All Pairings are in a Group

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. In this paper, we suggest that all pairings be in a group. It is possible that our observation can be applied into the implementations of pairing-based cryptosystems.

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

1 Introduction

A bilinear pairing is defined as follows:

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$$

where $\mathbb{G}_1$, $\mathbb{G}_2$ are additive groups and $\mathbb{G}_T$ is a multiplicative group. Also, for any $P_1,\ P_2 \in G_1$and $Q_1,\ Q_2 \in G_2$, we require

$$e(P_1 + P_2, Q_1) = e(P_1, Q_1)e(P_2, Q_1),$$

$$e(P_1, Q_1 + Q_2) = e(P_1, Q_1)e(P_1, Q_2).$$

In practical cryptographical applications, non-degeneracy and compatibility are often required for pairings. Since pairings can be constructed from elliptic curves, pairing-based cryptosystems have been widely studied in elliptic curve cryptography in recent years. Some detailed summaries on this subject can be found in [15] and [10].

An elementary problem in the implementation of pairing-based cryptosystems is to compute the pairings. Pairings on elliptic curves can be evaluated in polynomial time by Miller's algorithm [14]. Many efficient techniques have been suggested for optimizing the computation of the pairings [2, 1, 9, 13]. Some excellent summaries about pairing computations are recommended (see [8, 17]). One of the most elegant techniques for computing the pairings efficiently is to shorten the iteration loop in Miller's algorithm. Inspired by the Duursma-Lee method for some special supersingular curves in [4], Barreto *et al.* introduce the η_T pairing which has a half length of the Miller loop compared to the original Tate pairing on supersingular Abelian varieties [1]. Later, Hess *et al.* suggest the Ate pairing which shortens the length of the Miller loop obviously on ordinary elliptic curves [9]. Matsuda *et al.* optimize the Ate pairing and the twisted Ate pairing and show that both them are always at least as fast as the Tate pairing [13]. Inspired by the main results of [13], the authors of [19] give more choices on the Ate pairing.

We now give another look at the techniques of shortening the Miller loop. Using the fact that a fix power of the pairing is still a bilinear pairing, the Eta pairing and the Ate pairing are introduced. Factually, the new derivation in [20] for Scott's algorithm [16] also takes advantage of this fact. Recently, the authors of [12] give an improvement on the Ate pairing using the fact that the Combination of two pairings is also a pairing. Inspired by the above ideas, we first show that all pairings forms a group from an abstract angle. Then we apply it into shortening the Miller loop of the Ate pairing.

The rest of this paper is organized as follows. Section 2 introduces basic mathematical concepts of the Ate pairing. Section 3 gives our main results. We draw our conclusion in Section 4.

2 Ate Pairing and Twisted Ate Pairing

We recall the definition of the Ate pairing and twisted Ate pairing from [9, 13] in this subsection. The Ate pairing extends the η_T pairing on the ordinary elliptic curves.

Let $\mathbb{F}_q$ be a finite field with $q = p^m$ elements, where p is a prime. Let E be an ordinary elliptic curve over $\mathbb{F}_q$, r a large prime satisfying $r \mid \#E(\mathbb{F}_q)$ and let t denote the trace of Frobenius, i.e., $\#E(\mathbb{F}_q) = q+1-t$. Let $T = t-1$ and then $T \equiv$

$q \bmod r$. Let π_q be the Frobenius endomorphism, $\pi_q : E \to E : (x, y) \mapsto (x^q, y^q)$. Denote $Q \in \mathbb{G}_2 = E[r] \cap Ker(\pi_q - [q])$ and $P \in \mathbb{G}_1 = E[r] \cap Ker(\pi_q - [1])$. Let $N = gcd(T^k - 1, q^k - 1) > 0$ and $T^k - 1 = LN$, where k is its embedding degree. Denote the normalized function $f^{norm}_{T,Q} = f_{T,Q}/(z^r f_{T,Q})(\mathcal{O})$, where $Q \in \mathbb{G}_2$ and z is a local parameter for the infinity point $\mathcal{O}$. Then the Ate pairing is defined as $f^{norm}_{T,Q}(P)$ and

$$e(Q, P)^L = f^{norm}_{T,Q}(P)^{c(q^k-1)/N},$$

where $c = \sum_{i=0}^{k-1} T^{k-1-i} q^i \bmod N$.

Let E' over $\mathbb{F}_q$ be a twist of degree d of E, i.e., E' and E are isomorphic over $\mathbb{F}_{q^d}$ and d is minimal with this property. Let $m = gcd(k, d)$ and $e = k/m$. Then the twisted Ate pairing is defined as $f_{T^e,P}(Q)$ and

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

where $c_t = \sum_{i=0}^{m-1} T^{e(m-1-i)} q^{ei} \bmod N$.

The Ate pairing and twisted Ate pairing are both non-degenerate provided that $r \nmid L$. The length of the Miller loop of computing the reduced Ate pairing and the reduced twisted Ate pairing depend on the bit length of T and T^e respectively. Replacing T and T^e with $T \bmod r$ and $T^e \bmod r$ respectively, Matsuda *et al*. give the definition of the optimized Ate pairing and the twisted Ate pairing [13]. This also shows that computing the optimized versions of the Ate pairing and twisted Ate pairing is always at least as efficient as computing the Tate pairing. The authors of [19] suggest that $T^i(T^{ei}) \bmod r (1 \le i \le k)$ induce to some variants of the (twisted) Ate pairings.

3 Main Results

The follow results are very easy to the experts on pairings, but we have not found a location in the literature. Therefore, we present these facts and then shorten the Miller loop of the pairing on elliptic curves using them.

Let e be a bilinear pairing defined as follows:

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$$

where $\mathbb{G}_1,\ \mathbb{G}_2$ are additive groups and $\mathbb{G}_T$ is a multiplicative group. Also, for any $P_1,\ P_2 \in G_1$and $Q_1,\ Q_2 \in G_2$, we have

$$e(P_1 + P_2, Q_1) = e(P_1, Q_1)e(P_2, Q_1),$$

$$e(P_1, Q_1 + Q_2) = e(P_1, Q_1)e(P_1, Q_2).$$

Now we consider all pairings from $\mathbb{G}_1 \times \mathbb{G}_2$ to $\mathbb{G}_T$ and show that they forms a multiplicative group.

Lemma 1. *Let $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ be defined as above. Both e_1 and e_2 are the pairings from $\mathbb{G}_1 \times \mathbb{G}_2$ to $\mathbb{G}_T$. Then $f = e_1/e_2$ and $h = e_1e_2$ are also the pairings from $\mathbb{G}_1 \times \mathbb{G}_2$ to $\mathbb{G}_T$. In particular, a fix power of a pairing still defines a bilinear pairing.*

Proof: For any $P_1,\ P_2 \in G_1$ and $Q_1,\ Q_2 \in G_2$, we obtain

$$f(P_1+P_2, Q_1) = \frac{e_1(P_1 + P_2, Q_1)}{e_2(P_1 + P_2, Q_1)} = \frac{e_1(P_1, Q_1)}{e_2(P_1, Q_1)} \cdot \frac{e_1(P_2, Q_1)}{e_2(P_2, Q_1)} = f(P_1, Q_1) \cdot f(P_2, Q_1).$$

Similarly, we see that

$$f(P_1, Q_1 + Q_2) = f(P_1, Q_1)f(P_1, Q_2).$$

This shows that f is a new bilinear pairing from $\mathbb{G}_1 \times \mathbb{G}_2$ to $\mathbb{G}_T$.

For $h = e_1e_2$, we have

$$\begin{aligned} h(P_1 + P_2, Q_1) =& e_1(P_1 + P_2, Q_1) \cdot e_2(P_1 + P_2, Q_1) \\ =& e_1(P_1, Q_1)e_1(P_2, Q_1) \cdot e_1(P_1, Q_1)e_2(P_2, Q_1) \\ =& h(P_1, Q_1) \cdot h(P_2, Q_1). \end{aligned}$$

Similarly, we see that

$$h(P_1, Q_1 + Q_2) = h(P_1, Q_1)h(P_1, Q_2).$$

This also shows that $h = e_1e_2$ is a new bilinear pairing from $\mathbb{G}_1 \times \mathbb{G}_2$ to $\mathbb{G}_T$.

Finally, Let e be a pairing from $\mathbb{G}_1 \times \mathbb{G}_2$ to $\mathbb{G}_T$ and n be an integer. From

$$e(P_1 + P_2, Q_1)^n = (e(P_1, Q_1) \cdot e(P_2, Q_1))^n = e(P_1, Q_1)^n \cdot e(P_2, Q_1)^n$$

and

$$e(P_1, Q_1 + Q_2)^n = (e(P_1, Q_1) \cdot e(P_1, Q_2))^n = e(P_1, Q_1)^n \cdot e(P_1, Q_2)^n,$$

we conclude that e^n is also a new pairing. □

From the above lemma, we can easily obtain the following theorem.

Theorem 1. *Let I be a pairing from $\mathbb{G}_1 \times \mathbb{G}_2$ to $\mathbb{G}_T$ satisfying $I(P,Q) = 1_{G_T}$ where $P \in G_1,\ Q \in G_2$ and $1_{\mathbb{G}_T}$ is the identity in $\mathbb{G}_T$. Then the set of all pairings from $\mathbb{G}_1 \times \mathbb{G}_2$ to $\mathbb{G}_T$ is a multiplicative group with identity I.*

Proof: From Lemma 1, we easily obtain that the product of two pairings is still a pairing. Also, every pairing e from $\mathbb{G}_1 \times \mathbb{G}_2$ to $\mathbb{G}_T$ has its inverse elmenet I/e. This completes the whole proof of Theorem 1. □

Applying Theorem 1 into the bilinear pairing on elliptic curves, we can easily obtain the following useful corollary.

Corollary 1. *Let $e_1 \cdots e_n$ be the pairings from $\mathbb{G}_1 \times \mathbb{G}_2$ to $\mathbb{G}_T$ corresponding to their Miller loops $\lambda_1 \cdots \lambda_n$. Then*

$$e = \prod_{i=1}^{n} e_i^{s_i},\ s_i \in \mathbb{Z},\ 1 \leq i \leq n$$

is also a pairing from $\mathbb{G}_1 \times \mathbb{G}_2$ to $\mathbb{G}_T$ with its Miller loop $\lambda = \sum_{i=1}^{n} s_i \lambda_i$.

In pairing implementations, the short Miller loop are often required. So we can choose the suitable $s_i \in \mathbb{Z}$ making λ as small as possible. We now apply Corollary 1 into constructing some new pairings from the generalized Ate pairing.

Example 1. Let E be B-N curves over F_p in [3] with $k = 12$. Also $p = 36u^4 + 36u^3 + 24u^2 + 6u + 1$ and $r = 36u^4 + 36u^3 + 18u^2 + 6u + 1$. According to the main result of [19], we have

- $T_1 = 6u^2$
- $T_{10} = 36u^3 + 18u^2 + 6u + 2$
- $T_{11} = 36u^3 + 30u^2 + 12u + 3$

Also, note that all $f_{T_i,P}^{norm}$ give bilinear pairings, which is called the Ate$_i$ pairing. Let $e_1,\ e_2$ and e_3 be the pairing $f_{T_1,P}^{norm},\ f_{T_{10},P}^{norm}$ and $f_{T_{11},P}^{norm}$ respectively. Then using Theorem 1, we can define a new pairing $e = e_1^{-2} e_2^{-1} e_3$.

Since $T_{11} = T_{10} + 2T_1 + \lambda$ where$\lambda = (-2)T_1 + (-1)T_{10} + T_{11} = 6u + 1$, we easily have

$$\begin{aligned}(f^{norm}_{T_{11},P}) =&(f^{norm}_{T_{10},P} f^{norm}_{2T_1+\lambda,P} \cdot \frac{l^{norm}_{T_{10}P,T_1P}}{v^{norm}_{T_{11}P}})\\ &=(f^{norm}_{T_{10},P} \cdot (f^{norm}_{T_1,P})^2 \cdot f^{norm}_{\lambda,P} \frac{l^{norm}_{T_1P,T_1P}}{v^{norm}_{2T_1P}} \cdot \frac{l^{norm}_{2T_1P,\lambda P}}{v^{norm}_{(2T_1+\lambda)P}} \frac{l^{norm}_{T_{10}P,T_1P}}{v^{norm}_{T_{11}P}}).\end{aligned}$$

This shows that

$$(\frac{f^{norm}_{T_{11},P}}{(f^{norm}_{T_{10},P} \cdot (f^{norm}_{T_1,P})^2)}) = (f^{norm}_{\lambda,P} \frac{l^{norm}_{T_1P,T_1P}}{v^{norm}_{2T_1P}} \cdot \frac{l^{norm}_{2T_1P,\lambda P}}{v^{norm}_{(2T_1+\lambda)P}} \frac{l^{norm}_{T_{10}P,T_1P}}{v^{norm}_{T_{11}P}})$$

Therefore, we can see that e indeed defines a new pairing and also e have its explicit expression

$$f^{norm}_{\lambda,P} \frac{l^{norm}_{T_1P,T_1P}}{v^{norm}_{2T_1P}} \cdot \frac{l^{norm}_{2T_1P,\lambda P}}{v^{norm}_{(2T_1+\lambda)P}} \frac{l^{norm}_{T_{10}P,T_1P}}{v^{norm}_{T_{11}P}}.$$

So the Miller loop of the new pairing e is $\lambda = 6u + 1$. Since that $\lambda = 6u + 1$, we also enable that the Miller loop of the new pairing e reaches the lower bound $r^{1/\varphi(k)}$similar to [12]. However, our technique is not same as the main technique in [12].

Example 2. The pairing-friendly curves from [11] for $k = 16$ with a $\rho-$value of 5/4 have the following parametrization. $r = u^8 + 48u^4 + 625$ and $t = \frac{1}{35}(2u^5 + 41u + 35)$. Note that

- $T_1 = \frac{1}{35}(2u^5 + 41u) \pmod r$
- $T_5 = \frac{1}{35}(u^5 + 38u) \pmod r$

Then for $P \in G_1$ and $Q \in G_2$ in the generalized Ate pairing, we see that $e_1(P, Q) = f^{norm}_{T_1,P}(Q)^{(q^k-1)/r}$ and $e_2(P, Q) = f^{norm}_{T_5,P}(Q)^{(q^k-1)/r}$ gives two bilinear pairings. Therefore, $e = e_1^{-1}e_2^2$ defines a new pairing with the Miller loop $\lambda = (-1)T_1 + T_5 = u$ according to lemma 2. Also e has its explicit expression $e = (f^{norm}_{u,P} \frac{l_{T_1P,uP}}{v_{2T_5P}})^{(q^k-1)/r}$. Note that the Miller loop u also reach the lower bound $r^{1/\varphi(k)}$.

4 Conclusions and Further Work

In this paper, we suggest that the set of all pairings be a multiplicative group. Using this fact, some new pairing are introduced. It is possible that our observation can be applied into the implementations of pairing-based cryptosystems. It is an open problem how to construct a pairing on elliptic curves with the Miller loop shorter than $r^{1/\varphi(k)}$.

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. I. Duursma, H.-S. 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.
5. D. 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.
6. G. Frey and H-G. Rück. A remark concerning m-divisibility and the discrete logartihm in the divisor class group of curves. *Math. Comp.,* 62(206):865-874, 1994.
7. 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.
8. S.D. Galbraith. *Pairings - Advances in Elliptic Curve Cryptography*. Cambridge University Press, 2005.
9. F. Hess, N.P. Smart and F. Vercauteren. The Eta pairing revisited. *IEEE Transactions on Information Theory*, vol 52, pages 4595-4602, Oct. 2006.
10. 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.
11. E.J. Kachisa, E.F. Schaefer and M. Scott. Constructing Brezing-Weng pairing friendly elliptic curves using elements in the cyclotomic field. Preprint, 2007. Available from http://eprint.iacr.org/2007/452.
12. E. Lee, H.-S. Lee, and C.-M. Park. Efficient and Generalized Pairing Computation on Abelian Varieties. Preprint, 2008. Available at http://eprint.iacr.org/2008/040

13. S. Matsuda, N. Kanayama, F. Hess, and E. Okamoto. Optimised versions of the Ate and twisted Ate pairings. Preprint, to appear in the 11th IMA International Conference on Cryptography and Coding, 2007. Also available from http://eprint.iacr.org/2007/013.
14. V.S. Miller. Short programs for functions on curves. Unpublished manuscript, 1986. Available from http://crypto.stanford.edu/miller/miller.pdf.
15. K.G. Paterson. *Cryptography from Pairing - Advances in Elliptic Curve Cryptography*. Cambridge University Press, 2005.
16. M. Scott. Faster Pairings Using an Elliptic Curve with an Efficient Endomorphism. *Progress in Cryptology - INDOCRYPT 2005*, volume 3797 of *Lecture Notes in Computer Science*, pages. 258-269. Springer-Verlag, 2005.
17. M. Scott. Implementing cryptographic pairings. The 10th Workshop on Elliptic Curve Cryptography, 2006.
18. J.H. Silverman, *The arithmetic of elliptic curves*. Number 106 in Graduate Texts in Mathematics. Springer-Verlag, New York, 1986.
19. C. Zhao, F. Zhang and J. Huang. A Note on the Ate Pairing. Preprint, 2007. Available at http://eprint.iacr.org/2007/247
20. C. Zhao, F. Zhang and J. Huang. Speeding up the Bilinear Pairings Computation on Curves with Automorphisms. Unpublished. 2006. Available at http://eprint.iacr.org/2006/474.