Ate pairing for $y^2 = x^5 - \alpha x$ in characteristic five

Ryuichi Harasawa, Yutaka Sueyoshi, and Aichi Kudo

Department of Computer and Information Sciences, Faculty of Engineering,
Nagasaki University,
1-14 Bunkyomachi, Nagasaki-shi, Nagasaki, 852-8521, Japan
{harasawa, sueyoshi, kudo}@cis.nagasaki-u.ac.jp

Abstract

Recently, the authors proposed a method for computing the Tate pairing using a distortion map for $y^2 = x^5 - \alpha x$ ($\alpha = \pm 2$) over finite fields of characteristic five. In this paper, we show the Ate pairing, an invariant of the Tate pairing, can be applied to this curve. This leads to about 50% computational cost-saving over the Tate pairing.

Keywords: Tate/Ate pairing, Hyperelliptic curves

1 Introduction

As is well known, bilinear maps such as the Weil/Tate pairing give various cryptographic applications. This makes the study on the pairings active, for example the construction of curves suitable to the pairings and efficient pairing computations.

In 2004, P. S. L. M. Barreto et al. [1] proposed a new bilinear map, called the Eta pairing, for some types of curves, mainly supersingular (hyper)elliptic curves in characteristic two and three and Duursma-Lee type curves $y^2 = x^p - x + d$ [5] in characteristic p with $p \equiv 3 \pmod 4$. More precisely, the pairing gives the value obtained by raising that of the Tate pairing to the power of a certain constant. It turns out that the Eta pairing makes a lot of computational cost-saving over the Tate pairing. The main reason is that the computational procedure of the Eta pairing is just a part of that of the Tate pairing with little extra task.

After the appearance of the Eta pairing, F. Hess et al. [7] simplified the Eta pairing, called the Ate pairing, and extended it to ordinary elliptic curves.

For $y^2 = x^5 - \alpha x$ ($\alpha = \pm 2$) over finite fields of characteristic five, the authors constructed a distortion map and described a computation

of the Tate pairing using the map [6]. In this paper, we show the Ate pairing can be applied to this curve in a natural way. This leads to about 50% computational cost-saving over the Tate pairing. We remark that our distortion map for $y^2 = x^5 - \alpha x$ does not satisfy the (sufficient) condition for the Eta pairing as it is.

2 Ate pairing for $y^2 = x^5 - \alpha x$

In this section, we describe the Ate pairing for $y^2 = x^5 - \alpha x$. We refer the reader to [6] for more details on this curve.

Let $p = 5$, $q = p^r$ with r odd, $C/\mathbb{F}_q$ the curve defined by $y^2 = x^5 - \alpha x$ ($\alpha = \pm 2$) and id the identity element of $\mathrm{Jac}(C)$. Then we have $\#\mathrm{Jac}_{\mathbb{F}_q}(C) = q^2 + 1$ and the embedding degree is equal to 4 for every odd prime l dividing $q^2 + 1$.

There exists a simple quintuple operation on $\mathrm{Jac}(C)$ as follows, which is a variant of [4]:

Theorem 1 ([6, Theorem 1]).

$$p\ \mathrm{div}(x + a_0, b_0) = \mathrm{div}(x - a_0^{p^2},\ \alpha b_0^{p^2}) + ((b_0^p y + (\alpha x + a_0^p)^{\frac{p+1}{2}})/(x - a_0^{p^2})),$$

$$\begin{aligned} p\ \mathrm{div}(x^2 + a_1 x + a_0,\ b_1 x + b_0) = \mathrm{div}(&x^2 - a_1^{p^2} x + a_0^{p^2},\ -\alpha b_1^{p^2} x + \alpha b_0^{p^2}) \\ &+ ((\gamma y^2 + f_1(x) y + f_0(x))/(x^2 - a_1^{p^2} x + a_0^{p^2})), \end{aligned}$$

where

$$\begin{aligned} \gamma &:= ((a_0 b_1 - a_1 b_0) b_1 + b_0^2)^p, \\ f_1(x) &:= \alpha (a_1 b_1 - 2 b_0)^p x^3 - 2(2 a_0 b_1 - a_1 b_0)^p x^2 \\ &\quad + 2\alpha (a_0 a_1 b_1 - (a_1^2 - 2 a_0) b_0)^p x \\ &\quad - ((a_1^2 - 2 a_0) a_0 b_1 - (a_1^2 + 2 a_0) a_1 b_0)^p, \\ f_0(x) &:= (-x^2 + \alpha a_1^p x + a_0^p)^3. \end{aligned}$$

We obtain the following result from Theorem 1, which plays an important role for an efficient computation of pairings for $y^2 = x^5 - \alpha x$.

Proposition 1 ([6, Proposition 1]).

Let $D = \mathrm{div}(f(x), g(x))$ be a reduced divisor with $\deg f(x) = 2$, and D_i the reduced divisor such that $D_i \sim p^i D$ (especially $D_0 = D$). For $i \geq 1$, we set $pD_{i-1} = D_i + (\ell_i(x, y)/h_i(x))$, where $\ell_i(x, y)$ can be represented as

$\ell_i(x,y) = \gamma_i y^2 + (s_i x^3 + t_i x^2 + u_i x + v_i)y + (-x^2 + c_i x + d_i)^3$ *from Theorem* 1. *Then, for each coefficient of* ℓ_i, *we have*

$$\gamma_{i+1} = -\gamma_i^{p^2}, \quad s_{i+1} = \alpha s_i^{p^2}, \, t_{i+1} = -\alpha t_i^{p^2}, \, u_{i+1} = \alpha u_i^{p^2},$$
$$v_{i+1} = -\alpha v_i^{p^2}, \, c_{i+1} = -c_i^{p^2}, \, d_{i+1} = d_i^{p^2}.$$

Let π_q denote the q-th power Frobenius endomorphism and ζ_8 (resp. ζ_5) the morphism of C defined by $(x,y) \mapsto (\alpha x, \, \alpha^{\frac{1}{2}} y)$ (resp. $(x + \alpha^{\frac{1}{4}}, \, y)$). We shall use the same symbols for the endomorphisms of $\mathrm{Jac}(C)$ induced from these morphisms.

For a divisor $D = \sum_{P \in C} n_P(P)$, we write $\hat{D} = \sum_{P \in C \setminus \{(0,0), \mathcal{O}\}} n_P(P)$, the divisor obtained by eliminating $(0,0)$ and $\mathcal{O}$ from D.

By t_l we denote the Tate pairing of order l, and by $\mu_l \subset \mathbb{F}_{q^4}$ the set of l-th roots of unity. Since $\gcd(q^2+1, q) = 1$, there exists an integer ρ such that $\rho q \equiv 1 \pmod{q^2+1}$.

Under the notation above, we obtain the following result.

Theorem 2 (Main Theorem: Ate pairing for $y^2 = x^5 - \alpha x$).
We set $\eta = (\zeta_5 - \zeta_5^{-1}) + q \circ (\zeta_5^{\alpha^r} - \zeta_5^{-\alpha^r})$, *and suppose* $l || q^2 + 1$ [1]. *Then the pairing*

$$\hat{t}_l : \mathrm{Jac}_{\mathbb{F}_q}(C)[l] \times \mathrm{Jac}_{\mathbb{F}_q}(C)[l] \longrightarrow \mu_l$$

defined by

$$\hat{t}_l(D, E) = t_l(D, \zeta_8 \circ \eta(E))^\rho$$

is bilinear and has the property that $\hat{t}_l(D,E) \neq 1$ *for all* $D, E \neq \mathrm{id}$, *namely* $\zeta_8 \circ \eta$ *becomes a distortion map for* $\mathrm{Jac}_{\mathbb{F}_q}(C)[l] \setminus \{\mathrm{id}\}$. *Furthermore, assuming* $(0,0) \notin \mathrm{supp} D$ *or* $\deg \hat{E} = 2$, *we have*

$$\hat{t}_l(D, E) = f_q \circ \phi\,(\hat{E})^{2(q^2-1)},$$

where f_q *is a function of* $\mathbb{F}_q(C)$ *such that* $qD = D_q + (f_q)$ *with the reduced divisor* D_q *and* $\phi((a,b)) := (-a^{-5}\alpha^{\frac{1}{2}}, \, -2a^{-15}b^5\alpha\alpha^{\frac{3}{4}})$ *for* $(a,b) \in C$ *with* $a \neq 0$.

Remark 1.
For the Tate pairing based on [6] (*see Lemma* 1), *we need a function* $f_{q^2} \in \mathbb{F}_q(C)$ *such that* $q^2 D = D_{q^2} + (f_{q^2})$ *with the reduced divisor* D_{q^2}. *This shows that the cost of the Ate pairing is about a half of that of the Tate pairing based on* [6] (*see Table* 4).

[1] This condition seems to hold for cryptographic applications because the value of l should be chosen so that $l \geq 2^{160}$ in view of security.

Remark 2.

If $(0, 0) \in \mathrm{supp}D$ *and* $\deg\hat{E} = 1$, *then* $\hat{t}_l(D, E) = \pm f_q \circ \phi(\hat{E})^{2(q^2-1)}$ *holds, where the signature is determined so that* $\hat{t}_l(D, E) \in \mu_l$ [6, Theorem 7] [2].

Remark 3.

In the actual computation of $f_q \circ \phi(\hat{E})^{2(q^2-1)}$ *for the function* $f_q = \prod_{i,j} \frac{h_i(x,y)}{k_j(x,y)}$ (*the product of elements of* $\mathbb{F}_q(C)$), *we can omit* h_i*'s and* k_j*'s which belong to* $\mathbb{F}_q(x)$, *because the* x*-coordinate of each point of* $\mathrm{supp}\,\phi(\hat{E})$ *is an element of* $\mathbb{F}_{q^2}$.

The proof of Theorem 2 is similar to that for the supersingular elliptic curves [7, Section 3.2]. We describe the outline.

We first have the following result:

Lemma 1 ([6, Remark 3]).

With the notation above, we have

$$t_l(D, \zeta_8 \circ \eta(E)) = f_{q^2} \circ \phi(\hat{E})^{q^2-1}.$$

Next, setting $\hat{\pi}_q = \pi_q \circ \zeta_8^{2r}$, we have $\hat{\pi}_q \circ \pi_q = \pi_q \circ \hat{\pi}_q = q$ from Theorem 1, namely $\hat{\pi}_q$ is the dual of π_q.

For the proof of Theorem 2, we need two more lemmas.

Lemma 2.

With the notation above, we have

$$\hat{\pi}_q \circ \phi(\hat{E}) = \phi(\hat{E}).$$

Proof.

The equality follows from the direct computation. We note that the form of $\hat{E}$ is either $\hat{E} = \sum_{1 \le i \le w}(P_i)$ ($w = 1$ or 2) with $P_i \in \mathbb{F}_q(C)$ or $\hat{E} = (P) + (\pi_q(P))$ with $P \in \mathbb{F}_{q^2}(C) \setminus \mathbb{F}_q(C)$ because our curve has genus 2. □

[2] From Theorem 2 and this remark, the equality $\hat{t}_l(D, E)^2 = f_q \circ \phi(\hat{E})^{4(q^2-1)}$ holds for all $D, E \in \mathrm{Jac}_{\mathbb{F}_q}(C)[l] \setminus \{\mathrm{id}\}$. The pairing $\hat{t}_l^2$ keeps the same properties as those of $\hat{t}_l$ described in Theorem 2.

Lemma 3.
With the notation above, we have

$$(h \circ \hat{\pi}_q) = q(f_q),$$

where h is a function of $\mathbb{F}_q(C)$ such that $qD_q = D_{q^2} + (h)$.

Proof.
By definition, $\hat{\pi}_q$ is a bijection of degree q. Hence, by [9, Proposition 2.6. (Chapter II)], the equality $\hat{\pi}_q^*(\sum_{P \in C} n_P(P)) = q(\sum_{P \in C} n_P(\hat{\pi}_q^{-1}(P)))$ holds for every divisor $\sum_{P \in C} n_P(P)$ (for the definition of $\hat{\pi}_q^*$, see [9, p. 24 and p. 33]).
Therefore we have

$$\begin{aligned}
(h \circ \hat{\pi}_q) &= \hat{\pi}_q^*(h) \ \ (\text{by [9, Proposition 3.6. (Chapter II)] }) \\
&= \hat{\pi}_q^*(qD_q - D_{q^2}) \\
&= \hat{\pi}_q^*(q(\hat{\pi}_q \circ \pi_q(D)) - (\hat{\pi}_q \circ \pi_q(D_q))) \ \ (\text{by } \hat{\pi}_q \circ \pi_q = q) \\
&= q(q(\pi_q(D)) - \pi_q(D_q)) \\
&= q(qD - D_q) \ \ (\text{by } D,\, D_q \in \mathrm{Jac}_{\mathbb{F}_q}(C)) \\
&= q(f_q) \ \ (\text{by } qD = D_q + (f_q)). \ \ \square
\end{aligned}$$

Proof of Theorem 2.
The bilinearity of $\hat{t}_l$ and the property that $\hat{t}_l(D,\, E) \neq 1$ follow from [6, Theorem 4] and $\gcd(l, \rho) = 1$. For the latter assertion, from the definition of the functions f_q, f_{q^2}, h and Lemma 1, we have

$$\begin{aligned}
\hat{t}_l(D,\, E) &= \{(f_q^q h) \circ \phi\,(\hat{E})\}^{(q^2-1)\rho} \\
&= \{f_q^q \circ \phi\,(\hat{E}) \cdot (h \circ \hat{\pi}_q \circ \phi)(\hat{E})\}^{(q^2-1)\rho} \ \ (\text{by Lemma 2}) \\
&= \{f_q^{2q} \circ \phi\,(\hat{E})\}^{(q^2-1)\rho} \ \ (\text{by Lemma 3}) \\
&= f_q \circ \phi\,(\hat{E})^{2(q^2-1)} \\
&\qquad (\text{by } \rho q \equiv 1 \pmod{q^2+1} \text{ and } f_q \circ \phi\,(\hat{E}) \in \mathbb{F}_{q^4}^*). \ \ \square
\end{aligned}$$

3 Cost of the Ate pairing

In this section, we evaluate the cost for computing the Ate pairing $\hat{t}_l(D,\, E)$ described in the previous section [3]. The procedure of the Ate pairing is described in Table 1.

[3] The evaluation in this paper is more strict than that in [6].

Table 1. Ate pairing $\hat{t}_l(D,\, E)$

Input: Reduced divisors $D,\, E \in \mathrm{Jac}_{\mathbb{F}_q}(C)[l] \setminus \{\mathrm{id}\}$ **Output:** Ate pairing $\hat{t}_l(D,\, E)$.
Step 1: Represent $\frac{q+3}{8}$ as $\frac{q+3}{8} = \sum_{0 \le i \le k} r_i p^i$ with $0 \le r_i < p$ and $r_k > 0$. Decompose $\hat{E} = \sum_{1 \le i \le w} (P_i)$ $(w = 1$ or $2)$.
Step 2: Compute $\phi(P_i) = (\alpha_i,\, \beta_i)$ and $\alpha_i^2,\, \alpha_i^3,\, \beta_i^2,\, \alpha_i\beta_i,\, \alpha_i^2\beta_i,\, \alpha_i^3\beta_i$ $(1 \le i \le w)$.
Step 3: Compute the function $\ell(x, y) \in \mathbb{F}_q[x, y]$ s.t. $pD = D' + (\ell(x, y)/h(x))$ with the reduced divisor D' and $h(x) \in \mathbb{F}_q[x]$.
Step 4: $v \leftarrow 1$, $D' \leftarrow D$.
Step 5: for $i = 1$ to r (Recall $q = p^r$.) Compute the function $\ell(x, y) \in \mathbb{F}_q[x, y]$ s.t. $pD' = D'' + (\ell(x, y)/h(x))$ with the reduced divisor D'' and $h(x) \in \mathbb{F}_q[x]$. $v \leftarrow v^p \cdot \ell(\phi(\hat{E}))$, $D' \leftarrow D''$. **end for**
Step 6: $v \leftarrow (v^{q^2}/v)^2$, output v.

We mention that the parameters q and l should be chosen so that $q^4 \ge 2^{1024}$ and $l \ge 2^{160}$ in view of security.

By M (resp. I_{q^k}) we denote the cost of one multiplication on $\mathbb{F}_q$ (resp. the cost of one inversion on $\mathbb{F}_{q^k}$). Applying the Karatsuba method, we estimate the cost of one multiplication on $\mathbb{F}_{q^2}$ (resp. $\mathbb{F}_{q^4}$) as $3M$ (resp. $9M$), except for some special cases. For example, the multiplication of $a\alpha^{\frac{1}{2}}$ and $b\alpha^{\frac{1}{2}}$ for $a,\, b \in \mathbb{F}_q$ takes $1M$. Note that, for the evaluation in this paper, we ignore the cost of addition/subtraction (including doubling and the multiplication by $\alpha(= \pm 2)$) and the p-th power operation on $\mathbb{F}_q$, $\mathbb{F}_{q^2}$ and $\mathbb{F}_{q^4}$ (e.g. using normal bases).

We assume that $\deg \hat{E} = 2$ and that $\mathrm{supp}\, \hat{E}$ has no $\mathbb{F}_q$-rational point, that is, $\hat{E} = (P) + (\pi_q(P))$ with $P \in C(\mathbb{F}_{q^2}) \setminus C(\mathbb{F}_q)$. Otherwise, the computation of the Ate pairing is more simple.

Hereafter we use the notation "*distortion map*" not only for $\zeta_8 \circ \eta$ but also for the map ϕ.

3.1 Cost of the distortion map

With the notation above, we estimate the cost of the computation of $\phi(P)$ for $P \in C(\mathbb{F}_{q^2})$ (Step 2 in Table 1).

Table 2. Square root(s) for $\mathbb{F}_q$

Input: An element $A \in \mathbb{F}_q$ with $q = 5^r$ and r odd. **Output:** Square root(s) of A.
Step 1: If $A = 0$, then output 0.
Step 2: $B \leftarrow A^{\frac{q+3}{8}}$, $C \leftarrow B^2$ (Then we have $C = A^{\frac{q+3}{4}}$ and $A^{-1}C \in \mathbb{F}_5^*$.)
Step 3: If $C = A$, then output $\pm B$. If $C = -A$, then output $\pm 2B$. If $C = \alpha A$, then output $\pm 2B\alpha^{\frac{1}{2}}$. If $C = -\alpha A$, then output $\pm B\alpha^{\frac{1}{2}}$.

Before doing this, we should estimate the cost for decomposing E (with the form $\mathrm{div}(f(x), g(x))$) into $E = (P) + (\pi_q(P)) - 2(\mathcal{O})$. This task needs to solve a quadratic equation $f(x) = 0$ over $\mathbb{F}_q$, whose cost is dominated by the computation of square root(s) of the discriminant. The assumption $q \equiv 5 \pmod 8$ (recall $q = 5^r$ with r odd) gives an efficient method for computing the square root(s) of a given element in $\mathbb{F}_q$ (Table 2), which is a special case of the method in [3]. From this, the cost for computing the x-coordinate of the point P is regarded as that of one $\frac{q+3}{4}$-th power operation on $\mathbb{F}_q$. The computation of the y-coordinate of P needs one multiplication of an element of $\mathbb{F}_q$ and that of $\mathbb{F}_{q^2}$.

Given a point $P \in C(\mathbb{F}_{q^2})$, the procedure for computing $\phi(P)$ is described in Table 3, which takes $1I_q + 2 \cdot 1M + 3 \cdot 3M = 11M + 1I_q$. Here we use the fact $a^{-1} = f_0^{-1} \cdot a^q$ for $P = (a, b)$ and $E = \mathrm{div}(f(x), g(x))$ with $f(x) = x^2 + f_1 x + f_0$. Since the resulting point $\phi(P)$ is of the form $(E_1,\ E_2\alpha^{\frac{1}{4}})$ with $E_i \in \mathbb{F}_{q^2}^*$ $(i = 1, 2)$, the computations of E_1^2, E_1^3, $(E_2\alpha^{\frac{1}{4}})^2$ and $E_1^m(E_2\alpha^{\frac{1}{4}})$ $(1 \le m \le 3)$ take $6 \cdot 3M = 18M$ (the latter part of Step 2 in Table 1). Furthermore, if we compute $\phi(P)$ and the associated values, then we need not compute the values associated with $\phi(\pi_q(P))$ in the case of $\hat{E} = (P) + (\pi_q(P))$ with $P \in C(\mathbb{F}_{q^2}) \setminus C(\mathbb{F}_q)$ (see Subsection 3.2 for the detail).

3.2 Cost of substitution

In this subsection, we consider the cost of Step 5 in Table 1.

Given a function $\ell(x, y) \in \mathbb{F}_q[x, y]$ with the form $\ell(x, y) = \gamma y^2 + (sx^3 + tx^2 + ux + v)y + (-x^2 + cx + d)^3$ (Theorem 1) and $\phi(P) = (E_1,\ E_2\alpha^{\frac{1}{4}})$ with $E_i \in \mathbb{F}_{q^2}^*$ $(i = 1, 2)$, we estimate the cost of the computation of

Table 3. Distortion map ϕ

Input: A point $P = (a,\, b) \in C(\mathbb{F}_{q^2})$ with $a \neq 0$.
Output: The image $\phi(P)$.
Step 1: $A \leftarrow a^{-1}$, $B \leftarrow -A^p$.
$X \leftarrow B\alpha^{\frac{1}{2}}$.
Step 2: $C \leftarrow 2\alpha B^3 b^p \alpha^{\frac{1}{2}}$.
$Y \leftarrow C\alpha^{\frac{1}{4}}$.
Step 3: Output $(X,\, Y)$.

$\ell(\phi(\hat{E})) = \ell(\phi(P) + \phi(\pi_q(P)))$. We note that $\ell(x, y)$ can be computed by performing only the p-th power operations and addition/subtraction operations on $\mathbb{F}_q$ if we have done Step 3 (by Proposition 1), and that we perform Step 5 using the values obtained in Step 2. By this reason, it costs $6 \cdot 2M + 2 \cdot 3M = 18M$ to compute $\ell(\phi(P))$. After the computation of $\ell(\phi(P))$, it costs only $2 \cdot 3M = 6M$ for computing $\ell(\phi(\pi_q(P)))$ because we have $\ell(\phi(\pi_q(P))) = -(\gamma B^2)^q + \alpha^r(-sA^3B + tA^2B - uAB + vB)^q + (-A^2 - cA + d)^{3q}$ if $\phi(P) = (A,\, B)$. Here we use the fact $\phi \circ \pi_q = \zeta_8^{2r} \circ \pi_q \circ \phi$, namely $\phi(\pi_q(P)) = (-A^q,\ \alpha^r B^q)$. So it takes $(18 + 6)M + 9M = 33M$ to compute $\ell(\phi(\hat{E}))$.

We remark that, for each reduced divisor $E \in \mathrm{Jac}_{\mathbb{F}_q}(C)[l] \setminus \{\mathrm{id}\}$, we have $\mathrm{supp}\, \phi(\hat{E}) \cap C(\mathbb{F}_{q^2}) = \emptyset$ and $\mathrm{supp}(\ell(x, y)) \subset C(\mathbb{F}_{q^2})$ by the definitions of ϕ and $\ell(x, y)$. This gives $\mathrm{supp}(\ell(x, y)) \cap \mathrm{supp}\, \phi(\hat{E}) = \emptyset$, which means $\ell(\phi(\hat{E})) \neq 0, \infty$.

3.3 Total cost

In this subsection, we evaluate the total cost of the computation of the Ate pairing by applying the procedure in Table 1.

In Steps $1, 5$, we set $k = r = 120$ (cf. $\lceil \log_5 2^{256} \rceil = 111$) [4] and assume that r_i's in Step 1 are uniformly distributed on the set $\{0, 1, \ldots, p - 1\}$.

For Step 1, we estimate the cost for computing r_i's as $1M$ (because it costs about $(\log_2 \frac{q+3}{8})^2$ bit operations), and the cost for the decomposition of the reduced divisor E as $(3 \cdot 1 + 120 \cdot \frac{9}{5} + 2)M$ (by Subsection 3.1). The first term $3 \cdot 1M$ corresponds to the cost for the precomputation of the repeated p-th-power-and-multiply algorithm, and the second one for the algorithm and the last one for the computation of the y-coordinate. Thus, Step 1 takes $222M$.

[4] If $r = 113$, then the value $q^2 + 1$ has a 173-bit and a 348-bit prime factors.

Table 4. Cost of pairings for genus-2 hyperelliptic curves with embedding degree four

curve/$\mathbb{F}_q$	pairing (method)	cost
$y^2 = x^5 + a$,	Tate ([2])	$19851M + 240I_q$
$q = p \equiv 2, 3 \pmod 5$	Tate ([8])	$11020M + 162I_q$
$y^2 = x^5 - \alpha x$,	Tate (ours)	$10350M + 1I_q + 1I_{q^4}$
$q = 5^r$	Ate (ours)	$5319M + 1I_q + 1I_{q^4}$

For Step 2, it costs $11M + 1I_q + 18M = 29M + 1I_q$ by the argument of Subsection 3.1.

For Step 3, it costs $10M$ from Theorem 1.

For Step 5, it costs $33M + 9M$ for rewriting the value v, that is, the computation of $v^p \cdot \ell(\phi(\hat{E}))$. Therefore, Step 5 takes $120 \cdot 42M = 5040M$.

For Step 6, it costs $2 \cdot 9M + 1I_{q^4}$.

Consequently, we estimate the cost for computing the Ate pairing $\hat{t}_l(D, E)$ as $5319M + 1I_q + 1I_{q^4}$.

We list the cost of pairings for genus-2 hyperelliptic curves with embedding degree four (Table 4), which implies that the sizes of the definition fields are the same under the same level of security [5].

4 Conclusions

In this paper, we showed the Ate pairing can be applied to the curve $y^2 = x^5 - \alpha x$ and evaluated the cost of the pairing. The resulting cost for the Ate pairing is about 50% saving over that for the Tate pairing.

Acknowledgments

We are grateful to Steven Galbraith for valuable comments on the earlier version [6] and for giving us the motivation for this work.

References

1. P. S. L. M. Barreto, S. Galbraith, C. Ó hÉigeartaigh and M. Scott, *Efficient pairing computation on supersingular abelian varieties*, IACR Cryptology ePrint Archive, 2004/375, 2004.

[5] The evaluations in [2] and [8] exclude the cost for the final raising, but ours includes its cost. We cannot say that our method is always far more efficient than the method in [2] and [8] because the types of the definition fields are different.

2. Y. Choie and E. Lee, *Implementation of Tate pairing on hyperelliptic curves of genus* 2, International Conference on Information Security and Cryptology (ICISC 2003), Lecture Notes in Computer Science **2971**, pp. 97–111, Springer-Verlag, 2004.
3. H. Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Math., vol. **138**, Springer-Verlag, Berlin Heidelberg, 1993.
4. I. Duursma and K. Sakurai, *Efficient algorithms for the Jacobian variety of hyperelliptic curves* $y^2 = x^p - x + 1$ *over a finite field of odd characteristic* p, Coding theory, cryptography and related areas, pp. 73–89, Springer, Berlin, 2000.
5. I. Duursma and H. S. Lee, *Tate pairing implementation for hyperelliptic curves* $y^2 = x^p - x + d$, Advances in Cryptology - ASIACRYPT 2003, Lecture Notes in Computer Science **2894**, pp. 111–123, Springer-Verlag, 2003.
200
6. R. Harasawa, Y. Sueyoshi, and A. Kudo, *Tate pairing for* $y^2 = x^5 - \alpha x$ *in characteristic five*, IACR Cryptology ePrint Archive, 2006/114, 2006.
7. F. Hess, N. P. Smart and F. Vercauteren, *The Eta pairing revisited*, IACR Cryptology ePrint Archive, 2006/110, 2006.
8. C. Ó hÉigeartaigh and M. Scott, *Pairing calculation on supersingular genus 2 curves*, IACR Cryptology ePrint Archive, 2006/005, 2006.
9. J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Math., vol. **106**, Springer-Verlag, New York, 1986.