The arithmetic of characteristic 2 Kummer surfaces

Pierrick Gaudry[1] and David Lubicz[2,3]

[1] LORIA, Campus Scientifique, BP 239, F-54506 Vandoeuvre-lès-Nancy
[2] CÉLAR, BP 7419, F-35174 Bruz
[3] IRMAR, Université de Rennes 1, Campus de Beaulieu, F-35042 Rennes

Abstract. The purpose of this paper is a description of a model of Kummer surfaces in characteristic 2, together with the associated formulas for the pseudo-group law. Since the classical model has bad reduction, a renormalization of the parameters is required, that can be justified using the theory of algebraic theta functions. The formulas that are obtained are very efficient and may be useful in cryptographic applications. We also show that applying the same strategy to elliptic curves gives Montgomery-like formulas in odd characteristic that are of some interest, and we recover already known formulas by Stam in characteristic 2.

1 Introduction

Efficient group laws for elliptic curves and Jacobian of hyperelliptic curves have applications in algorithmic number theory and in cryptography. The case of elliptic curves has been widely studied for years. Still some recent developments [BL07] demonstrate that the topic is not closed. As for genus 2 curves, the literature is more recent and less extended. However, there are already a great variety of coordinate systems, with variants depending on the base field characteristic, on the particular class of curves considered, or on the relative costs of multiplications and inversions in the base field (see [CF05, Chapter 14]).

It would be also interesting to represent and compute with more general objects such as abelian varieties or Kummer varieties. We recall that a Kummer variety K is the singular projective variety obtained by quotienting an abelian variety A by the inverse automorphism acting on it. Obviously the group law of A does not pass through the quotient. Still, if $\overline{P}$ is a geometric point of K, for any positive integer n one can define a point $n\overline{P}$ on K in the following way: first lift $\overline{P}$ to a point P on A, compute nP and project it to K. The result of this computation does not depend on the chosen lift of $\overline{P}$ on A. This is what we call the pseudo-group law of K. Grossly speaking, the Kummer variety K carries over most of the information provided by the $\mathbb{Z}$-module structure of A and this $\mathbb{Z}$-module structure is what is mostly used in cryptographic applications. As a matter of fact, in the case that A is an elliptic curve given by a Weierstrass equation, its associate Kummer variety is usually referred to as its Montgomery form. In this representation, a point is given by its abscissa and algorithms are known to compute efficiently the pseudo-group law.

Following Chudnovsky and Chudnovsky [CC86], Gaudry [Gau07] has recently shown how to use the theory of theta functions in order to design efficient genus 2 pseudo-group law formulae in the case where the base field has odd characteristic p and under additional rationality conditions. The pseudo-group formulas are deduced from the classical Riemann duplication formulas for theta functions by an application of the Lefschetz principle since everything has good reduction modulo p.

Unfortunately, the formulas of [Gau07] have bad reduction modulo 2. The aim of this paper is to give analog formulas which apply over a finite field k of characteristic 2. A first question is to find an equation for Kummer quartic's surface in characteristic 2. Over a field of odd characteristic, it is possible following [Mum66] to recover such a model just by looking for the degree 4 invariant forms with respect to the action of the theta group. This technique together with some extra geometric arguments has been extended to cover the characteristic 2 case in [LP02]. In section 2, we recover the same equation as in [LP02] by using a different approach. Our point of view in order to prove all our results is to consider a Kummer surface K over k as the special fiber of a Kummer scheme $\tilde{K}$ over $W(k)$ where $W(k)$ denote the discrete valuation ring of characteristic 0 with residue field k. We obtain our results by looking for characteristic 0 formulas with good reduction on the special fiber. This allows us to interpret the coefficients appearing in the equation of K in term of the residue modulo 4 of the theta constants of $\tilde{K}$. This identification is important in order to state and prove the pseudo-addition formulas. Moreover, it should be noted that in this way, we describe moduli invariants defined over the base field which are the equivalent of the usual theta constants. Our proof is based on a characterisation of the canonical lift in the coordinate system provided by the level 2 canonical theta structure [Car07].

Another contribution of this article is the derivation of genus 1 formulas that are similar to the genus 2 formulas of [Gau07] in odd characteristic and their characteristic 2 counterpart. In the case of odd characteristic, one finds some formulas that are very similar to those associated to the Montgomery form, but with slightly different properties. In characteristic 2, we recover some formulas already published by Stam [Sta03].

Organisation of the paper The paper is organized as follows. We start with the theoretical background leading to appropriate coordinates giving a nice form for the equation of a Kummer surface in characteristic 2. Then the formulas for the associated pseudo-group law are given in section 3 and proved in section 4. In section 5, we give the formulae that relate our Kummer surface coordinates to the classical Mumford representation. In section 6, we give similar formulas for genus 1, in the cases of odd and even characteristic. Finally, in section 7 we summarize the different costs of the group law and give some running times.

2 Equations for Kummer surfaces in characteristic 2

Algebraic theta functions In this paragraph, we recall some basic facts on algebraic theta functions and fix some notations for the rest of the paper. For more details, we refer to [Mum66]. In order to simplify our presentation, we consider the case of abelian varieties over a field k but the theory can be generalized for abelian schemes over any ring [Mum67]. Let A_k be a g dimensional abelian variety over k. If x is a closed point of A_k, we denote by τ_x the translation by x morphism of A_k. Let $\mathscr{L}$ be a degree d ample line bundle on A_k. From here we suppose that d is prime to the characteristic of k or that A_k is ordinary. There exists an isogeny $\phi_{\mathscr{L}}$ from A_k onto its dual $\hat{A}_k$ defined by $\phi_{\mathscr{L}} : A_k \to \hat{A}_k, x \mapsto \tau_x^* \mathscr{L} \otimes \mathscr{L}^{-1}$. As $\mathscr{L}$ is ample, the kernel $K(\mathscr{L})$ of $\phi_{\mathscr{L}}$ is a finite group scheme. The theta group $G(\mathscr{L})$ is by definition the set of pairs (x, ψ) where x is a closed point of $K(\mathscr{L})$ and ψ is an isomorphism of line bundle $\psi : \mathscr{L} \to \tau_x^* \mathscr{L}$ together with the composition law $(x, \psi) \circ (y, \phi) = (x + y, \tau_y^* \psi \circ \phi)$. It is easy to see that $G(\mathscr{L})$ is a group which is a central extension of $K(\mathscr{L})$ by $\mathbb{G}_{m,k}$. Let $\delta = (d_1, \ldots, d_l)$ a finite sequence of integers such that $d_i | d_{i+1}$, we consider the finite group scheme $Z(\delta) = (\mathbb{Z}/d_1\mathbb{Z})_k \times_k \ldots \times_k (\mathbb{Z}/d_l\mathbb{Z})_k$ with elementary divisors given by δ. For a well chosen unique δ, the finite group scheme $K(\delta) = Z(\delta) \times \hat{Z}(\delta)$ is isomorphic to $K(\mathscr{L})$, where $\hat{Z}(\delta)$ is the Cartier dual of $Z(\delta)$ ([Mum70]). The Heisenberg group of type δ is the scheme $\mathcal{H}(\delta) = \mathbb{G}_{m,k} \times Z(\delta) \times \hat{Z}(\delta)$ together with the group law defined on closed points by $(\alpha, x_1, x_2).(\beta, y_1, y_2) = (\alpha.\beta.y_2(x_1), x_1 + y_1, x_2 + y_2)$. It is a central extension of $Z(\delta) \times \hat{Z}(\delta)$ by $\mathbb{G}_{m,k}$. By definition, a theta structure Θ_δ of type δ is an isomorphism from $\mathcal{H}(\delta)$ to $G(\mathscr{L})$ which fits in the following commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{G}_{m,k} \arrow[r] \arrow[d, equal] & \mathcal{H}(\delta) \arrow[r] \arrow[d, "\Theta_\delta"] & K(\delta) \arrow[r] \arrow[d, "\overline{\Theta_\delta}"] & 0 \\
0 \arrow[r] & \mathbb{G}_{m,k} \arrow[r] & G(\mathscr{L}) \arrow[r] & K(\mathscr{L}) \arrow[r] & 0
\end{tikzcd}$$

We note that Θ_δ induces an isomorphism, denoted $\overline{\Theta}_\delta$ in the preceding diagram, from $K(\delta)$ into $K(\mathscr{L})$ and as a consequence a decomposition $K(\mathscr{L}) = K_1(\mathscr{L}) \times K_2(\mathscr{L})$ where $K_2(\mathscr{L})$ is the Cartier dual of $K_1(\mathscr{L})$. An important fact that we are going to use in this paper is that a theta structure determines a basis of global sections of $\mathscr{L}$ up to a constant factor and as such an embedding of A_k into $\mathbb{P}_k^{d-1}$. We briefly recall the construction of this basis. First, as previously mentioned Θ_δ determines a decomposition $K(\mathscr{L}) = K_1(\mathscr{L}) \times K_2(\mathscr{L})$. We recall that if K is a subgroup of $K(\mathscr{L})$, a level subgroup $\tilde{K}$ over K is a subgroup of $G(\mathscr{L})$ which is the image of a section of K into $G(\mathscr{L})$. We define the maximal level subgroups $\tilde{K}_1$ over $K_1(\mathscr{L})$ and $\tilde{K}_2$ over $K_2(\mathscr{L})$ as the image by Θ_δ of the subgroups $(1, x, 0)_{x \in Z(\delta)}$ and $(1, 0, y)_{y \in \hat{Z}(\delta)}$ of $\mathcal{H}(\delta)$. Let B_k be the quotient of A_k by $K_2(\mathscr{L})$ and $\pi : A_k \to B_k$ be the natural projection. By the descent theory of Grothendieck, the data of $\tilde{K}_2$ is equivalent to the data of a couple $(\mathscr{L}_0, \lambda)$ where $\mathscr{L}_0$ is a degree one ample line bundle on B_k and λ is an isomorphism

$\lambda : \pi^*(\mathscr{L}_0) \to \mathscr{L}$. Let s_0 be the unique global section of $\mathscr{L}_0$ up to a constant factor and let $s = \lambda(\pi^*(s_0))$.

Proposition 1. *For all $i \in Z(\delta)$, let $(x_i, \psi_i) = \Theta_\delta((1, i, 0))$. We set $\vartheta_i^{\Theta_\delta} = (\tau_{-x_i}^* \psi_i(s))$. The elements $(\vartheta_i^{\Theta_\delta})_{i \in Z(\delta)}$ form a basis of the global sections of $\mathscr{L}$ which is uniquely determined up to a multiplication by a factor independent of i by the data of Θ_δ.*

This proposition is just a rephrasing of [Mum66], Theorem 2 which says that the space of global sections of $\mathscr{L}$ is the unique irreducible representation of weight 1 of the theta group scheme.

By the preceding proposition it is possible to identify the k-vector space of global sections of $\mathscr{L}$ with the vector space $k[Z(\delta)]$ of functions from $Z(\delta)$ to k. There is an action of $\mathcal{H}(\delta)$ on $k[Z(\delta)]$ given, for all $(\alpha, y_1, y_2) \in \mathcal{H}(\delta)$, $f \in k[Z(\delta)]$ and $x \in Z(\delta)$, by

$$(\alpha, y_1, y_2).f(x) = \alpha.y_2(x)f(x + y_1). \tag{1}$$

This action is compatible via Θ_δ with the natural action of $G(\mathscr{L})$ on the global sections of $\mathscr{L}$.

Let $(\vartheta_i^{\Theta_\delta})_{i \in Z(\delta)}$ be a basis of the global sections of $\mathscr{L}$ determined by a theta structure Θ_δ and let x be a closed point of A_k. Denote by $\mathscr{O}_{A_k}$ the structure sheaf of A_k and let $\rho : \mathscr{O}_{A_k,x} \to k'$ be the evaluation morphism onto the residual field of x. We can choose an isomorphism $\xi : \mathscr{L}_x \simeq \mathscr{O}_{A_k,x}$. For all $i \in Z(\delta)$ the evaluation of the section $\vartheta_i^{\Theta_\delta}$ in x is $\vartheta_i^{\Theta_\delta}(x) = \rho \circ \xi(\vartheta_i^{\Theta_\delta})$. The resulting projective point $(\vartheta_i^{\Theta_\delta}(x))_{i \in Z(\delta)}$ over $\overline{k}$ does not depend on the choice of the isomorphism ξ.

Applying this last construction to the closed point 0 of A_k, one can associate to any triple $(A_k, \mathscr{L}, \Theta_\delta)$ a point of $\mathbb{P}_k^d$, given by its homogeneous coordinates $(\vartheta_i^{\Theta_\delta}(0))_{i \in Z(\delta)}$. This point is called the theta null point associated to $(A_k, \mathscr{L}, \Theta_\delta)$.

Some generalities on Kummer surfaces. Let k be any field and A_k be an ordinary abelian surface over k. The Kummer surface K_{A_k} is the singular surface obtained by quotienting A_k by the automorphism i on A_k defined over geometric points by $i : P \mapsto -P$. Let $\pi : A_k \to K_{A_k}$ be the canonical projection morphism. We recall that a line bundle $\mathscr{L}_k$ on A_k is symmetric if $i^*\mathscr{L}_k \simeq \mathscr{L}_k$ and is totally symmetric if there exists a line bundle $\mathscr{M}_k$ on K_{A_k} such that $\mathscr{L}_k \simeq \pi^*\mathscr{M}_k$. As we are interested in computing actual equations for K_{A_k}, we suppose that A_k comes with a totally symmetric degree $d > 0$ ample line bundle $\mathscr{L}_k$ and a theta structure Θ_δ of type δ. The triple $(A_k, \mathscr{L}_k, \Theta_\delta)$ provides us with a well defined projective embedding ϕ_{Θ_δ} of A_k in $\mathbb{P}^{d-1}$. In the case that $\mathscr{L}_k$ is a totally symmetric degree 2 line bundle on A_k, the image of ϕ_{Θ_δ} is isomorphic to K_{A_k}.

If the characteristic of k is prime to 2, by general theory [Mum67,MB85], it is possible a build a scheme whose point functor parametrizes the set of triples of isomorphism classes of $(A_{k'}, \mathscr{L}_{k'}, \Theta_\delta)$, where $\mathscr{L}_{k'}$ is a degree 8 line bundle and k' is any algebraic extension of k. In the following, we suppose that k is finite of characteristic 2 and we are interested in the set that we denote by $\mathscr{A}_\delta$

of isomorphism classes of triples $(A_{k'}, \mathscr{L}_{k'}, \Theta_\delta)$ with k' any finite extension of k and Θ_δ a theta structure of type $\delta = (2,2)$. The previously mentioned general results do not apply in our case and in order to find a moduli representation of $\mathscr{A}_\delta$, we are going to consider objects lifted over $\mathbb{Z}_q$.

Lifting abelian surfaces. Let k be any finite extension of $\mathbb{F}_2$ and let $W(k)$ be the ring of Witt vectors with coefficients in k. Let A_k be an ordinary abelian surface over k. Denote by $\mathscr{A}_{A_k}^{loc}$ the local deformation space of A_k which is the set of abelian schemes $A_{W(k)}$ over $W(k)$ whose special fiber is A_k up to isomorphism. There exists a distinguished element in $\mathscr{A}_{A_k}^{loc}$ called the canonical lift $A_{W(k)}^c$ of A_k. The canonical lift is uniquely defined up to isomorphism by the property that any endomorphism of A_k lifts to a relative endomorphism of $A_{W(k)}^c$.

Let $\mathscr{L}_k$ be an ample totally symmetric degree 2 line bundle on A_k. It should be remarked, by applying the criterion of [Mum66] §2 Proposition 1 and because the characteristic of k is 2, that if $\mathscr{L}_k$ is a symmetric line bundle then it is totally symmetric. As a consequence we can and will suppose in the following that $\mathscr{L}_k$ is the square of a ample degree one symmetric line bundle on A_k. One can lift the line bundle $\mathscr{L}_k$ to a degree 2 ample line bundle $\mathscr{L}_{W(k)}^c$ on $A_{W(k)}^c$ which is also totally symmetric by applying again [Mum66] §2 Proposition 1. Moreover every other lift of $\mathscr{L}_k$ is of the form $\tau_x^* \mathscr{L}_{W(k)}^c$ for $x \in A_{W(k)}^c[2]^0$ where $A_{W(k)}^c[2]^0$ is the connected part of the 2 torsion of $A_{W(k)}^c$ and as a consequence is isomorphic to $\mathscr{L}_{W(k)}^c$.

Let $\delta = (2,2)$ and let Θ_δ be a theta structure of type δ for $(A_k, \mathscr{L}_k)$. By doing a base field extension if necessary, we can suppose that Θ_δ is defined over k. We recall that Θ_δ fixes a group isomorphism $Z(\delta)_k \xrightarrow{\sim} K(\mathscr{L}_k)^{et} = A_k[2]^{\mathrm{et}}$. As the maximal étale part of $A_k[2]$ considered as a group lifts bijectively to the maximal étale part of $A_{W(k)}^c[2]$ we deduce from Θ_δ a group scheme isomorphism

$$Z(\delta)_{W(k)} \xrightarrow{\sim} A_{W(k)}[2]^{\mathrm{et}}. \tag{2}$$

By [Car07, Th.2.2], once an isomorphism (2) is chosen, there exists a set of distinguished theta structures Θ_δ^d of type δ for $(A_{W(k)}^c, \mathscr{L}_{W(k)}^c)$ defined over $W(k)$. Moreover, an element in this set of theta structures is uniquely determined by the data of a section of p in the connected-étale sequence:

$$0 \longrightarrow A_{W(k)}^c[2]^0 \longrightarrow A_{W(k)}^c[2] \xrightarrow{p} A_{W(k)}^c[2]^{et} \longrightarrow 0. \tag{3}$$

The set of such splittings is a principal homogeneous space over $A_{W(k)}^c[2]^0$. Moreover, under the assumption of (2) $A_{W(k)}^c[2]^0$ is isomorphic to $\hat{Z}_{\delta,W(k)}$. This gives an action of $\hat{Z}_{\delta,W(k)}$ on the set of isomorphism classes of triples $(A_{W(k)}^c, \mathscr{L}_{W(k)}^c, \Theta_\delta^d)$ which definition depends only on $(A_k, \mathscr{L}_k, \Theta_\delta)$ and all elements of the same orbit for this action reduce to the same triple modulo 2.

We have proved the

Lemma 1. *Let $\delta = (2,2)$. There is a one on one correspondence between the set of isomorphism classes of triples $(A_k, \mathscr{L}_k, \Theta_\delta)$ and the quotient of the set* *of isomorphism classes of triples* $(A^c_{W(k)}, \mathscr{L}^c_{W(k)}, \Theta^d_\delta)$ *by the action of* $\hat{Z}_{\delta,W(k)}$ *defined by (3).*

Actually there is a canonical choice for a section of p in (3). By definition of the canonical lift, the 2-adic Tate module $\mathbb{T}_2$ of $A^c_{W(k)}$ comes with a natural splitting as a product of its étale part and its local part: $\mathbb{T}_2 = \mathbb{T}_2^0 \times \mathbb{T}_2^{et}$. On the 2-torsion this gives us a canonical splitting $A^c_{W(k)}[2] = A^c_{W(k)}[2]^0 \times A^c_{W(k)}[2]^{et}$. Following [Car07] we denote by Θ^c_δ the canonical theta structure defined by this splitting and (2). We have the

Lemma 2. *Let* $\delta = (2,2)$*. There is a one on one correspondence between the set of isomorphism classes of triples* $(A_k, \mathscr{L}_k, \Theta_\delta)$ *and the set of isomorphism classes of triples* $(A^c_{W(k)}, \mathscr{L}^c_{W(k)}, \Theta^c_\delta)$*.*

Denote by $\mathscr{A}^c_\delta$ the set of triples $(A^c_R, \mathscr{L}^c_R, \Theta^c_\delta)$, where R is an unramified extension of $\mathbb{Z}_2$, A^c_R is an abelian scheme over R which is a canonical lift of its special fiber, $\mathscr{L}^c_R$ is a totally symmetric ample line bundle of degree 2 and Θ^c_δ is the canonical theta structure of type $\delta = (2,2)$. The aim of the rest of this paragraph is to describe the locus of theta null points associated to the generic fiber of elements of $\mathscr{A}^c_\delta$.

If $\mathscr{K}$ is an algebraic extension of $\mathbb{Q}_2$, one can associate to any triple $(A_{\mathscr{K}}, \mathscr{L}_{\mathscr{K}}, \Theta_\delta)$, its theta null point $(a_u)_{u\in Z(\delta)}$. This theta null point belongs to an open dense sub-variety of $\mathbb{P}^3_{\mathbb{Q}_2}$, that we denote by $\mathcal{M}_\delta$. Note that as $(a_u)_{u\in Z(\delta)}$ are homogeneous coordinates, we can always take $(a_u) \in W(k)^{Z(\delta)}$ by multiplying if necessary by a suitable power of 2. We suppose that this point actually comes from the generic fiber of an ordinary abelian scheme over an unramified extension of $\mathbb{Z}_2$. It is proved in [Car05] that if $(a_u)_{u\in Z(\delta)}$ represents the generic fiber of an element of $\mathscr{A}^c_\delta$ then it verifies the equations, for all $u \in Z(\delta)$

$$a_u^2 = \omega \sum_{v\in Z(\delta)} \sigma(a_{v+u})\sigma(a_v), \tag{4}$$

where σ is the lift of the p^{th}-Frobenius of k over $W(k)$ and ω is a unit in $W(k)$. Let v_2 be the 2-adic valuation on $W(k)$. From (4), we deduce immediately that if $u \neq 0_{Z(\delta)}$, then $v_2(a_u) \geq 1$. Moreover, $a_0 \mod 2$ is non zero and we have just proved the

Lemma 3. *If* $(a_u) \in W(k)^{Z(\delta)}$ *represents the generic fiber of an element of* $\mathscr{A}^c_\delta$ *then it reduces modulo* 2 *to the point with homogeneous coordinates* $(1:0:0:0)$*.*

Equation in characteristic 2 Let k be any finite extension of $\mathbb{F}_2$. In this paragraph, we use the preceding results in order to give equations for an ordinary Kummer variety over k.

By lemma 1, one can associate to any ordinary Kummer surface together with a projective embedding defined over k a point $(a_u) \in \mathcal{M}_\delta$ with homogeneous coordinates in $W(k)$. Denote by $\mathscr{K}$ the fraction field of $W(k)$.

Let $(a_u) \in \mathcal{M}_\delta$ be a point with homogeneous coordinates $W(k)$ representing the generic fiber of an element of $\mathscr{A}^c_\delta$. We begin by renaming $a_u = a_{ij}$ in order to use the same notations as [Gau07]. Let $a = a_{00}$, $b = a_{10}$, $c = a_{01}$, $d = a_{11}$ and set

$$\begin{aligned}
4A' &= a^2 + b^2 + c^2 + d^2,\\
4B' &= a^2 + b^2 - c^2 - d^2,\\
4C' &= a^2 - b^2 + c^2 - d^2,\\
4D' &= a^2 - b^2 - c^2 + d^2.
\end{aligned}$$

Moreover we put

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

By [BL04] pp. 204, we can associate to a point $(a : b : c : d) \in \mathcal{M}_\delta \subset \mathbb{P}^3_{\mathbb{Q}_2}$ with $a, b, c, d \in W(k)$, a Kummer surface $K_{(a:b:c:d)}$ over $\mathscr{K}$ defined by the equation

$$\begin{aligned}
\Delta(x^4 + y^4 + z^4 + t^4) + 2Exyzt - F(x^2t^2 + y^2z^2)&\\
- G(x^2z^2 + y^2t^2) - H(x^2y^2 + z^2t^2) &= 0. \qquad (5)
\end{aligned}$$

In this equation, the letters (x, y, z, t) represent the canonical basis of global sections of the line bundle $\mathscr{L}^c_{\mathscr{K}}$ provided by the theta structure Θ^c_δ.

Because, as seen in the previous paragraph, the point $(a : b : c : d) \mod 2 = (1 : 0 : 0 : 0)$, the equation (5) has bad reduction modulo 2. In order to obtain a model with good reduction, we consider the blowing-up of the origin point of the special fiber. This corresponds to the following change of variables:

$$X = 2.x, Y = 2.y, Z = 2.z, T = 2.t. \qquad (6)$$

Let $a' = a = 1 \mod 2, b' = (1/2)b \mod 2, c' = (1/2)c \mod 2, d' = (1/2)d \mod 2$. Taking care of the change of variable (6), we obtain the following equation for the special fiber $K_{(1:b':c':d')}$ of $K_{(a:b:c:d)}$

$$\begin{aligned}
b'c'd'XYZT + c'^2b'^2(X^2T^2 + Y^2Z^2)&\\
+ b'^2d'^2(X^2Z^2 + Y^2T^2) + c'^2d'^2(X^2Y^2 + T^2Z^2) &= 0. \qquad (7)
\end{aligned}$$

An easy computation shows that if $b'c'd' \neq 0$, the set of points with homogeneous coordinates $P_{sing} = \{(1 : 0 : 0 : 0), (0 : 1 : 0 : 0), (0 : 0 : 1 : 0), (0 : 0 : 0 : 1)\}$ is exactly in the singular locus of $K_{(1:b':c':d')}$. In the case that $b'c'd' = 0$, $K_{(1:b':c':d')}$ is not reduced and as a consequence is not a Kummer surface.

Suppose that $(A^c_{W(k)}, \mathscr{L}^c_{W(k)}, \Theta^c_\delta)$ is represented by $(a : b : c : d) \in \mathbb{P}^3_{\mathbb{Q}_2}$. We keep the same notations as in the preceding paragraph and suppose that x, y, z, t is the basis of global sections of $\mathscr{L}^c_{W(k)}$ defined by Θ^c_δ. We denote by $\mathscr{O}_{A_{W(k)}}(D_+(x))$ the affine coordinate algebra of the open set $D_+(x)$. By definition of a quotient, the elements $(\frac{y}{x}, \frac{z}{x}, \frac{t}{x})$ of $\mathscr{O}_{A_{W(k)}}(D_+(x))$ generate the $W(k)$-subalgebra of sections invariant by the action of the inverse morphism $i_{W(k)}$. As a consequence, modulo p, on $D_+(X)$, the sections $(\frac{Y}{X}, \frac{Z}{X}, \frac{T}{X})$ generate the k-subalgebra of $\mathscr{O}_{A_k}(D_+(X))$ of sections invariant by the action of inverse morphism i_k. As x, y, z, t play the same role in the preceding argument, we deduce that $K_{(1:b':c':d')}$ is the quotient of the special fiber of $A^c_{W(k)}$ be the inverse morphism i_k. As a consequence, if $b'c'd' \neq 0$, $K_{(1:b':c':d')}$ is a Kummer surface over k.

Reciprocally, let $(b', c', d') \in k^3$ be such that $b'c'd' \neq 0$. We want to show that $K_{(1:b':c':d')}$ is indeed a Kummer surface. For this, let $(a, b, c, d) \in W(k)$ be such that

$$1 = a \mod 2, 2b' = b \mod 4, 2c' = c \mod 4 \quad \text{and} \quad 2d' = d \mod 4. \tag{8}$$

As $\mathcal{M}_\delta$ is an open dense sub-variety of $\mathbb{P}^3_{\mathbb{Q}_2}$ and the set verifying conditions (8) is a non empty 2-adic analytic open set, we can moreover suppose that $(a : b : c : d)$ is the homogeneous coordinates of a point representing the generic fiber of a triple $(A_{W(k)}, \mathscr{L}_{W(k)}, \Theta_\delta)$ where $A_{W(k)}$ an abelian surface over $W(k)$, $\mathscr{L}_{W(k)}$ is a totally symmetric line bundle on $A_{W(k)}$ and Θ_δ is a symmetric theta structure of type δ. Let A_k be the special fiber of $A_{W(k)}$. As $K_{(a:b:c:d)}$ is the quotient of $A_{W(k)}$ by the action of the inverse morphism $i_{W(k)}$, on the special fiber, $K_{(1:b':c':d')}$ is the quotient of A_k by the action of i_k.

We have obtained the following proposition (compare with [LP02] Proposition 4.1)

Proposition 2. *Let $\delta = (2, 2)$. There is a bijective correspondence between*

- *the set of triples $(A_k, \mathscr{L}_k, \Theta_\delta)$ where k is any finite extension of $\mathbb{F}_2$, A_k is an ordinary abelian variety over k, $\mathscr{L}_k$ a degree 2 totally symmetric ample line bundle and Θ_δ a theta structure of type δ defined over k,*
- *and the set of triples of elements $(b', c', d') \in k^3$ such that $b'c'd' \neq 0$.*

Let $(b', c', d') \in k^3$, an equation for the Kummer surface $K_{(1:b':c':d')}$ is given by

$$b'c'd'XYZT + c'^2b'^2(X^2T^2 + Y^2Z^2) \\ + b'^2d'^2(X^2Z^2 + Y^2T^2) + c'^2d'^2(X^2Y^2 + T^2Z^2) = 0.$$

3 Pseudo-group law formulas

Let k be a finite extension of $\mathbb{F}_2$ and let $\overline{k}$ be an algebraic closure of k. Let $(b', c', d') \in k^3$ be such that $b'c'd' \neq 0$ and let $K_{(1:b':c':d')}$ be the associated Kummer surface. Let A_k be an abelian variety such that its quotient by the action of the inverse morphism i gives $K_{(1:b':c':d')}$ and denote by $\pi : A_k \to K_{(1:b':c':d')}$

the natural projection. In all this section, if P is a geometric point of A_k, we denote by $\overline{P}$ the point $\pi(P)$. In the same manner, the notation $\overline{P}$ means that $\overline{P}$ is a geometric point of $K_{(1:b':c':d')}$ represented by a point P on A_k.

We give algorithms in order to compute the pseudo-group law on $K_{(1:b':c':d')}$.

Doubling Algorithm: `DoubleKummer(`$\overline{P}$`)`
Input: $\overline{P} = (x : y : z : t)$ a $\overline{k}$-point of $K_{(1:b':c':d')}$;
Output: The double $2\overline{P} = (x' : y' : z' : t')$ in $K_{(1:b':c':d')}(\overline{k})$.

1. $x' = (x^2 + y^2 + z^2 + t^2)^2$;
2. $y' = \frac{1}{b'}(xy + zt)^2$;
3. $z' = \frac{1}{c'}(xz + yt)^2$;
4. $t' = \frac{1}{d'}(xt + yz)^2$;
5. Return $2\overline{P} = (x', y', z', t')$.

Pseudo-addition Algorithm: `PseudoAddKummer(`$\overline{P}$`, `$\overline{Q}$`, `$\overline{R}$`)`
Input: $\overline{P} = (x : y : z : t)$ and $\overline{Q} = (\underline{x} : \underline{y} : \underline{z} : \underline{t})$ two $\overline{k}$-points of $K_{(1:b':c':d')}$ and $\overline{R} = (\bar{x} : \bar{y} : \bar{z} : \bar{t})$ one of the $\pi(P + Q)$ or $\pi(P - Q)$, with $\bar{x}\bar{y}\bar{z}\bar{t} \neq 0$.
Output: The point $(x' : y' : z' : t')$ among $\pi(P + Q)$ or $\pi(P - Q)$ which is different from $\overline{R}$.

1. $x' = (x\underline{x} + y\underline{y} + z\underline{z} + t\underline{t})^2/\bar{x}$;
2. $y' = (x\underline{y} + y\underline{x} + z\underline{t} + t\underline{z})^2/\bar{y}$;
3. $z' = (x\underline{z} + z\underline{x} + y\underline{t} + t\underline{y})^2/\bar{z}$;
4. $t' = (x\underline{t} + t\underline{x} + y\underline{z} + z\underline{y})^2/\bar{t}$;
5. Return $(x', y', z', t') = \pi(P + Q)$ or $\pi(P - Q)$.

As written, doubling requires 6 multiplications, 3 multiplications by constant that depends only on the Kummer surface, and 5 squares. The pseudo-addition requires 16 multiplications, 4 squares and 4 divisions.

This can be reduced, using the fact that in a Montgomery ladder setting, the base point is always the same in the pseudo-addition, so that the 4 divisions can be replaced by 3 multiplications. Additionally, playing Karatsuba-like tricks allows to save multiplications. For the doubling, one can for instance compute the 4 products xt, yz, $(x+y)(z+t)$ and $(x+z)(y+t)$, from which we can deduce $xt+yz$, $xz+yt = (x+y)(z+t)+xt+yz$ and $xy+zt = (x+z)(y+t)+xt+yz$. Thus the cost of doubling is 4 multiplications, 3 multiplications by constants, and 5 squares. Similarly, the pseudo-addition can follow these lines:

$$
\begin{aligned}
L_1 &= x\underline{x} \\
L_2 &= y\underline{y} \\
L_3 &= z\underline{z} \\
L_4 &= t\underline{t} \\
M_1 &= (y + z + t)(\underline{y} + \underline{z} + \underline{t}) \\
M_2 &= (x + y + t)(\underline{x} + \underline{y} + \underline{t}) \\
M_3 &= (x + z + t)(\underline{x} + \underline{z} + \underline{t}) \\
N &= (x + y + z + t)(\underline{x} + \underline{y} + \underline{z} + \underline{t})
\end{aligned}
$$

Then $L_1 + L_2 + L_3 + L_4$, $L_3 + L_4 + M_1 + M_3 + N$, $L_2 + L_4 + M_1 + M_2 + N$, $L_1 + L_4 + M_2 + M_3 + N$ give the required data for the pseudo-addition. Therefore, the pseudo-addition costs 11 multiplications and 4 squares. Finally, in a Montgomery ladder, one does one doubling and one pseudo-addition per bit of the scalar multiplier, and we obtain the following result:

Theorem 1. *Multiplying by a scalar a point on a Kummer surface with non-zero coordinates costs* 9 *squares,* 15 *general multiplications and* 3 *multiplications by constants that depend only on the Kummer surface, per bit of the scalar.*

4 Proof of the pseudo-group law

In this section, we prove the formulas described in section 3.

Let k be a finite field of characteristic 2, $\delta = (2, 2)$ and as in section 2 we consider a triple $(A_k, \mathscr{L}_k, \Theta_\delta)$ where A_k is an ordinary abelian surface over k, $\mathscr{L}_k$ is a degree 2 totally symmetric ample line bundle over A_k and Θ_δ is a theta structure of type δ. Let $(A^c_{W(k)}, \mathscr{L}^c_{W(k)}, \Theta^c_\delta)$ be deduced from $(A_k, \mathscr{L}_k, \Theta_\delta)$ as in lemma 2. We recall that $\mathscr{L}^c_{W(k)}$ lifts $\mathscr{L}_k$ and that Θ^c_δ is the canonical theta structure defined by the group isomorphism

$$\phi_1 : Z(\delta)_{W(k)} \xrightarrow{\sim} A[2]^{\mathrm{et}}_{W(k)}$$

deduced from Θ_δ.

We consider also $(A^c_{W(k)}, \mathscr{L}^{c2}_{W(k)}, \Theta^c_{2\delta})$ where $\mathscr{L}^{c2}_{W(k)}$ is the square $\mathscr{L}^c_{W(k)}$ and $\Theta^c_{2\delta}$ is the canonical theta structure for $\mathscr{L}^{c2}_{W(k)}$ defined by a choice of a group isomorphism

$$\phi_2 : Z(2\delta)_{W(k)} \xrightarrow{\sim} A[4]^{\mathrm{et}}_{W(k)}$$

We suppose that ϕ_2 is chosen such that the following diagram is commutative

$$\begin{tikzcd} Z(\delta)_{W(k)} \arrow[r, "\phi_1"] \arrow[d, "\nu"] & A[2]^{\mathrm{et}}_{W(k)} \arrow[d, "\mu"] \\ Z(2\delta)_{W(k)} \arrow[r, "\phi_2"] & A[4]^{\mathrm{et}}_{W(k)} \end{tikzcd} \tag{9}$$

where $\mu : A_{W(k)}[2]^{\mathrm{et}} \to A[4]^{\mathrm{et}}_{W(k)}$ is the natural inclusion and $\nu : Z(\delta)_{W(k)} \to Z(2\delta)_{W(k)}$ is deduced from the natural morphism $(\mathbb{Z}/2\mathbb{Z})^2 \to (\mathbb{Z}/4\mathbb{Z})^2$, $x \mapsto 2x$.

Let $(\vartheta_i^{\Theta^c_\delta})_{i\in Z(\delta)_{W(k)}}$ and $(\vartheta_i^{\Theta^c_{2\delta}})_{i\in Z(2\delta)_{W(k)}}$ be respectively the basis of the global sections of $\mathscr{L}^c_{W(k)}$ and $\mathscr{L}^{c2}_{W(k)}$ defined by Θ^c_δ and $\Theta^c_{2\delta}$. By [Car07], Θ^c_δ and $\Theta^c_{2\delta}$ are 2-compatible and we have for all $i \in Z(\delta)_{W(k)}$,

$$(\vartheta_i^{\Theta^c_\delta})^2_k = (\vartheta_{\nu(i)}^{\Theta^c_{2\delta}})_k. \tag{10}$$

It should be remarked that as Θ^c_δ and $\Theta^c_{2\delta}$ are 2-compatible, by [Mum83] p. 317, they are symmetric.

Let $\mathscr{K}$ be the fraction field of $W(k)$ and let $\overline{\mathscr{K}}$ be an algebraic closure of $\mathscr{K}$. From here we fix an embedding $\psi : \overline{\mathscr{K}} \to \mathbb{C}$. The generic fiber $A_{\mathscr{K}}$ of $A_{W(k)}$ can be viewed as a complex abelian variety $A_{\mathbb{C}} = A_{\mathscr{K}} \times_{\psi} Spec(\mathbb{C})$ with a polarization $\mathscr{L}^c_{\mathbb{C}}$ defined by $\mathscr{L}^c_{\mathbb{C}} = \mathscr{L}^c_{W(k)} \otimes_{W(k)} \mathbb{C}$. We remark that $K(\mathscr{L}^c_{\mathbb{C}})$ comes with a decomposition inherited from the theta structure Θ^c_{δ}. From this decomposition, we deduce a period matrix $(I\Omega)$ with I the 2 dimensional unity matrix and Ω an element of $\mathbb{H}_2$ the 2 dimensional Siegel upper half space. Denote by Λ_{Ω} the lattice $\mathbb{Z}^2 + \Omega\mathbb{Z}^2$ of $\mathbb{C}^2$ and let $A_{an} = \mathbb{C}^2/\Lambda_{\Omega}$ so that we have an analytic isomorphism $j_{an} : A_{\mathbb{C}} \to A_{an}$. Let $p : \mathbb{C}^2 \to \mathbb{C}^2/\Lambda_{\Omega}$ be the canonical projection.

We can suppose that Ω is chosen such that the subgroup of $A_{an}[2]$ given by $p((1/2)\mathbb{Z}^2)$ correspond via j_{an}^{-1} to the maximal étale part of $A_{\mathscr{K}}[2]$, where $A_{\mathscr{K}}$ is identified to $A_{\mathbb{C}}$ via ψ.

Let $\mathscr{L}_0$ be the square of the degree 1 line bundle on A_{an} defined by Ω and the characteristic 0 with respect to the decomposition defined by Ω following [BL04] Lemma 3.1.2. Let $\Theta_{0,\delta}$ be the theta structure for $\mathscr{L}_0$ of type δ associated to the characteristic 0 ([BL04] Lemma 6.6.5). In the same way, let $\mathscr{L}_0^2$ be the square of $\mathscr{L}_0$ and $\Theta_{0,2\delta}$ be its associated characteristic 0 theta structure.

For $a, b, \ell \in \mathbb{Z}$, we define the theta function with rational characteristics as

$$\vartheta_{\ell}\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z,\Omega) = \sum_{n\in\mathbb{Z}^2} \exp\Big[\pi i^t(n+\frac{a}{\ell})\Omega(n+\frac{a}{\ell}) + 2\pi i^t(n+\frac{a}{\ell}).(z+\frac{b}{\ell})\Big]. \quad (11)$$

It is well known that the pull back of the global sections of $\mathscr{L}_0$ and $\mathscr{L}_0^2$ on the universal covering of $A_{\mathbb{C}}$ can be represented up to a constant multiplicative factor by theta functions with rational characteristics. More precisely by this correspondence for all $i \in Z(\delta)$, $\vartheta_i^{\Theta_{0,\delta}}$ is represented by $\vartheta_2\left[\begin{smallmatrix} 0 \\ i \end{smallmatrix}\right](z, 1/2\Omega)$ and for all $i \in Z(2\delta)$, $\vartheta_i^{\Theta_{0,2\delta}}$ is represented by $\vartheta_4\left[\begin{smallmatrix} 0 \\ i \end{smallmatrix}\right](z, 1/4\Omega)$ (see for instance [Mum83] Proposition 1.3 p.124).

We recall the Riemann duplication formulas [Igu72]. For all $z \in \mathbb{C}$, $\epsilon \in \mathbb{Z}$ and $\Omega \in \mathbb{H}_2$, we have

$$\vartheta_2\left[\begin{smallmatrix} 0 \\ \epsilon \end{smallmatrix}\right](2z, 1/2\Omega)\vartheta_2\left[\begin{smallmatrix} 0 \\ \epsilon \end{smallmatrix}\right](0, 1/2\Omega) = \frac{1}{4}\sum_{e\in(\mathbb{Z}/2\mathbb{Z})^2} \vartheta_2\left[\begin{smallmatrix} 0 \\ \epsilon+e \end{smallmatrix}\right](z, 1/4\Omega)\vartheta_2\left[\begin{smallmatrix} 0 \\ e \end{smallmatrix}\right](z, 1/4\Omega). \quad (12)$$

As Θ^c_{δ} and $\Theta^c_{2\delta}$ are symmetric and 2-compatible, by [BL04] Proposition 6.9.4 there exists an element $d \in A_{W(k)}[2]$ such that for all $i \in Z(\delta)$, $\vartheta_{i+d}^{\Theta^c_{\delta}} = \vartheta_i^{\Theta_{0,\delta}}$ and for all $i \in Z(2\delta)$, $\vartheta_{i+d}^{\Theta^c_{2\delta}} = \vartheta_i^{\Theta_{0,2\delta}}$. Here, $Z(\delta)$ is identified as a sub-group of $Z(2\delta)$ with ν (see (9)).

Starting from a closed point x' on A_k which is not in $A_k[2]$. We can lift it to a point x of $A_{\mathscr{K}}$. On $A_{\mathscr{K}}$, formula (12) tells us that there exists $\omega \in \overline{W(k)}$ such that for all $i \in Z(\delta)$,

$$\vartheta_i^{\Theta^c_{\delta}}(2x)\vartheta_i^{\Theta^c_{\delta}}(0) = \frac{1}{4}\omega\sum_{e\in Z(\delta)} \vartheta_{\nu(i+e)}^{\Theta^c_{2\delta}}(x)\vartheta_{\nu(e)}^{\Theta^c_{2\delta}}(x) \quad (13)$$

Applying lemma 3 we obtain that there exists $(a_i) \in W(k)^{Z(\delta)}$ and $\zeta \in \overline{\mathscr{K}}$, such that for all $i \in Z(\delta)$, a_i is an invertible element of $W(k)$, with $\vartheta_0^{\Theta_\delta^c}(0) = \zeta a_0$ and for $i \neq 0$, $\vartheta_i^{\Theta_\delta^c}(0) = 2\zeta a_i$.

For $i \in Z(\delta)$, denote by $Z(\delta)_i$ a set of representatives of the elements of $Z(\delta)$ quotiented by the subgroup of $Z(\delta)$ generated by i. We remark that $Z(\delta)_0$ has the same cardinality as $Z(\delta)$. Equation (13) becomes

$$\vartheta_i^{\Theta_\delta^c}(2x) = \frac{\omega}{4\zeta a_i} \sum_{e \in Z(\delta)_i} \vartheta_{\nu(i+e)}^{\Theta_{2\delta}^c}(x) \vartheta_{\nu(e)}^{\Theta_{2\delta}^c}(x) \tag{14}$$

As the point defined by $(\vartheta_i^{\Theta_\delta^c}(2x))_{i \in Z(\delta)}$ is defined up to a constant factor, we can suppose that $\omega/(4\zeta)$ is a unit of $\overline{W(k)}$. Now, reducing modulo 2 and applying (10) we obtain

$$(\vartheta_i^{\Theta_\delta^c}(2x'))_k = \omega' \frac{1}{a_i'} \sum_{e \in Z(\delta)_i} (\vartheta_{\nu(i+e)}^{\Theta_\delta^c}(x'))_k^2 (\vartheta_{\nu(e)}^{\Theta_\delta^c}(x'))_k^2 \tag{15}$$

where $a_i' = a_i \mod 2$ and $\omega' = \omega/(4\zeta) \mod 2$. This is exactly the duplication formula. The pseudo addition formula can be proved in the same way.

5 Link to Rosenhain form and Mumford representation

It is interesting to have explicit formulas relying points on the Kummer surface to the classical Mumford representation of a divisor on the Jacobian of a genus 2 curve (see for instance [CF05, Chapter 14] for a description of these coordinates). They can be obtained as before, by lifting to the 2-adics, applying the formulas in [Gau07], making the appropriate coordinate change to have good reduction, so to get the formulas modulo 2. We skip the details and give the resulting formulas without further proof.

Let k be a finite field of characteristic 2, let $(b', c', d') \in k^3$ be such that $b'c'd' \neq 0$ and let $K_{(1:b':c':d')}$ be the associated Kummer surface. Let $\mathcal{C}$ be a curve such that the Jacobian of $\mathcal{C}$ is k-isomorphic to the abelian variety associated to $K_{(1:b':c':d')}$. An equation for $\mathcal{C}$ can be taken as follows:

$$\mathcal{C} : y^2 + x(x+1)y = x(x+1)(f_3x^3 + f_2x^2 + f_1x + f_0),$$

where

$$f_0 = \frac{b'^2c'^2}{d'^2}, \quad f_1 = f_0 + \frac{c'^2d'^2}{b'^2}, \quad f_2 = f_3 = \frac{b'^2d'^2}{c'^2}.$$

Now, if $\overline{P} = (x : y : z : t)$ is a point on $K_{(1:b':c':d')}$, it can be mapped to an element of the Jacobian of $\mathcal{C}$ in Mumford representation. We give only the generic case, where $z \neq 0$ and the resulting divisor is of weight 2, that is the Mumford representation is of the form $\langle X^2 + u_1X + u_0, v_1X + v_0\rangle$. We have:

$$u_0 = \frac{c'^2t^2}{d'^2z^2}, \qquad u_1 = 1 + \frac{c'^2y^2}{b'^2z^2} + \frac{c'^2t^2}{d'^2z^2}.$$

As for v_0 and v_1 they are not always defined over k, since the divisor could be defined on the Jacobian of the quadratic twist of $\mathcal{C}$, and also, the element associated to $\overline{P}$ is defined only up to plus or minus 1. In Mumford representation, with the form of equation we consider, two opposite elements have the same u_0 and u_1, and their v_0 values sum up to u_0. Let us denote them v_0 and v_0^-, so that $v_0 + v_0^- = u_0$. An easy, but tedious, computation shows that the product $v_0 v_0^-$ corresponding to the divisor associated to $\overline{P}$ is

$$v_0 v_0^- = \frac{c'^4 t^2}{d'^4 z^6} \left(b'^2 (t^4 + z^4) + d'^2 (x^2 z^2 + y^2 t^2) \right).$$

Knowing the sum and the product of v_0 and v_0^-, it is possible to get their value by solving a degree 2 equation. If the roots are in an extension of degree 2, it means that $\overline{P}$ maps to a point of the Jacobian of the quadratic twist of $\mathcal{C}$.

Once a choice has been made for v_0 (which corresponds to choose a sign for the element in the Jacobian), the value of v_1 is completely determined by the fact the Mumford representation should fit into the equation of the curve. This gives:

$$v_1 = f_1 + f_2 + f_3(u_0 + u_1^2) + u_1(f_2 + f_3) + \frac{f_0 + v_0}{u_0} + \frac{u_1 v_0^2}{u_0^2}.$$

Hence after precomputing a few constants that depend only on the surface, mapping a point on the Kummer surface to a corresponding divisor in Mumford representation costs about a dozen of multiplies, 2 inversions, and one resolution of an equation of degree 2 (plus additions and squares).

6 The case of genus 1

All dimension one Kummer varieties over k are isomorphic as algebraic varieties to $\mathbb{P}^1_k$. Only the pseudo-group law differs between a Kummer line and another one. In this section, we give algorithms to compute the pseudo-group law. We distinguish the case of even and odd characteristic.

6.1 The case of even characteristic.

Let k be a finite extension of $\mathbb{F}_2$. The results of section 2 carry over in dimension one. In particular, the set of ordinary Kummer lines over k is parametrized by the k-points of $\mathbb{A}^1_k$. Let $b' \in k$ and $K_{(1:b')}$ be the associated Kummer variety. We keep the same conventions as in section 3: let E_k be the elliptic curve such that its quotient by the inverse morphism i_k gives $K_{(1:b')}$. Denote by $\pi : E_k \to K_{(1:b')}$ the natural projection. The notation $\overline{P}$ means that $\overline{P}$ is a geometric point of $K_{(1:b')}$ represented by a point P of E_k.

Doubling Algorithm: `DoubleKummer(`$\overline{P}$`)`
Input: A point $\overline{P} = (x : y)$ in $K_{(1:b')}(\overline{k})$;
Output: The double $2\overline{P} = (x' : y')$ in $K_{(1:b')}(\overline{k})$.

1. $x' = (x^2 + y^2)^2$;
2. $y' = \frac{1}{b'}(xy)^2$;
3. Return $2\overline{P} = (x' : y')$.

Pseudo-addition Algorithm: `PseudoAddKummer(`$\overline{P}$`,` $\overline{Q}$`,` $\overline{R}$`)`
Input: $\overline{P} = (x : y)$ and $\overline{Q} = (\underline{x} : \underline{y})$ on $K_{(1:b')}$ and $\overline{R} = (\bar{x}, \bar{y})$ one of the $\pi(P+Q)$ and $\pi(P - Q)$, with $\bar{x}\bar{y} \neq 0$.
Output: The point $(x' : y')$ among $\pi(P + Q)$ and $\pi(P - Q)$ which is different from $\overline{R}$.

1. $x' = (x\underline{x} + y\underline{y})^2/\bar{x}$;
2. $y' = (x\underline{y} + y\underline{x})^2/\bar{y}$;
3. Return $(x', y') = \pi(P + Q)$ or $\pi(P - Q)$.

In this formulas, we recognize the variant of Lopez-Dahab formulas given by Stam in [Sta03].

6.2 The case of odd characteristic.

In this section, let p be an odd prime number and k a finite extension of $\mathbb{F}_p$. In this case, since everything has good reduction, we can use the Lefschetz principle to carry over all the known results over $\mathbb{C}$. This gives us that the set of Kummer varieties defined over k is parametrized by the k-points of $\mathbb{P}^1_k$. Let $(a : b)$ be the homogeneous coordinate of a k-point of $\mathbb{P}^1_{\mathbb{F}_p}$ which defines a Kummer line $K_{(a:b)}$. As a algebraic variety, $K_{(a:b)}$ is isomorphic to $\mathbb{P}^1_k$. We keep the same notations as the preceding section for E_k, π, P and $\overline{P}$. Let $A' = (a^2 + b^2)/2$ and $B' = (a^2 - b^2)/2$. The pseudo-group law is given by the following algorithms.

Doubling Algorithm: `Double(`$\overline{P}$`)`
Input: A point $\overline{P} = (x : y)$ in $K_{(a:b)}(\overline{k})$.
Output: The double $2\overline{P} = (x' : y')$.

1. $x_0 = (x^2 + y^2)$;
2. $y_0 = \frac{A'}{B'}(x^2 - y^2)$;
3. $x' = (x_0 + y_0)$;
4. $y' = \frac{a}{b}(x_0 - y_0)$;
5. Return $(x' : y')$.

Pseudo-addition Algorithm: `PseudoAdd(`$\overline{P}$`,` $\overline{Q}$`,` $\overline{R}$`)`
Input: Two points $\overline{P} = (x : y)$ and $\overline{Q} = (\underline{x} : \underline{y})$ on $K_{(a:b)}$, and $\overline{R} = (\bar{x} : \bar{y})$ one of the $\pi(\overline{P} + \overline{Q})$ or $\pi(\overline{P} - \overline{Q})$, with $\bar{x}\bar{y} \neq 0$.
Output: The point $(x' : y')$ among $\pi(\overline{P} + \overline{Q})$ and $\pi(\overline{P} - \overline{Q})$ which is different from $\overline{R}$.

1. $x_0 = (x^2 + y^2)(\underline{x}^2 + \underline{y}^2)$;
2. $y_0 = \frac{A'}{B'}(x^2 - y^2)(\underline{x}^2 - \underline{y}^2)$;
3. $X = (x_0 + y_0)/\bar{x}$;

4. $Y = (x_0 - y_0)/\bar{y}$;
5. Return $(x' : y')$.

Again these formulas are directly translated form the classical complex analytic theory of theta functions. Let $E_{\mathbb{C}}$ be a complex analytic elliptic curve defined by $\tau \in \mathbb{C}$ such that $\mathrm{Im}(\tau) > 0$. Keeping the definition (11) for the theta functions with rational characteristics, let us give names to some theta constants:

$$a = \vartheta_2 \left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](0, \tau), \quad b = \vartheta_2 \left[\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right](0, \tau), \quad A = \vartheta_2 \left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](0, 2\tau), \quad B = \vartheta_2 \left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right](0, 2\tau).$$

The duplication formulas for theta functions gives $2A^2 = a^2 + b^2$ and $2B^2 = a^2 - b^2$.

The pseudo-group law comes from classical duplication formulas for theta functions. For instance the doubling algorithm follows from the equalities:

$$\begin{cases} a\vartheta_2 \left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](\mathbf{z}, \tau) = \vartheta_2 \left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](\mathbf{z}, 2\tau)^2 + \vartheta_2 \left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right](\mathbf{z}, 2\tau)^2 \\ b\vartheta_2 \left[\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right](\mathbf{z}, \tau) = \vartheta_2 \left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](\mathbf{z}, 2\tau)^2 - \vartheta_2 \left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right](\mathbf{z}, 2\tau)^2 \end{cases}$$

$$\begin{cases} 2A\vartheta_2 \left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](2\mathbf{z}, 2\tau) = \vartheta_2 \left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](\mathbf{z}, \tau)^2 + \vartheta_2 \left[\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right](\mathbf{z}, \tau)^2 \\ 2B\vartheta_2 \left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right](2\mathbf{z}, 2\tau) = \vartheta_2 \left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](\mathbf{z}, \tau)^2 - \vartheta_2 \left[\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right](\mathbf{z}, \tau)^2 \end{cases}$$

In both the doubling and the pseudo-addition algorithms, the formulas start by squaring the coordinates of the input points. Therefore, it makes sense to manipulate the squares of the coordinates, in order to easily share the computation of these squares.

Just like with the Montgomery form, it is possible to design addition chains that allow to multiply a point on the Kummer-line by a scalar. The binary ladder yields the following operation count for such a scalar multiplication.

Theorem 2. *Multiplying by a scalar a point on a Kummer-line with non-zero coordinates costs* 6 *squares,* 3 *general multiplications and* 3 *multiplications by constants that depend only on the Kummer-line, per bit of the scalar.*

Link with a Weierstraß equation. Put $\lambda = \frac{a^4}{a^4 - b^4}$ and let E_λ be the curve of equation

$$E_\lambda \ : \ Y^2 = X(X-1)(X-\lambda).$$

Then, there is a map from the Kummer-line to $E_\lambda/\{\pm 1\}$ given by

$$(x, y) \mapsto \left(\frac{a^2 x}{a^2 x - b^2 y}, \ \ldots \right),$$

where the dots on the right-hand side are determined up to sign by the equation of E_λ. It is then straightforward to check that the doubling and the pseudo-addition algorithms are compatible with the group law on E_λ.

Comparison with the classical Montgomery form. The Kummer-line behaves very similarly to the classical Montgomery form. Here are the differences and similarities:

– With the Kummer line, in the cost per bit of a scalar multiplication, one general multiplication is replaced by a (supposedly) cheaper squaring, but there are 2 more multiplications by constants that depend only on the Kummer-line.
– When working over a prime finite field with p elements, the group order of the corresponding E_λ is divisible by 4, and so does the group order of its twist. In the case where $p \equiv 1 \mod 4$, the orders of the curve and its twists are divisible by 4 and 8, whereas in the case of $p \equiv 3 \mod 4$, the orders are divisible by 8 and 16.

These formulas could be of interest in cases where a square is much cheaper than a multiplication and constants are tiny. In the case of looking for factors of very large Mersenne-like integers using the ECM methods, this could yield some speed-up compared to the traditional use of the Montgomery form.

7 Cryptographical computer experiments

We summarize the costs of the different theta-based formulas in genus 1 and 2, in odd and even characteristics. In this table, M is for a general multiplication, S is for a square, and D is for a multiplication by a constant that depends only on the curve or the surface, and therefore can sometimes be made small. In these estimates, we assume that a binary ladder is used, so that the divisions occurring in the pseudo-addition are by elements that are constant all along the scalar multiplication, and are therefore replaced by multiplications, one of them being trivial.

Cost per bit of scalar multiplication	
Elliptic, odd characteristic	3 M + 6 S + 3 D
Elliptic, even characteristic	5 M + 5 S + 1 D
Genus 2, odd characteristic	7 M + 12 S + 9 D
Genus 2, even characteristic	15 M + 9 S + 3 D

These formulas have been implemented using the mp$\mathbb{F}_q$ library [GT07], yielding the running times given in the table below. The test platforms are a 2.4 Ghz AMD Opteron 250 and a 2.66 Ghz Intel Core2 Duo E6700, both running a Linux system in 64-bit mode. `curve25519` is the cryptosystem described in [Ber06] and is based on an elliptic curve in Montgomery form over a prime field with 255 bits. `surf127eps` is based on a Kummer surface with complex multiplication over a prime field with 127 bits. `curve2251` is based on an elliptic curve defined over $\mathbb{F}_{2^{251}}$, and `surf2113` is based on a Kummer surface defined over $\mathbb{F}_{2^{113}}$.

In the case of genus 1, and odd characteristic, we have used `curve25519` which is based on the Montgomery form instead of the formulas presented in this paper, since the gain of having one square instead of one multiplication does not compensate the additional multiplications by small constants. The other formulas are theta-based formulas.

The `surf127eps` system is based on a CM curve, since point counting in genus 2 is still problematic for these sizes. As a consequence, the coefficients depending on the surface in the formulas are random-looking elements, and multiplying by them is no cheaper than a generic multiplication.

Time in CPU cycle for a scalar multiplication				
	`curve25519`	`surf127eps`	`curve2251`	`surf2113`
Opteron K8	310,000	296,000	1,400,000	1,200,000
Core2	386,000	405,000	888,000	687,000

Conclusion

Genus 3 and 4 are of course amenable to similar study, but due to progresses in the discrete logarithm computations, it looks wise to stick to genus 1 and 2 for cryptographic applications.

On the theoretical side, a quartic equation for a non ordinary Kummer surface is given in [LP04]. But the question of the pseudo-addition formulas on such non ordinary Kummer surfaces is still open. When using Mumford's coordinates and Cantor-based formulas, the group law can be more efficient in the non-ordinary case, so this is worth being investigated.

Acknowledgments. We express our gratitude to Robert Carls for his very helpful comments on earlier drafts of this paper.

References

[Ber06] D. Bernstein. Curve25519: new diffie-hellman speed records. In M. Yung, Y. Dodis, A. Kiayias, and T. Malkin, editors, *PKC 2006*, volume 3958 of *Lecture Notes in Comput. Sci.*, pages 207–228. Springer-Verlag, 2006.

[BL04] C. Birkenhake and H. Lange. *Complex abelian varieties*, volume 302 of *Grundlehren der Mathematischen Wissenschaften [Fundament al Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2004.

[BL07] D. Bernstein and T. Lange. Faster addition and doubling on elliptic curves. In K. Kurosawa, editor, *ASIACRYPT 2007*, volume 4833 of *Lecture Notes in Comput. Sci.*, pages 29–50. Springer-Verlag, 2007.

[Car05] R. Carls. Theta null points of 2-adic canonical lifts. A preprint is available at `http://arxiv.org/math.NT/0509092`, 2005.

[Car07] R. Carls. Canonical coordinates on the canonical lift. *J. Ramanujan Math. Soc.*, 22(1):1–14, 2007.

[CC86] D. V. Chudnovsky and G. V. Chudnovsky. Sequences of numbers generated by addition in formal groups and new primality and factorization tests. *Adv. in Appl. Math.*, 7:385–434, 1986.

[CF05] H. Cohen and G. Frey, editors. *Handbook of elliptic and hyperelliptic curve cryptography.* Chapman & Hall / CRC, 2005.

[Gau00] P. Gaudry. *Algorithmique des courbes hyperelliptiques et applications à la cryptologie*. PhD thesis, École Polytechnique, 2000.

[Gau07] P. Gaudry. Fast genus 2 arithmetic based on Theta functions. *J. of Mathematical Cryptology*, 1:243–265, 2007.

[GT07] P. Gaudry and E. Thomé. The mpFq library and implementing curve-based key exchanges. In *SPEED: Software Performance Enhancement for Encryption and Decryption*, pages 49–64, 2007.

[Igu72] Jun-ichi Igusa. *Theta functions*. Springer-Verlag, New York, 1972. Die Grundlehren der mathematischen Wissenschaften, Band 194.

[LP02] Y. Laszlo and C. Pauly. The action of the Frobenius maps on rank 2 vector bundles in characteristic 2. *J. Algebraic Geom.*, 11(2):219–243, 2002.

[LP04] Y. Laszlo and C. Pauly. The Frobenius map, rank 2 vector bundles and Kummer's quartic surface in characteristic 2 and 3. *Adv. Math.*, 185(2):246–269, 2004.

[MB85] L. Moret-Bailly. Pinceaux de variétés abéliennes. *Astérisque*, 129:266, 1985.

[Mum66] D. Mumford. On the equations defining abelian varieties. I. *Invent. Math.*, 1:287–354, 1966.

[Mum67] D. Mumford. On the equations defining abelian varieties. II. *Invent. Math.*, 3:75–135, 1967.

[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.

[Mum83] D. Mumford. *Tata lectures on theta I*, volume 28 of *Progress in Mathematics*. Birkhäuser Boston Inc., Boston, MA, 1983. With the assistance of C. Musili, M. Nori, E. Previato and M. Stillman.

[Mum84] D. Mumford. *Tata lectures on theta II*, volume 43 of *Progress in Mathematics*. Birkhäuser Boston Inc., Boston, MA, 1984. Jacobian theta functions and differential equations, With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman and H. Umemura.

[Sta03] M. Stam. On Montgomery-like representations for elliptic curves over $GF(2^k)$. In Y. Desmedt, editor, *PKC 2003*, volume 2567 of *Lecture Notes in Comput. Sci.*, pages 240–254. Springer-Verlag, 2003.