Tate 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

In this paper, for the genus-2 hyperelliptic curve $y^2 = x^5 - \alpha x$ ($\alpha = \pm 2$) defined over finite fields of characteristic five, we construct a distortion map explicitly, and show the map indeed gives an input for which the value of the Tate pairing is not trivial. Next we describe a computation of the Tate pairing by using the proposed distortion map. Furthermore, we also see that this type of curve is equipped with a simple quintuple operation on the Jacobian group, which leads to giving an improvement for computing the Tate pairing. We indeed show that, for the computation of the Tate pairing for genus-2 hyperelliptic curves, our method is about twice as efficient as a previous work.

Keywords: Distortion map, Tate pairing, Hyperelliptic curves

1 Introduction

The Tate pairing was originally used as a tool for reducing the discrete logarithm problem on algebraic curves over a finite field to that on the multiplicative group on an extension field of the base field [9]. However, as is well known, the properties of the pairing (i.e., bilinearity and nondegeneracy) give also various cryptographic applications, for example one-round tripartite Diffie-Hellman protocol [11], ID-based encryption scheme [2] and short signature [3].

In order to realize these pairing-based protocols, we need a choice of curves suitable for ones. The main considerations we should notice are as follows:

1. the parameter, called *embedding degree*, is not too large,
2. an efficient Jacobian group arithmetic is equipped,

3. a distortion map, that is, a method for giving an input for which the value of the pairing is not trivial, is equipped.

The first topic concerns the computable feasibility of the Tate pairing, and the second one the efficient computation of the pairing, and the third one the practical use of pairing based protocols.

The main theme of this paper is about the third topic (i.e., the construction of a distortion map). For a class of supersingular elliptic curves, a distortion map for each of them can be explicitly constructed [1]. However, distorsion maps for only a few classes other than the one above have been explicitly constructed as long as we know. Especially, for curves of genus $g \geq 2$, it is hard to construct a distortion map as compared with $g = 1$ because the subgroup of l-torsion points of the Jacobian group is isomorphic to $(\mathbb{Z}/l\mathbb{Z})^{2g}$ for a prime l different from the characteristic of the base field. In other words, giving an endomorphism not defined over the base field is not sufficient to obtain a distortion map. Here is a remark that the paper [10] shows there exists a distortion map for supersingular algebraic curves.

In this paper, we explicitly construct a distortion map for the genus-2 supersingular hyperelliptic curve $y^2 = x^5 - \alpha x$ $(\alpha = \pm 2)$ over finite fields of characteristic five, and show that the map indeed gives an input for which the value of the Tate pairing is not trivial. And we describe a computation of the Tate pairing by using the proposed distortion map.

Note that, for a class of curves $y^2 = x^p - x + d$ over finite fields of characteristic p, the paper [8] gives an endomorphism not defined over the base field, but does not prove the endomorphism indeed becomes a distortion map. Furthermore, for a class of curves $y^2 = x^5 + a$ over prime fields $\mathbb{F}_p$ with $p \equiv 2, 3 \pmod 5$, the paper [5] constructs a distortion map and the paper [10] gives the proof that the map indeed becomes a distortion map under a certain condition which seems to hold in almost all cases.

We further see that the curve $y^2 = x^5 - \alpha x$ is equipped with a simple formula of quintuple operation (a variant of [7]). This fact leads to giving an improvement for computing the Tate pairing. We indeed show that, for the computation of the Tate pairing for genus-2 hyperelliptic curves, the computational cost using our method is about a half of that using the method of [5]. The reason why we compare our method with the one in [5] is that both of them consider genus-2 hyperelliptic curves with embedding degree four.

The remainder of this paper is organized as follows: In Section 2, we describe the mathematical facts required in this paper. In Section 3, we construct a distortion map for the hyperelliptic curve $y^2 = x^5 - \alpha x$. In Section 4, we describe some improvements of the computation of the Tate pairing by using the proposed distortion map. In Section 5, we estimate the cost for computing the Tate pairing by using the method. In Section 6, we give the conclusions.

2 Preliminaries

In this section, we describe the mathematical facts required in this paper. For more details, see [4] [9] [12] [14].

2.1 Hyperelliptic Curves

Let $p > 2$ be an odd prime and $q = p^r$ with r a positive integer. Let $\mathbb{F}_q$ be a finite field with q elements, and $C/\mathbb{F}_q$ a hyperelliptic curve of genus g defined by $y^2 = F(x)$ with $\deg F(x) = 2g+1$, and $\mathcal{O}$ the point at infinity.

By $\mathrm{Jac}(C)$ (resp. $\mathrm{Jac}_{\mathbb{F}_q}(C)$) we denote the *Jacobian group* of C (resp. the *Jacobian group* of C *defined over* $\mathbb{F}_q$). As is well known, each element of $\mathrm{Jac}(C)$ is represented as the form, called *Mumford's representation*, $D = \mathrm{div}(a(x), b(x))$ with $\deg a(x) \le g$, $\deg b(x) < \deg a(x)$, and $a(x) | b(x)^2 - F(x)$. If we set $a(x) = \prod_i (x - \alpha_i)$ and $P_i = (\alpha_i, b(\alpha_i))$ for $D = \mathrm{div}(a(x), b(x))$, then it is well known that D corresponds to the divisor $\sum_i (P_i) - \deg a(x)\,(\mathcal{O})$.

Let π_q denote the q-th power Frobenius endomorphism of $\mathrm{Jac}(C)$. Then its characteristic polynomial, say $\phi_q(t)$, is of the form

$$\phi_q(t) = \sum_{0 \le i \le 2g} a_i t^i \quad (a_i \in \mathbb{Z}).$$

For the a_i's above, it satisfies that $a_{2g} = 1$, $a_0 = q^g$, and for $1 \le i \le g$, $ia_{2g-i} - \sum_{1 \le k \le i} (\#C(\mathbb{F}_{q^k}) - q^k - 1) a_{2g-i+k} = 0$, $a_i = a_{2g-i} q^{g-i}$, where $C(\mathbb{F}_{q^k})$ denotes the set of $\mathbb{F}_{q^k}$-rational points on C. Furthermore, if we set $\phi_q(t) = \prod_{1 \le i \le 2g} (t - w_i)$, then it turns out that $\phi_{q^k}(t) = \prod_{1 \le i \le 2g} (t - w_i^k)$ and $\#\mathrm{Jac}_{\mathbb{F}_{q^k}}(C) = \phi_{q^k}(1)$.

2.2 Tate Pairing

Let $C/\mathbb{F}_q$ be an algebraic curve and l an odd prime with $l \not| q$ and $l | \#\mathrm{Jac}_{\mathbb{F}_q}(C)$. The *embedding degree* is defined as the smallest positive integer k such that $l|q^k-1$. Then there exists a nondegenerate bilinear map (so-called the *Tate pairing*)

$$t_l : \mathrm{Jac}_{\mathbb{F}_{q^k}}(C)[l] \times \ \mathrm{Jac}_{\mathbb{F}_{q^k}}(C)/l\,\mathrm{Jac}_{\mathbb{F}_{q^k}}(C) \longrightarrow \mu_l,$$

via

$$t_l(D,E) = f_D(E')^{\frac{q^k-1}{l}},$$

where $\mathrm{Jac}_{\mathbb{F}_{q^k}}(C)[l]$ is the subgroup consisting of l-torsion points of $\mathrm{Jac}_{\mathbb{F}_{q^k}}(C)$, $\mu_l \subset \mathbb{F}_{q^k}$ the set of l-th roots of unity, f_D a function such that $(f_D) = lD$, and E' a divisor such that $E' \sim E$ and $\mathrm{supp}D \cap \mathrm{supp}E' = \emptyset$.

For D, E as above, an endomorphism ϕ of $\mathrm{Jac}(C)$ is said to be a *distortion map* if $t_l(D, \phi(E)) \neq 1$ holds.

In general, we use Miller's algorithm [13] for computing the Tate pairing.

3 Distortion Map for $y^2 = x^5 - \alpha x$

3.1 Character of $y^2 = x^5 - \alpha x$

From now on, except for Theorem 2, we set $p = 5$ and $q = p^r$. Now we consider the genus-2 hyperelliptic curve defined by

$$C/\mathbb{F}_q:\ y^2 = x^5 - \alpha x \quad (\alpha = \pm 2).$$

Firstly, there exists a simple quintuple operation on $\mathrm{Jac}(C)$ as follows, which is a variant of [7]:

Theorem 1.
For $P = (a,b) \in C$, we have

$$p((P) - (\mathcal{O})) = ((-a^{p^2},\, \alpha b^{p^2})) - (\mathcal{O}) + (h_P(x,y)/k_P(x)),$$

where we define $h_P(x,y) = b^p y + (\alpha x - a^p)^{\frac{p+1}{2}}$ and $k_P(x) = x + a^{p^2}$.

This theorem gives the following formulae:

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

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

where

$$\begin{aligned}
\gamma &:= ((a_0b_1 - a_1b_0)b_1 + b_0^2)^p, \\
f_1(x) &:= \alpha(a_1b_1 - 2b_0)^p x^3 - 2(2a_0b_1 - a_1b_0)^p x^2 \\
&\quad + 2\alpha(a_0a_1b_1 - (a_1^2 - 2a_0)b_0)^p x \\
&\quad - ((a_1^2 - 2a_0)a_0b_1 - (a_1^2 + 2a_0)a_1b_0)^p, \\
f_0(x) &:= (-x^2 + \alpha a_1^p x + a_0^p)^3.
\end{aligned}$$

Hence we need ten multiplications (i.e., a_0b_1, a_1b_0, $(a_0b_1 - a_1b_0)b_1$, b_0^2, a_1b_1, $a_0(a_1b_1)$, a_1^2, $(a_1^2 - 2a_0)b_0$, $(a_1^2 - 2a_0)(a_0b_1)$, $(a_1^2 + 2a_0)(a_1b_0)$) and seven p-th power operations to compute γ, $f_1(x)$ and $f_0(x)$.

Theorem 1 comes from the following theorem.

Theorem 2.
Let p be an odd prime, and $\overline{\mathbb{F}}_p$ a fixed algebraic closure of $\mathbb{F}_p$, and $C/\overline{\mathbb{F}}_p$ a hyperelliptic curve defined by $y^2 = x^p + \alpha x + \beta$ with $\alpha \neq 0$. For $P = (a, b) \in C$, we set $Q = (\alpha^{-(p+1)}(a^{p^2} + \beta^p - \alpha^p\beta),\ \alpha^{-p(p+1)/2}\, b^{p^2})$, denoted by $Q = (x_Q, y_Q)$ for short, and $h(x, y) = b^p y - (\alpha x + a^p + \beta)^{(p+1)/2}$. Then we have

$$p((P) - (\mathcal{O})) = (\widetilde{Q}) - (\mathcal{O}) + (h(x, y)/(x - x_Q)),$$

where we define $\widetilde{Q} = (x_Q, -y_Q)$.

Proof of Theorem 2. First, we see from the direct computation that $y_Q^2 = x_Q^p + \alpha x_Q + \beta$, that is, Q is a point on C.

In the case $b = 0$, we have $p((P) - (\mathcal{O})) = (P) - (\mathcal{O}) + ((x - a)^{(p-1)/2})$ because of $2((P) - (\mathcal{O})) = (x - a)$. Therefore we obtain the desired result.

In the case $b \neq 0$, we consider the support of $h(x, y)$. To do this, we compute $h(x, y)h(x, -y)$ as follows:

$$\begin{aligned}
h(x, y)h(x, -y) &= (a^p + \alpha x + \beta)^{p+1} - b^{2p}y^2 \\
&= (b^2 + \alpha(x - a))^{p+1} - b^{2p}y^2 \\
&= b^{2p}(b^2 - y^2 + \alpha x - \alpha a) + \alpha^{p+1}(x - a)^{p+1} + \alpha^p b^2 (x - a)^p \\
&= b^{2p}(-x^p + a^p) + (x - a)^p(\alpha^{p+1}(x - a) + \alpha^p b^2) \\
&= \alpha^{p+1}(x - a)^p(x - x_Q),
\end{aligned}$$

and obtain $y = b$ (resp. y_Q) by solving $h(a, y) = 0$ (resp. $h(x_Q, y) = 0$). Therefore, it turns out that $(h(x, y)) = p(P) + (Q) - (p + 1)(\mathcal{O})$. From this result and $(x - x_Q) = (Q) + (\widetilde{Q}) - 2(\mathcal{O})$, we complete the proof. $\square$

From Theorem 1, we immediately obtain the following result, which plays an important role for an efficient computation of the Tate pairing for $y^2 = x^p - \alpha x$.

Proposition 1.
Let $D = \mathrm{div}(f(x), g(x))$ be a reduced divisor with $\mathrm{deg} f(x) = 2$, 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 $\ell_i(x,y) = \gamma_i y^2 + (s_i x^3 + t_i x^2 + u_i x + v_i)y + (-x^2 + c_i x + d_i)^3$ (see Theorem 1). Then, for each coefficient of ℓ_i, we have

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

Next we consider the characteristic polynomial $\phi_q(t)$ of the q-th power Frobenius endomorphism of $\mathrm{Jac}(C)$. Since the map $x \mapsto x^p - \alpha x$ turns out to be an automorphism of both $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$ as additive groups, we have $\#C(\mathbb{F}_p) = p + 1$, $\#C(\mathbb{F}_{p^2}) = p^2 + 1$, which implies

$$\phi_q(t) = \begin{cases} (t - \sqrt{q})^4 & (\, r \equiv 0 \pmod 8), \\ (t + \sqrt{q})^4 & (\, r \equiv 4 \pmod 8), \\ (t^2 + q)^2 & (\, r \equiv 2, 6 \pmod 8), \\ t^4 + q^2 & (\, r\text{: odd}). \end{cases} \tag{1}$$

Therefore, if r is odd and $l \neq p$ an odd prime with $l | \#\mathrm{Jac}_{\mathbb{F}_q}(C) = q^2 + 1$, then the embedding degree is four.

For the remainder of this paper, we set r and l as above because the other cases have the embedding degrees smaller than four, which gets less cryptographic interest.

3.2 Construction of a Distortion Map

Let the notation be the same as in the previous subsection. In this subsection, we construct a distortion map for $C/\mathbb{F}_q : \; y^2 = x^5 - \alpha x$ in characteristic five.

Firstly, it is easy to see that there exist morphisms π_p, ζ_8, ζ_5 from the curve above to itself defined by

$$\begin{aligned} \pi_p &: (x,y) \mapsto (x^p, \, y^p) \quad (p\text{-th power Frobenius}), \\ \zeta_8 &: (x,y) \mapsto (\alpha x, \, \alpha^{\frac{1}{2}} y), \\ \zeta_5 &: (x,y) \mapsto (x + \alpha^{\frac{1}{4}}, \, y), \end{aligned}$$

where $\alpha^{\frac{1}{4}}$ is a fixed fourth root of α and $\alpha^{\frac{1}{2}} = (\alpha^{\frac{1}{4}})^2$. Note that $\alpha^{\frac{1}{4}}$ is an element of $\mathbb{F}_{q^4} \setminus \mathbb{F}_{q^2}$ because $(\alpha^{\frac{1}{4}})^{q^2} = -\alpha^{\frac{1}{4}}$. Here we write the same symbol for the endomorphism of $\mathrm{Jac}(C)$ induced from each morphism above.

By definition, we see that ζ_8 (resp. ζ_5) is regarded as a primitive eighth (resp. fifth) root of unity in the endomorphism ring of $\mathrm{Jac}(C)$, and that the following relations are satisfied:

$$\begin{cases} \pi_p^i \circ \zeta_8^j = (-1)^{ij} \zeta_8^j \circ \pi_p^i \ , \\ \pi_p \circ \zeta_5 = \quad \zeta_5^{\alpha} \circ \pi_p \ , \\ \zeta_8 \circ \zeta_5 = \quad \zeta_5^{\alpha} \circ \zeta_8 \ , \\ \quad \pi_p^2 \quad = \quad -\zeta_8^2 \circ p \ . \end{cases} \tag{2}$$

In order to construct a distortion map, it is crucial to find a basis of $\mathrm{Jac}_{\mathbb{F}_{q^4}}(C)/l\,\mathrm{Jac}_{\mathbb{F}_{q^4}}(C)$ over $\mathbb{Z}/l\mathbb{Z}$. To achieve this, we begin with considering the eigenvalues of the q-th power Frobenius π_q on $\mathrm{Jac}(C)[l]$.

For our curve $y^2 = x^5 - \alpha x$, the characteristic polynomial of π_q is $t^4 + q^2$. In this case, the following fact is known:

Lemma 1 [10].
Let $C/\mathbb{F}_q$ be a genus-2 hyperelliptic curve for which the characteristic polynomial of π_q is $t^4 + q^2$, and l an odd prime with $l | q^2 + 1$. Then the eigenvalues of π_q on $\mathrm{Jac}(C)[l]$ are ± 1, $\pm q$.

Proof of Lemma 1. Since $q^2 \equiv -1 \pmod{l}$, we have

$$\begin{aligned} t^4 + q^2 &\equiv (t^2 - 1)(t^2 + 1) \\ &\equiv (t+1)(t-1)(t+q)(t-q) \pmod{l}. \ \square \end{aligned}$$

Next, for each eigenvalue given in Lemma 1, we find its corresponding eigenspace. When we define $\eta = (\zeta_5 - \zeta_5^{-1}) + q \circ (\zeta_5^{\alpha^r} - \zeta_5^{-\alpha^r})$, the following lemma holds:

Lemma 2.
For $D \in \mathrm{Jac}_{\mathbb{F}_q}(C)$, we have

$$\pi_q \circ \eta(D) = -q \circ \eta(D).$$

Proof of Lemma 2. Let m be the order of D. Then m divides $\#\mathrm{Jac}_{\mathbb{F}_q}(C) = q^2 + 1$. Hence, from (2), we have

$$\pi_q \circ \eta(D) = \{(\zeta_5^{\alpha^r} - \zeta_5^{-\alpha^r}) + q \circ (\zeta_5^{\alpha^{2r}} - \zeta_5^{-\alpha^{2r}})\}(\pi_q(D))$$

$$
\begin{aligned}
&= \{(\zeta_5^{\alpha^r} - \zeta_5^{-\alpha^r}) + q \circ (\zeta_5^{-1} - \zeta_5)\}(D) \\
&\qquad\qquad\qquad\qquad (\text{by } \alpha^2 \equiv -1 \pmod 5) \\
&= \{-q^2 \circ (\zeta_5^{\alpha^r} - \zeta_5^{-\alpha^r}) - q \circ (\zeta_5 - \zeta_5^{-1})\}(D) \\
&\qquad\qquad\qquad\qquad (\text{by } 1 \equiv -q^2 \pmod m) \\
&= -q \circ \eta(D). \quad \square
\end{aligned}
$$

From (2) and Lemma 2, we can obtain a basis of $\mathrm{Jac}_{\mathbb{F}_{q^4}}(C)/l\mathrm{Jac}_{\mathbb{F}_{q^4}}(C)$ over $\mathbb{Z}/l\mathbb{Z}$ as follows:

Theorem 3.
Let id *be the identity element of* $\mathrm{Jac}(C)$*. We assume* $l||q^2+1$ *and* $D \in \mathrm{Jac}_{\mathbb{F}_q}(C)[l] \setminus \{\mathrm{id}\}$*. Then the set* $\{\, D, \zeta_8(D), \eta(D), \zeta_8 \circ \eta(D) \,\}$ *forms a basis over* $\mathbb{Z}/l\mathbb{Z}$ *of both* $\mathrm{Jac}(C)[l]$ *and* $\mathrm{Jac}_{\mathbb{F}_{q^4}}(C)/l\mathrm{Jac}_{\mathbb{F}_{q^4}}(C)$.

Proof of Theorem 3. It is sufficient to show $\eta(D) \neq \mathrm{id}$. Indeed, if it holds, then we see from (2) and Lemma 2 that $\langle D\rangle$, $\langle \zeta_8(D)\rangle$, $\langle \eta(D)\rangle$, $\langle \zeta_8 \circ \eta(D)\rangle$ are the eigenspaces corresponding to the distinct π_q-eigenvalues $1, -1, -q, q$, respectively. Therefore, they are linearly independent over $\mathbb{Z}/l\mathbb{Z}$, which implies that they form a basis of $\mathrm{Jac}(C)[l]$ because $\mathrm{Jac}(C)[l]$ is isomorphic to $(\mathbb{Z}/l\mathbb{Z})^4$. Furthermore, the characteristic polynomial of the q^4-th power Frobenius is $(t+q^2)^4$ from (1), which implies $\mathrm{Jac}_{\mathbb{F}_{q^4}}(C) \cong (\mathbb{Z}/(q^2+1)\mathbb{Z})^4$ [15]. From this fact and the assumption $l||q^2+1$, we obtain the desired result for $\mathrm{Jac}_{\mathbb{F}_{q^4}}(C)/l\mathrm{Jac}_{\mathbb{F}_{q^4}}(C)$.

Let $D \in \mathrm{Jac}_{\mathbb{F}_q}(C)[l] \cap \mathrm{Ker}\,\eta$, and $\lambda = 2(\zeta_5 + \zeta_5^{-1}) + 1$. Since

$$
\begin{aligned}
N &:= \prod_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})} \eta^\sigma \\
&= \prod_{i=1,2} \{(\zeta_5^i - \zeta_5^{-i}) + q(\zeta_5^{i\alpha^r} - \zeta_5^{-i\alpha^r})\}^2 \\
&= \begin{cases} \lambda^2(q^2+q-1)^2 & (\alpha^r \equiv 2 \pmod 5), \\ \lambda^2(q^2-q-1)^2 & (\alpha^r \equiv -2 \pmod 5), \end{cases} \\
&= \begin{cases} 5\{q^2+1+(q-2)\}^2 & (\alpha^r \equiv 2 \pmod 5), \\ 5\{q^2+1-(q+2)\}^2 & (\alpha^r \equiv -2 \pmod 5), \end{cases}
\end{aligned}
$$

and $\gcd(l, N) = \gcd(l, q \mp 2) = 1$, we obtain $D \in \mathrm{Jac}_{\mathbb{F}_q}(C)[l] \cap \mathrm{Jac}(C)[N] = \{\mathrm{id}\}$, which completes the proof of the theorem. (Indeed, if $l | q \mp 2$, then $l | (q+2)(q-2) = (q^2+1) - 5$, which implies $l|5$. This contradicts with $l|q^2+1$.) $\square$

From Theorem 3 above and Lemma 3.3 of [10], we can obtain the following result:

Theorem 4.

With the notation above, if l is an odd prime with $l||q^2+1$, then the map

$$\widetilde{t_l} : \mathrm{Jac}_{\mathbb{F}_q}(C)[l] \times \ \mathrm{Jac}_{\mathbb{F}_q}(C)[l] \longrightarrow \mu_l,$$

via

$$\widetilde{t_l}(D,\, E) = t_l(D,\, \zeta_8 \circ \eta(E))$$

is bilinear and has the property that $\widetilde{t_l}(D, E) \neq 1$ holds whenever $D, E \neq$ id.

Proof of Theorem 4. The proof is the same as in Lemma 3.3 of [10]. We describe only the outline (see Lemma 3.3 of [10] for more details). The bilinearity follows from the definition of $\widetilde{t_l}$. For the second assertion, since it turns out $t_l(D',\, E')^q = t_l(\pi_q(D'),\, \pi_q(E'))$ for $D' \in \mathrm{Jac}_{\mathbb{F}_{q^k}}(C)[l]$ and $E' \in \mathrm{Jac}_{\mathbb{F}_{q^k}}(C)$, we see $t_l(D,\, E) = t_l(D,\, \zeta_8(E)) = t_l(D,\, \eta(E)) = 1$. Hence the desired result follows from Theorem 3 and the non-degeneracy of the Tate pairing. $\square$

As a result, from Theorem 4, the endmorphism $\zeta_8 \circ \eta$ becomes a distortion map for $\mathrm{Jac}_{\mathbb{F}_q}(C)[l] \setminus \{\mathrm{id}\}$.

3.3 Image of the Distortion Map $\zeta_8 \circ \eta$

In this subsection, we explicitly describe the image of $\mathrm{Jac}_{\mathbb{F}_q}(C)$ under the distortion map $\zeta_8 \circ \eta$ constructed in the previous subsection.

When we represent each element of $\mathrm{Jac}_{\mathbb{F}_q}(C)$ as $\mathrm{div}\,(a(x), b(x)) = \sum_i (\alpha_i, \beta_i) - \deg a(x)\,(\mathcal{O})$ $(\deg a(x) \leq 2)$, it is easy to see that each (α_i, β_i) becomes an $\mathbb{F}_{q^2}$-rational point on C. Therefore, in order to describe the image of $\zeta_8 \circ \eta$, it is sufficient to consider only $\zeta_8 \circ \eta((P) - (\mathcal{O}))$ for $P \in C(\mathbb{F}_{q^2})$.

Theorem 5.

For $P = (a, b) \in C(\mathbb{F}_{q^2})$, we have

$$\zeta_8 \circ \eta\Big((P) - (\mathcal{O})\Big) \sim \begin{cases} \Big((0,\,0)\Big) - (\mathcal{O}) & (a = 0), \\ (\phi(P)) + \Big((0,\,0)\Big) - 2\,(\mathcal{O}) & (a \neq 0), \end{cases}$$

where $\phi(P) := (-a^{-5}\alpha^{\frac{1}{2}},\, -2a^{-15}b^5\alpha\alpha^{\frac{3}{4}})$ for $a \neq 0$.

Proof of Theorem 5. We set four points P_i $(1 \le i \le 4)$ on C as follows:

$$\begin{aligned} P_1 &= (\alpha a + \alpha\alpha^{\frac{1}{4}},\ \alpha^{\frac{1}{2}} b), & P_2 &= (\alpha a - \alpha\alpha^{\frac{1}{4}},\ -\alpha^{\frac{1}{2}} b), \\ P_3 &= (-\alpha a + \alpha^{r+1}\alpha^{\frac{1}{4}},\ \alpha^r\alpha^{\frac{1}{2}} b), & P_4 &= (-\alpha a - \alpha^{r+1}\alpha^{\frac{1}{4}},\ -\alpha^r\alpha^{\frac{1}{2}} b). \end{aligned}$$

Then, from the definition of the endomorphism $\zeta_8 \circ \eta$ and the fact $q = (\zeta_8^2 \circ \pi_p^2)^r = \pi_q^2 \circ \zeta_8^{2r}$ (see (2)) and $(\alpha^{\frac{1}{4}})^{q^2} = -\alpha^{\frac{1}{4}}$, we see

$$\zeta_8 \circ \eta((P) - (\mathcal{O})) = \sum_{1 \le i \le 4} (P_i) - 4(\mathcal{O}).$$

Here we should notice that x-coordinates of the P_i's are distinct because $\alpha^r \ne \pm 1$ and $a \in \mathbb{F}_{q^2}$.

In the case $a = 0$, we can obtain the desired result from $(y) = \sum_{1 \le i \le 4}(P_i) - 4(\mathcal{O}) + ((0,\ 0)) - (\mathcal{O})$.

In the case $a \ne 0$, there exists a unique function of the form $h(x, y) = y - (c_3x^3 + c_2x^2 + c_1x + c_0)$ such that $h(P_i) = 0$ $(1 \le i \le 4)$. And when we set $A = (a^4 - \alpha)\alpha^r\alpha^{\frac{1}{2}} \ne 0$ [1], it turns out $Ac_3 = -2a^2b\alpha^{r+1}\alpha^{\frac{3}{4}}$, $Ac_2 = -ab\alpha^{r+1}\alpha^{\frac{1}{4}}$, $Ac_1 = -2a^4b\alpha^{r+1}\alpha^{\frac{3}{4}} - b\alpha^r\alpha^{\frac{3}{4}}$, and $Ac_0 = 0$.

Since we have

$$\begin{aligned} A^2h(x, y)h(x, -y) &= -(a^9\alpha\alpha^{\frac{1}{2}} + a^5\alpha^{\frac{1}{2}})x^6 + (a^4 - \alpha)x^5 \\ &\quad - (2a^{11}\alpha\alpha^{\frac{1}{2}} + 2a^7\alpha^{\frac{1}{2}})x^4 - (a^{10}\alpha - a^6 + 2a^2\alpha)x^3 \\ &\quad - (a^{13}\alpha\alpha^{\frac{1}{2}} + 2a^9\alpha^{\frac{1}{2}} + a\alpha^{\frac{1}{2}})x^2 + (a^8 - 2a^4\alpha - 1)x \\ &= -(a^4 - \alpha)(x^2 - 2a\alpha x - a^2 + \alpha^{\frac{1}{2}}) \\ &\quad (x^2 + 2a\alpha x - a^2 - \alpha^{\frac{1}{2}})(a^5\alpha\alpha^{\frac{1}{2}}x - 1)x, \end{aligned}$$

we obtain $(h(x, y)) = \sum_{1 \le i \le 4}(P_i) - 4(\mathcal{O}) + (\widetilde{\phi(P)}) + ((0,\ 0)) - 2(\mathcal{O})$, which completes the proof (see Theorem 2 for the symbol $\widetilde{\ }$). $\square$

4 Computation of the Tate Pairing

We use the same notation as in the previous section unless we specify. In this section, for the actual computation of the Tate pairing on $y^2 = x^5 - \alpha x$, we remark there exist some improvements in the same way as those proposed so far.

[1] The value A is the determinant of the coefficient matrix for the simultaneous equations with unknown c_i's. And the assumption $a \in \mathbb{F}_{q^2}$ implies $a^4 - \alpha \ne 0$.

We first introduce the following method for an efficient computation of the Tate pairing on genus-2 hyperelliptic curves with the embedding degree $k \geq 2$.

Theorem 6 [5].

Let $C/\mathbb{F}_q$ be a genus-2 hyperelliptic curve, l an odd prime with $l | \#\mathrm{Jac}_{\mathbb{F}_q}(C)$ and $l \not| q$. We assume that the embedding degree $k \geq 2$. Let D (resp. E) be an element of $\mathrm{Jac}_{\mathbb{F}_q}(C)[l]$ (resp. $\mathrm{Jac}_{\mathbb{F}_{q^k}}(C)$). Setting $E = \mathrm{div}(a(x), b(x))$, we assume $\deg a(x) = 2$ and $\mathrm{supp} D \cap \mathrm{supp} E'' = \emptyset$, where $E'' = E + 2(\mathcal{O})$. Then $t_l(D, E) = f_D(E'')^{\frac{q^k-1}{l}}$ holds, where f_D is a function such that $(f_D) = lD$. In other words, we do not need the process of finding a divisor E' such that $E' \sim E$ and $\mathrm{supp} D \cap \mathrm{supp} E' = \emptyset$. Furthermore, we can decrease the number of points substituted into functions required in Miller's algorithm.

Remark 1.

In the computation of $f_D(E'')$ of Theorem 6, the degrees in x and y of the functions into which we substitute E'' can be reduced to at most one, because the points (x, y) in $\mathrm{supp} E''$ satisfy the defining equation of the form $y^2 = F(x)$ and the x-coordinates of those points are roots of $a(x)$.

From Theorem 6, we can simplify the Tate pairing $\widetilde{t_l}(D, E)$ (Theorem 4) by using the distortion map $\zeta_8 \circ \eta$ as follows:

Theorem 7.

Let $D, E \in \mathrm{Jac}_{\mathbb{F}_q}(C)[l] \backslash \{\mathrm{id}\}$. We represent E as $E = \sum_{1 \leq i \leq w} ((\alpha_i, \beta_i)) - w(\mathcal{O})$ ($w = 1$ or 2), and set $P_i = (\alpha_i, \beta_i)$. Let f_D be a function such that $(f_D) = lD$. Since l is odd, we may assume $\alpha_1 \neq 0$ without loss of generality. Then we have

$$\widetilde{t_l}(D, E) = \begin{cases} \prod_{1 \leq i \leq w,\, \alpha_i \neq 0} f_D(\phi(P_i))^{\frac{q^4-1}{l}} & \\ & (\alpha_2 \neq 0 \text{ or } (0, 0) \notin \mathrm{supp}(f_D)), \\ \pm f_D(\phi(P_1))^{\frac{q^4-1}{l}} & (\text{otherwise}), \end{cases}$$

where ϕ is the same map as in Theorem 5 and the signature $\pm$ is determined to satisfy $\widetilde{t_l}(D, E) \in \mu_l$. (Note that $z \in \mu_l$ implies $-z \notin \mu_l$ because l is odd.)

Proof of Theorem 7.

(i) The case $\boldsymbol{\alpha_2 \neq 0}$: From Theorem 5, we have $\zeta_8 \circ \eta(E) \sim (\phi(P_1)) + (\phi(P_2)) - 2(\mathcal{O})$. And the fact that $\phi(P_i)$ is not an $\mathbb{F}_{q^2}$-rational point implies that $\phi(P_i)$ does not belong to $\mathrm{supp}(f_D)$. Therefore, the desired result follows from Theorem 6.

(ii) The case $\boldsymbol{(0,\ 0) \notin \mathrm{supp}(f_D)}$ and $\boldsymbol{w = 1}$: We have $\widetilde{t_l}(D,\ E) = f_D\Big((\phi(P_1)) + ((0,\ 0))\Big)^{\frac{q^4-1}{l}}$ from Theorem 5. Hence we obtain the desired result by using $f_D((0,\ 0)) \in \mathbb{F}_q^*$ and $q-1|\frac{q^4-1}{l}$.

(iii) The case $\boldsymbol{(0,\ 0) \notin \mathrm{supp}(f_D)}$ and $\boldsymbol{\alpha_2 = 0}$: It is obvious that $\widetilde{t_l}(D,\ E) = \widetilde{t_l}(D,\ (P_1) - (\mathcal{O}))\,\widetilde{t_l}(D,\ ((0,\ 0)) - (\mathcal{O}))$ by the linearity of the map $\widetilde{t_l}$. From **(ii)** above and $((0,\ 0)) - (\mathcal{O}) \in \mathrm{Jac}_{\mathbb{F}_q}(C)[2]$, it follows that $\widetilde{t_l}(D,\ (P_1) - (\mathcal{O})) = f_D(\phi(P_1))^{\frac{q^4-1}{l}}$ and $\widetilde{t_l}(D,\ ((0,\ 0)) - (\mathcal{O})) \in \mu_l \cap \mu_2 = \{1\}$, which implies the first assertion of the theorem.

(iv) The case $\boldsymbol{(0,\ 0) \in \mathrm{supp}(f_D)}$ and "$\boldsymbol{w = 1}$ or $\boldsymbol{\alpha_2 = 0}$" : From Theorem 5, it is easy to see that $\zeta_8 \circ \eta(E) = (\phi(P_1)) + ((0,\ 0)) - 2(\mathcal{O})$ for $w = 1$, and that $\zeta_8 \circ \eta(E) \sim (\phi(P_1)) - (\mathcal{O})$ for $\alpha_2 = 0$. Then, for both cases, $\zeta_8 \circ \eta(2E) \sim 2(\phi(P_1)) - 2(\mathcal{O})$ holds. Hence we obtain $\widetilde{t_l}(D,\ E)^2 = \{f_D(\phi(P_1))^{\frac{q^4-1}{l}}\}^2$ from Theorem 6, which implies the second assertion of the theorem. $\square$

Remark 2.

In the actual computation of $f_D(\phi(P_i))$ for the function $f_D = \prod_{i,j} \frac{h_i(x,y)}{k_j(x,y)}$ (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 $\phi(P_i)$ is an element of $\mathbb{F}_{q^2}$ and $q^2 - 1$ divides $\frac{q^4-1}{l}$.

Furthermore, we can consider also the following improvement based on [8].

Remark 3.

Let the notation be the same as in Theorem 7. If we define the function h as $h = f_D^{\frac{q^2+1}{l}}$, then it satisfies that $(h) = (q^2+1)D$. Therefore, we obtain

$$\widetilde{t_l}(D,\ E) = \pm \prod_{1 \leq i \leq w,\, \alpha_i \neq 0} h(\phi(P_i))^{q^2-1},$$

which gives an efficient Tate pairing computation because we use the p-th power operations on fields of characteristic p and the quintuple operation *on* $\mathrm{Jac}_{\mathbb{F}_q}(C)$ *as the main procedure. Here the signature* $\pm$ *is assigned in the same way as in Theorem 7. Note that, for the final raising to the* (q^2-1)*-st power, it requires only one division on* $\mathbb{F}_{q^4}$ *and two subtructions on* $\mathbb{F}_q$ *because* $z^{q^2-1} = z^{q^2}/z = (\sum_{0\le i\le 3}(-1)^i a_i \alpha^{\frac{i}{4}})/z$ *for* $0 \neq z = \sum_{0\le i\le 3} a_i\alpha^{\frac{i}{4}}$ $(a_i \in \mathbb{F}_q)$*, which might be more efficient than the original method (i.e., the repeated square-and-multiply algorithm).*

5 Cost of the Tate pairing

In this section, we evaluate the cost taken to compute the Tate pairing $t_l(D, \zeta_8 \circ \eta(E))$ by using the method of [8] (Remark 3).

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 forms. 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 costs 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 the point $(0, 0)$ does not belong to $\mathrm{supp}E$ (cf. Theorem 7), that is, $E = \mathrm{div}(x^2 + L_1x + L_0, M_1x + M_0)$ with $L_0 \neq 0$. If $L_0 = 0$ holds, then the computation of the Tate pairing is simpler than that in the case $L_0 \neq 0$.

Now we discuss the cost of the algorithm (Table 1) for computing the Tate pairing by using our proposed method. Hereafter we use the notation "*distortion map*" not only for $\zeta_8 \circ \eta$ but also for the map ϕ.

5.1 Cost of the Distortion Map

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

Before doing this, we should estimate the cost for decomposing E into $E = (P_1) + (P_2) - 2(\mathcal{O})$. This task needs to solve a quadratic equation 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

Table 1. Tate pairing $t_l(D,\, \zeta_8 \circ \eta(E))$

Input:	Reduced divisors $D,\, E \in \mathrm{Jac}_{\mathbb{F}_q}(C)[l]$ with $(0,\,0) \notin \mathrm{supp}E$.
Output:	Tate pairing $t_l(D,\, \zeta_8 \circ \eta(E))$.
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 E into the form $E = (P_1) + (P_2) - 2(\mathcal{O})$.
Step 2:	Compute $\phi(P_i) = (\alpha_i,\, \beta_i)$ and $\alpha_i^2,\, \alpha_i^3,\, \beta_i^2,\, \alpha_i\beta_i,\, \alpha_i^2\beta_i,\, \alpha_i^3\beta_i$ $(i = 1, 2)$.
Step 3:	Compute the function $\ell(x, y) \in \mathbb{F}_q[x, y]$ s.t. $pD = D' + (\ell(x, y)/h(x))$ with D' reduced divisor and $h(x) \in \mathbb{F}_q[x]$.
Step 4:	$v \leftarrow 1,\, D' \leftarrow D$.
Step 5:	**for $i = 1$ to $2r$** (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 D'' reduced divisor and $h(x) \in \mathbb{F}_q[x]$. $v \leftarrow v^p \cdot \ell(\phi(P_1)) \cdot \ell(\phi(P_2)),\, D' \leftarrow D''$. **end for**
Step 6:	$v \leftarrow (v^{q^2}/v)$, output v.

[6]. From this, the cost of the decomposition is regarded as that of one $\frac{q+3}{4}$-th power operation on $\mathbb{F}_q$.

Now we evaluate the cost for computing $\phi(P)$ $(P \in C(\mathbb{F}_{q^2}))$. The detail is described in Table 3. It costs $3 \cdot 3M + 1I_{q^2} = 9M + 1I_{q^2}$ to compute $\phi(P)$. Since the resulting point is of the form $(E_1,\, E_2\alpha^{\frac{1}{4}})$, where $E_i \in \mathbb{F}_{q^2}^*$ $(i = 1, 2)$, 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).

5.2 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 $\ell(x, y) = \gamma y^2 + (sx^3 + tx^2 + ux + v)y + (-x^2 + cx + d)^3$ 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 $\ell(\phi(P))$. We emphasize that $\ell(x, y)$ can be computed only by performing 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 $\ell(\phi(P))$.

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 $\pm B\alpha^{\frac{1}{2}}$.

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).

We remark that $\phi(P) \notin C(F_{q^2})$ (by the form of $\phi(P)$ above), and that $\mathrm{supp}(\ell(x, y)) \subset C(F_{q^2})$ (by the definition of $\ell(x, y)$ and Theorem 1). This gives the fact $\mathrm{supp}(\ell(x, y)) \cap \phi(P) = \emptyset$, which means $\ell(\phi(P)) \neq 0, \infty$.

5.3 Total Cost

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

In Steps $1, 5$, we set $k = r = 120$ (cf. $\lceil \log_5 2^{256} \rceil = 111$) 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 $(3 \cdot 1 + 120 \cdot \frac{9}{5})M$ (by Subsection 5.1). The former part $3 \cdot 1M$ corresponds to the cost for the precomputation of the repeated p-th-power-and-multiply algorithm. Thus, Step 1 takes $220M$.

For Step 2, it costs $2(9M + 1I_{q^2} + 18M) = 54M + 2I_{q^2}$ by the argument of Subsection 5.1.

Table 4. Cost of the Tate pairing

method	cost
previous work [5]	$19851M + 240I_q$
ours	$13253M + 2I_{q^2} + 1I_{q^4}$

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

For Step 5, it costs $2 \cdot 18M + 2 \cdot 9M$ for rewriting the value v, that is, the computation of $v^p \cdot \ell(\phi(P_1)) \cdot \ell(\phi(P_2))$. Therefore, Step 5 takes $240 \cdot 54M = 12960M$.

For Step 6, it costs $9M + 1I_{q^4}$ (see Remark 3).

Consequently, we estimate the cost for computing the Tate pairing $t_l(D, \zeta_8 \circ \eta(E))$ as $13253M + 2I_{q^2} + 1I_{q^4}$. The resulting cost is about a half of the one in [5] for genus-2 hyperelliptic curves with embedding degree four (Table 4 [2]). This situation is the same as that of this paper.

6 Conclusions

In this paper, we constructed a distortion map explicitly (Theorem 4) and described a computation of the Tate pairing by using the proposed map (Theorem 7 and Table 3) for a class of genus-2 hyperelliptic curve defined by $y^2 = x^5 - \alpha x$ ($\alpha = \pm 2$) in the characteristic five. In addition, we estimated the cost (Section 5) of the Tate pairing by using this method. Consequently, the cost using our method turned out to be about 50% saving as compared with that using the method of [5].

References

1. P. S. L. M. Barreto, H. Y. Kim, B. Lynn, M. Scott, *Efficient algorithms for pairing-based cryptosystems*, Advances in Cryptology - CRYPTO 2002, Lecture Notes in Computer Science **2442**, pp. 354–368, Springer-Verlag, 2002.
2. D. Boneh and M. Franklin, *Identity-based encryption from the Weil pairing*, Advances in Cryptology - CRYPTO 2001, Lecture Notes in Computer Science **2139**, pp. 213–229, Springer-Verlag, 2001.
3. D. Boneh, B. Lynn and H. Shacham, *Short signatures from the Weil pairing*, Advances in Cryptology - ASIACRYPT 2001, Lecture Notes in Computer Science **2248**, pp. 514–532, Springer-Verlag, 2001.
4. D. G. Cantor, *Computing in the Jacobian of a hyperelliptic curve*, Math. Comp. **48**, pp. 95–101, 1987.

[2] The evaluation in [5] excludes the cost for the final raising to the $\frac{q^4-1}{l}$-th power.

5. 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.
6. H. Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Math., vol. **138**, Springer-Verlag, Berlin Heidelberg, 1993.
7. 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.
8. 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.
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**, pp. 865–874, 1994.
10. S. D. Galbraith and J. Pujolás, *Distortion maps for genus two curves*, preprint, available at
http://www.isg.rhul.ac.uk/˜sdg/jordi-paper.pdf.
11. A. Joux, *A one-round protocol for tripartite Diffie-Hellman*, Algorithmic Number Theory Symposium - ANTS IV, Lecture Notes in Computer Science **1838**, pp. 385–394, Springer-Verlag, 2000.
12. N. Koblitz, *Hyperelliptic cryptosystems*, J. Cryptology, Vol. **1**, pp. 139–150, 1989.
13. V. Miller, *Short program for functions on curves*, unpublished manuscript.
14. H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer Universitext, Springer-Verlag, Berlin Heidelberg, 1993.
15. H. Stichtenoth and C. Xing, *On the structure of the divisor class group of a class of curves over finite fields*, Arch. Math. vol. **65**, pp. 141–150, 1995.
16. J. Tate, *Endomorphisms of abelian varieties over finite fields*, Inventiones Math. **2**, pp. 134–144, 1996.