Efficient and Generalized Pairing Computation on Abelian Varieties

Eunjeong Lee, Hyang-Sook Lee, and Cheol-Min Park

***Abstract*—In this paper, we propose a new method for constructing a bilinear pairing over (hyper)elliptic curves, which we call the *R-ate* pairing. This pairing is a generalization of the Ate and Ate$_i$ pairing, and can be computed more efficiently. Using the R-ate pairing, the loop length in Miller's algorithm can be as small as $\log(r^{1/\phi(k)})$ for some pairing-friendly elliptic curves which have not reached this lower bound. Therefore, we obtain savings of between 29% and 69% in overall costs compared to the Ate_i pairing. On supersingular hyperelliptic curves of genus 2, we show that this approach makes the loop length in Miller's algorithm shorter than that of the Ate pairing.**

***Index Terms*—Ate pairing, elliptic curves, hyperelliptic curves, pairing based cryptography, Tate pairing.**

I. Introduction

THE development of efficient algorithms for pairing computation has been a very important issue in pairing-based cryptosystems. The pairing computation on Abelian varieties is generally based on Miller's algorithm for rational functions from scalar multiplications of divisors. Many algorithms for efficient pairing computation have been developed by reducing the iteration loops in Miller's algorithm. Barreto *et al.* [1] and Galbraith *et al.* [11] proposed algorithms for fast computation of the Tate pairing over some supersingular elliptic curves. Duursma and Lee [6] improved the BKLS-GHS algorithms by shortening the loop length of Miller's algorithm over some hyperelliptic curves. Barreto *et al.* [2] extended the Duursma–Lee method to supersingular Abelian varieties using the Eta pairing approach. Recent breakthroughs include the Ate pairing on ordinary elliptic curves by Hess *et al.* [15], which is a generalization of Eta pairing, followed by the Ate pairing on hyperelliptic curves by Granger *et al.* [14]. Matsuda *et al.* [19] showed that the Ate pairing is always at least as fast as the Tate pairing by providing optimized versions of the Ate and the twisted Ate pairing. For fast pairing computation, it is known that the loop length in Miller's algorithm of the Ate pairing can be as small as $\Lambda_{r,k} = \log(r^{1/\phi(k)})$ where $\phi(k)$ is the Euler-phi function of embedding degree k and the prime number r is the order of cyclic subgroup of given Abelian variety [15]. Zhao *et al.* [25] showed that the loop length reaches $\Lambda_{r,k}$ for some ordinary elliptic curves by proposing the Ate$_i$ pairing.

In this paper, we propose a new method to construct a bilinear pairing over (hyper)elliptic curves. We call the pairing obtained by this method *R-ate* pairing. We show that the Ate and Ate$_i$ pairing can be constructed by this approach. Therefore, this new pairing is a generalization of the Ate and Ate$_i$ pairing. The R-ate pairing has two main advantages for efficient pairing computation. First, using the R-ate pairing, the loop length in Miller's algorithm can be as small as $\Lambda_{r,k}$ for some pairing-friendly elliptic curves which have not reached this lower bound. Therefore, this pairing enables the loop length to be around two or three times shorter than that of the Ate$_i$ pairing on the curves suggested in [3], [7], [8]. Second, we show that, on supersingular hyperelliptic curves of genus 2, the loop length of the R-ate pairing can be reduced by up to half compared to the Ate pairing. In particular, we consider the DL curve [6], $y^2 = x^5 - x + d$, and analyze the complexity of the R-ate pairing on the curve. This result shows that the R-ate pairing is around 19% faster than the Ate pairing on this curve at 160-bit security level.

Galbraith *et al.* suggested some open problems regarding hyperelliptic pairings in [12]. The first problem is related to loop shortening for the hyperelliptic Ate pairing. The R-ate pairing on hyperelliptic curves gives a positive answer for this question.

This paper is organized as follows. Section II includes the basic mathematical backgrounds such as the Tate, Ate, and Ate$_i$ pairings and Miller's algorithm. In Section III, we define the R-ate pairing and also investigate the criterion for the R-ate pairing to be computed efficiently. Section IV provides examples of the R-ate pairings on supersingular elliptic curves over a finite field in characteristic 3 and ordinary elliptic curves. Section V describes the R-ate pairings over supersingular hyperelliptic curves of genus two. Section VI includes the complexity analysis of the R-ate pairings over (hyper)elliptic curves provided in Sections IV and V.

II. Preliminaries on Pairings

In this section, we briefly recall the definitions of the Tate pairing, Ate pairing, and Ate$_i$ pairing over (hyper)elliptic curves and also review Miller's algorithm to compute pairings. For a good survey of pairings, refer to [12].

A. The Tate, Ate, and Ate$_i$ Pairings

Let $\mathbb{F}_q$ be a finite field with q elements, and C be a nonsingular curve of genus g over $\mathbb{F}_q$. We denote by J_C the group of degree zero divisor classes of C. If $g = 1$, then J_C is an elliptic curve group. We refer to [16] for the definitions and the notations related to divisors.

Manuscript received January 07, 2008; revised January 30, 2008. Current version published March 18, 2009. The work of E. Lee and H.-S. Lee was supported in part by KOSEF under Grant R01-2005-000-10713-0. The work of C.-M. Park was supported by BK 21.

E. Lee is with the Department of Mathematics, North Carolina State University, Raleigh, NC 27695-8205 USA (e-mail: ejlee@ncsu.edu).

H.-S. Lee and C.-M. Park are with the Department of Mathematics, Ewha Womans University, 11-1 Daehyun-dong, Seodaemun-gu, Seoul 120-750, Korea (e-mail: hsl@ewha.ac.kr; mpcm@ewha.ac.kr).

Communicated by A. Canteaut, Associate Editor for Complexity and Cryptography.

Digital Object Identifier 10.1109/TIT.2009.2013048

We recall the definition of the Tate pairing [9]. Let r be a positive divisor of the order of $J_C(\mathbb{F}_q)$ with $\gcd(r,q)=1$, and k be the smallest integer such that $r \mid (q^k-1)$; such k is called *the embedding degree*. Let $J_C[r]$ be the set of divisor classes of order dividing r. The *Tate pairing* is a map

$$\langle \cdot,\cdot \rangle_r : J_C[r] \times J_C(\mathbb{F}_{q^k})/rJ_C(\mathbb{F}_{q^k}) \to \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r$$
$$\langle D,E \rangle_r = f_{r,D}(E')$$

where $\mathrm{div}(f_{r,D}) = rD$ and $E' \sim E$ with $support(E') \cap support(\mathrm{div}(f_{r,D})) = \emptyset$. We define the reduced Tate paring by $e(D,E) = \langle D,E \rangle_r^{\frac{q^k-1}{r}}$ so that the pairing value is defined uniquely. Here r can be replaced by any integer N such that $r|N|q^k-1$ [11]. Thus, $e(D,E) = \langle D,E \rangle_N^{\frac{q^k-1}{N}}$.

Let φ be the q-power Frobenius endomorphism on J_C and $\mathbb{G}_1 = J_C[r] \cap \ker(\varphi - [1])$, $\mathbb{G}_2 = J_C[r] \cap \ker(\varphi - [q])$. For ordinary curves, the Ate pairing [14], [15] and the Ate$_i$ pairing [25] on divisors $D_1 \in \mathbb{G}_1, D_2 \in \mathbb{G}_2$ are defined as follows:

$$\text{Ate pairing } (g=1): a(D_2,D_1) = f_{t-1,D_2}(D_1)^{(q^k-1)/r}, \quad \text{where } t \text{ is a trace of } \varphi$$
$$\text{Ate pairing } (g \geq 2): a(D_2,D_1) = f_{q,D_2}(D_1)$$
$$\text{Ate}_i \text{ pairing } (g=1): a_i(D_2,D_1) = f_{q^i \bmod r,D_2}(D_1)^{(q^k-1)/r}, \quad \text{for } 0 < i < k.$$

The Ate (Ate$_i$) pairings can also be defined over $\mathbb{G}_1 \times \mathbb{G}_2$. These pairings are called the *Twisted Ate* pairings. For the details of the Twisted Ate pairing, see [14], [15]. For supersingular (hyper)elliptic curves, there exists a *distortion map* ψ such that $e(D,\psi(E)) \neq 1$ for two divisors $D,E \in \mathbb{G}_1$ with prime order [13], [23]. If we use the distortion map, we can define the Ate pairing on $\mathbb{G}_1 \times \mathbb{G}_1$ with the condition that $\psi(\mathbb{G}_1) = \mathbb{G}_2$. This pairing is called the *Eta* pairing [2], [6]. The Eta pairing is a special form of the Twisted Ate pairing on supersingular curves. But the Eta pairing is introduced before the Ate pairing.

B. Miller's Algorithm

The pairings over (hyper)elliptic curves are computed using the algorithm proposed by Miller [20]. The main part of Miller's algorithm is constructing the rational function $f_{n,D}$ and evaluating $f_{n,D}(E)$ with $\mathrm{div}(f_{n,D}) = nD - (nD)$ for divisors D and E. Let $G_{iD,jD}$ be a rational function with

$$\mathrm{div}(G_{iD,jD}) = iD + jD - (iD \oplus jD) \tag{1}$$

where $\oplus$ is the group law on J_C and $(iD \oplus jD)$ is reduced. Using the following relation, Miller's algorithm computes $f_{n,D}(E)$:

$$f_{i+j,D} = f_{i,D} f_{j,D} G_{iD,jD}.$$

In the case of elliptic curves, $G_{iD,jD}$ is the rational function which is the line passing through the points P_i and P_j divided by the vertical line passing through the point P_{i+j} where $iD = (P_i) - (\infty)$, $jD = (P_j) - (\infty)$ and $(i+j)D = (P_{i+j}) - (\infty)$.

The Miller's algorithm is explicitly described in Algorithm 1. We denote by $\mathtt{M}(D,E,\ell)$ the procedure in Algorithm 1 for the inputs $D,E \in J_C[r]$ and $\ell \in \mathbb{Z}/r\mathbb{Z}$. The procedure $\mathtt{M}$ returns the value $f_{\ell,D}(E)$ and ℓD. We call the steps in the **for**-loop of Miller's algorithm as *Miller operation* (MO) and the length of the **for**-loop as *Miller length*. That is, in Algorithm 1, steps 4 through 10 are for Miller operation and Miller length is $\lfloor \log_2 \ell \rfloor$. We also divide Miller operation into two parts: Miller doubling (MD) and Miller addition(MA).

Algorithm 1 Miller's Algorithm

procedure $\mathtt{M}(D,E,\ell)$

INPUT: $D,E \in J_C, \ell \in \mathbb{Z}/r\mathbb{Z}, \ell = \sum_{i=0}^{\lfloor \log_2 \ell \rfloor - 1} \ell_i 2^i$ $(\ell_i = 0,1)$

OUTPUT: $f_{\ell,D}(E), \ell D$

1: $T \leftarrow D$
2: $f \leftarrow 1$
3: **for** $i \leftarrow \lfloor \log_2 \ell \rfloor - 1$ down to 0 **do**
4: ◇ *Miller-doubling step* (MD)
5: $f \leftarrow f^2 \cdot G_{T,T}(E)$
6: $T \leftarrow 2T$
7: **if** $\ell_i = 1$ **then**
8: ◇ *Miller-addition step* (MA)
9: $f \leftarrow f \cdot G_{T,D}(E)$
10: $T \leftarrow T + D$
11: **end if**
12: **end for**
13: **return** f, T

III. The R-ate Pairing

In this section, we construct a new pairing, which we call the *R-ate* pairing because the R-ate pairing can be regarded as a ratio of any two pairings. We also investigate the criterion for the R-ate pairing to be computed efficiently.

A. Construction of the R-ate Pairing

We use the same notation as in the previous sections. We recall the Ate$_i$ pairing on an elliptic curve which is defined by

$$f_{T_i,D}(E), \quad T_i = q^i \bmod r.$$

Our observation is that the Ate$_i$ pairing is constructed from the parameters (q,r) which are used to define the Ate and Tate pairing. We extend this idea to define a new bilinear pairing by using any combinations of parameters of previously known pairings such as r, q, T_i. First, we define the R-ate pairing for arbitrary integers A and B.

Definition III.1: For $A,B,a,b \in \mathbb{Z}$ with $A = aB + b$, we define the R-ate pairing to be

$$R_{A,B}(D,E) = f_{a,BD}(E) \cdot f_{b,D}(E) \cdot G_{aBD,bD}(E). \tag{2}$$

Generally, this definition does not give a nondegenerate, bilinear pairing. However, if A and B are chosen parameters which determine the Miller loop for bilinear pairings, the R-ate pairing satisfies the condition of nondegeneracy and bilinearity.

Theorem III.2: Let C be a nonsingular curve over $\mathbb{F}_q$ and r be a large prime which divides $N = \#J_C(\mathbb{F}_q)$ (or $\#E(\mathbb{F}_q)$). Let D and E be divisors on C defined over $\mathbb{F}_q$ with an order dividing r. Let A and B be integers with the following characteristics.

1. $A = aB + b$ for $a, b \in \mathbb{Z}$.
2. $f_{A,D}(E)$ and $f_{B,D}(E)$ are nondegenerate bilinear pairings with the following relations:

$$e(D,E)^{L_1} = f_{A,D}(E)^{M_1}, \quad e(D,E)^{L_2} = f_{B,D}(E)^{M_2}$$

for some integers L_1, L_2, M_1 and M_2.

Let $M = \mathrm{lcm}(M_1, M_2)$, $d_1 = M/M_1, d_2 = M/M_2$, and $L = d_1L_1 - ad_2L_2$. If $r \nmid L$, then the R-ate pairing $R_{A,B}(D,E)$ is a nondegenerate bilinear pairing with the following relation:

$$e(D,E)^L = R_{A,B}(D,E)^M.$$

Proof: Let $D = \sum_{i=1}^{d}(P_i) - d(O)$. We have

$$\begin{aligned}(f_{aB,D}) &= (aB)(D) - D_{(aB)} - d(aB-1)(O)\\ &= aB(D) - aD_B - ad(B-1)(O)\\ &\quad + aD_B - D_{aB} - d(a-1)(O)\\ &= a(f_{B,D}) + (f_{a,BD}).\end{aligned}$$

Hence

$$f_{aB,D} = f_{B,D}^a \cdot f_{a,BD}.$$

Therefore

$$\begin{aligned}f_{A,D}(E) &= f_{aB+b,D}(E)\\ &= f_{aB,D}(E) \cdot f_{b,D}(E) \cdot G_{aBD,bD}(E)\\ &= f_{B,D}^a(E) \cdot f_{a,BD}(E) \cdot f_{b,D}(E) \cdot G_{aBD,bD}(E)\\ &= f_{B,D}^a(E) \cdot R_{A,B}(D,E).\end{aligned}$$

By assumption, $f_{A,D}(E)$ and $f_{B,D}^a(E)$ are bilinear pairings. So $R_{A,B}(D,E)$ is also a bilinear pairing. Moreover

$$\begin{aligned}f_{A,D}(E)^M &= f_{B,D}(E)^{aM} \cdot R_{A,B}(D,E)^M\\ e(D,E)^{d_1L_1} &= e(D,E)^{ad_2L_2} \cdot R_{A,B}(D,E)^M.\end{aligned}$$

Hence

$$e(D,E)^L = R_{A,B}(D,E)^M.$$

By this relation, the R-ate pairing $R_{A,B}(D,E)^M$ is nondegenerate if $r \nmid L$. □

In (2), the R-ate pairing requires Miller's algorithm twice for the initial divisors (BD) and D. However, if we choose B to be $q^i \bmod r$ which is the parameter for the Ate$_i$ pairing, we can construct the efficient R-ate pairing by making two initial divisors identical as shown in Corollary III.3. For simplicity, we represent $R(D,E)$ instead of $R_{A,B}(D,E)$ if A and B are clear from the context.

Corollary III.3: Let C be a nonsingular curve over $\mathbb{F}_q$ with embedding degree k and r be a large prime divisor of $\#J_C(\mathbb{F}_q)$. Let $\mathbb{G}_1 = J_C[r] \cap \ker(\varphi - [1])$, $\mathbb{G}_2 = J_C[r] \cap \ker(\varphi - [q])$, and $D_2 \in \mathbb{G}_2, D_1 \in \mathbb{G}_1$. We let

— $T_i \equiv q^i \bmod r$ for $0 < i < k$ and h_i be the smallest integer such that $T_i^{h_i} \equiv 1 \bmod r$;
— $N_i = \gcd(T_i^{h_i} - 1, q^k - 1)$ and $T_i^{h_i} - 1 = L_iN_i$.
— $c_i = \sum_{j=0}^{h_i-1} T_i^{h_i-1-j}(q^i)^j \bmod N_i$ and $M_i = (q^k-1)/N_i$.

For each chosen parameters (A,B) with $A = aB + b$, the R-ate pairing follows with the relation

$$e(D_2,D_1)^L = R(D_2,D_1)^M$$

for each L and M:

1. For $(A,B) = (q^i, r)$

$$\begin{aligned}R(D_2,D_1) &= f_{T_i,D_2}(D_1)\\ L &= iq^{i-1}\frac{q^k-1}{r} - kq^{k-1}a\\ M &= kq^{k-1} \cdot \frac{q^k-1}{r}.\end{aligned}$$

2. For $(A,B) = (q, T_1)$ where $q > T_1$

$$\begin{aligned}R(D_2,D_1) &= f_{a,D_2}(D_1)^q \cdot f_{b,D_2}(D_1) \cdot G_{aTD_2,bD_2}(D_1)\\ L &= M_1 - aL_1, \quad M = c_1M_1.\end{aligned}$$

3. For $(A,B) = (T_i, T_j)$

$$\begin{aligned}R(D_2,D_1) &= f_{a,D_2}(D_1)^{q^j} \cdot f_{b,D_2}(D_1) \cdot G_{aT_jD_2,bD_2}(D_1)\\ L &= d_iL_i - ad_jL_j\\ M &= \mathrm{lcm}(c_iM_i, c_jM_j) = d_ic_iM_i = d_jc_jM_j.\end{aligned}$$

4. For $(A,B) = (r, T_j)$

$$\begin{aligned}R(D_2,D_1) &= f_{a,D_2}(D_1)^{q^j} \cdot f_{b,D_2}(D_1) \cdot G_{aT_jD_2,bD_2}(D_1)\\ L &= d_0 - ad_jL_j,\\ M &= \mathrm{lcm}\left(\frac{q^k-1}{r}, c_jM_j\right) = d_0\frac{q^k-1}{r} = d_jc_jM_j.\end{aligned}$$

Proof: Since the proofs of cases 2 and 4 are similar to that of the case 3, we just prove cases 1 and 3.

Case 1. Let $q^i = ar + b$. In this case

$$f_{q^i,D_2}(D_1) = f_{ar,D_2}(D_1) \cdot f_{b,D_2}(D_1).$$

Since $b = T_i$

$$R(D_2,D_1) = f_{T_i,D_2}(D_1).$$

By [15, Lemma 2,3]

$$e(D_2,D_1)^{iq^{i-1}} = f_{q,D_2}(D_1)^{kq^{k-1}iq^{i-1}} = f_{q^i,D_2}(D_1)^{kq^{k-1}}.$$

By the property of the Tate pairing

$$e(D_2,D_1)^a = f_{ar,D_2}(D_1)^{\frac{q^k-1}{r}}.$$

Hence

$$e(D_2,D_1)^{iq^{i-1}\frac{q^k-1}{r} - kq^{k-1}a} = R(D_2,D_1)^{kq^{k-1}\cdot\frac{q^k-1}{r}}.$$

Case 3. Let $T_i = aT_j + b$. In this case

$$\begin{aligned}f_{T_i,D_2}(D_1) = f_{T_j,D_2}^a(D_1) &\cdot f_{a,T_jD_2}(D_1)\\ &\cdot f_{b,D_2}(D_1) \cdot G_{aT_jD_2,bD_2}(D_1).\end{aligned}$$

By [25, Theorem 1]

$$f_{a,T_jD_2}(D_1) = f_{a,D_2}(D_1)^{q^j}.$$

Hence

$$R(D_2, D_1) = f_{a,D_2}(D_1)^{q^j} \cdot f_{b,D_2}(D_1) \cdot G_{aT_jD_2,bD_2}(D_1).$$

Since

$$e(D_2, D_1)^{L_l} = f_{T_l,D_2}^{c_l M_l}(D_1)$$

for $l = i, j$

$$e(D_2, D_1)^{d_i L_i - a d_j L_j} = R(D_2, D_1)^M$$

where $M = \mathrm{lcm}(c_i M_i, c_j M_j)$, $M = d_i c_i M_i = d_j c_j M_j$. □

Remark III.4:

1) The R-ate pairing in the case 1 of Corollary III.3 is the Ate$_i$ pairing [25].
2) For supersingular elliptic curves and superspecial hyperelliptic curves, Corollary III.3 can be also applied to $\mathbb{G}_1 \times \mathbb{G}_2$ by [14], [15].

Algorithm 2 R-ate Pairing

`procedure R-ate` (P, Q, a, b)

INPUT: $P \in \mathbb{G}_1, Q \in \mathbb{G}_2, a, b, j \in \mathbb{Z}$.

OUTPUT: $R(Q, P) = f_{a,Q}(P)^{q^j} \cdot f_{b,Q}(P) \cdot G_{aT_jQ,bQ}(P)$.

1: Set $m_1 = \max\{a, b\}$, $m_2 = \min\{a, b\}$.
◇ *Compute f_a, f_b, aQ and bQ, where $\{a, b\} = \{m_1, m_2\}$.*
2: $c \leftarrow [\frac{m_1}{m_2}]$, $d \leftarrow m_1 - c \cdot m_2$.
3: $f_{m_2}, m_2Q \leftarrow \mathtt{M}(Q, P, m_2)$.
4: $f_{c,m_2}, c \cdot m_2Q \leftarrow \mathtt{M}(m_2Q, P, c)$.
5: $f_d, dQ \leftarrow \mathtt{M}(Q, P, d)$.
6: $f_1 \leftarrow f_{m_2}^c \cdot f_{c,m_2} \cdot f_d$.
7: $f_{m_1} \leftarrow f_1 \cdot G_{c \cdot m_2Q, dQ}(P)$.
8: $m_1Q \leftarrow c \cdot m_2Q + dQ$.
9: $f_2 \leftarrow f_a^{q^j} \cdot f_b$.
10: $Q_1 \leftarrow \varphi^j(aQ)$.
11: $f_3 \leftarrow f_2 \cdot G_{Q_1,bQ}(P)$.
12: **return** f_3

Algorithm 2 describes the computation of the R-ate pairing with respect to a and b which are explained in Corollary III.3. If c or d are very small, where $\max\{a, b\} = c\min\{a, b\} + d$, the performance of Algorithm 2 is similar to that of Miller's algorithm with the loop length $\log_2 \max\{a, b\}$. In the following section, we investigate the condition of the parameters a, b, c, and d which provides an efficient implementation of the R-ate pairing.

B. Criterion for the Efficient R-ate Pairing

In this section, we observe the condition when the R-ate pairing is more efficient than the Ate$_i$ pairing.

We recall pairings,

Ate$_i$: $f_{\mathsf{T},D_2}(D_1)$, where $\mathsf{T} = \min_{1 \le i \le k-1}\{T^i (\mathrm{mod}\ r)\}$

R-ate: $f_{a,D_2}(D_1)^{q^j} \cdot f_{b,D_2}(D_1) \cdot G_{aq^jD_2,bD_2}(D_1)$.

To estimate the complexity of Algorithm 2, we use the following notation:

M_i: the cost for a multiplication in $\mathbb{F}_{q^i}$;

$\mathcal{T}(\mathtt{M}(D_2, D_1, \ell))$: the cost for Miller's algorithm described in Algorithm 1 for $D_1 \in \mathbb{G}_1, D_2 \in \mathbb{G}_2$ and $\ell \in \mathbb{Z}$;

$\mathcal{T}_{G,A}(\mathcal{T}_{G,D})$: the cost for the rational function G appearing in a point addition (doubling) and an evaluation of G at D_1;

$\mathcal{T}_{\mathtt{MA}}(\mathcal{T}_{\mathtt{MD}})$: the cost for Miller addition (doubling) in Algorithm 1;

$\mathcal{T}_{\mathtt{MO}}$: the cost for Miller operation in Algorithm 1.

Then, from Algorithms 1 and 2, we obtain the following costs for the computation of pairings:

$$\begin{aligned} C(\text{Ate}_i) &= \mathcal{T}_{\mathtt{MO}} \cdot \log_2 \mathsf{T} \\ C(\text{R-ate}) &= \mathcal{T}_{\mathtt{MO}} \cdot (\log_2 \min\{a, b\} + \log_2 c + \log_2 d) \\ &\quad + \mathrm{Exp}(c) + \mathcal{T}_{\mathtt{MA}} + 4M_k + \mathcal{T}_{G,A} \end{aligned} \tag{3}$$

where $\mathrm{Exp}(c)$ is the cost for computing $f^c \in \mathbb{F}_{q^k}$, $\mathcal{T}_{\mathtt{MA}}$ is the cost for Steps 7 and 8, and $\mathcal{T}_{G,A}$ is the cost for Step 11.

From [15], [17], we assume the cost for a squaring is similar to the cost for a multiplication and the ratio of an inversion to a multiplication is 10. We ignore the cost for the Frobenius map since it is relatively small compared to the cost for a multiplication and also we omit the final powering step since the Ate$_i$ pairing and the R-ate pairing have the same final powering.

For simplicity, let us consider the ordinary elliptic curves with even embedding degree k. As seen in [11], [15], G can be considered as a line for even embedding degree. For a given elliptic curve $E/\mathbb{F}_q$, the tangent line $G_{T,T}$ at $T = (x_T, y_T) \in E(\mathbb{F}_{q^k})$ of step 5 in Algorithm 1 can be obtained by two squares, one multiplication, and one inversion in $\mathbb{F}_{q^k}$. The line $G_{T,D}$ through $T = (x_T, y_T)$ and $D = (x_D, y_D)$ of step 9 in Algorithm 1 can be obtained by one inversion and two multiplications in $\mathbb{F}_{q^k}$. The third point followed from the doubling $2T$ or the addition $T + D$ requires additional multiplications. This analysis is from the group operation of elliptic curves which is described in [16] as a formula. Each evaluation of the line at $D_1 \in E(\mathbb{F}_q)$ needs a multiplication of x-coordinate of D_1 which is an element in $\mathbb{F}_q$ and the slope of the line which is an element in $\mathbb{F}_{q^k}$. Thus, the costs for the elementary steps using affine coordinates in Full–Miller are as follows:

$$\begin{aligned} \mathcal{T}_{G,A} &= I_k + 2M_k + kM_1 \\ \mathcal{T}_{G,D} &= I_k + 3M_k + kM_1 \\ \mathcal{T}_{\mathtt{MA}} &= \mathcal{T}_{G,A} + 3M_k = I_k + 5M_k + kM_1 \\ \mathcal{T}_{\mathtt{MD}} &= \mathcal{T}_{G,D} + 4S_k = I_k + 7M_k + kM_1 \\ &= \mathcal{T}_{G,A} + 5M_k = \mathcal{T}_{\mathtt{MA}} + 2M_k = 17M_k + kM_1. \end{aligned} \tag{4}$$

Since the cost for Miller operation of Miller's algorithm depends on whether the addition step exists in Algorithm 1, we have

$$\mathcal{T}_{\mathtt{MD}} \le \mathcal{T}_{\mathtt{MO}} \le \mathcal{T}_{\mathtt{MA}} + \mathcal{T}_{\mathtt{MD}}$$

and $\mathcal{T}_{\mathtt{MO}} = \mathcal{T}_{\mathtt{MD}} + \frac{1}{2}\mathcal{T}_{\mathtt{MA}}$ on average due to the binary expansion of the integer ℓ.

Since $\mathcal{T}_{\mathtt{MO}} \ge \mathcal{T}_{\mathtt{MD}} = 17M_k + kM_1 \ge 17M_k$ and $\mathrm{Exp}(c) \le 2(\log_2 c)M_k$, we have

$$\mathrm{Exp}(c) \le 2(\log_2 c)M_k \le \frac{2(\log_2 c)\mathcal{T}_{\mathtt{MO}}}{17}.$$

From (3) and (4), we obtain $\mathcal{T}_{\mathtt{MA}}+4M_k+\mathcal{T}_{G,A} \le \mathcal{T}_{\mathtt{MA}}+\mathcal{T}_{\mathtt{MD}} \le 2\mathcal{T}_{\mathtt{MO}}$ and

$$C(\text{R-ate}) \le \mathcal{T}_{\mathtt{MO}} \cdot (\log_2(\min\{a,b\}) + \frac{19\log_2 c}{17} + \log_2 d + 2). \quad (5)$$

Therefore, the criterion for the R-ate pairing to be more efficient than the Ate$_i$ pairing follows:

$$\gamma(E) := \frac{\log_2(\min\{a,b\}) + \frac{19\log_2 c}{17} + \log_2 d + 2}{\log_2 \mathsf{T}} < 1 \implies \frac{C(\text{R-ate})}{C(\text{Ate}_i)} < 1. \quad (6)$$

The parameters a, b for the R-ate pairing satisfying (6) can be obtained by looking into the combinations for (A, B) in Corollary III.3. As $\gamma(E)$ gets smaller, the R-ate pairing becomes more efficient than the Ate$_i$ pairing. For example, the curves E_2 through E_5 in Section IV.B (Table I) have

$$\gamma(E_2) = \frac{(9/34)\log_2 r + 2}{(3/8)\log_2 r} \sim \frac{2}{3}$$
$$\gamma(E_3) = \frac{(1/4)\log_2 r + 2}{(3/4)\log_2 r} \sim \frac{1}{3}$$
$$\gamma(E_4) = \frac{(1/4)\log_2 r + 3}{(1/2)\log_2 r} \sim \frac{1}{2}$$
$$\gamma(E_5) = \frac{(1/4)\log_2 r + 2}{(1/2)\log_2 r} \sim \frac{1}{2}$$

which show the R-ate pairings on the curves are more efficient than the Ate$_i$ pairing. The values $\gamma(E_i), i = 2, \ldots, 5$, also represent the ratios for the timing results of both pairings on examples (see Table III in Section VI).

IV. The R-ate Pairing on Elliptic Curves

In this section, we discuss the computation of R-ate pairings on supersingular elliptic curves in characteristic 3 and ordinary elliptic curves including E_1, E_2, E_3, E_4 and E_5.

A. Supersingular Elliptic Curves

We give an example for the computation of R-ate pairing on the supersingular curve on $\mathbb{F}_{3^n}$,

$$S_1 : y^2 = x^3 - x + b, b = \pm 1, \quad \gcd(n, 6) = 1$$

whose order is

$$N = \#E(\mathbb{F}_{3^n}) = 3^n + 1 \pm 3^{\frac{(n+1)}{2}} ([2], [6]).$$

For the curve S_1, we can use the distortion map $\psi(x, y) = (\rho - x, \sigma y)$ to define the R-ate pairing on $\mathbb{G}_1 \times \mathbb{G}_1$, where $\rho^3 - \rho - b = 0$ and $\sigma^2 + 1 = 0$.

Since $3^n = \mp 3^{\frac{n-1}{2}}(T + 1)$, where $T = 3^n - N$, we use $(A, B) = (3^n, T)$ and thus we have the following R-ate pairing for $P, Q \in \mathbb{G}_1$

$$R(P, \psi(Q)) = f_{3^{\frac{(n-1)}{2}}, (T+1)P}(\psi(Q)) \cdot G_{TP,P}(\psi(Q))^{3^{\frac{(n-1)}{2}}}.$$

When $\pm(T + 1) < 0$, we use $(T + 1)P = -(T + 1)(-P)$. By the case 2 of Corollary III.3, this pairing has the relation $e(P, \psi(Q))^L = R(P, \psi(Q))^M$, with $L = M_1 - 3^{\frac{n-1}{2}} L_1$, $M = c_1 M_1$ for $T_1 = T$. Since $(c_1, N) = 1$, we have the reduced R-ate pairing $R(P, \psi(Q))^{\frac{q^k-1}{N}} = e(P, \psi(Q))^{L'}$ with $L' \equiv Lsc_1^{-1} \bmod N$, where $N_1 = Ns$.

By the final powering, we can ignore the vertical line and thus we only compute $l_{TP,P}(\psi(Q))$ instead of $G_{TP,P}(\psi(Q))$. Note that the explicit formulas for $(T + 1)P$ and $l_{TP,P}(\psi(Q))$ are simple [2] and this R-ate pairing has one shorter Miller length than the η_T pairing. We give Algorithm 3 for computation of the R-ate pairing without a cubic root.

We can similarly define the R-ate pairing on the supersingular elliptic curves in characteristic 2, $S_2 : y^2 + y = x^3 + x + b, b = 0, 1$ over $\mathbb{F}_{2^n}$ discussed in [2], [18].

Algorithm 3 R-ate Pairing on $y^2 = x^3 - x + 1$ over $\mathbb{F}_{3^n} (n \equiv 5, 7 \bmod 12)$

procedure R1(P, Q, ψ)
INPUT: $P, Q \in E(\mathbb{F}_{3^n})$, $\psi(x, y) = (\rho - x, \sigma y)$
OUTPUT: $R(P, \psi(Q))$
  $l \leftarrow l_{TP,P} = y_P(x - x_P) + y_P - y$
  $f \leftarrow l_{TP,P}(\psi(Q))$
  for j $= 0$ to $\frac{n-3}{2}$ **do**
    $f \leftarrow f^3$
    $x_P \leftarrow x_P^9 - 1, y_P \leftarrow -y_P^9$
    $u \leftarrow x_P + x_Q - 1$
    $g \leftarrow \sigma y_P y_Q - u^2 - \rho u - \rho^2$
    $f \leftarrow fg$
  end for
  return finalpower(f)

B. Ordinary Elliptic Curves

In this subsection, we consider the R-ate pairing on ordinary elliptic curves. As discussed in [15], [25], the Miller loop of the Ate (Ate$_i$) pairing can possibly be as small as $r^{1/\phi(k)}$. However some ordinary elliptic curves [3], [7], [8], [21] cannot reach this low bound. We show that the R-ate pairing gives this low bound on such curves.

Let $\mathbb{F}_p$ be a defining field of each elliptic curve and N be the order of $\mathbb{F}_p$-rational points with a large prime divisor r. Let

$$P_1 \in \mathbb{G}_1 = E[r] \cap \ker(\varphi - [1])$$
$$P_2 \in \mathbb{G}_2 = E[r] \cap \ker(\varphi - [q]).$$

and

$$\mathsf{T} = \min_{0<i<k}\{T_i\}, \quad T_i = q^i \bmod r.$$

The R-ate pairings $R(P_2, P_1)$ on ordinary elliptic curves, say $E_1, \ldots, E_5$, are as follows.

Example IV.1: Let E_1 be the curve over $\mathbb{F}_p$ in [21] with k, p, N, r, and T shown at the bottom of the following page.

Since $r = T_1 + b$ for $(A, B) = (r, T_1)$ which is case 4 of Corollary III.3, we have the efficient R-ate pairing with respect to a, b as follows:

$$R(P_2, P_1) = f_{b,P_2}(P_1) \cdot G_{T_1P_2,bP_2}(P_1)$$

where

$$\begin{aligned} &a = 1, \quad b = 100667465(27 \text{ bits}) \\ &L = d_0 - d_1 L_1 \\ &M = \operatorname{lcm}\left(\frac{q^k - 1}{r}, c_1 M_1\right) = d_0 \frac{q^k - 1}{r} = d_1 c_1 M_1. \end{aligned}$$

Note that the low bound, $r^{1/\phi(k)} \sim 2^{27}$, is comparable to b in bit size. Since $(d_0, r) = 1$, we have the reduced R-ate pairing $R(P_2, P_1)^{\frac{q^k-1}{r}}$ equal to $e(P_2, P_1)^{L'}$ with $L' \equiv L d_0^{-1} \bmod r$.

Example IV.2: Let E_2 be the curve over $\mathbb{F}_p$ in [21] with k, p, N, r and T also shown at the bottom of the page. Since $T_9 = a \cdot T_2 + b$ for $(A, B) = (T_9, T_2)$ which is case 3 of Corollary III.3, we have the efficient R-ate pairing with respect to a, b as follows:

$$\begin{aligned} R(P_2, P_1) &= f_{a,P_2}(P_1)^{q^2} \cdot f_{a^2,P_2}(P_1) \cdot G_{aT_2P_2,a^2P_2}(P_1) \\ &= f_{a,P_2}(P_1)^{q^2} \cdot f_{a,P_2}(P_1)^a \cdot f_{a,aP_2}(P_1) \\ &\quad \cdot G_{aT_2P_2,a^2P_2}(P_1) \end{aligned}$$

where

$$\begin{aligned} &a = 1028669(20 \text{ bits}), \quad b = 1058159911561 = a^2 \\ &L = d_9 L_9 - a d_2 L_2 \\ &M = \operatorname{lcm}(c_9 M_9, c_2 M_2) = d_9 c_9 M_9 = d_2 c_2 M_2 = d_2 c_2 \frac{q^k - 1}{N_2}. \end{aligned}$$

Note that the low bound, $r^{1/\phi(k)} \sim 2^{40}$, is comparable to b in bit size. Let $N_2 = rs$. Since $(d_2 c_2, r) = 1$, we have the reduced R-ate pairing $R(P_2, P_1)^{\frac{q^k-1}{r}}$ equal to $e(P_2, P_1)^{L'}$ with $L' \equiv L s (d_2 c_2)^{-1} \bmod r$.

Example IV.3: Let E_3 be the curve over $\mathbb{F}_p$ in [8] with

$$\begin{aligned} &k = 8 \\ &p = 1/4(81z^6 + 54z^5 + 45z^4 + 12z^3 + 13z^2 + 6z + 1) \\ &r = 9z^4 + 12z^3 + 8z^2 + 4z + 1 \\ &\mathsf{T} = T_1 = -9z^3 - 3z^2 - 2z - 1. \end{aligned}$$

Since $T_3 = T_2 + b$ for $(A, B) = (T_3, T_2)$ which is case 3 of Corollary III.3, we have the efficient R-ate pairing with respect to a, b as follows:

$$R(P_2, P_1) = f_{b,P_2}(P_1) \cdot G_{T_2P_2,bP_2}(P_1)$$

where

$$\begin{aligned} &a = 1, \quad b = 3z + 1 \\ &L = d_3 L_3 - d_2 L_2 \\ &M = \operatorname{lcm}(c_3 M_3, c_2 M_2) = d_3 c_3 M_3 = d_2 c_2 M_2 = d_2 c_2 \frac{q^k - 1}{N_2}. \end{aligned}$$

When $z < 0$, we can use $T_7 = T_6 - b$. Note that the low bound, $r^{1/\phi(k)} \sim z$, is comparable to b in bit size. Let $N_2 = rs$. Since $(d_2 c_2, r) = 1$, we have the reduced R-ate pairing $R(P_2, P_1)^{\frac{q^k-1}{r}}$ equal to $e(P_2, P_1)^{L'}$ with $L' \equiv L s (d_2 c_2)^{-1} \bmod r$. We implement the R-ate pairing on E_3 with these parameters for $z = 1013235040279$ (Section VI).

Remark IV.4: By [8], this curve has a twist curve of degree 4. Hence, we can use the twisted Ate pairing. For the twisted R-ate pairing, we can use $-4r = aT_2 + b$ where $a = 2z + 1, b = 3z^2 + 2z$. The twisted R-ate pairing is

$$R(P_1, P_2) = f_{a,P_1}(P_2)^{q^2} \cdot f_{b,P_1}(P_2) \cdot G_{aT_2P_1,bP_1}(P_2)$$

where $P_1 \in \mathbb{G}_1, P_2 \in \mathbb{G}_2$.

Example IV.5: Let E_4 be the curve over $\mathbb{F}_p$ in [7] with

$$\begin{aligned} &k = 10 \\ &p = 25z^4 + 25z^3 + 25z^2 + 10z + 3 \\ &r = 25z^4 + 25z^3 + 15z^2 + 5z + 1 \\ &\mathsf{T} = T_2 = 5z^2. \end{aligned}$$

Since $T_4 = aT_2 + b$ for $(A, B) = (T_4, T_2)$ which is case 3 of Corollary III.3, we have the efficient R-ate pairing with respect to a, b as follows:

$$\begin{aligned} R(P_2, P_1) &= f_{a,P_2}(P_1)^{q^2} \cdot f_{b,P_2}(P_1) \cdot G_{aT_2P_2,bP_2}(P_1) \\ &= f_{a,P_2}(P_1)^{q^2} \cdot f_{a+2,P_2}(P_1) \cdot G_{aT_2P_2,(a+2)P_2}(P_1) \\ &= f_{a,P_2}(P_1)^{q^2} \cdot f_{a,P_2}(P_1) \cdot f_{2,P_2}(P_1) \\ &\quad \cdot G_{aP_2,2P_2}(P_1) \cdot G_{aT_2P_2,(a+2)P_2}(P_1) \end{aligned}$$

$$\begin{aligned} k &= 7\,(E_1) \\ p &= 152683916815195328299425822768509148050335333587091954124192528892961908503610 31 \\ N &= 152683916815195328299425822768509148050335333587091954124192528892961909510284 96 \\ r &= 104072213104282429150399849503973550888567656476 1(160 \text{ bits}) \\ \mathsf{T} &= T_2 = 10133938509526225(54 \text{ bits}). \end{aligned}$$

$$\begin{aligned} k &= 10\,(E_2) \\ p &= 396120610547891063909698040682890664156040501831963430185626838652064692433391635091 \\ N &= 396120610547891063909698040682890664156040501831963430185626838653153188731457177400 \\ r &= 125373224226869067404938302067196601969906495432 1(160 \text{ bits}) \\ \mathsf{T} &= T_6 = 108849629806554230 9(60 \text{ bits}). \end{aligned}$$

where

$$a=-(5z+3),\quad b=-(5z+1)$$
$$L=d_4L_4-ad_2L_2$$
$$M=\mathrm{lcm}(c_4M_4,c_2M_2)=d_4c_4M_4=d_2c_2M_2=d_2c_2\frac{q^k-1}{N_2}.$$

When $z>0$, we can use $T_9=-aT_2-b$. Note that the low bound, $r^{1/\phi(k)}\sim z$, is comparable to b in bit size. Let $N_2=rs$. Since $(d_2c_2,r)=1$, we have the reduced R-ate pairing $R(P_2,P_1)^{\frac{q^k-1}{r}}$ equal to $e(P_2,P_1)^{L'}$ with $L'\equiv Ls(d_2c_2)^{-1} \bmod r$. For $z=-164286669864814370$ suggested in [7], we implement the R-ate pairing on E_4 with these parameters (Section VI).

Example IV.6: Let E_5 be the curve over $\mathbb{F}_p$ in [3] with

$$k=12$$
$$p=36z^4+36z^3+24z^2+6z+1$$
$$r=36z^4+36z^3+18z^2+6z+1$$
$$\mathsf{T}=T_1=6z^2.$$

Since $T_{10}=a\cdot T_1+b$ for $(A,B)=(T_{10},T_1)$ which is case 3 of Corollary III.3, we have the efficient R-ate pairing with respect to a,b as follows:

$$\begin{aligned}R(P_2,P_1)&=f_{a,P_2}(P_1)^q\cdot f_{b,P_2}(P_1)\cdot G_{aT_1P_2,bP_2}(P_1)\\&=f_{b+1,P_2}(P_1)^q\cdot f_{b,P_2}(P_1)\cdot G_{(b+1)T_1P_2,bP_2}(P_1)\\&=\{f_{b,P_2}(P_1)\cdot G_{bP_2,P_2}(P_1)\}^q\cdot f_{b,P_2}(P_1)\\&\quad\cdot G_{(b+1)T_1P_2,bP_2}(P_1),\end{aligned}$$

where

$$a=6z+3,\quad b=6z+2$$
$$L=d_{10}L_{10}-ad_1L_1$$
$$M=\mathrm{lcm}(c_{10}M_{10},c_1M_1)=d_{10}c_{10}M_{10}=d_1c_1M_1=d_1c_1\frac{q^k-1}{N_1}.$$

When $z<0$, we can use $T_4=-aT_1-b$. Note that the low bound, $r^{1/\phi(k)}\sim z$, is comparable to b in bit size. Let $N_1=rs$. Since $(d_1c_1,r)=1$, we have the reduced R-ate pairing $R(P_2,P_1)^{\frac{q^k-1}{r}}$ equal to $e(P_2,P_1)^{L'}$ with $L'\equiv Ls(d_1c_1)^{-1} \bmod r$. For $z=6917529027641089837$ suggested in [3], we implement the R-ate pairing on E_5 with these parameters (Section VI).

Remark IV.7: By [3], this curve has a twist curve of degree 6. Hence we can use the twisted Ate pairing. For the twisted R-ate pairing, we can use $2r=aT_{10}+b$ where $a=2z+1, b=6z^2+4z$. The twisted R-ate pairing is

$$R(P_1,P_2)=f_{a,P_1}(P_2)^{q^{10}}\cdot f_{b,P_1}(P_2)\cdot G_{aT_{10}P_1,bP_1}(P_2),$$

where $P_1\in\mathbb{G}_1$, $P_2\in\mathbb{G}_2$.

Table I summarizes the parameters for the Ate$_i$ pairing and the R-ate pairing discussed in the above examples.

V. The R-Ate Pairing on Supersingular Hyperelliptic Curves

The Ate pairing on hyperelliptic curves of genus g can reduce the loop length in Miller's algorithm up to g times shorter than the Tate pairing [14]. In this section, we show that, by using the R-ate pairing, the loop length of Miller's algorithm can be about half as small as that of the Ate pairing on supersingular hyperelliptic curves with $g=2$.

Theorem V.1: Let H be a supersingular hyperelliptic curve of genus 2 defined over $\mathbb{F}_q, q=p^n, n$ odd. Suppose $N=\#J_H(\mathbb{F}_q)=q^2+aq+b$ for some integers a and b, and let r be a large prime factor of N.

Then, for $D_1\in\mathbb{G}_1=J_C[r]\cap\ker(\varphi-[1])$ and $D_2\in\mathbb{G}_2=J_C[r]\cap\ker(\varphi-[q])$, the *R-ate* pairing is given by

$$R(D_2,D_1)=\begin{cases}\text{if } q^2>N,\\ \quad f^q_{-a,D_2}(D_1)\cdot f_{-b,D_2}(D_1)\cdot G_{-qaD_2,-bD_2}(D_1)\\ \text{if } q^2<N,\\ \quad f^q_{a,D_2}(D_1)\cdot f_{b,D_2}(D_1)\cdot \lambda_{qaD_2,bD_2}(D_1)\end{cases}\tag{7}$$

where

$$|a|\le 4\sqrt{q}+10, |b|\le 4\sqrt{q}+1, |a-b|\le 9\tag{8}$$

and λ_{qaD_2,bD_2} is a polynomial such that $\mathrm{div}(\lambda_{qaD_2,bD_2})+2(\infty)-(qaD_2)-(bD_2)$ is an effective divisor.

Furthermore, for $T_2=q^2-N$ and $T_1=q$, the relation to the Tate pairing is

$$e(D_2,D_1)^L=R(D_2,D_1)^M$$

where

$$\begin{aligned}&L=d_2L_2-ad_1L_1,\ M=\mathrm{lcm}(c_2M_2,c_1M_1), && \text{if } q^2>N\\&L=-(d_2L_2+ad_1L_1), M=\mathrm{lcm}(c_2M_2,c_1M_1), && \text{if } q^2<N\end{aligned}$$

using the notation defined in Corollary III.3.

Proof: Since H is supersingular, from [10], we know that

$$\begin{aligned}&N=\#J_H(\mathbb{F}_q)=q^2+a_1q+a_2+a_1+1\\&a_1\equiv 0 \pmod{p^{(n+1)/2}}\\&a_2\equiv 0 \pmod{p^n}\end{aligned}\tag{9}$$

where a_1 and a_2 are the coefficients of the characteristic polynomial of q-power Frobenius map on H. With combining the Hasse–Weil bound [10], [22], [24], and (9), we obtain

$$\begin{aligned}&-2q\le a_2=qa_2'\le 10q\\&|a_1|\le 4\sqrt{q}\\&N=q^2+q(a_1+a_2')+a_1+1\end{aligned}$$

for some integer a_2'.

Let $a=a_1+a_2'$ and $b=a_1+1$. Then

$$|a|\le 4\sqrt{q}+10, |b|\le 4\sqrt{q}+1,\quad |a-b|\le 9.$$

TABLE I
EXAMPLES: ORDINARY ELLIPTIC CURVES

Curve	Parameters ($T_i \equiv q^i \mod r$)
E_1 [21]	$k = 7$
	$p = 152683916815195328299425822768509148050335333587$ $0\backslash 91954124192528892961908503610 31$
	$r = 10407221310428242915039984950397355088856765647 61$
	$T_2 = 10133938509526225(54bits)$
	$r = T_1 + 100667465(27bits)$
E_2 [21]	$k = 10$
	$p = 396120610547891063909698040682890664156040501831 9$ $\backslash 63430185626838652064692433391635091$
	$r = 125373224226869067404938302067196601969906495432 1$
	$T_6 = 1088496298065542309(60bits)$
	$T_9 = 1028669 \cdot T_2 + 1058159911561(40bits)$
E_3 [8]	$k = 8$
	$p = 1/4(81z^6 + 54z^5 + 45z^4 + 12z^3 + 13z^2 + 6z + 1)$
	$r = 9z^4 + 12z^3 + 8z^2 + 4z + 1$
	$T_1 = -9z^3 - 3z^2 - 2z - 1$
	$T_3 = T_2 + 3z + 1$
E_4 [7]	$k = 10$
	$p = 25z^4 + 25z^3 + 25z^2 + 10z + 3$
	$r = 25z^4 + 25z^3 + 15z^2 + 5z + 1$
	$T_2 = 5z^2$
	$T_9 = (5z + 3)T_2 + (5z + 1)$
E_5 [3]	$k = 12$
	$p = 36z^4 + 36z^3 + 24z^2 + 6z + 1$
	$r = 36z^4 + 36z^3 + 18z^2 + 6z + 1$
	$T_1 = 6z^2$
	$T_{10} = (6z + 3)T_1 + 6z + 2$

In the case of $q^2 > N$, $T_2 = q^2 - N = (-a)q + (-b) = (-a)T_1 + (-b)$. As for case 3 of Corollary III.3, we have the R-ate pairing and the relation.

In the case of $q^2 < N$, $-T_2 = -(q^2 - N) = aq + b = aT_1 + b$. Since $f_{-T_2,D_2} = 1/(f_{T_2,D_2} \cdot v_{T_2D_2})$ where $\mathrm{div}(v_{T_2D_2}) = (T_2D_2) + (-T_2D_2)$, we have

$$\begin{aligned} 1/f_{T_2,D_2}(D_1) &= f_{-T_2,D_2}(D_1) \cdot v_{T_2D_2}(D_1) \\ &= f_{aT_1+b,D_2}(D_1) \cdot v_{T_2D_2}(D_1) \\ &= f_{T_1,D_2}(D_1)^a \cdot f_{a,D_2}^q \cdot f_{b,D_2}(D_1) \\ &\quad \cdot G_{qaD_1,bD_2}(D_1) \cdot v_{q^2D_2}(D_1) \\ &= f_{T_1,D_2}(D_1)^a \cdot R(D_2, D_1). \end{aligned}$$

From the definition of G in (1), G_{qaD_2,bD_2} is a rational function of the form $\frac{\lambda_{qaD_2,bD_2}}{v_{(qaD_2 \oplus bD_2)}}$ [20] such that

$$\begin{aligned} D' &:= \mathrm{div}(\lambda_{qaD_2,bD_2}) + 2(\infty) - (qaD_2) - (bD_2) > 0 \\ &\mathrm{div}(v_{(qaD_2 \oplus bD_2)}) + 4(\infty) - D' > 0. \end{aligned}$$

Since $(-q^2D_2) = (qaD_2 \oplus bD_2)$ and $\mathrm{div}(v_{q^2D_2}) = \mathrm{div}(v_{-q^2D_2})$

$$G_{qaD_2,bD_2}(D_1) \cdot v_{q^2D_2}(D_1) = \lambda_{qaD_2,bD_2}(D_1).$$

Following a similar proof as that for case 3 in Corollary III.3, we have the theorem. □

Remark V.2: The R-ate pairing with a, b defined in Theorem V.1 can be computed using Algorithm 2. Since $|d| \leq 9$ where $\max\{a, b\} = \min\{a, b\} + d$, we have

$$\begin{aligned} C(\text{R}-\text{ate}) \leq\ & \mathcal{T}_{\mathtt{MO}} \cdot (\log_2 \min\{a, b\} + \log_2 9) \\ & + \mathcal{T}_{\mathtt{MA}} + 3M_k + \mathcal{T}_{G,A} \quad (10) \end{aligned}$$

from (3). Since $\mathcal{T}_{\mathtt{MA}} + 3M_k + \mathcal{T}_{G,A} \leq 2\mathcal{T}_{\mathtt{MO}}$, the loop length in Miller's algorithm is up to $\log_2 \min\{a, b\} + 5$ which is about half of $\log_2 q$. Therefore, the R-ate pairing on supersingular hyperelliptic curves gives a positive answer for the open problem regarding loop shortening for the hyperelliptic Ate pairing suggested by Galbraith *et al.* in [12].

In the case of some curves like DL-curves, the cost for the Miller operation using the special automorphisms ([2], [6], [14]) is very small compared to the cost for computing G in (7). Therefore, the additional cost such as $\mathcal{T}_{\mathtt{MA}} + 3M_k + \mathcal{T}_{G,A}$ in (10) is expensive relative to the cost of Miller's algorithm using the automorphisms and thus the total cost may be larger than a half of the cost of the Ate pairing. As an example, we consider the R-ate pairing on the DL-curve, $y^2 = x^5 - x + d$ of genus 2. Since this curve is superspecial [14], the R-ate pairing can be defined on $\mathbb{G}_1 \times \mathbb{G}_2$. We also analyze its complexity in Section VI, and it shows that the R-ate pairing is around 19% faster than the Ate pairing on this curve.

Example V.3: We consider the R-ate pairing on $H_5 : y^2 = x^5 - x + d, d = 1, 2$ over $\mathbb{F}_{5^n}$ with

$k = 5$

$N^{\pm} = 5^{2n} + (3 \pm 5^{\frac{n+1}{2}})5^n + 1 \pm 5^{\frac{n+1}{2}}$

distortion map $\psi(x, y) = (\rho - x, 2y), \quad \rho^2 - \rho + 2d = 0.$

By Theorem V.1, the R-ate pairing on H_5 for $D, E \in J_H(\mathbb{F}_{5^n})[r]$ is as follows.

In the case of N^- $(q^2 > N)$, we have

$$\begin{aligned} R(D, \psi(E)) = & f_{-a,D}(\psi(E))^q \cdot f_{-b,D}(\psi(E)) \\ & \cdot G_{-aT_1D,-bD}(\psi(E)) \quad (11) \end{aligned}$$

where

$$a = 3 - 5^{\frac{n+1}{2}}, \quad b = 1 - 5^{\frac{n+1}{2}}.$$

Using the explicit formula for multiplication by 5 map [6], (11) can be computed by the following equation. We only consider degenerate divisors $D, E \in J_{H_5}(\mathbb{F}_{5^n})$. Let $\mu = 5^{\frac{n+1}{2}}$. Since $f_{1,D} = f_{2,D} = G_{\mu D,-D} = 1$ for degenerate divisor D

$$\begin{aligned} &R(D, \psi(E)) \\ &= \left(f^q_{\mu-3,D} \cdot f_{\mu-1,D} \cdot G_{(\mu-3)T_1D,(\mu-1)D}\right)(\psi(E)) \\ &= ((f_{\mu,D} \cdot f_{-3,D} \cdot G_{\mu D,-3D})^q \cdot (f_{\mu,D} \cdot f_{-1,D} \cdot G_{\mu D,-D}) \\ &\quad \cdot G_{(\mu-3)T_1D,(\mu-1)D})(\psi(E)) \\ &= \left(\left(f_{\mu,D} \cdot \frac{1}{\lambda_{2D,D}} \cdot G_{\mu D,-3D}\right)^q \cdot \left(f_{\mu,D} \cdot \frac{1}{v_D}\right)\right. \\ &\quad \left. \cdot\, G_{5^n(\mu-3)D,(\mu-1)D}\right)(\psi(E)). \end{aligned}$$

In the case of N^+ ($q^2 < N$), we have

$$R(D, \psi(E)) = f_{a,D}(\psi(E))^q \cdot f_{b,D}(\psi(E)) \cdot \lambda_{aT_1D,bD}(\psi(E)) \quad (12)$$

where

$$a = 5^{\frac{n+1}{2}} + 3, \quad b = 5^{\frac{n+1}{2}} + 1.$$

As above, (12) can be computed by the following equation:

$$\begin{aligned} &R(D, \psi(E)) \\ &= \left(f^q_{\mu+3,D} \cdot f_{\mu+1,D} \cdot \lambda_{(\mu+3)T_1D,(\mu+1)D}\right)(\psi(E)) \\ &= ((f_{\mu,D} \cdot f_{3,D} \cdot G_{\mu D,3D})^q \cdot (f_{\mu,D} \cdot f_{1,D} \cdot G_{\mu D,D}) \\ &\quad \cdot \lambda_{(\mu+3)T_1D,(\mu+1)D})(\psi(E)) \\ &= ((f_{\mu,D} \cdot G_{2D,D} \cdot G_{\mu D,3D})^q \cdot (f_{\mu,D}) \\ &\quad \cdot \lambda_{5^n(\mu+3)D,(\mu+1)D})(\psi(E)). \end{aligned} \quad (13)$$

The relation to the Tate pairing is the same as in Theorem V.1.

VI. Complexity Analysis

In this section, we examine the performance of the suggested pairings on various examples. We describe the R-ate pairing on ordinary elliptic curves E_1 through E_5 in Section IV-B and hyperelliptic curve H_5 in Section V. We also observe the complexity of the Ate$_i$ pairing and the R-ate pairing on $\mathbb{G}_2 \times \mathbb{G}_1$ for each elliptic curve. For H_5, we consider the complexity of the Ate$_i$ pairing and the R-ate pairing on $\mathbb{G}_1 \times \mathbb{G}_2$ where $\mathbb{G}_2 = \psi(\mathbb{G}_1), \psi$ is a distortion map as described in [13]. Algorithm 2 for the R-ate pairing consists of two parts: Miller's algorithms (Steps 3 through 5) and the additional parts (Steps 6 through 11). To compare the cost of the R-ate pairing with that of the Ate$_i$ pairing, we express the total cost of Algorithm 2 as the length of Miller loop by converting the cost for the additional parts to the number of Miller operations.

In Section III-B, we observed the costs of the R-ate pairing as (5) for ordinary elliptic curves with an even embedding degree on $\mathbb{G}_2 \times \mathbb{G}_1$. Let $m_i = \min\{a_i, b_i\}$ where (a_i, b_i) is the parameter of the R-ate pairing on $E_i, i = 1, \ldots, 5$.

$$C_{E_2}(\text{R}-\text{ate}) \le \left(2\log_2 m_2 + \frac{2(\log_2 m_2)}{17} + 2\right)\mathcal{T}_{\mathtt{MO}}$$

$$\begin{aligned} C_{E_3}(\text{R}-\text{ate}) &\le (\log_2 b_3 + 2)\mathcal{T}_{\mathtt{MO}} \\ C_{E_4}(\text{R}-\text{ate}) &\le (\log_2 m_4 + 3)\mathcal{T}_{\mathtt{MO}} \\ C_{E_5}(\text{R}-\text{ate}) &\le (\log_2 m_5 + 2)\mathcal{T}_{\mathtt{MO}}. \end{aligned}$$

For odd embedding degree, we need to add the cost for the computation of the vertical line in the Miller operation. Thus, for E_1, we have

$$\mathcal{T}_{\mathtt{MD}'} = \mathcal{T}_{\mathtt{MD}} + 1M_k, \mathcal{T}_{\mathtt{MA}'} = \mathcal{T}_{\mathtt{MA}} + 1M_k.$$

Using (3), the computation cost for the R-ate pairing on E_1 with respect to each (a_1, b_1) is as follows:

$$\begin{aligned} C_{E_1}(\text{R}-\text{ate}) &= \mathcal{T}(\mathtt{M}(P, Q, b_1)) + \mathcal{T}_{G,A} + 1M_k \\ &\le (\log_2 b_1 + 1)\mathcal{T}_{\mathtt{MO}}. \end{aligned}$$

For hyperelliptic curve H_5 described in Section V, we analyze the computation cost for the R-ate pairing of the case $(a, b) = (5^{\frac{n+1}{2}} + 3, 5^{\frac{n+1}{2}} + 1)$.

To estimate the cost, we denote the computation cost for basic operations as follows:

- $\mathcal{T}_{A\text{-deg}} = 3M_1 + I$: cost for an addition of degenerate divisors;
- $\mathcal{T}_{D\text{-deg}} = 2M_1 + I$: cost for a doubling of a degenerate divisor;
- $\mathcal{T}_{A\text{-gen}} = 25M_1 + I$: cost for an addition of general divisors [5];
- $\mathcal{T}_{G,A\text{-gen}} = I + (28 + 3k)M_1 + 10M_k$: cost for a Miller addition in Algorithm 1 on general divisors [14];
- $\mathcal{T}_{\mathtt{MO},5} = 3M_1 + 2M_k$: cost for a Miller operation with base 5 using Lemma 1 in [6].

From (13), we obtain the following cost for the R-ate on H_5:

$$\begin{aligned} C_{H_5}(\text{R-ate}) = \frac{n+1}{2}\mathcal{T}_{\mathtt{MO},5} &+ \mathcal{T}_{A\text{-deg}} + \mathcal{T}_{D\text{-deg}} \\ &+ \mathcal{T}_{A\text{-gen}} + \mathcal{T}_{G,A\text{-gen}} + 4M_k + I_k. \end{aligned} \quad (14)$$

To have the unique value of the R-ate pairing, we need to compute a final powering with

$$L = (q^5 - 1)/N^{\pm} = (5^n - 1)(5^{2n} + 3 \cdot 5^n \mp 5^{(n+1)/2}(5^n + 1)).$$

This computation can be obtained by seven multiplications and one inversion in $\mathbb{F}_{q^k}$. Therefore, the total cost for the R-ate pairing with the final powering, denoted by $\hat{C}$, satisfies

$$\begin{aligned} &\hat{C}_{H_5}(\text{R-ate}) \\ &= \frac{n+1}{2}\mathcal{T}_{\mathtt{MO},5} + \mathcal{T}_{A\text{-deg}} + \mathcal{T}_{D\text{-deg}} + \mathcal{T}_{A\text{-gen}} + \mathcal{T}_{G,A\text{-gen}} \\ &\quad + 11M_k + 2I_k \\ &= \frac{n+1}{2}\mathcal{T}_{\mathtt{MO},5} + 113M_1 + 41M_k \le \left(\frac{n+1}{2} + 25\right)\mathcal{T}_{\mathtt{MO},5} \end{aligned}$$

because $M_k \ge 5M_1$.

The Ate pairing costs

$$C_{H_5}(\text{Ate}) = n\mathcal{T}_{\mathtt{MO},5}$$

and $C_{H_5}(\text{Ate}) > C_{H_5}(\text{R-ate})$ when $n > \frac{n+1}{2} + 25$, i.e., $n > 51$. From the security issue, n should be larger than 88 and thus we

TABLE II
COMPLEXITIES OF EXAMPLES

Curve	pairing	Parameters for pairing	Miller-length for total cost
E_1 (k=7)	Ate_i	$T_2 = 10133938509526225$	$(1/3)\log_2 r$
	R-ate	$(1, 100667465)$	$(1/6)\log_2 r + 1$
E_2 (k=10)	Ate_i	$T_6 = 1088496298065542309$	$(3/8)\log_2 r$
	R-ate	$(1028669, 1028669^2)$	$(9/34)\log_2 r + 2$
E_3 (k=8)	Ate_i	$T_1 = -9z^3 - 3z^2 - 2z - 1$	$(3/4)\log_2 r$
	R-ate	$(1, 3z + 1)$	$(1/4)\log_2 r + 2$
E_4 (k=10)	Ate_i	$T_2 = 5z^2$	$(1/2)\log_2 r$
	R-ate	$(5z + 3, 5z + 1)$	$(1/4)\log_2 r + 3$
E_5 (k=12)	Ate_i	$T_1 = 6z^2$	$(1/2)\log_2 r$
	R-ate	$(6z + 3, 6z + 2)$	$(1/4)\log_2 r + 2$
$H_5^{\pm}$ $(k = 5)$	Ate	5^n	n
	R-ate	$(5^{\frac{(n+1)}{2}} + 3, 5^{\frac{(n+1)}{2}} + 1)$	$\frac{(n+1)}{2} + 25$

TABLE III
THE MILLER LENGTH AND TIMING COST FOR Ate_i AND R-ATE ON EACH EXAMPLE

Curve(k)	E_1	E_2	E_3	E_4	E_5	H_5
Miller-loop length for Ate_i	54	60	123	117	128	89
Miller-loop length for R-ate	28	44	43	62	68	70
Timing for Ate_i (Magma)	0.085	0.048	0.035	0.156	0.202	0.067
Timing for R-ate (Magma)	0.038	0.034	0.011	0.083	0.099	0.055

can conclude that the R-ate is faster than the Ate pairing on H_5. In addition, since

$$\frac{C_{H_5}(\text{Ate}) - \hat{C}_{H_5}(\text{R}-\text{ate})}{C_{H_5}(\text{Ate})} = \frac{1}{2} - \frac{51}{2n}$$

as the security level n becomes higher, the cost for the R-ate pairing approaches half of the cost of the Ate pairing. We implemented the R-ate pairing and the Ate pairing for $n = 89$ at 160-bit security level. In this case, the R-ate pairing improves the overall timings by about 19% compared to the Ate pairing.

Table II summarizes the total cost in terms of the length of Miller loop for the R-ate pairing on the curves we discussed.

Table III shows the length of Miller's algorithm for pairing computation on each curve and the timing costs for Ate_i and R-ate. We tested two pairings using Magma [4] on a machine with Xeon 3.0 GHz and all the timing results are in seconds. Miller's algorithm described in Algorithm 1 and the R-ate pairing described in Algorithm 2 are coded using divisor operations on elliptic curves and hyperelliptic curves built in Magma. We implement pairings with the parameters for E_1 through E_5 given in Section IV-B and pairings on $y^2 = x^5 - x + 1/\mathbb{F}_{5^{89}}$ for H_5. The implementation results in Table III support our theoretical complexity analysis. The R-ate pairings on E_1, E_4, E_5 are 50% faster, the E_2 case is 29% faster, the E_3 case is 69% faster than the Ate_i pairing, and the H_5 case is 19% faster than the Ate pairing.

ACKNOWLEDGMENT

E. Lee and H.-S. Lee wish to thank the Korea Institute for Advanced Study.

REFERENCES

[1] P. S. L. M. Barreto, H. Y. Kim, B. Lynn, and M. Scott, "Efficient algorithms for pairing-based cryptosystems," in *Advances in Cryptology—CRYPTO 2002 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2002, vol. 2442, pp. 354–368.

[2] P. S. L. M. Barreto, S. Galbraith, C. O. hEigeartaigh, and M. Scott, "Efficient pairing computation on supersingular Abelian varieties," *Des., Codes Cryptogr.*, vol. 42, no. 3, pp. 239–271, 2007.

[3] P. S. L. M. Barreto and M. Naehrig, "Pairing-friendly elliptic curves of prime order," in *Selected Areas in Cryptography—SAC 2005 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2006, vol. 2897, pp. 319–331.

[4] W. Bosma, J. Cannon, and C. Playoust, "The Magma algebra system. I. The user language," *J. Symbolic Comput.*, vol. 24, no. 3–4, pp. 235–265, 1997.

[5] Y. Choie and E. Lee, "Implementation of Tate pairing on hyperelliptic curves of genus 2," in *Information Security and Cryptology—ICISC 2003 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2004, vol. 2971, pp. 97–111.

[6] I. Duursma and H.-S. Lee, "Tate pairing implementation for hyperelliptic curves $y^2 = x^p - x + d$," in *Advances in Cryptography—AsiaCrypt 2003 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2003, vol. 2894, pp. 111–123.

[7] D. Freeman, "Constructing pairing-friendly elliptic curves with embedding degree 10," in *Algorithmic Number Theory Symp.—ANTS-VII (Lecture Notes in Computer Science)*. Berlin: Germany, 2006, vol. 4076, pp. 452–465.

[8] D. Freeman, M. Scott, and E. Teske, "A Taxonomy of Pairing-Friendly Elliptic Curves," [Online]. Available: http://eprint.iacr.org/2006/372

[9] G. Frey and H.-G. Rück, "A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves," *Math. Comput.*, vol. 62, no. 206, pp. 865–874, 1994.

[10] S. Galbraith, "Supersingular curves in cryptography," in *Advances in Cryptology—AsiaCrypt 2001 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2002, vol. 2248, pp. 495–513.

[11] S. Galbraith, K. Harrison, and D. Soldera, "Implementing the Tate pairing," in *Algorithmic Number Theory Symposium—ANTS-V (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2002, vol. 2369, pp. 324–337.

[12] S. Galbraith, F. Hess, and F. Vercauteren, "Hyperelliptic pairings," in *Pairing-Based Cryptography—Pairing 2007 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2007, vol. 4575, pp. 108–131.

[13] S. Galbraith, J. Pujolàs, C. Ritzenthaler, and B. Smith, "Distortion maps for genus two curves," Preprint, arxiv math_NT/0611471.

[14] R. Granger, F. Hess, R. Oyono, N. Theriault, and F. Vercauteren, "Ate pairing on hyperelliptic curves," in *Advances in Cryptology—EuroCrypt 2007 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2007, vol. 4515, pp. 430–447.

[15] F. Hess, N. P. Smart, and F. Vercauteren, "The Eta pairing revisited," *IEEE Trans. Inf. Theory*, vol. 52, no. 10, pp. 4595–4602, Oct. 2006.

[16] N. Koblitz, *Algebraic Aspects of Cryptography*. New York: Springer-Verlag, 1998.

[17] N. Koblitz and A. Menezes, "Pairing-based cryptography at high security levels," in *Cryptography and Coding (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2005, vol. 3796, pp. 3–36.

[18] S. Kwon, "Efficient Tate pairing computation for elliptic curves over binary fields," in *Information Security and Privacy—ACISP 2005 (Lecture Notes in Computer Science)*. Berlin, Germany: Sspringer-Verlag, 2005, vol. 3574, pp. 134–145.

[19] S. Matsuda, N. Kanayama, F. Hess, and E. Okamoto, "Optimised versions of the Ate and twisted Ate pairings," in *Cryptography and Coding (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2007, vol. 4887, pp. 302–312.

[20] V. Miller, "The Weil pairing and its efficient calculation," *J. Cryptogr.*, vol. 17, no. 4, pp. 235–261, 2004.

[21] A. Murphy and N. Fitzpatrick, Elliptic curves for pairing applications [Online]. Available: http://eprint.iacr.org/2005/302

[22] H. Stictenoth, *Algebraic Function Fields and Codes*. Berlin, Germany: Springer-Verlag, 1993.

[23] E. Verheul, "Evidence that XTR is more secure than supersingular elliptic curve cryptosystems," in *Advances in Cryptology—EuroCrypt 2001 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2001, vol. 2045, pp. 195–210.

[24] C. Xing, "On supersingular Abelian varieties of dimension two over finite fields," *Finite Fields Their Applic.*, vol. 2, no. 4, pp. 407–421, 1996.

[25] C. Zhao, F. Zhang, and J. Huang, "A note on the Ate pairing," *Int. J. Inf. Security Arch.*, vol. 7, no. 6, pp. 379–382, 2008.

Eunjeong Lee received the B.S., M.S., and Ph.D. degrees in mathematics from Pohang University of Science and Technology, Pohang, Korea, in 1993, 1995, and 2004, respectively.

She has been a Visiting Scholar at the Department of Mathematics of North Carolina State University, Raleigh, NC, since July 2008. Her research interests include efficient computation for cryptosystems using elliptic and hyperelliptic curves.

Hyang-Sook Lee received the B.S. and M.S. degrees in mathematics from Ewha Womans University, Seoul, Korea, in 1986 AND 1988, respectively. She received the Ph.D. degree in mathematics from Northwestern University, Evanston, IL, in 1994.

She has been a Professor in the Department of Mathematics of Ewha Womans University, Seoul, Korea since 1995. Her research interests include pairing computation on pairing based cryptography, elliptic, and hyperelliptic curves.

Cheol-Min Park received the B.S. degree in mathematics education, and the M.S. and Ph.D. degrees in mathematics from Seoul National University, Seoul, Korea, in 1999, 2001, 2006 respectively.

He has been a Postdoctoral Scholar at the Institute of Mathematical Sciences of Ewha Womans University since 2007. His research interests include elliptic and hyperelliptic curves.