Faster Computation of Self-pairings

Chang-An Zhao, Fangguo Zhang and Dongqing Xie

[1] School of Computer Science and Educational Software,
Guangzhou University, Guangzhou 510006, P.R.China
[2] Guangdong Key Laboratory of Information Security Technology,
Sun Yat-Sen University, Guangzhou 510275, P.R.China
changanzhao@gzhu.edu.cn
isszhfg@mail.sysu.edu.cn

Abstract. Self-pairings have found interesting applications in cryptographic schemes, such as ZSS short signatures and so on. In this paper, we present a novel method for constructing a self-pairing on supersingular elliptic curves with even embedding degrees, which we call the Ateil pairing. This pairing improves the efficiency of the self-pairing computation on supersingular curves over finite fields with large characteristic. On the basis of the η_T pairing, we propose a generalization of the Ateil pairing, which we call the Ateil$_i$ pairing. The optimal Ateil$_i$ pairing which has the shortest Miller loop length is faster than previously known self-pairing on supersingular elliptic curves over finite fields with small characteristic. We also propose a new self-pairing based on the Weil pairing which is faster than the previously known self-pairing on ordinary elliptic curves with embedding degree *one*.

Keywords: Tate pairing, Weil pairing, Self pairing, Pairing based cryptography.

1 Introduction

Since pairings on elliptic curves have found many cryptographic applications [23], it leads to fast developments of algorithmic foundations of pairings. Two extensive surveys of pairing computations can be found in [2] and [9]. More recently, a multitude of efficient techniques which speed up pairing computations have been proposed. We categorize them into the following cases:

– Shortening the loop length in Miller's algorithm. In the case of the Tate pairing, we refer to [7, **?**,**?**,16, 31, 15, 32, 25, 12]. In the case of the Weil pairing, we refer to [33, 12, 30].

- Speeding up the basic doubling and addition steps in Miller's algorithm [1, 6].
- Speeding up the final exponentiation in the computation of the Tate pairing or its variants [24].

All of the above improvements are very practical and lead to fast implementations. Pairings which feature specific properties are often required in cryptographic applications. In particular, the self-pairing $e(P, P)$ has been used in a wide range of cryptographic applications including, but not limited to, short signatures [28, 27], ID-based Chameleon hashing schemes [29], on-line/off-line signature scheme [27]. To the best of our knowledge, there is no other study for computing self-pairings except [21]. It is known that $e(P, P)$ will be equal to *one* if we directly compute the Tate or Weil pairings. Thus the latter P should be mapped to another point which is independent with P for keeping non-degeneracy in cryptographic protocols and schemes. Note that the distortion map exists only on supersingular curves and ordinary curves with embedding degree *one* [18]. Therefore, we will mainly consider the self-pairing computation in the two cases.

In this paper, we present a new self-pairing on supersingular elliptic curves with even embedding degrees, which we call the Ateil pairing. There are two points to call this name. Firstly, it is like the Tate pairing, but faster than the self-pairing based on the Tate pairing (hence we miss the "T"). Secondly, it comes from the Weil pairing (hence we add"eil" in the end). This new pairing only has *one* Miller loop despite it is devised by the Weil pairing. We show that it is the fastest self-pairing on supersingular elliptic curves over finite fields with large characteristics. Based on the η_T pairing, we present a natural generalization of the Ateil pairing, which we call the Ateil_i pairing. The optimal Ateil_i pairing with the shortest Miller loop is faster than the self-pairing based on the η_T pairing. In the case of ordinary elliptic curves with embedding degree *one*, we apply the denominator elimination technique in the computation of the self-pairing based on the Weil pairing. Note that this technique does not exist when computing the self-pairing based on the Tate pairing on the same curves. It is shown that our new self-pairings achieve better performance than the previously known self-pairings at any security level.

The remainder of this paper is structured as follows. In Section 2, we provide some background and notation used through this study. In Section 3, we provide a method for constructing self-pairings on supersingular elliptic curves with even embedding degrees. In Section 4, we present a new self-pairing on ordinary elliptic curves with embedding degree *one*. In such, we provide an analysis of the computational complexity of the presented self-pairing and give a comparison to the complexity of different self-pairings. We draw our conclusion in Section 5.

2 Mathematical Preliminaries

2.1 Tate Pairing

Let $\mathbb{F}_q$ be a finite field with $q = p^m$ elements where p is a prime, and E be an elliptic curve defined over $\mathbb{F}_q$. Consider a large prime r such that $r | \#E(\mathbb{F}_q)$, where $\#E(\mathbb{F}_q)$ is denoted as the order of the rational points group $E(\mathbb{F}_q)$. Let k be the embedding degree with respect to r, i.e., the smallest positive integer such that $r | q^k - 1$. Let $P \in E[r]$ and $R \in E(\mathbb{F}_{q^k})$. For each integer i and point P, let $f_{i,P}$ be a rational function on E such that $(f_{i,P}) = i(P) - (iP) - (i-1)(\mathcal{O})$. Assume that D is a divisor which is equivalent to $(R) - (\mathcal{O})$ with its support disjoint from $(f_{r,P})$. Denote μ_r by the algebraic group of r-th roots of unity in $\mathbb{F}_{q^k}$. The reduced Tate pairing [8] is a bilinear map

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

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

Note that the evaluation of $f_{r,P}$ at the divisor D can be computed by Miller's algorithm in polynomial time [19, 20].

2.2 Weil Pairing

Using the same notation as previous, one may make a few slight modifications and then define the Weil pairing. Let k be the minimal positive integer such that $E[r] \subset E(\mathbb{F}_{q^k})$. Suppose that $P,\ Q \in E[r]$ and $P \neq Q$. Let D_P and D_Q be two divisors which are equivalent to $(P) - (\mathcal{O})$ and $(Q) - (\mathcal{O})$, respectively. Assume that $f_{r,P}$ and $f_{r,Q}$ are two rational functions on E satisfying $(f_{r,P}) = rD_P$ and $(f_{r,Q}) = rD_Q$, respectively. The Weil pairing [20] is a bilinear map

$$\hat{e} : E[r] \times E[r] \to \mu_r,$$

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

In general, computing the Weil pairing is always slower than computing the reduced Tate pairing since it involves two Miller loops [9]. However, it has been shown that the variant of the Weil pairing is faster than that of the Tate pairing on certain pairing-friendly curves [30]. This results also indicate that the special structure of the Weil pairing is useful for pairing computations. In the following, we will take full advantages of the symmetry of the structure of the Weil pairing and then present new self-pairings with great efficiency.

3 The Ateil Pairing Approach

In practical implementations, the self-pairing $e(P, P)$ can be designed by $Type$ 1 pairings [11], i.e., it can be constructed on supersingular elliptic curves with even embedding degrees. For interests, we cite all cases as Table 1. Note that the computation of the pairings on E_1 and E_2 has been discussed [18]. In the mean time, The η_T pairing can be defined on E_3 and E_4 [3]. Since the distortion map ϕ [26] is an isogeny, we list its dual isogeny ϕ^{-1} for convenience.

In this section, we will explore the computation of the self-pairings on the curves given in Table 1. Our general understanding of the construction of the self-pairings comes mostly from the following theorem.

Theorem 1. *Let E be the supersingular curves over the ground field $\mathbb{F}_q$ given in Table 1. Let r be a large prime dividing the order of $E(\mathbb{F}_q)$. The embedding degree with respect to r is equal to k. Let π_q be the Frobenius endomorphism and take $P \in \mathbb{G}_1 = Ker(\pi_q - [1]) \cap E[r]$. The self-pairing based on the Weil pairing can be given by*

$$e_s(P,P) \triangleq \hat{e}(P,\phi(P))^{2(q^{k/2}-1)} = f_{r,P}(\phi(P))^{4(q^{k/2}-1)}.$$

Proof. It follows from the definition of the Weil pairing that

$$e_s(P,P) \triangleq \hat{e}(P,\phi(P))^{2(q^{k/2}-1)} = (\frac{f_{r,P}(\phi(P))}{f_{r,\phi(P)}(P)})^{2(q^{k/2}-1)}.$$

Since the distortion map in Table 1 is an automorphism, we have

$$f_{r,\phi(P)}(P)^{(q^{k/2}-1)} = f_{r,P}(\phi^{-1}(P))^{(q^{k/2}-1)},$$

Table 1. Popular pairing-friendly curves with distortion maps

No.	**Elliptic curve data**	**Distortion map**	k
1	$E_1 : y^2 = x^3 - 3x$ over $\mathbb{F}_p$, where $p \equiv 3 \pmod 4$. $\#E(\mathbb{F}_p) = p + 1$	$\phi : \quad (x, y) \to (-x, iy)$, $\phi^{-1} : (x, y) \to (-x, -iy)$, where $i^2 + 1 = 0$.	2
2	$E_2 : y^2 = x^3 - 1$ over $\mathbb{F}_p$, where $p \equiv 5 \pmod 6$ $\#E(\mathbb{F}_p) = p + 1$	$\phi : \quad (x, y) \to (\beta x, y)$, $\phi^{-1} : (x, y) \to (\beta^2 x, y)$, where $\beta^2 + \beta + 1 = 0$.	2
3	$E_3 : y^2 + y = x^3 + x + b$ over $\mathbb{F}_{2^l}$, where $b = 0$ or 1. $\#E_5(\mathbb{F}_{2^l}) = 2^l \pm 2^{(l+1)/2} + 1$ (l odd)	$\phi : \quad (x, y) \to (x + s^2, y + sx + t)$, $\phi^{-1} : (x, y) \to (x + s^2, y + sx + t + 1)$, where $s \in \mathbb{F}_{2^{2l}}$ and $t \in \mathbb{F}_{2^{4l}}$ satisfy $s^2 + s + 1 = 0$ and $t^2 + t + s = 0$.	4
4	$E_4 : y^2 + y = x^3 - x + b$ over $\mathbb{F}_{3^l}$, where $b = 1$ or -1. $\#E_6(\mathbb{F}_{3^l}) = 3^l \pm 3^{(l+1)/2} + 1$ (l odd)	$\phi : \quad (x, y) \to (\alpha - x, iy)$, $\phi^{-1} : (x, y) \to (\alpha - x, -iy)$, where $i \in \mathbb{F}_{3^{2l}}$ and $\alpha \in \mathbb{F}_{3^{3l}}$ satisfy $i^2 = -1$ and $\alpha^3 - \alpha - b = 0$.	6

which has been discussed in Proposition 2 of the paper [21]. Now it suffices to demonstrate that

$$(\frac{1}{f_{r,P}(\phi^{-1}(P))})^{(q^{k/2}-1)} = f_{r,P}(\phi(P))^{(q^{k/2}-1)},$$

i.e.

$$(f_{r,P}(\phi^{-1}(P))f_{r,P}(\phi(P)))^{(q^{k/2}-1)} = 1. \quad (1)$$

Let $P = (x_P, y_P) \in \mathbb{G}_1$. We will show that the equality (1) holds in the following.

Case 1. We first consider the curve E_1. Let $q = p$, where $p \equiv 3 \pmod 4$. The rational function $f_{r,P}$ can be written as $a(x) + b(x)y$, where $a(x)$ and $b(x)$ are the rational functions over the finite field $\mathbb{F}_q$ in terms of x [10]. We have

$$f_{r,P}(\phi^{-1}(P)) = a(-x_P) - b(-x_P)y_P i$$

and

$$f_{r,P}(\phi(P)) = a(-x_P) + b(-x_P)y_P i.$$

It follows from Fermat's little Theorem and $i^2 + 1 = 0$ that

$$(f_{r,P}(\phi^{-1}(P))f_{r,P}(\phi(P)))^{(q^{k/2}-1)} = 1.$$

Case 2. Now we consider the curve E_2. Let $q = p$, where $p \equiv 2 \pmod 3$. Similar to Case 1, the rational function $f_{r,P}$ can be written as $c(y) + d(y)x + e(y)x^2$, where $c(y)$, $d(y)$ and $e(y)$ are the rational functions over the finite field $\mathbb{F}_q$ in terms of y. Applying $\beta^2 + \beta + 1 = 0$, we get

$$\begin{aligned} f_{r,P}(\phi^{-1}(P)) =& c(y_P) + d(y_P)x_P\beta + e(y_P)x_P^2\beta^2 \\ =& (c(y_P) - e(y_P)x_P^2) + (d(y_P)x_P - e(y_P)x_P^2)\beta \end{aligned}$$

and

$$\begin{aligned} f_{r,P}(\phi(P)) =& c(y_P) + d(y_P)x_P\beta^2 + e(y_P)x_P^2\beta^4 \\ =& (c(y_P) - d(y_P)x_P) + (e(y_P)x_P^2 - d(y_P)x_P)\beta \\ =& (c(y_P) - e(y_P)x_P^2) - (d(y_P)x_P - e(y_P)x_P^2)(\beta + 1). \end{aligned}$$

It follows from Fermat's little Theorem and $\beta^2 + \beta + 1 = 0$ that

$$(f_{r,P}(\phi^{-1}(P))f_{r,P}(\phi(P)))^{(q^{k/2}-1)} = 1.$$

Case 3. Now we consider the curve E_3. Let $q = 2^l$. Similar to the above, the rational function $f_{r,P}$ can be written as $a(x) + b(x)y$, where $a(x)$ and $b(x)$ are the rational functions over the finite field $\mathbb{F}_q$ in terms of x. For convenience, we use the notation a and b for $a(x_P + s^2)$ and $b(x_P + s^2)$, respectively. Then

$$\begin{aligned} f_{r,P}(\phi^{-1}(P)) =& a + b(y_P + sx_P + t + 1) \\ =& (a + by_P + bsx_P) + b(t + 1) \end{aligned}$$

and

$$\begin{aligned} f_{r,P}(\phi(P)) =& a + b(y_P + sx_P + t) \\ =& (a + by_P + bsx_P) + bt. \end{aligned}$$

Since $s \in \mathbb{F}_{q^{k/2}}$ and $t^2 + t = s$, it follows from Fermat's little Theorem that

$$(f_{r,P}(\phi^{-1}(P))f_{r,P}(\phi(P)))^{(q^{k/2}-1)} = 1.$$

Case 4. Now we consider the curve E_4. Let $q = 3^l$. The rational function $f_{r,P}$ can be written as $a(x) + b(x)y$, where $a(x)$ and $b(x)$ are the rational functions over the finite field $\mathbb{F}_q$ in terms of x. For convenience, we use the notation a and b for $a(\alpha - x_P)$ and $b(\alpha - x_P)$, respectively. Then

$$f_{r,P}(\phi^{-1}(P)) = a + by_P i$$

and

$$f_{r,P}(\phi(P)) = a - by_P i.$$

It follows from Fermat's little Theorem that

$$(f_{r,P}(\phi^{-1}(P))f_{r,P}(\phi(P)))^{(q^{k/2}-1)} = 1.$$

Therefore the equality (1) holds in all cases. This completes the whole proof.

We call our new pairing in Theorem 1 the Ateil pairing. In the case of the supersingular curves with embedding degree $k = 2$, we see that at any security level the Ateil pairing is faster than the self-pairing based on the reduce Tate pairing since the final exponentiation of the former is simpler than that of the latter and both of them have the same Miller loop. However, in the case of the supersingular curves with embedding degree $k = 4$ or 6, the self-pairing based on the η_T pairing whose Miller loop is half the length of that required for the reduced Tate pairing. This leads to the proposed pairing in Theorem 1 is slower than the self-pairing based on the η_T pairing in this case. We next provide the improvement of the Ateil pairing, as compared to the self-pairing based on the η_T pairing.

3.1 An Improvement on the η_T Pairing

Our goal is to construct a new self-pairing which has the same Miller loop as the η_T pairing. It is known that the η_T pairing is the fastest pairing on supersingular elliptic curves over finite fields with small characteristics 2 or 3 and Hess *et. al* give another approach for the η_T pairing in Section 3.2 of [13]. We will mainly consider the self-pairing computation in this case. The following lemma is useful for generating the Ateil pairing on supersingular elliptic curves over finite fields with small characteristics.

Lemma 1. *Let E be the supersingular curves defined as Theorem 1. Let r be a large prime satisfying $r \mid \#E(\mathbb{F}_q)$ and denote the trace of the Frobenius endomorphism with t, i.e., $\#E(\mathbb{F}_q) = q + 1 - t$. The embedding degree with respect to r is equal to k. Write $T = t - 1$. For $T^i = (t-1)^i \equiv q^i \bmod r$ where $1 \le i \le k-1$, we denote $T_i = T^i \bmod r$. Let a be the smallest positive integer such that $T_i^a \equiv 1 \bmod r$. There exists an integer L such that $T_i^a - 1 = Lr$. Given the two points $P,\ Q \in \mathbb{G}_1 = Ker(\pi_q - [1]) \cap E[r]$, we have*

$$\hat{e}(P,\phi(Q))^{2(q^{k/2}-1)L} = \frac{f_{T_i,P}(\phi(Q))}{f_{T_i,Q}(\phi^{-1}(P))}^{2(q^{k/2}-1)c},$$

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

Proof. It is obvious from the definition of the Weil pairing and $f_{r,\phi(Q)}(P) = f_{r,Q}(\phi^{-1}(P))$ (see Proposition 2 of [21]) that

$$\hat{e}(P,\phi(Q))^{2(q^{k/2}-1)L} = (\frac{f_{r,P}(\phi(Q))}{f_{r,\phi(Q)}(P)})^{2L(q^{k/2}-1)} = (\frac{f_{Lr,P}(\phi(Q))}{f_{Lr,Q}(\phi^{-1}(P))})^{2(q^{k/2}-1)}.$$

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

$$\hat{e}(P,\phi(Q))^{2(q^{k/2}-1)L} = (\frac{f_{T_i^a-1,P}(\phi(Q))}{f_{T_i^a-1,Q}(\phi^{-1}(P))})^{2(q^{k/2}-1)} = (\frac{f_{T_i^a,P}(\phi(Q))}{f_{T_i^a,Q}(\phi^{-1}(P))})^{2(q^{k/2}-1)} \tag{1}$$

Since $(\hat{\pi}_q \circ \pi)(P) = [q]P = [T]P$, we have $\hat{\pi}_q^i(P) = [T^i]P = [T_i]P$. Due to the discussion in Section 3.2 of [13] (or see the proof of Theorem 1 in [3]), we see that

$$f_{T_i^a,P}(\phi(Q)) = (f_{T_i,P}(\phi(Q)))^{\sum_{j=0}^{a-1} T_i^{(a-1-j)} q^j} \tag{2}$$

Using the same argument for $f_{T_i^a,Q}(\phi^{-1}(P))$, we have

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

Substituting (2) and (3) into the equation (1), we have

$$\hat{e}(P,Q)^{2(q^{k/2}-1)L} = (\frac{f_{T_i,P}(\phi(Q))}{f_{T_i,Q}(\phi^{-1}(P))})^{2(q^{k/2}-1)c},$$

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

On the basis of Lemma 1, we can define a new powered pairing as $(\frac{f_{T_i,P}(\phi(Q))}{f_{T_i,Q}(\phi^{-1}(P))})^{2(q^{k/2}-1)}$ which will be non-degenerate provided that $r \nmid L$. It has the same loop length as the η_T pairing when $i = 1$. Despite this new pairing has the simple exponentiation, it is slower than the η_T pairing since it involves two Miller iteration loops. Applying $Q = P$ in the new defined pairing $(\frac{f_{T_i,P}(\phi(Q))}{f_{T_i,Q}(\phi^{-1}(P))})^{2(q^{k/2}-1)}$, we have the following results.

Theorem 2. *Using the same notation as above, the self-pairing based on the* η_T *pairing can be given by*

$$e_s(P,P) \triangleq (\frac{f_{T_i,P}(\phi(P))}{f_{T_i,P}(\phi^{-1}(P))})^{2(q^{k/2}-1)} = f_{T_i,P}(\phi(P))^{4(q^{k/2}-1)}.$$

Proof. It is immediate from the proof of Theorem 1 and Lemma 1.

We call our new pairing in Theorem 2 the Ateil_i pairing. Some remarks on the Ateil_i pairing are stated as follows.

Remark 1. A series of the Ateil_i pairing can be obtained as i varies. We call the Ateil_i pairing with the shortest Miller loop is optimal. Due to the discussion in [25, 12], the optimal Ateil_i pairing has the same loop length as the η_T pairing.

Remark 2. The loop length of the Ateil_i pairing is as same as that of the η_T pairing when $i = 1$. For $T_i < 0$, the generalized version of the Ateil pairing suggests to use $T_i \cdot (T_i)^{k/2} = T_i \cdot (-1) \pmod r$ provided that $k > 2$.

Remark 3. At any security level, the optimal Ateil_i pairing will be faster than the self-pairing based on the η_T pairing since the former has a simpler final exponentiation than the latter and both of them have the same Miller loop.

Remark 4. The optimal Ateil_i pairing on supersingular elliptic curves over finite fields with characteristic *three* can achieves better performance when implementing ZSS short signatures [28].

4 Self-pairing on Elliptic Curves with Embedding Degree *one*

Since the distortion maps exist on not only supersingular elliptic curves but also ordinary elliptic curves with embedding degree *one*, we will consider self-pairing computation on the latter curves in this section. Koblitz and Menezes first gave the concrete construction of ordinary curves with embedding degree *one* and analyzed the efficiency of pairing computations on these curves [18].

Assume that the prime $p = A^2 + 1$. The equation of the elliptic curve E_5 over $\mathbb{F}_p$ is defined by

$$E_5 : y^2 = x^3 + ax,$$

where $a = -1$ or -4. The order of the group $E_5(\mathbb{F}_p)$ is $\#E_5(\mathbb{F}_p) = p - 1$. Note that the distortion map on E_5 is given by $\phi :\ (x, y) \to (-x, Ay)$. In the following, we will provide the efficiency of the computation of self-pairings based on the Weil and Tate pairing, respectively.

4.1 Self-pairing Based on the Weil pairing

It is known that the denominator elimination techniques can be used for speeding up the reduced Tate pairing [4] and the powered Weil pairing [18, 17] due to the final exponentiation. However, these methods can not be applied in the case of pairing computations on the curve E_5 with embedding degree *one*. To apply the denominator elimination techniques in self-pairing computations, we will define a new fixed power of the Weil pairing. Let $P \in E_5(\mathbb{F}_p)$ have prime order r. The self-pairing based on the Weil pairing can be defined as

$$e_s(P,P) = \hat{e}(P, \phi(P))^4. \tag{4}$$

The following lemma shows that the proposed self-pairing (4) can be computed efficiently.

Lemma 2. *The denominator elimination technique can be applied when computing the self-pairing (4) on the curve E_5 with embedding degree one.*

Proof. In the case of the doubling steps of the self-pairings, after initially setting $T = P$, $f_1 = f_2 = 1$, for each bit of r we do

$$\begin{aligned} T &\leftarrow 2T \\ f_1 &\leftarrow f_1^2 \frac{l_{T,T}(\phi(P))}{v_{2T}(\phi(P))} \\ f_2 &\leftarrow f_2^2 \frac{l_{\phi(T),\phi(T)}(P)}{v_{\phi(2T)}(P)} \end{aligned}$$

Assume that $P = (x_P, y_P)$ and $2T = (x_{2T}, y_{2T})$. We obtain $\phi(P) = (-x_P, Ay_P)$ and $\phi(2T) = (-x_{2T}, Ay_{2T})$. It is easy to check that

$$\begin{aligned} v_{2T}(\phi(P)) =& - x_P - x_{2T} \\ v_{\phi(2T)}(P) =& x_{2T} - x_P = (-1) \cdot v_{2T}(\phi(P)). \end{aligned}$$

Note that we can ignore -1 due to the final power $four$. Thus the denominators in the doubling steps can be eliminated. Similarly, it can be seen that the denominators in the addition steps can be also eliminated. This completes the proof of Lemma 2.

Now we will consider the doubling and addition steps of self-pairing computations in Miller's algorithm.

Doubling Step Assume that $T = (x_T, y_T)$, $[2]T = (x_{2T}, y_{2T})$ and $P = (x_P, y_P)$. Let $l_{T,T}$ be the equation of the tangent line through the point T and λ be the slope of the line. We have

$$l_{T,T}(\phi(P)) = (Ay_P - y_T) - \lambda(-x_P - x_T) = (-y_T + \lambda(x_P + x_T)) + y_P \cdot A.$$

Observe that if the slope of the tangent line through the point T is λ, then the slope of the tangent line through the point $\phi(T)$ is $-A\lambda$. It follows that

$$l_{\phi(T),\phi(T)}(P) = y_P - Ay_T + A\lambda(x_P + x_T).$$

Then

$$(-A)l_{\phi(T),\phi(P)}(P) = (-y_T + \lambda(x_P + x_T)) - y_P A.$$

Since $A^4 = 1 \pmod p$ and the final power equals $four$, we can replace $l_{\phi(T),\phi(T)}(P))$ by $(-Al_{\phi(T),\phi(T)}(P))$ in the whole computation.

Note that we can cache $R_1 = A \cdot y_P$. The formulas for the doubling steps in affine coordinates will be given by

$$\begin{aligned} \lambda =& \frac{3x_T^2 + a}{2y_T};\ x_{2T} = \lambda^2 - 2x_T;\ y_{2T} = \lambda \cdot (x_T - x_{2T}) - y_T \\ t_1 =& - y_T + \lambda \cdot (x_P + x_T),\ t_2 = R_1,\ f_1 \leftarrow f_1^2 \cdot (t_1 + t_2),\ f_2 \leftarrow f_2^2 \cdot (t_1 - t_2) \end{aligned}$$

The total cost of the operation for the doubling steps in affine coordinates will be 1I+5M+4S, where I, M and S denote the costs of inversion, multiplication and squaring in the ground field $\mathbb{F}_p$.

Now we consider the operation count for the doubling steps in Jacobian coordinates. A point $(X, Y, Z, W = Z^2)$ in the modified Jacobian coordinates corresponds to the point (x, y) in affine coordinates with $x = X/Z^2$, $y = Y/Z^3$. Let $T = (X_T, Y_T, Z_T, W_T = Z_T^2)$ and $N = 2T = (X_N, Y_N, Z_N, W_N = Z_N^2)$. Based on the explicit-formulas database given by Bernstein and Lange [5], the following formulas compute a doubling in $6M + 10S$.

$$\begin{aligned} B =& X_T^2; C = Y_T^2; D = C^2; E = W_T^2; S = 2((X_T + C)^2 – B – D); M = 3B + aE; \\ X_N =& M^2 - 2S; Y_N = M \cdot (S - X_N) - 8D; Z_N = (Y_T + Z_T)^2 - C - W_T; \\ w_N =& Z_N^2; t_1 = Z_N \cdot W_T \cdot R_1; t_2 = -2C + M \cdot (W_T \cdot x_P + X_T); \\ l_1 =& t_1 + t_2; l_2 = t_1 - t_2; f_1 \leftarrow f_1^2 \cdot l_1; f_2 \leftarrow f_2^2 \cdot l_2; \end{aligned}$$

Addition Step Assume that $T = (x_T, y_T)$, $P = (x_P, y_P)$ and $N = T + P = (x_N, y_N)$. Let $l_{T,P}$ be the equation of the line through points T and P. Denote by λ the slope of the line $l_{T,P}$. We have

$$l_{T,P}(\phi(P)) = (Ay_P - y_P) - \lambda(-x_P - x_P) = (-y_P + 2\lambda x_P) + y_P \cdot A.$$

Observe that if the slope of the line through points T and P is λ, then the slope of the line through points $\phi(T)$ and $\phi(P)$ is $-A\lambda$. It follows that

$$l_{\phi(T),\phi(P)}(P)) = (y_P - Ay_P) - (-A\lambda)(x_P - (-x_P)) = A(-y_P + 2\lambda x_P) + y_P.$$

Then

$$(-A)l_{\phi(T),\phi(P)}(P) = (-y_P + 2\lambda x_P) - y_P \cdot A.$$

Since $A^4 = 1 \pmod p$ and the final power equals $four$, it follows that $l_{\phi(T),\phi(P)}(P))$ can be replaced by $(-Al_{\phi(T),\phi(P)}(P))$ in the whole computation.

Similar to the doubling step, we can cache $R_1 = A \cdot y_P$. The formulas for the addition steps in affine coordinates can be given by

$$\lambda = \frac{y_T - y_P}{x_T - x_P};\ x_N = \lambda^2 - x_P - x_T;\ y_N = \lambda \cdot (x_P - x_N) - y_P;$$
$$t_1 = -y_P + 2\lambda \cdot x_P;\ t_2 = R_1,\ f_1 \leftarrow f_1 \cdot (t_1 + t_2),\ f_2 \leftarrow f_2 \cdot (t_1 - t_2)$$

The total cost of the operation for the addition steps in affine coordinates will be 1I+5M+1S.

Now we consider the operation count for the addition steps in Jacobian coordinates. Note that we will cache $R_1 = A \cdot y_P$, $R_3 = y_P^2$, and $R_4 = x_P^2$. Let $T = (X_T, Y_T, Z_T, W_T = Z_T^2)$ and $N = (X_N, Y_N, Z_N, W_N = Z_N^2) = T + P$. Based on the explicit-formulas database given by Bernstein and Lange [5], the following formulas compute an addition step in $9M + 7S$.

$$U_2 = x_P \cdot W_T; S_2 = (y_P) \cdot Z_T \cdot W_T; H = U_2 - X_T; HH = H^2; I = 4HH;$$
$$J = H \cdot I; M = S_2 - Y_T; R = 2M; V = X_T \cdot I; R_2 = R^2; X_N = R_2 - J - 2V;$$
$$Y_N = R \cdot (V - X_N) - 2Y_T \cdot J; Z_N = (Z_T + H)^2 - W_T - HH; W_N = Z_N^2;$$
$$t_1 = (Z_N + R_1)^2 - W_N + R_3; t_2 = (Z_N + y_P)^2 - W_N - R_3 + 2((R + x_P)^2 - R_2 - R_4);$$
$$l_1 = t_1 + t_2;\quad l_2 = t_1 - t_2;\quad f_1 = f_1 \cdot l_1;\quad f_2 = f_2 \cdot l_2;$$

4.2 Self-pairing Based on the Tate Pairing

The self-pairing can be defined on the basis of the reduced Tate pairing. Similar to the paper [18], we could choose R to be the point $(0, 0)$ on the curve E_5. Thus the divisor D equals to $(\phi(P) + R) - (R)$. The self-pairing based on the Tate pairing is given by

$$e_s(P, P) = \bar{e}(P, \phi(P)) = (\frac{f_{r,P}(\phi(P) + R)}{f_{r,P}(R)})^{(p-1)/r}. \tag{5}$$

Note that we can not replace the divisor D by the point $\phi(P)$ for computing the reduced Tate pairing $\bar{e}(P, \phi(P))$. We next analyze the cost of the doubling and addition steps for computing $\bar{e}(P, \phi(P))$ in detail.

Doubling Step Let $T = (x_T, y_T)$ and $2T = (x_{2T}, y_{2T})$ in affine coordinate systems. The function $l_{T,T}$ and v_{2T} correspond respectively, to the tangent line to the curve E_5 at the point T and the vertical line through the point $2T$. For each bit of r we do

$$\begin{aligned} \lambda =& \frac{3x_T^2 + a}{2y_T};\ x_{2T} = \lambda^2 - 2x_T;\ y_{2T} = \lambda \cdot (x_T - x_{2T}) - y_T \\ f_1 \leftarrow& f_1^2 \cdot l_{T,T}(\phi(P) + R) \cdot v_{2T}(R);\ f_2 \leftarrow f_2^2 \cdot l_{T,T}(R) \cdot v_{2T}(\phi(P) + R). \end{aligned}$$

The formulas need 1I+8M+4S to compute the doubling step in affine coordinates. Koblitz and Menezes have considered the doubling steps which cost 13M+9S in Jacobian coordinates [18]. Ionica and Joux have given the improved formulas for the doubling steps in this case which cost 10M+10S [14].

Addition Step Assume that $T = (x_T, y_T)$, $P = (x_P, y_P)$ and $N = T + P = (x_N, y_N)$. The formulas for the addition steps will be given by

$$\begin{aligned} \lambda =& \frac{y_T - y_P}{x_T - x_P};\ x_N = \lambda^2 - x_P - x_T;\ y_N = \lambda \cdot (x_P - x_N) - y_P; \\ f_1 \leftarrow& f_1 \cdot l_{T,P}(\phi(P) + R) \cdot v_{T+P}(R);\ f_2 \leftarrow f_2 \cdot l_{T,P}(R) \cdot v_{T+P}(\phi(P) + R). \end{aligned}$$

The total cost of the operation for the addition steps in affine coordinates will be 1I+8M+1S. Ionica and Joux have developed the improved formulas for the addition steps in Jacobian coordinates which cost 18M+3S [14].

4.3 Efficiency Consideration for Self-pairing on the Curve with Embedding Degree *one*

In this subsection, we compare the efficiency of computing the self-pairings with different structures on the curve E_5. We first note that the presented self-pairing (4) has the simpler final exponentiation than the reduced Tate pairing (5) which leads to the reduction of the computational complexity. Furthermore, we summarize the computational costs of basic doubling and addition steps for different pairings into Table 2.

Table 2. Comparison of Basic Steps for Different Self-pairings on Curves with Embedding Degrees *one*

Coordinate System	Self-pairings	Doubling Steps	Addition Steps
Affine coordinate	Proposed pairing (4)	1I+5M+4S	1I+5M+1S
	Tate pairing (5)	1I+8M+4S	1I+8M+1S
Jacobian coordinate	Proposed pairing (4)	6M+10S	9M+7S
	Tate pairing (5)	10M+10S	18M+3S

As shown in Table 2, computing the proposed self-pairing (4) needs fewer multiplications than computing the reduced Tate pairing (5) on the curve E_5 with embedding degree *one* in each step. We conclude that the proposed self-pairing (4) is faster than the self-pairing (5) based on the Tate pairing at any security level.

5 Conclusion

In this paper, the computation of the self-pairing is considered in all cases. Using the symmetry of the structure of the Weil pairing, we have presented the Ateil pairing with *one* Miller loop. The proposed pairings achieve better performance than the previously known self-pairings at any security level. From the Ateil pairing approach, we see that the variant of the Weil pairing may be preferred in certain cases.

References

1. C. Arene, T. Lange, M. Naehrig and C. Ritzenthaler. "Faster Computation of the Tate Pairing," Preprint, 2009. Available from http://eprint.iacr.org/2009/155.
2. R. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen, and F. Vercauteren. Handbook of Elliptic and Hyperelliptic Curve Cryptography, Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2006.

3. P.S.L.M. Barreto, S. Galbraith, C. ÓhÉigeartaigh, and M. Scott. "Efficient pairing computation on supersingular Abelian varieties," *Designs, Codes and Cryptography*, vol. 42, no. 3. Springer Netherlands, 2007.
4. P.S.L.M. Barreto, H.Y. Kim, B. Lynn, and M. Scott. "Efficient algorithms for pairing-based cryptosystems," *Advances in Cryptology-Crypto'2002*, volume 2442 of *Lecture Notes in Computer Science*, pp. 354-368. Springer-Verlag, 2002.
5. D. J. Bernstein and T. Lange. Explicit-formulas database. http://www.hyperelliptic.org/EFD
6. C. Costello, T. Lange, and M. Naehrig. "Faster Pairing Computations on Curves with High-Degree Twists," *Public Key Cryptography - PKC 2010*, Volume 6056 of *Lecture Notes in Computer Science*, pp. 224-242, Springer-Verlag, 2010.
7. I. Duursma, H.-S. Lee. "Tate pairing implementation for hyperelliptic curves $y^2 = x^p - x + d$," *Advances in Cryptology-Asiacrypt'2003*, volume 2894 of *Lecture Notes in Computer Science*, pp. 111-123. Springer-Verlag, 2003.
8. G. Frey and H-G. Rück. "A remark concerning m-divisibility and the discrete logartihm in the divisor class group of curves," *Math. Comp.,* vol. 62(206), pp.865-874, 1994.
9. S. Galbraith. Pairings. Chapter IX of In: I. Blake, G. Seroussi, N. Smart(eds) Advances in Elliptic Curve Cryptography. Cambridge University Press, 2005.
10. S. D. Galbraith, F. Hess, and F. Vercauteren. "Aspects of Pairing Inversion," *IEEE Trans. Inform. Theory* vol.54, No. 12, pp. 5719-5728, 2008.
11. S.D. Galbraith, K. Paterson, N. Smart. "Pairings for cryptographers," *Discr. Appl. Math.* vol. 156, pp. 3113-3121, 2008.
12. F. Hess. "Pairing lattices," *Pairing 2008,* Volume 5209 of *Lecture Notes in Computer Science,* pp. 18-38, Springer-Verlag, 2008.
13. F. Hess, N.P. Smart and F. Vercauteren. "The Eta pairing revisited," *IEEE Trans. Infor. Theory*, vol 52, pp. 4595-4602, Oct. 2006.
14. S. Ionica and A. Joux. "Another approach to pairing computation in Edwards coordinates," *IndoCrypt 2008*, Volume 5365 of *Lecture Notes in Computer Science*, pp. 400-413, 2008.
15. E. Lee, H.-S. Lee, and C.-M. Park. "Efficient and generalized pairing computation on Abelian varieties," *IEEE Trans. Inform. Theory,* vol. 55, no.4, pp. 1793-1803, 2009.
16. S. Matsuda, N. Kanayama, F. Hess, and E. Okamoto. "Optimised versions of the Ate and twisted Ate pairings," *The 11th IMA International Conference on Cryptography and Coding*, Volume 4887 of *Lecture Notes in Computer Science*, pp. 302-312. Springer-Verlag, 2007.
17. B. G. Kang, J. H. Park. "On the relationship between squared pairings and plain pairings," Inf. Process. Lett. vol. 97(6), pp. 219-224, 2006.

18. N. Koblitz, and A. J. Menezes. "Pairing-based cryptography at high security levels," *Cryptography and Coding*, Volume 3796 of *Lecture Notes in Computer Science*, pp. 13-36. Springer-Verlag, 2005.
19. V.S. Miller. "Short programs for functions on curves," Unpublished manuscript, 1986. Available from http://crypto.stanford.edu/miller/miller.pdf.
20. V.S. Miller. "The Weil pairing and its efficient calculation," J. Cryptology, vol. 17, no. 44, pp. 235-261, 2004.
21. C. M. Park, M. H. Kim, and M. Yung. "A Remark on Implementing the Weil Pairing," *CISC 2005*, Volume 3822 of *Lecture Notes in Computer Science*, pp. 313-323, 2005.
22. K. G. Paterson, "ID-based signatures from pairings on elliptic curves," Electronics Letters, vol. 38, No. 18, pp. 1025-1026, 2002.
23. K.G. Paterson. Cryptography from Pairing - Advances in Elliptic Curve Cryptography. Cambridge University Press, 2005.
24. M. Scott, N. Benger, M. Charlemagne, L. J. Dominguez Perez, and E. J. Kachisa. "On the Final Exponentiation for Calculating Pairings on Ordinary Elliptic Curves," *Pairing 2009*, Volume 5671 of *Lecture Notes in Computer Science*, pp. 78-88, 2009.
25. F. Vercauteren. "Optimal pairings," *IEEE Trans. Inform. Theory,* vol. 56, no.1, pp. 455-461, 2009.
26. E. Verheul, "Evidence that XTR is more secure than supersingular elliptic curve cryptosystems," *Advances in Cryptology - Eurocrypt 2001*, Volume 2045 of *Lecture Notes in Computer Science*, pp. 195-210, Springer-Verlag, 2001.
27. F. Zhang, X. Chen, W. Susilo and Y. Mu. "A New Signature Scheme Without Random Oracles from Bilinear Pairings," *VietCrypt 2006*, Volume 4341 of *Lecture Notes in Computer Science*, pp.67-80, Springer-Verlag, 2006.
28. F. Zhang, R. Safavi-Naini and W. Susilo, "An efficient signature scheme from bilinear pairings and its applications," *PKC 2004*, Volume 2947 of *Lecture Notes in Computer Science*, pp.277-290, Springer-Verlag, 2004.
29. F. Zhang, R. Safavi-Naini, W. Susilo, "ID-Based Chameleon Hashes from Bilinear Pairings," Cryptology ePrint Archive, Report 2003/208.
30. C.-A. Zhao, D.Q. Xie, F. Zhang, J. Zhang and B.-L. Chen. "Computing Bilinear Pairings on Elliptic Curves with Automorphisms," *Designs, Codes and Cryptography*, To appear.
31. C.-A. Zhao, F. Zhang and J. Huang. "A note on the Ate pairing," *Int. J. Inf. Security,* vol. 7, no. 6, pp. 379-382, 2008.
32. C.-A. Zhao, F. Zhang and J. Huang. "All pairings are in a group," *IEICE Trans. Fundamentals,* vol E91-A, no.10, pp. 3084-3087, 2008.

33. C.-A. Zhao, F. Zhang and D.Q. Xie. "Reducing the Complexity of the Weil Pairing Computation," *ChinaCrypt'2009,* pp. 117-125, 2009.