Optimised versions of the Ate and Twisted Ate Pairings

Seiichi Matsuda[1], Naoki Kanayama[1], Florian Hess[2], and Eiji Okamoto[1]

[1] University of Tsukuba, Japan
[2] Technische Universität Berlin, Germany

Abstract. The Ate pairing and the twisted Ate pairing for ordinary elliptic curves which are generalizations of the η_T pairing for supersingular curves have previously been proposed. It is not necessarily the case that both pairings are faster than the Tate pairing. In this paper we propose optimized versions of the Ate and twisted Ate pairings with the loop reduction method and show that both pairings are always at least as fast as the Tate pairing. We also provide suitable families of elliptic curves that our optimized Ate and optimized twisted Ate pairings can be computed with half the loop length compared to the Tate pairing.

1 Introduction

In 2000, Sakai *et al* [14] proposed an ID-based key agreement protocol using a bilinear pairing, and pairing-based cryptosystems became one of the most attractive areas of research in elliptic curve cryptography. Famous examples are Identity Based Encryption [5] and Short Signature [6]. Using a bilinear pairing, one can construct a nonconventional protocol and reduce the bandwidth. The pairing computation, however, takes up much more computational costs than main cryptographic primitives such as modular exponentiation or scalar multiplication over elliptic curves, so an efficient algorithm for computing the pairing presents an important issue in pairing-based cryptography.

Some leading algorithms of computing pairing have been proposed. Such examples are an efficient algorithm called the BKLS algorithm [2] which was proposed, and the new pairing on a supersingular (hyper)elliptic curve over a finite field of characteristic p which was proposed by Duursma *et al* a year later [8]. Barreto *et al* [1] generalized this pairing over supersingular curves with trace t to be the η pairing and proposed the η_T pairing, where $T = t - 1$, that can be computed with half the loop length compared to the η pairing. For these results, they consider pairings on $\mathbb{G}_1 \times \mathbb{G}_2$, where $\mathbb{G}_1 = E(\mathbb{F}_q)[r], \mathbb{G}_2 = E(\mathbb{F}_{q^k})[r]$. Hess *et al* [11] extended η_T pairing over an ordinary curve and proposed the Ate pairing on $\mathbb{G}_2 \times \mathbb{G}_1$ and the twisted Ate pairing on $\mathbb{G}_1 \times \mathbb{G}_2$. Note that the latter can only be faster than the Tate pairing when $|T^e| \leq r$ using a twist $E'/\mathbb{F}_{q^e}$.

In this paper, we propose an optimized version of the Ate and twisted Ate pairing which can be more efficiently computed than the standard Ate and twisted Ate pairing if certain conditions are met. We provide some families of elliptic curves for which these conditions are satisfied.

2 Background

2.1 Tate pairing

Let $\mathbb{F}_q$ be a finite field with $q = p^m$ elements where p is prime and let E be an elliptic curve defined over $\mathbb{F}_q$. Denote subgroup order by r such that $r|\sharp E(\mathbb{F}_q)$ and the embedding degree by k such that the smallest positive integer with $r|q^k - 1$.

Let $P \in E(\mathbb{F}_q)[r]$ and $Q \in E(\mathbb{F}_{q^k})$, and consider the divisor $D = (Q+R)-(R)$ with R a random point in $E(\mathbb{F}_{q^k})$. For every integer a, let $f_{a,P}$ be a function with divisor $\mathrm{div}(f_{a,P}) = a(P) - (aP) - (a-1)(O)$, then the Tate pairing is a well-defined, nondegenerate, bilinear pairing

$$\langle \cdot, \cdot \rangle_r : \begin{cases} E(\mathbb{F}_q)[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) & \to \mathbb{F}^*_{q^k}/(\mathbb{F}^*_{q^k})^r \\ (P, Q) & \mapsto \langle P, Q \rangle_r = f_{r,P}(D) \end{cases}$$

We will require a unique element of $\mathbb{F}^*_{q^k}$ for pairing-based protocols, so one may define the reduced Tate pairing as $e(P,Q) = \langle P, Q \rangle_r^{(q^k-1)/r} = f_{r,P}(Q)^{(q^k-1)/r}$. Galbraith *et al* [10] shows that r can be replaced by any integer N such that $r|N|q^k - 1$, i.e. $e(P,Q) = f_{N,P}(Q)^{(q^k-1)/N}$

One can compute $f_{r,P}(Q)$ using Miller's algorithm. If k is even, then vertical line g_{aP} through aP can be ignored due to the final powering operation.

Miller's Algorithm
INPUT: $P \in E(\mathbb{F}_p)[r], Q \in E(\mathbb{F}_{p^k})/rE(\mathbb{F}_{p^k})$
OUTPUT: $f \in \mathbb{F}_{p^k}$
$f \leftarrow 1, V \leftarrow P$ and $n = r - 1$
for $i \leftarrow \lfloor \log_2 n \rfloor - 1$ downto 0 do
$\quad f \leftarrow f^2 \cdot g_{V,V}(Q)/g_{2V}(Q)$ and $V \leftarrow 2V$
$\quad$ if $n_i = 1$ then
$\quad\quad f \leftarrow f \cdot g_{V,P}(Q)/g_{V+P}(Q)$ and $V \leftarrow V + P$
return f

2.2 η and η_T pairing

For $P \in E(\mathbb{F}_q)[r], Q \in E(\mathbb{F}_{q^k})[r]$ where E is a supersingular curve with distortion map ψ, there exists an automorphism γ such that $\gamma\psi^q(P) = \psi(P)$. For $M = (q^k - 1)/N, T \in \mathbb{Z}$, the following equation holds:

$$(\langle P, \psi(Q) \rangle_N^M)^L = (\eta_T(P,Q)^M)^{aT^{a-1}},$$

where $a \in \mathbb{N}, L, c \in \mathbb{Z}, T^a + 1 = LN, T = q + cN$. Barreto *et al* [1] have proposed the η pairing for $T = q$ on the above definition and also introduced improved version of it with the choice $T = q - N$ and refer to the pairing as η_T pairing. Since $T = q - N = \mp t - 1$, the η_T pairing can be computed with half the loop length compared to the η pairing.

2.3 Ate pairing

Let Frobenius endomorphism $\pi_q : E \to E : (x, y) \mapsto (x^q, y^q)$ and let $\mathbb{G}_1 = E[r] \cap \mathrm{Ker}(\pi_q - [1]), \mathbb{G}_2 = E[r] \cap \mathrm{Ker}(\pi_q - [q])$. Denote the group order of the elliptic curve by $\sharp E(\mathbb{F}_q) = q+1-t$ and let $T = t-1$. Let $N = \gcd(T^k - 1, q^k - 1), T^k - 1 = LN$. For $Q \in \mathbb{G}_2, P \in \mathbb{G}_1$, we have the Ate pairing:

$$a_T : (Q, P) \mapsto f_{T,Q}(P)^{c_T(q^k-1)/N}$$

where $c_T = \sum_{i=0}^{k-1} T^{k-1-i} q^i \equiv kq^{k-1} \mod r$. The Ate pairing is nondegenerate for $r \nmid L$ and bilinear. One can compute $f_{T,Q}(P)$ using Miller's algorithm with loop length $\lfloor \log_2 |T| \rfloor$. If $q \sim r$ and the average size of trace equals to $\sqrt{q}$, the Ate pairing can be computed with half the loop length compared to the Tate pairing.

2.4 Twist

Let E and E' be two ordinary elliptic curves over $\mathbb{F}_q$ with $q = p^n$ and $p \geq 5$. E' is called a twist of degree d of E if there exists an isomorphism $\psi : E' \to E$ defined over $\mathbb{F}_q$ and d is minimal. We remark that the condition $k \mid \sharp \mathrm{Aut}(E)$ holds true if and only if E admits a twist of degree k.

Let $D \in \mathbb{F}_q^*$, then the twists corresponding to $D \mod (\mathbb{F}_q^*)^d$ are given by

$$\begin{aligned}
d = 2 \qquad & E : y^2 = x^3 + ax + b, \\
& E' : y^2 = x^3 + a/D^2 x + b/D^3, \\
& \psi : E' \to E : (x, y) \mapsto (Dx, D^{3/2} y), \\
d = 4 \qquad & E : y^2 = x^3 + ax, \\
& E' : y^2 = x^3 + a/Dx, \\
& \psi : E' \to E : (x, y) \mapsto (D^{1/2} x, D^{3/4} y), \\
d = 3, 6 \qquad & E : y^2 = x^3 + b, \\
& E' : y^2 = x^3 + b/D, \\
& \psi : E' \to E : (x, y) \mapsto (D^{1/3} x, D^{1/2} y).
\end{aligned}$$

2.5 Twisted Ate pairing

Let E be an elliptic curve admitting a unique twist E' of degree m over $\mathbb{F}_{q^e}$ for $m = \gcd(k, \sharp \mathrm{Aut}(E))$ and $e = k/m$. One can alternatively represent $\mathbb{G}_2$ as $\mathbb{G}_2 = E[r] \cap \mathrm{Ker}([\zeta_m]\pi_q^e - 1)$ where ζ_m is the primitive mth root of unity such that $[\zeta_m] : (x, y) \mapsto (\zeta_m^2 x, \zeta_m^3 y)$. For $P \in \mathbb{G}_1, Q \in \mathbb{G}_2$, we have the twisted Ate pairing:

$$a_{T^e}^{\mathrm{twist}} : (P, Q) \mapsto f_{T^e,P}(Q)^{c_{T^e}(q^k-1)/N}$$

where $c_{T^e} = \sum_{i=0}^{m-1} T^{e(m-1-i)} q^{ei} \equiv kq^{k-1} \mod r$. The Ate pairing is nondegenerate for $r \nmid L$ and bilinear. Note that this pairing can only be faster than the Tate pairing when $|T^e| \leq r$.

3 Optimized versions of Ate and twisted Ate pairings

We can regard the optimized versions of Ate and twisted Ate pairing as an η_T pairing. Let E be an ordinary elliptic curve over $\mathbb{F}_q$ and let $P \in \mathbb{G}_1$ and $Q \in \mathbb{G}_2$ such that $\mathbb{G}_1 = E[r] \cap \mathrm{Ker}(\pi_q - [1])$ and $\mathbb{G}_2 = E[r] \cap \mathrm{Ker}(\pi_q - [q])$.

Theorem 1. *Let $r \geq 5$ be the subgroup order and let S be an integer with $S \equiv q \bmod r$. Define $N = \gcd(S^k - 1, q^k - 1)$ and $S^k - 1 = LN$. Let $c_S = \sum_{i=0}^{k-1} S^{k-1-i} q^i \bmod N$. Then*

$$a_S : (Q, P) \mapsto f_{S,Q}(P)^{c_S(q^k-1)/N}$$

defines a bilinear pairing $\mathbb{G}_2 \times \mathbb{G}_1 \to \mathbb{F}_{q^k}^*[r]$. If $k \mid \sharp\mathrm{Aut}(E)$ then

$$a_S^{\mathrm{twist}} : (P, Q) \mapsto f_{S,P}(Q)^{c_S(q^k-1)/N}$$

also defines a bilinear pairing $\mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{F}_{q^k}^*[r]$. Both pairings a_S and a_S^{twist} are non-degenerate if and only if $r \nmid L$.

We will show that under certain conditions a suitable choice of S yields pairings a_S and a_S^{twist} which are more efficient than the Ate pairing a_T and the twisted Ate pairing a_T^{twist} for $T = t - 1$. For these choices of S we call a_S and a_S^{twist} optimised Ate and optimised twisted Ate pairing.

Proof. The proof is essentially the same as in [11], but slightly more general.

We let $\psi = \pi_q$ for the Ate pairing case and $\psi = \gamma\pi_q$ for the twisted Ate pairing case, where $\gamma \in \mathrm{Aut}(E)$ is an automorphism of order k such that $(\gamma\pi_q)(Q) = Q$ and $(\gamma\pi_q)(P) = [q]P$. If we interchange P and Q for the twisted Ate pairing we have $\psi(P) = P$, $\psi(Q) = [q]Q = [S]Q$ and need to consider $f_{S,Q}(P)^{c_S(q^k-1)/N}$ like for the Ate pairing. This allows us to deal with both cases in one go.

From Lemma 1 of [11] we obtain

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

and

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

Lemma 2 of [1] yields

$$f_{S^k,Q} = f_{S,Q}^{S^{k-1}} f_{S,SQ}^{S^{k-2}} \cdots f_{S,S^{k-1}Q}. \tag{2}$$

Since ψ is purely inseparable of degree q, we obtain from Lemma 4 in [11]

$$f_{S,\psi^i(Q)} \circ \psi^i = f_{S,Q}^{q^i}. \tag{3}$$

We have $\psi^i(Q) = S^iQ$ and $\psi^i(P) = P$. Combining this with (2) and (3) gives

$$f_{S^k,Q}(P) = f_{S,Q}(P)^{\sum_{i=0}^{k-1} S^{k-1-i}q^i}. \tag{4}$$

Substituting (4) into (1) gives

$$e(Q,P)^L = f_{S,Q}(P)^{c_S(q^k-1)/N}. \tag{5}$$

Now (5) shows that a_S and a_S^{twist} are bilinear pairings, which are non-degenerate if and only if $r \nmid L$. □

If we want to apply the twisted Ate pairing for $k \nmid \sharp\mathrm{Aut}(E)$, we can consider the base extension E_1 of E over $\mathbb{F}_{q^e}$, where $e = k/\gcd(k, \sharp\mathrm{Aut}(E))$. The embedding degree of E_1 with respect to r is $m = k/e$, and we have $m \mid \sharp\mathrm{Aut}(E_1)$. We can thus apply the twisted Ate pairing from Theorem 1 to E_1, replacing q by q^e, k by m and using $S \equiv q^e \bmod r$.

4 Performance Evaluation

We provide some families of elliptic curves admitting a twist of degree 4 and 6, and compare the costs of optimized versions with the standard pairings.

4.1 Polynomial Families

Let $\rho \equiv \log p/\log r$ be the ratio between the bit lengths of the finite field and the order of the subgroup. If $D = 1, 2, 3$ in CM equation $4p - t^2 = DV^2$, the following elliptic curves are generated without CM algorithm [9].

$$\begin{aligned} E_1 &: y^2 = x^3 + ax && (D = 1)\\ E_2 &: y^2 = x^3 - 30ax^2 + 56a^3 && (D = 2)\\ E_3 &: y^2 = x^3 + b && (D = 3) \end{aligned}$$

where E_1(respectively E_2 and E_3) is a twist of degree 4(respectively 2 and 6).

Some polynomial families with square polynomial have been presented such as for $k = 4, 6$ when $\rho \sim 2$ [7], for $k = 8$ when $\rho \sim 3/2$ [9] and for $k = 12$ when $\rho \sim 1$ [4]. These detailed parameterizations are in Appendix.

4.2 Efficiency Comparison

We follow the analysis of [12] and compare the Tate pairing $f_{r,P}(Q)$, Ate pairing $f_{T,Q}(P)$, twisted Ate pairing $f_{T^e,P}(Q)$, optimized Ate pairing $f_{S,Q}(P)$ and optimized twisted Ate pairing $f_{S,P}(Q)$ on ordinary elliptic curves admitting a twist of degree 6 when $k = 6, 12$ and degree 4 when $k = 4, 8$. We refer to $f_{N,P}(Q)$ as a Miller-Lite operation and $f_{N,Q}(P)$ as a Full-Miller operation. We denote the cost of the Miller-Lite operation by C_{Lite} and the cost of the Full-Miller operation by C_{Full}. Assume both operations use projective coordinates. On the form

$Y^2 = X^3 + AX + B$, the costs for Miller-operations are estimated as follows [11]. When $A = -3$:

$$C_{\text{Lite}} = (4S_1 + (2e+7)M_1 + S_k + M_k)\log_2 N$$
$$C_{\text{Full}} = (4S_e + 6M_e + 2eM_1 + S_k + M_k)\log_2 N$$

When $A = 0$:

$$C_{\text{Lite}} = (5S_1 + (2e+6)M_1 + S_k + M_k)\log_2 N$$
$$C_{\text{Full}} = (5S_e + 6M_e + 2eM_1 + S_k + M_k)\log_2 N$$

where $s = 2^i 3^j, M_s = 3^i 5^j M_1, S_s = M_s$. Using the parameters in Appendix, we estimate the loop length for each pairings.

Table 1. The Costs Required for the Different Pairings

Security Level	Method	Cost(average size t)	
		Standard	Optimized
$k=4, d=4$	Tate	4960	
$\log_2 p \sim 320$	Ate	4800	2400
$\log_2 r \sim 160$	twisted Ate	4960	2480
$k=6, d=6$	Tate	11008	
$\log_2 p \sim 512$	Ate	11008	5504
$\log_2 r \sim 256$	twisted Ate	11008	5504
$k=8, d=4$	Tate	17664	
$\log_2 p \sim 384$	Ate	16896	16896
$\log_2 r \sim 256$	twisted Ate	26496	13248
$k=12, d=6$	Tate	26880	
$\log_2 p \sim 256$	Ate	16256	16256
$\log_2 r \sim 256$	twisted Ate	26880	20160

Table 1 represents the costs for different pairing on elliptic curves with $k = 4, 6, 8, 12$. When $\rho \sim 2$, we have $r \sim |t|$ and conclude the optimized Ate and optimized twisted Ate pairings are twice as fast as Tate, Ate and twisted Ate pairings. When $k = 8$ we see that the optimized twisted Ate pairing is more efficient than the optimized Ate pairing.

5 Conclusion

We have proposed optimized versions of the Ate and twisted Ate pairing which are always at least as fast as the Tate pairing. We have also showed that our optimized Ate and optimized twisted Ate pairings require a Miller loop of only half the length of the Miller loop of the Ate and twisted Ate pairings, if ordinary elliptic curves admitting twists of degree 4 and degree 6 with $\rho \sim 2$ are employed.

References

1. P.S.L.M. Barreto, S. Galbraith, C. O'hEigeartaigh, and M. Scott, "Efficient pairing computation on supersingular abelian varieties," *Cryptology ePrint Archive*, Report 2004/375, 2004. http://eprint.iacr.org/2004/375
2. P.S.L.M. Barreto, H.Y. Kim, B. Lynn, and M. Scott, "Efficient algorithms for pairing-based cryptosystems," *Crypto 2002*, Lecture Notes on Computer Science, Vol. 2442, pp354–368, 2002.
3. P.S.L.M. Barreto, Ben Lynn, and M. Scott, "On the Selection of Pairing-Friendly Groups," *SAC 2003*, Lecture Notes in Computer Science, Vol. 3006, pp17–25, 2003.
4. P.S.L.M. Barreto and Michael Naehrig, "Pairing-Friendly Elliptic Curve of Prime Order", *Cryptology ePrint Archive*, Report 2005/133, 2005. http://eprint.iacr.ogr/2005/133
5. D. Boneh and M. Franklin, "Identity-based Encryption from the Weil pairing", *CRYPTO 2001*, Lecture Notes on Computer Science, Vol. 2139, pp.213–229, 2001.
6. D. Boneh, B. Lynn and H. Shacham, "Short Signatures from Weil pairing", *ASIACRYPT 2001*, Lecture Notes on Computer Science, Vol. 2248, pp.514–532, 2001.
7. Pu Duan, Shi Cui and Choong Wah Chan, "Effective Polynomial Families for Generating More Pairing-friendly Elliptic Curve", *Cryptology ePrint Archive*, Report 2005/236, 2005. http://eprint.iacr.org/2005/236
8. Iwan Duursma and Hyang-Sook Lee, "Tate Pairing Implementation for Hyperelliptic Cruves $y^2 = x^p - x + d$," *ASIACRYPT 2003*, Lecture Notes on Computer Science, Vol. 2894, pp111-123, 2003.
9. David Freeman, M. Scott and Edlyn Teske, "A taxonomy of pairing-friendly elliptic curves," *Cryptology ePrint Archive*, Report 2006/372, 2006. http://eprint.iacr.org/2005/372
10. S. Galbraith, K. Harrison and S. Soldera, "Implementing the Tate pairing," ANTS V, Lecture Notes on Computer Science, vol.2369, pp.324–337, 2002.
11. F. Hess, N.P. Smart and F. Vercauteren, "The Eta Pairing Revisited," *IEEE Transaction on Information Theory*, vol.52, pp4595-4602, NO. 10, OCTOBER 2006.
12. N. Koblitz and A. Menezes, "Pairing-based cryptography at high security level," *Cryptography and Coding: 10th IMA International Conference*, Lecture Notes on Computer Science, Vol. 3796, pp13-36, 2005.
13. Arjen K. Lenstra, "Selecting Cryptographic Key Sizes," *Journal of CRYPTOLOGY*, vol.14, No.4, pp255-293, December, 2001.
14. R. Sakai, K. Ohgishi and M. Kasahara, "Cryptosystems based on pairing", *SCIS 2000*, 2000.
15. M.Scott, "Scaling security in pairing-based protocols," *Cryptology ePrint Archive*, Report 2005/139, 2005. http://eprint.iacr.org/2005/139
16. Michael Scott, Neil Costigan, and Wesam Abdulwahab, "Implementing Cryptographic Pairings on Smartcards," *Cryptology ePrint Archive*, Report 2006/144, 2006. http://eprint.iacr.org/2006/144

Appendix

We show the following parameterizations for $k = 4, 6, 8, 12$ [7, 4, 9] and the value of $T = t - 1$ and $S = p \bmod r$.

$k = 4$
$t = 4z^2 + 2z + 2$
$r = 4z^2 + 1$
$p = 8z^4 + 6z^2 + 2z + 1$
$DV^2 = 4z^2(2z^2 - 1)^2$
$T = 4z^2 + 2z + 1$
$S = 2z$

$k = 6$
$t = 3z^2 + 1$
$r = 3z^2 - 3z + 1$
$p = 9z^4 - 9z^3 + 9z^2 - 3z + 1$
$DV^2 = 3(3z^2 - 2z + 1)^2$
$T = 3z^2$
$S = 3z - 1$

$k = 8$
$t = -9z^3 - 3z^2 - 2z$
$r = 9z^4 + 12z^3 + 8z^2 + 4z + 1$
$p = \frac{1}{4}(81z^6 + 54z^5 + 45z^4 + 12z^3 + 13z^2 + 6z + 1)$
$DV^2 = (3z + 1)^2$
$T = -9z^3 - 3z^2 - 2z - 1$
$T^2 = 81z^6 + 54z^5 + 45z^4 + 30z^3 + 10z^2 + 4z + 1$
$S = T$ (for optimized Ate pairing)
$S = p^2 \bmod r = -18z^3 - 15z^2 - 10z - 4$ (for optimized twisted Ate pairing)

$k = 12$
$t = 6z^2 + 1$
$r = 36z^4 + 36z^3 + 18z^2 + 6z + 1$
$p = 36z^4 + 36z^3 + 24z^2 + 6z + 1$
$DV^2 = 3(6z^2 + 4z + 1)^2$
$T = 6z^2$
$T^2 = 36z^4$
$S = T$ (for optimized Ate pairing)
$S = p^2 \bmod r = -36z^3 - 18z^2 - 6z - 1$ (for optimized twisted Ate pairing)