Reducing the Complexity of the Weil Pairing Computation

Chang-An Zhao[1,2,3] and Fangguo Zhang[2,3]

[1] School of Computer Science and Educational Software, Guangzhou University, Guangzhou 510006, P.R.China

[2] School of Information Science and Technology, Sun Yat-Sen University, Guangzhou 510275, P.R.China

[3] Guangdong Key Laboratory of Information Security Technology, Sun Yat-Sen University, Guangzhou 510275, P.R.China

changanzhao@gmail.com

isszhfg@mail.sysu.edu.cn

Abstract. In this paper, we investigate to compute the variants based on the Weil pairing with short Miller iteration loops.

Keywords: Weil pairing, ate pairing, elliptic curves, pairing based cryptography.

1 Introduction

The weil and Tate pairings have been widely used to construct pairing based cryptography [20]. Since the Tate pairing can be computed more efficiently than the Weil pairing, the researchers have mainly considered the Tate pairing computations [10, 1] and presented some variants based on the Tate pairing, such as the eta pairing [3], the ate pairing [12, 16] and the R-ate pairing [15]. Vercauteren gives an efficient method to find an optimal pairing for fast paring computations [11] and Hess states an integral framework that covers all known efficiently-computable pairing functions based on the Tate pairing [22].

The Tate pairing or its variants are preferable in practical implementations although the Weil pairing was widely used to construct pairing based protocols. The computation of the variants based on the Tate pairing involves the Miller iteration loop and the final exponentiation to get a unique value. Many useful optimizations for Miller's algorithm [18] are proposed for computing the variants

of the Tate pairing except the work of [19, 17, 14, 7]. The Weil pairing computation does not need the final exponentiation while it involves two Miller iteration loops.

In this paper, we investigate how to speed up the Weil pairing computations with Frobenius endomorphisms. Similar to the ate pairing, the new variants based on the Weil pairing are proposed with short Miller iteration loops. Computing the new variants of the Weil pairing is twice faster than computing the standard Weil pairing under several certain conditions. It is clear that the new variants are computed slower than the optimal pairings . However, it is a novel approach for speeding up the Weil pairing computation.

The rest of this paper is organized as follows. Section 2 introduces basic mathematical concepts of the pairings on elliptic curves. Section 3 gives our main results and Section 4 presents some examples. We draw our conclusion in Section 5.

2 Mathematical Preliminaries

This section briefly recalls the definition of the Tate pairing, the ate pairing and the Weil pairing.

2.1 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 $\mathcal{O}$ be the point at infinity. $\#E(\mathbb{F}_q)$ is denoted as the order of the rational points group $E(\mathbb{F}_q)$ and r is a large prime satisfying $r|\#E(\mathbb{F}_q)$. Let k be the embedding degree, i.e., the smallest positive integer such that $r|q^k - 1$.

Let $P \in E[r]$ and $Q \in E(\mathbb{F}_{q^k})$. For each integer i and point P, let $f_{i,P}$ be a rational function on E such that

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

Let D be a divisor [21] which is linearly equivalent to $(R) - (\mathcal{O})$ with its support disjoint from $(f_{r,P})$. The Tate pairing [8] is a bilinear map

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

$$\tilde{e}(P, R) = f_{r,P}(D).$$

Assume that all Miller functions are normalized in this paper [22, 11]. One can define the reduced Tate pairing [4] as

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

Notice that $f_{r,P}(R)^{a(q^k-1)/r} = f_{ar,Q}(R)^{(q^k-1)/r}$ for any integer a [9].

2.2 Ate pairing and Twisted Ate pairing

We recall the definition of the (twisted) ate pairing and its variants from [12, 16, 23] in this subsection. The ate pairing extends the eta pairing [3] on 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 $\mathbb{F}_q$. Let r be a large prime satisfying $r \mid \#E(\mathbb{F}_q)$. Denote the trace of Frobenius by t, i.e., $\#E(\mathbb{F}_q) = q + 1 - t$. Let $T = t - 1 \equiv q \pmod{r}$. 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. Then the ate pairing is defined as $f_{T,Q}(P)$ and

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

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

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 $e = k/m$. Denote $T_e = T^e \equiv q^e \pmod{r}$. 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 $r \nmid L$. Denote $T_i = T^i \equiv q^i \pmod{r}$ and $T_{ei} = (T^e)^i \equiv (q^e)^i \pmod{r}$. Then the ate pairing and twisted ate pairing can be generalized as $f_{T_e,Q}(P)$ and $f_{T_{ei},P}(Q)$ respectively [23]. The generalized version of the (twisted) ate pairing provides more choices in practical implementations.

2.3 Weil Pairing

Using the same notation as previous, one may make a few slight modifications and then define the Weil pairing. Let k be the minimal positive integer such that

$E[r] \subset E(\mathbb{F}_{q^k})$. According to the results in [2], if $r \nmid q-1$ and $(r,q)=1$, then $E[r] \subset E(\mathbb{F}_{q^k})$ if and only if $r|q^k-1$, i.e., the embedding degree for the Weil pairing is equal to the embedding degree for the Tate pairing in this case.

Suppose that $P,\ Q \in E[r]$ and $P \neq Q$. Let D_P and D_Q be two divisors which are linearly equivalent to $(P)-(\mathcal{O})$ and $(Q)-(\mathcal{O})$, respectively. Let $f_{r,P}$ and $f_{r,Q}$ be two rational functions on E such that $(f_{r,P})=rD_P$ and $(f_{r,Q})=rD_Q$. Then the Weil pairing is a map [19]

$$e_r : E[r] \times E[r] \to \mu_r,$$

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

For good efficiency, one can define the powered Weil pairing [17, 14] as

$$\hat{e}_r(P,Q) = e_r(P,Q)^{(q^l-1)},$$

where l is a divisor of k. Notice that the denominator elimination technique can be applied when computing the powered Weil pairing.

3 Main Results

In this section, The main results of this paper are summarized in the following theorem.

Theorem 1. *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 $T=t-1 \equiv q \pmod r$. 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 E' over $\mathbb{F}_q$ be a twist of degree d of E. Let $m=gcd(k,d)$ and $e=k/m$. Denote $S_i = T_{ei} \equiv T^{ei} \equiv (q^e)^i \pmod r$, where $0<i<k-1$. Let a be the smallest integer such that $S_i^a \equiv 1 \pmod r$. Let L be an integer such that $S_i^a - 1 = Lr$. Then for such P and Q, the Weil pairing satisfies*

$$e_r(P,Q)^L = \left(\frac{f_{S_i,P}(Q)}{f_{S_i,Q}(P)}\right)^c,$$

where $c = \sum_{j=0}^{a-1} S_i^{a-1-j} q^{ej} \equiv a q^{ei(a-1)} \pmod r$.

Proof. It is obvious from the definition of the Weil pairing that

$$e_r(P,Q)^L = (\frac{f_{r,P}(Q)}{f_{r,Q}(P)})^L = \frac{f_{Lr,P}(Q)}{f_{Lr,Q}(P)}.$$

Applying the identity $Lr = S_i^a - 1$ into the above equation, we obtain

$$e_r(P,Q)^L = \frac{f_{S_i^a-1,P}(Q)}{f_{S_i^a-1,Q}(P)} = \frac{f_{S_i^a,P}(Q)}{f_{S_i^a,Q}(P)}. \tag{1}$$

The second equality holds since P and Q are two points in $E[r]$ [6]. By Lemma 2 in [3, 12], we see that

$$f_{S_i^a,P} = f_{S_i,P}^{S_i^{a-1}} f_{S_i,S_iP}^{S_i^{a-2}} \cdots f_{S_i,S_i^{a-1}P} \tag{2}$$

Lemma 5 in [12] and the discussions in [16, 23] yield that $f_{S_i,S_i^jP}(Q) = f_{S_i,P}(Q)^{q^{ej}}$ with $0 \le j \le a-1$. Then

$$f_{S_i^a,P}(Q) = (f_{S_i,P}(Q))^{\sum_{j=0}^{a-1} S_i^{(a-1-j)} q^{ej}} \tag{3}$$

By using the same argument for $f_{s_i^a,P}(Q)$, we have

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

Substituting (3) and (4) into the equation (1), we have

$$e_r(P,Q)^L = (\frac{f_{S_i,P}(Q)}{f_{S_i,Q}(P)})^c,$$

where $c = \sum_{j=0}^{a-1} S_i^{a-1-j} q^{ej} \equiv aq^{ei(a-1)} \pmod r$. This completes the whole proof.

Some remarks on Theorem 1 are given as follows.

Remark 1. If $r \nmid L$, then the new pairings are non-degenerate. If the curve has a quadratic twist, we only obtain a trivial pairing since $S_i = \pm 1 \mod r$.

Remark 2. A series of the variants based on the Weil pairing can be obtained as i varies. Also, the length of the Miller loops for the new pairing depends on the bit-length of $S_i = T^{ei} \equiv q^{ei} \pmod r$.

Remark 3. We define the powered variants of the Weil pairing as $(\frac{f_{S_i,P}(Q)}{f_{S_i,Q}(P)})^{q^l-1}$ which enables the denominator elimination technique.

4 Applications

In this section, we apply Theorem 1 for obtaining some new variants based on the Weil pairing with short Miller iteration loops on pairing-friendly curves.

Cyclotomic family with $k = 8$ The authors give a family of curves with $k = 8$ and $D = 1$ which makes the quartic twist possible [13]. Its parametrization is given by

$$p = (125 - 82x - 15x^2 + 8x^3 - 3x^4 + 2x^5 + x^6)/180$$
$$r = (25 - 8x^2 + x^4)/450$$

Notice that this family of elliptic curves has a quartic twist, i.e., $d = 4$. Since $k = 8$, we have $e = \frac{k}{(k,d)} = 2$. Thus, we can choose $S_i = (p^2)^3 \equiv (x^2 - 4)/3 \pmod{r}$ for defining the new variants of the Weil pairing with short Miller loops. In practical implementations, $(\frac{f_{S_i,P}(Q)}{f_{S_i,Q}(P)})^{p^4-1}$ can be used for good efficiency. The Miller loop of the new variants only will be half of that required for the Weil pairing.

Cyclotomic family with $k = 18$ The authors give a family of curves with $k = 8$ and $D = 3$ which makes the sextic twist possible [13]. Its parametrization is given by

$$p = (2401 + 1763x + 343x^2 + 259x^3 + 188x^4 + 37x^5 + 7x^6 + 5x^7 + x^8)/21$$
$$r = (343 + 37x^3 + x^6)/343$$

Notice that this family of elliptic curves has a sextic twist, i.e., $d = 6$. Since $k = 18$, we have $e = \frac{k}{(k,d)} = 3$. Thus, we can choose $S_i = (p^3)^5 \equiv x^3 + 18 \pmod{r}$ for defining the new variants of the Weil pairing with short Miller loops. In practical implementations, $(\frac{f_{S_i,P}(Q)}{f_{S_i,Q}(P)})^{p^9-1}$ can be used for good efficiency. Similar to the previous examples, the Miller loop of the new variants only will be half of that required for the Weil pairing.

Barreto-Naehrig curves The authors give a family of curves with $k = 12$ [5]. There exists a twist of degree $d = 6$ for the family. Its parametrization is given by

$$p = 36x^4 + 36x^3 + 24x^2 + 6x + 1$$
$$r = 36x^4 + 36x^3 + 18x^2 + 6x + 1$$

Since $k = 18$ and $d = 6$, it follows that $e = \frac{k}{(k,d)} = 2$. Thus, we can choose $S_i = (p^2)^4 \equiv 36x^3 + 18x^2 + 6x + 1 \pmod{r}$ for defining the new variants of

the Weil pairing. The bit length of S_i is 3/4 of that of r which provides a faster pairing than the Weil pairing. Also, using the techniques in [15] which are extended in [24, 22, 11], we could construct the new variants based on the Weil pairing which has the same Miller loops as the twisted R-ate pairing, i.e., the length of the Miller loops for computing the new variants can be half of that required for the Weil pairing.

5 Conclusions

In this paper, we propose some variants of the Weil pairing. The new variants are computed twice faster than the standard Weil pairing, while they are slower than the optimal pairings based on the Tate pairing. We provide a novel approach to speed up the Weil pairing computation. It is possible to further optimize the results.

References

1. R. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen, and F. Vercauteren. *Handbook of Elliptic and Hyperelliptic Curve Cryptography.* Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2006.
2. R. Balasubramanian and N. Koblitz. The Improbability That an Elliptic Curve Has Sub-exponential Discrete Log Problem Under the Menezes-Okamoto-Vanstone Algorithm. J. Cryptology, vol. 11, pp. 141-145, 1998.
3. P.S.L.M. Barreto, S. Galbraith, C. ÓhÉigeartaigh, and M. Scott. Efficient pairing computation on supersingular Abelian varieties. *Designs, Codes and Cryptography*, vol. 42, no. 3. pp. 239-271. Springer Netherlands, 2007.
4. 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*, pp. 354-368. Springer-Verlag, 2002.
5. 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, pp. 319-331. Springer, 2006.
6. 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*, pp. 111-123. Springer-Verlag, 2003.
7. Eisenträer K., Lauter K., Montgomery P.L., Fast elliptic curve arithmetic and improved Weil pairing evaluation. In Proceeding of CT-RSA'2003, volume 2612 of *Lecture Notes in Computer Science*, pp. 343-354. Springer-Verlag, 2003.

8. G. Frey and H-G. Rück. A remark concerning m-divisibility and the discrete logartihm in the divisor class group of curves. *Math. Comp.,* vol. 62(206). pp. 865-874, 1994.
9. 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*, pp. 324-337. Springer-Verlag, 2002.
10. S.D. Galbraith. *Pairings - Advances in Elliptic Curve Cryptography.* Cambridge University Press, 2005.
11. F. Hess. Pairing Lattices. Preprint, 2008. Available at http://eprint.iacr.org/2008/125.
12. F. Hess, N.P. Smart and F. Vercauteren. The Eta pairing revisited. *IEEE Transactions on Information Theory*, vol 52, pp. 4595-4602, Oct. 2006.
13. 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.
14. B. G. Kang, J. H. Park. On the relationship between squared pairings and plain pairings. Inf. Process. Lett. vol. 97(6), pp. 219-224, 2006.
15. 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.
16. 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*, volume 4887 of *Lecture Notes in Computer Science*, pp. 302-312. Springer-Verlag, 2007.
17. A. J. Menezes and N. Koblitz, Pairing-based cryptography at high security levels, Cryptography and Coding, volume 3796 of *Lecture Notes in Computer Science* pp. 13-36. Springer-Verlag, 2005.
18. V.S. Miller. Short programs for functions on curves. Unpublished manuscript, 1986. Available from http://crypto.stanford.edu/miller/miller.pdf.
19. V.S. Miller. The Weil pairing and its Efficient Calculation, J. Cryptology, vol.17, pp. 235-261, 2004.
20. K.G. Paterson. *Cryptography from Pairing - Advances in Elliptic Curve Cryptography.* Cambridge University Press, 2005.
21. J.H. Silverman, *The arithmetic of elliptic curves.* Number 106 in Graduate Texts in Mathematics. Springer-Verlag, New York, 1986.
22. F. Vercauteren. Optimal Pairings. Preprint, 2008. Available at http://eprint.iacr.org/2008/096.
23. C.-A. Zhao, F. Zhang and J. Huang. A Note on the Ate Pairing. Preprint 2007, to appear in Internationl Journal of Information Security. Also available at http://eprint.iacr.org/2007/247.

24. C.-A. Zhao, F. Zhang and J. Huang. All Pairings Are in a Group. Preprint, 2008. Available at http://eprint.iacr.org/2008/085.