Computation of Tate Pairing for Supersingular Curves over characteristic 5 and 7

Kunpeng Wang [a] Bao Li [a]

[a] *State Key Laboratory of Information Security (Graduate School of Chinese Academy of Science), Beijing, 100039*

Abstract

We compute Tate pairing over supersingular elliptic curves via the generic BGhES[3] method for $p = 5, 7$. In those cases, the point multiplication by p is efficiently computed by the Frobenius endomorphism. The function in a cycle can be efficiently computed by the method of continued fraction.

Key words: Tate pairing, continued fraction, Frobenius Endomorphism, supersingular

1 Introduction

The Tate pairing have many cryptographic applications, such as one-round 3-way key establishment, identity-based encryption, and short signatures [8]. For a fixed positive integer m, the Tate pairing e_m is a bilinear map that takes as input an m-torsion points on an elliptic curve and an m-torsion points on the quotient of the elliptic curve, the image is an m-th root of unity in the field.

For cryptographic applications, the objective is to have a bilinear map with a specific recipe for efficient evaluation, and no clear way to invert. The Tate

⋆ Supported by the National Natural Science Foundation of China (Grant No. 90304013), the National High-Tech Research and Development Plan of China (Grant No. 2003AA144151) and the Presidential Foundation of Graduate School of Chinese Academy of Science (Grant No. Y1039)

Email addresses: kunpengwang@263.net (Kunpeng Wang), lb@is.ac.cn (Bao Li).

pairing provide a such tool. Let E be an elliptic curve, $P \in E$ is a point with order ℓ, $Q \in E/\ell E$. The Tate pairing $e_\ell(P,Q)$ has a practical definition which involves finding function f_ℓ with prescribed zeros and poles on the curve, and evaluating the function at Q.

In [11], Miller gave an algorithm for computing the functions of the definition of the Weil pairing, the function is just the function that define the Tate pairing. Since then, many improvement on Miller's algorithm have been given, see e.g.[4,7,6,5].

In [3], the authors provided a generic method for improve the Miller's algorithm. The realization and improvement of this method in $p = 2, 3$ can be found in [4,9,10]. In this paper, we will provide a realization of this method for some supersingular elliptic curves in the case $p = 5, 7$.

In [1], the authors provided a bilinear map between an elliptic E and a quadratic curve E_P, thus the function of the elliptic curve is just a function of a real quartic function field. When p is a small positive integer, say $p = 3, 4, 5, \cdots$, we can compute the function f_{pP} with $\mathrm{div}(f_{pP}) = p(P)-(pP)-(p-1)(\mathcal{O})$ by the means of the continued fraction in the above quadratic function fields within $p-1$-steps. The advantage of this method is that we need not to compute $2P, 3P, \cdots, (p-1)P$. When p is small, the continued fraction method is efficient.

For the supersingular elliptic curves, the point multiplication pP may be computed by apply the Frobenius Endomorphism, which takes minor time when we adopt a normal basis of the finite field. This means our method takes $O(log\#E)$ in time complexity ($\#E$ is the size of the Mordell group).

The paper is organized as follows. In section 2, we define the Tate pairing over elliptic curves, in section 3, we introduce the continued fraction expansions of quadratic functions, in section 4 we introduce a quartic model of the elliptic curves, in section 5, we compute the Tate pairing on supersingular elliptic curves of character 5 and 7. Section 6 is the conclusion.

2 The Tate Pairing and the Miller's Algorithm

Let K be a field, an elliptic curve $E(K)$ over K is the set of solutions (x, y) over K to an equation of the Weierstrass form $E : y^2+a_1xy+a_3 = x^3+a_2x^2+a_4x + a_6$, where $a_i \in K$, together with an additional point at infinity, denoted $\mathcal{O}$. In our case, we always take $K = \mathbb{F}_q$, the finite field with q elements.

There exits an abelian group law on E by the tangent-chord law, see [12] for the detailed definition and the coordinate formula of the group law.

The divisor group $\mathrm{Div}(E)$ of E is a free abelian group with basis $\{(P)|P \in E(\tilde{\mathbb{F}_q})\}$, where $\tilde{\mathbb{F}_q}$ is the algebraic closure of $\mathbb{F}_q$. Thus the elements of $\mathrm{Div}(E)$ is of form $\mathcal{A} = \sum_P a_P(P)$. Any element $\mathcal{A}$ of $\mathrm{Div}(E)$ is called a divisor of E. The degree of a divisor $\mathcal{A} = \sum_P a_P(P)$ is the sum $\deg \mathcal{A} = \sum_P a_P$.

Let $f : E(\tilde{\mathbb{F}_q}) \to \tilde{\mathbb{F}_q}$ be a function on the curve and let $\mathcal{A} = \sum_P a_P(P)$ be a divisor of degree 0. We define $f(\mathcal{A}) = \prod_P f(P)^{a_P}$. Note that, since $\sum_P a_P = 0$, $f(\mathcal{A}) = (cf)(\mathcal{A})$ for any factor $c \in \tilde{\mathbb{F}_q}$. The divisor of a function f is $\mathrm{div}(f) = \sum_P \mathrm{ord}_P(F)(P)$ where $\mathrm{ord}_P(f)$ is the order of the zero or pole of f at P. A divisor $\mathcal{A}$ is called a principal divisor if $\mathcal{A} = \mathrm{div}(f)$ for some function f. It is known that a divisor $\mathcal{A} = \sum_P a_P(P)$ is principal if and only if the degree $\mathcal{A}$ is zero and $\sum_P a_P P = \mathcal{O}$ (see [12]).

Two divisors $\mathcal{A}$ and $\mathcal{B}$ are equivalent, and we write $\mathcal{A} \sim \mathcal{B}$, if their difference $\mathcal{A} - \mathcal{B}$ is a principal divisor. Let $P \in E[\ell] = \{Q \in E(\tilde{\mathbb{F}_q})|\ell Q = \mathcal{O}\}$, where ℓ is coprime to q, and let $\mathcal{A}_P$ be a divisor equivalent to $(P) - (O)$; under these circumstances the divisor $\ell\mathcal{A}_P$ is principal, and hence there is a function f_P such that $\mathrm{div}(f_\ell) = \ell\mathcal{A}_P = \ell(P) - \ell(O)$.

The Tate pairing of order ℓ is the map $e_\ell : E(\mathbb{F}_q)[\ell] \times E(\mathbb{F}_{q^k})/\ell E(\mathbb{F}_{q^k}) \to \mathbb{F}_{q^k}$ defined as

$$e_\ell(P, Q) = f_\ell(A_Q)^{(q^k-1)/\ell}.$$

It satisfies the following properties:

(1) (Bilinearity) $e_\ell(P1+P2, Q) = e_\ell(P1, Q) \cdot e_\ell(P2, Q)$ and $e_\ell(P, Q1+Q2) = e_\ell(P, Q1) \cdot e(P, Q2)$ for all $P, P1, P2 \in E(\mathbb{F}_q)[\ell]$ and all $Q, Q1, Q2 \in E(\mathbb{F}_{q^k})/\ell E(\mathbb{F}_{q^k})$.

(2) (Non-degeneracy) If $e(P, Q) = 1$ for all $Q \in E(\mathbb{F}_{q^k})/\ell E(\mathbb{F}_{q^k})$, then $P = \mathcal{O}$. Alternatively, for each $P \neq \mathcal{O}$ there exists $Q \in E(\mathbb{F}_{q^k})/\ell E(\mathbb{F}_{q^k})$ such that $e(P, Q) \neq 1$.

(3) (Compatibility) Let $\ell = h\ell'$. If $P \in E(\mathbb{F}_q)[\ell]$ and $Q \in E(\mathbb{F}_{q^k})/\ell' E(\mathbb{F}_{q^k})$, then $e_{\ell'}(hP, Q) = e_\ell(P, Q)^h$.

Notice that, because $P \in E(\mathbb{F}_q)$, f_ℓ is a rational function with coefficients in $\mathbb{F}_q$.

Let $P \in E(\mathbb{F}_q)[l]$ and $Q \in E(\mathbb{F}_{q^k})/\ell E(\mathbb{F}_{q^k})$ be linearly independent points. The following theorem shows that in order to compute the Tate pairing, we need only to compute the function f_ℓ.

Theorem 1 ([4]) *Let r be a factor of ℓ. As long as $k > 1$, $e_r(P,Q) = f_P(Q)^{(q^k-1)/r}$ for $Q \neq \mathcal{O}$.*

In the next, for each pair of points $U, V \in E(\mathbb{F}_q)$ we define $g_{U,V} : E(\mathbb{F}_{q^k}) \to \mathbb{F}_{q^k}$ to be (the equation of) the line passes both points U and V (if $U = V$, then $g_{U,V}$ is the tangent to the curve at U, and if either one of U, V is the point at infinity $\mathcal{O}$, then $g_{U,V}$ is the vertical line at the other point). The shorthand g_U stands for $g_{U,-U}$: if $U = (u, v)$ and $Q = (x, y)$, then $g_U(Q) = x - u$.

Theorem 2 (Miller's formula,in [4])*Let P be a point on $E(\mathbb{F}_q)$ and f_c be a function with divisor $\mathrm{div}(f_c) = c(P) - (cP) - (c-1)(\mathcal{O}), \quad c \in \mathbb{Z}$. For all $a, b \in \mathbb{Z}$, $f_{a+b}(Q) = f_a(Q)f_b(Q)g_{aP,bP}/g_{(a+b)P}(Q)$.*

Let the binary representation of $\ell \geq 0$ be $\ell = (\ell_t, \cdots, \ell_1, \ell_0)$ where $\ell_i \in \{0, 1\}$ and $\ell_t \neq 0$. Millers algorithm computes $f_P(Q) = f_\ell(Q), Q \neq \mathcal{O}$ by coupling the above formulas with the double-and-add method to calculate ℓP :

Algorithm 1 (Miller's algorithm)

set $f \leftarrow 1$ *and* $V \leftarrow P$;

for $i \leftarrow t-1, t-2, \cdots, 1, 0$ *do* {

  set $f \leftarrow f^2 \cdot g_{V,V}(Q)/g_{2V}(Q)$ *and* $V \leftarrow 2V$;

  if $\ell_i = 1$ *then set* $f \leftarrow f^2 \cdot g_{V,P}(Q)/g_{V+P}(Q)$ *and* $V \leftarrow V + P$;

}

return f;

3 Real Quadratic Function Fields

In this section, we present the basic facts of real quadratic functions. Basic references for this subject are [2,16,14,13]. Let $K/\mathbb{F}_q$ be a real quadratic function field with the finite field $\mathbb{F}_q$ of constants of odd characteristic to be their constant field. Then for some indeterminate w of $\mathbb{F}_q$, the quadratic function field is of the form $K = \mathbb{F}_q(w)(\sqrt{D(w)})$, where $D(w)$ is a squarefree polynomial of even degree whose leading coefficient is a square in $\mathbb{F}_q^\times = \mathbb{F}_q - \{0\}$.

Let $\alpha \in K$ be an element of the form $\alpha = (p + \sqrt{D(w)})/q$, where $0 \neq q, p \in \mathbb{F}_q[w]$ and $q|(D - p^2)$. Put $q_0 = Q$, $p_0 = P$, $a_0 = d = \lfloor \sqrt{D(w)} \rfloor$, $q_{-1} = (D - p^2)/q$, $r_0 = 0$. The continued fraction expansion of α can be computed as follows:

$$\begin{cases} p_i = a_{i-1}q_{i-1} - p_{i-1} = d - r_{i-1} \\ q_i = (D - p_i^2)/q_{i-1} = q_{i-2} + a_{i-1}(r_{i-1} - r_{i-2}) \\ a_i = (p_i + d) \text{ div } q_i \\ r_i = (p_i + d) \mod q_i. \end{cases} \tag{1}$$

The continued fraction is $\alpha = [a_0, a_1, \cdots]$, and the partial quotient is $\alpha_0 = \sqrt{D(w)}, \alpha_1, \cdots$ where $\alpha_i = (p_i + \sqrt{D(w)})/q_i$ for $i = 1, 2, \cdots$.

4 The Quartic Model of an Elliptic Curve

The main subjects of this section are quoted from references[1,13] with some modifications of symbols.

In the case $\mathbb{F}_q$ be a field of odd characteristic, the definition equation of an elliptic curve E can always be written as

$$E : y^2 = x^3 + Ax + B,$$

where $A, B \in \mathbb{F}_q$ and $\Delta = -4A^3 - 27B^2 \neq 0$. Let $K = \mathbb{F}_q(E) = K(x, y)$ be the corresponding function field for E.

Let $P = (a, b) \neq \mathcal{O}$ be a $\mathbb{F}_q$-rational point on $E \quad (a, b \in \mathbb{F}_q)$. We construct a plane quartic model for E, with respect to $\mathcal{O}$ and P are the two points at infinity. Indeed, let

$$\sigma : (x, y) \mapsto (w, z) = \left(\frac{y + b}{x - a}, 2x + a - \left(\frac{y + b}{x - a} \right)^2 \right). \tag{2}$$

Then we have

$$z^2 = w^4 - 6aw^2 - 8bw + c, \tag{3}$$

where $c = -4A - 3a^2$ and $B = b^2 - a^3 - Aa$.

Denote the curve defined by (3) as E_P. Thus E_P is a plane quartic model for E. The map defined by (2) provides a birational map between E and E_P, the inverse map is

$$\sigma^{-1} : (w, z) \mapsto (x, y) = \left(\frac{1}{2}(w^2 + z - a), \frac{1}{2}(w^3 + wz - 3aw - 2b) \right). \tag{4}$$

In fact let $D_P(w) = w^4 - 6aw^2 - 8bw + c$, then $K = \mathbb{F}_q(w)(\sqrt{D_P(w)})$ is a real quadratic congruence function field of genus 1 with respect to $\mathfrak{O} = \mathbb{F}_q[w][\sqrt{D_P(w)}]$.

If $Q \neq \mathcal{O}, P$ is a point on E, then we also denote the equivalent point on E_P by Q. To distinguish between the two curves, we write for the coordinates $Q = (x_Q, y_Q), Q = (w_Q, z_Q)$ if Q lies on E or E_P respectively. We also let w_Q be the value $w(Q)$ under the transformation (2) and x_Q be the value $v(Q)$ under the transformation (4). The conjugation in $K = \mathbb{F}_q(w)(z)$ yields a biregular $\mathbb{F}_q$-morphism of $E_P(k)$, given by $Q = (w_Q, z_Q) \mapsto Q^* = (w_Q, -z_Q)$ for $Q \neq \mathcal{O}, P$, and $\mathcal{O}^* = P$, $P^* = \mathcal{O}$.

Lemma 3 *([1,13]) Symbols are just as above, we have $Q + Q^* = P$.*

We now require the additional condition that the order of $P = (a, b)$ is different from 2, i.e. $b \neq 0$. Furthermore, we assume Q to be a $\mathbb{F}_q$-rational point on E that $Q \neq P$. As in [1], we define

Definition 4 *([1,13]) Let $Q \in E(\mathbb{F}_q)$ be such that $Q \neq P$. We set*

$$f_Q = \begin{cases} \dfrac{x - x(Q^*)}{w - w(Q)}, & \textit{if} \quad Q \neq \mathcal{O}; \\ x - x(Q^*), & \textit{if} \quad Q = \mathcal{O}. \end{cases}$$

Lemma 5 *([1,13]) Let Q be as above, we have*

$$(f_Q) = (P) + (-Q^*) - (\mathcal{O}) - (Q).$$

We develop the continued fraction expansion of $\sqrt{D_P(w)}$, and obtain a sequence of partial quotients $\alpha_0 = \sqrt{D_P(w)}, \alpha_1, \alpha_2, \cdots$.

Lemma 6 *([1,13]) In the continued fraction expansions of $\alpha_0 = \sqrt{D_P(w)}$, we have that*

$$f_{iP} = c_i \alpha_{i-1}$$

for $i \geq 2$.

The above lemmas are quoted from [1,13]. Let $P = (a, b) \in E$ be a point of order ℓ with $(\ell, q) = 1$. In order to get the function f_{pP} such that

$$\mathrm{div}(f_{pP}) = p(P) - (pP) - (p-1)(O),$$

we need only to compute the first $p-1$-steps of the continued fraction expansion of $\sqrt{D_P(w)}$:

Theorem 7 *Let* $\alpha_0 = \sqrt{D_P(w)}$*,* $\alpha_1, \alpha_2, \cdots$ *be the partial quotient sequence obtained by the continued fraction of* $\sqrt{D_P(w)}$*, then*

$$\mathrm{div}(\alpha_1\alpha_2\cdots\alpha_{p-1}) = p(P) - (pP) - (p-1)(O).$$

Proof. By Lemmas 3,5 and 6, we have

$$\begin{aligned}\mathrm{div}(\alpha_1) &= (P) + (P) - (\mathcal{O}) - (2P)\\ \mathrm{div}(\alpha_2) &= (P) + (2P) - (\mathcal{O}) - (3P)\\ &\vdots\\ \mathrm{div}(\alpha_{p-1}) &= (P) + ((p-1)P) - (\mathcal{O}) - (pP).\end{aligned} \tag{5}$$

Add them all and we have $\mathrm{div}(\alpha_1\alpha_2\cdots\alpha_{p-1}) = p(P) - (pP) - (p-1)(O)$.

Thuse let $f_{pP} = \alpha_1\alpha_2\cdots\alpha_{p-1}$, then we have the desired function.

5 The Supersingular Curves

5.1 The Supersingular curves over characteristic 5

Let n be an integer, consider the supersingular elliptic curves $E_1/\mathbb{F}_{5^n} : y^2 = x^3+1$. The number $\#E_1(\mathbb{F}_{5^n})$ of the rational points of the elliptic curve $E_1(\mathbb{F}_{5^n})$ is computed as follows (we refer the readers to [15] for details).

Let $\#E_1(\mathbb{F}_5) = 5+1-a$, write $X^2 - aX + 5 = (X-\alpha)(X-\beta)$. Then for all $n \geq 1$, we have

$$\#E_1(\mathbb{F}_{5^n}) = 5^n + 1 - (\alpha^n + \beta^n). \tag{6}$$

By direct calculation we have

$$E_1(\mathbb{F}_5) = \{(0,1),(0,4),(2,2),(2,3),(4,0),\mathcal{O}\}.$$

Thus $\#E_1(\mathbb{F}_5) = 6 = 5+1-0$, so $a = 0$ and $X^2+5 = (X-\sqrt{-5})(X+\sqrt{-5})$. This means $\alpha = \sqrt{-5}$, $\beta = -\sqrt{-5}$. By (6) we have

$$\#E_1(\mathbb{F}_{5^n}) = \begin{cases} 5^n+1, & \text{if } \ 2 \not| n;\\ 5^n \pm 2\cdot 5^{\frac{n}{2}} + 1, & \text{if } \ 2|n.\end{cases} \tag{7}$$

Here we only consider the $2 \not| n$ case.

Let τ be the Frobenus endomorphism:

$$\tau : (x, y) \mapsto (x^5, y^5), \quad (x, y) \in E, \tag{8}$$

then it satisfies $(\tau^2+5)(x, y) = \mathcal{O}$, see [15] for details. By the finite field theory, the time of computing the map τ takes negligible time provided that we are working in a normal basis of $\mathbb{F}_{5^n}$ over $\mathbb{F}_5$. This tells us that we can efficiently compute the point $5P$ for a point $P = (x, y) \in E(\mathbb{F}_{5^n})$ by

$$5(x, y) = -\tau^2(x, y) = -(x^{5^2}, y^{5^2}) = (x^{5^2}, -y^{5^2}). \tag{9}$$

In order to compute the function f_ℓ over the E, we need compute the function f_P where

$$\mathrm{div}(f) = n(P) - n(\mathcal{O}).$$

Let f_P be a rational function satisfying

$$\mathrm{div}(f_P) = 5(P) - (5P) - 4(\mathcal{O}).$$

Then this function can be efficiently computed by the method provided in Theorem 7. The point multiplication $5P$ can be efficiently computed by (9).

$$\begin{aligned}
\mathrm{div}(f_P) &= 5(P) - (5P) - 4(\mathcal{O}), \\
\mathrm{div}(f_{5P}) &= 5(5P) - (5^2P) - 4(\mathcal{O}), \\
&\cdots \\
\mathrm{div}(f_{5^{n-1}P}) &= 5(5^{n-1}P) - (5^nP) - 4(\mathcal{O}).
\end{aligned}$$

Thus

$$\mathrm{div}(f_P^{5^{n-1}} f_{5P}^{5^{n-2}} f_{5^2P}^{5^{n-3}} \cdots f_{5^{n-1}P}) = 5^n(P) - (5^nP) - (5^n - 1)(O).$$

By the fact that $\#E(\mathbb{F}_{5^n}) = 5^n + 1$, let

$$f_{5^n+1} = f_P^{5^{n-1}} f_{5P}^{5^{n-2}} f_{5^2P}^{5^{n-3}} \cdots f_{5^{n-1}P} \cdot g_{5^nP,P} \cdot g_{(5^n+1)P}^{-1},$$

then we have

$$\mathrm{div}(f_{5^n+1}) = (5^n + 1)((P) - (O)) = \frac{5^n + 1}{\ell}(\ell(P) - \ell(\mathcal{O})) = \frac{5^n + 1}{\ell}\mathrm{div}(f_\ell),$$

where f_ℓ is a rational function satisfying $\mathrm{div}(f_\ell) = \ell(P) - \ell(\mathcal{O})$. Thus we have the Tate pairing

$$e_\ell(P, Q) = f_\ell(Q)^{\frac{5^{2n}-1}{\ell}} = f_\ell(Q)^{\frac{5^n+1}{\ell}(5^n-1)} = f_{5^n+1}(Q)^{5^n-1}.$$

Suppose that $P=(x,y), Q=(c,d)$, then the algorithm is listed as follows(here x_P, y_P means the x-coordinate and the y-coordinate of P, σP means the image of P under the map (2) and $z_{\sigma P}, w_{\sigma P}$ means the z-coordinate and the w-coordinate of σP):

Algorithm 2 (Algorithm for characteristic 5)

input $E : y^2 = x^3+1$; $P=(x,y), Q=(c,d) \in E$; n;

set $\tilde{Q} = (w_{\tilde{Q}}, z_{\tilde{Q}}) \leftarrow \sigma Q$; $V \leftarrow P$; $f \leftarrow 1$;

for $i \leftarrow n-1, \cdots, 1, 0$; *do*{

  set $f \leftarrow f^5$; $D_V \leftarrow w^4 - 6x_V w^2 - 8y_V w - 3x_V^2$;

  set $\alpha = z$;

  set $q \leftarrow 1; q_m \leftarrow 0; q_{-1} \leftarrow D_V; P \leftarrow 0; r_{-1} \leftarrow d \leftarrow a \leftarrow \lfloor \sqrt{D_V} \rfloor; r \leftarrow 0;$

  for $j \leftarrow 1,2,3,4$ *do*{

    $p \leftarrow d - r$;

    $q_m \leftarrow q_{-1} + a(r + r_{-1});$ $q_{-1} \leftarrow q$; $q \leftarrow q_m$;

    $a \leftarrow (p+d) \operatorname{div} q$;

    $r_{-1} \leftarrow r;$ $r \leftarrow (p+d) \mod q$;

    $\alpha \leftarrow (p+z)/q$;

    $f \leftarrow f \cdot \alpha(\tilde{Q})$;

  }

  $V \leftarrow -\tau^2 V$;

}

set $f \leftarrow f \cdot g_{V,P}(Q)$;

set $V \leftarrow V + P$;

set $f \leftarrow f / g_V(Q)$;

set $f \leftarrow f^{5^n-1}$;

return f;

5.2 The Supersingular curves over characteristic 7

Let n be an integer, consider the supersingular elliptic curves $E_1/\mathbb{F}_{7^n} : y^2 = x^3+1$. The number $\#E_1(\mathbb{F}_{7^n})$ of the rational points of the elliptic curve $E_1(\mathbb{F}_{7^n})$

is computed as follows (we refer the readers to [15] for details).

Let $\#E_1(\mathbb{F}_7) = 7 + 1 - a$, write $X^2 - aX + 7 = (X - \alpha)(X - \beta)$. Then for all $n \geq 1$, we have

$$\#E_1(\mathbb{F}_{7^n}) = 7^n + 1 - (\alpha^n + \beta^n). \tag{10}$$

By direct calculation we have

$$E_1(\mathbb{F}_7) = \{(0,0), (1,3), (1,4), (3,3), (3,4), (5,2), (5,5), \mathcal{O}\}.$$

Thus $\#E_1(\mathbb{F}_7) = 8 = 7+1-0$, so $a = 0$ and $X^2+7 = (X - \sqrt{-7})(X + \sqrt{-7})$. This means $\alpha = \sqrt{-7},\ \beta = -\sqrt{-7}$. By (10) we have

$$\#E_1(\mathbb{F}_{7^n}) = \begin{cases} 7^n + 1, & \text{if} \quad 2 \not| n; \\ 7^n \pm 2 \cdot 7^{\frac{n}{2}} + 1, & \text{if} \quad 2 | n. \end{cases} \tag{11}$$

Just as the $p = 5$ case, we only consider the case $2 \not| n$.

Let τ be the Frobenius endomorphism:

$$\tau : (x, y) \mapsto (x^7, y^7), \quad (x, y) \in E, \tag{12}$$

then it satisfies $(\tau^2+7)(x, y) = \mathcal{O}$, see [15] for details. By the finite field theory, the time of computing the map τ takes negligible time provided that we are working in a normal basis of $\mathbb{F}_{7^n}$ over $\mathbb{F}_7$. This tells us that we can efficiently compute the point $7P$ for a point $P = (x, y) \in E(\mathbb{F}_{7^n})$ by

$$7(x, y) = -\tau^2(x, y) = -(x^{7^2}, y^{7^2}) = (x^{7^2}, -y^{7^2}). \tag{13}$$

In order to compute the function f_ℓ over the E, we need compute the function f_P where

$$\mathrm{div}(f) = n(P) - n(\mathcal{O}).$$

Let f_P be a rational function satisfying

$$\mathrm{div}(f_P) = 7(P) - (7P) - 6(\mathcal{O}).$$

Then this function can be efficiently computed by the method provided in Theorem 7. The point $7P$ can be efficiently computed by (13).

For the case $2 \not| n$, we have

$$\begin{aligned} \mathrm{div}(f_P) &= 7(P) - (7P) - 6(\mathcal{O}), \\ \mathrm{div}(f_{7P}) &= 7(7P) - (7^2P) - 6(\mathcal{O}), \\ &\cdots \\ \mathrm{div}(f_{7^{n-1}P}) &= 7(7^{n-1}P) - (7^nP) - 6(\mathcal{O}). \end{aligned}$$

Thus

$$\mathrm{div}(f_P^{7^{n-1}} f_{7P}^{7^{n-2}} f_{7^2P}^{7^{n-3}} \cdots f_{7^{n-1}P}) = 7^n(P) - (7^nP) - (7^n - 1)(O).$$

By the fact that $\#E(\mathbb{F}_{7^n}) = 7^n + 1$, let

$$f_{7^n+1} = f_P^{7^{n-1}} f_{7P}^{7^{n-2}} f_{7^2P}^{7^{n-3}} \cdots f_{7^{n-1}P} \cdot g_{7^nP,P} \cdot g_{(7^n+1)P}^{-1},$$

then we have

$$\mathrm{div}(f_{7^n+1}) = (7^n+1)((P) - (O)) = \frac{7^n+1}{\ell}(\ell(P) - \ell(\mathcal{O})) = \frac{7^n+1}{\ell}\mathrm{div}(f_\ell),$$

where f_ℓ is a rational function satisfying $\mathrm{div}(f_\ell) = \ell(P) - \ell(\mathcal{O})$. Thus we have the Tate pairing

$$e_\ell(P,Q) = f_\ell(Q)^{\frac{7^{2n}-1}{\ell}} = f_\ell(Q)^{\frac{7^n+1}{\ell}(7^n-1)} = f_{7^n+1}(Q)^{7^n-1}.$$

Suppose that $P = (x,y), Q = (c,d)$, then the algorithm is listed as follows(here x_P, y_P means the x-coordinate and the y-coordinate of P, σP means the image of P under the map (2) and $z_{\sigma P}, w_{\sigma P}$ means the z-coordinate and the w-coordinate of σP):

Algorithm 3 (Algorithm for characteristic 7)

input $E : y^2 = x^3 + 1$; $P = (x,y), Q = (c,d) \in E$; n;

set $\tilde{Q} = (w_{\tilde{Q}}, z_{\tilde{Q}}) \leftarrow \sigma Q$; $V \leftarrow P$; $f \leftarrow 1$;

for $i \leftarrow n-1, \cdots, 1, 0$; *do*{

  set $f \leftarrow f^7$; $D_V \leftarrow w^4 - 6x_V w^2 - 8y_V w - 4 - 3x_V^2$;

  set $\alpha = z$;

  set $q \leftarrow 1; q_m \leftarrow 0; q_{-1} \leftarrow D_V; P \leftarrow 0; r_{-1} \leftarrow d \leftarrow a \leftarrow \lfloor\sqrt{D_V}\rfloor; r \leftarrow 0;$

  for $j \leftarrow 1, \cdots, 6$ *do*{

    $p \leftarrow d - r$;

$q_m \leftarrow q_{-1} + a(r + r_{-1});\quad q_{-1} \leftarrow q;\quad q \leftarrow q_m;$

$a \leftarrow (p + d)$ div $q;$

$r_{-1} \leftarrow r;\quad r \leftarrow (p + d) \mod q;$

$\alpha \leftarrow (p + z)/q;$

$f \leftarrow f \cdot \alpha(\tilde{Q});$

}

$V \leftarrow -\tau^2 V;$

}

set $f \leftarrow f \cdot g_{V,P}(Q);$

set $V \leftarrow V + P;$

set $f \leftarrow f/g_V(Q);$

set $f \leftarrow f^{7^n-1};$

return $f;$

The time complexity of the above two algorithms are $O(n)$. The majority part of the complexity is come from the computation of f_{5P}(resp.f_{7P} for characteristic 7). We conjecture that there is a more efficient algorithm for compute this function then that given in this paper.

6 Conclusion

This method also applicable for elliptic curves $Y^2 = X^3+1$ over characteristics 11, 17, $\cdots$, and for $Y^2 = X^3 + X$ over characteristics 19, 23, $\cdots$.

References

[1] W.W.Adams, M.J.Razar, Multiples of points on elliptic curves and continued fractions, Prac. London Math. Soc. **41**(1980)481–498

[2] E.Artin, Quadratische Körper im Gebiete der höheren Kongruenzen I, II. Math. Zeitschr. **19**(1924)153–206

[3] P.S.L.M.Barreto, S. Galbraith, C.O.hEigeartaigh, M.Scott, Efficient pairing computation on supersingular Abelian varieties, http://eprint. iacr. org/ 2004/ 375

[4] P.S.L.M.Barreto, H.Y. Kim, B.Lynn, M.Scott, Efficient algorithms for pairing-based cryptosystems, Proceedings of the 22nd Annual International Cryptology Conference on Advances in Cryptology,LNCS 2442, 354 - 368

[5] I.F.Blake, V.Kumar Murty, G.Xu, Refinements of Miller's algorithm for computing Weil/Tate Pairing,Cryptology ePrint Archive: Report 2004/065

[6] K.Eisenträger, K. Lauter and P. L. Montgomery, Fast Elliptic curve arithmetic and improved Weil pairing Evaluation, Topics in Cryptology, CT-RSA03, LNCS **2612**, Springer-Verlag Heidelberg, 2003, pp. 343–354.

[7] S.Galbraith, K. Harrison and D. Soldera, Implementing the Tate Pairing, Algorithm Number Theory Symposium, ANTS-V (C. Fieker and D. Kohel EDS.), LNCS **2369**, Springer-Verlag Heidelberg, 2002,pp. 324–337.

[8] A.Joux, The Weil and Tate pairings as building blocks for public key cryptosystems(survy), Algorithmic Number Theory, ANTS-V (C. Fieker and D. Kohel EDS.),LNCS **2369**, Springer-Verlag Heidelberg,2002,20-32

[9] T.Kerins, P. Marnane, E.M. Popovici, P.S.L.M. Barreto, Efficitnt hardware for Tate pairing calculation in character three, http://eprint.iacr.org/2005/065.pdf

[10] S.Kwon, Efficient Tate pairing computation for supersingular elliptic curves over binary fields, http://eprint.iacr.org/2004/303.pdf

[11] V.Miller, Short programs for functions on curves, Unpublished Manuscript,1986

[12] J.H.Silverman, The arithmetic of elliptic curves, Springer-Verlag,1986

[13] A.Stein, Equivalences between elliptic curves and real quadratic congruence function fields, J. Théor. Nombres Bordeaux **9** (1997) 75–95

[14] K.Wang,The arithmetic structure of quadratic function fields, PhD desertation, Beijng,2000

[15] L.C.Washington, Elliptic curves Number Theory and Cryptography,Chapman & Hall/CRC,2003

[16] E.Weiss, Algebraic Number Theory, McGraw-Hill, New York 1963