Pairing Computation on Edwards Curves with High-Degree Twists

Liangze Li[1,3], Hongfeng Wu[2(✉)], and Fan Zhang[1]

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

Abstract. Elliptic curve can be seen as the intersection of two quadratic surfaces in space. In this paper, we used the geometry approach to explain the group law for general elliptic curves given by intersection of two quadratic surfaces, then we construct the Miller function over the intersection of quadratic surfaces. As an example, we obtain the Miller function of Tate pairing computation on twisted Edwards curves. Then we present the explicit formulae for pairing computation on Edwards curves. Our formulae for the doubling step are a littler faster than that proposed by Arène et al.. Moreover, when $j = 1728$ and $j = 0$ we consider quartic and sextic twists to improve the efficiency respectively. Finally, we present the formulae of refinements technique on Edwards curves to obtain gain up when the embedding degree is odd.

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

1 Introduction

To compute pairings efficiently is always a bottleneck for implementing pairing-based cryptography. The basic method of computing pairings is Miller's algorithm [20]. Consequently, various improvements were presented in [1,13,14,17,21]. 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 [2]. Then twisted Edwards curves which are the generalization of Edwards curves were introduced by Bernstein et al. in [3]. Bernstein and Lange also pointed out several advantages of applying the Edwards curves to cryptography. Edwards curves are far superior in elliptic curve cryptography because of fast addition formulae. Pairing computation over Edwards curves was first considered in [8,16]. In 2009, Arène et al. [1]

D. Lin et al. (Eds.): Inscrypt 2013, LNCS 8567, pp. 185–200, 2014.
DOI: 10.1007/978-3-319-12087-4_12

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.

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 $S_{a,d}: aX^2+Y^2 = Z^2+dW^2,\ XY = ZW$. 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 [19]. In some situations it is more effectively to write an elliptic curve as the intersection of two quadratic surfaces in space. Jacobi quartic curve is another example of the importance [7,18]. In [22], we use a straightforward way 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. In this paper, we used the geometry approach of [19] to explain the group law for general elliptic curves given by intersection of two quadratic surfaces, then we construct the Miller function over the intersection of quadratic surfaces. As an example, we obtain the Miller function of Tate pairing computation on twisted Edwards curves. Of course, you can use a similar approach to compute Tate pairing on any elliptic curves given by intersection of two quadratic surfaces. However, for the sake of integrity, we recalculate the explicit formulae for pairing computation on twisted Edwards curves. The high-twists had been sufficiently studied by Costello, Lange and Naehrig [6] on Weierstrass curves. As the result given by [11], one elliptic curve and its quartic/sextic twist can't both be written in a rational twisted Edwards form, so we turn to Weierstrass curves for the high-degree twists of twisted Edwards curves. These twists enable us to reduce the cost of substituting to a half and a third respectively in $j = 1728$ case and $j = 0$ case. For Edwards curves, it is an interesting problem to find an efficient way to compute ate pairing on twisted Edwards curves.

When the embedding degree is even, the traditional denominator elimination technique is used. While the denominator elimination can not be used if the embedding degree is odd, so we consider the refinement technique to improve the efficiency. In [5], Blake et al. presented three refinements to Miller's algorithm over Weierstrass curves by reducing the total number of vertical lines in Miller's algorithm. This method can be used for both Weil and Tate Pairing over Weierstrass curves with any embedding degree. In [23], L. Xu and D. Lin study the refinements formulas for Edwards curves. If we see the Edwards curves as the intersection of two quadratic surfaces in space, our refinements over Edwards curves cost less than the refinements of L. Xu and D. Lin [23], because in our method we use one plane to replace two lines of the Miller function in [23].

In this paper, we use $\mathbf{m}$ and $\mathbf{s}$ denote the costs of multiplication and squaring in the base field $\mathbb{F}_q$ while $\mathbf{M}$ and $\mathbf{S}$ denote the costs of multiplication and squaring in the extension $\mathbb{F}_{q^k}$.

2 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 [20]. The main ideal of Miller's algorithm is to inductively build up such a function f_P by constructing the function $f_{n,P}$. The function $f_{n,P}$ is defined by $(f_{n,P}) = n(P) - ([n]P) - (n-1)(O)$, n is an integer smaller than r.

Let $g_{P,T} \in \mathbb{F}_q(E)$ be the rational function satisfying $\mathrm{div}(g_{P,T}) = (P) + (T) - (O) - (P + T)$, where $P + T$ denotes the sum of P and T on E, and additions of the form $(P) + (T)$ denote formal additions in the divisor group.

If $P \in E$, define $f_{0,P} = f_{1,P} = 1$. Inductively, for $n > 0$, define $f_{n+1,P} := f_{n,P} g_{P,nP}$, then we have

$$f_{m+n,P} = f_{m,P} \cdot f_{n,P} \cdot g_{mP,nP}.$$

3 Edwards Curves

In this section, we review the preliminaries of Edwards curves. Let $\mathbb{F}_q$ be a finite field with characteristic greater than 3. A twisted Edwards curve is a quartic curve over $\mathbb{F}_q$, defined by

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

where a, d are distinct nonzero elements of $\mathbb{F}_q$. In [3], Bernstein et al. proved that an elliptic curve over a field K with the group $4|\sharp E(K)$ if and only if E is birationally equivalent over K to a twisted Edwards curve. The sum of two points (x_1, y_1) and (x_2, y_2) on the twisted Edwards curve $E_{a,d}$ is

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2} \right).$$

The point $(0, 1)$ is the unit of the addition law. The inverse of a point (x, y) on $E_{a,d}$ is $(-x, y)$.

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:

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

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 $S_{a,d}$ can be found in [4,15].

4 Group Law Over the Intersection of Quadratic Surfaces

Let E denote the intersection of quadratic surfaces. The group law of this kind of curve is different from that of cubic 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 E at exactly four points. Although these planes are not functions on E, their divisors can be well defined as:

$$(\Pi) = \sum_{P \in \Pi \cap E} n_P(P) \tag{3}$$

where n_P is the intersection multiplicity of Π and E at P. Then the quotient of two projective planes is a well defined function which gives principal divisor. Let $O \in E(\mathbb{F}_q)$ be the neutral element, there must be a plane intersects E with multiply three at O, and its fourth intersecting points with E is O'. It is also obvious that P_1, P_2, P_3 and P_4 are coplaner if and only if $P_1 + P_2 + P_3 + P_4 = O'$.

4.1 Miller Function Over the Intersection of Quadratic Surfaces

In this section we construct the Miller function over the intersection of quadratic surfaces.

Let E be the intersection of two quadratic surfaces, O is the neutral element; P_1 and P_2 be two different points on E, $\Pi_{P_1,P_2,O'}$ denote the projective plane passing through P_1, P_2 and O'. The group law given above shows that $-P_1 - P_2$ is the third intersection, by (3) we can get:

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

Similarly, $\Pi_{T+P,O,O'}$ intersects with E at $P_1 + P_2$, O', O and $-P_1 - P_2$. Then:

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

Thus,

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

The geometry interpolation derives the formula of Miller's function directly. The Miller's function with divisor $(P_1) + (P_2) - (P_1 + P_2) - (O)$ can be given

$$g_{P_1,P_2} = \frac{\Pi_{P_1,P_2,O'}}{\Pi_{P_1+P_2,O,O'}} \tag{4}$$

In Miller's algorithm, P is always a fixed point, T is always nP for some integer n. For the addition steps, Miller function $g_{T,P}$ over E can be given by setting $P_1 = T, P_2 = P$. For the doubling steps, Miller function $g_{T,T}$ over E is given by setting $P_1 = P_2 = T$.

Note that the planes appear in the formula always pass through O'. Particularly, if P_1, P_2 and O' are pairwise distinct points on $S_{a,d}$. We use the equation $C_X X + C_Y Y + C_Z Z + C_W W = 0$ to denote a projective plane. By solving linear equations, we get the coefficients of the plane $\Pi_{P_1,P_2,O'}$ in Miller function of twisted Edwards curves as follows:

$$\begin{aligned} C_X &= W_2(Z_1 + Y_1) - W_1(Z_2 + Y_2), \\ C_Y &= X_2 W_1 - X_1 W_2, \\ C_W &= X_1(Y_2 + Z_2) - X_2(Z_1 + Y_1) \end{aligned} \tag{5}$$

In the case that $P_1 = P_2$, we have

$$C_X = Y_1 Z_1 - a X_1^2,\ C_Y = X_1 Z_1 - X_1 Y_1,\ C_W = d X_1 W_1 - Z_1^2. \tag{6}$$

5 Pairing Computation on $S_{a,d}$ with Even Embedding Degrees

In this section, we analysis computation steps in Miller's algorithm explicitly. The results in this section are mainly from [22]. For an addition step or doubling step, 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. For the evaluating part, some standard methods such as denominator elimination and subfield simplification can be used, as we introduce below.

As usual, we choose $P \in S_{a,d}(\mathbb{F}_q)[r]$ and $Q \in S_{a,d}(\mathbb{F}_{q^k})$, where $k > 1$ is the embedding degree. In fact as stated in [13], Q can be chosen from a subgroup which is given by a twist of $S_{a,d}$. More precisely, for $d = \#\mathrm{Aut}(S_{a,d})$, there is degree-$d$ twist of $S_{a,d}$ over $\mathbb{F}_{q^{k/d}}$ denoted as E' such that $Q \in \psi(E'(\mathbb{F}_{q^{k/d}}))$ with $\psi : E' \to S_{a,d}$ an isomorphism over $\mathbb{F}_{q^{k/d}}$. It is noticeable that E' is not necessary to have a twisted Edwards model.

In this part, 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 $Q' = (X_0 : Y_0 : W_0 : Z_0) \in$

$S_{a\delta^{-2},d\delta^{-2}}(\mathbb{F}_{q^{k/2}})$, we can see that $Q = (X_0 : \delta Y_0 : W_0 : \delta Z_0) \in S_{a,d}(\mathbb{F}_{q^k})$. 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 $\eta = \frac{W_0}{Y_0+Z_0}$. It is clearly that $(W_3X_0 - X_3W_0)/(Y_0 + Z_0)$ in $\mathbb{F}^*_{q^{k/2}}$, then it can be discarded in pairing computation thanks to the final exponentiation, This fact is usually called the denominator elimination technique.

In generally, Let $\mathbb{F}_q$ be an ordinary elliptic curve with neutral elements $O \in E(\mathbb{F}_q)$, then Miller function $g_{P_1,P_2} = \frac{\Pi_{P_1,P_2,O'}}{\Pi_{P_1+P_2,O,O'}} = \frac{\Pi_{P_1,P_2,O'}/\Pi_{O,O,O'}}{\Pi_{P_1+P_2,O,O'}//\Pi_{O,O,O'}}$. let $E'/\mathbb{F}_q$ is a degree-d twist of $E/\mathbb{F}_q$ with d even, thus the isomorphism $\phi : E' \to E$ is defined over $\mathbb{F}_{q^d}$. Then for any $Q' \in E'(\mathbb{F}_q)$ and $P \neq O \in E(\mathbb{F}_q)$, the value of function $\Pi_{P,O,O'}/\Pi_{O,O,O'} \in \mathbb{F}_q(E)$ at $Q = \phi(Q') \in \mathbb{F}^*_{q^{d/2}}$ if $Q \neq \pm P$. Thus it is eliminated by the final exponential.

Note that $\theta, \eta \in \mathbb{F}_{q^{k/2}}$ are fixed during pairing 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).

Addition Steps. Let $P_1 = T$ and $P_2 = P$ be distinct points with $Z_1Z_2 \neq 0$. By variant of formula (2) and (5), 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 $1\mathbf{M} + k\mathbf{m} + 12\mathbf{m} + 1\mathbf{m_c}$.

Doubling Steps. For $P_1 = P_2 = T$, $P_3 = 2T$. By the formulae of (2) and (6), 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.

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	$1\mathbf{M}+1\mathbf{S}+k\mathbf{m}$ $+4\mathbf{m}+7\mathbf{s}+2\mathbf{m_c}$	$1\mathbf{M}+k\mathbf{m}$ $+12\mathbf{m}+1\mathbf{m_c}$	$1\mathbf{M}+k\mathbf{m}$ $+14\mathbf{m}+1\mathbf{m_c}$

5.1 Pairing Computation on $S_{a,d}$ with Twists of Degree 4 or 6

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 $j(E) = 1728$.

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, the j-invariant of $E_{a,-a} : ax^2 + y^2 = 1 - ax^2y^2$ equal to 1728, thus, there exist twists of degree 4. The case $a = 1$ is the "classical" Edwards curve $x^2 + y^2 = 1 - x^2y^2$ with complex multiplication $D = -4$ [12]. Furthermore, $j_{a,d} = 0$ 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. The case $a = 1$ is the Edwards curve $x^2+y^2 = 1-(7+4\sqrt{3})x^2y^2$ with complex multiplication $D = -3$ [12]. But Galbraith showed one elliptic curve and its quartic/sextic twist can't both be written in a rational twisted Edwards form [11], so we turn to Weierstrass curves for the high-degree twists of twisted Edwards curves.

Twists of Degree 4

Lemma 1 ([22], 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*

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

The inverse transformation is $(x,y) \mapsto ((1+y)/(\delta^2(1-y)), (1+y)/(\delta^3 x(1-y)))$. 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 $Q \in S_{a,-a}(\mathbb{F}_{q^k})$ 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:

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

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

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

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.

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 $b_0, b_2 \in \mathbb{F}_{q^{k/4}}$. This special representation may lead to some optimization of the main multiplication in $\mathbb{F}_{q^k}$, but when using the field towering the cost will remain approximately $1\mathbf{M}$.

Therefore, the addition step costs $1\mathbf{M} + (\frac{k}{2} + 14)\mathbf{m} + 1\mathbf{m_c}$, where $1\mathbf{m_c}$ is constant multiplication by a. For a mixed addition step, the costs reduce to $1\mathbf{M} + (\frac{k}{2} + 12)\mathbf{m} + 1\mathbf{m_c}$. The doubling step costs $1\mathbf{M} + 1\mathbf{S} + (\frac{k}{2} + 4)\mathbf{m} + 7\mathbf{s} + 2\mathbf{m_c}$, where $2\mathbf{m_c}$ are constant multiplications by a and d.

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.

By the way, according to the definition of Ate pairing, the point addition and doubling are performed in $\mathbb{F}_{q^k}$. Thanks to the Lemma 1, we can choose $Q' \in W_a$ such that $Q=\psi(Q') \in S_{a,-a}$. So, is there a efficient way to compute ate pairing on twisted Edwards curves?

Twists of Degree 6. We denote $M=\frac{2(a+d)}{a-d}$ and $N=\frac{4}{a-d}$ when given a,d.

Lemma 2 ([22], 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 $W_{M,N}: v^2=u^3-\frac{M^3N^3}{27}\delta^6$ is a twist of degree 6 over $\mathbb{F}_{q^{k/6}}$ of $E_{a,d}$. The isomorphism can be given as*

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

The inverse transformation is $(x,y) \mapsto ((y(MN\delta^2-3N\delta^2)-(MN\delta^2+3N\delta^2))/3(y-1), -N^2\delta^3(1+y)/x)$.

Similarly with the twists of degree 4 case, for the evaluation of $g_{P_1,P_2}(Q)$ with $P_3=P_1+P_2 \neq O, O'$, we get

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

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

Furthermore, the reduced $g(Q)$ can be denoted as $\beta=b_0+b_2\delta^2+b_5\delta^5$, where $b_5 \in \mathbb{F}_q$ and $b_0, b_2 \in \mathbb{F}_{q^{k/6}}$. The cost of main multiplication is still $1\mathbf{M}$ with some possibilities of further optimization. Therefore, the addition step costs

$1\mathbf{M} + (\frac{k}{3} + 14)\mathbf{m} + 2\mathbf{m_c}$. For a mixed addition step, the costs reduce to $1\mathbf{M} + (\frac{k}{3} + 12)\mathbf{m} + 2\mathbf{m_c}$. The doubling step costs $1\mathbf{M} + 1\mathbf{S} + (\frac{k}{3} + 4)\mathbf{m} + 7\mathbf{s} + 3\mathbf{m_c}$.

Likewise, 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 total cost of Tate pairing computation on twisted Edwards curves with $j = 1728$ or $j = 0$.

	DBL	mADD	ADD
This paper	$1\mathbf{M} + 1\mathbf{S} + \frac{k}{2}\mathbf{m}$	$1\mathbf{M} + \frac{k}{2}\mathbf{m}$	$1\mathbf{M} + \frac{k}{2}\mathbf{m}$
$j = 1728$	$+4\mathbf{m} + 7\mathbf{s} + 2\mathbf{m_c}$	$+12\mathbf{m} + 1\mathbf{m_c}$	$+14\mathbf{m} + 1\mathbf{m_c}$
This paper	$1\mathbf{M} + 1\mathbf{S} + \frac{k}{3}\mathbf{m}$	$1\mathbf{M} + \frac{k}{3}\mathbf{m}$	$1\mathbf{M} + \frac{k}{3}\mathbf{m}$
$j = 0$	$+4\mathbf{m} + 7\mathbf{s} + 3\mathbf{m_c}$	$+12\mathbf{m} + 2\mathbf{m_c}$	$+14\mathbf{m} + 2\mathbf{m_c}$

6 Refinements Over Twisted Edwards Curves

When the embedding degree is odd, to improve the efficiency we may use the refinements technique to reduce the cost of the multiplication and squaring in the extension field $\mathbb{F}_{q^k}$. The refinements technique is first prosed by [5]. In [23], L. Xu and D. Lin study the refinements formulas for Edwards curves. From formula (4), the iterative formula over the intersection of quadratic surfaces can be rewritten as:

$$f_{n,P} \cdot f_{m,P} \cdot g_{nP,mP} = f_{n,P} \cdot f_{m,P} \cdot \frac{\Pi_{nP,mP,O'}}{\Pi_{(n+m)P,O',O}}$$

In fact, we can study the refinements over Edwards curves based on the following observations.

Theorem 1.

$$\frac{\Pi_{T,T,O'}}{\Pi_{2T,O',O}} \cdot \frac{\Pi_{2T,P,O'}}{\Pi_{2T+P,O',O}} = \frac{\Pi_{T,T,O'}}{\Pi_{-2T,-P,O'}} \cdot \frac{\Pi_{P,O',O}}{\Pi_{O',O,O}}$$

Proof. By the group law described in Sect. 4, we can get

$$\left(\frac{\Pi_{T,T,O'}}{\Pi_{2T,O',O}} \cdot \frac{\Pi_{2T,P,O'}}{\Pi_{2T+P,O',O}}\right) = 2(T) + (P) - (2T + P) - 2(O)$$

we reconstruct the divisor $2(T)+(P)-(2T+P)-2(O)$ as:

$$\frac{(T)+(T)+(O')+(-2T)+(P)+(O')+(O)+(-P)}{(-2T)+(-P)+(O')+(2T+P)+(O)+3(O')}$$

while, from the formula (3) the above divisor is exactly

$$\left(\frac{\Pi_{T,T,O'}}{\Pi_{-2T,-P,O'}}\cdot\frac{\Pi_{P,O',O}}{\Pi_{O',O,O}}\right)$$

Since, in the Miller's algorithm we choose all the rational functions to be normalized. Thus,

$$\frac{\Pi_{T,T,O'}}{\Pi_{2T,O',O}}\cdot\frac{\Pi_{2T,P,O'}}{\Pi_{2T+P,O',O}}=\frac{\Pi_{T,T,O'}}{\Pi_{-2T,-P,O'}}\cdot\frac{\Pi_{P,O',O}}{\Pi_{O',O,O}}$$

□

Theorem 2.

$$\frac{\Pi_{4T,r_iP,O'}}{\Pi_{4T+r_iP,O',O}}\cdot\frac{\Pi_{2T,2T,O'}}{\Pi_{4T,O',O}}\cdot\frac{\Pi^2_{T,T,O'}}{\Pi^2_{2T,O',O}}=\frac{\Pi^2_{T,T,O'}}{\Pi_{-2T,-2T,O'}\cdot\Pi_{4T+r_iP,O',O}}\cdot\frac{\Pi_{4T,r_iP,O'}}{\Pi_{O',O,O}}$$

Proof. By the group law described in Sect. 4, we can get

$$\left(\frac{\Pi_{4T,r_iP,O'}}{\Pi_{4T+r_iP,O',O}}\cdot\frac{\Pi_{2T,2T,O'}}{\Pi_{4T,O',O}}\cdot\frac{\Pi^2_{T,T,O'}}{\Pi^2_{2T,O',O}}\right)=4(T)+(r_iP)-(4T+r_iP)-4(O)$$

we reconstruct the divisor $4(T)+(r_iP)-(4T+r_iP)-4(O)$ as:

$$\frac{2(T)+2(T)+2(O')+2(-2T)+(4T)+(r_iP)+(O')+(-4T-r_iP)}{2(-2T)+(O')+(4T)+(4T+r_iP)+(O')+(O)+(-4T-r_iP)+(O')+3(O)}$$

while, by the formula (3) we can get the above divisor is exactly

$$\left(\frac{\Pi^2_{T,T,O'}}{\Pi_{-2T,-2T,O'}\cdot\Pi_{4T+r_iP,O',O}}\cdot\frac{\Pi_{4T,r_iP,O'}}{\Pi_{O',O,O}}\right)$$

since, in the Miller's algorithm we choose all the rational functions to be normalized. So we have:

$$\frac{\Pi_{4T,r_iP,O'}}{\Pi_{4T+r_iP,O',O}}\cdot\frac{\Pi_{2T,2T,O'}}{\Pi_{4T,O',O}}\cdot\frac{\Pi^2_{T,T,O'}}{\Pi^2_{2T,O',O}}=\frac{\Pi^2_{T,T,O'}}{\Pi_{-2T,-2T,O'}\cdot\Pi_{4T+r_iP,O',O}}\cdot\frac{\Pi_{4T,r_iP,O'}}{\Pi_{O',O,O}}$$

□

$2T+P$-form Refinement. In the *ith* basic Miller iteration of Algorithm 1, we can displace the explicit formula of f as follows:

$$f\leftarrow f^2\cdot\frac{\Pi_{T,T,O'}(Q)}{\Pi_{2T,O',O}(Q)}\cdot\frac{\Pi_{2T,P,O'}(Q)}{\Pi_{2T+P,O',O}(Q)}$$

Our $2T + P$-form refinement is based on Theorem 1, the formula of f in the *ith* basic Miller iteration in our algorithm is:

$$f \leftarrow f^2 \cdot \frac{\Pi_{T,T,O'}(Q)}{\Pi_{-2T,-P,O'}(Q)} \cdot \frac{\Pi_{P,O',O}(Q)}{\Pi_{O',O,O}(Q)}$$

$4T+r_iP$–form Refinements. When $r_i = 0, 1, 2, 3$, in the *ith* basic Miller iteration of Algorithm 4.1 in [5], we can display an explicit formula of f in the *ith* basic Miller iteration as follows:

$$f \leftarrow f^4 \cdot f_{r_i,P} \cdot \frac{\Pi_{4T,r_iP,O'}(Q)}{\Pi_{4T+r_iP,O',O}(Q)} \cdot \frac{\Pi_{2T,2T,O'}(Q)}{\Pi_{4T,O',O}(Q)} \cdot \frac{\Pi^2_{T,T,O'}(Q)}{\Pi^2_{2T,O',O}(Q)}$$

where $f_{2,P} = \frac{\Pi_{P,P,O'}}{\Pi_{2P,O',O}}$, $f_{3,P} = \frac{\Pi_{2P,P,O'}}{\Pi_{3P,O',O}} \cdot \frac{\Pi_{P,P,O'}}{\Pi_{2P,O',O}}$, $2P$ and $3P$ can be precalculated. When $r_i = 0$, the above formula turns to:

$$f \leftarrow f^4 \cdot \frac{\Pi_{2T,2T,O'}(Q)}{\Pi_{4T,O',O}(Q)} \cdot \frac{\Pi^2_{T,T,O'}(Q)}{\Pi^2_{2T,O',O}(Q)}$$

Our $4T + r_iP$-form refinement is based on Theorem 2. The original formula of updating f in the *ith* basic Miller's iteration can be replaced as:

$$f \leftarrow f^4 \cdot f_{r_i,P} \cdot \frac{\Pi^2_{T,T,O'}(Q)}{\Pi_{-2T,-2T,O'}(Q) \cdot \Pi_{4T+r_iP,O',O}(Q)} \cdot \frac{\Pi_{4T,r_iP,O'}(Q)}{\Pi_{O',O,O}(Q)}$$

When $r_i = 0$ the above formula turns to:

$$f \leftarrow f^4 \cdot \frac{\Pi^2_{T,T,O'}(Q)}{\Pi_{-2T,-2T,O'}(Q) \cdot \Pi_{O',O,O}(Q)}$$

6.1 Pairing Computation on $S_{a,d}$ with Odd Embedding Degrees

For a projective line Π, we define $\Pi(Q)$ to be the value of $\frac{\Pi}{Z}(Q)$, which is actually the value of Π when substituting the coordinates of Q with $Z_Q = 1$. If we precalculate the coordinates of Q such that $\Pi_{O',O,O}(Q) = 1$ (this can easily be done in practice), then the plane $\Pi_{O',O,O}$ can be eliminated in our formulae. In this case, we can save one multiplication. In most cases (see $3T + r_iP$ and $4T+r_iP$-form refinements), the total number of the planes which present in each new formula is smaller than that in original formula. This also can save some multiplications of the extension field $\mathbb{F}_q^k$.

In fact, the plane $\Pi_{T,O',O}$ is the equation $W_T X - X_T W = 0$. For any point Q, if we precalculate its coordinates with $W_Q = 1$, then:

$$\Pi_{T,P,O'}(Q) = C_X X_Q + C_Y(Y_Q + Z_Q) + C_W,\ \Pi_{T,O',O}(Q) = W_T X_Q - X_T.$$

so, it takes **2km** to evaluate $\Pi_{T,P,O}$ at Q, and **km** to evaluate $\Pi_{T,O',O}$ at Q.

If we calculate the coordinates of Q such that $X_Q - W_Q = 1$, that is $\Pi_{O',O,O}(Q) = 1$, then:

$$\Pi_{T,P,O'}(Q) = C_X + C_Y(Y_Q + Z_Q) + (C_W + C_X)W_Q,\ \Pi_{T,O',O}(Q) = (W_T - X_T)X_Q + X_T.$$

so, it takes **2km** to evaluate $\Pi_{T,P,O}$ at Q, and **km** to evaluate $\Pi_{T,O',O}$ at Q.

The cost of updating points in our formulae is the same with the original ones, so we ignore this cost in the base field in the following table.

Iteration forms	$2T + P$	$3T$	$4T$
Original algorithm	$2S + 4M + 6km$	$2S + 4M + 6km$	$4S + 4M + 6km$
Our algorithm	$2S + 3M + 4km$	$2S + 3M + 5km$	$4S + 2M + 4km$
Iteration forms	$4T + P$	$4T + 2P$	$4T + 3P$
Original algorithm	$4S + 6M + 9km$	$4S + 8M + 9km$	$4S + 8M + 9km$
Our algorithm	$4S + 4M + 7km$	$4S + 6M + 7km$	$4S + 6M + 7km$

The refinements over Edwards curves in [23] are corresponding to our $4T + r_iP$-refinements. Our $4T$ and $4T + P$-refinement cost less than the "00" and "01" cases in [23]. By combining their two lines into one plane we can reduce one **M**. Comparing to their "10" and "11" cases, our $4T+2P$ and $4T+3P$-refinement use precalculation to get more improvements. See the comparison in the following table.

	$4T$(case"00")	$4T + P$(case"01")	$4T + 2P$(case"10")	$4T + 3P$(case"11")
Result 1 [23]	$5S + 3M$	$4S + 7M$	$4S + 7M$	$4S + 11M$
Result 2 [23]	$5S + 3M$	$4S + 8M$	$4S + 8M$	$4S + 10M$
Result this paper	$4S + 2M$	$4S + 4M$	$4S + 6M$	$4S + 6M$

Acknowledgment. This work was supported by National Natural Science Foundation of China (No. 11101002, No. 11271129 and No. 61370187) and Beijing Natural Science Foundation (No. 1132009).

A Examples of Pairing-Friendly Edwards Curves

We list some pairing friendly Edwards curves with various k=6,12,24. We use construction 6.6 in [10] to present it. $h = \#S_{1,d}(\mathbb{F}_p)/r$, $\rho = \log_2(p)/\log_2(r)$.

k =6, $\rho = 1.99$, $\lceil \log_2(p) \rceil = 511$, $\lceil \log_2(r) \rceil = 257$, $\lceil \log_2(p^k) \rceil = 3063$,

p =44692693099808656998580083327352824590117294422835042122429200465254107669101255894363776709837049695943172869161549919107677836207766000278874710851962 17,

r =1157920892373161954235709850086879132491274769309617791781887340
53461721558841,
h =$2^6 \cdot 3 \cdot 11^4 \cdot 31^2 \cdot 15659837533^2 \cdot 24137588942339208198652 7^2$,
d =3664251552441012307564539365366691396566209647164298880039621750
38550651579400749412066958104806298693456087744210663737315137925
25747580224215243612885716.

k =12, $\rho = 1.48$, $\lceil \log_2(p) \rceil = 239$, $\lceil \log_2(r) \rceil = 161$, $\lceil \log_2(p^k) \rceil = 2861$,
p =5889490310694441330739011548712381814951849552463124431529211730
78632117,
r =14615016530104764195638243240757034706068926150 01,
h =$2^4 \cdot 3 \cdot 13^2 \cdot 19^2 \cdot 331^2 \cdot 1120711^2$,
d =3039686049194322977578848038674418249362581181730689600918590539
56432956.

k =12, $\rho = 1.49$, $\lceil \log_2(p) \rceil = 383$, $\lceil \log_2(r) \rceil = 257$, $\lceil \log_2(p^k) \rceil = 4589$,
p =1313400206546489077704631059395345592330370814691407061669418717
81698452360783727142491357153402842748519815544714 37,
r =1157920892373165737821551871767212460418194942614239462794724036
61265709211401,
h =$2^4 \cdot 3^5 \cdot 3245503^2 \cdot 52627646891^2$,
d =2086750387520096896070418610187776681469852959441702575044395173
98780297270374071502899550813840255196636221792 4268.

k =24, $\rho = 1.24$, $\lceil \log_2(p) \rceil = 319$, $\lceil \log_2(r) \rceil = 257$, $\lceil \log_2(p^k) \rceil = 7642$,
p =7120003282946788688767832825047892963122039770343506948090350241
49143440464464180057177127640101,
r =1157926942199022831048968574721142864333630419694136944823750216
16015000100401,
h =$2^4 \cdot 3^3 \cdot 5^4 \cdot 17^2 \cdot 280717^2$,
d =6563654562067688285838956119740898916476600058476145431602456870
26515961016144451301736185502 73.

References

1. Arene, C., Lange, T., Naehrig, M., Ritzenthaler, C.: Faster computation of the tate pairing. J. Number Theory **131**, 842–857 (2011)
2. Bernstein, D.J., Lange, T.: Faster addition and doubling on elliptic curves. In: Kurosawa, K. (ed.) ASIACRYPT 2007. LNCS, vol. 4833, pp. 29–50. Springer, Heidelberg (2007)
3. Bernstein, D.J., Birkner, P., Joye, M., Lange, T., Peters, C.: Twisted Edwards curves. In: Vaudenay, S. (ed.) AFRICACRYPT 2008. LNCS, vol. 5023, pp. 389–405. Springer, Heidelberg (2008)
4. Bernstein, D.J., Lange, T.: A complete set of addition laws for incomplete Edwards curves. J. Number Theory **131**, 858–872 (2011)
5. Blake, I.F., Murty, V.K., Xu, G.: Refinements of Miller's algorithm for computing the Weil/Tate pairing. J. Algorithm **58**, 134–149 (2006)
6. Costello, C., Lange, T., Naehrig, M.: Faster pairing computations on curves with high-degree twists. In: Nguyen, P.Q., Pointcheval, D. (eds.) PKC 2010. LNCS, vol. 6056, pp. 224–242. Springer, Heidelberg (2010)
7. Duquesne, S., Fouotsa, E.: Tate pairing computation on Jacobi's elliptic curves. In: Abdalla, M., Lange, T. (eds.) Pairing 2012. LNCS, vol. 7708, pp. 254–269. Springer, Heidelberg (2013)
8. Das, M.P.L., Sarkar, P.: Pairing computation on twisted Edwards form elliptic curves. In: Galbraith, S.D., Paterson, K.G. (eds.) Pairing 2008. LNCS, vol. 5209, pp. 192–210. Springer, Heidelberg (2008)
9. Edwards, H.M.: A normal form for elliptic curves. Bull. Am. Math. Soc. **44**, 393–422 (2007)
10. Freeman, D., Scott, M., Teske, E.: A taxonomy of pairing-friendly elliptic curves. J. Cryptol. **23**(2), 224–280 (2010)
11. Galbraith, S.D.: Mathematics of Public Key Cryptography. Cambridge University Press, Cambridge (2012)
12. Galbraith, S.D., Lin, X., Scott, M.: Endomorphisms for faster elliptic curve cryptography on a large class of curves. J. Cryptogr. **24**(3), 446–469 (2011)
13. Hess, F., Smart, N.P., Vercauteren, F.: The eta pairing revisited. IEEE Trans. Inf. Theory **52**, 4595–4602 (2006)
14. Hess, F.: Pairing lattices. In: Galbraith, S.D., Paterson, K.G. (eds.) Pairing 2008. LNCS, vol. 5209, pp. 18–38. Springer, Heidelberg (2008)
15. Hisil, H., Wong, K.K.-H., Carter, G., Dawson, E.: Twisted Edwards curves revisited. In: Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, vol. 5350, pp. 326–343. Springer, Heidelberg (2008)
16. Ionica, S., Joux, A.: Another approach to pairing computation in Edwards coordinates. In: Chowdhury, D.R., Rijmen, V., Das, A. (eds.) INDOCRYPT 2008. LNCS, vol. 5365, pp. 400–413. Springer, Heidelberg (2008)
17. Koblitz, N., Menezes, A.: Pairing-based cryptography at high security levels. In: Smart, N.P. (ed.) Cryptography and Coding 2005. LNCS, vol. 3796, pp. 13–36. Springer, Heidelberg (2005)
18. Li, L., Wu, H., Zhang, F.: Faster pairing computation on Jacobi quartic curves with high-degree twists. http://eprint.iacr.org/2012/551.pdf
19. Merriman, J.R., Siksek, S., Smart, N.P.: Explicit 4-descents on an elliptic curve. Acta Arithmetica **77**(4), 385–404 (1996)
20. Miller, V.S.: The weil pairing and its efficient calculation. J. Cryptol. **17**(44), 235–261 (2004)

21. Vercauteren, F.: Optimal pairings. IEEE Trans. Inf. Theory **56**, 455–461 (2010)
22. Wu, H., Li, L., Zhang, F.: The pairing computation on Edwards curves. Math. Prob. Eng. **2013**, Article ID 136767, 8 pp. (2013). doi:10.1155/2013/136767
23. Xu, L., Lin, D.: Refinement of Miller's algorithm over Edwards curves. In: Pieprzyk, J. (ed.) CT-RSA 2010. LNCS, vol. 5985, pp. 106–118. Springer, Heidelberg (2010)