



**HAL**  
open science

## Efficient $(3, 3)$ -isogenies on fast Kummer surfaces

Maria Corte-Real Santos, Craig Costello, Benjamin Smith

► **To cite this version:**

Maria Corte-Real Santos, Craig Costello, Benjamin Smith. Efficient  $(3, 3)$ -isogenies on fast Kummer surfaces. 2024. hal-04433463v2

**HAL Id: hal-04433463**

**<https://inria.hal.science/hal-04433463v2>**

Preprint submitted on 3 Sep 2024

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution 4.0 International License

# EFFICIENT (3,3)-ISOGENIES ON FAST KUMMER SURFACES

MARIA CORTE-REAL SANTOS, CRAIG COSTELLO, AND BENJAMIN SMITH

ABSTRACT. We give an alternative derivation of  $(N, N)$ -isogenies between fast Kummer surfaces which complements existing works based on the theory of theta functions. We use this framework to produce explicit formulæ for the case of  $N = 3$ , and show that the resulting algorithms are more efficient than all prior  $(3, 3)$ -isogeny algorithms.

## 1. INTRODUCTION

Isogenies of elliptic curves are well-understood, at least from an algorithmic point of view, in theory and in practice. Given the Weierstrass equation of an elliptic curve  $E$ , and a generator  $P$  of a finite subgroup of  $E$ , Vélu's formulæ [54] allow us to write down polynomials defining a normalized quotient isogeny  $\Phi : E \rightarrow E/\langle P \rangle$  (with variants for alternative curve models [40], or for rational subgroups with irrational generators [34]). Building on these formulæ, there also exist highly efficient algorithms for evaluating an isogeny at points of  $E$  *without* deriving a polynomial representation for the isogeny itself (including [3], [19], and [45], for example). Interest in these formulæ and algorithms has recently intensified with the development of *isogeny-based cryptography* as a source of cryptosystems conjectured to be resistant against quantum attacks.

As a generalization of an elliptic curve, we consider principally polarized abelian varieties, and the first non-elliptic examples are Jacobians of genus-2 curves. Genus-2 curves are hyperelliptic curves with affine plane models

$$C : y^2 = f(x) \quad \text{where } f(x) \text{ is squarefree of degree 5 or 6,}$$

in characteristic not dividing 30, and the Jacobian  $\mathcal{J} = \text{Jac}(C)$  of  $C$  is a 2-dimensional principally polarized abelian variety (p.p.a.v.), birational to  $C^{(2)}$ , parameterizing the degree-0 Picard group of the curve  $C$ .

Mumford [41], Cantor [10], Grant [32], and Flynn [27, 29] laid the ground for explicit geometric and number-theoretic computations with genus-2 Jacobians. Casels and Flynn's text [11] presents a unified view of genus-2 arithmetic. Later, Gaudry [31] proposed Kummer surfaces of genus-2 Jacobians as a setting for efficient discrete-logarithm-based cryptosystems, building on a variant [15] of Lentra's ECM factoring algorithm [37]. The Kummer surface  $\mathcal{K}$  of a Jacobian  $\mathcal{J}$  is the image of the quotient morphism  $\pi : \mathcal{J} \rightarrow \mathcal{K} = \mathcal{J}/\langle \pm 1 \rangle$ ; as such, it is the genus-2 analogue of the  $x$ -coordinate of elliptic curves. Geometrically, Kummer surfaces have convenient models as quartic surfaces in  $\mathbb{P}^3$  with 16 point singularities.

Cosset put Chudnovsky and Chudnovsky's Kummer ECM into practice in [17], while high-speed, high-security Kummer-based implementations of Diffie–Hellman key exchange [2, 6, 46] and signature schemes [46, 47] can give significant practical improvements over elliptic curves in many contexts.

However, while the basic arithmetic of genus-2 Jacobians and Kummer surfaces has matured, and while cryptographic applications have driven great improvements in the efficiency of the resulting formulæ and algorithms, the corresponding explicit theory of isogenies lags behind. First, note that just as elliptic isogenies factor naturally into compositions of scalar multiplications and isogenies with prime cyclic kernel (i.e., isomorphic to  $\mathbb{Z}/N\mathbb{Z}$  with  $N$  prime), isogenies of abelian surfaces (including Jacobians of genus-2 curves) decompose into compositions of scalar multiplications and  $(N, N)$ -isogenies (with kernel isomorphic to  $(\mathbb{Z}/N\mathbb{Z})^2$ ).<sup>1</sup> The fundamental task, then, is to compute and evaluate  $(N, N)$ -isogenies where  $N$  is prime. We can do this on the level of the Jacobian (using e.g. correspondences on genus-2 curves [52]), or we can use the fact that isogenies commute with  $-1$  to move down to the more tractable Kummer surfaces. Indeed, as Cassels and Flynn note, “we lose nothing by going down to the Kummers, because [the map] lifts automatically to a map of abelian varieties.” [11, §9.3].

The case  $N = 2$  is classical: explicit methods and formulæ go back to Richelot [48], and were re-developed in modern terms by Bost and Mestre [8] and Cassels and Flynn [11, §3]. Going further, we find some first efforts at explicit curve-based formulæ for the case  $N = 3$  by Smith [51] (building on an ineffective general method due to Dolgachev and Lehavi [25]), and more general results due to Couvignes and Ezome [21]. Moving to general Kummer surfaces, Bruin, Flynn and Testa [9], Nicholls [42], and Flynn [28] gave more powerful formulæ for  $N = 3, 4$ , and 5, respectively, in a number-theoretic context; Nicholls even gives a method for general  $N$ . Flynn and Ti revisited the formulæ for  $N = 3$  in a cryptographic context [30], and Decru and Kunzweiler [24] further optimized these formulæ, drastically improving their efficiency. However, none of these formulæ make use of the special symmetries of the most efficient Kummer surfaces that have been used in cryptographic implementations.

Bisson, Cosset, Lubicz, and Robert have advanced an ambitious program [4, 16, 38, 49, 50] based on the theory of theta functions [41] to provide asymptotically efficient algorithms for arbitrary odd  $N$  (and beyond genus 2 to arbitrarily high dimension). The `AVIsogenies` software package based on their results is publicly available [5]. These algorithms are certainly compatible with fast Kummer surfaces, but they target isogeny evaluation for general abelian varieties, rather than the construction of compact explicit formulæ in genus 2 that can be studied, analysed, and optimized in their own right. Nevertheless, these techniques were recently revisited by Dartois, Maino, Pope and Robert [22] in the context of cryptography to efficiently compute chains of  $(2, 2)$ -isogenies between products of elliptic curves in the theta model.

**1.1. Contributions.** In this article, we give a general method for deriving explicit formulæ for isogenies of fast Kummer surfaces, optimizing the approach of Bruin, Flynn, and Testa by exploiting the high symmetry of these “fast” surfaces, which are the most relevant for applications over finite fields. Our methods are elementary in the sense that they avoid explicitly using the heavy machinery of theta functions required in [18, 22, 39] (though of course theta functions implicitly play a fundamental role in our techniques). We apply these methods to give explicit examples

---

<sup>1</sup>In some special cases, depending on the endomorphism ring of the Jacobian, we can also have isogenies with cyclic kernel [26]. These isogenies are beyond the scope of this article.

for  $N = 3$  and 5. For example, for  $N = 3$  we obtain a map  $\phi : \mathcal{K} \rightarrow \mathcal{K}'$  defined by

$$\phi((X_1 : X_2 : X_3 : X_4)) = (\phi_1(X_1, X_2, X_3, X_4) : \cdots : \phi_4(X_1, X_2, X_3, X_4)) ,$$

where

$$\begin{aligned} \phi_1(X_1, X_2, X_3, X_4) &= X_1 (c_1 X_1^2 + c_2 X_2^2 + c_3 X_3^2 + c_4 X_4^2) + c_5 X_2 X_3 X_4 , \\ \phi_2(X_1, X_2, X_3, X_4) &= X_2 (c_2 X_1^2 + c_1 X_2^2 + c_4 X_3^2 + c_3 X_4^2) + c_5 X_1 X_3 X_4 , \\ \phi_3(X_1, X_2, X_3, X_4) &= X_3 (c_3 X_1^2 + c_4 X_2^2 + c_1 X_3^2 + c_2 X_4^2) + c_5 X_1 X_2 X_4 , \\ \phi_4(X_1, X_2, X_3, X_4) &= X_4 (c_4 X_1^2 + c_3 X_2^2 + c_2 X_3^2 + c_1 X_4^2) + c_5 X_1 X_2 X_3 , \end{aligned}$$

and  $c_i$  are rational functions in the theta-null constants  $a, b, c, d$  defining  $\mathcal{K}$  and the coordinates of the generators of the kernel (see Section 4.1 for the explicit expressions). This map can be evaluated with at most 88 multiplications and 12 squarings in the field containing the theta constants and generator coordinates.

To illustrate the potential benefits of our formulæ in practical applications, we give experimental results on cryptographic hash functions based on chains of  $(3, 3)$ -isogenies, as in [12] and [24]. In Section 5 we present 3DAC: a three-dimensional *differential addition chain*, and use it to construct  $(N^k, N^k)$ -isogeny kernels correctly, efficiently, and securely. Combined with our  $(3, 3)$ -isogeny formulæ, this allows us to efficiently compute  $(3^k, 3^k)$ -isogenies on fast Kummer surfaces. The hash function we define in Section 6 uses these isogenies, exploiting the efficient arithmetic of fast Kummer surfaces for the first time, to gain speed-ups of between 8x and 9x over the Castryk–Decru hash function [12] and between 32x and 34x over the Decru–Kunzweiler hash function [24].

**1.2. Software.** The source code accompanying this paper is written in MAGMA [7], Python and SageMath [53] and is publicly available under the MIT license. It is available at

<https://github.com/mariascrs/KummerIsogenies>.

**Acknowledgements.** We thank Chris Nicholls for making the code accompanying his thesis available to us, which we used to obtain the formulae for  $(2, 2)$ -isogenies presented in Section 3. We also thank Sam Frengley for many helpful conversations during the preparation of this paper. We are also grateful to the anonymous reviewers, whose comments helped to significantly improve the article. The first author was supported by UK EPSRC grant EP/S022503/1. This work was supported by the HYPERFORM consortium, funded by France through Bpifrance; it also received funding from the France 2030 program, managed by the French National Research Agency under grant agreement No. ANR-22-PETQ-0008 PQ-TLS, and from the French National Research Agency under grant agreement No. ANR-19-CE48-0008 CIAO.

## 2. FAST KUMMER SURFACES AND THEIR ARITHMETIC

Let  $\mathbb{k}$  be a perfect field—typically, a finite field or a number field—of characteristic  $p \neq 2, 3$ , or 5, and fix an algebraic closure  $\bar{\mathbb{k}}$ . If  $\mathbb{k} = \mathbb{F}_q$ , then we measure the time complexity of our algorithms in terms of elementary operations in  $\mathbb{F}_q$ . We let  $\mathbf{M}$ ,  $\mathbf{S}$ , and  $\mathbf{a}$  denote the cost of a single multiplication, squaring, and addition (or subtraction) in  $\mathbb{F}_q$ , respectively.

**2.1. Genus-2 curves and their Jacobians.** Every smooth genus-2 curve over  $\mathbb{k}$  is isomorphic to a curve of the form  $C : y^2 = f(x)$ , where  $f(x) \in \mathbb{k}[x]$  is a squarefree polynomial of degree 6.

For our applications we may suppose that  $f(x)$  has all its roots in  $\mathbb{k}$ , so (after, for example, mapping one root to 0, one to 1, and one to  $\infty$ , as in [43, §2.1]) we can assume  $C$  has a *Rosenhain model*

$$C \cong C_{\lambda, \mu, \nu} / \mathbb{k} : y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu) \quad \text{with } \lambda, \mu, \nu \in \mathbb{k};$$

the values  $\lambda$ ,  $\mu$ , and  $\nu$  are called *Rosenhain invariants* of  $C_{\lambda, \mu, \nu}$ .

Fix a prime  $N$  not divisible by  $\text{char}(\mathbb{k})$ . The  $N$ -torsion subgroup  $\mathcal{J}[N]$  of  $\mathcal{J}$  is a  $\mathbb{Z}/N\mathbb{Z}$ -module of rank 4, that is,  $\mathcal{J}[N] \cong (\mathbb{Z}/N\mathbb{Z})^4$ ; and the (canonical) principal polarisation on  $\mathcal{J}$  induces a non-degenerate, bilinear, and antisymmetric  $N$ -Weil pairing

$$e_N : \mathcal{J}[N] \times \mathcal{J}[N] \rightarrow \mu_N.$$

A subgroup  $G \subseteq \mathcal{J}[N]$  is *isotropic* if  $e_N(P, Q) = 1$  for all  $P, Q \in G$ , and *maximal isotropic* if it is not properly contained in any isotropic subgroup of  $\mathcal{J}[N]$ . Since  $N$  is prime, if  $G$  is maximal isotropic then  $G \cong (\mathbb{Z}/N\mathbb{Z})^2$ ; we say  $G$  is an  $(N, N)$ -subgroup. If  $G$  is a maximal isotropic subgroup of  $\mathcal{J}[N]$ , then the quotient isogeny of abelian varieties

$$\Phi : \mathcal{J} \rightarrow A' := \mathcal{J}/G$$

is an isogeny of p.p.a.v.s: that is, there is a principal polarization on  $A'$  that pulls back via  $\Phi$  to  $N$  times the principal polarization on  $\mathcal{J}$ . We say that  $\Phi$  is an  $(N, N)$ -isogeny.

Being a principally polarized abelian surface,  $A'$  is (as a p.p.a.v.) the Jacobian of a genus 2 curve, say  $\mathcal{J}'$ , or a product of elliptic curves  $E'_1 \times E'_2$  (equipped with the product polarisation). The case  $A' = \mathcal{J}$  is the general case, and the primary focus of this paper.

**2.2. Isogenies and Kummer surfaces.** The Kummer surface  $\mathcal{K}$  of a Jacobian  $\mathcal{J}$  is the image of the quotient map  $\pi : \mathcal{J} \rightarrow \mathcal{K} = \mathcal{J}/\{\pm 1\}$ . Geometrically, it has a quartic model in  $\mathbb{P}^3$  with sixteen point singularities, called *nodes*; the nodes are the images in  $\mathcal{K}$  of the 2-torsion points of  $\mathcal{J}$ , since these are precisely the points fixed by  $-1$ .

Any  $(N, N)$ -isogeny  $\Phi : \mathcal{J} \rightarrow \mathcal{J}'$  descends to a morphism of Kummer surfaces  $\phi : \mathcal{K} \rightarrow \mathcal{K}'$ , such that the following diagram commutes:

$$\begin{array}{ccc} \mathcal{J} & \xrightarrow{\quad \Phi \quad} & \mathcal{J}' \\ \downarrow \pi & & \downarrow \pi' \\ \mathcal{K} & \xrightarrow{\quad \phi \quad} & \mathcal{K}' \end{array}$$

Abusing terminology, we say a morphism  $\phi$  of Kummer surfaces is an  $(N, N)$ -isogeny if it is induced by an  $(N, N)$ -isogeny  $\Phi$  between the corresponding Jacobians.

**2.3. Fast Kummer surfaces.** Following Gaudry [31], fast Kummer surfaces are defined by four *fundamental theta constants*, which can be computed from the Rosenhain invariants of a genus-2 curve  $C/\mathbb{k}$ . Given a hyperelliptic curve  $C/\mathbb{k}$  with

Rosenhain invariants  $\lambda, \mu, \nu \in \mathbb{k}$ , we define *fundamental theta constants*  $a, b, c, d \in \overline{\mathbb{k}}$  and *dual theta constants* as  $A, B, C, D \in \overline{\mathbb{k}}$  such that

$$\begin{aligned} A^2 &= a^2 + b^2 + c^2 + d^2, & B^2 &= a^2 + b^2 - c^2 - d^2, \\ C^2 &= a^2 - b^2 + c^2 - d^2, & D^2 &= a^2 - b^2 - c^2 + d^2. \end{aligned}$$

The theta constants are related to Rosenhain invariants through the relations

$$\lambda = \frac{a^2 c^2}{b^2 d^2}, \quad \mu = \frac{c^2 e^2}{d^2 f^2}, \quad \nu = \frac{a^2 e^2}{b^2 f^2},$$

where  $e, f \in \overline{\mathbb{k}}$  satisfy  $e^2/f^2 = (AB + CD)/(AB - CD)$ .

We define the *fast* Kummer model  $\mathcal{K}$  corresponding to  $\mathcal{C}$  as

$$(1) \quad \begin{aligned} \mathcal{K} : & X_1^4 + X_2^4 + X_3^4 + X_4^4 - 2E \cdot X_1 X_2 X_3 X_4 - F \cdot (X_1^2 X_4^2 + X_2^2 X_3^2) \\ & - G \cdot (X_1^2 X_3^2 + X_2^2 X_4^2) - H \cdot (X_1^2 X_2^2 + X_3^2 X_4^2) = 0, \end{aligned}$$

where  $X_1, X_2, X_3, X_4$  are coordinates on  $\mathbb{P}^3$  and the coefficients  $E, F, G, H$  are rational functions in  $a, b, c, d$ , namely

$$(2) \quad \begin{aligned} E &:= 256abcdA^2B^2C^2D^2/(a^2d^2 - b^2c^2)(a^2c^2 - b^2d^2)(a^2b^2 - c^2d^2), \\ F &:= (a^4 - b^4 - c^4 + d^4)/(a^2d^2 - b^2c^2), \\ G &:= (a^4 - b^4 + c^4 - d^4)/(a^2c^2 - b^2d^2), \\ H &:= (a^4 + b^4 - c^4 - d^4)/(a^2b^2 - c^2d^2). \end{aligned}$$

This model of  $\mathcal{K}$  is often referred to as the *canonical* parameterisation [47]. Note that  $A^2, B^2, C^2$ , and  $D^2$  are linear combinations of  $a^2, b^2, c^2$ , and  $d^2$ , so the equation of  $\mathcal{K}$  is determined entirely by  $a, b, c, d$ ; in fact,  $\mathcal{K}$  is determined by the projective point  $(a : b : c : d) \in \mathbb{P}^3$ . The identity element on  $\mathcal{K}$  is  $\mathcal{O}_{\mathcal{K}} = (a : b : c : d)$ .

**2.4. Nodes of the Kummer surface.** The *nodes* of  $\mathcal{K}$  are the sixteen points

$$\begin{aligned} \mathcal{O}_{\mathcal{K}} &= (a : b : c : d), & T_1 &= (a : b : -c : -d), & T_2 &= (a : -b : c : -d), & T_3 &= (a : -b : -c : d), \\ T_4 &= (b : a : d : c), & T_5 &= (b : a : -d : -c), & T_6 &= (b : -a : d : -c), & T_7 &= (b : -a : -d : c), \\ T_8 &= (c : d : a : b), & T_9 &= (c : d : -a : -b), & T_{10} &= (c : -d : a : -b), & T_{11} &= (c : -d : -a : b), \\ T_{12} &= (d : c : b : a), & T_{13} &= (d : c : -b : -a), & T_{14} &= (d : -c : b : -a), & T_{15} &= (d : -c : -b : a). \end{aligned}$$

Each of the  $T_i$  is the image in  $\mathcal{K}$  of a two-torsion point  $\tilde{T}_i$  in  $\mathcal{J}[2]$ . Since  $\tilde{T}_i = -\tilde{T}_i$ , the translation-by- $\tilde{T}_i$  map on  $\mathcal{J}$  induces a morphism  $\sigma_i : \mathcal{K} \rightarrow \mathcal{K}$ . In fact,  $\sigma_i$  lifts to a linear map on  $\mathbb{A}^4$ : that is, it acts like a matrix on the coordinates  $(X_1, X_2, X_3, X_4)$  on  $\mathbb{P}^3$ . Further,  $\sigma_i$  and  $\sigma_j$  commute resp. anticommute if  $e_2(\tilde{T}_i, \tilde{T}_j) = 1$  resp.  $-1$ .

In particular, if we define

$$U_1 := \text{diag}(1, 1, -1, -1), \quad U_2 := \text{diag}(1, -1, 1, -1),$$

and

$$V_1 := \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad V_2 := \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Then

$$(3) \quad U_1^2 = U_2^2 = I_4, \text{ and } U_1 U_2 = U_2 U_1, \quad V_1^2 = V_2^2 = I_4, \text{ and } V_1 V_2 = V_2 V_1,$$

and

$$(4) \quad U_1V_2 = -V_2U_1, \quad U_2V_1 = -V_1U_2, \quad U_1V_1 = V_1U_1, \quad U_2V_2 = V_2U_2.$$

Taking the labelling of the nodes above, with  $T_0 = (a : b : c : d)$  as the image of  $\tilde{T}_0 = \mathcal{O}_{\mathcal{J}}$ , the corresponding translations are such that

$$T_i = \sigma_i((a : b : c : d)) \quad \text{for } 0 \leq i \leq 15;$$

that is,

$$\begin{array}{cccc} \sigma_0 = I_4 & \sigma_1 = U_1 & \sigma_2 = U_2 & \sigma_3 = U_1U_2 \\ \sigma_4 = V_1 & \sigma_5 = V_1U_1 & \sigma_6 = V_1U_2 & \sigma_7 = V_1U_1U_2 \\ \sigma_8 = V_1V_2 & \sigma_9 = V_1V_2U_1 & \sigma_{10} = V_1V_2U_2 & \sigma_{11} = V_1V_2U_1U_2 \\ \sigma_{12} = V_2 & \sigma_{13} = V_2U_1 & \sigma_{14} = V_2U_2 & \sigma_{15} = V_2U_1U_2 \end{array}$$

Now Eqs. (3) and (4) show that  $(\tilde{T}_1, \tilde{T}_2, \tilde{T}_{12}, \tilde{T}_4)$  is a symplectic basis (with respect to the 2-Weil pairing) of  $\mathcal{J}[2]$ , where we define a symplectic basis as follows.

**Definition 2.1.** Let  $\mathcal{J}$  be the Jacobian of a genus 2 curve  $\mathcal{C}$ . We say that a basis  $\{Q_1, Q_2, Q_3, Q_4\}$  for  $\mathcal{J}[D]$  is *symplectic* with respect to the  $D$ -Weil pairing if

$$e_D(Q_1, Q_3) = e_D(Q_2, Q_4) = \zeta$$

where  $\zeta$  is a primitive  $D$ -th root of unity, and  $e_D(Q_i, Q_j) = 1$  otherwise.

**2.5. Operations on the Kummer surface.** Let  $\pi : \mathcal{J} \rightarrow \mathcal{K}$  be the quotient by  $-1$ . The multiplication-by- $m$  maps  $[m]$  on  $\mathcal{J}$  induce *pseudo-multiplications*  $\pi(P) \mapsto [m]_*(\pi(P)) = \pi([m]P)$ . We can express the pseudo-doubling map  $[2]_*$  on  $\mathcal{K}$  as a composition of four basic building blocks, each a morphism from  $\mathbb{P}^3$  to  $\mathbb{P}^3$ :

- (1) the *Hadamard involution*  $\mathcal{H} : \mathbb{P}^3 \rightarrow \mathbb{P}^3$ , which is induced by the linear map on  $\mathbb{A}^4$  defined by the matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix};$$

- (2) the *squaring* map

$$\mathcal{S} : (X_1 : X_2 : X_3 : X_4) \mapsto (X_1^2 : X_2^2 : X_3^2 : X_4^2);$$

- (3) the *scaling* maps

$$\mathcal{C}_{(\alpha:\beta:\gamma:\delta)} : (X_1 : X_2 : X_3 : X_4) \mapsto (\alpha X_1 : \beta X_2 : \gamma X_3 : \delta X_4)$$

for each  $(\alpha : \beta : \gamma : \delta) \in \mathbb{P}^3(\mathbb{k})$ ; and

- (4) the *inversion* map

$$\begin{aligned} \mathcal{I} : (X_1 : X_2 : X_3 : X_4) &\mapsto (X_2X_3X_4 : X_1X_3X_4 : X_1X_2X_4 : X_1X_2X_3) \\ &= (1/X_1 : 1/X_2 : 1/X_3 : 1/X_4), \end{aligned}$$

well-defined when all  $X_i \neq 0$ .

We can readily see that  $\mathcal{H}$  costs 8  $\mathbb{k}$ -additions,  $\mathcal{S}$  costs 4  $\mathbb{k}$ -squarings,  $\mathcal{C}$  costs 4  $\mathbb{k}$ -multiplications, and  $\mathcal{I}$  costs 6  $\mathbb{k}$ -multiplications. Now, if  $\mathcal{K}$  is a Kummer surface with fundamental theta constants  $(a : b : c : d)$ , then pseudo-doubling is given by

$$[2]_* = \mathcal{C}_{\mathcal{I}(\mathcal{O}_{\mathcal{K}})} \circ \mathcal{H} \circ \mathcal{S} \circ \mathcal{C}_{\mathcal{I}((A:B:C:D))} \circ \mathcal{H} \circ \mathcal{S}.$$

While  $\mathcal{K}$  inherits scalar multiplication from  $\mathcal{J}$ , it loses the group law:  $\pi(P) = \pm P$  and  $\pi(Q) = \pm Q$  in  $\mathcal{K}$  do not uniquely determine  $\pi(P + Q) = \pm(P + Q)$  (unless at least one of  $P$  and  $Q$  is in  $\mathcal{J}[2]$ ). However, the operation  $\{\pi(P), \pi(Q)\} \mapsto \{\pi(P + Q), \pi(P - Q)\}$  is well-defined, so we have a *pseudo-addition* operation  $(\pi(P), \pi(Q), \pi(P - Q)) \mapsto \pi(P + Q)$ .

By abuse of notation, we let  $R = (r_1 : r_2 : r_3 : r_4)$  and  $S = (s_1 : s_2 : s_3 : s_4)$  be points on  $\mathcal{K}$ , and let  $T^+ = (t_1^+ : t_2^+ : t_3^+ : t_4^+)$  and  $T^- = (t_1^- : t_2^- : t_3^- : t_4^-)$  denote the sum  $R + S$  and difference  $R - S$ , respectively. There exist biquadratic forms  $B_{ij}$  [11, Theorem 3.9.1] for  $\mathcal{K}$  such that for  $1 \leq i, j \leq 4$  we have

$$t_i^+ t_j^- + t_i^- t_j^+ = \lambda B_{ij}(r_1, r_2, r_3, r_4; s_1, s_2, s_3, s_4) = \lambda B_{ij}(R; S),$$

where  $\lambda \in \bar{\mathbb{k}}$  is a common projective factor depending only on the affine representations chosen for  $R, S, T^+, T^-$ . The biquadratic forms  $B_{i,j}$  for fast Kummer surfaces are given explicitly by Renes and Smith [47, §5.2].

These biquadratic forms are the basis of explicit pseudo-addition and doubling laws on  $\mathcal{K}$ . For example, if the difference  $T^-$  is known, then the  $B_{ij}$  can be used to compute the coordinates of  $T^+$ . As we will see in Section 3, the  $B_{ij}$  will also be crucial in determining equations for our  $(N, N)$ -isogenies.

### 3. $(N, N)$ -ISOGENIES ON FAST KUMMER SURFACES

Throughout this section,  $\Phi : \mathcal{J} = \text{Jac}(C) \rightarrow \mathcal{J}'$  is an  $(N, N)$ -isogeny with kernel  $G \subset \mathcal{J}[N]$  (a maximal  $N$ -Weil isotropic subgroup of  $\mathcal{J}[N]$ ), where  $N$  is a prime number not equal to the characteristic of the base field  $\mathbb{k}$ . Our goal is to compute an explicit and efficiently-computable collection of polynomials defining the induced map  $\phi : \mathcal{K} \rightarrow \mathcal{K}'$  when  $\mathcal{K}$  and  $\mathcal{K}'$  admit *fast* models.

**3.1. A warm-up with  $N = 2$ .** We first dispose of the case  $N = 2$ . Let  $\tilde{T}_0, \dots, \tilde{T}_{15}$  be the 16 points in  $\mathcal{J}[2]$ , and let  $T_0, \dots, T_{15}$  be their images in  $\mathcal{K}$ . Recall that  $T_i = \sigma_i(T_0)$ , where  $\sigma_i : \mathcal{K} \rightarrow \mathcal{K}$  is a morphism defining the translation-by- $T_i$  map. There are precisely fifteen (images of)  $(2, 2)$ -subgroups in  $\mathcal{K}$ , and they are the images of

$$\tilde{G}_{ij} := \{\tilde{T}_0, \tilde{T}_i, \tilde{T}_j, \tilde{T}_i + \tilde{T}_j\} \subset \mathcal{J}[2]$$

in  $\mathcal{K}$ , where  $1 \leq i \neq j \leq 15$  such that the linear maps corresponding to  $\sigma_i$  and  $\sigma_j$  commute. This gives 15 corresponding  $(2, 2)$ -isogenies given by  $\phi : \mathcal{K} \rightarrow \mathcal{K}' = \mathcal{K}/G_{i,j}$ . For each unique  $(2, 2)$ -subgroup, we can associate a morphism  $\alpha : \mathcal{K} \rightarrow \mathcal{K}$  induced by a linear map on  $\mathbb{A}^4$  such that the corresponding  $(2, 2)$ -isogeny  $\mathcal{K} \rightarrow \tilde{\mathcal{K}}$  is given by

$$\psi := \mathcal{H} \circ \mathcal{S} \circ \alpha.$$

We give matrices specifying the linear map  $\alpha$  for each of the  $(2, 2)$ -subgroups in Appendix A. For now, it suffices to note that the nonzero entries of these  $4 \times 4$  matrices are all fourth roots of unity.

Note however, that  $\tilde{\mathcal{K}}$  will not be in the correct form, as given by Equation (1). We must therefore apply a final scaling  $\mathcal{C}_U$  where  $U = (\mathcal{S}^{-1} \circ \mathcal{I} \circ \psi)(\mathcal{O}_{\mathcal{K}})$ . From this we obtain a  $(2, 2)$ -isogeny  $\phi := \mathcal{C}_U \circ \psi : \mathcal{K} \rightarrow \mathcal{K}' = \mathcal{K}/G_{i,j}$ , where  $\mathcal{K}$  and  $\mathcal{K}'$  are fast Kummer surfaces.

**Example 3.1.** Consider the  $(2, 2)$ -subgroup

$$G_{1,2} = \{(a : b : c : d), (a : b : -c : -d), (a : -b : c : -d), (a : -b : -c : d)\}.$$



Here  $\alpha$  is the identity map and the  $(2, 2)$ -isogeny is given by

$$(X_1 : X_2 : X_3 : X_4) \mapsto \left( \frac{X_1^2 + X_2^2 + X_3^2 + X_4^2}{A} : \frac{X_1^2 + X_2^2 - X_3^2 - X_4^2}{B} : \frac{X_1^2 - X_2^2 + X_3^2 - X_4^2}{C} : \frac{X_1^2 - X_2^2 - X_3^2 + X_4^2}{D} \right)$$

We call this the *distinguished kernel*: the kernel of the first half of doubling. Indeed,  $U = (A : B : C : D)$  and we recover the first three steps  $\mathcal{C}_{\mathcal{I}(A:B:C:D)} \circ \mathcal{H} \circ \mathcal{S}$  of the doubling map on fast Kummer surfaces.

*Remark 3.2.* Though the formulæ for  $(2, 2)$ -isogenies on fast Kummer surfaces are extremely compact, we remark that the final scaling requires the computation of square roots in  $\bar{\mathbb{k}}$ . If  $R, S$  are the 2-torsion points generating the isogeny, let  $P, Q \in \mathcal{K}$  be such that  $R = [2]_*P, S = [2]_*Q$ . The coordinates of  $P, Q$  contain the square roots needed for the final scaling (up to a projective factor). We therefore suspect that these square roots may be inferred directly from coordinates of the 4-torsion, though we have not been able to derive such formulæ.

**3.2. The general case: odd  $N$ .** From this point forward, we suppose  $N$  is an odd prime. Since  $N$  is odd, the  $(N, N)$ -isogeny  $\Phi$  restricts to an isomorphism of 2-torsion subgroups  $\mathcal{J}[2] \rightarrow \mathcal{J}'[2]$ . Furthermore, since  $\Phi$  is an isogeny of p.p.a.v. it is compatible with the  $N$ -Weil pairing by definition, and so it maps the symplectic structure on  $\mathcal{J}[2]$  associated with the fast Kummer  $\mathcal{K}$  onto a symplectic 2-torsion structure on  $\mathcal{J}'[2]$ , which is associated with a fast Kummer  $\mathcal{K}'$ . The isogeny  $\Phi$  therefore descends to a morphism  $\phi : \mathcal{K} \rightarrow \mathcal{K}'$  of fast Kummers. Our goal is to construct explicit equations for  $\phi$ .

To do so, we follow the strategy taken by Cassels and Flynn [11, §9], Bruin, Flynn and Testa [9], Nicholls [42, §5], and Flynn [28], adapting it to the case of *fast* Kummer surfaces. We will observe that the special forms of the affine translation maps  $\sigma_i$  are very helpful in this setting, and lead to nice results.

In practice, we are given a fast Kummer  $\mathcal{K}$  and the image  $\pi(G)$  of an  $(N, N)$ -subgroup  $G$  of  $\mathcal{J}$  in  $\mathcal{K}$ . There exists a fast Kummer  $\mathcal{K}' \cong (\mathcal{J}'/G)/\langle \pm 1 \rangle$ , and our goal is to find  $\mathcal{K}'$  and the map  $\phi : \mathcal{K} \rightarrow \mathcal{K}'$  induced by the quotient  $(N, N)$ -isogeny  $\Phi$  with kernel  $G$ . Crucially,  $\phi$  “commutes” with the action by 2-torsion points, in the sense of the following definition.

**Definition 3.3.** An *isogeny of fast Kummer surfaces* is a morphism  $\phi : \mathcal{K} \rightarrow \mathcal{K}'$  induced by an isogeny  $\Phi : \mathcal{J} \rightarrow \mathcal{J}'$  such that when lifted to a map on the ambient space, we have

$$\phi \circ U_i^{\mathcal{K}} = U_i^{\mathcal{K}'} \circ \phi \quad \text{and} \quad \phi \circ V_i^{\mathcal{K}} = V_i^{\mathcal{K}'} \circ \phi \quad \text{for } i = 1, 2,$$

where  $U_i$  and  $V_i$  are as defined in [Section 2.4](#).

We want to compute  $\phi : \mathcal{K} \rightarrow \mathcal{K}'$ , but  $\mathcal{K}'$  is unknown. However, as  $\mathcal{K}$  and  $\mathcal{K}'$  are both embedded in  $\mathbb{P}^3$ ,  $\phi$  must be defined by forms of degree  $N$ , and it must commute with the actions of the  $U_i$  and  $V_i$ . This imposes heavy constraints on the shape of the forms defining  $\phi$ , and we can hope to interpolate them using linear algebra given the action of  $G$ , and therefore to interpolate the image Kummer  $\mathcal{K}'$  by pushing the theta constants  $(a : b : c : d)$  through the isogeny.

Let  $\mathcal{K}[N]$  be the image of  $\mathcal{J}[N]$  on  $\mathcal{K}$  and fix  $R, S \in \mathcal{K}[N]$ . From this point forward, we write  $\langle R, S \rangle \subset \mathcal{K}[N]$  for the image of the subgroup  $G$  of  $\mathcal{J}[N]$  generated by the preimages of  $R, S$ . By abuse of notation, we say that  $R, S$  are  $N$ -torsion points on  $\mathcal{K}$ .

The first step is to compute two sets of homogeneous forms of degree  $N$  in the coordinates of  $\mathcal{K}$  that are invariant under translation by  $R$  and by  $S$ . The following lemma, due to Nicholls [42, §5.8.4], describes how we can use the biquadratic forms associated to the Kummer surface introduced in Section 2.3 to construct these homogeneous forms.

**Lemma 3.4.** *Fix Kummer surface  $\mathcal{K}$  with coordinates  $X_1, X_2, X_3, X_4$  and associated biquadratic forms  $B_{i,j}$  for  $1 \leq i, j \leq 4$ . Let  $N$  be an odd prime number, and fix a point  $R \in \mathcal{K}[N]$  of order  $N$ .*

*We denote by  $I \in \{1, 2, 3, 4\}^N$  a list of indices  $I = (i_1, \dots, i_N)$ . Letting  $\tau$  be a permutation of  $\{1, \dots, N\}$ , we write*

$$\tau(I) = \tau((i_1, \dots, i_N)) := (i_{\tau(1)}, \dots, i_{\tau(N)}).$$

*Then, for each  $I \in \{1, 2, 3, 4\}^N$  we define*

$$F_I := \sum_{\tau \in C_N} X_{i_{\tau(1)}} \cdot \prod_{k=1}^{(N-1)/2} B_{i_{\tau(2k)}, i_{\tau(2k+1)}}(X_1, X_2, X_3, X_4; kR),$$

*where  $C_N$  is the cyclic group of order  $N$ . Then, the set  $\mathcal{F}_R := \{F_I\}$  contains homogeneous forms of degree  $N$  invariant under translation by  $R$ .*

Applying the lemma above to  $N$ -torsion points  $R$  and  $S$ , we obtain the two sets  $\mathcal{F}_R$  and  $\mathcal{F}_S$ . The homogeneous forms of degree  $N$  in each set will generate a space of dimension  $m_N \geq 4$ . Our experiments suggest  $m_N = 2N + 2$  for  $N \leq 19$ , and possibly beyond, though we have not proven this.

The next step is to compute a basis for these two spaces, say  $F_1^R, \dots, F_{m_N}^R$  is a basis for the space generated by the homogeneous forms in  $\mathcal{F}_R$ , and  $F_1^S, \dots, F_{m_N}^S$  a basis for the space generated by  $\mathcal{F}_S$ .

The intersection of these spaces contains homogeneous forms of degree  $N$  that are invariant under translation by any point in the kernel  $G$  of our  $(N, N)$ -isogeny. The intersection will be of dimension 4, and a basis for this intersection gives an  $(N, N)$ -isogeny  $\psi : \mathcal{K} \rightarrow \tilde{\mathcal{K}}$ . Explicitly, the third step is to compute a basis of this intersection, say  $f_1, f_2, f_3, f_4$ . Then, our  $(N, N)$ -isogeny is given by  $\psi = (f_1 : f_2 : f_3 : f_4)$ .

We note that  $\tilde{\mathcal{K}}$  may not be in the correct form given by Equation (1). When computing chains of isogenies, however, it is important to ensure that our  $(N, N)$ -isogenies have domain and image in the same form. Therefore, the last step is to apply a linear transformation  $\mathbf{M} : \tilde{\mathcal{K}} \rightarrow \mathcal{K}'$ , where  $\mathcal{K}'$  is a fast Kummer surface. Post-composing the map  $\psi$  with this linear transformation gives a  $\bar{\mathbb{k}}$ -rational  $(N, N)$ -isogeny  $\phi : \mathcal{K} \rightarrow \mathcal{K}'$  between fast Kummer surfaces generated by kernel  $G = \langle R, S \rangle$ .

*Remark 3.5.* The compactness and efficiency of our isogeny formulae is determined by the choice of basis we make for the spaces generated by the forms in  $\mathcal{F}_R$  and  $\mathcal{F}_S$ . An open question that arises from this work, therefore, is finding a solution to the following problem: let  $f_1, \dots, f_n \in \mathbb{Q}(a_1, \dots, a_k)[x_1, \dots, x_m]$  be a basis of polynomials defined over a function field. Find a “nice” basis  $g_1, \dots, g_n$  where  $g_1, \dots, g_n$  are  $\mathbb{Q}(a_1, \dots, a_k)$ -linear combinations of the  $f_i$ .

#### 4. EXPLICIT (3, 3)-ISOGENIES ON FAST KUMMERS

We now specialise the discussion in [Section 3](#) to  $N = 3$  to construct (3, 3)-isogenies between fast Kummer surfaces.

Let  $\mathcal{J} = \text{Jac}(C)$  be the Jacobian of a genus 2 curve  $C$  defined over  $\bar{\mathbb{k}}$ . Suppose we have a (3, 3)-subgroup of  $\mathcal{J}[3]$ , which induces an isogeny  $\phi$  on the corresponding fast Kummer surface  $\mathcal{K} = \mathcal{J}/\{\pm 1\}$  with kernel  $G = \langle R, S \rangle$  for some  $R, S \in \mathcal{K}[3]$  (i.e.,  $G$  is the image of the (3, 3)-subgroup in  $\mathcal{K}$ ).

Exploiting the fact that  $\phi$  is an isogeny of fast Kummer surfaces, we obtain the following lemma, demonstrating that it is determined by five  $\bar{\mathbb{k}}$ -rational functions in the coordinates of  $\mathcal{O}_{\mathcal{K}} = (a : b : c : d)$ ,  $R$  and  $S$ .

**Lemma 4.1.** *Let  $R$  and  $S$  be distinct 3-torsion points on  $\mathcal{K}$  generating a (3, 3)-subgroup  $G \subset \mathcal{K}[3]$ , and set  $\mathcal{O}_{\mathcal{K}} = (a : b : c : d)$ . The (3, 3)-isogeny of fast Kummer surfaces  $\phi : \mathcal{K} \rightarrow \mathcal{K}'$  generated by kernel  $G$  is in the form*

$$(X_1 : X_2 : X_3 : X_4) \longmapsto (\phi_1(X_1, X_2, X_3, X_4) : \cdots : \phi_4(X_1, X_2, X_3, X_4)) ,$$

where

$$\begin{aligned} \phi_1(X_1, X_2, X_3, X_4) &= X_1 (c_1 X_1^2 + c_2 X_2^2 + c_3 X_3^2 + c_4 X_4^2) + c_5 X_2 X_3 X_4 , \\ \phi_2(X_1, X_2, X_3, X_4) &= X_2 (c_2 X_1^2 + c_1 X_2^2 + c_4 X_3^2 + c_3 X_4^2) + c_5 X_1 X_3 X_4 , \\ \phi_3(X_1, X_2, X_3, X_4) &= X_3 (c_3 X_1^2 + c_4 X_2^2 + c_1 X_3^2 + c_2 X_4^2) + c_5 X_1 X_2 X_4 , \\ \phi_4(X_1, X_2, X_3, X_4) &= X_4 (c_4 X_1^2 + c_3 X_2^2 + c_2 X_3^2 + c_1 X_4^2) + c_5 X_1 X_2 X_3 , \end{aligned}$$

with  $c_i \in \bar{\mathbb{k}}[a, b, c, d, r_1, r_2, r_3, r_4, s_1, s_2, s_3, s_4]$ .

*Proof.* By [Lemma 3.4](#), the isogeny  $\phi$  is given by cubic forms. That is,  $\phi$  is defined by polynomials

$$\begin{aligned} \phi_i &= c_{i,1} X_1^3 + c_{i,2} X_1 X_2^2 + c_{i,3} X_1 X_3^2 + c_{i,4} X_1 X_4^2 + c_{i,5} X_2 X_3 X_4 \\ &+ c_{i,6} X_2 X_1^2 + c_{i,7} X_2^3 + c_{i,8} X_2 X_3^2 + c_{i,9} X_2 X_4^2 + c_{i,10} X_1 X_3 X_4 \\ &+ c_{i,11} X_3 X_1^2 + c_{i,12} X_3 X_2^2 + c_{i,13} X_3^3 + c_{i,14} X_3 X_4^2 + c_{i,15} X_1 X_2 X_4 \\ &+ c_{i,16} X_4 X_1^2 + c_{i,17} X_4 X_2^2 + c_{i,18} X_4 X_3^2 + c_{i,19} X_4^3 + c_{i,20} X_1 X_2 X_3 , \end{aligned}$$

where  $c_{i,j}$  are  $\bar{\mathbb{k}}$ -rational functions in the coordinates of  $\mathcal{O}_{\mathcal{K}}$ ,  $R$ , and  $S$  for  $1 \leq i \leq 4$  and  $1 \leq j \leq 20$ . We are looking for an isogeny of fast Kummer surfaces in the sense of [Definition 3.3](#), and compatibility with the translations by 2-torsion thus forces

$$(5) \quad \sigma'_i((\phi_1 : \phi_2 : \phi_3 : \phi_4)) = \phi(\sigma_i(X_1 : X_2 : X_3 : X_4))$$

for all  $1 \leq i \leq 15$ , where  $\sigma_i$  is the action of the 2-torsion point  $T_i \in \mathcal{K}$ , and similarly  $\sigma'_i$  is the action of  $T'_i \in \mathcal{K}'$  (as defined in [Section 2.4](#)). Equation (5) gives rise to relations between the coefficients of the cubic monomials, from which we deduce that  $\phi$  is of the form as in the statement of the lemma. See `section4/lemma-4.1.m` in the code accompanying this paper. Clearing denominators (as our Kummer surfaces lie in  $\mathbb{P}^3$ ), we obtain the  $c_i \in \bar{\mathbb{k}}[a, b, c, d, r_1, r_2, r_3, r_4, s_1, s_2, s_3, s_4]$ .  $\square$

By [Lemma 4.1](#), to determine explicit formulae for the (3, 3)-isogeny  $\phi$  generated by kernel  $G = \langle R, S \rangle \subset \mathcal{K}$ , it suffices to determine the coefficients  $c_1, \dots, c_5$ . We

follow the method given in [Section 3](#) and compute the  $G$ -invariant cubic forms. Define

$$\begin{aligned} B_{ij}^R(X_1, X_2, X_3, X_4) &:= B_{i,j}(X_1, X_2, X_3, X_4; R), \\ B_{ij}^S(X_1, X_2, X_3, X_4) &:= B_{i,j}(X_1, X_2, X_3, X_4; S). \end{aligned}$$

By [Lemma 3.4](#), the cubic forms invariant under translation by  $R$  and  $S$  are given by

$$\begin{aligned} F_{ijk}^R &:= X_i B_{jk}^R + X_j B_{ki}^R + X_k B_{ij}^R, \\ F_{ijk}^S &:= X_i B_{jk}^S + X_j B_{ki}^S + X_k B_{ij}^S, \end{aligned}$$

respectively, where  $1 \leq i, j, k \leq 4$ . Let  $\mathcal{F}_R = \{F_{ijk}^R\}_{1 \leq i, j, k \leq 4}$  and similarly define  $\mathcal{F}_S$ . The cubic forms in  $\mathcal{F}_R$  and  $\mathcal{F}_S$  each generate a space of dimension 8, for which we choose a basis

$$\{F_{111}^R, F_{234}^R, F_{222}^R, F_{134}^R, F_{333}^R, F_{124}^R, F_{444}^R, F_{123}^R\},$$

and similarly for  $\mathcal{F}_S$ . These spaces will intersect in a space of dimension 4, which will give a description of the  $(3, 3)$ -isogeny. We compute a basis

$$\begin{aligned} f_1 &:= z_1 F_{111}^R + z_2 F_{234}^R, & f_2 &:= z_3 F_{222}^R + z_4 F_{134}^R, \\ f_3 &:= z_5 F_{333}^R + z_6 F_{124}^R, & f_4 &:= z_7 F_{444}^R + z_8 F_{123}^R \end{aligned}$$

for the intersection, with  $z_1, \dots, z_8 \in \bar{\mathbb{k}}$  such that there exist  $w_1, \dots, w_8 \in \bar{\mathbb{k}}$  with

$$\begin{aligned} f_1 &= w_1 F_{111}^S + w_2 F_{234}^S, & f_2 &= w_3 F_{222}^S + w_4 F_{134}^S, \\ f_3 &= w_5 F_{333}^S + w_6 F_{124}^S, & f_4 &= w_7 F_{444}^S + w_8 F_{123}^S. \end{aligned}$$

From this, we obtain a  $(3, 3)$ -isogeny  $\psi = (f_1 : f_2 : f_3 : f_4) : \mathcal{K} \rightarrow \tilde{\mathcal{K}}$ .

To move  $\tilde{\mathcal{K}}$  to the correct form, we first define

$$D_1 := (ab - cd)(ab + cd), \quad D_2 := (ac - bd)(ac + bd), \quad D_3 := (ad - bc)(ad + bc).$$

For a point  $P = (x_1 : x_2 : x_3 : x_4)$ , we define

$$\gamma(P) := (D_{23}(x_1 x_2 ab - x_3 x_4 cd) + D_{13}(x_1 x_3 ac - x_2 x_4 bd) + D_{12}(x_1 x_4 ad - x_2 x_3 bc)),$$

and  $h_i(P)$  as the coordinates of  $(\mathcal{H} \circ \mathcal{S})(P)$ , for  $i = 1, 2, 3, 4$ .

Applying a linear transformation  $\mathbf{M}$  to  $\tilde{\mathcal{K}}$ , where  $\mathbf{M}$  is defined as

$$\mathbf{M} := \begin{pmatrix} 1/\alpha_1 & 0 & 0 & 0 \\ 0 & 2/\alpha_2 & 0 & 0 \\ 0 & 0 & 2/\alpha_1 & 0 \\ 0 & 0 & 0 & 2/(3\alpha_2) \end{pmatrix}$$

and where

$$\begin{aligned} \alpha_1 &:= D_3(\gamma(R)(s_4 s_3 ab - s_1 s_2 cd) - \gamma(S)(r_4 r_3 ab - r_1 r_2 cd)), \\ \alpha_2 &:= D_1(\gamma(R)(s_2 s_3 ad - s_1 s_4 bc) - \gamma(S)(r_2 r_3 ad - r_1 r_4 bc)), \end{aligned}$$

we get a simple and efficiently computable expression for our  $(3, 3)$ -isogeny  $\phi := \mathbf{M}(f_1, f_2, f_3, f_4)^T$ , whose image is in the desired form. Formulæ for the intersection and  $\mathbf{M}$  can be found and verified in the file `section4/linear-transform.m` in the accompanying code.

**4.1. Explicit formulae for (3, 3)-isogenies.** We now give explicit formulæ for the isogeny  $\phi : \mathcal{K} \rightarrow \mathcal{K}'$  with kernel  $G = \langle R, S \rangle$ . By Lemma 4.1, it suffices to give explicit formulae for the coefficients  $c_i \in \overline{\mathbb{k}}[a, b, c, d, r_1, r_2, r_3, r_4, s_1, s_2, s_3, s_4]$  for  $i \in \{1, 2, 3, 4, 5\}$ . We set

$$\begin{aligned}\beta_1 &:= D_{23}(\gamma(R) \cdot (s_3 s_4 ab - s_1 s_2 cd) - \gamma(S) \cdot (r_3 r_4 ab - r_1 r_2 cd)), \\ \beta_2 &:= h_1(R) \cdot h_2(S) - h_2(R) \cdot h_1(S).\end{aligned}$$

Then, maintaining the notation above and letting  $D_{ij} := D_i \cdot D_j$ , we find

$$\begin{aligned}c_1 &= 2\beta_1 h_1(R) h_1(S), \\ c_2 &= \beta_1 (h_1(R) h_2(S) + h_2(R) h_1(S)) \\ &\quad + \beta_2 (\gamma(R)(s_3 s_4 ab - s_1 s_2 cd) + \gamma(S)(r_3 r_4 ab - r_1 r_2 cd)) D_{23}, \\ c_3 &= \beta_1 (h_1(R) h_3(S) + h_3(R) h_1(S)) \\ &\quad + \beta_2 (\gamma(R)(s_2 s_4 ac - s_1 s_3 bd) + \gamma(S)(r_2 r_4 ac - r_1 r_3 bd)) D_{13}, \\ c_4 &= \beta_1 (h_1(R) h_4(S) + h_4(R) h_1(S)) \\ &\quad + \beta_2 (\gamma(R)(s_2 s_3 ad - s_1 s_4 bc) + \gamma(S)(r_2 r_3 ad - r_1 r_4 bc)) D_{12}, \\ c_5 &= 2\beta_2 \gamma(S) \gamma(R).\end{aligned}$$

Note that the  $c_1, \dots, c_5$  are symmetric in  $R$  and  $S$ , as one would expect.

*Remark 4.2.* The (3, 3)-isogeny is defined over the field of definition of the fundamental constants  $a, b, c, d$  of  $\mathcal{K}$  and the kernel generators  $R, S$  (rather than the subgroup  $\langle R, S \rangle$ ).

**4.2. Evaluating points under the (3, 3)-isogeny.** Consider the (3, 3)-isogeny  $\phi : \mathcal{K} \rightarrow \mathcal{K}'$  and assume the coefficients  $c_1, \dots, c_5$  have been computed. Given a point  $P = (x_1 : x_2 : x_3 : x_4) \in \mathcal{K}$ , the image  $\phi(P) = (x'_1 : x'_2 : x'_3 : x'_4)$  is given by

$$\begin{aligned}x'_1 &:= x_1(c_1 x_1^2 + c_2 x_2^2 + c_3 x_3^2 + c_4 x_4^2) + c_5 x_2 x_3 x_4, \\ x'_2 &:= x_2(c_2 x_1^2 + c_1 x_2^2 + c_4 x_3^2 + c_3 x_4^2) + c_5 x_1 x_3 x_4, \\ x'_3 &:= x_3(c_3 x_1^2 + c_4 x_2^2 + c_1 x_3^2 + c_2 x_4^2) + c_5 x_1 x_2 x_4, \\ x'_4 &:= x_4(c_4 x_1^2 + c_3 x_2^2 + c_2 x_3^2 + c_1 x_4^2) + c_5 x_1 x_2 x_3.\end{aligned}$$

The fundamental theta constants of the image surface  $\mathcal{K}'$  can be computed in the same way, i.e., as  $\phi((a : b : c : d))$ . Via Equation (2), we can then compute the constants  $E', F', G', H'$  defining the equation of the surface  $\mathcal{K}'$ .

**4.3. Implementation.** We implemented (3, 3)-isogeny evaluation using the formulæ above. We give explicit operation counts for  $\mathbb{k} = \mathbb{F}_q$ , which will be necessary for our cryptographic application in Section 6. To optimise the computation, we implement the following algorithms:

- (1) **TriplingConstantsFromThetas:** given fundamental theta constants  $(a : b : c : d)$ , compute *tripling constants* consisting of:
  - their inverses  $(1/a : 1/b : 1/c : 1/d)$ ;
  - their squares  $(a^2 : b^2 : c^2 : d^2)$ ;
  - squared dual theta constants  $(A^2 : B^2 : C^2 : D^2)$ ; and
  - their inverses  $(1/A^2 : 1/B^2 : 1/C^2 : 1/D^2)$ .

For  $\mathbb{k} = \mathbb{F}_q$ , this requires 12M, 4S, and 6a.

- (2) **Compute33Coefficients**: given coordinates of  $R, S$  and the tripling constants, compute the coefficients  $c_1, \dots, c_5$  defining the  $(3, 3)$ -isogeny. When  $\mathbb{k} = \mathbb{F}_q$ , this requires 76M, 8S, and 97a.
- (3) **Isogeny33Evaluate**: given the coefficients  $c_1, \dots, c_5$ , computes the image of a point  $P \in \mathcal{K}$  under the corresponding  $(3, 3)$ -isogeny (as explained in [Section 4.2](#)). For  $\mathbb{k} = \mathbb{F}_q$ , this requires 26M, 4S and 16a.
- (4) **ComputeImageThetas**: given coefficients  $c_1, \dots, c_5$  and the tripling constants, compute the fundamental theta constants defining the image curve. For  $\mathbb{k} = \mathbb{F}_q$ , this requires 26M and 16a.

Details of the implementation can be found in the accompanying code.

**4.4. A note on  $(5, 5)$ -isogenies on fast Kummers.** Suppose we now have a  $(5, 5)$ -subgroup of  $\mathcal{J}[5]$ , which induces a  $(5, 5)$ -isogeny  $\phi$  on the corresponding fast Kummer surface  $\mathcal{K} = \mathcal{J}/\{\pm 1\}$  with kernel  $G = \langle R, S \rangle$  for some  $R, S \in \mathcal{K}[5]$  (i.e.,  $G$  is the image of the  $(5, 5)$ -subgroup in  $\mathcal{K}$ ).

Following the method in [Section 3](#), we first compute the  $G$ -invariant quintic forms. Let  $B_{i,j}^R$  and  $B_{i,j}^S$  be as before (where now  $R, S$  are the 5-torsion points), and define

$$\begin{aligned} B_{ij}^{2R}(X_1, X_2, X_3, X_4) &:= B_{i,j}(X_1, X_2, X_3, X_4; 2R), \\ B_{ij}^{2S}(X_1, X_2, X_3, X_4) &:= B_{i,j}(X_1, X_2, X_3, X_4; 2S). \end{aligned}$$

By [Lemma 3.4](#) (and following Flynn [28]), the quintic forms invariant under translation by  $R$  are given by

$$\begin{aligned} F_{ijklm}^R &:= X_i B_{jk}^R B_{lm}^{2R} + X_i B_{jl}^R B_{km}^{2R} + X_i B_{jm}^R B_{kl}^{2R} + \\ &X_i B_{kl}^R B_{jm}^{2R} + X_i B_{km}^R B_{jl}^{2R} + X_i B_{lm}^R B_{jk}^{2R} + \\ &X_j B_{ik}^R B_{lm}^{2R} + X_j B_{il}^R B_{km}^{2R} + X_j B_{im}^R B_{kl}^{2R} + \\ &X_j B_{kl}^R B_{im}^{2R} + X_j B_{km}^R B_{il}^{2R} + X_j B_{lm}^R B_{ik}^{2R} + \\ &X_k B_{ji}^R B_{lm}^{2R} + X_k B_{jl}^R B_{im}^{2R} + X_k B_{jm}^R B_{il}^{2R} + \\ &X_k B_{il}^R B_{jm}^{2R} + X_k B_{im}^R B_{jl}^{2R} + X_k B_{lm}^R B_{ji}^{2R} + \\ &X_l B_{jk}^R B_{im}^{2R} + X_l B_{ji}^R B_{km}^{2R} + X_l B_{jm}^R B_{ki}^{2R} + \\ &X_l B_{ki}^R B_{jm}^{2R} + X_l B_{km}^R B_{ji}^{2R} + X_l B_{im}^R B_{jk}^{2R} + \\ &X_m B_{jk}^R B_{li}^{2R} + X_m B_{jl}^R B_{ki}^{2R} + X_m B_{ji}^R B_{kl}^{2R} + \\ &X_m B_{kl}^R B_{ji}^{2R} + X_m B_{ki}^R B_{jl}^{2R} + X_m B_{li}^R B_{jk}^{2R}, \end{aligned}$$

where  $1 \leq i, j, k, l, m \leq 4$ . We similarly define  $F_{ijklm}^S$ : the quintic forms invariant under translation by  $S$ .

Let  $\mathcal{F}_R = \{F_{ijklm}^R\}$  and  $\mathcal{F}_S = \{F_{ijklm}^S\}$ . Working modulo the equation defining the Kummer surface  $\mathcal{K}$ , the quintic forms in  $\mathcal{F}_R$  and  $\mathcal{F}_S$  each generate a space of dimension 12, for which we choose a basis

$$\left\{ \begin{aligned} &F_{14444}^R, F_{23333}^R, F_{23334}^R, F_{23344}^R, F_{23444}^R, F_{24444}^R, \\ &F_{33333}^R, F_{33334}^R, F_{33344}^R, F_{33444}^R, F_{34444}^R, F_{44444}^R \end{aligned} \right\},$$

and similarly for  $\mathcal{F}_S$ . These spaces intersect in a space of dimension 4, which gives a description of the (5, 5)-isogeny. Finding the final scaling map to put the image into the correct form is left as future work.

## 5. GENERATING $(N^k, N^k)$ -SUBGROUPS

In the remaining two sections, we turn to building a hash function based on the (3, 3)-isogenies derived in the previous section. The hash function will compute  $(3^k, 3^k)$ -isogenies as chains of (3, 3)-isogenies, and will start each such chain by computing a  $(3^k, 3^k)$ -subgroup on a fast Kummer surface. This section describes how such  $(N^k, N^k)$ -subgroups can be computed (for prime number  $N$  and integer  $k \geq 1$ ) in a way that is amenable to efficient and secure cryptographic implementations.

We do this in two steps: first, in [Section 5.1](#) we show how to compute a *symplectic* basis for the  $N^k$ -torsion on the Jacobian  $\mathcal{J}$ , which we then push down to the corresponding fast Kummer surface  $\mathcal{K} = \mathcal{J}/\{\pm 1\}$ ; and second, we use this basis to compute the generators  $R, S$  of the  $(N^k, N^k)$ -subgroup  $G$  using the *three-dimensional differential addition chain* introduced in [Section 5.2](#).

**5.1. Generating a symplectic basis on  $\mathcal{K}$ .** We first compute a symplectic basis for the  $N^k$ -torsion on the Jacobian  $\mathcal{J}$  of the genus-2 curve  $C_{\lambda, \mu, \nu}$  corresponding to  $\mathcal{K}$ . We compute this basis by generating  $N^k$ -torsion points on  $\mathcal{J}$  until the  $N^k$ -Weil pairing condition given in [Definition 2.1](#) is satisfied.<sup>2</sup> These points are then pushed down to  $\mathcal{K}$  via

$$\begin{aligned} \pi: \mathcal{J} &\rightarrow \mathcal{K}, \\ P &\mapsto (\mathcal{C}_{\mathcal{I}(\mathcal{O}_{\mathcal{K}})} \circ \mathcal{H} \circ \mathcal{C}_{(\mathcal{I} \circ \mathcal{H} \circ \mathcal{S})(\mathcal{O}_{\mathcal{K}})} \mathcal{S} \circ \mathcal{H} \circ \kappa)(P). \end{aligned}$$

Here,  $\mathcal{C}$ ,  $\mathcal{H}$ ,  $\mathcal{S}$  and  $\mathcal{I}$  are the standard Kummer operations defined in [Section 2.5](#) and  $\kappa: \mathcal{J} \rightarrow \mathcal{K}^{\text{Sqr}}$  maps points in Mumford coordinates on  $\mathcal{J}$  to the *squared* Kummer surface  $\mathcal{K}^{\text{Sqr}}$  as follows. For generic points  $P = (x^2 + u_1x + u_0, v_1x + v_0) \in \mathcal{J}$ , we have

$$\kappa: (x^2 + u_1x + u_0, v_1x + v_0) \mapsto (X_1: X_2: X_3: X_4)$$

with

$$\begin{aligned} X_1 &= a^2(u_0(\mu - u_0)(\lambda + u_1 + \nu) - v_0^2), & X_2 &= b^2(u_0(\nu\lambda - u_0)(1 + u_1 + \mu) - v_0^2), \\ X_3 &= c^2(u_0(\nu - u_0)(\lambda + u_1 + \mu) - v_0^2), & X_4 &= d^2(u_0(\mu\lambda - u_0)(1 + u_1 + \nu) - v_0^2). \end{aligned}$$

For special points  $P = (x - u_0, v_0)$ , the map  $\kappa$  is defined by first adding a point of order 2 on  $\mathcal{J}$ . Indeed, by adding  $(x - u'_0, 0) \in \mathcal{J}[2]$  (with  $u'_0 \neq u_0$ ) we get the point

$$\left( x^2 - (u_0 + u'_0)x + u_0u'_0, \frac{v_0}{u_0 - u'_0}x - \frac{v_0u'_0}{u_0 - u'_0} \right),$$

to which we can apply  $\kappa$ . The translation is then undone by applying the action of the corresponding 2-torsion point on  $\mathcal{K}^{\text{Sqr}}$ . Finally,  $\kappa(\mathcal{O}_{\mathcal{J}}) := (a^2: b^2: c^2: d^2)$ .

The map  $\kappa$  is due to Bisson, Cosset and Robert [5], while the subsequent operations that map from  $\mathcal{K}^{\text{Sqr}}$  to  $\mathcal{K}$  appear in Renes and Smith [47, Section 4.3]. Note that the map  $\pi$  corresponds to a (2, 2)-isogeny, which will not affect the order of the basis points if  $N$  is coprime to 2. If, however,  $2 \mid N$  then one must additionally check the order of the image points on  $\mathcal{K}$ .

<sup>2</sup>In our implementation, we compute the  $N^k$ -Weil pairing of points on  $\mathcal{J}[N^k]$  using MAGMA's in-built functionality.

*Remark 5.1.* For applications where  $N$ ,  $k$ , and the domain Kummer  $\mathcal{K}$  are fixed, the symplectic basis for  $\mathcal{J}[N^k]$  can be computed as part of the set-up once and for all, and the image of these basis points (under  $\pi$ ) can be hardcoded as system parameters. For instance, this will be the case for our cryptographic application in [Section 6](#). In these scenarios, optimising the efficiency of the operations in this subsection is not a priority; the important goal is to optimise the efficiency of the *online* part of the  $(N^k, N^k)$ -subgroup generation procedure, which amounts to optimising the three-dimensional differential addition chain in the following subsection.

**5.2. Three-dimensional differential addition chains.** Let  $Q_1, Q_2, Q_3, Q_4 \in \mathcal{K}$  be the images of a symplectic basis for  $\mathcal{J}[N^k]$  under the map  $\pi$  described above. In this subsection we show how to use this basis to compute the two generators  $R$  and  $S$  of our  $(N^k, N^k)$ -subgroup.

As a first simplification, we restrict to  $(N^k, N^k)$ -subgroups with generators of the form

$$(6) \quad \begin{aligned} R &= Q_1 + [\alpha]Q_3 + [\beta]Q_4, \\ S &= Q_2 + [\beta]Q_3 + [\gamma]Q_4, \end{aligned}$$

where  $\alpha, \beta, \gamma \in \mathbb{Z}/N^k\mathbb{Z}$ . There are  $N^{3k}$  such  $(N^k, N^k)$ -subgroups (for example, see [\[35, Table 1\]](#)), and there are  $O(N^{3k-1})$  subgroups that we lose by imposing this restriction [\[35, Def. 3\]](#). In other words, at least half of the  $(N^k, N^k)$ -subgroups can be obtained with kernel generators of the form in [\(6\)](#), so in a cryptographic context we lose at most one bit of security by simplifying in this manner.

The remainder of this subsection presents the 3DAC algorithm that allows us to compute the kernel generators  $R$  and  $S$  via Equation [\(6\)](#). Our task is to define an algorithm that computes  $P_1 + [\beta]P_2 + [\gamma]P_3$  for given scalars  $\beta, \gamma \in \mathbb{Z}/N^k\mathbb{Z}$  and for the points  $P_1, P_2$  and  $P_3$  on  $\mathcal{K}$ . The analogous computation on  $\mathcal{J}$  could utilise a straightforward 3-way multiexponentiation algorithm, but on the Kummer surface we need a three-dimensional *differential addition chain*. Such an addition chain is only allowed to include the computation of the sum  $Q + R$  if the difference  $\pm(Q - R)$  has already been computed at a previous stage.

Three-dimensional differential addition chains have been studied previously by Rao [\[44\]](#) and more generally by Hutchinson and Karabina [\[33\]](#). However, both of those works study the general scenario whereby three scalars are in play. Viewing Equation [\(6\)](#), we see that there is no scalar multiplication of the point  $P_1$  in our case, which allows for some convenient simplifications. Moreover, the chain due to Rao [\[44\]](#) is non-uniform and the chain due to Hutchinson and Karabina [\[33\]](#) is not fixed length unless the input scalars are. Our algorithm 3DAC satisfies both of these properties regardless of the input scalars, making it secure for use in cryptographic applications, such as the hash function we present in [Section 6](#). We remark that these properties would not be necessary for a hash function involving only public data, but for other cryptographic applications where inputs to the hash function (or, more broadly, the scalars  $\beta$  and  $\gamma$ ) are secret, such as key derivation functions, these properties are an imperative first-step towards protecting the secret data from side-channel attacks.

We derived the 3DAC chain by extending the two-dimensional differential addition chain due to Bernstein [\[1\]](#), the fastest known two-dimensional differential addition chain that is fixed length and uniform. Beyond the points  $P_1, P_2, P_3$ , 3DAC also needs seven additional combinations of sums and/or differences of these



three points. We specify the full ten-tuple of inputs as

$$\mathcal{D} := (P_1, P_2, P_3, P_2 + P_3, P_2 - P_3, P_1 - P_2, P_1 - P_3, [2](P_2 + P_3), \\ P_1 + P_2 + P_3, P_1 - P_2 - P_3),$$

for points  $P_1, P_2, P_3 \in \mathcal{K}$ . In line with [Remark 5.1](#), these additional sums and differences can be (pre)computed on  $\mathcal{J}$  and their image in  $\mathcal{K}$  specified as part of the system parameters.

Given the tuple  $\mathcal{D}$  above and the two scalars  $\beta, \gamma \in \mathbb{Z}/N^k\mathbb{Z}$ , our 3DAC algorithm computes the point  $P_1 + [\beta]P_2 + [\gamma]P_3$  on  $\mathcal{K}$  using  $3\ell - 2$  pseudo-additions and  $\ell - 1$  pseudo-doublings on  $\mathcal{K}$ , where  $\ell$  is the bitlength of  $N^k$ . See [Appendix B](#) for the full description of the algorithm.

## 6. A HASH FUNCTION FROM (3, 3)-ISOGENIES

Isogenies between *superspecial* Jacobians of genus 2 curves have been proposed for use in post-quantum isogeny-based cryptography (e.g., [\[13, 30\]](#)). We follow suit and henceforth restrict our attention superspecial Jacobians defined over  $\bar{\mathbb{k}} = \bar{\mathbb{F}}_p$ .

**Definition 6.1.** We say that the Jacobian  $\mathcal{J}$  of a genus 2 curve is *superspecial* if the Hasse–Witt matrix  $M \in \mathbb{F}_p^{2 \times 2}$  vanishes identically. We say that a Kummer surface  $\mathcal{K} = \mathcal{J}/\{\pm 1\}$  is *superspecial* if the corresponding Jacobian  $\mathcal{J}$  is superspecial.

It can be shown that every superspecial  $\mathcal{J}/\bar{\mathbb{F}}_p$  is  $\bar{\mathbb{F}}_p$ -isomorphic to a Jacobian defined over  $\mathbb{F}_{p^2}$ . Similarly, the corresponding superspecial Kummer surface  $\mathcal{K}/\bar{\mathbb{F}}_p$  is  $\bar{\mathbb{F}}_p$ -isomorphic to a Kummer surface with model defined over  $\mathbb{F}_{p^2}$ .

As an application to exhibit our algorithms, we construct a fundamental cryptographic primitive: a hash function. The first isogeny-based hash function was introduced by Charles, Goren and Lauter who use isogenies between supersingular elliptic curves [\[14\]](#). The use of higher dimensional isogenies between superspecial Jacobians of genus-2 curves to construct a variant of the Charles–Goren–Lauter (CGL) hash function was previously explored by Castryck, Decru and Smith [\[13\]](#) using (2, 2)-isogenies. They argue that although the computation of higher dimensional isogenies is more expensive, breaking the security of the hash function requires  $\tilde{O}(p^{3/2})$  time, rather than  $\tilde{O}(p^{1/2})$  time as in the CGL hash function. Therefore, smaller parameters can be used to obtain the same security. Following this, Castryck and Decru [\[12\]](#) use multiradical formulae for (3, 3)-isogenies to construct such a hash function and obtain an asymptotic speed-up of around a factor of 9. Later work by Decru and Kunzweiler [\[24\]](#) construct a hash function using (3, 3)-isogenies between general Kummer surfaces by improving on the formulae given by Bruin, Flynn and Testa [\[9\]](#).

In this section, we describe a variant of the CGL hash function [\[14\]](#), called **KuHash**, that uses the formulae introduced in [Section 4](#) to compute chains of (3, 3)-isogenies between fast Kummer surfaces. We obtain a speed-up of around  $8 - 9x$ , and around  $32 - 34x$  compared to the Castryck–Decru and Decru–Kunzweiler hash functions, respectively, for security levels  $\lambda = 128, 192$  and  $256$ .

**6.1. Chains of (3, 3)-isogenies.** We first present the **Isogeny33Chain** routine ([Algorithm 2](#)) for computing chains of (3, 3)-isogenies. Though we use it as a building

block for a hash function, we note that it can also be used in a variety of cryptographic applications. In particular, we have been careful to ensure that each component of the algorithm is amenable to constant-time cryptographic software.

*Tripling algorithm.* We start by presenting TPL (Algorithm 1), the algorithm to compute  $[3]P$  from a point  $P \in \mathcal{K}$  and the associated tripling constants (as defined in Section 4.3). This algorithm requires 26M, 12S and 32a.

---

**Algorithm 1** TPL( $P, \text{TC}$ ):

---

**Input:** Point  $P \in \mathcal{K}$  and tripling constants  $\text{TC}$  (with  $i$ -th entry denoted  $\text{TC}_i$ )

**Output:** Point  $Q \in \mathcal{K}$  where  $Q = [3]P$ .

```

1:  $R \leftarrow \mathcal{S}(P)$ 
2:  $R \leftarrow \mathcal{H}(R)$ 
3:  $Q \leftarrow \mathcal{S}(R)$ 
4:  $Q \leftarrow \mathcal{C}_{\text{TC}_5}(Q)$ 
5:  $Q \leftarrow \mathcal{H}(Q)$ 
6:  $Q \leftarrow \mathcal{C}_{\text{TC}_4}(Q)$ 
7:  $Q \leftarrow \mathcal{S}(Q)$ 
8:  $Q \leftarrow \mathcal{H}(Q)$ 
9:  $S \leftarrow \mathcal{C}_{\text{TC}_5}(R)$ 
10:  $Q \leftarrow \mathcal{C}_S(Q)$ 
11:  $Q \leftarrow \mathcal{H}(Q)$ 
12:  $Q \leftarrow \mathcal{C}_{\mathcal{I}(P)}(Q)$ 
13: return  $Q$ 

```

---

*Naïve strategies.* Given a  $(3^k, 3^k)$ -subgroup  $G = \langle R, S \rangle \subset \mathcal{K}[3^k]$ , we use TPL and the algorithms from Section 4.3 to compute an isogeny with kernel  $\langle R, S \rangle$  as a chain of  $(3, 3)$ -isogenies of length  $k$ . A naïve way of doing so is the following. Set  $P_0 := R$ ,  $Q_0 := S$  and  $\mathcal{K}_0 := \mathcal{K}$ , and then execute the following four steps for  $i = 1$  to  $k$ :

- (1) Compute the tripling constants on  $\mathcal{K}_{i-1}$  using `TriplingConstantsFromThetas`
- (2) Compute 3-torsion points  $(P_i, Q_i) := (3^{k-i}R, 3^{k-i}S)$  using  $k - i$  repeated applications of TPL on  $R$  and  $S$ .
- (3) Compute the  $(3, 3)$ -isogeny  $\varphi_i : \mathcal{K}_{i-1} \rightarrow \mathcal{K}_i$  with kernel  $\langle P_i, Q_i \rangle$ , and the images of  $P_{i-1}, Q_{i-1}$  under this isogeny using `Compute33Coefficients` and `Isogeny33Evaluate`.
- (4) Compute the theta constants of the image  $\mathcal{K}_i$  of  $\varphi_i$  using `ComputeImageThetas`.

The  $(3^k, 3^k)$ -isogeny with kernel  $G$  will be given by  $\varphi_k \circ \dots \circ \varphi_1 : \mathcal{K}_0 \rightarrow \mathcal{K}_k$ .

*Optimal strategies.* A more efficient way to compute isogeny chains is to use *optimal strategies* [23]. This allow us to reduce the number of executions of TPL needed to compute the kernel at each step in the chain by storing intermediate points obtained during the triplings and pushing them through each isogeny. In our case, the cost of tripling is around 1.1x the cost of computing the image of a point under the isogeny, and so we shift the cost in this way to obtain the strategies (see [23] for further details on optimising this approach). We give this algorithm in detail in Algorithm 2, and note that invoking the optimal strategies results in a 3.7–6.6x

reduction of the cost to compute a chain of  $(3, 3)$ -isogenies for the set of parameters we specify in [Section 6.3](#).

---

**Algorithm 2** `Isogeny33Chain( $k, \mathcal{O}_{\mathcal{K}}, R, S, \text{strategy}$ ):`

---

**Input:** Fundamental theta constants  $\mathcal{O}_{\mathcal{K}} = (a : b : c : d)$  defining Kummer surface  $\mathcal{K}$ , generators  $R, S \in \mathcal{K}$  of  $(3^k, 3^k)$ -subgroup for  $k \geq 1$ , and optimal strategy `strategy`.

**Output:** Fundamental theta constants defining image Kummer surface  $\mathcal{K}'$  of  $(3^k, 3^k)$ -isogeny  $\varphi : \mathcal{K} \rightarrow \mathcal{K}'$  with  $\ker \varphi = \langle R, S \rangle$ .

```

1: for  $e = k - 1$  to 1 do
2:    $P, Q = R, S$ 
3:    $\text{pts} = []$ 
4:    $\text{inds} = []$ 
5:    $i \leftarrow 0$ 
6:    $\text{TC} \leftarrow \text{TriplingConstantsFromThetas}(\mathcal{O}_{\mathcal{K}})$ 
7:   while  $i < k - e$  do
8:     Append  $[R, S]$  to  $\text{pts}$ 
9:     Append  $i$  to  $\text{inds}$ 
10:     $m \leftarrow \text{strategy}[k - i - e + 1]$ 
11:    for  $j = 1$  to  $m$  do
12:       $R \leftarrow \text{TPL}(R, \text{TC})$ 
13:       $S \leftarrow \text{TPL}(S, \text{TC})$ 
14:       $i \leftarrow i + m$ 
15:     $\text{cs} \leftarrow \text{Compute33Coefficients}(P, Q, \text{TC})$ 
16:     $\mathcal{O}_{\mathcal{K}} \leftarrow \text{ComputingImageThetas}(\text{cs})$ 
17:    for  $[P_1, P_2]$  in  $\text{pts}$  do
18:       $P_1 \leftarrow \text{Isogeny33Evaluate}(P_1, \text{cs})$ 
19:       $P_2 \leftarrow \text{Isogeny33Evaluate}(P_2, \text{cs})$ 
20:    if  $\text{pts}$  not empty then
21:       $[R, S] \leftarrow \text{pts}[-1]$ 
22:       $i \leftarrow \text{inds}[-1]$ 
23:      Remove last element from  $\text{pts}$  and  $\text{inds}$ 
24:     $\text{TC} \leftarrow \text{TriplingConstantsFromThetas}(\mathcal{O}_{\mathcal{K}})$ 
25:     $\text{cs} \leftarrow \text{Compute33Coefficients}(R, S, \text{TC})$ 
26:     $\mathcal{O}_{\mathcal{K}} \leftarrow \text{ComputingImageThetas}(\text{cs})$ 
27: return  $\mathcal{O}_{\mathcal{K}}$ 

```

---

**6.2. A cryptographic hash function.** We are now ready to present the hash function `KuHash` that uses chains of  $(3, 3)$ -isogenies between fast Kummer surfaces. For a fixed security parameter  $\lambda$  and working over characteristic  $p \approx 2^\lambda$ , the hash function parses the message into three scalars  $\alpha, \beta, \gamma \in \mathbb{Z}/3^k\mathbb{Z}$  which are fed into the 3DAC algorithm to compute a  $(3^k, 3^k)$ -subgroup  $G = \langle R, S \rangle$ . This is then used to compute the corresponding  $(3^k, 3^k)$ -isogeny  $\varphi : \mathcal{K} \rightarrow \mathcal{K}'$ , and the output of the hash function is the fundamental theta constants of the image surface  $\mathcal{K}'$ .

To optimise our hash function, we want to ensure that the  $(3^k, 3^k)$ -isogeny is  $\mathbb{F}_{p^2}$ -rational. Given a security parameter  $\lambda$ , we choose a suitably sized prime  $p = 16f \cdot 3^k - 1 \approx 2^\lambda$  (the fact that  $16 \mid p+1$  ensures rational 2-torsion), where  $f$  is a small

cofactor, and take a small pseudo-random walk<sup>3</sup> from the superspecial Jacobian of the curve  $C_0 : y^2 = x^6 + 1$  to arrive at our starting Jacobian  $\mathcal{J} = \text{Jac}(C)$ . Since  $\mathcal{J}(\mathbb{F}_{p^2}) \cong (\mathbb{Z}/(p+1)\mathbb{Z})^4$ , the Rosenhain invariants of  $C$  are all rational in  $\mathbb{F}_{p^2}$  and we use these to compute  $\mathcal{O}_{\mathcal{K}} = (a : b : c : d)$ , i.e. the fundamental theta constants of the starting Kummer surface  $\mathcal{K} = \mathcal{J}/\{\pm 1\}$ . Using the methods described in Section 5.1, we compute a symplectic basis for  $\mathcal{J}[3^k]$ , which (together with the auxiliary sums and differences defined in Section 5.2) is pushed down to our starting fast Kummer surface  $\mathcal{K}$  via  $\pi : \mathcal{J} \rightarrow \mathcal{K}$  to obtain the two tuples of points  $\mathcal{D}_R$  and  $\mathcal{D}_S$ . The setup routine outputs **gens** =  $\{\mathcal{D}_R, \mathcal{D}_S\}$  and **data** =  $\{k, \lceil \lambda/\log(3) \rceil, \mathcal{O}_{\mathcal{K}}\}$ .

The hash function takes as input **data**, **gens** and a message<sup>4</sup> **msg** =  $(\alpha, \beta, \gamma)$ , where  $\alpha, \beta, \gamma \in \mathbb{Z}/3^k\mathbb{Z}$ , and the output of the hash function is a tuple of elements  $\mathbb{F}_{p^2}$ , namely the fundamental theta constants of the image Kummer surface  $\mathcal{K}'$  under the  $(3^k, 3^k)$ -isogeny defined by scalars  $(\alpha, \beta, \gamma)$ . The output is of size  $8 \log(p)$  without normalising the theta constants  $(a', b', c', d')$ , and of size  $6 \log(p)$  with normalisation  $(a'/d', b'/d', c'/d')$ , which comes at a cost of one inversion and 3M. We fully specify **KuHash** in Algorithm 3.

We remark that, as the message must be parsed into three scalars lying in  $\mathbb{Z}/3^k\mathbb{Z}$ , our hash function requires an input message of length  $3k \log_2(3)$  bits. To allow for arbitrary length messages, after each  $(3^k, 3^k)$ -isogeny is computed, we must sample a new symplectic basis on the image Kummer surface. We can do this efficiently using [36, Alg. 1] (the full version of [35]). However, we emphasize that our main objective in presenting the hash function **KuHash** is to benchmark our algorithm **Isogeny33Chain** for computing chains of  $(3, 3)$ -isogenies against others in the literature. We therefore restrict our implementation and experiments to messages of length  $3k \log_2(3)$ .

---

**Algorithm 3** **KuHash**(**msg**, **data**, **gens**)

---

**Input:** A message **msg**, auxiliary data **data** and generators **gens** of  $\mathcal{K}[3^k]$ .

**Output:** Fundamental theta constants  $(a', b', c', d')$  of image Kummer surface  $\mathcal{K}'$

- 1: Parse **msg** as  $\alpha, \beta, \gamma$ .
  - 2: Parse **data** as  $k, \ell, \mathcal{O}_{\mathcal{K}}$ .
  - 3: Parse **gens** as two sets  $\mathcal{D}_R, \mathcal{D}_S$  (see Section 5.2).
  - 4:  $R \leftarrow \text{3DAC}(\mathcal{D}_R, \alpha, \beta, \ell, \mathcal{O}_{\mathcal{K}})$
  - 5:  $S \leftarrow \text{3DAC}(\mathcal{D}_S, \beta, \gamma, \ell, \mathcal{O}_{\mathcal{K}})$
  - 6:  $(a' : b' : c' : d') \leftarrow \text{Isogeny33Chain}(k, \mathcal{O}_{\mathcal{K}}, R, S)$
  - 7: **return**  $(a', b', c', d')$
- 

**6.3. Implementation.** We implement **KuHash** and give parameters for security levels  $\lambda = 128, 192$ , and 256.

*Security.* Let  $\lambda$  be the security parameter and  $p \approx 2^\lambda$ . We follow the discussion in [13, §7.4] to determine the security of the hash function **KuHash**. In particular, the security of our hash function is not affected by taking  $N = 3$  rather than

---

<sup>3</sup>In our implementation, we used **MAGMA**'s inbuilt Richelot isogeny routine to take 20  $(2, 2)$ -isogenies away from  $C_0$ .

<sup>4</sup>In practice, the input message **msg** to the hash function would be a bit string, which would then be parsed into the scalars  $\alpha, \beta, \gamma$ .

$N = 2$ , and as a result the security of our hash function relies on similar problems, namely [Problem 6.2](#) and [Problem 6.3](#) below.

**Problem 6.2.** *Given two superspecial genus 2 curves  $C_1, C_2$  defined over  $\mathbb{F}_{p^2}$  find a  $(3^k, 3^k)$ -isogeny between  $\text{Jac}(C_1)$  and  $\text{Jac}(C_2)$ .*

**Problem 6.3.** *Given a superspecial genus 2 curve  $C_1$  defined over  $\mathbb{F}_{p^2}$ , find*

- *a curve  $C_2$  and a  $(3^k, 3^k)$ -isogeny  $\text{Jac}(C_1) \rightarrow \text{Jac}(C_2)$ ,*
- *a curve  $C'_2$  and a  $(3^{k'}, 3^{k'})$ -isogeny  $\text{Jac}(C_1) \rightarrow \text{Jac}(C'_2)$ ,*

*such that  $\text{Jac}(C_2)$  and  $\text{Jac}(C'_2)$  are  $\overline{\mathbb{F}}_p$ -isomorphic. Here, we can have  $k = k'$ , but the kernels of the corresponding isogenies must be different.*

Previous works take the general Pollard- $\rho$  attack to be the best classical attack against these problems, which runs in  $\tilde{O}(p^{3/2})$ . We take a more conservative approach and consider the Costello–Smith algorithm [20] to be the best classical attack, which runs in  $\tilde{O}(p)$ . The best quantum attack is based on Grover’s claw-finding algorithm and runs in  $\tilde{O}(p^{1/2})$  [20, Theorem 2].

Considering these attacks, we obtain the following parameters:

- $\lambda = 128$  :  $p = 5 \cdot 2^4 \cdot 3^k - 1$  with  $k = 75$ ;
- $\lambda = 192$  :  $p = 37 \cdot 2^4 \cdot 3^k - 1$  with  $k = 115$ ;
- $\lambda = 256$  :  $p = 11 \cdot 2^4 \cdot 3^k - 1$  with  $k = 154$ .

*Cost Metric.* To benchmark `KuHash`, we count  $\mathbb{F}_p$ -operations. Indeed, our implementation in Python/SageMath will call underlying  $\mathbb{F}_p$ -operations to compute  $\mathbb{F}_{p^2}$ -operations. For simplicity, our cost metric will take  $\mathbf{M} = \mathbf{S}$  and ignore  $\mathbf{a}$ , as additions have only a very minor impact on performance. Note that it is relatively straightforward to convert this cost into a more fine-grained metric (e.g., bit operations, cycle counts, etc.).

*Results.* We ran `KuHash` in SageMath version 10.1 using Python 3.11.1 and record the cost, as per the cost metric above, averaging over 100 random inputs for each prime size. We present the results in [Table 1](#). Taking the  $\mathbb{F}_{p^2}$ -operation count from [24, §3.2] and using our cost metric, the cost of computing the coefficients of Decru and Kunzweiler’s  $(3, 3)$ -isogeny is 6702 (assuming 1  $\mathbb{F}_{p^2}$ -multiplication is equivalent to 3  $\mathbb{F}_p$ -multiplications). We use this to obtain a lower bound on the cost of the Decru–Kunzweiler hash function. Though this is a lower bound, we see in [Table 1](#) that the cost already exceeds the total cost of `KuHash`.

The codebase for the other  $(3, 3)$ -isogeny CGL hash variant by Castryck and Decru [12] uses Gröbner basis calculations, which is not realistic to convert to a fixed number of  $\mathbb{F}_p$ -operations. Therefore, for fair comparison, we ran all three hash functions in `MAGMA V2.25-6` on Intel(R) Core™ i7-1065G7 CPU @ 1.30GHz  $\times$  8 with 15.4 GiB memory, and record the time taken to run the hash functions for the different  $\lambda$  in [Table 1](#). We again average over 100 random inputs for each prime size.

Comparing the time taken per input bit for  $\lambda = 128$  and 256, we observe a speed-up of around 8 – 9x compared to the Castryck–Decru hash function, and around 32 – 34x compared to the Decru–Kunzweiler hash function. For a precise comparison between implementations, however, exact  $\mathbb{F}_p$ -operation counts of the Castryck–Decru and Decru–Kunzweiler hash functions are required. We note that an advantage of the algorithms developed with our approach is that we do not rely

	$\lambda$	Message Length	Cost	Time (s)	Time per input bit (ms)
KuHash	128	$225 \log_2(3)$	177956	0.18	0.50
	192	$345 \log_2(3)$	286636	0.29	0.53
	256	$462 \log_2(3)$	396942	0.53	0.72
[24]	128	$240 \log_2(3)$	$> 536160$	5.99	15.75
	171	$315 \log_2(3)$	$> 703710$	10.16	20.35
	256	$477 \log_2(3)$	$> 1065618$	18.29	24.19
[12]	128	357	-	1.51	4.23
	171	547	-	2.82	5.16
	256	732	-	4.81	6.57

TABLE 1. Comparison of cost using cost metric and time taken to run KuHash and hash functions in [12] and [24]. All results are averaged over 100 runs with random inputs. We remark that the cost of KuHash is the same for all runs because it is uniform.

on in-built functionality and all our algorithms are uniform. Therefore, we are able to give precise  $\mathbb{F}_p$ -operation counts for KuHash.

#### REFERENCES

- [1] Daniel J. Bernstein. *Differential addition chains*. 2006. URL: <http://cr.yp.to/ecdh/diffchain-20060219.pdf>.
- [2] Daniel J. Bernstein, Chitchanok Chuengsatiansup, Tanja Lange, and Peter Schwabe. “Kummer strikes back: new DH speed records”. In: *Advances in Cryptology - ASIACRYPT 2014 - 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014. Proceedings, Part I*. Vol. 8873. Lecture Notes in Computer Science. Springer, Heidelberg, 2014, pp. 317–337. ISBN: 978-3-662-45611-8; 978-3-662-45610-1. DOI: [10.1007/978-3-662-45611-8\\_17](https://doi.org/10.1007/978-3-662-45611-8_17).
- [3] Daniel J. Bernstein, Luca De Feo, Antonin Leroux, and Benjamin Smith. “Faster computation of isogenies of large prime degree”. In: *ANTS XIV—Proceedings of the Fourteenth Algorithmic Number Theory Symposium*. Vol. 4. Open Book Series. Math. Sci. Publ., Berkeley, CA, 2020, pp. 39–55. ISBN: 978-1-935107-08-8; 978-1-935107-07-1. DOI: [10.2140/obs.2020.4.39](https://doi.org/10.2140/obs.2020.4.39).
- [4] Gaëtan Bisson. “Endomorphism rings in cryptography”. PhD thesis. Institut National Polytechnique de Lorraine-INPL; Technische Universiteit Eindhoven, 2011.
- [5] Gaëtan Bisson, Romain Cosset, and Damien Robert. AVIsogenies – a library for computing isogenies between abelian varieties. URL: <http://avisogenies.gforge.inria.fr>. Nov. 2012.

- [6] Joppe W. Bos, Craig Costello, Hüseyin Hisil, and Kristin E. Lauter. “Fast Cryptography in Genus 2”. In: *Journal of Cryptology* 29.1 (2016), pp. 28–60. DOI: [10.1007/S00145-014-9188-7](https://doi.org/10.1007/S00145-014-9188-7).
- [7] Wieb Bosma, John Cannon, and Catherine Playoust. “The Magma algebra system. I. The user language”. In: *Journal of Symbolic Computation* 24.3-4 (1997). Computational algebra and number theory (London, 1993), pp. 235–265. ISSN: 0747-7171,1095-855X. DOI: [10.1006/jsco.1996.0125](https://doi.org/10.1006/jsco.1996.0125).
- [8] Jean-Benoît Bost and Jean-François Mestre. “Moyenne arithmético-géométrique et périodes des courbes de genre 1 et 2”. In: *Gazette des Mathématiciens* 38 (1988), pp. 36–64. ISSN: 0224-8999,2275-0622.
- [9] Nils Bruin, E. Victor Flynn, and Damiano Testa. “Descent via  $(3, 3)$ -isogeny on Jacobians of genus 2 curves”. In: *Acta Arithmetica* 165.3 (2014), pp. 201–223. ISSN: 0065-1036,1730-6264. DOI: [10.4064/aa165-3-1](https://doi.org/10.4064/aa165-3-1).
- [10] David G. Cantor. “Computing in the Jacobian of a hyperelliptic curve”. In: *Mathematics of Computation* 48.177 (1987), pp. 95–101. ISSN: 0025-5718,1088-6842. DOI: [10.2307/2007876](https://doi.org/10.2307/2007876).
- [11] J. W. S. Cassels and E. Victor Flynn. *Prolegomena to a middlebrow arithmetic of curves of genus 2*. Vol. 230. London Mathematical Society Lecture Note Series. Cambridge University Press, Cambridge, 1996, pp. xiv+219. ISBN: 0-521-48370-0. DOI: [10.1017/CB09780511526084](https://doi.org/10.1017/CB09780511526084).
- [12] Wouter Castryck and Thomas Decru. “Multiradical isogenies”. In: *Arithmetic, geometry, cryptography, and coding theory 2021*. Vol. 779. Contemporary Mathematics. Amer. Math. Soc., Providence, RI, 2022, pp. 57–89. ISBN: 978-1-4704-6794-4. DOI: [10.1090/conm/779/15671](https://doi.org/10.1090/conm/779/15671).
- [13] Wouter Castryck, Thomas Decru, and Benjamin Smith. “Hash functions from superspecial genus-2 curves using Richelot isogenies”. In: *Journal of Mathematical Cryptology* 14.1 (2020), pp. 268–292. ISSN: 1862-2976,1862-2984. DOI: [10.1515/jmc-2019-0021](https://doi.org/10.1515/jmc-2019-0021).
- [14] Denis Xavier Charles, Kristin E. Lauter, and Eyal Z. Goren. “Cryptographic Hash Functions from Expander Graphs”. In: *Journal of Cryptology* 22.1 (2009), pp. 93–113. DOI: [10.1007/S00145-007-9002-X](https://doi.org/10.1007/S00145-007-9002-X).
- [15] David V. Chudnovsky and Gregory V. Chudnovsky. “Sequences of numbers generated by addition in formal groups and new primality and factorization tests”. In: *Advances in Applied Mathematics* 7.4 (1986), pp. 385–434.
- [16] Romain Cosset. “Applications des fonctions thêta à la cryptographie sur courbes hyperelliptiques”. PhD thesis. Université Henri Poincaré - Nancy, 2011. URL: <https://theses.hal.science/tel-00642951>.
- [17] Romain Cosset. “Factorization with genus 2 curves”. In: *Mathematics of Computation* 79.270 (2010), pp. 1191–1208. ISSN: 0025-5718,1088-6842. DOI: [10.1090/S0025-5718-09-02295-9](https://doi.org/10.1090/S0025-5718-09-02295-9).
- [18] Romain Cosset and Damien Robert. “Computing  $(\ell, \ell)$ -isogenies in polynomial time on Jacobians of genus 2 curves”. In: *Mathematics of Computation* 84.294 (2015), pp. 1953–1975. ISSN: 0025-5718,1088-6842. DOI: [10.1090/S0025-5718-2014-02899-8](https://doi.org/10.1090/S0025-5718-2014-02899-8).
- [19] Craig Costello and Hüseyin Hisil. “A simple and compact algorithm for SIDH with arbitrary degree isogenies”. In: *Advances in Cryptology—ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7,*



- 2017, *Proceedings, Part II*. Vol. 10625. Lecture Notes in Computer Science. Springer, Cham, 2017, pp. 303–329. ISBN: 978-3-319-70697-9; 978-3-319-70696-2. DOI: [10.1007/978-3-319-70697-9\\_1](https://doi.org/10.1007/978-3-319-70697-9_1).
- [20] Craig Costello and Benjamin Smith. “The supersingular isogeny problem in genus 2 and beyond”. In: *Post-Quantum Cryptography - 11th International Conference, PQCrypto 2020, Paris, France, April 15-17, 2020, Proceedings*. Vol. 12100. Lecture Notes in Computer Science. Springer, Cham, 2020, pp. 151–168. ISBN: 978-3-030-44223-1; 978-3-030-44222-4. DOI: [10.1007/978-3-030-44223-1\\_9](https://doi.org/10.1007/978-3-030-44223-1_9).
- [21] Jean-Marc Couveignes and Tony Ezome. “Computing functions on Jacobians and their quotients”. In: *LMS Journal of Computation and Mathematics* 18.1 (2015), pp. 555–577. ISSN: 1461-1570. DOI: [10.1112/S1461157015000169](https://doi.org/10.1112/S1461157015000169).
- [22] Pierrick Dartois, Luciano Maino, Giacomo Pope, and Damien Robert. *An Algorithmic Approach to (2, 2)-isogenies in the Theta Model and Applications to Isogeny-based Cryptography*. Cryptology ePrint Archive, Paper 2023/1747. 2023. URL: <https://eprint.iacr.org/2023/1747>.
- [23] Luca De Feo, David Jao, and Jérôme Plût. “Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies”. In: *Journal of Mathematical Cryptology* 8.3 (2014), pp. 209–247. DOI: [10.1515/JMC-2012-0015](https://doi.org/10.1515/JMC-2012-0015).
- [24] Thomas Decru and Sabrina Kunzweiler. “Efficient Computation of  $(3^n, 3^n)$ -Isogenies”. In: *AFRICACRYPT 2023*. Vol. 14064. Lecture Notes in Computer Science. Springer, 2023, pp. 53–78.
- [25] Igor V. Dolgachev and David Lehavi. “On isogenous principally polarized abelian surfaces”. In: *Curves and abelian varieties*. Vol. 465. Contemporary Mathematics. Amer. Math. Soc., Providence, RI, 2008, pp. 51–69. ISBN: 978-0-8218-4334-5. DOI: [10.1090/conm/465/09100](https://doi.org/10.1090/conm/465/09100).
- [26] Alina Dudeanu, Dimitar Jetchev, Damien Robert, and Marius Vuille. “Cyclic Isogenies for Abelian Varieties with Real Multiplication”. In: *Moscow Mathematical Journal* 22.4 (2022), pp. 613–655.
- [27] E. Victor Flynn. “Curves of genus 2”. PhD thesis. University of Cambridge, 1989.
- [28] E. Victor Flynn. “Descent via  $(5, 5)$ -isogeny on Jacobians of genus 2 curves”. In: *Journal of Number Theory* 153 (2015), pp. 270–282. ISSN: 0022-314X,1096-1658. DOI: [10.1016/j.jnt.2015.01.018](https://doi.org/10.1016/j.jnt.2015.01.018).
- [29] E. Victor Flynn. “The Jacobian and Formal Group of a Curve of Genus 2 over an Arbitrary Ground Field”. In: *Mathematical Proceedings of the Cambridge Philosophical Society* 107.3 (1990), pp. 425–441. DOI: [10.1017/S0305004100068729](https://doi.org/10.1017/S0305004100068729).
- [30] E. Victor Flynn and Yan Bo Ti. “Genus Two Isogeny Cryptography”. In: *Post-Quantum Cryptography - 10th International Conference, PQCrypto 2019, Chongqing, China, May 8-10, 2019 Revised Selected Papers*. Ed. by Jintai Ding and Rainer Steinwandt. Vol. 11505. Lecture Notes in Computer Science. Springer, 2019, pp. 286–306. DOI: [10.1007/978-3-030-25510-7\\_16](https://doi.org/10.1007/978-3-030-25510-7_16).
- [31] Pierrick Gaudry. “Fast genus 2 arithmetic based on theta functions”. In: *Journal of Mathematical Cryptology* 1.3 (2007), pp. 243–265. ISSN: 1862-2976,1862-2984. DOI: [10.1515/JMC.2007.012](https://doi.org/10.1515/JMC.2007.012).



- [32] David Grant. “Formal groups in genus two”. In: *Journal für die Reine und Angewandte Mathematik* 411 (1990), pp. 96–121. ISSN: 0075-4102,1435-5345. DOI: [10.1515/crll.1990.411.96](https://doi.org/10.1515/crll.1990.411.96).
- [33] Aaron Hutchinson and Koray Karabina. “Constructing multidimensional differential addition chains and their applications”. In: *Journal of Cryptographic Engineering* 9.1 (2019), pp. 1–19. DOI: [10.1007/S13389-017-0177-2](https://doi.org/10.1007/S13389-017-0177-2).
- [34] David Kohel. *Endomorphism rings of elliptic curves over finite fields*. University of California, Berkeley, 1996.
- [35] Sabrina Kunzweiler, Yan Bo Ti, and Charlotte Weitkämper. “Secret Keys in Genus-2 SIDH”. In: *SAC 2021*. Vol. 13203. Lecture Notes in Computer Science. Springer, 2021, pp. 483–507.
- [36] Sabrina Kunzweiler, Yan Bo Ti, and Charlotte Weitkämper. *Secret Keys in Genus-2 SIDH*. Cryptology ePrint Archive, Paper 2021/990. 2021. URL: <https://eprint.iacr.org/2021/990>.
- [37] Hendrik W. Lenstra. “Factoring integers with elliptic curves”. In: *Annals of Mathematics. Second Series* 126.3 (1987), pp. 649–673. ISSN: 0003-486X,1939-8980. DOI: [10.2307/1971363](https://doi.org/10.2307/1971363).
- [38] David Lubicz and Damien Robert. “Arithmetic on abelian and Kummer varieties”. In: *Finite Fields and their Applications* 39 (2016), pp. 130–158. ISSN: 1071-5797,1090-2465. DOI: [10.1016/j.ffa.2016.01.009](https://doi.org/10.1016/j.ffa.2016.01.009).
- [39] David Lubicz and Damien Robert. “Fast change of level and applications to isogenies”. In: *Research in Number Theory* 9.1 (2023), Paper No. 7, 28. ISSN: 2522-0160,2363-9555. DOI: [10.1007/s40993-022-00407-9](https://doi.org/10.1007/s40993-022-00407-9).
- [40] Dustin Moody and Daniel Shumow. “Analogues of Vélú’s formulas for isogenies on alternate models of elliptic curves”. In: *Mathematics of Computation* 85.300 (2016), pp. 1929–1951. ISSN: 0025-5718,1088-6842. DOI: [10.1090/mcom/3036](https://doi.org/10.1090/mcom/3036).
- [41] David Mumford. *Tata lectures on theta. II*. Modern Birkhäuser Classics. Jacobian theta functions and differential equations, With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman and H. Umemura, Reprint of the 1984 original. Birkhäuser Boston, Inc., Boston, MA, 2007, pp. xiv+272. ISBN: 978-0-8176-4569-4; 0-8176-4569-1. DOI: [10.1007/978-0-8176-4578-6](https://doi.org/10.1007/978-0-8176-4578-6).
- [42] Chris Nicholls. “Descent methods and torsion on Jacobians of higher genus curves”. PhD thesis. University of Oxford, 2018.
- [43] Ryo Ohashi. “On the Rosenhain forms of superspecial curves of genus two”. In: *Finite Fields and their Applications* 97 (2024), Paper No. 102445, 25. ISSN: 1071-5797,1090-2465. DOI: [10.1016/j.ffa.2024.102445](https://doi.org/10.1016/j.ffa.2024.102445).
- [44] Srinivasa Rao Subramanya Rao. “Three Dimensional Montgomery Ladder, Differential Point Tripling on Montgomery Curves and Point Quintupling on Weierstrass’ and Edwards Curves”. In: *Progress in Cryptology - AFRICACRYPT 2016 - 8th International Conference on Cryptology in Africa, Fes, Morocco, April 13-15, 2016, Proceedings*. Ed. by David Pointcheval, Abderrahmane Nitaj, and Tajjeeddine Rachidi. Vol. 9646. Lecture Notes in Computer Science. Springer, 2016, pp. 84–106. DOI: [10.1007/978-3-319-31517-1\\_5](https://doi.org/10.1007/978-3-319-31517-1_5).

- [45] Joost Renes. “Computing isogenies between Montgomery curves using the action of  $(0, 0)$ ”. In: *Post-Quantum Cryptography - 9th International Conference, PQCrypto 2018, Fort Lauderdale, FL, USA, April 9-11, 2018, Proceedings*. Vol. 10786. Lecture Notes in Computer Science. Springer, Cham, 2018, pp. 229–247. ISBN: 978-3-319-79063-3; 978-3-319-79062-6. DOI: [10.1007/978-3-319-79063-3\\_1](https://doi.org/10.1007/978-3-319-79063-3_1).
- [46] Joost Renes, Peter Schwabe, Benjamin Smith, and Lejla Batina. “ $\mu$ Kummer: Efficient Hyperelliptic Signatures and Key Exchange on Microcontrollers”. In: *Cryptographic Hardware and Embedded Systems - CHES 2016 - 18th International Conference, Santa Barbara, CA, USA, August 17-19, 2016, Proceedings*. Ed. by Benedikt Gierlichs and Axel Y. Poschmann. Vol. 9813. Lecture Notes in Computer Science. Springer, 2016, pp. 301–320. DOI: [10.1007/978-3-662-53140-2\\_15](https://doi.org/10.1007/978-3-662-53140-2_15).
- [47] Joost Renes and Benjamin Smith. “qDSA: Small and Secure Digital Signatures with Curve-Based Diffie-Hellman Key Pairs”. In: *Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part II*. Ed. by Tsuyoshi Takagi and Thomas Peyrin. Vol. 10625. Lecture Notes in Computer Science. Springer, Cham, 2017, pp. 273–302. DOI: [10.1007/978-3-319-70697-9\\_10](https://doi.org/10.1007/978-3-319-70697-9_10).
- [48] Friedrich Julius Richelot. “De transformatione integralium Abelianorum primi ordinis commentatio. Caput secundum. De computatione integralium Abelianorum primi ordinis”. In: *Journal für die Reine und Angewandte Mathematik* 16 (1837), pp. 285–341. ISSN: 0075-4102,1435-5345. DOI: [10.1515/crll.1837.16.285](https://doi.org/10.1515/crll.1837.16.285).
- [49] Damien Robert. “Efficient algorithms for abelian varieties and their moduli spaces”. PhD thesis. Université de Bordeaux (UB), 2021. URL: <https://hal.science/tel-03498268>.
- [50] Damien Robert. “Theta functions and cryptographic applications”. PhD thesis. Université Henri Poincaré - Nancy, 2010.
- [51] Benjamin Smith. “Computing low-degree isogenies in genus 2 with the Dolgachev-Lehavi method”. In: *Arithmetic, geometry, cryptography and coding theory*. Vol. 574. Contemporary Mathematics. Amer. Math. Soc., Providence, RI, 2012, pp. 159–170. ISBN: 978-0-8218-7572-8. DOI: [10.1090/conm/574/11418](https://doi.org/10.1090/conm/574/11418).
- [52] Benjamin Smith. “Explicit endomorphisms and correspondences”. PhD thesis. The University of Sydney, 2006.
- [53] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.2)*. <https://www.sagemath.org>. 2021.
- [54] Jacques Vêlu. “Isogénies entre courbes elliptiques”. In: *Comptes Rendus Hebdomadaires des Séances de l’Académie des Sciences. Séries A et B* 273 (1971), A238–A241. ISSN: 0151-0509.

APPENDIX A. EXPLICIT (2, 2)-ISOGENIES ON FAST KUMMERS

The 15 unique (2, 2)-subgroups are given by

$$\begin{aligned}
G_{1,2} &:= \{(a : b : c : d), (a : b : -c : -d), (a : -b : c : -d), (a : -b : -c : d)\}, \\
G_{1,4} &:= \{(a : b : c : d), (a : b : -c : -d), (b : a : d : c), (b : a : -d : -c)\}, \\
G_{1,6} &:= \{(a : b : c : d), (a : b : -c : -d), (b : -a : d : -c), (b : -a : -d : c)\}, \\
G_{2,8} &:= \{(a : b : c : d), (a : -b : c : -d), (c : d : a : b), (c : -d : a : -b)\}, \\
G_{2,9} &:= \{(a : b : c : d), (a : -b : c : -d), (c : d : -a : -b), (c : -d : -a : b)\}, \\
G_{3,12} &:= \{(a : b : c : d), (a : -b : -c : d), (d : c : b : a), (d : -c : -b : a)\}, \\
G_{3,14} &:= \{(a : b : c : d), (a : -b : -c : d), (d : c : -b : -a), (d : -c : b : -a)\}, \\
G_{4,8} &:= \{(a : b : c : d), (b : a : d : c), (c : d : a : b), (d : c : b : a)\}, \\
G_{4,9} &:= \{(a : b : c : d), (b : a : d : c), (c : d : -a : -b), (d : c : -b : -a)\}, \\
G_{5,10} &:= \{(a : b : c : d), (b : a : -d : -c), (c : -d : a : -b), (d : -c : -b : a)\}, \\
G_{5,11} &:= \{(a : b : c : d), (b : a : -d : -c), (c : -d : -a : b), (d : -c : b : -a)\}, \\
G_{6,8} &:= \{(a : b : c : d), (b : -a : d : -c), (c : d : a : b), (d : -c : b : -a)\}, \\
G_{6,9} &:= \{(a : b : c : d), (b : -a : d : -c), (c : d : -a : -b), (d : -c : -b : a)\}, \\
G_{7,10} &:= \{(a : b : c : d), (b : -a : -d : c), (c : -d : a : -b), (d : c : -b : -a)\}, \\
G_{7,11} &:= \{(a : b : c : d), (b : -a : -d : c), (c : -d : -a : b), (d : c : b : a)\}.
\end{aligned}$$

For each (2, 2)-subgroup  $G_{i,j}$ , the corresponding (2, 2)-isogeny  $\mathcal{K} \rightarrow \tilde{\mathcal{K}}$  is given by

$$\psi_{i,j} := \mathcal{H} \circ \mathcal{S} \circ \alpha$$

where  $\alpha : \mathcal{K} \rightarrow \mathcal{K}$  is induced by a linear map on  $\mathbb{A}^4$ . If  $i$  is a root of  $x^2 + 1$  in  $\overline{\mathbb{K}}[x]$ , then the maps  $\alpha$  for each (2, 2)-subgroup  $G_{i,j}$  are defined by the following matrices:

$$\begin{aligned}
G_{1,2} &: \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, & G_{1,4} &: \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}, & G_{1,6} &: \begin{pmatrix} 1 & i & 0 & 0 \\ 0 & -i & 0 & 0 \\ 0 & 0 & 1 & i \\ 0 & 0 & 1 & -i \end{pmatrix}, \\
G_{2,8} &: \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \end{pmatrix}, & G_{2,9} &: \begin{pmatrix} 1 & 0 & i & 0 \\ 1 & 0 & -i & 0 \\ 0 & 1 & 0 & i \\ 0 & 1 & 0 & -i \end{pmatrix}, & G_{3,12} &: \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & -1 & 0 \end{pmatrix}, \\
G_{3,14} &: \begin{pmatrix} 1 & 0 & 0 & i \\ 1 & 0 & 0 & -i \\ 0 & 1 & i & 0 \\ 0 & 1 & -i & 0 \end{pmatrix}, & G_{4,8} &: \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}, & G_{4,9} &: \begin{pmatrix} 1 & 1 & i & i \\ 1 & 1 & -i & -i \\ 1 & -1 & i & -i \\ 1 & -1 & -i & i \end{pmatrix}, \\
G_{5,10} &: \begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix}, & G_{5,11} &: \begin{pmatrix} 1 & -1 & -i & -i \\ 1 & -1 & i & i \\ 1 & 1 & -i & i \\ 1 & 1 & i & -i \end{pmatrix}, & G_{6,8} &: \begin{pmatrix} 1 & i & 1 & i \\ 1 & i & -1 & -i \\ 1 & -i & 1 & -i \\ 1 & -i & -1 & i \end{pmatrix}, \\
G_{6,9} &: \begin{pmatrix} 1 & -i & -i & -1 \\ 1 & -i & i & 1 \\ 1 & i & -i & 1 \\ 1 & i & i & -1 \end{pmatrix}, & G_{7,10} &: \begin{pmatrix} 1 & -i & -1 & -i \\ 1 & -i & 1 & i \\ 1 & i & -1 & i \\ 1 & i & 1 & -i \end{pmatrix}, & G_{7,11} &: \begin{pmatrix} 1 & i & i & 1 \\ 1 & i & -i & -1 \\ 1 & -i & i & -1 \\ 1 & -i & -i & 1 \end{pmatrix}.
\end{aligned}$$

APPENDIX B. THREE-DIMENSIONAL ADDITION CHAIN

We describe the three-dimensional addition chain 3DAC needed to compute kernel generators of the form  $P_1 + [\beta]P_2 + [\gamma]P_3$ . We obtained this chain by extending Bernstein's two-dimensional differential addition chain [1], the fastest known chain of this kind that is both fixed length and uniform. 3DAC computes  $P_1 + [\beta]P_2 + [\gamma]P_3$ ,

given scalars  $\beta, \gamma \in \mathbb{Z}/3^k\mathbb{Z}$ , the length  $\ell$  of the chain, the fundamental theta constants  $\mathcal{O}_{\mathcal{K}}$  of a fast Kummer surface  $\mathcal{K}$ , and a tuple of points

$$(7) \quad \mathcal{D} := (P_1, P_2, P_3, P_2 + P_3, P_2 - P_3, P_1 - P_2, P_1 - P_3, [2](P_2 + P_3), \\ P_1 + P_2 + P_3, P_1 - P_2 - P_3)$$

on  $\mathcal{K}$ . 3DAC requires three subroutines: DBLTHRICEADD, ENCODE, and IND. DBLTHRICEADD is defined to compute the mapping

$$(P, Q, P - Q, R, S, R - S, T, U, T - U) \mapsto ([2]P, P + Q, R + S, T + U)$$

for points  $P, Q, R, S, T$ , and  $U$  in  $\mathcal{K}$ , using one pseudo-doubling and three pseudo-additions on  $\mathcal{K}$ .

ENCODE takes two  $\ell$ -bit scalars  $\beta, \gamma \in \mathbb{Z}/3^k\mathbb{Z}$  and outputs a single bit  $\mathbf{b}$  and four  $(\ell - 1)$ -bit scalars  $b_i$  for  $i = 0, 1, 2, 3$ . The bit  $\mathbf{b}$  selects the input for the differential addition that kickstarts the chain (see Step 5 of Algorithm 6), after which the  $j$ -th bits (for  $j = 1, \dots, \ell$ ) of each of the four  $b_i$  determine one of 16 input permutations that is fed into the DBLTHRICEADD routine (see Step 10 of Algorithm 6).

---

**Algorithm 4** ENCODE( $\beta, \gamma$ ):

---

**Input:** two  $\ell$ -bit scalars  $\beta = (\beta[\ell - 1], \dots, \beta[0])$  and  $\gamma = (\gamma[\ell - 1], \dots, \gamma[0])$

**Output:** a bit  $\mathbf{b} \in \{0, 1\}$ , and four  $(\ell - 1)$ -bit scalars  $(b_0, b_1, b_2, b_3)$

```

1:  $\mathbf{b} \leftarrow \beta[1]$ 
2: for  $i = 1$  to  $\ell - 1$  do
3:    $b_1[i] \leftarrow \beta[i] \oplus \beta[i + 1]$ 
4:    $b_0[i] \leftarrow b_1[i] \oplus \gamma[i] \oplus \gamma[i + 1]$ 
5:    $b_2[i] \leftarrow \beta[i + 1] \oplus \gamma[i + 1]$ 
6:    $b_3[i] \leftarrow \mathbf{b}$ 
7:    $\mathbf{b} \leftarrow b_1[i] \oplus (b_0[i] \oplus 1) \otimes \mathbf{b}$ 
8: return  $\mathbf{b}, (b_0, b_1, b_2, b_3)$ 

```

---

The indexing algorithm IND is used to choose one of four points as the last input to the DBLTHRICEADD algorithm.

---

**Algorithm 5** IND( $I$ ):

---

**Input:** a 6-tuple of integers  $I = (I_1, \dots, I_6)$

**Output:** an integer index  $\text{ind} \in \{1, 2, 3, 4\}$

```

1: switch  $([I_3 - I_1, I_4 - I_2])$ 
2: case  $[-1, -1]$ :  $\text{ind} \leftarrow 1$ 
3: case  $[1, 1]$ :  $\text{ind} \leftarrow 2$ 
4: case  $[1, -1]$ :  $\text{ind} \leftarrow 3$ 
5: case  $[-1, 1]$ :  $\text{ind} \leftarrow 4$ 
6: end switch
7: return  $\text{ind}$ 

```

---

---

**Algorithm 6** 3DAC( $\mathcal{D}, \beta, \gamma, \ell, \mathcal{O}_K$ ):

---

**Input:** Scalars  $\beta, \gamma \in \mathbb{Z}/3^k\mathbb{Z}$ , the length of chain  $\ell$ , fundamental theta constants  $\mathcal{O}_K$ , and a tuple  $\mathcal{D}$  of points on  $\mathcal{K}$  as in Eq. (7).

**Output:**  $P_1 + [\beta]P_2 + [\gamma]P_3$  where  $P_1, P_2, P_3$  are  $\mathcal{D}_1, \mathcal{D}_2, \mathcal{D}_3$ , respectively.

```
1: initialise  $P \leftarrow (\mathcal{D}_4, \mathcal{D}_8, \mathcal{D}_4, \mathcal{D}_9)$ 
2: initialise  $D \leftarrow (\mathcal{D}_2, \mathcal{D}_3, \mathcal{D}_4, \mathcal{D}_5)$ 
3: initialise  $\Delta \leftarrow (\mathcal{D}_1, \mathcal{D}_{10}, \mathcal{D}_6, \mathcal{D}_7)$ 
4: initialise  $I \leftarrow (1, 1, 2, 2, 1, 1)$ 
5:  $\mathbf{b}, (b_0, b_1, b_2, b_3) \leftarrow \text{ENCODE}(\beta, \gamma)$ 
6: if  $\mathbf{b} = 1$  then
7:    $(P_3, I_6) \leftarrow ((P_3, D_2, D_1), I_6 + 1)$ 
8: else
9:    $(P_3, I_5) \leftarrow ((P_3, D_1, D_2), I_5 + 1)$ 
10: switch  $((b_0, b_1, b_2, b_3))$ 
11: case  $(0, 0, 0, 0)$ :  $I \leftarrow (I_1 + I_3, I_2 + I_4, 2I_3, 2I_4, I_3 + I_5, I_4 + I_6)$ 
    $(P_2, P_1, P_3, P_4) \leftarrow \text{DBLTHRICEADD}(P_2, P_1, D_3, P_3, P_2, D_2, P_2, P_4, \Delta_{\text{IND}(I)})$ 
12: case  $(0, 0, 0, 1)$ :  $I \leftarrow (I_1 + I_3, I_2 + I_4, 2I_3, 2I_4, I_3 + I_5, I_4 + I_6)$ 
    $(P_2, P_1, P_3, P_4) \leftarrow \text{DBLTHRICEADD}(P_2, P_1, D_3, P_3, P_2, D_1, P_2, P_4, \Delta_{\text{IND}(I)})$ 
13: case  $(0, 0, 1, 0)$ :  $I \leftarrow (I_1 + I_3, I_2 + I_4, 2I_3, 2I_4, I_3 + I_5, I_4 + I_6)$ 
    $(P_2, P_1, P_3, P_4) \leftarrow \text{DBLTHRICEADD}(P_2, P_1, D_4, P_3, P_2, D_2, P_2, P_4, \Delta_{\text{IND}(I)})$ 
14: case  $(0, 0, 1, 1)$ :  $I \leftarrow (I_1 + I_3, I_2 + I_4, 2I_3, 2I_4, I_3 + I_5, I_4 + I_6)$ 
    $(P_2, P_1, P_3, P_4) \leftarrow \text{DBLTHRICEADD}(P_2, P_1, D_4, P_3, P_2, D_1, P_2, P_4, \Delta_{\text{IND}(I)})$ 
15: case  $(0, 1, 0, 0)$ :  $I \leftarrow (I_1 + I_3, I_2 + I_4, 2I_1, 2I_2, I_1 + I_5, I_2 + I_6)$ 
    $(P_2, P_1, P_3, P_4) \leftarrow \text{DBLTHRICEADD}(P_1, P_2, D_3, P_3, P_1, D_2, P_1, P_4, \Delta_{\text{IND}(I)})$ 
16: case  $(0, 1, 0, 1)$ :  $I \leftarrow (I_1 + I_3, I_2 + I_4, 2I_1, 2I_2, I_1 + I_5, I_2 + I_6)$ 
    $(P_2, P_1, P_3, P_4) \leftarrow \text{DBLTHRICEADD}(P_1, P_2, D_3, P_3, P_1, D_1, P_1, P_4, \Delta_{\text{IND}(I)})$ 
17: case  $(0, 1, 1, 0)$ :  $I \leftarrow (I_1 + I_3, I_2 + I_4, 2I_1, 2I_2, I_1 + I_5, I_2 + I_6)$ 
    $(P_2, P_1, P_3, P_4) \leftarrow \text{DBLTHRICEADD}(P_1, P_2, D_4, P_3, P_1, D_2, P_1, P_4, \Delta_{\text{IND}(I)})$ 
18: case  $(0, 1, 1, 1)$ :  $I \leftarrow (I_1 + I_3, I_2 + I_4, 2I_1, 2I_2, I_1 + I_5, I_2 + I_6)$ 
    $(P_2, P_1, P_3, P_4) \leftarrow \text{DBLTHRICEADD}(P_1, P_2, D_4, P_3, P_1, D_1, P_1, P_4, \Delta_{\text{IND}(I)})$ 
19: case  $(1, 0, 0, 0)$ :  $I \leftarrow (I_1 + I_3, I_2 + I_4, 2I_5, 2I_6, I_3 + I_5, I_4 + I_6)$ 
    $(P_2, P_3, P_1, P_4) \leftarrow \text{DBLTHRICEADD}(P_3, P_2, D_2, P_1, P_2, D_3, P_3, P_4, \Delta_{\text{IND}(I)})$ 
20: case  $(1, 0, 0, 1)$ :  $I \leftarrow (I_1 + I_3, I_2 + I_4, 2I_5, 2I_6, I_1 + I_5, I_2 + I_6)$ 
    $(P_2, P_3, P_1, P_4) \leftarrow \text{DBLTHRICEADD}(P_3, P_1, D_1, P_1, P_2, D_3, P_3, P_4, \Delta_{\text{IND}(I)})$ 
21: case  $(1, 0, 1, 0)$ :  $I \leftarrow (I_1 + I_3, I_2 + I_4, 2I_5, 2I_6, I_3 + I_5, I_4 + I_6)$ 
    $(P_2, P_3, P_1, P_4) \leftarrow \text{DBLTHRICEADD}(P_3, P_2, D_2, P_1, P_2, D_4, P_3, P_4, \Delta_{\text{IND}(I)})$ 
22: case  $(1, 0, 1, 1)$ :  $I \leftarrow (I_1 + I_3, I_2 + I_4, 2I_5, 2I_6, I_1 + I_5, I_2 + I_6)$ 
    $(P_2, P_3, P_1, P_4) \leftarrow \text{DBLTHRICEADD}(P_3, P_1, D_1, P_1, P_2, D_4, P_3, P_4, \Delta_{\text{IND}(I)})$ 
23: case  $(1, 1, 0, 0)$ :  $I \leftarrow (I_1 + I_3, I_2 + I_4, 2I_5, 2I_6, I_1 + I_5, I_2 + I_6)$ 
    $(P_2, P_3, P_1, P_4) \leftarrow \text{DBLTHRICEADD}(P_3, P_1, D_2, P_1, P_2, D_3, P_3, P_4, \Delta_{\text{IND}(I)})$ 
24: case  $(1, 1, 0, 1)$ :  $I \leftarrow (I_1 + I_3, I_2 + I_4, 2I_5, 2I_6, I_3 + I_5, I_4 + I_6)$ 
    $(P_2, P_3, P_1, P_4) \leftarrow \text{DBLTHRICEADD}(P_3, P_2, D_1, P_1, P_2, D_3, P_3, P_4, \Delta_{\text{IND}(I)})$ 
25: case  $(1, 1, 1, 0)$ :  $I \leftarrow (I_1 + I_3, I_2 + I_4, 2I_5, 2I_6, I_1 + I_5, I_2 + I_6)$ 
    $(P_2, P_3, P_1, P_4) \leftarrow \text{DBLTHRICEADD}(P_3, P_1, D_2, P_1, P_2, D_4, P_3, P_4, \Delta_{\text{IND}(I)})$ 
26: case  $(1, 1, 1, 1)$ :  $I \leftarrow (I_1 + I_3, I_2 + I_4, 2I_5, 2I_6, I_3 + I_5, I_4 + I_6)$ 
    $(P_2, P_3, P_1, P_4) \leftarrow \text{DBLTHRICEADD}(P_3, P_2, D_1, P_1, P_2, D_4, P_3, P_4, \Delta_{\text{IND}(I)})$ 
27: end switch
28: return  $P_4$ 
```

---

UNIVERSITY COLLEGE LONDON, UK  
*Email address:* `maria.santos.20@ucl.ac.uk`

MICROSOFT RESEARCH, USA  
*Email address:* `craigco@microsoft.com`

INRIA AND ÉCOLE POLYTECHNIQUE, INSTITUT POLYTECHNIQUE DE PARIS, PALAISEAU, FRANCE  
*Email address:* `smith@lix.polytechnique.fr`