Efficient Pairing Computation on Curves

Rongquan Feng, Hongfeng Wu
School of Mathematical Sciences, Peking University, Beijing 100871, P.R. China
E-mail: fengrq@math.pku.edu.cn, wuhf@math.pku.edu.cn

Abstract

In this paper, a method for the efficient computation of Tate pairings on curves which is a generalization of Barreto, etc.'s method [2] is presented. It can reduce the number of loops in the computation of the Tate pairing. The method can be applied not only to supersingular curves but to non-supersingular curves. An example shows the cost of the algorithm in this paper can be reduced by 18% or 13% than the best known algorithm in some elliptic curves.

Keywords: Tate pairing, Eta pairing, Ate pairing, curves, efficient algorithm

1 Introduction

Since Shamir [23] proposed the idea of identity-based cryptography, the pairing-based protocols have been used in many application fields. Bilinear pairings present us the new cryptographic applications such as identity-based encryptions [5], short signature schemes [6], etc. For the practical applications of these systems, it is important to show efficient algorithms for the computation of the Tate pairing. There has been a lot of works on the efficient computation of the Tate pairing. In these works, Duursma and Lee [8] presented how to reduce the loop length in the computation of the Tate pairing for a special family of supersingular elliptic and hyperelliptic curves. In 2004, Barreto, etc. [2] generalized the method of Duursma and Lee and gave a more efficient computation of the Tate pairing on supersinguler curves. The eta pairing is the best result on reducing the number of the main loop length for computing the Tate pairing. Currently the eta pairing is one of the fastest algorithms for computing the bilinear pairing. Under some conditions, the eta pairing is a non-degenerate bilinear pairing. Therefore the eta pairing can be used in pairing-based cryptosystems.

In this paper, a method for the efficient computation of Tate pairings on curves which is a generalization of Barreto, etc.'s method is presented. It can reduce the number of loops in the computation of the Tate pairing and can be used not only on supersingular but also on non-supersingular curves. This method is consistent with the eta pairing when the conditions of the eta pairing are satisfied. An example shows the cost of the algorithm in this paper can be reduced by 18% or 13% than the best known algorithm.

This paper is organized as follows. Section 2 gives a brief background on the Tate pairing which include Barreto, etc.'s result presented in [2]. In Section 3, Barreto, etc.'s method is generalized. Efficient computations of Tate pairings on non-supersingular curves can be achieved by this new method. Some examples to apply this method are discussed in Section 4. Section 5 shows some advices on the choice of parameters. Finally the conclusion is given in Section 6.

2 Preliminaries

The terminology and notation in this paper follows that found in Barreto, etc. [2]. For more information on the Tate pairing defined at abelian varieties and on the Miller's algorithm, the readers are referred to [2], [11] and [24].

Let C be a smooth, projective, and absolutely irreducible curve over a finite field $K = \mathbb{F}_{q^k}$. Denoted by $\mathrm{Pic}_0^K(C)$ the degree zero divisor class group of C over K. Let r be an integer such that $r \mid \sharp\mathrm{Pic}_0^K(C)$ and let $\mathrm{Pic}_0^K(C)[r]$ be the divisor classes of order dividing r. Let D_1 be a divisor representing a class in $\mathrm{Pic}_0^K(C)[r]$ and D_2 be a divisor on C defined over K such that the supports of D_1 and D_2 are disjoint. Let f be a function whose divisor is equal to rD_1. Then the Tate pairing $\langle D_1, D_2\rangle_r = f(D_2)$ is a well-defined, non-degenerate, bilinear pairing

$$\mathrm{Pic}_0^K(C)[r] \times \mathrm{Pic}_0^K(C)/r\mathrm{Pic}_0^K(C) \to K^*/(K^*)^r,$$

The output of this pairing is defined up to a coset of $(K^*)^r$. Hence one defines the reduced pairing $\tau(D_1, D_2) = \langle D_1, D_2\rangle_r^{(q^k-1)/r}$ to obtain a unique value. One important property of the reduced pairing is

$$\tau(D_1, D_2) = \langle D_1, D_2\rangle_r^{(q^k-1)/r} = \langle D_1, D_2\rangle_N^{(q^k-1)/N}$$

when $N \mid (q^k - 1)$ and $N = hr$ for some h.

Throughout this paper, C will be an elliptic or a hyperelliptic curve and r will be a prime with $r \mid \sharp\mathrm{Pic}_0^K(C)$. We assume also that the curve C is a pairing-friendly curve with embedding degree k which allows denominator elimination in the computation of Tate pairings by using Miller's algorithm (see [1]).

For any integer $n \in \mathbb{N}$, let D_n be a reduced divisor equivalent to nD and let $f_{n,D}$ be the function whose divisor is $nD - D_n - m(\infty)$ for some $m \in \mathbb{N}$. When C is an elliptic curve, then $D = (P) - (\infty)$, where P is a point. Thus $D_n = (nP) - (\infty)$ and $f_{n,D}$ is just the Miller's function. If $n \in \mathbb{Z}$ with $n < 0$ then $nD = (-n)(-D)$. So D_n is a divisor equivalent to $(-n)(-D)$ and $f_{n,D}$ is a function with divisor $(-n)(-D) - (Dn) - m(\infty)$ for some m. Then the Tate pairing is $\langle D, D'\rangle_n = f_{n,D}(D')$.

The following theorem is the main result in the paper [2].

Theorem 1 [2] *Let C be a supersingular curve over $\mathbb{F}_q$ with distortion map ψ and even embedding degree k. Let D be a divisor on C defined over $\mathbb{F}_q$ with order dividing $N \in \mathbb{N}$ and let $M = (q^k - 1)/N$. Suppose $T \in \mathbb{Z}$ is such that*

1. *$TD \equiv \gamma(D)$ in the divisor class group where γ is an automorphism of C which is defined over $\mathbb{F}_q$.*
2. *γ and ψ satisfy the condition*

$$\gamma\psi^q(Q) = \psi(Q)$$

for all points $Q \in C(\mathbb{F}_q)$.

3. $T^a + 1 = LN$ *for some* $a \in \mathbb{N}$ *and* $L \in \mathbb{Z}$.

4. $T = q + cN$ *for some* $c \in \mathbb{Z}$.

Then

$$(\langle D, \psi(D')\rangle_N^M)^L = (f_{T,D}(\psi(D')))^{aMT^{a-1}}.$$

Hess, etc. proposed the Ate pairing in [14]. Although the Tate pairing as defined above allows arguments $P \in E[r]$ and $Q \in \mathbb{F}_{q^k}$, one often works with specific subgroups to speed-up the pairing computation in practice. Let π_q be the Frobenius endomorphism of the elliptic curve E, *i.e.*, $\pi_q(x, y) = (x^q, y^q)$, then the subgroups $G_1 = E[r] \cap Ker(\pi_q - [1])$ or $G_2 = E[r] \cap Ker(\pi_q - [q])$ seems to be optimal. In practice one has always used the Tate pairing on $G_1 \times G_2$, but from a theoretical point of view, the Tate pairing on $G_2 \times G_1$ has a much nicer structure.

Theorem 2 [14] *Let E be an elliptic curve over $\mathbb{F}_q$, r be a large prime with $r \mid \sharp E(\mathbb{F}_q)$ and let t be the trace of the Frobenius endomorphism, i.e., $\sharp E(\mathbb{F}_q) = q + 1 - t$. For $T = t - 1$, $Q \in G_2 = E[r] \cap Ker(\pi_q - [q])$ and $P \in G_1 = E[r] \cap Ker(\pi_q - [1])$, we have the following:*

1. *$f_{T,Q}(P)$ defines a bilinear pairing, which we call the Ate pairing.*
2. *Let $N = \gcd(T^k - 1, q^k - 1)$ and $T^k - 1 = LN$, with k the embedding degree, then $\tau(Q, P)^L = f_{T,Q}(P)^{c(q^k-1)/N}$, where $c = \sum_{i=0}^{k-1} T^{k-1-i} q^i \equiv kq^{k-1} \pmod{r}$.*
3. *The Ate pairing is non-degenerate when $r \nmid L$.*

Theorem 2 allows us to simplify the Tate pairing with a restriction. In this paper, a different restrict way to simplify the Tate pairing on curves is used. The theorem in the next section shows that we can also simplify the Tate pairing not only on elliptic curves but also on hyperelliptic curves.

3 Main results

In this section, We will prove the following theorem.

Theorem 3 *Let C be an elliptic or hyperelliptic curve (supersingular or non-supersingular) over $\mathbb{F}_q$ with embedding degree k which allows denominator elimination. Let D be a divisor on C defined over $\mathbb{F}_q$ with order dividing $N \in \mathbb{N}$ and let $M = (q^k - 1)/N$. Let D' be a divisor on C defined over $\mathbb{F}_{q^k}$ such that the supports of D and D' are disjoint. Suppose $T \in \mathbb{Z}$ is such that*

1. *$T^a + bT + c = LN$ for some $a, b, c \in \mathbb{N}$ and $L \in \mathbb{Z}$.*
2. *Let γ be an automorphism of divisor class group of C which is defined over $\mathbb{F}_q$ such that $TD \equiv \gamma(D)$ in the divisor class group and let ζ be an endomorphism in divisor class group of C which allows denominator elimination with $\gamma \circ \zeta(D') = D'$ up to a scalar multiple in $\mathbb{F}_q^*$.*

Then

$$(\langle D, D' \rangle_N^M)^L = \prod_{j=0}^{a-1} (f_{T,D}(\zeta^j(D')))^{MT^{a-1-j}} \cdot f_{bT,D} \cdot l_{T^a,bT} \cdot f_{c,D}(D')^M,$$

where $l_{T^a,bT}$ is the equation of the line through the points T^aD and bTD.

First note that, since TD is equivalent to $\gamma(D)$ we have $D_{T^i} = \gamma^i(D)$. Write d for the degree of the finite part of D. Then $D = \sum_{j=1}^d (P_j) - d(\infty)$ and so $D_{T^i} = \sum_{j=1}^d (\gamma^i(P_j)) - d(\infty)$.

Lemma 1 *With notation as above and D any divisor such that TD is equivalent to $\gamma(D)$. Then*

$$f_{T,D}(\zeta(D'))^M = f_{T,TD}(D')^M.$$

Proof. The argument is an analogue of the method used in [2]. Since $(f_{T,D}) = TD - D_T - (T-1)d(\infty)$, $(f_{T,D})^T = T(f_{T,D})$ and $(f_{T,TD}) = TD_T - D_{T^2} - (T-1)d(\infty)$, using the assumption $TD \equiv \gamma(D)$, we have

$$\begin{aligned} \gamma^*(f_{T,TD}) &= \gamma^*(TD_T - D_{T^2} - (T-1)d(\infty)) \\ &= TD - D_T - (T-1)d(\infty) \\ &= (f_{T,D}). \end{aligned}$$

Also,

$$\gamma^*(f_{T,TD}) = (\gamma^* f_{T,TD}) = (f_{T,TD} \circ \gamma).$$

Hence, we have (up to a scalar multiple in $\mathbb{F}_q^*$)

$$f_{T,TD} \circ \gamma = f_{T,D}.$$

Applying ζ to the above yields

$$f_{T,TD} \circ \gamma \circ \zeta = f_{T,D} \circ \zeta.$$

From $\gamma \circ \zeta(D') = D'$, the result follows immediately. □

Lemma 2 [2] *With notation as above, we have*

$$(f_{T^a,D}) = (f_{T,D}^{T^{a-1}} f_{T,TD}^{T^{a-2}} \cdots f_{T,T^{a-1}D}).$$

Proof. We prove only the non-supersingular case too. Note that $f_{N,D}^L = f_{LN,D} = f_{T^{a+1},D}$. Since $T^a + bT + c = LN$, we know that $(T^a + bT + c)D \equiv 0$, which implies $(T^a + bT)D \equiv -D$ and so up to a scalar multiple in $\mathbb{F}_q^*$, we have

$$f_{T^a+bT+1,D} = f_{T^a,D} f_{bT,D} l_{T^a,bT} f_{c,D}.$$

Evaluating at D' and raising to the power M we have

$$f_{T^a+bT+1,D}(D') = f_{T^a,D} f_{bT,D} l_{T^a,bT}(D').$$

By Lemma 2, this is

$$\prod_{j=0}^{a-1} f_{T,T^jD} f_{bT,D} l_{T^a,bT}(D')^{MT^{a-1-j}}.$$

Now substituting T^jD for D in Lemma 1 implies that

$$f_{T,T^jD}(D')^{MT^{a-1-j}} = (f_{T,D}(\zeta^j(D')))^{MT^{a-1-j}}.$$

Hence the result follows. □

Noting that $(\langle D, D'\rangle_N^M)^L$ is non-degenerate if L does not divide N.

4 Examples

In this section, some examples will be given. It is clear that the conditions in Theorem 3 are satisfied when the conditions in Theorem 1 hold. So Theorem 3 is an extension of Theorem 1. The following first 2 examples are from [2] while Examples 3 and 4 deal with non-supersingular curves.

Example 1 *Consider the supersingular curve $E: y^2+y=x^3+x+b$ over $\mathbb{F}_{2^m}$, where $b=0,1$ and m is odd. The embedding degree is $k=4$. The field $\mathbb{F}_{2^{4m}}$ has a basis $1, s, t, st$ over $\mathbb{F}_{2^m}$, where s and t satisfy $s^2=s+1$ and $t^2=t+s$. A distortion map ψ is given by*

$$\psi(x,y) = (x+s^2, y+sx+t).$$

Define

$$\phi(x,y) = (x+1, y+x).$$

Then $\phi^4(P)=P$ for any $P=(x,y)\in E(\mathbb{F}_{2^m})$. Let $q=2^m$ then $[q]P=\phi^m(P)$. Set $\gamma=\phi^m$. Let $N=\sharp E(\mathbb{F}_{2^m})=2^m\pm 2^{(m+1)/2}+1$ and $M=(2^{4m}-1)/N$. Taking $T=\mp 2^{(m+1)/2}-1$, $a=2$ and $L=2$, we have $T^a+1=LN$. Let ζ be the q^{th}-power Frobenius morphism. Then $\gamma(\zeta(\psi(Q)))=\psi(Q)$ for any $Q\in E(\mathbb{F}_{2^{4m}})$. Therefore, we have

$$(\langle P, \psi(Q)\rangle_N^M)^2 = (f_{T,P}^T(\psi(Q))\cdot f_{T,P}(\zeta(\psi(Q))))^M = (f_{T,P}(\psi(Q)))^{2TM}.$$

From $T=q-N$ and $f_{T,P}^{NM}=1$, we have

$$f_{T,P}^{TM} = f_{T,P}^{qM}/f_{T,P}^{NM} = f_{T,P}^{qM} = (f_{T,P}\circ\zeta)^M.$$

Therefore

$$\langle P, \psi(Q)\rangle_N^M = f_{T,P}(\zeta(\psi(Q)))^M.$$

Example 2 *Consider the supersingular curve $E: y^2=x^3-x+b$ over $\mathbb{F}_{3^m}$, where $B=\pm1$ and $\gcd(m,6)=1$. The embedding degree is $k=6$. It is well-known that $\sharp E(\mathbb{F}_{3^m})=3^m+1+B'3^{(m+1)/2}$, where B' is defined as*

$$B' = \begin{cases} B & \text{if } m\equiv 1 \pmod{12}, \\ -B & \text{if } m\equiv 7 \pmod{12}. \end{cases}$$

A distortion map ψ is given by $\psi(x,y) = (\rho - x, \sigma y)$, where $\sigma^2 = -1$ and $\rho^3 = \rho + b$. Let π be the 3-power Frobenius morphism and let $\phi(x,y) = (x - B, -y)$. Set $q = 3^m$ and $\gamma = \phi^m$. Then

$$[q](x,y) = \phi^m \pi^{2m}(x,y) = \phi^m(x,y) = \gamma(x,y).$$

Let $N = 3^m \pm 3^{(m+1)/2} + 1$ and $M = (3^{6m} - 1)/N = (3^{3m} - 1)(3^m + 1)(3^m \mp 3^{(m+1)/2} + 1)$. Taking $T = q - N = \mp 3^{(m+3)/2} - 1$, $a = 3$ and $L = \mp 3^{(m+3)/2}$, we have $T^a + 1 = LN$. Let ζ be the q^{th}-power Frobenius morphism then we have $\gamma(\zeta(\psi(Q))) = \psi(Q)$ for any $Q \in E(\mathbb{F}_{3^m})$. By Theorem 3, we have

$$(\langle P, \psi(Q)\rangle_N^M)^L = (f_{T,P}^{T^2}(\psi(Q)) \cdot f_{T,P}^T(\zeta(\psi(Q))) \cdot f_{T,P}(\zeta^2(\psi(Q))))^M.$$

From $f_{T,P}^{TM}(\psi(Q)) = f_{T,P}^M(\zeta(\psi(Q))$, we have

$$\langle P, \psi(Q)\rangle_N^M = f_{T,P}(\zeta^2(\psi(Q)))^{3M/L}.$$

Example 3 *Consider the non-supersingular curves $E: y^2 = x^3 + dx$ over $\mathbb{F}_p$, where $p \equiv 1 \pmod 4$ is a prime and $d \neq 0$. Choose suitable p and k such that the curve E is of the pairing-friendly type. Let $\alpha \in \mathbb{F}_q$ be an element of order 4. Then the map $\gamma: E \to E$ given by $(x,y) \to (-x, \alpha y)$ and $\infty \to \infty$ is an automorphism defined over $\mathbb{F}_p$. Let $P \in E(\mathbb{F}_p)$ be a point of prime order r with $r \mid \sharp E(\mathbb{F}_p)$. Then γ acts on P as a multiplication map $[T]$, where T is an integer satisfying $T^2 \equiv -1 \pmod r$. Thus there is an integer L such that $T^2 + 1 = Lr$. Let $\zeta = \gamma^3$ then we have $\gamma \circ \zeta = 1$ and $\zeta(P) = (x, -\alpha y)$. Let $N = r$ and $M = (p^k - 1)/N$. Choose $Q \in E(\mathbb{F}_{p^k})$ such that the denominator elimination is allowed. Therefore*

$$(\langle P, Q\rangle_N^M)^L = (f_{T,P}^T(Q) \cdot f_{T,P}(\zeta(Q)))^M;$$

Noting that Q and $\gamma(Q)$ have the same x-coordinate, we can save a multiplication in the computation of evaluation of the line function in each loop. Furthermore, we can choose suitable curves such $N = r = T^2 + 1$, i.e., $L = 1$. In this case the Tate pairing is

$$\langle P, Q\rangle_N^M = (f_{T,P}^T(Q) \cdot f_{T,P}(\zeta(Q)))^M.$$

Thus we have the following algorithm to compute the Tate pairing $\tau(P,Q) = \langle P, Q\rangle_N^M$ on $E: y^2 = x^3 + dx$, where $\lambda_{R,P}$ is the slope of the line through points R and P (or the tangent line at R when $P = R$).

Algorithm 1 Computation of $\tau(P,Q)$ on $E: y^2 = x^3 + dx$.

———————————————————————————-

Input: $P = (x_P, y_P)$, $Q = (x_Q, y_Q)$, $T = \sum_{i=0}^{m} T_i 2^i$, where $T_i \in \{0, 1\}$

Output: $\tau(P,Q)$

———————————————————————————-

1: Begin
2: $R = P$, $Q' = (x_Q, -\alpha y_Q)$, $f_1 = f_2 = 1$;
3: for $i = m-1$ to 0 do
4: $temp = \lambda_{R,R}(x_Q - x_R)$, $l_{R,R}(Q) = y_Q - y_R - temp$, $l_{R,R}(Q') = -\alpha y_Q - y_R - temp$;

5: $f_1 = f_1^2 \cdot l_{R,R}(Q)$*,* $f_2 = f_2^2 \cdot l_{R,R}(Q')$*,* $R = 2R$*;*
6: If $T_i = 1$ *then*
7: $temp = \lambda_{R,P}(x_Q - x_R)$*,* $l_{R,R}(Q) = y_Q - y_R - temp$*,* $l_{R,R}(Q') = -\alpha y_Q - y_R - temp$*;*
8: $f_1 = f_1 \cdot l_{R,P}(Q)$*,* $f_2 = f_2 \cdot l_{R,P}(\zeta(Q))$*,* $R = R + P$*;*
9: end for
10: $f_1 = f_1^T$*;*
11: Return $\tau(P,Q) = (f_1 f_2 f_3)^M$*.*
——————————————————————————————-

Example 4 *Consider the non-supersingular curves* $E : y^2 = x^3 + B$ *over* $\mathbb{F}_p$*, where* p *is a prime with* $p \equiv 1 \pmod 3$*. We focus on pairing-friendly elliptic curves again so that the denominator can be omitted in the Miller's algorithm. Note that many curves that have been suggested for practical use in pairing-based cryptography are in fact of this type. Also we can generate the pairing-friendly curves of this type with large embedding degree such as* 12 *(see [3]). Let* $\beta \in \mathbb{F}_p$ *be an element of order* 3*. Then the map* $\gamma : E \to E$ *given by* $(x, y) \to (\beta x, y)$ *and* $\infty \to \infty$ *is an automorphism defined over* $\mathbb{F}_p$*. Let* $P \in E(\mathbb{F}_p)$ *be a point of prime order* r*. Then* γ *acts on* P *as a multiplication map* $[T]$*, where* T *is an integer satisfying* $T^2 + T \equiv -1 \pmod r$*. Thus there is an integer* L *such that* $T^2 + T + 1 = Lr$*. Let* $\zeta(x, y) = (\beta^2 x, y)$ *then* $\gamma \circ \zeta(P) = (P)$*. Let* $N = r$ *and* $M = (p^k - 1)/N$*. Choose* $Q \in E(\mathbb{F}_{p^k})$ *such that the denominator elimination is allowed. By Theorem 3, we have*

$$(\langle P, Q\rangle_N^M)^L = (f_{T,P}^{T+1}(Q) \cdot f_{T,P}(\zeta(Q)) \cdot l_{T^2,T}(Q))^M,$$

where $l_{T^2,T}(Q) = y_Q - y_P$ *is the equation of the line through points* T^2P *and* TP*. Especially, if we can generate a suitable elliptic curve such that* $N = r = T^2 + T + 1$*, then we can compute the Tate pairing as*

$$\langle P, Q\rangle_N^M = (f_{T,P}^{T+1}(Q) \cdot f_{T,P}(\zeta(Q)) \cdot l_{T^2,T}(Q))^M.$$

Now we have the following algorithm to compute the L*-th power of the Tate pairing* $\tau(P,Q)^L = \langle P, Q\rangle_N^M$ *on* $E : y^2 = x^3 + B$*, where* $l_{R,P}$ *is the equation of the line through points* R *and* P *(or the tangent line at* R *when* $P = R$*).*

Algorithm 2 Computation of $\tau(P,Q)^L$ ***on*** $E : y^2 = x^3 + B$***.***
——————————————————————————————-
Input: $P = (x_P, y_P)$*,* $Q = (x_Q, y_Q)$*,* $T = \sum_{i=0}^{m} T_i 2^i$ *where* $T_i \in \{0, 1\}$
Output: $\tau(P,Q)^L$
——————————————————————————————-
1: Begin
2: $R = P$*,* $f_1 = f_2 = 1$*,* $f_3 = y_Q - y_P$*;*
3: for $i = m - 1$ *to* 0 *do*
4: $f_1 = f_1^2 \cdot l_{R,R}(Q)$*,* $f_2 = f_2^2 \cdot l_{R,R}(\zeta(Q))$*,* $R = 2R$*;*
5: If $T_i = 1$ *then*
6: $f_1 = f_1 \cdot l_{R,P}(Q)$*,* $f_2 = f_2 \cdot l_{R,P}(\zeta(Q))$*,* $R = R + P$*;*

7: end for
8: $f_1 = f_1^{T+1}$*;*
9: Return $\tau(P,Q)^L = (f_1 f_2 f_3)^M$.
——————————————————————————-

For comparing our method with the algorithm in [21], consider the elliptic curve E_{512} : $y^2 = x^3 + 5$ *over* $\mathbb{F}_p$*, where*

$$p = 1145747568399549380635317418620582531453546123676759744111\\ 5533728505070527823154532657656991234473986641703193940343\\ 5598236286688787343269095020893934936 43.$$

The embedding degree of E_{512} *is* $k = 2$*. We choose* $T = 2^{80} + 2^{16}$ *which gives a prime* $N = T^2 + T + 1$ *of 161 bits. In this case we has a very low Hamming weight of* T*. Choose the points* $P = (x_P, y_P) \in E_{512}(\mathbb{F}_p)[N]$ *and* $Q = (x_Q, y_Q) \in E_{512}(\mathbb{F}_{p^2})$ *such that* $x_Q \in \mathbb{F}_p$*. Then we have the following algorithm to compute the Tate pairing* $\tau(P,Q) = \langle P,Q\rangle_N^M$ *on* E_{512}*.*

Algorithm 3 Computation of $\tau(P,Q)$ ***on*** E_{512}***.***

——————————————————————————-
Input: $P = (x_P, y_P)$, $Q = (x_Q, y_Q)$, $T = 2^{80} + 2^{16}$
Output: $\tau(P,Q)$
——————————————————————————-
1: Begin
2: $R = P$, $Q' = (\beta^2 x_Q, y_Q)$, $f_1 = f_2 = 1$, $f_3 = y_Q - y_P$*;*
3: for $i = 39$ *to* 0 *do*
4: $f_1 = (f_1^2 \cdot l_{R,R}(Q))^2 \cdot l_{2R,2R}(Q)$, $f_1 = (f_1^2 \cdot l_{R,R}(Q'))^2 \cdot l_{2R,2R}(Q')$, $R = 4R$.
5: if $T_i = 1$ *then*
6: $f_1 = f_1 \cdot l_{R,P}(Q)$, $f_2 = f_2 \cdot l_{R,P}(Q')$, $R = R + P$*;*
7: end for
8: $f_1 = f_1^{T+1}$*;*
9: Return $\tau(P,Q) = (f_1 f_2 f_3)^{(p-1)(p+1)/N}$.
——————————————————————————-

Note that in this algorithms, we use the direct algorithm to compute $4R$ *as in [10] which cost about* 25 *multiplications in* $\mathbb{F}_p$ *if we assume that the computational cost of an inverse in* $\mathbb{F}_p^*$ *is 10M. We assume also one square and one multiplication in* $\mathbb{F}_{p^2}^*$ *as 2M and 3M. For the final power we use the method in [20]. Thus the total cost of the Algorithm 3 is 2864M while the algorithm in [21] requires 3329M or 3163M with extra storage. Therefore the cost of this algorithm can be reduced by* 14% *or* 10%*.*

One needs to compute the scalar multiplication of a point in the computation of Tate pairings. However in the Jacobian projective coordinates we have a more efficient method to perform it. Let the point $P = (X_1, Y_1, Z_1)$ *correspond to the point* $(X_1/Z_1^2, Y_1/Z_1^3)$ *in affine coordinates. Set* $2P = (X_2, Y_2, Z_2)$*. Then* $X_2 = 9X_1^4 - 8X_1Y_1^2$, $Y_2 = 3X_1^2(4X_1Y_1^2 - X_2) - 8Y_1^4$

and $Z_2 = 2Y_1Z_1$. *According to the affine line equation, we have*

$$\begin{aligned} l_{P,P}(x,y) &= y - \frac{Y_1}{Z_1^3} - \frac{3X_1^2}{2Y_1Z_1}\left(x - \frac{X_1}{Z_1^2}\right) = y - \frac{3X_1^2}{2Y_1Z_1}x - \frac{2BZ_1^6 - X_1^3}{2Y_1Z_1^3} \\ &= \frac{Z_2Z_1^2y - 2Y_1^2 - (3X_1^2)(Z_1^2x - X_1)}{2Y_1Z_1^3}. \end{aligned}$$

Since $p \equiv 3 \pmod 4$, -1 *ia a quadratic non-residue in* $\mathbb{F}_p$. *Let* $i^2 = -1$ *then any element in* $\mathbb{F}_{p^2}$ *have a "complex number" form. Let* $Q = (x_Q, y_Q) \in E_{512}(\mathbb{F}_{p^2})$, *where* $x_Q = s + ti$ *and* $y_Q = u + vi$ *with* $s, t, u, v \in \mathbb{F}_p$. *Let us restrict* Q *to be the form where* $t = u = 0$. *Then we can ignore the denominator in the computation of the Tate pairing. Therefore we can let* $Q = (x_Q, iy_Q)$, *where* $x_Q, y_Q \in \mathbb{F}_p$. *Hence*

$$l_{P,P}(Q) = \frac{Z_2Z_1^2y_Qi - 2Y_1^2 - (3X_1^2)(Z_1^2x_Q - X_1)}{2Y_1Z_1^3}.$$

Since $Y_1, Z_1 \in \mathbb{F}_p$, *we can assume that*

$$l_{P,P}(x,y) = Z_2Z_1^2y - 2Y_1^2 - (3X_1^2)(Z_1^2x - X_1)$$

and then we have

$$l_{P,P}(Q) = Z_2Z_1^2y_Qi - 2Y_1^2 - (3X_1^2)(Z_1^2x_Q - X_1).$$

Therefore we need only 11M to compute $l_{R,R}(Q)$ *and* $2R$ *from the point* R. *Noting that* $\zeta(Q) = (\beta^2 x_Q, y_Qi)$, *we need 13M to compute* $l_{R,R}(Q)$, $l_{R,R}(\zeta(Q))$ *and* $2R$. *Furthermore we can let* $P = (x_p, y_P, 1)$, *thus the point addition of* $R + P$, $l_{R,P}(Q)$ *and* $l_{R,P}(\zeta(Q))$ *will cost 15M. Therefore, in the Jacobian projective coordinates we need only 2739M (not forgetting the point* $P = (x_P, y_P, 1)$*) to compute the Tate pairing of* E_{512} *by application of Theorem 3. Thus the cost of our algorithm can be reduced by* 18% *or* 13%. *Also it should be pointed out that the above method can be applied to Example 3 too.*

5 What about T and ζ

In order to use Theorems 3, a main problem is to find T, γ and ζ which satisfy the conditions. There is no general method to find them until now. Usually the automorphism γ of C will be chosen as the T multiplications map as in above examples. In this section, some ideas and strategies for choosing T and ζ will be proposed.

The integer T and the endomorphism ζ should be chosen so that $f_T(\zeta(D'))$ (or $f_T(\zeta^j(\psi(D')))$) can be computed efficiently by $f_T(D')$ (or $f_T(\psi(D'))$). At first, we would like to choose T such that the absolute value $|T|$ is small enough to reduce the iterative numbers in the computation of the Tate pairing. By practical experiences, in order to find ζ which can correspond to T, some special numbers, such as p, the characteristic of the field, or q, or q^k, or $q - \sharp\mathrm{Pic}_0^K(C)$ would be considered to be candidates for T.

Let E be a general curve over the field K with $\mathrm{char}(K) \neq 2$. For any point $P = (x, y) \in E$ and an integer $T > 0$, we have

$$[T]P = \left(\frac{\phi_T(x,y)}{\psi_T^2(x,y)}, \frac{\omega_T(x,y)}{\psi_T^3(x,y)} \right),$$

where $\psi_T(x, y)$ is the division polynomial. Let $\zeta(x, y) = (x', y')$. In order to decide the endomorphism ζ after T is chosen, we need to solve the equations

$$\frac{\phi_T(x',y')}{\psi_T^2(x',y')} = x \quad \text{and} \quad \frac{\omega_T(x',y')}{\psi_T^3(x',y')} = y$$

with unknowns x' and y'. But in general these equations can not be solved in some practical applications. So how to choose ζ is still a difficult problem.

Generally, we have the following strategies to consider this problem.

1. Choose T, ζ so that we have $f_{T,D}(\zeta^j(D'))^M = f_{T,D}(D')^{MT^{j'}}$ for some integer j'. For general curves, this aim may be difficult to get. But at least we hope to compute $f_{T,D}(\zeta^j(D'))^M$ from $f_{T,D}(D')^M$ more easily.
2. In the iterative procedure, we need to compute the line function value of $l(x, y) = y - y' - \lambda(x - x')$ at $\psi(Q)$ or Q. We hope to choose T and ζ such that $\zeta^j(\psi(Q))$ and $\psi(Q)$ have the same x-coordinate. Then it is free to compute $l(\zeta^j(\psi(Q))$ from $l(\psi(Q))$. Similarly, if they have the same y-coordinate, then we can use the projective coordinates to simplify the computation as in Example 4.

6 Conclusion

A method for the efficient computation of Tate pairings on elliptic and hyperelliptic curves which is a generalization of Barreto, etc.'s method [2] is presented in this paper. Our method is different from F. Hess etc.[14]. It can reduce the number of loops in the computation of the Tate pairing and can be used not only on supersingular but also on non-supersingular curves. It can also be used on curves with large embedding degrees. This method is consistent with eta pairings when the conditions of eta pairings are satisfied. An example shows the cost of the algorithm in this paper can be reduced by 18% or 13% than the best known algorithm.

References

[1] P.S.L.M. Barreto, B. Lynn and M. Scott, On the selection of pairing-friendly groups, SAC 2003, LNCS 3006, 17–25, Spinger-Verlag, 2004.

[2] P.S.L.M. Barreto, S. Galbraith, C. Ó hÉigeartaigh and M. Scott, Efficient pairing computation on supersingular abelian varieties, Cryptology ePrint Archive, Report 2004/375, 2004.

[3] P.S.L.M. Barreto and M. Naehrig, Pairing-friendly elliptic curves of prime order, SAC 2005, LNCS 3897, 319–331, Springer-Velag, 2006.

[4] I.F. Blake, G. Seroussi and N.P. Smart, *Advances in Elliptic Curve Cryptography*, Cambridge University Press, 2005.

[5] D. Boneh and M. Franklin, Identity-based encryption from the Weil pairing, SIAM Journal of Computing 32(3), 586–615, 2003.

[6] D. Boneh, B. Lynn and H. Shacham, Short signatures from the Weil pairing, *Advances in Cryptology – Asiacrypt'2001*, LNCS 2248, 514–532, Springer-Verlag, 2002.

[7] D.G. Cantor, Computing in the jacobian of a hyperelliptic curve, Math. Comp. 48(177), 95–101, 1987.

[8] I. Duursma and H.-S. Lee, Tate pairing implementation for hyperelliptic curves $y^2 = x^p - x + d$, *Advances in Cryptology – Asiacrypt'2003*, LNCS 2894, 111–123, Springer-Verlag, 2003.

[9] R. Dutta, R. Barua and P. Sarkar, Pairing-based cryptography: A survey, Cryptology ePrint Archive, Report 2004/064.

[10] R. Feng anf H. Wu, Encapsulated scalar multiplications and line functions in the computation of Tate pairing, TAMC 2007, LNCS 4484, 159–170, Springer-Verlag, 2007.

[11] G. Frey and H.-G. Ruck, A remark concerning m-divisibility and the discrete logarithm problem in the divisor class group of curves. Math. Comp. 52, 865–874, 1994.

[12] S. Galbraith, K. Harrison and D. Soldera, Implementing the Tate pairing, *Algorithmic Number Theory – ANTS V*, LNCS 2369, 324–337, Springer-Verlag, 2002.

[13] S. Galbraith, Pairings, *Advances in Elliptic Curve Cryptography*, London Math. Soc. Lecture Note Ser. 317, 183–213, Cambridge Univ. Press, 2005.

[14] F. Hess, N. Smart and F. Vercauteren, The Eta-pairing revisited, IEEE Transactions on Information Theory, 52(10):4595C4602, 2006.

[15] N. Koblitz and A. Menezes, Pairing-based cryptography at high security levels, Cryptology ePrint Archive, Report 2005/076, 2005.

[16] S. Kwon, Efficient Tate pairing computation for elliptic curves over binary fields, ACISP 2005, LNCS 3574, 134–145, 2005.

[17] A.J. Menezes, *Elliptic Curve Public Key Cryptosystems*, Kluwer Academic Publishers, 1993.

[18] V. Miller, Short programs for functions on curves, Unpublished manuscript, 1986.

[19] V. Miller, The Weil pairing, and its efficient calculation, Journal of Cryptology 17(4), 235–261, September 2004.

[20] M. Scott, Computing the Tate pairing, CT-RSA 2005, LNCS 3376, 293–304, Springer-Verlag, 2005.

[21] M. Scott, Faster pairings using an elliptic curve with an efficient endomorphism, *Advances in Cryptology – Indocrypt'2005*, LNCS 3797, 258–269, Springer-Verlag, 2005.

[22] M. Scott and P.S.L.M. Barreto, Compressed pairings, *Advances in Cryptology – Crypto'2004*, LNCS 3152, 140–156, Springer-Verlag, 2004.

[23] A. Shamir, Identity-based cryptosystems and signature schemes, *Advances in Cryptology – Crypto'84*, LNCS 196, 47–53, Springer-Verlag, 1985.

[24] J.H. Silverman, *The Arithmetic of Elliptic Curves*, GTM 106, Springer-Verlag, 1986.