated by $-|S'|$ is an optimal strategy for μ (without constraint).

(iii) $|S'| > |S| - m$, S' is an optimal strategy for μ' with constraint at the beginning and $|S'| - |S| + m$ steps before the end and S'' translated by $-|S'|$ is an optimal strategy for μ (without constraint).

By the above lemma, the dynamic programming approach used previously still holds but it is a bit more complex to implement. If we want to compute an optimal strategy of depth $n - 1 \geq m + 1$ with constraints at the beginning and m steps before the end, we need to have previously computed:

- All optimal strategies for μ' of more than $n - m$ leaves with constraint at the beginning;
- All optimal strategies for μ of less than $n - 1$ and more than $m + 2$ leaves with constraint m steps before the end;
- All optimal strategies S' for μ' of $n - m + 1 \leq |S'| \leq n - 1$ leaves with constraint at the beginning and $|S'| - n + m$ steps before the end;
- All optimal strategies for μ of at most m leaves (without constraint).

We can then test all possibilities for left and right branches to minimize the cost.

E.3. **Using optimal strategies in isogeny computations.** As suggested in [11, § 1.3.8], we can represent any strategy S in a unique way as a sequence of integers $(s_1, \cdots, s_{t-1})$ by considering the tree topology T_S of S (as defined in Appendix E.1). To establish this sequence $(s_1, \cdots, s_{t-1})$, we write down for every internal node of the tree T_S the number of leaves to its right and walk on it depth-first left-first.

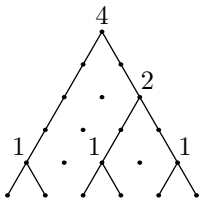


FIGURE 6. Strategy of depth 5 represented by $(4, 1, 2, 1, 1)$.

Given a strategy and a basis of the kernel, it is natural to compute the isogeny chain recursively, as proposed in [11, § 1.3.8]. An iterative version of the same algorithm derived from [12, Algorithm 2] and [1] has been implemented in this work. We present it in Algorithm 20 for the generic case (in any dimension, not taking gluing constraints into account).

Algorithm 21 applies specifically to dimension 4 isogenies derived from Kani's lemma when the first isogenies of the chain involving gluings $f_1, \cdots, f_{m+1}$ are already computed. The changes between Algorithms 20 and 21 are modest and are due to the fact that $f_{m+1} \circ \cdots \circ f_1$ is given on entry and that we want to avoid an unnecessary doubling corresponding to the extreme left edge of the strategy (going to the leaf at the origin, which is not used). Note that Algorithm 21 not only applies to full isogeny computation $F = f_e \circ \cdots \circ f_1$ but also to partial chain computation when we cannot access the 2^{e+2}-torsion.

Algorithm 20: Computing an isogeny chain with a strategy.

Data: A level 2 theta-structure $(\mathcal{A}, \mathcal{L}, \Theta_{\mathcal{L}})$, a basis $\mathscr{B}_{K''} := (T''_1, \cdots, T''_g)$ of a maximal isotropic subgroup $K'' \subseteq \mathcal{A}[2^{e+2}]$ such that $[2^{e+1}]K'' = K_2(\Theta_{\mathcal{L}})$ and a strategy $S = (s_1, \cdots, s_{t-1})$ of depth $e-1$.

Result: A 2^e-isogeny $F : \mathcal{A} \longrightarrow \mathcal{B}$ of kernel $[4]K''$ expressed as a chain of 2-isogenies $f_i : A_i \longrightarrow A_{i+1}$ $(1 \leq i \leq e)$.

```
k ⟵ 1;
L_levels ⟵ [0];
L_basis ⟵ [B_{K''}];
for i = 1 to e do
    B ⟵ last element of L_basis;
    while Σ_{x ∈ L_levels} x ≠ e − k do
        Append s_k to L_levels;
        B ⟵ [2^{s_k}]B;
        Append B to L_basis;
        k ⟵ k + 1;
    end
    Use Algorithm 4 with input B to compute the isogeny f_i of kernel
     [4]⟨B⟩;
    Remove the last elements of L_levels and L_basis;
    L_basis ⟵ [f_i(C) | C ∈ L_basis] (Algorithm 1);
end
return f_1, ··· , f_e;
```

Univ. Bordeaux, CNRS, INRIA, Bordeaux INP, IMB, UMR 5251, F-33400, Talence, France and INRIA, IMB, UMR 5251, F-33400, Talence, France

Email address: pierrick dot dartois at u-bordeaux dot fr

Algorithm 21: Computing an isogeny chain derived from Kani's lemma in dimension 4 with a strategy.

Data: A basis $\mathscr{B}_{K''} := (T_1'', \cdots, T_4'')$ of a maximal isotropic subgroup $K'' \subseteq E_1^2 \times E_2^2[2^{e+2}]$ such that $[2^{e+1}]K'' = K_2(\Theta_{\mathcal{C}})$ and $[4]K'' = \ker(F)$ where $F \in \mathrm{End}(E_1^2 \times E_2^2)$ is given by (19), the 2^{m+1}-isogeny chain $f_{m+1} \circ \cdots \circ f_1$ of Lemma 23 and a strategy $S = (s_1, \cdots, s_{t-1})$ of depth $e - m - 1$ with constraint at the beginning and m steps before the end.

Result: A chain of 2-isogenies $f_1, \cdots, f_e$ such that $F = f_e \circ \cdots \circ f_1$.

```
k ⟵ 1;
L_levels ⟵ [0];
L_basis ⟵ [B_{K''}];
for i = m + 1 to e do
    B ⟵ last element of L_basis;
    while Σ_{x∈L_levels} x ≠ e − k do
        Append s_k to L_levels;
        if i > m + 1 or Σ_{x∈L_levels} x ≠ e − k then
            /* We avoid a useless doubling when i = m + 1 */
            B ⟵ [2^{s_k}]B;
            Append B to L_basis;
        end
        k ⟵ k + 1;
    end
    Remove the last element of L_levels;
    if i > m + 1 then
        Use Algorithm 4 with input B to compute the isogeny f_i of kernel
         [4]⟨B⟩;
        Remove the last element of L_basis;
        L_basis ⟵ [f_i(C) | C ∈ L_basis];
    else
        L_basis ⟵ [f_{m+1} ∘ ··· ∘ f_1(C) | C ∈ L_basis];
    end
end
return f_1, ··· , f_e;
```