Polynomials for Ate Pairing and $\mathbf{Ate}_i$ Pairing

Zhitu Su[*], Hui Li[†], and JianFeng Ma[‡]
Key lab of Computer Networks and Information Security(Xidian University)
of Ministry of Education, Xidian University
Xi'an, China

May 8, 2008

Abstract

The irreducible factor $r(x)$ of $\Phi_k(u(x))$ and $u(x)$ are often used in constructing pairing-friendly curves. $u(x)$ and $u_c \equiv u(x)^c \pmod{r(x)}$ are selected to be the Miller loop control polynomial in Ate pairing and Ate_i pairing. In this paper we show that when $4|k$ or the minimal prime which divides k is larger than 2, some $u(x)$ and $r(x)$ can not be used as curve generation parameters if we want Ate_i pairing to be efficient. We also show that the Miller loop length can not reach the bound $\frac{\log_2 r}{\varphi(k)}$ when we use the factorization of $\Phi_k(u(x))$ to generate elliptic curves.

1 Introduction

How to implement cryptosystem efficiently is very important in Public-key Cryptography. As pairing-based Cryptography is concerned, the computation of Tate pairing is the bottleneck. Many work have been done such as [8, 2]. All these work are based on Miller's algorithm[12, 13]. The loop length in Miller's algorithm for Tate pairing is about $\log_2 r$. Recently a lot of works are focus on shorten the loop length in Miller's algorithm such as eta pairing [1] which extends [4], Ate pairing [10], optimized Ate pairing [5], Ate_i pairing [17], R-rate pairing [6], optimal pairing [16]. $u(x)$ and $u_c \equiv u(x)^c \pmod{r(x)}$ are selected to be the Miller loop control polynomial in [10, 17]. The Ate_i pairing can be more efficient for some elliptic curves [17]. Usually we select these curves with short Miller loop by computer search. In this paper, we show that some elliptic curves are not suitable for Ate_i pairing. This will aid computer searching. The remainder of this paper is organized as following: in section 2 we describe some backgrounds on pairings. In section 3 our results are presented.

[*]ztsu@mail.xidian.edu.cn
[†]lihui@mail.xidian.edu.cn
[‡]jfma@mail.xidian.edu.cn

2 Some backgrounds

Let $E(\mathbb{F}_q)$ be an elliptic curve over finite field $\mathbb{F}_q$ and $\#E(\mathbb{F}_q)$ be its group order. If its group order has a large enough prime factor r and r divides $q^k - 1$ where k is a small positive integer, but does not divide $q^i - 1$, $0 < i < k$. We call k the *embedding degree* of $E(\mathbb{F}_q)$ and $E(\mathbb{F}_q)$ *pairing-friendly curve*. Usually we use Brezing-Weng's method [3] to generate pairing-friendly curves which can be summarized as follows [7]:

Fix a integer k and a positive square free integer D :
1. Choose a number field K containing $\sqrt{-D}$ and a primitive k-th root of unity ζ_k.
2. Find an irreducible polynomial $r(x) \in \mathbb{Z}[x]$ such that $\mathbb{Q}[x]/(r(x)) \cong K$.
3. Let $t(x) \in \mathbb{Q}[x]$ be a polynomial mapping to $\zeta_k + 1 \in K$.
4. Let $y(x) \in \mathbb{Q}[x]$ be a polynomial mapping to $\frac{\zeta_k - 1}{\sqrt{-D}} \in K$.
5. Let $p(x) \in \mathbb{Q}[x]$ be given by $(t(x)^2 + Dy(x)^2/4$. If $p(x)$ and $r(x)$ represent primes, then the triple $(t(x), r(x), p(x))$ represents a family of curves with embedding degree k and discriminant D.

Let $P \in E[r]$ and $f_{i,P}$ be an $\mathbb{F}_{q^k}$-rational function whose divisor is $(f_{i,P}) = i(P) - ([i]P) - (i-1)\mathcal{O}$. Then the Tate pairing is well-defined, non-degenerated, bilinear pairing

e: $E[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) \rightarrow \mathbb{F}^*_{q^k}/(\mathbb{F}^*_{q^k})^r$

$e(P,Q) \rightarrow \langle P,Q \rangle = f_{r,P}(D)$

For practical purposes, we often use the reduced Tate pairing

$\hat{e}(P,Q) = f_{r,P}(D)^{\frac{q^k-1}{r}}$.

To compute Tate pairing, it requires about $\log_2 r$ iterations of Miller loop. The Ate pairing [10] can short the loop length in Miller's algorithm. Let E be an ordinary elliptic curves over $\mathbb{F}_q$, r a large prime which $r|\#E(\mathbb{F}_q)$ and t the trace of Frobenius(i.e. $\#E(\mathbb{F}_q) = q + 1 - t$). Let π_q be the Frobenius endomorphism, π_q: $E \rightarrow E$: $(x, y) \rightarrow (x^q, y^q)$. For $T = t - 1$, $Q \in \mathbb{G}_2 = E[r] \cap \mathrm{Ker}(\pi_q - [q])$ and $P \in \mathbb{G}_1 = E[r] \cap \mathrm{Ker}(\pi_q - [1])$. $f_{T,Q}(P)$ defines a bilinear pairing which called Ate pairing. It requires about $\log(t-1)$ iterations. Let $T_i \equiv T^i \pmod r$. In [17], the authors define a new pairing $f_{T_i,Q}(P)$ called Ate_i pairing which iterates T_i times in pairing computation using Miller's algorithm. If T and T_i are strictly less than r, we gain some advantages.

Let $E(\mathbb{F}_q)$ be an elliptic curve whose trace $t \neq 0$ and $E(\mathbb{F}_q)$ has a subgroup of order r. In [7] ω is defined to be $\frac{\log r}{\log|t|}$. When the size of subgroup order is fixed, the larger ω is, the shorter the loop length is in Ate pairing. If we use the factorization of $\Phi_k(u(x))$ to construct elliptic curves, then $\omega \leq \varphi(k)$ [7]. It has been conjectured in [16] that any non-degenerate pairing on an elliptic curves without efficiently computable endomorphism different from powers of Frobennius requires at least $\frac{\log_2 r}{\varphi(k)}$ basic Miller iterations. If we take the k-th cyclotomic polynomial to represent the subgroup r, x the Frobenius trace and use Brezing-Weng's method to generate pairing-friendly elliptic curves, then the Miller loop length is about $\frac{\log_2 r}{\varphi(k)}$.

3 Polynomials for Ate pairing and Ate_i pairing

In this section we assume that the use of an irreducible factor of $\Phi_k(u(x))$ to construct pairing-friendly curves. As Ate paring is concerned, we have the following Theorem.

Theorem 1. *Let* $\mathrm{deg}u(x) = a$*, the minimal Miller loop length for* Ate *pairing is* $\frac{a\log_2 r}{(a-1)\varphi(k)}$.

Proof. Suppose $\Phi_k(u(x)) = r_1(x)r_2(x)$, from [7] we know that $\mathrm{deg}r_1(x) = a_1\varphi(k)$, $\mathrm{deg}r_2(x) = a_2\varphi(k)$ where $a_1 + a_2 = a$. If $a_1 \geq a_2$, we select $r_1(x)$ to represent the subgroup r. Then $\lim_{x\to\infty} \frac{\log r_1(x)}{\log t(x)} = \frac{a_1}{a}\varphi(k) = \frac{a_1}{a_1+a_2}\varphi(k)$. Since $\Phi_k(u(x))$ splits, $a_2 \geq 1$. So the maximal value of ω is $\frac{a-1}{a}\varphi(k)$(i.e. the minimal Miller loop length for Ate pairing is $\frac{a\log_2 r}{(a-1)\varphi(k)}$). □

If a ia large enough, then $\omega \approx \varphi(k)$.

To construct elliptic curves with property described above, we must find $u(x)$ and $r(x)$ such that $r(x)|\Phi_k(u(x))$ and $\mathrm{deg}r(x) = (a-1)\varphi(k)$ where $\mathrm{deg}u(x) = a$. The method described in [15] can be used to find these polynomials. In [15] power integral basis is employed to find $u(x)$ which would make $\Phi_k(u(x))$ factorable and we know that one irreducible factor of $\Phi_k(u(x))$ is of degree $\varphi(k)$. Usually $\Phi_k(u(x))$ splits into two irreducible factors, so the other has degree $(a-1)\varphi(k)$. The irreducible factor of degree $(a-1)\varphi(k)$ has some special property.

Proposition 1. *For a fixed* k*, if* $\Phi_k(u(x))$ *splits into two irreducible factors, then there is an irreducible factor* $r(x)$ *such that* $2 \cdot \mathrm{deg}u(x) \leq \mathrm{deg}r(x)$ *iff* $\varphi(k) \geq 4$.

Proof. Assume $\Phi_k(u(x)) = r_1(x)r_2(x), \mathrm{deg}r_1(x) = a_1\varphi(k), \mathrm{deg}r_2(x) = a_2\varphi(k)$, where $a_1 + a_2 = a$ and $a_1 \geq a_2$. If $a_1\varphi(k) \geq 2a$, then $a_1\varphi(k) \geq 2(a_1 + a_2)$. It follows that $\varphi(k) \geq \frac{2a_2}{a_1} + 2$. Since $0 < \frac{a_2}{a_1} \leq 1$ and $2|\varphi(k)$, we have $\varphi(k) \geq 4$.

If $\varphi(k) \geq 4$, then $a_1\varphi(k) \geq 4a_1$. Since $a_1 \geq a_2$, $a_1 \geq \frac{a}{2}$. So $a_1\varphi(k) \geq 4a_1 \geq 4 \cdot \frac{a}{2} = 2a$. □

Using PARI[14], we have following examples.

Example 1. $k = 15$, $u(x) = x^7 - 7x^6 + 20x^5 - 29x^4 + 20x^3 - 2x^2 - 4x$, $\Phi_{15}(u(x)) = (x^8 - 9x^7 + 35x^6 - 76x^5 + 99x^4 - 76x^3 + 30x^2 - 4x + 1)(x^{48} - 47x^{47} + 1074x^{46} + \cdots + 8x + 1)$, $\varphi(15) = 8$, $a = 7$, $(a-1)\varphi(15) = (7-1)\cdot 8 = 48$

Example 2. $k = 8$, $u(x) = x^3$, $\Phi_8(u(x)) = (x^4 + 1)(x^8 - x^4 + 1)$.

Example 3. $k = 10$, $u(x) = \frac{600}{541}x^7 + \frac{1305}{541}x^6 + \frac{4496}{541}x^5 + \frac{6895}{541}x^4 + \frac{11280}{541}x^3 + \frac{8515}{541}x^2 + \frac{1034}{541}x - \frac{1651}{541}$, $\Phi_{10}(u(x)) = \frac{1}{85662167761}(x^8 + 2x^7 + \cdots - 4x + 1)$ $(129600000000x^{20} + 868320000000x^{19} + \cdots + 11009524377905)$

According to Proposition 1, if $\varphi(k) \geq 4$ then $\deg r(x) = (a-1)\varphi(k) > 2a = 2 \cdot \deg u(x)$. This provides important information for constructing pairing-friendly curves. If some $\sqrt{-D} \in \mathbb{Q}[x]/(r(x))$, Brezing-Weng's method can be used to generating curve with such property. Otherwise we can take Scott-Barreto's approach [7, 11].

Before discussing Ate_i pairing, we introduce some properties about $u(x)$ and $u_c(x) \equiv u(x)^c \pmod{r(x)}$ where $1 < c < k$.

The following lemma extends the result of Galbraith, McKee and Valença [9].

Lemma 1. *Let ζ_k be a primitive k-th root of unity and $\mathbb{Q}(\zeta_k)$ the k-th cyclotomic field. Then $\Phi_k(u(x))$ splits where $u(x) \in \mathbb{Q}[x]$ iff there exists an finite extension $\mathbb{E}$ of $\mathbb{Q}$ such that $\zeta_k \in \mathbb{E}$ and $u(x) = \zeta_k$ has a solution in $\mathbb{E}$.*

Proof. See [15]. □

Lemma 2. *If $\Phi_k(u(x))$ is reducible and has $r(x)$ as an irreducible factor, then $\Phi_{\frac{k}{(c,k)}}(u_c(x))$ is also reducible where $1 < c < k$ and $u_c(x) \equiv u(x)^c \pmod{r(x)}$. $r(x)$ is a common factor for $\Phi_{\frac{k}{(c,k)}}(u_c(x))$.*

Proof. Let θ be a root for the equation $u(x) = \zeta_k$ and $r(\theta) = 0$, then $u(\theta)^c = \zeta_k^c$ is a $\frac{k}{(c,k)}$-th primitive root of unity(i.e. $u(\theta)^c = \zeta_{\frac{k}{(c,k)}}$). Hence $u(x)^c = \zeta_{\frac{k}{(c,k)}}$ has a solution θ, according to Lemma 1, $\Phi_{\frac{k}{(c,k)}}(u(x)^c)$ splits. Since $\Phi_{\frac{k}{(c,k)}}(u(\theta)^c) = 0$ and $r(x)$ is irreducible, we have $r(x)|\Phi_{\frac{k}{(c,k)}}(u(x)^c)$. From the assumption we know that $u(x)^c = f(x)r(x) + u_c(x)$, hence $u_c(\theta) = \zeta_{\frac{k}{(c,k)}}$. By the same reason mentioned above, we can draw the conclusion. □

Let S denote the set $\{u_c(x) \equiv u(x)^c \pmod{r(x)}, \gcd(c,k) = 1\}$. These are the k-th primitive root of unity modulo $r(x)$. They form a group. There is some $u_{min}(x) \in S$ has minimal degree. Given $u_c \in S$, there exists $s \in \mathbb{Z}^+$ such that $u_c(x) \equiv u_{min}(x)^s \pmod{r(x)}$. If $u(x) \equiv u_{min}(x)^c \pmod{r(x)}$, then $\deg u(x) \geq u_{min}(x)$. By lemma 2, $r(x)|\Phi_k(u_{min}(x))$. So if we use $u_{min}(x)$ and $r(x)$ as curve's generation parameters, we gain no advantages in using Ate_i pairing when k is prime.

Example 4. *$k = 8$, $u(x) = \frac{2}{3}x^3 + \frac{1}{3}x^2 + x - \frac{5}{3}$, and $r(x) = 16x^8 + 32x^7 + 88x^6 - 8x^5 - 31x^4 - 308x^3 - 16x^2 - 44x + 353$, let $c = 3, 5, 7$ such that $\gcd(\mathrm{c,k}) = 1$, then $u_3(x) = \frac{2}{9}x^7 + \frac{1}{9}x^6 + \frac{11}{18}x^5 - \frac{29}{36}x^4 + \frac{2}{3}x^3 - \frac{14}{9}x^2 + \frac{25}{18}x - \frac{49}{36}$, $u_5(x) = -\frac{2}{3}x^3 - \frac{1}{3}x^2 - x + \frac{5}{3}$, $u_7(x) = -\frac{2}{9}x^7 - \frac{1}{9}x^6 - \frac{11}{18}x^5 + \frac{29}{36}x^4 - \frac{2}{3}x^3 + \frac{14}{9}x^2 - \frac{25}{18}x + \frac{49}{36}$.*

Example 5. *$k = 5$, if $u(x) = \frac{600}{541}x^7 - \frac{1305}{541}x^6 + \frac{4496}{541}x^5 - \frac{6895}{541}x^4 + \frac{11280}{541}x^3 - \frac{8515}{541}x^2 + \frac{1034}{541}x + \frac{1651}{541}$, then $\Phi_5(u(x)) = \frac{1}{85662167761}r_1(x)r_2(x)$ where $r_1(x) = x^8 - 2x^7 + 7x^6 - 10x^5 + 16x^4 - 10x^3 - 2x^2 + 4x + 1$ and $r_2(x) = 129600000000x^{20} - 868320000000x^{19} + \cdots + 11009524377905$, we select $r(x) = r_2(x)$, then $\deg u_2(x) = 14, \deg u_3(x) = 19, \deg u_4(x) = 19$.*

Theorem 2. *Suppose* $4|k$ *or the minimal prime which divides* k *is larger than* 2, *if* $\Phi_k(u(x)) = r_1(x)r_2(x)$ *and* $\text{deg}r_1(x) \geq \text{deg}r_2(x)$, *then there does not exist* $u_c(x) \equiv u(x)^c \pmod{r_1(x)}$, *where* $\gcd(c,k) \neq 1$, $1 < c < k$ *and* $c \neq \frac{\varphi(k)}{2}$ *such that* $\text{deg}u_c(x) < \text{deg}u(x)$.

Proof. Let $k = p_1^{l_1} \cdots p_m^{l_m}$ where $p_1 < p_2 \cdots < p_m$, $u_c(x) \equiv u(x)^c \pmod{r_1(x)}$, $\text{deg}u_c(x) = b$ and $\text{deg}r_1(x) = a_1\varphi(k)$, then the degree of $\Phi_{\frac{k}{(c,k)}}(u_c(x))$ is $b\varphi(\frac{k}{(c,k)})$. By Lemma 2, $\Phi_{\frac{k}{(c,k)}}(u_c(x))$ is factorable and has $r_1(x)$ as an irreducible factor. Hence we have $b\varphi(\frac{k}{(c,k)}) > a_1\varphi(k)$(i.e. $b > \frac{a_1\varphi(k)}{\varphi(\frac{k}{(c,k)})}$). When $\gcd(c,k) \neq 1$, the maximal value for $\varphi(\frac{k}{(c,k)})$ is $\frac{\varphi(k)}{p_1-1}$ if $l_1 = 1$ or $\frac{\varphi(k)}{p_1}$ if $l_1 > 1$. If $a > b$ where $a = \text{deg}u(x)$, it follows that $a_1 < \frac{a}{p_1}$ or $a_1 < \frac{a}{p_1-1}$. Since $4|k$ or the minimal prime which divides k is larger than 2, we have $a_1 < \frac{a}{2}$. But $a_1 \geq \frac{a}{2}$, a contradiction. So $\text{deg}u_c(x) \geq \text{deg}u(x)$. □

Example 6. *Let* $k = 8$, $u(x) = \frac{3}{280}x^7 + \frac{19}{140}x^5 + \frac{99}{140}x^3 + \frac{26}{35}x$, *we have* $\Phi_8(u(x)) = \frac{1}{6146560000}r_1(x)r_2(x)$ *where* $r_1 = x^8 + 12x^6 + 56x^4 + 72x^2 + 100$ *and* $r_2 = 81x^{20} + 3132x^{18} + \cdots - 44255232x^2 + 61465600$, *we select* $r(x) = r_2(x)$, *when* $c = 2, 6$ *we have* $\text{deg}u_2(x) = 14, \text{deg}u_6(x) = 14$.

Hence if $u_{min}(x) \in \{u_s(x) \equiv u(x)^s \pmod{r(x)}, 1 < s < k, \gcd(\text{s},\text{k}) = 1\}$ such that $u_{min}(x)$ has minimal degree, by Theorem 2, $\text{deg}u_c(x) \geq \text{deg}u_{min}(x)$ for all $u_c(x) \equiv u(x)^c \pmod{r(x)}, 1 < c < k$. Hence curves that have such property should be avoided in Ate_i pairing.

Proposition 2. *If the irreducible factors of* $\Phi_k(u(x))$ *are used to generate pairing-friendly curves, then the Miller loop length of* Ate_i *pairing can not reach the bound* $\frac{\text{log}r}{\varphi(k)}$.

Proof. Suppose $r(x)$ is an irreducible factor of $\Phi_k(u(x))$ and $\text{deg}r(x) = a\varphi(k)$, by Lemma 2, $r(x)|\Phi_{\frac{k}{(c,k)}}(u_c(x))$ where $u_c \equiv u(x)^c \pmod{r(x)}$. Let $\text{deg}u_c(x) = b$, if the Miller loop length of Ate_i pairing is $\frac{\text{log}r}{\varphi(k)}$, then $b = a$, which means that $\text{deg}\Phi_{\frac{k}{(c,k)}}(u_c(x)) = a \cdot \varphi(\frac{k}{(c,k)})$. Since $r(x)$ is irreducible factor of $\Phi_{\frac{k}{(c,k)}}(u_c(x))$, then $\text{deg}r(x) = a \cdot \varphi(k) < \text{deg}\Phi_{\frac{k}{(c,k)}}(u_c(x)) = a \cdot \varphi(\frac{k}{(c,k)})$, a contradiction. □

References

[1] P.S.L.M. Barreto, S.D. Galbraith, C.Ó hÉigeartaigh, and M. Scott, Efficient pairing computation on supersingular abelian varieties, *Designs, Codes and Cryptography*, 42(3), 239-271(2007).

[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*, LNCS 2442, 354-368(2002).

[3] F. Brezing and A. Weng, Elliptic curves suitable for pairing based cryptography, *Designs, Codes and Cryptography*, 37, 133-141(2005).

[4] I. Duursma and H. Lee,Tate Pairing Implementation for Hyperelliptic Curves $y^2 = x^p - x + d$, *Advances in Cryptology-Asiacrypt'2003*, LNCS 2894, 111-123(2003).

[5] S. Matsuda, N. Kanayama, F. Hess, and E. Okamoto. Optimised Versions of the Ate and Twisted Ate Pairings, *The 11th IMA International Conference on Cryptography and Coding*, LNCS 4887, 302-312(2007).

[6] E.Lee, H.Lee, and C.Park, Efficient and Generalized Pairing Computation on Abelian Varieties, Cryptology ePrint Archive Report 2008/040, Available at: http://eprint.iacr.org/2008/040.

[7] D. Freeman, M. Scott, E. Teske, A taxonomy of pairing-friendly elliptic curves, Cryptology ePrint Archive Report 2006/372, Available at: http://eprint.iacr.org/2006/372.

[8] S.D. Galbraith, K. Harrison and S. Soldera, Implementing the Tate pairing, *Algorithmic Number Theory Symposium ANTS-V*, LNCS 2369, 324-337(2002).

[9] S. Galbraith, J. McKee, and P. Valença, Ordinary abelian varieties having small embedding degree, Finite Fields and Their Applications, 13, 800-814(2007).

[10] F. Hess, N. Smart, and F. Vercauteren, The Eta Pairing Revisited, *IEEE Transactions on Information Theory*, 52(10), 4595-4602(2006).

[11] W.D.B Junior, S.D. Galbraith, Constructing Pairing-Friendly Elliptic Curves Using Gröbner Basis Reduction, *The 11th IMA International Conference on Cryptography and Coding*, LNCS 4887, 336-345(2007).

[12] V.S. Miller, Short Programs for functions on Curves, Unpublished manuscript 1986, Available at http://crypto.stanford.edu/miller/miller.pdf.

[13] V.S. Miller, The Weil Pairing,and Its Efficient Calaculation, *Journal of Cryptology*, 17, 235-261(2004).

[14] PARI/GP, Computer Algebra System, Available at: http://pari.math.u-bordeaux.fr.

[15] Zhitu Su, Hui Li, and Jianfeng Ma, Factoring Polynomials for Constructing Pairing-friendly Elliptic Curves, Cryptology ePrint Archive Report 2008/008, Available at: http://eprint.iacr.org/2008/008.

[16] F. Vercauteren, Optimal Pairings, Cryptology ePrint Archive Report 2008/096, Available at: http://eprint.iacr.org/2008/096.

[17] C. Zhao, F. Zhang and J. Huang, A Note on the Ate Pairing, Cryptology ePrint Archive Report 2007/247, Available at: http://eprint.iacr.org/2007/247.