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

Ryuichi Harasawa, Yutaka Sueyoshi, and Aichi Kudo

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

Abstract

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

Keywords: Ate pairing, Hyperelliptic curves

1 Introduction

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

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

Two years later after the appearance of the Eta pairing, F. Hess et al. [4] simplified the Eta pairing, called the Ate pairing, and extended it to ordinary elliptic curves.

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

of the Tate pairing using that [3]. In this note, we show the Ate pairing can be applied to this curve in the natural way. This leads to about 50% computational cost-saving over the Tate pairing. We remark that our distortion map for $y^2 = x^5 - \alpha x$ does not satisfy the (sufficient) condition for the Eta pairing as it is.

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

In this section, we describe the Ate pairing for $y^2 = x^5 - \alpha x$. We refer the readers to [3] for more details on this curve, including the facts needed in this note and the concrete computation of the pairing.

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

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

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

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

Under the notation above, we obtain the following result.

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

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

defined by

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

is bilinear and has the property that $\hat{t}_l(D, E) \neq 1$ for all $D, E \neq \mathrm{id}$. Furthermore, assuming $(0,\ 0) \notin \mathrm{supp} D$ or $\deg E' = 2$, we have

$$\hat{t}_l(D,\ E) = f \circ \phi\,(E')^{2(q^2-1)},$$

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

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

Remark 1.

For the Tate pairing based on [3] (*see Lemma* 1 *below*), *we need a function* f_D *such that* $q^2D = D_{q^2} + (f_D)$ *with the reduced divisor* D_{q^2}. *This shows that the cost of the Ate pairing is about a half of that of the Tate pairing based on* [3].

Remark 2.

If $(0, 0) \in \mathrm{supp}D$ *and* $\deg E' = 1$, *then* $\hat{t}_l(D, E) = \pm\{f \circ \phi\,(E')^{2(q^2-1)}\}$ *holds, where the signature is determined so that* $\hat{t}_l(D, E) \in \mu_l$ [3, Theorem 7].

The proof of Theorem 1 is similar to that for the supersingular elliptic curves [4, Section 3.2]. We describe the outline.

We first have the following result [3, Remark 3]:

Lemma 1.

With the notation above, we have

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

Next, we set $\hat{\pi}_q = \pi_q \circ \zeta_8^{2r}$. Then we have $\hat{\pi}_q \circ \pi_q = \pi_q \circ \hat{\pi}_q = q$ from [3], namely $\hat{\pi}_q$ is the dual of π_q.

For the proof of Theorem 1, we need two more lemmas.

Lemma 2.

With the notation above, we have

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

Proof.

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

Lemma 3.

With the notation above, we have

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

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 [5, Proposition 2.6. (Chapter II)], the equality $\hat{\pi}_q^*(\sum_{P\in C} n_P(P)) = q(\sum_{P\in C} n_P(\hat{\pi}_q^{-1}(P)))$ holds for every divisor $\sum_{P\in C} n_P(P)$. (For the definition of $\hat{\pi}_q^*$, see [5, p. 24 and p. 33].)

Therefore we have

$$\begin{aligned}
(h\circ\hat{\pi}_q) &= \hat{\pi}_q^*(h) \ \ (\text{by [5, Proposition 3.6. (Chapter II)] }) \\
&= \hat{\pi}_q^*(qD_q - D_{q^2}) \\
&= \hat{\pi}_q^*(q(\hat{\pi}_q\circ\pi_q(D)) - (\hat{\pi}_q\circ\pi_q(D_q))) \ \ (\text{by } \hat{\pi}_q\circ\pi_q = q) \\
&= q(q(\pi_q(D)) - \pi_q(D_q)) \\
&= q(qD - D_q) \ \ (\text{by } D,\, D_q \in \mathrm{Jac}_{\mathbb{F}_q}(C)) \\
&= q(f) \ \ (\text{by } qD = D_q + (f)).\ \square
\end{aligned}$$

Proof of Theorem 1.

The bilinearity of $\hat{t}_l$ and the property that $\hat{t}_l(D,\, E) \neq 1$ follow from [3, Theorem 4] and $\gcd(l, \rho) = 1$. For the latter assertion, from the definition of the functions f, h, f_D and Lemma 1, we have

$$\begin{aligned}
\hat{t}_l(D,\, E) &= \{(f^q h)\circ\phi\,(E')\}^{(q^2-1)\rho} \\
&= \{f^q\circ\phi\,(E')\cdot(h\circ\hat{\pi}_q\circ\phi)(E')\}^{(q^2-1)\rho} \ \ (\text{by Lemma 2}) \\
&= \{f^{2q}\circ\phi\,(E')\}^{(q^2-1)\rho} \ \ (\text{by Lemma 3}) \\
&= f\circ\phi\,(E')^{2(q^2-1)} \\
&\qquad (\text{by } \rho q \equiv 1 \pmod{q^2+1} \text{ and } f\circ\phi\,(E') \in \mathbb{F}_{q^4}^*).\ \square
\end{aligned}$$

Acknowledgemants

We are grateful to Steven Galbraith for comments on the earlier version [3] and for giving us the motivation for this work.

References

1. P. S. L. M. Barreto, S. Galbraith, C. Ó hÉigeartaigh and M. Scott, *Efficient pairing computation on supersingular abelian varieties*, IACR Cryptology ePrint Archive, 2004/375, 2004.
2. 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.

3. 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.
4. F. Hess, N. P. Smart and F. Vercauteren, *The Eta pairing revisited*, IACR Cryptology ePrint Archive, 2006/110, 2006.
5. J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Math., vol. **106**, Springer-Verlag, New York, 1986.