Efficient pairing computation with theta functions

David Lubicz, Damien Robert

Efficient Pairing Computation With Theta Functions

David Lubicz[1,2], Damien Robert[3]

[1] DGA-MI, BP 7419, F-35174 Bruz
[2] IRMAR, Universté de Rennes 1, Campus de Beaulieu, F-35042 Rennes
[3] LORIA, CARAMEL Project
Campus Scientifique
BP 239
54506 Vandoeuvre-lès-Nancy Cedex

Abstract. In this paper, we present a new approach based on theta functions to compute Weil and Tate pairings. A benefit of our method, which does not rely on the classical Miller's algorithm, is its generality since it extends to all abelian varieties the classical Weil and Tate pairing formulas. In the case of dimension 1 and 2 abelian varieties our algorithms lead to implementations which are efficient and naturally deterministic. We also introduce symmetric Weil and Tate pairings on Kummer varieties and explain how to compute them efficiently. We exhibit a nice algorithmic compatibility between some algebraic groups quotiented by the action of the automorphism -1, where the $\mathbb{Z}$-action can be computed efficiently with a Montgomery ladder type algorithm.

1 Introduction

In recent years, many new and interesting cryptographic protocols have been proposed which use the existence of pairings on abelian varieties. In order to obtain efficient and secure implementations of these protocols it is important to be able to compute quickly these pairings. Miller has proposed a method (see for instance [2]) to compute the function on an algebraic curve given up to a constant factor by the data of a principal divisor. This method is a key ingredient of all known algorithms to compute pairings. In this paper, we propose a different approach based on theta functions. We first make explicit the link between Weil and Tate pairings and the intersection pairing on the degree 1 homology of an abelian variety. Our method appears to be a very natural and straightforward way to compute the pairing associated to the Riemann form (or its arithmetic counterpart the commutator pairing) of an abelian variety. It is then easy to deduce practical formulas to compute Weil and Tate pairings. A first benefit of our approach is its generality: where Miller's algorithm rely on the representation of an abelian variety as the Jacobian of an algebraic curve, our method works with any abelian varieties. The case of the Tate pairing is noticeable: while the original definition of Tate [8] deals with any abelian varieties, the formula of

Lichtenbaum [9] used in cryptographic applications is restricted to Jacobian of curves. This restriction does not appear in our formulas. Our algorithm also expand the algorithmic toolbox based on theta functions to compute with abelian varieties.

For the complexity analysis of our algorithm we focus on the case of level 2 and 4 theta functions in order to obtain the best running time and memory consumption. The only difference between the two cases lies in the initialisation phase of the algorithm: in level 4 one can recover enough information from the data of two points to compute the pairings. This is not possible with the level 2 embedding since it does not distinguish a point and its opposite. Nonetheless it is possible to define a "symmetric pairing" on the quotient of an abelian variety by the action of the automorphism -1. These notions extend the definition of the trace pairing proposed in [3].

We have chosen to present all the formulas of this paper using the classical analytic theory of theta functions. In order to consider also rationality problems which are essential to the definition of the Tate pairing, we make the assumption that all the abelian varieties that we consider are defined over a number field K and we suppose given a fixed embedding of K in its algebraic closure $\mathbb{C}$. Nonetheless, it should be understood that all our algorithms apply to the case of abelian varieties defined over any field of characteristic not equal to 2. To see this one can invoke the Lefschetz's principle or use Mumford's theory of algebraic theta functions. We refer to [10] for proofs of the main formulas of this paper in the theory of Mumford.

Our paper in organized as follows: in Section 2 we recall some basic definitions about theta functions. The Section 3 we give a method to compute the usual pairings by using a double and add algorithm based a theta addition formula. In Section 5 we make a precise assessment about the complexity of our algorithm. We also introduce symmetric pairings on Kummer varieties and explain how to adapt our algorithms to compute them efficiently. We end the paper with an example of computation in Section 6.

2 Some notations and basic facts

In this section, in order to fix the notations, we recall some well known facts on analytic theta functions (see for instance [14,6]). Let $\mathbb{H}_g$ be the g dimensional Siegel upper-half space which is the set of $g \times g$ symmetric matrices Ω whose imaginary part is positive definite. For $\Omega \in \mathbb{H}_g$, we denote by $\Lambda_\Omega = \Omega\mathbb{Z}^g + \mathbb{Z}^g$ the lattice of $\mathbb{C}^g$ defined by Ω. If A is an abelian variety of dimension g over the number field K with a principal polarisation then A is analytically isomorphic to $\mathbb{C}^g/\Lambda_\Omega$ for a certain $\Omega \in \mathbb{H}_g$. In the rest of this paper, we denote by $\pi : \mathbb{C}^g \to \mathbb{C}^g/\Lambda_\Omega = A$ the canonical projection. The classical theory of theta functions gives a lot of functions on $\mathbb{C}^g$ that are pseudo-periodic with respect to Λ_Ω and can be used as a projective coordinate system for A. More precisely, for $a, b \in \mathbb{Q}^g$, the theta function with rational characteristics (a, b) is an analytic function on $\mathbb{C}^g \times \mathbb{H}_g$

given by:

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

In order to write the pseudo-periodicity relations verified by the theta functions it is convenient to introduce a certain pairing on $\mathbb{C}^g$. First we identify $\mathbb{C}^g$ to $\mathbb{R}^{2g}$ via the isomorphism $\mathbb{R}^{2g} \to \mathbb{C}^g$, $(x_1, x_2) \mapsto \Omega x_1 + x_2$. Then for $\alpha, \beta \in \mathbb{R}^{2g}$ with $\alpha = (\alpha_1, \alpha_2)$ and $\beta = (\beta_1, \beta_2)$, we put $e_\Omega(\alpha, \beta) = \exp(2\pi i(\alpha_1\beta_2 - \alpha_2\beta_1))$. The pseudo-periodicity of $\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right]$ is given by

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

We say that a function f on $\mathbb{C}^g$ is Λ_Ω-quasi-periodic of level $\ell \in \mathbb{N}$ if for all $z \in \mathbb{C}^g$ and $m \in \mathbb{Z}^g$, we have:$f(z+m) = f(z)$, $f(z+\Omega.m) = \exp(-\pi i\ell^t m.\Omega.m - 2\pi i\ell^t z.m)f(z)$. For any $\ell \in \mathbb{N}^*$, the set $H_{\Omega,\ell}$ of Λ_Ω-quasi-periodic functions of level ℓ is a finite dimensional $\mathbb{C}$-vector space whose basis can be given by the theta functions with characteristics: $(\theta\left[\begin{smallmatrix} 0 \\ b/\ell \end{smallmatrix}\right](z, \ell^{-1}.\Omega))_{b\in[0,\dots,\ell-1]^g}$. If $\ell = k^2$, then an alternative basis of $H_{\Omega,\ell}$ is $(\theta\left[\begin{smallmatrix} a/k \\ b/k \end{smallmatrix}\right](kz,\Omega))_{a,b\in[0,\dots,k-1]^g}$. A theorem of Lefschetz tells that if $\ell \geq 3$, the functions in $H_{\Omega,\ell}$ give a projective embedding of A in $\mathbb{P}^{\ell^g-1}$, the projective space over $\mathbb{C}$ of dimension $\ell^g - 1$. For $\ell = 2$, the functions in $H_{\Omega,2}$ does not give a projective embedding of A. It is easy to check that for all $f \in H_{\Omega,2}$, we have $f(-z) = f(z)$. Under some well known general conditions [7, cor 4.5.2], the image of the embedding defined by $H_{\Omega,2}$ in $\mathbb{P}^{\ell^2-1}$ is the Kummer variety associated to A, which is the quotient of A by the automorphism -1.

Once we have chosen a level $\ell \in \mathbb{N}$, for the rest of this paper, we adopt the following conventions: we let $Z(\overline{\ell}) = (\mathbb{Z}/\ell\mathbb{Z})^g$ and for a point $z_P \in \mathbb{C}^g$ and $i \in Z(\overline{\ell})$ we put $\theta_i(z_P) = \theta\left[\begin{smallmatrix} 0 \\ i/\ell \end{smallmatrix}\right](z_P, \Omega/\ell)$. If $\ell = k^2$, for $i, j \in Z(\overline{k})$, we let $\theta_{i,j}(z_P) = \theta\left[\begin{smallmatrix} i/k \\ j/k \end{smallmatrix}\right](k.z_P, \Omega)$. We denote by $\widetilde{P}$ the element of $\mathbb{A}^{\ell^g}(\mathbb{C})$ with coordinates $\widetilde{P}_i = \theta_i(z_P)$ and let P be the associated point of A that we consider depending on the situation as embedded in $\mathbb{P}^{\ell^g-1}$ or as a point on the analytic variety $\mathbb{C}^g/\Lambda_\Omega$. In this paper, for $n, \ell \in \mathbb{N}$, such that n divides ℓ we will implicitly consider $Z(\overline{n})$ as a subgroup of $Z(\overline{\ell})$ via the morphism $x \mapsto (\ell/n).x$.

We denote by Ξ_ℓ the theta divisor of level ℓ on A which is the divisor of zero of $\theta\left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](z, \ell^{-1}.\Omega)$. There is an isogeny $\varphi_\ell : A \to \hat{A} = \mathrm{Pic}^0_A$, defined by $x \mapsto \tau_x^*\,\Xi_\ell - \Xi_\ell$ where τ_x is the translation by x morphism on A. The kernel of φ_ℓ is $A[\ell]$. For $\ell = 1$ we let $\Xi_1 = \Xi$. We denote by $K(A)$ the function field of A and if $f \in K(A)$, we denote (f) the divisor of the function f. Let $Z^0(A)$ be the group of 0-cycles of A that is the free commutative group over the set of closed points of A. If $D = \sum n_i P_i$ is an element of $Z^0(A)$ and $f \in K(A)$ then we put $f(D) = \prod_i f(P_i)^{n_i}$.

3 Weil and Tate pairings and theta functions

In this section, we present formulas to compute Weil and Tate pairings from the knowledge of the theta coordinates of some points.

3.1 The Weil pairing

For $\Omega \in \mathbb{H}_g$, let $A = \mathbb{C}^g/\Lambda_\Omega$ be the associated complex abelian variety and denote by $\pi : \mathbb{C}^g \to A$ the natural projection. Let ℓ be a positive integer, we denote by μ_ℓ the subgroup of $\mathbb{C}^*$ of ℓ^{th} roots of unity. For $z_P, z_Q \in \mathbb{C}^g$, let P, Q be the associated points of A, we consider the pairing: $e_W : A[\ell] \times A[\ell] \to \mu_\ell$, $(P, Q) \mapsto e_\Omega(z_P, z_Q)^\ell$. It is clear that e_W does not depend on the choice of z_P and z_Q representing P and Q respectively and that e_W is a non-degenerate skew linear form. The following proposition gives an expression of this pairing in term of the values of certain theta functions.

Lemma 1. *Let $\Omega \in \mathbb{H}_g$. Let $a, b \in \mathbb{Q}^g$, let ℓ be a positive integer and let $z_P, z_Q \in \mathbb{C}^g$ be such that $\ell.z_P = \ell.z_Q = 0 \mod \Lambda_\Omega$. Set $z_P = \Omega.z_{P1} + z_{P2}$ and $z_Q = \Omega.z_{Q1} + z_{Q2}$ with for $i = 1, 2$, $z_{Pi}, z_{Qi} \in \mathbb{R}^g$. Let $P = \pi(z_P)$ and $Q = \pi(z_Q)$. For all $z \in \mathbb{C}^g$, we have:*

$$e_W(P, Q) = \frac{\theta \begin{bmatrix} a+z_{Q1} \\ b+z_{Q2} \end{bmatrix} (z, \Omega)}{\theta \begin{bmatrix} a+z_{Q1} \\ b+z_{Q2} \end{bmatrix} (z + \ell.z_P, \Omega)} \frac{\theta \begin{bmatrix} a \\ b \end{bmatrix} (z + \ell.z_P, \Omega)}{\theta \begin{bmatrix} a \\ b \end{bmatrix} (z, \Omega)}. \tag{3}$$

Proof. By (2), we have:

$$\theta \begin{bmatrix} a+z_{Q1} \\ b+z_{Q2} \end{bmatrix} (z + \ell.z_P, \Omega) = e_\Omega(\Omega.(a + z_{Q1}) + (b + z_{Q2}), \Omega.\ell z_{P1} + \ell z_{P2})$$
$$\exp[(\pi i \ell^2({}^t z_{P1}.\Omega.z_{P1}) - 2\pi i {}^t z_{P1}.z] \theta \begin{bmatrix} a+z_{Q1} \\ b+z_{Q2} \end{bmatrix} (z, \Omega),$$

$$\theta \begin{bmatrix} a \\ b \end{bmatrix} (z + \ell.z_P, \Omega) = e_\Omega(\Omega.a + b, \Omega.\ell z_{P1} + \ell z_{P2})$$
$$\exp[-\pi i \ell^2({}^t z_{P1}.\Omega.z_{P1}) - 2\pi i {}^t z_{P1}.z] \theta \begin{bmatrix} a \\ b \end{bmatrix} (z, \Omega).$$

The lemma follows from immediately.

Let $e'_W : A[\ell] \times A[\ell] \to \mu_\ell$ be the usual Weil pairing. We recall a possible definition for e'_W [13, p. 184]. Let $P, Q \in A[\ell]$. Let $D = \tau_Q^* \Xi - \Xi$, then D represents a point of $\hat{A}[\ell] = \mathrm{Pic}^0_A[\ell]$. As a consequence, there exists a function $f_Q \in K(A)$ such that $(f_Q) = \ell.D$. In the same way, there exists a function $g_Q \in K(A)$ such that $(g_Q) = [\ell]^*(D)$. As $[\ell]^*(f_Q) = \ell.[\ell]^* D = (g_Q^\ell)$ there exists a constant $c \in \mathbb{C}^*$ such that $[\ell]^* f_Q = c.g_Q^\ell$. Thus for X a general point of A, $\frac{g_Q(X)}{g_Q(X+P)}$ is an element of μ_ℓ which is equal to $e'_W(P, Q)$.

Proposition 1. *Keeping the notations from above, let $z_P = \Omega.z_{P1} + z_{P2}$ and $z_Q = \Omega.z_{Q1} + z_{Q2}$ be elements of $\mathbb{C}^g$ such that $P = \pi(z_P)$ and $Q = \pi(z_Q)$. For $z \in \mathbb{C}^g$, we have the following equalities, up to a multiplication by a constant:*

$$g_Q(z) = \frac{\theta \begin{bmatrix} z_{Q1} \\ z_{Q2} \end{bmatrix} (\ell.z, \Omega)}{\theta \begin{bmatrix} 0 \\ 0 \end{bmatrix} (\ell.z, \Omega)}, f_Q(z) = \mu_Q(z)^{-1} \left(\frac{\theta \begin{bmatrix} 0 \\ 0 \end{bmatrix} (z + z_Q)}{\theta \begin{bmatrix} 0 \\ 0 \end{bmatrix} (z)} \right)^\ell, \tag{4}$$

where $\mu_Q(z) : \mathbb{C}^g \to \mathbb{C}$ is given by $\mu_Q(z) = \frac{\theta \begin{bmatrix} 0 \\ 0 \end{bmatrix} (z + \ell z_Q)}{\theta \begin{bmatrix} 0 \\ 0 \end{bmatrix} (z)}$.

Remark 1. In the preceding equations, the domain of the functions g_Q and f_Q is $\mathbb{C}^g$ but we will see in the course of the proof that g_Q and f_Q are periodic with respect to Λ_Ω and are in fact well defined functions on A.

Proof. As $\pi^*\,\Xi$ is the divisor of zero of $\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](z,\Omega)$, π^*D is the divisor of zero of $g'(z)=\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](z+z_Q,\Omega)/\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](z,\Omega)$. But $g(z)=\exp[\pi i^t z_{Q1}\Omega z_{Q1}+2\pi i^t z_{Q1}(z+z_{Q2})]g'(z)$ has the same zero divisor as $g'(z)$ and $g(z)=\theta\left[\begin{smallmatrix}z_{Q1}\\z_{Q2}\end{smallmatrix}\right](z,\Omega)/\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](z,\Omega)$. Let $\widetilde{[l]}:\mathbb{C}^g\to\mathbb{C}^g$, $z\mapsto \ell z$. It is clear from its definition that up to a multiplication by a constant $g_Q=g\circ\widetilde{[l]}$ which gives the left hand of (4). It is easily seen using (2) that $g_Q(z)$ is periodic with respect to Λ_Ω and as a consequence descends to a function on A.

We turn to the proof of the second equality. As $\mu_Q(z)$ is a non vanishing function, the zero divisor of the function $\mu_Q(z)^{-1}\left(\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](z+z_Q)/\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](z)\right)^\ell$ is $\pi^*(\ell D)$. Moreover, it is easily seen using (2) that this function is periodic with respect to Λ_Ω, and descends to a function on A which up to a multiplication by a constant is $f_Q(z)$.

Corollary 1. *The pairing e_W is the Weil pairing.*

Proof. This is an immediate consequence of Lemma 1 with $a=b=0$, Proposition 1 and the definition of the Weil pairing as $e'_W(P,Q)=\frac{g_Q(X)}{g_Q(X+P)}$.

Corollary 2. *Let $\Omega\in\mathbb{H}_g$. Let $a,b\in\mathbb{Q}^g$, let ℓ be a positive integer and let $z_P,z_Q\in\mathbb{C}^g$ be such that $\ell.z_P=\ell.z_Q=0 \mod \Lambda_\Omega$. Let $P,Q\in A$ be such that $P=\pi(z_P)$ and $Q=\pi(z_Q)$ and let:*

$$\begin{aligned} L(z_P,z_Q)&=\frac{\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](\ell.z_P+z_Q,\Omega)}{\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](z_Q,\Omega)}\frac{\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](0,\Omega)}{\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](\ell.z_P,\Omega)},\\ R(z_P,z_Q)&=\frac{\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](\ell.z_Q+z_P,\Omega)}{\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](z_P,\Omega)}\frac{\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](0,\Omega)}{\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](\ell.z_Q,\Omega)}. \end{aligned} \tag{5}$$

If $L(z_P,z_Q)$ and $R(z_P,z_Q)$ are well defined and non null, we have:

$$e_\Omega(z_P,z_Q)^\ell=e_W(P,Q)=L(z_P,z_Q)^{-1}.R(z_P,z_Q). \tag{6}$$

Proof. Since $Q+\ell P=Q$ and $\ell P=0$, $L(z_P,z_Q)$ does not depend on $\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right]$ so we can assume that $a=b=0$. The corollary can then be proved by a direct computation.

But it also follows immediately from Proposition 1 and the formula $e_W(P,Q)=f_P(Q-0)/f_Q(P-0)$. In fact, using the notations of Proposition 1, we have

$$\frac{f_P(Q-0)}{f_Q(P-0)}=\frac{\mu_P(z_Q)\mu_Q(0)}{\mu_P(0)\mu_Q(z_P)}.$$

The result follows an immediate computation.

Remark 2. One can recognize in (6) a classical formula to compute the first Chern class of a line bundle from the knowledge of its factors of automorphy, see for instance [1, Th. 2.1.2]

3.2 The Tate pairing

Let K be a number field. In this section, we suppose that $\mu_\ell \subset K$ and that $A[\ell]$ is rational over K. Let $\overline{K}$ be the algebraic closure of K and let $G = \mathrm{Gal}(\overline{K}/K)$. Let $\delta_1 : K^*/K^{*\ell} \to \mathrm{Hom}(G, \mu_\ell)$ (resp. $\delta_2 : A(K)/[\ell]A(K) \to \mathrm{Hom}(G, A[\ell])$) be the connecting morphism of the Galois cohomology long exact sequence associated to the Kummer exact sequence (resp. to the exact sequence $0 \to A[\ell] \to A(\overline{K}) \to A(\overline{K}) \to 0$). There exists a bilinear application often referred to as the Tate pairing $e_T : A(K)/[\ell]A(K) \times A[\ell] \to K^*/K^{*\ell}$ such that for $(P, Q) \in A(K)/[\ell]A(K) \times A[\ell]$, $e_W(\delta_2(P), Q) = \delta_1(e_T(P, Q))$.

Proposition 2. *Let K be a number field and let A be a dimension g abelian variety over K. Let $\Omega \in \mathbb{H}_g$ be such that A is analytically isomorphic to $\mathbb{C}^g/\Lambda_\Omega$. Let $a, b \in \mathbb{Q}^g$, and let ℓ be a positive integer. Let $P \in A(K)/[\ell]A(K)$ and $Q \in A[\ell]$ and let $z_P, z_Q \in \mathbb{C}^g$ be such that $\pi(z_P) = P$ and $\pi(z_Q) = Q$ where $\pi : \mathbb{C}^g \to A$ is the natural projection (by abuse of notation we use P, Q to denote the corresponding points of an algebraic and analytic model of A). Suppose that*

$$\frac{\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](z_P + z_Q)}{\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](z_P)} \frac{\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](0)}{\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](z_Q)} \in K^*, \tag{7}$$

then we have

$$e_T(P, Q) = \frac{\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](\ell.z_Q + z_P)}{\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](z_P)} \frac{\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](0)}{\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](\ell.z_Q)}. \tag{8}$$

Proof. By Proposition 1, we have

$$f_Q(P - 0) = \frac{\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](z_P)}{\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](\ell.z_Q + z_P)} \frac{\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](\ell.z_Q)}{\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](0)} \left(\frac{\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](z_P + z_Q)}{\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](z_P)} \frac{\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](0)}{\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](z_Q)} \right)^\ell.$$

Taking care of the fact that $e_T(P, Q)$ has value in $K^*/K^{*\ell}$ we just have to prove that $e_T(P, Q) = f_Q(0 - P)$. The proof follows exactly the same computations as [16, p. 280]. Let $P_0 \in A(\overline{K})$ such that $\ell P_0 = P$. Following the definition of the connection morphism δ_2, we have $\delta_2(P) = \mathfrak{f}$ where $\mathfrak{f} : G \to A[\ell]$, $\sigma \mapsto P_0^\sigma - P_0$ is a co-cycle (in fact a morphism since $A[\ell]$ is rational over K) representing an element of $H^1(G, \mu_\ell)$.

By definition of the Weil pairing, we have $e_W(P_0^\sigma - P_0, Q) = \frac{g_Q(P_0)}{g_Q(P_0^\sigma)}$. On the other side, as $[\ell]^*(f_Q) = c.(g_Q)^\ell$ where $c \in \mathbb{C}^*$ is a constant, we have $\left(\frac{g_Q(P_0)}{g_Q(0)}\right)^\ell = \frac{f_Q(P)}{f_Q(0)}$. But then $\delta_1(f_Q(0 - P))$ is represented by the co-cycle $\mathfrak{g} : G \to \frac{g_Q(P_0)}{g_Q(P_0^\sigma)}$. Comparing this with the preceding equation concludes the proof.

Remark 3. Let θ_c^0 be the canonical theta function given by (see [1, sec. 3.2]):

$$\theta_c^0(z) = \exp(\frac{\pi}{2}{}^t z(\mathrm{Im}\,\Omega)z)\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](z, \Omega).$$

Then θ_c^0 is an holomorphic function on $\mathbb{C}^g$ verifying: $\theta_c^0(z + \lambda) = \mathfrak{a}(\lambda, z)\theta_c^0(z)$, for all $z \in \mathbb{C}^g$, $\lambda \in \Lambda_\Omega$. Here, $\mathfrak{a}(\lambda, z) = \chi(\lambda).\exp(\pi H(z, \lambda) + \frac{\pi}{2}H(\lambda, \lambda))$ is the

canonical factor of automorphy, where H is the hermitian form whose matrix is given by $(\operatorname{Im}\Omega)^{-1}$.

Computing the expression (8) for $e_T(P,Q)$ we obtain that a representative of $e_T(P,Q)$ is given by $e_T(P,Q) = \frac{\theta_c^0(\ell.z_Q+z_P)}{\theta_c^0(z_P)}\frac{\theta_c^0(0)}{\theta_c^0(\ell.z_Q)} = \exp(\pi H(z_P,\ell z_Q))$ which gives a nice geometric interpretation of the Tate pairing. On the other side, we recall that $e_\Omega(.,.) = \exp(2\pi i \operatorname{Im} H(.,.))$ and as a consequence, we can write the Weil pairing as $e_W(P,Q) = \exp(2\pi i \operatorname{Im} H(z_P,\ell z_Q))$. Compared to its counterpart for the Weil pairing, the expression for the Tate pairing has to be taken cautiously as it involves rationality conditions to be correct.

4 Pairing computations

In this section, we describe a general method to compute Weil or Tate pairings which does not rely on the usual Miller's loop and prove its correctness. We postpone to the next section the analysis of the running time of these algorithms.

Let $n, \ell \in \mathbb{N}$. We suppose that 2 divides n and that ℓ and n are relatively prime. Let A be an abelian variety over $\mathbb{C}$ with period matrix Ω. We represent A as a closed subvariety of $\mathbb{P}^{n^g-1}$ by the way of level n theta functions and we suppose that this embedding is defined over K. Denote by $\widetilde{A}$ the pullback of A via the natural projection $\kappa : \mathbb{A}^{n^g} \to \mathbb{P}^{n^g-1}$. In the following, we adopt the following convention: if P is a point of A, we denote by $\widetilde{P}$ an affine lift of P that is a point $\widetilde{P}$ of $\mathbb{A}^{n^g}$ such that $\kappa(\widetilde{P}) = P$.

An important ingredient of our algorithm is the Riemann addition formulas. The usual form of these formulas works for theta functions of level divisible by 4 (see for instance [6, p. 139]). In this paper we need a slight generalisation of these formulas for working also with level 2 theta functions. We recall that following the convention for the notation of theta functions described at the end of the introduction, we let for all $i \in Z(\overline{n})$, $z \in \mathbb{C}^g$, $\theta_i(z) = \theta\left[\begin{smallmatrix}0\\ i/n\end{smallmatrix}\right](z, \Omega/n)$. Moreover, we recall that in the following we consider $Z(\overline{n})$ (resp. $Z(\overline{2})$) as a subgroup of $Z(\overline{2n})$ via the map $x \mapsto 2x$ (resp. $x \mapsto nx$).

Theorem 1. *Let $i,j,k,l \in Z(\overline{2n})$. We suppose that $i+j$, $i+k$ and $i+l \in Z(\overline{n})$. Let $\hat{Z}(\overline{2})$ be the dual group of $Z(\overline{2})$. For all $\chi \in \hat{Z}(\overline{2})$ and $z_1, z_2 \in \mathbb{C}^g$ we have*

$$\left(\sum_{\eta\in Z(\overline{2})} \chi(\eta)\theta_{i+j+\eta}(z_1+z_2)\theta_{i-j+\eta}(z_1-z_2)\right)\left(\sum_{\eta\in Z(\overline{2})} \chi(\eta)\theta_{k+l+\eta}(0)\theta_{k-l+\eta}(0)\right)$$
$$= \left(\sum_{\eta\in Z(\overline{2})} \chi(\eta)\theta_{i+k+\eta}(z_1)\theta_{i-k+\eta}(z_1)\right)\left(\sum_{\eta\in Z(\overline{2})} \chi(\eta)\theta_{j+l+\eta}(z_2)\theta_{j-l+\eta}(z_2)\right) \tag{9}$$

Proof. For $i \in Z(\overline{2n})$ and $z \in \mathbb{C}^g$, we let $\theta'_i(z) = \theta\left[\begin{smallmatrix}0\\ i/(2n)\end{smallmatrix}\right](z, \Omega/(2n))$. Let $i,j \in Z(\overline{2n})$ be such that $i+j \in Z(\overline{n})$ and let $z_1, z_2 \in \mathbb{C}^g$. The usual duplication

formula [6, p. 139] gives $\theta_{i+j}(z_1+z_2)\theta_{i-j}(z_1-z_2) = \frac{1}{2^g}\sum_{\eta\in Z(\overline{2})}\theta'_{i+\eta}(z_1)\theta'_{j+\eta}(z_2)$. For $\chi \in \hat{Z}(\overline{2})$, using this formula, we compute

$$\sum_{\eta\in Z(\overline{2})}\chi(\eta)\theta_{i+j+\eta}(z_1+z_2)\theta_{i-j+\eta}(z_1-z_2) = \frac{1}{2^g}\sum_{\eta_1,\eta_2\in Z(\overline{2})}\chi(\eta_1+\eta_2)\theta'_{i+\eta_1}(z_1)\theta'_{j+\eta_2}(z_2)$$
$$= \frac{1}{2^g}\left(\sum_{\eta\in Z(\overline{2})}\chi(\eta)\theta'_{i+\eta}(z_1)\right)\left(\sum_{\eta\in Z(\overline{2})}\chi(\eta)\theta'_{j+\eta}(z_2)\right). \quad (10)$$

Using this last equation to compute the left and right hand sides of the preceding equation we obtain the result.

We suppose that the theta null point $\widetilde{0} = (\theta_i(0))_{i\in Z(\overline{n})}$ is known. We deduce immediately from Theorem 1 an algorithm that takes as inputs $\widetilde{P} = (\widetilde{P}_i)_{i\in Z(\overline{n})}$, $\widetilde{Q} = (\widetilde{Q}_i)_{i\in Z(\overline{n})}$ and $\widetilde{P-Q} = (\widetilde{(P-Q)}_i)_{i\in Z(\overline{n})}$ and outputs $\widetilde{P+Q} = (\widetilde{(P+Q)}_i)_{i\in Z(\overline{n})}$. We write $\widetilde{P+Q} = \mathrm{PseudoAdd}(\widetilde{P},\widetilde{Q},\widetilde{P-Q})$. Indeed we will see latter (Proposition 3) that if $n = 4$, we can recover the projective point $P+Q$ from P and Q using the Riemann addition formulas. It is then easy to see that if we moreover know $\widetilde{P},\widetilde{Q}$ and $\widetilde{P-Q}$, then there is a unique affine point $\widetilde{P+Q}$ above $P+Q$ that satisfy the addition formulas from Theorem 1. If $n = 2$, the point $\widetilde{P+Q}$ is also unique provided the abelian variety satisfy the generic condition from Theorem 3.

Chaining the algorithm PseudoAdd in a classical Montgomery ladder [2, alg. 9.5 p. 148] yields an algorithm that takes as inputs $\widetilde{Q} = (\widetilde{Q}_i)_{i\in Z(\overline{n})}$, $\widetilde{P+Q} = (\widetilde{(P+Q)}_i)_{i\in Z(\overline{n})}$, $\widetilde{P} = (\widetilde{P}_i)_{i\in Z(\overline{n})}$ and an integer ℓ and outputs $\widetilde{P+\ell Q}$. We write $\widetilde{P+\ell Q} = \mathrm{ScalarMult}(\widetilde{P+Q},\widetilde{Q},\widetilde{P},\ell)$. In particular, we have $\ell\widetilde{P} = \mathrm{ScalarMult}(\widetilde{P},\widetilde{P},\widetilde{0},\ell)$. The following lemma tells that the output of ScalarMult does not depend on the particular chain of PseudoAdd calls it uses.

Lemma 2. *Let $L = \{0,1,\dots,\ell\}$ be a Lucas sequence. Let $A_0 = \widetilde{P}$, $B_0 = \widetilde{0}$, $A_1 = \widetilde{P+Q}$ and $B_1 = \widetilde{Q}$. For $m \in L, m \geqslant 2$, write $m = j+k$ with $j,k,j-k \in L$. Let $B_m = \mathrm{PseudoAdd}(B_j,B_k,B_{j-k})$ and $A_m = \mathrm{PseudoAdd}(A_j,B_k,A_{j-k})$. Then $A_\ell = \widetilde{P+\ell Q}$. In other words $\widetilde{P+\ell Q}$ does not depend on the Lucas sequence used to compute it.*

Proof. If there exist $z_P, z_Q \in \mathbb{C}^g$ such that $\widetilde{P} = (\theta_i(z_P))_{i\in Z(\overline{n})}$, $\widetilde{Q} = (\theta_i(z_Q))_{i\in Z(\overline{n})}$ and $\widetilde{P+Q} = (\theta_i(z_P+z_Q))_{i\in Z(\overline{n})}$ then by Theorem 1 and an easy recursion we see that $A_j = (\theta_i(z_P+jz_Q))_{i\in Z(\overline{n})}$ and $B_j = (\theta_i(jz_Q))_{i\in Z(\overline{n})}$. Hence $A_\ell = (\theta_i(z_P+\ell z_Q)) = \widetilde{P+\ell Q}$.

Otherwise there exist λ_P, λ_Q and λ_{P+Q} in $\mathbb{C}^*$ such that $\widetilde{P} = \lambda_P(\theta_i(z_P))_{i\in Z(\overline{n})}$, $\widetilde{Q} = \lambda_Q(\theta_i(z_Q))_{i\in Z(\overline{n})}$ and $\widetilde{P+Q} = \lambda_{P+Q}(\theta_i(z_P+z_Q))_{i\in Z(\overline{n})}$. Since we have

$$\mathrm{PseudoAdd}(\lambda_{P+Q}\widetilde{P+Q},\lambda_Q\widetilde{Q},\lambda_P\widetilde{P}) = \frac{\lambda_{P+Q}^2\lambda_Q^2}{\lambda_P}\mathrm{PseudoAdd}(\widetilde{P+Q},\widetilde{Q},\widetilde{P}),$$

an easy recursion shows that $B_j = \lambda_Q^{j^2}(\theta_i(jz_Q))_{i\in Z(\overline{n})}$ and $A_j = \frac{\lambda_{P+Q}^{j}\lambda_Q^{j(j-1)}}{\lambda_P^{j-1}}(\theta_i(z_P+jz_Q))_{i\in Z(\overline{n})}$. Hence $A_\ell = \frac{\lambda_{P+Q}^{\ell}\lambda_Q^{\ell(\ell-1)}}{\lambda_P^{\ell-1}}(\theta_j(z_P+\ell z_Q))_{j\in Z(\overline{n})} = \widetilde{P+\ell Q}$.

Remark 4. There is a natural action of $\overline{K}^*$ on $\mathbb{A}^{n^g} - \{0\}$ by multiplication of the coordinates of a point that we denote by $\alpha * \widetilde{P}$ for $\alpha \in \overline{K}^*$ and $\widetilde{P} \in \mathbb{A}^{n^g}(\overline{K})$. In the proof of the preceding lemma we have seen the effect of this action on the output of the algorithm ScalarMult: let $P, Q \in A(\overline{K})$ and let $\widetilde{P}, \widetilde{Q}, \widetilde{P+Q}$ be affine lifts of P, Q and $P+Q$. Let $\widetilde{R} = \text{ScalarMult}(\widetilde{P+Q}, \widetilde{Q}, \widetilde{P}, \ell)$. Let $\alpha, \beta, \gamma \in \overline{K}$, we have

$$\text{ScalarMult}(\alpha * \widetilde{P+Q}, \beta * \widetilde{Q}, \gamma * \widetilde{P}, \ell) = (\alpha^\ell \beta^{\ell(\ell-1)}/\gamma^{\ell-1}) * \widetilde{R}, \tag{11}$$

$$\text{ScalarMult}(\alpha * \widetilde{P}, \alpha * \widetilde{P}, \widetilde{0}, \ell) = \alpha^{\ell^2} * \text{ScalarMult}(\widetilde{P}, \widetilde{P}, \widetilde{0}, \ell). \tag{12}$$

Given P and Q with projective coordinates $(\theta_i(z_P))_{i\in Z(\overline{n})}$ and $(\theta_i(z_Q))_{i\in Z(\overline{n})}$ for $z_P, z_Q \in \mathbb{C}^g$, we would like to compute $e_W(P,Q)$ and $e_T(P,Q)$.

We can state the main theorem of this section

Theorem 2. *We suppose that n and ℓ are relatively prime. For $X, Y \in A(\overline{K})$, denote by $\widetilde{X}$, $\widetilde{Y}$, $\widetilde{X+Y}$ any affine lifts of X, Y and $X+Y$. Recall that for $i \in Z(\overline{n})$, we denote by $\widetilde{X}_i$ the coordinate i of the point $\widetilde{X}$. For $\ell \in \mathbb{N}$ and $i \in Z(\overline{n})$, let $f_T(\widetilde{X}, \widetilde{Y}, \widetilde{X+Y}, \ell, i) = \frac{\text{ScalarMult}(\widetilde{X+Y}, \widetilde{X}, \widetilde{Y}, \ell)_i}{\text{ScalarMult}(\widetilde{X}, \widetilde{X}, \widetilde{0}, \ell)_i} \frac{\widetilde{0}_i}{\widetilde{Y}_i}$. Then for $P, Q \in A[\ell]$ and $i \in Z(\overline{n})$, we have:*

$$e_W(P,Q)^n = f_T(\widetilde{P}, \widetilde{Q}, \widetilde{P+Q}, \ell, i)^{-1} f_T(\widetilde{Q}, \widetilde{P}, \widetilde{P+Q}, \ell, i), \tag{13}$$

whenever the right hand side is well defined.

Moreover, for $P \in A(K)/[\ell]A(K)$, $Q \in A[\ell]$, if we suppose that $\widetilde{P}$, $\widetilde{Q}$ and $\widetilde{P+Q}$ are affine lifts of P, Q and $P+Q$ with coordinates in K, then we have for $i \in Z(\overline{n})$,

$$e_T(P,Q)^n = f_T(\widetilde{Q}, \widetilde{P}, \widetilde{P+Q}, \ell, i), \tag{14}$$

whenever the right hand side is well defined.

Proof. Let $z_P, z_Q \in \mathbb{C}^g$ such that $\pi(z_P) = P$ and $\pi(z_Q) = Q$ (recall that $\pi : \mathbb{C}^g \to A = \mathbb{C}^g/\Lambda_\Omega$ is the natural projection). Let $\widetilde{P} = (\theta_i(z_P))_{i\in Z(\overline{n})}$, $\widetilde{Q} = (\theta_i(z_Q))_{i\in Z(\overline{n})}$ and $\widetilde{P+Q} = (\theta_i(z_P+z_Q))_{i\in Z(\overline{n})}$. Then applying Corollary 2, if $P, Q \in A[\ell]$, we obtain that

$$e_{\Omega/n}(z_P, z_Q)^\ell = e_W(P,Q)^n = f_T(\widetilde{P}, \widetilde{Q}, \widetilde{P+Q}, \ell, i)^{-1} f_T(\widetilde{Q}, \widetilde{P}, \widetilde{P+Q}, \ell, i).$$

In the same way, by Proposition 2 (which apply for $i = 0$, but it is easy to see that the same result is true for any $i \in Z(\overline{n})$), we have for $P \in A(K)/[\ell]A(K)$ and $Q \in A[\ell]$, $e_T(P,Q)^n = f_T(\widetilde{P}, \widetilde{Q}, \widetilde{P+Q}, \ell, i)$.

Next, let $\alpha, \beta, \gamma \in \overline{K}$. By Remark 4, we have

$$f_T(\alpha * \widetilde{X}, \beta * \widetilde{Y}, \gamma * \widetilde{X+Y}, \ell, i) = \frac{\gamma^\ell}{\alpha^\ell \beta^\ell} . f_T(\widetilde{X}, \widetilde{Y}, \widetilde{X+Y}, \ell, i).$$

This shows that the expressions (13) and (14) for the Weil and Tate pairing does not depend on the choice of affine liftings (rational over K in the case of the Tate pairing) of P, Q and $P+Q$.

As we have shown that the formulas of Theorem 2 does not depend on a choice of the affine lifts of the input points of the algorithm (as long as the choices are the same for the computation of the two functions f_T in the case of the Weil pairing), from now on we only consider projective points.

In order to have a working algorithm to compute Weil and Tate pairings, it remains to explain how to compute $P+Q$ from the knowledge of P and Q. As the formulas to compute the pairings only involve one of the level n theta functions, and since the number of the coordinates used in the computation of ScalarMult is n^g, for the sake of efficiency it is important to have a small n. As 2 divides n, from now on, we focus on the only two interesting cases: $n = 2$ and $n = 4$.

We first treat the case $n = 4$. Let $z_P, z_Q \in \mathbb{C}^g$ and let $P = (P_i)_{i \in Z(\overline{n})} = (\theta_i(z_P))_{i \in Z(\overline{n})}$ and $Q = (Q_i)_{i \in Z(\overline{n})} = (\theta_i(z_Q))_{i \in Z(\overline{n})}$. From the knowledge of P and Q, with the addition formula (9), one can compute the products:

$$\left(\sum_{\eta \in Z(\overline{2})} \chi(\eta) \theta_{i+j+\eta}(z_P + z_Q) \theta_{i-j+\eta}(z_P - z_Q) \right) \left(\sum_{\eta \in Z(\overline{2})} \chi(\eta) \theta_{k+l+\eta}(0) \theta_{k-l+\eta}(0) \right), \tag{15}$$

for $\chi \in \hat{Z}(\overline{2})$ and $i, j, k, l \in Z(\overline{2n})$ such that $i+j$, $i+k$, and $i+l \in Z(\overline{n})$. If we can prove that for any such choice of $i, j, k, l \in Z(\overline{2n})$ and $\chi \in \hat{Z}(\overline{2})$ there exist $k' \in k + Z(\overline{n})$ and $l' \in l + Z(\overline{n})$ such that $\sum_{\eta \in Z(\overline{2})} \chi(\eta) \theta_{k'+l'+\eta}(0) \theta_{k'-l'+\eta}(0) \neq 0$, then by summing over the characters the left bracket of (15) one can compute all the products $\theta_i(z_P + z_Q)\theta_j(z_P - z_Q)$, for $i, j \in Z(\overline{n})$ from which it is easy to recover by taking quotients the projective point $(\theta_i(z_P + z_Q))_{i \in Z(\overline{n})}$.

Now, using equation (10), we have

$$\sum_{\eta \in Z(\overline{2})} \chi(\eta) \theta_{k+l+\eta}(0) \theta_{k-l+\eta}(0) = \frac{1}{2^g} \left(\sum_{\eta \in Z(\overline{2})} \chi(\eta) \theta'_{k+\eta}(0) \right) \left(\sum_{\eta \in Z(\overline{2})} \chi(\eta) \theta'_{l+\eta}(0) \right), \tag{16}$$

where for $k \in Z(\overline{8})$, $\theta'_k(z) = \theta \left[{}^0_{k/8} \right] (z, \Omega/8)$. We have the

Proposition 3. *Let $\delta \in \mathbb{N}$ be such that 4 divides δ. For any $a \in K(\overline{2\delta})$ there exists an element $b \in a + K(\delta)$ such that for all $\chi \in \hat{Z}(\overline{2})$ we have*

$$\sum_{\eta \in Z(\overline{2})} \chi(\eta) \theta \left[{}^0_{(b+\eta)/(2\delta)} \right] (0, 1/(2\delta).\Omega) \neq 0.$$

Proof. This is just a rephrasing of [11, equation (*) p. 339].

Applying the preceding proposition to the factors of the right hand of equation (16), we obtain that there exists $k' \in k + Z(\overline{n})$ and $l' \in l + Z(\overline{n})$ such that $\sum_{\eta \in Z(\overline{2})} \chi(\eta)\theta_{k'+l'+\eta}(0)\theta_{k'-l'+\eta}(0) \neq 0$ and we are done.

In the case $n = 2$, as usual, for all $i \in Z(\overline{2})$, we put $\theta_i(z) = \theta \left[\begin{smallmatrix} 0 \\ i/2 \end{smallmatrix} \right] (z, 1/2.\Omega)$. Then by Theorem 1, we have for any $\chi \in \hat{Z}(\overline{2})$ and for well chosen pairs of quadruples $(i, j, k, l), (i', j', k', l') \in Z(\overline{2})^4$ an equation

$$\begin{aligned} &\left(\sum_{\eta \in Z(\overline{2})} \chi(\eta)\theta_{i+\eta}(z_P + z_Q)\theta_{j+\eta}(z_P - z_Q) \right) \left(\sum_{\eta \in Z(\overline{2})} \chi(\eta)\theta_{k+\eta}(0)\theta_{l+\eta}(0) \right) \\ &= \left(\sum_{\eta \in Z(\overline{2})} \chi(\eta)\theta_{i'+\eta}(z_P)\theta_{j'+\eta}(z_P) \right) \left(\sum_{\eta \in Z(\overline{2})} \chi(\eta)\theta_{k'+\eta}(z_Q)\theta_{l'+\eta}(z_Q) \right). \end{aligned} \tag{17}$$

If the kernel of χ does not contain the subgroup of $Z(\overline{2})$ generated by $k + l$ then we have $\sum_{\eta \in Z(\overline{2})} \chi(\eta)\theta_{k+\eta}(0)\theta_{l+\eta}(0) = 0$, so it is not possible to recover $\theta_{i+\eta}(z_P + z_Q)$ as before. This is consistent with the fact that for $i \in Z(\overline{2})$ and $z \in \mathbb{C}^g$, $\theta_i(z) = \theta_i(-z)$, the right hand side of (17) is invariant for the transformation $z_Q \mapsto -z_Q$ while it is not the case of the left hand side. The best we can hope is that for almost all period matrices $\Omega \in \mathbb{H}_g$ there exists a $k \in Z(\overline{2})$ such that for all $l \in Z(\overline{2})$ and $\chi \in \hat{Z}(\overline{2})$ such that $k + l$ is in the kernel of χ, we have $\sum_{\eta \in Z(\overline{2})} \chi(\eta)\theta_{k+\eta}(0)\theta_{l+\eta}(0) \neq 0$. This is exactly the content of Theorem 3. In order to prove this theorem, we let $T_{k,l,\chi} = \sum_{\eta \in Z(\overline{2})} \chi(\eta)\theta_{k+\eta}(0)\theta_{l+\eta}(0)$ and we state the following lemma:

Lemma 3. *For $\Omega \in \mathbb{H}_g$, the two following properties are equivalent:*

1. *There exists a $k \in Z(\overline{2})$ such that for all $\ell \in Z(\overline{2})$ and $\chi \in \hat{Z}(\overline{2})$ such that $k + l$ is in the kernel of χ, we have $T_{k,l,\chi} \neq 0$.*
2. *For all $i, j \in Z(\overline{2})$ such that ${}^t i.j = 0$, $\theta_{i,j}(0) \neq 0$.*

Proof. For $\chi \in \hat{Z}(\overline{2})$, let $\mu \in Z(\overline{2})$ be such that $\chi(\eta) = (-1)^{{}^t \eta.\mu}$. Let $\rho : Z(\overline{4}) \to Z(\overline{2})$, $x \mapsto x \mod Z(\overline{2})$ be the canonical projection. Then we have (see [14, prop 1.3 p. 124]), for all $i \in Z(\overline{4})$ $\sum_{\eta \in Z(\overline{2})} \chi(\eta)\theta'_{i+\eta}(0) = 2^g.\theta_{\mu,\rho(i)}(0)$, where $\theta'_k(z) = \theta \left[\begin{smallmatrix} 0 \\ k/4 \end{smallmatrix} \right] (z, 1/4.\Omega)$. Combining this relation together with (16), for all $i, j \in Z(\overline{4})$ such that $i + j \in Z(\overline{2})$, let $k = i + j$, $l = i - j$, we obtain the equality

$$T_{k,l,\chi} = T_{i+j,i-j,\chi} = 2^g.\theta_{\mu,\rho(i)}(0)\theta_{\mu,\rho(j)}(0) = 2^g.\theta_{\mu,k+l}(0)^2. \tag{18}$$

Since $\chi(k + l) = (-1)^{{}^t (k+l).\mu}$ the lemma follows immediately from (18).

It is well known that for $z \in \mathbb{C}^g$, and $k, l \in Z(\overline{2})$, we have $\theta_{k,l}(-z) = (-1)^{{}^t k.l}\theta_{k,l}(z)$. As a consequence, for all $k, l \in Z(\overline{2})$ such that ${}^t k.l = 1$ (the odd characteristics), we have $\theta_{k,l}(0) = 0$. Denote by $\mathcal{M}_4$ the quasi-projective variety over $\mathbb{C}$ defined

as the locus of zeros of $\theta_{i,j}(0)$ considered as functions of Ω. It is clear that $\mathcal{M}_4$ parametrizes the set of principally polarized abelian varieties together with a level 4 structure since from the knowledge of a point in $\mathcal{M}_4$ one can recover the projective embedding of the corresponding abelian variety provided by the Riemann equations.

Theorem 3. *For all $k, l \in Z(\overline{2})$ such that ${}^t k.l = 0$, the function $\theta_{k,l}(0)$ on $\mathcal{M}_4$ is non-trivial and as consequence, its zero locus is a proper subvariety of $\mathcal{M}_4$ of codimension 1.*

Proof. We sketch the proof of the theorem. Suppose on the contrary that for $k, l \in Z(\overline{2})$ such that ${}^t k.l = 0$, $\theta_{k,l}(0)$ is a constant function of Ω. This is a degree 1 relation for level 4 theta constants, call it $R_{k,l}$. We have for all $k \in Z(\overline{4})$, $\theta_k(0) = \theta \left[{}^{0}_{(2k)/8} \right] (0, (2\Omega)/8)$. Thus, the level 4 degree 1 relations $R_{k,l}$ induce degree 1 relations for level 8 theta constants. The hypothesis ${}^t k.l = 0$ means that these level 8 relations are not a linear combination of the symmetry relations $\theta_k(0) = \theta_{-k}(0)$ for all $k \in Z(\overline{8})$. This is a contradiction with the description of $\mathcal{M}_8$ the modular space of level 8 marked abelian varieties given by Mumford in [12, main th. p. 83] as an open subset of the reduced projective variety given by the symmetry relations and the Riemann relations.

Remark 5. The preceding theorem shows that the symmetric pairing computation algorithms that we describe in the next section works for a general abelian variety. However, one can ask if the closed proper subset of $\mathcal{M}_4$, given by the cancellation of some even level 4 theta constants contains noticeable abelian varieties. Actually, this is the case since a theorem of Frobenius [15, cor. 6.7 p. 3.102] tells us that the locus of Jacobian of hyperelliptic curves inside $\mathcal{M}_4$ can be given by equations of the form $\theta_{k,l}(0) = 0$ where (k, l) is an even characteristic. As a consequence, the algorithms of Section 5.2 to compute symmetric pairings don't apply to Jacobian of hyperelliptic of genus g when $g \geqslant 3$. It should be noted however that following [7, cor 4.5.2 and remark (2)], the condition that for all $k, l \in Z(\overline{2})$ such that ${}^t k.l = 0$, $\theta_{k,l}(0) \neq 0$ is equivalent to the fact the level 2 theta functions give a projectively normal embedding. Considering this result, the condition of Theorem 3 should be considered as natural.

5 Complexity analysis

In this section, we explain how to use the results of the preceding section to compute efficiently pairings on abelian and Kummer varieties with a special focus on dimension 1 and 2 since these cases are particularly interesting for cryptographic applications.

5.1 Abelian varieties

We begin with the case of abelian varieties since the main loop of the algorithm can also be used for the computation of symmetric pairings on Kummer varieties.

Initialisation phase The initialisation phase depends on the representation of the points P and Q on the abelian variety A. If P and Q are given by theta coordinates of level 4 we can apply the procedure described in Section 4 to compute the homogeneous coordinates of $(\theta_i(P+Q))_{i\in Z(\overline{4})}$.

Suppose that another coordinate system is used to represent P and Q that we denote by $(X_i)_{i\in I}$ where X_i are rational functions on a Zariski open subset of A. Then by definition there exist formulas to compute $\theta_i(P)$ and $\theta_i(Q)$ from the knowledge of $X_i(P)$ and $X_i(Q)$. In practise, the dictionary between some useful coordinate system and the theta coordinates can easily be deduced from well known properties of theta functions. It should be remarked that in order to carry out these computations we might have to do a base field extension since in the projective embedding of A provided by the level 4 theta functions the 4-torsion of A is rational over the base field, whereas this may not the case with other models of A. The advantage of the level 4 is that no square root extraction is required for the computation of $P+Q$, contrarily to the level 2 case as we will see.

From the knowledge of $\theta\left[\begin{smallmatrix}0\\ i/4\end{smallmatrix}\right](z_X, 1/4.\Omega)$, $i\in\mathbb{Z}(\overline{4})$ for $X = P, Q, P+Q$ we can then compute the level 2 coordinates given by

$$\Big(\sum_{j\in Z(\overline{2})} \theta\left[\begin{smallmatrix}0\\ (i+2j)/4\end{smallmatrix}\right](z_X, 1/4.\Omega)\Big)_{i\in Z(\overline{2})}$$

for the coordinates of the (isogeneous) points $X = P, Q, P+Q$.

Pairing computation phase As we have seen before, we can carry out the computations of the main loop of the algorithm with level 2 theta functions since at the end we only need one theta coordinate to compute the pairings. This is more efficient because we only need 2^g coordinates to represent a point and we can do the computation on the field of definition of the 2-torsion of A.

We suppose that we are given the level 2 coordinates of P, Q, $P+Q$. Rather than considering the formulas of Theorem 1 for the double and add algorithm, we use the level 2 formulas given in [4] for the genus 2 case, and in [5] for the genus 1 case. For instance, let E be an elliptic curve defined by $\Omega\in\mathbb{H}_1$, let $\Omega' = \Omega/2$ and put

$$a = \vartheta\left[\begin{smallmatrix}0\\ 0\end{smallmatrix}\right](0,\Omega');\ b = \vartheta\left[\begin{smallmatrix}0\\ 1/2\end{smallmatrix}\right](0,\Omega');\ A = \vartheta\left[\begin{smallmatrix}0\\ 0\end{smallmatrix}\right](0,2\Omega');\ B = \vartheta\left[\begin{smallmatrix}1/2\\ 0\end{smallmatrix}\right](0,2\Omega').$$

The duplication formulas are given by the equalities:

$$\begin{cases} a\vartheta\left[\begin{smallmatrix}0\\ 0\end{smallmatrix}\right](z,\Omega') = \vartheta\left[\begin{smallmatrix}0\\ 0\end{smallmatrix}\right](z,2\Omega')^2 + \vartheta\left[\begin{smallmatrix}1/2\\ 0\end{smallmatrix}\right](z,2\Omega')^2, \\ b\vartheta\left[\begin{smallmatrix}0\\ 1/2\end{smallmatrix}\right](z,\Omega') = \vartheta\left[\begin{smallmatrix}0\\ 0\end{smallmatrix}\right](z,2\Omega')^2 - \vartheta\left[\begin{smallmatrix}1/2\\ 0\end{smallmatrix}\right](z,2\Omega')^2. \end{cases}$$

$$\begin{cases} 2A\vartheta\left[\begin{smallmatrix}0\\ 0\end{smallmatrix}\right](2z,2\Omega') = \vartheta\left[\begin{smallmatrix}0\\ 0\end{smallmatrix}\right](z,\Omega')^2 + \vartheta\left[\begin{smallmatrix}0\\ 1/2\end{smallmatrix}\right](z,\Omega')^2, \\ 2B\vartheta\left[\begin{smallmatrix}1/2\\ 0\end{smallmatrix}\right](2z,2\Omega') = \vartheta\left[\begin{smallmatrix}0\\ 0\end{smallmatrix}\right](z,\Omega')^2 - \vartheta\left[\begin{smallmatrix}0\\ 1/2\end{smallmatrix}\right](z,\Omega')^2. \end{cases}$$

Let $x = \theta\left[\begin{smallmatrix}0\\ 0\end{smallmatrix}\right](z,\Omega')$ and $z = \theta\left[\begin{smallmatrix}0\\ 1/2\end{smallmatrix}\right](z,\Omega')$ using the above formulas yield the following algorithms:

Doubling Algorithm:
Input: A point $P = (x : z)$.
Output: The double $2.P = (x' : z')$.

1. $x_0 = (x^2 + z^2)^2$;
2. $z_0 = \frac{A^2}{B^2}(x^2 - z^2)^2$;
3. $x' = (x_0 + z_0)$;
4. $z' = \frac{a}{b}(x_0 - z_0)$;
5. Return $(x' : z')$.

Differential Addition Algorithm:
Input: Two points $P = (x : z)$ and $Q = (\widetilde{x} : \widetilde{z})$ on E, and $R = (\overline{x} : \overline{z}) = P - Q$, with $\overline{x}\overline{z} \neq 0$.
Output: The point $P + Q = (x' : z')$.

1. $x_0 = (x^2 + z^2)(\widetilde{x}^2 + \widetilde{z}^2)$;
2. $z_0 = \frac{A^2}{B^2}(x^2 - z^2)(\widetilde{x}^2 - \widetilde{z}^2)$;
3. $x' = (x_0 + z_0)/\overline{x}$;
4. $z' = (x_0 - z_0)/\overline{z}$;
5. Return $(x' : z')$.

Recall that in order to compute the pairing $e_T(P, Q)$, we have to compute $\widetilde{P + \ell Q} = \text{ScalarMult}(\widetilde{P + Q}, \widetilde{Q}, \widetilde{P}, \ell)$ and $\ell\widetilde{Q} = \text{ScalarMult}(\widetilde{Q}, \widetilde{Q}, \widetilde{0}, \ell)$. It should be remarked that in the computation of $\widetilde{P + \ell Q}$, we need exactly the same values of $j.Q$ for some $j \in \{1, \ldots, \ell\}$ as those required to obtain $\ell\widetilde{Q}$. Since we want to avoid a division in each step, we use a Montgomery ladder so that the differences in the adding step are always the same points. To speed up the differential additions, we have renormalised the theta null point (a, b) to $(1, b/a)$. It is easy to see by doing the same computation as in Remark 4 that this does not change the value of the Tate pairing $e_T(P, Q)$. Moreover we also have renormalised the theta null point (A, B). Looking back at the proof of 1, we see that this change each affine addition by the constant factor B^{-2}. This also does not affect the final value of the Tate pairing $e_T(P, Q)$, since we use the same Lucas sequence for computing $\ell\widetilde{Q}$ and $\widetilde{P + \ell Q}$.

This give the following steps for the pairing: from $(j-1)Q$, jQ and $P + jQ$ we compute $2(j-1)Q$, $(2j-1)Q$, $P + (2j-1)Q$ or $(2j-1)Q$, $2jQ$ and $P + 2jQ$ depending on the binary decomposition of ℓ. We remark that at each step we do a doubling and two adding, and that we add the same point to the triple $(j-1)Q, jQ, P+jQ$. For instance in genus 1, we only have to compute $\frac{A^2}{B^2}(x^2-z^2)$ once, where $(x : z)$ are the coordinates of the doubled point.

The figure below summarises the cost per bit of computation of the Tate pairing with our algorithm in genus 1 and 2 with the following notations: S is for squaring, M is for general multiplication, m is for multiplication by a constant.

Tate pairing	First pairing $e(P, Q)$	Following pairings $e(P', Q)$
Dimension 1	8S+4m+4M	2S+1m+2M
Dimension 2	13S+12m+11M	4S+3m+4M

The algorithms that we have presented in this section are deterministic and generalize immediately to the higher dimension case. Usually when computing a pairing, the field of definition of Q has a smaller degree than the field of definition of P, so that at each step one adding and one doubling is done with points in the smaller field. We also remark that if we have to compute several pairings $e(P_1, Q)$, $e(P_2, Q)$, ... with the same Q, it makes sense to store the results of the computations of the jQ so that for the next pairings we only

have to compute the $P_i + jQ$. For instance when $g = 1$ if we store the $\log_2(\ell)$ coordinates $(x^2 + z^2, \frac{A^2}{B^2}(x^2 - z^2))$ of each doubling step, we can compute the subsequent pairings with only five multiplications at each step.

5.2 Kummer varieties

Let A be a principally polarized abelian variety of dimension g defined by $\Omega \in \mathbb{H}_g$. As we have seen in the introduction, the level 2 theta functions defined by Ω give a projective embedding of the Kummer variety associated to a A. We recall that the Kummer variety $\mathscr{K}_A$ of A is the quotient of A by the action of the automorphism -1 of A. Let $\zeta : A \to \mathscr{K}_A$ be the natural projection. In the following, if $P \in A(\overline{K})$ we denote by $\overline{P}$ its image by ζ. The construction of $\mathscr{K}_A$ does not preserve the group structure of A. Nonetheless, we remark that from the data of $\overline{P} \in \mathscr{K}_A(K)$ one can compute $2\overline{P}$ without ambiguity, and from the data of $\overline{P}$, $\overline{Q}$ and $\overline{P - Q}$ one can compute $\overline{P + Q}$. As a consequence, $\mathscr{K}_A$ inherits from A of an action of $\mathbb{Z}$ on its points which can be computed by a Montgomery ladder like algorithm.

Let e be a pairing on A, and let $\overline{K}_0^*$ be the quotient of $\overline{K}^*$ by the action of the automorphism -1. Let $\zeta_0 : \overline{K}^* \to \overline{K}_0^*$ be the natural projection. The pairing e gives a well defined application $\overline{e} : \mathscr{K}_A(\overline{K}) \times \mathscr{K}_A(\overline{K}) \to \overline{K}_0^*$, $(\overline{P}, \overline{Q}) \mapsto \zeta_0(e(P, Q))$. It is easily seen that the elements of $\overline{K}_0^*$ are in bijection with the set $S = \{x + 1/x, x \in \overline{K}^*\}$. Identifying $\overline{K}_0^*$ with S, the application ζ_0 is given by $\zeta_0(x) = x + 1/x$, $x \in \overline{K}^*$ from which we deduce the expression of $\overline{e} : (\overline{P}, \overline{Q}) \mapsto e(P, Q) + e(-P, Q)$. This pairing has been introduced in [3]. In the following, if e is a pairing, we say that $\overline{e}$ is the symmetric pairing associated to e. The symmetric pairing $\overline{e}$ can be seen as a version of e for compressed coordinates as it takes as input points with 2^g coordinates rather than 4^g.

Its cryptographic relevance comes from the compatibility of $\overline{e}$ with the $\mathbb{Z}$-set structures of $\mathscr{K}_A$ and $\overline{K}_0^*$: for all $\lambda, \mu \in \mathbb{Z}$, $\overline{P}, \overline{Q} \in \mathscr{K}_A$, we have $\overline{e}(\lambda.\overline{P}, \mu.\overline{Q}) = (\lambda\mu).\overline{e}(\overline{P}, \overline{Q})$. In [3], the authors give an algorithm based on Lucas sequences to compute the action of $\mathbb{Z}$ on $\overline{K}_0$ for certain finite fields. Here we would like to emphasize that the compatibility of the $\mathbb{Z}$-structure of $\mathscr{K}_A$ and $\overline{K}_0$ is also algorithmic. It comes from the fact and on any quotient of an algebraic group by the automorphism -1 there exists a natural Montgomery ladder algorithm to compute the resulting $\mathbb{Z}$-action. In the case of $\overline{K}_0$ we obtain very simple and general formulas. For $x \in \overline{K}$, and $i, j \in \mathbb{Z}$, we have

$$(x^i + \frac{1}{x^i})^2 = (x^{2i} + \frac{1}{x^{2i}} + 2); \quad (x^i + \frac{1}{x^i})(x^j + \frac{1}{x^j}) = (x^{i+j} + \frac{1}{x^{i+j}}) + (x^{i-j} + \frac{1}{x^{i-j}}).$$

We have seen that the codomain of the Tate pairing e_T is the multiplicative group $K^*/K^{*\ell}$. Again, we can take the quotient of this group by the action of (-1) on it, denote it by $(K^*/K^{*\ell})_0$. It is clear that there is a bijection between the set $(K^*/K^{*\ell})_0$ and the set $S_T = \{x + 1/x, x \in K_T\}$ where K_T is a set of representatives of $K^*/K^{*\ell}$. Moreover, one can compute the $\mathbb{Z}$-action on such representatives using the preceding algorithm.

Initialisation phase We suppose that we know the level 2 coordinates $\theta_i(z_P)$ and $\theta_i(z_Q)$, $i \in Z(\overline{2})$ of P and Q. We may assume (by multiplying by a projective factor) that the values of the projective coordinates $(\theta_i(z_P))_{i\in Z(\overline{2})}$ and $(\theta_i(z_Q))_{i\in Z(\overline{2})}$ are in K. Using Theorem 1 and Theorem 3, we obtain that for a general choice of $\mathscr{K}_A$, it is possible to compute for all $i, j \in Z(\overline{2})$ and $\chi \in \hat{Z}(\overline{2})$ such that $\chi(i-j) = 1$, $\sum_{\eta\in Z(\overline{2})} \chi(\eta)\theta_{i+\eta}(z_P+z_Q)\theta_{j+\eta}(z_P+z_Q)$ from the inputs. By summing over the characters, we obtain for all $i, j \in Z(\overline{2})$

$$\kappa_{ij} = \theta_i(z_P+z_Q)\theta_j(z_P-z_Q) + \theta_j(z_P+z_Q)\theta_i(z_P-z_Q). \tag{19}$$

We suppose that $\theta_0(z_P+z_Q)\theta_0(z_P-z_Q) \neq 0$, if necessary by replacing the index 0 by another one. By rescaling the projective coordinates, we do our computations as if $\theta_0(z_P-z_Q) = 1$ hence we know $\theta_0(z_P+z_Q)$.

For $i \in Z(\overline{2})$, let $\mathfrak{P}_i(X) = X^2 - 2\frac{\kappa_{i0}}{\kappa_{00}}X + \frac{\kappa_{ii}}{\kappa_{00}}$. The roots of $\mathfrak{P}_i(X)$ are $\frac{\theta_i(z_P+z_Q)}{\theta_0(z_P+z_Q)}$, $\frac{\theta_i(z_P-z_Q)}{\theta_0(z_P-z_Q)}$. If P or Q is a point of 2-torsion, $\overline{P+Q} = \overline{P-Q} \in \mathscr{K}_A$ so each $\mathfrak{P}_i(X)$ has a double root. Otherwise, we may suppose that there exist $\alpha \in Z(\overline{2})$, $\alpha \neq 0$ such that the matrix $M = \begin{pmatrix} \theta_0(z_P+z_Q) & \theta_0(z_P-z_Q) \\ \theta_\alpha(z_P+z_Q) & \theta_\alpha(z_P-z_Q) \end{pmatrix}$ is invertible.

We can compute $\{\theta_\alpha(z_P+z_Q), \theta_\alpha(z_P-z_Q)\}$ by finding the roots of $\mathfrak{P}_\alpha(X)$. As by hypothesis, $P+Q, P-Q \in A(K)$, we deduce that these roots are in K. We fix an arbitrary ordering $(\theta_\alpha(z_P+z_Q), \theta_\alpha(z_P-z_Q))$ of these roots (depending on the ordering, we will compute $\overline{P-Q}$ or $\overline{P+Q}$).

We can then find $\{\theta_i(z_P+z_Q), \theta_i(z_P-z_Q)\}$ by solving the system

$$\begin{pmatrix} \theta_0(z_P+z_Q) & \theta_0(z_P-z_Q) \\ \theta_\alpha(z_P+z_Q) & \theta_\alpha(z_P-z_Q) \end{pmatrix} \begin{pmatrix} \theta_i(z_P-z_Q) \\ \theta_i(z_P+z_Q) \end{pmatrix} = \begin{pmatrix} \kappa_{i0} \\ \kappa_{i\alpha} \end{pmatrix}. \tag{20}$$

This method requires one square root.

Pairing computation phase Let $P \in A(K)/[\ell]A(K)$ and $Q \in A[\ell]$ and denote by $\overline{P}, \overline{Q}$ the corresponding points on $\mathscr{K}_A$. Denote by $\theta_i(z)$, $i \in Z(\overline{2})$, the level 2 theta functions associated to Ω. We present two methods to compute the symmetric Tate pairing.

A first method is to consider the formula $\overline{e}_T(\overline{P}, \overline{Q}) = e_T(P, Q) + e_T(P, -Q)$. We have explained in the last paragraph how to compute the set $S = \{\overline{P+Q}, \overline{P-Q}\}$ at the expence of a square root extraction. By choosing a point in S, we can use the algorithm from Section 5.1 to compute $e(P, Q)$ (resp $e(P, -Q)$). We can then compute $\overline{e}_T(P, Q) = e(P, Q) + e(P, -Q)$ with a simple division.

Another approach is to work in the algebra $\mathscr{A} = K[X]/(\mathfrak{P}_\alpha(X))$ for $\alpha \in Z(\overline{2})$ as before. We denote by g the unique automorphism of the algebra of $\mathscr{A}$ leaving K invariant and different from the identity. For each $i \in Z(\overline{2})$ by using equation (20) we can express $\theta_i(z_P+z_Q) = \gamma_i X + \delta_i$. (We can always compute an inverse of $\gamma X + \delta$ except when $-\delta/\gamma$ is a root of $\mathfrak{P}_\alpha$. But in this case we have found a root of $\mathfrak{P}_\alpha$ and we can use the first method.) Now, consider the vector $(T_j)_{j\in Z(\overline{2})}$ where

$T_0 = 1$, $T_\alpha = X$ and $T_j = \gamma_j X + \delta_j$. We compute $R = \text{ScalarMult}(T, Q, P, \ell)_i$. Then it is easily seen that

$$R + g.R = \text{ScalarMult}(P + Q, Q, P, \ell)_i + \text{ScalarMult}(P - Q, Q, P, \ell)_i.$$

By Proposition 2, and using the fact that $\theta_i(-z_Q) = \theta_i(z_Q)$ we have for $i \in Z(\overline{2})$ $\overline{e}_T(\overline{P}, \overline{Q}) = \frac{[\theta_i(\ell.z_Q + z_P) + \theta_i(-\ell.z_Q + z_P)]\theta_i(0)}{\theta_i(z_P)\theta_i(\ell.z_Q)}$. We can now compute

$$\overline{e}_T(P, Q) = \frac{[\text{ScalarMult}(P + Q, Q, P, \ell)_i + \text{ScalarMult}(P - Q, Q, P, \ell)_i]\theta_i(0)}{\theta_i(z_P)\text{ScalarMult}(Q, Q, 0, \ell)_i}, \tag{21}$$

By an application of Lemma 4, the result of (21) is a well defined element of $(K^*/K^{*\ell})_0$.

With this method, we have to compute 1 ScalarMult with value in $\mathscr{A}$ and 1 ScalarMult with value in K. It is interesing to note that it avoids the non determinism of the square root computation of the first method.

In some cryptographic applications, it is important to have a unique value as the result of the Tate pairing. In order to have this property, it is common to compose the Tate pairing with a ℓ^{th} root extraction on K which can be done in the case that K is a finite field by an exponentiation in K_0^*. This operation can be performed using the Montgomery ladder type algorithm presented above.

The symmetric Weil pairing computation Since we compute $\overline{P + Q}$ with the first method, we can compute the Weil pairing as in the level 4 case.

We explain how to compute it with the second method: let $P, Q \in A[\ell]$ and denote by $\overline{P}, \overline{Q}$ the corresponding points in $\mathscr{K}_A$. Denote by $\theta_i(z)$, $i \in Z(\overline{2})$ the level 2 theta functions associated to Ω. By Corollary 2, we have:

$$\overline{e}_W(\overline{P}, \overline{Q}) = \frac{\theta_i(z_Q)\theta_i(\ell.z_P)[\theta_i(\ell.z_Q + z_P)\theta_i(z_Q - \ell z_P) + \theta_i(\ell.z_Q - z_P)\theta_i(z_Q + \ell z_P)]}{\theta_i(z_P)\theta_i(\ell.z_Q)\theta_i(z_Q + \ell.z_P)\theta_i(z_Q - \ell.z_P)}. \tag{22}$$

The denominator of this expression can be easily computed from the knowledge of $\theta_i(z_Q)$, $\theta_i(\ell.z_Q)$, $\theta_i(z_P)$ and $\theta_i(\ell.z_P)$ by using the addition formula (1), and the numerator can be computed in the algebra $\mathscr{A}$ in the following way. Keeping the notations from above, we compute $R' = \text{ScalarMult}(T, Q, P, \ell)_i.\text{ScalarMult}(gT, P, Q, \ell)_i$. Then it is easily seen that

$$\begin{aligned} R' + g.R' = {} & \text{ScalarMult}(P + Q, Q, P, \ell)_i.\text{ScalarMult}(P - Q, P, Q, \ell)_i \\ & + \text{ScalarMult}(P - Q, Q, P, \ell)_i.\text{ScalarMult}(P + Q, P, Q, \ell)_i, \end{aligned} \tag{23}$$

which gives the numerator of (22).

6 An example in dimension 2

In this section we give an example of compution of the pairings on a dimension 2 Jacobian. Let H be the hyperelliptic curve over the prime field $\mathbb{F}_p$, $p = 331$, given

by the equation:

$$Y^2 = X^5 + 204X^4 + 198X^3 + 80X^2 + 179X.$$

Let J be the Jacobian of H. The cardinal of $J(\mathbb{F}_p)$ is $2^6 \cdot 1889$ (since we are in level 2, all the 2-torsion points of J are rational), so that we let $\ell = 1889$, and the embedding degree k corresponding to ℓ is 4. A theta null point of level 2 associated to J is given by $(328 : 213 : 75 : 1)$. Let $P = (255 : 89 : 30 : 1)$, we have $P \in J[\ell](\mathbb{F}_p)$. Let $\mathbb{F}_{p^k} \simeq \mathbb{F}_p(t)/(t^4 + 3t^2 + 290t + 3)$. We let Q be the $\mathbb{F}_{p^k}$-point of ℓ-torsion whose coordinates are:

$$(158t^3 + 67t^2 + 9t + 293 : 290t^3 + 25t^2 + 235t + 280 : 155t^3 + 84t^2 + 15t + 170 : 1).$$

We compute (and fix an arbitrary ordering):

$$P + Q = (217t^3 + 271t^2 + 33t + 303 : 308t^3 + 140t^2 + 216t + 312 : 274t^3 + 263t^2 + 284t + 302 : 1),$$
$$P - Q = (62t^3 + 16t^2 + 255t + 129 : 172t^3 + 157t^2 + 43t + 222 : 258t^3 + 39t^2 + 313t + 150 : 1).$$

Finally, we let $r = \frac{p^k - 1}{\ell} = 6354480$ and $\zeta = t^r$ be a primitive ℓ^{th}-root of unity. We then compute using the doubling and differential addition algorithms:

$$\ell\widetilde{P} = (12, 141, 31, 327) = 327.\widetilde{0},$$
$$\ell\widetilde{Q} = (21t^3 + 280t^2 + 101t + 180, 164t^3 + 311t^2 + 111t + 129,$$
$$137t^3 + 282t^2 + 123t + 134, 324t^3 + 17t^2 + 187t + 271) = (324t^3 + 17t^2 + 187t + 271).\widetilde{0},$$
$$\text{ScalarMult}(\widetilde{P+Q}, \widetilde{Q}, \widetilde{P}, \ell) = (45t^3 + 118t^2 + 219t + 308, 152t^3 + 97t^2 + 166t + 40,$$
$$200t^3 + 267t^2 + 201t + 192, 117t^3 + 42t^2 + 106t + 205) = (117t^3 + 42t^2 + 106t + 205).\widetilde{P},$$
$$\text{ScalarMult}(\widetilde{P+Q}, \widetilde{P}, \widetilde{Q}, \ell) = (50t^3 + 31t^2 + 84t + 309, 168t^3 + 196t^2 + 275t + 234,$$
$$67t^3 + 186t^2 + 159t + 102, 243t^3 + 320t^2 + 222t + 200) = (243t^3 + 320t^2 + 222t + 200).\widetilde{Q}.$$

We then compute (following the previous ordering):

$$e_W(P, Q) = \frac{243t^3 + 320t^2 + 222t + 200}{327} \cdot \frac{324t^3 + 17t^2 + 187t + 271}{117t^3 + 42t^2 + 106t + 205} = \zeta^{-1},$$
$$e_T(P, Q) = \left(\frac{117t^3 + 42t^2 + 106t + 205}{324t^3 + 17t^2 + 187t + 271}\right)^r = \zeta^{1068},$$
$$e_T(Q, P) = \left(\frac{243t^3 + 320t^2 + 222t + 200}{327}\right)^r = \zeta^{1184}.$$

Here the Tate pairings are normalized by taking their $r = (p^k - 1)/\ell$-power. The symmetric pairings are then given by $\overline{e}_W(P, Q) = 61t^3 + 285t^2 + 196t + 257$ and $\overline{e}_T(P, Q) = 194t^3 + 163t^2 + 97t + 164$.

7 Conclusion

In this paper, we have presented an algorithm based on theta functions to compute Weil and Tate pairings. It would be interesting to carry out a fine grained study of the efficiency of our algorithm depending on the target implementation (software, hardware etc.) and to compare it with existing implementations based on Miller's algorithm.

Acknowledgement

The authors of this paper would like to thank anonymous referees for their careful reading and helpful comments on an earlier version of the paper.

References

1. Christina Birkenhake and Herbert Lange. *Complex abelian varieties*, volume 302 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2004.
2. Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Frederik Vercauteren, editors. *Handbook of elliptic and hyperelliptic curve cryptography*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2006.
3. Steven Galbraith and Xibin Lin. Computing pairings using x-coordinates only. *Designs, Codes and Cryptography*, 2008.
4. P. Gaudry. Fast genus 2 arithmetic based on Theta functions. *J. of Mathematical Cryptology*, 1:243–265, 2007.
5. Pierrick Gaudry and David Lubicz. The arithmetic of characteristic 2 Kummer surfaces and of elliptic Kummer lines. *Finite Fields Appl.*, 15(2):246–260, 2009.
6. Jun-ichi Igusa. *Theta functions*. Springer-Verlag, New York, 1972. Die Grundlehren der mathematischen Wissenschaften, Band 194.
7. Shoji Koizumi. Theta relations and projective normality of Abelian varieties. *Amer. J. Math.*, 98(4):865–889, 1976.
8. Serge Lang. Reciprocity and correspondences. *Amer. J. Math.*, 80:431–440, 1958.
9. Stephen Lichtenbaum. Duality theorems for curves over p-adic fields. *Invent. Math.*, 7:120–136, 1969.
10. David Lubicz and Damien Robert. Computing isogenies between abelian varieties, 2010. http://arxiv.org/abs/1001.2016.
11. D. Mumford. On the equations defining abelian varieties. I. *Invent. Math.*, 1:287–354, 1966.
12. D. Mumford. On the equations defining abelian varieties. II. *Invent. Math.*, 3:75–135, 1967.
13. D. Mumford. *Abelian varieties*. Tata Institute of Fundamental Research Studies in Mathematics, No. 5. Published for the Tata Institute of Fundamental Research, Bombay, 1970.
14. David 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.
15. David 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.
16. Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986. Corrected reprint of the 1986 original.