J. Korean Math. Soc. **45** (2008), No. 4, pp. 1057–1073

TATE PAIRING COMPUTATION ON THE DIVISORS OF HYPERELLIPTIC CURVES OF GENUS 2

EUNJEONG LEE† AND YOONJIN LEE‡

ABSTRACT. We present an explicit Eta pairing approach for computing the Tate pairing on *general divisors* of hyperelliptic curves H_d of genus 2, where $H_d : y^2 + y = x^5 + x^3 + d$ is defined over $\mathbb{F}_{2^n}$ with $d = 0$ or 1. We use the *resultant* for computing the Eta pairing on general divisors. Our method is very general in the sense that it can be used for *general* divisors, not only for *degenerate* divisors. In the pairing-based cryptography, the efficient pairing implementation on general divisors is significantly important because the decryption process definitely requires computing a pairing of general divisors.

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 [4] and its significance as a cryptanalytic tool [9, 16]. Recently, the Tate pairing and the Weil pairing have been used to construct various cryptosystems [4, 5, 6, 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 [2, 3, 7, 10, 11, 18, 19].

Most of pairing-based cryptosystems use a divisor D as a system parameter, which is a generator of an additive cyclic group with prime order ℓ. Generally, inputs for pairing computation are usually aD for arbitrary integer $a \in \{0, \ldots, \ell\}$. 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 [1], 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, but the divisors do not always have to be written as a sum of points in the defining field $\mathbb{F}_{2^n}$; such points are called *degenerate divisors* [13]. Since the algorithm proposed in [1] works only for degenerate divisors, we need to develop an algorithm which works for

Received November 24, 2006; Revised June 26, 2007.

2000 *Mathematics Subject Classification.* 11T71, 14G50, 94A60.

Key words and phrases. Tate pairing, Ate pairing, Eta pairing, hyperelliptic curve, pairing-based cryptosystems.

†The author was supported by KOSEF, grant number R01-2005-000-10713-0.

‡The author was supported by NSERC.

general divisors as well.

Recent developments [1, 8] on the Tate pairing implementation on hyperelliptic curves over a finite field $\mathbb{F}_q$ have focused on the case of *degenerate divisors* as mentioned before. However, in the pairing-based cryptography, the efficient Tate pairing implementation over *general divisors* is significantly important. For instance, in the Boneh-Franklin identity-based encryption scheme, the private keys are general divisors, and therefore the decryption process requires computing a pairing of general divisors.

In this paper, in terms of efficiency of bilinear and non-degenerate pairing on H_d, we compare the Eta pairing and the Ate pairing on supersingular hyperelliptic curves. Furthermore, we obtain very efficient algorithm for a pairing computation over general 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 [1]. In recent years Duursma and Lee [8] introduced a closed formula of the Tate paring for a very special family of hyperelliptic curves for the Tate pairing computation. This closed formula significantly reduced the total number of iterations for the Tate pairing computation over such curves. Barreto and others [1] showed why such curves are very special to have 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.

We find a general method for computing the Eta pairing over divisor class groups of the curves H_d in a very explicit way. So far only pointwise approach has been made in [1] for the Tate pairing computation on the hyperellitic curves H_d over $\mathbb{F}_{2^n}$. The paper [1] works only for degenerate divisors. Hence, when divisors are not a sum of degenerate divisors, we present a general method and algorithms for computing the Eta pairing over divisors by extending the idea of [1] and using the resultant. We estimate a timing result of our algorithm for the Eta pairing using our theoretical complex analysis and known timing result of a multiplication in $\mathbb{F}_{2^n}$. According to our estimation, the Eta pairing on $H_d(\mathbb{F}_{2^{79}})$ can be obtained in $2.4ms$ for general divisors.

This paper is organized as follows. In Section 2, we begin with a brief summary of the Tate pairing, the Eta pairing and the Ate pairing. Section 3 discusses the Eta pairing and the Ate pairing on H_d for efficient pairing on H_d. In Section 4, we obtain main results and algorithms for the Eta pairing computation on the divisors of H_d. We finish our paper with complex analysis to estimate the timing of the Eta pairing algorithm in Section 5. We use *SINGULAR* software package for symbolic computations.

2. Tate, Eta and Ate pairing

In this section, we recall the basic definitions and properties (see [14] 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 of 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 $\deg(F) = 2g + 1$, $h(x) \in \mathbb{F}_q[x]$, $\deg(h) \leq g$ and there are no singular points on H.

Now let

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

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 ∞. 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 2.1 (Reduced divisor [14], [17]**).** *Let $\mathbb{F}_q(H)$ be the function field given by H defined over $\mathbb{F}_q$. Then each nontrivial divisor class of J_H can be represented by*

$$D = \sum_{i=1}^{r} (P_i) - r(\infty), \text{ where } r \leq g,\ P_i \neq \infty,\ P_i \in H.$$

Let $P_i = (a_i,\ b_i)$, $1 \leq i \leq r$ 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) $\deg(v_D) < \deg(u_D) \leq g$
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 denote a divisor class by $D = [u_D, v_D]$, where D is a reduced divisor and u_D, v_D are polynomials in $\mathbb{F}_q[x]$ satisfying the three conditions in Theorem 2.1.

Now we recall the definition of the Tate pairing [9]. 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 embedding degree.* Let $J_H[\ell] = \{D \in J_H \mid \ell D = \infty\}$. The *Tate pairing* is a map

$$\begin{aligned} \langle \cdot, \cdot \rangle_\ell : J_H[\ell] \times J_H(\mathbb{F}_{q^k})/\ell J_H(\mathbb{F}_{q^k}) &\to \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^\ell \\ \langle D, E \rangle_\ell &= f_{\ell,D}(E'), \end{aligned} \tag{2}$$

where $\text{div}(f_{\ell,D}) = \ell D$ and $E' \sim E$ with $\text{support}(E') \cap \text{support}(\text{div}(f_{\ell,D})) = \emptyset$. To obtain a unique value, the *reduced* pairing is defined by

$$t(D, E) = \langle D, E \rangle_\ell^{(q^k-1)/\ell} = \langle D, E \rangle_N^{(q^k-1)/N} \in \mu_\ell$$

for $\ell \mid N \mid (q^k - 1)$, where μ_ℓ is the set of ℓth roots of unity.

What follows is a useful result for the resultant computation, and for the proof we refer to [22, Ch. VI].

Theorem 2.2. *Let F be a field, $A, B \in F[x]$, $\alpha_1, \alpha_2, \ldots, \alpha_m \in \bar{F}$ (= algebraic closure of F) be all the roots of A, $\deg A = m$, $\deg B = n$, and a be the leading coefficient of A. Then we have*

$$\mathrm{res}(A, B) = a^n \prod_{i=1}^{m} B(\alpha_i),$$

where $\mathrm{res}(A, B)$ denotes the resultant of A and B.

We can make the evaluation of the rational function at a divisor much more efficient by using the following reduction technique.

Lemma 2.3. *With the same notations as in Theorem 2.2 we have*

$$\mathrm{res}(A, B) = (-1)^{mn}\mathrm{res}(B, A). \tag{3}$$

In addition, efficient reduction method for computing the resultant is also introduced in [22, Ch. VI]. *When $m \geq n$, by Euclidean division algorithm, there exist $Q(x), R(x) \in F(x)$ such that $A(x) = Q(x)B(x) + R(x)$ with $\deg R < n$. Then*

$$\mathrm{res}(A, B) = (-1)^{mn}\mathrm{res}(B, R). \tag{4}$$

Barreto and others [1] 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 degenerate divisors.

Eta pairing

We recall the Eta pairing introduced in [1] which is very useful for efficient computation of the Tate pairing. The Eta pairing is defined on supersingular curve with even embedding degree $k > 1$, and there is a distortion map ψ whose x-coordinate is defined over $\mathbb{F}_{q^{k/2}}$. This type of distortion map allows denominator elimination when the final powering $(q^k - 1)/\ell$ is raised.

Let ψ be a distortion map on a hyperelliptic curve H over $\mathbb{F}_q$ with $q = p^n$. For $T \in \mathbb{Z}$ and two divisors $D, E \in J_H(\mathbb{F}_q)$, the *Eta pairing* [1] is defined by

$$\eta_T(D, E) = f_{T,D}(\psi(E)),$$

where $D' + (f_{T,D}) = TD$ for a reduced divisor D'.

For the relation between the Tate pairing and the Eta pairing, we refer to [1, Theorem 1]. This is a generalization of Duursma-Lee's method [8] and gives a further improvement with shorter loop length by choosing a proper T.

Remark 2.4. The result is given in [1, Theorem 1], but in the proof of the theorem some validity is missing. In more detail, in the proof of Lemma 1 in [1], they wrote

$$\gamma^*(\sum_P n_P(P)) = \sum_P \sum_{S \in \gamma^{-1}(P)} n_P e_\gamma(S)(S) = \sum_P n_P(\gamma^{-1}(P)),$$

where the last equality is not always true since the ramification index $e_\gamma(S)$ is not necessarily 1. The condition 2 related to a distortion map in [1, Theorem 1] is satisfied only for $\mathbb{F}_q$-rational points on H. However, when we work on Jacobian variety with dimension g, a divisor defined over $\mathbb{F}_q$ generally consists of $\mathbb{F}_{q^g}$-rational points on C.

In Lemma 2.5, we rewrite [1, Lemma 1] with correct proof. We also want to point out that the divisor D does not have to be in $J_H(\mathbb{F}_q)$, and we may have D in $J_H(\mathbb{F}_{q^b})$ for some $b \in \mathbb{N}$.

Let H be a supersingular hyperelliptic curve. Assume that, for some $b \in \mathbb{N}$, the multiplication by p^b has an extremely special form such that

$$p^b((P) - (\infty)) \equiv ([p^b]P) - (\infty) \tag{5}$$

and the map $[p^b]$ of the multiplication by p^b has degree p^{2b}. From the general fact about the map between curves over a finite field [20, Corollary 2.12], the map $[p^b]$ can be written as $[p^b] = \phi\pi_{p^b}^2$, where ϕ is some separable automorphism and π_{p^b} is a Frobenius map of p^bth power. If we write $[q^b] = \widehat{\pi_{q^b}} \circ \pi_{q^b}$, then we have $\widehat{\pi_{q^b}} = \phi^n \pi_{q^b}$.

Lemma 2.5. *Let H be a supersingular curve over $\mathbb{F}_q$ as above. Let D, E be divisors on H defined over $\mathbb{F}_{q^b}$ with order dividing $N \in \mathbb{N}$ and let $M = (q^k - 1)/N$. Suppose $T \in \mathbb{Z}$ is such that $TD \equiv q^b D \pmod{\ell}$ and $T = q^b + cN$ for some $c \in Z$. Let ψ be a distortion map on the curve H over $\mathbb{F}_{p^n}$. Assume that for any divisor E in $J_H(\mathbb{F}_q)$*

$$\phi^n \psi^{[q^b]}(E) = \psi(E), \tag{6}$$

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

$$\psi^{[s]}(x, y) = (\sum a_{ij}^s x^i y^j, \sum b_{ij}^s x^i y^j).$$

Then for divisors D, E in $J_H(\mathbb{F}_q)$, we have

$$\eta(TD, E)^M = \eta(D, E)^{TM}.$$

Proof. For an automorphism γ defined over $\mathbb{F}_q$, we note that $f_{T,\gamma(D)} \circ \gamma = (f_{T,D})^{\deg(\gamma)}$. Since the divisors D, E and the morphisms ϕ, π_q are defined over $\mathbb{F}_{q^b}$, we obtain

$$\begin{aligned} f_{T,TD}(\psi(E)) &= f_{T,q^bD}(\psi(E)) = (f_{T,D} \circ [q^b]^{-1}(\psi(E)))^{q^{2b}} \\ &= f_{T,D} \circ \phi^{-n}\pi_{q^b}^{-2}\pi_{q^b}^2(\psi(E)) = (f_{T,D} \circ \psi^{[q^b]})(E) \\ &= f_{T,D}(\psi(E))^{q^b} \end{aligned}$$

from Eq. (6). The desired result is obtained by

$$f_{T,TD}(\psi(E))^M = f_{T,D}(\psi(E))^{Mq^b} = f_{T,D}(\psi(E))^{M(T-cN)} = f_{T,D}(\psi(E))^{TM}.$$

□

Let $T^a + 1 = LN$ for some $a, L \in \mathbb{N}$. Then, by Lemma 2.5 and lemmas in [1], the relation between the Eta pairing and the Tate pairing is as follows:

$$\langle D, \psi(E)\rangle_N^{ML} = \eta_T(D,E)^{MaT^{a-1}}$$

Ate pairing

Grager et al. [12] generalize the Eta pairing on supersingular curves to ordinary curves by restricting the pairing to cyclic subgroups G_1 and G_2 such that

$$G_1 = J_H[\ell] \cap \ker(\pi_q - [1]), \quad G_2 = J_H[\ell] \cap \ker(\pi_q - [q]).$$

Let $\mathrm{lc}_\infty(f_{q,D}) = (z^\ell f_{q,D})(\infty)$, where $z \in \mathbb{F}_q(H)$ is a uniformizer at ∞ over $\mathbb{F}_q$.

Theorem 2.6 ([12]). *Let H be a supersingular hyperelliptic curve over $\mathbb{F}_q$, and G_1, G_2 be given as above. Then with $e = \gcd(k, q^k - 1)$*

$$\hat{a}(\cdot,\cdot) : G_1 \times G_2 \to \mu_r : (D,E) \mapsto (f_{q,D}/\mathrm{lc}_\infty(f_{q,D})(E))^e$$

defines a non-degenerate bilinear pairing. Furthermore, the pairing $\hat{a}$ satisfies

$$\langle D, \psi(E)\rangle_N^M = \hat{a}(D,E)^{(k/e)q^{k-1}}.$$

Remark 2.7. We want to compare the Eta pairing and the Ate pairing. In Lemma 2.5 with $b = 1$, the condition Eq. (6)

$$\gamma\psi^{[q]}(D) = \psi(D)$$

for $D \in J_H(\mathbb{F}_q)$ and the endomorphism ψ identifies the subgroup $G_2 = \psi(G_1)$. In Section 3, we discuss the difference between Eta pairing and the Ate pairing on H_d over $\mathbb{F}_q$.

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

$$H_d : y^2 + y = x^5 + x^3 + d, \quad d = 0 \text{ or } 1 \tag{7}$$

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 nice group structures.

3. Efficient pairing on H_d

In this section, we consider the Eta pairing and the Ate pairing on H_d. Let $q = 2^n$ with n coprime to 6.

Endomorphism

We use the same endomorphism ψ used in [1]. We identify the tower of extension fields as follows:

$$\begin{aligned}
&\mathbb{F}_{2^{12n}} \cong \mathbb{F}_2(\alpha,\ w,\ s_0)\\
&\ |\qquad s_0^2 + s_0 + w^5 + w^3 = 0\\
&\mathbb{F}_{2^{6n}} \cong \mathbb{F}_2(\alpha,\ w)\\
&\ |\qquad w^6 + w^5 + w^3 + w^2 + 1 = 0\\
&\mathbb{F}_{2^n} \cong \mathbb{F}_2(\alpha).
\end{aligned}$$

We define an endomorphism ψ (or called the distortion map) by

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

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

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

In particular, if $(x_0,\ y_0)$ belongs to $H_d(\mathbb{F}_{2^n}) \subset H_d(\mathbb{F}_{2^{12n}})$, 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 $\mathbb{F}_{2^{12n}}$.

Octupling formula

There is an octupling formula of the point in [1]. As pointed in [1], octupling a divisor on the curve H_d is computationally very simple, of which complexity is almost the same as octupling of a point on elliptic curves.

Lemma 3.1. *Let H_d be a hyperelliptic curve defined by $y^2 + y = x^5 + x^3 + b$ over $\mathbb{F}_{2^n}$. Then for a point $P = (\alpha,\ \beta)$ in H_d,*

$$8(P) - 8(\infty) = [\alpha_1,\ \beta_1] + \operatorname{div}\left(\frac{g_{4,P}(x,\ y)^2 g_{8,P}(x,\ y)}{u_{4,P}(x)^2 u_{8,P}(x)}\right),\ \textit{where}$$

$$\begin{aligned}
&\alpha_1 = \alpha^{64} + 1,\ \ \beta_1 = (\alpha^2 + \beta)^{64} + 1,\\
&g_{4,P}(x,\ y) = y + x^3 + (\alpha^2 + \alpha)^4 x^2 + \alpha^4 x + \beta^4 + b,\\
&g_{8,P}(x,\ y) = y + (\alpha^2 + 1)^{16} x^2 + (\alpha^2 + \alpha)^{16} x + (\alpha^3 + \alpha + \beta + b + 1)^{16},\\
&u_{4,P}(x) = x^2 + x + (\alpha^2 + \alpha)^8,\\
&u_{8,P}(x) = x + (\alpha_1).
\end{aligned}$$

We denote $f_{8,D} = \frac{G_{8,D}}{U_{8,D}}$, where

$$(8) \qquad G_{8,D} = \prod_{P \in \text{support}(D)} g_{4,P}^2 g_{8,P}, \quad U_{8,D} = \prod_{P \in \text{support}(D)} u_{4,P}^2 u_{8,P}.$$

Eta Pairing on H_d

According to the result in [1, Section 7], the Eta pairing over the curve H_d is optimal when T is taken to be $\pm 2^{(3n+1)/2} - 1$. We take $T = -2^{(3n+1)/2} - 1$. In this case, by setting $T = -T$ and $D = -D$, we have $T = 2^{(3n+1)/2} + 1$.

Let $\kappa = \frac{n-1}{2}$. As n is coprime to 6, $T = 2^{(3n+1)/2} + 1 = 8^\kappa \cdot 2^2 + 1$. Then

$$\eta_T(D,E) = f_{T,D}(\psi(E)) = \left(\prod_{i=0}^{\kappa-1} f_{8,D_i}^{4\cdot 8^{\kappa-1-i}} \cdot f_{4,D_\kappa} \cdot \mathcal{A} \right)(\psi(E)),$$

where $D_{i+1} + (f_{8,D_i}) = 8D_i$ with a divisor $D_0 = D$ and a rational function $\mathcal{A}$ is obtained from the final addition.

Now, with the notation as Eq. (8), we set

$$\hat{\eta}(D,E) := \left(\prod_{i=0}^{\kappa-1} G_{8,D_i}^{48^{\kappa-1-i}} \cdot G_{4,8^\kappa D} \cdot \mathcal{A} \right)(\psi(E)). \tag{9}$$

The Tate pairing and the Eta pairing over the curve H_d are related as follows [1, Theorem 1, Section 7.2]:

$$\langle D,E \rangle_N^M = \eta_T(D,E)^{\frac{2MT}{L}} = \hat{\eta}(D,E)^{\frac{2MT}{L}}, \tag{10}$$

where $M = (2^{12n}-1)/N$, $N = 2^{2n} - 2^{(3n+1)/2} + 2^n - 2^{(n+1)/2} + 1$, $L = 2^{n+1} + 2^{(n+3)/2} + 2$ and $\frac{2MT}{L} = (2^{6n}-1)(2^{4n}2^{(n+1)/2} - 2^{3n} + 1)$.

Ate Pairing on H_d

Since the embedding degree is 12, $\gcd(k, 2^{nk} - 1) = 3$. Then from the definition of the Ate pairing, we have

$$\hat{a}(D,E) = f_{q,D}(E)^3$$

for $D \in G_1, E \in G_2$. Since $q < T = 2^{(3n+1)/2} + 1$, the loop length of Miller algorithm is less than the Eta pairing.

In summary, on H_d, we can define the following two efficient bilinear and nondegenerate pairings:

$$\begin{array}{rll} \eta_T: & J(\mathbb{F}_q)[\ell] \times J(\mathbb{F}_q)[\ell] \to \mu_\ell, & (D,E) \mapsto f_{T,D}(\psi(E))^{\frac{2MT}{L}} \\ \hat{a}: & G_1 \times G_2 \to \mu_\ell, & (D,E) \mapsto f_{q,D}(E)^3. \end{array}$$

From Eq. (10), it is enough to compute $\hat{\eta}$ for the Eta pairing $f_{T,D}(\psi(E))^{\frac{2MT}{L}}$ which does not involve the denominator of $f_{T,D}$. Even though the Ate pairing has a 2/3 loop length of the Eta pairing, $f_{q,D}$ is a fraction of G_{8,D_i} and U_{8,D_i} defined in Eq. (8) for each $i, 0 \le i \le n-1$. The computation of the denominator $U_{8,D_i}(E)$ for each loop causes expensive timing cost.

In the following section, we find explicit formula to compute the Eta pairing on general divisors which are represented by Mumford representation. In the final section, we estimate a timing of our algorithm for the Eta pairing with known timing result of finite field operations.

4. Closed formula for the Eta pairing on H_d

What follows is the main theorem of this section. Barreto et al. [1] provide an explicit formula for $\hat{\eta}(P,Q)$ on points P and Q in $H_d(\mathbb{F}_{2^n})$. We find a closed formula for $\hat{\eta}(D,E)$ with general divisors D and E in $J_{H_d}(\mathbb{F}_{2^n})$ in Theorem 4.1.

Notation: In this theorem, for any polynomial g, $g^{[i]}$ denotes raising the power of 2^i to only the coefficients of $g(x)$, and also for just constant a, $a^{[i]} = a^{2^i}$.

Theorem 4.1. *For general divisors D and E in $J_{H_d}(\mathbb{F}_{2^n})$, the Eta pairing with $T = 2^{(3n+1)/2} + 1$ is given by*

(11)

$$\hat{\eta}(D,E) = \prod_{i=0}^{(n-3)/2} \left(\mathrm{res}_X(G_{i,4}(X, v_E^{[e]}(X)),\ u_E^{[e]}(X)) \cdot \mathrm{res}_X(G_{i,8}(X, v_E^{[e]}(X)),\ u_E^{[e]}(X))\right)^4 \cdot \Lambda,$$

where

$$e = \frac{3n-9-6i}{2},\quad e' = \frac{3n-3+6i}{2},$$

$$A_4 = w^4 + X^4,\quad B_4 = X^4 + X^2 + w^4 + w^2 + v_{D,1}^{2^{e'}},$$

$$C_4 = Y^2 + X^6 + X^4(w+w^2) + X^2(1+w) + w^2 + \gamma + v_{D,0}^{2^{e'}} + s_0,$$

$$A_8 = X^2 + X + w^2 + w,\quad B_8 = X + w + v_{D,1}^{2^{e'}} + 1,$$

$$C_8 = Y + X^2(w^4) + X(w^4 + w^2) + w^2 + \gamma + v_{D,0}^{2^{e'}} + s_0,$$

$$G_{i,4}(X,Y) = \mathrm{res}_Z(A_4Z^2 + B_4Z + C_4,\ u_D^{[e']}(Z)),$$

$$G_{i,8}(X,Y) = \mathrm{res}_Z(Z^3 + A_8Z^2 + B_8Z + C_8,\ u_D^{[e']}(Z)),$$

and the first term Λ is given by

$$\Lambda = \mathrm{res}_X\left(\mathrm{res}_Z(AZ^2 + BZ + C,\ u_D^{[3n-1]}(Z)),\ u_E(X)\right) \text{ with}$$

$$A = X^2 + w^2,$$

$$B = X^2 + X + w^2 + w + v_{D,1}^{2^{3n-1}},$$

$$C = v_E(X) + X^3 + (w^4 + w + 1)X^2 + w^4X + w^3 + v_{D,0}^{2^{3n-1}} + \gamma((n-1)/2) + b + s_0,$$

and $\gamma(i) = 1$ if $i \equiv 1 \pmod 4$ and $\gamma(i) = 0$ otherwise.

The explicit formulae for $G_{i,4}(X, v_E^{[e]}(X))$ and $G_{i,8}(X, v_E^{[e]}(X))$ are given in Table 1.

Proof. Let $\kappa = \frac{n-1}{2}$. The intermediate formulas for the Eta pairing for points $P = (\alpha, \beta), Q = (x_Q, y_Q)$ in [1, Appendix B] are given by

$$g_{i,4}(\psi(Q))^{2\cdot 8^{\kappa-1-i}} = y_Q^{2e} + (\alpha^{2e'} + \alpha^{e'})x_Q^{4e} + (\alpha + 1 + x_Q^{4e})x_Q^{2e} + \beta^{e'} + \gamma(i) + (x_Q^{4e} + x_Q^{2e})w + (x_Q^{4e} + \alpha^{e'} + 1)w^2$$

$$
\begin{aligned}
&+ (\alpha^{e'} + \alpha^{2e'})w^4 + s_0,\\
g_{i,8}(\psi(Q))^{8^{\kappa-1-i}} &= y_Q^e + (\alpha^{2e'} + \alpha^{e'})x_Q^e + \beta^{e'} + \alpha^{2e'}(\alpha^{e'} + x_Q^{2e})\\
&+ \alpha^{e'} + \gamma(i) + (\alpha^{2e'} + \alpha^{e'})w + (\alpha^{2e'} + x_Q^e + 1)w^2\\
&+ (x_Q^{2e} + x_Q^e)w^4 + s_0,
\end{aligned}
$$

where $\gamma(i) = 1$ if $i \equiv 1 \pmod 4$ and $\gamma(i) = 0$ otherwise.

If we let $X := x^{2^e}$ and $Z := \alpha^{2^{e'}}$ then by Theorem 2.2 we can derive Eq. (11) except the last term Λ.

For the first term Λ, we need four times of $D_{(3n-3)/2}$ and one addition with D. Let $D = (P_1) + (P_2) - 2(\infty)$ and D_j' be the reduced divisor equivalent to $2^{(3n+1)/2}((P_j) - (\infty))$. As pointed in [1, Appendix B.7] (we only consider $n \equiv 3 \pmod 4$ without loss of generality), the reduced divisor D_j' has the form of $\phi(P_j) + (-P_j) - 2(\infty)$ and thus we have

$$(2^{(3n+1)/2} + 1)D = \phi(P_1) + \phi(P_2) - 2(\infty) + (v_{P_1}v_{P_2}) = D_1' + D_2' + D,$$

where v_{P_j} is a vertical line at P_j.
Then $T = 8^\kappa \cdot 4 + 1$ and $(P_{\kappa,j}) - (\infty) = 8^\kappa((P_j) - (\infty))$. Since

$$
\begin{aligned}
8^\kappa D &= D_\kappa + (f_{8^\kappa,D})\\
&= (P_{\kappa,1}) + (P_{\kappa,2}) - 2(\infty) + (f_{8^\kappa,D}),\\
4 \cdot 8^\kappa D &= 4D_\kappa + 4(f_{8^\kappa,D})\\
&= 4\left((P_{\kappa,1}) - (\infty)\right) + 4\left((P_{\kappa,2}) - (\infty)\right) + 4(f_{8^\kappa,D})\\
&= D_1' + (f_{4,P_{\kappa,1}}) + D_2' + (f_{4,P_{\kappa,2}}) + 4(f_{8^\kappa,D}),\\
(4 \cdot 8^\kappa + 1)D &= D_1' + D_2' + D + (f_{4,P_{\kappa,1}}) + (f_{4,P_{\kappa,2}}) + 4(f_{8^\kappa,D})\\
&= \phi(P_1) + \phi(P_2) - 2(\infty) + (v_{P_1}v_{P_2}) + (f_{4,P_{\kappa,1}})\\
&\quad + (f_{4,P_{\kappa,2}}) + 4(f_{8^\kappa,D})
\end{aligned}
$$

and we can ignore the vertical lines, the first rational function for one addition with D is

$$f_{4,P_{\kappa,1}} \cdot f_{4,P_{\kappa,2}}.$$

Note that $P_{\kappa,j} = (\alpha_j^{2^{6\kappa}} + 1,\ \beta_j^{2^{6\kappa}} + \alpha_j^{2^{6\kappa+1}} + \gamma(\kappa))$, where $\gamma(\kappa) = 1$ if $\kappa \equiv 1 \pmod 4$ and $\gamma(\kappa) = 0$ otherwise. (Note that we assume $n \equiv 3 \pmod 4$, so κ is odd). By Lemma 3.1,

$$g_{4,P_{\kappa,j}} = y + x^3 + (\alpha_j^{2^{6\kappa+3}} + \alpha_j^{2^{6\kappa+2}})x^2 + \alpha_j^{2^{6\kappa+2}}x + \beta_j^{2^{6\kappa+2}} + \alpha_j^{2^{6\kappa+3}} + \gamma(\kappa) + b.$$

Since $\alpha_j^{2^{6\kappa+2}} = \alpha_j^{2^{3n-1}}$ is a root of $u_D^{[3n-1]}$ and we omit vertical lines appearing in $f_{4,P_{\kappa,1}} \cdot f_{4,P_{\kappa,2}}$, the first rational function for one addition with D is given by

$$
\begin{aligned}
R(x,y) &:= g_{4,P_{\kappa,1}} \cdot g_{4,P_{\kappa,2}}\\
&= \mathrm{res}_Z((x^2+1)Z^2 + (x^2 + x + v_{D,1}^{2^{3n-1}})Z + y + x^3 + v_{D,0}^{2^{3n-1}} + \gamma(\kappa) + b, u_D^{[3n-1]}(Z)).
\end{aligned}
$$

Then the polynomial $L(X,Y)$ has the form

$$\begin{aligned} L(X,Y) &= R \circ \psi(X,Y) \\ &= \mathrm{res}_Z(AZ^2 + BZ + C, u_D^{[3n-1]}(Z)), \end{aligned}$$

where

$$\begin{aligned} A &= (x^2+1) \circ \psi, \\ B &= (x^2 + x + v_{D,1}^{2^{3n-1}}) \circ \psi, \\ C &= (y + x^3 + v_{D,0}^{2^{3n-1}} + \gamma(\kappa) + b) \circ \psi. \end{aligned}$$

Since $\psi(X,Y) = (X+w,\ Y + (w^4+1)X^2 + (w^4+w^2)X + s_0)$, we have

$$\begin{aligned} A &= X^2 + w^2, \\ B &= X^2 + X + w^2 + w + v_{D,1}^{2^{3n-1}}, \\ C &= Y + X^3 + (w^4 + w + 1)X^2 + w^4 X + w^3 + v_{D,0}^{2^{3n-1}} + \gamma(\kappa) + b + s_0. \end{aligned}$$

Therefore, we have $\Lambda = \mathrm{res}_X\left(L(X, v_E(X)),\ u_E(X)\right)$, so the result follows. □

Closed formula for $\hat{\eta}(D,E)$

We find the closed formula for $\hat{\eta}(D,E)$ by Lemma 2.3. In Algorithm 1 we describe an algorithm for computing the $\hat{\eta}$-pairing on divisors.

To compute the resultant in Eq. (11), by Eq. (4), we have

$$\mathrm{res}_X(G_{i,4}(X, v_E^{[e]}(X)),\ u_E^{[e]}(X)) = \mathrm{res}_X(R_{i,4}(X),\ u_E^{[e]}(X)),$$

where $R_{i,4}(X) = G_{i,4}(X, v_E^{[e]}(X)) \pmod{u_E^{[e]}}$. We simplify $G_{i,4}(X, v_E^{[e]}(X))$ as follows:

$$G_{i,4}(X, v_E^{[e]}(X)) = X^{12} + h_{i,5}X^{10} + h_{i,4}X^8 + h_{i,3}X^6 + h_{i,2}X^4 + h_{i,1}X^2 + h_{i,0}$$

with $h_{i,j}$ given in Table 1. Refer to the step 13 in Algorithm 2.

Using the reduction formula $X^j = \mu_j^{[e]} X + \nu_j^{[e]} \pmod{u_E^{[e]}(X)}$ given by

$$\begin{aligned} &\mu_2 = u_{E,1}, && \nu_2 = u_{E,0} \\ &\mu_j = u_{E,1}\mu_{j-1} + \nu_{j-1}, && \nu_j = u_{E,0}\mu_{j-1},\ j = 3,\ldots,6,8,10,12, \end{aligned} \tag{12}$$

we obtain

$$\begin{aligned} R_{i,4}(X) &= (\vec{\mu} \cdot \vec{h_i})X + \vec{\nu} \cdot \vec{h_i} \\ &= R_{i,4,1}X + R_{i,4,0}, \end{aligned} \tag{13}$$

where

$$\begin{aligned} \vec{\mu} &= (\mu_{12}, \mu_{10}, \mu_8, \mu_6, \mu_5, \mu_4, \mu_3, \mu_2, 1, 0), \\ \vec{\nu} &= (\nu_{12}, \nu_{10}, \nu_8, \nu_6, \nu_5, \nu_4, \nu_3, \nu_2, 0, 1), \\ \vec{h_i} &= (1, h_{i,5}, h_{i,4}, h_{i,3}, 0, h_{i,2}, 0, h_{i,1}, 0, h_{i,0}) \\ R_{i,4,1} &:= \vec{\mu} \cdot \vec{h_i} \ \text{ and } \ R_{i,4,0} := \vec{\nu} \cdot \vec{h_i}. \end{aligned}$$

This computation corresponds to the steps 15, 16 and 17 in Algorithm 2. Therefore,

$$\begin{aligned}\mathrm{res}_X(G_{i,4}(X, v_E^{[e]}(X)),\ u_E^{[e]}(X)) &= \mathrm{res}_X(R_{i,4}(X),\ u_E^{[e]}(X)\ ) \\ &= R_{i,4,1}^2 - u_{E,1}^{[e]} R_{i,4,1} R_{i,4,0} + u_{E,0}^{[e]} R_{i,4,0}^2\end{aligned}$$

as described in the step 21 in Algorithm 1. In this algorithm, we use $\mu_2[e] = \mu_2^{2^e}$ and $\nu_2[e] = \nu_2^{2^e}$ instead of $u_{E,1}^{[e]}$ and $u_{E,0}^{[e]}$ because $\mu_2 = u_{E,1}$ and $\nu_2 = u_{E,0}$.

Let

$$G_{i,8}(X, v_E^{[e]}(X)) = k_{i,4}X^4 + k_{i,3}X^3 + k_{i,2}X^2 + k_{i,1}X + k_{i,0}$$

with $k_{i,j}$ given in Table 1. Refer to the step 14 in Algorithm 2.

By proceeding in a similar way as for the case of $G_{i,4}$, we obtain

$$\begin{aligned}\mathrm{res}_X(G_{i,8}(X, v_E^{[e]}(X)),\ u_E^{[e]}(X)) &= \mathrm{res}_X(R_{i,8}(X),\ u_E^{[e]}(X)\ ) \\ &= R_{i,8,1}^2 - u_{E,1}^{[e]} R_{i,8,1} R_{i,8,0} + u_{E,0}^{[e]} R_{i,8,0}^2,\end{aligned}$$

as we see the step 22 in Algorithm 2. We therefore obtain the closed formula for $\hat{\eta}(D, E)$:

(14)

$$\begin{aligned}&\hat{\eta}(D, E) \\ &= \Lambda\left(\prod_{i=0}^{(n-3)/2} \mathrm{res}_X(G_{i,4}(X, v_E^{[e]}(X)), u_E^{[e]}(X)) \cdot \mathrm{res}_X(G_{i,8}(X, v_E^{[e]}(X)), u_E^{[e]}(X))\right)^4 \\ &= \Lambda\left(\prod_{i=0}^{(n-3)/2} (R_{i,4,1}^2 - u_{E,1}^{[e]} R_{i,4,1} R_{i,4,0} + u_{E,0}^{[e]} R_{i,4,0}^2)(R_{i,8,1}^2 - u_{E,1}^{[e]} R_{i,8,1} R_{i,8,0} + u_{E,0}^{[e]} R_{i,8,0}^2)\right)^4\end{aligned}$$

and this gives the steps 25, 26 and 27 in Algorithm 2. In the steps 25 and 26 of the algorithm, for Λ, let $\vec{L}$ be a vector with coefficients of $L(X, Y)$ defined in Table 1. Hence the value Λ is equal to

$$L_1^2 - u_{E,1} L_1 L_0 + u_{E,0} L_0^2,$$

where $L_1 = \vec{L} \cdot \vec{\mu}$ and $L_0 = \vec{L} \cdot \vec{\nu}$.

5. Complexity of the Eta pairing on general divisors over H_d

Now we compute the complexity of Algorithm 1. We use the following notations: m is the time for a multiplication in $\mathbb{F}_{2^n}$ and m_{12} for a multiplication in $\mathbb{F}_{2^{12n}}$.

The first precomputation of the step 2 through the step 5 needs $11m$ as shown in Table 1. Note that we ignore the time cost for squaring because it is negligible comparing to the time for multiplications. The second precomputation for the step 7 and the step 8, we need $13m$ by counting the number of multiplications in Eq. (12).

In **for** loop, we need $12m$ for the step 13 and the step 14 as shown in Table 1. To count the number of operations for reduction step (Step 16 and Step 17),

Algorithm 1 Eta pairing over $H_d : y^2 + y = x^5 + x^3 + b$ by the resultant

:

INPUT: $D = [U_D,\ V_D]$, $E = [U_E,\ V_E] \in J_{H_d}(\mathbb{F}_{2^n})$, endomorphism ψ, $q = 2^n$

OUTPUT: $\hat{\eta}(D,\ E)$

1: : Precompute powers of coefficients using u_D and v_D for $0 \leq i \leq n-1$ (Table 1).

2: : $a_0[i] \leftarrow a_0^{2^i},\ a_1[i] \leftarrow a_1^{2^i},\ a_2[i] \leftarrow a_2^{2^i}$.

3: : $b_0[i] \leftarrow b_0^{2^i},\ b_1[i] \leftarrow b_1^{2^i},\ b_2[i] \leftarrow b_2^{2^i},\ b_3[i] \leftarrow b_3^{2^i},\ b_4[i] \leftarrow b_4^{2^i},\ b_5[i] \leftarrow b_5^{2^i}$

4: : $c_0[i] \leftarrow c_0^{2^i},\ c_1[i] \leftarrow c_1^{2^i},\ c_2[i] \leftarrow c_2^{2^i}$

5: : $d_0[i] \leftarrow d_0^{2^i},\ d_1[i] \leftarrow d_1^{2^i},\ d_2[i] \leftarrow d_2^{2^i},\ d_3[i] \leftarrow d_3^{2^i},\ d_4[i] \leftarrow d_4^{2^i}$

6: : Precompute powers of coefficients using u_E and v_E for $0 \leq i \leq n-1$.

7: : $\vec{\mu}[i] \leftarrow (\mu_{12}^{2^i}, \mu_{10}^{2^i}, \mu_8^{2^i}, \mu_6^{2^i}, \mu_5^{2^i}, \mu_4^{2^i}, \mu_3^{2^i}, \mu_2^{2^i}, 1, 0)$ (Eq. (12))

8: : $\vec{\nu}[i] \leftarrow (\nu_{12}^{2^i}, \nu_{10}^{2^i}, \nu_8^{2^i}, \nu_6^{2^i}, \nu_5^{2^i}, \nu_4^{2^i}, \nu_3^{2^i}, \nu_2^{2^i}, 0, 1)$(Eq. (12))

9: : $v_1[i] \leftarrow v_{E,1}^{2^i},\ v_0[i] \leftarrow v_{E,0}^{2^i}$

10:: Set $f \leftarrow 1$

11:: for $i = 0$ to $(n-3)/2$ do

12:: $e = (3n - 9 - 6i)/2 \bmod n,\ e' = (3n - 5 + 6i)/2 \bmod n$

13:: $G_{i,4} \leftarrow X^{12} + h_{i,5}X^{10} + h_{i,4}X^8 + h_{i,3}X^6 + h_{i,2}X^4 + h_{i,1}X^2 + h_{i,0}$ (Table 1)

14:: $G_{i,8} \leftarrow k_{i,4}X^4 + k_{i,3}X^3 + k_{i,2}X^2 + k_{i,1}X + k_{i,0}$ (Table 1)

15:: Set $\vec{h}_i = (1, h_{i,5}, h_{i,4}, h_{i,3}, 0, h_{i,2}, 0, h_{i,1}, 0, h_{i,0})$

16:: Compute $R_{4,1} \leftarrow \vec{\mu}[e] \cdot \vec{h}_i$

17:: Compute $R_{4,0} \leftarrow \vec{\nu}[e] \cdot \vec{h}_i$

18:: Set $\vec{k}_i = (0, 0, 0, 0, 0, k_{i,4}, k_{i,3}, k_{i,2}, k_{i,1}, k_{i,0})$

19:: Compute $R_{8,1} \leftarrow \vec{\mu}[e] \cdot \vec{k}_i$

20:: Compute $R_{8,0} \leftarrow \vec{\nu}[e] \cdot \vec{k}_i$

21:: Compute $F_4 \leftarrow R_{4,1}^2 - \mu_2[e]R_{4,1}R_{4,0} + \nu_2[e]R_{4,0}^2$

22:: Compute $F_8 \leftarrow R_{8,1}^2 - \mu_2[e]R_{8,1}R_{8,0} + \nu_2[e]R_{8,0}^2$

23:: compute $f \leftarrow f \cdot F_4 \cdot F_8$

24:: end for

25:: $L_1 \leftarrow \vec{L} \cdot \vec{\mu},\ L_0 \leftarrow \vec{L} \cdot \vec{\nu}$ where $\vec{L}$ is a vector with coefficients of $L(X, Y)$ defined in Table 1.

26:: $\Lambda \leftarrow L_1^2 - u_{E,1}L_1L_0 + u_{E,0}L_0^2$

27:: Return $f^4 \cdot \Lambda$.

we consider the entries of $\vec{h}_i$. From Table 1, we know that it appears as

$\vec{h}_i =$

j	s_0w^5	s_0w^4	s_0w^3	s_0w^2	s_0w^1	s_0	w^5	w^4	w^3	w^2	w	1
12	0	0	0	0	0	0	0	0	0	0	0	1
10	0	0	0	0	0	0	0	0	0	0	0	$*$
8	0	0	0	0	0	0	0	1	0	$\delta_{i0}+1$	δ_{i0}	$*$
6	0	0	0	0	0	0	0	$*$	0	0	$*$	$*$
5	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	$*$	0	$*$	$*$	$*$	$*$	$*$
3	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	$*$	$*$	$*$	$*$	$*$	$*$	$*$
1	0	0	0	0	0	0	0	0	0	0	0	0
0	0	$*$	0	$*$	0	$*$	$*$	$*$	$*$	$*$	$*$	$*$

where $*$ represents a nonzero entry at the position. Therefore, the computation of $R_{4,1} = \vec{h}_i \cdot \vec{\mu}$ in the step 16 needs $19m$ which is the number of $*$'s for $j = 2, \ldots, 6, 8, 10, 12$ plus one for δ_{i0}. Similarly, we need $19m$ for the step 17.

The entries of k_i is shown as

$$\vec{k_i} = \left(\begin{array}{c|cccccccccccc} j & s_0w^5 & s_0w^4 & s_0w^3 & s_0w^2 & s_0w^1 & s_0 & w^5 & w^4 & w^3 & w^2 & w & 1 \\ \hline 12 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 10 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 8 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & * & 0 & 0 & 1 & 0 \\ 3 & 0 & 0 & 0 & 0 & 0 & * & * & * & * & * & * & * \\ 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & * \\ 1 & 0 & 0 & 0 & 0 & 0 & * & * & * & * & * & 0 & * \\ 0 & 0 & 0 & 0 & * & * & * & 1 & * & * & * & * & * \end{array}\right)$$

and thus the computation of $R_{8,1} = \vec{k_i} \cdot \vec{\mu}$ in Step 19 needs $9m$ which is the number of $*$'s for $j = 2, \ldots, 4$. Similarly, we need $9m$ for Step 20. In Step 21, since $R_{4,0}^2 \in \mathbb{F}_{2^{6n}}$, we need $6m$ for $\nu[e]R_{4,0}^2$. For $\mu_2[e]R_{4,1}R_{4,2}$, we need $2m_{12} + 12m$. To update the value f in Step 23, we need $2m_{12}$, and in Step 25 we need $24m$ for the inner products. The final exponentiation of $\hat{\eta}$ for unique pairing value requires $\frac{n+1}{2}$ squarings, 4 Frobenius actions, 2 multiplications and a division [1, Section 7.5].

Hence, the total complexity for the Eta pairing on general divisors on H_d is

$$\begin{aligned} T_b &= 11m + 13m + 24m + 18m + 2m_{12} \\ &\quad + \frac{n-3}{2}(12m + 2 \cdot 19m + 2 \cdot 9m + 2 \cdot 18m + 2m_{12} + 2m_{12}) + 2m_{12} + 1I_{12} \\ &= 66m + 4m_{12} + 1I_{12} + \frac{n-3}{2}(104m + 4m_{12}), \end{aligned}$$

where I_{12} is time for an inversion in $\mathbb{F}_{12}$. As mentioned in [15], $\mathbb{F}_{q^{12}}$ is a pairing friendly field of which multiplication m_{12} can be implemented by $5 \cdot 3^2 m$. Therefore, the complexity of T_b has the minimal cost as

$$\begin{aligned} T_b &= 66m + 180m + 1I_{12} + \frac{n-3}{2}(104m + 4 \cdot 45m) \\ &= 246m + 142m(n-3) + 1I_{12}. \end{aligned}$$

When $n = 79$ as given in [1], T_b takes 11488 m and one inversion in $\mathbb{F}_{q^{12}}$. According to [23], a field multiplication in $\mathbb{F}_{2^{163}}$ can be performed in $2.3\mu s$ on SPARC 32-bit 900MHz. If we apply this timing result to T_b, then the Eta pairing on H_d using Algorithm 1 can be obtained in $2.64ms$. The timing result of the Eta pairing on general divisors of Barreto. et al [1] takes $4.20ms$ on Pentium IV with 3GHz. This timing result for Algorithm 1 is comparable to the implementation result in [1] on $H(\mathbb{F}_{2^{79}})$ and furthermore, Algorithm 1 includes all divisors with supporting points in $\mathbb{F}_{q^2}$ not in $\mathbb{F}_q$.

TABLE 1. The explicit formulae for $G_{i,4}, G_{i,8}$ and Ł on H_b

Input	$u_D(Z), v_D(Z), u_E(X), v_E(X),\ e' = (3n-5+6i)/2,\ e = (3n-9-6i)/2$	
Output	$G_{i,4}(X, v_E^{[e]}(X)),\ G_{i,8}(X, v_E^{[e]}(X)),\ L(X, v_E(X))$	
	$\delta_0 = u_{D,1}^2 + u_{D,1},\ \delta_1 = u_{D,1}v_{D,1},\ \delta_2 = u_{D,0}u_{D,1},\ \delta_3 = u_{D,1}v_{D,0}$ $\epsilon_0 = u_{D,0}^2 + u_{D,0},\ \epsilon_1 = u_{D,0}v_{D,1} + u_{D,1}v_{D,0}$ $\epsilon_2 = u_{D,0}u_{D,1} + u_{D,1}^3 + u_{D,1}v_{D,1} + u_{D,1},\ \epsilon_3 = u_{D,1}\epsilon_1$	$6m$
a_0	$(0,0,0,0,0,0,0,\delta_0,0,u_{D,1},0,\delta_1)$	
a_1	$(0,0,0,0,0,0,0,0,0,0,0,u_{D,1})$	
a_2	$(0,0,0,0,0,0,0,0,0,0,0,\delta_0)$	
b_0	$(0,\ \delta_0, 0, u_{D,1}, 0,\ \delta_1+1,\ \delta_2+\delta_0,\ \delta_0\gamma + u_{D,0} + \epsilon_3 - \delta_3 + u_{D,1} + 1,\ \delta_2+\delta_0+1,$ $u_{D,1}\gamma + \delta_2 + \delta_0 + \delta_3 + \delta_1,\ \epsilon_0 + \delta_2,\ (\delta_1+1)\gamma + (\delta_0 + \epsilon_0 + v_{D,1}\epsilon_1 + v_{D,0}^2))$	$1m$
b_1	$(0,0,0,0,0,\ u_{D,1},\ \delta_0,\ \delta_0+\delta_2,\ u_{D,1}, 0,\ \delta_1,\ u_{D,1}\gamma + \delta_3 + \delta_1)$	
b_2	$(0,0,0,0,0,\ \delta_0, 0,\ u_{D,1},\ u_{D,1}^2,\ \delta_2+\delta_1+1,\ \delta_1+u_{D,1},\ \delta_0\gamma+\epsilon_3+\delta_3+u_{D,1}^2+u_{D,0}+1)$	
b_3	$(0,0,0,0,0,0,0,\ \delta_0, 0, 0,\ u_{D,1}^2, \delta_2+\delta_1+\delta_0)$	
b_4	$(0,0,0,0,0,0,0,\ 1, 0, \delta_0+1, \delta_0,\ \epsilon_0+\delta_2+u_{D,1})$	
b_5	$(0,0,0,0,0,0,0,0,0,0,0,\delta_0)$	
$G_{i,4}$	$X^{12} + (b_5^{(e')})X^{10} + (b_4^{(e')})X^8 + (v_{E,1}^{2^{e+1}} a_2^{(e')} + b_3^{(e')})X^6 + (v_{E,0}^{2^{e+1}} a_2^{(e')} + v_{E,1}^{2^{e+2}} + v_{E,1}^{2^{e+1}} a_1^{(e')} + b_2^{(e')})X^4$ $(v_{E,0}^{2^{e+1}} a_1^{(e')} + v_{E,1}^{2^{e+1}} a_0^{(e')} + b_1^{(e')})X^2 + (v_{E,0}^{2^{e+2}} + v_{E,0}^{2^{e+1}} a_0^{(e')} + b_0^{(e')})$	$6m$
c_0	$(0,0,0,0,0,0,0,0,0,\ u_{D,1}^2,\ \delta_0,\ \epsilon_2)$	
c_1	$(0,0,0,0,0,0,0,0,0,0,0,\ \delta_0)$	
c_2	$(0,0,0,0,0,0,0,0,0,0,0,\ u_{D,1}^2)$	
d_0	$(0,0,0,\ u_{D,1}^2,\ \delta_0,\ \epsilon_2+1,\ 1,\ u_{D,0}^2+u_{D,1}^2+1,\ \delta_2+\delta_0+1,\ u_{D,1}^2\gamma + u_{D,1}(u_{D,0}^2+\epsilon_1) + \epsilon_0 + \epsilon_2,$ $\delta_0\gamma + u_{D,1}(\delta_2+\epsilon_0) + \epsilon_3 + \delta_3,$ $(\epsilon_2+1)\gamma + v_{D,0}^2 + \epsilon_1(v_{D,1} + u_{D,1}^2) + \delta_3 + u_{D,0}(u_{D,0}^2 + 1 + u_{D,1}^2 + \delta_3))$	$4m$
d_1	$(0,0,0,0,0,\delta_0,\ u_{D,1},\ u_{D,1}^2+\epsilon_2,\ u_{D,1},\ u_{D,1}^3+\delta_1, 0,\ \delta_0\gamma + u_{D,1}(\epsilon_0+\delta_2) + u_{D,1}^2 + \epsilon_3 + \delta_3)$	
d_2	$(0,0,0,0,0,u_{D,1}^2, u_{D,1}, \delta_0+\epsilon_2+1, u_{D,1}^2, \delta_0, \delta_2+1, u_{D,1}^2\gamma + \epsilon_0 + 1 + u_{D,1}(u_{D,0}^2+\epsilon_1) + u_{D,1}^2)$	
d_3	$(0,0,0,0,0,0,0,u_{D,1}, 0, u_{D,1}^2, 0, \delta_2)$	
d_4	$(0,0,0,0,0,0,0,u_{D,1}^2, 0, 0, 1, u_{D,0}^2+1)$	
$G_{i,8}$	$(d_4^{(e')})X^4 + (v_{E,1}^{2^e} c_2^{(e')} + d_2^{(e')} + d_3^{(e')})X^3 + (v_{E,0}^{2^e} c_2^{(e')} + v_{E,1}^{2^{e+1}} + v_{E,1}^{2^e} c_1^{(e')})X^2$ $+(v_{E,0}^{2^e} c_1^{(e')} + v_{E,1}^{2^e} c_0^{(e')} + d_1^{(e')})X + (v_{E,0}^{2^{e+1}} + v_{E,0}^{2^e} c_0^{(e')} + d_0^{(e')})$	$6m$
$a_{L,0}$	$(0,0,0,0,0,0,0,0,0,\delta_0,u_{D,1},\delta_1)^{(3n-1)}$	
$a_{L,1}$	$(0,0,0,0,0,0,0,0,0,0,0,\delta_0)^{(3n-1)}$	
$a_{L,2}$	$(0,0,0,0,0,0,0,0,0,0,0,\delta_0)^{(3n-1)}$	
$b_{L,0}$	$(0,0,0,\delta_0,u_{D,1},\delta_1+1,\delta_0,\epsilon_0+\delta_2+u_{D,1},\delta_2+\delta_1,\delta_0(\gamma+b)+\epsilon_3+\delta_3+u_{D,0}+1,$ $u_{D,1}(\gamma+b)+\delta_3,(\delta_1+1)(b+\gamma)+v_{D,1}\epsilon_1+v_{D,0}^2+1)^{(3n-1)}$	
$b_{L,1}$	$(0,0,0,0,0,\delta_0,u_{D,1}^2,\delta_1,0,\delta_0,\delta_2,\delta_0(\gamma+b)+\epsilon_3+\delta_3+\delta_0)^{(3n-1)}$	
$b_{L,2}$	$(0,0,0,0,0,\delta_0,u_{D,1}^2,\delta_0+\delta_1,\delta_0,u_{D,1},\delta_2+\delta_1+u_{D,1}+1,\delta_0(\gamma+b)+\epsilon_0+\epsilon_3+\delta_2+\delta_3+\delta_1+\delta_0+1)^{(3n-1)}$	
$b_{L,3}$	$(0,0,0,0,0,0,0,0,0,\delta_0,u_{D,1}^2,\delta_1+\delta_0)^{(3n-1)}$	
$b_{L,4}$	$(0,0,0,0,0,0,0,\delta_0,0,1,\delta_0+1,\epsilon_0+\delta_2)^{(3n-1)}$	
$b_{L,5}$	$(0,0,0,0,0,0,0,0,0,0,0,\delta_0)^{(3n-1)}$	
L	$X^6 + b_{L,5}X^5 + b_{L,4}X^4 + (v_{E,1}a_{L,2} + b_{L,3})X^3 + (v_{E,0}a_{L,2} + v_{E,1}^2 + v_{E,1}a_{L,1} + b_{L,2})X^2$ $(v_{E,0}a_{L,1} + v_{E,1}a_{L,0} + b_{L,1})X + (v_{E,0}^2 + v_{E,0}a_{L,0} + b_{L,0})$	$6m$

The 12-tuples $\Gamma = (\beta_5,\beta_4,\beta_3,\beta_2,\beta_1,\beta_0,\alpha_5,\alpha_4,\alpha_3,\alpha_2,\alpha_1,\alpha_0)^{(e')}$ represents $\Gamma = \sum_{j=0}^{5}(\beta_j^{2^{e'}} s_0 w^j + \alpha_j^{2^{e'}} w^j)$.

References

[1] P. S. L. M. Barreto, S. D. Galbraith, C. O'hEigeartaigh, and M. Scott, *Efficient pairing computation on supersingular abelian varieties*, Des. Codes Cryptogr. **42** (2007), no. 3, 239–271.

[2] P. S. L. M. Barreto, H. Y. Kim, B. Lynn, and M. Scott, *Efficient algorithms for pairing-based cryptosystems*, Advances in cryptology—CRYPTO 2002, 354–368, Lecture Notes in Comput. Sci., 2442, Springer, Berlin, 2002.

[3] P. S. L. M. Barreto, B. Lynn, and M. Scott, *On the selection of pairing-friendly groups*, Selected areas in cryptography, 17–25, Lecture Notes in Comput. Sci., 3006, Springer, Berlin, 2004.

[4] D. Boneh and M. Franklin, *Identity-based encryption from the Weil pairing*, SIAM J. Comput. **32** (2003), no. 3, 586–615.

[5] D. Boneh, B. Lynn, and H. Shacham, *Short signatures from the Weil pairing*, Advances in cryptology—ASIACRYPT 2001 (Gold Coast), 514–532, Lecture Notes in Comput. Sci., 2248, Springer, Berlin, 2001.

[6] L. Chen and C. Kudla, *Identity Based Authenticated Key Agreement Protocols from Pairings*, Cryptology eprint Archives, Number 2002/184.

[7] Y. Choie and E. Lee, *Implementation of Tate pairing on hyperelliptic curves of genus 2*, Information security and cryptology—ICISC 2003, 97–111, Lecture Notes in Comput. Sci., 2971, Springer, Berlin, 2004.

[8] I. Duursma and H. Lee, *Tate pairing implementation for hyperelliptic curves* $y^2 = x^p - x + d$, Advances in cryptology—ASIACRYPT 2003, 111–123, Lecture Notes in Comput. Sci., 2894, Springer, Berlin, 2003.

[9] G. Frey and H.-G. Rück, *A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves*, Math. Comp. **62** (1994), no. 206, 865–874.

[10] S. Galbraith, *Supersingular curves in cryptography*, Advances in cryptology—ASIACRYPT 2001 (Gold Coast), 495–513, Lecture Notes in Comput. Sci., 2248, Springer, Berlin, 2001.

[11] S. Galbraith, K. Harrison, and D. Soldera, *Implementing the Tate pairing*, Algorithmic number theory (Sydney, 2002), 324–337, Lecture Notes in Comput. Sci., 2369, Springer, Berlin, 2002.

[12] R. Granger, F. Hess, R. Oyono, N. Theriault, and F. Vercauteren, *Ate pairing on hyperelliptic curves*, Proceedings of Euro 2007, 430–447, Lecture Notes in Comput. Sci., 4515, Springer, Berlin, 2007.

[13] M. Katagi, I. Kitamura, T. Akishita, and T. Takagi, *Novel efficient implementations of hyperelliptic curve cryptosystems using degenerate divisors*, In Information Security Applications-WISA'2004, 345–359, Lecture Notes in Comput. Sci., 3325, Springer, Berlin, 2005.

[14] N. Koblitz, *Algebraic Aspects of Cryptography*, With an appendix by Alfred J. Menezes, Yi-Hong Wu and Robert J. Zuccherato. Algorithms and Computation in Mathematics, 3. Springer-Verlag, Berlin, 1998.

[15] N. Koblitz and A. Menezes, *Pairing-based cryptography at high security levels*, Cryptography and coding, 13–36, Lecture Notes in Comput. Sci., 3796, Springer, Berlin, 2005.

[16] A. J. Menezes, T. Okamoto, and S. Vanstone, *Reducing elliptic curve logarithms to logarithms in a finite field*, IEEE Trans. Inform. Theory **39** (1993), no. 5, 1639–1646.

[17] D. Mumford, *Tata Lectures on Theta. II*, Jacobian theta functions and differential equations. With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman and H. Umemura. Progress in Mathematics, 43. Birkhauser Boston, Inc., Boston, MA, 1984.

[18] K. Rubin and A. Silverberg, *Using Abelian Varieties to Improve Pairing-Based Cryptography*, to appear in Journal of Cryptology.

[19] M. Scott and P. S. Barreto, *Compressed pairings*, Advances in cryptology—CRYPTO 2004, 140–156, Lecture Notes in Comput. Sci., 3152, Springer, Berlin, 2004.

[20] J. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, 106. Springer-Verlag, New York, 1986.

[21] E. R. Verheul, *Evidence that XTR is more secure than supersingular elliptic curve cryptosystems*, Advances in cryptology—EUROCRYPT 2001 (Innsbruck), 195–210, Lecture Notes in Comput. Sci., 2045, Springer, Berlin, 2001.

[22] C. K. Yap, *Fundamental Problems of Algorithmic Algebra*, Oxford University Press, New York, 2000.

[23] A. Weimerskirch, D. Stebila, and S. Shantz, *Generic* $GF(2^m)$ *arithmetic in software and its application to ECC*, Proceedings of ACISP 2003, 79–92, Lecture Notes in Comput. Sci., 2727, Springer, Berlin, 2003.

EUNJEONG LEE
KOREA INSTITUTE FOR ADVANCED STUDY
SEOUL 130-722, KOREA
E-mail address: ejlee@kias.re.kr

YOONJIN LEE
DEPARTMENT OF MATHEMATICS
EWHA WOMANS UNIVERSITY
SEOUL 120-750, KOREA
E-mail address: yoonjinl@ewha.ac.kr