A Note on the Ate Pairing

Chang-An Zhao, Fangguo Zhang and Jiwu Huang

[1] School of Information Science and Technology,
Sun Yat-Sen University, Guangzhou 510275, P.R.China
[2] Guangdong Key Laboratory of Information Security Technology,
Sun Yat-Sen University, Guangzhou 510275, P.R.China
zhcha@mail2.sysu.edu.cn
isszhfg@mail.sysu.edu.cn
isshjw@mail.sysu.edu.cn

Abstract. The Ate pairing has been suggested since it can be computed efficiently on ordinary elliptic curves with small values of the traces of Frobenius t. However, not all pairing-friendly elliptic curves have this property. In this paper, we generalize the Ate pairing and find a series of variations of the Ate pairing. We show that the shortest Miller loop of the variations of the Ate pairing can possibly be as small as $r^{1/\varphi(k)}$ on more pairing-friendly curves generated by the method of complex multiplications, and hence speed up the pairing computation significantly.

Keywords: Tate pairing, Ate pairing, Elliptic curves, Pairing-based cryptosystems.

1 Introduction

Pairing-based cryptosystems have been one of the most active areas in elliptic curve cryptography since 2000. Some detailed summaries on this subject can be found in [19, 14]. There are three early developing contributions which inspire many other pairing-based cryptographic applications in this area: Sakai *et al.*'s pairing-based key agreement [20], Joux's three-party key agreement [13] and Boneh and Franklin's identity-based encryption [4]. A bottleneck for implementing pairing-based cryptosystems is to compute the bilinear pairings.

Many efficient algorithms for computing the pairings have been proposed. Some excellent summaries of pairings are recommended [11, 21]. BKLS-GHS algorithm [2, 10] was proposed for its good efficiency on supersingular elliptic curves of small characteristic. Later the Duursma-Lee method for some special supersingular curves was presented in [7]. Barreto *et al.* extended the Duursma-Lee method and proposed the Eta pairing [1] which can be computed efficiently on supersingular Abelian varieties. Inspired by the Eta pairing, Hess *et al.* suggested the Ate pairing [12] on ordinary elliptic curves. The main techniques in [1, 12] were to shorten the iteration loop in Miller's algorithm [17]. Matsuda *et al.* optimized the Ate pairings and the twisted Ate pairings and showed that both of them are always at least as fast as the Tate pairing [16]. The Ate pairing has been one of the fastest pairings till now.

The Miller loop of the Ate pairing is often determined by the value of the trace of Frobenius t modulo the subgroup order r. For fast pairing computation, $t-1 \bmod r$ should be made as small as possible. There do exist some special pairing-friendly curves with t which can be as small as $r^{1/\varphi(k)}$ [6]. Freeman has also discussed how to construct the curves which are optimal for the Ate pairing [9]. However, not all pairing-friendly elliptic curves have this excellent property [18, 5], i.e., the Miller loop of the Ate pairing does not achieve $r^{1/\varphi(k)}$ on these curves. Therefore, computing the Ate pairing is not always highly efficient for pairing-friendly curves with t whose size is about $\sqrt{q}$.

In this paper, we tackle this problem by generalizing the Ate pairing. We find a series of the variations of the Ate pairing which include the original Ate pairing in [12, 16] as a particular case. We explore how to choose the generalized Ate pairing having the shortest Miller loop which could possibly be as small as $r^{1/\varphi(k)}$. For more ordinary elliptic curves suitable for pairing-based crytosystems, the Miller loop of the generalized Ate pairing can be as small as $r^{1/\varphi(k)}$ and hence speeds up the pairing computations significantly.

This paper is organized as follows. Section 2 introduces basic mathematical concepts of the Tate pairing and the Ate pairing. Section 3 generalizes the Ate pairing and shows how to choose the optimal parameter of the generalized Ate pairing for fast pairing computations. Section 4 gives efficiency considerations. We summarizes our work in section 5 .

2 Mathematical Preliminaries

2.1 The Tate Pairing

Let $\mathbb{F}_q$ be a finite field with $q = p^m$ elements, where p is a prime. Let E be an elliptic curve defined over $\mathbb{F}_q$, and let $\mathcal{O}$ be the point at infinity. Let r be a prime such that $r|\#E(\mathbb{F}_q)$, and let k be the embedding degree, i.e., the minimal positive integer such that $r|q^k - 1$. We also assume that r^2 does not divide $q^k - 1$ and k is greater than 1.

Let $P \in E[r]$ and $Q \in E(\mathbb{F}_{q^k})$, and let D be the divisor which is equivalent to $(Q) - (\mathcal{O})$. For every integer i and point P, let $f_{i,P}$ be a function such that

$$(f_{i,P}) = i(P) - (iP) - (i-1)(\mathcal{O}).$$

Then the Tate pairing is a map

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

$$e(P, Q) = f_{r,P}(D).$$

By Theorem 1 in [2], one can define the reduced Tate pairing as

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

The above definition is convenient since a unique element of $\mathbb{F}_{q^k}$ is required in many cryptographic protocols. Note that $f_{r,P}(Q)^{(q^k-1)/r} = f_{N,P}(Q)^{(q^k-1)/N}$ provided that $r \mid N \mid q^k - 1$.

2.2 Miller's Algorithm

In this subsection, we briefly recall how the Tate pairing can be computed in polynomial time using Miller's algorithm [17].

Let $P \in E[r]$ and $Q \in E(\mathbb{F}_{q^k})$. Let $l_{R,T}$ be the equation of the line through points R and T, and let v_S be the equation of the vertical line through point S. Then for $i, j \in \mathbb{Z}$, we have

$$f_{i+j,P}(Q) = f_{i,P}(Q) f_{j,P}(Q) \frac{l_{iP,jP}(Q)}{v_{(i+j)P}(Q)}.$$

Miller's algorithm is described as follows.

Miller's algorithm

Input: $r = \sum_{i=0}^{n} l_i 2^i$, where $l_i \in \{0,1\}$. $P \in E[r]$ and $Q \in E(F_{q^k})$.

Output: $e(P,Q)$

1. $T \leftarrow P$, $f_1 \leftarrow 1$
2. for $i = n-1, n-2, ..., 1, 0$ do
   - 2.1 $f_1 \leftarrow f_1^2 \cdot \frac{l_{T,T}(Q)}{v_{2T}(Q)}$, $T \leftarrow 2T$
   - 2.2 if $l_i = 1$ then
   - 2.3 $f_1 \leftarrow f_1 \cdot \frac{l_{T,P}(Q)}{v_{T+P}(Q)}$, $T \leftarrow T + P$
3. return $f_1^{(q^k-1)/r}$

2.3 The Ate Pairing

We cite the definition of the Ate pairing from [12] for convenient discussions. Let E be an ordinary elliptic curve over $\mathbb{F}_q$, r a large prime with $r \mid \#E(\mathbb{F}_q)$ and denote the trace of Frobenius with t, i.e., $\#E(\mathbb{F}_q) = q + 1 - t$. Let k be its embedding degree, i.e., the minimal positive integer such that $q^k \equiv (t-1)^k \equiv 1 \bmod r$. Let π_q be the Frobenius endomorphism, $\pi_q : E \to E : (x,y) \mapsto (x^q, y^q)$. For $T = t-1$, $Q \in \mathbb{G}_2 = E[r] \cap Ker(\pi_q - [q])$ and $P \in \mathbb{G}_1 = E[r] \cap Ker(\pi_q - [1])$, we define the Ate pairing as follows:

$$(Q, P) \mapsto f_{T,Q}(P).$$

We also have the reduced Ate pairing $f_{T,Q}(P)^{(q^k-1)/r}$ which equals a fixed power of the reduced Tate pairing. The Ate pairing is much more efficient than the Tate pairing on ordinary elliptic curves with small traces of Frobenius t.

3 The Generalizations of the Ate Pairing

3.1 The Generalized Ate pairing

The main result of this paper is summarized in the following theorem.

Theorem 1. *Let E be an ordinary elliptic curve over $\mathbb{F}_q$, r a large prime with $r \mid \#E(\mathbb{F}_q)$ and denote the trace of Frobenius by t. Let k be its embedding degree. For $T^i \equiv (t-1)^i \equiv q^i \bmod r$ where $i \in \mathbb{Z}_k$, we denote $T_i = T^i \bmod r$. For $Q \in \mathbb{G}_2 = E[r] \cap Ker(\pi_q - [q])$ and $P \in \mathbb{G}_1 = E[r] \cap Ker(\pi_q - [1])$, we have the following:*

- *$f_{T_i,Q}(P)$ defines a bilinear pairing, which we call the Ate$_i$ Pairing.*
- *let a be the minimal positive integer such that $T_i^a \equiv 1 \mod r$. Let $N = gcd(T_i^a - 1, q^k - 1)$ and $T_i^a - 1 = LN$, then*

$$e(Q,P)^L = f_{T_i,Q}(P)^{c(q^k-1)/N}$$

where $c \equiv \sum_{j=0}^{a-1} T_i^{a-1-j}(q^i)^j \mod N$.
- *for $r \nmid L$, the Ate$_i$ Pairing is non-degenerate.*

It is easily checked that such a in Theorem 1 must exist and divide k by Lagrange's Theorem. The proof of Theorem 1 parallels the proof in [12].

Proof of Theorem 1: Note that $r \mid N$ since $T_i^a \equiv 1 \bmod r$ and $q^k \equiv 1 \bmod r$. Thus we have

$$e(Q,P) = f_{r,Q}(P)^{(q^k-1)/r} = f_{N,Q}(P)^{(q^k-1)/N}.$$

Lemma 1 in [12] implies

$$\begin{aligned} e(Q,P)^L =& f_{N,Q}(P)^{L(q^k-1)/N} = f_{LN,Q}(P)^{(q^k-1)/N} \\ =& f_{T_i^a-1,Q}(P)^{(q^k-1)/N} = f_{T_i^a,Q}(P)^{(q^k-1)/N} \end{aligned} \tag{1}$$

By lemma 2 in [12], we have

$$f_{T_i^a,Q} = f_{T_i,Q}^{T_i^{a-1}} f_{T_i,T_iQ}^{T_i^{a-2}} \cdots f_{T_i,T_i^{a-1}Q}. \tag{2}$$

Now we need to derive the relations between f_{T_i,T_i^jQ} and $f_{T_i,Q}$, where $j \in \mathbb{Z}_a$. Since $\pi_{q^i}^j$ is purely inseparable of degree q^{ij} and $\pi_{q^i}^j(Q) = [q^{ij}]Q = [T^{ij}]Q = [T_i^j]Q$, we have

$$\begin{aligned} (\pi_{q^i}^j)^*(f_{T_i,T_i^jQ}) =& (\pi_{q^i}^j)^*(f_{T_i,\pi_{q^i}^j}(Q)) \\ =& q^{ij}T_i(Q) - q^{ij}(T_iQ) - q^{ij}(T_i-1)(\mathcal{O}) \\ =& (f_{T_i,Q}^{q^{ij}}). \end{aligned}$$

Also, $(\pi_{q^i}^j)^*(f_{T_i,T_i^jQ}) = (f_{T_i,T_i^jQ} \circ \pi_{q^i}^j)$, hence we can easily obtain

$$f_{T_i,T_i^j(Q)} = f_{T_i,Q}^{\sigma^{ij}}$$

with σ the q-th power Frobenius automorphism of $\overline{\mathbb{F}}_q$. Since $P \in \cap Ker(\pi_q - [1])$, we have

$$f_{T_i,T_i^j(Q)}(P) = f_{T_i,Q}^{\sigma^{ij}}(P) = (f_{T_i,Q}(P))^{q^{ij}}. \tag{3}$$

Substituting the above equality (3) into (2), we get

$$f_{T_i^a,Q} = f_{T_i,Q}^{\sum_{j=0}^{a-1} T_i^{a-1-j}(q^i)^j}. \tag{4}$$

Finally, substituting (4) into (1) yields

$$e(Q,P)^L = f_{T_i,Q}(P)^{c(q^k-1)/N}$$

where $c \equiv \sum_{j=0}^{a-1} T_i^{a-1-j}(q^i)^j \bmod N$. This equation shows that $f_{T_i,P}$ is a bilinear pairing, which is non-degenerate provided that $r \nmid L$. This completes the whole proof of Theorem 1. □

By Theorem 1, we can obtain a series of the Ate$_i$ pairings $f_{T_i,Q}(P)$ as i varies in $\mathbb{Z}_k$. We also can define the reduced Ate$_i$ pairing by $f_{T_i,Q}(P)^{(q^k-1)/r}$ which is also a fixed power of the reduced Tate pairing. Note that $T_i = T^i \equiv q^i \bmod r$ and the Miller loop of $f_{T_i,Q}(P)$ is determined by the bit length of T_i. Furthermore, we can also generate the twisted Ate pairing easily and obtain a series of the generalized twisted Ate pairing using the same idea.

3.2 Selection of the Optimal T_i

In this subsection, we discuss how to choose T_i which has the shortest bit length for fast pairing computations.

By non-degeneracy, T_i can not be ± 1. Let $\phi_d(x)$ be d-th cyclotomic polynomial with its degree $\varphi(d)$ for some positive integer d [15]. Since $x^k - 1 = \prod_{d|k} \phi_d(x)$ and $T_i^k - 1 \equiv 0 \bmod r$, T_i must satisfy the equation $\phi_d(x) \equiv 0 \bmod r$ for some d. For optimal parameters, we should make $d = k$, i.e., the minimal T_i should be a root of $\phi_k(x) \equiv 0 \bmod r$. Therefore, we can compute $T_i = T^i \equiv q^i \bmod r$, and choose T_i which has the shortest bit length for fast pairing computations.

We found that the optimal T_i is of size $r^{1/\varphi(k)}$ on many pairing-friendly elliptic curves [6, 18, 5] although some of these curves have large values of Frobenius traces t. However, it should be pointed out that the optimal T_i maybe not reach the lower bound $r^{1/\varphi(k)}$ in some special cases (see examples in [3, 8]). An open problem is what relations of q, k and r can makes that the smallest $q^i \bmod r$ reach the lower bound $r^{1/\varphi(k)}$.

4 Efficiency Consideration

In [12], Hess *et al*. give a detailed efficiency analysis of computing the Ate pairing on special pairing-friendly curves with t as small as $r^{1/\varphi(k)}$. In this case, the optimal T_i equals to $T = t - 1$.

The Miller loop of the optimized Ate pairing equals to $T \equiv q \bmod r$ in [16]. Note T is often of size $\sqrt{q}$, which does not achieve $r^{1/\varphi(k)}$ for some pairing-friendly curves [18, 5]. However, we can make that the optimal T_i is possibly as small as $r^{1/\varphi(k)}$ on these pairing-friendly elliptic curves. Therefore, the Ate_i pairing which have the optimal T_i can be computed more faster than the original Ate pairing or the optimized Ate pairing in [16]. In a sense, the optimal Ate_i pairing seems to be computed efficiently for more pairing-friendly curves.

We list some pairing-friendly curves which have large values of the trace of Frobenius in Appendix. Since these ordinary curves is suitable for different security levels and the cost of Arithmetic in finite fields is often determined by various efficient techniques, we only compare the bit length of the loop of the pairings on these pairing-friendly curves. Note the following Ate_i pairing has the minimal loop T_i which is as small as $r^{1/\varphi(k)}$.

Table 1. comparisons of bit length of the loops of the pairings

Methods	$E_1(k{=}10)$	$E_2(k{=}11)$	$E_3(k{=}22)$	$E_4(k{=}28)$	$E_5(k{=}18)$	$E_6(k{=}26)$	$E_7(k{=}34)$
Tate	187	169	237	234	160	160	183
Ate	140	34	191	60	133	93	103
Ate_i	47	17	24	20	27	14	12

5 Conclusions and Further Work

We have found that a series of the generalized Ate pairings which are called the Ate_i pairings $f_{T_i,Q}(P)$. We have discussed how to choose the shortest T_i for fast pairing computations and shown that the Miller loop of the optimal Ate_i pairing can achieve $r^{1/\varphi(k)}$ for more pairing-friendly curves. We proposed an open problem that what relations of q, k and r on pairing-friendly elliptic curves can make that the optimal T_i can reach the lower bound $r^{1/\varphi(k)}$. Another open problem is whether there exists a method to construct pairing-friendly curves directly having the property which $T = q \bmod r$ is the smallest in $T^i \equiv q^i \bmod r$.

Acknowledgement

We would like to thank Florian Hess, Michael Scott and Steven Galbraith for their helpful comments and suggestions on an early draft of this paper.

References

1. P.S.L.M. Barreto, S. Galbraith, C. ÓhÉigeartaigh, and M. Scott. Efficient pairing computation on supersingular Abelian varieties. *Designs, Codes and Cryptography*, volume 42, number 3. Springer Netherlands, 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*, volume 2442 of *Lecture Notes in Computer Science*, pages. 354-368. Springer-Verlag, 2002.
3. P.S.L.M. Barreto and M. Naehrig. Pairing-friendly elliptic curves of prime order. *Proceedings of SAC 2005-Workshop on Selected Areas in Cryptography*, volume 3897 of Lecture Notes in Computer Science, pages 319-331. Springer, 2006.
4. D. Boneh and M. Franklin. Identity-based encryption from the Weil pairing. *SIAM Journal of Computing*, 32(3): 586-615, 2003.
5. Aya Comuta, Mitsuru Kawazoe, and Tetsuya Takahashi. How to construct pairing-friendly curves for the embedding degree k = 2n, n is an odd prime. Preprint, 2006. Available from http://eprint.iacr.org/2006/427.
6. P. Duan, S. Cui and C.W. Chan. Special polynomial families for generating more suitable elliptic curves for pairing-based cryptosystems. The 5th WSEAS International Conference on Electronics, Hardware, Wireless & Optimal Communications, 2006.
7. I. Duursma, Hyang-Sook Lee. Tate pairing implementation for hyperelliptic curves $y^2 = x^p - x + d$, *Advances in Cryptology-Asiacrypt'2003*, volume 2894 of *Lecture Notes in Computer Science*, pages. 111-123. Springer-Verlag, 2003.
8. David Freeman. Constructing Pairing-Friendly Elliptic Curves with Embedding Degree 10, *Algorithmic Number Theory Symposium ANTS-VII*, volume 4076 of Lecture Notes in Computer Science, pages 452-465. Springer-Verlag, 2006.
9. D. Freeman, M. Scott, E. Teske. A taxonomy of pairing-friendly elliptic curves. Preprint, 2006. Available from http://eprint.iacr.org/2006/372.
10. S. Galbraith, K. Harrison, and D. Soldera. Implementing the Tate pairing, *Algorithm Number Theory Symposium ANTS V*, volume 2369 of *Lecture Notes in Computer Science*, pages 324-337. Springer-Verlag, 2002.

11. S.D. Galbraith. *Pairings - Advances in Elliptic Curve Cryptography*. Cambridge University Press, 2005.
12. F. Hess, N.P. Smart and F. Vercauteren. The Eta pairing revisited. *IEEE Transactions on Information Theory*, vol 52, pages. 4595-4602, Oct. 2006.
13. A. Joux. A one round protocol for tripartite DiffieCHellman. *ANTS-4: Algorithmic Number Theory. Springer-Verlag*, volume 1838 of *Lecture Notes in Computer Science*, pages 385-394. Springer-Verlag, 2000.
14. A. Joux. The Weil and Tate pairings as building blocks for public key cryptosystems. *ANTS-5: Algorithmic Number Theory*, volume 2369 of *Lecture Notes in Computer Science*, pages 20-32. Springer- Verlag, 2002.
15. R. Lidl and H. Niederreiter. *Finite Fields*. Number 20 in Encyclopedia of Mathematics and its Applications, 2nd ed., Cambridge University Press, Cambridge, UK, 1997.
16. S. Matsuda, N. Kanayama, F. Hess, and E. Okamoto. Optimised versions of the Ate and twisted Ate pairings. Preprint, 2007. Availabe from http://eprint.iacr.org/2007/013.
17. V.S. Miller. Short programs for functions on curves. Unpublished manuscript, 1986. Available from http://crypto.stanford.edu/miller/miller.pdf.
18. A. Murphy and N. Fitzpatrick. Elliptic curves for pairing applications. Preprint, 2005. Available from http://eprint.iacr.org/2005/302.
19. K.G. Paterson. *Cryptography from Pairing - Advances in Elliptic Curve Cryptography*. Cambridge University Press, 2005.
20. R. Sakai, K. Ohgishi and M. Kasahara. Cryptosystems based on pairing. *2000 Symposium on Cryptography and Information Security C SCIS 2000*, 2000.
21. M. Scott. Implementing cryptographic pairings. The 10th Workshop on Elliptic Curve Cryptography, 2006.

Appendix

We give the following pairing-friendly elliptic curves with various embedding degrees. We also list the value of $T \equiv q \bmod r$ and the minimal value of T_i.

E_1 with $k = 10$ in [18]

- r=118497265990650143638940886913063255688422174813106568961(187bits)
- q = 26916561140498229883766759145747954228067854557496271814329796276308782360965160815950571330669569 (324 bits)
- $T = q \equiv -1135746083062455547947511038949266819809535 \bmod r$(140 bits)
- the minimal $T_i = T^9 \equiv 104334294221056 \bmod r$ (i=9)(47 bits)

E_2 with $k = 11$ in [18]

- r= 449044374966079776811018938862000399066079697680411 (169 bits)
- q = 135744191922235220338207401639447477029019429786298117343074149119872959316646592409004721 1 (300 bits)
- $T = q \equiv$ 13503834436 mod r(34 bits)
- the minimal $T_i = T^6 \equiv 116206 \bmod r$ (i=6)(17 bits)

E_3 with $k = 22$ in [18]

- r= 14607248004283973541083919485581590238083428040091851435923 0300179430401 (237 bits)
- q = 453827150719960768522443070426066215487961797570080936189767346452985493536135520775131589586025456605202387452210825 32592382511(425 bits)
- $T = q \equiv$ -854387230496757984093309676917973020089728193676722569 216 mod r(191 bits)
- the minimal $T_i = T^7 \equiv 13075456 \bmod r$ (i=7)(24 bits)

E_4 with $k = 28$ in [18]

- r= 208276590274254899637564628862472689660689004802935956638554 91908821297 (234 bits)
- q = 118143400917763386229164321169531765478830849813868372220241582503104530249717254933438182948872577386372276967001960963118937209(426 bits)
- $T = q \equiv$ -379891970942617223 mod r(60 bits)
- the minimal $T_i = T^5 \equiv 724247 \bmod r$(i=5) (20 bits)

E_5 with $k = 18$ in [5]

- r = 730767328960794658374478759845478477419642392323 (160 bits)
- q = 148219456970417656877736253822173212415791168671331480760944628140 12058758352127 (264 bits)
- $T = q \equiv$ 769985598329417598574210795272718088934 3 mod r) (133 bits)
- the minimal $T_i = T^{11} \equiv 94906623 \bmod r$ (i=11) (27 bits)

E_6 with $k = 26$ in [5]

- r = 764696222581341148650511408773719240195697919573 (160 bits)

- q = 18285492543987287680645893866289922483693928837435505359 (184 bits)
- $T = q \equiv 855187064021038061481397205\!9 \bmod r)$ (93 bits)
- the minimal $T_i = T^{15} \equiv 9779 \bmod r$ (i=15) (14 bits)

E_7 with $k = 34$ in [5]

- r = 10267261474026538061953029801463094309944057146657157201 (183 bits)
- q = 19326928722523970823211392049806096197843339094443289507368327 (204 bits)
- $T = q \equiv 8790878313605026490203306721143 \bmod r)$ (103 bits)
- the minimal $T_i = T^{19} \equiv 2743 \bmod r$ (i=19) (12 bits)