Powered Tate pairing computation

Bo Gyeong Kang[⋆1] and Je Hong Park[2]

[1] Department of Mathematics, Korea Advanced Institute of Science and Technology,
373-1 Guseong-dong, Yuseong-gu, Daejeon, 305-701, Korea
snubogus@kaist.ac.kr
[2] National Security Research Institute,
161 Gajeong-dong, Yuseong-gu, Daejeon, 305-350, Korea
jhpark@etri.re.kr

Abstract. In this paper, we introduce a powered Tate pairing on a supersingular elliptic curve that has the same shortened loop as the modified Tate pairing using the eta pairing approach by Barreto *et al.* The main significance of our approach is to remove the condition which the latter should rely on. It implies that our method is simpler and *potentially* general than the eta pairing approach, although they are equivalent in most practical cases.

Keywords: Powered Tate pairing, Tate pairing, Bilinear map, Elliptic Curve Cryptosystem

1 Introduction

Currently, one of the most active areas in elliptic curve cryptography is the construction of cryptographic protocols based on bilinear maps. These protocols depend on the existence of efficiently computable, non-degenerate bilinear maps over certain groups. The Weil or Tate pairing is an example of a method to realize a bilinear map on certain pairs of points on elliptic curves. So efficient computation of pairings is essential to practical applications in pairing-based cryptosystems. There has been a lot of work on the efficient implementation of pairings on elliptic curves with a sufficiently small security multiplier such as supersingular curves or MNT curves [3–5, 8]. These results are based in some manner on the algorithm of Miller [11]. It is an extension of the well-known double-and-add method of performing point scalar multiplication on elliptic curves, so it is usually presented as a loop through the binary expansion of the group order. To improve this algorithm, one focused on how to perform elimination of irrelevant factors and denominators during the computation of pairings, which were rendered conceptually simpler and substantially more efficient. Along with these techniques, a new type of improvement to shorten the loop occurring in the Miller algorithm was introduced by Duursma and Lee [7]. Recently, Barreto *et al.* developed a general technique for computing pairings on supersingular Abelian varieties, called the η pairing approach. It is thought of as a generalized version of the result by Duursma and Lee on supersingular elliptic curves in characteristic three. Taking a step forward, they presented η_T pairing which is expected to provide the improvement of the total computation for the Tate pairing by a factor close to 2. Barreto *et al.*'s approaches, however, require a condition: the existence of an automorphism λ such that $\lambda\psi^q(Q) = \psi(Q)$ where $Q \in E(\mathbb{F}_q)$ and ψ is a distortion map.

[⋆] This work was done while the first author was studying in the University of Maryland, USA.

Our Contributions Here, we have paid our attention to the fact that Barreto *et al.* were not able to prove whether the condition for the η pairing is necessary or not. Our idea to answer this question is to use another map instead of the automorphism λ. As a candidate, we consider the multiplication by q, denoted by $[q]$-map. At a first glance, it does not seem to be the proper map in replacement of the automorphism because it is just an endomorphism. However, it leads us to have the derived q-th powered Tate pairing [3] which has the same shortened loop as the η pairing without any conditions. This is a simpler proof of bilinearity and potentially more general as well. In other words, our results can be extended to implement the reduced Tate pairing that contains the modified pairing defined by distortion maps. The η pairing seems to be realized only in the case of the modified pairing because the condition requires a distortion map [4]. From efficiency point of view, however, our results are equivalent with those of Barreto *et al.* in most known practical cases based on elliptic curves because both of them work over the same defined set. So the main significance of our works is to provide flexibility to already efficient algorithm.

Organizations This paper is organized as follows. In Section, 2 we briefly review the Tate pairing and the Miller algorithm. In Section 3, after giving well known propositions about elliptic curves, we define the ζ pairing and propose the q-th powered Tate pairing. New pairing computation algorithm derived from the ζ_T pairing which saves of a factor by 2 is proposed in Section 4. At last, our conclusion is drawn in Section 5 with comments about further works.

2 Preliminaries

2.1 Elliptic curves

Let q be a prime or prime power and let $\mathbb{F}_q$ denote the finite field with q elements and let p be a characteristic of $\mathbb{F}_q$. An elliptic curve E defined over $\mathbb{F}_q$ can be described as the set of points (x, y) satisfying the Weierstrass equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, where $a_i \in \mathbb{F}_q$. Let $x(P)$ and $y(P)$ denote the rational functions mapping $P \in E$ to its affine x- and y-coordinates, respectively. If K is an extension of the field $\mathbb{F}_q$, the set of K-rational points of E, which we denote by $E(K)$, is the set of points P such that $x(P), y(P) \in K$, together with a special element $\mathcal{O}$, called point at infinity. There exists an abelian group law on E. Explicit formulas for computing the coordinates of a point $P_3 = P_1 + P_2$ from the coordinates of P_1 and P_2 are well known [12]. For any $r \in \mathbb{Z}$, denote r times addition of P as $[r]P$. Let $K = \mathbb{F}_{q^k}$. Then the q-th power Frobenius endomorphism of E is the mapping $\sigma : E(\mathbb{F}_{q^k}) \to E(\mathbb{F}_{q^k})$, where $(x, y) \mapsto (x^q, y^q)$. Thus a point $P \in E(\mathbb{F}_{q^k})$ is defined over $\mathbb{F}_{q^i}$ if and only if $\sigma^i(P) = P$. Using the Frobenius map, we can define the trace map

$$\mathrm{Tr} : E(\mathbb{F}_{q^k}) \to E(\mathbb{F}_q) \quad \text{as } \mathrm{Tr}(R) = \sum_{i=0}^{k-1} \sigma^i(R),$$

for any point $R \in E(\mathbb{F}_{q^k})$.

The Hasse bound states that the number of points, say *order* is $\#E(\mathbb{F}_q) = q + 1 - t$, where $|t| \le 2\sqrt{q}$. Here t is called the *trace* of the Frobenius endomorphism. Curves whose trace t is a multiple of the characteristic p are called supersingular. The order of a point $P \in E$ is the least

[3] As noted in [10], there is no difference as a bilinear map used for any cryptographic application if the pairing is replaced by its m-th power, where m is a fixed integer not divisible by r.

[4] The use of distortion maps may differ cryptographic properties [1].

nonzero integer r such that $[r]P = \mathcal{O}$, where $[r]P$ is the sum of r terms equal to P. The order of a point divides the curve order, so $r|\#E(\mathbb{F}_q)$. For a given integer r, the set of all points $P \in E(K)$ such that $[r]P = \mathcal{O}$ is denoted $E(K)[r]$ and $E[r]$ denotes $E(\overline{\mathbb{F}}_q)[r]$.

A subgroup G of an elliptic curve $E(\mathbb{F}_q)$ is said to have *security multiplier* k if its order r divides $q^k - 1$, but does not divide $q^i - 1$ for any $0 < i < k$. If E is supersingular, the value of k is bounded by $k \leq 6$.

A divisor on E is a formal sum $\mathcal{D} = \sum_{P \in E(\mathbb{F}_{q^k})} n_P(P)$ where $n_P \in \mathbb{Z}$. The set of points $P \in E(\mathbb{F}_{q^k})$ such that $n_P \neq 0$ is called the support of $\mathcal{D}$. The degree of $\mathcal{D}$ is the value $\deg(\mathcal{D}) = \sum_P n_P$. The zero divisor has all $n_P = 0$. An abelian group structure is defined on the set of divisors $\mathrm{Div}(E)$ by the addition of corresponding coefficients in their formal sums. Let $f : E(\mathbb{F}_{q^k}) \to \mathbb{F}_{q^k}$ be a function on the curve and let $\deg(\mathcal{D}) = 0$. We define $f(\mathcal{D}) \equiv \prod_P f(P)^{n_P}$. The divisor of a function f is $\mathrm{div}(f) \equiv \sum_P \mathrm{ord}_P(f)(P)$ where $\mathrm{ord}_P(f)$ is referred to as the order or valuation at P. It follows from this definition that $\mathrm{div}(f) = 0$ if and only if f is a nonzero constant. A divisor $\mathcal{D}$ is called *principal* if $\mathcal{D} = \mathrm{div}(f)$ for some function f. A divisor $\mathcal{D}$ is principal if and only if $\deg(\mathcal{D}) = 0$ and $\sum_P [n_P]P = \mathcal{O}$. We say two divisors $\mathcal{D}$ and $\mathcal{D}'$ are *equivalent*, $\mathcal{D}' \sim \mathcal{D}$ if there exists a function g such that $\mathcal{D}' = \mathcal{D} + \mathrm{div}(g)$.

2.2 The Tate pairing

Let $P \in E(\mathbb{F}_{q^k})[r]$ and $Q \in E(\mathbb{F}_{q^k})$ and let f_P be the rational function with divisor $\mathrm{div}(f_P) = r(P) - r(\mathcal{O})$. The existence of this function is well known [8]. Take a point $S \in E(\mathbb{F}_q)$ such that $\mathcal{A}_Q = (Q + S) - (S)$ and (f_P) have disjoint supports. Then the Tate pairing $\tau : E(\mathbb{F}_{q^k})[r] \times (E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})) \to \mathbb{F}^*_{q^k}/(\mathbb{F}^*_{q^k})^r$ is defined as

$$\tau(P, \overline{Q}) := \overline{f_P(\mathcal{A}_Q)},$$

where $\overline{Q}$ is the equivalence class in $E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})$ containing Q, and $\overline{f_P(\mathcal{A}_Q)}$ is the equivalence class in $\mathbb{F}^*_{q^k}/(\mathbb{F}^*_{q^k})^r$ containing $f_P(\mathcal{A}_Q)$. Using the isomorphism between $\mathbb{F}^*_{q^k}/(\mathbb{F}^*_{q^k})^r$ and the elements of order r in $\mathbb{F}^*_{q^k}$, and assuming $k > 1$, we can define the *reduced* Tate pairing [3, 4, 2]

$$\tau(P, Q) = f_P(Q)^{\frac{q^k-1}{r}}.$$

This means that the function f_P is now evaluated on a point rather than on a divisor, and has a unique value. If E is supersingular, this definition can be modified via a distortion map $\psi : E(\mathbb{F}_q) \to E(\mathbb{F}_{q^k})$. This means that the group $\mathbb{G}_2$ can be selected in $E(\mathbb{F}_q)$ instead of a non-optimal choice $E(\mathbb{F}_{q^k})$. It is called the modified Tate pairing.

2.3 Miller's algorithm

An essential part in computing the Tate pairing is the evaluation of f_P. Miller showed how to compute f_P iteratively, using the divisors of the lines drawn by the secant-and-tangent addition rule [11]. Throughout this paper, we define $g_{U,V} : E(\mathbb{F}_{q^k}) \to \mathbb{F}_{q^k}$ to be the line through points $U, V \in E$. The shorthand g_U stands for $g_{U,-U}$ which is the vertical line passing through U. If $U = (u, v)$ and $Q = (x, y)$, then $g_U(Q) = x - u$.

It is also well known [8] that there exists a rational function $f_{c,P}$ on E with divisor $\mathrm{div}(f_{c,P}) = c(P) - ([c]P) - (c-1)(\mathcal{O})$, $c \in \mathbb{Z}$. Since $[r]P = \mathcal{O}$, Miller's algorithm computes $f_P(Q) = f_{r,P}(Q)$, $Q \neq \mathcal{O}$ by building up these functions $f_{c,P}$ according to the following formula

$$f_{i+j,P}(Q) = f_{i,P}(Q) \cdot f_{j,P}(Q) \cdot g_{[i]P,[j]P}(Q)/g_{[i+j]P}(Q).$$

Several optimization techniques to reduce computational efforts of the Miller algorithms have been proposed [3, 4, 2]. They focused on how to perform elimination of irrelevant factors and denominators during the computation of pairings, which is rendered conceptually simpler and substantially more efficient. Independently, the loop shortening approach for supersingular curves was introduced by Duursma and Lee [7] and then generalized by Barreto *et al.* [2] using the η pairing.

2.4 The η pairing

Here, we review the η pairing by Barreto *et al.* [2]. Let $q = p^m$ and consider supersingular curves over $\mathbb{F}_q$ with the security multiplier $k = 2d$ $(d > 1)$ and with suitable distortion maps ψ. Define $f_{p^i,[p^j]P}$ to be functions on E such that

$$\mathrm{div}(f_{p^i,[p^j]P}) = p^i([p^j]P) - ([p^{i+j}]P) - (p^i - 1)(\mathcal{O}).$$

Then one can choose the function $f_{p^i,[p^j]P}$ such that

$$f_{p^{i+1},P} = f^p_{p^i,P} f_{p,[p^i]P}.$$

Using this relation, we obtain

$$\langle P, \psi(Q)\rangle_{q^d+1} := f_{q^d,P}(\psi(Q)) = \prod_{i=0}^{dm-1} f_{p,[p^i]P}(\psi(Q))^{p^{dm}-1-i}$$

which leads us to have modified Tate pairing τ by exponentiating to the power $(q^k - 1)$ [2]. Then the η pairing is defined as

$$\eta(P, Q) := f_{q,P}(\psi(Q)).$$

Then it is easily checked that

$$\langle P, \psi(Q)\rangle_{q^d+1} := f_{q^d,P}(\psi(Q)) = \eta(P, Q)^{q^{d-1}} \eta([q]P, Q)^{q^{d-2}} \cdots \eta([q^{d-1}]P, Q).$$

Barreto *et al.* [2] showed that if ψ satisfies

$$\lambda(\psi^q(Q)) = \psi(Q) \tag{1}$$

for some automorphism λ on the curve, then

$$\eta([q]P, Q) = \eta(P, Q)^q$$

and so

$$\langle P, \psi(Q)\rangle_{q^d+1} = \eta(P, Q)^{dq^{d-1}}.$$

So the loop occurring in the Miller algorithm to compute the Tate pairing can be shortened from a product of dm terms to a product of m terms.

The authors in [2] mentioned that they are not sure whether the bilinearity of the η pairing holds without the condition (1) in [2]. Their intuition tells us that it does not seem to be satisfied, but they could not prove it. From this point forward, we focus our efforts on showing the other possible pairings which have the same shortened loop as the η pairing. They can be improved by a factor of roughly 2 in parallel with η_T in terms of generalized parameters of supersingular elliptic curves.

3 Powered Tate Pairings

Our idea is simply induced by the question: what if we use another map instead of the automorphism λ in the condition (1). As a candidate for possible maps in replacement of λ, we use the multiplication by q, say $[q]$-map which has useful properties in case of supersingular curves. First, we briefly introduce some well known results that are necessary to handle the $[q]$-map on supersingular curves. Through these, we can derive Lemma 1, which yields an efficient formula of q-th powered pairing in Theorem 1. Let ϕ be an endomorphism and $P \in E(\mathbb{F}_q)$. We refer to [6, 12] for the followings.

Definition 1. The *ramification index* of ϕ at P is defined by

$$e_\phi(P) = \mathrm{ord}_P(u \circ \phi)$$

where u is an uniformizing parameter for $\phi(P)$.

We define $\phi^* : \mathrm{Div}(E) \to \mathrm{Div}(E)$ to be the homomorphism with

$$\phi^*\Big(\sum n_Q(Q)\Big) = \sum_Q \sum_{P \in \phi^{-1}(Q)} n_Q e_\phi(P)(P).$$

Proposition 1. Suppose g to be a nonzero rational function. Then

$$\mathrm{div}(g \circ \phi) = \phi^*(\mathrm{div}(g)).$$

Proof. See [6, Prop.11.9]. □

Proposition 2. Let E be a supersingular curve. Then $[q]$-map (multiplication by q) is purely inseparable which means $e_{[q]} = q^2$ and $E[q] = \{\mathcal{O}\}$.

Proof. See [12, Chap. III, Coro.6.4]. □

Lemma 1. *Let E be a supersingular curve and let $P \in E(\mathbb{F}_q)$. Then*

$$\mathrm{div}(f_{q,[q]P} \circ [q]) = \mathrm{div}(f_{q,P}^{q^2})$$

Proof. It is sufficient to show that both rational functions have the same number of zeros and poles at the same point. By Propositions 1 and 2, and the properties of the $[q]$-map, we have

$$\begin{aligned}
\mathrm{div}(f_{q,[q]P} \circ [q]) &= [q]^*(\mathrm{div}(f_{q,[q]P})) \\
&= [q]^*\big(q([q]P) - ([q^2]P) - (q-1)(\mathcal{O})\big) \\
&= e_{[q]}(P)q(P) - e_{[q]}([q]P)([q]P) - e_{[q]}(\mathcal{O})(q-1)(\mathcal{O}) \\
&= q^2\big(q(P) - ([q]P) - (q-1)(\mathcal{O})\big) \\
&= q^2\,\mathrm{div}(f_{q,P}) = \mathrm{div}(f_{q,P}^{q^2}).
\end{aligned}$$

□

Let ψ be a distortion map from $E(\mathbb{F}_q)$ to $E(\mathbb{F}_{q^k})$. Let $P \in E(\mathbb{F}_q)[r]$. By definition of a distortion map [13], $\{P, \psi(P)\}$ is a generating set for $E[r]$[5]. Recall that the modified Tate pairing is defined

[5] It is known that in cases of supersingular elliptic curves, we can pick generators of $E[r]$ as representatives of $E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})$ [8].

by $\tau(P, \psi(P))$, which is a special case of the reduced Tate pairing denoted by $\tau(P, R)$ where R is a random point in $E(\mathbb{F}_{q^k})[r]$. Our following results hold not only for the modified pairing, but can be extended to the reduced pairing. Especially, R can be transformed into a point $Q = R - \sigma^d(R)$ whose trace is zero [4] if the trace of R is not zero. This means that Q is contained in the q-eigenspace of σ and so we have $\sigma(Q) = [q]Q$. By defining

$$\zeta(P, Q) := f_{q,P}(\sigma(Q)) = \prod_{i=0}^{m-1} f_{p,[p^i]P}(\sigma(Q))^{p^{m-1-i}},$$

the bilinear property of the ζ pairing is obtained as follows.

Lemma 2. *For $Q = R - \sigma^d(R)$ where $P \in E(\mathbb{F}_q)[r]$ and $R \in E(\mathbb{F}_{q^k})[r]$ with $R \notin E(\mathbb{F}_{q^d})$,*

$$\zeta([q]P, Q) = \zeta(P, Q)^q$$

Proof. By Lemma 1, we have $f_{q,[q]P} \circ [q] = f_{q,P}^{q^2}$ (up to scalar multiple). Then

$$\begin{aligned}
\zeta([q]P, Q) &= f_{q,[q]P}(\sigma(Q)) = f_{q,[q]P} \circ [q](Q) \\
&= f_{q,P}(Q)^{q^2} = f_{q,P}(\sigma^2(Q)) = f_{q,P}(\sigma(Q))^q \\
&= \zeta(P, Q)^q.
\end{aligned}$$

□

The trace zero subgroup and the image of distortion map in eta pairing approach are the same sets. So this proof can be applied to prove the bilinearity of the η pairing [9] in much simpler way. The following theorem gives a result as comparable to the eta pairing approach.

Theorem 1. *Let $P \in E(\mathbb{F}_q)[r]$ and let $R \in E(\mathbb{F}_{q^k})[r]$ with $R \notin E(\mathbb{F}_{q^d})$. Let $Q = R - \sigma^d(R)$. Then we have*

$$\tau(P, Q)^q = \zeta(P, Q)^{dq^{d-1}(q^d-1)} = f_{q,P}(-Q)^{d(q^d-1)}.$$

Proof. By Lemma 2, $P \in E(\mathbb{F}_q)$ and the property of Q whose trace is zero, it is easily checked that

$$\begin{aligned}
\langle P, Q\rangle_{q^d+1}^q &= \langle P, \sigma(Q)\rangle_{q^d+1} = f_{q,P}(\sigma(Q))^{q^{d-1}} f_{q,[q]P}(\sigma(Q))^{q^{d-2}} \cdots f_{q,[q^{d-1}]P}(\sigma(Q)) \\
&= \zeta(P, Q)^{q^{d-1}} \zeta([q]P, Q)^{q^{d-2}} \cdots \zeta([q^{d-1}]P, Q) \\
&= \zeta(P, Q)^{dq^{d-1}}.
\end{aligned}$$

Raise both sides to the $(q^d - 1)$-th power, we have the first equality as

$$\tau(P, Q)^q = \tau(P, \sigma(Q)) = \zeta(P, Q)^{dq^{d-1}(q^d-1)}.$$

Additionally, since $q^d \equiv -1 \pmod r$ induces

$$\zeta(P, Q)^{dq^{d-1}} = f_{q,P}(\sigma(Q))^{dq^{d-1}} = f_{q,P}([q^d]Q)^d = f_{q,P}(-Q)^d,$$

the second equality is completed by exponentiating both sides to the $(q^d - 1)$-th power. □

Corollary 1. *Let $P \in E(\mathbb{F}_q)[r]$ and let $R \in E(\mathbb{F}_{q^k})[r]$ with $R \notin E(\mathbb{F}_{q^d})$. Let $Q = R - \sigma^d(R)$. Then we have*

$$\tau(P, R)^{2q} = \tau(P, Q)^q = f_{q,P}(-Q)^{d(q^d-1)}$$

Proof. By Galois invariance of [8, Chap.I, Thm.1.7] and $P \in E(\mathbb{F}_q)$, we have

$$\tau(P,R)^{q^d} = \tau(\sigma^d(P), \sigma^d(R)) = \tau(P, \sigma^d(R)).$$

This implies

$$\tau(P,Q) = \tau(P, R - \sigma^d(R)) = \tau(P,R)\tau(P,\sigma^d(R))^{-1} = \tau(P,R)\tau(P,R)^{-q^d} = \tau(P,R)^{1-q^d}.$$

Since $q^d \equiv -1 \pmod r$, $1 - q^d \equiv 2 \pmod r$ holds, and so we obtain $\tau(P,R)^2 = \tau(P,Q)$. By Theorem 1, after exponentiating to the power q, the proof is completed. □

Since $(2q, r) = 1$, $\tau(P,R)^{2q}$ is sufficient to be used in real applications instead of $\tau(P,R)$. As a side effect, $x(-Q) \in \mathbb{F}_{q^d}$, a denominator elimination technique is also applicable to compute $f_{q,P}(-Q)^{d(q^d-1)}$. Most of all, on the contrary to the η pairing which requires additional condition (1), Theorem 1 and Corollary 1 do not rely on any special conditions, except supersingular curves.

4 Extension

Barreto *et al.* [2] proposed the η_T pairing induced from the η pairing and claimed that it is about twice as fast as the technique by Duursma and Lee [7], because the loop in the Miller's algorithm can be shortened from $\log(q)$ to $\log(t) \sim \frac{1}{2}\log(q)$. In this section, we propose new pairing formulae that have comparable efficiency to the η_T pairing. Ours is originally derived from the idea of the ζ pairing, thus, the same advantage as the ζ pairing obtained by independence from the condition (1) can be guaranteed.

Let $N = hr = q + 1 - t$ be the order of $E(\mathbb{F}_q)$. Denote $n = q - N = t - 1$, then since $q = t - 1 \bmod N$, we have $(t-1)^k = 1 \bmod N$. By definition of security parameter k, $(t-1)^i \neq 1 \bmod r$ for any $i < k$. Since N is a multiple of r, it can be reduced to $(t-1)^i \neq 1 \bmod N$. This implies that $(t-1)^d = -1 \bmod N$. Namely,

$$n^d = (t-1)^d = aN - 1$$

for a constant a. Then we have

$$\mathrm{div}(f_{n^d,P} \cdot g_P) = aN(P) - aN(\mathcal{O}) = \mathrm{div}(f_{aN,P}) = \mathrm{div}(f_{N,P}^a) \tag{2}$$

where $\mathrm{div}(g_P) = (P) + (-P) - 2(\mathcal{O})$. In parallel with the η_T, denote

$$\zeta_T(P,Q) = f_{n,P}(\sigma(Q)).$$

Through the following lemmas, we show that ζ_T is sufficient to compute the Tate pairing.

Lemma 3. *Let $P \in E(\mathbb{F}_q)[r]$. Then*

$$\mathrm{div}(f_{n,[n]P} \circ [q]) = \mathrm{div}(f_{n,P}^{q^2})$$

Proof. Let $\phi = [q]$. Then we can consider $\phi^{-1}([n]P) = \phi^{-1}([q]P) = P$ since $[n]P = [q]P$. By Propositions 1 and 2,

$$\begin{aligned}
\mathrm{div}(f_{n,[n]P} \circ [q]) &= [q]^*(\mathrm{div}(f_{n,[n]P})) \\
&= [q]^*\big(n([n]P) - ([n^2]P) - (n-1)(\mathcal{O})\big) \\
&= e_{[q]}(P)n(P) - e_{[q]}([n]P)([n]P) - e_{[q]}(\mathcal{O})(n-1)(\mathcal{O}) \\
&= q^2\big(n(P) - ([n]P) - (n-1)(\mathcal{O})\big) = q^2\,\mathrm{div}(f_{n,P}) = \mathrm{div}(f_{n,P}^{q^2}).
\end{aligned}$$

□

Lemma 4. *Let $P \in E(\mathbb{F}_q)[r]$ and let $R \in E(\mathbb{F}_{q^k})[r]$ with $R \notin E(\mathbb{F}_{q^d})$. Let $Q = R - \sigma^d(R)$. Then*

$$f_{n,[n]P}(\sigma(Q))^M = (f_{n,P}(\sigma(Q))^{nM}$$

when $M = (q^k - 1)/N$.

Proof. By Lemma 3, we have $f_{n,[n]P} \circ [q] = f_{n,P}^{q^2}$ (up to scalar multiple). Then

$$\begin{aligned} f_{n,[n]P}(\sigma(Q)) &= f_{n,[n]P} \circ [q](Q) \\ &= (f_{n,P}(Q))^{q^2} = f_{n,P}([q^2]Q) = f_{n,P}(\sigma(Q))^q. \end{aligned}$$

Because of $q = n + N$ and $NM = q^k - 1$, we have

$$f_{n,P}(\sigma(Q))^{qM} = f_{n,P}(\sigma(Q))^{(n+N)M} = f_{n,P}(\sigma(Q))^{nM}. \tag{3}$$

The proof is thus completed. □

Theorem 2. *Let $P \in E(\mathbb{F}_q)[r]$ and let $R \in E(\mathbb{F}_{q^k})[r]$ with $R \notin E(\mathbb{F}_{q^d})$. Let $Q = R - \sigma^d(R)$. Then*

$$\tau(P,Q)^{aq} = \zeta_T(P,Q)^{dn^{d-1}M} \tag{4}$$

Proof. Since N does not divide $q^i - 1$ for any $i < k$ in cases of supersingular curves, the value of $q^d - 1$ is a factor of M. This enables $g_P(\sigma(Q))$ to be dropped off by being raised to the M-th power. Also, by a standard recurrence relation, it is written as

$$f_{n^d,P} = \prod_{i=0}^{d-1} f_{n,[n^i]P}^{n^{d-1-i}}.$$

Thus combining these with Lemma 4, we have

$$\begin{aligned} \tau(P,\sigma(Q))^a &= f_{N,P}(\sigma(Q))^{aM} \\ &= \Big(f_{n^d,P}(\sigma(Q)) \cdot g_P(\sigma(Q))\Big)^M \\ &= \Big(f_{n,P}(\sigma(Q))^{n^{d-1}} f_{n,[n]P}(\sigma(Q))^{n^{d-2}} \cdots f_{n,[n^{d-1}]P}(\sigma(Q))\Big)^M \\ &= f_{n,P}(\sigma(Q))^{dn^{d-1}M} = \zeta_T(P,Q)^{dn^{d-1}M}. \end{aligned}$$

Because of $\tau(P,\sigma(Q))^a = \tau(P,Q)^{aq}$, the proof is completed. □

The left hand side of Eq. (4) is a certain proper powered Tate pairing. So it is naturally derived that ζ_T has somehow potential bilinear property. Hasse bound tells that $t^2 \leq 4q$ [12], thus the loop is shortened to $\log(n) \sim \log(t)$ which is roughly one half of $\log(q)$.

Remark 1. As mentioned in [2], the final powering of η_T requires a more complicated formula than that of the η pairing. One reason is that the cost of raising to the power n over $\mathbb{F}_{q^k}$ is usually more expensive than just a q-th Frobenius map. However, ζ_T can provide a much simper powering by Eq. (3). Note that $q^{d-1} = (n+N)^{d-1} = n^{d-1} + cN$ for a constant c. Since $f_{n,P}(\sigma(Q))^{NM} = 1$, we have

$$f_{n,P}(\sigma(Q))^{dq^{d-1}M} = f_{n,P}(\sigma(Q))^{d(n^{d-1}+cN)M} = f_{n,P}(\sigma(Q))^{dn^{d-1}M}$$

which results in

$$\tau(P,Q)^{aq} = f_{n,P}(\sigma(Q))^{dq^{d-1}M}.$$

By the same argument, this technique is applicable to η_T as well. So the loss of efficiency occurring by the final powering of ζ_T and η_T compared with ζ and η is almost compensated for through our observation.

Remark 2. As explored in our paper, our approach is more general than the eta pairing approach in principle. But S. Galbraith pointed out that two methods are equally applicable for the most important examples [9], because the trace zero subgroup and the image of our distortion map is the same. He commented that one has always been able to find a distortion map with satisfying the condition (1) and so it is quite possible that such distortion maps always exist.

5 Conclusion

We proposed a new pairing ζ that is not affected by a certain condition such as the existence of the appropriate automorphism and distortion map. Additionally, we derived a loop shortening version of the ζ pairing, called ζ_T which is parallel to the η_T pairing. Our q-th powered Tate pairing derived from the ζ pairing provides the same efficiency comparison with the plain Tate pairing using the η pairing, but the former is simpler and potentially general than the latter.

Acknowledgement

We would like to thank Steven Galbraith and Paulo S.L.M. Barreto for valuable comments on an earlier version of this manuscript.

References

1. P.S.L.M. Barreto. The Well-Tempered Pairing. *Elliptic Curve Cryptography - ECC'2004*. Invited Talk.
2. P.S.L.M. Barreto, S. Galbraith, C.O. hEigeartaigh and M. Scott. Efficient pairing computation on supersingular abelian varieties. *Cryptology ePrint Archive*, Report 2004/375.
3. P.S.L.M. Barreto, H.Y. Kim, B. Lynn and M. Scott. Efficient algorithms for pairing-based cryptosystems. *Advances in Cryptology - CRYPTO 2002*, Lecture Notes in Comput. Sci. **2442**, pp. 354–368, 2002.
4. P.S.L.M. Barreto, B. Lynn and M. Scott. On the selection of pairing-friendly groups. *Selected Areas in Cryptography - SAC 2003*, Lecture Notes in Comput. Sci. **3006**, pp. 17–25, 2004.
5. P.S.L.M. Barreto, B. Lynn and M. Scott. Efficient implementation of pairing-based cryptosystems. *J. Cryptology*, Vol. **17**(4): 17–25 (2004).
6. L.S. Charlap and D.P. Robbins. An Elementary Introduction to Elliptic Curves. *CRD Expository Report*, No. 31.,1988.
7. I. Duursma and H.-S. Lee. Tate pairing implementation for hyperelliptic curves $y^2 = x^p - x + d$. *Advances in Cryptology - ASIACRYPT 2003*, Lecture Notes in Comput. Sci. **2894**, pp. 111–123, 2003.
8. S. Galbraith. Pairings, Chapter IX of book *Advances in elliptic curve cryptography* edited by I. Blake, G. Seroussi and N. Smart. London Mathematical Society Lecture Note Series, Vol. **317**, Cambridge University Press, 2005.
9. S. Galbraith. E-mail Communications, 2005.
10. N. Koblitz and A. Menezes. Pairing-based cryptography at high security levels. *Cryptology ePrint Archive*, Report **2005/076**.
11. V.S. Miller. Short programs for functions on curves. IBM Thomas J. Watson Research Center, 1986.
12. J.H. Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Math. **106**, Springer-Verlag. 1986.
13. E.R. Verheul. Evidence that XTR is more secure than supersingular elliptic curve cryptosystems. *J. Cryptology*, Vol. **17**(4): 277–296 (2004).