Faster Pairing Computation on Jacobi quartic Curves with High-Degree Twists

Liangze Li[1], Hongfeng Wu[2⋆], Fan Zhang[1]

[1] LMAM, School of Mathematical Sciences, Peking University, Beijing 100871, China
[2] College of Sciences, North China University of Technology, Beijing 100144, China
liliangze2005@163.com, whfmath@gmail.com, viczf@pku.edu.cn

Abstract. In this paper, we propose an elaborate 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 the Miller function. Then we present explicit formulae for the addition and doubling steps in Miller's algorithm to compute Tate pairing on Jacobi quartic curves. Both the addition step and doubling step of our formulae for Tate pairing computation on Jacobi curves are faster than previously proposed ones. Finally, we present efficient formulas for Jacobi quartic curves with twists of degree 4 or 6. For twists of degree 4, both the addition steps and doubling steps in our formulas are faster than the fastest result on Weierstrass curves. For twists of degree 6, the addition steps of our formulae are faster than the fastest result on Weierstrass curves.

Keywords: Elliptic curve, Jacobi quartic curve, Tate pairing, Miller function, Group law

1 Introduction

In recent years, pairings on elliptic curves have become extremely useful in cryptography, and pairing-based cryptography develops rapidly. The efficient algorithms for pairing computation play a very important role in pairing-based cryptograph. The well-known method for pairing computation is Miller's algorithm. Consequently, many improvements on Miller's algorithm were presented. The Weierstrass model is widely used in the early stage of elliptic curves cryptography, and many efficient formulae for pairing computation for this model can be found in [1, 7, 5, 14, 16].

One of the ideas to make improvements is to compute pairings on other elliptic curve models which provides more efficient algorithms for the group law. Various elliptic curve models and coordinate systems reveal different efficiency of pairing computation. So it's very necessary to carry out more research on pairing computation for different models of elliptic curves. Recently, other models, for

⋆ Corresponding author.Supported in part by the National Natural Science Foundation of China (No. 11101002)

example, Edwards curves [9, 2] and twisted Edwards curves [3] are widely used. Pairing computation on twisted Edward curves was first considered by Das and Sarkar [8] and Ionic and Joux [13]. Then, in 2009, Arène, Lange et al.[1] developed explicit formulae for pairing computation on twisted Edwards curves. Arène, Lange et al.'s formulae for computing the Tate pairing on Edwards curves are as fast as the fastest previously published formulaes on Weierstrass curves.

The use of Jacobi quartic curves in cryptology was explained in [6] and [4]. Then many other formulae for point addition and doubling on Jacobi quartic curves are given in the literatures, see [11] for a brief development history of Jacobi quartic curves. Later while pairing computation on Jacobi quartic curves was proposed by Wang et al. [12] in 2011. A complicated geometric interpretation of Jacobi quartic curves was given in [12]. They pointed out that the doubling step of their algorithm for computing Tate pairing was competitive with that for Weierstrass curves and Edwards curves. However the addition step of Wang et al.'s algorithm needs to be optimized.

The cost of the algorithm for pairing computation over Jacobi quartic curves consist 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 present a geometric interpretation of the group law on Jacobi quartic curves which is based on the observation that they can be seen as the intersection of two quadratic surfaces in space. For general elliptic curves given by intersection of two quadratic surfaces, the geometric interpretation of group law had been discussed by Merriman et al. in [15]. And we put it into a more elaborate description for Jacobi quartic curves. Using the geometric interpretation we construct the Miller function. Then, we present explicit formulae for the addition step and doubling step in Miller's algorithm to compute Tate pairing on Jacobi quartic curves. The Miller function in this paper can reduce the cost of updating the iteration function in Miller's algorithm. So, both the addition step and doubling step of our formulae for pairing computation on Jacobi quartic curve are faster than that proposed by Wang et al. [12]. Finally, to reduce the cost of evaluating the Miller function on Jacobi quartic curves, we employ quadratic, quartic or sextic twists to our formulae. The high-twists had been sufficiently studied by Costello, Lange and Naehrig[7] on Weierstrass curves. But only quadratic and quartic twist had been studied for Jacobi quartic curves in [12, 10]. We overcome the complexity of sextic twists formulas, and the costs of substituting in $j = 0$ case reduce to a third. For twists of degree 4, both the addition steps and double steps in our formulae for Tate pairing computation on Jacobi quartic curves are faster than the fastest result on Weierstrass curves. For twists of degree 6, the addition steps in our formulae for Tate pairing computation on Jacobi quartic curves are faster than the fastest result on Weierstrass curves, while the doubling steps are a little slower than the fastest result on Weierstrass curves.

The remainder of this paper is organized as follows: Section 2 recalls the preliminaries of Tate pairing and Miller algorithm; the background of Jacobi quartic curves. Section 3 introduces the geometric interpretation of the group law

on Jacobi quartic curves. Section 4,5 propose explicit formulae of Tate pairing on Jacobi quartic curves in. Section 6 shows high-degree twists pairing computation. Finally we conclude the paper.

Note that we use $\mathbf{m}$ and $\mathbf{s}$ denote the costs of multiplication and squaring in the base field $\mathbb{F}_q$; $\mathbf{M}$ and $\mathbf{S}$ denote the costs of multiplication and squaring in the extension field $\mathbb{F}_{q^k}$; $\mathbf{m_c}$ denotes the cost of multiply by a constant in the base field.

2 Preliminaries

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

2.1 Tate pairing

Let $p > 3$ be a prime and $\mathbb{F}_q$ be a finite field with $q = p^n$. E is an elliptic curve defined over $\mathbb{F}_q$ with neutral element denoted by O. r is a prime such that $r|\#E(\mathbb{F}_q)$. Let $k > 1$ denote the embedding degree with respect to r, i.e. k is the smallest positive integer such that $r|q^k - 1$. For any point $P \in E(\mathbb{F}_q)[r]$, there exists a rational function f_P defined over $\mathbb{F}_q$ such that $\mathrm{div}(f_P) = r(P) - r(O)$, which is unique up to a non-zero scalar multiple. The group of r-th roots of unity in $\mathbb{F}_{q^k}$ is denoted by μ_r. The reduced Tate pairing is then defined as follows:

$$T_r : \ E(\mathbb{F}_q)[r] \times E(\mathbb{F}_{q^k}) \to \mu_r : \ (P, Q) \mapsto f_P(Q)^{(q^k-1)/r}.$$

The rational function f_P can be computed in polynomial time by using Miller's algorithm ([16]). Let $r = (r_{l-1}, \cdots, r_1, r_0)_2$ be the binary representation of r, where $r_{l-1} = 1$. Let $g_{P_1,P_2} \in \mathbb{F}_q(E)$ be the rational function satisfying $\mathrm{div}(g_{P_1,P_2}) = (P_1) + (P_2) - (O) - (P_1 + P_2)$, where $P_1 + P_2$ denotes the sum of P_1 and P_2 on E, and additions of the form $(P_1) + (P_2)$ denote formal additions in the divisor group. The Miller's algorithm starts with $T = P, f = 1$ is written below as Algorithm 1.

2.2 The Jacobi quartic curves

A Jacobi quartic elliptic curve defined over a finite field $\mathbb{F}_q$ is given by the following equation:

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

where $d, a \in \mathbb{F}_q$, $d \neq 0$ and the discriminant $\triangle = 256(a^2 - d)^2 \neq 0$. In [4], O.Billet and M.Joye proved that if an elliptic curve defined over $\mathbb{F}_q$ has an $\mathbb{F}_q$-point of order 2 then E is birationally equivalent to a Jacobi quartic curve over $\mathbb{F}_q$.

The projective closure of $E_{a,d}$ in $\mathbb{P}^2$ is

$$\{(X : Y : Z) \in \mathbb{P}^2 : Y^2Z^2 = dX^4 + 2aX^2Z^2 + Z^4\}.$$

Algorithm 1 Miller's algorithm

Ensure: $r = \sum_{i=0}^{l-1} r_i 2^i$, where $r_i \in \{0,1\}$. $P \in E(\mathbb{F}_q), Q \in E(\mathbb{F}_{q^k})$.
return $f_r^{(q^k-1)/r}(Q)$
1: $f \leftarrow 1, T \leftarrow P$
2: **for** $i = l-2$ down to 0 do **do**
3: $f \leftarrow f^2 \cdot g_{T,T}(Q), T \leftarrow 2T$
4: **if** $r_i = 1$ then **then**
5: $f \leftarrow f \cdot g_{T,P}(Q), T \leftarrow T + P$
6: **end if**
7: **end for**
8: return $f^{(q^k-1)/r}$

This curve consists of the points (x, y) on the affine curve $E_{a,d}$, embedded as usual into $\mathbb{P}^2$ 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 $\Omega = (0 : 1 : 0)$. This point is singular.

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

$$J_{a,d}: \quad 2aX^2 + Z^2 + dW^2 - Y^2 = 0,\ X^2 - ZW = 0. \tag{1}$$

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 $(-X : Y : W : Z)$.

Dedicated point addition in $J_{a,d}$ Given $P_1 = (X_1 : Y_1 : W_1 : Z_1)$ and $P_2 = (X_2 : Y_2 : W_2 : Z_2)$ be two different points on E. Let $P_1 + P_2 = (X_3 : Y_3 : W_3 : Z_3)$, the dedicated point addition is given in [11] as follows:

$$\begin{aligned} X_3 &= (X_1Y_2 - Y_1X_2)(W_1Z_2 - Z_1W_2), \\ Y_3 &= (Y_1Y_2 - 2aX_1X_2)(W_1Z_2 + Z_1W_2) - 2X_1X_2(Z_1Z_2 + dW_1W_2), \\ Z_3 &= (X_1Y_2 - Y_1X_2)^2, \\ W_3 &= (W_1Z_2 - Z_1W_2)^2 \end{aligned} \tag{2}$$

Without any assumption on the curve constants, Y_3 can be alternatively written as:

$$Y_3 = (W_1Z_2 + Z_1W_2 - 2X_1X_2)(Y_1Y_2 - 2aX_1X_2 + Z_1Z_2 + dW_1W_2) - Z_3.$$

Dedicated point doubling in $J_{a,d}$ If $P_1 = P_2$, let $2P_1 = (X_3 : Y_3 : W_3 : Z_3)$, the dedicated point doubling is given in [11] as follows:

$$\begin{aligned} X_3 &= 2X_1Y_1(2{Z_1}^2 + 2a{X_1}^2 - {Y_1}^2), \\ Y_3 &= 2{Y_1}^2({Y_1}^2 - 2a{X_1}^2) - (2{Z_1}^2 + 2a{X_1}^2 - {Y_1}^2)^2, \\ Z_3 &= (2{Z_1}^2 + 2a{X_1}^2 - {Y_1}^2)^2, \\ W_3 &= 4{X_1}^2{Y_1}^2 \end{aligned} \tag{3}$$

3 Geometric interpretation of the group law over $J_{a,d}$

To give an elaborate geometric interpretation of the group law on Jacobi quartic curves, we consider projective planes which are given by homogeneous projective equations $\Pi = 0$. In this paper, we still use the symbol Π to denote projective planes. In fact, any plane Π intersects $J_{a,d}$ at exactly four points, counted with appropriate multiplicities. Although these planes are not functions on $J_{a,d}$, their divisors can be well defined as:

$$\mathrm{div}(\Pi) = \sum_{R \in \Pi \cap J_{a,d}} n_R(R) \tag{4}$$

where n_R is the intersection multiplicity of Π and $J_{a,d}$ at 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.

When saying plane Π passes three points P_1, P_2 and P_3(not necessary distinct), which means Π exactly satisfies $\mathrm{div}(\Pi) \geq (P_1) + (P_2) + (P_3)$. In fact, by Riemann-Roch theorem or by explicit discussion on multiplicity, one can prove that there exists a unique plane which satisfies that inequality. So we may denote this plane by Π_{P_1,P_2,P_3} from now on.

Abel-Jacobi theorem connects the group law with principal divisor. And we can get the lemma below.

Lemma 1 *For quartic Jacobi curve $J_{a,d}$ with neutral element $O = (0 : 1 : 0 : 1)$. 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* $\mathrm{div}(\Pi) = (P_1) + (P_2) + (P_3) + (P_4)$.

Proof. Firstly, it is an easy calculation to get that $\mathrm{div}(Y - Z - aW) = 4(O)$.

Then the "if" part follows directly: if $\mathrm{div}(\Pi) = (P_1) + (P_2) + (P_3) + (P_4)$, the principal divisor $\mathrm{div}(\frac{\Pi}{Y-Z-aW}) = (P_1) + (P_2) + (P_3) + (P_4) - 4(O)$ is translated to equation $P_1 + P_2 + P_3 + P_4 = O$ by the Abel-Jacobi Theorem.

For the "only if" part, suppose $P_1 + P_2 + P_3 + P_4 = O$. Consider the plane Π_{P_1,P_2,P_3}, we can assume that $\mathrm{div}(\Pi_{P_1,P_2,P_3}) = (P_1) + (P_2) + (P_3) + (P_4')$, so it derives $P_1 + P_2 + P_3 + P_4' = O$ from the "if" part. Then we get $P_4 = P_4'$, i.e. $\mathrm{div}(\Pi_{P_1,P_2,P_3}) = (P_1) + (P_2) + (P_3) + (P_4)$. □

By this lemma, we can easily construct planes to give the group law: The fourth intersection of $\Pi_{P_1,O,O}$ and the curve is $-P_1$ i.e. the negative point of P_1. The fourth intersection of $\Pi_{P_1,P_2,O}$ and the curve is $-P_1 - P_2$, and its negative point gives $P_1 + P_2$. Actually, this geometric interpretation is parallel with the tangent and chord law for the cubic plane curves.

The neutral element we chose here is the same with that of [11], so we can claim that our explicit formulae for in negative point, point addition and point doubling are equivalent with that of [11].

4 Miller Function over $J_{a,d}$

4.1 Construction of Miler function

In this section we construct the Miller function over $J_{a,d}$. Let P_1 and P_2 be two points on $J_{a,d}$, by Lemma 1 we can get:

$$\begin{aligned}\mathrm{div}(\Pi_{P_1,P_2,O}) &= (P_1) + (P_2) + (-P_1 - P_2) + (O)\\ \mathrm{div}(\Pi_{P_1+P_2,O,O}) &= (P_1 + P_2) + 2(O) + (-P_1 - P_2)\end{aligned}$$

Thus,

$$\mathrm{div}(\frac{\Pi_{P_1,P_2,O}}{\Pi_{P_1+P_2,O,O}}) = (P_1) + (P_2) - (P_1 + P_2) - (O)$$

So for addition steps, the Miller function $g_{T,P}$ over $J_{a,d}$ can be given by setting $P_1 = T, P_2 = P$:

$$g_{T,P} = \frac{\Pi_{T,P,O}}{\Pi_{T+P,O,O}} \tag{5}$$

For doubling steps, we set $P_1 = P_2 = T$, and the Miller function $g_{T,T}$ over $J_{a,d}$ is given as:

$$g_{T,T} = \frac{\Pi_{T,T,O}}{\Pi_{2T,O,O}} \tag{6}$$

Then the remainder work is to compute the equation of these planes. The planes we use are of the form $C_X X + C_Y(Y - Z) + C_W W = 0$, because they always pass through $O = (0 : 1 : 0 : 1)$. Thus we only need to compute C_X, C_Y and C_W. To get a unified description, we use P_1, P_2 for both addition and doubling steps, and consider $P_1 \neq P_2$ and $P_1 = P_2$ respectively when necessary. Assume that $P_1 = (X_1 : Y_1 : W_1 : Z_1), P_2 = (X_2 : Y_2 : W_2 : Z_2)$ and $P_3 = P_1 + P_2 = (X_3 : Y_3 : W_3 : Z_3)$.

4.2 Equation of $\Pi_{P_1,P_2,O}$ with $P_1 \neq P_2$

In the case that P_1, P_2 and O are pairwise distinct points on $J_{a,d}$, by solving linear equations, we get the coefficients of the plane $\Pi_{P_1,P_2,O}$ as follows:

$$\begin{aligned}C_X &= W_1(Z_2 - Y_2) - W_2(Z_1 - Y_1),\\ C_Y &= X_2 W_1 - X_1 W_2\\ C_W &= X_2(Z_1 - Y_1) - X_1(Z_2 - Y_2)\end{aligned}$$

4.3 Equation of $\Pi_{P_1,P_2,O}$ with $P_1 = P_2$

Suppose $P_1 = P_2 \neq O$. The tangent line to $J_{a,d}$ at P_1 is the intersection of the tangent planes to $2aX^2 + Z^2 + dW^2 - Y^2 = 0$ and $X^2 - ZW = 0$ at P_1. The tangent plane to $2aX^2 + Z^2 + dW^2 - Y^2 = 0$ at P_1 is $2aX_1X + Z_1Z + dW_1W - Y_1Y = 0$. The tangent plane to $X^2 - ZW = 0$ at P_1 is $2X_1X - W_1Z - Z_1W = 0$. Then $\Pi_{P_1,P_1,O}$ is of the form:

$$\lambda(2aX_1X + Z_1Z + dW_1W - Y_1Y) + \mu(2X_1X - W_1Z - Z_1W) = 0.$$

Note that $\Pi_{P_1,P_1,O}$ passes O, i.e. $\lambda(Z_1 - Y_1) - \mu W_1 = 0$. One can verify that $\lambda = W_1, \mu = Z_1 - Y_1$ satisfy the equation. Hence, the equation of $\Pi_{P_1,P_1,O}$ is

$$W_1(2aX_1X + Z_1Z + dW_1W - Y_1Y) + (Z_1 - Y_1)(2X_1X - W_1Z - Z_1W) = 0.$$

Then we can get the coefficients of $\Pi_{P_1,P_1,O}$ as follows:

$$\begin{aligned} C_X &= 2aX_1W_1 + 2X_1(Z_1 - Y_1), \\ C_Y &= -Y_1W_1, \\ C_W &= dW_1^2 - Z_1^2 + Y_1Z_1. \end{aligned}$$

4.4 Equation of $\Pi_{P_3,O,O}$

Similar with the case above, since $\Pi_{P_3,O,O}$ passes through the tangent line of $J_{a,d}$ at O, it is of the form:

$$\lambda(Z - Y) - \mu W = 0.$$

For it passes P_3, we have $\lambda = -W_3, \mu = Y_3 - Z_3$, then the equation of $\Pi_{P_3,O,O}$ is

$$W_3(Y - Z) + (Z_3 - Y_3)W = 0.$$

4.5 Explicit formula of Miller function

We summarize the above results as follows:

Theorem 2 *Let* $J_{a,d}: \quad 2aX^2 + Z^2 + dW^2 - Y^2 = 0,\ X^2 - ZW = 0$ *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* $P_3 = P_1 + P_2 = (X_3 : Y_3 : W_3 : Z_3)$. *Then the Miller function* $g_{P_1,P_2}(X, Y, W, Z)$ *which satisfies*

$$\mathrm{div}(g_{P_1,P_2}) = (P_1) + (P_2) - (P_3) - (O)$$

is of the form:

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

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

$$\begin{aligned} C_X &= W_1(Z_2 - Y_2) - W_2(Z_1 - Y_1) \\ C_Y &= X_2W_1 - X_1W_2 \\ C_W &= X_2(Z_1 - Y_1) - X_1(Z_2 - Y_2). \end{aligned}$$

If $P_1 = P_2$, *the coefficients are given by*

$$\begin{aligned} C_X &= 2aX_1W_1 + 2X_1(Z_1 - Y_1) \\ C_Y &= -Y_1W_1 \\ C_W &= dW_1^2 - Z_1^2 + Y_1Z_1. \end{aligned}$$

5 Tate pairing computation on $J_{a,d}$ using projective coordinates

In this section, we analysis steps in Miller's algorithm explicitly. For an addition step or doubling step, as is shown in Algorithm 1, each addition or doubling steps consist of three parts: computing the point $T+P$ or $2T$ and the function $g_{T,P}$ or $g_{T,T}$, evaluating $g_{T,P}$ or $g_{T,P}$ at Q, then updating the variable f by $f \leftarrow f \cdot g_{T,P}(Q)$ or by $f \leftarrow f^2 \cdot g_{T,T}(Q)$.

The updating part, as operation in $\mathbb{F}_{q^k}$, costs $1\mathbf{M}$ for addition step and $1\mathbf{M}+1\mathbf{S}$ for doubling step. It is usually the main cost, but with little room for optimization in one step. For the evaluating part, some standard methods such as denominator elimination and subfield simplification can be used, as we introduce below.

We assume that embedding degree k is even. Let δ be a generator of $\mathbb{F}_{q^k}$ over $\mathbb{F}_{q^{k/2}}$ with $\delta^2 \in \mathbb{F}_{q^{k/2}}$. Suppose $Q' = (X_0 : Y_0 : W_0 : Z_0) \in J_{a\delta^2,d\delta^4}(\mathbb{F}_{q^{k/2}})$, we can see that $Q = (\delta X_0 : Y_0 : \delta^2 W_0 : Z_0) \in J_{a,d}(\mathbb{F}_{q^k})$. If $P_3 = P_1 + P_2 \neq O$, for evaluation of $g_{P_1,P_2}(Q)$, we have

$$\begin{aligned} g_{P_1,P_2}(Q) &= \frac{\Pi_{P_1,P_2,O}(Q)}{\Pi_{P_3,O,O}(Q)} \\ &= \frac{C_X\delta X_0 + C_Y(Y_0 - Z_0) + C_W\delta^2 W_0}{W_3(Y_0 - Z_0) + (Z_3 - Y_3)\delta^2 W_0} \\ &= \frac{C_X\frac{X_0}{Y_0-Z_0}\delta + C_Y + C_W\frac{W_0\delta^2}{Y_0-Z_0}}{W_3 + (Z_3 - Y_3)\frac{W_0\delta^2}{Y_0-Z_0}} \\ &\in (C_X\theta\delta + C_Y + C_W\eta)\mathbb{F}^*_{q^{k/2}}, \end{aligned}$$

where $\theta = \frac{X_0}{Y_0-Z_0}$ and $\eta = \frac{W_0\delta^2}{Y_0-Z_0}$. Note that $\theta, \eta \in \mathbb{F}_{q^{k/2}}$ and they are fixed during the whole computation, so they can be precomputed. The coefficients C_X, C_Y and C_W are in $\mathbb{F}_q$, thus the evaluation at Q given the coefficients of the plane can be computed in $k\mathbf{m}$ (multiplications by θ and η need $\frac{k}{2}\mathbf{m}$ each).

The computation of the coordinates of points and the coefficients of planes, as a part of much variety, is discussed respectively for addition and doubling step as follows.

5.1 Addition step

Let $P_1 = T$ and $P_2 = P$ be distinct points. By Theorem 2 and formulas (2), the explicit formulas for computing $P_3 = T + P$ and C_X, C_Y, C_W are given as

follows:

$$\begin{aligned}
A &= X_1 \cdot X_2;\ B = Y_1 \cdot Y_2;\ C = Z_1 \cdot Z_2;\ D = W_1 \cdot W_2;\\
E &= (X_1 - Y_1) \cdot (X_2 + Y_2) - A + B;\\
F &= W_1 \cdot Z_2;\ G = W_2 \cdot Z_1\\
H &= (Y_1 - W_1) \cdot (Y_2 + W_2) - B + D;\\
I &= (X_2 - W_2) \cdot (X_1 + W_1) - A + D;\\
J &= (X_2 + Z_2) \cdot (X_1 - Z_1) - A + C;\\
Z_3 &= E^2;\ X_3 = E \cdot (F - G);\\
Y_3 &= (F + G - 2A) \cdot (B - 2aA + C + dD) - Z_3;\\
C_X &= H + F - G;\ C_Y = I;\ C_W = E - J;
\end{aligned}$$

The coordinate W_3 is not computed in this step, because it is not used in the following doubling step. Then the total costs of computing $T + P$ and C_X, C_Y, C_W is $12\mathbf{m} + 1\mathbf{s} + 2\mathbf{m_c}$, where $2\mathbf{m_c}$ are multiplication by a and d. Since P is fixed during pairing computation, we can use the mixed addition which means $Z_2 = 1$, then the costs reduce to $10\mathbf{m} + 1\mathbf{s} + 2\mathbf{m_c}$.

So the total costs of an addition step are $1\mathbf{M} + (k + 12)\mathbf{m} + 1\mathbf{s} + 2\mathbf{m_c}$, while a mixed addition step costs $1\mathbf{M} + (k + 10)\mathbf{m} + 1\mathbf{s} + 2\mathbf{m_c}$.

5.2 Doubling step

From Theorem 2, for $P_1 = P_2 = T$, $P_3 = 2T$, we have:

$$\begin{aligned}
C_X &= 2aX_1W_1 + 2X_1(Z_1 - Y_1)\\
C_Y &= -Y_1W_1\\
C_W &= dW_1^2 - Z_1^2 + Y_1Z_1
\end{aligned}$$

In order to exclude W_1, we multiply the coefficients by $2Y_1Z_1$, and get:

$$\begin{aligned}
C'_X &= 2X_1Y_1(Y_1^2 - 2Y_1Z_1) + 2X_1Y_1(2Z_1^2 + 2aX_1^2 - Y_1^2)\\
C'_Y &= -2X_1^2Y_1^2\\
C'_W &= -2Y_1Z_1(2Z_1^2 + 2aX_1^2 - Y_1^2) + 2Y_1^2Z_1^2
\end{aligned}$$

Now the explicit formulas for computing $2P$ and C'_X, C'_Y, C'_W are given as follows:

$$\begin{aligned}
A &= X_1^2;\ B = Y_1^2;\ C = Z_1^2;\ D = aA;\ E = 2C + 2D - B;\\
F &= (X_1 + Y_1)^2 - A - B;\ G = (Y_1 + Z_1)^2 - B - C;\\
Z_3 &= E^2;\ W_3 = F^2;\ X_3 = ((E + F)^2 - Z_3 - W_3)/2;\\
Y_3 &= 2B \cdot (B - 2D) - Z_3;\ C'_X = F \cdot (B - G) + X_3;\\
C'_Y &= -W_3/2;\ C'_W = ((G - E)^2 - Z_3)/2.
\end{aligned}$$

The total costs are $2\mathbf{m} + 9\mathbf{s} + 1\mathbf{m_c}$, where $1\mathbf{m_c}$ is multiplication by a. Hence, a doubling step costs $1\mathbf{M} + 1\mathbf{S} + (k + 2)\mathbf{m} + 9\mathbf{s} + 1\mathbf{m_c}$.

For doubling step (DBL), mixed addition step (mADD) and addition step (ADD), we compare the costs of pairing computation on Jacobi curves in [12] and on twisted Edwards curves [1] in the following table.

	DBL	mADD	ADD
Edwards [1]	$6\mathbf{m}+5\mathbf{s}+2\mathbf{m_c}$	$12\mathbf{m}+1\mathbf{m_c}$	$14\mathbf{m}+1\mathbf{m_c}$
Jacobi quartic [12]	$4\mathbf{m}+8\mathbf{s}+1\mathbf{m_c}$	$16\mathbf{m}+1\mathbf{s}+4\mathbf{m_c}$	$18\mathbf{m}+1\mathbf{s}+4\mathbf{m_c}$
This paper	$2\mathbf{m}+9\mathbf{s}+1\mathbf{m_c}$	$10\mathbf{m}+1\mathbf{s}+2\mathbf{m_c}$	$12\mathbf{m}+1\mathbf{s}+2\mathbf{m_c}$

6 High Twisted Pairing

Let $d|k$, an elliptic curve E' over $\mathbb{F}_{q^{k/d}}$ is called a twist of degree d of $E/\mathbb{F}_{q^{k/d}}$ if there is an isomorphism $\psi : E' \to E$ defined over $\mathbb{F}_{q^k}$, and this is the smallest extension of $\mathbb{F}_{q^{k/d}}$ over which ψ is defined. Depending on the j-invariant $j(E)$ of E, there exist twists of degree at most 6, since $\mathrm{char}(\mathbb{F}_q) > 3$. Pairing friendly curves with twists of degree higher than 2 arise from constructions with j-invariants $j(E) = 0$ and $j(E) = 1728$.

6.1 Jacobi quartic curve with $j = 1728$

The Jacobi quartic curve $J_{0,d} : Y^2 = dW^2 + Z^2, X^2 = ZW$ has j-invariant equal to 1728, hence, there exist twists of degree 4.

Assume that $4|k$. Let δ be a generator of $\mathbb{F}_{q^k}$ over $\mathbb{F}_{q^{k/4}}$ and $\delta^4 \in \mathbb{F}_{q^{k/4}}$, which implies $\delta^2 \in \mathbb{F}_{q^{k/2}}$. Suppose $Q' = (X_0 : Y_0 : W_0 : Z_0) \in J_{0,d\delta^4}(\mathbb{F}_{q^{k/4}})$, we can get $Q = (\delta X_0 : Y_0 : \delta^2 W_0 : Z_0) \in J_{0,d}(\mathbb{F}_{q^k})$.

Theorem 2 shows us the explicit formulae of Miller function g_{P_1,P_2}, then we can get:

$$\begin{aligned} g_{P_1,P_2}(Q) &= \frac{\Pi_{P_1,P_2,O}(Q)}{\Pi_{P_3,O,O}(Q)} \\ &= \frac{C_X\delta X_0 + C_Y(Y_0 - Z_0) + C_W\delta^2 W_0}{W_3(Y_0 - Z_0) + (Z_3 - Y_3)\delta^2 W_0} \\ &= \frac{C_X\frac{X_0}{Y_0-Z_0}\delta + C_Y + C_W\frac{W_0}{Y_0-Z_0}\delta^2}{W_3 + (Z_3 - Y_3)\frac{W_0}{Y_0-Z_0}\delta^2} \\ &\in (C_X\theta\delta + C_Y + C_W\eta\delta^2)\mathbb{F}^*_{q^{k/2}}, \end{aligned}$$

where $\theta = \frac{X_0}{Y_0-Z_0}$ and $\eta = \frac{W_0}{Y_0-Z_0}$. Note that $\theta, \eta \in \mathbb{F}_{q^{k/4}}$ and they are fixed during the whole computation, so they can be precomputed. The coefficients C_X, C_Y and C_W are in $\mathbb{F}_q$, thus the evaluation at Q given the coefficients of the plane can be computed in $\frac{k}{2}\mathbf{m}$ (multiplications by θ and η need $\frac{k}{4}\mathbf{m}$ each).

The high twist not only reduces the cost of evaluating $g(Q)$ but also the cost of updating f, which is the main multiplication in Miller's algorithm as a multiplication in $\mathbb{F}_{q^k}$. Consider $\mathbb{F}_{q^k}$ as an $\mathbb{F}_{q^{k/4}}$-vector space with basis $1, \delta, \delta^2, \delta^3$. Then an arbitrary element $\alpha \in \mathbb{F}_{q^k}$ can be denoted as $a_0 + a_1\delta + a_2\delta^2 + a_3\delta^3$ with $a_i \in \mathbb{F}_{q^{k/4}}, i = 0, 1, 2, 3$. And the reduced value of $g(Q)$ we've gotten above can be denoted as $\beta = b_0 + b_1\delta + b_2\delta^2$, where $b_0 \in \mathbb{F}_q$ and $b_1, b_2 \in \mathbb{F}_{q^{k/4}}$. When using the Schoolbook method, multiplying α by β costs $4 \cdot \frac{k}{4}\mathbf{m}$ for computing

$a_i \cdot b_0, i = 0,1,2,3$ and costs $8(\frac{k}{4})^2\mathbf{m}$ for $a_i \cdot b_1$ and $a_i \cdot b_2$. The total cost $(\frac{k^2}{2}+k)\mathbf{m}$ equals to $(\frac{1}{2}+\frac{1}{k})\mathbf{M}$, considering that a general multiplication in $\mathbb{F}_{q^k}$ costs $\mathbf{M} = k^2\mathbf{m}$. Namely the quartic twist may reduce the cost of the main multiplication in Miller's algorithm to $(\frac{1}{2}+\frac{1}{k})\mathbf{M}$.
Addition step: Using the algorithm in section 5.1, $1\mathbf{m_c}$ can be saved for $a = 0$. Hence, a addition step in Miller's algorithm costs $(\frac{1}{2}+\frac{1}{k})\mathbf{M}+(\frac{k}{2}+12)\mathbf{m}+1\mathbf{s}+1\mathbf{m_c}$, and a mixed addition step in Miller's algorithm costs $(\frac{1}{2}+\frac{1}{k})\mathbf{M}+(\frac{k}{2}+10)\mathbf{m}+1\mathbf{s}+1\mathbf{m_c}$, where $1\mathbf{m_c}$ is multiplication by d.
Doubling step: Using the algorithm in section 5.1, we compute X_1Y_1 instead of computing $A = X_1^2$ and $F = (X_1+Y_1)^2 - A - B$ since $a = 0$ led to $D = 0$ in algorithm. Furthermore, $1\mathbf{m_c}$ can be saved for $a = 0$. Hence a doubling step in Miller's algorithm costs $(\frac{1}{2}+\frac{1}{k})\mathbf{M}+1\mathbf{S}+(\frac{k}{2}+2)\mathbf{m}+8\mathbf{s}$.

6.2 Jacobi quartic curves with $j = 0$

The Jacobi quartic curve $E_{a,d} : y^2 = dx^4 + 2ax^2 + 1$ has j-invariant $j_{a,d} = \frac{16(4a^2+12d)^3}{d(a^2-4d)^2}$. Hence, $j_{a,d} = 0$ if and only if $a^2 + 3d = 0$. Now we look into the Jacobi quartic curve

$$E_{a,-a^2/3} : y^2 = -\frac{a^2}{3}x^4 + 2ax^2 + 1$$

which has j-invariant equal to 0, hence, there exist twists of degree 6.

Lemma 3 *Assume that $6|k$, δ is a generator of $\mathbb{F}_{q^k}$ over $\mathbb{F}_{q^{k/6}}$ with $\delta^6 \in \mathbb{F}_{q^{k/6}}$, which implies $\delta^2 \in \mathbb{F}_{q^{k/2}}$ and $\delta^3 \in \mathbb{F}_{q^{k/3}}$. Then the Weierstrass elliptic curve*

$$W_a : v^2 = u^3 + \frac{64a^3}{27}\delta^6$$

is a twist of degree 6 over $\mathbb{F}_{q^{k/6}}$ of $E_{a,-a^2/3}$. The isomorphism can be given as

$$\begin{aligned}\psi : W_a &\longrightarrow E_{a,-a^2/3}\\ (u,v) &\longmapsto (x,y) = \left(\frac{6u\delta+8a\delta^3}{3v}, \frac{3u-2a\delta^2}{6\delta^2}(\frac{6u\delta+8a\delta^3}{3v})^2 - 1\right).\end{aligned}$$

Proof. Firstly, we check that ψ is well defined, i.e. $\psi(u,v) \in E_{a,-a^2/3}$. Note that

$$y = \frac{3u-2a\delta^2}{6\delta^2}(\frac{6u\delta+8a\delta^3}{3v})^2 - 1 = (\frac{vx}{4\delta^3} - a)x^2 - 1$$

so

$$\begin{aligned}y + 1 + ax^2 &= \frac{vx^3}{4\delta^3}\\ &= \frac{2}{v^2}(u + \frac{4a\delta^2}{3})^3\\ &= \frac{2}{v^2}(u^3 + \frac{64a^3\delta^6}{27}) + \frac{8a\delta^2}{v^2}(u+\frac{4a\delta^2}{3})^2 - \frac{32a^2\delta^4}{3v^2}(u+\frac{4a\delta^2}{3})\\ &= 2 + 2ax^2 - \frac{16a^2\delta^3}{3v}x\end{aligned}$$

Then we have

$$(y+1+ax^2)(y-1-ax^2) = -\frac{vx^3}{4\delta^3}\frac{16a^2\delta^3}{3v}x = -\frac{4a^2}{3}x^4,$$
$$y^2 = -\frac{a^2}{3}x^4 + 2ax^2 + 1.$$

Moreover, it can be easily checked that ψ is invertible and satisfies $\psi(O) = O$, i.e. ψ is an isomorphism. Besides, the minimal field that ψ can be defined over is $\mathbb{F}_{q^k}$ which has degree 6 over $\mathbb{F}_{q^{k/6}}$. Hence, the twist degree is 6. □

For $Q' \in W_a(\mathbb{F}_{q^{k/6}})$, we have $(x_Q, y_Q) = \psi(Q') \in E_{a,-a^2/3}(\mathbb{F}_{q^k})$. Then its corresponding point $Q \in J_{a,-a^2/3}(\mathbb{F}_{q^k})$ can be given as $(X_Q : Y_Q : W_Q : Z_Q) = (x_Q : y_Q : x_Q^2 : 1)$. One can check by substitution that:

$$\frac{X_Q}{Y_Q - Z_Q - aW_Q} = \frac{x_Q}{y_Q - 1 - ax_Q^2} = -\frac{y_Q + 1 + ax_Q^2}{\frac{4}{3}a^2x_Q^3} = -\frac{3v}{16a^2\delta^3}$$
$$\frac{W_Q}{Y_Q - Z_Q - aW_Q} = \frac{x_Q^2}{y_Q - 1 - ax_Q^2} = -\frac{3u}{8a^2\delta^2} - \frac{1}{2a}$$
$$\frac{Y_Q - Z_Q}{Y_Q - Z_Q - aW_Q} = 1 - \frac{aW_Q}{Y_Q - Z_Q - aW_Q} = \frac{3u}{8a\delta^2} + \frac{1}{2}$$

For $\theta = \frac{3v}{8a}$ and $\eta = \frac{3u}{4a}$, we have

$$\frac{X_Q}{Y_Q - Z_Q - aW_Q} = -\frac{1}{2a}\theta\delta^{-3}$$
$$\frac{W_Q}{Y_Q - Z_Q - aW_Q} = -\frac{1}{2a}\eta\delta^{-2} - \frac{1}{2a}$$
$$\frac{Y_Q - Z_Q}{Y_Q - Z_Q - aW_Q} = -\frac{1}{2}\eta\delta^{-2} + \frac{1}{2}$$

with $\theta, \eta \in \mathbb{F}_{q^{k/6}}$. Then for the evaluation of $g_{P_1,P_2}(Q)$ with $P_3 = P_1 + P_2 \neq O$, we get

$$\begin{aligned}
g_{P_1,P_2}(Q) &= \frac{\Pi_{P_1,P_2,O}(Q)}{\Pi_{P_3,O,O}(Q)} \\
&= \frac{C_X X_Q + C_Y(Y_Q - Z_Q) + C_W W_Q}{W_3(Y_Q - Z_Q) + (Z_3 - Y_3)W_Q} \\
&= \frac{C_X \frac{X_Q}{Y_Q - Z_Q - aW_Q} + C_Y \frac{Y_Q - Z_Q}{Y_Q - Z_Q - aW_Q} + C_W \frac{W_Q}{Y_Q - Z_Q - aW_Q}}{W_3 \frac{Y_Q - Z_Q}{Y_Q - Z_Q - aW_Q} + (Z_3 - Y_3)\frac{W_Q}{Y_Q - Z_Q - aW_Q}} \\
&= \frac{-C_X \frac{1}{2a}\theta\delta^{-3} + C_Y(-\frac{1}{2}\eta\delta^{-2} + \frac{1}{2}) - C_W(\frac{1}{2a}\eta\delta^{-2} + \frac{1}{2a})}{W_3(-\frac{1}{2}\eta\delta^{-2} + \frac{1}{2}) - (Z_3 - Y_3)(\frac{1}{2a}\eta\delta^{-2} + \frac{1}{2a})} \\
&= \frac{-C_X\theta\delta - (aC_Y + C_W)\eta\delta^2 + (aC_Y - C_W)\delta^4}{(-aW_3 + Y_3 - Z_3)\eta\delta^2 + (aW_3 - Z_3 + Y_3)\delta^4} \\
&\in (-C_X\theta\delta - (aC_Y + C_W)\eta\delta^2 + (aC_Y - C_W)\delta^4)\mathbb{F}_{q^{k/2}}^*.
\end{aligned}$$

So we can reduce $g_{P_1,P_2}(Q)$ to the representative in the last line. Moreover we may precompute θ and η since they are fixed during the whole computation. When $C_X, C_Y, C_W \in \mathbb{F}_q$ and $\theta, \eta \in \mathbb{F}_{q^{k/6}}$ are given, the evaluation at Q can be computed in $\frac{k}{3}\mathbf{m} + \mathbf{m_c}$, with $\frac{k}{6}\mathbf{m}$ each for multiplications by θ and η and a constant multiplication by a.

Similarly with the $j = 1728$ case, consider $\mathbb{F}_{q^k}$ as an $\mathbb{F}_{q^{k/6}}$-vector space with basis $1, \delta, \delta^2, \ldots, \delta^5$. Then an arbitrary element $\alpha \in \mathbb{F}_{q^k}$ can be denoted as $a_0 + a_1\delta + a_2\delta^2 + \ldots + a_5\delta^5$ with $a_i \in \mathbb{F}_{q^{k/6}}, i = 0, 1, \ldots, 5$. And the reduced $g(Q)$ we've gotten above can be denoted as $\beta = b_0 + b_3\delta^3 + b_4\delta^4$, where $b_0 \in \mathbb{F}_q$ and $b_3, b_4 \in \mathbb{F}_{q^{k/6}}$. When using the Schoolbook method, multiplying α by β costs $6 \cdot \frac{k}{6}\mathbf{m}$ for computing $a_i \cdot b_0, i = 0, 1, 2, 3$ and costs $12(\frac{k}{6})^2\mathbf{m}$ for $a_i \cdot b_3$ and $a_i \cdot b_4$. The total cost $(\frac{k^2}{3} + k)\mathbf{m}$ equals to $(\frac{1}{3} + \frac{1}{k})\mathbf{M}$, considering that a general multiplication in $\mathbb{F}_{q^k}$ costs $\mathbf{M} = k^2\mathbf{m}$. Namely the sextic twist may reduce the cost of the main multiplication in Miller's algorithm to $(\frac{1}{3} + \frac{1}{k})\mathbf{M}$.

Special simplification has not been found for this case. Hence, we use the algorithm in section 5.1. Then the total cost of addition step using mixed addition is $(\frac{1}{3} + \frac{1}{k})\mathbf{M} + (\frac{k}{3} + 10)\mathbf{m} + 1\mathbf{s} + 3\mathbf{m_c}$, where $3\mathbf{m_c}$ are multiplication by a, a and d, and the total cost of doubling step is $(\frac{1}{3} + \frac{1}{k})\mathbf{M} + \mathbf{S} + (\frac{k}{3} + 2)\mathbf{m} + 9\mathbf{s} + 2\mathbf{m_c}$, where $2\mathbf{m_c}$ are both multiplication by a.

6.3 Comparisons

The following table shows the concrete comparison with previous results on elliptic curves with high-twist. We denote twisted degree by td. So these expenses in the following table.

	DBL	mADD	ADD
$y^2 = x^3 + ax, td = 4$ [7]	$(\frac{k}{2} + 2)m + 8s + 1m_c$	$(\frac{k}{2} + 9)m + 5s$	$(\frac{k}{2} + 12)m + 7s$
$y^2 = x^3 + c^2, td = 6$ [7]	$(\frac{k}{3} + 3)m + 5s$	$(\frac{k}{3} + 10)m + 2s + 1m_c$	$(\frac{k}{3} + 14)m + 2s + 1m_c$
$y^2 = x^3 + b, td = 6$ [7]	$(\frac{k}{3} + 2)m + 7s + 1m_c$	$(\frac{k}{3} + 10)m + 2s$	$(\frac{k}{3} + 14)m + 2s$
$y^2 = dx^4 + 1, td = 4$ [10]	$(\frac{k}{2} + 3)m + 7s + 1m_c$	$(\frac{k}{2} + 12)m + 7s + 1m_c$	$(\frac{k}{2} + 12)m + 11s + 1m_c$
$td = 4$ this paper §6.1	$(\frac{k}{2} + 2)m + 8s$	$(\frac{k}{2} + 10)m + 1s + 1m_c$	$(\frac{k}{2} + 12)m + 1s + 1m_c$
$td = 6$ this paper	$(\frac{k}{3} + 2)m + 9s + 2m_c$	$(\frac{k}{3} + 10)m + 1s + 3m_c$	$(\frac{k}{3} + 12)m + 1s + 3m_c$

7 Conclusion

In this paper, we present a elaborate geometric interpretation of the group law on Jacobi quartic curves which is seen as the intersection of two quadratic surfaces in space. Using the geometric interpretation we construct the Miller function. Then, we present explicit formulae for the addition step and doubling step in Miller's algorithm to compute the Tate pairing on Jacobi quartic curves. Finally, we present efficient formulas for Jacobi quartic curves with twists of degree 4 or 6.

The Miller function in this paper can help to reduce the cost of updating the iteration function in Miller's algorithm. So, both the addition step and doubling step of our formulae for pairing computation on Jacobi quartic curve are faster than that proposed by Wang et al.[12]. The high-twists can help to reduce the cost of evaluating the Miller function on Jacobi quartic curves. For twists of degree 4, both the addition steps and double steps in our formulae for Tate pairing computation on Jacobi quartic curves are faster than the fastest result on Weierstrass curves. For twists of degree 6, the addition steps in our formulae for Tate pairing computation on Jacobi quartic curves are faster than the fastest result on Weierstrass curves, while the doubling steps are a little slower than the fastest result on Weierstrass curves.

References

1. C. Arène, T. Lange, M. Naehrig and C. Ritzenthaler. Faster Computation of the Tate Pairing, Journal of Number Theory 131, pp. 842-857, 2011.
2. D. J. Bernstein and T. Lange, Faster addition and doubling on elliptic curves. ASIACRYPT 2007, LNCS 4833, pp. 29-50, Springer, 2007.
3. D.J. Bernstein, P. Birkner, M. Joye, T. Lange and C. Peters. Twisted Edwards curves, In AFRICACRYPT 2008, LNCS 5023, 389–405, Springer, 2008.
4. O. Billet and M. Joye. The Jacobi model of an elliptic curve and side-channel analysis, AAECC 2003, LNCS 2643, pp.34–42, Springer, 2003.
5. S. Chatterjee, P. Sarkar, R. Barua. Efficient computation of Tate pairing in projective coordinate over general characteristic fields. LNCS 3506, pp. 168-181. Springer, 2005.
6. D.V. Chudnovsky and G.V. Chudnovsky. Sequences of numbers generated by addition in formal groups and new primality and factorization tests. Advances in Applied Mathematics, 7(4):385–434, 1986.
7. C. Costello, T. Lange and M. Naehrig. Faster pairing computations on curves with high-degree twists. In PKC 2010, LNCS 6056, pages 224–242. Springer, 2010.
8. M. Das and P. Sarkar. Pairing computation on twisted edwards form elliptic curves. Pairing-Based Cryptography–Pairing 2008, LNCS 5209, pp. 192–210, Springer, 2008.
9. H.M. Edwards. A normal form for elliptic curves. Bulletin of the American Mathematical Society, 44(3):393–422, 2007.
10. E. FOUOTSA and S. Duquesne. Tate pairing computation on Jacobi's elliptic curves. Pairing 2012, Available: http://www.emmanuelfouotsa.org/Portals/22/Users/206/06/206/slidesPairing2012.pdf.
11. H. Hisil, Kenneth Koon-Ho Wong. Jacobi quartic curves revisited. In Gary Carter and EdDawson, (Eds.), ACISP 2009, LNCS 5594, pp. 452-468, Springer, 2009.
12. Hong Wang, Kunpeng Wang, Lijun Zhang and Bao Li. Pairing Computation on Elliptic Curves of Jacobi Quartic Form. Chinese Journal of Electronics, 2011: 20(4), pp. 655-661.
13. Sorina Ionica and Antoine Joux. Another approach to pairing computation in Edwards coordinates. D. Chowdhury, V. Rijmen and A. Das, (eds.) Progress in Cryptology–INDOCRYPT 2008, LNCS 5365, pp. 400-413, Springer, 2008.
14. N. Koblitz and A.J. Menezes. Pairing-based cryptography at high security levels, Cryptography and Coding, LNCS 3796, pp. 13-36, Springer, 2005.

15. J.R. Merriman and S. Siksek. and N.P. Smart. Explicit 4-descents on an elliptic curve, Acta Arithmetica, vol 77(4), pp. 385–404, 1996.
16. V.S. Miller. The Weil pairing and its efficient calculation. J. Cryptol. 17(44), pp. 235-261, 2004.