Tate Pairing Computation on Jacobi's Elliptic Curves*

Sylvain Duquesne[1] and Emmanuel Fouotsa[2]

[1] IRMAR, UMR CNRS 6625, Université Rennes 1,
Campus de Beaulieu 35042 Rennes cedex, France
sylvain.duquesne@univ-rennes1.fr

[2] Département de Mathématiques, Université de Yaoundé 1
Faculté des Sciences, BP 812 Yaoundé, Cameroun
emmanuel.fouotsa@prmais.org

Abstract. We propose for the first time the computation of the Tate pairing on Jacobi intersection curves. For this, we use the geometric interpretation of the group law and the quadratic twist of Jacobi intersection curves to obtain a doubling step formula which is efficient but not competitive compared to the case of Weierstrass curves, Edwards curves and Jacobi quartic curves. As a second contribution, we improve the doubling and addition steps in Miller's algorithm to compute the Tate pairing on the special Jacobi quartic elliptic curve $Y^2 = dX^4 + Z^4$. We use the birational equivalence between Jacobi quartic curves and Weierstrass curves together with a specific point representation to obtain the best result to date among all the curves with quartic twists. In particular for the doubling step in Miller's algorithm, we obtain a theoretical gain between 6% and 21%, depending on the embedding degree and the extension field arithmetic, with respect to Weierstrass curves [6] and Jacobi quartic curves [23].

Keywords: Jacobi quartic curves, Jacobi intersection curves, Tate pairing, Miller function, group law, geometric interpretation, birational equivalence.

1 Introduction

While first used to solve the discrete logarithm problem on elliptic curve group [20,12], bilinear pairings are now useful to construct many public key protocols for which no other efficient implementation is known [18,3]. A survey of some of these protocols can be found in [9]. The efficient computation of pairings depends on the model chosen for the curve. Pairing computation on the Edwards model of elliptic curves have been done successively in [7], [17] and [1]. The recent results on pairing computation using elliptic curves of Weierstrass form can be found in [5,6]. Recently in [23] Wang et al. have computed the Tate pairing on

* This work was supported in part by French ANR projects no. 07-BLAN-0248 "ALGOL" and 09-BLAN-0020-01 "CHIC".

M. Abdalla and T. Lange (Eds.): Pairing 2012, LNCS 7708, pp. 254–269, 2013.

Jacobi quartic elliptic curves using the geometric interpretation of the group law. In this paper, we focus on Jacobi intersection curves and the special Jacobi quartic elliptic curves $Y^2 = dX^4 + Z^4$ over the field of large characteristic p not congruent to 3 modulo 4.

We use the geometric interpretation of the group law of Jacobi intersection curves to obtain the first explicit formulas for the Miller function in Tate pairing computation in this case. For pairing computation with even embedding degree, we define and use the quadratic twist of this curve. This allows the Miller doubling stage to be slightly more efficient than when using Weierstrass curves, Edwards curves and Jacobi quartic curves. Moreover, for pairing computation with embedding degree divisible by 4, we define and use the quartic twist of the curve $Y^2 = dX^4 + Z^4$. Our result is an improvement of the result obtained by Wang et al. in [23] and is to our knowledge the best result to date on pairing computation among all curves with quartic twists.

The rest of this paper is organized as follows: Section 2 gives a background on the two forms of Jacobi elliptic curves mentioned above, including background on pairings that we will use in the remainder of the paper. In Section 3, we first look for Miller functions on Jacobi intersection curves using the geometric interpretation of the group law and then compute the Tate pairing on this curve. Section 4 presents the computation of the Tate pairing on the Jacobi quartic curve mentioned above using birational equivalence. Finally, we conclude in Section 5.

2 Background on Pairings and on Jacobi's Elliptic Curves

In this section we briefly review pairings on elliptic curves, Jacobi intersection curves and the Jacobi quartic curves. We also define twists of Jacobi's curves.

2.1 The Tate Pairing

In this section E is an elliptic curve defined over a finite field $\mathbb{F}_q$. The neutral element is denoted O. Let r be a large prime divisor of the group order $\sharp E(\mathbb{F}_q)$ and k the embedding degree of E with respect to r, i.e the smallest integer such that r divides $q^k - 1$. Consider a point $P \in E(\mathbb{F}_q)[r]$ and the function $f_{r,P}$ with divisor $\mathrm{Div}(f_{r,P}) = r(P) - r(O)$. Let $Q \in E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})$ and μ_r be the group of r-th roots of unity in $\mathbb{F}_{q^k}^*$. The reduced Tate pairing e_r is defined as

$$e_r(P, Q) = f_{r,P}(Q)^{\frac{q^k-1}{r}} \in \mu_r.$$

If one knows the function $h_{R,S}$ such that $\mathrm{Div}(h_{R,S}) = (R)+(S)-(S+R)-(O)$ where R and S are two points of E, then the Tate pairing can be computed in an iterative way by Miller's algorithm [22] in Algorithm 1. This algorithm computes in the i-th iteration the evaluation at a point Q of the function $f_{i,P}$ having divisor $\mathrm{Div}(f_{i,P}) = i(P) - ([i]P) - (i-1)(O)$, called Miller's function.

Algorithm 1. Miller Algorithm
Input : $P \in E(\mathbb{F}_q)[r]$, $Q \in E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})$ $r = (r_{n-1}, r_{n-2}, ...r_1, r_0)_2$ with $r_{n-1} = 1$. **Output:** The Tate pairing of P and Q : $f_{r,P}(Q)^{\frac{q^k-1}{r}}$
1.Set $f \leftarrow 1$ and $R \leftarrow P$ 2.For $i = n-2$ down to 0 Set $f \leftarrow f^2 \cdot h_{R,R}(Q)$ and $R \leftarrow 2R$ if $r_i = 1$ then $f \leftarrow f \cdot h_{R,P}(Q)$ and $R \leftarrow R + P$ 3. $f \leftarrow f^{\frac{q^k-1}{r}}$

After $n-1$ iterations, the evaluation at Q of the function f having divisor $r(P)-r(O)$ is obtained. More informations on pairings can be found in [13] and [8].

Notation 1. *The following notations will be permanently used in this work.*
m, s : cost of multiplication and squaring in the base field $\mathbb{F}_q$
m_c: cost of the multiplication by the constant c in $\mathbb{F}_q$
M, S: cost of multiplication and squaring in the extension field $\mathbb{F}_{q^k}$

2.2 The Jacobi Intersection Curves

A Jacobi intersection form elliptic curve over $\mathbb{F}_q$ is defined by

$$E_a : \begin{cases} x^2 + y^2 = 1 \\ ax^2 + z^2 = 1 \end{cases} \quad \text{where } a \text{ belongs to } \mathbb{F}_q \text{ and } a(a-1) \neq 0.$$

The Jacobi intersection curve E_a is isomorphic to an elliptic curve on the Weierstrass form $y^2 = x(x-1)(x-a)$. The affine version of the unified addition formulas is given in [4] by $(x_3, y_3, z_3) = (x_1, y_1, z_1) + (x_2, y_2, z_2)$ such that :

$$x_3 = \frac{x_1y_2z_2 + y_1z_1x_2}{y_2^2 + z_1^2x_2^2}, y_3 = \frac{y_1y_2 - x_1z_1x_2z_2}{y_2^2 + z_1^2x_2^2}, z_3 = \frac{z_1z_2 - ax_1y_1x_2y_2}{y_2^2 + z_1^2x_2^2}$$

See [4,10] for further results on Jacobi intersection curves. An affine point (x, y, z) on a Jacobi intersection curves is represented by the projective homogeneous coordinates (X : Y : Z : T) satisfying

$$\begin{cases} X^2 + Y^2 = T^2 \\ aX^2 + Z^2 = T^2 \end{cases}$$

and $(x, y, z) = (X/T, Y/T, Z/T)$ with $T \neq 0$. The negative of $(X : Y : Z : T)$ is $(-X : Y : Z : T)$. The neutral element $P_0 = (0, 1, 1)$ is represented by $(0 : 1 : 1 : 1)$. By setting $T = 0$ we get four points at infinity: $\Omega_1 = (1 : s : t : 0)$, $\Omega_2 = (1 : s : -t : 0)$, $\Omega_3 = (1 : -s : t : 0)$ and $\Omega_4 = (1 : -s : -t : 0)$ where $1 + s^2 = 0$ and $a + t^2 = 0$.

Group Law on Jacobi Intersection Curves. The first formulas for addition law on points of Jacobi intersection curves given by Chudnovsky and Chudnovsky in [4] used projective homogeneous coordinates. In [15], Hisil et al. improved these formulas by representing points as a sextuplet $(X : Y : Z : T : XY : ZT)$ as follows:

The sum of the points represented by $(X_1 : Y_1 : Z_1 : T_1 : U_1 : V_1)$ and $(X_2 : Y_2 : Z_2 : T_2 : U_2 : V_2)$ where $U_1 = X_1Y_1$; $V_1 = Z_1T_1$ and $U_2 = X_2Y_2$; $V_2 = Z_2T_2$ is the point $(X_3 : Y_3 : Z_3 : T_3 : U_3 : V_3)$ such that:

$$\begin{aligned}
X_3 &= X_1T_1Y_2Z_2 + Y_1Z_1X_2T_2,\\
Y_3 &= Y_1T_1Y_2T_2 - X_1Z_1X_2Z_2,\\
Z_3 &= Z_1T_1Z_2T_2 - aX_1Y_1X_2Y_2,\\
T_3 &= T_1^2Y_2^2 + Z_1^2X_2^2,\\
U_3 &= X_3Y_3,\\
V_3 &= Z_3T_3.
\end{aligned}$$

with the algorithm:
$E \leftarrow X_1Z_2; F \leftarrow Y_1T_2; G \leftarrow Z_1X_2; H \leftarrow T_1Y_2; J \leftarrow U_1V_2; K \leftarrow V_1U_2;$
$X_3 \leftarrow (H + F)(E + G) - J - K; Y_3 \leftarrow (H + E)(F - G) - J + K;$
$Z_3 \leftarrow (V_1 - aU_1)(U_2 + V_2) + aJ - K; T_3 \leftarrow (H + G)^2 - 2K; U_3 \leftarrow X_3Y_3; V_3 \leftarrow Z_3T_3.$
This point addition costs $11m + 1s + 2m_a$.

The doubling of the point represented by $(X_1 : Y_1 : Z_1 : T_1 : U_1 : V_1)$ is the point $(X_3 : Y_3 : Z_3 : T_3 : U_3 : V_3)$ such that:

$$\begin{aligned}
X_3 &= 2X_1Y_1Z_1T_1,\\
Y_3 &= -Z_1^2T_1^2 - aX_1^2Y_1^2 + 2(X_1^2Y_1^2 + Y_1^4),\\
Z_3 &= Z_1^2T_1^2 - aX_1^2Y_1^2,\\
T_3 &= Z_1^2T_1^2 + aX_1^2Y_1^2,\\
U_3 &= X_3Y_3,\\
V_3 &= Z_3T_3.
\end{aligned}$$

with the algorithm: $E \leftarrow V_1^2; F \leftarrow U_1^2; G \leftarrow aF; T_3 \leftarrow E + G; Z_3 \leftarrow E - G; Y_3 \leftarrow 2(F + Y_1^4) - T_3; X_3 \leftarrow (U_1 + V_1)^2 - E - F; U_3 \leftarrow X_3Y_3; V_3 \leftarrow Z_3T_3.$
This point doubling costs $2m + 5s + 1m_a$.

2.3 The Jacobi Quartic Curve

A Jacobi quartic elliptic curve over a finite field $\mathbb{F}_q$ is defined by $E_d : y^2 = dx^4 + 2\delta x^2 + 1$ with discriminant $\triangle = 256d(\delta^2 - d)^2 \neq 0$. In [2] Billet and Joye proved that if $E : y^2 = x^3 + ax + b$ has a point of order 2 denoted $(\theta, 0)$ then E is birationally equivalent to the Jacobi quartic:

$$Y^2 = dX^4 - 2\delta X^2Z^2 + Z^4$$

where $d = -(3\theta^2 + 4a)/16$ and $\delta = 3\theta/4$. In the remainder of this paper, we will focus our interest on the special Jacobi quartic curve $E_d : Y^2 = dX^4 + Z^4$

because this curve has interesting properties such as quartic twist which contribute to an efficient computation of pairing.
The affine model of this curve is $y^2 = dx^4 + 1$ with $(x, y) = (\frac{X}{Z}, \frac{Y}{Z^2})$. The special Jacobi quartic curve E_d is birationally equivalent to the Weierstrass curve $E : y^2 = x^3 - 4dx$ using the maps

$$\varphi \begin{cases} (0:1:1) \longmapsto O \\ (0:-1:1) \longmapsto (0,0) \\ (X:Y:Z) \longmapsto \left(2\frac{(Y+Z^2)}{X^2}, 4\frac{Z(Y+Z^2)}{X^3}\right) \end{cases} ; \varphi^{-1} \begin{cases} (0,0) \longmapsto (0:-1:1) \\ (x,y) \longmapsto (2x : 2x^3 - y^2 : y) \\ O \longmapsto (0:1:1) \end{cases}$$

Group Law on the Curve $Y^2 = dX^4 + Z^4$. Here we specialize formulas for point doubling and point addition on the curve E_d from the formulas on the affine model given in [16].

The point addition $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$ on the affine model of E_d is given by:

$$x_3 = \frac{x_1^2 - x_2^2}{x_1 y_2 - y_1 x_2} \text{ and } y_3 = \frac{(x_1 - x_2)^2}{(x_1 y_2 - y_1 x_2)^2}(y_1 y_2 + 1 + d x_1^2 x_2^2) - 1.$$

By replacing x_1 by $\frac{X_1}{Z_1}$, x_2 by $\frac{X_2}{Z_2}$, y_1 by $\frac{Y_1}{Z_1^2}$, y_2 by $\frac{Y_2}{Z_2^2}$, $x_3 = \frac{X_3}{Z_3}$ and y_3 by $\frac{Y_3}{Z_3^2}$ a simple calculation yields to

$$X_3 = X_1^2 Z_2^2 - Z_1^2 X_2^2,\ Z_3 = X_1 Z_1 Y_2 - X_2 Z_2 Y_1,$$
$$Y_3 = (X_1 Z_2 - X_2 Z_1)^2 (Y_1 Y_2 + (Z_1 Z_2)^2 + d(X_1 X_2)^2) - Z_3^2.$$

The point doubling $(x_3, y_3) = 2(x_1, y_1)$ on the affine model of E_d is given by :

$$x_3 = \frac{2y_1}{2 - y_1^2} x_1 \text{ and } y_3 = \frac{2y_1}{2 - y_1^2}\left(\frac{2y_1}{2 - y_1^2} - y_1\right) - 1.$$

By replacing x_1 by $\frac{X_1}{Z_1}$, y_1 by $\frac{Y_1}{Z_1^2}$, x_3 by $\frac{X_3}{Z_3}$ and y_3 by $\frac{Y_3}{Z_3^2}$, a simple calculation yields to:

$$X_3 = 2X_1 Y_1 Z_1,$$
$$Z_3 = Z_1^4 - dX_1^4,$$
$$Y_3 = 2Y_1^4 - Z_3^2.$$

2.4 Twists of Jacobi Curves

A twist of an elliptic curve E defined over a finite field $\mathbb{F}_q$ is an elliptic curve E' over $\mathbb{F}_q$ that is isomorphic to E over an algebraic closure of $\mathbb{F}_q$. The smallest integer t such that E and E' are isomorphic over $\mathbb{F}_{q^t}$ is called the degree of the twist. The points input of a pairing on a curve of embedding degree k take the form $P \in E(\mathbb{F}_q)$ and $Q \in E(\mathbb{F}_{q^k})$. However many authors have shown that one can use the twist of a curve to take the input $Q \in E'(\mathbb{F}_{q^{k/t}})$ where operations can be performed more efficiently [11].

Let $E : y^2 = x^3 + ax + b$ over $\mathbb{F}_q$ be an elliptic curve in Weierstrass form. The equation defining the twist E' has the form $y^2 = x^3 + a\omega^4 x + b\omega^6$ where $\omega \in \mathbb{F}_{q^k}$ and the isomorphism between E' and E is

$$\begin{array}{rccc} \psi: & E' & \longrightarrow & E \\ & (x', y') & \longmapsto & (x'/\omega^2, y'/\omega^3). \end{array}$$

Some details on twists can be found in [6].

Quadratic Twist of Jacobi Intersection Curves

Definition 1. *Let the Jacobi intersection curve E_a defined as in Subsection 2.2. A quadratic ($t = 2$) twist of E_a over the extension $\mathbb{F}_{q^{k/2}}$ of $\mathbb{F}_q$ (k even) is the curve*

$$\begin{cases} \delta^2 x^2 + y^2 = 1 \\ a\delta^2 x^2 + z^2 = 1 \end{cases}$$

Where $\{1, \delta\}$ is the basis of $\mathbb{F}_{q^k}$ as a $\mathbb{F}_{q^{k/2}}$-vector space and $\delta^2 \in \mathbb{F}_{q^{k/2}}$.

Proposition 1. *Let $E_{a,\delta}$ over $\mathbb{F}_{q^{k/2}}$ be a quadratic twist of E_a. The $\mathbb{F}_{q^k}$ isomorphism between $E_{a,\delta}$ and E_a is given by*

$$\begin{array}{rccc} \psi: & E_{a,\delta} & \rightarrow & E_a \\ & (x, y, z) & \mapsto & (\delta x, y, z) \end{array}$$

Twist of Jacobi Quartic Curves. To obtain the twist of the Jacobi quartic curve defined by $Y^2 = dX^4 + Z^4$, we use the birational maps defined in Subsection 2.3 and the twist of Weierstrass curves defined at the beginning of this subsection.

Definition 2. *A quartic twist of the Jacobi quartic curve $Y^2 = dX^4 + Z^4$ over the extension $\mathbb{F}_{q^{k/4}}$ of $\mathbb{F}_q$ is the curve*

$$E_{d,\omega} : Y^2 = d\omega^4 X^4 + Z^4$$

where $\omega \in \mathbb{F}_{q^k}$ is such that $\omega^2 \in \mathbb{F}_{q^{k/2}}$, $\omega^3 \in \mathbb{F}_{q^k} \backslash \mathbb{F}_{q^{k/2}}$ and $\omega^4 \in \mathbb{F}_{q^{k/4}}$. That is $\{1, \omega, \omega^2, \omega^3\}$ is a basis of $\mathbb{F}_{q^k}$ as a vector space over $\mathbb{F}_{q^{k/4}}$.

Proposition 2. *Let $E_{d,\omega}$ over $\mathbb{F}_{q^{k/4}}$ be a twist of E_d. The $\mathbb{F}_{q^k}$ isomorphism between $E_{a,\delta}$ and E_a is given by*

$$\begin{array}{rccc} \psi: & E_{d,\omega} & \rightarrow & E_d \\ & (X : Y : Z) & \mapsto & \left(\frac{X}{\omega^2} : \frac{Y}{\omega^6} : \frac{Z}{\omega^3}\right) \end{array}$$

3 Pairing on Jacobi Intersection Curves

3.1 Geometric Interpretation of the Group Law

The aim of this section is to find the function $h_{R,S}$. For this, we give more details on the geometric interpretation in [21] of the group law of Jacobi intersection curves. We consider $P_0 = (0, 1, 1)$ the $\mathbb{F}_q$-rational point on the curve which shall be the identity. Three points P_1, P_2, P_3 of the curve will sum to zero if and only if the four points P_0, P_1, P_2, P_3 are coplanar. The negation of a point $-P_1$ is given as the residual intersection of the plane through P_1 containing the tangent line to the curve at P_0.

Let $f_{P_1,P_2}(x,y,z) = 0$ be the equation of the plane defined by the points P_1, P_2 and P_0. If $P_1 = P_2$ take f_{P_1,P_1} to be the tangent plane to the curve at P_1 passing through P_0. This plane intersects E_a at $R = -(P_1 + P_2) = -P_3$. Then $\mathrm{Div}(f_{P_1,P_2}) = (P_1)+(P_2)+(R)+(P_0)-(\Omega)$ where $\Omega = (\Omega_1)+(\Omega_2)+(\Omega_3)+(\Omega_4)$ is a rational divisor.

Let $g_R(x,y,z) = 0$ be the equation of the plane passing through R and containing the tangent line to the curve at P_0. This plane intersects the curve E_a at the point $-R$. Then $\mathrm{Div}(g_R) = (R) + 2(P_0) + (-R) - (\Omega)$
Define

$$h_{P_1,P_2} = \frac{f_{P_1,P_2}}{g_R}$$

then

$$\mathrm{Div}\ (h_{P_1,P_2}) = (P_1) + (P_2) - (P_1 + P_2) - (P_0)$$

Theorem 1. *The functions f_{P_1,P_2} and g_R are defined as follows :*

$$f_{P_1,P_2}(x,y,z) = \alpha x + \beta(y-1) + \gamma(z-1)$$

with:

$$\alpha = \begin{cases} (z_2-1)(y_1-1) - (y_2-1)(z_1-1) & \text{if } P_1 \neq P_2, \\ x_1(-a(y_1-1)+z_1-1) & \text{if } P_1 = P_2. \end{cases}$$
$$\beta = \begin{cases} x_2(z_1-1) - x_1(z_2-1) & \text{if } P_1 \neq P_2, \\ y_1(z_1-1) & \text{if } P_1 = P_2. \end{cases}$$
$$\gamma = \begin{cases} x_1(y_2-1) - x_2(y_1-1) & \text{if } P_1 \neq P_2, \\ -z_1(y_1-1) & \text{if } P_1 = P_2. \end{cases}$$

and

$$g_{P_3}(x,y,z) = (z_3-1)(y-1) + (1-y_3)(z-1).$$

Proof 1.
1. Let $f_{P_1,P_2}(x,y,z) = \alpha x + \beta y + \gamma z + \theta = 0$ be the equation of the plane. Because $P_0 = (0,1,1)$ belongs to this plane we have $\theta = -\beta - \gamma$. Thus $f_{P_1,P_2}(x,y,z) = \alpha x + \beta y + \gamma z - \beta - \gamma = 0$.
If P_1 and P_2 are different then by evaluating the previous equation at the points P_1 and P_2 we obtain two linear equations in α, β and γ :

$$\alpha x_1 + \beta(y_1-1) + \gamma(z_1-1) = 0$$

$$\alpha x_2 + \beta(y_2-1) + \gamma(z_2-1) = 0$$

with the solutions

$$\alpha = \begin{vmatrix} y_1-1 & z_1-1 \\ y_2-1 & z_2-1 \end{vmatrix},\ \beta = \begin{vmatrix} z_1-1 & x_1 \\ z_2-1 & x_2 \end{vmatrix},\ \gamma = \begin{vmatrix} x_1 & y_1-1 \\ x_2 & y_2-1 \end{vmatrix}$$

If $P_1 = P_2 \neq P_0$ then the tangent line to the curve at P_1 is collinear to the vector $(y_1z_1, -x_1z_1, -ax_1y_1) = (x_1, y_1, 0) \wedge (ax_1, 0, z_1)$. Thus one can take $\overrightarrow{n} = x_1(-a(y_1-1) + z_1 - 1), y_1(z_1-1), -z_1(y_1-1)) = (\alpha, \beta, \gamma)$ as a normal vector to the plane.

2. Assume that $g_R(x, y, z) = ax + by + cz + d = 0$. The tangent line to the curve at P_0 is the intersection of the planes $v = 1$ and $w = 1$. Thus P_0 and one arbitrary point $(1, 1, 1)$ on the line belong to the plane. This implies that $a = 0$ and $b = -c - d$ such that $g_R(x, y, z) = c(-y + z) + d(-y + 1) = 0$. Because $R = (u, v, w)$ belongs to the plane, we have $c = d(-v + 1)/(v - w)$ and by replacing this value of c in $g_R(x, y, z) = c(-y+z) + d(-y+1) = 0$ we obtain the desired result.

3.2 Miller Function on Jacobi Intersection Curves

In this section we show how to use the geometric interpretation of the group law to compute pairings. We assume that k is even. Let $(x_Q, y_Q, z_Q) \in E_{a,\delta}(\mathbb{F}_{q^{k/2}})$. Twisting (x_Q, y_Q, z_Q) with δ ensures that the second argument of the pairing is on $E_a(\mathbb{F}_{q^k})$ and is of the form $Q = (\delta x_Q, y_Q, z_Q)$, where x_Q, y_Q and z_Q are in $\mathbb{F}_{q^{k/2}}$.

Addition. By Theorem 1,

$$\begin{aligned} h_{P_1,P_2}(\delta x_Q, y_Q, z_Q) &= \frac{\alpha x_Q\delta + \beta(y_Q-1) + \gamma(z_Q-1)}{(z_3-1)y_Q + (1-y_3)z_Q + (y_3-z_3)} \\ &= \frac{z_Q-1}{(z_3-1)y_Q + (1-y_3)z_Q + (y_3-z_3)}\left(\alpha\frac{x_Q}{z_Q-1}\delta + \beta\frac{y_Q-1}{z_Q-1} + \gamma\right) \end{aligned}$$

To obtain the expression of this function in projective coordinates X, Y, Z and T, we set $x_i = \frac{X_i}{T_i}$, $y_i = \frac{Y_i}{T_i}$ and $z_i = \frac{Z_i}{T_i}$; i=1, 2, 3. The point Q can be maintained in affine coordinates ($T_Q = 1$). The function becomes:

$$\begin{aligned} h_{P_1,P_2}(\delta x_Q, y_Q, z_Q) &= \frac{T_3(z_Q-1)\left(\alpha'\frac{x_Q}{z_Q-1}\delta + \beta'\frac{y_Q-1}{z_Q-1} + \gamma'\right)}{T_1T_2[(Z_3-T_3)y_Q + (T_3-Y_3)z_Q + (Y_3-Z_3)]} \\ &= \frac{T_3(z_Q-1)}{T_1T_2[(Z_3-T_3)y_Q + (T_3-Y_3)z_Q + (Y_3-Z_3)]}(\alpha' M_1\delta + \beta' N_1 + \gamma') \end{aligned}$$

where $\alpha' = (Z_2-T_2)(Y_1-T_1)-(Y_2-T_2)(Z_1-T_1)$, $\beta' = X_2(Z_1-T_1)-X_1(Z_2-T_2)$, $\gamma' = X_1(Y_2 - Z_2) - X_2(Y_1 - T_1)$ and $M_1 = \frac{x_Q}{z_Q-1}$, $N_1 = \frac{y_Q-1}{z_Q-1}$.

we can easily see that $\frac{T_3(z_Q-1)}{T_1T_2[(Z_3-T_3)y_Q+(T_3-Y_3)z_Q+(Y_3-Z_3)]} \in \mathbb{F}_{q^{k/2}}$ so it can be discarded in pairing computation since the final output of Miller loop is raised to the power $(q^k - 1)/r$ and $q^{k/2} - 1$ is a factor of $(q^k - 1)/r$ since k is even. Thus we only have to evaluate

$$(\alpha' M_1)\delta + \beta' N_1 + \gamma'$$

Since $Q = (\delta x_Q, y_Q, z_Q)$ is fixed during pairing computation, the quantities $M_1 = \frac{x_Q}{z_Q-1}$, $N_1 = \frac{y_Q-1}{z_Q-1}$ can be precomputed in $\mathbb{F}_{q^{k/2}}$. Each of the multiplication of α' by $M_1 \in \mathbb{F}_{q^{k/2}}$ and β' by $N_1 \in \mathbb{F}_{q^{k/2}}$ costs $\frac{k}{2}m$. Computing the coefficients α' , β' and γ' requires $6m$ and the point addition in Subsection 2.2 requires $11m + 1s + 2c$. Thus the point addition and Miller value computation require a total of $1M + (k+17)m + 1s + 2m_a$. The point P_2 is not changed during pairing computation and can be given in affine coordinates i.e. $T_2 = 1$. Applying such a mixed addition reduces the cost to $1M + (k+16)m + 1s + 2m_a$.

Doubling. By Theorem 1,

$$\begin{aligned} h_{P_1,P_1}(\delta x_Q, y_Q, z_Q) &= \frac{x_1(-a(y_1-1)+z_1-1)x_Q\delta + y_1(z_1-1)(y_Q-1) - z_1(y_1-1)(z_Q-1)}{(z_3-1)y_Q+(1-y_3)z_Q+(y_3-z_3)} \\ &= \frac{x_1(-a(y_1-1)+z_1-1)x_Q\delta + y_1(z_1-1)(y_Q-1) - z_1(y_1-1)(z_Q-1)}{(z_3-1)y_Q+(1-y_3)z_Q+(y_3-z_3)} \\ &= \frac{(z_Q-1)(x_1(-a(y_1-1)+z_1-1))\frac{x_Q}{z_Q-1}\delta + y_1(z_1-1)\frac{y_Q}{z_Q-1} - z_1(y_1-1)}{(z_3-1)y_Q+(1-y_3)z_Q+(y_3-z_3)} \end{aligned}.$$

In projective coordinates the function becomes:

$$\begin{aligned} h_{P_1,P_1}(\delta x_Q, y_Q, z_Q) &= \frac{T_3(z_Q-1)\left(\alpha_1'\frac{x_Q}{z_Q-1}\delta + \beta_1'\frac{y_Q}{z_Q-1} - \gamma_1')\right)}{T_1^3[(Z_3-T_3)y_Q+(T_3-Y_3)z_Q+(Y_3-Z_3)]} \\ &= \frac{T_3(z_Q-1)}{T_1^3[(Z_3-T_3)y_Q+(T_3-Y_3)z_Q+(Y_3-Z_3)]}(\alpha_1' M_2\delta + \beta_1' N_2 - \gamma_1') \end{aligned}.$$

Where $M_2 = 2a\frac{x_Q}{z_Q-1}$ and $N_2 = a\frac{y_Q}{z_Q-1}$. $\alpha_1' = X_1(-a(Y_1-T_1)+Z_1-T_1)$; $\beta_1' = Y_1(Z_1-T_1)$; $\gamma_1' = Z_1(Y_1-T_1)$.

We can also verify that $\frac{T_3(z_Q-1)}{T_1^3[(Z_3-T_3)y_Q+(T_3-Y_3)z_Q+(Y_3-Z_3)]} \in \mathbb{F}_{q^{k/2}}$ such that it can be discarded thanks to the final exponentiation. Thus we only have to evaluate

$$(\alpha_1' M_2)\delta + \beta_1' N_2 - \gamma_1'$$

Again the quantities $M_2 = 2a\frac{x_Q}{z_Q-1}$ and $N_2 = a\frac{y_Q}{z_Q-1}$ are precomputed in $\mathbb{F}_{q^{k/2}}$. Note that each of the multiplications $\alpha_1' M_2$ and $\beta_1' N_2$ costs $\frac{k}{2}m$. Computing α_1',β_1' and γ_1' requires $3m$ and the point doubling from Subsection 2.2 requires $2m + 5s + 1m_a$. Thus the point doubling and Miller value computation require a total of $1M + 1S + (k+5)m + 5s + 1m_a$.

3.3 Comparison of Results

The comparison of results is given in Table 1. These comparisons are made for the Tate pairing and curves with a quadratic twist.

Table 1. Comparisons of our pairing formulas with the previous fastest formulas

Curves	Doubling	Mixed Addition
Weierstrass(a=0)[6]	$1M + 1S + (k+2)m + 7s + 1m_b$	$1M + (k+10)m + 2s$
Twisted Edwards [1]	$1M + 1S + (k+6)m + 5s + 2m_a$	$1M + (k+12)m + 1m_a$
Jacobi quartic[23]	$1M + 1S + (k+4)m + 8s + 1m_a$	$1M + (k+16)m + 1s + 4m_{a,d}$
This work	$1M + 1S + (k+5)m + 5s + 1m_a$	$1M + (k+16)m + 1s + 2m_a$

4 Tate Pairing Computation on $E_d : Y^2 = dX^4 + Z^4$

Wang et al. in [23] considered pairings on Jacobi quartics and gave the geometric interpretation of the group law. We use a different way, namely birational equivalence between Jacobi quartic curves and Weierstrass curves, of obtaining the formulas. We specialize to the particular curves $E_d : Y^2 = dX^4 + Z^4$ to obtain better results for these up to 26% improvement compared to the result in [23]. To derive the Miller function $H(X, Y, Z)$ for E_d, we first write the Miller function $h(x, y)$ on the Weierstrass curve E. Then by using the birational equivalence we have $H(X, Y, Z) = h(\varphi(X, Y, Z))$.

4.1 The Miller Function

The Jacobi quartic curve $E_d : Y^2 = dX^4 + Z^4$ is birationally equivalent to the Weierstrass curve $E : y^2 = x^3 - 4dx$. Given two points $P_1(x_1, y_1)$ and $P_2(x_2, y_2)$ such that $P_3(x_3, y_3) = P_1 + P_2$, then the Miller function $h(x, y)$ for this Weierstrass curve such that a relation $\mathrm{Div}(h) = (P_1) + (P_2) - (P_3) - (O)$ holds is given by:

$$h(x, y) = \tfrac{y-\lambda x-\alpha}{x-x_3}$$

Where $\lambda = \frac{y_2-y_1}{x_2-x_1}$ if $P_1 \neq P_2$ and $\lambda = \frac{3x_1^2-4d}{2y_1}$ if $P_1 = P_2$ and $\alpha = y_1 - \lambda x_1$.
As explained at the beginning of this section, the Miller function for the Jacobi quartic $E_d : Y^2 = dX^4 + Z^4$ is given by $H(X, Y, Z) = h(\varphi(X, Y, Z))$. A simple calculation gives:

$$H(X, Y, Z) = \tfrac{4X_3^2X^2}{2X_3^2(Y+Z^2)-2X^2(Y_3+Z_3^2)} \left(\tfrac{ZY+Z^3}{X^3} - \tfrac{1}{2}\lambda\left(\tfrac{Y+Z^2}{X^2}\right) - \tfrac{\alpha}{4}\right)$$

where

$$\lambda = \begin{cases} \frac{-2X_1^3Z_2(Y_2+Z_2^2)+2X_2^3Z_1(Y_1+Z_1^2)}{X_1X_2[-X_1^2(Y_2+Z_2^2)+X_2^2(Y_1+Z_1^2)]} & \text{if } P_1 \neq P_2, \\ \frac{Y_1+2Z_1^2}{X_1Z_1} & \text{if } P_1 = P_2. \end{cases}$$

and

$$\alpha = \begin{cases} \frac{-4(Y_1+Z_1^2)(Y_2+Z_2^2)(Z_2X_1-Z_1X_2)}{X_1X_2[-X_1^2(Y_2+Z_2^2)+X_2^2(Y_1+Z_1^2)]} & \text{if } P_1 \neq P_2, \\ \frac{-2Y_1(Y_1+Z_1^2)}{X_1^3Z_1} & \text{if } P_1 = P_2. \end{cases}$$

Remark 1. It is simple to verify that our formula obtained by change of variables is exactly the same result obtained by Wang et al. in [23] using the geometric interpretation of the group law.

Indeed, by setting $x_1 = \frac{X_1}{Z_1}$, $x_2 = \frac{X_2}{Z_2}$, $y_1 = \frac{Y_1}{Z_1^2}$ and $y_2 = \frac{Y_2}{Z_2^2}$ in their Miller function obtained for the curve $E_{d,a} : y^2 = dx^4 + 2ax + 1$ (by taking $a = 0$), we get exactly the same result that we found above.
The correctness of the formulas in this work can be checked at
`http://www.prmais.org/Jacobi-Formulas.txt`.

4.2 Simplification of the Miller Function

By using twist technique as explained earlier, the point Q in the Tate pairing computation can be chosen to be $\left(\frac{X_Q}{\omega^2} : \frac{Y_Q}{\omega^6} : \frac{Z_Q}{\omega^3}\right)$ or $(x_Q\omega, y_Q, 1)$ in affine coordinates where X_Q, Y_Q, Z_Q, x_Q and y_Q are in $\mathbb{F}_{q^{k/4}}$. Thus

$$H(x_Q\omega, y_Q, 1) = \frac{2X_3^2x_Q^2\omega^2}{X_3^2(y_Q+1)-x_Q^2\omega^2(Y_3+Z_3^2)}\left(-\frac{1}{2}\lambda\left(\frac{y_Q+1}{x_Q^2\omega^4}\right)\omega^2+\left(\frac{y_Q+1}{x_Q^3\omega^4}\right)\omega-\frac{\alpha}{4}\right).$$

Write $-\frac{\alpha}{4} = \frac{A}{D}$ and $-\frac{1}{2}\lambda = \frac{B}{D}$ then

$$H(x_Q\omega, y_Q, 1) = \frac{2X_3^2x_Q^2\omega^2D^{-1}}{X_3^2(y_Q+1)-x_Q^2\omega^2(Y_3+Z_3^2)}\left(B\left(\frac{y_Q+1}{x_Q^2\omega^4}\right)\omega^2+D\left(\frac{y_Q+1}{x_Q^3\omega^4}\right)\omega+A\right)$$

We can easily see that $\frac{2X_3^2x_Q^2\omega^2}{D(X_3^2(y_Q+1)-x_Q^2\omega^2(Y_3+Z_3^2))} \in \mathbb{F}_{q^{k/2}}$ so it can be discarded in pairing computation thanks to the final exponentiation. Thus we only have to evaluate

$$H = B\left(\frac{y_Q+1}{x_Q^2\omega^4}\right)\omega^2+D\left(\frac{y_Q+1}{x_Q^3\omega^4}\right)\omega+A$$

Since $Q = (x_Q\omega, y_Q, 1)$ is fixed during pairing computation, the quantities $\frac{y_Q+1}{x_Q^3\omega^4}$ and $\frac{y_Q+1}{x_Q^2\omega^4}$ can be precomputed in $\mathbb{F}_{q^{k/4}}$. Note that each of the multiplications $D\left(\frac{y_Q+1}{x_Q^3\omega^4}\right)$ and $B\left(\frac{y_Q+1}{x_Q^2\omega^4}\right)$ costs $\frac{k}{4}m$.

Remark 2. We can use the fact that in the expression of H the term ω^3 is absent and $A \in \mathbb{F}_q$. Thus in Miller's algorithm, the cost of the main multiplication in $\mathbb{F}_{q^k}$ is not $1M$ but $\left(\frac{1}{k}+\frac{1}{2}\right)M$ assuming that schoolbook multiplication is used. But if we are using pairing friendly fields the embedding degree will be of the form $k = 2^i3^j$. Then we follow [19] and the cost of a multiplication or a squaring in the field $\mathbb{F}_{q^k}$ is 3^i5^j multiplications or squaring in $\mathbb{F}_q$ using Karatsuba and (or) Toom-Cook multiplication method. In this case, in Miller's algorithm, the cost of the main multiplication in $\mathbb{F}_{q^k}$ is $\left(\frac{7\cdot3^{i-2}5^j+2^{i-2}3^j}{3^i5^j}\right)M$. In the next sections ε stands for $\frac{1}{k}+\frac{1}{2}$ or $\frac{7\cdot3^{i-2}5^j+2^{i-2}3^j}{3^i5^j}$. A summary of how to obtain these costs is given in appendix.

In the next sections, we will compute A, B and D. In the work of Hisil et al. [16], there are different formulas in affine version for scalar multiplication. They used one of them to improve points addition and point doubling. These improved formulas have been used by Wang et al. to compute pairings. But in our case we obtained our formulas from a different affine version. For efficiency the point is represented by $(X : Y : Z : X^2 : Z^2)$ with $Z \neq 0$. We present the first time that this representation is used when $d \neq 1$. Thus we will use the points $P_1 = (X_1 : Y_1 : Z_1 : U_1 : V_1)$ and $P_2 = (X_2 : Y_2 : Z_2 : U_2 : V_2)$ where $U_i = X_i^2$, $V_i = Z_i^2$, $i = 1, 2$.

Remark 3. Note that if X^2 and Z^2 are known then expressions of the form XZ can be computed using the formula $((X+Z)^2 - X^2 - Z^2)/2$. This allows the replacement of a multiplication by a squaring presuming a squaring and three additions are more efficient. The operations concerned with this remark are followed by $*$ in the Tables 2 and 3.

4.3 Point Addition and Miller Iteration

When $P_1 \neq P_2$ we have $A = (Y_1 + Z_1^2)(Y_2 + Z_2^2)(Z_1X_2 - Z_2X_1)$, $D = X_1X_2[-X_1^2(Y_2 + Z_2^2) + X_2^2(Y_1 + Z_1^2)]$ and $B = X_1^3Z_2(Y_2 + Z_2^2) - X_2^3Z_1(Y_1 + Z_1^2)$.

Using the algorithm in Table 2 the computation of A, B, D and the point addition can be done in $18m+5s+1m_d$ or $12m+11s+1m_d$ according to Remark 3. Applying mixed addition($Z_2 = 1$), this cost is reduced to $15m + 4s + 1m_d$ or $12m + 7s + 1m_d$. Thus the point addition and Miller value computation require a total of $\varepsilon M + 1S + \left(\frac{k}{2} + 15\right) m + 4s + 1m_d$ or $\varepsilon M + 1S \left(\frac{k}{2} + 12\right) m + 7s + 1m_d$.

Table 2. Combined formulas for addition and Miller value computation

Operations	*Values*
$U := Y_1 + V_1$	$U = Y_1 + Z_1^2$
$V := Y_2 + V_2$	$V = Y_2 + Z_2^2$
$R := Z_2X_1$ *	$R = Z_2X_1$
$S := Z_1X_2$ *	$S = Z_1X_2$
$A := S - R$	$A = Z_1X_2 - Z_2X_1$
$A := AV$	$A = (Y_2 + Z_2^2)(Z_1X_2 - Z_2X_1)$
$A := AU$	$A = (Y_1 + Z_1^2)(Y_2 + Z_2^2)(Z_1X_2 - Z_2X_1)$
$U := U_2U$	$U = X_2^2(Y_1 + Z_1^2)$
$V := U_1V$	$V = X_1^2(Y_2 + Z_2^2)$
$B := RV - SU$	$B = X_1^3Z_2(Y_2 + Z_2^2) - X_2^3Z_1(Y_1 + Z_1^2)$
$D := X_1X_2$ *	$D = X_1X_2$
$E := dD^2$	$E = d(X_1X_2)^2$
$D := D(U - V)$	$D = X_1X_2[-X_1^2(Y_2 + Z_2^2) + X_2^2(Y_1 + Z_1^2)]$
$X_3 := (R + S)(R - S)$	$X_3 = X_1^2Z_2^2 - Z_1^2X_2^2$
$W_1 := X_1Z_1$ *	$W_1 = X_1Z_1$
$W_2 := X_2Z_2$ *	$W_2 = X_2Z_2$
$Z_3 := W_1Y_2 - W_2Y_1$	$Z_3 = X_1Z_1Y_2 - X_2Z_2Y_1$
$U := Y_1Y_2$	$U = Y_1Y_2$
$V := Z_1Z_2$ *	$V = Z_1Z_2$
$V := V^2 + E$	$V = (Z_1Z_2)^2 + d(X_1X_2)^2$
$E := (R - S)^2$	$E = (X_1Z_2 - X_2Z_1)^2$
$U_3 := X_3^2$	$U_3 = X_3^2$
$V_3 := Z_3^2$	$V_3 = Z_3^2$
$Y_3 := E(U + V) - V_3$	$Y_3 = (X_1Z_2 - X_2Z_1)^2(Y_1Y_2 + (Z_1Z_2)^2 + d(X_1X_2)^2) - Z_3^2$

4.4 Point Doubling and Miller Iteration

When $P_1 = P_2$ we have $A = Y_1(Y_1 + Z_1^2)$, $D = 2X_1^3Z_1$ and $B = -X_1^2(Y_1 + 2Z_1^2)$. The computation of A, B, D and the point doubling can be done using the algorithm in Table 3 with $4m + 6s + 1m_d$ or $3m + 7s + 1m_d$ according to the Remark 3.

Table 3. Combined formulas for doubling and Miller value computation

Operations	*Values*
$U := U_1^2$	$U = X_1^4$
$V := V_1^2$	$V = Z_1^4$
$Z_3 := V - dU$	$Z_3 = Z_1^4 - dX_1^4$
$E := X_1 Z_1$ $*$	$E = X_1 Z_1$
$D := 2U_1 E$	$D = 2X_1^3 Z_1$
$A := (2Y_1 + V_1)^2/4 - U$	$A = Y_1(Y_1 + Z_1^2)$
$B := -U_1(Y_1 + 2V_1)$	$B = -X_1^2(Y_1 + 2Z_1^2)$
$X_3 := 2EY_1$	$X_3 = 2X_1 Y_1 Z_1$
$V_3 := Z_3^2$	$V_3 = Z_3^2$
$Y_3 := 2V - Z_3$	$Y_3 = dX_1^4 + Z_1^4 = Y_1^2$
$Y_3 := 2Y_3^2 - V_3$	$Y_3 = 2Y_1^4 - Z_3^2$
$U_3 := X_3^2$	$U_3 = X_3^2$

Thus the point doubling and Miller value computation require a total of $\varepsilon M + 1S + (\frac{k}{2} + 4)m + 6s + 1m_d$ or $\varepsilon M + 1S + (\frac{k}{2} + 3)m + 7s + 1m_d$.

4.5 Comparison

The comparison of results is summarized in Table 4 and Table 5. These comparisons are made for the Tate pairing and curves with a quartic twist. In Table 4 we assume that Schoolbook multiplication method is used whereas the comparisons in Table 5 are made using Karatsuba and Toom-Cook method for curves with $k = 2^i 3^j$. We also present an example of comparison in the cases $k = 8$ and $k = 16$ since these values are the most appropriate for cryptographic applications when a quartic twist is used.

Table 4. Comparison of our pairing formulas with the previous fastest formulas with an example using Schoolbook multiplication method

Curves	Doubling	Mixed Addition
Weierstrass(b=0)[6]	$1M + 1S + (\frac{k}{2} + 2)m + 8s + 1m_a$	$1M + (\frac{k}{2} + 9)m + 5s$
Jacobi quartic(a=0)[23]	$1M + 1S + (\frac{k}{2} + 5)m + 6s$	$1M + (\frac{k}{2} + 16)m + 1s + 1m_d$
This work	$(\frac{1}{k} + \frac{1}{2})M + 1S + (\frac{k}{2} + 3)m + 7s + 1m_d$	$(\frac{1}{k} + \frac{1}{2})M + (\frac{k}{2} + 12)m + 7s + 1m_d$
Example: $k = 8$		
Weierstrass(b=0)[6]	$98m + 16s + 1m_a$	$77m + 5s$
Jacobi quartic (a=0)[23]	$101m + 14s$	$84m + 1s + 1m_d$
This work	$75m + 15s + 1m_d$	$57m + 6s + 1m_d$

Remark 4. If we assume that $m = s = m_c$ and $k = 8$ then for the doubling step the total costs are $115m$, $115m$ and $91m$ for Weierstrass curve, Jacobi quartic curve (a=0)[23] and *this work* respectively. Hence we obtain in this work

a theoretical gain of 21% with respect to Weierstrass curves and Jacobi quartic curves. Similarly for the addition step we obtain a theoretical gain of 22% and 26% over Weierstrass and Jacobi quartic curves respectively. This theoretical gain increases together with the value of k.

Table 5. Comparison of our pairing formulas with the previous fastest formulas with an example on pairing friendly fields

Curves	Doubling	Mixed Addition
Weierstrass(b=0)[6]	$1M + 1S + (\frac{k}{2} + 2)m + 8s + 1m_a$	$1M + (\frac{k}{2} + 9)m + 5s$
Jacobi quartic(a=0)[23]	$1M + 1S + (\frac{k}{2} + 5)m + 6s$	$1M + (\frac{k}{2} + 16)m + 1s + 1m_d$
This work	$\left(\frac{7\cdot 3^{i-2}5^j + 2^{i-2}3^j}{3^i 5^j}\right) M + 1S + (\frac{k}{2} + 3)m + 7s + 1m_d$	$\left(\frac{7\cdot 3^{i-2}5^j + 2^{i-2}3^j}{3^i 5^j}\right) M + (\frac{k}{2} + 12)m + 7s + 1m_d$
Example 1: $k = 8$		
Weierstrass(b=0)[6]	$33m + 35s + 1m_a$	$40m + 5s$
Jacobi quartic (a=0)[23]	$36m + 33s$	$84m + 1s + 1m_d$
This work	$30m + 34s + 1m_d$	$39m + 7s + 1m_d$
Example 2: $k = 16$		
Weierstrass(b=0)[6]	$91m + 89s + 1m_a$	$98m + 5s$
Jacobi quartic (a=0)[23]	$94m + 87s$	$105m + 1s + 1m_d$
This work	$78m + 88s + 1m_d$	$87m + 7s + 1m_d$

Remark 5. We assume again that $m = s = m_c$. For $k = 8$ and for the doubling step we obtain a theoretical gain of 6% over Weierstrass curves and Jacobi quartic curves (a=0)[23]. This theoretical gain increases together with the value of k. When $k = 16$ the gain is 8% both for the addition and doubling step over Weierstrass curves. The improvement is 13% in addition step over Jacobi quartic curves.

Remark 6. The security and the efficiency of pairing-based systems requires using pairing-friendly curves. The Jacobi models of elliptic curves studied in this work are isomorphic to Weierstrass curves. Thus we can obtain pairing friendly curves of such models using the construction given by Galbraith et al.[14] or by Freeman et al.[11]. Some examples of pairing friendly curves of Jacobi quartic form can be found in [23].

5 Conclusion

In this work we have computed the Tate pairing on Jacobi intersection curves using the geometric interpretation of the group law. Our results show that the doubling step is efficient but not competitive compared to the results using other elliptic curves. The addition step may require further improvements. Furthermore we significantly improved the doubling and the addition step in Miller's algorithm to compute the Tate pairing on the special Jacobi quartic elliptic curve $E_d : Y^2 = dX^4 + Z^4$. Our result is the best to date among all the curves with a quartic twist.

Acknowledgements. The authors thank Nadia El Mrabet and Hongfeng Wu for helpful discussions. The authors also thank the anonymous referees and the program committee for their useful comments.

References

1. Arene, C., Lange, T., Naehrig, M., Ritzenthaler, C.: Faster computation of the Tate pairing. Journal of Number Theory 131(5), 842–857 (2011)
2. Billet, O., Joye, M.: The Jacobi Model of an Elliptic Curve and Side-Channel Analysis. In: Fossorier, M.P.C., Høholdt, T., Poli, A. (eds.) AAECC 2003. LNCS, vol. 2643, pp. 34–42. Springer, Heidelberg (2003)
3. Boneh, D., Franklin, M.: Identity-based encryption from the Weil pairing. SIAM Journal of Computing 32(3), 586–615 (2003)
4. Chudnovsky, D.V., Chudnovky, G.V.: Sequences of numbers generated by addition in formal groups and new primality and factorization tests. Advances in Applied Mathematics 7(2), 385–434 (1986)
5. Costello, C., Hisil, H., Boyd, C., Nieto, J.G., Wong, K.K.-H.: Faster Pairings on Special Weierstrass Curves. In: Shacham, H., Waters, B. (eds.) Pairing 2009. LNCS, vol. 5671, pp. 89–101. Springer, Heidelberg (2009)
6. Costello, C., Lange, T., Naehrig, M.: Faster Pairing Computations on Curves with High-Degree Twists. In: Nguyen, P.Q., Pointcheval, D. (eds.) PKC 2010. LNCS, vol. 6056, pp. 224–242. Springer, Heidelberg (2010)
7. Das, M.P.L., Sarkar, P.: Pairing Computation on Twisted Edwards Form Elliptic Curves. In: Galbraith, S.D., Paterson, K.G. (eds.) Pairing 2008. LNCS, vol. 5209, pp. 192–210. Springer, Heidelberg (2008)
8. Duquesne, S., Frey, G.: Background on pairings. In: Cohen, H., Frey, G. (eds.) Handbook of Elliptic and Hyperelliptic Curves Cryptography, pp. 115–124. Chapman and Hall/CRC (2005)
9. Dutta, R., Barua, R., Sarkar, P.: Pairing-based cryptography: A survey. Cryptology ePrint Archive, Report 2004/064 (2004)
10. Feng, R., Nie, M., Wu, H.: Twisted Jacobi Intersections Curves. In: Kratochvíl, J., Li, A., Fiala, J., Kolman, P. (eds.) TAMC 2010. LNCS, vol. 6108, pp. 199–210. Springer, Heidelberg (2010)
11. Freeman, D., Scott, M., Teske, E.: A taxonomy of pairing-friendly elliptic curves. Journal of Cryptology 23(2), 224–280 (2010)
12. Frey, G., Müller, M., Rück, H.: The Tate Pairing and the Discrete Logarithm applied to Elliptic Curve Cryptosystems. IEEE Transactions on Information Theory 45(5), 1717–1719 (1999)
13. Galbraith, S.D.: Pairings. In: Seroussi, G., Blake, I., Smart, N. (eds.) Advances in Elliptic Curve Cryptography, pp. 193–213. Cambridge University Press (2005)
14. Galbraith, S.D., McKee, J.F., Valenca, P.C.: Ordinary abelian varieties having small embedding degree. Finite Fields Applications 13, 800–814 (2007)
15. Hisil, H., Wong, K.K., Carter, G., Dawson, E.: Faster group operations on elliptic curves. In: Australasian Information Security Conference (AISC), Wellington, New Zealand, vol. 98, pp. 7–19 (2009)
16. Hisil, H., Wong, K.K.-H., Carter, G., Dawson, E.: Jacobi Quartic Curves Revisited. In: Boyd, C., Nieto, J.G. (eds.) ACISP 2009. LNCS, vol. 5594, pp. 452–468. Springer, Heidelberg (2009)

17. Ionica, S., Joux, A.: Another Approach to Pairing Computation in Edwards Coordinates. In: Chowdhury, D.R., Rijmen, V., Das, A. (eds.) INDOCRYPT 2008. LNCS, vol. 5365, pp. 400–413. Springer, Heidelberg (2008)
18. Joux, A.: A One-Round Protocol for Tripartite Diffie-Hellman. In: Bosma, W. (ed.) ANTS 2000. LNCS, vol. 1838, pp. 385–394. Springer, Heidelberg (2000)
19. Koblitz, N., Menezes, A.: Pairing-Based Cryptography at High Security Levels. In: Smart, N.P. (ed.) Cryptography and Coding 2005. LNCS, vol. 3796, pp. 13–36. Springer, Heidelberg (2005)
20. Menezes, A., Okamoto, T., Vanstone, S.: Reducing elliptic curve logarithms to logarithms in a finite field. IEEE Transactions on Information Theory 39(5), 1639–1646 (1993)
21. Merriman, J.R., Siksek, S., Smart, N.P.: Explicit 4-descents on an elliptic curve. Acta Arithmetica 77, 385–404 (1996)
22. Miller, S.V.: The Weil pairing, and its efficient calculation. Journal of Cryptology 17(4), 235–261 (2004)
23. Wang, H., Wang, K., Zhang, L., Li, B.: Pairing Computation on Elliptic Curves of Jacobi Quartic Form. Chinese Journal of Electronics 20(4), 655–661 (2011)

A Appendix: Cost of the Main Multiplication in Miller's Algorithm

The main multiplication in Miller's algorithm is of the form $f \cdot h$ where f and h are in $\mathbb{F}_{q^k}$. Since $\mathbb{F}_{q^k}$ is a $\mathbb{F}_{q^{k/4}}$-vector space with basis $\{1, \omega, \omega^2, \omega^3\}$, f and h can be written as : $f = f_0 + f_1\omega + f_2\omega^2 + f_3\omega^3$ and $h = h_0 + h_1\omega + h_2\omega^2 + h_3\omega^3$ with f_i and h_i in $\mathbb{F}_{q^{k/4}}$, $i = 0, 1, 2, 3$. However in our case $h_3 = 0$, $h_0 \in \mathbb{F}_q$ and $k = 2^i 3^j$.

Schoolbook Method: A full multiplication $f.h$ costs k^2 multiplications in the base field $\mathbb{F}_q$ using schoolbook method. But thanks to the particular form of h_0 and h_3, each of the multiplications $f_i \cdot h_0$ costs $\frac{k}{4}$ and each of the multiplications $f_i \cdot h_1$, $f_i \cdot h_2$ costs $\frac{k^2}{16}$, $i = 0, 1, 2, 3$. Then final cost of the product $f \cdot h$ in the base field $\mathbb{F}_q$ is $8\frac{k^2}{16} + 4\frac{k}{4} = \frac{k^2}{2} + k$. Finally the ratio of the cost in this case by the cost of the general multiplication is $\frac{\frac{k^2}{2}+k}{k^2} = \frac{1}{2} + \frac{1}{k}$.

Karatsuba Method: The computation of $f \cdot h$ is done by computing the three products: $u = (f_0 + f_1\omega)(h_0 + h_1\omega)$ which costs $2^{i-2}3^j + 2(3^{i-2}5^j)$, $v = f_2(h_2 + h_3\omega)$ which costs $2(3^{i-2}5^j)$ and $w = (f_0 + f_2 + (f_1 + f_3)\omega)(h_0 + h_2 + (h_1 + h_3)\omega)$ which costs $3(3^{i-2}5^j)$. The final cost is then $7 \cdot 3^{i-2}5^j + 2^{i-2}3^j$.