Computing isogenies between Jacobian of curves of genus 2 and 3

Enea Milio

Computing isogenies between Jacobian of curves of genus 2 and 3

Enea Milio

Contents

1 Introduction **2**

2 Evaluation of the η and η_X functions **3**
2.1 Definitions 3
2.2 Evaluation of $\eta[\mathfrak{u}, y]$ 4
2.3 Evaluation of $\eta_X[\mathfrak{u}, y]$ 6

3 Computation of the equation of the curve in the hyperelliptic case **7**
3.1 Kummer variety 7
3.2 Computing the equation of the isogenous curve in genus 2 10
3.3 Computing the equation of the isogenous curve in genus 3 if $\mathcal{D}$ is hyperelliptic . 13

4 Computing equations for the isogeny **14**
4.1 Rational fractions describing the isogeny 14
4.2 Computing the rational fractions from the image of a single formal point 15
4.3 Computing the image of a formal point 16
4.4 Example for hyperelliptic curves of genus 3 18

5 Algebraic theta functions **19**
5.1 Analytic theta functions 20
5.2 Rosenhain invariants 21
5.3 Non-hyperelliptic curves of genus 3 23

6 Implementation **25**

Abstract

We present a quasi-linear algorithm to compute isogenies between Jacobians of curves of genus 2 and 3 starting from the equation of the curve and a maximal isotropic subgroup of the ℓ-torsion, for ℓ an odd prime number, generalizing the Vélu's formula of genus 1. This work is based from the paper *Computing functions on Jacobians and their quotients* of Jean-Marc Couveignes and Tony Ezome. We improve their genus 2 case algorithm, generalize it for genus 3 hyperelliptic curves and introduce a way to deal with the genus 3 non-hyperelliptic case, using algebraic theta functions.

1 Introduction

Starting from a projective, smooth, absolutely integral curve $\mathcal{C}$ of genus $g \in \{2, 3\}$ on a finite field K and a maximal isotropic subgroup $\mathcal{V}$ of the ℓ-torsion of the Jacobian $J_{\mathcal{C}}$ of $\mathcal{C}$, we want to compute the equation of the $(\ell, \ldots, \ell)$-isogenous curve $\mathcal{D}$ such that $J_{\mathcal{D}} = J_{\mathcal{C}}/\mathcal{V}$, if it exists, and equations for the isogeny. The computation of $\mathcal{V}$ is a different problem that we do not treat here. We take it as an input of our algorithms.

In genus $g = 1$, this problem is solved by Vélu's formula [32]. Let E be an elliptic curve and G be a finite subgroup of cardinality a prime number ℓ of the elliptic curve $E' = E/G$. A point P of E is sent by the isogeny $f : E \to E'$ to the point

$$x(f(P)) = x(P) + \sum_{Q \in G \setminus \{0\}} x(P+Q) - x(Q), \quad y(f(P)) = y(P) + \sum_{Q \in G \setminus \{0\}} y(P+Q) - y(Q).$$

Then, using the addition formula, it is possible to obtain the equation of E' in the Weierstrass form and a rational fraction F such that the isogeny is $f : (x, y) \in E \mapsto (F(x), cyF'(x)) \in E'$, for some $c \in K$. See also [4, Section 4.1].

For $g \geq 2$, a first generalization has been done in [9, 19, 20]. The authors explains how to compute separable isogenies between principally polarized abelian varieties A and $A/\mathcal{V}$ of dimension g with a complexity of $\tilde{O}(\ell^{\frac{rg}{2}})$ operations in K, where $r = 2$ if the odd prime number ℓ, different from the characteristic of K, is a sum of two squares and $r = 4$ otherwise. For the former, the complexity is quasi-optimal since it is quasi-linear in ℓ^g, the degree of the isogeny (the cardinality of the maximal isotropic subgroup $\mathcal{V}$ of $A[\ell]$). Here, the abelian varieties are represented through their theta null points. A magma package, AVIsogenies [2], implementing the ideas of these papers is available but the implementation concerns only the dimension 2 case, that is generically, the Jacobian of hyperelliptic curves of genus 2.

Note that for $g = 2$ and $\ell = 2$, the isogenies between Jacobian of hyperelliptic curves can be computed using the Richelot construction (see [7, Chapter 9]). For $\ell = 3$, an algebraic-geometric approach has been introduced by Dolgachev and Lehavi (see [12, 29]). For $g = 3$ and $\ell = 2$, there exists an algorithm [28] computing $(2, 2, 2)$-isogenies from the Jacobian of a hyperelliptic curve of genus 3 over a finite field of characteristic > 3, using Recillas' trigonal construction.

Another generalization, which is the starting point of the present paper, has been introduced in [10]. In this paper, its authors explain how to define and compute functions, from zero-cycles, on $J_{\mathcal{C}}$ and on $J_{\mathcal{C}}/\mathcal{V}$ for any genus $g \geq 2$ and for any field of characteristic p different of $\ell \neq 2$ and 2. We call them η and η_X functions respectively and in both cases, computations are done in $J_{\mathcal{C}}$. After that, they focus on the genus 2 case for finite fields of cardinality q. The computation of the equation of $\mathcal{D}$ is done starting from an embedding using η_X functions from $J_{\mathcal{C}}$ to the Kummer surface of $J_{\mathcal{D}} = J_{\mathcal{C}}/\mathcal{V}$ viewed in $\mathbb{P}^3$ and doing a parameterization using the geometry of the Kummer surface. We will give more details about this. Finally they explain how to describe the isogeny in a compact form through rational fractions of degrees in $O(\ell)$. This form is related to the Mumford representation of the points of the Jacobian and the computation use a system of differential equations. The resulting algorithm is quasi-linear in the degree ℓ^2.

In this paper, we recall in Section 2 the definition of the η and η_X functions and how to evaluate them. These functions are seen as building blocks and we try to reduce as much as possible the number of times we evaluate them. Then in Section 3, we first describe the

particular geometry of Kummer varieties, which admit a (m, n)-configuration when seen in $\mathbb{P}^{2^g-1}$, that is a set of m hyperplanes (the tropes) and m points (the image in $\mathbb{P}^{2^g-1}$ of the 2-torsion points) such that each hyperplane contains n of the m points and each of these points is contained in exactly m hyperplanes. Then in the genus 2 case, we use the $(16, 6)$-configuration to compute the equation of $\mathcal{D}$ and explain how to optimize this computation. We prove that the knowledge of the equation of the quartic describing the Kummer surface is not necessary and use only 11 evaluations of η_X functions. We then turn to genus 3. Here the curves are either hyperelliptic or non-hyperelliptic (in which case they can be viewed as plane quartics). These two cases have to be treated differently. We describe how the genus 2 method can be naturally generalized in the case where $\mathcal{D}$ is hyperelliptic, using the $(64, 29)$-configuration of the Kummer threefold. We focus on genus 3 but it is clear that similar results exists for $g > 3$. In Section 4, we recall the definition of the rational fractions we want to describe the isogeny and how to compute them following [10] except for one step which is not practical. Indeed, this step require the computation of many algebraic equations between the 9 functions forming a basis of $H^0(J_{\mathcal{C}}/\mathcal{V}, \mathcal{O}_{J_{\mathcal{C}}/\mathcal{V}}(3Y))$, where Y is a principal polarization of $J_{\mathcal{C}}/\mathcal{V}$. And such a basis is computed through a probabilistic Las Vegas algorithm, requiring the field K to be finite. We give another solution based on a good model of the Kummer surface allowing one to compute the pseudo-addition law and to lift a point of the Kummer to the Jacobian. We generalize all these results in the genus 3 case. In Section 5, we construct algebraic theta functions as functions satisfying the same algebraic relations between the analytic theta functions. We use these algebraic theta functions to compute the equation of $\mathcal{D}$ in genus 2 through the description of its Rosenhain form by theta constants. Then we focus on the generic genus 3 case where $\mathcal{D}$ is non-hyperelliptic. We use theta based formulas coming from the theory of the reconstruction of a plane quartic from its bitangents. Finally, in Section 6, we speak about our implementation.

2 Evaluation of the η and η_X functions

In this section, we recall the definition of the η and η_X functions of [10]. We use the same notations of this paper and refer to it for more details.

2.1 Definitions

This is [10, Section 2.1]. Let $\mathcal{C}$ be a projective, smooth, absolutely integral curve over a field K and of genus $g \geq 2$. We denote by $\mathrm{Pic}(\mathcal{C})$ its Picard group, $\mathrm{Pic}^d(\mathcal{C})$ the component of the Picard group of linear equivalence classes of divisors of degree d and $J := J_{\mathcal{C}} := \mathrm{Pic}^0(\mathcal{C})$ the Jacobian variety of $\mathcal{C}$. If D is a divisor on $\mathcal{C}$, then we denote by $\iota(D)$ its linear equivalence class.

Let $W \subset \mathrm{Pic}^{g-1}(\mathcal{C})$ be the algebraic set representing classes of effectives divisors of degree $g-1$. The *theta characteristics* are the K-rational points θ in $\mathrm{Pic}^{g-1}(\mathcal{C})$ such that $2\theta = \omega$, where ω designes the canonical divisor class. They differ by a 2-torsion point in J. The translate $W_{-\theta}$ of W by θ is a divisor on J. If D is any effective divisor of $\mathcal{C}$ of degree $g-1$, then, by the Riemann-Roch theorem on effectives divisors, $\ell(D) = \ell(\Omega - D) \geq 1$, with Ω a divisor in the linear class of ω (see [15, Chapter 2.3, Pages 244–245]). This implies that $[-1]^*W = W_{-\omega}$ and we deduce from it that

$$[-1]^*W_{-\theta} = W_{-\theta}. \tag{1}$$

The latter is said to be a *symmetric* divisor on J.

Consider now any K-point O on $\mathcal{C}$, whose linear equivalence class is $o = \iota(O)$ in $\mathrm{Pic}^1(\mathcal{C})$. The translate $W_{-(g-1)o}$ of W by $-(g-1)o$ is a divisor on J but not necessarily a symmetric one. Taking $\vartheta = \theta - (g-1)o \in J(K)$ we can construct a symmetric divisor:

$$[-1]^* W_{-(g-1)o-\vartheta} = W_{-(g-1)o-\vartheta}. \tag{2}$$

Let I be a positive integer, $e_1, \ldots, e_I \in \mathbb{Z}$ and $u_1, \ldots, u_I \in J(\bar{K})$. The formal sum $\mathfrak{u} = \sum_{1 \le i \le I} e_i [u_i]$ is a zero-cycle on $J_{\bar{K}}$. Define the *sum* and *degree* functions of a zero-cycle by

$$s(\mathfrak{u}) = \sum_{1 \le i \le I} e_i u_i \in J(\bar{K}) \qquad \text{and} \qquad \deg(\mathfrak{u}) = \sum_{1 \le i \le I} e_i \in \mathbb{Z}. \tag{3}$$

Let D be a divisor on $J_{\bar{K}}$. The divisor $\sum_{1 \le i \le I} e_i D_{u_i} - D_{s(\mathfrak{u})} - (\deg(\mathfrak{u}) - 1)D$ is principal ([17, Chapter III, Section 3, Corollary 1]) so it defines a function up to a multiplicative constant. To fix this constant, we choose a point $y \in J(\bar{K})$ such that the value of the function is 1 at y. This implies that we want y not to be in the support of this divisor. This unique function is denoted by $\eta_D[\mathfrak{u}, y]$. To resume, it satisfies

$$(\eta_D[\mathfrak{u}, y]) = \sum_{1 \le i \le I} e_i D_{u_i} - D_{s(\mathfrak{u})} - (\deg(\mathfrak{u}) - 1)D \qquad \text{and} \qquad \eta_D[\mathfrak{u}, y](y) = 1. \tag{4}$$

We will sometimes denote by $\eta_D[\mathfrak{u}]$ the function defined up to a multiplicative constant. Moreover, this function satisfies the following additive property, which can be proved in comparing divisors

$$\eta_D[\mathfrak{u} + \mathfrak{v}, y] = \eta_D[\mathfrak{u}, y] \cdot \eta_D[\mathfrak{v}, y] \cdot \eta_D[[s(\mathfrak{u})] + [s(\mathfrak{v})], y]. \tag{5}$$

For ours applications, we are mainly interested in the cases where $D = W_{-(g-1)o}$ or $D = W_{-(g-1)o-\vartheta} = W_{-\theta}$. Note that we have

$$\eta_{W_{-\theta}}[\mathfrak{u}, y](x) = \eta_{W_{-(g-1)o}}[\mathfrak{u}, y + \vartheta](x + \vartheta) \tag{6}$$

so that we will focus on the first divisor; and to simplify the notations, we write $\eta[\mathfrak{u}, y]$ instead of $\eta_{W_{-(g-1)o}}[\mathfrak{u}, y]$.

2.2 Evaluation of $\eta[\mathfrak{u}, y]$

Fix $\mathfrak{u}$ a zero-cycle on J with $u_i \in J(K)$ for $1 \le i \le I$, $y \in J(K)$ not in the support of $\eta[\mathfrak{u}]$ and $x \in J(K)$ not in the support of $\eta[\mathfrak{u}, y]$. Assume that $x = \iota(D_x - gO)$ and $y = \iota(D_y - gO)$ where D_x and D_y are effectives divisors of degree g not having O in their support (this is the generic case). Write $D_x = X_1 + \ldots + X_g$ and $D_y = Y_1 + \ldots + Y_g$. This writing is unique (see [11, Section 2.6]). Make also the assumption that $\deg(\mathfrak{u}) = 0 \in \mathbb{Z}$ and $s(\mathfrak{u}) = 0 \in J(K)$. This is not a restriction because if $\mathfrak{u}$ does not satisfy these properties, then the zero-cycle $\mathfrak{u}' = \mathfrak{u} - [s(\mathfrak{u})] - (\deg(\mathfrak{u}) - 1)[0]$ does and the functions $\eta[\mathfrak{u}]$ and $\eta[\mathfrak{u}']$ have the same divisor.

The computation of $\eta[\mathfrak{u}, y](x)$ goes as follows. See [10, Section 2] for the details.

1. For every $1 \le i \le I$, find an effective divisor $D^{(i)}$ of degree $2g-1$ such that $D^{(i)}$ does neither meet D_x or D_y and $\iota(D^{(i)}) - \omega - o$ is the class u_i. Taking $U_i - gO$ in the class of u_i, where U_i is effective of degree g, and taking a canonical divisor Ω on $\mathcal{C}$, the divisor $D^{(i)}$ can be found looking at the Riemann-Roch space $\mathcal{L}(U_i - (g-1)O + \Omega)$. The condition on the degree of $D^{(i)}$ and the Riemann-Roch theorem say that $\ell(D^{(i)}) = g$.

2. Find a non-zero function h in $K(\mathcal{C})$ with divisor $\sum_{1\leq i\leq I} e_i D^{(i)}$. This function exists thanks to the conditions on the zero-cycle.

3. For every $1 \leq i \leq I$, compute a basis $f^{(i)} = (f_k^{(i)})_{1\leq k\leq g}$ of $\mathcal{L}(D^{(i)})$. This step and the previous one are effectives Riemann-Roch theorem.

4. Compute $\delta_x^{(i)} = \det(f_k^{(i)}(X_j))_{1\leq k,j\leq g}$ and $\delta_y^{(i)} = \det(f_k^{(i)}(Y_j))_{1\leq k,j\leq g}$.

5. Compute $\alpha[h](x) = \prod_{i=1}^{g} h(X_i)$ and $\alpha[h](y) = \prod_{i=1}^{g} h(Y_i)$.

6. Return $\eta[\mathfrak{u}, y](x) = \frac{\alpha[h](x)}{\alpha[h](y)} \cdot \prod_{1\leq i\leq I} (\delta_x^{(i)}/\delta_y^{(i)})^{e_i}$.

In the case that D_x (or D_y) is not simple, then the $\delta_x^{(i)}$ are zero and the product $\prod_{1\leq i\leq I}(\delta_x^{(i)})^{e_i}$ is not defined (some e_i is negative) while $\eta[\mathfrak{u}, y](x)$ is. This last value can be obtained considering the field $L = K((t))$ for a formal parameter t. Indeed, assume for example $D_x = nX_1 + X_{n+1} + \ldots + X_g$ and $X_i \neq X_j$ if $i \neq j$. Fix a local parameter $z \in K(\mathcal{C})$ at X_1 and n distinct scalars $(a_j)_{1\leq j\leq n}$ in K (if $\#K$ is too small, then consider a small degree extension of it). Denote by $X_1(t), X_2(t), \ldots, X_n(t)$ the points in $\mathcal{C}(L)$ associated with the values $a_1 t, \ldots, a_n t$ of the local parameter z. Do the computations of the algorithm with $D_x(t) = X_1(t) + \ldots + X_n(t) + X_{n+1} + \ldots + X_g$ and set $t = 0$ in the result. The necessary t-adic accuracy is $g(g-1)/2$.

Denote by $\mathfrak{O}$ a positive absolute constant. Any statement containing this symbol is true if this symbol is replaced by a big enough real number. Similarly, denote by $\mathfrak{e}(z)$ a real function in the real parameter z belonging to the class $o(1)$.

Theorem 1. *There exists a deterministic algorithm that takes as input*

- *a finite field K with cardinality q;*
- *a curve $\mathcal{C}$ of genus $g \geq 2$ over K;*
- *a collection of K-points $(u_i)_{1\leq i\leq I}$ in the Jacobian J of $\mathcal{C}$;*
- *a zero-cycle $\mathfrak{u} = \sum_{1\leq i\leq I} e_i[u_i]$ on J such that $\deg(\mathfrak{u}) = 0$ and $s(\mathfrak{u}) = 0$;*
- *a point O in $\mathcal{C}(K)$;*
- *and two points $x, y \in J(K)$ not in $\bigcup_{1\leq i\leq I} W_{-(g-1)o+u_i}$.*

Denote $|e| = \sum_{1\leq i\leq I} |e_i|$. The algorithm computes $\eta[\mathfrak{u}, y](x)$ in time $(g \cdot |e|)^{\mathfrak{O}} \cdot (\log q)^{1+\mathfrak{e}(q)}$. Using fast exponentiation and equation (5), the complexity is $g^{\mathfrak{O}} \cdot I \cdot (\log |e|) \cdot (\log q)^{1+\mathfrak{e}(q)}$ and there exists a subset $FAIL(K, \mathcal{C}, \mathfrak{u}, O)$ of $J(K)$ with density $\leq g^{\mathfrak{O}g} \cdot I \cdot \log(|e|)/q$ such that the algorithm succeeds whenever neither of x nor y belongs to this subset.

Fast multiple evaluation. For ours applications, we need to evaluate $\eta[\mathfrak{u}, y]$ at many random points x of the Jacobian to do linear algebra. So we could ask if there is some redundant computations. This is not the case because the divisors $D^{(i)}$ at step 1 depend on x so that it is also the case for h and the basis $f^{(i)}$. But if we do not consider this dependancy and take $D^{(i)} = U_i - (g-1)O + \Omega$ (for example, and we assume that the condition on y neither interfere), then h, the basis $f^{(i)}$, the values $\delta_y^{(i)}$ and $\alpha[h](y)$ can be computed once and for all.

The points x where the computation does not work are simply discarded. In practice, this allows us to gain a considerable amount of time, as the Riemann-Roch effectives algorithms are done only one time. The random x can be obtained in taking g random points of the curve $\mathcal{C}$ so that we directly have the points X_i.

2.3 Evaluation of $\eta_X[\mathfrak{u}, y]$

In the preceding subsection, we have defined functions on a given curve $\mathcal{C}$. Let $\mathcal{V} \subset J[\ell]$ be a maximal isotropic subgroup for the commutator pairing. We introduce now functions on the quotient $J/\mathcal{V}$. This is [10, Sections 4 and 5].

Let $f : J \to J/\mathcal{V}$ be the quotient map and let $\mathcal{L} = \mathcal{O}_J(\ell W_{-\theta})$ be a symmetric line bundle. There exists a line bundle $\mathcal{M}$ on $J/\mathcal{V}$ which is a symmetric principal polarization and which satisfies $\mathcal{M} = f^*\mathcal{L}$. The map f is a $(\ell, \dots, \ell)$-isogeny. As $h^0(\mathcal{M}) = 1$, there exists a unique effective divisor Y on $J/\mathcal{V}$ associated with $\mathcal{M}$. The divisor $X = f^*Y$ is effective, linearly equivalent to $\ell W_{-\theta}$ and invariant by $\mathcal{V}$ (by translation).

We are interested in the function $\eta_X[\mathfrak{u}, y]$ (see Equation (4)) for some zero-cycle $\mathfrak{u} = \sum_{1\le i\le I} e_i[u_i]$ in J and $y \in J(K)$ with the usual restrictions. Taking $v_i = f(u_i)$ and letting $\mathfrak{v} = \sum_{1\le i\le I} e_i[v_i]$ be a zero-cycle on $J/\mathcal{V}$ and in considering the function $\eta_Y[\mathfrak{v}, f(y)]$ on $J/\mathcal{V}$ having $\sum_{1\le i\le I} e_i Y_{v_i} - Y_{s(\mathfrak{v})} - (\deg(\mathfrak{v}) - 1)Y$ as divisor and taking value 1 at $f(y)$, we can identify the function $\eta_Y[\mathfrak{v}, f(y)] \circ f$ with $\eta_X[\mathfrak{u}, y]$. This allows us to work on the isogenous variety in staying in the starting Jacobian. A point z in $J/\mathcal{V}$ is seen as a point x in J such that $f(x) = z$.

We want now to evaluate the function $\eta_X[\mathfrak{u}, y]$ at x. The trick consists to construct a function $\Phi_{\mathcal{V}}$ having $X - \ell W_{-\theta}$ as divisor. Indeed, assuming that $s(\mathfrak{u}) = 0$ and $\deg(\mathfrak{u}) = 0$, the divisor of $\eta_X[\mathfrak{u}, y]$ is $\sum_{i=1}^{I} e_i X_{u_i}$ while the divisor of $\prod_{1\le i\le I} \Phi_{\mathcal{V}}(x - u_i)^{e_i}$ is $\sum_{i=1}^{I} e_i(X_{u_i} - \ell W_{-\theta+u_i})$. To compensate, consider the function $(\eta[\mathfrak{u}](x + \vartheta))^\ell$ which has divisor $\ell \sum_{i=1}^{I} e_i W_{-(g-1)o-\vartheta+u_i} = \ell \sum_{i=1}^{I} e_i W_{-\theta+u_i}$ because $\vartheta = \theta - (g-1)o$. The condition on y allows us to write

$$\eta_X[\mathfrak{u}, y](x) = (\eta[\mathfrak{u}, y + \vartheta](x + \vartheta))^\ell \cdot \prod_{1\le i\le I} (\Phi_{\mathcal{V}}(x - u_i))^{e_i} \cdot \prod_{1\le i\le I} (\Phi_{\mathcal{V}}(y - u_i))^{-e_i}. \tag{7}$$

The construction and computation of $\Phi_{\mathcal{V}}$ goes as follows. For any $w \in \mathcal{V}$, define $w' := \frac{\ell+1}{2} \cdot w$ (ℓ has to be odd). Fix $\phi_u, \phi_y \in J(K)$ and consider the functions

$$\theta_w(x) := \eta[\ell[w'] - \ell[0], w' - x + \vartheta](x - w' + \vartheta),$$

$$\tau[\phi_u, \phi_y](x) := \eta[[(\ell - 1)\phi_u] + (\ell - 1)[-\phi_u] - \ell[0], \phi_y + \vartheta](x + \vartheta),$$

and

$$a_w(x) = \theta_w(x) \cdot \tau[\phi_u, \phi_y](x - w).$$

Then we can define $\Phi_{\mathcal{V}}$ as

$$\Phi_{\mathcal{V}}(x) = \sum_{w\in\mathcal{V}} a_w(x).$$

This is also equal to $\sum_i \mathrm{tr}_{L_i/K}(a_{w_i}(x))$ if the subgroup $\mathcal{V}$ is given by a collection of fields extensions (L_i/K) and points $w_i \in \mathcal{V}(L_i)$ such that $\mathcal{V}$ is the disjoint union of the K-Zariski closures of all w_i.

As $\#\mathcal{V} = \ell^g$, the number of calls to the η function to compute η_X is borned by $1 + 4 \cdot I \cdot \ell^g$.

Theorem 2. *There exists a deterministic algorithm that takes as input*

- *a finite field K with characteristic p and cardinality q;*
- *a curve $\mathcal{C}$ of genus $g \geq 2$ over K;*
- *a zero-cycle $\mathfrak{u} = \sum_{1 \leq i \leq I} e_i[u_i]$ in the Jacobian J of $\mathcal{C}$ such that $u_i \in J(K)$ for every $1 \leq i \leq I$, $\deg(\mathfrak{u}) = 0$ and $s(\mathfrak{u})$;*
- *a theta characteristic θ defined over K;*
- *an odd prime integer $\ell \neq p$;*
- *a maximal isotropic K-subgroup scheme $\mathcal{V} \subset J[\ell]$;*
- *two classes x and y in $J(K)$ such that $y \notin (\bigcup_i W_{-\theta+u_i}) \cup (\bigcup_i X_{u_i})$.*

The algorithm returns FAIL or $\eta_X[\mathfrak{u}, y](x)$ in time $I \cdot (\log |e|) \cdot g^{\mathfrak{O}} \cdot (\log q)^{1+\mathfrak{e}(q)} \cdot \ell^{g(1+\mathfrak{e}(\ell^g))}$, where $|e| = \sum_{1 \leq i \leq I} |e_i|$. For given K, $\mathcal{C}$, $\mathfrak{u}$, θ, $\mathcal{V}$, there exists a subset FAIL$(K, \mathcal{C}, \mathfrak{u}, \theta, \mathcal{V})$ of $J(K)$ with density $\leq I \cdot (\log |e|) \cdot g^{\mathfrak{O}g} \cdot \ell^{g^2} \cdot (\log \ell)/q$ and such that the algorithm succeeds whenever none of x and y belongs to this subset.

Fast multiple evaluation. What we said about multiple evaluation of $\eta[\mathfrak{u}, y]$ functions on random points x is still valid here. The divisors ϕ_u and ϕ_y have to been chosen once and for all and some precomputations concerning $\mathcal{V}$, ϕ_u and ϕ_y can be done.

3 Computation of the equation of the curve in the hyperelliptic case

Until now we have defined functions on J and on $J/\mathcal{V}$. If the genus of $\mathcal{C}$ is 2, then this quotient is generically the Jacobian of a genus 2 hyperelliptic curve $\mathcal{D}$, while if it is 3, this is generically the Jacobian of a genus 3 curve $\mathcal{D}$, which can be hyperelliptic or non-hyperelliptic (a plane quartic) and the latter is the generic case. The aim of this section is to compute a model of $\mathcal{D}$ when $\mathcal{D}$ is hyperelliptic of genus 2 or 3 in using the geometry of the Kummer variety.

3.1 Kummer variety

We assume $char(K) \neq 2$. A principal polarization of the principally polarized abelian variety $J_{\bar{K}}$ is $\mathcal{O}_{J_{\bar{K}}}(W_{-\theta})$ (see [21, Chapter III]). The symmetric divisor $W_{-\theta}$ is a symmetric theta divisor, sometimes denoted by Θ in the literature. The map $J_{\bar{K}} \to \mathbb{P}^{2^g-1} = \mathbb{P}^{2^g-1}(\bar{K})$ given by the linear system $|2W_{-\theta}|$ factors through the projection $J_{\bar{K}} \to J_{\bar{K}}/\langle \pm 1 \rangle$ and a morphism $J_{\bar{K}}/\langle \pm 1 \rangle \to \mathbb{P}^{2^g-1}$, which is a closed embedding ([12, Proposition 2.3]). The Kummer variety of $J_{\bar{K}}$ is $J_{\bar{K}}/\langle \pm 1 \rangle$. We identify it with its image in $\mathbb{P}^{2^g-1}$.

Proposition 3. *Let A be a Jacobian variety of dimension $g \geq 2$ defined over an arbitrary field. If $\eta_1, \ldots, \eta_{2^g}$ is a basis of $H^0(A, \mathcal{O}_A(2W_{-\theta}))$ and if $\phi = (\eta_1, \ldots, \eta_{2^g}) : A \to \mathbb{P}^{2^g-1}$, then the image $\phi(A)$ can be described by an intersection of quartics.*

Proof. This is [24, Proposition 3.1]. □

In the genus 2 case, 1 quartic is enough to describe $\phi(A)$. According to [30, Theorem 2.5] (extending [24, Theorem 3.3]), in the case of a hyperelliptic curve of genus 3 defined over a field whose characteristic is not 2, 1 quadric and 34 quartics are needed (in our case, we have always computed a lot of equations and reduced them in computing a Gröbner basis and this yielded 1 quadric and 35 quartics). Finally, in the non-hyperelliptic case of genus 3 curves, it is possible, instead of quartics, to describe the Kummer by 8 cubics equations ([5, Theorem 7.5]).

From a basis of $H^0(J_{\bar{K}}, \mathcal{O}_{J_{\bar{K}}}(2W_{-\theta}))$ (built from η or η_X functions), these equations can be computed in evaluating the functions in the basis at random points and in doing then linear algebra. In genus 2, the basis is of cardinality 4 and a quartic has at most 35 coefficients, so that the number of evaluations is at least 35. This number is 330 in genus 3 for quartics and 36 for quadrics because the basis has 8 elements, but in the non-hyperelliptic case as the Kummer can be described by cubics, 120 evaluations are needed. (Recall that the number of monomials of degree d with v variables is $\binom{v+d-1}{d}$).

Having these equations help the computation of the isogenies but they are not necessary. Computing them does not impact the complexity of the algorithms but have a huge impact on the practical computations (see next subsection).

Let $a \in J_{\bar{K}}[2]$ and $y \in J$. Define the function $\eta_a = \eta_{W_{-\theta}}[2[a] - 2[0], y]$ (resp. $\eta_a = \eta_X[2[a]-2[0], y]$) whose divisor is $2(W_{-\theta+a} - W_{-\theta})$ (resp. $2(X_a - X)$). This is a level 2 function and these functions generate the space of the functions belonging to $H^0(J_{\bar{K}}, \mathcal{O}_{J_{\bar{K}}}(2W_{-\theta}))$ (resp. $H^0(J_{\bar{K}}, \mathcal{O}_{J_{\bar{K}}}(2X))$ or equivalently $H^0(J_{\bar{K}}/\mathcal{V}, \mathcal{O}_{J_{\bar{K}}/\mathcal{V}}(2Y))$), which is of dimension 2^g. Fixing a basis $\eta_1, \ldots, \eta_{2^g}$ give us the map from $J_{\bar{K}}$ to the Kummer variety of the Jacobian of $\mathcal{C}$ (resp. of $\mathcal{D}$) in $\mathbb{P}^{2^g-1}$ over $\bar{K}$. Call $Z_1, \ldots, Z_{2^g}$ the projective coordinates associated to this basis. Using linear algebra, it is possible to write η_a in function of the basis. This gives an equation Z_a in function of the Z_i, and the equation $Z_a = 0$ is the image of $W_{-\theta+a}$ in the Kummer seen in $\mathbb{P}^{2^g-1}$. The hyperplanes Z_a for $a \in J_{\bar{K}}[2]$, which are called *singular planes* or *tropes*, with the set of the images of the 2-torsion points in $\mathbb{P}^{2^g-1}$, called *singular points* or *nodes*, constitute a configuration.

Definition 4. *A (m, n)-configuration in $\mathbb{P}^N$ is the data of m hyperplanes and m points such that each hyperplane contains n points and each point is contained in n hyperplanes.*

The configuration can be described through a symplectic basis of the 2-torsion: let $e_1, \ldots, e_g, f_1, \ldots, f_g$ be such a basis. We represent an element $a = \epsilon_1 e_1 + \ldots + \epsilon_g e_g + \rho_1 f_1 + \ldots + \rho_g f_g$ by the matrix $\left(\begin{smallmatrix} \epsilon_1 & \cdots & \epsilon_g \\ \rho_1 & \cdots & \rho_g \end{smallmatrix}\right)$, of characteristic $\sum_{i=1}^{g} \epsilon_i \rho_i$.

Kummer surfaces have been thoroughly studied (see [1, Section 10.2] for example) and their $(16, 6)$-configuration is a corollary of the next proposition.

Proposition 5. *There is a 2-torsion point a_0 such that for any $a' = \left(\begin{smallmatrix} \epsilon_1 & \epsilon'_1 \\ \rho_1 & \rho'_1 \end{smallmatrix}\right)$ and $a'' = \left(\begin{smallmatrix} \epsilon_2 & \epsilon'_2 \\ \rho_2 & \rho'_2 \end{smallmatrix}\right)$ in $J_{\bar{K}}[2]$, the following conditions are equivalent*

- *the image of a' in $\mathbb{P}^3$ is contained in the singular plane $Z_{a_0+a''}$;*
- *either $((\epsilon_1, \rho_1) = (\epsilon_2, \rho_2)$ and $(\epsilon'_1, \rho'_1) \neq (\epsilon'_2, \rho'_2))$ or $((\epsilon_1, \rho_1) \neq (\epsilon_2, \rho_2)$ and $(\epsilon'_1, \rho'_1) = (\epsilon'_2, \rho'_2))$.*

Proof. This is [1, Proposition 10.2.5], where $K = \mathbb{C}$. It is easy to prove that there is a $(16, 6)$-configuration. A hyperelliptic curve of genus 2 has 6 Weierstrass points $r_1, \ldots, r_6$ from which

we deduce the 16 2-torsion points. For $i \in \{1, \dots, 6\}$ and $a \in J_{\bar{K}}[2]$, the $r_i - \theta + a$ are the only 2-torsion points in $W_{-\theta+a}$, where we identify the points in $\mathcal{C}$ with the points in Pic^1. Moreover, the 2-torsion point $r_j - \theta + a$ is in $W_{-\theta+a+(r_i-\theta)+(r_j-\theta)}$ for $i \in \{1, \dots, 6\}$.

Note that the trope Z_0 contains the image of the six 2-torsions points $a_i = r_i - \theta$ and knowing the matrices associated to these six points, we can compute a_0 because this trope correspond to the case $a'' = a_0$. Moreover, we deduce that $a_0 \notin \{r_i - \theta\}_{i \in \{1,\dots,6\}}$. See also Remark 10 for the computation of a_0.

In the analytic theta function theory (see Section 5), we have that the six theta constants having odd characteristic are equal to 0. Here, note that the image of a 2-torsion point a' is in the trope $Z_{a_0+a''}$ for some a'' when the characteristic of $a' + a'' + \left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right)$ is odd. The shift by $\left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right)$ comes from the way this proposition is proved in [1]. □

Corollary 6. *Any two different singular planes have exactly two singular points in common.*

Proof. The proof proceeds case by case. See [1, Corollary 10.2.8] and the paragraph following. □

In genus 3, there is a $(64, 28)$-configuration for hyperelliptic and non-hyperelliptic curves and for the former, the configuration can be extended to a $(64, 29)$-configuration.

Proposition 7. *Let $\mathcal{C}$ be a genus 3 curve. There exists a 2-torsion point a_0 such that for all $a' = \left(\begin{smallmatrix} \epsilon_1 & \epsilon'_1 & \epsilon''_1 \\ \rho_1 & \rho'_1 & \rho''_1 \end{smallmatrix}\right)$ and $a'' = \left(\begin{smallmatrix} \epsilon_2 & \epsilon'_2 & \epsilon''_2 \\ \rho_2 & \rho'_2 & \rho''_2 \end{smallmatrix}\right)$ in $J_{\bar{K}}[2]$, the image of the point a' in $\mathbb{P}^7$ is contained in $Z_{a_0+a''}$ if and only if one of the following conditions is satisfied*

- *$a' = a''$;*
- *$(\epsilon_1, \rho_1) = (\epsilon_2, \rho_2)$ and $(\epsilon'_1, \rho'_1) \neq (\epsilon'_2, \rho'_2)$ and $(\epsilon''_1, \rho''_1) \neq (\epsilon''_2, \rho''_2)$;*
- *$(\epsilon_1, \rho_1) \neq (\epsilon_2, \rho_2)$ and $(\epsilon'_1, \rho'_1) = (\epsilon'_2, \rho'_2)$ and $(\epsilon''_1, \rho''_1) \neq (\epsilon''_2, \rho''_2)$;*
- *$(\epsilon_1, \rho_1) \neq (\epsilon_2, \rho_2)$ and $(\epsilon'_1, \rho'_1) \neq (\epsilon'_2, \rho'_2)$ and $(\epsilon''_1, \rho''_1) = (\epsilon''_2, \rho''_2)$;*
- *$a' = a'' + a_0 + 2r - \theta$ and $\mathcal{C}$ is hyperelliptic, where r is any Weierstrass point, seen in $\mathrm{Pic}^1(\mathcal{C})$.*

Proof. We have obtained this result in adapting the proof of [1, Proposition 10.2.5], using $\left(\begin{smallmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \end{smallmatrix}\right)$. In the hyperelliptic case, the divisor $W_{-\theta}$ contains 29 points of 2-torsion (coming from the combination of two Weierstrass points among the 8, giving us $\binom{8}{2} + 1 = 29$) against 28 in the non-hyperelliptic case (coming from the 28 bitangents, see Section 5.3). Among the 29 points, exactly one is such that the multiplicity of $W_{-\theta}$ at this point is even: this is the point $2r$ in W and thus $2r - \theta$ in $W_{-\theta}$ (recall that if r_1, r_2 are linear classes of divisors in $\mathrm{Pic}^1(\mathcal{C})$ coming from Weierstrass points, then $2r_1 \sim 2r_2$). As in the genus 2 case, we can compute a_0 knowing the points in $W_{-\theta}$. Note that because of the first condition, we have that a_0 is one of the 2-torsion points in $W_{-\theta}$.

Moreover, it is well-known that the analytic theta constants having odd characteristic are equal to 0 and that a genus 3 curve is hyperelliptic if and only if (exactly) one even theta constant is equal to 0.

□

3.2 Computing the equation of the isogenous curve in genus 2

We focus now in the genus 2 case. Let $\mathcal{C}$ be a hyperelliptic curve of genus 2 over a finite field K of characteristic $\neq 2$. We assume that the curve is given by an imaginary model so that we have $\mathcal{C} : Y^2 = h_{\mathcal{C}}(X)$ for $h_{\mathcal{C}}$ of degree 5 and having a unique point at infinity O. Coming back at the notations of Section 2.1, the K-point we choose is O. We have that $2O$ is a canonical divisor so that we can take $\theta = \iota(O) := o$ as a theta characteristic and then $\vartheta = 0 \in J(K)$. We use the η and η_X functions defined by the divisor W_{-o}.

Let $r_1, \ldots, r_6$ be the 6 Weierstrass points of the curve $\mathcal{C}$, where r_6 is the (unique) point at infinity O. Assume to simplify that these points are in $\mathcal{C}/K$. By an abuse of notation, we also denote r_i the class of r_i in $\mathrm{Pic}^1(\mathcal{C})$. The 2-torsion points in J are $a_i := r_i - o$ for $i \in \{1, \ldots, 6\}$ and $a_{ij} := r_i + r_j - 2o$ for $1 \leq i, j \leq 5$.

Note that as $\vartheta = 0$, then by Equation (7) we have for $i \in \{1, \ldots, 16\}$ that $\eta[\mathfrak{u}, y](a_i) = 0$ implies that $\eta_X[\mathfrak{u}, y](a_i) = 0$. The converse is also true because of the $(16, 6)$-configuration of the Kummers of $\mathcal{C}$ and $\mathcal{D}$. So the description of the two configurations with the 2-torsion points of J is the same.

Fix $y \in J$. As in the preceding subsection, define the level 2 functions $\eta_{a_i} = \eta_X[2[a_i] - 2[0], y]$ and $\eta_{a_{ij}} = \eta_X[2[a_{ij}] - 2[0], y]$ (but what we will say remains true if we replace η_X by η). Note that the function η_{a_6} is constant according to its divisor and by definition we have $\eta_{a_6}(y) = 1$. But this function has to be equal to 0 at the closed subvariety W_{-o} of J and in particular at the six 2-torsion points a_1, ..., a_6 to be coherent with the $(16, 6)$-configuration in $\mathbb{P}^3$. Indeed, looking at divisors, we have for $a = a_i \neq a_6$ or $a = a_{ij}$ that $\eta_a(x) = 0$ for the values $x \in \{a_1 + a, \ldots, a_6 + a\}$.

The (16,6)-configuration Fix $\eta_1, \ldots, \eta_4$ a basis of the η_{a_i} and $\eta_{a_{ij}}$ functions. This defines a map ϕ from J to the Kumer surface of the Jacobian $J_{\mathcal{D}}$ of $\mathcal{D}$ seen in $\mathbb{P}^3$ and we denote by $Z_1, \ldots, Z_4$ the projective coordinates associated to this basis, as already done in the previous subsection. For all $a = a_i$ and $a = a_{ij}$, writing η_a in function of this basis give equations of the form $\eta_a = \alpha_1\eta_1 + \ldots + \alpha_4\eta_4$ for $\alpha_k \in K$. Denote then $Z_a = \alpha_1 Z_1 + \ldots + \alpha_4 Z_4$ the tropes. The nodes are the image by ϕ of the 2-torsion points. The $(16, 6)$-configuration is described by Table 1, where for each trope we have written the 6 2-torsions points whose images are in it.

Z_{a_1}	a_1	a_6	a_{12}	a_{13}	a_{14}	a_{15}		$Z_{a_{14}}$	a_1	a_4	a_{14}	a_{23}	a_{25}	a_{35}
Z_{a_2}	a_2	a_6	a_{12}	a_{23}	a_{24}	a_{25}		$Z_{a_{15}}$	a_1	a_5	a_{15}	a_{23}	a_{24}	a_{34}
Z_{a_3}	a_3	a_6	a_{13}	a_{23}	a_{34}	a_{35}		$Z_{a_{23}}$	a_2	a_3	a_{14}	a_{15}	a_{23}	a_{45}
Z_{a_4}	a_4	a_6	a_{14}	a_{24}	a_{34}	a_{45}		$Z_{a_{24}}$	a_2	a_4	a_{13}	a_{15}	a_{24}	a_{35}
Z_{a_5}	a_5	a_6	a_{15}	a_{25}	a_{35}	a_{45}		$Z_{a_{25}}$	a_2	a_5	a_{13}	a_{14}	a_{25}	a_{34}
Z_{a_6}	a_1	a_2	a_3	a_4	a_5	a_6		$Z_{a_{34}}$	a_3	a_4	a_{12}	a_{15}	a_{25}	a_{34}
$Z_{a_{12}}$	a_1	a_2	a_{12}	a_{34}	a_{35}	a_{45}		$Z_{a_{35}}$	a_3	a_5	a_{12}	a_{14}	a_{24}	a_{35}
$Z_{a_{13}}$	a_1	a_3	a_{13}	a_{24}	a_{25}	a_{45}		$Z_{a_{45}}$	a_4	a_5	a_{12}	a_{13}	a_{23}	a_{45}

Table 1: $(16, 6)$-configuration in genus 2

We want to use this configuration to compute the equation of the isogenous curve $\mathcal{D}$. To achieve this, we compute the image in $\mathbb{P}^3$ of the six 2-torsion points lying in a trope (anyone) and then we do a parameterization step. This is justified by the fact that according to [1,

Proposition 10.2.3 and Corollary 10.2.4], the intersection of a trope with the Kummer is a conic and this intersection is of multiplicity 2.

Let Z_a be a trope. It contains the six points $\phi(a_1+a),\ldots,\phi(a_6+a)$ in $\mathbb{P}^3$. As we can not compute the η_X functions at 2-torsion points directly, because these functions have poles at these points and the algorithm to evaluate the η_X functions at these points does not behave well, we compute the image by ϕ of each of these six points in computing the intersection of 3 tropes. Indeed, as the Kummer surface is seen in a projective space of dimension 3, we need 3 equations to determine a point. We use the following properties that can be deduced from Table 1: $\{Z_{a_1}=0,Z_{a_2}=0,Z_{a_3}=0\}=\{\phi(a_6)\}$ and for $i\in\{1,\ldots,5\}$, $\{Z_{a_i}=0,Z_{a_6}=0\}=\{\phi(a_i),\phi(a_6)\}$. Thus, by shifting, looking at the intersection $\{Z_{a_1+a}=0,Z_{a_2+a}=0,Z_{a_3+a}=0\}$ gives us the projective point $p_6=\phi(a_6+a)$. The others points can be computed similarly in looking $\{Z_{a_i+a}=0,Z_{a_6+a}=0,Z_b=0\}$ for some good choosen trope Z_b. Otherwise, if we have the equation of the quartic $\kappa_{\mathcal{D}}$ describing the Kummer surface associated to $\mathcal{D}$, we can obtain the points by $\{Z_{a_i+a}=0,Z_{a_6+a}=0,\kappa_{\mathcal{D}}=0\}$. Thus, we have the projectives points $p_i=\phi(a_i+a)$, for $i\in\{1,\ldots,6\}$.

Parameterization. Choose any point among $\{p_1,\ldots,p_6\}$, say p_1. We look for equations of the form $E_j=\alpha_{j,1}Z_1+\ldots+\alpha_{j,4}Z_4$ passing by p_1 and p_j, for $j\in\{2,\ldots,6\}$. Recall that the 6 points are in the trope $Z_a=\alpha_1Z_1+\ldots+\alpha_4Z_4=0$. Let $k=\min_{i\in\{1,2,3,4\}}\{i:\alpha_i\neq 0\}$ so that $\alpha_kZ_k=-\sum_{i=k+1}^{4}\alpha_iZ_i$ and the equations E_j can be written in function of the three Z_i for $i\neq k$. So we rewrite E_j in putting $\alpha_{j,k}=0$ for $j\in\{2,\ldots,6\}$. Moreover, the fact that E_j evaluated in p_1 has to be equal to 0 yield a relation between $\alpha_{j,1},\ldots,\alpha_{j,4}$. Assume to simplify that $k=1$ so that we have $\alpha_{j,1}=0$ and that $\alpha_{j,2}$ can be written in function of $\alpha_{j,3}$ and $\alpha_{j,4}$: $\alpha_{j,2}=P(\alpha_{j,3},\alpha_{j,4})$. We obtain an affine parameterization in taking $\alpha_{j,3}=1$ and $\alpha_{j,4}=x$ and we look at the equation $E=P(1,x)Z_2+Z_3+xZ_4$. Now, for $j\in\{2,\ldots,6\}$, evaluating E in p_j yield an equation of degree 0 or 1 in x. If it is 1, then we obtain the value x and if it is 0, then x is the point at infinity. Thus, we have 5 of the 6 Weierstrass points of a model of $\mathcal{D}$. The last one, associated to p_1, can be obtained in intersecting the equation $\kappa_{\mathcal{D}}$ of the Kummer surface with the trope Z_a and the equation E, factorizing, evaluating in p_1 and solving the factor having x (this idea is implicit in [10]).

Optimization. For this method to work, it requires to compute the equation of the Kummer surface and the 6 tropes Z_{a_i+a}, for $i\in\{1,\ldots,6\}$. This makes at most $35\times 4+(6+4)\times 4=180$ evaluations of η_X functions. We explain how this number can be greatly reduced.

A good choice of basis is $\eta_1=\eta_{a_6},\eta_2=\eta_{a_1},\eta_3=\eta_{a_2},\eta_4=\eta_{a_{12}}$ (Z_{a_6} and Z_{a_1} contain $\phi(a_1)$ while Z_{a_2} not, and Z_{a_6}, Z_{a_1}, Z_{a_2} contain $\phi(a_6)$ while $Z_{a_{12}}$ not; this proves that the four functions are independent). We have noted that, with this basis, the equation of the Kummer surface $\kappa_{\mathcal{D}}$ does not have any exponent of degree 3 and 4 so it has at most 19 coefficients so that the cost of the computation of $\kappa_{\mathcal{D}}$ is reduced, but we will not use this fact. We will take advantage of the facts that the value of η_{a_6} is known without computation and that we have obviously $Z_{a_6}=Z_1$, $Z_{a_1}=Z_2$, $Z_{a_2}=Z_3$ and $Z_{a_{12}}=Z_4$. Moreover, for any $a\in J[2]$, there is $a_i\in\{a_6,a_1,a_2,a_{12}\}$ such that Z_a contains $\phi(a_i)$ and such that exactly three of the four tropes Z_1, …, Z_4 associated to the functions in the basis contain $\phi(a_i)$. So all the tropes can be written in function of three elements among $\{Z_1,Z_2,Z_3,Z_4\}$ and as we have defined all the η_X functions such that their values at y is 1, the evaluations at only two points are enough for computing a trope.

The trope we fix for the parameterization is $Z_{a_6} = Z_1$. Note that we have $p_6 = \phi(a_6) = (0:0:0:1)$ (see Table 1) so fixing this point, we obtain the affine parameterization $Z_1 = 0$, $Z_2 + xZ_3 = 0$. Moreover, $p_1 = \phi(a_1) = (0:0:1:0)$ giving $x = 0$ and $p_2 = \phi(a_2) = (0:1:0:0)$ giving $x = \infty$. Thus, with this basis, we always obtain a degree 5 model for the isogenous curve $\mathcal{D}$ and the image of three of the six points in the fixed trope Z_{a_6} are obtained for free.

It remains to compute the images of a_3, a_4 and a_5 in $\mathbb{P}^3$. We have (according to Table 1): $\{Z_{a_6} = 0, Z_{a_{34}} = 0, Z_{a_{35}} = 0\}$ giving us $p_3 = \phi(a_3)$, $\{Z_{a_6} = 0, Z_{a_{34}} = 0, Z_{a_{45}} = 0\}$ giving us $p_4 = \phi(a_4)$, $\{Z_{a_6} = 0, Z_{a_{35}} = 0, Z_{a_{45}} = 0\}$ giving us $p_5 = \phi(a_5)$.

Thus, we can obtain the images of $a_1, \ldots, a_6$ in $\mathbb{P}^3$ in computing the tropes $Z_{a_{34}}$, $Z_{a_{35}}$ and $Z_{a_{45}}$ which can be done in $(3+3) \times 2 = 12$ evaluations of η_X functions. There is a slight amelioration in noting that for $a, b \in J[2]$ and $x \in J$

$$\eta_{a+b}(x) = \eta_X[2[a] - 2[0], y + b](x + b) \cdot \eta_b(x) \tag{8}$$

(look at the divisors and the evaluations at y for the proof). Let $b = a_{45}$, and take some random point $z \in J$ (not of 2-torsion). The function $\eta_{a_{35}}(x + a_{45}) \cdot \eta_{a_{45}}(x)$ has the same divisor as $\eta_{a_{34}}(x)$ and the constant between the two functions can be established in evaluating $\eta_{a_{35}}(x + a_{45})$ at y. It remains to evaluate η_{a_i} for $a_i \in \{a_1, a_2, a_{12}, a_{35}, a_{45}\}$ at the points z and $z + a_{45}$ for computing $Z_{a_{34}}$, $Z_{a_{35}}$, $Z_{a_{45}}$. So $1 + 5 \times 2 = 11$ evaluations are enough instead of 12.

For the parameterization, if we want to avoid the computation of the equation of the Kummer surface, which is costly in term of number of evaluations of the η_X functions, a solution consists to do the parameterization two times for two differents fixed points. This yields two sets of 5 Weierstrass points (for differents models of the curve) and we look then for a change of variables sending exactly 4 elements of the first set in the second set. Applying the transformation on the fifth point of the first set give us the unknown Weierstrass point of the second set. This implies we have an efficient way to determine if a given transformation produces an isogenous curve or not. For example, the knowledge of the cardinality of the Jacobian of $\mathcal{C}$ is a sufficient data, and it can also be used to distinguish a curve from its twist. Recall that a nonsingular projective model of a hyperelliptic curve is $Y^2 = \prod_{i=1}^{6} c_i X^i Z^{6-i}$ in the projective space with weight $(1, 3, 1)$ and that a transformation is of the form $(X : Y : Z) \mapsto (\alpha X + \beta Z : \gamma Y : \delta X + \epsilon Z)$ with $\alpha\epsilon - \beta\delta = 1$.

Example. Let $\mathcal{C}$ given by the equation $(X - 179)(X - 237)(X - 325)(X - 344)(X - 673)$ on $\mathbb{F}_{1009}$. A maximal isotropic subgroup of the $\ell = 3$ torsion is generated by $T_1 =< X^2 + 714X + 513,182X + 273 >$ and $T_2 =< X^2 + 654X + 51,804X + 545 >$ (these are Mumford representation). We fix $y =< X^2 + 425X + 637,498X + 930 >$, $\phi_u =< X^2 + 462X + 658,365X + 522 >$, $\phi_y =< X^2 + 512X + 883,827X + 148 >$. We put $r_1 = (179, 0)$, $r_2 = (237, 0)$, $r_3 = (325, 0)$, $r_4 = (344, 0)$, $r_5 = (673, 0)$ and $r_6 = \infty$. We take the good basis of η_X functions defined with the zero-cycles $2[u_i] - 2[0]$ for $u_i \in \{0, r_1 - r_6, r_2 - r_6, r_1 + r_2 - 2r_6\}$. Then

$$Z_{a_1} = Z_2, \qquad Z_{a_2} = Z_3, \qquad Z_{a_6} = Z_1, \qquad Z_{a_{34}} = 953Z_2 + 55Z_3 + 2Z_4,$$

$$Z_{a_{35}} = 806Z_2 + 131Z_3 + 73Z_4, \qquad Z_{a_{45}} = 894Z_2 + 123Z_3 + 1002Z_4$$

giving us the nodes $(0:0:1:0), (0:1:0:0), (0:947:689:1), (0:304:71:1), (0:869:468:1), (0:0:0:1)$ which are in the trope $Z_1 = 0$. Fixing the point $(0:0:0:1)$, we take the parameterization $Z_1 = 0$, $Z_2 + xZ_3 = 0$ and we obtain the values $\{0, \infty, 498, 351, 397, x_1\}$ for x

respectively. Fixing the point $(0:0:1:0)$, we take the parameterization $Z_1 = 0$, $Z_2 + xZ_4 = 0$ and we obtain the values $\{x_2, \infty, 62, 705, 140, 0\}$ for x respectively.

For the transformation, we take the one sending 498 to 62 and 351 to 705 which is $(X : Y : Z) \mapsto (229X + 37Z : Y : Z)$. Then 397 is sent to 140, 0 to 37, ∞ to ∞ and 837 to 0. Two models of the curve $\mathcal{D}$ are $11X(X-498)(X-351)(X-397)(X-837)$ and $X(X-62)(X-705)(X-140)(X-37)$ (after checking quadratic twist).

3.3 Computing the equation of the isogenous curve in genus 3 if $\mathcal{D}$ is hyperelliptic

We focus now on the genus 3 case and we assume that $\mathcal{D}$ is hyperelliptic with an imaginary model. We make use of the $(64, 29)$-configuration to compute the equation of $\mathcal{D}$ and this configuration does not depend on $\mathcal{C}$ so the nature of this curve does not matter in theory. In practice, when $\mathcal{C}$ is also hyperelliptic (with an imaginary model), the link between the two curves is clearer because the description of the 2-torsion is similar and working on $\mathcal{C}$ is as if we were working directly on $\mathcal{D}$ (just replace η_X functions by η functions on $\mathcal{D}$).

So in our exposition we assume that $\mathcal{C} : Y^2 = \prod_{i=1}^{7}(X - r_i)$ is hyperelliptic. The eighth Weierstrass point is r_8, the unique point at infinity O. We use similar notations as in the genus 2 case. There are 64 2-torsions points a_i, a_{ij}, a_{ijk} and a basis $\eta_1, \ldots, \eta_8$ of the η_a functions (which are here η_X functions) for $a \in J[2]$ is of cardinality 8. As before, the 2-torsion points in the trope Z_{a_8} are the 8 $\phi(a_i)$ and the 21 $\phi(a_{ij})$ the tropes can be computed by linear algebra and the image of a 2-torsion point a in $\mathbb{P}^7$ can be obtained intersecting all the 29 tropes Z_{a_i+a} and $Z_{a_{ij}+a}$ (this can be optimized obviously, because 7 among them is enough).

The $(64, 29)$-configuration holds properties that the $(64, 28)$-configuration does not have. Let $i \in \{1, \ldots, 7\}$. As the images of the points $\{a_{i1}, \ldots, a_{i7}, a_i\}$ are in the trope Z_{a_8}, then the trope $Z_{a_8+a_i} = Z_{a_i}$ contains the points $\{\phi(a_{i1}+a_i), \ldots, \phi(a_{i7}+a_i), \phi(a_i+a_i)\} = \{\phi(a_1), \ldots, \phi(a_8)\}$. Thus, the intersection of the 8 tropes $\{Z_{a_1}, \ldots, Z_{a_8}\}$ is equal to $\{\phi(a_1), \ldots, \phi(a_8)\}$ and in fact, any 4 tropes among these 8 have this intersection. A last property we use is that for any triple of points among $\{\phi(a_1), \ldots, \phi(a_8)\}$, there always is a trope not in $\{Z_{a_1}, \ldots, Z_{a_8}\}$ which contain these three points and no other among them. All these properties can be proved by brute force using Proposition 7. There are obviously 64 8-tuple of tropes having similar properties (just shift by a 2-torsion point).

We choose the tropes $Z_{a_{ij}}$ for $ij \in \{24, 37, 67\}$ and $Z_{a_{ijk}}$ for $ijk \in \{123, 145, 167, 256, 345\}$ so that the point $\phi(a_i)$ for $i \in \{1, \ldots, 8\}$ is contained in exactly three of these 8 tropes. For any a_i, this gives 3 tropes and adding the four tropes $\{Z_{a_1}, \ldots, Z_{a_4}\}$, we obtain 7 equations from which we deduce $\phi(a_i)$ in $\mathbb{P}^7$. So computing 12 tropes is enough to obtain the image of the eight 2-torsion points $a_1, \ldots, a_8$ in $\mathbb{P}^7$. If the basis $\eta_1, \ldots, \eta_8$ is defined using 8 of the 12 torsions points used for these 12 tropes, then we only need to compute 4 tropes.

Once we have $\{\phi(a_1), \ldots, \phi(a_8)\}$ in $\mathbb{P}^7$, we can do the parameterisation. The four tropes $\{Z_{a_1}, \ldots, Z_{a_4}\}$ give 4 equations. This time, we fix two points instead of one, which give us 2 others equations. The rest is similar as in the genus 2 case.

In the case the curve $\mathcal{C}$ is non-hyperelliptic, then we can compute all the tropes and the image of the 2-torsion points and look for 4 tropes intersecting in 8 points, and proceding as above. This is not optimal.

4 Computing equations for the isogeny

Once we have the equation of the hyperelliptic curve $\mathcal{D}$ of genus 2 or 3, we want to compute rational fractions expliciting the isogeny. The algorithm is composed as follows

- compute the image by the isogeny of a single formal point at low precision;
- extend this image at a big enough precision;
- use this image to compute the rational fractions using continuous fractions.

In the first subsection we will define the rational fractions we want to compute and recall the results of [10] (genus 2 case only) for doing the second and third step. For the first step, the method given in [10] is not efficient so we present a better solution in the last subsection.

4.1 Rational fractions describing the isogeny

See [10, Section 6.1] for more details in genus 2. Let $g \in \{2,3\}$. Assume we have $\mathcal{D}$ given by an affine singular model $Y^2 = h_{\mathcal{D}}(X)$, where $h_{\mathcal{D}}$ is of degree $2g+1$. Let $O_{\mathcal{D}}$ be the point at infinity. Then $(2g-2)O_{\mathcal{D}}$ is a canonical divisor and a point in the Jacobian $J_{\mathcal{D}}$ of $\mathcal{D}$ can be written generically as $z = Q_1 + \ldots + Q_g - gO_{\mathcal{D}}$, where $O_{\mathcal{D}} \notin \{Q_1, \ldots, Q_g\}$ and for all i in $\{1, \ldots, g\}$, $-Q_i \notin \{Q_1, \ldots, Q_g\}$. Such a divisor can be represented by its Mumford coordinates. For $g = 2$, define

$$\mathbf{s}(z) = X(Q_1) + X(Q_2), \qquad \mathbf{p}(z) = X(Q_1)X(Q_2)$$
$$\mathbf{q}(z) = \frac{Y(Q_2) - Y(Q_1)}{X(Q_2) - X(Q_1)} \qquad \mathbf{r}(z) = \frac{Y(Q_1)X(Q_2) - Y(Q_2)X(Q_1)}{X(Q_2) - X(Q_1)}.$$

and for $g = 3$ define

$$\begin{aligned}
\mathbf{s}(z) &= X(Q_1) + X(Q_2) + X(Q_3),\\
\mathbf{p}(z) &= X(Q_1)X(Q_2) + X(Q_1)X(Q_3) + X(Q_2)X(Q_3),\\
\mathbf{a}(z) &= X(Q_1)X(Q_2)X(Q_3),\\
\mathbf{r}(z) &= \frac{((X(Q_2)-X(Q_3))Y(Q_1)+(X(Q_3)-X(Q_1))Y(Q_2)+(X(Q_1)-X(Q_2))Y(Q_3))}{(X(Q_1)-X(Q_2))(X(Q_1)-X(Q_3))(X(Q_2)-X(Q_3))},\\
\mathbf{t}(z) &= \frac{(X^2(Q_2)-X^2(Q_3))Y(Q_1)+(X^2(Q_3)-X^2(Q_1))Y(Q_2)+(X^2(Q_1)-X^2(Q_2))Y(Q_3)}{((X(Q_1)-X(Q_2))(X(Q_1)-X(Q_3))(X(Q_2)-X(Q_3))},\\
\mathbf{e}(z) &= \frac{(X^2(Q_2)X(Q_3)-X(Q_2)X^2(Q_3))Y(Q_1)+(X(Q_1)X^2(Q_3)-X^2(Q_1)X(Q_3))Y(Q_2)+(X^2(Q_1)X(Q_2)-X(Q_1)X^2(Q_2))Y(Q_3)}{(X(Q_1)-X(Q_2))(X(Q_1)-X(Q_3))(X(Q_2)-X(Q_3))},
\end{aligned}$$

The Mumford representation of z is $< X^2 - \mathbf{s}(z)X + \mathbf{p}(z), \mathbf{q}(z)X + \mathbf{r}(z) >$ in genus 2 and $< X^3 - \mathbf{s}(z)X^2 + \mathbf{p}(z)X - \mathbf{a}(z), \mathbf{r}(z)X^2 - \mathbf{t}(z)X + \mathbf{e}(z) >$ in genus 3. Let now $F : \mathcal{C} \to J_{\mathcal{D}}$ be the function $F(P) = f(P - O_{\mathcal{C}})$ (recall that f is the isogeny, and we denote here by $O_{\mathcal{C}}$ the unique point at infinity of an imaginary model of $\mathcal{C}$). As for every point $P = (u, -v)$ on $\mathcal{C}$ we have that $F(-P) = F((u,-v)) = -F(P)$, and as $v^2 = h_{\mathcal{C}}(u)$, we deduce that there exists rational fractions $\mathbf{S}$, $\mathbf{P}$, $\mathbf{Q}$, $\mathbf{R}$ when $g = 2$ satisfying

$$\mathbf{s}(F(P)) = \mathbf{S}(u), \quad \mathbf{p}(F(P)) = \mathbf{P}(u), \quad \mathbf{q}(F(P)) = v\mathbf{Q}(u), \quad \mathbf{r}(F(P)) = v\mathbf{R}(u),$$

and $\mathbf{S}$, $\mathbf{P}$, $\mathbf{A}$, $\mathbf{R}$, $\mathbf{T}$, $\mathbf{E}$ when $g = 3$ satisfying

$$\mathbf{s}(F(P)) = \mathbf{S}(u), \quad \mathbf{p}(F(P)) = \mathbf{P}(u), \quad \mathbf{a}(F(P)) = \mathbf{A}(u),$$
$$\mathbf{r}(F(P)) = v\mathbf{R}(u), \quad \mathbf{t}(F(P)) = v\mathbf{T}(u), \quad \mathbf{e}(F(P)) = v\mathbf{E}(u),$$

and such that $F((u,v)) =< X^2 - \mathbf{S}(u)X + \mathbf{P}(u), v(\mathbf{Q}(u)X + \mathbf{R}(u)) >$ or $F((u,v)) =< X^3 - \mathbf{S}(u)X^2 + \mathbf{P}(u)X - \mathbf{A}(u), v(\mathbf{R}(u)X^2 - \mathbf{T}(u)X + \mathbf{E}(u)) >$ in the Jacobian $J_{\mathcal{D}}$ of $\mathcal{D}$ in Mumford coordinates.

The degrees of these rational fractions is bounded by 2ℓ, 2ℓ, $3\ell+3$, $3\ell+3$ respectively when $g = 2$.

4.2 Computing the rational fractions from the image of a single formal point

See [10, Section 6.2] for more details in genus 2. Again $g \in \{2, 3\}$. The morphism $F : \mathcal{C} \to J_{\mathcal{D}}$ induces a map $F^* : H^0(J_{\mathcal{D}}, \Omega^1_{J_{\mathcal{D}}/K}) \to H^0(\mathcal{C}, \Omega^1_{\mathcal{C}/K})$. It is a classical result that a basis of $H^0(\mathcal{C}, \Omega^1_{\mathcal{C}/K})$ is given by dX/Y, ..., $X^{g-1}dX/Y$. Identifying $J_{\mathcal{D}}$ with $\mathcal{D}^{(g)}$ ($\mathcal{D}^g$ quotiented by permutations) we can see $H^0(J_{\mathcal{D}}, \Omega^1_{J_{\mathcal{D}}/K})$ as the invariant subspace of $H^0(\mathcal{D}^{(g)}, \Omega^1_{\mathcal{D}^{(g)}/K})$ by the permutation of g factors. A basis of this space is $dX_1/Y_1 + \ldots + dX_g/Y_g$, ..., $X_1^{g-1}dY_1/Y_1 + \ldots + X_g^{g-1}dX_g/Y_g$. Let $(m_{i,j})_{1\le i,j\le g}$ be the matrix of F^* with respect to these two bases. Thus for $i \in \{1, \ldots, g\}$

$$F^*(X_1^{i-1}dX_1/Y_1 + \ldots + X_g^{i-1}dX_g/Y_g) = (m_{1,i} + \ldots + m_{g,i}X^{g-1})dX/Y.$$

Let $P = (u, v)$ be a point on $\mathcal{C}$ such that $v \neq 0$ and let Q_i be g points on $\mathcal{D}$ and as in the previous subsection, such that $F(P)$ is the class of $Q_1 + \ldots + Q_g - gO_{\mathcal{D}}$. Let t be a formal parameter and set $L = K((t))$. Define $u(t) = u + t$ and $v(t)$ as the square root of $h_{\mathcal{C}}(u(t))$ which is equal to v when $t = 0$. The point $P(t) = (u(t), v(t))$ lie on $\mathcal{C}(L)$. The image of $P(t)$ by F is the class of $Q_1(t) + \ldots + Q_g(t) - gO_{\mathcal{D}}$ for g L-points $Q_1(t)$, ..., $Q_g(t)$ on $\mathcal{D}(L)$. We explain in the next subsection how to compute them at a given precision. Write $Q_i(t) = (x_i(t), y_i(t))$. The coordinates satisfy the non-singular first-order system of differential equations for $i \in \{1, \ldots, g\}$

$$\begin{cases} \frac{x_1^{i-1}\dot{x}_1(t)}{y_1(t)} + \ldots + \frac{x_g^{i-1}\dot{x}_g(t)}{y_g(t)} = \frac{(m_{1,i}u(t)^0 + \ldots + m_{g,i}u(t)^{g-1})\dot{u}(t)}{v(t)}, \\ y_i(t)^2 = h_{\mathcal{D}}(x_i(t)). \end{cases} \tag{9}$$

This system can be used to compute the rational fractions of Section 4.1 in three steps. Indeed, assume we have been able to compute for a single point $(u(t), v(t))$ the g points $(x_j(t) + O(t^g), y_j(t) + O(t^g))$ at precision g.

1. Looking at coefficients of degrees from 0 to $g-1$ in the first line of Equation (9) for a fixed index i gives g equations with the g unknown $m_{1,i}$, ..., $m_{g,i}$ that we can solve. Thus we obtain the numbers $m_{j,i}$ for $i, j \in \{1, \ldots, g\}$.

2. Now, we want to increase the accuracy of the formal expansions. This can be done degree by degree. The RHS of the first line of Equation (9) is known up to any given precision. Assume we know $x_j(t)$ and $y_j(t)$ up to $O(t^d)$ for all j (and their derivatives up to $O(t^{d-1})$). If $c_{j,d}$ is the coefficient of degree d of $x_j(t)$, then the coefficient of degree $d-1$ of its derivative is $dc_{j,d}$. For $j \in \{1, \ldots, g\}$, define $\dot{x}_j^{d-1}(t)$ as the sum of $\dot{x}_j(t)$ up to degree $d-2$ plus $dc_{j,d}t^{d-1}$, where $c_{j,d}$ is a variable, plug it in Equation (9) and deduce for each i an equation in the $c_{j,d}$ looking at the coefficients of degree $d-1$ in t. This give g equations with g unknown that we solve. The second line of Equation (9) allows us to compute $y_1(t) + O(t^{d+1})$ and $y_2(t) + O(t^{d+1})$.

3. Do rational reconstruction using continued fractions to deduce the rational fractions. For example, for $\mathbf{S}$ in genus 2, put $s(t) = x_1(t) + x_2(t)$ and remark that $s(t) = s_{\leq 0}(t) + 1/(1/(s(t) - s_{\leq 0}(t)))$, where $s_{\leq 0}(t)$ designates the sum of the monomials of degree less or equal to 0 in $s(t)$. So while the degree of s in t is > 0, put $s(t) = 1/(s(t) - s_{\leq 0}(t))$ in keeping track of the $s_{\leq 0}(t)$. Then sum up all. This gives a rational fraction in t. Evaluate it in $t - u(0)$ to obtain $\mathbf{S}(t)$.

In practice, these three steps are negligible with respect to the time of computation of the image of the single formal point. See Section 6.

4.3 Computing the image of a formal point

Let $L = K[t]/(t^g)$ and $P(t) = (u(t), v(t)) \in \mathcal{C}(L)$. We want to compute $F(P(t))$ which is in the Jacobian of $\mathcal{D}$ over the field L.

We could want to do it using intersection of tropes. This seems to us that this imply we have to look at the divisor $Y_{F(P(t))}$ (which is not symmetric), seen as $X_{P(t)-O_\mathcal{C}}$. A zero-cyle we could consider to obtain this divisor would be $[P(t) - O_\mathcal{C}] + [Q] + [-(P(t) - O_\mathcal{C}) - Q] - 3[0]$ for some point $Q \in J$, producing a function in $H^0(J_L, \mathcal{O}_{J_L}(3X))$, that is a level 3 function. Thus, we would need a basis a level 3 functions and algebraic relations between them, which is costly to compute. This is the idea in [10, Section 6.3].

We propose to compute $F(P(t))$ in two step. First we compute the image of $P(t)$ in the Kummer surface of $\mathcal{D}$ and then we lift this point in the Jacobian. The lifting step is easy to do in genus 2 if the Kummer surface is constructed as in [7] or as in [31, 24, 30] in genus 3. Thus for any given representation of the Kummer variety, we can search for a linear change of variables allowing one to go from it to the good representation. We recall first what these two good representations are.

Standard representation of the Kummer surface. Let $\mathcal{D} : Y^2 = h_\mathcal{D}(X) = \sum_{i=0}^5 c_i X^i$ be a hyperelliptic curve and $x = (x_1, y_1) + (x_2, y_2) - 2O_\mathcal{D}$ a generic reduced divisor. Let $F_0(x_1, x_2) = 2c_0 + c_1(x_1 + x_2) + 2c_2(x_1x_2) + c_3(x_1 + x_2)x_1x_2 + 2c_4(x_1x_2)^2 + c_5(x_1 + x_2)(x_1x_2)^2$ and $\beta_0(x) = (F_0(x_1, x_2) - 2y_1y_2)/(x_1 - x_2)^2$. Put

$$K_2 = e_2^2 - 4e_1e_3, \qquad K_1 = -2(2c_0e_1^3 + c_1e_1^2e_2 + 2c_2e_1^2e_3 + c_3e_1e_2e_3 + 2c_4e_1e_3^2 + c_5e_2e_3^2),$$

$$K_0 = (c_1^2 - 4c_0c_2)e_1^4 - 4c_0c_3e_1^3e_2 - 2c_1c_3e_1^3e_3 - 4c_0c_4e_1^2e_2^2 + 4(c_0c_5 - c_1c_4)e_1^2e_2e_3 +$$
$$(c_3^2 + 2c_1c_5 - 4c_2c_4)e_1^2e_3^2 - 4c_0c_5e_1e_2^3 - 4c_1c_5e_1e_2^2e_3 - 4c_2c_5e_1e_2e_3^2 - 2c_3c_5e_1e_3^3 - c_5^2e_3^4.$$

Then an equation for the Kummer surface of the Jacobian of $\mathcal{D}$ is $\kappa_{cf} : K_2e_4^2 + K_1e_4 + K_0$ in the variables e_1, e_2, e_3, e_4.

The image of the divisor x is $(1 : x_1 + x_2 : x_1x_2 : \beta_0(x))$ in the Kummer surface associated to $\mathcal{D}$, seen in $\mathbb{P}^3$, and represented by the equation κ_{cf}. In the case where the divisor x is of the form $(x_1, y_1) - O_\mathcal{D}$, its image is $(0 : 1 : x_1 : c_5x_1^2)$ and the image of $0 \in J_\mathcal{D}$ is $(0 : 0 : 0 : 1)$. Thus, if we have a point in the Kummer surface represented in this way, and using the equation of $\mathcal{D}$, it is easy to deduce the two corresponding opposite points in the Jacobian.

Note that as we need to compute the image of only one formal point in our algorithm, this step is done only one time. We have to make a choice between the two opposite points and we do not have the compatibility problems we would have if we had to make this choice several times.

Representation of the Kummer variety of dimension 3. The preceding representation has been generalized in genus 3 in [31, Chapter 3]. The author defines for a genus 3 hyperelliptic curve of the form $Y^2 = h_{\mathcal{D}}(X)$, with $h_{\mathcal{D}}(X)$ of degree 7, eight functions defining a map from the Jacobian to the Kummer, seen in $\mathbb{P}^7$. In particular, for a generic reduced divisor $x = (x_1, y_1)+(x_2, y_2)+(x_3, y_3)-3O_{\mathcal{D}}$, the four first functions are 1, $x_1+x_2+x_3$, $x_1x_2+x_1x_3+x_2x_3$, $x_1x_2x_3$ so that lifting to the Jacobian is easy. We do not write here all the equations but refer the reader to [24, Section 2], where the author extends the embedding to the Kummer to non-generic divisors. On the other side, the author of [30] has defined eight functions $\xi_1, \ldots, \xi_8$ on an arbitrary hyperelliptic curve of genus 3 (over a field of characteristic different of 2) defining an embedding to the Kummer (see [30, Section 3] for the definition and the relation with the eight functions of [31, 24]). These are the functions we use and we denote by κ_s the associated set of equations for the Kummer variety, which is described by 1 quadric and 34 quartics, as already said.

From a representation to another. We explain now how to change representation. Recall that we started from the curve $\mathcal{C}$ and through a basis $\eta_1, \ldots, \eta_{2^g}$ of η_X functions, which are level 2 functions, we can obtain equations $\kappa_{\mathcal{D}}$ of the Kummer variety of the Jacobian of $\mathcal{D}$ and the image of all the 2-torsions points in it. On the other side, starting from the equation of $\mathcal{D}$, we can compute easily the equations κ_{cf} ($g = 2$) or κ_s ($g = 3$) and the image of all the 2-torsions points in them.

We insist on the fact that working on $\mathcal{D}$ is almost free as we do not have to care on the isogeny. Moreover, it is not possible (for now) to write a η_X function as a combination of η functions defined over $\mathcal{D}$ or as a combination of the functions used to define κ_{cf} or κ_s, because in the first case we work on $J = J_{\mathcal{C}}$ and in the others on $J_{\mathcal{D}}$. We need for it to have for $x \in J_{\mathcal{C}}$ the point $f(x) \in J_{\mathcal{D}}$, which is what we want to compute.

First start with the genus 2 case. We look for a change of variables to go from the quartic $\kappa_{\mathcal{D}}$ to the quartic κ_{cf} of the form

$$\begin{array}{rclcrcl} S_1 &=& m_1Z_1 + m_2Z_2 + m_3Z_3 + m_4Z_4, & & S_2 &=& m_5Z_1 + m_6Z_2 + m_7Z_3 + m_8Z_4, \\ S_3 &=& m_9Z_1 + m_{10}Z_2 + m_{11}Z_3 + m_{12}Z_4, & & S_4 &=& m_{13}Z_1 + m_{14}Z_2 + m_{15}Z_3 + m_{16}Z_4, \end{array}$$

such that $\kappa_{cf}(S_1, S_2, S_3, S_4) = \kappa_{\mathcal{D}}(Z_1, Z_2, Z_3, Z_4)$. We can do a Gröbner basis with the 16 unknown $m_1, \ldots, m_{16}$, but in practice, this does not work. We can add some conditions noting that we can send $0 = (0 : 0 : 0 : 1) \in \kappa_{\mathcal{D}}$ to $0 = (0 : 0 : 0 : 1) \in \kappa_{cf}$. This gives $m_4 = m_8 = m_{12} = 0$. We can not put $m_{16} = 1$ despite projectivity because of the equality we want between the Kummers quartics. In practice, this works very well, but it requires to compute the equation $\kappa_{\mathcal{D}}$ which is costly.

In the case we do not want to compute this equation, we can look for a transformation sending the 2-torsions points in $\kappa_{\mathcal{D}}$ to the 2-torsions points in κ_{cf}. We also want to preserve the group structures. We assume that we have all the 2-torsion points in the Kummer κ_{cf} as they can be computed directly and this computation does not depend on ℓ, while we have on the $\kappa_{\mathcal{D}}$ representation the 2-torsions points associated to $a_1, \ldots, a_6$, a_{12}, a_{34} and a_{35}. The first six are known since we needed them to compute the equation of $\mathcal{D}$ (in the optimized version) and the last three are obtained looking at the intersections $\{Z_{a_{12}} = 0, Z_{a_{34}} = 0, Z_{a_{35}} = 0\}$, $\{Z_{a_3} = 0, Z_{a_{12}} = 0, Z_{a_{34}} = 0\}$, $\{Z_{a_3} = 0, Z_{a_{12}} = 0, Z_{a_{35}} = 0\}$ respectively (and these tropes have been already computed to find the equation of $\mathcal{D}$ except for Z_{a_3} which can be computed during the computation of the other tropes adding the cost of the evaluation of η_{a_3} at two

points). We send 0 to 0, giving us the conditions $m_4 = m_8 = m_{12} = 0$. We can fix $m_{16} = 1$. Then, with three *for* loops, we test all the 2-torsion points in κ_{cf} onto which the points $\phi(a)$ can be send to, for $a \in \{a_3, a_4, a_5\}$. For each point, this give 3 conditions on the m_i (3 and not 4 because of the projectivity). Moreover, as we want to preserve the group structure, for a choice of the images of a_3, a_4 and a_5, this fix an image for a_{34} and a_{35}. Thus we obtain $4 + 3 \times 5 = 19$ conditions on the 16 m_i and we compute a Gröbner basis. This can give many solutions and we can verify if the points in the Kummer $\kappa_{\mathcal{D}}$ associated to the 2-torsion points a_1, a_2 and a_{12} are sent to 2-torsions points in κ_{cf}. In practice, this method is fast enough.

In the genus 3 case, we proceed with the same idea to go from $\kappa_{\mathcal{D}}$ to κ_s. This time we have 64 unknown variables. We fix a basis of the 2-torsion points in the Jacobian of $\mathcal{C}$ and we want to send 0 to 0 and the points in this basis to 2-torsion points of the Jacobian of $\mathcal{D}$, seen in $\mathbb{P}^7$ by the map defined by the functions used to compute κ_s, and preserving the group structure. Using 4 *for* loops, we obtain enough conditions to obtain the transformation. However, in practice, this takes too many time (many hours in our examples) so that we have to improve this step. A solution consists to compute only the quadric in the equations of the Kummer varieties $\kappa_{\mathcal{D}}$ and κ_s. But for the former, the computation depends on ℓ. We look for a transformation that sends a quadric to the other, which give us many conditions on the 64 unknown variables. Then we proceed in the same way but with only 3 *for* loops. In our examples, it took around half an hour to test all the possibilities (but a solution was found in a few minutes). This is still not satisfactory and this step has to be improved.

Image of a single point. Let $(u(t), v(t))$ be a point on $\mathcal{C}(L)$. We want the image of $P(t) = (u(t), v(t)) - O$ in the Kummer surface represented by κ_{cf}. We can not directly compute the image of P by the η_X function as this is a point in which these functions have a pole. But this is not the case of its multiples in the Jacobian. It is well-known that Kummer surface are not endowed with a group structure but a pseudo-addition law can be defined in it. This means that if we have the points $\pm P_1$, $\pm P_2$, $\pm(P_1 + P_2)$ in the Kummer, then we can compute $\pm(P_1 - P_2)$ in it. Let $m > 1$ be an integer. Compute the image of $mP(t)$, $(m+1)P(t)$ and $(2m+1)P(t)$ in the Kummer $\kappa_{\mathcal{D}}$ (compute $(\eta_1(nP(t)) : \ldots : \eta_4(nP(t)))$ for $n \in \{m, m+1, 2m+1\}$), then use the transformation to deduce the corresponding points in the Kummer surface represented by κ_{cf}, do the pseudo-addition to deduce the image of $P(t)$ by the isogeny in the Kummer κ_{cf} and deduce from it a point in the Jacobian of $\mathcal{D}(L)$. Thus, using κ_{cf} has the double advantage that we can do pseudo-addition in it and that lifting to the Jacobian is easy.

This idea also works in genus 3. See [30] for the pseudo-addition.

4.4 Example for hyperelliptic curves of genus 3

As the moduli space of hyperelliptic curves is of dimension 5 in the 6-dimensional moduli space of genus 3 curves, if we start from a hyperelliptic curve of genus 3 and a maximal isotropic subgroup of the ℓ-torsion, the corresponding isogenous curve is generically non-hyperelliptic. The nature of the isogenous curve can be established looking for the type of the configuration or the equations describing the kummer threefold, in particular the presence of a quadric.

We have built examples of isogenous hyperelliptic curves using [34, Satz 4.4.2], which states that if the Jacobian of $\mathcal{C}$ has complex multiplication by $\mathcal{O}_K$ with $\mathbb{Q}(i) \subset K$ and is simple, then $\mathcal{C}$ is hyperelliptic, and using the fact that an isogeny preserves the field of complex multiplication. Curves with these properties are provided in [34], from which we have build examples on finite

fields. For instance, the curves on $\mathbb{F}_{120049}$

$$\mathcal{C} : X^7 + 118263X^5 + 44441X^3 + 81968X,$$

$$\mathcal{D} : X^7 + 87967X^6 + 102801X^5 + 70026X^4 + 30426X^3 + 37313X^2 + 77459X,$$

are $(5, 5, 5)$-isogenous. The Mumford coordinates of the generators of the isotropic subgroup are

$$T_1 =< X^3 + 90254X^2 + 103950X + 34646, 63966X^2 + 19029X + 62065 >,$$

$$T_2 =< X^3 + 29700X^2 + 10920X + 14179, 77142X^2 + 66846X + 84040 >,$$

$$T_3 =< X^3 + 119858X^2 + 87344X + 82114, 51063X^2 + 95007X + 64731 >$$

and the isogeny is described by the following equations
$\mathbf{S} = (26590u^{13} + 38875u^{12} + 11144u^{11} + 39196u^{10} + 48794u^9 + 80531u^8 + 56286u^7 + 42203u^6 + 49314u^5 + 34405u^4 + 28021u^3 + 82360u^2 + 112863u + 64433)/(u^8 + 107005u^7 + 34717u^6 + 96329u^5 + 81848u^4 + 90494u^3)$,
$\mathbf{P} = (13588u^{13} + 99739u^{12} + 60510u^{11} + 3267u^{10} + 56188u^9 + 27913u^8 + 79606u^7 + 79490u^6 + 39953u^5 + 101739u^4 + 118959u^3 + 88791u^2 + 59459u + 44419)/(u^8 + 107005u^7 + 34717u^6 + 96329u^5 + 81848u^4 + 90494u^3)$,
$\mathbf{A} = (87680u^{12} + 77147u^{11} + 47767u^{10} + 91104u^9 + 101830u^8 + 51358u^7 + 106657u^6 + 1059u^5 + 28890u^4 + 72926u^3 + 40489u^2 + 20614u + 13587)/(u^7 + 107005u^6 + 34717u^5 + 96329u^4 + 81848u^3 + 90494u^2)$,
$\mathbf{R} = (12306u^{20} + 37665u^{19} + 84758u^{18} + 83076u^{17} + 51365u^{16} + 42432u^{15} + 76312u^{14} + 63248u^{13} + 97292u^{12} + 25304u^{11} + 38304u^{10} + 26932u^9 + 108075u^8 + 40558u^7 + 5431u^6 + 22057u^5 + 100345u^4 + 113409u^3 + 73221u^2 + 39576u + 78248)/(u^{16} + 107005u^{15} + 32931u^{14} + 103407u^{13} + 67011u^{12} + 105334u^{11} + 109571u^{10} + 59270u^9 + 83877u^8 + 34998u^7 + 98548u^6 + 24580u^5)$,
$\mathbf{T} = (39012u^{20} + 43063u^{19} + 41666u^{18} + 90531u^{17} + 18614u^{16} + 112658u^{15} + 99705u^{14} + 15123u^{13} + 56542u^{12} + 44122u^{11} + 40721u^{10} + 103078u^9 + 29236u^8 + 114961u^7 + 99184u^6 + 32122u^5 + 94412u^4 + 42358u^3 + 4616u^2 + 66587u + 86686)/(u^{16} + 107005u^{15} + 32931u^{14} + 103407u^{13} + 67011u^{12} + 105334u^{11} + 109571u^{10} + 59270u^9 + 83877u^8 + 34998u^7 + 98548u^6 + 24580u^5)$,
$\mathbf{E} = (77510u^{19} + 5507u^{18} + 57109u^{17} + 115038u^{16} + 83721u^{15} + 32646u^{14} + 7900u^{13} + 28888u^{12} + 83235u^{11} + 112193u^{10} + 99943u^9 + 38123u^8 + 70050u^7 + 48716u^6 + 15860u^5 + 65499u^4 + 38669u^3 + 35838u^2 + 82517u + 82266)/(u^{15} + 107005u^{14} + 32931u^{13} + 103407u^{12} + 67011u^{11} + 105334u^{10} + 109571u^9 + 59270u^8 + 83877u^7 + 34998u^6 + 98548u^5 + 24580u^4)$.

5 Algebraic theta functions

The η_a functions we have used which are η and η_X functions associated to zero-cycles constructed from 2-torsions points are algebraic theta functions of level 2, up to a factor. There are formulas allowing one to write the equation of the hyperelliptic curves and the non-hyperelliptic curves of genus 2 and 3 from the algebraic theta functions. The obstruction we have to face on to use these formulas comes from the choice of the divisor y. Indeed, all the η_a functions have value 1 at y so that these differents functions are not compatible between them. By compatible, we mean that we want these η_a functions to satisfy the algebraic relations of the analytic theta functions. In this section, we begin to recall the definition and some fundamental properties of the analytic theta functions, then we explain how to make the η_a functions compatible in genus 2 and 3 so that we can use theta based formulas for computing isogenies.

5.1 Analytic theta functions

Analytic theta functions have been widely studied and are well understood from many points of views. Good references are [22, 23, 1]. In this section, g is an integer ≥ 1.

Let $z \in \mathbb{C}^g$ and Ω in the Siegel upper-half space $\mathcal{H}_g$ (the $g \times g$ symmetric matrices over the complex numbers with positive definite imaginary part). The classical theta function is

$$\theta(z, \Omega) = \sum_{n \in \mathbb{Z}^g} \exp\left(i\pi\, {}^t n \Omega n + 2i\pi\, {}^t n z\right)$$

and the classical theta function with characteristic (a, b), where $a, b \in \mathbb{Q}^g$, is

$$\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z, \Omega) = \exp\left(i\pi\, {}^t a \Omega a + 2i\pi\, {}^t a (z + b)\right) \theta(z + \Omega a + b, \Omega). \tag{10}$$

Let n be an integer ≥ 2 and Ω fixed. Then the n^{2g} theta functions of the form $\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z, \Omega)^n$ for a, b representatives of the classes of $\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g$ are said to be of level n and n^g linearly independent functions between them provide an embedding from the abelian variety seen as the torus $\mathbb{C}^g/(\Omega\mathbb{Z}^{2g} + \mathbb{Z}^{2g})$ to $\mathbb{P}^{n^g-1}(\mathbb{C})$ unless $n = 2$ where the embedding is only from the Kummer variety $\mathbb{C}^g/(\Omega\mathbb{Z}^{2g} + \mathbb{Z}^{2g})/\sim$, for $\sim$ the equivalence relation such that $z \sim -z$. Many bases and the relations between them can be found in [8, Chapitre 3].

Let $a, b \in \mathbb{Q}^g$ and $m_1, m_2 \in \mathbb{Z}^g$. According to [22, Page 123] we have

$$\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z + \Omega m_1 + m_2, \Omega) = \exp\left(-i\pi\, {}^t m_1 \Omega m_1 - 2i\pi\, {}^t m_1 z\right) \exp\left(2i\pi({}^t a m_2 - {}^t b m_1)\right) \theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z, \Omega),$$

$$\text{and} \qquad \theta\left[\begin{smallmatrix} a+m_1 \\ b+m_2 \end{smallmatrix}\right](z, \Omega) = \exp\left(2i\pi\, {}^t a m_2\right) \theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z, \Omega). \tag{11}$$

Moreover, using the definitions, we can see that

$$\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](-z, \Omega) = \theta\left[\begin{smallmatrix} -a \\ -b \end{smallmatrix}\right](z, \Omega).$$

Let $\mathcal{C}$ be a smooth projective curve of genus g over $\mathbb{C}$ and W be the image of the symmetrical product $\mathcal{C}^{(g-1)}$ in $\mathrm{Pic}^{g-1}(\mathcal{C})$ (as in Section 2.1). A theorem of Riemann asserts that there exists a theta characteristic κ (κ is a divisor class of degree $g-1$ and 2κ is the canonical class), called the Riemann's constant, such that Θ, the zero divisor of the classical theta function $\theta(z, \Omega) = \theta\left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](z, \Omega)$, is W translated by κ (see [1, Theorem 11.2.4]). Moreover, $\mathcal{O}_{J_\mathcal{C}}(\Theta)$ defines a principal polarization. Thus, for $g \in \{2, 3\}$, the 2^{2g} level 2 functions η_a (for the 2-torsion point a in $J_\mathcal{C}$) of the previous sections correspond over $\mathbb{C}$ to the functions $\eta_{a,b}(z) := \alpha_{a,b} \cdot \theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z, \Omega)^2 / \theta\left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](z, \Omega)^2$, for some constants $\alpha_{a,b}$, a and b representatives of the classes of $\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g$ and some Ω fixed (corresponding to $\mathcal{C}$). We want to multiply the η_a functions by constants such that these new functions verify the same algebraic relations as between the analytic theta functions. We speak then of algebraic theta functions. We begin with a result that will allow us to determine the constants $\alpha_{a,b}^2$ associated to the 2-torsion points $\Omega a + b$ and then we will use formulas to choose the good square roots.

From now on, let a, b be representatives of $\frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g}$. Using Equations (10) and (11), we have

$$\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z + \Omega a + b, \Omega) = \exp\left(-i\pi\, {}^t a \Omega a - 2i\pi\, {}^t a z + 4i\pi\, {}^t a b\right) \theta\left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](z, \Omega)$$

from which we deduce

$$\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z, \Omega) = \theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right]((z - \Omega a - b) + (\Omega a + b), \Omega) = \exp\left(i\pi\, {}^t a \Omega a - 2i\pi\, {}^t a z + 6i\pi\, {}^t a b\right) \theta\left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](z - \Omega a - b, \Omega).$$

And applying these equalities, we obtain

$$\eta_{a,b}(\Omega a+b)=\alpha_{a,b}\exp\left(-2i\pi\,{}^t a\Omega a\right)\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](0,\Omega)^2/\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](\Omega a+b,\Omega)^2$$

and

$$\eta_{a,b}(0)=\alpha_{a,b}\exp\left(2i\pi\,{}^t a\Omega a+4i\pi\,{}^t ab\right)\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](\Omega a+b,\Omega)^2/\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](0,\Omega)^2$$

if the denominators are not 0. Finally, the product of these two functions give us this fundamental relation

$$\eta_{a,b}(\Omega a+b)\eta_{a,b}(0)=\alpha_{a,b}^2\exp\left(4i\pi\,{}^t ab\right). \tag{12}$$

A lot of algrebraic relations between the analytic theta functions can be deduced from the two following propositions.

Proposition 8 (Riemann's theta formula)**.** *Let m_1,m_2,m_3,m_4 in $\mathbb{R}^{2g}$. Put $n_1=\frac{1}{2}(m_1+m_2+m_3+m_4)$, $n_2=\frac{1}{2}(m_1+m_2-m_3-m_4)$, $n_3=\frac{1}{2}(m_1-m_2+m_3-m_4)$, $n_4=\frac{1}{2}(m_1-m_2-m_3+m_4)$. Then*

$$\theta_{m_1}\theta_{m_2}\theta_{m_3}\theta_{m_4}=\frac{1}{2^g}\sum_{\alpha}\exp\left(4i\pi m_1'\,{}^t\alpha''\right)\theta_{n_1+\alpha}\theta_{n_2+\alpha}\theta_{n_3+\alpha}\theta_{n_4+\alpha},$$

where, for $m\in\mathbb{R}^{2g}$, we denote $m=(m',m'')$ and $\theta_m=\theta\left[\begin{smallmatrix}m'\\m''\end{smallmatrix}\right](0,\Omega)$ and where α runs over a complete set of representatives of $\frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g}$.

Proof. See [16, Chapter IV, Theorem 1]. □

Proposition 9 (Duplication formula)**.** *For a, b representatives of $\frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g}$,*

$$\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](z,\Omega)^2=\frac{1}{2^g}\sum_{\beta\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g}\exp\left(4i\pi\,{}^t a\beta\right)\theta\left[\begin{smallmatrix}0\\b+\beta\end{smallmatrix}\right](z,\frac{\Omega}{2})\theta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right](z,\frac{\Omega}{2}).$$

Proof. See [16, Chapter IV, Theorem 2]. □

5.2 Rosenhain invariants

A hyperelliptic curve of genus 2 can be written in the Rosenhain form $Y^2=X(X-1)(X-\mathfrak{r}_1)(X-\mathfrak{r}_2)(X-\mathfrak{r}_3)$, where over $\mathbb{C}$, we have

$$\mathfrak{r}_1=\frac{\theta_0^2\theta_1^2}{\theta_3^2\theta_2^2},\qquad \mathfrak{r}_2=\frac{\theta_1^2\theta_{12}^2}{\theta_2^2\theta_{15}^2},\qquad \mathfrak{r}_3=\frac{\theta_0^2\theta_{12}^2}{\theta_3^2\theta_{15}^2}.$$

Here, we denote the analytic theta constants (the theta functions for $z=0$ fixed) of level 2 using Dupont's notation

$$\theta_{b_0+2b_1+4a_0+8a_1}(\Omega):=\theta\left[\begin{smallmatrix}a/2\\b/2\end{smallmatrix}\right](0,\Omega)$$

for $a={}^t(a_0,a_1)$, $b={}^t(b_0,b_1)$ and $a_i,b_i\in\{0,1\}^2$. We drop the Ω when we work on a fixed abelian variety.

There are 16 theta constants and 6 among them are identically zero: the odd theta constants, that is, those for which ${}^t ab\equiv 1 \bmod 2$. Otherwise we speak of even theta constants.

We come back to the algebraic case with the notations of Section 3.2. Let e_1,e_2,f_1,f_2 be a symplectic basis of the 2-torsion of some hyperelliptic curve of genus 2 with an imaginary model. We want to find the 2-torsion point which is at the intersection of the tropes Z_a for a

2-torsion point a having odd characteristic. According to Proposition 5, if we put $a'' = \left(\begin{smallmatrix}1&1\\1&1\end{smallmatrix}\right)$, then the image in $\mathbb{P}^3$ of any of the six 2-torsion points having odd characteristic lie in the trope $Z_{a_0+a''}$, where a_0 is the shifting point of this proposition. The trope $Z_0 = Z_{a_6}$ contains the image of the points $\{a_1, \ldots, a_6\}$; thus $Z_{a_0+a''}$ contains the image of $\{a_1+a_0+a'', \ldots, a_6+a_0+a''\}$ and the intersection $\{Z_{a_1+a_0+a''} = 0, \ldots, Z_{a_6+a_0+a''}\}$ of six tropes is $\{a_0 + a''\}$. The 2-torsion point $a_0 + a''$ is thus the one corresponding to $z = 0$ (with respect to the choosen symplectic basis). Note that $a_0 + a'' \notin \{a_1, \ldots, a_6\}$ because otherwise the point $\left(\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right)$ would be in $Z_{a_0+a''}$ but it is of even characteristic.

Remark 10. This give another way of computing a_0: compute the unique point at the intersection of the six tropes Z_a with a of odd characteristic and add $\left(\begin{smallmatrix}1&1\\1&1\end{smallmatrix}\right)$ at the result.

Assume to simplify that we have computed all the tropes Z_a and that, thus, we know the images in $\mathbb{P}^3$ of all the 2-torsion points with respect to some basis of the level 2 functions. For all $a \in J_{\bar{K}}[2]$ and $a \notin \{a_1, \ldots, a_6\}$, we take a lift a' in $\mathbb{A}^4$ of its image in $\mathbb{P}^3$, evaluate all the tropes at a' and divide by the value obtained in evaluating Z_{a_6} at a' (because $\eta_{a_6}(a) = 1$) so that we obtain $(\eta_{a_1}(a), \ldots, \eta_{a_{45}}(a)) \in \mathbb{A}^{16}$.

As explained in the previous subsection, we want these theta functions to be compatible. Recall that $a'' = \left(\begin{smallmatrix}1&1\\1&1\end{smallmatrix}\right)$. Thus, following Equation 12, we compute $\eta_a(a_0 + a_2)\eta_a(a_0 + a_2 + a)$, for a with even characteristic, giving us $\alpha_a^2 \neq 0$. With Dupont's notation, we have until now the algebraic counterpart of θ_i^4/θ_0^4 ($\neq 0$ for $i \in \{0, 1, 2, 3, 4, 6, 8, 9, 12, 15\}$). Yet for the Rosenhain invariants, we need (the algebraic counterpart of) θ_i^2/θ_0^2 for $i \in \{1, 2, 3, 12, 15\}$ which we know, taking square roots, up to a sign. More precisely, we need $\frac{\theta_0^2}{\theta_3^2}$, $\frac{\theta_1^2}{\theta_2^2}$ and $\frac{\theta_{12}^2}{\theta_{15}^2}$ and we could obtain 8 curves because there are 2^3 possibilities of sign giving us 8 triples of Rosenhain invariants. One of them or its twist is isogenous to the starting curve $\mathcal{C}$ and this curve can be found comparing the cardinality of the Jacobians. But using the algebraic relations between the theta constants we can directly determine the good curve. Indeed, according to the Duplication formula, we have: $(\theta_4\theta_6)^2 = (\theta_0\theta_2)^2 - (\theta_1\theta_3)^2$ and taking square: $(\theta_4\theta_6)^4 = (\theta_0\theta_2)^4 + (\theta_1\theta_3)^4 - 2(\theta_0\theta_2\theta_1\theta_3)^2$ so that we can determine the value of $\mathfrak{r}_1$ (in the algebraic case). This property can be proven using the Duplication formula to write all the $\theta_i^2(\Omega)$ in function of $\theta_j(\Omega/2)$ for $j \in \{0, 1, 2, 3\}$ and comparing the two sides of the equality. Similarly, $\mathfrak{r}_2$ is determined using $(\theta_4\theta_9)^2 = (\theta_1\theta_{12})^2 - (\theta_2\theta_{15})^2$. This last property can be proven by the Duplication formula and can also be deduced from the first one looking at the action of the matrix $\begin{pmatrix} -1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & -1 \\ 1 & -1 & -1 & 0 \end{pmatrix}$ on the theta constants (see [16, Chapter 5, Theorem 2] or [8, Proposition 3.1.24]). Finally, note that $\mathfrak{r}_1\mathfrak{r}_2\mathfrak{r}_3 = \frac{\theta_0^4\theta_1^4\theta_{12}^4}{\theta_2^4\theta_3^4\theta_{15}^4}$ from which we deduce the value of $\mathfrak{r}_3$.

The fact that the Rosenhain invariants can be determined with the knowledge of quotients of fourth power of theta constants is not surprising as both are generators for the modular functions invariants by $\Gamma_2(2)$. Moreover, the functions θ_i^2/θ_0^2 are invariants for $\Gamma_2(2, 4)$ and the index $[\Gamma_2(2) : \Gamma_2(2, 4)]$ is 16 so that the choice of the square roots we have to take is determined by the choice of 4 well-choosen quotients (forming a basis) and at each choice corresponds an isomorphic curve. If we need the algebraic counterpart of the θ_i^2/θ_0^2 (this is of independent interest), we generate many relations from the Duplication formula as we have done before and do a Gröbner basis for determining relations between the unknown signs. We take a random choice of square roots for the 4 determining the system.

5.3 Non-hyperelliptic curves of genus 3

We focus now on the case of non-hyperelliptic curves $\mathcal{D}$ of genus 3 on a field K. Assume K is algebraically closed. We have seen that the Kummer variety of such a curve has a $(64, 28)$-configuration and we can apply similar techniques as in the hyperelliptic case to compute the tropes and the image of the 2-torsion points in $\mathbb{P}^7$. However, we do not know if there is a parameterization allowing one to recover the equation of the curve with these data. The only way we have found consists in using theta based formulas and the theory of bitangents (see [33, 25]). The following exposition is based on [27, 26] and we refer to these references for more details.

As the curve $\mathcal{D}/K$ is non-hyperelliptic, it can be embedded as a non-singular plane quartic in $\mathbb{P}^2$. We denote by x_1, x_2, x_3 the coordinates in this projective plane.

Definition 11. *A line l is called a bitangent of $\mathcal{D}$ if the intersection divisor $(l \cdot \mathcal{D})$ is of the form $2P + 2Q$ for some points P, Q of $\mathcal{D}$. If $P = Q$, the point P is called a hyperflex.*

Let $\mathcal{K}$ be the canonical bundle and let $\Sigma = \{L \in \mathrm{Pic}^2(\mathcal{D}) : L^2 = \mathcal{K}\}$ be the set of theta characteristic bundles. This set is composed of the two disjoint subsets $\Sigma_i = \{L \in \Sigma : h^0(L) = i\}$ of even ($i = 0$) and odd ($i = 1$) theta bundles. There is a canonical bijection between the set of bitangents, Σ_1 and the set of odd characteristics for a fixed symplectic basis of the 2-torsion. We can deduce from it

Proposition 12. *A smooth plane quartic has exactly 28 bitangents.*

The $(64, 28)$-configuration comes from this proposition. Indeed, if l is a bitangent and $(l \cdot \mathcal{D}) = 2P + 2Q$, then $2P + 2Q$ is a canonical divisor and $P + Q$ is a theta characteristic as in Section 2.1 (from which we can build the η and η_X functions). Then if l' is another bitangent giving us the points P' and Q', then the divisor $P' + Q' - P - Q$ is in W_{-P-Q} and it is a 2-torsion point. Only the 28 2-torsion points coming from bitangents are in W_{-P-Q}.

The equation of $\mathcal{D}$ as a plane quartic is determined and can be reconstructed knowing the equations of 7 bitangents forming an Aronhold system (see [6, 18]), which is a set of 7 bitangents such that if we take 3 bitangents among these 7, then the points at which these bitangents intersect the plane quartic do not lie on a conic in $\mathbb{P}^2$.

There exists 288 Aronhold system for a given plane quartic and we focus on the following one.

Proposition 13. *An Aronhold system of bitangents for a quartic is $\beta_1 : x_1 = 0$, $\beta_2 : x_2 = 0$, $\beta_3 : x_3 = 0$, $\beta_4 : x_1 + x_2 + x_3 = 0$, $\beta_5 : \alpha_{11}x_1 + \alpha_{12}x_2 + \alpha_{13}x_3 = 0$, $\beta_6 : \alpha_{21}x_1 + \alpha_{22}x_2 + \alpha_{23}x_3 = 0$, $\beta_7 : \alpha_{31}x_1 + \alpha_{32}x_2 + \alpha_{33}x_3 = 0$, for $[\alpha_{i1} : \alpha_{i2} : \alpha_{i3}] \in \mathbb{P}^2$.*

In our case, we do not have the embedding to $\mathbb{P}^2$ because it seems to us that we can not construct it with η_X functions (what would the zero-cycle $\mathfrak{u}$ be ?). However, we can find in [13] the following expression of α_{ij} with theta constants. We fix a symplectic basis and use the Dupont's notation

$$\theta_{b_0+2b_1+4b_2+8a_0+16a_1+32a_2}(\Omega) := \theta \begin{bmatrix} a/2 \\ b/2 \end{bmatrix} (0, \Omega)$$

for $a = {}^t(a_0, a_1, a_2)$, $b = {}^t(b_0, b_1, b_2)$ and $a_i, b_i \in \{0, 1\}^2$.

$$\alpha_{11} = \frac{\theta_{12}\theta_5}{\theta_{33}\theta_{40}}, \quad \alpha_{21} = \frac{\theta_{27}\theta_5}{\theta_{54}\theta_{40}}, \quad \alpha_{31} = -\frac{\theta_{12}\theta_{27}}{\theta_{33}\theta_{54}},$$

$$\alpha_{12} = \frac{\theta_{21}\theta_{28}}{\theta_{56}\theta_{49}}, \quad \alpha_{22} = \frac{\theta_2\theta_{28}}{\theta_{47}\theta_{49}}, \quad \alpha_{32} = \frac{\theta_2\theta_{21}}{\theta_{47}\theta_{56}},$$
$$\alpha_{13} = \frac{\theta_7\theta_{14}}{\theta_{42}\theta_{35}}, \quad \alpha_{23} = \frac{\theta_{16}\theta_{14}}{\theta_{61}\theta_{35}}, \quad \alpha_{33} = \frac{\theta_{16}\theta_7}{\theta_{61}\theta_{42}}.$$

The reconstruction of the plane quartic from its bitangents comes from the following result.

Theorem 14 (Riemann)**.** *Let $\beta_1, \dots, \beta_7$ be an Aronhold system of bitangents as in Proposition 13. Then an equation for the curve is*

$$(x_1\xi_1 + x_2\xi_2 - x_3\xi_3)^2 - 4x_1\xi_1x_2\xi_2 = 0$$

where ξ_1, ξ_2, ξ_3 are given by

$$\begin{cases} \xi_1 + \xi_2 + \xi_3 + x_1 + x_2 + x_3 = 0, \\ \frac{\xi_1}{\alpha_{i1}} + \frac{\xi_2}{\alpha_{i2}} + \frac{\xi_3}{\alpha_{i3}} + k_i(\alpha_{i1}x_1 + \alpha_{i2}x_2 + \alpha_{i3}x_3) = 0, \qquad i \in \{i, 2, 3\} \end{cases}$$

with k_1, k_2, k_3 solutions of

$$\begin{pmatrix} \frac{1}{\alpha_{11}} & \frac{1}{\alpha_{21}} & \frac{1}{\alpha_{31}} \\ \frac{1}{\alpha_{12}} & \frac{1}{\alpha_{22}} & \frac{1}{\alpha_{32}} \\ \frac{1}{\alpha_{13}} & \frac{1}{\alpha_{23}} & \frac{1}{\alpha_{33}} \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \end{pmatrix} = \begin{pmatrix} -1 \\ -1 \\ -1 \end{pmatrix}, \qquad \begin{pmatrix} \lambda_1\alpha_{11} & \lambda_2\alpha_{21} & \lambda_3\alpha_{31} \\ \lambda_1\alpha_{12} & \lambda_2\alpha_{22} & \lambda_3\alpha_{32} \\ \lambda_1\alpha_{13} & \lambda_2\alpha_{23} & \lambda_3\alpha_{33} \end{pmatrix} \begin{pmatrix} k_1 \\ k_2 \\ k_3 \end{pmatrix} = \begin{pmatrix} -1 \\ -1 \\ -1 \end{pmatrix}.$$

It is then possible to find the equation of all the bitangents. Moreover, starting from the equation of a plane quartic, [26, Proposition 3] describes a way to compute an associated Aronhold system. We do not use these facts.

It remains to us to explain how to compute the values α_{ij}. We proceed as in Section 5.2. Assuming we have all the tropes and the image of the 2-torsion points in $\mathbb{P}^7$, we deduce the evaluation of the η_a in the torsion points a' when $\eta_0(a') \neq 0$. We use Equation 12 to multiply the η_a^2 by a constant so that we obtain the algebraic counterpart of θ_i^4/θ_0^4. Then we could try all the possibilities for the choice of fourth roots (assuming testing if two curves are isogenous takes not too much time). Otherwise, we generate many relations between square of theta constants using the Duplication formulas or the Riemann's theta formula and using Gröbner bases and fixing 6 square roots ($[\Gamma_3(2) : \Gamma_3(2,4)] = 2^6$), we can compute a compatible set of algebraic theta functions $c_a\eta_a^2$ (for some constant c_a). Finally, for the projective point $(\alpha_{11} : \alpha_{12} : \alpha_{13})$, choose any square root of α_{11} and then consider the following equalities (coming from Riemann's theta formula)

$$\begin{array}{l} \theta_{61}\theta_{45}\theta_{16}\theta_0 - \theta_{56}\theta_{40}\theta_{21}\theta_5 + \theta_{49}\theta_{33}\theta_{28}\theta_{12} = 0, \\ \theta_5\theta_{12}\theta_{33}\theta_{40} - \theta_{21}\theta_{28}\theta_{49}\theta_{56} - \theta_{42}\theta_{35}\theta_{14}\theta_7 = 0. \end{array}.$$

From the first one, we have

$$(\theta_{61}\theta_{45}\theta_{16}\theta_0)^2 = (\theta_{56}\theta_{40}\theta_{21}\theta_5)^2 + (\theta_{49}\theta_{33}\theta_{28}\theta_{12})^2 - 2\theta_{56}\theta_{40}\theta_{21}\theta_5\theta_{49}\theta_{33}\theta_{28}\theta_{12}$$

from which we deduce the good square root of α_{12}^2. Similarly, the second equality give us α_{13}. For the two other projectives points, we proceed in the same way using

$$\begin{array}{l} \theta_{49}\theta_{47}\theta_{28}\theta_2 - \theta_{54}\theta_{40}\theta_{27}\theta_5 - \theta_{61}\theta_{35}\theta_{16}\theta_{14} = 0, \\ \theta_{54}\theta_{47}\theta_{27}\theta_2 - \theta_{49}\theta_{40}\theta_{28}\theta_5 + \theta_{56}\theta_{33}\theta_{21}\theta_{12} = 0, \end{array}$$

$$\begin{array}{l} -\theta_{55}\theta_{32}\theta_{20}\theta_3 + \theta_{54}\theta_{33}\theta_{21}\theta_2 + \theta_{56}\theta_{47}\theta_{27}\theta_{12} = 0, \\ \theta_{54}\theta_{33}\theta_{27}\theta_{12} - \theta_{56}\theta_{47}\theta_{21}\theta_2 + \theta_{61}\theta_{42}\theta_{16}\theta_7 = 0. \end{array}$$

6 Implementation

We have implemented all the algorithms presented here using the computational algebra system *magma* [3]. In the case of hyperelliptic curves, the reduced divisors are represented through their Mumford coordinates and addition between the reduced divisors x_1, x_2 is done with the Cantor's algorithm, giving us the reduced divisor of $x_1 + x_2$. In the non-hyperelliptic case (genus 3), we have represented divisors as formal sums of points and used the *Reduction* function of magma to reduce divisors. This makes the handling of divisors heavy so that in this case, our implementation has to be improved, first from an arithmetic point of view. We should use the algorithm of [14] for fast addition.

In this paper, we only have optimized the number of evaluations of η_X functions in the genus 2 case using the parameterization method. The method computing the isogeny directly in the Rosenhain form with algebraic theta functions requires the computation of more than the 6 tropes of the other method, so it is less efficient. We did not optimize our implementation in this case but computed all the tropes (from which we deduce all the $\phi(a) \in \mathbb{P}^3$) and verified that it worked. For genus 3, we did not care about optimization. The point-counting algorithms are not efficient in practice and computing isotropic subgroups is hard. In the non-hyperelliptic case, we only tested our algorithm using η functions instead of η_X functions, so without computing isogenies. This should not matter because what we want to do is being able to compute the equation of the curve from the geometry of its Kummer in $\mathbb{P}^7$. Note that it is easy to verify that two curves are isomorphic. It is enough to compute isomorphic classes invariants (Igusa invariants in genus 2, Shioda invariants for hyperelliptic curves of genus 3 and Dixmier-Ohno invariants for plane quartics). We give now an example of computation with have done for genus 2 curves using the parameterization method. Let

$$\mathcal{C} : Y^2 = 74737X^5 + 28408X^4 + 89322X^3 + 47216X^2 + 55281X + 86566$$

be a hyperelliptic curve over $\mathbb{F}_{100019}$ whose Weierstrass points live in $\mathbb{F}_{100019^5}$. Then $\mathcal{C}$ is $(7,7)$-isogenous to the curve

$$\mathcal{D} : Y^2 = 34480X^5 + 27167X^4 + 78914X^3 + 49217X^2 + 75306X + 92103.$$

We no not put the isotropic subgroup as it is too big to be put here. It lives in a extension of $\mathbb{F}_{100019}$ of degree 30. The computation of $\mathcal{D}$ took 27 seconds. This includes the computation of the trope Z_{a_3} so that we have the image of the points $\{a_1, \ldots, a_6, a_{12}, a_{34}, a35\}$ in $\mathbb{P}^3$. The computation of the matrix allowing one to go from a representation of the Kummer to the good one took slightly less than 1 second. Computing the image of a single formal point at small precision, which means 9 evaluations of η_X functions (if η_{a_6} is in the basis, 12 otherwise) took around 30 seconds. Extending the precision can be done in 0.4 second and the reconstruction of rational fractions in 0.02 second. At the end, we can verify the correctness of the rational fractions in testing if the image of a point is in the Jacobian of $\mathcal{D}$ and in testing the homomorphic property of the isogeny.

Our implementation is not fast compared to the one of AVIsogenies (at small primes) but we beat them at some examples. We intend now to improve our code. The method exposed here is promising compared to the other method because its complexity in the prime number ℓ does not depend of ℓ being a sum of squares of not. Moreover, being able to compute the functions directly at 2-torsion points and at non-generic points would be an improvement. We manage to have results when using η functions but nothing with η_X functions. Finally, it

would be interesting to be able to compute cyclic isogenies. This requires a better knowledge of what the polarization looks like to construct the corresponding η_X function.

Acknowledgements

This research have been done while the author was a postdoc in the Caramba team of Nancy. I thank Pierrick Gaudry for suggesting me to work on [10], for helping me in my first footsteps and for giving me the idea of using the pseudo-addition law in the Kummer. I also thank Christophe Ritzenthaler for a fruitful discussion we had, leading me to Equation 12. Finally, I thank Jean-Marc Couveignes for answering to the many questions I asked him about his paper.

References

[1] C. Birkenhake and H. Lange. *Complex abelian varieties, 2nd ed*, volume 302 of *Grundlehren der mathematischen Wissenschaften*. Springer-Verlag Berlin, 2003.

[2] G. Bisson, R. Cosset, and D. Robert. AVIsogenies (Abelian Varieties and Isogenies). Magma package for explicit isogenies computation between abelian varieties. `http://avisogenies.gforge.inria.fr/`, 2010.

[3] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[4] A. Bostan, F. Morain, B. Salvy, and É. Schost. Fast algorithms for computing isogenies between elliptic curves. *Math. Comp.*, 77(263):1755–1778, 2008.

[5] L. Brambila-Paz, S.B. Bradlow, O. Garca-Prada, and S. Ramanan. *Moduli Spaces and Vector Bundles*, volume 359 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, 2009.

[6] L. Caporaso and E. Sernesi. Recovering plane curves from their bitangents. *Journal of Algebraic Geometry*, 12(2):225–244, 2003.

[7] J.W.S Cassels and E.V. Flynn. *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2*, volume 230 of *London Mathematical Society. Lecture Note Series*. Cambridge University Press, 1996.

[8] R. Cosset. *Applications des fonctions thêta à la cryptographie sur courbes hyperelliptiques*. PhD thesis, Université Henri Poincaré - Nancy 1, 2011.

[9] R. Cosset and D. Robert. Computing (ℓ, ℓ)-isogenies in polynomial time on Jacobians of genus 2 curves. *Mathematics of Computation*, 84:1953–1975, 2015.

[10] J.-M. Couveignes and T. Ezome. Computing functions on Jacobians and their quotients. *LMS Journal of Computation and Mathematics*, 18:555–577, 2015.

[11] C. Diem. *On arithmetic and the discrete logarithm problem in class groups of curves*. PhD thesis, Habilitationsschrift, Universität Leipzig, 2008.

[12] I. Dolgachev and D. Lehavi. On isogenous principally polarized abelian surfaces. In *Curves and abelian varieties*, volume 465 of *Contemp. Math.*, pages 51–69. Amer. Math. Soc., Providence, RI, 2008.

[13] A. Fiorentino. Weber's formula for the bitangents of a smooth plane quartic. *arXiv:1612.02049*, 2016.

[14] S. Flon, R. Oyono, and C. Ritzenthaler. Fast addition on non-hyperelliptic genus 3 curves. In *Algebraic geometry and its applications*, volume 5 of *Ser. Number Theory Appl.*, pages 1–28. World Sci. Publ., Hackensack, NJ, 2008.

[15] P. Griffiths and J. Harris. *Principles of algebraic geometry*. John wiley and sons, Inc., 1978.

[16] J.I. Igusa. *Theta functions*, volume 194 of *Grundlehren der mathematischen Wissenschaften*. Springer-Verlag Berlin Heidelberg, 1972.

[17] S. Lang. *Abelian varieties*. Interscience Tracts in Pure and Applied Mathematics. No. 7. Interscience Publishers, Inc., New York; Interscience Publishers Ltd., London, 1959.

[18] D Lehavi. Any smooth plane quartic can be reconstructed from its bitangents. *Israel Journal of Mathematics*, 146(1):371–379, 2005.

[19] D. Lubicz and D. Robert. Computing isogenies between Abelian Varieties. *Compositio Mathematica*, 148(05):1483–1515, 2012.

[20] D. Lubicz and D. Robert. Computing separable isogenies in quasi-optimal time. *LMS Journal of Computation and Mathematics*, 18:198–216, 2015.

[21] J.S. Milne. Abelian varieties (v2.00), 2008. Available at www.jmilne.org/math/.

[22] D. Mumford. *Tata lectures on theta I*, volume 28 of *Progress in Mathematics*. Birkhäuser Boston, 1983.

[23] D. Mumford. *Tata lectures on theta II*, volume 43 of *Progress in Mathematics*. Birkhäuser Boston, 1984.

[24] J.S. Müller. Explicit Kummer varieties of hyperelliptic Jacobian threefolds. *LMS Journal of Computation and Mathematics*, 17(1):496–508, 2014.

[25] B. Riemann. Sur la théorie des fonctions abéliennes, 1898. Oeuvres de Riemann, second edition (p. 487).

[26] C. Ritzenthaler. *Point Counting on Genus 3 Non Hyperelliptic Curves*, pages 379–394. Springer Berlin Heidelberg, Berlin, Heidelberg, 2004.

[27] C. Ritzenthaler. *Problèmes arithmétiques relatifs à certaines familles de courbes sur les corps finis*. PhD thesis, Université Paris 7 – Denis Diderot, June 2003.

[28] B. Smith. Isogenies and the Discrete Logarithm Problem in Jacobians of Genus 3 Hyperelliptic Curves. In Nigel Smart, editor, *Eurocrypt 2008*, volume 4965, pages 163–180, Istanbul, Turkey, April 2008. International Association for Cryptologic Research.

[29] B. Smith. Computing low-degree isogenies in genus 2 with the Dolgachev-Lehavi method. *Arithmeric, Geometry and Coding Theory - Contemporary mathematics*, 574:159–170, 2012.

[30] M. Stoll. An explicit theory of heights for hyperelliptic Jacobians of genus three. *arXiv:1701.00772v2*, 2017. `http://www.mathe2.uni-bayreuth.de/stoll/magma/index.html`.

[31] A.G.J. Stubbs. *Hyperelliptic curves.* PhD thesis, University of Liverpool, 2000.

[32] J. Vélu. Isogénies entre courbes elliptiques. *Compte Rendu Académie Sciences Paris Série A-B*, 273:A238–A241, 1971.

[33] H. Weber. Theorie der Abelschen Funktionen vom Geschlecht 3. *Berlin : Druck und Verlag von Georg Reimer*, 1876.

[34] A. Weng. *Konstruktion kryptographisch geeigneter Kurven mit komplexer Multiplikation.* PhD thesis, Universität GH Essen, 2001.