Arithmetic on Abelian and Kummer Varieties

DAVID LUBICZ AND DAMIEN ROBERT

Abstract. A Kummer variety is obtained as the quotient of an abelian variety by the automorphism (-1) acting on it. Kummer varieties can be seen as a higher dimensional generalisation of the x-coordinate representation of a point of an elliptic curve given by its Weierstrass model. Although there is no group law on the set of points of a Kummer variety, the multiplication of a point by a scalar still makes sense, since it is compatible with the action of (-1), and can efficiently be computed with a Montgomery ladder. In this paper, we explain that the arithmetic of a Kummer variety is not limited to this scalar multiplication and is much richer than usually thought. We describe a set of composition laws which exhaust this arithmetic and explain how to compute them efficiently in the model of Kummer varieties provided by level 2 theta functions. Moreover, we present concrete example where these laws turn out to be useful in order to improve certain algorithms. As an application interesting for instance in cryptography, we explain how to recover the full group law of the abelian variety with a representation almost as compact and in many cases as efficient as the level 2 theta functions model of Kummer varieties.

1. Introduction

Efficient group law for abelian varieties has many applications in algebraic number theory and cryptography. Let k be a finite field, the problem consists in representing the set of rational points $A(k)$ of an abelian variety defined over k and computing natural composition laws on this set of points such as additions or Weil and Tate pairings. For cryptographic applications, we would like, for a level of security roughly given by the cardinality of $A(k)$, to have a representation as compact as possible and be able to compute quickly all the composition laws.

If the case of elliptic curves has been widely studied for years, the literature about the higher dimensional cases is less developed. For instance, it is known that all absolutely simple principally polarized abelian surfaces are isomorphic to the jacobian $\mathrm{Jac}(H)$ of a hyperelliptic curve H of genus 2. The addition law can then be computed using Cantor's algorithm [Can87] and these formulas have been optimized in [Lan05; HC]. Unfortunately, even with these formulas, genus 2 curves do not provide the same efficiency as elliptic curves for a similar level of security.

To obtain a more compact representation and improved arithmetic, an idea is to lose information and consider the Kummer variety $\mathcal{K}_A = A/(-1)$ associated to the abelian variety A. For an elliptic curve in Weierstrass coordinates $E : y^2 = x^3 + ax + b$, a geometric point P on the Kummer line $\mathcal{K}_E$ is simply represented by its x-coordinate $x(P)$. On a Kummer variety, since we can't distinguish between a geometric point $P \in A(\overline{k})$ (where $\overline{k}$ is an algebraic closure of k) and its opposite $-P$, the addition law is only defined up to an ambiguity; more precisely from the points $[P]$ (in the following we often denote by $[P]$ the projection of a geometric point $P \in A(k)$ to $\mathcal{K}_A$) and $[Q]$ one can recover two possible additions: $[P+Q]$ and $[P-Q]$. Nevertheless, one can still compute *differential additions*; from the data of $[P]$, $[Q]$ and $[P-Q]$ the point $[P+Q]$ is uniquely determined.

By using differential additions in a Montgomery ladder [Mon92; Mon87], it is then still possible to compute scalar multiplications on Kummer varieties. As this is sufficient for some cryptographic protocols based on the discrete logarithm problem, it makes sense to use Kummer varieties in cryptography. In the dimension 2 case, since the publication of fast formulas for Kummer surfaces [Gau07; GL09],

2010 *Mathematics Subject Classification.* Primary: 14K25, Secondary: 11G20, 14Q15, 14Q20.

Key words and phrases. abelian varieties, arithmetic, theta functions.

The first and second authors were supported by the ANR Peace (reference ANR-12-BS01-0010-01), and the second author was furthermore supported by the ERC Starting Grant ANTICS 278537, the ANR Simpatic and the Lirima Laboratory through the project team Macisa.

using Kummer surfaces for cryptography has been somewhat competitive with elliptic curves. Recently the duel has even been tipping in favor of Kummer surfaces [BCH+13; BCL+14]. We note that the fast formulas in [Gau07] do not use Mumford coordinates but instead are based on a model of the Kummer surfaces provided by theta functions of level 2 [Mum66; Mum67a; Mum67b] (so in particular the 2-torsion is rational in this model). On a Kummer surface, a point will be represented by 4 projective coordinates (the four level 2 theta functions) while on a Kummer line we just need two projective coordinates. This is somewhat assuaged by the fact that on a Kummer surface we can work with fields of half the size for an equivalent security.

Nonetheless, it should be remarked that the arithmetic provided by differential addition does not allow one to implement all cryptographic primitives. For instance the verification of a ECDSA signature requires the computation of the addition law. While in the case of the Kummer line it is easy to go back to the elliptic curve (at the cost of one square root), in dimension 2 it is harder to go back from the Kummer surface to the abelian surface. One way would be to go to level 4 theta functions from the level 2 theta functions, but there is a lack of explicit formulas in the literature explaining how to do this step. The other way would be to go from the level 2 theta coordinates to the Mumford coordinates (u, v^2) on the Kummer surface using the formulas from [CR15; Cos11]; and then compute a square root to find the Mumford coordinates (u, v) on A. But converting theta coordinates to Mumford coordinates is pretty slow.

Moreover, while elliptic curves have an efficient addition law (especially on Montgomery curves because they are birationally equivalent to twisted Edwards curves [BBJ+08]), it is not the case for abelian surfaces (the level 4 theta model is even worse than Mumford coordinates since it requires 16 projective coordinates; the cost of the addition law is described in [Rob10]). This explains why, for cryptographic applications, we are incited do as many arithmetic operations as possible on the Kummer variety. Considering this background, the aim of this paper is threefold:

- give a comprehensive picture of the arithmetic of Kummer varieties using tools that we have developed for computing isogenies and optimal pairings on abelian varieties [LR12; LR13] ;
- provide an efficient algorithm to compute the fiber of the natural projection from an abelian variety onto its associated Kummer variety;
- deduce a compact while still efficient representation of abelian varieties based on theta functions.

More precisely, we point out that what can be computed on a Kummer variety goes well beyond differential additions. We introduce the so called *compatible addition law* which is well defined on a Kummer variety. We give example of useful computations which can be carried out with compatible addition though out of reach of differential additions. We give an algorithm to compute compatible additions in the model of Kummer varieties provided by level 2 theta functions and we explain that by using differential and compatible additions it is possible to compute the fiber of the natural projection $A \to \mathcal{K}_A$ (from level 4 to level 2) up to one choice of sign. This shows that compatible and differential additions exhaust all the arithmetic of Kummer varieties.

Finally the main point of the paper is to use compatible additions to give a more compact and more efficient model for the abelian variety A. Indeed representing a point in the Kummer surface using level 2 theta coordinates require 2^g projective coordinates while representing a point on A using level 4 theta coordinates require 4^g of them. But all these extra coordinates only encode a choice of sign! We give a model (a generalisation of hybrid level $(2, \ldots, 2, 4)$ theta functions) that only needs one extra coordinate to encode this choice of sign and has a scalar multiplication as fast as the one on the Kummer variety.

While, in view of cryptographic applications, we mainly consider the case of dimensions 1 and 2, the algorithms we develop in this paper are valid in any dimension. The paper is organized as follows: In Section 2, we describe the arithmetic on an abstract Kummer variety, and construct the new more efficient model for abelian varieties. Then Section 3 explains how to compute efficiently this arithmetic with the model provided by level 2 theta functions. Section 4 deals with change of level formulas and explains how to go back and forth between the model given by level 4 theta functions and the new model introduced in Section 2. Finally, in Section 5 we give explicit formulae for all the algorithms described in the preceding sections for abelian surfaces.

2. Arithmetic on Abelian and Kummer varieties

In this section, we introduce the compatible addition on the set of points of Kummer varieties. We use this compatible addition to construct an efficient model for the abelian variety. Then we give two examples of useful computations which can be carried out directly on a Kummer variety with compatible additions. First, a multiway addition which allows to compute the sum $P_0 + \ldots + P_n$ from the knowledge of $P_0, \ldots, P_n$ and the sums $(P_0 + P_1), \ldots, (P_0 + P_n)$. Secondly we explain how to compute a multi-dimensional Montgomery ladder while keeping only 2 points in memory at each step.

2.1. **Compatible additions.** Let A be an abelian variety and denote by $\mathcal{K}_A$ its associated Kummer variety. Let $\pi : A \to \mathcal{K}_A$ be the canonical projection. In this section, we adopt the following convenient convention: for $P \in A(k)$, we denote by $[P] \in \mathcal{K}_A(k)$ the point $\pi(P)$ of $\mathcal{K}_A$. So, the notation $[P] \in \mathcal{K}_A(k)$ means that there exists $P \in A(k)$ and that $\pi(P) = [P]$.

Definition 2.1. Given a model of $\mathcal{K}_A$ defined over the field k, a *schematic addition* is an algorithm which provided with two points $[P], [Q] \in \mathcal{K}_A(k)$, outputs equations defining the dimension 0 scheme of degree two $\mathcal{S} = \{[P+Q], [P-Q]\}$. More precisely this algorithm should output a rational parametrisation of $\mathcal{S}$, that is a polynomial $\mathcal{P} \in k[t]$ of degree 2 in one variable, and a rational isomorphism $f : \operatorname{Spec} k[t]/\mathcal{P}(t) \to \mathcal{S}$ together with its inverse f^{-1}.

We will see in Section 3 that the level 2 theta model of the Kummer variety admits a schematic addition. From now on we suppose that we have a model admitting schematic additions and we will look at the arithmetic we can derive on this model and on the abelian variety.

First we note that if $[Q]$ is a point of 2-torsion, $[P + Q] = [P - Q]$ so that by the hypothesis we can compute the action of translation by points of 2-torsion (this costs one schematic addition and finding the double root of a degree 2 univariate polynomial). From the *schematic addition* it is also easy to see that we can then compute *doublings* and *differential additions* on the Kummer variety (this costs one schematic addition and finding the second root of a degree 2 univariate polynomial given the first root). In fact most models of Kummer varieties have dedicated faster formulae for the doubling and differential additions than for the schematic addition. This is indeed the case with the theta model we consider in Sections 3 and 5. So in the following we will distinguish between schematic additions and differential additions.

The following very simple idea show that we can compute *some* additions on $\mathcal{K}_A$.

Proposition 2.2. *Let $P, Q, R, S \in A(k)$ be such that $P+Q = R+S$ and $P-Q \neq R-S$, $P-Q \neq S-R$. Then the point $[P + Q] = [R + S]$ of $\mathcal{K}_A$ is well defined from the knowledge of $[P], [Q], [R], [S]$ and can be computed as the intersection of the output of two schematic additions.*

Remark 2.3. We note that an equivalent reformulation of the condition of the Proposition is that there is no point of 2-torsion $U \in A(k)$ such that ($P = R + U$ and $Q = S + U$) or ($P = S + U$ and $Q = R + U$).

Proof. From the hypothesis about $\mathcal{K}_A$ and of the Proposition, the two schemes $\{[P + Q], [P - Q]\}$ and $\{[R + S], [R - S]\}$ in $\mathcal{K}_A$ can be computed with two schematic additions. By the discussion above, we may assume that none of the point is of 2-torsion. From the hypothesis of the Proposition their intersection has degree 1 and is equal to $\{[P + Q]\}$. This intersection is computed as the gcd of the two degree two univariate polynomials resulting from the schematic additions. □

Definition 2.4 (Compatible addition)**.** Under the hypotheses of the Proposition, we call $[P + Q]$ the *compatible addition* of P and Q with respect to R and S.

Remark 2.5. By looking at the proof of Proposition 2.2, we expect a compatible addition to cost roughly two schematic additions. Indeed the two schematic additions will output two degree two polynomials $P_1 = X^2 + aX + b$ and $P_2 = X^2 + cX + d$ in $k[X]$ parametrizing the two schemes $\{[P + Q], [P - Q]\}$ and $\{[R + S], [R - S]\}$. We recall that P_1 and P_2 have a common root if and only if $(ad - bc)(c - a) = (d - b)^2$ and in this case this root is $(d - b)/(a - c)$, so the intersection is easy to compute from the data of P_1 and P_2.

Actually, once we have computed the scheme $\{[P+Q],[P-Q]\}$ we just need to recover enough information about $\{[R+S],[R-S]\}$ to distinguish between $[P+Q]$ and $[P-Q]$. So we don't need the full schematic addition on $[R]$ and $[S]$ (see Section 5 for more details). Nonetheless, since schematic additions are in general much more expensive than differential additions on a Kummer variety, a compatible addition is an arithmetic operation that should not be used too often.

2.2. **An efficient model for the abelian variety.** This simple idea of doing compatible additions is surprisingly powerful. As a first application, we introduce a family of embeddings of A into $\mathcal{K}_A^2$ and explain that the addition law of A carry on via these isomorphisms onto a law which can be efficiently computed using the compatible addition. This is the content of the:

Theorem 2.6. *Let $P_0 \in A(k)$ be a point not in the 2-torsion of A. Then the map $\alpha_{P_0} : A \to \mathcal{K}_A^2$, given on geometric points by $P \mapsto ([P],[P+P_0])$ is injective. If $f : \mathcal{K}_A \to \mathbb{P}_k^m$ is an embedding of the Kummer variety, then $f_{P_0} : A \to \mathbb{P}_k^m \times \mathbb{P}_k^m$, given on geometric points by $P \mapsto (f([P]), f([P+P_0]))$ is an embedding.*

Finally, given a couple $([P_1],[P_2]) \in \mathcal{K}_A(k)^2$ it is easy to check if it lies in $\alpha_{P_0}(A(k))$.

Proof. The natural projection $A \to \mathcal{K}_A$ has degree 2, so if $([P],[P+P_0]) = ([Q],[Q+P_0])$ then either $P = Q$, or $P = -Q$. But in the latter case, since $P + P_0 = Q + P_0$ or $P + P_0 = -Q - P_0$ in A and P_0 is not a point of 2-torsion, we have $P = -P$ so α_{P_0} is injective in all cases.

In particular, the map f_{P_0} is injective on the geometric points. It remains to see that it is also injective on the tangent spaces. But since f is an embedding, whenever $[P]$ is a smooth point of K_A then f is injective at the tangent space at $[P]$, so f_P is also injective at P. But $[P]$ is smooth if and only if P is not of two torsion, and P and $P + P_0$ can never be simultaneously of two torsion, so f is always injective on the tangent spaces.

The couple $([P_1],[P_2]) \in \mathcal{K}_A(k)^2$ lies in $\alpha_{P_0}(A(k))$ if and only if $[P_2] \in \{[P_1+P_0],[P_1-P_0]\}$ in $\mathcal{K}_A(k)^2$ which can be tested by the way of a schematic addition. □

Corollary 2.7. *Provided that there exists an algorithm for the schematic addition on K_A, then there exists an algorithm to compute the addition on A from the representation given by Theorem 2.6: from the knowledge of $([P_1],[P_1+P_0])$ and $([P_2],[P_2+P_0])$ one can compute $([P_1+P_2],[P_1+P_2+P_0])$ using a finite number of schematic additions on K_A.*

More precisely, a doubling on A with this model costs a doubling and a differential addition on $\mathcal{K}_A$, a differential addition on A costs two differential additions on $\mathcal{K}_A$, and an addition costs (generically) two compatible additions and a differential addition.

Proof. In Proposition 2.2 set $P = P_1, Q = (P_2 + P_0), R = P_1 + P_0, S = P_2$ to recover $[P_1 + P_2 + P_0]$. The conditions of Proposition 2.2 hold if $2P_0 \neq 0$ and $2P_1 - 2P_2 \neq 0$. By hypothesis, we can rule out the case $2P_0 = 0$. Suppose that $2P_1 - 2P_2 = 0$ then $[P_1 - P_2]$ is a point of 2-torsion on $\mathcal{K}_A$, so we can compute the addition by $[P_1 - P_2]$. From $[P_2 + P_0]$ we can compute $[2P_2 + P_0]$ using a differential addition, and we recover $[P_1 + P_2 + P_0] = [2P_2 + P_0] + [P_1 - P_2]$. We have shown that we can compute $[P_1 + P_2 + P_0]$.

Next, in Proposition 2.2 set $P = P_1, Q = P_2, R = P_0 + P_1, S = -P_0 + P_2$ to recover $[P_1 + P_2]$. Note that $[-P_0 + P_2]$ can be computed with a differential addition since we know $[P_0]$, $[P_2]$ and $[P_0 + P_2]$ by hypothesis. Again, we can apply the Proposition at the condition that $2P_0 - 2P_2 \neq 0$ and $2P_1 - 2P_2 + 2P_0 \neq 0$. If $2P_0 - 2P_2 = 0$ then $P_0 - P_2$ is a point of 2-torsion so that we can compute the addition by $[P_0 - P_2]$, so that we can compute $[P_1 + P_2] = [P_0 + P_1] + [P_0 - P_2]$.

On the other hand, if $2P_0 = 2P_2 - 2P_1$. By permuting P_1 and P_2 we also know that $2P_0 = 2P_1 - 2P_2$, otherwise we could compute $[P_1 + P_2]$ via a compatible addition (so in this case P_0 is a point of 4-torsion). We can also assume that neither P_1 or P_2 is a point of 2-torsion, otherwise we could compute $[P_1 + P_2]$ directly. We can then use Proposition 2.2 again, this time with $P = P_1$, $Q = P_2$, $R = P_0 + P_1 + P_2$, $S = -P_0$. We can apply this Proposition if $2P_0 + 2P_2 \neq 0$ and $2P_0 + 2P_1 \neq 0$. But by the above $2P_0 + 2P_2 = 2P_1 \neq 0$ because P_1 is not a point of 2-torsion, and similarly $2P_0 + 2P_1 \neq 0$. So in all cases we can recover $[P_1 + P_2]$ and $[P_1 + P_2 + P_0]$. □

Remark 2.8. On elliptic curves, we recover a representation studied by Kohel in [Koh11]. If $P_0' \in A(k)$ is another point not of 2-torsion, one can go from the representation $([P],[P+P_0]) \in \mathcal{K}_A(k)^2$ to the

representation $([P],[P+P_0']) \in \mathcal{K}_A(k)^2$ only once we have fixed a choice in $\{P+P_0', P-P_0'\}$. The ambiguity comes from the fact that (-1) is an automorphism on A with which we can act on our representations.

In the model of Theorem 2.6 doing an addition of $([P_1],[P_1+P_0])$ and $([Q_1],[Q_1+P_0])$ requires in the generic case two compatible additions and a differential addition. Since a compatible addition requires two schematic addition, we see that an addition on this model can be quite costly (we refer to Section 5 for the explicit cost in the model given by theta functions). Luckily scalar multiplication are much better behaved. Indeed the scalar multiplication $([P_1],[P_1+P_0]) \mapsto ([nP_1],[nP_1+P_0])$ can be computed with a Montgomery ladder of the form $([mP_1],[(m+1)P_1],[(m+1)P_1+P_0])$ where each step will use one doubling and two differential additions on the Kummer variety. So compared to the scalar multiplication on the Kummer variety this will be around 50 percent slower. An even better idea is to use the standard trick to only compute $[(n-1)P_1],[nP_1]$ on the Kummer variety (via a standard Montgomery ladder). Then at the end one can recover $[nP_1+P_0]$ by doing a compatible addition $(nP_1)+(P_0) = ((n-1)P_1)+(P_1+P_0)$. So this only adds an extra computation at the end compared to the standard multiplication on the Kummer variety. Of course, the same trick will work for a multiscalar multiplication: we compute the multiscalar multiplication directly on the Kummer variety, except at the last step.

Finally, it might seem that we need twice as many coordinates to represent the point $P_1 \in A(k)$ using the representation $([P_1],[P_1+P_0]) \in \mathcal{K}_A(k)^2$ than we need to represent a point in the Kummer variety. But actually, in a way similar to the case of elliptic curves in Weierstrass form where we only need one extra coordinate to encode the choice of sign, once we have $[P_1] \in \mathcal{K}_A(k)$ we can encode $[P_1+P_0]$ as the corresponding root in the degree two scheme $\{[P_1+P_0],[P_1-P_0]\}$. By hypothesis we have a rational parametrisation of the scheme, so this can be done by using only one coordinate. In the level 2 representation of the Kummer variety, we then represent a point of A by a pair in $\mathbb{P}^{2^g-1}(k) \times \mathbb{P}^1(k)$. We refer to Section 5 for an analysis of the arithmetic in this representation. In particular, recovering $([nP_1],[nP_1+P_0])$ in this representation at the last step of the Montgomery ladder costs $20M+32S+14M_0$ (since we only need Z, not X in the notations of Section 5.2).

2.3. **Arithmetic on the Kummer variety.** The model of Theorem 2.6 relies on the efficient arithmetic of the underlying Kummer variety. In this section we explain how compatible additions can also be used in this setting. The strategy is to combine Theorem 2.6 with Remark 2.8 to switch to a more efficient representation when needed.

First by a trivial corollary of Theorem 2.6, we obtain:

Corollary 2.9 (Multiway additions)**.** *Let $[P_0] \in \mathcal{K}_A(k)$ be a point not of 2-torsion. Then from $[P_1],\dots,[P_n] \in \mathcal{K}_A(k)$ and $[P_0+P_1],\dots,[P_0+P_n] \in \mathcal{K}_A(k)$, one can compute $[P_1+\cdots+P_n]$ and $[P_0+P_1+\cdots+P_n]$ using $2(n-1)$ compatible additions.*

Remark 2.10. The idea behind Corollary 2.9 is that giving the points $[P_0+P_i]$ on $\mathcal{K}_A$ "fixes" the sign of P_i relatively to P_0. Since $P_1, \dots, P_n$ have "compatible" signs with respect to P_0, this explains why we are able to compute $[P_1+\cdots+P_n]$ and $[P_0+P_1+\cdots+P_n]$.

Another application of compatible additions is to do multi-scalar multiplication on the Kummer variety. More precisely, we assume that we are given the points $[P],[Q]$ and $[P+Q]$ in $\mathcal{K}_A(k)$, and we want to compute $[\alpha P+\beta Q]$ for some $\alpha,\beta \in \mathbb{Z}$. An easy approach is to do a 2-dimensional Montgomery ladder. At each step we have the four elements $[mP+nQ]$, $[(m+1)P+nQ]$, $[mP+(n+1)Q]$, $[(m+1)P+(n+1)Q]$. Depending on whether the current bits of (α,β) is $(0,0)$, $(1,0)$, $(0,1)$ or $(1,1)$, we add $[mP+nQ]$, $[(m+1)P+nQ]$, $|mP+(n+1)Q]$ or $[(m+1)P+(n+1)Q]$ to the four points. This costs a doubling and three differential additions (the point $[P-Q]$ is easily obtained from $[P]$,$[Q]$ and $[P+Q]$).

A less trivial approach [Ber06] consists in working with three points and doing one doubling and two differential additions at each step. Actually, one can see that we only need to keep track of two elements in the square. This is easier to see this on an example:

Example 2.11. Suppose that we have only computed $[nP + (m+1)Q]$ and $[(n+1)P + mQ]$. If we are lucky the current bits of (α, β) are $(1,0)$ or $(0,1)$ and we don't need the two missing elements for this step. In this case we can go to the next bits with only one doubling and one differential addition. If however the bits are for instance $(0,0)$ then we need to recover $[nP + mQ]$. But this can be done by a compatible addition with (in the terminology of Proposition 2.2) $[x] = [nP + (m+1)Q]$, $[y] = [-Q]$, $[z] = [(n+1)P + mQ]$, $[t] = [-P]$. (For the conditions of the Proposition to hold we need that $2P + 2Q \neq 0$ and $(2n+2)P + (2m+2)Q \neq 0$. But if this is not the case then the points $[(2n)P + (2m+1)Q]$, $[(2n+1)P + (2mQ)]$ are easy to compute directly.) In this case we need one compatible addition and two differentiable additions.

We expect to need to reconstruct a missing element in the square with probability $1/2$. But when we compute this missing element, we can choose which two out the three elements we keep for the next step. Continuing the example, we now have $[nP + mQ]$, $[(n+1)P + mQ]$ and $[nP + (m+1)Q]$. We look at the next bits of (α, β) and see that they are $(0,0)$ and $(1,0)$. Then for the current step we compute only $[(2n)P + (2n)Q]$, $[(2n+1)P + (2n)Q]$. We know that we won't need to do a compatible addition for the next two steps.

Using this strategy of keeping the two points among the three that appear next (forgetting about the fourth point), a Monte Carlo simulation shows that on average there will be 1.111 differential additions, 0.888 doubling and 0.293 compatible additions per bits. (A cleverer strategy could detect when we will not use the two points before the next compatible addition anyway and take this opportunity to replace some differential additions by doublings.)

So depending on the cost of a compatible addition compared to doublings and differential additions, this strategy might be better than [Ber06]. But one should take care that since compatible additions are not done for each bits, an implementation of this algorithm may not be safe against side channel attacks.

Of course we can extend Example 2.11 to multiscalar multiplication. Such a setting can appear when using a multidimensional GLV ladder to speed-up the scalar multiplication [GLV01]. The generalisation of [Ber06] to this setting uses a Montgomery chain with $n+1$ points at each step [Bro06] (where n is the number of points in the multiscalar multiplication). By using compatible additions, we only need to keep 2 points at each step.

Proposition 2.12. *Given points $[P_1], \ldots, [P_n] \in \mathcal{K}_A(k)$ and also the 2^n sums $[\sum \varepsilon_i P_i] \in \mathcal{K}_A(k)$ for $i \in \{1, \ldots, n\}$, $\varepsilon_i \in \{0,1\}$, there exists an algorithm to compute $[\sum \alpha_i P_i]$ for $\alpha_i \in \mathbb{N}$ in at most one compatible addition and two differential additions per bits.*

Remark 2.13. In the preceding statement, we can assume that P_1 is not 2-torsion otherwise it is easy to go back to a multiscalar multiplication with $n-1$ points. Then by Corollary 2.9 it suffices to have the $[P_1 + P_i]$ to recover the other sums.

Proof. Indeed we have the following recursive algorithm: if we already have $[\sum m_i P_i]$ and $[P_1 + \sum m_i P_i]$ then let $Q = \sum \varepsilon_i P_i$ where ε_i is equal to the current bit of α_i. We can recover $[\sum m_i P_i + Q]$ via a compatible addition between $[Q]$, $[\sum m_i P_i]$ and $[P_1 + \sum m_i P_i]$, $[Q - P_1]$ and then use two differential additions to recover $[\sum n_i P_i]$ and $[P_1 + \sum n_i P_i]$ where $n_i = 2m_i + \varepsilon_i$.

We need to check that the condition of Proposition 2.2 holds in order to do the compatible addition. Suppose the contrary. Since P_1 is not a point of 2-torsion, the only possibility is that $2(P_1 + \sum m_i P_i - Q) = 0$. But in this case $\sum n_i P_i = 3Q - 2P_1$ and $P_1 + \sum n_i P_i = 3Q - P_1$ which are easy to compute directly via a finite (independent of the size of n_i) number of differential additions. □

Remark 2.14 (Multiscalar multiplication)**.** We can reinterpret Proposition 2.12 as follow: the standard approach to a multiscalar multiplication $\sum m_i P_i$ is to precompute the $\sum \varepsilon_i P_i$, $\varepsilon_i \in \{0,1\}$ and do a double and add algorithm. Proposition 2.12 can be seen as an adaptation of this algorithm to the coordinates from Theorem 2.6: we represent a point on A by the couple $([\sum m_i P_i], [\sum m_i P_i + P_1])$ in the Kummer. The only difference is that rather than doing a doubling and addition (which will involve two compatible additions on the Kummer), we do it the reverse way: first a compatible addition to change the representation to $([\sum m_i P_i], [\sum m_i P_i + Q])$ using Remark 2.8 (keeping the notations of Proposition 2.12), and then a doubling and differential addition on the Kummer. We see that changing the representation in Theorem 2.6 may give more efficient operations.

Of course the strategy given at the end of Example 2.11 to reduce the number of compatible additions applies too, but the probability of having to do a compatible addition per bit tend to one exponentially fast in n. Moreover, to prevent some side channel attacks, it may be better to always do a compatible addition at each step anyway. However it is possible to replace the two differential additions by one doubling and one differential addition, by computing $[\sum n_i P_i]$ and $[Q + \sum n_i P_i]$ instead. This strategy of changing the couple of point we keep each time costs 1 compatible addition, 1 differential addition and 1 doubling by bits.

Coming back to Example 2.11, if we relax the condition that in the differential chain each difference should be P, Q, $P+Q$ or $P-Q$, then [Ber06] obtains a differential chain (the "extended-gcd" chain) that uses around 1.76 additions by bit. This algorithm constructs a differential chain $\mathfrak{R}$ (where each element in $\mathfrak{R}$ is a couple), starting with $\mathfrak{R} = \{(0,0),(0,1),(1,0),(1,1)\}$ and requiring that one can add $P+Q$ (and $-P-Q$) only when P,Q and $P-Q$ are already in $\mathfrak{R}$. By using "compatible additions" for the multiscalar multiplication (and assuming that the points P_i are linearly independent for simplicity here), one only need to construct a chain $\mathfrak{R}$ of tuples such that if $P, Q, R, S \in \mathfrak{R}$ are such that $P+Q = R+S$, then one can add $P+Q$ (and $-P-Q$) to $\mathfrak{R}$ provided that

- $P-Q \in \mathfrak{R}$;
- or $P-Q \neq \pm R - S$.

3. Arithmetic with theta functions

The aim of this section is to illustrate Theorem 2.6 by using level 2 theta coordinates to represent the Kummer variety $\mathcal{K}_A$. We will see that in this case, the addition on the corresponding model of A can be computed slightly more efficiently than by using two compatible additions.

This section starts by a survey of all the results on theta functions that we use in the rest of the paper. The main results are duplication formulas and Riemann relations. We explain that a sufficient condition for the Riemann relations to allow to compute the addition of an abelian varieties is closely related to the rank of the multiplication map in the graded ring of theta functions. We deduce algorithms to compute addition on abelian varieties and compatible addition on Kummer varieties. We also study the three-way addition introduced in [LR13] and conclude the Section by a summary of all forms of additions derived from Riemann relations.

For simplicity we will define theta functions for abelian variety over the complex field $\mathbb{C}$. It should be noted that by using the algebraic theory of theta functions from [Mum66; Mum67a; Mum67b], all results of Sections 3 and 4 are valid over any algebraically closed field of odd characteristic k. Indeed in [Mum66] Mumford explains how to generalize Theorems 3.1, 3.2 and 4.2 and Corollary 4.3 from $\mathbb{C}$ to the algebraic setting. In the algebraic theory, instead of looking at a lift $z \in \mathbb{C}^g$ of a point $P \in \mathbb{C}^g/\Lambda$, one take arbitrary affine lift and keep track of the projective factors. These techniques are developed in [LR12, Section 3] and also apply in a straightforward way to the results of this paper.

3.1. Duplication formulae and Riemann relations.

Let A be an abelian variety over $\mathbb{C}$ and $\mathscr{L}$ be an ample symmetric line bundle on A. Writing $A = \mathbb{C}^g/\Lambda$ where Λ is a $\mathbb{Z}$-lattice of rank $2g$ of $\mathbb{C}^g$, a section $f \in \Gamma(A, \mathscr{L})$ corresponds to an analytic function f on $\mathbb{C}^g$ which satisfy the condition

$$f(z+\lambda) = a_{\mathscr{L}}(z,\lambda) f(z) \quad \forall z \in \mathbb{C}^g, \lambda \in \Lambda,$$

for a certain automorphic factor $a_{\mathscr{L}} : \mathbb{C}^g \times \Lambda \to \mathbb{C}^*$ which satisfy the cocycle condition $a_{\mathscr{L}}(z, \lambda+\lambda') = a_{\mathscr{L}}(z,\lambda) a_{\mathscr{L}}(z+\lambda, \lambda')$.

In fact, the Chern class of $\mathscr{L}$ can be described by a (positive) hermitian form H such that $E(\Lambda,\Lambda) \subset \mathbb{Z}$ where $E = \operatorname{Im} H$ and by the theorem of Appell-Humbert the automorphic factor $a_{\mathscr{L}}$ can be chosen so that

$$a_{\mathscr{L}}(z,\lambda) = \chi(\lambda) e^{\pi H(z,\lambda) + \pi/2 H(\lambda,\lambda)\pi/2}, \tag{1}$$

for a certain quasi-character $\chi : \Lambda \to [1]$. (For more details we refer to [Mum70; BL04]).

More concretely, if A has a principal polarisation, up to a linear transform of $\mathbb{C}^g$, we can write $\Lambda = \mathbb{Z}^g + \Omega\mathbb{Z}^g$ where $\Omega \in \mathfrak{H}_g$ is in the Siegel upper half space. Then one can define a principal symmetric line bundle $\mathscr{L}_0$ associated to the hermitian form H_0 corresponding to the matrix $(\operatorname{Im}\Omega)^{-1}$ and the quasi-character $\chi_0(\lambda) = e^{\pi i E(\lambda_1,\lambda_2)}$ where $\lambda = \lambda_1 + \lambda_2$ is the decomposition of λ in $\mathbb{Z}^g \oplus \Omega\mathbb{Z}^g$.

We recall the definition of the theta functions with characteristics $a, b \in \mathbb{Q}^g$:

$$\theta \left[\begin{smallmatrix} a \\ b \end{smallmatrix} \right] (z, \Omega) = \sum_{n \in \mathbb{Z}^g} e^{\pi i \, {}^t(n+a) \cdot \Omega \cdot (n+a) + 2\pi i \, {}^t(n+a) \cdot (z+b)}. \tag{2}$$

These theta functions with characteristics are related by

$$\begin{aligned} \theta \left[\begin{smallmatrix} a \\ b \end{smallmatrix} \right] (z, \Omega) &= e^{\pi i \, {}^t a \Omega a + 2\pi i \, {}^t a \cdot (z+b)} \theta \left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix} \right] (z + \Omega a + b, \Omega), \\ \theta \left[\begin{smallmatrix} a+n \\ b+m \end{smallmatrix} \right] (z, \Omega) &= e^{2\pi i \, {}^t a \cdot m} \theta \left[\begin{smallmatrix} a \\ b \end{smallmatrix} \right] (z, \Omega), \end{aligned} \tag{3}$$

where $m, n \in \mathbb{Z}^g$; and satisfy the functional equation

$$\theta \left[\begin{smallmatrix} a \\ b \end{smallmatrix} \right] (z + \Omega m + n, \Omega) = e^{-2\pi i \, {}^t b \cdot m + 2\pi i \, {}^t a \cdot n} e^{-\pi i \, {}^t m \Omega m - 2\pi i \, {}^t m z} \theta \left[\begin{smallmatrix} a \\ b \end{smallmatrix} \right] (z). \tag{4}$$

Let $n \in \mathbb{N}$ and $\mathscr{L} = \mathscr{L}_0^n$. We have $\dim \Gamma(A, \mathscr{L}_0^n) = n^g$ and if $n = n_1 n_2$, a basis of the global sections $\Gamma(A, \mathscr{L}_0^n)$ is given by

$$\theta \left[\begin{smallmatrix} a/n_1 \\ b/n_2 \end{smallmatrix} \right] (n_1 z, \frac{n_1}{n_2} \Omega) \quad a \in Z(n_1), b \in Z(n_2), \tag{5}$$

where $Z(n) = \mathbb{Z}^g / n\mathbb{Z}^g$ (this is an easy generalisation of [Mum83, pp. 123–124]). One should note that the basis given in Equation (5) corresponds to the factor of automorphy from Equation (1) twisted by a coboundary so that the sections are periodic with respect to $\mathbb{Z}^g$. In other words, we have chosen $\mathscr{L}$ in its isomorphic class such that sections $f \in \Gamma(A, \mathscr{L})$ satisfy

$$\begin{aligned} f(z+m) &= f(z), \\ f(z + \Omega m) &= e^{-\pi i n \, {}^t m \cdot \Omega \cdot m - 2\pi i n \, {}^t z \cdot m} f(z). \end{aligned} \tag{6}$$

From Equation (5), we see that the period matrix Ω defines more than an ample line bundle $\mathscr{L}_0$, it also gives a canonical basis of sections of $\mathscr{L}_0^n$ for all $n \in \mathbb{N}$. In the following, we will take the basis of sections coming from the decomposition $n_1 = 1$, $n_2 = n$ and to simplify the notations we let for $i \in Z(n)$

$$\theta_i^{\mathscr{L}_0^n}(z) = \theta \left[\begin{smallmatrix} 0 \\ i/n \end{smallmatrix} \right] (z, \Omega/n). \tag{7}$$

We will often denote this function by θ_i when the context is clear. This is the unique basis (up to multiplication by a constant) such that translation by a point of n-torsion is given by

$$\theta_b(z + \frac{m_1}{n} + \frac{\Omega m_2}{n}) = e^{-\pi i \, {}^t m_2 \cdot \frac{\Omega}{n} \cdot m_2 - 2\pi i \, {}^t m_2 \cdot z} e^{-2\pi i \, {}^t b \cdot m_2} \theta_{b+m_1}(z), \tag{8}$$

for $m_1, m_2 \in \mathbb{Z}^g$ (for more details on the canonical choice of a basis of sections, see [Mum91; Mum66]).

When $n = 4$, the decomposition $n_1 = 2$, $n_2 = 2$ in Equation (5) yields the classical basis of level 4 theta functions $\theta \left[\begin{smallmatrix} a/2 \\ b/2 \end{smallmatrix} \right] (2z, \Omega)$. More generally, in terms of the basis from Equation (5), the action of translation by a point of n-torsion is given in projective coordinates by

$$\left(\theta \left[\begin{smallmatrix} a/n_1 \\ b/n_2 \end{smallmatrix} \right] (n_1(z + \frac{m_1}{n} + \frac{\Omega m_2}{n}), \frac{n_1}{n_2} \Omega) \right)_{a,b} = \left(e^{-2\pi i \, {}^t m_2 \cdot b/n} \theta \left[\begin{smallmatrix} (a+m_2)/n_1 \\ (b+m_1)/n_2 \end{smallmatrix} \right] (n_1 z, n_1 \Omega / n_2) \right)_{a,b}. \tag{9}$$

This can be seen from Equation (8) and the linear change of variables

$$\theta \left[\begin{smallmatrix} a/n_1 \\ b/n_2 \end{smallmatrix} \right] (n_1 z, \frac{n_1}{n_2} \Omega) = \frac{1}{n_1^g} \sum_{\beta \in \frac{1}{n_1}\mathbb{Z}^g / \mathbb{Z}^g} e^{-2\pi i \, {}^t a \cdot \beta} \theta \left[\begin{smallmatrix} 0 \\ b/n + \beta \end{smallmatrix} \right]. \tag{10}$$

By a theorem of Lefschetz, when $n \geqslant 3$ the line bundle $\mathscr{L}$ is very ample, so the n^g theta functions θ_i gives an embedding of A into the projective space $\mathbb{P}_{\mathbb{C}}^{n^g - 1}$ ([Mum83, Theorem 1.3, pp. 125–134],[BL04, Theorem 4.5.1]). Since $\theta_i(-z) = \theta_{-i}(z)$, when $n = 2$ the morphism to projective space factorizes through the Kummer variety $\mathcal{K}_A$. When $\mathscr{L}_0$ is an irreducible principal polarisation on A, the morphism to projective space associated to $\mathscr{L} = \mathscr{L}_0^2$ is actually an embedding of the Kummer variety $\mathcal{K}_A$ ([BL04, Theorem 4.8.1]).

The most important tools concerning the arithmetic of abelian (and Kummer) varieties embedded by theta functions are the duplication formulae and Riemann relations. From now on, we suppose that $\mathscr{L} = \mathscr{L}_0^n$ is totally symmetric, or equivalently that n is even [Mum66, Corollary 4 pp. 315].

Theorem 3.1 (Duplication formulae)**.** *Fix $z_1, z_2 \in \mathbb{C}^g$. Then for all $i, j \in \mathbb{Z}(n)$,*

$$\theta \left[\begin{smallmatrix} 0 \\ \frac{i}{n} \end{smallmatrix} \right] (z_1 + z_2, \frac{\Omega}{n}) \theta \left[\begin{smallmatrix} 0 \\ \frac{j}{n} \end{smallmatrix} \right] (z_1 - z_2, \frac{\Omega}{n}) = \sum_{t \in \frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g} \theta \left[\begin{smallmatrix} t \\ \frac{i+j}{2n} \end{smallmatrix} \right] (2z_1, 2\frac{\Omega}{n}) \theta \left[\begin{smallmatrix} t \\ \frac{i-j}{2n} \end{smallmatrix} \right] (2z_2, 2\frac{\Omega}{n}).$$

Reciprocally, for all $\chi \in \frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g$ and $i, j \in \mathbb{Z}(2n)$ such that $i + j \in \mathbb{Z}(n)$

$$\theta \left[\begin{smallmatrix} \chi \\ \frac{i}{n} \end{smallmatrix} \right] (2z_1, 2\frac{\Omega}{n}) \theta \left[\begin{smallmatrix} \chi \\ \frac{j}{n} \end{smallmatrix} \right] (2z_2, 2\frac{\Omega}{n}) = \frac{1}{2^g} \sum_{t \in \frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g} e^{-2i\pi 2\, {}^t\chi \cdot t} \theta \left[\begin{smallmatrix} 2\chi \\ \frac{i+j}{2n} + t \end{smallmatrix} \right] (z_1 + z_2, \frac{\Omega}{n}) \theta \left[\begin{smallmatrix} 0 \\ \frac{i-j}{2n} + t \end{smallmatrix} \right] (z_1 - z_2, \frac{\Omega}{n}).$$

Proof. See [Igu72, Theorem 2 pp. 139, 141], an algebraic proof is given by [Mum66] by applying the isogeny theorem [Mum66, Theorem 4] to the element of $\mathrm{End}(A \times A)$ given by the matrix $\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$. For a generalisation, see [Koi76; Kem89]. □

We can rewrite the duplication formulae in the standard basis (7). For this, we let for $\chi \in \hat{Z}(2)$ and $i \in Z(n)$, $U^{\mathscr{L}}_{\chi,i}(z) = \sum_{t \in Z(2)} \chi(t)\theta_{i+t}(z)$. In terms of theta functions with characteristics, the level $2n$ theta function $U^{\mathscr{L}^2}_{\chi,i}(z)$ is equal to $\theta \left[\begin{smallmatrix} \chi \\ \frac{i}{n} \end{smallmatrix} \right] (2z, \frac{2\Omega}{n})$, where we have identified $Z(2)$ to its dual group $\hat{Z}(2)$ via the map $x \mapsto \chi(z) = e^{\pi i\, {}^t x \cdot z}$. It is easy to check that if $t \in Z(2)$, $U^{\mathscr{L}^2}_{\chi,i+t} = \chi(t) U^{\mathscr{L}^2}_{\chi,i}$ and that duplication formulae from Theorem 3.1 can be rewritten as

$$\theta^{\mathscr{L}}_{i+j}(z_1 + z_2)\theta^{\mathscr{L}}_{i-j}(z_1 - z_2) = \sum_{\chi \in \hat{Z}(2)} U^{\mathscr{L}^2}_{\chi,i}(z_1) U^{\mathscr{L}^2}_{\chi,j}(z_2) \tag{11}$$

$$U^{\mathscr{L}^2}_{\chi,i}(z_1) U^{\mathscr{L}^2}_{\chi,j}(z_2) = \frac{1}{2^g} \sum_{t \in Z(2)} \chi(t) \theta^{\mathscr{L}}_{i+j+t}(z_1 + z_2)\theta^{\mathscr{L}}_{i-j+t}(z_1 - z_2), \tag{12}$$

for $z_1, z_2 \in \mathbb{C}^g$, $\chi \in \hat{Z}(2)$ and $i, j \in Z(2n)$ such that $i + j, i - j \in Z(n)$.

Theorem 3.2 (Riemann relations)**.** *Let $z_1, z_2, z_3, z_4, z \in \mathbb{C}^g$, such that $2z = z_1 + z_2 + z_3 + z_4$ and let $z'_1 = z - z_1$, $z'_2 = z - z_2$, $z'_3 = z - z_3$, $z'_4 = z - z_4$. Then for all characters $\chi \in \hat{Z}(2)$ and all $i, j, k, l, m \in Z(n)$ such that $i + j + k + l = 2m$, if $i' = m - i$, $j' = m - j$, $k' = m - k$ and $l' = m - l$, then*

$$\Big(\sum_{t \in Z(2)} \chi(t)\theta_{i+t}(z_1)\theta_{j+t}(z_2)\Big).\Big(\sum_{t \in Z(2)} \chi(t)\theta_{k+t}(z_3)\theta_{l+t}(z_4)\Big) = \Big(\sum_{t \in Z(2)} \chi(t)\theta_{i'+t}(z'_1)\theta_{j'+t}(z'_2)\Big).\Big(\sum_{t \in Z(2)} \chi(t)\theta_{k'+t}(z'_3)\theta_{l'+t}(z'_4)\Big). \tag{13}$$

In particular, we have the addition formulae for $z_1, z_2 \in \mathbb{C}^g$ (with χ, i, j, k, l like before):

$$\Big(\sum_{t \in Z(2)} \chi(t)\theta_{i+t}(z_1 + z_2)\theta_{j+t}(z_1 - z_2)\Big).\Big(\sum_{t \in Z(2)} \chi(t)\theta_{k+t}(0)\theta_{l+t}(0)\Big) = \Big(\sum_{t \in Z(2)} \chi(t)\theta_{-i'+t}(z_2)\theta_{j'+t}(z_2)\Big).\Big(\sum_{t \in Z(2)} \chi(t)\theta_{k'+t}(z_1)\theta_{l'+t}(z_1)\Big). \tag{14}$$

We also have the three-ways additions formulae for $z_1, z_2, z_3 \in \mathbb{C}^g$:

$$\Big(\sum_{t \in Z(2)} \chi(t)\theta_{i+t}(z_1 + z_2 + z_3)\theta_{j+t}(z_1)\Big).\Big(\sum_{t \in Z(2)} \chi(t)\theta_{k+t}(z_2)\theta_{l+t}(z_3)\Big) = \Big(\sum_{t \in Z(2)} \chi(t)\theta_{i'+t}(0)\theta_{j'+t}(z_2 + z_3)\Big).\Big(\sum_{t \in Z(2)} \chi(t)\theta_{k'+t}(z_1 + z_3)\theta_{l'+t}(z_1 + z_2)\Big). \tag{15}$$

Proof. We can verify (13) by expressing the left hand side and right hand side of the equation in term of the $U^{\mathscr{L}^2}_{\chi,i}$ basis using (11). Then (14) and (15) are immediate consequences of (13) (using that $\theta_i(-z_2) = \theta_{-i}(z_2)$) For more details, see [LR12] or [Mum66]. A slightly different form is also given in [Mum66, pp. 334–335]; see also [Mum83; Koi76] for an analytic proof. □

If $4|n$, following [Mum83], by applying (13) with $z_1 = z_2$ and $z_3 = z_4 = 0$, we obtain a complete set of equations for the embedding of A into $\mathbb{P}^{Z(n)}$. It is clear that Riemann equations are parametrized by the (projective) *theta null point* $0_A = (\theta_i(0))_{i\in Z(n)}$ which is defined in particular by the data of Ω and n. If $n = 2$, since the Riemann equations are trivial, they do not give equations for the embedding of $\mathcal{K}_A$ is $\mathbb{P}^{Z(2)}$. Nonetheless, in the case that $\dim A = 1$, $\mathcal{K}_A$ is just the projective line and there is no equations and if $\dim A = 2$ then the embedding of $\mathcal{K}_A$ is $\mathbb{P}^{Z(2)}$ is given by a well known quartic equation (see [Mum66, §5] for instance) the coefficients of which can easily be computed from the knowledge of the level 2 theta null point. In the following, we suppose that A is given by the way of its theta null point so that we have a projective model of A on which we would like to have an efficient and complete arithmetic.

3.2. **Addition from Riemann relations.** It is clear that Equation (14) can be used to compute the addition law on A. It order to do so, it is important to know when the factor of the left hand side of (14), $\sum_{t\in Z(2)} \chi(t)\theta_{k+t}(0)\theta_{l+t}(0)$ does not cancel. By Equation (12), we have $\sum_{t\in Z(2)} \chi(t)\theta_{k+t}(0)\theta_{l+t}(0) = U^{\mathscr{L}^2}_{\chi,k_0}(0)U^{\mathscr{L}^2}_{\chi,l_0}(0)$ where $k_0, l_0 \in Z(2n)$ are such that $k_0 + l_0 = k$ and $k_0 - l_0 = l$. To understand the arithmetic of theta functions, we thus need to investigate the noncancellation of the level $2n$ theta functions $U^{\mathscr{L}^2}_{\chi,i}$. Actually, this noncancellation is closely related to the rank of the natural multiplication map $\Gamma(A,\mathscr{L}) \otimes \Gamma(A,\mathscr{L}) \to \Gamma(A,\mathscr{L}^2)$.

To see this, following Mumford [Mum66, p. 328], we consider the morphism $\xi : A\times A \to A\times A$, $(x,y) \mapsto (x+y, x-y)$. Let π_1 and π_2 the first and second projections $A \times A \to A$. Let $\Delta : X \to X \times X$ be the diagonal; Δ induces the multiplication map $\Delta^* : \Gamma(A,\pi_1^*\mathscr{L}) \otimes \Gamma(A,\pi_2^*\mathscr{L}) \to \Gamma(A,\mathscr{L}^2)$, $\pi_1^*\theta_i^{\mathscr{L}} \otimes \pi_2^*\theta_j^{\mathscr{L}} \mapsto (\theta_i^{\mathscr{L}} \otimes \theta_j^{\mathscr{L}})$. If $S : A \to A \times A$ is the inclusion map $x \mapsto (x, 0)$ then Δ fits into the commutative diagram

$$\begin{array}{ccc} (A,\mathscr{L}^2) & & \\ {\scriptstyle S}\downarrow & \searrow^{\Delta} & \\ (A\times A, \pi_1^*\mathscr{L}^2 \otimes \pi_2^*\mathscr{L}^2) & \xrightarrow{\xi} & (A\times A, \pi_1^*\mathscr{L} \otimes \pi_2^*\mathscr{L}). \end{array}$$

so $\Delta^* = S^*\xi^*$. But ξ^* is given by the duplication formula from Theorem 3.1 and $S^* : \Gamma(A \times A, \pi_1^*\mathscr{L}^2 \otimes \pi_2^*\mathscr{L}^2) \to \Gamma(A,\mathscr{L}^2)$ is given by $\pi_1^*\theta_i^{\mathscr{L}^2} \otimes \pi_2^*\theta_j^{\mathscr{L}^2} \mapsto \theta_j^{\mathscr{L}^2}(0)\theta_i^{\mathscr{L}^2}$. We finally get that the map $\Gamma(A,\mathscr{L}) \otimes \Gamma(A,\mathscr{L}) \to \Gamma(A,\mathscr{L}^2)$ is given by

$$\sum_{t\in\hat{Z}(2)} \chi(t)\left(\theta^{\mathscr{L}}_{i+t} \otimes \theta^{\mathscr{L}}_{j+t}\right) \mapsto U^{\mathscr{L}^2}_{\chi,\frac{i+j}{2}} U^{\mathscr{L}^2}_{\chi,\frac{i-j}{2}}(0), \tag{16}$$

which makes clear the link between the noncancellation of the $U^{\mathscr{L}^2}_{\chi,i}(0)$ and the rank of the multiplication map.

Theorem 3.3. *Let $\mathscr{L}_0$ be a principal symmetric line bundle on A. Then the multiplication map*

$$\Gamma(A,\mathscr{L}_0^m) \otimes \Gamma(A,\mathscr{L}_0^n) \to \Gamma(A,\mathscr{L}_0^{n+m})$$

is surjective when $m \geqslant 2$ and $n \geqslant 3$. In particular, if $\mathscr{L} = \mathscr{L}_0^n$ with $n > 2$ even, then $\Gamma(A,\mathscr{L}) \otimes \Gamma(A,\mathscr{L}) \to \Gamma(A,\mathscr{L}^2)$ is surjective, or equivalently for any $\chi \in \hat{Z}(2)$, $i \in Z(2n)$, there exists $i_0 \in Z(n)$ such that $U^{\mathscr{L}^2}_{\chi,i+i_0}(0) \neq 0$.

If $\mathscr{L} = \mathscr{L}_0^2$, then the rank of the multiplication map is equal to the number of even theta null coordinates $U^{\mathscr{L}^2}_{\chi,i}(0) \neq 0$ for $\chi \in \hat{Z}(2)$, $i \in Z(4)$ such that $\chi(2i) = 1$.

Proof. This Theorem is proved analytically in [Koi76], and algebraically in [Kem88] (see also [Kem89, Lemma 17]). When n is divisible by 4, Mumford has a finer result in [Mum66, p. 340]. □

The use of the words odd and even for the theta null coordinates comes from the fact that when $n=2$, we have $U^{\mathscr{L}^2}_{\chi,i}(-z)=\chi(2i)U^{\mathscr{L}^2}_{\chi,i}(z)$. So when $\chi(2i)=-1$, the function $U^{\mathscr{L}^2}_{\chi,i}$ is odd and we have $U^{\mathscr{L}^2}_{\chi,i}=0$. In terms of theta functions with characteristics, the functions $U^{\mathscr{L}^2}_{\chi,i}$ correspond to the usual level 4 theta functions $\{\theta\left[\begin{smallmatrix}a/2\\ b/2\end{smallmatrix}\right](2\cdot,\Omega)\mid a,b\in\mathbb{Z}\}$ and $\chi(2i)$ corresponds to $(-1)^{{}^t a\cdot b}$ which determines the $2^{g-1}(2^g+1)$ even theta functions from the $2^{g-1}(2^g-1)$ odd ones.

Remark 3.4 (Normal projectivity)**.** If $\mathscr{L}$ is a very ample line bundle on a smooth projective variety X, the corresponding embedding of X into projective space is said to be projectively normal if the homogeneous ring associated to this embedding is integrally closed. This condition is equivalent to the condition that $S^n\Gamma(X,\mathscr{L})\to\Gamma(X,\mathscr{L}^n)$ is surjective for all $n\geqslant 2$ [Har00, Exercise 5.14 p. 126], or equivalently by [BL04, p. 187] that $\Gamma(X,\mathscr{L}^n)\otimes\Gamma(X,\mathscr{L})\to\Gamma(X,\mathscr{L}^{n+1})$ is surjective for $n\geqslant 1$. (We remark that the condition that $\Gamma(X,\mathscr{L}^n)\otimes\Gamma(X,\mathscr{L})\to\Gamma(X,\mathscr{L}^{n+1})$ is surjective for n sufficiently large is equivalent to $\mathscr{L}$ being very ample by [Mum69, p. 38]).

By Theorem 3.3, if $\mathscr{L}=\mathscr{L}_0^n$ where $\mathscr{L}_0$ is a principal ample symmetric line bundle and $n\geqslant 3$, then $(A,\mathscr{L})$ is projectively normal. If n is totally symmetric, then by definition $\mathscr{L}$ descends to an ample line bundle $\mathscr{M}$ on $\mathcal{K}_A$, and if $\pi:A\to\mathcal{K}_A$ denotes the projection, then $\pi^\star\Gamma(\mathcal{K}_A,\mathscr{M})=\Gamma(A,\mathscr{L})^+$ where $\Gamma(A,\mathscr{L})^+$ denotes the section invariant under the action by -1. By [Koi76, Corollary 4.5.2],[Kem88] the multiplication map $\Gamma(A,\mathscr{L}_0^{2m})^+\otimes\Gamma(A,\mathscr{L}_0^{2n})^+\to\Gamma(A,\mathscr{L}_0^{2(n+m)})^+$ is surjective when $n\geqslant 1$ and $m\geqslant 2$. So if $n>2$, the variety $(\mathcal{K}_A,\mathscr{M})$ is projectively normal. When $n=2$, we have $\Gamma(A,\mathscr{L})^+=\Gamma(A,\mathscr{L})$ or in other words $\mathscr{L}$ can be seen as a line bundle on $\mathcal{K}_A$. Then $(\mathcal{K}_A,\mathscr{L})$ is projectively normal if and only if $\Gamma(A,\mathscr{L})\otimes\Gamma(A,\mathscr{L})\to\Gamma(A,\mathscr{L}^2)^+$ is surjective, but by Theorem 3.3 this is equivalent to the condition that every even theta null coordinate is nonzero.

Remark 3.5 (Non-annulation of the even theta null coordinates)**.** When $g=1$, it is well known that the three even theta null coordinates are never 0 for an elliptic curve. When $g=2$ the product of the square of the 10 even theta null coordinates define a modular form χ_{10} of weight 10 on the Siegel modular space whose locus is the abelian surfaces that are isomorphic to a product of two elliptic curves [GL12, Section 2.6]. More precisely, when Ω is in the fundamental domain defined by Gottschling [Got59] then the even theta null coordinates are nonzero except $\theta\left[\begin{smallmatrix}1&1\\1&1\end{smallmatrix}\right](0,\Omega)$ which cancels exactly when $\Omega=\begin{pmatrix}\tau_1&0\\0&\tau_2\end{pmatrix}$, that is when $(A,\mathscr{L})$ is isomorphic to a product of elliptic curves with the product polarization. For more details we refer to [Dup06].

When $g>2$ it is well known that Jacobians of hyperelliptic curves are characterized by the cancellation of some even theta null coordinates [Mum84, §6], so an absolutely simple abelian variety can have a zero even theta null coordinate.

Corollary 3.6. *Let $\mathscr{L}=\mathscr{L}_0^n$, where n is even and $\mathscr{L}_0$ is principal and symmetric, coming from a period matrix Ω. We represent the abelian variety $(A,\mathscr{L})$ via the corresponding theta null point.*

If $n>2$ then for all $z_1,z_2\in\mathbb{C}^g$, if we are given $(\theta_i(z_1))_{i\in Z(n)}$ and $(\theta_i(z_2))_{i\in Z(n)}$, then one can recover all products $\theta_i(z_1+z_2)\theta_j(z_1-z_2)$ for $i,j\in Z(n)$.

If $n=2$ and we assume that the even theta null coordinates are nonzero, then from the same data we can recover all terms of the form $\theta_i(z_1+z_2)\theta_j(z_1-z_2)+\theta_j(z_1+z_2)\theta_i(z_1-z_2)$ for $i,j\in Z(2)$.

Proof. When $n>2$, for all $i,j\in Z(n)$ and $\chi\in\hat{Z}(2)$, we can find $k,l\in Z(n)$ such that $i+j+k+l\in 2Z(n)$ and $\sum_{t\in Z(2)}\chi(t)\theta_{k+t}(0)\theta_{l+t}(0)\neq 0$. Indeed, we may as well take $k=i,l=j$, and if needed translate them by a suitable element by using Theorem 3.3 so that $U^{\mathscr{L}^2}_{\chi,\frac{k+l}{2}}(0)U^{\mathscr{L}^2}_{\chi,\frac{k-l}{2}}(0)\neq 0$. By Theorem 3.2 we can then recover $\sum_{t\in Z(2)}\chi(t)\theta_{i+t}(z_1+z_2)\theta_{j+t}(z_1-z_2)$. By summing over $\chi\in\hat{Z}(2)$, we then recover $\theta_i(z_1+z_2)\theta_j(z_1-z_2)$.

The case $n=2$ is done similarly, we refer to [LR10] and [Rob10] for more details. □

By the discussion of Remark 3.4 for $n=2$, it should not be surprising that when the even theta null coordinates are nonzero we can recover the symmetric elements $\theta_i(z_1+z_2)\theta_j(z_1-z_2)+\theta_j(z_1+z_2)\theta_i(z_1-z_2)$. **From now on we will always assume that we are in this case when $n=2$.** It is easy from

Corollary 3.6 to describe equations of the degree 2 scheme $\{[P+Q],[P-Q]\}$ for $[P],[Q] \in \mathcal{K}_A$ which is the output of the *schematic addition*, see Section 5.2. We refer to [LR13] for more details and to Section 5 for explicit formulas in dimension 2.

When $n > 2$ is even we can thus compute the addition of the projective points $P_1, P_2 \in A(k)$. Indeed, for $j = 1, 2$, let $z_j \in \mathbb{C}^g$ be such that $P_j = (\theta_i(z_j))_{i \in Z(n)}$. If $\theta_{i_0}(z_1 - z_2) \neq 0$, then the projective point $(\theta_i(z_1 + z_2)\theta_{i_0}(z_1 - z_2))_{i \in Z(n)}$ represents the point $P_1 + P_2$.

3.3. **Affine additions.** One can see that the relations in Theorem 3.2 are stronger than just computing additions on the variety A. To explain this, we introduce the affine theta coordinates of $z \in \mathbb{C}^g$ as the point of $\mathbb{A}^{Z(n)}$ given by $(\theta_i(z))_{i \in Z(n)}$. Then, if we know the affine theta coordinates of $z_1, z_2 \in \mathbb{C}^g$ and also the affine theta coordinates of the point $z_1 - z_2$, then by Corollary 3.6 we can recover the affine theta coordinates of the point $z_1 + z_2 \in \mathbb{C}^g$. This affine differential addition allows us to recover the analytic addition law on $(\mathbb{C}^g, +)$ which is above the abelian variety $A \simeq \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g)$. This affine differential addition is an essential building block for algorithms on abelian varieties that needs a bit more arithmetic, like isogenies [LR12; CR15] or pairings [LR10; LR13].

In this context, the affine three-way addition formulae from Equation (15) are also very useful; let $z_1, z_2, z_3 \in \mathbb{C}^g$, then given the affine coordinates of $z_1, z_2, z_3, z_2 + z_3, z_1 + z_3, z_1 + z_2$ one can use Equation (15) to recover the affine coordinates of $z_1 + z_2 + z_3$. (We refer to [LR13] for a proof which use a result similar to Theorem 3.3 but for sections of fibers translated by points, see also [Kem88]).

Unlike the standard addition, the (affine) differential addition can also be computed when the level n is two. Indeed, for the differential addition, by Corollary 3.6 we know the elements $\theta_i(z_1 + z_2)\theta_j(z_1 - z_2) + \theta_j(z_1 + z_2)\theta_i(z_1 - z_2)$, from which it is easy to also recover the coordinates $\theta_i(z_1 + z_2)$ if we also know the $\theta_i(z_1 - z_2)$.

We show that the affine three-way addition can also be computed when the even theta null coordinates are nonzero. This is a strengthening a result of [LR13] which the same result is proved only for general points.

Proposition 3.7. *Let $\mathscr{L} = \mathscr{L}_0^n$ with n even and $z_1, z_2, z_3 \in \mathbb{C}^g$. Then from the affine level n theta coordinates of $z_1, z_2, z, z_2 + z_3, z_1 + z, z_1 + z_2$, one can compute the affine coordinates of $z_1 + z_2 + z_3$ up to a sign.*

Proof. If $n \geqslant 4$, this was already proven in [LR13]. We can thus assume that $n = 2$. If z_1, z_2 or z is a point of 2-torsion, we can directly compute the (affine) action of translation by it using Equation (8). If not one can do a compatible addition to recover $z_1 + z_2 + z_3$ projectively. We then need to find the projective factor λ. Writing $z_1 + 2z_2 + z_3 = (z_1 + z_2) + (z_2 + z_3) = (z_1 + z_2 + z_3) + z_2$ where the two terms on the right can be computed exactly by a differential addition gives λ^2. □

Of course in practice it is faster to use Equation (15) to compute the three-way addition because it will give enough relations in the generic case that to use the method of the proof of Proposition 3.7.

Corollary 3.8. *Let n be even, and assume that we have m points $P_i \in A(k)$ given by their theta coordinates $(\theta_k(z_i)_{k \in \mathbb{Z}(n)})$. Assume that we also know the theta coordinates $(\theta_k(z_i + z_j)_{k \in \mathbb{Z}(n)})$ for all $i \neq j$. Then for any $(\lambda_i)_{i=1}^m \in \mathbb{Z}^m$, there exists an algorithm to recover the theta coordinates of $(\theta_k(\lambda_1 z_1 + \cdots + \lambda_m z_m)_{k \in \mathbb{Z}(n)})$ of the sum $\sum \lambda_i z_i$.*

Proof. By an easy recursive application of Proposition 3.7 we can recover the affine theta coordinates of all points $\sum \varepsilon_i z_i$ where $\varepsilon_i \in \{0, 1\}$. One can then use differential additions to recover the affine theta coordinates of $\sum \lambda_i z_i$. □

3.4. **Summary.** Lest the reader be overwhelmed by all the different additions available from Riemann relations, a summary is probably welcome. Assume that the level n is even. Then (with the further hypothesis that the even theta null coordinates are nonzero if $n = 2$), we can (provided we have the theta null point):

- Given the affine (resp. projective) theta coordinates of z_1, z_2 and $z_1 - z_2$ compute the differential addition to get the affine (resp. projective) theta coordinates of $z_1 + z_2$ (Corollary 3.6);

- Given z in affine (resp. projective) theta coordinates compute the doubling $2z$ as a special case of the differential addition;
- Given the affine theta coordinates of z_1, z_2, z_3, z_1+z_2, z_1+z_3 and z_2+z_3 compute the affine three way addition to get the affine theta coordinates of $z_1+z_2+z_3$ (Proposition 3.7);
- More generally given the affine theta coordinates of z_i $(i=1,\dots,m)$ and of z_i+z_j $(i\neq j)$ compute a multiway addition to get the affine theta coordinates of $z_1+\cdots+z_m$ (Corollary 3.8);
- Given the projective theta coordinates of z_1 and z_2 compute the schematic addition $\{z_1+z_2, z_1-z_2\}$ (by the discussion following Corollary 3.6);
- As a corollary of the schematic addition, given the projective theta coordinates of z_1, z_2 and one extra coordinate $\theta_i(z_1+z_2)/\theta_j(z_1+z_2)$ with $i\neq j$, provided it is well defined (or the coordinate $\theta_i(z_1-z_2)/\theta_j(z_1-z_2)$), compute the addition z_1+z_2 in projective coordinates (Indeed [LR13] and Section 5.2 explain how Corollary 3.6 gives an algorithm for the schematic addition where the degree two scheme is parametrized by the roots $\{\theta_i(z_1+z_2)/\theta_j(z_1+z_2), \theta_i(z_1-z_2)/\theta_j(z_1-z_2)\}$);
- Given the projective theta coordinates of z_i $(i=1,\dots,m)$ and the projective theta coordinates of z_i+z_0 (with z_0 not of 2-torsion), compute the projective theta coordinates of $z_0+z_1+\cdots+z_m$ and $z_1+\cdots+z_m$ (Corollary 2.9);
- When $n>2$, given the projective theta coordinates of z_1 and z_2, compute the projective theta coordinates of z_1+z_2 (Corollary 3.6).

We refer to Section 5 for explicit formulae for abelian surfaces with $n=2$. In general the more information we have, the faster are the algorithms to compute the addition. In particular differential additions are very fast on the Kummer variety, especially in the generic case when the coordinates of z_1-z_2 are all nonzero as in [Gau07].

Using Theorem 2.6 with level 2 theta functions, the addition of $([P],[P+P_0])$ and $([Q],[Q+Q_0])$ uses two compatible additions. But when $[P+Q]$ is computed on the Kummer variety by the first compatible addition, rather than doing a second one we can compute $[P+Q+P_0]$ on the Kummer variety using the (projective) three way addition. By Section 5 this method is faster (and indeed we use the extra information we have just computed).

Remark 3.9. If we represent $\mathcal{K}_A$ via the embedding given by level 2 theta functions, then by Corollary 3.6 and Section 5.2 we have explicit formulae for the schematic addition, and so we can represent $P\in A$ using Theorem 2.6 by $([P],[P+P_0])$. It is straightforward to apply the isogeny and pairing algorithms from [LR12; LR13] on this representation.

For an isogeny $f:A\to B$, what we can compute is the map from the representation from $([P],[P+P_0])$ on A to the representation $([Q],[Q+f(P_0)])$ on B. In the case that f is an endomorphism so that $B=A$, we will usually want to compute the endomorphism with respect to the same representation $([Q],[Q+P_0])$ on A. Such is the case, for instance, when we want to use f to speed-up the scalar multiplication as in [GLV01]. To obtain f we can apply Remark 2.8 and compute once and for all an element in $\{[P_0+f(P_0)],[P_0-f(P_0)]\}\subset\mathcal{K}_A(k)$ (such a choice may amount to replacing f by $-f$).

4. Arithmetic, levels and isogenies

In this section we give formulae to go back and forth between the embedding given by Theorem 2.6 where the Kummer variety is embedded via level 2 theta coordinates and the embedding of the abelian variety given by level 4 theta coordinates.

As an application, we explain how to compute the fiber of the natural projection $\pi:A\to\mathcal{K}_A$ (from level 4 to level 2). The main result, extending the usual genus 1 case, says that we can compute this fiber only with differential and compatible additions up to one choice of sign (which involves taking a square root). We conclude the section by giving an efficient compression scheme for even higher level theta coordinates.

4.1. Level 4 theta coordinates.

If $E:y^2=f(x)$ is an elliptic curve given by its Weierstrass equation, working on the Kummer line amounts to forgetting the coordinate y. Reciprocally, given a point $[P]=x(P)$ on the Kummer line, finding the points $P,-P$ on E above it comes down to computing a square root to find $\{(x(P),\sqrt{f(x(P))}),(x,-\sqrt{f(x(P))})\}$.

If we use Theorem 2.6 to represent the abelian variety A as a subvariety of $\mathcal{K}_A \times \mathcal{K}_A$ where $\mathcal{K}_A$ is embedded using level 2 theta functions, then the fiber is easy to compute: given $[P] \in \mathcal{K}_A(k)$ we need to compute $[P+P_0] \in \mathcal{K}_A(k)$ to get the representation $([P],[P+P_0]) \in A(k)$. But the schematic addition between $[P]$ and $[P_0]$ outputs a degree 2 polynomial whose roots encode $[P+P_0]$ and $[P-P_0]$ which are the two points above $[P]$ (see Section 5 for explicit formulae). Hence computing the fiber only requires a square root.

Now to compute the fiber in level 4 theta coordinates it only remains to show how to convert back and forth from these coordinates to the model from Theorem 2.6.

If $(A,\mathscr{L}_0)$ is a principally polarised abelian variety, the map from the abelian variety (level 4) to the Kummer variety (level 2) is given by the duplication formulae from Theorem 3.1. More precisely, if $\mathscr{L} = \mathscr{L}_0^2$ and we work with the basis $(\theta_i^{\mathscr{L}})_{i\in Z(2)}$ of level 2 theta functions for the embedding of $\mathcal{K}_A$ and the basis $(\theta_i^{\mathscr{L}^2})_{i\in Z(4)}$ of level 4 theta functions for the embedding of A, then the natural projection $A \to \mathcal{K}_A$ is given by

$$\theta_{i+j}^{\mathscr{L}}(x)\theta_{i-j}^{\mathscr{L}}(x) = \frac{1}{2^g}\sum_{t\in Z(2)} \theta_{i+t}^{\mathscr{L}^2}(x)\theta_{j+t}^{\mathscr{L}^2}(0) \tag{17}$$

Indeed, we note that on the left of Equation (17) we get a product of two level 2 theta functions, so by Theorem 3.3 and Remark 3.4 we get all even coordinates $\Gamma(A,\mathscr{L}^2)^+$. Thus Equation (17) defines the projection map π from $(A,\mathscr{L}^2)$ to $(\mathcal{K}_A,\mathscr{L}^{2+})$.

We suppose here that we know the abelian variety A via its level 4 theta null point $\widetilde{0}_A = (\theta_i(0))_{i\in Z(n)}$. For $i \in Z(4)$, we note T_i the point of 4-torsion corresponding to $-\frac{i}{4} \in \frac{1}{4}\mathbb{Z}^g/\mathbb{Z}^g$ from Equation (9). Fix a point $i_0 \in Z(4)$, given P in $(A,\mathscr{L}^2)$ Equation (9) shows how to compute $P+T_{i_0}$ from which we get $([\pi(P)],[\pi(P+T_{i_0})])$. This explains how to go from level 4 to the embedding from Theorem 2.6 with $P_0 = T_{i_0}$.

It remains to explain how to invert Equation (17) to go from $([\pi(P)],[\pi(P+T_{i_0})])$ to P. It will be easier to work with the variables $U_{\chi,i}^{\mathscr{L}^2}$ from Section 3 since Equation (12) gives

$$U_{\chi,i}^{\mathscr{L}^2}(P)U_{\chi,j}^{\mathscr{L}^2}(0) = \sum_{t\in Z(2)} \chi(t)\theta_{i+j+t}^{\mathscr{L}}(P)\theta_{i-j+t}^{\mathscr{L}}(P). \tag{18}$$

Since the odd theta null values are null, using Equation (18) directly allows only to recover the coordinates $U_{\chi,i}^{\mathscr{L}^2}$ such that $\chi(2i)=1$.

Let i be an element of $Z(4)$, from Equation (9) we compute that $U_{\chi,i}(T_i) = U_{\chi,0}(0) \neq 0$. With the equation

$$U_{\chi,i}^{\mathscr{L}^2}(P)U_{\chi,i}^{\mathscr{L}^2}(T_i) = \sum_{t\in Z(2)} \chi(t)\theta_{2i+t}^{\mathscr{L}}(P+T_i)\theta_t^{\mathscr{L}}(P-T_i), \tag{19}$$

we can then recover $U_{\chi,i}^{\mathscr{L}^2}(P)$ provided that we know the level 2 theta coordinates of $[P+T_i]$ and $[P-T_i]$. We already know by hypothesis $[P+T_{i_0}] \in \mathcal{K}_A(k)$. From $T_i \in A$ we can compute $([T_i],[T_i+T_0]) \in \mathcal{K}_A \times \mathcal{K}_A$. Then we just need to use a compatible addition (Proposition 2.2) to recover $P+T_i$, and then a differential addition to get $P-T_i$.

Remark 4.1. One should be careful here because Equation (19) makes sense for affine coordinates and we are working with projective coordinates. What happens is that by taking an affine lift of the level 4 theta null point, we can use Equation (9) to get a canonical lift of the 4-torsion points T_i. Let $z \in \mathbb{C}^g$ be a lift of P, then if we take any affine lift $\widetilde{P+T_i}$ of $[P+T_i] \in \mathcal{K}_A$ it is equal to $z+T_i$ up to a projective factor λ. But then computing $\widetilde{P-T_i}$ affinely via a differential addition gives that $\widetilde{P-T_i}$ is equal to $z-T_i$ up to the projective factor λ^{-1}; so these factors cancels out in Equation (19).

4.2. **A compact representation of higher level theta coordinates.** Let $(A,\mathscr{L}_0^n)$ be an abelian variety described by level n theta functions with $2 \mid n$ and $n > 2$. There exists a generalisation of the duplication formulae given by [Koi76; Kem89] which gives the projection map π from A to $\mathcal{K}_A$ (in level 2). Unfortunately this change of level map is harder to inverse than the duplication formulae. Instead we will investigate another map that comes from isogenies.

Theorem 4.2 (Isogeny theorem)**.** *Let $n = n_1 n_2$ and $\ell = \ell_1 \ell_2$. Let $\pi : A = \mathbb{C}^g/(\mathbb{Z}^g \oplus \Omega\mathbb{Z}^g) \to B = \mathbb{C}^g/(\mathbb{Z}^g \oplus \frac{l_1}{l_2}\Omega\mathbb{Z}^g) : z \mapsto l_1 z$ be the canonical isogeny with kernel $K = \frac{1}{\ell_1}\mathbb{Z}^g/\mathbb{Z}^g \oplus \frac{1}{\ell_2}\Omega\mathbb{Z}^g/\Omega\mathbb{Z}^g$. Then if we use the basis with level $\ell n = (\ell_1 n_1)(\ell_2 n_2)$ from Equation (5) for A and the basis with level $n = n_1 n_2$ for B, we get that*

$$\pi^*\left(\theta\begin{bmatrix} a/n_1 \\ b/n_2 \end{bmatrix}(n_1 z, \frac{n_1}{n_2}(\frac{\ell_1}{\ell_2}\Omega))\right) = \theta\begin{bmatrix} a\ell_1/n_1\ell_1 \\ b\ell_2/n_2\ell_2 \end{bmatrix}(n_1(\ell_1 z), \frac{n_1\ell_1}{n_2\ell_2}\Omega)$$

Proof. This is immediate. □

Corollary 4.3. *Let $A = \mathbb{C}^g/(\mathbb{Z}^g \oplus \Omega\mathbb{Z}^g)$ be an abelian variety, that we represent via the embedding of level n theta functions where $n = 2m$ is greater or equal to 4. Let $\pi : A \to B = \mathbb{C}^g/(\mathbb{Z}^g \oplus \frac{\Omega}{m}\mathbb{Z}^g) : z \mapsto z$ be the canonical isogeny of kernel $K = \frac{1}{m}\Omega\mathbb{Z}^g/\Omega\mathbb{Z}^g$, where we represent B with level 2 theta coordinates. Then*

$$(\theta_i^B(\pi(z))_{i\in Z(2)} = (\theta^A_{\varphi(i)}(z))$$

where $\varphi : Z(2) \to Z(n)$ is the natural embedding.

We can also see the theta coordinates as affine coordinates on $\mathbb{C}^g$ rather than as projective coordinates on the abelian variety $A = \mathbb{C}^g/\Lambda$. We recall from Section 3 that we define the affine coordinates of $z \in \mathbb{C}^g$ as $\theta_i(z)$, $i \in Z(n)$. It is easy to lift π to an affine map $\widetilde{\pi}$ such that $\widetilde{\pi}^*\theta_i^B = \theta^A_{\varphi(i)}$:

Theorem 4.4. *Let $e_1, \dots, e_g$ be a basis of $\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g$ given by affine theta coordinates (they can be recovered from the affine theta null point of level n on A via Equation (8)).*

Let $z \in \mathbb{C}^g$. Then

- *The affine theta null point $\widetilde{0}_A$ can be recovered from the $1 + g(g+1)/2$ points $\widetilde{\pi}(0_A)$, $\widetilde{\pi}(e_i)$, $\widetilde{\pi}(e_i + e_j)$;*
- *The affine theta null point z can be recovered from the above data and the $1 + g$ points $\widetilde{\pi}(z)$, $\widetilde{\pi}(z + e_i)$. In particular we can encode a point on A by using $(1 + g)2^g$ coordinates (once we know the theta null point).*

Proof. If we combine Equation (9) with the form of $\widetilde{\pi}$ given by Corollary 4.3, then it is straightforward to see that we can recover the theta coordinates of z from the theta coordinates of the points $\widetilde{\pi}(z + \sum \lambda_i e_i)$ where $\lambda_i \in \{0, \dots, \ell - 1\}$. But $\widetilde{\pi}(z + \sum \lambda_i e_i) = \widetilde{\pi}(z) + \sum \widetilde{\pi}(\lambda_i e_i)$. By Corollary 3.8, we can recover the right hand term from the points $\widetilde{\pi}(0_A)$, $\widetilde{\pi}(e_i)$, $\widetilde{\pi}(e_i + e_j)$, $\widetilde{\pi}(z)$, $\widetilde{\pi}(z + e_i)$ by using three-way additions and differential additions. □

Remark 4.5. If $n \geqslant 4$ and $g > 1$ we thus also get a more compact representation of a point x in the abelian variety A than by using the level n theta functions as coordinates. We can also compute the arithmetic directly on this representation: if we know the coordinates of $x, y \in A$ given by $\widetilde{\pi}(x)$, $\widetilde{\pi}(x + e_i)$, $\widetilde{\pi}(y)$, $\widetilde{\pi}(y + e_i)$; then we can recover the coordinates $\widetilde{\pi}(x + y)$, $\widetilde{\pi}(x + y + e_i)$ by doing some three-way additions. (Of course if we already know $\widetilde{\pi}(x - y)$, $\widetilde{\pi}(x - y + e_i)$ it is faster to do differential additions).

Remark 4.6. If we only know $\pi(z)$, since B is represented by theta functions of level 2 this mean that we know $\pi(z) \in \mathcal{K}_B$, and the best we can hope is to recover the preimage $[z] + \operatorname{Ker}\pi \in A$. This preimage can be recovered in a similar way as we did in the inversion of the duplication formula. First we fix a choice of $\pi(z) + \pi(e_1)$; we can recover all the other points $\pi(z) + \pi(e_i)$ by a compatible addition with $\pi(e_1 + e_i)$. Now we fix an affine lift $\lambda_i\widetilde{\pi}(z + e_i)$ where λ_i is an unknown projective factor. By computing differential additions, and since $\widetilde{\pi}(z + me_i) = \widetilde{\pi}(z)$ we recover λ_i^m as in [LR12; CR15]. We choose λ_i satisfying these equations; by Theorem 4.4 we can then recover one of the element z (or $-z$) in the preimage. In total there is $2m^g$ possible choices, so we recover all elements in the preimage.

Example 4.7. Let D be the diagonal matrix with entries $(1, \dots, 1, 2)$ and let A' be the abelian variety $A' = \mathbb{C}^g/(\mathbb{Z}^g + D\Omega\mathbb{Z}^g)$ where $\Omega \in \mathfrak{H}_g$. Then Ω induces a polarisation $\mathscr{L}$ of type $(1, \dots, 1, 2)$ on A'; a basis of sections of $\mathscr{L}^2$ is given by

$$\theta\begin{bmatrix} 0 \\ b \end{bmatrix}(\cdot, \Omega(2D)^{-1})_{b\in(2D)^{-1}\mathbb{Z}^g/\mathbb{Z}^g}.$$

If A' is simple, then by [BL04, Theorem 4.3.1] $\mathscr{L}$ has no fixed components so that $\mathscr{L}^2$ is a very ample line bundle by [BL04, Theorem 4.5.5]. So in this case we can embed the abelian variety A' using only $2 \cdot 2^g$ projective coordinates. Unfortunately A' is not principally polarized in general since the Néron Severi group of an abelian variety is $\mathbb{Z}$ generically.

Still, if we let $\pi : A' \to A = \mathbb{C}^g/(\Omega\mathbb{Z}^g + \mathbb{Z}^g)$, then a similar reasoning as in Corollary 4.3 and Theorem 4.4 show that for $z \in \mathbb{C}^g$, the level $(2, 2, \ldots, 2, 4)$-theta coordinates of z with respect to A' can be recovered from the level 2 theta coordinates with respect to A of the two points $\widetilde{\pi}(z)$ and $\widetilde{\pi}(z + e)$ where e is the point of 4-torsion generating $D^{-2}\mathbb{Z}^g/\mathbb{Z}^g$. Thus we see that hybrid level-$(2, 2, \ldots, 4)$ theta functions are a particular case of Theorem 2.6.

5. Explicit formulae for abelian surfaces

Let $(a_i)_{i \in Z(2)}$ be the level two theta null point representing a Kummer variety $\mathcal{K}_A$ of dimension 2. Let $x = (x_i)_{i \in Z(2)}$ and $y = (y_i)_{i \in Z(2)}$, we let $X = x + y$ and $Y = x - y$. We will give formulae for the coordinates $2\kappa_{ij} = X_i Y_j + X_j Y_i$.

Let $i \in Z(2), \chi \in \hat{Z}(2)$ and let

$$z_i^\chi = \Big(\sum_{t \in Z(2)} \chi(t) x_{i+t} x_t\Big)\Big(\sum_{t \in Z(2)} \chi(t) y_{i+t} y_t\Big)/\Big(\sum_{t \in Z(2)} \chi(t) a_{i+t} a_t\Big).$$

By Equation (12), $\sum_t \chi(t) a_{i+t} a_t$ is simply the classical theta null point $\theta \left[\begin{smallmatrix} \chi/2 \\ i/2 \end{smallmatrix}\right] (0, \Omega)^2$. Then Theorem 3.2 gives

$$\begin{aligned}
4X_{00}Y_{00} &= z_{00}^{00} + z_{00}^{01} + z_{00}^{10} + z_{00}^{11};\\
4X_{01}Y_{01} &= z_{00}^{00} - z_{00}^{01} + z_{00}^{10} + z_{00}^{11};\\
4X_{10}Y_{10} &= z_{00}^{00} + z_{00}^{01} - z_{00}^{10} - z_{00}^{11};\\
4X_{11}Y_{11} &= z_{00}^{00} - z_{00}^{01} - z_{00}^{10} + z_{00}^{11};\\
\\
2(X_{10}Y_{00} + X_{00}Y_{10}) &= z_{10}^{00} + z_{10}^{01};\\
2(X_{11}Y_{01} + X_{01}Y_{11}) &= z_{10}^{00} - z_{10}^{01};\\
2(X_{01}Y_{00} + X_{00}Y_{01}) &= z_{01}^{00} + z_{01}^{10};\\
2(X_{11}Y_{10} + X_{10}Y_{11}) &= z_{01}^{00} - z_{01}^{10};\\
2(X_{11}Y_{00} + X_{00}Y_{11}) &= z_{11}^{00} + z_{11}^{11};\\
2(X_{01}Y_{10} + X_{10}Y_{01}) &= z_{11}^{00} - z_{11}^{11};
\end{aligned}$$

As usual, we let M represent the cost of a multiplication (in the field of definition of x and y), S represent the cost of a square, and M_0 represent the cost of a multiplication coming from the theta null point $(a_i)_{i \in Z(2)}$ (so a data that depend only on the Kummer variety). Finally I represent the cost of an inversion, which we will replace by some multiplications using the fact that we have projective coordinates. We may suppose that $a_0 = 1$. Also we note $A_i^\chi = \sum \chi(t) a_{i+t} a_i$. We have seen that from the duplication formulae, if $a_i = \theta \left[\begin{smallmatrix} 0 \\ i/2 \end{smallmatrix}\right] (0, \Omega/2)$ then $A_i^\chi = \theta \left[\begin{smallmatrix} \chi/2 \\ i/2 \end{smallmatrix}\right] (0, \Omega)^2$. For homogeneity reasons, we may also assume that $A_{00}^{00} = 1$.

Lemma 5.1. *Given the theta coordinates of x and y, computing all the κ_{ij} requires $10M + 20S + 9M_0$. When $x = y$, the cost reduces to $6M + 14S + 9M_0$.*

Proof. To compute the four z_i^{00} we need $4M+8S+3M_0$. To compute the two z_i^{10} we need $2M+4M+2M_0$. But actually, since we already have the squares x_i^2 from the computation of the z_i^{00}, we can compute the product $x_{i+t}x_t$ as $2x_{i+t}x_t = (x_{i+t} + x_t)^2 - x_{i+t}^2 - x_t^2$ so the actual cost is $2M + 4S + 2M_0$. In total to compute all κ_{ij} we need $4M + 8S + 3M_0 + 3(2M + 4S + 2M_0) = 10M + 20S + 9M_0$. When $x = y$, the cost reduces to $8S + 3M_0 + 3(2M + 2S + 2M_0) = 6M + 14S + 9M_0$. □

5.1. **Differential additions.**

Lemma 5.2. *Given the coordinates of x, y and $Y = x - y$, assuming that the coordinates of Y are nonzero, computing the coordinates of $X = x + y$ requires $4M + 8S + 3M_0 + 4I$.*

When the coordinates of the theta null point are nonzero, a doubling costs $8S + 6M_0$.

Proof. In the generic case where the coordinates of Y are nonzero, the first four equations are enough to give the κ_{ii} and can be used to compute the differential addition X from x, y, Y in $4M + 8S + 3M_0 + 4I$ (in the non generic case we need all the κ_{ij}). Similarly, to compute the double of x (again in the generic case where the coordinates of the theta null point are nonzero), we need $8S + 6M_0$. □

Remark 5.3. Once we have computed the differential addition $x + y$, computing another differential addition $x + y'$ involving the same point x costs only $4M + 4S + 3M_0 + 4I$.

Lemma 5.4. *There exists an algorithm to compute the multiplication $m_1P_1 + \cdots + m_dP_d$, via a d-multiscalar Montgomery ladder with a cost of $7dM + (8 + 4d)S + (6 + 3d)M_0$ by step.*

Proof. In a one dimensional Montgomery ladder, computing the scalar multiplication nP, the differential additions will involve the point P so up to some precomputations the $4I$ from the formula above become $3M$. One step of the Montgomery ladder then costs $7M + 12S + 9M_0$; we recover the formulas from [Gau07] this way. In [Gau07] a $3M - 3S - 3M_0$ tradeoff is described. For the complexity analysis here we assume that we have small constants so the cost of M_0 is small and we have not done this trade off.

In a d-multiscalar Montgomery ladder, the algorithm from [Bro06] costs 1 doubling and d differential addition on the Kummer variety by step. This gives a complexity of $8S + 6M_0 + d(7M + 4S + 3M_0) = 7dM + (8 + 4d)S + (6 + 3d)M_0$. □

5.2. **Compatible additions.**

Lemma 5.5. *A compatible addition costs $28M + 32S + 14M_0$.*

Proof. We describe the degree two scheme $\{X, Y\}$ by the polynomial $\mathfrak{P}_\alpha(Z) = Z^2 - 2\frac{\kappa_{\alpha 0}}{\kappa_{00}}Z + \frac{\kappa_{\alpha\alpha}}{\kappa_{00}}$ whose roots are $\{\frac{X_\alpha}{X_0}, \frac{Y_\alpha}{Y_0}\}$ (where α is such that $X_\alpha Y_0 - X_0 Y_\alpha \neq 0$). To compute κ_{00} and $\kappa_{\alpha\alpha}$ we need $4M + 8S + 3M_0$, and to compute $\kappa_{\alpha 0}$ we need $2M + 4S + 2M_0$; so in total to compute $\mathfrak{P}_\alpha$, we need $6M + 12S + 5M_0 + 2I$.

Once we have a root Z, if we let $Z' = 2\frac{\kappa_{\alpha 0}}{\kappa_{00}} - Z$ be the conjugate root (corresponding to $\frac{Y_\alpha}{Y_0}$), we can recover the coordinates X_i, Y_i by solving the equation

$$\begin{pmatrix} 1 & 1 \\ Z & Z' \end{pmatrix} \begin{pmatrix} Y_i/Y_0 \\ X_i/X_0 \end{pmatrix} = \begin{pmatrix} 2\kappa_{0i}/\kappa_{00} \\ 2\kappa_{\alpha i}/\kappa_{00} \end{pmatrix}.$$

We find $X_i = \frac{2(Z\kappa_{0i} - \kappa_{\alpha i})}{\kappa_{00}(Z - Z')} = \frac{Z\kappa_{0i} - \kappa_{\alpha i}}{Z\kappa_{00} - \kappa_{\alpha 0}}$ for $i \neq 0, \alpha$ (here we have $X_0 = 1$, $X_\alpha = Z$). But usually we will express $Z = (X_0 : X_\alpha) \in \mathbb{P}^1$ as a point in the projective line, and we find that

$$X_i = \frac{X_\alpha \kappa_{0i} - X_0 \kappa_{\alpha i}}{X_\alpha \kappa_{00} - X_0 \kappa_{\alpha 0}}.$$

Recovering the projective coordinates of X then costs $8M$ (given the κ_{ij}). To sum up, given $Z = (X_0 : X_\alpha)$ recovering X costs in total $(10M + 20S + 9M_0) + 8M = 18M + 20S + 9M_0$.

For a compatible addition, where $x + y = z + t$, we can find Z as the common root between $\mathfrak{P}_\alpha$ and the similar polynomial $\mathfrak{P}'_\alpha(Z) = Z^2 - 2\frac{\kappa'_{\alpha 0}}{\kappa'_{00}}Z + \frac{\kappa'_{\alpha\alpha}}{\kappa'_{00}}$ coming from the symmetric coordinates $z_i t_j + t_i z_j$. Computing the coefficients needed for $\mathfrak{P}'_\alpha$ costs $6M + 12S + 5M_0$. The common root is

$$Z = \frac{\frac{\kappa'_{\alpha\alpha}}{\kappa'_{00}} - \frac{\kappa_{\alpha\alpha}}{\kappa_{00}}}{-2\frac{\kappa_{\alpha 0}}{\kappa 00} + 2\frac{\kappa'_{\alpha 0}}{\kappa'_{00}}} = \frac{\kappa'_{\alpha\alpha}\kappa_{00} - \kappa_{\alpha\alpha}\kappa'_{00}}{2(\kappa'_{\alpha 0}\kappa_{00} - \kappa_{\alpha 0}\kappa'_{00})}.$$

Computing Z projectively costs $4M$. In the end, a compatible addition costs $(18M + 20S + 9M_0) + (6M + 12S + 5M_0) + 4M = 28M + 32S + 14M_0$. □

5.3. **Multiscalar multiplication.** We compute the cost of a multiscalar multiplication using the strategy outlined in Proposition 2.12 and Remark 2.14; which cost one compatible addition, one differential addition and one doubling by multibits. With the same notations as this Proposition, we assume that we have precomputed all data corresponding to the $\sum \varepsilon_i P_i$, $\varepsilon_i \in \{0,1\}$. For the compatible addition, due to the precomputations we gain $(1M+4S+2S\times 3+9M_0)+(1M+4S+2S+5M_0) = 2M+16S+14M_0$ and the compatible addition costs $26M+16S$. The doubling and the differential addition then cost $(8S+6M_0)+(7M+3M_0) = 7M+8S+9M_0$ (reusing what we have already computed for the compatible addition). Finally we get a cost of $33M+24S+9M_0$ by multibits.

Combined with Lemma 5.4, for a d-dimensional GLV scheme, using compatible additions or only differential additions according to the size of d, we get the following complexity result:

Lemma 5.6. *A d-dimensional scalar multiplication can be computed in time $Max(7dM+(8+4d)S+(6+3d)M_0, 33M+24S+9M_0)$ per multibits.*

In particular, even for large d we are competitive with the best result using Mumford coordinates (in Jacobian form) [HC] which needs $52M+11S$ for a `mDBLADD` (Mixed Doubling-and-Addition).

We note that there is probably a lot of room for improvement here. First, we only need the square of the coordinates of the point computed via a compatible addition, there may be a way to compute them directly faster. Also we have not used the equation of the Kummer surface to speed up the computations.

5.4. **Addition on the abelian variety.**

Lemma 5.7. *In the $([x],[x+T])$ representation from Section 2.2, a doubling costs $4M+12S+12M_0$, a differential addition $24M+12S+6M_0$ and an addition $50M+32S+20M_0$.*

Proof. In the model from Section 2.2, a doubling costs one doubling and one differential addition in the Kummer, for a cost of $4M+12S+12M_0$. A differential addition costs two differential additions in the Kummer, for a cost of $(4M+8S+3M_0+4I)+(4M+4S+3M_0+4I) = 8M+12S+6M_0+(6M+4M+4M) = 24M+12S+6M_0$.

A standard addition is much more expensive: we compute $x+y+T$ via a compatible addition $(x+T)+y = x+(y+T)$, for a cost of $28M+32S+14M_0$. We could compute $x+y$ via another compatible addition, but it is faster to do a three-way addition, using Equation (15). For all $\chi \in \hat{Z}(2)$,

$$\Big(\sum_{t\in Z(2)} \chi(t)(x+y+T)_t T_t\Big)\Big(\sum_{t\in Z(2)} \chi(t) x_t y_t\Big) = \Big(\sum_{t\in Z(2)} \chi(t) 0_t (x+y)_t\Big)\Big(\sum_{t\in Z(2)} \chi(t)(y+T)_t (x+T)_t\Big).$$

To recover $x+y$, this costs $(4M+4M+3M_0)+(1M+1I)\times 4+3M_0 = 12M+6M_0+4I = 22M+6M_0$. In total a standard addition costs $(28M+32S+14M_0)+(22M+6M_0) = 50M+32S+20M_0$.

If we will add y a lot of times so we are allowed to make precomputations first, then as in Section 5.3 the cost of the compatible addition to compute $x+y+T$ is $28M+16S$, the cost of the three-way addition is $20M+6M_0$ for a total cost of $48M+16S+6M_0$. □

As we can see the arithmetic is expensive in this representation. To be efficient, as discussed in Section 2.2 one needs to go to the level 2 Kummer model (once the necessary precomputations have been done in this representation), and only switch back to this representation at the end using a compatible addition. Using Lemma 5.6 (and neglecting the precomputations and the compatible addition at the end), a d-dimensional scalar multiplication can then be computed in time $\mathrm{Max}(7dM+(8+4d)S+(6+3d)M_0, 33M+24S+9M_0)$ per multibits on the abelian variety.

6. Conclusion

In this paper we have shown how a simple type of addition on a Kummer variety which we called the compatible addition can be used to do some arithmetic that does not come from differential additions.

We have used this tool to explain how to go from a level 2 theta representation to a level 4 theta representation and to derive an efficient representation of an abelian variety A by embedding it into $\mathcal{K}_A^2$. If $\mathcal{K}_A$ is represented by theta functions of level 2, this representation only add one extra coordinates (more precisely this gives an embedding of A into $\mathbb{P}^{2^g-1}\times\mathbb{P}^1$), and benefits from the same efficient scalar multiplication as the one in $\mathcal{K}_A$.

References

[BBJ+08] D. Bernstein, P. Birkner, M. Joye, T. Lange, and C. Peters. "Twisted edwards curves". In: *Progress in Cryptology–AFRICACRYPT 2008* (2008), pp. 389–405 (cit. on p. 2).

[Ber06] D. J. Bernstein. "Differential addition chains". 2006. URL: http://cr.yp.to/ecdh/diffchain-20060219.pdf (cit. on pp. 5–7).

[BCL+14] D. J. Bernstein, C. Chuengsatiansup, T. Lange, and P. Schwabe. "Kummer strikes back: new DH speed records". 2014. eprint: 2014/134.pdf (cit. on p. 2).

[BL04] C. Birkenhake and H. Lange. *Complex abelian varieties*. Second. Vol. 302. Grundlehren der Mathematischen Wissenschaften [Fundament al Principles of Mathematical Sciences]. Berlin: Springer-Verlag, 2004, pp. xii+635. ISBN: 3540204881 (cit. on pp. 7, 8, 11, 16).

[BCH+13] J. W. Bos, C. Costello, H. Hisil, and K. Lauter. "Fast cryptography in genus 2". In: *Advances in Cryptology–EUROCRYPT 2013*. Springer, 2013, pp. 194–210 (cit. on p. 2).

[Bro06] D. R. Brown. "Multi-dimensional Montgomery ladders for elliptic curves". 2006. eprint: 2006/220 (cit. on pp. 6, 17).

[Can87] D. G. Cantor. "Computing in the Jacobian of a hyperelliptic curve". In: *Math. Comp.* 48.177 (1987), pp. 95–101. ISSN: 0025-5718 (cit. on p. 1).

[Cos11] R. Cosset. "Application des fonctions thêta à la cryptographie sur courbes hyperelliptiques". PhD thesis. 2011 (cit. on p. 2).

[CR15] R. Cosset and D. Robert. "An algorithm for computing (ℓ, ℓ)-isogenies in polynomial time on Jacobians of hyperelliptic curves of genus 2". Nov. 2015 (cit. on pp. 2, 12, 15).

[Dup06] R. Dupont. "Moyenne arithmetico-geometrique, suites de Borchardt et applications". In: *These de doctorat, Ecole polytechnique, Palaiseau* (2006) (cit. on p. 11).

[GLV01] R. P. Gallant, R. J. Lambert, and S. A. Vanstone. "Faster Point Multiplication on Elliptic Curves with Efficient Endomorphisms". In: *CRYPTO*. Ed. by J. Kilian. Vol. 2139. Lecture Notes in Computer Science. Springer, 2001, pp. 190–200. ISBN: 3540424563 (cit. on pp. 6, 13).

[Gau07] P. Gaudry. "Fast genus 2 arithmetic based on Theta functions". In: *Journal of Mathematical Cryptology* 1.3 (2007), pp. 243–265 (cit. on pp. 1, 2, 13, 17).

[GL09] P. Gaudry and D. Lubicz. "The arithmetic of characteristic 2 Kummer surfaces and of elliptic Kummer lines". In: *Finite Fields and Their Applications* 15.2 (2009), pp. 246–260 (cit. on p. 1).

[GL12] E. Z. Goren and K. E. Lauter. "Genus 2 curves with complex multiplication". In: *International Mathematics Research Notices* 2012.5 (2012), pp. 1068–1142 (cit. on p. 11).

[Got59] E. Gottschling. "Explizite bestimmung der randflächen des fundamentalbereiches der modulgruppe zweiten grades". In: *Mathematische Annalen* 138.2 (1959), pp. 103–124 (cit. on p. 11).

[Har00] R. Hartshorne. *Algebraic geometry*. Springer, 2000 (cit. on p. 11).

[HC] H. Hisil and C. Costello. "Jacobian Coordinates on Genus 2 Curves". In: (). eprint: 2014/385 (cit. on pp. 1, 18).

[Igu72] J.-I. Igusa. *Theta functions*. Die Grundlehren der mathematischen Wissenschaften, Band 194. New York: Springer-Verlag, 1972, pp. x+232 (cit. on p. 9).

[Kem88] G. Kempf. "Multiplication over abelian varieties". In: *American Journal of Mathematics* 110.4 (1988), pp. 765–773 (cit. on pp. 10–12).

[Kem89] G. Kempf. "Linear systems on abelian varieties". In: *American Journal of Mathematics* 111.1 (1989), pp. 65–94 (cit. on pp. 9, 10, 14).

[Koh11] D. Kohel. "Arithmetic of split Kummer surfaces: Montgomery endomorphism of Edwards products". In: *Coding and Cryptology*. Springer, 2011, pp. 238–245 (cit. on p. 4).

[Koi76] S. Koizumi. "Theta relations and projective normality of abelian varieties". In: *American Journal of Mathematics* (1976), pp. 865–889 (cit. on pp. 9–11, 14).

[Lan05] T. Lange. "Formulae for arithmetic on genus 2 hyperelliptic curves". In: *Applicable Algebra in Engineering, Communication and Computing* 15.5 (2005), pp. 295–328 (cit. on p. 1).

[LR10] D. Lubicz and D. Robert. "Efficient pairing computation with theta functions". In: *Algorithmic Number Theory*. Lecture Notes in Comput. Sci. (2010). Ed. by G. Hanrot, F. Morain, and E. Thomé. 9th International Symposium, Nancy, France, ANTS-IX, July 19-23, 2010, Proceedings. DOI: 10.1007/978-3-642-14518-6_21 (cit. on pp. 11, 12).

[LR12] D. Lubicz and D. Robert. "Computing isogenies between abelian varieties". In: *Compos. Math.* 148.5 (2012), pp. 1483–1515. ISSN: 0010-437X. DOI: 10.1112/S0010437X12000243. URL: http://dx.doi.org/10.1112/S0010437X12000243 (cit. on pp. 2, 7, 10, 12, 13, 15).

[LR13] D. Lubicz and D. Robert. "A generalisation of Miller's algorithm and applications to pairing computations on abelian varieties". In: (2013). preprint (cit. on pp. 2, 7, 12, 13).

[Mon87] P. L. Montgomery. "Speeding the Pollard and elliptic curve methods of factorization". In: *Mathematics of computation* 48.177 (1987), pp. 243–264 (cit. on p. 1).

[Mon92] P. L. Montgomery. "Evaluating recurrences of form Xm+n= f (Xm, Xn, Xm- n) via Lucas chains". In: *Available at ftp. cwi. nl:/pub/pmontgom/lucas. ps. gz* 349 (1992) (cit. on p. 1).

[Mum66] D. Mumford. "On the equations defining abelian varieties. I". In: *Invent. Math.* 1 (1966), pp. 287–354 (cit. on pp. 2, 7–10).

[Mum67a] D. Mumford. "On the equations defining abelian varieties. II". In: *Invent. Math.* 3 (1967), pp. 75–135 (cit. on pp. 2, 7).

[Mum67b] D. Mumford. "On the equations defining abelian varieties. III". In: *Invent. Math.* 3 (1967), pp. 215–244 (cit. on pp. 2, 7).

[Mum69] D. Mumford. "Varieties defined by quadratic equations". In: *Questions on Algebraic Varieties (CIME, III Ciclo, Varenna, 1969)* (1969), pp. 29–100 (cit. on p. 11).

[Mum70] D. Mumford. *Abelian varieties*. Tata Institute of Fundamental Research Studies in Mathematics, No. 5. Published for the Tata Institute of Fundamental Research, Bombay, 1970, pp. viii+242 (cit. on p. 7).

[Mum83] D. Mumford. *Tata lectures on theta I*. Vol. 28. Progress in Mathematics. With the assistance of C. Musili, M. Nori, E. Previato and M. Stillman. Boston, MA: Birkhäuser Boston Inc., 1983, pp. xiii+235. ISBN: 3764331097 (cit. on pp. 8, 10).

[Mum84] D. Mumford. *Tata lectures on theta II*. Vol. 43. Progress in Mathematics. Jacobian theta functions and differential equations, With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman and H. Umemura. Boston, MA: Birkhäuser Boston Inc., 1984, pp. xiv+272. ISBN: 0817631100 (cit. on p. 11).

[Mum91] D. Mumford. *Tata lectures on theta III*. Vol. 97. Progress in Mathematics. With the collaboration of Madhav Nori and Peter Norman. Boston, MA: Birkhäuser Boston Inc., 1991, pp. viii+202. ISBN: 0817634401 (cit. on p. 8).

[Rob10] D. Robert. "Fonctions thêta et applications à la cryptographie". PhD thesis. Université Henri-Poincarré, Nancy 1, France, July 2010. URL: http://www.normalesup.org/~robert/pro/publications/academic/phd.pdf. Slides http://www.normalesup.org/~robert/pro/publications/slides/2010-07-phd.pdf, TEL: tel-00528942. (Cit. on pp. 2, 11).

IRMAR, Universté de Rennes 1, Campus de Beaulieu, F-35042 Rennes FRANCE
E-mail address: david.lubicz@univ-rennes1.fr
URL: http://perso.univ-rennes1.fr/david.lubicz/

Délégation Générale de l'Armement, CELAR - BP 57419, 35174 Bruz Cedex

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

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

Équipe MACISA, LIRIMA (Laboratoire International de Recherche en Informatique et Mathématiques Appliquées)