Tate pairing computation on the divisors of hyperelliptic curves for cryptosystems

Eunjeong Lee and Yoonjin Lee

Korea Institute for Advanced Study (KIAS), 207-43 Cheongnyangni 2-dong,
Dongdaemun-gu, Seoul 130-722, Korea, E-mail: ejlee@kias.re.kr,
Dept. of Mathematics, Simon Fraser University, Burnaby, British Columbia
CANADA V5A 1S6, E-mail: yoonjinl@sfu.ca

August 20, 2005

Abstract. In recent papers [4] and [9], Barreto et al and Choie et al worked on hyperelliptic curves H_b defined by $y^2 + y = x^5 + x^3 + b$ over a finite field $\mathbb{F}_{2^n}$ with $b = 0$ or 1 for a secure and efficient pairing-based cryptosystems. We find a completely general method for computing the Tate-pairing over divisor class groups of the curves H_b in a very explicit way. In fact, the Tate-pairing is defined over the entire divisor class group of a curve, not only over the points on a curve. So far only pointwise approach has been made in [4] and [9] for the Tate-pairing computation on the hyperelliptic curves H_b over $\mathbb{F}_{2^n}$. Furthermore, we obtain a very efficient algorithm for the Tate pairing computation over divisors by reducing the cost of computing. We also find a crucial condition for divisor class group of hyperelliptic curve to have a significant reduction of the loop cost in the Tate pairing computation.

Keywords- Tate pairing computation, hyperelliptic curve cryptosystems, pairing-based cryptosystems

1 Introduction

Pairing-based cryptosystems have been one of the most active research areas in cryptology due to discovery of an identity-based encryption scheme [5] and its significance as a cryptanalytic tool([12], [16]). Recently, the Tate pairing and the Weil pairing have been used to construct various cryptosystems([5], [6], [8], [21]). It is therefore significantly important to develop efficient methods of the paring computation for the purpose of practical applications of the pairings to the cryptosystems([1], [2], [3], [10], [13], [14], [18], [19]).

In recent papers [4] and [9], Barreto et al and Choie et al worked on hyperelliptic curves H_b defined by $y^2+y = x^5+x^3+b$ over a finite field $\mathbb{F}_{2^n}$ with $b = 0$ or 1 for a secure and efficient pairing-based cryptosystems.

Most of pairing-based cryptosystems use a divisor D as a system papermeter, which is a generator of additive cyclic group with prime order ℓ. Generally, inputs for pairing computation are usually aD for arbitrary integer $a \in \{0, ..., \ell\}$. Even though the generator D is constructed to be special such as $D = (P) - (O), P \in H(\mathbb{F}_{p^n})$ which was dealt with in [4], aD does not need to have such a good property. In fact, the Tate pairing computation is defined over the entire divisor class group of a curve and the divisors do not have to be written as the sum of points contained in the defining field $\mathbb{F}_{2^n}$. Since the algorithm proposed in [4] works for only points belonging to $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$, we need an efficient algorithm applicable to general divisors.

In this paper we find a completely general method for computing Tate pairings over divisor class groups of the curves H_b in a very explicit way. So far only pointwise approach has been made in [4], [9] for the Tate pairing computation on the hyperellitic curves H_b over $\mathbb{F}_{2^n}$. The paper [4] works for only points belonging to $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$. The algorithm in [9] is for general divisors, but the loop cost is twice than that of [4]. Hence, when divisors are not a sum of rational points, there has been no general method for efficient Tate pairing computation. We thus present a very general method and algorithms for computing the Tate pairings over divisors by extending the idea of [4].

Furthermore, we obtain very efficient algorithm for the Tate pairing computation over divisors by reducing the cost of computing. The reduction of the loop cost was made by using the divisor version of the *Eta pairing*; the Eta pairing was introduced in [4]. In recent years Duursma and Lee [11] introduced a closed formula of the Tate paring for a very special family of hyperelliptic curves for the Tate pairing computation; this significantly reduced the total number of iterations for the Tate pairing computation over such curves. Barreto and others [4] clarified why such curves are very special enough to make a reduction of the loop cost for the final computation of the Tate pairing. They provided us with a sufficient condition for a hyperelliptic curve to have a significant reduction of the loop cost in the Tate pairing computation; however, the condition that they found was not completely correct as we can see in Remark 1. We hence find a correct condition, and this condition is quite general in a sense that it works not only for points, but also for divisors of a curve which can cover any inputs for pairings appearing in pairing-based cryptosystems.

We begin with brief background information in Section 2, and Section 3 gives octupling formulas for divisors and reduction formulas for evaluating the Tate pairing on the divisors over H_b. Section 4 discusses the endomorphism for pairing computation and *Eta pairing* for reducing the cost of computation. In Section 5 we obtain main results and algorithms for the Tate pairing computation on the divisors of H_b. We finish our paper with some remarks in Section 6.

2 Preliminaries

In this section, we recall the basic definitions and properties (see [15] for further details). Let $\mathbb{F}_q$ be a finite field with q elements and $\bar{\mathbb{F}}_q$ be the algebraic closure of $\mathbb{F}_q$. Hyperelliptic curves defined over $\mathbb{F}_q$ are algebraic curves with genus g which are described by the following equation;

$$H/\mathbb{F}_q : y^2 + h(x)y = F(x), \tag{1}$$

where $F(x)$ in $\mathbb{F}_q[x]$ is a monic polynomial with $\deg(F) = 2g+1$, $h(x) \in \mathbb{F}_q[x]$, $\deg(h) \le g$ and there are no singular points on H.

Now let

$$H = \{(a,b) \in \bar{\mathbb{F}}_q \times \bar{\mathbb{F}}_q \mid b^2 + h(a)b = F(a)\} \cup \{\mathcal{O}\},$$

and let $H(\mathbb{F}_q) = H \cap (\mathbb{F}_q \times \mathbb{F}_q)$ be a set of rational points on H with the infinite point $\mathcal{O}$. We denote the group of degree zero divisor classes of H by J_H, and it is simply called the *Jacobian* of H. Note that each divisor class can be uniquely represented by the *reduced divisor* using the *Mumford representation* [17]. Reduced divisors of the curve H can be found as follows.

Theorem 1 (Reduced divisor [15], [17]). *Let K be the function field given by H defined over $\mathbb{F}_q$. Then each nontrivial divisor class of J_H can be represented by*

$$D = \sum_{i=1}^{r} P_i - r\mathcal{O}, \text{ where } r \le g,\ P_i \ne \mathcal{O},\ P_i \in H.$$

Let $P_i = (a_i,\ b_i)$, $1 \le i \le r$ and $u_D(x) = \prod_{i=1}^{r}(x - a_i)$. Then there exists a unique polynomial $v_D(x) \in \bar{\mathbb{F}}_q[x]$ satisfying

1) $\deg(v_D) < \deg(u_D) \le g$
2) $b_i = v_D(a_i)$
3) $u_D(x) \mid v_D(x)^2 + v_D(x)h(x) - F(x)$,

and $D = \text{g.c.d.}(\text{div}(u_D(x)),\ \text{div}(v_D(x) + y))$.

We will denote a divisor class as $D = [u_D, v_D]$, where D is a reduced divisor and u_D, v_D are polynomials in $\mathbb{F}_q[x]$ satisfying the three conditions in Theorem 1.

Now we recall the definition of the Tate pairing(see [12] for further details). Let ℓ be a positive divisor of the order of $J_H(\mathbb{F}_q)$ with $\gcd(\ell,\ q) = 1$, and k be the smallest integer such that $\ell \mid (q^k - 1)$; such k is called *the security multiplier*. Let $J_H[\ell] = \{D \in J_H \mid \ell D = \mathcal{O}\}$. The *Tate pairing* is a map

$$\begin{aligned} t : J_H[\ell] \times J_H(\mathbb{F}_{q^k})/\ell J_H(\mathbb{F}_{q^k}) &\to \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^\ell \\ t(D,E) &= f_D(E') \end{aligned} \tag{2}$$

where $\text{div}(f_D) = \ell D$ and $E' \sim E$ with *support*$(E') \cap$ *support*$(\text{div}(f_D)) = \emptyset$.

In fact, the fields of characteristic 2 are the most commonly used field in the cryptosystems. In this paper we work on the following curves:

$$H_b : y^2 + y = x^5 + x^3 + b, \quad b = 0 \text{ or } 1 \tag{3}$$

which is defined over $\mathbb{F}_{2^n}$ with n coprime to 6.

The curves H_0 and H_1 are hyperelliptic curves, and their divisor class groups have good group structures. To determine ℓ, we need to know the orders of $J_{H_0}(\mathbb{F}_q)$ and $J_{H_1}(\mathbb{F}_q)$, and they are given as follows.

Theorem 2 ([22]). *Let* $\gcd(n,6)=1$. *For the curve* H_b, *we have*

$$\#J_{H_0}(\mathbb{F}_{2^n}) = 2^{2n}+2^n+1+(-1)^{[(n+1)/4]}2^{(n+1)/2}(2^n+1), \qquad (4)$$
$$\#J_{H_1}(\mathbb{F}_{2^n}) = 2^{2n}+2^n+1-(-1)^{[(n+1)/4]}2^{(n+1)/2}(2^n+1), \qquad (5)$$

where $[\ ]$ *denotes the floor function value, and* $J_{H_b}(\mathbb{F}_{2^n})$ *is a cyclic group.*

3 Efficient computations on J_{H_b}

As pointed in [9], [4], octupling a divisor on the curve H_b is computationally very simple, of which complexity is almost the same as octupling of a point on elliptic curves.

For a divisor $D=[u_D,v_D]$ of the curve H_b with $u_D(x), v_D(x)\in\mathbb{F}_{2^n}[x]$, we can find a very explicit formula for $8[D]$ in terms of the coefficients of u_D and v_D without inversions in $\mathbb{F}_{2^n}$ from the doubling formula. This is a divisor version of the result in [9], [4] for octupling formula of the point.

Proposition 1. *Let* H_b *be a hyperelliptic curve defined by* $y^2+y=x^5+x^3+b$ *over* $\mathbb{F}_{2^n}$. *Then for a divisor* $D=[u_D,\ v_D]=[x^2+u_{D,1}x+u_{D,0},\ v_{D,1}x+v_{D,0}]$ *in* J_{H_b} *and for some* $U_D(x)\in\mathbb{F}_{2^n}[x]$,

$$\begin{aligned}
8[D] = \operatorname{div}\left(\frac{G_D(x,\ y)}{U_D(x)}\right) &+ [U_8(x),\ V_8(x)],\ \textit{where}\\
G_D(x,\ y) &= G_{D,4}(x,\ y)^2\cdot G_{D,8}(x,\ y)\\
U_8(x) &= x^2+{u_{D,1}}^{64}x+(1+u_{D,1}+u_{D,0})^{64}\\
V_8(x) &= (v_{D,1}+u_{D,1})^{64}x+(v_{D,1}+u_{D,1}+v_{D,0}+u_{D,0}+1)^{64}
\end{aligned}$$

and $G_{D,4}, G_{D,8}$ *are described in Table 1. In the table,* nM *indicates that it requires* n *multiplications in* $\mathbb{F}_{2^n}$.

In the following Proposition 2 for any divisor $E=[u_E,v_E]$ we obtain the reduction formulae for $G_{D,4}, G_{D,8}$ at each point (x_j,y_j) of a divisor E. These formulae will be very useful for efficient computation of our main result. Basically we represent $G_{D,4}$ and $G_{D,8}$ as linear polynomials in x_j as follows.

Proposition 2. *Let* E *be a divisor of the curve* H_b *be defined by*

$$E = Q_1+Q_2-2\mathcal{O} = [u_E, v_E],$$

such that $u_E=x^2+u_{E,1}x+u_{E,0}$, $v_E=v_{E,1}x+v_{E,0}$, *and* $Q_j=(x_j,y_j)$ *for* $j=1,2$.

Let $G_{D,4}(Q_j)=C_{D,1}x_j+C_{D,2}$ *and* $G_{D,8}(Q_j)=C_{D,3}x_j+C_{D,4}$. *Then* $C_{D,i}$*'s (with* $i=1,2,3,4$*) are given in the following table 2 (We note that* $C_{D,i}$*'s are expressed in terms of coefficients of* u_E *and* v_E*). Therefore, we obtain*

$$G_D(E) = (C_{D,1}^2u_{E,0}+C_{D,1}C_{D,2}u_{E,1}+C_{D,2}^2)^2(C_{D,3}^2u_{E,0}+C_{D,3}C_{D,4}u_{E,1}+C_{D,4}^2).$$

Table 1. Octupling formula with divisor representation

INPUT	$D = [u_D, v_D] \in J_{H_b}(\mathbb{F}_{2^n})$
OUTPUT	$G_{D,4}(x,y) = (y + x^3 + b)^2 + (y + x^3 + b)(\delta_1 x^2 + \delta_2 x + \delta_3) + \delta_4 x^4 + \delta_5 x^3 + \delta_6 x^2 + \delta_7 x + \delta_8$ $G_{D,8}(x,y) = (y + b + 1)^2 + (y + b + 1)(\epsilon_1 x^2 + \epsilon_2 x + \epsilon_3) + \epsilon_4 x^4 + \epsilon_5 x^3 + \epsilon_6 x^2 + \epsilon_7 x + \epsilon_8$
Initiation (Cost: 4M)	$w_0 = u_{D,1} v_{D,1}, \quad w_1 = u_{D,1} u_{D,0}, \quad w_2 = u_{D,1} v_{D,0}, \ w_3 = u_{D,0} v_{D,1}$
$G_{D,4}$ (Cost: 2M)	$w_4 = w_2 + w_3$ $\delta_1 = ({u_{D,1}}^2 + u_{D,1})^4, \quad \delta_2 = {u_{D,1}}^4, \quad \delta_3 = w_0^4, \quad \delta_5 = w_1^4$ $\delta_4 = ({u_{D,0}}^2 + u_{D,0})^4 + \delta_5, \quad \delta_7 = w_2^4, \quad \delta_6 = (u_{D,1} w_4 + u_{D,0})^4 + \delta_7$ $\delta_8 = (v_{D,1} w_4 + {v_{D,0}}^2)^4$
$G_{D,8}$ (Cost: 5M)	$w_5 = u_{D,1}({u_{D,0}}^2 + u_{D,0} + w_2 + w_3), \quad w_6 = u_{D,1}(w_1 + v_{D,0})$ $\epsilon_1 = {u_{D,1}}^{32}, \quad \epsilon_2 = \delta_1^4, \quad \epsilon_3 = ({u_{D,1}}^3 + u_{D,1} + w_0 + w_1)^{16}, \quad \epsilon_4 = (u_{D,1} + u_{D,0} + 1)^{32}$ $\epsilon_5 = ({u_{D,1}}^2 + u_{D,1} + w_1)^{16}, \quad \epsilon_6 = (\epsilon_3 + {u_{D,0}}^2 + u_{D,0} + w_1 + w_5)^{16}$ $\epsilon_7 = (w_5 + w_6)^{16}, \quad \epsilon_8 = ({u_{D,0}}^3 + ({u_{D,1}}^2 + v_{D,1})(w_2 + w_3) + {v_{D,0}}^2 + u_{D,0} + w_6)^{16}$
Total cost	11 M

Proof. From $u_E(x_j) = {x_j}^2 + u_{E,1} x_j + u_{E,0}$, we have

$$ {x_j}^2 = u_{E,1} x_j + u_{E,0}. \tag{6} $$

Since $y_j = v_E(x_j)$, we also have

$$ y_j = v_{E,1} x_j + v_{E,0}. \tag{7} $$

By using Equations (6) and (7) the functions $G_{D,4}$ and $G_{D,8}$ can be written as linear polynomials as given in the table 2. Since $G_D(E) = G_D(Q_1) G_D(Q_2)$, the result as asserted follows immediately from Proposition 2. □

4 Endomorphism and Eta pairing

Barreto and others [4] classified certain curves which are very special enough to have an efficient algorithm for the Tate pairing computation. They provided us with a sufficient condition for a hyperelliptic curve to have a significant reduction of the loop cost in the final computation of the Tate pairing over points.

In the rest of this section we find a correct condition, and this condition is quite general since it works not only for points, but also for divisors of a curve.

Let H be a hyperelliptic curve over some finite field $\mathbb{F}_{p^n}$, and let ψ be an endomorphism on the curve H. For two divisors D, E in $J_H(\mathbb{F}_{p^n})$, the *Eta pairing* is defined by

$$ \eta(D,E) = \prod_{i=0}^{n-1} h_{D_i}(\psi(E))^{p^{m(n-1-i)}}, \tag{8} $$

Table 2. Reduction formula of $G_{D,4}, G_{D,8}$ for the point evaluation

INPUT	$E = (x_1, y_1) + (x_2, y_2) - 2\mathcal{O} \in J_{H_b}(\mathbb{F}_{2^{12n}})$ $G_{D,4}(x, y) = (y + x^3 + b)^2 + (y + x^3 + b)(\delta_1 x^2 + \delta_2 x + \delta_3) + \delta_4 x^4 + \delta_5 x^3 + \delta_6 x^2 + \delta_7 x + \delta_8$ $G_{D,8}(x, y) = (y + b + 1)^2 + (y + b + 1)(\epsilon_1 x^2 + \epsilon_2 x + \epsilon_3) + \epsilon_4 x^4 + \epsilon_5 x^3 + \epsilon_6 x^2 + \epsilon_7 x + \epsilon_8$
OUTPUT	$C_{D,i}$ for $i = 1, ..4$ where $G_4(x_j, y_j) = C_{D,1} x_j + C_{D,2}$ and $G_8(x_j, y_j) = C_{D,3} x_j + C_{D,4}$
Initiation	$k_1 = u_{E,0} + v_{E,1} + {u_{E,1}}^2,\ k_2 = u_{E,1} u_{E,0} + v_{E,0} + b,\ k_3 = v_{E,0} + b + 1$
$G_{D,4}$	$W = k_1^2 + u_{E,1}(k_1\delta_1 + \delta_5 + \delta_4 u_{E,1}) + \delta_1 k_2 + \delta_2 k_1 + \delta_6$ $C_{D,1} = u_{E,1} W + u_{E,0}(k_1\delta_1 + \delta_5) + \delta_3 k_1 + \delta_2 k_2 + \delta_7$ $C_{D,2} = u_{E,0} W + k_2^2 + \delta_4 {u_{E,0}}^2 + \delta_3 k_2 + \delta_8$
$G_{D,8}$	$W = {v_{E,1}}^2 + u_{E,1}(v_{E,1}\epsilon_1 + \epsilon_5 + \epsilon_4 u_{E,1}) + \epsilon_1 k_3 + \epsilon_2 v_{E,1} + \epsilon_6$ $C_{D,3} = u_{E,1} W + u_{E,0}(v_{E,1}\epsilon_1 + \epsilon_5) + \epsilon_3 v_{E,1} + \epsilon_2 k_3 + \epsilon_7$ $C_{D,4} = u_{E,0} W + k_3^2 + \epsilon_4 {u_{E,0}}^2 + \epsilon_3 k_3 + \epsilon_8$

where

$$D_{i+1} + (h_{D_i}) = p^m D_i \tag{9}$$

with a divisor $D_0 = D$ and some positive integer m.

Assume that the multiplication by p^m has an extremely special form such that

$$p^m((P) - (\mathcal{O})) \equiv ([p^m]P) - (\mathcal{O}) \tag{10}$$

and the map $[p^m]$ of the multiplication by p^m has degree p^{2m}. From the general fact about the map between curves over a finite field [20, Corollary 2.12], the map $[p^m]$ can be written as $[p^m] = \phi\pi^2$, where ϕ is some separable automorphism and π is a Frobenius map of p^mth power.

Let $q = p^{mn}$, then it follows from Eq. (10) that H has a property that

$$q(P) - q(\mathcal{O}) = (\gamma(P)) - (\mathcal{O}) + (g_P) \tag{11}$$

for some automorphism γ on H and some function g_P. Thus γ can be given by $\gamma = \phi^n \pi^{2n}$.

The following theorem is very crucial for efficient computation of the Tate-pairing. Originally the result was given in [4, Theorem 1], but it is only for the points over a defining field. Furthermore, their sufficient condition was not quite correct as we will show in Remark 1. We hence provide correct sufficient condition as follows, and this is quite general in a sense that it works for divisors.

Theorem 3. *Let $q = p^{mn}$, γ be an automorphism of J_H induced from Eq. (11) with $\gamma = \phi^n \pi^{2n}$, and ψ be an endomorphism on the curve H over $\mathbb{F}_{p^n}$.*

Assume that

$$\phi^n \psi^{[q]} = \psi, \tag{12}$$

where $\psi^{[q]}$ denotes a map obtained by raising the coefficients of ψ by qth power, that is, if $\psi(x,y) = (\sum a_{ij}x^iy^j, \sum b_{ij}x^iy^j)$, then $\psi^{[q]}(x,y) = (\sum a_{ij}^q x^iy^j, \sum b_{ij}^q x^iy^j)$.

Then for a divisor D in $J_H(\mathbb{F}_{p^n})$ and a divisor E in J_H, we have

$$\eta(qD, E) = \eta(D, E)^q.$$

Remark 1. In [4], Barreto and others showed that, for $P, Q \in H(\mathbb{F}_{p^n})$,

$$\eta(qP, Q) = \eta(P, Q)^q$$

under the assumption $\gamma\psi^{[q]}(Q) = \psi(Q)$. However, this assumption is not correct for some cryptographically useful curves. For example, the curve $y^2 = x^3 - x + d, d = \pm 1$ over $\mathbb{F}_{3^n}$ does not have this property. By [4], $q = 3^n, \phi(x,y) = (x-d, -y)$ and $\psi(x,y) = (\rho - x, iy)$, $\rho^3 = \rho + d, i^2 = -1$. When $n \equiv 1 \pmod 6$, we get, for $Q = (x,y)$,

$$\gamma\psi^{[q]}(Q) = \phi(\rho^{3^{2n}} + b - x, -i^{3^{2n}}y) = \phi(\rho - x, -iy) = (\rho - x - d, iy) \neq \psi(Q).$$

Proof of Theorem 3.

Proof. We have

$$\gamma(D) + (g_D) = qD,$$

where a function g_D is given by

$$g_D = \prod_{i=0}^{i=n-1} h_{D_i}^{p^{m(n-1-i)}}.$$

Hence, $\eta(D, E) = g_D(\psi(E))$. From the fact that $\deg \gamma = q^2$ and γ is an automorphism, we can derive

$$\gamma^*(h_{D_{n+i}}) = \gamma^*(p^{mi}D_n - D_{n+i+1}) = p^{mi}q^2D - q^2D_{i+1} = q^2(h_{D_i}) \tag{13}$$

Since $h_{D_i}, h_{D_{n+i}}[x] \in \mathbb{F}_{p^n}[x]$ and $q = p^{mn}$, the right side of Eq. (13) is

$$q^2(h_{D_i}) = h_{D_i}(\pi^{2n}) \tag{14}$$

and the left side is

$$\gamma^*(h_{D_{n+i}}) = h_{D_{n+i}}(\gamma) = h_{D_{n+i}}(\phi^n\pi^{2n}). \tag{15}$$

Therefore, comparing g_{qD} with g_D, we have that

$$g_{qD}(\phi^n) = g_D. \tag{16}$$

Then we have $\eta(D,E)^q = g_D(\psi(E))^q = g_D(\psi^{[q]}(E))$; the last equality is from the fact that both D and E are defined over $\mathbb{F}_q$.

Furthermore, $\eta(qD, E) = g_{qD}(\psi(E)) = g_D(\phi^{-n})(\psi(E))$ by Eq. (16).

Our assertion therefore follows immediately from Eq. (12). □

Let $H_b : y^2 + y = x^5 + x^3 + b$ be the hyperelliptic curve over $\mathbb{F}_{2^n}$ as before. We concern with the twisted Tate pairing

$$\begin{aligned}\hat{t} \;:\; J_{H_b}(\mathbb{F}_{2^n})[\ell] \times J_{H_b}(\mathbb{F}_{2^n})/\ell J_{H_b}(\mathbb{F}_{2^{12n}}) \;&\longrightarrow\; \mathbb{F}^*_{2^{12n}} \\ \hat{t}(D,\ E) \;&=\; f_D(\psi(E))^{\frac{2^{12n}-1}{\ell}}.\end{aligned}$$

We use the same endomorphism ψ used in [9]. We identify $\mathbb{F}_{2^{12n}} \cong \mathbb{F}_2(\alpha,\ \tau,\ s_0)$ with α, τ, s_0 defined as follows . We will use a similar notation as in [4], but we will rewrite the field $\mathbb{F}_{2^{6n}}$ in a slightly different way for efficiency (or to represent with simple primitive polynomial).

We first take $\alpha \in \mathbb{F}_{2^n}$ to be such that its minimal polynomial $irr(\alpha,\ \mathbb{F}_2) \in \mathbb{F}_2[x]$, and then $\tau \in \mathbb{F}_{2^{6n}}$ with the minimal polynomial $irr(\tau,\ \mathbb{F}_{2^n}) = x^6 + x + 1 \in \mathbb{F}_{2^n}[x]$. Finally we choose $s_0 \in \mathbb{F}_{2^{12n}}$ that has the minimal polynomial $irr(s_0,\ \mathbb{F}_{2^{6n}}) = x^2 + x + \tau^5 \in \mathbb{F}_{2^{6n}}[x]$.

$$\begin{array}{l}\mathbb{F}_{2^{12n}} \cong \mathbb{F}_2(\alpha,\ \tau,\ s_0) \\ \quad | \qquad s_0^2 + s_0 + \tau^5 = 0 \\ \mathbb{F}_{2^{6n}} \cong \mathbb{F}_2(\alpha,\ \tau) \\ \quad | \qquad \tau^6 + \tau + 1 = 0 \\ \mathbb{F}_{2^n} \cong \mathbb{F}_2(\alpha)\end{array}$$

We define an endomorphism ψ by

$$\psi : H_b(\mathbb{F}_{2^{12n}}) \longrightarrow H_b(\mathbb{F}_{2^{12n}})$$

such that $\psi(x,\ y) = (x + w,\ y + s_2x^2 + s_1x + s_0)$, where

$$w = \tau^5 + \tau^4 + \tau^2, s_2 = \tau^5 + \tau, s_1 = \tau^3 + \tau^2 + \tau + 1, s_0^2 = s_0 + \tau^5.$$

In particular, if $(x_0,\ y_0)$ belongs to $H_b(\mathbb{F}_{2^n}) \subset H_b(\mathbb{F}_{2^{12n}})$, then the *x-coordinate* of $\psi(x_0,\ y_0)$ is in $\mathbb{F}_{2^{6n}}$ and *y-coordinate* of $\psi(x_0,\ y_0)$ is in $\mathbb{F}_{2^{12n}}$.

For any divisor E of H_b, let $E = Q_1 + Q_2 = [u_E,\ v_E] = x^2 + u_{E,1}x + u_{E,0},\ v_{E,1}x+v_{E,0}] \in J_{H_b}$ with $Q_j = (x_j, y_j)$ for $j = 1, 2$. Then the endomorphism ψ on divisors are easily deduced as follows: $E' = \psi(E) = [u_{E'},\ v_{E'}]$, where

$$u_{E'} = x^2 + u_{E,1}x + (u_{E,0} + u_{E,1}w + w^2), \tag{17}$$

$$v_{E'} = (v_{E,1} + s_2u_{E,1} + s_1)x + (v_{E,1}w + v_{E,0} + s_2u_{E,0} + s_0). \tag{18}$$

Let $q = 2^{3n}$ with n coprime to 6, then due to the octupling formula in [9], [4], our curve H_b satisfies the property in Eq. (11), and $\gamma = \phi^n\pi^{2n}$, where $\phi(x, y) = (x + 1,\ y + x^2 + 1)$ and π is a Frobenius map of 2^3th power.

In the following lemma we prove that our curve H_b also satisfies the crucial condition in Eq. (12) for Theorem 3.

Lemma 1. *Let E be a divisor of the curve H_b, and ϕ be a map defined on the curve H_b such that $\phi(x,y) = (x+1,\ y+x^2+1)$. Then we have the following*

$$\phi^n \psi^{[8^n]}(E) = \psi(E).$$

Proof. In fact, we have

$$\psi^{[8^n]}(x,\ y) = (x+w^{8^n},\ \ y+s_2^{8^n}x^2+s_1^{8^n}x+s_0^{8^n}) = (x+w+1,\ y+(s_2+1)x^2+s_1x+s_0^{8^n});$$

this is from the fact that $w^{8^n} = w+1$ and $s_2^{8^n} = s_2+1$ for any odd n, and $s_1^{8^n} = s_1$ for any n. We observe that

$$s_0^{8^n} = \begin{cases} s_0 + w^2 & \text{if } n \equiv 1 \pmod 4 \\ s_0 + w^2 + 1 & \text{if } n \equiv 3 \pmod 4 \end{cases} \tag{19}$$

We note that $\phi^4 = 1$, so we have $\phi^n = \phi$ if $n \equiv 1 \pmod 4$ while $\phi^n = \phi^3$ if $n \equiv 3 \pmod 4$.

$$\phi^n\psi^{[8^n]}(x,y) = \begin{cases} \phi(x+w+1,\ y+(s_2+1)x^2+s_1x+s_0+w^2) & \text{if } n \equiv 1 \pmod 4 \\ \phi^3(x+w+1,\ y+(s_2+1)x^2+s_1x+s_0+w^2+1) & \text{if } n \equiv 3 \pmod 4 \end{cases}$$

Therefore, in both cases, we have that $\phi^n\psi^{[8^n]}(x,y) = \psi(x,y)$. It thus also follows immediately that $\phi^n\psi^{[8^n]}(E) = \psi(E)$ for any divisor E. $\square$

Therefore, we can reduce the loop cost for computing $f_D(\psi(E))^{\frac{2^{12n}-1}{\ell}}$ by using the η pairing as given in Theorem 4.

5 Main Theorem and Algorithms

First, we describe how to compute the Tate pairing

$$\hat{t}(D,\ E) \ = \ f_D(\psi(E))^{\frac{2^{12n}-1}{\ell}},$$

where ψ is the endomorphism defined in Section 4.

From the following lemma, we can get $\hat{t}(D,\ E)$ by computing $2^{6n}D$ instead of computing $(2^{6n}+1)D$.

Lemma 2 ([9]). *Let $\hat{t}$ be the twisted Tate pairing on $H_b : y^2+y = x^5+x^3+b$ ($b = 0$ or 1);*

$$\hat{t} : J_{H_b}(\mathbb{F}_{2^n})[\ell] \times J_{H_b}(\mathbb{F}_{2^{12n}})/\ell J_{H_b}(\mathbb{F}_{2^{12n}}) \longrightarrow \mathbb{F}^*_{2^{12n}}$$

Then $\hat{t}(D,\ E) = (f_D(\psi(E))^{\frac{8^{2n}+1}{\ell}})^{2^{6n}-1} = \tilde{f_D}(\psi(E))^{2^{6n}-1}$, where $2^{6n}D = \mathrm{div}(\tilde{f_D}) + \tilde{D}$.

The following lemma gives the general formula for $[8^i]D$ for any positive integer i. It may be useful to express $[8^i]D$ in terms of the coefficients of u_D (resp. v_D) explicitly.

Lemma 3. *Let $D = [x^2+u_{D,1}x+u_{D,0},\ v_{D,1}x+v_{D,0}]$ be a divisor in J_{H_b}. Let D_i denote $[8^i]D = [u_{D_i},\ v_{D_i}]$ for each integer $i \geq 1$, and $u_{D_i}(x) = x^2+u_{D_i,1}x+u_{D_i,0}$ and $v_{D_i}(x) = v_{D_i,1}x + v_{D_i,0}$ with $u_{D_i,j}, v_{D_i,j} \in \mathbb{F}_{2^n}$ for $j = 0, 1$. Then the coefficients of $u_{D_i}(x)$ (resp. $v_{D_i}(x)$) can be determined by the coefficients of $u_D(x)$ (resp. $v_D(x)$) as follows.*

$$\begin{cases} u_{D_i,1} = u_{D,1}^{8^{2i}} \\ u_{D_i,0} = u_{D,0}^{8^{2i}} + iu_{D,1}^{8^{2i}} + i^2 \\ v_{D_i,1} = iu_{D,1}^{8^{2i}} + v_{D,1}^{8^{2i}} \\ v_{D_i,0} = i(v_{D,1}^{8^{2i}} + u_{D,1}^{8^{2i}} + u_{D,0}^{8^{2i}} + 1) + v_{D,0}^{8^{2i}} \end{cases} \tag{20}$$

Now, we are ready to obtain the following main result.

Theorem 4. *Let $E = [u_E, v_E] = [x^2 + u_{E,1}x + u_{E,0},\ v_{E,1}x + v_{E,0}]$ be a divisor in J_{H_b}, and let $E' = \psi^{[8^n]}(E) = [u_{E'}, v_{E'}]$ with $u_{E'}(x) = x^2 + u_{E',1}x + u_{E',0}$ and $v_{E'}(x) = v_{E',1}x + v_{E',0}$. We define $G_{D_i}(E')$ to be*

$$(C_{D_i,1}^2 u_{E',0} + C_{D_i,1}C_{D_i,2}u_{E',1} + C_{D_i,2}^2)^2(C_{D_i,3}^2 u_{E',0} + C_{D_i,3}C_{D_i,4}u_{E',1} + C_{D_i,4}^2),$$

where $C_{D_i,j}$'s are the values obtained from Table 2 with input vaules D_i and E'. Then the Tate pairing value for $D, E \in J_{H_b}$ is given by

$$\hat{t}(D,\ E) = \left(\prod_{i=0}^{n-1} G_{D_i}(E')^{8^{n-1-i}}\right)^{2(2^{6n}-1)}.$$

Proof. A function $\tilde{f_D}$ is defined by $2^{6n}D = \mathrm{div}(\tilde{f_D}) + \tilde{D}$ as given in Lemma 2. Then by Eq. (9) (with $p^m = 2^3$) we have

$$\tilde{f_D} = \prod_{i=0}^{2n-1} h_{D_i}^{8^{2n-1-i}}.$$

From the definition of Eta pairing

$$\eta(D, E) = \prod_{i=0}^{n-1} h_{D_i}(\psi(E))^{8^{n-1-i}},$$

it is easy to see that $\tilde{f_D}(\psi(E))$ can be written in terms of Eta pairing as follows.

$$\tilde{f_D}(\psi(E)) = \eta(D, E)^{8^n}\eta(8^n D, E).$$

It then follows from Theorem 3 and Lemma 1 that

$$\tilde{f_D}(\psi(E)) = \eta(D,E)^{2\cdot 8^n}. \tag{21}$$

Furthermore, we have $\eta(D,E)^{8^n} = \prod_{i=0}^{n-1} h_{D_i}(\psi^{[8^n]}(E))^{8^{n-1-i}}$ as D_i and E are defined over $\mathbb{F}_{2^n}$. As given in Proposition 1 and 2, $h_{D_i} = \frac{G_{D_i}}{U_{D_i}}$ for some U_{D_i} in $\mathbb{F}_{2^n}[x]$. In fact, the denominator $U_{D_i}(\psi^{[8^n]}(E))$ can be ignored in the final exponentiation since the denominator belongs to $\mathbb{F}_{2^{6n}}$, that is,

$$\begin{aligned}
\hat{t}(D,\ E) &= f_D(\psi(E))^{\frac{2^{12n}-1}{\ell}} = \tilde{f_D}(\psi(E))^{2^{6n}-1} \\
&= (\eta(D,E)^q)^{2(2^{6n}-1)} = \left(\prod_{i=0}^{n-1} h_{D_i}(\psi^{[8^n]}(E))^{8^{n-1-i}}\right)^{2(2^{6n}-1)} \\
&= \left(\prod_{i=0}^{n-1} G_{D_i}(E')^{8^{n-1-i}}\right)^{2(2^{6n}-1)}
\end{aligned}$$

We already know how to compute $G_{D_i}(E')$ in an explicit way as shown in Table 2 with input values D_i and E'. Therefore, our assertion follows immediately. □

Algorithm 5

INPUT $D = [u_D,\ v_D],\ E = [u_E,\ v_E] \in J_{H_b}(\mathbb{F}_{2^n})$, endomorphism ψ, $q = 8^n$
OUTPUT $\hat{t}(D,\ E)$
1: Compute $E' = \psi^{[q]}(E) = [x^2 + u_{E',1}x + u_{E',0},\ v_{E',1}x + v_{E',0}]$ by Equations (17) and (18).
2: $f \leftarrow 1,\ G \leftarrow 1,\ S \leftarrow D$
3: for $i = 1$ to n do
4: compute $G_{S,4}$ and $G_{S,8}$ using Table 1 with S as input.
5: compute $C_{S,1}, C_{S,2}, C_{S,3}, C_{S,4}$ using Table 2 with E' as input.
6: $G \leftarrow G^8 \cdot (C_1^2 u_{E',0} + C_1C_2u_{E',1} + C_2^2)^2 \cdot (C_3^2u_{E',0} + C_3C_4u_{E',1} + C_4^2)$
7: $S \leftarrow [U_8, V_8]$ using Proposition 1 with S as input.
8: Return $G^{2(q^2-1)}$

In Step 8, let $G = c + ds_0,\ c,\ d \in \mathbb{F}_{2^{6n}}$. Then the final exponentiation can be easily computed as follows;

$$\begin{aligned}
\hat{t}(D,\ E) &= (c+ds_0)^{2(2^{6n}-1)} = \left(\frac{c+d\bar{s_0}}{c+ds_0}\right)^2 = \left(\frac{(c+d\bar{s_0})^2}{\mathrm{Norm}(c+ds_0)}\right)^2 \\
&= \left(\frac{c^2+d^2(\tau^5+1)}{c(c+d)+d^2\tau^5}\right)^2 + \left(\frac{d^2}{c(c+d)+d^2\tau^5}\right)^2 s_0^2 \\
&= \left(\frac{c^2+d^2(\tau^5+1)}{c(c+d)+d^2\tau^5}\right)^2 \tau^5 + \left(\frac{d^2}{c(c+d)+d^2\tau^5}\right)^2 s_0,
\end{aligned}$$

for the last equality we used the fact that $s_0^2 = s_0 + \tau^5$.

6 Remarks

For the problem of computing the Tate pairing over divisors, we can approach the problem in a very naive way as follows. For the polynomials in the representation of a divisor, we can represent the coefficients of the polynomials by the *symmetric functions* on their roots. Then it is possible to compute the Tate pairing over divisors by using the elimination method via *Gröbner bases* computation. However, this naive approach certainly requires overly complicated tedious computation process, and it is almost impossible to use the result for implementation of the Tate pairing. It is therefore definitely sufficient to find a much simpler and explicit method for computing the Tate pairing over divisors. In this paper we achieved this task, and we found a very general method and algorithms for computing the Tate pairings over divisors.

Very recently Barreto and others in [4] obtained a closed formula for the Tate paring computation over points of the curves H_b. This is a nice result, however, there result is restrictive since it can be applied only for the divisors which can be written as the sum of points contained in the defining field $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$. As a matter of fact, one can derive the general final closed formula for the Tate paring computation over any divisors in a similar approach made in [4] by using our main Theorem 4 and Lemma 3.

References

1. P.S. Barreto, H.Y.Kim, B. Lynn and M. Scott, Efficient Algorithms for Pairing-Based Cryptosystems, *Advances in Cryptology-Crypto 2002*, LNCS **2442**, pp.354-368 (2002).
2. P. Barreto, B. Lynn and M. Scott, On the Selection of Pairing Friendly Groups, *SAC 2003*, LNCS **3006** pp.17-25 (2004).
3. P. Barreto, Compressed Pairings, *Advances in Cryptology-Crypto 2004*, LNCS **3152**, pp.140-156 (2004).
4. P. Barreto, S. Galbraith, C. hEigeartaigh, and M. Scott, *Efficient Pairing Computation on Supersingular Abelian Varieties*, Cryptology eprint Archives, Available at http://eprint.iacr.org, (2004), Number 2004/375.
5. D. Boneh and M. Franklin, Identity-based encryption from the Weil pairing. *SIAM J. Comput.* **32**, No. 3, pp.586–615 (2003) (electronic).
6. D. Boneh, H. Shacham and B. Lynn, Short signatures from the Weil pairing, *Advances in Cryptology-AsiaCrypt 2001*, LNCS **2248**, pp. 514-532 (2001).
7. D.G. Cantor, Computing in the Jacobian of a Hyperelliptic Curves, *Math. Comp*, *48*, No.177, pp.95-101 (1987).
8. L. Chen and C. Kudla, Identity Based Authenticated Key Agreement Protocols from Pairings, Cryptology eprint Archives, Available at http://eprint.iacr.org, (2002), Number 2002/184.
9. Y. Choie, J. Kim and E. Lee, Efficient Computation of the Tate Pairing on Hyperelliptic Curves for Cryptosystems, preprint.
10. Y. Choie and E. Lee, Implementation of Tate Pairing on Hyperelliptic Curves of Genus 2, *Information security and cryptology-ICISC 2003*, LNCS **2971**, pp.97-111 (2004)

11. I. Duursma and H. Lee, Tate pairing implementation for hyperelliptic curves $y^2 = x^p - x + d$, *Advances in cryptology-AsiaCrypt 2003*, LNCS **2894**, pp. 111–123 (2003).
12. G. Frey and H-G. Rück, A remark concerning m-divisibility in the divisor class group of curves, *Math.Comp.* **62**, No.206, pp.865-874 (1994).
13. S. Galbraith, Supersingular curves in Cryptography, *Advances in Cryptology-AsiaCrypt 2001*, LNCS **2248**, pp.495-513 (2002).
14. S. Galbraith, K. Harrison, and D. Soldera, Implementing the Tate pairing, *Algorithmic Number Theory Symposium - ANTS-V*, LNCS **2369**, pp.324-337 (2002).
15. N. Koblitz, *Algebraic aspects of cryptography*, Springer-Verlag (1998).
16. A.J. Menezes, T. Okamoto and S. Vanstone, Reducing elliptic curve logarithms to logarithms in a finite field, *IEEE Transactions of Information Theory*, **39**, No 5, pp.1639-1646 (1993).
17. D. Mumford, *Tata Lectures on Theta II*, Birkhäuser, (1984).
18. K. Rubin and A. Silverberg, The Best and Worst of Supersingular Abelian Varieties in Cryptology, eprint 2002/006.
19. M. Scott and P.S. Barreto, Compressed pairings, In *Proceedings,* Lecture Notes in Computer Science, Santa Barbara, US, 2004. Advances in ryptology-Crypto"2004, Springer-Verlag, to appear.
20. J. Silverman, The Arithmetic of Elliptic Curves, Springer-Verlag New York (1986).
21. E.R. Verheul, Evidence that XTR Is More Secure than Supersingular Elliptic Curve Cryptosystems, *Advances in Cryptology-AisaCrypt 2001*, LNCS **2248**, pp.433-551 (2002).
22. C. Xing, On supersingular abelian varieties of dimension two over finite fields, *Finite fields and their application*, **2**, pp.407-421 (1996).