Japan J. Indust. Appl. Math., 24 (2007), 251–274 Area ⟨3⟩

Tate and Ate Pairings for $y^2 = x^5 - \alpha x$ in Characteristic Five

Ryuichi HARASAWA[a,*], Yutaka SUEYOSHI[b,*] and Aichi KUDO[c,*]

Department of Computer and Information Sciences
Faculty of Engineering, Nagasaki University
1–14 Bunkyo-machi, Nagasaki 852–8521, Japan
[a] *E-mail: harasawa@cis.nagasaki-u.ac.jp*
[b] *E-mail: sueyoshi@cis.nagasaki-u.ac.jp*
[c] *E-mail: kudo@cis.nagasaki-u.ac.jp*

Received October 30, 2006
Revised February 14, 2007

In this paper, we consider the Tate and Ate pairings for the genus-2 supersingular hyperelliptic curves $y^2 = x^5 - \alpha x$ ($\alpha = \pm 2$) defined over finite fields of characteristic five. More precisely, we construct a distortion map explicitly, and show that the map indeed gives an input for which the value of the Tate pairing is not trivial. We next describe a computation of the Tate pairing by using the proposed distortion map. We also see that this type of curve is equipped with a simple quintuple operation on the Jacobian group, which leads to an improvement for computing the Tate pairing. We further show the Ate pairing, a variant of the Tate pairing for elliptic curves, can be applied to this curve. The Ate pairing yields an algorithm which is about 50 % more efficient than the Tate pairing in this case.

Key words: hyperelliptic curves, distortion map, Tate and Ate pairings

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 [15]. 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 [28], ID-based encryption scheme [4] and short signatures [5].

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

1. The parameter, called *embedding degree*, is not too large.
2. Arithmetic in the Jacobian is efficient.
3. The curve is equipped with a distortion map. Such a map can be seen a method for giving an input for which the value of the pairing is not trivial.

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. We remark, for the third topic, that there exists an

*This paper is the full version of [21]. In addition to the paper presented at the symposium the current paper gives a clean mathematical background, provides exact cost evaluations, and gives implementational evidence of the speed-ups obtained. Preprint versions of this paper appeared in the ePrint archive as [22, 23].

alternative method other than the one using distortion maps (e.g. using the trace map [4, 16]).

The main theme of this paper is about the third topic (i.e. the construction of a distortion map). A distortion map becomes a useful tool when one constructs some protocol requiring a bilinear map with symmetry. The paper [17] shows there exists a distortion map for all supersingular algebraic curves. This is why a class of supersingular curves gets interest of a lot of cryptologic researchers. Contrarily, it is known that there exists no distortion map for ordinary elliptic curves [41].

For some supersingular curves, distortion maps have been constructed [2, 11, 17, 18, 19]. Generally, for curves of genus $g \geq 2$, it is harder to construct a distortion map in comparison 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, unlike supersingular elliptic curves case, giving an endomorphism not defined over the base field is not sufficient to obtain a distortion map.

In this paper, we explicitly construct a distortion map for the genus-2 supersingular hyperelliptic curves $y^2 = x^5 - \alpha x$ ($\alpha = \pm 2$) over finite fields of characteristic five, which are Koblitz curves [31], and show that the map indeed gives an input for which the value of the Tate pairing is not trivial. We next describe the computation of the Tate pairing by using the proposed distortion map. We note that the curve above is equipped with a simple formula of quintuple operation (a variant of [12]). This fact leads to an improvement for computing the Tate pairing.

We remark that for a class of supersingular curves $y^2 = x^p - x + d$ ($d = \pm 1$) over finite fields of characteristic p with embedding degree being p or $2p$ [12], the paper [11] constructs an endomorphism not defined over the base field. The paper [18] gives a proof that the map indeed becomes a distortion map in the case of $p = 5$. For the curve $y^2 = x^5 + a$ over prime fields $\mathbb{F}_p$, it is proven that this curve is supersingular and has an embedding degree of four under $p \equiv 2, 3 \pmod 5$ [7]. The paper [8] constructs an endomorphism not defined over the base field and [17] gives a proof that the map indeed becomes a distortion map under a certain condition which seems to hold in almost all cases.

We further show the Ate pairing [25], a variant of the Tate pairing for elliptic curves, can be applied to the curve $y^2 = x^5 - \alpha x$ with respect to the proposed distortion map. The Ate pairing yields an algorithm which is about 50 % more efficient than the Tate pairing in this case. The main reason is that the computational procedure of the Ate pairing has a much shorter loop than the Tate pairing on the cost of some extra computations. Our distortion map for $y^2 = x^5 - \alpha x$ does not satisfy the sufficient conditions for the Eta pairing [1] as it is. We remark that it is shown that these conditions are not necessary [29]. After acceptance of this paper we became aware of the recent paper [20] which also gives a generalization of the Ate pairing to hyperelliptic curves. Their work is clearly independent and focuses on finite fields of characteristic 2 and 3.

We finally implement the Tate and Ate pairings for our curve in an actual size of fields, which takes far much runnning time in comparison with pairings for other

pairing-friendly curves, e.g. the Eta pairing for supersingular (hyper-)elliptic curves in characteristic two. The main reason is that there exists no efficient arithmetic on fields in characteristic five. However, the experimental result also shows the possibility that the pairing computation for our curve will reach at practical level.

The remainder of this paper is organized as follows: In Section 2, we describe the mathematical background required in this paper. In Section 3, we construct a distortion map for the 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 show the Ate pairing can be applied to the curve with respect to the distortion map. In Section 6, we estimate the cost for computing the Ate pairing. In Section 7, we provide the implementation results of the Tate and Ate pairings for our curve. In Section 8, we give the conclusion.

2. Preliminaries

In this section, we describe the mathematical background required in this paper. For more details, see [6, 15, 30, 39].

2.1. Hyperelliptic curves

Let $p > 2$ be an odd prime and let $\mathbb{F}_q$ and $\overline{\mathbb{F}}_q$ be a finite field with $q = p^r$ elements and its algebraic closure, respectively. Let $C/\mathbb{F}_q$ be a genus-g hyperelliptic curve defined over $\mathbb{F}_q$ whose defining equation is of the form $y^2 = F(x)$ with $\deg F(x) = 2g+1$ and let $\mathbb{F}_q[C]$ (resp. $\mathbb{F}_q(C)$) denote the coordinate ring (resp. the function field) of $C/\mathbb{F}_q$. For each extension field $\mathbb{F}_q \subseteq \mathbb{K} \subseteq \overline{\mathbb{F}}_q$, a point $(x, y) \in \mathbb{K}^2$ on C or the point at infinity $\mathcal{O}$ is called a $\mathbb{K}$-*point* on C. The set of $\mathbb{K}$-points on C is denoted by $C(\mathbb{K})$.

A *divisor* $D = \sum n_P(P)$ is a formal sum of $\overline{\mathbb{F}}_q$-points on C where $n_P = 0$ for all but finitely many P, which forms an additive group under an obvious manner. The *degree* and the *support* of a divisor D are defined by $\deg D = \sum n_P$ and $\operatorname{supp} D = \{P \in C(\overline{\mathbb{F}}_q) \mid n_P \neq 0\}$, respectively. For $P = (\alpha, \beta) \in C(\overline{\mathbb{F}}_q) \setminus \{\mathcal{O}\}$, the point $\widetilde{P} := (\alpha, -\beta)$ on C is said to be the *opposite* of P, and we define $\widetilde{\mathcal{O}} = \mathcal{O}$. For P above and $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$, we define $P^\sigma = (\sigma(\alpha), \sigma(\beta)) \in \overline{\mathbb{F}}_q(C)$ and $\mathcal{O}^\sigma = \mathcal{O}$, where $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ denotes the Galois group of $\overline{\mathbb{F}}_q$ over $\mathbb{F}_q$.

Let $\mathrm{Div}(C)$ (resp. $\mathrm{Div}^0(C)$) denote the group of divisors (resp. the subgroup of $\mathrm{Div}(C)$ consisting of divisors of degree zero). A divisor $D = \sum n_P(P)$ is *defined over* $\mathbb{F}_q$ if $D = D^\sigma := \sum n_P(P^\sigma)$ holds for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$, and $\mathrm{Div}_{\mathbb{F}_q}(C)$ (resp. $\mathrm{Div}^0_{\mathbb{F}_q}(C)$) denotes the set of divisors defined over $\mathbb{F}_q$ (resp. the set of degree-zero divisors defined over $\mathbb{F}_q$). Setting $\alpha_P = \min\{m_P, n_P\}$ for two divisors $D_1 = \sum m_P(P)$ and $D_2 = \sum n_P(P)$, we define the *greatest common divisor* by $\gcd(D_1, D_2) = \sum_{P \neq \mathcal{O}} \alpha_P(P) - \big(\sum_{P \neq \mathcal{O}} \alpha_P\big)(\mathcal{O})$, which is an element of $\mathrm{Div}^0(C)$.

For a point $P \in C(\overline{\mathbb{F}}_q)$, let $v_P(\,\cdot\,)$ denote the discrete valuation at P, that is, if $v_P(f) = m > 0$ (resp. $m < 0$) for $f \in \overline{\mathbb{F}}_q(C)^*$, then P is a zero (resp. pole) of f of order $|m|$. A divisor $D \in \mathrm{Div}(C)$ is a *principal divisor* if there exists some $f \in \overline{\mathbb{F}}_q(C)^*$ such that $D = \sum v_P(f)(P)$, denoted by (f), and $\mathrm{Prin}(C)$ (resp. $\mathrm{Prin}_{\mathbb{F}_q}(C)$)

denotes the set of principal divisors (resp. the set of principal divisors defined over $\mathbb{F}_q$), which forms a subgroup of $\mathrm{Div}^0(C)$ (resp. $\mathrm{Div}^0_{\mathbb{F}_q}(C)$). Two divisors D_1, D_2 are *linearly equivalent*, denoted by $D_1 \sim D_2$, if there exists some function $f \in \overline{\mathbb{F}}_q(C)^*$ such that $D_1 = D_2 + (f)$. For $f \in \overline{\mathbb{F}}_q(C)^*$ and $D = \sum n_P(P)$ with $\mathrm{supp}(f) \cap \mathrm{supp}\, D = \emptyset$, we define $f(D) = \prod f(P)^{n_P}$.

We define the *Jacobian group* of the curve C (resp. the *Jacobian group* of the curve C *defined over* $\mathbb{F}_q$), denoted by $\mathrm{Jac}(C)$ (resp. $\mathrm{Jac}_{\mathbb{F}_q}(C)$), by the quotient group $\mathrm{Div}^0(C)/\mathrm{Prin}(C)$ (resp. $\mathrm{Div}^0_{\mathbb{F}_q}(C)/\mathrm{Prin}_{\mathbb{F}_q}(C)$), which is isomorphic to the ideal class group of the coordinate ring $\overline{\mathbb{F}}_q[C]$ (resp. $\mathbb{F}_q[C]$).

Each class in $\mathrm{Jac}(C)$ has a representative of the form $D = \sum_{P \neq \mathcal{O}} n_P(P) - \big(\sum_{P \neq \mathcal{O}} n_P\big)(\mathcal{O})$, where $n_P > 0$ and $\widetilde{P} \notin \mathrm{supp}\, D$ hold whenever $P \in \mathrm{supp}\, D \setminus \{\mathcal{O}\}$ except for $P = \widetilde{P}$, in which case $n_P = 1$. Such a divisor is said to be a *semi-reduced divisor*. Furthermore, for each class in $\mathrm{Jac}(C)$, there exists a unique semi-reduced divisor with $\sum_{P \neq \mathcal{O}} n_P \leq g$. Such a divisor is called a *reduced divisor*. We use the notation $\overline{D}$ for the class in $\mathrm{Jac}(C)$ (or $\mathrm{Jac}(C)/l\,\mathrm{Jac}(C)$ for an integer l) to which D belongs. Vice versa, we assume that the class $\overline{D}$ is represented by the unique reduced divisor in it which we denote by D. For an integer l, we let $\mathrm{Jac}_{\mathbb{F}_q}(C)[l] = \{\overline{D} \in \mathrm{Jac}_{\mathbb{F}_q}(C) \mid l\overline{D} = \overline{0}\}$, where we mean by $\overline{0}$ the identity element of $\mathrm{Jac}_{\mathbb{F}_q}(C)$.

Let $D = \sum_{P_i \neq \mathcal{O}} n_{P_i}(P_i) - \big(\sum_{P_i \neq \mathcal{O}} n_{P_i}\big)(\mathcal{O})$ be a semi-reduced divisor, $P_i = (\alpha_i, \beta_i)$ and $a(x) = \prod (x - \alpha_i)^{n_i}$. There exists a unique $b(x) \in \overline{\mathbb{F}}_q[x]$ satisfying $\deg b(x) < \deg a(x)$, $\beta_i = b(\alpha_i)$ and $a(x) \mid b(x)^2 - F(x)$. For such D, $a(x)$ and $b(x)$, it is known that the equation $D = \gcd((a(x)), (y - b(x)))$ holds, denoted by $D = \mathrm{div}(a(x), b(x))$ for short. We remark that a semi-reduced divisor $\mathrm{div}(a(x), b(x))$ corresponds to the integral ideal in $\overline{\mathbb{F}}_q[C]$ whose $\overline{\mathbb{F}}_q[x]$-basis consists of $a(x)$ and $y - b(x)$. The form $\mathrm{div}(a(x), b(x))$ is the one used in the case of representing each semi-reduced divisor of hyperelliptic curves, which is called the *Mumford representation*. We mention that $D = \mathrm{div}(a(x), b(x))$ is defined over $\mathbb{F}_q$ if and only if so are both of $a(x)$ and $b(x)$.

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

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

For the a_i's above, it satisfies that $a_{2g} = 1$, $a_0 = q^g$, and for $1 \leq i \leq g$, $i a_{2g-i} - \sum_{1 \leq k \leq i} (\#C(\mathbb{F}_{q^k}) - q^k - 1) a_{2g-i+k} = 0$, $a_i = a_{2g-i} q^{g-i}$.

2.2. Tate pairing

Let $C/\mathbb{F}_q$ be an algebraic curve and l an odd prime with $l \nmid q$ and $l \mid \#\mathrm{Jac}_{\mathbb{F}_q}(C)$. The *embedding degree* is defined by the smallest positive integer k such that $l \mid q^k - 1$.

Then there exists a nondegenerate bilinear map, called the *(modified) Tate pairing*,

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

defined by

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

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

For $\overline{D} \in \mathrm{Jac}_{\mathbb{F}_q}(C)[l]$, an endomorphism ϕ of $\mathrm{Jac}(C)$ is said to be a *distortion map* if $t_l(\overline{D}, \phi(\overline{D})) \neq 1$ holds. A distortion map becomes a helpful tool to realize a lot of cryptographic protocols using pairings. We mention that our definition of a distortion map differs from that in [17, 18]. Their definition is more general than ours.

In general, we use Miller's algorithm [33, 34] for computing the Tate pairing.

Remark 1 (Embedding degree). Let $q = p^r$ and let s be the smallest integer such that $l \mid p^s - 1$. Namely, $\mathbb{F}_{p^s}$ is the smallest field satisfying $\mu_l \subseteq \mathbb{F}_{p^s}$. Then we have $s = dk$ with $d = \gcd(r, s)$ and k the embedding degree [26]. This implies $s \leq rk$. The equality holds if and only if r divides s. For cryptographic applications using pairings, it is recommended that the parameter l (resp. s) satisfies $l \geq 2^{160}$ (resp. $p^s \geq 2^{1024}$) in order to achieve security (e.g. [14, 32]). The condition $q^k \geq 2^{1024}$ claimed in many papers on pairings is not strict [26]. We mention that one must pay attention not to obtain a security parameter which is much smaller than expected.

On the other hand, in view of cost performance, it is preferable that the sizes of the fields $\mathbb{F}_q, \mathbb{F}_{q^k}$ are small satisfying the security conditions above.

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

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

Unless explicitly stated otherwise, we set $p = 5$ and $q = p^r$, and consider the genus-2 hyperelliptic curves defined by

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

They are Koblitz curves [31], i.e. curves defined over small fields.

We start from the following result, which is a variant of [12]:

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

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

Proof. 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. □

Applying the theorem above to our curve C, we get a simple quintuple operation on $\mathrm{Jac}(C)$ as follows:

COROLLARY 1. *For $P = (a, b) \in C(\overline{\mathbb{F}}_q) \setminus \{\mathcal{O}\}$, we have*

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

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 corollary gives the following formulae:

$$\begin{aligned} p\,\mathrm{div}(x + a_0, b_0) &= \mathrm{div}\big(x - a_0^{p^2}, \alpha b_0^{p^2}\big) + \big(\big(b_0^p y + (\alpha x + a_0^p)^{\frac{p+1}{2}}\big)\big/\big(x - a_0^{p^2}\big)\big), \\ p\,\mathrm{div}(x^2 + a_1 x + a_0, b_1 x + b_0) &= \mathrm{div}\big(x^2 - a_1^{p^2} x + a_0^{p^2}, -\alpha b_1^{p^2} x + \alpha b_0^{p^2}\big) \\ &\quad + \big((\gamma y^2 + f_1(x) y + f_0(x))\big/\big(x^2 - a_1^{p^2} x + a_0^{p^2}\big)\big), \end{aligned}$$

where

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

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

From Corollary 1, we further obtain the following result, which plays an important role for an efficient computation of the Tate pairing for $y^2 = x^5 - \alpha x$.

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

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

We next 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 $l \mid \#\mathrm{Jac}_{\mathbb{F}_q}(C) = q^2 + 1$, then the embedding degree is equal to 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 are less interesting for cryptographic purposes. In our case, we can choose $\mathbb{F}_{q^k}$ sufficiently large in view of security while we can choose small $\mathbb{F}_q$ in view of cost performance (see Remark 1).

3.2. Construction of a distortion map

In this subsection, we construct a distortion map for $C/\mathbb{F}_q\colon y^2 = x^5 - \alpha x$ ($\alpha = \pm 2$) 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

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

where $\alpha^{\frac{1}{4}}$ is a fixed fourth root of α and $\alpha^{\frac{1}{2}} = (\alpha^{\frac{1}{4}})^2$. We shall use the same symbols for the endomorphisms of $\mathrm{Jac}(C)$ induced from these morphisms above. Since r is odd and $\alpha = \pm 2$, we have $(\alpha^{\frac{1}{4}})^{q^2} = (\alpha^r \alpha^{\frac{1}{4}})^q = -\alpha^{\frac{1}{4}}$, which implies that $\alpha^{\frac{1}{4}}$ is an element of $\mathbb{F}_{q^4} \setminus \mathbb{F}_{q^2}$.

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:

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

Here, we consider $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$ and $\alpha = a + 5\mathbb{Z}$ for some integer a so that $\zeta_5^\alpha = \zeta_5^a$.

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 ([17]). *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 $l \mid q^2 + 1$. Then the eigenvalues of π_q on $\mathrm{Jac}(C)[l]$ are ± 1, $\pm q$.*

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

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

□

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

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

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

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

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

□

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 2. *If $l \parallel q^2 + 1$ and $\overline{D} \in \mathrm{Jac}_{\mathbb{F}_q}(C)[l] \setminus \{\overline{0}\}$, then $\{\overline{D}, \zeta_8(\overline{D}), \eta(\overline{D}), \zeta_8 \circ \eta(\overline{D})\}$ 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. If $\eta(\overline{D}) \neq \overline{0}$, then we see from (2) and Lemma 2 that $\langle \overline{D} \rangle$, $\langle \zeta_8(\overline{D}) \rangle$, $\langle \eta(\overline{D}) \rangle$, $\langle \zeta_8 \circ \eta(\overline{D}) \rangle$ 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 $\mathrm{Jac}_{\mathbb{F}_{q^4}}(C) \cong (\mathbb{Z}/(q^2+1)\mathbb{Z})^4$ [40]. From this fact and the assumption $l \parallel q^2+1$, we obtain the desired result for $\mathrm{Jac}_{\mathbb{F}_{q^4}}(C)/l\,\mathrm{Jac}_{\mathbb{F}_{q^4}}(C)$. So, we only need to show $\eta(\overline{D}) \neq \overline{0}$.

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

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

Then, since $\gcd(l, N) = \gcd(l, q \mp 2) = 1$, we obtain $\overline{D} \in \mathrm{Jac}_{\mathbb{F}_q}(C)[l] \cap \mathrm{Jac}(C)[N] = \{\overline{0}\}$, which completes the proof of the theorem. Indeed, if $l \mid q \mp 2$, then $l \mid (q+2)(q-2) = (q^2+1) - 5$. This implies $l \mid 5$, which contradicts $l \mid q^2+1$. □

Remark 2. According to the Cohen–Lenstra heuristic [10], it is highly unlikely that l^2 divides $\#\mathrm{Jac}_{\mathbb{F}_q}(C)$ for a sufficiently large l.

From Theorem 2 above and [17, Lemma 3.3], we can obtain the following result:

Theorem 3. *With the notation above, if l is an odd prime with $l \parallel q^2+1$, then the map*

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

defined by

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

is bilinear and has the property that $\widetilde{t_l}(\overline{D}, \overline{E}) \neq 1$ holds for all $\overline{D}, \overline{E} \neq \overline{0}$.

Proof. The proof is the same as in Lemma 3.3 of [17]. We describe only the outline (see [17, Lemma 3.3] for more details). The bilinearity follows from the definition of $\widetilde{t_l}$. For the second assertion, since it turns out $t_l(\overline{D'}, \overline{E'})^q = t_l(\pi_q(\overline{D'}), \pi_q(\overline{E'}))$ for $\overline{D'} \in \mathrm{Jac}_{\mathbb{F}_{q^k}}(C)[l]$ and $\overline{E'} \in \mathrm{Jac}_{\mathbb{F}_{q^k}}(C)/l\,\mathrm{Jac}_{\mathbb{F}_{q^k}}(C)$, we see

$t_l(\overline{D},\overline{E}) = t_l(\overline{D},\zeta_8(\overline{E})) = t_l(\overline{D},\eta(\overline{E})) = 1$. Indeed, since

$$\begin{aligned} t_l(\overline{D},\zeta_8(\overline{E}))^q &= t_l(\pi_q(\overline{D}),\pi_q\circ\zeta_8(\overline{E})) \\ &= t_l(\overline{D},-\zeta_8(\overline{E})) \\ &= t_l(\overline{D},\zeta_8(\overline{E}))^{-1}, \end{aligned}$$

we obtain $t_l(\overline{D},\zeta_8(\overline{E}))^{q+1} = 1$. So we have $t_l(\overline{D},\zeta_8(\overline{E})) \in \mu_l \cap \mu_{q+1} = \{1\}$ from $\gcd(l, q+1) = 1$. Similarly, we can show the other equalities.

Hence the desired result follows from Theorem 2 and the non-degeneracy of the Tate pairing. □

As a result, from Theorem 3, the endmorphism $\zeta_8\circ\eta$ becomes a distortion map for each element of $\mathrm{Jac}_{\mathbb{F}_q}(C)[l]\setminus\{\overline{0}\}$.

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.

Representing each reduced divisor defined over $\mathbb{F}_q$ as $\mathrm{div}(a(x),b(x)) = \sum_{1\le i\le \deg a(x)}((\alpha_i,\beta_i)) - \deg a(x)(\mathcal{O})$ $(\deg a(x)\le 2)$, we see that each (α_i,β_i) becomes an $\mathbb{F}_{q^2}$-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 $P\in C(\mathbb{F}_{q^2})\setminus\{\mathcal{O}\}$.

THEOREM 4. *For $P=(a,b)\in C(\mathbb{F}_{q^2})\setminus\{\mathcal{O}\}$, we have*

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

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

Proof. Since $P=(a,b)$ satisfies $b^2 = a^5 - \alpha a$, the following four points are on the curve as can be checked easily.

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

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

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

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

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

In the case $a\neq 0$, there exists a unique function of the form $h(x,y)=y-(c_3x^3+c_2x^2+c_1x+c_0)$ such that $h(P_i(a,b))=0$ for $1\le i\le 4$. Let A be the determinant of the coefficient matrix for the simultaneous equations with unknown c_i's. We have $A=(a^4-\alpha)\alpha^r\alpha^{\frac{1}{2}}$, which is a nonzero element because the assumption $a\in\mathbb{F}_{q^2}$ implies $a^4-\alpha\neq 0$. It then 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

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

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

By definition, we have

$$\zeta_8\circ\eta((P)+(Q)-2(\mathcal{O}))=\zeta_8\circ\eta((P)-(\mathcal{O}))+\zeta_8\circ\eta((Q)-(\mathcal{O})).$$

We mention that $2((0,0)-(\mathcal{O}))=(x)$, which is equal to $\overline{0}$ as an element of $\mathrm{Jac}(C)$.

4. Computation of the Tate pairing

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

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

THEOREM 5 ([8]). *Let $C/\mathbb{F}_q$ be a genus-2 hyperelliptic curve, l an odd prime with l dividing $\#\mathrm{Jac}_{\mathbb{F}_q}(C)$ but not q. We assume that the embedding degree $k\ge 2$. Let $\overline{D}$ (resp. $\overline{E}$) be an element of $\mathrm{Jac}_{\mathbb{F}_q}(C)[l]$ (resp. $\mathrm{Jac}_{\mathbb{F}_{q^k}}(C)/l\,\mathrm{Jac}_{\mathbb{F}_{q^k}}(C)$). Representing $E=\mathrm{div}(a(x),b(x))$, we assume that $\deg a(x)=2$ and $\mathrm{supp}\,D\cap\mathrm{supp}\,E''=\emptyset$, where $E''=E+2(\mathcal{O})$. Then $t_l(\overline{D},\overline{E})=f_D(E'')^{\frac{q^k-1}{l}}$ holds, where $f_D\in\mathbb{F}_q(C)$ 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.*

In order to make the notation simple, for a divisor $D=\sum n_P(P)$, we define $\hat{D}$ as $\hat{D}=\sum_{P\in C(\overline{\mathbb{F}}_q)\setminus\{(0,0),\mathcal{O}\}}n_P(P)$, the divisor obtained by eliminating $(0,0)$ and $\mathcal{O}$ from D.

From Theorem 5, we can simplify the Tate pairing $\widetilde{t}_l(\overline{D},\overline{E})$ using the distortion map $\zeta_8\circ\eta$ as follows:

THEOREM 6. *Let $\overline{D},\overline{E}\in \mathrm{Jac}_{\mathbb{F}_q}(C)[l]\setminus\{\overline{0}\}$, and $f_D\in\mathbb{F}_q(C)$ a function such that $(f_D)=lD$. Then we have*

$$\widetilde{t}_l(\overline{D},\overline{E}) = \begin{cases} f_D(\phi(\hat{E}))^{\frac{q^4-1}{l}} & (\deg\hat{E}=2 \text{ or } (0,0)\notin \operatorname{supp} D),\\ \pm f_D(\phi(\hat{E}))^{\frac{q^4-1}{l}} & (\text{otherwise}), \end{cases}$$

where ϕ is the same map as in Theorem 4 *and the signature $\pm$ is determined so that $\widetilde{t}_l(\overline{D},\overline{E})\in\mu_l$ holds. We note that $z\in\mu_l$ implies $-z\notin\mu_l$ because l is odd.*

Proof. We represent E as $E=\sum_{1\le i\le w}((\alpha_i,\beta_i))-w(\mathcal{O})$ ($w=1$ or 2), and set $P_i=(\alpha_i,\beta_i)$. Since l is odd, we may assume $\alpha_1\neq 0$ without loss of generality. Then we have $\hat{E}=(P_1)+(P_2)$ (i.e. $\deg\hat{E}=2$) if and only if $w=2$ and $\alpha_2\neq 0$ (otherwise $\hat{E}=(P_1)$). We further see $\operatorname{supp}\phi(\hat{E})\cap\operatorname{supp} D=\emptyset$ because of $\operatorname{supp} D\subset C(\mathbb{F}_{q^2})$ and $\operatorname{supp}\phi(\hat{E})\cap C(\mathbb{F}_{q^2})=\emptyset$.

(i) The case $\deg\hat{E}=2$: From Theorem 4, we have $\zeta_8\circ\eta(E)\sim\phi(\hat{E})-2(\mathcal{O})$. Therefore, the desired result follows from Theorem 5.

(ii) The case $(0,0)\notin\operatorname{supp} D$ and $w=1$: We have $\widetilde{t}_l(\overline{D},\overline{E})=f_D(\phi(\hat{E})+((0,0)))^{\frac{q^4-1}{l}}$ from Theorem 4. Hence we obtain the desired result by using $f_D((0,0))\in\mathbb{F}_q^*$ and $q-1\mid\frac{q^4-1}{l}$.

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

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

REMARK 3. Applying the so-called squared Tate pairing [13], we obtain the equality $\widetilde{t}_l(\overline{D},\overline{E})^2=f_D(\phi(\hat{E}))^{\frac{2(q^4-1)}{l}}$ for all $\overline{D},\overline{E}\in\mathrm{Jac}_{\mathbb{F}_q}(C)[l]\setminus\{\overline{0}\}$. The pairing $\widetilde{t}_l^2$ keeps the same properties as those of $\widetilde{t}_l$ described in Theorem 3.

REMARK 4 ([2, 11]). Let the notation be as in Theorem 6. We define the function $f_{q^2}\in\mathbb{F}_q(C)$ by $q^2D=D_{q^2}+(f_{q^2})$ with reduced divisor D_{q^2}. Then we

have $(a(x)\cdot f_{q^2}) = \frac{q^2+1}{l}(f_D)$ for $D = \mathrm{div}(a(x), b(x))$, which implies

$$\widetilde{t}_l(\overline{D}, \overline{E}) = \pm(a(x)\cdot f_{q^2})(\phi(\hat{E}))^{q^2-1}.$$

Here the signature $\pm$ is assigned in the same way as in Theorem 6.

Moreover, applying Corollary 1 repeatedly, we can represent f_{q^2} as the form $\prod_i \frac{\ell_i(x,y)}{h_i(x)}$. Then, as in [2] we can omit $h_i(x)$'s and $a(x)$ for the computation of $\widetilde{t}_l(\overline{D}, \overline{E})$, because the values $h_i(\phi(\hat{E}))$ and $a(\phi(\hat{E}))$ belong to $\mathbb{F}_{q^2}^*$. Indeed, the x-coordinate of each point of $\mathrm{supp}\,\phi(\hat{E})$ is an element of $\mathbb{F}_{q^2}$, and $(\mathrm{supp}\,\phi(\hat{E}) \cap \big(\bigcup_i \mathrm{supp}(h_i(x)) \cup \mathrm{supp}(a(x))\big) \subset (\mathrm{supp}\,\phi(\hat{E}) \cap C(\mathbb{F}_{q^2})) = \emptyset$ holds from Corollary 1.

As a result, we obtain

$$\widetilde{t}_l(\overline{D}, \overline{E}) = \pm\left(\prod_i \ell_i(\phi(\hat{E}))\right)^{q^2-1}.$$

This 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 main procedures [11].

Remark 5. The final raising of a nonzero element z to the (q^2-1)-st power requires only one inversion and five multiplications on $\mathbb{F}_{q^2}$ because $z^{q^2-1} = z^{q^2}/z = (a_0 - a_1\alpha^{\frac{1}{4}})/(a_0 + a_1\alpha^{\frac{1}{4}}) = (a_0 - a_1\alpha^{\frac{1}{4}})^2/(a_0^2 - a_1^2\alpha^{\frac{1}{2}})$ for $z = a_0 + a_1\alpha^{\frac{1}{4}}$ ($a_i \in \mathbb{F}_{q^2} = \mathbb{F}_q(\alpha^{\frac{1}{2}})$), which is more efficient than the original method (i.e. the repeated square-and-multiply algorithm). There exists another method [27] for performing the computation of z^{q^2-1} on $\mathbb{F}_{q^4}$: $z^{q^2-1} = (z\cdot z^q)^{q^2+q}/(z\cdot z^q)^{q^2+1}$. We note that the denominater is equal to $N_{\mathbb{F}_{q^4}/\mathbb{F}_q}(z)$, which is an element of $\mathbb{F}_q$. So, it needs three q-th power operations on $\mathbb{F}_{q^4}$ and two (resp. eight) multiplications on $\mathbb{F}_{q^4}$ (resp. $\mathbb{F}_q$) and one inversion on $\mathbb{F}_q$. Compairing the costs of the two methods above, we see later (Subsection 6.1) that the former method is more efficient than the latter one. Therefore, we apply the former one for the final raising to the (q^2-1)-st power when we evaluate the cost of pairings and implement them.

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

In this section, we describe the Ate pairing [25] for $y^2 = x^5 - \alpha x$.

Since $\gcd(q^2+1, q) = 1$, there exists an integer ρ such that $\rho q \equiv 1 \pmod{q^2+1}$. Then we obtain the following result:

Theorem 7 (Ate pairing for $y^2 = x^5 - \alpha x$). *The map*

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

defined by

$$\hat{t}_l(\overline{D}, \overline{E}) = \widetilde{t}_l(\overline{D}, \overline{E})^{\rho}$$

is bilinear and has the property that $\hat{t}_l(\overline{D},\overline{E}) \neq 1$ *for all* $\overline{D},\overline{E} \neq \overline{0}$. *Furthermore, we have*

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

where $f_q \in \mathbb{F}_q(C)$ *is a function such that* $qD = D_q + (f_q)$ *with reduced divisor* D_q *and the signature* $\pm$ *is assigned in the same way as in* Theorem 6 *(recall that* ρ *is odd by definition).*

Remark 6. For the Tate pairing based on Remark 4, we need a function f_{q^2} such that $q^2D = D_{q^2} + (f_{q^2})$. Finding the function f_m using Miller's algorithm requires running time depending on $\log m$. This shows that the cost of the Ate pairing is about a half of that of the Tate pairing based on Remark 4 (see Table 5).

The proof of Theorem 7 is similar to that for the supersingular elliptic curves [25, Section III.B]. We describe the outline.

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 (2), namely $\hat{\pi}_q$ is the dual of π_q.

For the proof of Theorem 7, we need two lemmas.

Lemma 3. *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 $\hat{E} = \sum_{1\leq i\leq w}(P_i)$ ($w = 1$ 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. □

Lemma 4. *With the notation above, we have*

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

where h *is a function such that* $qD_q = D_{q^2} + (h)$.

Proof. By definition, $\hat{\pi}_q$ is a bijection of degree q. Hence, by [38, Proposition 2.6 (Chapter II)], the equality $\hat{\pi}_q^*\big(\sum n_P(P)\big) = q\big(\sum n_P(\hat{\pi}_q^{-1}(P))\big)$ holds for every divisor $\sum n_P(P)$ (for the definition of $\hat{\pi}_q^*$, see [38, p. 24 and p. 33]).

Therefore we have

$$\begin{aligned}
(h \circ \hat{\pi}_q) &= \hat{\pi}_q^*(h) \quad \text{(by [38, Proposition 3.6 (Chapter II)])} \\
&= \hat{\pi}_q^*(qD_q - D_{q^2}) \\
&= \hat{\pi}_q^*(q(\hat{\pi}_q \circ \pi_q(D)) - (\hat{\pi}_q \circ \pi_q(D_q))) \quad (\text{by } \hat{\pi}_q \circ \pi_q = q) \\
&= q(q(\pi_q(D)) - \pi_q(D_q)) \\
&= q(qD - D_q) \quad (\text{by } \overline{D}, \overline{D_q} \in \mathrm{Jac}_{\mathbb{F}_q}(C)) \\
&= q(f_q) \quad (\text{by } qD = D_q + (f_q)).
\end{aligned}$$

□

Proof of Theorem 7. The bilinearity of $\hat{t}_l$ and the property that $\hat{t}_l(\overline{D},\overline{E}) \neq 1$ follow from Theorem 3 and $\gcd(l,\rho) = 1$. For the latter assertion, from the

definition of the functions f_q, h, f_D and Remark 4 and the fact that ρ is odd, we have

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

6. Cost of the Ate pairing

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

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

Input:	$\overline{D},\overline{E}\in \mathrm{Jac}_{\mathbb{F}_q}(C)[l]\setminus\{\overline{0}\}$.
Output:	Ate pairing $\hat{t}_l(\overline{D},\overline{E})$.
Step 1:	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 $\alpha_i^2,\beta_i^2,\alpha_i\beta_i,\alpha_i^2\beta_i,\alpha_i^3\beta_i$ $(1\le i\le w)$.
Step 3:	Compute the function $\ell(x,y)\in\mathbb{F}_q[x,y]$ s.t. $pD=D'+(\ell(x,y)/h(x))$ with reduced divisor D' and $h(x)\in\mathbb{F}_q[x]$.
Step 4:	$v\leftarrow 1$, $D'\leftarrow D$.
Step 5:	**for** $\boldsymbol{i=1}$ **to** $\boldsymbol{r}$ (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.

Before estimating the cost we specify the case handled here. Consult the appendix of other cases.

1. We represent the input values $\overline{D},\overline{E}$ as the Mumford representation, and assume $\deg\hat{E}=2$ and $\deg f(x)=2$ for $D=\mathrm{div}(f(x),g(x))$. Otherwise, the computation of the Ate pairing is more simple. According to [14] we see that a divisor E with $\deg\hat{E}=1$ (i.e. a degenerate-like divisor) satisfies $\hat{t}_l(\overline{D},\overline{E})\neq 1$ for a random element $\overline{D}\in\mathrm{Jac}_{\mathbb{F}_q}(C)[l]\setminus\{\overline{0}\}$, which leads to a more efficient pairing computation (see Table 5).
2. For the computations of $\phi(\hat{E})$ and $f_q(\phi(\hat{E}))$, we regard E and $\phi(\hat{E})-2(\mathcal{O})$ as divisors (i.e. formal sums of $\overline{\mathbb{F}}_q$-points on C) not as the Mumford representation.

3. We assume that $\operatorname{supp}\hat{E}$ has no $\mathbb{F}_q$-point on C, that is, $\hat{E} = (P) + (\pi_q(P))$ with $P \in C(\mathbb{F}_{q^2}) \setminus C(\mathbb{F}_q)$.

In the appendix we treat the case that $\operatorname{supp}\hat{E}$ has an $\mathbb{F}_q$ rational point and study the formulas for the case that E is kept in Mumford representation.

By M_k (resp. I_k or F_k) we denote the cost of one multiplication on $\mathbb{F}_{q^k}$ (resp. the cost of one inversion on $\mathbb{F}_{q^k}$ or the cost of one p-th power operation on $\mathbb{F}_{q^k}$), and omit the index in the case of $k = 1$. Applying the Karatsuba method, except for some special cases, we can estimate $1M_2 = 3M$, $1M_4 = 9M$, $1I_2 = 4M + 1I$ and $1I_4 = 16M + 1I$ (see Subsection 6.1, or [25] for the more general cases). We further can obtain $1F_k = kF$, for $k = 2$ and 4, when we represent $\mathbb{F}_{q^k} = \mathbb{F}_q(\alpha^{1/k})$. We mention that for the evaluation in this paper, we do not count the cost of addition/subtraction (including doubling and the multiplication by α ($= \pm 2$)) and the shift operation on $\mathbb{F}_q$, $\mathbb{F}_{q^2}$ and $\mathbb{F}_{q^4}$. Therefore, we do not count the cost of the multiplications of the form $\alpha^{i/4} \cdot \alpha^{j/4}$ for $0 \le i, j \le 3$.

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

6.1. Field operation

We estimate the costs of the multiplication and the inversion operations on $\mathbb{F}_{q^2}$ and $\mathbb{F}_{q^4}$ with $\mathbb{F}_{q^2} = \mathbb{F}_q(\alpha^{\frac{1}{2}})$ and $\mathbb{F}_{q^4} = \mathbb{F}_q(\alpha^{\frac{1}{4}})$.

We first consider the operations on $\mathbb{F}_{q^2}$. Let $a = a_0 + a_1\alpha^{\frac{1}{2}}$ and $b = b_0 + b_1\alpha^{\frac{1}{2}}$ ($a_i, b_i \in \mathbb{F}_q$) be two elements of $\mathbb{F}_{q^2}$ with $a \neq 0$. Then we have $ab = (a_0b_0 + \alpha a_1b_1) + \{(a_0 + a_1)(b_0 + b_1) - (a_0b_0 + a_1b_1)\}\alpha^{\frac{1}{2}}$ and $a^{-1} = (a_0^2 - \alpha a_1^2)^{-1}(a_0 - a_1\alpha^{\frac{1}{2}})$, which implies $1M_2 = 3M$ and $1I_2 = 2M + 1I + 2M = 4M + 1I$.

For the operations on $\mathbb{F}_{q^4}$, it is easy to see that $1M_4 = 3M_2 = 9M$ and $1I_4 = 2M_2 + 1I_2 + 2M_2 = 16M + 1I$ in the same way.

6.2. Cost of the distortion map

We estimate the cost of the computation of $\phi(P)$ for $P \in C(\mathbb{F}_{q^2}) \setminus C(\mathbb{F}_q)$ (Step 2 in Table 1).

Before doing this, we should estimate the cost for decomposing E (of the form $\operatorname{div}(f(x), g(x))$) 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 of $\mathbb{F}_q$ (Table 2), which is a special case of the method in [9]. From this, the cost for computing the x-coordinate of the point P is regarded as the sum of those of one $\frac{q+3}{8}$-th power operation and one square 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 $P = (a, b) \in C(\mathbb{F}_{q^2}) \setminus \{\mathcal{O}\}$ with $a \neq 0$, the procedure for computing $\phi(P)$ is described in Table 3, which takes $1I + 2 \cdot 1M + 3M_2 + 2F_2 = 11M + 1I + 4F$. Here we use the fact $a^{-1} = -f_0^{-1} \cdot (a + f_1)$ for $E = \operatorname{div}(f(x), g(x))$ with $f(x) = x^2 + f_1x + f_0$ from the relation between solutions and coefficients with respect to equations. Since the resulting point $\phi(P)$ is of the form $(\varepsilon_1, \varepsilon_2\alpha^{\frac{1}{4}})$ with

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:	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 $r_k > 0$. $B \leftarrow A^{\frac{q+3}{8}}$, $C \leftarrow B^2$ (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 $\pm B\alpha^{\frac{1}{2}}$.

$\varepsilon_i \in \mathbb{F}_{q^2}^*$ $(i = 1, 2)$, the computations of ε_1^2, $(\varepsilon_2\alpha^{\frac{1}{4}})^2$ and $\varepsilon_1^m(\varepsilon_2\alpha^{\frac{1}{4}})$ for $1 \le m \le 3$ take $5M_2 = 15M$ (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 6.3 for the detail).

Table 3. Distortion map ϕ

Input:	A point $P = (a, b) \in C(\mathbb{F}_{q^2}) \setminus \{\mathcal{O}\}$ 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).

6.3. 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 $\ell(x, y) = \gamma y^2 + (sx^3 + tx^2 + ux + v)y + (-x^2 + cx + d)^3$ (see Corollary 1) and $\phi(P) = (\varepsilon_1, \varepsilon_2\alpha^{\frac{1}{4}})$ with $\varepsilon_i \in \mathbb{F}_{q^2}^*$ $(i = 1, 2)$, we estimate the cost of the computation of $\ell(\phi(\hat{E})) = \ell(\phi(P) + \phi(\pi_q(P)))$. We note that $\ell(x, y)$ can be computed in $7 \cdot 2F = 14F$ 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 $6 \cdot 2M + 2M_2 = 18M$ to compute $\ell(\phi(P))$. After the computation of $\ell(\phi(P))$, it costs only $2M_2 = 6M$ for computing $\ell(\phi(\pi_q(P)))$ because we have $\ell(\phi(\pi_q(P))) = -(\gamma n^2)^q + \alpha^r(-sm^3n + tm^2n - umn + vn)^q + (-m^2 - cm + d)^{3q}$ if $\phi(P) = (m, n)$. Here we use the fact $\phi \circ \pi_q = \zeta_8^{2r} \circ \pi_q \circ \phi$, namely $\phi(\pi_q(P)) = (-m^q, \alpha^r n^q)$, and mention that we do not count the cost of the q-th power operation on $\mathbb{F}_{q^2}$ and $\mathbb{F}_{q^4}$ because the computation is performed by only shift operations and

addition/subtraction operations on $\mathbb{F}_q$. So it takes $(18+6)M + 1M_4 = 33M$ to compute $\ell(\phi(\hat{E}))$.

We emphasize that for each $\overline{E} \in \mathrm{Jac}_{\mathbb{F}_q}(C)[l] \setminus \{\overline{0}\}$, 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 $\ell(\phi(\hat{E})) \neq 0, \infty$.

6.4. Total cost

In this subsection, we evaluate the total cost of the computation of the Ate pairing by applying the procedure in Table 1. For a real number x, we denote by $\lceil x \rceil$ the smallest integer greater than or equal to x.

For Step 1, we estimate the cost for computing r_i's (in Step 2 of Table 2) as $1M$ because it costs about $\lceil \log_2 \frac{q+3}{8} \rceil^2$ bit operations, and the cost for the decomposition of the reduced divisor E as $3 \cdot 1M + (\lceil \frac{4}{5} r \rceil M + r \cdot 1F) + 2M$. 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. Here we assume, in Step 2 of Table 2, that $k = r$ and r_i's are uniformly distributed on the set $\{0, 1, \ldots, p-1\}$ (recall that $q = p^r$). Thus, Step 1 takes $(\lceil \frac{4}{5} r \rceil + 6)M + rF$.

For Step 2, it costs $(11M + 1I + 4F) + 15M = 26M + 1I + 4F$ by the argument of Subsection 6.2.

For Step 3, it costs $10M + 7F$ from Corollary 1.

For Step 5, it costs $1F_4 + (14F + 33M) + 1M_4 = 42M + 18F$ for rewriting the value v, that is, the computation of $v^p \cdot \ell(\phi(\hat{E}))$. Therefore, Step 5 takes $33M + (r-1) \cdot (42M + 18F) = (42r - 9)M + 18(r-1)F$, where the first term $33M$ corresponds to the cost for the first routine (i.e. the case of $i = 1$) in Step 5.

For Step 6, it costs $(5M_2 + 1I_2) + 1M_4 = 28M + 1I$ (see Remark 5).

Consequently, we estimate the cost for computing the Ate pairing $\hat{t}_l(\overline{D}, \overline{E})$ as $(42r + \lceil \frac{4}{5} r \rceil + 61)M + 2I + (19r - 7)F$.

As is well known, the inversion is the most heavy operation on $\mathbb{F}_q$ (see Table 4). We need only two inversions to compute the Ate pairing with the procedure in Table 1. The reason is that we need no inversion to obtain the functions $\ell(x,y)$'s into which the divisor $\hat{E}$ is substituted, which is a common property among the class of curves $y^2 = x^p - x + d$ $(d = \pm 1)$ [12].

Table 4. Running time for operations on $\mathbb{F}_q$ with $q = 5^{113}$

multiplication (M)	inversion (I)	p-th power raising (F)	ratio (I/M)
62 μs	617 μs	21 μs	9.95

7. Experimental results

In this section, we implement the Tate and Ate pairings for our curve. We set $r = 113$ for $q = p^r$ and let $\mathbb{F}_q = \mathbb{F}_p[t]/(t^{113} + t^{24} - 1)$. The reason why we choose $r = 113$ is as follows (see Remark 1): (i) the value $q^2 + 1$ has a 173-bit and

a 348-bit prime factors (if l is one of these two primes, then we have $l \parallel q^2+1$); (ii) the embedding degree is equal to four and $q^4 \geq 2^{1024}$ holds (recall that r is an odd prime and that $l \nmid p^4-1$ and that $\lceil \log_5 2^{256} \rceil = 111$).

All computations are performed on a 2.5 GHz Pentium IV with 256 Mb RAM. The language is C with Borland C++ compiler 5.5.1 and with no mathematical library.

Table 5 shows that the Ate pairing is about 50 % more efficient than the Tate pairing, and that the pairing computation for $\deg \hat{E} = 1$ is about 50 % more efficient than that for $\deg \hat{E} = 2$. This implies that the length of the loop (the number of the iteration in Step 5 of Table 1) and the number of points substituted into functions lead directly to the cost performance of these pairings. We further see that the method which represents the divisor $\hat{E} - 2(\mathcal{O})$ as the sum of points is about 50 % more efficient than the one which represents the divisor above as the Mumford representation (see Section 6 and Appendix). The reason is that for the former method, we have a nice relation among three objects, the q-th power Frobenius map, the proposed ditortion map and the functions $\ell(x,y)$'s into which the divisor $\hat{E}$ is substituted. So, if we have a similar one for the Mumford representation, then we might improve the computation of the pairings for our curve. This is one of our future works. We note that the experimental results in the papers [8, 24] show that the difference of the running time of both methods is not so much for the curves $y^2 = x^5 + a$ over $\mathbb{F}_p$ with $p \equiv 2, 3 \pmod 5$ using Miller's Algorithm. However, for our curve, we must deal with more complicated functions (i.e. functions with higher degrees) than those which appear in Miller's algorithm based on the addition chain.

Table 5. Running time for pairings for $y^2 = x^5 - \alpha x$ over $\mathbb{F}_q$ with $q = 5^{113}$

pairing	representation of divisors		theoretical cost	time
Tate pairing	formal sum of points	$\deg \hat{E} = 1$ [14]	$4773M + 2I + 4059F$	420 ms
		$\deg \hat{E} = 2$	$9668M + 2I + 4174F$	764 ms
	Mumford representation		$16312M + 2I + 4061F$	1390 ms
Ate pairing	formal sum of points	$\deg \hat{E} = 1$ [14]	$2409M + 2I + 2025F$	212 ms
		$\deg \hat{E} = 2$	$4898M + 2I + 2140F$	395 ms
	Mumford representation		$8185M + 2I + 2027F$	698 ms

On the other hand, Tables 4 and 5 also show that pairing calculation for our curve is less efficient than that for other pairing-friendly curves, e.g. the Eta pairing for supersingular (hyper-)elliptic curves in characteristic two and three [1] (or [3, 35, 36, 37] from the view of hardware), and the Tate pairing for $y^2 = x^5 + a$ over prime fields $\mathbb{F}_p$ with $p \equiv 2, 3 \pmod 5$ [24]. The main reason is that there exists no fast arithmetic on fields in characteristic five, and that the class of the curves with embedding degree more than four, which contains supersingular (hyper-)elliptic curves above for the Eta pairing, enables one to set the size of definition fields smaller than that for our curve under the same level of security.

8. Conclusions and future works

In this paper, we constructed a distortion map explicitly and described a computation of the Tate pairing by using the proposed map for genus-2 supersingular hyperelliptic curves defined by $y^2 = x^5 - \alpha x$ ($\alpha = \pm 2$) in characteristic five. Next we showed that the Ate pairing can be applied to the curve for the linearly independent groups obtained via the distortion map. Moreover, we described the detailed computational procedure of the Tate and Ate pairings for our curve, and evaluated these two pairings. As a result, we showed the Ate pairing is about 50 % more efficient than the Tate pairing. The experimetnal results also show that our curve is not the most suitable one in comparison with other pairing-friendly curves for now. But, we expect that the pairing computation for our curve will reach at practical level in the future.

There exists also a problem of the construction of pairing-friendly curves of genus more than one, particularly non-supersingular curves. These problems are our future works.

Appendix

We consider $\hat{t}_l(\overline{D}, \overline{E})$ in the two cases: (i) $\hat{E}$ has an $\mathbb{F}_q$-point on C; (ii) we represent $\hat{E} - 2(\mathcal{O})$ using the Mumford representation. For simplicity, the case which we dealed with in Section 6 will be called "general case" in the following. We estimate the cost of the distortion map (Step 2 in Table 1, Table 3) and the cost of $\ell(\phi(\hat{E}))$ (Step 5 in Table 1). In fact, the computation of $\ell(\phi(\hat{E}))$ becomes the main part of the procedure of the Ate pairing (as well as the Tate pairing).

1. Cost of $\hat{t}_l(\overline{D}, \overline{E})$ with supp $\hat{E}$ having an $\mathbb{F}_q$-point on C

We consider the case $\hat{E} = (P_1) + (P_2)$ with $P_i \in C(\mathbb{F}_q)$ for $i = 1, 2$.

Given P_i's, we can estimate the cost of $\phi(\hat{E})$ as $1I + 2M + 2(3M + 2F) = 8M + 1I + 4F$ by the same way as in Subsection 6.2. After that, it takes $2 \cdot 5M = 10M$ to obtain the values associated with $\phi(P_i)$'s (i.e. the latter part of Step 2 in Table 1). We note that each value associated with $\phi(P_i)$'s is represented as $\varepsilon\alpha^{j/4}$ for some $\varepsilon \in \mathbb{F}_q$ and $0 \leq j \leq 3$.

We next consider the computation of $\ell(\phi(\hat{E}))$ (Step 5 in Table 1), given $\ell(x, y) = \gamma y^2 + (sx^3 + tx^2 + ux + v)y + (-x^2 + cx + d)^3$. By the same way as in Subsection 6.3, it takes $2(6M + 2M_2) + 1M_4 = 33M$, which is the same as that in the general case.

2. Cost of $\hat{t}_l(\overline{D}, \overline{E})$ using the Mumford representation

We consider the case where we represent $\hat{E} - 2(\mathcal{O})$ using the Mumford representation throughout the whole procedure of the Ate pairing.

Let $E = \mathrm{div}(a(x), b(x))$ with $a(x) = x^2 + a_1 x + a_0$ and $b(x) = b_1 x + b_0$. Recall that, representing formally $E = (P_1) + (P_2) - 2(\mathcal{O})$ with $P_i = (\alpha_i, \beta_i)$, we have $a(x) = (x - \alpha_1)(x - \alpha_2)$ and $\beta_i = b(\alpha_i)$ for $i = 1, 2$. In addition, the assumption $\deg \hat{E} = 2$ implies $a_0 \neq 0$.

Applying Theorem 4 and the relations above, we can represent the image of the distortion map as follows:

COROLLARY 2. *With the notation above, let*

$$\phi(\hat{E}) - 2(\mathcal{O}) = \mathrm{div}(f(x), g(x)).$$

Then we have

$$f(x) = \begin{cases} x^2 + a_1^{-5}\alpha^{\frac{1}{2}}x - \alpha a_1^{-10} & (P_1 = P_2), \\ x^2 - (a_0^{-1}a_1)^5\alpha^{\frac{1}{2}}x + \alpha a_0^{-5} & (P_1 \neq P_2), \end{cases}$$

$$g(x) = \begin{cases} 2\{a_0a_1(2a_1b_1 + b_0)^{-1}\}^5\alpha\alpha^{\frac{1}{4}}x \\ \quad - 2\{a_0a_1(2a_1b_1 + b_0)^{-1}\}^5\{a_1^{-5} - 2\alpha a_1^{-1}\}^5\alpha^{\frac{3}{4}} & (P_1 = P_2), \\ 2a_0^{-10}\{b_0(a_1^2 - a_0) - a_1a_0b_1\}^5\alpha\alpha^{\frac{1}{4}}x \\ \quad + 2a_0^{-10}(a_0b_1 - a_1b_0)^5\alpha\alpha^{\frac{3}{4}} & (P_1 \neq P_2). \end{cases}$$

We note that $P_1 = P_2$ holds if and only if $a_1^2 + a_0 = 0$.

From the result above, we evaluate the cost of the distortion map as $5M + 2I + 3F$ in the case of $P_1 = P_2$ and as $9M + 1I + 4F$ in the case of $P_1 \neq P_2$.

We next consider the computation of $\ell(\phi(\hat{E}))$ (Step 5 in Table 1), given $\ell(x, y) = \gamma y^2 + (sx^3 + tx^2 + ux + v)y + (-x^2 + cx + d)^3$. Let $\phi(\hat{E}) - 2(\mathcal{O}) = \mathrm{div}(f(x), g(x))$ with $f(x) = x^2 + f_1x + f_0$ and $g(x) = g_1x + g_0$.

For the computation of $\ell(\phi(\hat{E}))$, it is possible to deal with operations modulo $f(x)$ because the x-coordinate of each $\phi(P_i)$ is a root of $f(x)$. From the defining equation and the direct computation, we have

$$\begin{aligned} y^2 \bmod f(x) &= x^5 - \alpha x \bmod f(x) \\ &= \{(f_1^2 + f_0)^2 - \alpha\}x + f_1f_0(f_1^2 - 2f_0). \end{aligned}$$

So, it takes $4M$ to compute $y^2 \bmod f(x)$, which can be computed in advance. We note that each coefficient of the final expression is of the form $\varepsilon\alpha^{j/2}$ with $\varepsilon \in \mathbb{F}_q$ and $j = 0$ or 1.

We set $\sigma_1x + \sigma_0 = sx^3 + tx^2 + ux + v \bmod f(x)$ and $\tau_1x + \tau_0 = (-x^2 + cx + d)^3 \bmod f(x)$, and let $c' = (c + f_1) \in \mathbb{F}_{q^2}$ and $d' = (d + f_0) \in \mathbb{F}_q$. Then we have

$$\begin{cases} \sigma_1 = \sigma_1(s, t, u) = (f_1^2 - f_0)s - f_1t + u, \\ \sigma_0 = \sigma_0(s, t, v) = f_1f_0s - f_0t + v, \\ \tau_1 = \tau_1(c', d') = [\{(f_1^2 - f_0)c' + 2f_1d'\}c' - 2d'^2)]c', \\ \tau_0 = \tau_0(c', d') = f_0(f_1c' + 2d')c'^2 + d'^3. \end{cases}$$

So, we obtain the values above in $2M + 2M + (4M + 2M_2) + (5M + 2M_2) = 25M$ after the computation $y^2 \bmod f(x)$. Hence, we estimate the cost of the computation

$\ell(x,y) \bmod f(x)$ as $2M + 25M = 27M$, where the first term $2M$ is the cost of $\gamma y^2 \bmod f(x)$.

Next, given $\ell'(x,y) := \ell(x,y) \bmod f(x)$, we estimate the computation of $\ell'(\phi(\hat{E}))$. We see that $\ell'(x,y)$ is of the form $(\varepsilon_1 x+\varepsilon_0)y+(\lambda_1 x+\lambda_0)$ with $\varepsilon_i, \lambda_i \in \mathbb{F}_{q^2}$ for $i = 1, 2$ because the polynomial $f(x)$ is defined over $\mathbb{F}_{q^2}$ (or because of the consideration above).

Representing formally $\phi(P_i) = (m_i, n_i)$ for $i = 1, 2$, we have the following relations using proper elements κ_i's of $\mathbb{F}_q$:

$$\begin{cases} \delta_1 := m_1 + m_2 & = -f_1 & = \kappa_1 \alpha^{\frac{1}{2}}, \\ \delta_2 := m_1 \cdot m_2 & = f_0 & = \kappa_2, \\ \delta_3 := n_1 + n_2 & = 2g_0 - f_1 g_1 & = \kappa_3 \alpha^{\frac{3}{4}}, \\ \delta_4 := n_1 \cdot n_2 & = (f_0 g_1 - f_1 g_0) g_1 + g_0^2 & = \kappa_4 \alpha^{\frac{1}{2}}, \\ \delta_5 := m_1 \cdot n_1 + m_2 \cdot n_2 & = (f_1^2 - 2f_0) g_1 - f_1 g_0 & = \kappa_5 \alpha^{\frac{1}{4}}, \\ \delta_6 := m_1 \cdot n_2 + m_2 \cdot n_1 & = 2f_0 g_1 - f_1 g_0 & = \kappa_6 \alpha^{\frac{1}{4}}, \\ \delta_7 := \delta_2 \cdot \delta_3 & & = \kappa_7 \alpha^{\frac{3}{4}}. \end{cases}$$

We mention that for $1 \le i \le 4$, there exist elements ρ_i's of $\mathbb{F}_q$ such that $f_1 = \rho_1 \alpha^{\frac{1}{2}}$, $f_0 = \rho_2$, $g_1 = \rho_3 \alpha^{\frac{1}{4}}$ and $g_0 = \rho_4 \alpha^{\frac{3}{4}}$ from Corollary 2. We can compute δ_i's above in advance, whose cost is $7M$ after the computation $y^2 \bmod f(x)$.

From the direct computation, we obtain

$$\begin{aligned} \ell'(\phi(\hat{E})) = \ & \delta_4\{(\delta_2\varepsilon_1 + \delta_1\varepsilon_0)\varepsilon_1 + \varepsilon_0^2\} \\ & + (\delta_7\lambda_1 + \delta_5\lambda_0)\varepsilon_1 + (\delta_6\lambda_1 + \delta_3\lambda_0)\varepsilon_0 \\ & + (\delta_2\lambda_1 + \delta_1\lambda_0)\lambda_1 + \lambda_0^2, \end{aligned}$$

which takes $(6M + 2M_2) + 3(4M + 1M_2) + 1M_2 = 36M$. We note that the multiplication of the form $\mu_1(\mu_2 \alpha^{\frac{1}{4}})$ with $\mu_i \in \mathbb{F}_{q^2}$ takes $1M_2$.

Finally, we estimate the total cost of the computation of $\ell(\phi(\hat{E}))$ (Step 5 in Table 1) as $27M + 36M = 63M$ (cf. $33M$ in the general case).

Following the consideration above, in case $\hat{E}$ has no multiple point, we can estimate the cost of the Ate pairing $\hat{t}_l(\overline{D}, \overline{E})$ using the Mumford representation as $(72r + 49)M + 2I + (18r - 7)F$ with $q = p^r$, which is about twice as much as that in the general case. We note that, in case $\hat{E}$ has a multiple point, the computation of the Ate pairing (as well as the Tate pairing) is more simple because the divisor E is of the form $E = 2((P) - (\mathcal{O}))$ for some $P \in C(\mathbb{F}_q)$.

Acknowledgments. We are grateful to Steven Galbraith for valuable comments on the earlier version [22] and for giving us the motivation for this work. Moreover we would like to thank the referees for a lot of useful comments, suggestions and encouragements which make this paper more valuable.

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, to appear in Designs, Codes and Cryptography.

[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, Lecture Notes in Computer Science, **2442**, Springer-Verlag, 2002, 354–368.

[3] J.L. Beuchat, M. Shirase, T. Takagi and E. Okamoto, An algorithm for η_T pairing calculation in characteristic three and its hardware implementation. IACR Cryptology ePrint Archive, 2006/327, 2006.

[4] D. Boneh and M. Franklin, Identity-based encryption from the Weil pairing. SIAM J. Computing, **32** (2003), 586–615.

[5] D. Boneh, B. Lynn and H. Shacham, Short signatures from the Weil pairing. Advances in Cryptology—ASIACRYPT 2001, Lecture Notes in Computer Science, **2248**, Springer-Verlag, 2001, 514–532.

[6] D.G. Cantor, Computing in the Jacobian of a hyperelliptic curve. Math. Comp., **48** (1987), 95–101.

[7] Y. Choie, E. Jeong and E. Lee, Supersingular hyperelliptic curves of genus 2 over finite fields. IACR Cryptology ePrint Archive, 2002/032, 2006.

[8] 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**, Springer-Verlag, 2004, 97–111.

[9] H. Cohen, A Course in Computational Algebraic Number Theory. Graduate Texts in Math., **138**, Springer-Verlag, Berlin Heidelberg, 1993.

[10] H. Cohen and H.W. Lenstra Jr., Heuristics on class groups of number fields. Number Theory, Lecture Notes in Mathematics, **1068**, Springer-Verlag, 1984, 33–62.

[11] 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**, Springer-Verlag, 2003, 111–123.

[12] 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, Springer, Berlin, 2000, 73–89.

[13] K. Eisenträger, K. Lauter and P.L. Montgomery, Improved Weil and Tate pairings for elliptic and hyperelliptic curves. Algorithmic Number Theory Symposium—ANTS VI, Lecture Notes in Computer Science, **3076**, Springer-Verlag, 2004, 169–183.

[14] G. Frey and T. Lange, Fast bilinear maps from the Tate-Lichtenbaum pairing on hyperelliptic curves. Algorithmic Number Theory Symposium—ANTS VII, Lecture Notes in Computer Science, **4076**, Springer-Verlag, 2006, 466–479.

[15] 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), 865–874.

[16] S.D. Galbraith, K.G. Paterson and N.P. Smart, Pairings for cryptographers. IACR Cryptology ePrint Archive, 2006/165, 2006.

[17] S.D. Galbraith and J. Pujolás, Distortion maps for genus two curves. Proceedings of a workshop on Mathematical Problems and Techniques in Cryptology, 2005, 46–58. Available at `http://www.isg.rhul.ac.uk/~sdg/jordi-paper.pdf`.

[18] S.D. Galbraith, J. Pujolás, C. Ritzenthaler and B. Smith, Distortion maps for genus two curves. IACR Cryptology ePrint Archive, 2006/375, 2006.

[19] S.D. Galbraith and V. Rotger, Easy decision Diffie–Hellman groups. LMS J. Comput. Math., **7** (2004), 201–218.

[20] R. Granger, F. Hess, R. Oyono, N. Theriault and F. Vercauteren, Ate pairing on hyperelliptic curves. Technical Report CSTR-06-020, 2006.

[21] R. Harasawa, Y. Sueyoshi and A. Kudo, Distortion map for $y^2 = x^5 - \alpha x$ in characteristic five. Proceedings of the 2006 Symposium on Cryptography and Information Security (SCIS 2006), 4C2–3, Hiroshima, 2006.

[22] 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.

[23] R. Harasawa, Y. Sueyoshi and A. Kudo, Ate pairing for $y^2 = x^5 - \alpha x$ in characteristic five. IACR Cryptology ePrint Archive, 2006/202, 2006.

[24] C. Ó hÉigeartaigh and M. Scott, Pairing calculation on supersingular genus 2 curves. IACR Cryptology ePrint Archive, 2006/005, 2006.

[25] F. Hess, N.P. Smart and F. Vercauteren, The Eta pairing revisited. IEEE Transactions on Information Theory, **52**-10, October 2006, 4595–4602.

[26] L. Hitt, On an improved definition of embedding degree. IACR Cryptology ePrint Archive, 2006/415, 2006.

[27] T. Itoh and S. Tsujii, A fast algorithm for computing multiplicative inversion in $GF(2^m)$ using normal bases. Information and Computation, **78** (1988), 171–177.

[28] A. Joux, A one-round protocol for tripartite Diffie–Hellman. Algorithmic Number Theory Symposium—ANTS IV, Lecture Notes in Computer Science, **1838**, Springer-Verlag, 2000, 385–394.

[29] G. Kang and J.H. Park, Powered Tate pairing computation. IACR Cryptology ePrint Archive, 2005/260, 2005.

[30] N. Koblitz, Hyperelliptic cryptosystems. J. Cryptology, **1** (1989), 139–150.

[31] N. Koblitz, CM curves with good cryptographic properties. Advances in Cryptology—CRYPTO '91, Lecture Notes in Computer Science, **576**, Springer-Verlag, 1992, 279–287.

[32] A.K. Lenstra and E.R. Verheul, The XTR public key system. Advances in Cryptology—CRYPTO 2000, Lecture Notes in Computer Science, **1880**, Springer-Verlag, 2000, 1–19.

[33] V. Miller, Short program for functions on curves. IBM Thomas J. Watson Research Center, 1986. Available at `http://crypto.stanford.edu/miller/miller.ps`.

[34] V. Miller, The Weil pairing, and its efficient calculation. J. Cryptology, **17** (2004), 235–261.

[35] R. Ronan, C. Ó hÉigeartaigh, C. Murphy, T. Kerins and P.S.L.M. Baretto, Hardware implementation of the η_T pairing in characteristic 3. IACR Cryptology ePrint Archive, 2006/371, 2006.

[36] R. Ronan, C. Ó hÉigeartaigh, C. Murphy, M. Scott and W. Marnane, An embedded processor for a pairing-based cryptosystem. Proceedings of the Third International Conference on Information Technology: New Generations (ITNG'06), IEEE Computer Society, 2006.

[37] C. Shu, S. Kwon and K. Gaj, FPGA accelerated Tate pairing based cryptosystem over binary fields. IACR Cryptology ePrint Archive, 2006/179, 2006.

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

[39] H. Stichtenoth, Algebraic Function Fields and Codes. Springer Universitext, Springer-Verlag, Berlin Heidelberg, 1993.

[40] H. Stichtenoth and C. Xing, On the structure of the divisor class group of a class of curves over finite fields. Arch. Math., **65** (1995), 141–150.

[41] E.R. Verheul, Evidence that XTR is more secure than supersingular elliptic curve cryptosystems. Advances in Cryptology—EUROCRYPT 2001, Lecture Notes in Computer Science, **2045**, Springer-Verlag, 2001, 195–210.