Pairing Computation on Elliptic Curves of Jacobi Quartic Form

Hong Wang, Kunpeng Wang, Lijun Zhang, and Bao Li
{hwang,kpwang,ljzhang,lb}@is.ac.cn

State Key Laboratory of Information Security
Graduate University of Chinese Academy of Science

Abstract. This paper proposes explicit formulae for the addition step and doubling step in Miller's algorithm to compute Tate pairing on Jacobi quartic curves.
We present a geometric interpretation of the group law on Jacobi quartic curves, which leads to formulae for Miller's algorithm. The doubling step formula is competitive with that for Weierstrass curves and Edwards curves. Moreover, by carefully choosing the coefficients, there exist quartic twists of Jacobi quartic curves from which pairing computation can benefit a lot. Finally, we provide some examples of supersingular and ordinary pairing friendly Jacobi quartic curves.

Key words: elliptic curve, Jacobi quartic curve, Tate pairing, Miller function, group law, geometric interpretation

1 Introduction

Since the seminal work of Miller[20] and Koblitz[17] in 1985, elliptic curve cryptology has progressed rapidly over the years. The implementation of elliptic curve cryptosystem involves mainly two operations: point scalar multiplication and pairing computation. A well known elliptic curve model is the Weierstrass model in the form of cubic equation $y^2 = x^3 + ax + b$. The group law of the Weierstrass curves is explicitly defined by the chord and tangent rule, and many efficient formulae for point addition[12] and pairing computation[1, 6, 16] are proposed for Weierstrass curves.

Besides the Weierstrass equation, there are still many other forms of elliptic curve equations, some are cubic and others quartic. For example, Edwards elliptic curve is a quartic form $x^2+y^2 = 1+dx^2y^2$ introduced by Edwards[8] in 2007, then it was generalized to twisted Edwards curves by Bernstein, Lange et al.[3]. The point addition formula of twisted Edwards curves is unified. When the formula is optimized for addition and doubling separately, it is faster than the formula for Weierstrass form curves. Pairing computation on twisted Edwards curves was first considered by Das and Sarkar[18] and then by Ionica and Joux[16] using birational maps between twisted Edwards curves and Weierstrass curves. Then Arene, Lange et al.[1] developed explicit formulae for pairing computation on twisted Edwards curves based on geometric interpretation of group law instead

of birational maps. They announced their formulae of pairing computation are competitive with the formulae for Weierstrass curves.

Edwards curves have achieved great success in point scalar multiplication. Pairing computation on Edwards curves is almost as efficient as that on Weierstrass curves, but only quadratic twists can be used. Inspired by the good quality of Edwards curves, it seems worthy of studying other kinds of elliptic curves which are not Weierstrass form. In this paper, we focus our interest on Jacobi quartic elliptic curves $y^2 = dx^4 + 2ax^2 + 1$, which are also quartic form. Many formulae for point addition and doubling of this form are given in the literatures, see [4, 5] or [15] for a brief development history. Point addition and doubling on Jacobi quartic curves are also faster than that on Weierstrass curves. But to the best of our knowledge, no formulae for pairing computaion are given on Jacobi quartic curves. One way to obtain the pairing computation formulae is to use the birational maps between Jacobi quartic curves and Weierstrass curves, but the process is complicated and hard to comprehend.

In this paper, we show an easy way to obtain the Tate pairing computation formulae. First we present a geometric interpretation of group law for Jacobi quartic curves, then we give our formulae for pairing computation based on this geometric interpretation. The addition step formula we give needs to be optimized which we consider as the further work. The doubling step formula is efficient and competitive with that for Weierstrass curves and Edwards curves. To accelerate pairing computation, we define a kind of curves which are twists of Jacobi quartic curves. Moreover, we demonstrate there exist quartic twists of Jacobi quartic curves if a is chosen to be zero. It induces the quartic twist technique in pairing computation while in Edwards curves only quadratic twist technique is applied. As is well known, higher twists benefit more in pairing computation than lower twists.

This paper is organized as follows: section 2 gives a brief background of Jacobi quartic curves and pairing on elliptic curves. Section 3 shows the geometric interpretation of the group law. Section 4, 5, 6 define twisted Jacobi quartic curves and propose explicit formulae of Miller function on Jacobi quartic curves. Then some examples of pairing friendly curves are given in section 7. We conclude in section 8.

2 Background on Jacobi Quartic Curves and Pairing

This section gives the definition of Jacobi quartic curves and some basics of Tate pairing that will be used later.

2.1 Jacobi Quartic Curve

A Jacobi quartic elliptic curve over a field K with $char(K) \neq 2$ is defined by

$$E_{d,a} : y^2 = dx^4 + 2ax^2 + 1$$

where $a, d \in K$ and discriminant $\Delta = 256(a^2 - d)^2 \neq 0$.

Each elliptic curve over K with even number of K-rational points can be transformed to Jacobi quartic form. The birational equivalence between $E_{d,a}$ and a Weierstrass form elliptic curve $y^2 = x^3 + bx + c$ is given in [5].

2.2 Tate Pairing

Here we briefly give basics of Tate pairing, other pairing definitions can be found in [22]. Let E be an elliptic curve with neutral element $\mathcal{O}$ defined over a finite field F_q. Let $r|\#E(F_q)$, where r is a prime and $\#E(F_q)$ is the number of F_q-rational points on E. The embedding degree of E with respect to r is defined to be the smallest integer k such that $r|q^k - 1$.

Let $P \in E(F_q)[r]$, $Q \in E(F_{q^k})$ and $f_{r,P}$ be a function such that divisor $div(f_{r,P}) = r(P) - r(\mathcal{O})$. Assume that the function $f_{r,P}$ is normalised, i.e., $u_{\mathcal{O}}^r f_{r,P}(\mathcal{O}) = 1$ for a uniformizer $u_{\mathcal{O}}$ at $\mathcal{O}$, then the reduced Tate pairing is defined by

$$\begin{aligned} t(.,.) : E(F_q)[r] \times E(F_{q^k})/rE(F_{q^k}) &\longrightarrow \mu_r \\ (P, Q) &\longmapsto f_{r,P}(Q)^{(q^k-1)/r} \end{aligned}$$

where $\mu_r \subset F_{q^k}^*$ is the group of r-th roots of unity.

2.3 Miller's Algorithm

Tate pairing can be computed in an iterative way by Miller's algorithm [21]. Let the binary representation of $r = (r_{l-1}, \ldots, r_1, r_0)$ and h_{P_1,P_2} be a function called Miller function such that $div(h_{P_1,P_2}) = (P_1) + (P_2) - (P_1 + P_2) - (\mathcal{O})$, where P_1 and P_2 are two points on E. Miller's algorithm is as follows:

Input: P and Q
Output: $t(P, Q)$
1. Set $f = 1$ and $P_1 = P$.
2. For $i = l - 2$ downto 0 do
$f \leftarrow f^2 \cdot h_{P_1,P_1}(Q)$, $P_1 \leftarrow 2P_1$.
if $r_i = 1$, then $f \leftarrow f \cdot h_{P_1,P}(Q)$, $P_1 \leftarrow P_1 + P$.
3. Return $f = f^{(q^k-1)/r}$.

The key task of Miller's algorithm is to find function h_{P_1,P_2}. If E is in Weierstrass form, then this task can be easily accomplished by using the chord and tangent rule for point addition. But if E is given in other forms, generally it is not as easy as Weierstrass form to find this function. Once this function is found, then Miller's algorithm can be applied to compute Tate pairing.

There are many improvements of Miller's algorithm and some very useful techniques are worth mentioning, such as denominator cancellation, choosing subgroup order with low Hamming weight, final power acceleration [2], using higher twists [7] and reducing iterations [13].

3 Geometric Interpretation of the Group Law

The group law of Jacobi quartic form curves is quite different from that of Weierstrass form curves which is defined by the chord and tangent rule. In this section, we show the geometric interpretation for the group law of Jacobi quartic form curves.

Rewrite the Jacobi quartic equation in projective form

$$Y^2Z^2 = dX^4 + 2aX^2Z^2 + Z^4.$$

There is a singular point $(0:1:0)$ in projective plane $\mathbb{P}^2$, which is a point at infinity in affine plane, denote it as ∞. Select $\mathcal{O} = (0,1)$ as neutral point, note the fact $\mathcal{O}' = (0,-1)$ is a point on the curve. The geometric interpretation of the group law is shown in the following:

3.1 Negative Point

An affine plane curve given by equation $f_P = 0$ which defines negative point must satisfy $div(f_P) = (P) + (-P) - 2(\mathcal{O})$. Let $l_0 = 0$ be the vertical line across point $\mathcal{O}$ and $\mathcal{O}'$ with $div(l_0) = (\mathcal{O}) + (\mathcal{O}') - 2(\infty)$, in fact $l_0 = x$. Let $C_P = 0$ be a conic across P, R, and $\mathcal{O}'$ with $div(C_P) = (P) + (R) + 2(\mathcal{O}') - 4(\infty)$. Define

$$f_P = \frac{C_P}{l_0^2},$$

then $-P = R$. The function C_P is given as follows:

Lemma 1. *Let $C_P = 0$ be a conic with $div(C_P) = (P) + (R) + 2(\mathcal{O}') - 4(\infty)$, and $P = (x_1, y_1)$, then*

$$C_P = y + 1 - cx^2$$

with $c = (y_1 + 1)/x_1^2$.

Proof. Suppose $C_P = a_0x^2 + a_1xy + a_2y^2 + a_3x + a_4y + a_5$. The fact that $\infty = (0:1:0)$ lies on homogenous form of $C_P = 0$ forces $a_2 = 0$, and $\mathcal{O}' = (0,1)$ lies on $C_P = 0$ forces $a_4 = a_5$. Furthermore, $\mathcal{O}'$ and ∞ are a zero of order 2 and a pole of order 4 respectively, which lead to $a_1 = 0$ and $a_3 = 0$. Since multiplying C_P by a constant does not change the divisor of C_P, let $a_4 = 1$, then $C_P = y + 1 - cx^2$, and $c = (y_1 + 1)/x_1^2$ is obtained from the fact that C_P is zero at P.

Solving the system of equations $C_P = 0$ and $E_{d,a} = 0$, it is easy to have $R = (-x_1, y_1)$. From the above analysis, $-P = R = (-x_1, y_1)$.

Remark 1. If $P = \mathcal{O}'$, then rewrite $c = (y_1 + 1)/x_1^2 = (dx_1^2 + 2a)/(y_1 - 1)$. Substitute $(x_1, y_1) = \mathcal{O}' = (0,-1)$, then $c = -a$. By simple calculating, the order of $C_{\mathcal{O}'}$ at $\mathcal{O}'$ is 4, so $div(C_{\mathcal{O}'}) = 4(\mathcal{O}') - 4(\infty)$. Then $div(C_{\mathcal{O}'}/l_0^2) = 2(\mathcal{O}') - 2(\mathcal{O})$, which means $-\mathcal{O}' = \mathcal{O}'$, so $\mathcal{O}'$ is a point of order 2.

An example of negative point is given in Fig.1.

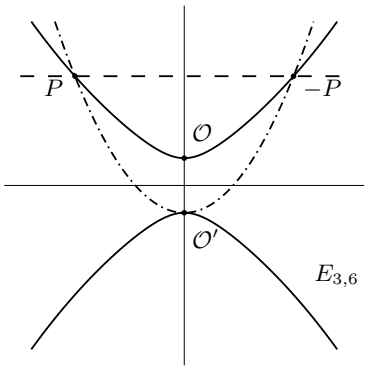

Fig. 1. Negative point

3.2 Point Addition

Assume that $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, $P_3 = (x_3, y_3)$ are three points on Jacobi quartic curve $E_{d,a}$ and $P_3 = P_1 + P_2$, $P_1, P_2 \neq \mathcal{O}$. Let $C_{P_1,P_2} = 0$ be a cubic across P_1, P_2, R, $\mathcal{O}'$, with $div(C_{P_1,P_2}) = (P_1) + (P_2) + (R) + 3(\mathcal{O}') - 6(\infty)$. Let f_R be a function satisfying $div(f_R) = (R) + (-R) - 2(\mathcal{O})$. Define

$$f_{P_1,P_2} = \frac{C_{P_1,P_2}}{f_R l_0^3}.$$

Then function f_{P_1,P_2} satisfies $div(f_{P_1,P_2}) = (P_1)+(P_2)-(-R)-(\mathcal{O})$, so $P_3 = -R$. The function C_{P_1,P_2} is given in the following:

Lemma 2. *Let $C_{P_1,P_2} = 0$ be a cubic with $div(C_{P_1,P_2}) = (P_1) + (P_2) + (R) + 3(\mathcal{O}') - 6(\infty)$, then*

$$C_{P_1,P_2} = y + 1 + ax^2 + sx + sxy + tx^3$$

with

$$s = \begin{vmatrix} y_1 + 1 + ax_1^2 & x_1^3 \\ y_2 + 1 + ax_2^2 & x_2^3 \end{vmatrix} \Big/ \begin{vmatrix} x_1^3 & x_1(1+y_1) \\ x_2^3 & x_2(1+y_2) \end{vmatrix},$$

$$t = \begin{vmatrix} x_1(1+y_1) & y_1 + 1 + ax_1^2 \\ x_2(1+y_2) & y_2 + 1 + ax_2^2 \end{vmatrix} \Big/ \begin{vmatrix} x_1^3 & x_1(1+y_1) \\ x_2^3 & x_2(1+y_2) \end{vmatrix}.$$

Proof. Assume $C_{P_1,P_2} = s_1x^3 + s_2x^2y + s_3xy^2 + s_4y^3 + s_5x^2 + s_6xy + s_7y^2 + s_8x + s_9y + s_{10}$. The fact $(0:1:0)$ lies on homogenous equation of $C_{P_1,P_2} = 0$ forces $s_4 = 0$, and $(0,-1)$ lies on C_{P_1,P_2} forces $s_7 = s_9 - s_{10}$. Since $\mathcal{O}'$ and ∞ are a zero of order 3 and a pole of order 6 respectively and $d \neq a^2$ from $\Delta \neq 0$, then $s_2 = s_3 = s_7 = 0$, $s_5 = as_9$, $s_6 = s_8$, $s_9 = s_{10}$. From the fact $s_9 \neq 0$, or else C_2 intersects $E_{d,a}$ with no other points besides $\mathcal{O}'$, P_1, P_2, then

$C_{P_1,P_2} = y + 1 + ax^2 + sx + sxy + tx^3$. Since P_1, P_2 lie on cubic $C_{P_1,P_2} = 0$, the coefficients s and t are easy to obtain by solving the system of these two equations.

3.3 Point Doubling

Assume $P_3 = 2P_1$. Let $C_{P_1,P_1} = 0$ be a cubic across P_1, R, $\mathcal{O}'$, with $div(C_{P_1,P_1}) = 2(P_1) + (R) + 3(\mathcal{O}') - 6(\infty)$. The geometric interpretation of point doubling is similar to the point addition. Let f_R and l_0 be defined the same as that in point addition. Define

$$f_{P_1,P_1} = \frac{C_{P_1,P_1}}{f_R l_0^3}.$$

Then function f_{P_1,P_1} satisfies $div(f_{P_1,P_1}) = 2(P_1) - (-R) - (\mathcal{O})$, so $P_3 = -R$. The function C_{P_1,P_1} is given in the following:

Lemma 3. *Let $C_{P_1,P_1} = 0$ be a cubic with $div(C_{P_1,P_1}) = 2(P_1) + (R) + 3(\mathcal{O}') - 6(\infty)$, then*

$$C_{P_1,P_1} = y + 1 + ax^2 + sx + sxy + tx^3$$

with

$$s = \begin{vmatrix} 2dx_1^3 + 2ax_1 + 2ax_1y_1 & 3x_1^2y_1 \\ y_1 + 1 + ax_1^2 & x_1^3 \end{vmatrix} / \begin{vmatrix} 3x_1^2y_1 & 2dx_1^4 + 2ax_1^2 + y_1 + y_1^2 \\ x_1^3 & x_1 + x_1y_1 \end{vmatrix},$$

$$t = \begin{vmatrix} 2dx_1^4 + 2ax_1^2 + y_1 + y_1^2 & 2dx_1^3 + 2ax_1 + 2ax_1y_1 \\ x_1 + x_1y_1 & y_1 + 1 + ax_1^2 \end{vmatrix} / \begin{vmatrix} 3x_1^2y_1 & 2dx_1^4 + 2ax_1^2 + y_1 + y_1^2 \\ x_1^3 & x_1 + x_1y_1 \end{vmatrix}.$$

Proof. The proof is similar to that of lemma 2, the coefficients s, t are obtained by the fact P_1 is a zero of order 2 of C_{P_1,P_1}.

From lemma 2 and lemma 3, we obtain the following theorem.

Theorem 1. *Let $E_{d,a} : y^2 = dx^4 + 2ax^2 + 1$ be a Jacobi quartic curve defined over a finite field F_q, $\mathcal{O} = (0, 1)$ be the neutral element, $\mathcal{O}' = (0, -1)$, $\infty = (0 : 1 : 0)$. Let $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ be two points on $E_{d,a}$ different from $\mathcal{O}$ and $P_3 = (x_3, y_3)$ be a point on $E_{d,a}$. Let $C_{P_1,P_2} = 0$ be a conic passing through P_1, P_2, $\mathcal{O}'$, R with $div(C_{P_1,P_2}) = (P_1) + (P_2) + (R) + 3(\mathcal{O}') - 6(\infty)$, let $l_0 = 0$ be the vertical line across $\mathcal{O}$ and $\mathcal{O}'$, f_R be a function with $div(f_R) = (R) + (-R) - 2(\mathcal{O})$, then*

$$C_{P_1,P_2} = y + 1 + ax^2 + sx + sxy + tx^3.$$

The function $f_{P_1,P_2} = \frac{C_{P_1,P_2}}{f_R l_0^3}$ with $div(f_{P_1,P_2}) = (P_1) + (P_2) - (-R) - (\mathcal{O})$ defines the addition(doubling if $P_1 = P_2$) of P_1 and P_2 by $P_3 = -R$. The simplized coefficients of C_{P_1,P_2} are given in the following:

(a) If $P_1 \neq P_2$ and $P_1, P_2 \neq \mathcal{O}'$, then

$$\begin{cases} s = \frac{(y_1+1+ax_1^2)x_2^3-(y_2+1+ax_2^2)x_1^3}{x_1x_2[x_1^2(y_2+1)-x_2^2(y_1+1)]} \\ t = \frac{(y_2+1+ax_2^2)(y_1+1)x_1-(y_1+1+ax_1^2)(y_2+1)x_2}{x_1x_2[x_1^2(y_2+1)-x_2^2(y_1+1)]} \end{cases} \tag{1}$$

(b) If $P_1 = P_2$, then

$$\begin{cases} s = -\frac{y_1+2}{2x_1} \\ t = \frac{y_1+y_1^2-2ax_1^2}{2x_1^3} \end{cases} \tag{2}$$

Remark 2. There is a case $P_1 \neq P_2 = \mathcal{O}'$ which is not included in theorem 1. In this case, define $V_{P_1} = x - x_1$ with $div(V_{P_1}) = (P_1) + (S) - 2(\infty)$, $S = (x, -y)$. Then $div(\frac{C_S}{V_P l_0}) = (-S) + (\mathcal{O}') - (P_1) - (\mathcal{O})$ which means $-S + \mathcal{O}' = P_1$, since $2\mathcal{O}' = \mathcal{O}$, then $(x_1, y_1) + (0, -1) = P_1 + \mathcal{O}' = -S = (-x_1, -y_1)$.

Fig. 2 shows an example of point addition and doubling:

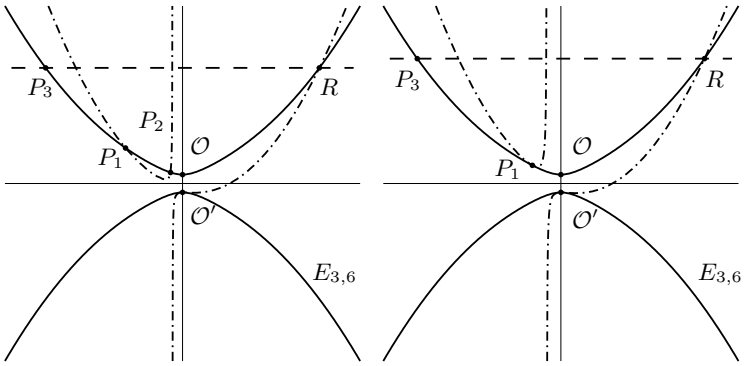

Fig. 2. Point addition and doubling

4 Miller Function on Jacobi Quartic Curves

From the geometric interpretation of the group law in section 3, the Miller function is obtained as follows:

Theorem 2. *Let $E_{d,a}$ be a Jacobi quartic curve, $\mathcal{O} = (0, 1)$ and $\mathcal{O}' = (0, -1)$. Let $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ be two points on $E_{d,a}$ different from $\mathcal{O}'$. Let $P_3 = (x_3, y_3) = P_1 + P_2$. Then the Miller function $h(x, y)$ which satisfies*

$$div(h) = (P_1) + (P_2) - (P_3) - (\mathcal{O})$$

is given by

$$h(x,y) = \frac{C_{P_1,P_2}}{f_{P_3} l_0^3} = \frac{y+1+ax^2+sx+sxy+tx^3}{x(y+1-cx^2)}, \tag{3}$$

where $c = (y_3+1)/x_3^2$ *and* s, t *are the same as in theorem 1.*

Proof. Since $div(f_{P_3}) = div(C_{P_3}/l_0^2) = (P_3) + (-P_3) - 2(\mathcal{O})$, and $div(l_0) = div(x) = (\mathcal{O}) + (\mathcal{O}') - 2(\infty)$, then divisor $div(f_{P_3} l_0^3) = (P_3) + (-P_3) + (\mathcal{O}) + 3(\mathcal{O}') - 6(\infty)$. From theorem 1, $div(C_{P_1,P_2}) = (P_1)+(P_2)+(-P_3)+3(\mathcal{O}')-6(\infty)$, then $div(h) = div(\frac{C_{P_1,P_2}}{f_{P_3} l_0^3}) = (P_1) + (P_2) - (P_3) - (\mathcal{O})$.

5 Twisted Jacobi Quartic Curves

In this section, we define a class of curves called twisted Jacobi quartic curves since they are twists of Jacobi quartic curves. These curves are used to accelerate pairing computation in the following section.

Definition 1. *A twisted Jacobi quartic curve over* F_{q^m} *is given by:*

$$E_{d,a,\delta} : y^2 = dx^4 + 2a\delta^2 x^2 + \delta^4 \tag{4}$$

with $d, a \in F_q$, $\delta^2, \delta^4 \in F_{q^m}$ *and* $d \neq a^2$.

The following proposition is easily obtained from definition 1.

Proposition 1. *Let* $E_{d,a,\delta}$ *over* F_{q^m} *be a twist of* $E_{d,a}$*, The map*

$$\begin{array}{rccc} \phi : E_{d,a,\delta} & \longrightarrow & E_{d,a} \\ (x,y) & \longmapsto & (\frac{x}{\delta}, \frac{y}{\delta^2}) \end{array}$$

maps points on $E_{d,a,\delta}$ *to points on* $E_{d,a}$.

(a) If $a \neq 0$*, there exist quadratic twists when* $\delta^2, \delta^4 \in F_{q^{k/2}}$ *and* $\delta \in F_{q^k}$*, then* $m = k/2$*, choose* $(x,y) \in (F_{q^{k/2}}, F_{q^{k/2}})$ *we have* $(\frac{x}{\delta}, \frac{y}{\delta^2}) \in (F_{q^k}, F_{q^{k/2}})$*;*
(b) If $a = 0$*, there exist quartic twists when* $\delta^4 \in F_{q^{k/4}}$ *and* $\delta \in F_{q^k}$*, then* $m = k/4$*, choose* $(x,y) \in (F_{q^{k/4}}, F_{q^{k/4}})$ *we have* $(\frac{x}{\delta}, \frac{y}{\delta^2}) \in (F_{q^k}, F_{q^{k/2}})$.

6 Explicit formulae for Miller functions

Here we set the following notations which will be used in the rest of this paper.

M, S	multiplication and squaring in F_{q^k}
m, s	multiplication and squaring in F_q

Assume that embedding degree k is even. Now we give the formulae of Miller functions using quadratic twist technique.

From proposition 1, by quadratic twist map, point Q in the Tate pairing is chosen to be $(x/\delta, y/\delta^2) \in (F_{q^k}, F_{q^{k/2}})$, where $\delta \in F_{q^k}$, $\delta^2 \in F_{q^{k/2}}$, $(x, y) \in (F_{q^{k/2}}, F_{q^{k/2}})$ is a point on twisted Jacobi quartic curve $E_{d,a,\delta}$. From theorem 2, the Miller function

$$h(x_Q, y_Q) = \frac{x_Q^2}{y_Q + 1 - cx_Q^2}\left(\frac{y_Q + 1 + ax_Q^2}{x_Q^3} + \frac{1 + y_Q}{x_Q^2}s + t\right),$$

where $Q = (x_Q, y_Q) = (\delta^{-1}x, \delta^{-2}y)$. Write $s = M_1/N$, $t = M_2/N$, we have

$$\begin{aligned} h(\delta^{-1}x, \delta^{-2}y) &= \frac{\delta^{-2}x^2}{\delta^{-2}y+1-c\delta^{-2}x^2}\left(\frac{\delta^{-2}y+1+a\delta^{-2}x^2}{\delta^{-2}x^3}\delta + \frac{M_1}{N}\frac{1+\delta^{-2}y}{\delta^{-2}x^2} + \frac{M_2}{N}\right) \\ &= \frac{x^2}{N(y+\delta^2-cx^2)}(N \cdot \xi \cdot \delta + M_1 \cdot \eta + (M_2 - aM_1)), \end{aligned}$$

where $\xi = \frac{y+\delta^2+ax^2}{x^3}$, $\eta = \frac{y+\delta^2+ax^2}{x^2} = x \cdot \xi$.

Since $c, N \in F_q$, $x^2, y \in F_{q^{k/2}}$, then $\frac{x^2}{N(y+\delta^2-cx^2)} \in F_{q^{k/2}}$, so it can be discarded in pairing computation since it is well known that if $u \in F_{q^{k/2}}$ then $u^{\frac{q^k-1}{r}} = 1$. Now we only have to evaluate

$$N \cdot \xi \cdot \delta + M_1 \cdot \eta + M_3 \tag{5}$$

where $M_3 = M_2 - aM_1$.

We have the coefficients $\xi, \eta \in F_{q^{k/2}}$, $N, M_1, M_3 \in F_q$, $\delta \in F_{q^k}$. It is unnecessary to multiply $N \cdot \xi$ with δ since the element in F_{q^k} can be represented by $u + v \cdot \delta$ with $u, v \in F_{q^{k/2}}$. $N \cdot \xi$ and $M_1 \cdot \eta$ need $\frac{k}{2}m$ respectively. So only km are needed besides calculation in M_1, M_3 and N. Since $Q = (\delta^{-1}x, \delta^{-2}y)$ is fixed during pairing computation, ξ, η can be precomputed.

Now we deal with operations in M_1, M_3, N. For efficiency, the points are represented in extended homogeneous projective coordinate proposed by Hisil et al.[15]. $(X : Y : T : Z) = (\lambda X : \lambda Y : \lambda T : \lambda Z)$, and $T = X^2/Z$. Let $P_i = (X_i : Y_i : T_i : Z_i)$, $i = 1, 2, 3$.

6.1 Addition

When $P_1 \neq P_2$, rewrite the denominator of s and t in theorem 2 as follows:

$$\begin{aligned} N' &= x_1x_2(x_1^2(y_2 + 1) - x_2^2(y_1 + 1)) \\ &= \frac{X_1X_2}{Z_1^2Z_2^2}(T_1(Y_2 + Z_2) - T_2(Y_1 + Z_1)) \\ &= \frac{X_1X_2}{Z_1^2Z_2^2}((T_1Y_2 - Y_1T_2) + (T_1Z_2 - Z_1T_2)). \end{aligned}$$

The numerators of s and t can be rewritten as:

$$\begin{aligned} M_1' &= (y_1 + 1 + ax_1^2)x_2^3 - (y_2 + 1 + ax_2^2)x_1^3 \\ &= \frac{1}{Z_1^2Z_2^2}[(Y_1 + Z_1 + aT_1)X_2Z_1T_2 - (Y_2 + Z_2 + aT_2)X_1T_1Z_2]. \end{aligned}$$

$$\begin{aligned} M_2' &= (y_2 + 1 + ax_2^2)(y_1 + 1)x_1 - (y_1 + 1 + ax_1^2)(y_2 + 1)x_2 \\ &= \frac{1}{Z_1^2Z_2^2}[(Y_2 + Z_2 + aT_2)(Y_1 + Z_1)X_1Z_2 - (Y_1 + Z_1 + aT_1)(Y_2 + Z_2)Z_1X_2] \\ &= \frac{1}{Z_1^2Z_2^2}[(Y_1 + Z_1 + aT_1)(Y_2 + Z_2 + aT_2)(X_1Z_2 - X_2Z_1) + aM_1'Z_1^2Z_2^2]. \end{aligned}$$

Then we obtain:

$$\begin{aligned} M_1 &= (Y_1 + Z_1 + aT_1)X_2Z_1T_2 - (Y_2 + Z_2 + aT_2)X_1T_1Z_2, \\ M_3 &= (Y_1 + Z_1 + aT_1)(Y_2 + Z_2 + aT_2)(X_1Z_2 - Z_1X_2), \\ N &= X_1X_2[(T_1Y_2 - Y_1T_2) + (T_1Z_2 - Z_1T_2)]. \end{aligned}$$

We use the point addition formula proposed by Hisil, Wong, Carter, and Dawson[15].

$$\begin{aligned} X_3 &= (X_1Y_2 - Y_1X_2)(T_1Z_2 - Z_1T_2), \\ Y_3 &= (T_1Z_2 + Z_1T_2 - 2X_1X_2)(Y_1Y_2 - 2aX_1X_2 + Z_1Z_2 + dT_1T_2) - Z_3, \\ Z_3 &= (X_1Y_2 - Y_1X_2)^2. \end{aligned}$$

From above two formulae, $P_3 = P_1 + P_2$ and (M_1, M_3, N) are computed as follows:

$$\begin{aligned} &A = X_1X_2; B = Y_1Y_2; C = Z_1Z_2; D = T_1T_2; E = Y_1 + Z_1 + aT_1; \\ &F = Y_2 + Z_2 + aT_2; G = (X_1 - Z_1)(X_2 + Z_2) - A + C; \\ &H = (Y_1 + T_1)(Y_2 - T_2) - B + D; I = T_1Z_2; \\ &J = Z_1T_2; K = (X_1 - Y_1)(X_2 + Y_2) - A + B; \\ &M_1 = EJX_2 - FIX_1; M_3 = EFG; N = A(H + I - J); \\ &Z_3 = K^2; Y_3 = (I + J - 2A)(B - 2aA + C + dD) - Z_3; \\ &X_3 = K(I - J). \end{aligned}$$

As we will see in the following subsection, T_3 is not needed in the doubling step. Then the total cost of $P_3 = (X_3, Y_3, Z_3)$ and (M_1, M_3, N) is $18m + 1s + 3m_a + m_d$, where m_a, m_d denote the cost of multiplication by constant a and d. Since P_2 is fixed during pairing computation, let $Z_2 = 1$, then $P_2 = (x_2, y_2, x_2^2, 1)$. The cost of computing P_3 and (M_1, M_3, N) is $16m + 1s + 3m_a + m_d$. So the cost of addition step reduced to $1M + (k + 16)m + 1s + 3m_a + m_d$.

Results and performance comparison are summarized in Table 1.

Table 1. Costs of mixed addition step

	mixed addition
Weierstrass, $a_4 = -3$[1]	$1M + km + 6m + 6s$
Weierstrass, $a_4 = 0$[1]	$1M + km + 6m + 6s$
Edwards[16]	$1M + km + 14m + 4s + 1m_d$
twisted Edwards[1]	$1M + km + 12m$
Jacobi quartic	$1M + km + 16m + 1s + 3m_a + m_d$

6.2 Doubling

From Theorem 2, if $P_1 = P_2$, we obtain:

$$\begin{aligned} M_1 &= -(Y_1 + 2Z_1)X_1^2, \\ M_3 &= (aX_1^2 + Z_1^2 + Y_1Z_1)Y_1, \\ N &= 2X_1^3. \end{aligned}$$

The point doubling formula is also from [15].

$$\begin{aligned} X_3 &= 2X_1Y_1(2Z_1^2 + 2aX_1^2 - Y_1^2), \\ Y_3 &= 2Y_1^2(Y_1^2 - 2aX_1^2) - (2Z_1^2 + 2aX_1^2 - Y_1^2)^2, \\ Z_3 &= (2Z_1^2 + 2aX_1^2 - Y_1^2)^2. \end{aligned}$$

Now the explicit formulae for computing $P_3 = 2P_1$ and (M_1, M_3, N) are given as follows:

$$\begin{aligned} &A = X_1^2; B = Y_1^2; C = Z_1^2; D = (X_1 + Y_1)^2 - A - B; \\ &E = ((Y_1 + Z_1)^2 - B - C)/2; F = aA; G = C + F; H = B - 2F; \\ &I = 2G - B; X_3 = DI; Z_3 = I^2; Y_3 = 2BH - Z_3; \\ &M_1 = -(Y_1 + 2Z_1)A; M_3 = Y_1(G + E); N = 2AX_1. \end{aligned}$$

From the strategy proposed in [15], if a point doubling is followed by another point doubling, the above doubling formula is used, then the total cost of computing P_3 and (M_1, M_3, N) is $5m + 6s + 1m_a$, a doubling step in Miller's algorithm costs $1M+1S+(k+5)m+6s+1m_a$. If a point doubling is followed by a point addition, then $T_3 = D^2$ need to be computed in point doubling, and X_3 can be computed as $X_3 = ((D+I)^2 - T_3 - Z_3)/2$, the total cost of computing P_3 and (M_1, M_3, N) is $4m + 8s + 1m_a$, a doubling step in Miller's algorithm costs $1M + 1S + (k + 4)m + 8s + 1m_a$.

Results and performance comparison are summarized in Table 2.

Table 2. Costs of doubling step

	doubling
Weierstrass, $a_4 = -3$[1]	$1M + 1S + km + 6m + 5s$
Weierstrass, $a_4 = 0$[1]	$1M + 1S + km + 3m + 8s$
Edwards[16]	$1M + 1S + km + 8m + 4s + 1m_d$
twisted Edwards[1]	$1M + 1S + km + 6m + 5s$
Jacobi quartic	$1M + 1S + km + 4m + 8s + 1m_a$

Remark 3. If $a = 0$, the Jacobi quartic curve $y^2 = dx^4 + 1$ has quartic twists and Q can be chosen as $(x/\delta, y/\delta^2) \in (F_{q^k}, F_{q^{k/2}})$ where $x, y \in F_{q^{k/4}}$. In this case, pairing computation is more efficient compared to the quadratic twist case. The addition step needs $1M' + (k + 16)m + 1s + m_d$, the doubling step needs $1M' + 1S' + (k + 5)m + 6s$ or $1M' + 1S' + (k + 4)m + 8s$, where M', S' denote the multiplication and squaring in $\mathbb{F}_{q^{k/4}}$.

7 Construction of Pairing Friendly Jacobi Quartic Curves

In order to make the pairing computation on a Jacobi quartic curve feasible and efficient, the curve should be pairing friendly. In this section, we give two kinds of supersingular curves in Jacobi quartic form that can be constructed directly, then we give two examples of ordinary pairing friendly Jacobi quartic curves.

7.1 Supersingular Jacobi Quartic Curves

Let the elliptic curves we consider be defined over a finite field F_q and $char(F_q) > 3$. To get the supersingular curves in Jacobi quartic form, we make use of the birational equivalence between Weierstrass form and Jacobi quartic form which arises in [5], that is,

$$\begin{array}{ccc} y^2 = x^3 + bx + c & \longrightarrow & Y^2 = dX^4 + 2aX^2Z^2 + Z^4 \\ \mathcal{O}_E & \longmapsto & (0:1:1) \\ (e,0) & \longmapsto & (0:-1:1) \\ (x,y) & \longmapsto & (2(x-e):(2x+e)(x-e)^2 - y^2 : y) \end{array}$$

and the inverse map is

$$\begin{array}{rcl} (0:1:1) & \longmapsto & \mathcal{O}_E \\ (0:-1:1) & \longmapsto & (e,0) \\ (X:Y:Z) & \longmapsto & (\frac{2(Y+Z^2)}{X^2} - \frac{e}{2}, \frac{(4(Y+Z^2)-3eX^2)Z}{X^3}). \end{array}$$

where $\mathcal{O}_E$ is the point at infinity, $(e,0)$ is a point of order 2. The relation between the two equations is $d = -(3e^2+4b)/16$ and $a = -3e/4$. Two triplets $(X_1 : Y_1 : Z_1)$ and $(X_2 : Y_2 : Z_2)$ are equivalent if and only if there exists $t \neq 0$ such that $X_1 = tX_2$, $Y_1 = t^2Y_2$ and $Z_1 = tZ_2$.

There are two kinds of well known supersingular curves in Weierstrass form defined over prime field F_p, i.e., $y^2 = x^3 + bx$, $p \equiv 3 \mod 4$, and $y^2 = x^3 + c$, $p \equiv 2 \mod 3$. Since $\#E(F_p) = p+1$, there always exists a point of order 2, then by the birational equivalence, we obtain the corresponding supersingular Jacobi quartic form curves.

Case 1. $y^2 = x^3 + bx$, $p \equiv 3 \mod 4$. If Legendre symbol$(\frac{-b}{p}) = -1$, then there is only one point of order 2, that is $(e,0) = (0,0)$. The corresponding supersingular equation is

$$Y^2 = -\frac{b}{4}X^4 + Z^4.$$

Moreover, if $(\frac{-b}{p}) = 1$, then there are another two such points, namely $(\pm b^{\frac{p+1}{4}}, 0)$. In this case, it is also easy to get another two kinds of curves by the relations of equation parameters.

Case 2. $y^2 = x^3 + c$, $p \equiv 2 \mod 3$. By a simple calculation, we have that if $p \equiv 5 \mod 12$, then the only point of order 2 is $(-c^{1/3}, 0) = (-c^{(2p-1)/3}, 0)$; if $p \equiv 11 \mod 12$, there are another two such points $(c^{(2p-1)/3}(1 \pm \sqrt{-3})/2, 0)$. The supersingular Jacobi quartic curve corresponding to $(-c^{(2p-1)/3}, 0)$ is

$$Y^2 = -\frac{3e^2+4b}{16}X^4 - \frac{3e}{4}X^2Z^2 + Z^4$$

where $e = -c^{(2p-1)/3}$.

7.2 Ordinary Pairing Friendly Jacobi Quartic Curves

Pairing based cryptosystems require both the discrete logarithm problems on the curve and in the multiplicative group of the finite field F_{p^k} are intractable. Since the embedding degree k of supersingular curves defined over a prime field is only 2, and due to the MOV[19] and FR[10] reduction, the field F_p must be chosen much larger than that for the ordinary curves to achieve the same security level. So in order to make the implementation more efficient, ordinary pairing friendly curves are favorable.

It is obvious that a Jacobi quartic curve which always has a point of order 2 can only be transformed from a Weierstrass curve with even group order. Fortunately, pairing friendly curves with even cofactor can be produced by GMV[11] method and some other constructions which are provided by Freeman, Scott, and Teske[9]. Considering the efficiency of pairing computation and different security levels, we present two examples of pairing friendly Jacobi quartic curves with $k = 6, 8$ transformed from examples given in [1].

The first example has only quadratic twists while the second has quartic twists. Let the parameters $(k, D, \rho, F_p, d, a, h, r)$ represent a Jacobi quartic curve $Y^2 = dX^4 + 2aX^2Z^2 + Z^4$ defined over F_p, with the number of rational points $\#E(F_p) = hr$, $\rho = \frac{log(p)}{log(r)}$ and D be the discriminant in the construction.

Example 1. $k = 6$, $D = 7230$, $\rho = 1.22$, $\lceil log(p) \rceil = 201$, $\lceil log(r) \rceil = 165$,
$p = 2051613663768129606093583432875887398415301962227490187508801$,
$d = 1863953287635956721384182076223832049126572428227767512756240$,
$a = 631772460235361970180500642413596623379371813277881622943722$,
$h = 4 \cdot 7 \cdot 733 \cdot 2230663$,
$r = 448125454133085799139574382013313854347434423662 77$.

Example 2. $k = 8$, $D = 1$, $\rho = 1.50$, $\lceil log(p) \rceil = 337$, $\lceil log(r) \rceil = 224$,
$p = 233773665369910566926038390015691888142454746929295686689625913289090943703572348756028778874481604289$,
$d = 175330249027432925194528792511768916106841060196971765017219434966818207777679261567021584155861203219$,
$a = 0$,
$h = 4 \cdot 315669989 \cdot 558193107149 \cdot 14429732414341$,
$r = 22985796260053765810955211899935144604417092746113717429138553265289$.

8 Conclusion and Further Work

This paper presents a geometric interpretation of the group law on Jacobi quartic curves, from which explicit formulae of the Miller function for Tate pairing computation are obtained. The doubling step is efficient, whereas the addition step may require further improvement. We define twisted Jacobi quartic curves and use the twist map to accelerate the pairing computation on Jacobi quartic curves. Furthermore, we demonstrate the existence of quartic twists of Jacobi quartic curves with $a = 0$, and we give a numerical example of such curves.

As many formulae[4, 14, 15] have been proposed for the point addition on Jacobi quartic curves, future work may need to accelerate the addition step in the pairing computation and to identify more efficient formula.

References

1. Christophe Arene, Tanja Lange, Michael Naehrig, Christophe Ritzenthaler. Faster Computation of the Tate Pairing, available at http://eprint.iacr.org/2009/155.pdf
2. Paulo S.L.M.Barreto, Hae Yong Kim, Ben Lynn, and Michael Scott. Efficient algorithms for pairing-based cryptosystems. CRYPTO 2002, pp.354-368, 2002.
3. Daniel Bernstein, Perter Birkner, Marc Joye, Tanja Lange, and Christiane Peters. Twisted Edwards curves. Africacrypt 2008, pp.389-405, 2008.
4. Daniel Bernstein, Tanja Lange. Faster addition and doubling on elliptic curves. ASIACRYPT 2007. LNCS, vol. 4833, pp.29-50. 2007.
5. Olivier Billet and Marc Joye. The Jacobi Model of an Elliptic Curve and Side-Channel Analysis, AAECC 2003. LNCS, vol. 2643, pp.34-42, 2003.
6. Sanjit Chatterjee, Palash Sarkar, and Rana Barua. Efficient computation of Tate pairing in projective coordinate over general characteristic fields. ICISC 2004, LNCS, vol.3506, pp.168-181, 2005.
7. Craig Costello, Tanja Lange, Michael Naehrig. Faster Pairing Computations on Curves with High-Degree Twists, available at http://eprint.iacr.org/2009/615.pdf
8. Harold M.Edwards. A normal form for elliptic curves. Bulletion of the American Mathematical Society, 44:393-422, 2007.
9. David Freeman, Michael Scott, Edlyn Teske. A Taxonomy of Pairing-Friendly Elliptic Curves. J. Cryptology,23(2):224-280, 2010.
10. Gerhard Frey and Hans-Georg R*ü*ck. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. Math. Comp., 62(206):865-874, 1994.
11. Steven D.Galbraith, J.McKee, P.Valença. Ordinary abelian varieties having small embedding degree. Finite Fields Appl. 13, 800-814, 2007.
12. Darrel Hankerson, Alfred Menezes, Scott Vanstone. Guide to Elliptic Curve Cryptography, Springer-Verlag, New York, 2004.
13. Florian Hess, Pairing Lattices, Pairing 2008, LNCS, vol. 4833, pp.18-38, 2008.
14. Huseyin Hisil, Kenneth Koon-Ho Wong, Gary Carter, Ed Dawon. Faster Group Operations on Elliptic Curves, Australasian Information Security Conference(AISC 2009), Wellington, New Zealand(January 2009); Conferences in Research and Practice in Information Technology(CRPIT), vol. 98, pp.7-19, 2009.
15. Huseyin Hisil, Kenneth Koon-Ho Wong, Gary Carter, and Ed Dawson. Jacobi Quartic Curves Revisited, ACISP 2009, LNCS 5594, pp.452-468, 2009.
16. Sorina Ionica and Antoine Joux. Another approach to pairing computation in Edwards coordinates. INDOCRYPT 2008, pp.400-413, 2008.
17. Neal Koblitz, Elliptic curve cryptosystems. Mathematics of Computation, 48(5), pp. 203-209, 1987.
18. M.Prem Laxman Das and Palash Sarkar. Pairing Computation on Twisted Edwards Form Elliptic Curves, Pairing 2008, LNCS, vol.5209, pp.192-210, 2008.
19. Alfred Menezes, Tatsuaki Okamoto, and Scott Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. IEEE Trans. Inform. Theory, 39(5):1639-1646, 1993.

20. Victor S.Miller, Use of elliptic curves in cryptography. Advances in Cryptology-Proc. CRYPTO 85. LNCS, vol.218, pp. 417-428, 1986.
21. Victor S.Miller. The Weil pairing, and its efficient calculation. J. Cryptology,17(4):235-261, 2004.
22. F. Vercauteren. Optimal Pairings, available at http://eprint.iacr.org/2008/096.pdf