On the relationship between squared pairings and plain pairings

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 investigate the relationship between the squared Weil/Tate pairing and the plain Weil/Tate pairing. Along these lines, we first show that the squared pairing for arbitrary chosen point can be transformed into a plain pairing for the trace zero point which has a special form to compute them more efficiently. This transformation requires only a cost of some Frobenius actions. Additionally, we show that the squared Weil pairing can be computed more efficiently for trace zero point and derive an explicit formula for the 4th powered Weil pairing as an optimized version of the Weil pairing.

Keywords: Weil/Tate pairing, Squared pairing, Pairing-based cryptosystems

1 Introduction

After Boneh and Franklin [6] proposed an identity-based encryption scheme using the Weil pairing, many cryptographic schemes based on the Weil or Tate pairing have been introduced. Although these pairings both provide good functionality for use in cryptosystems, pairing computations are often the bottleneck to realize cryptographic applications practically. So, fast implementations of these pairings have become a subject of active research areas in elliptic curve cryptography.

The computation of the Weil/Tate pairing can be performed using an algorithm first presented by Miller [14]. Recently proposed improvements [11, 2, 8, 1] are based in some manner on it. Specifically, they make a use of elimination of irrelevant factors and denominators during the computation of Tate pairings on supersingular curves which were originally proposed as a suitable setting for pairing-based schemes. However, recent works have additionally focused on optimizing pairing computations of certain ordinary curves such as MNT curves [15, 4, 17, 16, 3]. Although there are a number of advantages in using supersingular curves such

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

as distortion maps, a small number of usable curve or doubt of their long term security has led one to investigate the use of ordinary curves. Especially, Barreto et al. [4] showed how to select groups in MNT curves where many optimization techniques proposed for supersingular curves [11, 2] have a counterpart. Independently, the notion of the squared pairing was introduced by Eisenträger et al. [9]. The objective of this notion is to generalize consecutive computation of plain pairing and squaring on it by unified approach. The authors show that, when computing the squared pairing, partial factors can be discarded in each step. Additionally, their algorithm is deterministic and does not depend on a random choice of points for evaluation of the pairing. However, by reason of security, they only considered a general case where there is no cancelation of denominators.

Our main contribution in this paper is to connect the squared pairing to the plain one. We show that for a very small cost, the squared pairing for a randomly chosen point R on $E(\mathbb{F}_{q^{2d}})$ can be transformed into the plain pairing for a trace zero point Q which has x-coordinate over a smaller field $\mathbb{F}_{q^d}$. From a practical point of view, our result seems to show that there is no real advantage in computing the squared pairing directly. At the same time, our result can be regarded as showing how to compute the squared pairing in a much more efficient fashion using several optimization techniques in [4]. Especially, we applied these techniques for the Tate pairing to the squared Weil pairing using the fact that $(1 - p^d)$th power of the Weil pairing is the same as the squared one.[3] Taking a step forward, we can derive an interesting explicit formula for the 4th powered Weil pairing by adapting several optimization techniques to compute the squared Weil pairing. This squared or 4th powered Weil pairing is much faster than the plain one, so it becomes more meaningful with respect to the claim in [13]: the proper powered Weil pairing (actually it is the squared Weil pairing) can be computed faster than the Tate pairing at high security levels. Throughout this paper, our main concern is pairings defined over ordinary curves with suitable embedding degree such as MNT curves. However, the principles can of course be easily adapted to the cases of supersingular curves.

The paper is organized as follows. After introducing the squared pairing and Eisenträger et al.'s algorithm briefly in Section 2, we present the connection between the squared Tate pairing and the plain pairing in Section 3. In Section 4, we show that a similar property holds for the squared or 4th powered Weil pairing. Finally, we draw our conclusions in Section 5.

[3] Our work had almost been done independently before Koblitz and Menezes's paper [13] came out in public. They used the method of properly powering the Weil pairing to drop off some redundant factors, which has turned out to be just the squared Weil pairing through our work.

2 Preliminaries

In this section, we give a brief summary of several mathematical backgrounds and definitions of Tate and squared pairings. Additionally, we review Miller's algorithm for the Tate pairing computation and Eisenträger et al.'s algorithm for the squared pairing.

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 by point at infinity.

For $P, Q \in E(K)$, we can define the sum $P + Q$ according to some simple rule. 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 [5]. $E(K)$ is an abelian group under this operation with the identity element $\mathcal{O}$. It is easy to show that $E(\mathbb{F}_q)$ is a subgroup of $E(K)$. The number of points of $E(K)$ is called its *order*. The Hasse bound states that $\#E(\mathbb{F}_q) = q + 1 - t$, where $|t| \leq 2\sqrt{q}$. Here t is called the *trace* of the Frobenius endomorphism stated below. Curves whose trace t is a multiple of the characteristic p are called supersingular. The order of a point $P \in E$ is the smallest integer $r > 0$ such that $[r]P = \mathcal{O}$. The set of r-torsion points of E, denoted $E(K)[r]$, is the set $\{P \in E(K) \mid [r]P = \mathcal{O}\}$.

Let $K = \mathbb{F}_{q^k}$. Then the q-th power Frobenius endomorphism of E is the mapping

$$\sigma : E(\mathbb{F}_{q^k}) \to E(\mathbb{F}_{q^k}), \quad \text{where } (x, y) \mapsto (x^q, y^q).$$

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 characteristic polynomial of the Frobenius map σ is

$$\pi(u) = u^2 - tu + q.$$

Since $\pi(u) = (u-1)(u-q) \bmod r$, the eigenvalues are 1 and q. The 1-eigenspace of σ on $E[r]$ is $E(\mathbb{F}_q)[r]$ and the q-eigenspace of σ on $E[r]$ consists of all points $R \in E[r]$ satisfying $\mathrm{Tr}(R) = \mathcal{O}$ [4, 10]. In fact, it is well known that if $r | \#E(\mathbb{F}_q)$, there is a basis P, Q for $E[r]$ such that $\sigma(P) = P$ and $\sigma(Q) = [q]Q$.

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 all $0 < i < k$. If E is supersingular, the value of k is bounded by $k \le 6$. The group $E[r] \cong \mathbb{Z}_r \times \mathbb{Z}_r$ lies in $E(\mathbb{F}_{q^k})$. Let $P \in E(\mathbb{F}_q)$ be a point of order r such that $\langle P \rangle$ has security multiplier k. Then $E(\mathbb{F}_{q^k})$ contains a point Q of the same order r but linearly independent of P.

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 $n_P = 0$. The sum of two divisors $\mathcal{D} = \sum_P n_P(P)$ and $\mathcal{D}' = \sum_P n'_P(P)$ is the divisor $\mathcal{D} + \mathcal{D}' = \sum_P (n_P + n'_P)(P)$. Given a nonzero rational function $f : E(\mathbb{F}_{q^k}) \to \mathbb{F}_{q^k}$, the divisor of f is the divisor $(f) = \sum_P \mathrm{ord}_P(f)(P)$ where $\mathrm{ord}_P(f)$ is the multiplicity of f at P. It follows from this definition that $(fg) = (f) + (g)$ and $(f/g) = (f) - (g)$ for any two nonzero rational functions f and g defined on E; moreover $(f) = 0$ if and only if f is a nonzero constant. We say two divisors $\mathcal{D}$ and $\mathcal{D}'$ are equivalent, $\mathcal{D}' \sim \mathcal{D}$ if there exists a function g such that $\mathcal{D}' = \mathcal{D} + (g)$. For any function f and any divisor $\mathcal{D} = \sum_P n_P(P)$ of degree zero, we define $f(\mathcal{D}) = \prod_P f(P)^{n_P}$.

2.2 Squared Pairings

Let $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ denote finite abelian groups in which the discrete logarithm problem is hard. By a pairing we shall mean a non-degenerate bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. The Weil or Tate pairing is one of examples defined on an elliptic curve. Let $P, Q \in E[r]$ and pick two divisors $\mathcal{A}_P$ and $\mathcal{A}_Q$ which are equivalent to $(P) - (\mathcal{O})$ and $(Q) - (\mathcal{O})$, respectively, and such that $\mathcal{A}_P$ and $\mathcal{A}_Q$ have disjoint supports. Let f_P be the rational function with divisor $(f_P) = r(P) - r(\mathcal{O}) = r \cdot \mathcal{A}_P$. Analogously, let f_Q be a function on E whose divisor $(f_Q) = r \cdot \mathcal{A}_Q$. Then the Weil pairing $\omega : E[r] \times E[r] \to \mathbb{F}_{q^k}$ is defined as

$$\omega(P, Q) := \frac{f_P(\mathcal{A}_Q)}{f_Q(\mathcal{A}_P)}.$$

The Tate pairing is also defined based on $f_P(\mathcal{A}_Q)$. Let $P \in E(\mathbb{F}_q)[r]$ and $Q \in E(\mathbb{F}_{q^k})$ be linearly independent points. Then the (reduced) Tate pairing $\tau(P, Q) \in \mathbb{F}_{q^k}$ on $E(\mathbb{F}_q)[r] \times E(\mathbb{F}_{q^k})$ is defined as

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

But it can be easily computed by

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

as proven in [4]. It means that the function f_P is now evaluated on a point rather than on a divisor. Furthermore, it makes the Miller's algorithm deterministic. If E is supersingular, this definition can be modified via a distorsion map $\phi : E(\mathbb{F}_q) \to E(\mathbb{F}_{q^k})$. It means that the group $\mathbb{G}_2$ can be selected in $E(\mathbb{F}_q)$ instead of a non-optimal choice $E(\mathbb{F}_{q^k})$.

The squared Weil pairing is defined by

$$\psi(P,Q) = (-1)^r \frac{f_P(Q) \cdot f_Q(-P)}{f_P(-Q) \cdot f_Q(P)},$$

for r-torsion points P, Q on E with neither being the identity and $P \neq \pm Q$. Additionally, the squared Tate pairing v is defined by

$$v(P,Q) := \left(\frac{f_P(Q)}{f_P(-Q)}\right)^{(q^k-1)/r}.$$

Then it was shown in [9] that $\psi(P,Q) = \omega(P,Q)^2$ and $v(P,Q) = \tau(P,Q)^2$.

2.3 Miller's algorithm

An essential part in computing the Weil/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 [14]. 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 well known that there exists a rational function $f_{c,P}$ on E with divisor $(f_{c,P}) = c(P) - ([c]P) - (c-1)(\mathcal{O})$, $c \in \mathbb{Z}$ [9]. Since $rP = \mathcal{O}$, Miller's algorithm computes $f_P(Q) = f_{r,P}(Q)$, $Q \neq \mathcal{O}$ by coupling the above formulas with the double-and-add method to calculate rP.

Theorem 1. Let P be a point on $E(\mathbb{F}_q)$ and $f_{c,P}$ be a rational function with divisor $(f_{c,P}) = c(P) - ([c]P) - (c-1)(\mathcal{O})$, $c \in \mathbb{Z}$. For all $i, j \in \mathbb{Z}$,

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

2.4 Eisenträger et al.'s algorithm

In [9], Eisenträger et al. proposed an algorithm to compute the squared Weil/Tate pairing. At first, we introduce the algorithm for $\psi(P,Q)$ where P and Q are r-torsion points on E. This algorithm is based on Miller's formula with an addition-subtraction chain for r. For each j in the chain, form a tuple $t_j = \Big[[j]P, [j]Q, n_j, d_j\Big]$ such that

$$\frac{n_j}{d_j} = \frac{f_{j,P}(Q) \cdot f_{j,Q}(-P)}{f_{j,P}(-Q) \cdot f_{j,Q}(P)}.$$

The squared pairing needs n_r/d_r. The recurrence formula is

$$\frac{n_{i+j}}{d_{i+j}} = \frac{n_i}{d_i} \cdot \frac{n_j}{d_j} \cdot \frac{g_{[i]P,[j]P}(Q)}{g_{[i]P,[j]P}(-Q)} \cdot \frac{g_{[i+j]P}(-Q)}{g_{[i+j]P}(Q)} \cdot \frac{g_{[i]Q,[j]Q}(-P)}{g_{[i]Q,[j]Q}(P)} \cdot \frac{g_{[i+j]Q}(P)}{g_{[i+j]Q}(-P)}, \tag{1}$$

and begins with $t_1 = [P, Q, 1, 1]$. But there is no need to compute all value in the recurrence formula. The vertical lines through $[i+j]P$ and $[i+j]Q$ do not appear in the formulae for n_{i+j} and d_{i+j}, because the contributions from Q and $-Q$ (or from P and $-P$) are equal.

For the squared Tate pairing computation $v(P,Q)$ with $P \in E(\mathbb{F}_q)[r]$ and $Q \in E(\mathbb{F}_{q^k})$, above algorithm can be simplified because

$$\frac{n_j}{d_j} = \frac{f_{j,P}(Q)}{f_{j,P}(-Q)}.$$

So the recurrence formula is

$$\frac{n_{i+j}}{d_{i+j}} = \frac{n_i}{d_i} \cdot \frac{n_j}{d_j} \cdot \frac{g_{[i]P,[j]P}(Q)}{g_{[i]P,[j]P}(-Q)} \tag{2}$$

and begins with $t_1 = [P, 1, 1]$. Given t_i and t_j, t_{i+j} or t_{i-j} can be obtained as the case of the squared Weil pairing without changing Q.

3 Squared Tate pairing

Suppose the security multiplier k to be even, and let $d = k/2$. As stated above, the objective of [4] is to generate the group $\mathbb{G}_2$ in MNT curves that makes computation of the Tate pairing more efficient, and so they use the twist of the curve $E(\mathbb{F}_{q^d})$ to generate $\mathbb{G}_2$. It allows the denominator elimination optimization established for certain supersingular curves [2]. But in our case, we fix $\mathbb{G}_2$ as $E(\mathbb{F}_{q^k})$ in advance, and suppose that an arbitrary base points in $\mathbb{G}_2$ is given. Hence we use an alternative way to pick a generator *on the fly* that makes the same optimization possible. For any $R \in E(\mathbb{F}_{q^k})$, the point $Q := R - \sigma^d(R)$ satisfies $\sigma^d(Q) = \sigma^d(R) - R = -Q$. This means $x(Q)^{q^d-1} = 1$ and $y(Q)^{q^d-1} = -1$.

Theorem 2. *For any $R \in E(\mathbb{F}_{q^k})$, let $Q = R - \sigma^d(R)$. Then we have $\tau(P,R)^{1-q^d} = \tau(P,Q)$ where $P \in E(\mathbb{F}_q)$. Furthermore, $v(P,R) = \tau(P,Q)$.*

Proof. By Galois invariance of [10, Chap.I, Thm.1.7], we have $\tau(\sigma(P), \sigma(Q)) = \tau(P, Q)^q$. Since $P \in E(\mathbb{F}_q)$, $\tau(P, R)^{q^d} = \tau(\sigma^d(P), \sigma^d(R)) = \tau(P, \sigma^d(R))$. 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 $\tau(P, R)^2 = \tau(P, Q)$, which implies $v(P, R) = \tau(P, Q)$. □

Theorem 2 shows that computation of the squared pairing for a random point $R \in E(\mathbb{F}_{q^k})$ can be reduced to evaluate the Tate pairing for the trace zero point $Q = R - \sigma^d(R)$.

Lemma 1. For $P \in E(\mathbb{F}_q)[r]$ and $Q \in E(\mathbb{F}_{q^k})$ with $x(Q) \in \mathbb{F}_{q^d}$. Let $g_{[a]P}(X)$ be the vertical line through $[a]P$. Then $g_{[a]P}(Q)^{q^d-1} = 1$.

Proof. Since $[a]P$ has coordinate in $\mathbb{F}_q$, $g_{[a]P}(X) = x(X) - x([a]P) \in \mathbb{F}_q[x]$. Because of $x(Q) \in \mathbb{F}_{q^d}$, $g_{[a]P}(Q) = x(Q) - x([a]P)$ is contained in $\mathbb{F}_{q^d}$. This implies $g_{[a]P}(Q)^{q^d-1} = 1$. □

From Lemma 1, the denominators in the Tate pairing evaluation can disappear. This makes our method for general base points to have competitive efficiency with specific point which lies in a proper subfield $\mathbb{F}_{q^d}$ at the cost of a few Frobenius actions.

4 Squared and 4th Powered Weil pairings

In this section we first show that the observations of the previous section about the relation between the squared and plain Tate pairings hold in the Weil pairing.

Theorem 3. *Let $P, R \in E[r]$ be linearly independent and furthermore, $P \in E(\mathbb{F}_q)$ and $R \in E(\mathbb{F}_{q^k})$. Let $Q := R - \sigma^d(R)$, then we have*

$$\psi(P, R) = \omega(P, Q).$$

Proof. Since $[r]Q = [r](R - \sigma^d(R)) = [r]R - \sigma^d([r]R) = \mathcal{O}$ by [18], $Q \in E[r]$. Furthermore, it is clear that $\omega(P, Q) = \omega(P, R - \sigma^d(R)) = \omega(P, R) \cdot \omega(P, \sigma^d(R))^{-1}$. By [14, Def.1], $\omega(\sigma(P), \sigma(R)) = \omega(P, R)^q$, and since $P \in E(\mathbb{F}_q)$, $\omega(P, \sigma^d(R)) = \omega(\sigma^d(P), \sigma^d(R)) = \omega(P, R)^{q^d}$. So $\omega(P, Q) = \omega(P, R)^{1-q^d} = \omega(P, R)^2 = \psi(P, R)$ due to the fact $1 - q^d \equiv 2 \pmod{r}$. □

Theorem 3 shows that computation of the squared Weil pairing for arbitrary random point is transformed into that of the original Weil pairing for trace zero point. But the squared Weil pairing can be computed more efficiently for trace zero points as opposed to the original one.

Assume that $P, Q \in E[r]$ be linearly independent and furthermore, $P \in E(\mathbb{F}_q)$ and $Q \in E(\mathbb{F}_{q^k})$. Let S and T be points on E such that the divisor $\mathcal{A}_P := (P+S) - (S)$ and $\mathcal{A}_Q := (Q+T) - (T)$ have disjoint support. Then it is shown in [9] that

$$\omega(P,Q) = \frac{f_P((Q+T)-(T))}{f_Q((P+S)-(S))} = \frac{f_P(Q+T-S)}{f_P(T-S)} \cdot \frac{f_Q(S-T)}{f_Q(P+S-T)}.$$

If any 2-torsion point $U \neq \mathcal{O}$ is contained in $E(\mathbb{F}_{q^d})$, we can pick T and S such that $T - S = U$. Suppose $E(\mathbb{F}_q)$ does not contain a 2-torsion point ($\neq \mathcal{O}$). It implies t odd, where $\#E(\mathbb{F}_q) = q+1-t$. Since $\#E(\mathbb{F}_{q^3}) = q^3+1-t^3+3qt$ by using Weil's Theorem, it is even and so a 2-torsion point U exists in $E(\mathbb{F}_{q^3})$. Hence this condition is quite acceptable under the circumstances where security multiplier k divisible by 3 is chosen.[4] In addition since orders of $Q+U$ and $P-U$ are $2r$, the functions f_P, f_Q do not have zeros and poles at $Q+U$ and $P-U$. Thus it is unnecessary to be concerned about the case where $\omega(P,Q)$ is not defined.

Theorem 4. *Let $U \in E(\mathbb{F}_{q^d})[2]$, $P \in E(\mathbb{F}_q)[r]$. Given r torsion point $Q \in E(\mathbb{F}_{q^k})$ whose trace is zero, then*

$$\psi(P,Q) = (-1)^r \left(\frac{f_Q(P-U)}{f_P(Q+U)} \right)^{q^d-1}. \tag{3}$$

Furthermore, $x(Q), x(P), x(Q+U)$ and $x(P-U)$ are contained in $\mathbb{F}_{q^d}$. As a result, denominator elimination technique can be applicable to compute both of $f_Q(P-U)$ and $f_P(Q+U)$.

Proof. Suppose the characteristic of $\mathbb{F}_q$ is larger than 3 and let E have the Weierstass equation $y^2 = x^3 + ax + b$. The Weil pairing is defined as follows:

$$\omega(P,Q) = \frac{f_P(Q+U)}{f_P(U)} \cdot \frac{f_Q(-U)}{f_Q(P-U)} = \left(\frac{f_P(U)}{f_P(Q+U)} \cdot \frac{f_Q(P-U)}{f_Q(-U)} \right)^{-1}.$$

Raise both sides to $(1-q^d)$-th power. The left hand side is

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

since $\omega(P,Q)$ is a r-th root of unity and since $1 - q^d \equiv 2 \pmod{r}$.
For the right side, it is clear that $f_P(U)^{q^d-1} = 1$ because of $P, U \in E(\mathbb{F}_{q^d})$. Let V, W be elements of the group $\langle Q \rangle$ in $E(\mathbb{F}_{q^k})$. Then

$$\sigma^d(V) = -V \text{ and } \sigma^d(W) = -W$$

hold, because Q generates q-eigenspace of σ. Since $-V = (x(V), -y(V))$, it follows that

$$x(V)^{q^d} = x(V), \quad y(V)^{q^d} = -y(V) \quad \text{and}$$
$$x(W)^{q^d} = x(W), \quad y(W)^{q^d} = -y(W).$$

[4] In [13] a 2-torsion point $U \in E(\mathbb{F}_q)$ is taken by assuming the order of $E(\mathbb{F}_q)$ to be even. We can just adapt their assumption without much loss of cases.

Let

$$\gamma := \begin{cases} \frac{3x(V)^2+a}{2y(V)} & \text{if V=W,} \\ \frac{y(V)-y(W)}{x(V)-x(W)} & \text{otherwise.} \end{cases}$$

Then we have

$$\begin{aligned} g_{V,W}(-U) &= y(V) - y(-U) + \gamma(x(V) - x(-U)) \\ g_{V,W}(-U)^{q^d} &= -y(V) - y(-U) - \gamma(x(V) - x(-U)). \end{aligned}$$

Since y-coordinate of 2-torsion point U is zero, we have $g_{V,W}(-U)^{q^d-1} = -1$. In addition, $g_V(-U)^{q^d-1} = (x(V) - x(-U))^{q^d-1} = 1$ because $x(V), x(-U)$ lie in $\mathbb{F}_{q^d}$. Since $f_Q(-U)$ is written as proper compositions of $g_{V,W}$ and g_V, we can easily reduce $f_Q(-U)^{q^d-1} = (-1)^r$. Hence the right side of (3) is obtained.

It is obvious that $x(Q), x(P)$ and $x(P-U)$ lie in $\mathbb{F}_{q^d}$. In addition, since $y(U) = 0$ and since

$$x(Q+U) = \left(\frac{y(Q) - y(U)}{x(Q) - x(U)}\right)^2 - x(Q) - x(U),$$

we have $x(Q+U)^{q^d-1} = 1$ which implies $x(Q+U) \in \mathbb{F}_{q^d}$. This completes the proof. □

Remark 1. Although we proved Theorem 4 only for $p > 3$, this result can be extended to other cases except supersingular curves in binary fields.

Combining these two results, additionally, we can derive an explicit formula for the 4th powered Weil pairing.

Corollary 1. *For randomly chosen $R \in E(\mathbb{F}_{q^k})[r]$ and a 2-torsion point $U \in E(\mathbb{F}_{q^d})$, we have*

$$\omega(P,R)^4 = \psi(P,R)^2 = \omega(P,Q)^2 = \psi(P,Q) = (-1)^r \left(\frac{f_Q(P-U)}{f_P(Q+U)}\right)^{q^d-1},$$

where $Q := R - \sigma^d(R)$.

Proof. It is clear by combining Theorem 3 with Theorem 4. □

5 Conclusion

In this paper, we investigated the relationship between squared pairings and plain pairings. First, we showed that the squared Weil/Tate pairing for arbitrary chosen point is equal to the plain Weil/Tate pairing for the trace zero point which has a special form to compute them more efficiently. Using this relation for the Weil pairing, we derived an explicit formula for the 4th powered Weil pairings represented as the optimized Weil pairing. Our observations can bring more meaningful insight into the possibility of switching to the proper powered Weil pairing at high security levels.

Acknowledgement

The authors of this paper would like to thank Paulo S.L.M. Barreto, Lawrence C. Washington and Steve Galbraith for valuable comments on an earlier version of this manuscript.

References

1. P.S.L.M. Barreto, S. Galbraith, C.O. hEigeartaigh and M. Scott. Efficient pairing computation on supersingular abelain varieties. *Cryptology ePrint Archive*, Reprot **2004/375**.
2. 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.
3. P.S.L.M. Barreto, B. Lynn and M. Scott. Efficient algorithms for pairing-based cryptosystems. *J. Cryptology*, Vol. **17**(4): 321–334 (2004).
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. I. Blake, G. Seroussi and N. Smart. *Elliptic Curves in Cryptography.* London Mathematical Society Lecture Notes Series, **265**, Cambridge Univ. Press, 1999.
6. D. Boneh and M. Franklin. Identity-based encryption from the Weil pairing. *SIAM J. Comput.*, Vol. **32**(3): 586–615 (2003).
7. D. Boneh, B. Lynn and H. Shacham. Short signatures from the Weil pairing. *J. Cryptology*, Vol. **17**(4): 297–319 (2004).
8. 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.
9. K. Eisenträger, K. Lauter and P.L. Montgomery. Improved Weil and Tate pairings for elliptic and hyperelliptic curves. *Algorithmic Number Theory - ANTS 2004*, Lecture Notes in Comput. Sci. **3076**, pp. 169–183, 2004.
10. S. Galbraith. Pairings, Chapter IX of book *Advances in elliptic curve cryptography* edited by I. Blake, G. Seroussi and N. Smart. To be published by Cambridge University Press.
11. S. Galbraith, K. Harrison and D. Soldera. Implementing the Tate pairing. *Algorithmic Number Theory - ANTS V*, Lecture Notes in Comput. Sci. **2369**, pp. 324–337, 2002.
12. T. Izu and T. Takagi. Efficient computations of the Tate pairing for the large MOV degrees. *Information Security and Cryptology - ICISC 2002*, Lecture Notes in Comput. Sci. **2587**, pp. 283–297, 2003.
13. N. Koblitz and A. Menezes. Pairing-based cryptography at high security levels. *Cryptology ePrint Archive*, Reprot **2005/076**.
14. V.S. Miller. The Weil pairing, and its efficient calculation. *J. Cryptology*, Vol. **17**(4): 235–261 (2004).
15. A. Miyaji, M. Nakabayashi and S. Takano. New explicit conditions of elliptic curve traces for FR-reduction. *IEICE T. Fund. Electr.*, **E84-A**(5): 1234–1243 (2001).
16. D. Page, N.P. Smart and F. Vercauteren. A comparison of MNT curves and supersingular curves. *Cryptology ePrint Archive*, Report **2004/165**.
17. M. Scott and P.S.L.M. Barreto. Generating more MNT elliptic curves. *Cryptology ePrint Archive*, Report **2004/058**.
18. J. H. Silverman. *The Arithmetic of Elliptic Curves.* Graduate Texts in Math. Vol. **106**, Springer-Verlag, 1986.