Pairing computation on Edwards 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 geometry approach to explain the group law on twisted Edwards curves which are seen as the intersection of quadric surfaces in place. Using the geometric interpretation of the group law we obtain the Miller function for Tate pairing computation on twisted Edwards curves. Then we present the explicit formulae for pairing computation on twisted Edwards curves. Our formulae for the doubling step are a littler faster than that proposed by Arène et.al.. Finally, to improve the efficiency of pairing computation we present twists of degree 4 and 6 on twisted Edwards curves.

Keywords: Edwards curves, Tate pairing, Miller functions, Cryptography

1 Introduction

Pairing-based cryptography has been one of the most active areas in elliptic curve cryptography since 2000. Some details on this subject can be found in [2, 6]. How to compute pairings efficiently is a bottleneck for implementing pairing-based cryptography. The most efficient method of computing pairings is Miller's algorithm [16]. Consequently, various improvements were presented in [1, 10, 11, 14, 17]. One way to improve the efficiency is to find other models of elliptic curves which can provide more efficient algorithms for pairing computation. Edwards curves were one of the popular models. Edwards curve was discovered by Edwards [9] and was applied in cryptography by Bernstein and Lange [3]. Then twisted Edwards curves which are the generalization of Edwards curves were introduced by Bernstein et al. in [4]. Bernstein and Lange also pointed out several advantages of applying the Edwards curves to cryptography. Pairing computation over Edwards curves was first considered in [8] and [13]. In 2009, Arène et.al. [1] gave the geometric interpretation of the group law and presented explicit formulae for computing the Tate pairing on twisted Edwards curves. Their formulae are faster than all previously proposed formulas for pairings computation on twisted Edwards curves. Their formulae are even competitive with all published formulae for pairing computation on Weierstrass curves.

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

Any elliptic curve defined over a field K with characteristic different from 2 is birationally equivalent to an Edwards curve over some extension of K, i.e. a curve given by $x^2+y^2=1+dx^2y^2$ with $d \notin \{0,1\}$. In fact, the twisted Edwards can be seen as the intersection of two quadratic surfaces in space. That is to say the twisted Edwards curves can be given by $SW_{a,d}: \ aX^2+Y^2-Z^2-dW^2=0, \ XY-ZW=0$. 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]. In this paper, we proposed a more detailed geometry approach to explain the group law for the case of twisted Edwards curves which are seen as the intersection of two quadratic surfaces. Using the geometric interpretation of the group law we obtain the Miller function of Tate pairing computation on twisted Edwards curves. Then we present the explicit formulae for pairing computation on twisted Edwards curves. The doubling step of our formulae is a littler faster than that in [1]. Finally, to reduce the cost of evaluating the Miller function on twisted Edwards curve, we employ quadratic, quartic or sextic twists to the formulae of the Tate pairing computation. The high-twists had been sufficiently studied by Costello, Lange and Naehrig[7] on Weierstrass curves. By using the high-twist on twisted Edwards curves the costs of substituting in $j=1728$ case and $j=0$ case can be reduced to a half and a third respectively.

The remainder of the paper is organized as follows: In Section 2, we provide some backgrounds and notations used in this paper. In Section 3, we give a geometry approach to explain the group law on twisted Edwards curves. In Section 4, we present pairing computation on twisted Edwards curves. In Section 5, we employ quartic and sextic twists to the formulae of the Tate pairing computation. In Section 6, we conclude our paper.

2 Preliminaries

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.

Algorithm 1 Miller's algorithm

Input: $r = \sum_{i=0}^{l-1} r_i 2^i$, where $r_i \in \{0, 1\}$. $P \in E(\mathbb{F}_q), Q \in E(\mathbb{F}_{q^k})$.

Output: $f_r^{(q^k-1)/r}(Q)$

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 $f^{(q^k-1)/r}$

2.2 Edwards curves

For $\mathrm{char}(\mathbb{F}_q) \neq 2$, a twisted Edwards curve defined over $\mathbb{F}_q$ is given by:

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

where a, d are distinct nonzero elements of $\mathbb{F}_q$. The projective closure of $E_{a,d}$ in $\mathbb{P}^2$ is

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

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 are exactly two such points, namely $\Omega_1 = (1 : 0 : 0)$ and $\Omega_2 = (0 : 1 : 0)$. These points are singular.

In fact, the twisted Edwards curve can be seen as the intersection of two quadric surfaces in space. That is, the twisted Edwards curve can be written as:

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

More generally, every elliptic curve defined over a field K with $\mathrm{char}(K) \neq 2$ can be written in this normal form over an extension of K. Set $O = (0 : 1 : 0 : 1)$ as the neutral element, the group law on (1) is given by

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

and

$$(X_1 : Y_1 : W_1 : Z_1) + (X_2 : Y_2 : W_2 : Z_2) = (X_3 : Y_3 : W_3 : Z_3)$$

where

$$\begin{aligned} X_3 &= (X_1Y_2 + Y_1X_2)(Z_1Z_2 - dW_1W_2), \\ Y_3 &= (Y_1Y_2 - aX_1X_2)(Z_1Z_2 + dW_1W_2), \\ W_3 &= (Y_1Y_2 - aX_1X_2)(X_1Y_2 + X_2Y_1), \\ Z_3 &= (Z_1Z_2 - dW_1W_2)(Z_1Z_2 + dW_1W_2) \end{aligned} \tag{2}$$

The point $O' = (0 : -1 : 0 : 1)$ has order 2. Note that the above formula is unified, that is it can be applied to both adding two distinct points and doubling a point. The fast arithmetic on twisted Edwards given by (1) can be found in [12, 5].

We use **m** and **s** denote the costs of multiplication and squaring in the base field $\mathbb{F}_q$ while **M** and **S** denote the costs of multiplication and squaring in the extension $\mathbb{F}_{q^k}$.

3 Geometric interpretation of the group law on twisted Edwards curves

The aim of this section is to give the elaborate geometric interpretation of the group law on twisted Edwards curves which are seen as the intersection of two quadric surfaces in space. 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 $SW_{a,d}$ at exactly four points. Although these planes are not functions on $SW_{a,d}$, their divisors can be well defined as:

$$\mathrm{div}(\Pi) = \sum_{R \in \Pi \cap SW_{a,d}} n_R(R) \tag{3}$$

where n_R is the intersection multiplicity of Π and $SW_{a,d}$ at R. Then the quotient of two projective planes is a well defined function which gives 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), we 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 the above inequality. So we may denote this plane by Π_{P_1,P_2,P_3} from now on.

3.1 Group Law over the twisted Edwards curves

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

Lemma 1 *For twist Edwards curve $SW_{a,d}$ with neutral element $O = (0 : 1 : 0 : 1)$, let $O' = (0 : -1 : 0 : 1)$. 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 $\mathrm{div}(\Pi) = (P_1) + (P_2) + (P_3) + (P_4)$.*

Proof. Firstly, it is an easy calculation to get that $\mathrm{div}(X - W) = 3(O) + (O')$.

Then the "if" part follows directly: if $\mathrm{div}(\Pi) = (P_1) + (P_2) + (P_3) + (P_4)$, the principal divisor $\mathrm{div}(\frac{\Pi}{X-W}) = (P_1) + (P_2) + (P_3) + (P_4) - 3(O) - (O')$ 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 [4], so we can claim that our explicit formulae for negative point, point addition and point doubling are equivalent with which of [4].

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

4.1 Construction of Miller function

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

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

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 $SW_{a,d}$ can be given by setting $P_1 = T, P_2 = P$:

$$g_{T,P} = \frac{\Pi_{T,P,O'}}{\Pi_{T+P,O,O'}} \tag{4}$$

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

$$g_{T,T} = \frac{\Pi_{T,T,O'}}{\Pi_{2T,O,O'}} \tag{5}$$

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 $SW_{a,d}$, by solving linear equations, we get the coefficients of the plane $\Pi_{P_1,P_2,O'}$ as follows:

$$\begin{aligned} C_X &= W_2(Z_1 + Y_1) - W_1(Z_2 + Y_2), \\ C_Y &= X_2W_1 - X_1W_2, \\ C_W &= X_1(Y_2 + Z_2) - X_2(Z_1 + Y_1) \end{aligned} \tag{6}$$

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 $SW_{a,d}$ at P_1 is the intersection of the tangent planes to $aX^2+Y^2-Z^2-dW^2 = 0$ and $XY-ZW = 0$ at P_1. The tangent plane to $aX^2 + Y^2 - Z^2 - dW^2 = 0$ at P_1 is $aX_1X + Y_1Y - Z_1Z - dW_1W = 0$. The tangent plane to $XY - ZW = 0$ at P_1 is $Y_1X + X_1Y - W_1Z - Z_1W = 0$. Then $\Pi_{P_1,P_1,O'}$ is of the form:

$$\lambda(aX_1X + Y_1Y - Z_1Z - dW_1W) + \mu(Y_1X + X_1Y - W_1Z - Z_1W) = 0.$$

Note that $O' \in \Pi_{P_1,P_1,O'}$, i.e. $\lambda(Y_1 + Z_1) + \mu(X_1 + W_1) = 0$. One can verify that $\lambda = -X_1, \mu = Z_1$ satisfy the equation. Hence, the equation of $\Pi_{P_1,P_1,O'}$ is

$$-X_1(aX_1X + Y_1Y - Z_1Z - dW_1W) + Z_1(Y_1X + X_1Y - W_1Z - Z_1W) = 0.$$

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

$$\begin{aligned} C_X &= Y_1Z_1 - aX_1^2, \\ C_Y &= X_1Z_1 - X_1Y_1, \\ C_W &= dX_1W_1 - Z_1^2. \end{aligned} \tag{7}$$

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

The plane $\Pi_{P_3,O,O'}$ can be regarded as a special case of $\Pi_{P_1,P_2,O'}$. For $P_3 \neq O, O'$ we have:

$$\begin{aligned} C_X &= W_3, \\ C_Y &= 0, \\ C_W &= -X_3 \end{aligned}$$

Thus, we have $\Pi_{P_3,O,O'} : W_3X - X_3W = 0$.

5 Pairing computation

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 $Q' = (X_0 : Y_0 : W_0 : Z_0) \in SW_{a\delta^{-2},d\delta^{-2}}(\mathbb{F}_{q^{k/2}})$, we can see that $Q = (X_0 : \delta Y_0 : W_0 : \delta Z_0) \in SW_{a,d}(\mathbb{F}_{q^k})$. If $P_3 = P_1 + P_2 \neq O, O'$, for evaluation of $g_{P_1,P_2}(Q)$, we have

$$\begin{aligned} g_{P_1,P_2}(Q) &= \frac{\Pi_{P_1,P_2,O'}(Q)}{\Pi_{P_3,O,O'}(Q)} \\ &= \frac{C_X X_0 + C_Y \delta(Y_0 + Z_0) + C_W W_0}{W_3 X_0 - X_3 W_0} \\ &= \frac{C_X \frac{X_0}{Y_0+Z_0} + C_Y \delta + C_W \frac{W_0}{Y_0+Z_0}}{(W_3 X_0 - X_3 W_0)/(Y_0 + Z_0)} \\ &\in (C_X\theta + C_Y\delta + C_W\eta)\mathbb{F}^*_{q^{k/2}}, \end{aligned}$$

where $\theta = \frac{X_0}{Y_0+Z_0}$ and $\eta = \frac{W_0}{Y_0+Z_0}$. Note that $\theta, \eta \in \mathbb{F}_{q^{k/2}}$ 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 steps

Let $P_1 = T$ and $P_2 = P$ be distinct points with $Z_1 Z_2 \neq 0$. By variant of formula (2) and (6), the explicit formulas for computing $P_3 = T + P$ and C_X, C_Y, C_W are given as follows:

$$\begin{aligned} A = X_1 \cdot X_2, B = Y_1 \cdot Y_2, C = Z_1 \cdot W_2, D = Z_2 \cdot W_1, E = W_1 \cdot W_2, \\ F = (X_1 - Y_1) \cdot (X_2 + Y_2) - A + B, G = B + aA, H = D - C, \\ I = D + C, X_3 = I \cdot F, Y_3 = G \cdot H, Z_3 = F \cdot G, W_3 = I \cdot H, \\ C_X = (W_1 - Y_1) \cdot (W_2 + Y_2) - E + B + H, C_W = X_2 \cdot Z_1 - X_1 \cdot Z_2 - F, \\ C_Y = (X_1 - W_1) \cdot (X_2 + W_2) - A + E. \end{aligned}$$

With these formulas $T + P$ and C_X, C_Y, C_W can be computed in $14\mathbf{m} + 1\mathbf{m_c}$, where $1\mathbf{m_c}$ is constant multiplication by a. For a mixed addition step, in which the base point P is chosen to have $Z_2 = 1$, the costs reduce to $12\mathbf{m} + 1\mathbf{m_c}$.

Therefore, the total costs of an addition step are $1\mathbf{M} + k\mathbf{m} + 14\mathbf{m} + 1\mathbf{m_c}$, while a mixed addition step costs $1\mathbf{M} + k\mathbf{m} + 12\mathbf{m} + 1\mathbf{m_c}$.

5.2 Doubling steps

For $P_1 = P_2 = T$, $P_3 = 2T$. By the formulae of (2) and (7), our explicit formulas for computing $P_3 = 2T$ and C_X, C_Y, C_W are given as follows:

$$\begin{aligned} A = {X_1}^2, B = {Y_1}^2, C = {Z_1}^2, D = aA, E = B + D, F = 2C - E, \\ G = (X_1 + Y_1)^2 - A - B, H = (Y_1 + Z_1)^2 - B - C, \\ X_3 = G \cdot F, Y_3 = E \cdot (B - D), Z_3 = E \cdot F, W_3 = G \cdot (B - D), \\ 2C_X = H - 2D, 2C_Y = (X_1 + Z_1)^2 - A - C - G, \\ 2C_W = d((X_1 + W_1)^2 - A) - C - E. \end{aligned}$$

By the above formulae, $2T$ and C_X, C_Y, C_W can be computed in $4\mathbf{m} + 7\mathbf{s} + 2\mathbf{m_c}$, where $2\mathbf{m_c}$ are constant multiplications by a and d.

So total costs of our formulae for a doubling step are $1\mathbf{M}+1\mathbf{S}+k\mathbf{m}+4\mathbf{m}+7\mathbf{s}+2\mathbf{m_c}$. While the total costs of the formulae for the doubling step proposed in [1] are $1\mathbf{M}+1\mathbf{S}+k\mathbf{m}+6\mathbf{m}+5\mathbf{s}+2\mathbf{m_c}$, where $2\mathbf{m_c}$ are both constant multiplication by a.

6 High-Degree Twists

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 Edwards curves with $j = 1728$

For twisted Edwards curve $E_{a,-a} : ax^2 + y^2 = 1 - ax^2y^2$, the j-invariant equal to 1728, hence, there exist twists of degree 4.

Lemma 2 *Assume that $4|k$, δ is a generator of $\mathbb{F}_{q^k}$ over $\mathbb{F}_{q^{k/4}}$ and $\delta^4 \in \mathbb{F}_{q^{k/4}}$, which implies $\delta^2 \in \mathbb{F}_{q^{k/2}}$. Then the Weierstrass curve*

$$W_a : \frac{2}{a}v^2 = u^3 + \frac{1}{\delta^4}u$$

is a twist of degree 4 over $\mathbb{F}_{q^{k/4}}$ of $E_{a,-a}$. The isomorphism can be given as

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

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

$$\frac{1}{x^2} = \frac{\delta^2 v^2}{u^2} = \frac{a}{2\delta^2 u}(\delta^4 u^2 + 1).$$

We have

$$\frac{1}{x^2} - a = \frac{a}{2\delta^2 u}(\delta^2 u - 1)^2, \frac{1}{x^2} + a = \frac{a}{2\delta^2 u}(\delta^2 u + 1)^2.$$

Then

$$\frac{1 - ax^2}{1 + ax^2} = (\frac{\delta^2 u - 1}{\delta^2 u + 1})^2 = y^2, \text{thus } ax^2 + y^2 = 1 - ax^2 y^2.$$

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 4 over $\mathbb{F}_{q^{k/4}}$. Hence, the twist degree is 4. □

For $Q' \in W_a(\mathbb{F}_{q^{k/4}})$, we have $(x_Q, y_Q) = \psi(Q') \in E_{a,-a}(\mathbb{F}_{q^k})$. Then its corresponding point $Q \in SW_{a,-a}(\mathbb{F}_{q^k})$ can be given as $(X_Q : Y_Q : W_Q : Z_Q) = (x_Q : y_Q : x_Q y_Q : 1)$. One can check by substitution that:

$$\frac{X_Q + W_Q}{Y_Q + Z_Q} = x_Q = \frac{u}{\delta v}$$
$$\frac{X_Q - W_Q}{Y_Q + Z_Q} = x_Q \cdot \frac{1 - y_Q}{1 + y_Q} = \frac{1}{\delta^3 v}$$

For $\theta = \frac{u}{2v}$ and $\eta = \frac{1}{2v}$, we have $\frac{X_Q}{Y_Q+Z_Q} = \theta\delta^{-1} + \eta\delta^{-3}$ and $\frac{W_Q}{Y_Q+Z_Q} = \theta\delta^{-1} - \eta\delta^{-3}$ with $\theta, \eta \in \mathbb{F}_{q^{k/4}}$. Then for the evaluation of $g_{P_1,P_2}(Q)$ with $P_3 = P_1 + P_2 \neq O, O'$, we get

$$\begin{aligned}
g_{P_1,P_2}(Q) &= \frac{\Pi_{P_1,P_2,O'}(Q)}{\Pi_{P_3,O,O'}(Q)} \\
&= \frac{C_X X_Q + C_Y(Y_Q + Z_Q) + C_W W_Q}{W_3 X_Q - X_3 W_Q} \\
&= \frac{C_X \frac{X_Q}{Y_Q+Z_Q} + C_Y + C_W \frac{W_Q}{Y_Q+Z_Q}}{W_3 \frac{X_Q}{Y_Q+Z_Q} - X_3 \frac{W_Q}{Y_Q+Z_Q}} \\
&= \frac{C_X(\theta\delta^{-1} + \eta\delta^{-3}) + C_Y + C_W(\theta\delta^{-1} - \eta\delta^{-3})}{W_3(\theta\delta^{-1} + \eta\delta^{-3}) - X_3(\theta\delta^{-1} - \eta\delta^{-3})} \\
&= \frac{(C_X - C_W)\eta + (C_X + C_W)\theta\delta^2 + C_Y\delta^3}{(W_3 + X_3)\eta + (W_3 - X_3)\theta\delta^2} \\
&\in ((C_X - C_W)\eta + (C_X + C_W)\theta\delta^2 + C_Y\delta^3)\mathbb{F}^*_{q^{k/2}}.
\end{aligned}$$

So we can reduce $g_{P_1,P_2}(Q)$ to $(C_X - C_W)\eta + (C_X + C_W)\theta\delta^2 + C_Y\delta^3$. 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 $\theta, \eta \in \mathbb{F}_{q^{k/4}}$ are given, the evaluation at Q can be computed in $\frac{k}{2}\mathbf{m}$, with $\frac{k}{4}\mathbf{m}$ each for multiplications by θ and η.

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 $\beta = b_0 + b_2\delta^2 + b_3\delta^3$, where $b_3 \in \mathbb{F}_q$ and $b_0, b_2 \in \mathbb{F}_{q^{k/4}}$. When using the Schoolbook method, multiplying α by β costs $4 \cdot \frac{k}{4}\mathbf{m}$ for computing $a_i \cdot b_3, i = 0, 1, 2, 3$ and costs $8(\frac{k}{4})^2\mathbf{m}$ for $a_i \cdot b_0$ 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 $(\frac{1}{2} + \frac{1}{k})\mathbf{M}$.

Therefore, the **Addition step** costs $(\frac{1}{2} + \frac{1}{k})\mathbf{M} + (\frac{k}{2} + 14)\mathbf{m} + 1\mathbf{m_c}$, where $1\mathbf{m_c}$ is constant multiplication by a. For a mixed addition step, the costs reduce to $(\frac{1}{2} + \frac{1}{k})\mathbf{M} + (\frac{k}{2} + 12)\mathbf{m} + 1\mathbf{m_c}$.

The **Doubling step** costs $(\frac{1}{2} + \frac{1}{k})\mathbf{M} + 1\mathbf{S} + (\frac{k}{2} + 4)\mathbf{m} + 7\mathbf{s} + 2\mathbf{m_c}$, where $2\mathbf{m_c}$ are constant multiplications by a and d.

6.2 Edwards curves with $j = 0$

The twisted Edwards curve $ax^2 + y^2 = 1 + dx^2y^2$ has j-invariant $j_{a,d} = 16(a^2 + 14ad + d^2)^3/ad(a-d)^4$, hence, $j_{a,d} = 0$ if and only if $a = (-7 \pm 4\sqrt{3})d$. Note that 3 is a square in finite field $\mathbb{F}_q$ if and only if $q \equiv \pm 1 \pmod{12}$. Now we assume that $q \equiv \pm 1 \pmod{12}$ and a, d satisfy the relation $a = (-7 \pm 4\sqrt{3})d$. Then Edwards curve $E_{a,d} : ax^2 + y^2 = 1 + dx^2y^2$ has j-invariant equal to 0, hence, there exist twists of degree 6.

We denote $M = \frac{2(a+d)}{a-d}$ and $N = \frac{4}{a-d}$ when given a, d.

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*

$$W_{MN} : v^2 = u^3 - \frac{M^3N^3}{27}\delta^6$$

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

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

Proof. Firstly, we check that ψ is well defined, i.e. $\psi(u, v) \in E_{a,d}$. We denote $u' = u - \frac{MN\delta^2}{3}$, then

$$v^2 = u^3 - \frac{M^3N^3\delta^6}{27} = u'(u'^2 + MN\delta^2u' + \frac{M^2N^2\delta^4}{3}),$$

$$x = \frac{N\delta u'}{v}, y = \frac{u' - N\delta^2}{u' + N\delta^2}.$$

Note that

$$\frac{1}{x^2} = \frac{v^2}{N^2\delta^2 u'^2} = \frac{1}{N^2\delta^2 u'}(u'^2 + MN\delta^2 u' + \frac{M^2N^2\delta^4}{3}).$$

Since $M - Na = -2, M - Nd = 2, M^2 = 3$, we have

$$\frac{1}{x^2} - a = \frac{1}{N^2\delta^2 u'}(u' - N\delta^2)^2, \frac{1}{x^2} - d = \frac{1}{N^2\delta^2 u'}(u' + N\delta^2)^2.$$

Thus

$$\frac{1 - ax^2}{1 - dx^2} = (\frac{u' - N\delta^2}{u' + N\delta^2})^2 = y^2, \text{i.e. } ax^2 + y^2 = 1 + dx^2y^2.$$

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

$$\frac{X_Q + W_Q}{Y_Q + Z_Q} = x_Q = \frac{Nu}{v}\delta - \frac{MN^2}{3v}\delta^3$$
$$\frac{X_Q - W_Q}{Y_Q + Z_Q} = x_Q \cdot \frac{1 - y_Q}{1 + y_Q} = \frac{N^2}{v}\delta^3$$

For $\theta = \frac{Nu}{2v}\delta^6$ and $\eta = \frac{N^2}{6v}\delta^6$, we have

$$\frac{X_Q}{Y_Q + Z_Q} = \theta\delta^{-5} + (3 - M)\eta\delta^{-3}$$
$$\frac{W_Q}{Y_Q + Z_Q} = \theta\delta^{-5} - (3 + M)\eta\delta^{-3}$$

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

$$\begin{aligned}
g_{P_1,P_2}(Q) &= \frac{\Pi_{P_1,P_2,O'}(Q)}{\Pi_{P_3,O,O'}(Q)} \\
&= \frac{C_X X_Q + C_Y(Y_Q + Z_Q) + C_W W_Q}{W_3 X_Q - X_3 W_Q} \\
&= \frac{C_X \frac{X_Q}{Y_Q+Z_Q} + C_Y + C_W \frac{W_Q}{Y_Q+Z_Q}}{W_3 \frac{X_Q}{Y_Q+Z_Q} - X_3 \frac{W_Q}{Y_Q+Z_Q}} \\
&= \frac{C_X(\theta\delta^{-5} + (3 - M)\eta\delta^{-3}) + C_Y + C_W(\theta\delta^{-5} - (3 + M)\eta\delta^{-3})}{W_3(\theta\delta^{-5} + (3 - M)\eta\delta^{-3}) - X_3(\theta\delta^{-5} - (3 + M)\eta\delta^{-3})} \\
&= \frac{(C_X + C_W)\theta + (3(C_X - C_W) - M(C_X + C_W))\eta\delta^2 + C_Y\delta^5}{(W_3 - X_3)\theta + (3(W_3 + X_3) - M(W_3 - X_3))\eta\delta^2} \\
&\in ((C_X + C_W)\theta + (3(C_X - C_W) - M(C_X + C_W))\eta\delta^2 + C_Y\delta^5)\mathbb{F}^*_{q^{k/2}}.
\end{aligned}$$

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 $M = \frac{2(a+d)}{a-d}$.

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 $\beta = b_0 + b_2\delta^2 + b_5\delta^5$, where $b_5 \in \mathbb{F}_q$ and $b_0, b_2 \in \mathbb{F}_{q^{k/6}}$. When using the Schoolbook method, multiplying α by β costs $6 \cdot \frac{k}{6}\mathbf{m}$ for computing $a_i \cdot b_5, i = 0, 1, 2, 3$ and costs $12(\frac{k}{6})^2\mathbf{m}$ for $a_i \cdot b_0$ and $a_i \cdot b_2$. 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 $(\frac{1}{3} + \frac{1}{k})\mathbf{M}$.

Therefore, the **Addition step** costs $(\frac{1}{3} + \frac{1}{k})\mathbf{M} + (\frac{k}{3} + 14)\mathbf{m} + 2\mathbf{m_c}$, where $2\mathbf{m_c}$ are multiplications by a and $\frac{2(a+d)}{a-d}$. For a mixed addition step, the costs reduce to $(\frac{1}{3} + \frac{1}{k})\mathbf{M} + (\frac{k}{3} + 12)\mathbf{m} + 2\mathbf{m_c}$.

The **Doubling step** costs $(\frac{1}{3} + \frac{1}{k})\mathbf{M} + 1\mathbf{S} + (\frac{k}{3} + 4)\mathbf{m} + 7\mathbf{s} + 3\mathbf{m_c}$, where $3\mathbf{m_c}$ are multiplications by a, d and $\frac{2(a+d)}{a-d}$.

The following table shows the concrete comparison for doubling step(DBL), mixed addition step (mADD) and addition step (ADD).

	DBL	mADD	ADD
Arène et.al. [1]	$1\mathbf{M} + 1\mathbf{S} + k\mathbf{m}$ $+6\mathbf{m} + 5\mathbf{s} + 2\mathbf{m_c}$	$1\mathbf{M} + k\mathbf{m}$ $+12\mathbf{m} + 1\mathbf{m_c}$	$1\mathbf{M} + k\mathbf{m}$ $+14\mathbf{m} + 1\mathbf{m_c}$
this paper $j \neq 0, 1728$	$1\mathbf{M} + 1\mathbf{S} + k\mathbf{m}$ $+4\mathbf{m} + 7\mathbf{s} + 2\mathbf{m_c}$	$1\mathbf{M} + k\mathbf{m}$ $+12\mathbf{m} + 1\mathbf{m_c}$	$1\mathbf{M} + k\mathbf{m}$ $+14\mathbf{m} + 1\mathbf{m_c}$
this paper $j = 1728$	$(\frac{1}{2} + \frac{1}{k})\mathbf{M} + 1\mathbf{S} + \frac{k}{2}\mathbf{m}$ $+4\mathbf{m} + 7\mathbf{s} + 2\mathbf{m_c}$	$(\frac{1}{2} + \frac{1}{k})\mathbf{M} + \frac{k}{2}\mathbf{m}$ $+12\mathbf{m} + 1\mathbf{m_c}$	$(\frac{1}{2} + \frac{1}{k})\mathbf{M} + \frac{k}{2}\mathbf{m}$ $+14\mathbf{m} + 1\mathbf{m_c}$
this paper $j = 0$	$(\frac{1}{3} + \frac{1}{k})\mathbf{M} + 1\mathbf{S} + \frac{k}{3}\mathbf{m}$ $+4\mathbf{m} + 7\mathbf{s} + 3\mathbf{m_c}$	$(\frac{1}{3} + \frac{1}{k})\mathbf{M} + \frac{k}{3}\mathbf{m}$ $+12\mathbf{m} + 2\mathbf{m_c}$	$(\frac{1}{3} + \frac{1}{k})\mathbf{M} + \frac{k}{3}\mathbf{m}$ $+14\mathbf{m} + 2\mathbf{m_c}$

7 Conclusion

In this paper, we propose an elaborate geometry approach to explain the group law on Edwards curves which are seen as the intersection of two quadric surfaces in space. Using the geometric interpretation of the group law we obtain the Miller function of Tate pairing computation on twisted Edwards curves. Then we present the explicit formulae for pairing computation on twisted Edwards curves. The doubling step of our formulae is a littler faster than that in [1]. Finally, to improve the efficiency we present quartic and sextic twists on twisted Edwards curves. By using high-twists the costs of substituting in $j = 1728$ case

and $j = 0$ case can be reduced to a half and a third respectively. Above all, it's interesting to consider more efficient formulae for pairing computation on twist Edwards curves .

References

1. C. Arene, T. Lange, M. Naehrig and C. Ritzenthaler. Faster Computation of the Tate Pairing, Journal of Number Theory 131, pp. 842–857, 2011.
2. R. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen, and F. Vercauteren. *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, CRC Press, 2005.
3. D. J. Bernstein and T. Lange, Faster addition and doubling on elliptic curves. In K. Kurosawa, editor, Advances in Cryptology-ASIACRYPT 2007, volume 4833 of Lect. Notes Comput. Sci., pages 29–50. Springer, 2007.
4. D. J. Bernstein, P. Birkner, M. Joye, T. Lange and C. Peters. Twisted Edwards curves, In AFRICACRYPT 2008, LNCS 5023, 389-405, Springer, 2008.
5. D. J. Bernstein and Tanja Lange. A complete set of addition laws for incomplete Edwards curves, Journal of Number Theory, 131 (2011), pp. 858872, 2011.
6. I. F. Blake, G. Seroussi, and N. P. Smart, *Advances in Elliptic Curve Cryptography*, Cambridge University Press, London, 2005.
7. C. Costello, T. Lange and M. Naehrig. Faster Pairing Computations on Curves with High-Degree Twists, Public Key Cryptography–PKC 2010, Volume 6056 of *LNCS*, pp. 224–242, Springer-Verlag, 2010.
8. M. Prem Laxman Das and Palash Sarkar. Pairing computation on twisted Edwards form elliptic curves. In Pairing-Based Cryptography–Pairing 2008, Second International Conference, Egham, UK, 2008, Proceedings, volume 5209 of Lecture Notes in Computer Science, Berlin, pp. 192C-210, 2008.
9. H.M. Edwards. A normal form for elliptic curves. Bulletin of the American Mathematical Society, 44:393C422, 2007.
10. F. Hess, N.P. Smart and F. Vercauteren. The Eta pairing revisited, IEEE Trans. Infor. Theory, vol 52, pp. 4595–4602, Oct. 2006.
11. F. Hess. Pairing Lattices. In: Galbraith, S.D., Paterson, K.G. (eds.) Pairing 2008. volume 5209 of *LNCS*, pp. 18–38. Springer-Verlag, 2008.
12. H. Hisil, K. Koon-HoWong, G. Carter and Ed Dawson. Twisted Edwards curves revisited. In ASIACRYPT 2008, Melbourne, volume 5350 of Lecture Notes in Computer Science, Berlin, pages 326C343, 2008.
13. S. Ionica and Antoine Joux. Another approach to pairing computation in Edwards coordinates. Dipanwita Roy Chowdhury, Vincent Rijmen, and Abhijit Das, editors. Progress in Cryptology - INDOCRYPT 2008, volume 5365 of Lecture Notes in Computer Science, Springer, 2008, pp 400C413. http://eprint.iacr.org/2008/292.
14. N. Koblitz and A.J. Menezes. Pairing-based cryptography at high security levels, Cryptography and Coding, Volume 3796 of *LNCS*, pp. 13–36. Springer-Verlag, 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), 235-261 (2004).
17. F. Vercauteren. Optimal pairings. IEEE Trans. Inf. Theory 56, 455–461, 2010.