Efficient and Generalized Pairing Computation on Abelian Varieties

Eunjeong Lee[1], Hyang-Sook Lee[2], and Cheol-Min Park[2]

[1]School of Computational Sciences, Korea Institute for Advanced Study,
Hoegiro 87, Dongdaemun-gu, Seoul 130-722, Korea
ejlee@kias.re.kr
[2]Department of Mathematics, Ewha Womans University,
11-1 Daehyun-dong, Seodaemun-gu, Seoul 120-750, Korea
{hsl,mpcm}@ewha.ac.kr

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 also improves efficiency of the pairing computation. 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 from 29% to 69% savings 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.

Key words: pairing, elliptic curves, hyperelliptic curves, pairing based cryptography, Tate pairing.

1 Introduction

The development of efficient algorithms for the pairing computation has been a very important issue in the pairing based cryptosystems. The pairing computation on abelian varieties is generally based on the Miller's algorithm for rational functions from scalar multiplications of divisors. Many algorithms for efficient computation of the pairing have been developed by reducing the iteration loops in Miller's algorithm. Barreto et al. [1] and Galbraith et al. [11] proposed the 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 the 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 the hyperelliptic curves by Granger et al. [12]. Matsuda et al. [21] showed that the Ate pairing is always at least as fast as the Tate pairing by providing the 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 the *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 computation of pairings. 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 2 or 3 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.

This paper is organized as follows. Section 2 includes the basic mathematical backgrounds such as the Tate, Ate and Ate_i pairings and the Miller's algorithm. In Section 3 we define the R-ate pairing and also investigate the criterion for the R-ate pairing to be computed efficiently. Section 4 provides the examples of the R-ate pairings on supersingular elliptic curves over a finite field in characteristic 3 and ordinary elliptic curves. Section 5 gives the examples of the R-ate pairings over supersingular hyperelliptic curves of genus two. Section 6 includes the complexity analysis of the R-ate pairings over (hyper)elliptic curves provided in Section 4 and 5.

2 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 the Miller's algorithm to compute the pairings. For a good survey of pairings, refer to [13].

2.1 The Tate, Ate and Ate_i pairings

Let $\mathbb{F}_q$ be a finite field with q elements, and C be a non-singular 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.

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 divisor classes of order dividing r. The *Tate pairing* is a map

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

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 $r \mid N \mid q^k - 1$ [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 [12, 15] and the Ate_i pairing [25] on divisors $D_1 \in \mathbb{G}_1, D_2 \in \mathbb{G}_2$ are defined as following:

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

The $\mathrm{Ate}(\mathrm{Ate}_i)$ 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 [12, 15]. For supersingular (hyper)elliptic curves, there exist a *distortion map* ψ such that $e(D, \psi(E)) \neq 1$ for two divisors $D, E \in \mathbb{G}_1$ with prime order [14, 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.

2.2 Miller's algorithm

The pairings over (hyper)elliptic curves are computed using the algorithm proposed by Miller [19]. The main part of the 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 $f_{n,D}(E)$.

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

Algorithm 1 Miller's algorithm

`procedure` $\mathtt{M}(D, E, \ell)$
INPUT: $D, E \in J_C,\ \ell \in \mathbb{Z},\ \ell = \sum_{i=0}^{\lfloor \log_2 \ell \rfloor - 1} \ell_i 2^i \quad (\ell_i = 0, 1)$
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: $\quad \diamond$ *Miller-doubling step* (`MD`)
5: $\quad\quad f \leftarrow f^2 \cdot G_{T,T}(E)$
6: $\quad\quad T \leftarrow 2T$
7: $\quad$ **if** $\ell_i = 1$ **then**
8: $\quad\quad \diamond$ *Miller-addition step* (`MA`)
9: $\quad\quad\quad f \leftarrow f \cdot G_{T,D}(E)$
10: $\quad\quad\quad T \leftarrow T + D$
11: $\quad$ **end if**
12: **end for**
13: **return** f, T

In the case of elliptic curves, $G_{iD,jD}$ 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 `M` returns the value $f_{\ell,D}(E)$ and ℓD. We call the steps in **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, the steps 4 through 10 are for Miller-operation and the Miller-length is $\lfloor \log_2 \ell \rfloor$. We also divide Miller-operation into two parts: Miller-doubling(`MD`), Miller-addition(`MA`).

3 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.

3.1 Construction of the R-ate pairing

We use the same notations 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 3.1. *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 non-degenerate, 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 non-degeneracy and bilinearity.

Theorem 3.2. *Let C be a non-singular curve over $\mathbb{F}_q$ and r a large prime which divide $N = \#J_C(\mathbb{F}_q)(or \#E(\mathbb{F}_q))$. Let D and E be divisors on C defined over $\mathbb{F}_q$ with an order dividing r. Let A and B be integers such that*
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 $M = lcm(M_1, M_2)$, $d_1 = M/M_1, d_2 = M/M_2$ 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

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

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,

$$f_{A,D}(E)^M = f_{B,D}(E)^{aM} \cdot R_{A,B}(D, E)^M.$$

$$e(D,E)^{d_1L_1} = e(D,E)^{ad_2L_2} \cdot R_{A,B}(D,E)^M.$$

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 Eq. (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 3.3. For simplicity, we represent $R(D,E)$ instead of $R_{A,B}(D,E)$ if A and B are clear from the context.

Corollary 3.3. *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*
- $T_i \equiv q^i \mod r$ for $0 < i < k$ and h_i be the smallest integer such that $T_i^{h_i} \equiv 1 \mod r$.
- $N_i = gcd(T_i^{h_i} - 1, q^k - 1)$ and $T_i^{h_i} - 1 = L_i N_i$.
- $c_i = \sum_{j=0}^{h_i-1} T_i^{h_i-1-j}(q^i)^j \mod N_i$ 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 $(A,B) = (q^i, r)$,

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

$$L = iq^{i-1}\frac{q^k-1}{r} - kq^{k-1}a, \quad M = kq^{k-1} \cdot \frac{q^k-1}{r}.$$

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

$$R(D_2,D_1) = f_{a,D_2}(D_1)^q \cdot f_{b,D_2}(D_1) \cdot G_{aTD_2,bD_2}(D_1)$$

$$L = M_1 - aL_1, \quad M = c_1M_1.$$

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

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

$$L = d_iL_i - ad_jL_j, \ M = lcm(c_iM_i, c_jM_j) = d_ic_iM_i = d_jc_jM_j.$$

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

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

$$L = d_0 - ad_jL_j, \ M = lcm(\frac{q^k-1}{r}, c_jM_j) = d_0\frac{q^k-1}{r} = d_jc_jM_j.$$

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

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

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

$$f_{T_i,D_2}(D_1) = f^a_{T_j,D_2}(D_1) \cdot f_{a,T_jD_2}(D_1) \cdot f_{b,D_2}(D_1) \cdot G_{aT_jD_2,bD_2}(D_1).$$

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

$$e(D_2, D_1)^{L_l} = f^{c_lM_l}_{T_l,D_2}(D_1)$$

for $l = i, j$,

$$e(D_2, D_1)^{d_iL_i - ad_jL_j} = R(D_2, D_1)^M$$

where $M = lcm(c_iM_i, c_jM_j)$, $M = d_ic_iM_i = d_jc_jM_j$.

□

Remark 3.4. *1. The R-ate pairing in the case 1 of Corollary 3.3 is the* Ate_i *pairing [25].*

2. For supersingular elliptic curves and superspecial hyperelliptic curves, Corollary 3.3 can be also appllied to $\mathbb{G}_1 \times \mathbb{G}_2$ *by [12, 15].*

Algorithm 2 describes the computation of the R-ate pairing with respect to a and b which are explained in Corollary 3.3. 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 the 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 provide the efficient R-ate pairing.

Algorithm 2 R-ate pairing

`procedure R-ate`(P, Q, a, b)
INPUT: $P, Q \in C,\ a,\ b,\ j \in \mathbb{Z},\ m_1 = max\{a, b\},\ m_2 = min\{a, b\}$.
OUTPUT: $R(Q, P) = f_{a,Q}(P)^{q^j} \cdot f_{b,Q}(P) \cdot G_{aT_iQ,bQ}(P)$

1: $\diamond$ *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: $Q_1 \leftarrow \phi^j(aQ)$.
11: $f_3 \leftarrow f_2 \cdot G_{Q_1,bQ}(P)$.
12: **return** f_3

3.2 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 the pairings,

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

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

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

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

$\mathcal{T}(\mathtt{M}(D_1, D_2, \ell))$: 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 the Miller-addition (doubling) in Algorithm 1

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

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

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

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

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.

Thus, the costs for the elementary steps using affine coordinates in Full-Miller are as following:

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

Since the cost for the 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.

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

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

From Eq. (3) and Eq. (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

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

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

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

The parameters a, b for the R-ate pairing satisfying Eq. (6) can be obtained by looking into the combinations for (A, B) in Corollary 3.3. 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 4.2(Table 1) have

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

$$\gamma(E_4) = \frac{(1/4)\log_2 r + 3}{(1/2)\log_2 r} \sim \frac{1}{2} \qquad \gamma(E_5) = \frac{(1/4)\log_2 r + 2}{(1/2)\log_2 r} \sim \frac{1}{2}$$

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 the examples (Table 3 in Section 6).

4 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.

4.1 Supersingular Elliptic curves

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

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

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 3.3, 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 $L' \equiv L s c_1^{-1} \mod N$, 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].

4.2 Ordinary Elliptic curves

In this section, 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, 20] cannot reach this low bound. We show that the R-ate pairing gives this low bound on such curves.

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

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)

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

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

and

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

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

Example 4.1.

Let E_1 be the curve over $\mathbb{F}_p$ in [20] with

$k = 7$
$p = 152683916815195328299425822768509148050335333587091954124192528892961908503610 31$
$N = 152683916815195328299425822768509148050335333587091954124192528892961909510284 96$
$r = 1040722131042824291503998495039735508885676564761$(160 bits)
$\mathsf{T} = T_2 = 10133938509526225$(54 bits).

Since $r = T_1 + b$ for $(A, B) = (r, T_1)$ which is the case 4 of Corollary 3.3, we have the efficient R-ate pairing with respect to a, b as following:

$$R(P_2, P_1) = f_{b,P_2}(P_1) \cdot G_{T_1 P_2, bP_2}(P_1),$$

where

$$a = 1, \qquad b = 100667465(27 \text{ bits})$$
$$L = d_0 - d_1 L_1, \quad M = lcm(\tfrac{q^k-1}{r}, c_1 M_1) = d_0 \tfrac{q^k-1}{r} = d_1 c_1 M_1.$$

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 $L' \equiv L d_0^{-1} \mod r$.

Example 4.2.

Let E_2 be the curve over $\mathbb{F}_p$ in [20] with

$k = 10$
$p = 39612061054789106390969804068289066415604050183196343018562683865206469243339163509 1$
$N = 39612061054789106390969804068289066415604050183196343018562683865315318873145717740 0$
$r = 125373224226869067404938302067196601969906495432 1$(160 bits)
$\mathsf{T} = T_6 = 1088496298065542309$(60 bits).

Since $T_9 = a \cdot T_2 + b$ for $(A, B) = (T_9, T_2)$ which is the case 3 of Corollary 3.3, we have the efficient R-ate pairing with respect to a, b as following:

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

where

$$\begin{aligned} &a = 1028669\text{(20 bits)}, \quad b = 1058159911561 = a^2 \\ &L = d_9L_9 - ad_2L_2, \qquad M = lcm(c_9M_9, c_2M_2) = d_9c_9M_9 = d_2c_2M_2 = d_2c_2\tfrac{q^k-1}{N_2}. \end{aligned}$$

Note that the low bound, $r^{1/\phi(k)} \sim 2^{40}$, is comparable to b in bit size. Let $N_2 = rs$. Since $(d_2c_2, r) = 1$, 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 $L' \equiv Ls(d_2c_2)^{-1} \mod r$.

Example 4.3.

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 the case 3 of Corollary 3.3, we have the efficient R-ate pairing with respect to a, b as following:

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

where

$$\begin{aligned} &a = 1, \qquad\qquad b = 3z + 1 \\ &L = d_3L_3 - d_2L_2, \quad M = lcm(c_3M_3, c_2M_2) = d_3c_3M_3 = d_2c_2M_2 = d_2c_2\tfrac{q^k-1}{N_2}. \end{aligned}$$

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 $(d_2c_2, r) = 1$, 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 $L' \equiv Ls(d_2c_2)^{-1} \mod r$. In implementation (Section 6), we select $z = 1013235040279$ for the above parameters.

Remark 4.4. *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 4.5.

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 the case 3 of Corollary 3.3, we have the efficient R-ate pairing with respect to a, b as following:

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

where

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

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 $L' \equiv Ls(d_2c_2)^{-1} \mod r$. For $z = -164286669864814370$ suggested in [7], we implement the R-ate pairing on E_4 with these parameters (Section 6).

Example 4.6.

Let E_5 be the curve over $\mathbb{F}_p$ in [3] with

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

Since $T_{10} = a \cdot T_1 + b$ for $(A, B) = (T_{10}, T_1)$ which is the case 3 of Corollary 3.3, we have the efficient R-ate pairing with respect to a, b as following:

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

where

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

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 $L' \equiv Ls(d_1c_1)^{-1} \mod r$. For $z = 6917529027641089837$ suggested in [3], we implement the R-ate pairing on E_5 with these parameters (Section 6).

Remark 4.7. *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 1 summarizes the parameters for the Ate_i pairing and the R-ate pairing discussed in the above examples.

Table 1: Examples : ordinary elliptic curves

Curve	Parameters ($T_i \equiv q^i \mod r$)
E_1 [20]	$k = 7$
	$p = 152683916815195328299425822768509148050335333587091954124192528892961908503610 31$
	$r = 10407221310428242915039984950397355088856765647 61$
	$T_2 = 10133938509526225(54bits)$
	$r = T_1 + 100667465(27bits)$
E_2 [20]	$k = 10$
	$p = 396120610547891063909698040682890664156040501831963430185626838652064692433391635091$
	$r = 125373224226869067404938302067196601969906495432 1(160bits)$
	$T_6 = 1088496298065542309(60bits)$
	$T_9 = 1028669 \cdot T_2 + 1058159911561(40bits)$
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]	$k = 12$
	$p = 36z^4 + 36z^3 + 24z^2 + 6z + 1$
	$r = 36z^4 + 36z^3 + 18z^2 + 6z + 1$
	$T_1 = 6z^2$
	$T_{10} = (6z + 3)T_1 + 6z + 2$

5 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 [12]. In this section, we show that,

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 5.1. *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*

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

where

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

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

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

with the notations defined in Corollary 3.3.

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 Hess-Weil bound [10, 22, 24] and Eq. (9), we obtain

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

for some integer a_2'.

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

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

In the case of $q^2 > N$, $T_2 = q^2 - N = (-a)q + (-b) = (-a)T_1 + (-b)$. As the case 3 of Corollary 3.3, 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

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

From the definition of G in Eq. (1), G_{qaD_2,bD_2} is a rational function of the form $\frac{\lambda_{qaD_2,bD_2}}{v_{(qaD_2 \oplus bD_2)}}$ [19] 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 the similar proof as the case 3 in Corollary 3.3, we have the theorem. □

Remark 5.2. *The R-ate pairing with a, b defined in Theorem 5.1 can be computed using Algorithm 2. Since $|d| \leq 9$ where $\max\{a, b\} = \min\{a, b\} + d$, we have*

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

from Eq. (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 $\log_2 q$.

In the case of some curves like DL-curves, the cost for the Miller-operation using the special automorphisms ([2, 6, 12]) is very small compared to the cost for computing G in Eq. (7). Therefore, the additional cost such as $\mathcal{T}_{\mathtt{MA}} + 3M_k + \mathcal{T}_{G,A}$ in Eq. (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 [12], the R-ate pairing can be defined on $\mathbb{G}_1 \times \mathbb{G}_2$. We also analyze its complexity in Section 6, and it shows that the R-ate pairing is around 19% faster than the Ate pairing on this curve.

Example 5.3.

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

$$\begin{aligned} &k = 5 \\ &N^{\pm} = 5^{2n} + (3 \pm 5^{\frac{n+1}{2}})5^n + 1 \pm 5^{\frac{n+1}{2}} \\ &\text{distortion map } \psi(x, y) = (\rho - x, 2y), \quad \rho^2 - \rho + 2d = 0. \end{aligned}$$

By Theorem 5.1, the R-ate pairing on H_5 for $D, E \in J_H(\mathbb{F}_{5^n})[r]$ is as following.
In the case of N^- ($q^2 > N$), we have

$$R(D, \psi(E)) = f_{-a,D}(\psi(E))^q \cdot f_{-b,D}(\psi(E)) \cdot G_{-aT_1D,-bD}(\psi(E)), \tag{11}$$

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], Eq. (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,

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

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

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

where

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

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

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

The relation to the Tate pairing is the same as Theorem 5.1.

6 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 4.2 and the hyperelliptic curve H_5 in Section 5. 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 $\mathbb{G}_2 = \psi(\mathbb{G}_1)$, ψ is a distortion map as described in [14]. Algorithm 2 for the R-ate pairing consists of two parts: Miller's algorithms (Step 3 through Step 5) and the additional parts (Step 6 through Step 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 3.2, we observed the costs of the R-ate pairing as Eq. (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 $E_i, i = 1, \ldots, 5$.

$$\begin{aligned} C_{E_2}(\text{R-ate}) &\leq (2\log_2 m_2 + \tfrac{2(\log_2 m_2)}{17} + 2)\mathcal{T}_{\mathtt{MO}} \\ C_{E_3}(\text{R-ate}) &\leq (\log_2 b_3 + 2)\mathcal{T}_{\mathtt{MO}} \\ C_{E_4}(\text{R-ate}) &\leq (\log_2 m_4 + 3)\mathcal{T}_{\mathtt{MO}} \\ C_{E_5}(\text{R-ate}) &\leq (\log_2 m_5 + 2)\mathcal{T}_{\mathtt{MO}}. \end{aligned}$$

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 Eq. (3), the computation cost for the R-ate pairing on E_1 with respect to each (a_1, b_1) as following :

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

For the hyperelliptic curve H_5 described in Section 5, 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 following:

$\mathcal{T}_{A-deg} = 3M_1 + I$: cost for an addition of degenerate divisors

$\mathcal{T}_{D-deg} = 2M_1 + I$: cost for a doubling of a degenerate divisor

$\mathcal{T}_{A-gen} = 25M_1 + I$: cost for an addition of general divisors [5]

$\mathcal{T}_{G,A-gen} = I + (28 + 3k)M_1 + 10M_k$: cost for a Miller-addition in Algorithm 1 on general divisors [12]

$\mathcal{T}_{\mathtt{MO},5} = 3M_1 + 2M_k$: cost for a Miller-operation with base 5 using Lemma 1 in [6]

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

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

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

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

Table 2: 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	$(5^{\frac{(n+1)}{2}} + 3, 5^{\frac{(n+1)}{2}} + 1)$	$\frac{(n+1)}{2} + 25$

because $M_k \geq 5M_1$.

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

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

as the security level n becomes higher, the cost for the R-ate pairing approaches to a 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 2 summarizes the total cost in terms of the length of Miller-loop for the R-ate pairing on the curves we discussed.

Table 3 shows the length of Miller's algorithm for the 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 the pairings with the parameters for E_1 through E_5 given in Section 4.2 and the pairings on $y^2 = x^5 - x + 1$ / $\mathbb{F}_{5^{89}}$ for H_5. The implementation results in Table 3 support our theoretical complexity analysis. The R-ate pairings on E_1, E_4, E_5 are 50% faster, E_2 case is 29% faster, E_3 case is 69% faster than the Ate_i pairing and H_5 case is 19% faster than the Ate pairing.

Table 3: The Miller-length and timing cost for Ate_i and R-ate on each example

Curve(k)	$E_1(7)$	$E_2(10)$	$E_3(8)$	$E_4(10)$	$E_5(12)$	$H_5(5)$
length of Miller-loop for Ate_i	54	60	123	117	128	89
length of Miller-loop 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

Acknowledgment

The authors E. Lee and H.-S. Lee were supported by KOSEF, grant number R01-2005-000-10713-0, and the author C.-M. Park was supported by BK 21. The second author also expresses her gratitude to KIAS.

References

[1] P.S.L.M. Barreto, H.Y. Kim, B. Lynn and M. Scott. Efficient Algorithms for Pairing-Based Cryptosystems. *Advances in Cryptology - CRYPTO 2002*, LNCS Vol. 2442, Springer-Verlag, pp. 354-368, 2002.

[2] P.S.L.M. Barreto, S. Galbraith, C. ÓhEigeartaigh and M. Scott. Efficient Pairing Computation on Supersingular Abelian Varieties. *Design, Codes and Cryptography*, Vol. 42, No.3, pp.239-271, 2007.

[3] P.S.L.M. Barreto and M. Naehrig. Pairing-friendly elliptic curves of prime order. *Selected Areas in Cryptography - SAC 2005*, LNCS Vol. 2897, Springer-Verlag, pp. 319-331, 2006.

[4] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput*, 24(3-4):235-265, 1997.

[5] Y. Choie and E. Lee. Implementation of Tate pairing on hyperelliptic curves of genus 2. *Information Security and Cryptology - ICISC 2003*, LNCS Vol. 2971, Springer-Verlag, pp. 97-111, 2004.

[6] I. Duursma and H. Lee. Tate pairing implementation for hyperelliptic curves $y^2 = x^p - x + d$. *Advances in Cryptography - AsiaCrypt 2003*, LNCS Vol. 2894, Springer-Verlag, pp. 111-123, 2003.

[7] D. Freeman. Constructing Pairing-Friendly Elliptic Curves with Embedding Degree 10. *Algorithmic Number Theory Symposium - ANTS-VII*, LNCS Vol. 4076, Springer-Verlag, pp. 452-465, 2006.

[8] D. Freeman, M. Scott, E. Teske. A taxonomy of pairing-friendly elliptic curves. Preprint 2006, Available at 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. *Mathematics of Computation*, Vol. 62, No. 206, pp. 865-874, 1994.

[10] S. Galbraith. Supersingular curves in cryptography. *Advances in Cryptology - AsiaCrypt 2001*, LNCS Vol.2248, Springer-Verlag, pp. 495-513, 2002.

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

[12] R. Granger, F. Hess, R. Oyono, N. Theriault and F. Vercauteren. Ate Pairing on Hyperelliptic Curves. *Advances in Cryptology - EuroCrypt 2007*, Springer-Verlag LNCS 4515, pp. 430-447, 2007.

[13] S.D. Galbraith, F. Hess, and F. Vercauteren. Hyperelliptic Pairings. *Pairing-Based Cryptography - Pairing 2007*, Springer-Verlag LNCS 4575, pp. 108-131, 2007.

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

[15] F. Hess, N.P. Smart and F. Vercauteren. The Eta Pairing Revisited. *IEEE Trans. Information Theory*, Vol. 52, pp. 4595-4602 2006.

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

[17] N. Koblitz and A. Menezes. Pairing-based cryptography at high security levels. *Cryptography and Coding*, LNCS Vol. 3796, Springer-Verlag, pp. 3-36, 2005.

[18] S. Kwon. Efficient Tate Pairing Computation for Elliptic Curves over Binary Fields. *Information Security and Privacy - ACISP 2005*, LNCS Vol. 3574, Springer-Verlag, pp. 134-145, 2005.

[19] V. Miller. The Weil pairing and its efficient calculation. *J. Cryptology*, Vol.17, No.4, pp. 235-261, 2004.

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

[21] S. Matsuda, N. Kanayama, F. Hess and E. Okamoto. Optimised versions of the Ate and twisted Ate pairings. *To appear at Eleventh IMA International Conference on Cryptography and Coding*, Available at http://eprint.iacr.org/2007/013.pdf

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

[23] E. Verheul. Evidence that XTR Is More Secure than Supersingular Elliptic Curve Cryptosystems. *Advances in Cryptology - EuroCrypt 2001*, LNCS Vol.2045, Springer-Verlag, pp.195-210, 2001.

[24] C. Xing. On supersingular abelian varieties of dimension two over finite fields. *Finite fields and their application*, Vol.2, No.4, pp.407-421, 1996.

[25] C. Zhao, F. Zhang and J. Huang. A Note on the Ate Pairing. Preprint, 2007. Available at http://eprint.iacr.org/2007/247.