Pairing Computation in Jacobi Quartic Curves Using Weight Projective Coordinates

Yajuan Ren

College of Science, North China University of Technology, Beijing 100144, China

ncutszfx@163.com

Keywords: Elliptic curve; Jacobi quartic curve; Tate pairing; Miller function; Cryptography

Abstract. In this paper, we present the pairing computation on Jacobi quadric curves using weight projective coordinates. In our algorithm, the cost of addition step reduced to 1M+(k+9)m+3s+1m_t, and the cost of doubling step is 1M+1S+(k+3)m+8s+2m_a+1m_d.

Introduction

The fast algorithms for pairing computation play an important role in pairing-based cryptography. Generally, we using Miller's algorithm to compute pairing. Consequently, many improvements on Miller's algorithm were presented. A well-known elliptic curve model is Weierstrass model, and many efficient formulas for pairing computation for this model can be found in [1, 2, 3, 4, 5]. One of the ideas to make improvements is to try to compute pairings on other elliptic curve models which provide more efficient algorithms for the group law.

The use of Jacobi quartic curves in cryptology was explained in [6] and [7]. Then many other formulas for point addition and doubling on Jacobi quartic curves are given in the literature, see [8] for a brief development history of Jacobi quartic curves. While pairing computation on Jacobi quartic curves was proposed by Wang et al. [9] in 2011. In [10], Zhang et al. proposed a geometric approach to explain the group law on Jacobi quartic curves which are seen as the intersection of two quadratic surfaces in space. Using the geometry interpretation, we construct Miller function. Then we present explicit formulae for the addition and doubling steps in Miller's algorithm to compute the Tate pairing on Jacobi quartic curves. Note that they used the projective coordinates.

The cost of the algorithm for pairing computation over Jacobi quartic curves consists three parts: the cost of updating the point, the cost of updating the iteration function, and the cost of evaluating the Miller function at some point Q. In this paper, we using geometric interpretation of the group law on Jacobi quartic curves proposed in [10] and weight projective coordinates to compute Tate pairing of Jacobi quartic curves over finite field. In our algorithm, the cost of addition step reduced to $1M+(k+9)m+3s+1m_t$, and the cost of doubling step is $1M+1S+(k+3)m+8s+2m_a+1m_d$.

Note that we use m and s denote the costs of multiplication and squaring in the base field F_q; M and S denote the costs of multiplication and squaring in the extension field F_{q^k}; m_c denotes the cost of multiply by a constant in the base field.

Preliminaries

In this section we briefly review the preliminaries of Tate pairing and the background of Jacobi quartic curves.

Tate Pairing. Let F_q be a finite field, p is an odd prime, $q=p^n,(3,q)=1$. E be an elliptic curve defined over F_q with neutral element denoted by O. n is a prime, $n|\#\mathrm{E}(\mathrm{F_q})$. Let $k>1$ denote the embedding degree with respect to n, that is k is the smallest integer such that $n\,|\,q^k-1$. For any point $P\in E(F_q)[n]$, there exists a rational function f_P defined over F_q such that $div(f_p)=n(P)-n(O)$. The rational function is unique up to a non-zero scalar multiple according to Riemann-Roach theorem. The group of n-th roots of unity in F_{q^k} is denoted by μ_n. The reduced Tate pairing is then defined as

$$T_n : E(F_q)[n] \times E(F_{q^k}) \to \mu_n : \ (P,Q) \mapsto f_P(Q)^{(q^k-1)/n}.$$

The rational function f_P can be computed in polynomial time by using Miller's algorithm ([5]). Let $n = (n_{l-1}, \cdots, n_1, n_0)_2$ be the binary representation of n ,where $n_{l-1} = 1$ .Let $g_{T,S} \in F_q(E)$ be the rational function with divisor $div(g_{T,S}) = (T) + (S) - (O) - (T+S)$, where $T+S$ denotes the sum of T and S on E ,and additions of the form $(T)+(S)$ denote formal addition in the divisor group. The Miller's algorithm which starts with $T = P,\ f = 1$ is as follows:

Algorithm 1 Miller's algorithm

Output: $n = \sum_{i=0}^{l-1} n_i 2^i$ **,** where $n_i \in \{0,1\}. P \in E(F_q), Q \in E(F_{q^k})$

return $f_n^{(q^k-1)/n}(Q)$

1: $f \leftarrow 1, T \leftarrow P$

2: **for** $i = l-2$ down to 0 do **do**

3: $f \leftarrow f^2 \cdot g_{T,T}(Q), T \leftarrow [2]T$

4: **if** ni = 1 then **then**

5: $f \leftarrow f \cdot g_{T,P}(Q), T \leftarrow T+P$

6: **end if**

7: **end for**

8: return $f_n^{(q^k-1)/n}$

The Jacobi Quartic Curves. A Jacobi quartic elliptic curve over a finite field F_q is defined by the following equation $E_{a,d} : y^2 = dx^4 + 2ax^2 + 1$ where $d, a \in F_q$ and the discriminant

$\Delta = 256(a^2 - d)^2 \neq 0$. In [7], Billet and Joye proved that if $E : y^2 = x^3 + ax + b$ has a point of order 2 then E is bi-rationally equivalent to a Jacobi quartic curve. The projective closure of $E_{a,d}$ in P^2 is

$\{(X:Y:Z) \in P^2 : Y^2 Z^2 = dX^4 + 2aX^2Y^2 + Z^4\}$. This curve consists of the points (x,y) on the affine curve $E_{a,b}$, embedded as usual into P^2 by $(x,y) \mapsto (x:y:1)$, and extra points at infinity, i.e., points when $Z = 0$ .There is exactly one infinity point, namely $O = (0:1:0)$.This point is singular.

In fact, the Jacobi quartic curve can be seen as the intersection of quadratic surfaces in space. That is, the Jacobi quartic curve can be written as the form

$$J_{a,d} : 2aX^2 + Z^2 + dW^2 - Y^2 = 0, X^2 - ZW = 0$$

With the projective coordinates $(X:Y:W:Z)$, the identity element is represented by the quadruplet $O = (0:1:0:1)$. The negative of $(X:Y:W:Z)$ is $(-X:Y:W:Z)$.

In [10], a geometric interpretation of the group law on Jacobi quartic curves was presented. A projective plane is given by a homogeneous projective equation $\Pi = 0$. By abuse of notation we still use the symbol Π to denote the projective plane. Since the intersection of Π and $J_{a,d}$ is the intersection of two quadratic curves on the projective plane, any plane Π intersects $J_{a,d}$ at exactly four points, counted with appropriate multiplicities. The divisor of Π is defined as:

$$div(\Pi) = \sum_{R \in \Pi \cap J_{a,d}} n_R(R)$$

Where n_R is the intersection multiplicity of Π and $J_{a,d}$ at the point R.Then the quotient of two projective planes is a well-defined function which gives a principal divisor. As we will see, this divisor leads to the geometric interpretation of the group law on $J_{a,d}$.

Lemma 1. ([10]) For Jacobi quartic curve $J_{a,d}$ with neutral element $O = (0:1:0:1)$. Then 4 points (not necessary distinct) P_1, P_2, P_3 and P_4 satisfy $P_1 + P_2 + P_3 + P_4 = O$ if and only if there is a plane Π with $div(\Pi) = (P_1) + (P_2) + (P_3) + (P_4)$.

Theorem 2. ([10]) Let $J_{a,d} : 2aX^2 + Z^2 + dW^2 - Y^2 = 0, X^2 - ZW = 0$ be a Jacobi quartic curve, $O = (0:1:0:1)$. Let $P_1 = (X_1: Y_1: W_1: Z_1)$, $P_2 = (X_2: Y_2: W_2: Z_2)$ be two points on $J_{a,d}$. Let $P_3 = P_1 + P_2 = (X_1: Y_1: W_1: Z_1)$. Then Miller function $g_{P_1,P_2}(X,Y,W,Z)$ which satisfies

$$div(g_{P_1,P_2}) = (P_1) + (P_2) - (P_3) - (O) \text{ is } g_{P_1,P_2}(X,Y,Z,W) = \frac{\prod_{P_1,P_2,O}}{\prod_{P_3,O,O}} = \frac{C_X X + C_Y(Y-Z) + C_W W}{W_3(Y-Z) + (Z_3 - Y_3)W}.$$

In the case $P_1 \neq P_2$ and $P_1, P_2 \neq O$, the coefficients are given by

$$C_X = W_1(Z_2 - Y_2) - W_2(Z_1 - Y_1), C_Y = X_2W_1 - X_1W_2, C_W = X_2(Z_1 - Y_1) - X_1(Z_2 - Y_2).$$

If $P_1 = P_2 \neq O$, the coefficients are given by

$$C_X = 2aX_1W_1 + 2X_1(Z_1 - Y_1), C_Y = -Y_1W_1, C_W = dW_1^2 - Z_1^2 + Y_1Z_1.$$

Pairing Computation Using Weighted Projective Coordinates

For Jacobi quartic curves, the weighted projective coordinates which represent the points as $(X:Y:Z) = (\lambda X : \lambda^2 Y : \lambda Z)$ for all nonzero $\lambda \in F_q$ on the curve

$$JW_{a,d} : Y^2 = dX^4 + 2aX^2Z^2 + Z^4.$$

Unlike the homogeneous projective case, this curve is non-singular provided that $\Delta \neq 0$ (see [8]). Billet and Joye [7] proposed a faster inversion-free unified addition algorithm on the curve
$Y^2 = dX^4 + 2aX^2Z^2 + Z^4$.
The point addition in projective weighted coordinates are given by [5]:
$(X_3 : Y_3 : Z_3) = (X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2)$
where
$X_3 = X_1Z_1Y_2 + Y_1X_2Z_2,\ Z_3 = Z_1^2Z_2^2 - X_1^2X_2^2,$
$Y_3 = (X_1X_2 + Z_1Z_2)^2((X_1^2 + Z_1^2)(X_2^2 + Z_2^2) + Y_1Y_2 + (2a-2)X_1Z_1X_2Z_2) - X_3^2 - Z_3^2$
The doubling formula in projective weighted coordinates are given by [5]:
$(X_3 : Y_3 : Z_3) = [2](X_1 : Y_1 : Z_1)$
where
$X_3 = 2X_1Y_1Z_1, Z_3 = Z_1^4 - X_1^4, Y_3 = 2Y_1^4 - aX_3^2 - Z_3^2.$

Formula of Tate Pairing Using Weighted Projective Coordinates. Let $\theta \in F_{q^k}$ such that $\theta^2 \in F_{q^{k/2}}, \theta^4 \in F_{q^{k/4}},$ and $\theta^3 \notin F_{q^{k/2}}$. That is $1, \theta, \theta^2, \theta^3$ is a basis of F_{q^k} as a vector space over $F_{q^{k/4}}$.

For a point $(X:Y:Z)$ on the curve $JW_\theta : Y^2 = d\theta^4 X^4 + 2a\theta^2 X^2 Z^2 + Z^4$, then $(\theta X : Y : Z)$ be a point on $Y^2 = dX^4 + 2aX^2Z^2 + Z^4$. Hence, choose $Q^{'} = (X_{Q^{'}} : Y_{Q^{'}} : Z_{Q^{'}}) \in JW_\theta(F_{q^{k/2}})$, then

$Q = (X_Q : Y_Q : Z_Q) = (\theta X_{Q^{'}} : Y_{Q^{'}} : Z_{Q^{'}}) \in JW_{a,d}(F_{q^k})$.

Here, let $x = X/Z$ and $y = Y/Z^2$.

From Theorem 2, the Miller function

$h(x,y) = (c_x x + c_y(y-1) + c_{x^2}x^2)/(x_3^2 y + (1-y_3)x^2 - x_3^2)$.

Therefore, in weighted projective coordinates, for addition step, the Miller function

$$h(x_Q, y_Q) = \frac{c_x x_Q + c_y(y_Q - 1) + c_{x^2}x_Q^2}{x_3^2 y_Q + (1-y_3)x_Q^2 - x_3^2} = \frac{x_{Q^{'}}^2\theta^2}{x_3^2 y_{Q^{'}} + (1-y_3)\theta^2 x_{Q^{'}}^2 - x_3^2}\cdot\left(c_x\cdot\frac{1}{\theta x_{Q^{'}}} + c_y\cdot\frac{y_{Q^{'}}-1}{\theta^2 x_{Q^{'}}^2} + c_{x^2}\right)$$

$$= \frac{x_{Q^{'}}^2\theta^2}{x_3^2 y_{Q^{'}} + (1-y_3)\theta^2 x_{Q^{'}}^2 - x_3^2}\cdot\left(c_x\cdot\zeta\cdot\theta + c_y\eta + c_{x^2}\right)$$

$$= \frac{x_{Q^{'}}^2\theta^2}{x_3^2 y_{Q^{'}} + (1-y_3)\theta^2 x_{Q^{'}}^2 - x_3^2}\cdot\frac{1}{Z_1^2 Z_2^2}\cdot\left(C_X\cdot\zeta\cdot\theta + C_Y\eta + C_{X^2}\right)$$

Where $\zeta = \dfrac{1}{\theta^2 x_{Q^{'}}}, \eta = \dfrac{y_{Q^{'}}-1}{\theta^2 x_{Q^{'}}^2}$. Since $x_3, y_3, y_{Q^{'}}, Z_1, Z_2$ and θ^2 all belong to $F_{q^{k/2}}$, then $\dfrac{x_{Q^{'}}^2\theta^2}{x_3^2 y_{Q^{'}} + (1-y_3)\theta^2 x_{Q^{'}}^2 - x_3^2}\cdot\dfrac{1}{Z_1^2 Z_2^2} \in F_{q^{k/2}}$ .So it can be discarded in pairing computation, so we only have to evaluate $C_X\cdot\zeta\cdot\theta + C_Y\cdot\eta + C_{X^2}$.

Weighted Projective Coordinates. Let $T = (X_1 : Y_1 : Z_1), P = (X_2 : Y_2 : Z_2) \in JW_{ad}$ and $T + P = (X_3 : Y_3 : Z_3)$. We represent a point with $Z \neq 0$ using the sextuplet $(X : Y : Z : X^2 : Z^2 : XZ)$, using this redundant coordinates.

Addition Step. From Theorem 2, we can get in addition step:

$C_X = X_1^2(Z_2^2 - Y_2) - X_2^2(Z_1^2 - Y_1), C_Y = X_1^2 X_2 Z_2 - X_2^2 X_1 Z_1, C_{X^2} = X_2 Z_2(Z_1^2 - Y_1) - X_1 Z_1(Z_2^2 - Y_2)$

Let $t = 2(a-1)$the addition step in pairing computation $T + P$ and C_X, C_Y, C_{X^2} are computed as follows:

$A_1 = X_1^2, B_1 = Z_1^2, C_1 = X_1 Z_1,\ A_2 = X_2^2, B_2 = Z_2^2, C_2 = X_2 Z_2,$

$D = A_1\cdot A_2,\ E = B_1\cdot B_2,\ F = C_1\cdot C_2,\ G = Y_1\cdot Y_2,\ H = D + E + 2F, I = (B_1 - Y_1)\cdot(B_2 - Y_2),$

$J = (A_1 + B_1)\cdot(A_2 + B_2) + tF + G, K = A_3 + B_3,\ Z_3 = E - D,$

$A_3 = X_3^2, B_3 = Z_3^2, X_3 = (C_1 + Y_1)\cdot(C_2 + Y_2) - F - G,$

$Y_3 = H\cdot J - K, C_3 = ((X^3 + Z^3)^2 - K)/2,\ C_X = (A_1 - B_1 + Y_1)\cdot(A_2 + B_2 - Y_2) - D + I,$

$C_Y = (A_1 - C_1)\cdot(A_2 + C_2) - D + F,\ C_{X^2} = (C_2 - B_2 + Y_2)\cdot(C_1 + B_1 - Y_1) - F + I.$

Then the total cost of computation $T + P = (X_3\text{:}\ Y_3\text{:}\ Z_3\text{:}\ X_3^2 : Z_3^2 : X_3 Z_3)$ and C_X, C_Y, C_{X^2} is $10m + 3s + 1m_t$, where m_t denote the cost of multiplication by constant $t = 2(a-1)$. Since P is fixed during pairing computation, let $Z_2 = 1$ .The cost of computing $T + P$ and C_X, C_Y, C_{X^2} is $9m + 3s + 1m_t$.So the cost of addition step reduced to $1M + (k+9)m + 3s + 1m_t$.

Doubling Step. From Theorem 2, we can get in doubling step:

$C_X = 2aX_1^3 Z_1 + 2X_1 Z_1(Z_1^2 - Y_1), C_Y = -X_1^2 Y_1, C_{X^2} = dX_1^4 + Y_1 Z_1^2 - Z_1^4.$

Using the redundant coordinates $(X_1 : Y_1 : Z_1 : X_1^2 : Z_1^2 : X_1Z_1)$, the doubling step in pairing computation $2P$ and C_X, C_Y, C_{X^2} can be computed as follows:

$$A = X_1^2,\ B = Z_1^2, C = X_1Z_1, H = A^2, I = B^2,\ X_3 = 2Y_1 \cdot C, Z_3 = I - H,$$

$$D = X_3^2, E = Z_3^2, F = \left(\left(X_3 + Z_3\right)^2 - D - E\right)/2,\ J = Y_1^2,\ Y_3 = 2J^2 - aD - E,$$

$$C_X = 2C \cdot \left(aA + \left(B - Y_1\right)\right),\ C_Y = -A \cdot Y_1,\ C_{X^2} = dH + \left(\left(Y_1 + B\right)^2 - J - I\right)/2 - H$$

Then the total cost of the coordinates of $2P$ and C_X, C_Y, C_{X^2} is $3m + 8s + 2m_a + 1m_d$. So the cost of doubling step is $1M + 1S + \left(k + 3\right)m + 8s + 2m_a + 1m_d$.

Acknowledgments

This work was supported by National Natural Science Foundation of China (No.61370187) and the General program of science and technology development project of Beijing Municipal Education Commission (KM201510009013).

References

[1] L. Li, H. Wu and F. Zhang: *Proc. The 9th China International Conference on Information Security and Cryptologyp* (Guangzhou, China, Nov.27-Nov.30, 2013), Vol. 8567, p.185.

[2] S. Chatterjee, P. Sarkar, R. Barua: *Proc. Information Security and Cryptology-ICISC 2004* (Seoul, Korea, December 2-3, 2004), Vol. 3506, p. 168.

[3] C. Costello, T. Lange and M. Naehrig: *Proc. 13th International Conference on Practice and Theory in Public Key Cryptography 2010* (Paris, France, May 26-28, 2010), Vol. 6056, P. 224.

[4] N. Koblitz and A.J. Menezes: Cryptography and Coding, Vol. 3796 (2005), p. 13.

[5] V.S. Miller: Journal of Cryptology, Vol. 17 (2004) No. 44, p. 235.

[6] D.V. Chudnovsky and G.V. Chudnovsky: Advances in Applied Mathematics, Vol.7 (1986) No. 4, p.385.

[7] O. Billet and M. Joye: *Proc. Applied Algebra, Algebraic Algorithms and Error-Correcting Codes-AAECC 2003* (Toulouse, France, May 12-16, 2003), Vol. 2643, p.34.

[8] H. Hisil, Kenneth Koon-Ho Wong: *Proc. 14th Australasian Conference ACISP 2009* (Brisbane, Australia, July 1-3, 2009), Vol. 5594, p. 452.

[9] H. Wang, K. Wang, L. Zhang and B. Li: Chinese Journal of Electronics, Vol. 20(2011) No. 4, p. 655.

[10] F. Zhang, L. Li and H. Wu: *Proc. 6th International Conference INTRUST 2014* (Beijing, China, December 16-17, 2014), Vol. 9473, p. 310.

[11] H. Hisil, K.K.-H. Wong, G. Carter and E. Dawson: *Proc. Seventh Australasian Information Security Conference AISC 2009* (Wellington, New Zealand, January 11-15, 2009), Vol. 98, p. 7.