Self-pairings on supersingular elliptic curves with embedding degree *three*

Binglong Chen and Chang-An Zhao

Department of Mathematics, Sun Yat-Sen University, Guangzhou 510275, P.R.China.
mcscbl@mail.sysu.edu.cn
zhaochan3@mail.sysu.edu.cn

Abstract. Self-pairings are a special subclass of pairings and have interesting applications in cryptographic schemes and protocols. In this paper, we explore the computation of the self-pairings on supersingular elliptic curves with embedding degree $k = 3$. We construct a novel self-pairing which has the same Miller loop as the Eta/Ate pairing. However, the proposed self-pairing has a simple final exponentiation. Our results suggest that the proposed self-pairings are more efficient than the other ones on the corresponding curves. We compare the efficiency of self-pairing computations on different curves over large characteristic and estimate that the proposed self-pairings on curves with $k = 3$ require 44% less field multiplications than the fastest ones on curves with $k = 2$ at AES 80-bit security level.

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

1 Introduction

Pairing based cryptography has been one of the most active area in cryptologic research in the past years [7, 23]. This leads to the improvement of mathematical algorithmic foundations of pairings. For the general bilinear pairing $e(P, Q)$ on (hyper-)elliptic curves, many variants of the Tate pairings have been proposed in efficiency [6, 2, 13, 12, 18, 24, 14].

Self-pairings $e(P, P)$ are a special subclass of pairings, which are of vital use in several cryptographic applications, such as on-line/off-line signature scheme of Zhang *et al*. [27] and the designated confirmer signature [26]. Since both input

points are equal in the self-pairings, it is natural to ask whether self-pairings can be computed faster than the general case. By using the distortion maps on supersingular elliptic curves [25, 9], the authors of [28] propose the novel self-pairing with a simple final exponentiation. This idea has been also generalized to the hyperelliptic case [10].

It is known that self-pairings can be constructed on supersingular elliptic curves with distortion maps. Verheul first introduces the notion of distortion maps on supersingular elliptic curve with $k = 3$ [25]. This curve is defined over a finite field $\mathbb{F}_{p^2}$ for p a prime $p \equiv 2 \pmod 3$, and has $p^2 - p + 1$ $\mathbb{F}_{p^2}$-rational points. The general bilinear pairings on this elliptic curve have been studied by Hu *et al.* in [19] and improved by Galbraith *et al.* in [8]. This curve has many merits in performance. Firstly, the Miller loop of the Eta/Ate pairings on this curve can be shortened to a half of that of the reduced Tate pairing. This is better than computing pairings on supersingular curves over large prime fields with $k = 2$. Secondly, the authors of [5] propose a variant Miller's iteration formula which makes the denominator elimination technique available for pairing friendly curves with odd embedding degrees. Finally, for supersingular elliptic curves with $k = 3$ we can generate the suitable parameters which allow the pairings to be computed quickly [8], i.e., the bit length of the Miller loop and the order of the prime field $\mathbb{F}_p$ can be chosen to have a low Hamming weight. Therefore, it is meaningful to consider the self-pairing computation on supersingular curves with $k = 3$.

The self-pairing computation has been investigated on supersingular elliptic curves with even embedding degrees [28]. It should be remarked that the novel self-pairings have been obtained by using distortion maps which are non-trivial automorphisms of these curves simultaneously. However, the distortion map on supersingular elliptic curves with $k = 3$ is not an automorphism of the curve. This leads to the ignorance of this kind of curves in [28]. In this paper, we tackle this problem and propose a new self-pairing with a simple final exponentiation by using distortion maps. Although the structure of the proposed self-pairing is like that of the Tate pairing, the whole results are obtained by employing the Weil pairing. We conclude that the proposed self-pairing is the fastest on supersingular elliptic curves with $k = 3$.

The recent prominent developments of the function field Sieve algorithm on finite fields with small characteristic [17, 16, 11] lead to the weakness of pairings

on supersingular elliptic curves with characteristic 2 or 3. Thus we compare the efficiency of self-pairings on the different curves over large characteristic. Our results indicate that the proposed self-pairing on curves with $k = 3$ can be more efficient than the fastest one on curves with $k = 2$ at AES 80-bit security level.

The remained of this paper is organized as follows. Section 2 gives preliminaries of pairings and supersingular elliptic curves with $k = 3$. The main results are presented in Section 3. Efficiency considerations are given in Section 4. Some conclusions are drawn in Section 5.

2 Mathematical background

In this section we first recall the definitions of the Tate and Weil pairings, and Miller's algorithm to compute them. Then we give some facts about supersingular elliptic curves with $k = 3$.

2.1 Tate pairing

Let $\mathbb{F}_q$ be a finite field with $q = p^m$ elements, where p is a prime. Let E be an elliptic curve defined over $\mathbb{F}_q$, and let P_∞ be the point at infinity. Let r be a prime such that $r \mid \#E(\mathbb{F}_q)$, where $\#E(\mathbb{F}_q)$ denotes the order of the rational point group $E(\mathbb{F}_q)$. Assume that r^2 does not divide $q^k - 1$ and k is greater than 1, where k is the embedding degree with respect to r. We denote by $E[r]$ the r-torsion group of E.

Let $P \in E[r]$ and $R \in E(\mathbb{F}_{q^k})$. Let D_P be a degree zero divisor which is equivalent to $(P) - (P_\infty)$. For every integer i and point P, let $f_{i,P}$ be a rational function such that its divisor $\mathrm{div}(f_{i,P}) = i(P) - ([i]P) - (i-1)(P_\infty)$. In particular, $\mathrm{div}(f_{r,P}) = rD_P$. Let μ_r be the r-th roots of unity in $\mathbb{F}_{q^k}$. Then the reduced Tate pairing [3] is defined as follows

$$e : E[r] \times E(\mathbb{F}_{q^k}) \to \mu_r,$$
$$e(P, R) = f_{r,P}(R)^{\frac{q^k-1}{r}}.$$

Note that $f_{r,P}(R)^{a(q^k-1)/r} = f_{ar,P}(R)^{(q^k-1)/r}$ for any integer a. If points P and R can be restricted to specific subgroups of the r-torsion group $E[r]$, the variants of the reduced Tate pairing can be constructed in efficiency [6, 2, 13, 18, 24, 14].

2.2 Weil pairing

Using the same notation as before, one can make a few slight modifications and then define the Weil pairing. Let k be the minimal positive integer such that $E[r] \subset E(\mathbb{F}_{q^k})$. According to the results in [1], if $r \nmid q-1$ and $(r,q)=1$, then $E[r] \subset E(\mathbb{F}_{q^k})$ if and only if $r|q^k-1$, i.e., the embedding degree for the Weil pairing is equal to the embedding degree for the Tate pairing in this case.

Suppose that $P,\ Q \in E[r]$ and $P \neq Q$. Let D_P and D_Q be two degree zero divisors which are equivalent to $(P)-(P_\infty)$ and $(Q)-(P_\infty)$, respectively. Let $f_{r,P}$ and $f_{r,Q}$ be two rational functions on E with $\mathrm{div}(f_{r,P}) = rD_P$ and $\mathrm{div}(f_{r,Q}) = rD_Q$. Then the Weil pairing [15, 22] is a map

$$\hat{e} : E[r] \times E[r] \to \mu_r,$$
$$\hat{e}(P,Q) = (-1)^r \frac{f_{r,Q}(P)}{f_{r,P}(Q)}.$$

Note that the Weil pairing also plays an essential role in algorithmic foundations of pairings. For example, the pairing variants of the Weil pairing can be obtained [14, 29]. The new self-pairings are proposed by using the symmetric structure of the Weil pairing [28, 10].

2.3 Miller's algorithm

In essence, Miller's algorithm [21, 22] is to compute the evaluation of the rational function $f_{i,P}$ at point R in polynomial time.

For $P_1, P_2 \in E$, we denote by l_{P_1,P_2} the equation of the line through points P_1 and P_2 (if $P_1 = P_2$, then l_{P_1,P_2} is the tangent to the curve E at P_1 or P_2, and if one of P_1 or P_2 is the infinity point, then the l_{P_1,P_2} is a vertical line at the other point). We define v_{P_1} to be the equation of the line between P and P_∞ if P_1 is not equal to P_∞.

Now we restrict P to be a point in $E[r]$. Recall $f_{j,P}$ to be a rational function on the elliptic curve with its divisor $\mathrm{div}(f_{j,P}) = j(P) - ([j]P) - (j-1)(P_\infty)$. Then for $i, j \in Z$, we have

$$\mathrm{div}(f_{i+j,P}) = \mathrm{div}(f_{i,P} f_{j,P} \frac{l_{iP,jP}}{v_{(i+j)P}}).$$

This gives an iteration formula which is useful in Miller's algorithm. For even embedding degrees, the denominator technique can be applied since the evaluation

of $v_{(i+j)P}$ at the corresponding point belongs to a proper subfield of $\mathbb{F}_{q^k}$ [3]. For odd embedding degrees, the authors of [5] propose an efficient iteration formula, i.e.,

$$\mathrm{div}(f_{i+j,P}) = \mathrm{div}(\frac{1}{f_{-i,P}f_{-j,P}l_{-iP,-jP}}).$$

This speeds up the computations of the basic doubling and addition steps in Miller's algorithm on pairing friendly curves with odd embedding degrees. It should be also mentioned that the authors of [20, 8] give another efficient denominator elimination technique if the odd embedding degree is divisible by 3.

Note that all rational functions above are defined up to a non-zero constant. In implementations, one often requires a unique value in finite fields. So we fix a local uniformizer at the infinity point as $t_{P_\infty} = x/y$ on elliptic curves with short Weierstrass form. Following [12] we will assume that all rational functions f are normalized at infinity, i.e., the Laurent expansion of f at the infinity point P_∞ is of the form $f = t_{P_\infty}^i + \cdots$ for some $i \in \mathbb{Z}$. Then the evaluation of the rational functions can be determined uniquely in implementations.

2.4 Supersingular elliptic curves with embedding degree *three*

In this subsection, we will recall the construction of the supersingular elliptic curve with $k = 3$ which has been given in [25]. This curve is useful in pairing implementations and has been considered for general pairings in [19, 8]. Now we mainly investigate the self-pairing computation on this curve.

Let p be a prime with $p \equiv 2 \pmod 3$. Consider the underlying supersingular elliptic curves over $\mathbb{F}_{p^2}$

$$E: \ y^2 = x^3 + \rho^2, \tag{1}$$

where $\rho \in \mathbb{F}_{p^2} \backslash \mathbb{F}_p$ and ρ^2 is not a cube in $\mathbb{F}_{p^2}$. The order of the rational point group $E(\mathbb{F}_{p^2})$ is $p^2 - p + 1$. Let r be a large prime dividing $p^2 - p + 1$ and then the embedding degree for E with respect to r is $k = 3$.

Suppose that β is an element in $\mathbb{F}_{p^6}$ with $\beta^3 = \rho$. Let $a = \rho^{-(2p-1)/3}$ and $b = \rho^{-(p-1)}$. One can define a distortion map ϕ [25] on the curve E as follows.

$$\begin{aligned} &\phi : E \to E, \\ &(x, y) \to (a\beta x^p, by^p). \end{aligned}$$

Note that there exists another distortion map ψ on the curve E

$$\begin{aligned}&\psi : E \to E,\\ &(x, y) \to ((a\beta)^{-p}x^p, by^p).\end{aligned}$$

which satisfies $\psi \circ \phi = \pi_{p^2}$, where π_{p^2} is the well-known Frobenius endomorphism on the curve E. By Lemma 8 of [9], the distortion map ϕ maps the 1-eigenspace of Frobenius to the p^2-eigenspace of Frobenius in $E[r]$. It will be shown that the distortion map ψ also maps the 1-eigenspace of Frobenius to the p^2-eigenspace of Frobenius in $E[r]$ as follows.

Lemma 1. *Let $P \in \mathbb{G}_1 = Ker(\pi_{p^2} - [1]) \cap E[r] = Ker(\hat{\pi}_{p^2} - [p^2]) \cap E[r]$ where $\hat{\pi}_{p^2}$ is the dual of Frobenius endomorphism π_{p^2}. Then $\psi(P) \in \mathbb{G}_2 = Ker(\pi_{p^2} - [p^2]) \cap E[r] = Ker(\hat{\pi}_{p^2} - [1]) \cap E[r]$.*

Proof. Let $P = (x_0, y_0) \in \mathbb{G}_1$ and then $\psi(P) = ((a\beta)^{-p}x_0^p, by_0^p)$. By Lemma 3 of [4], it suffices to show that $tr(\psi(P)) = P_\infty$. Note that

$$\begin{aligned}tr(\psi(P)) &= \psi(P) + \pi_{p^2}(\psi(P)) + \pi_{p^2}^2(\psi(P))\\ &= ((a\beta)^{-p}x_0^p, by_0^p) + ((a\beta)^{-p^3}x_0^p, by_0^p) + ((a\beta)^{-p^5}x_0^p, by_0^p).\end{aligned}$$

The second equality in the above holds because x_0, y_0 and b are contained in $\mathbb{F}_{p^2}$. The three distinct points $\psi(P)$, $\pi_{p^2}(\psi(P))$ and $\pi_{p^2}^2(\psi(P))$ have the same y-coordinate, which implies that they are collinear. It gives that $tr(\psi(P)) = P_\infty$ by the group law of elliptic curves and thus $\psi(P) \in \mathbb{G}_2$. □

3 Self-pairings on supersingular elliptic curves with embedding degree *three*

The main result of this paper is summarized in the following theorem.

Theorem 1. *Let E be the supersingular elliptic curve defined by the equation (1). Let r be a large prime satisfying $r \mid \#E(\mathbb{F}_{p^2}) = p^2 - p + 1$ and $r^2 \nmid (p^6 - 1)$. Let T_i be the integers such that $T_i \equiv (p^2)^i \pmod{r}$ with $i = 1,\ 2$. Then*

$$e_s(P, P) \triangleq f_{T_i,P}(\psi(P))^{3(p+1)(p^3-1)}.$$

is a self-pairing for $P \in \mathbb{G}_1 = Ker(\pi_{p^2} - [1]) \cap E[r]$,

The proof of Theorem 1 is split into the following short lemmas. It follows from Lemma 5 of [12] that the rational function $f_{m,\psi(P)} \circ \psi$ equals $f_{m,P}^{\deg \psi}$ multiplying by a non-zero constant provided that ψ is a purely inseparable map on E. For our purposes, the exact value of the non-zero constant is determined in the following lemma.

Lemma 2. *Let $P \in \mathbb{G}_1 = Ker(\pi_{p^2} - [1]) \cap E[r]$ and m be an integer. Then there exists a non-zero constant γ_m such that*

$$f_{m,\psi(P)} \circ \psi = \gamma_m f_{m,P}^p,$$

where $\gamma_m = (b(a\beta)^p)^m$ if $r|m$ and $\gamma_m = (b(a\beta)^p)^{(m-1)}$ otherwise.

Proof. By definition we have

$$\mathrm{div}(f_{m,\psi(P)}) = m(\psi(P)) - ([m]\psi(P)) - (m-1)(P_\infty).$$

Since the map ψ is purely inseparable of degree p, it follows that

$$(\psi^*)\mathrm{div}(f_{m,\psi(P)}) = pm(P) - p([m]P) - p(m-1)(P_\infty) = \mathrm{div}(f_{m,P}^p).$$

Therefore,

$$f_{m,\psi(P)} \circ \psi = \gamma_m f_{m,P}^p$$

for some non-zero constant γ_m. Let $t_{P_\infty} = x/y$ be the local parameter at infinity for this curve. Assume that the order of the rational function $f_{m,\psi(P)}$ at the infinity point is h. Then $h = -m$ if $r \mid m$ and $h = -(m-1)$ if $r \nmid m$. Since $f_{m,\psi(P)}$ is normalized by assumption, the local expansion of $f_{m,\psi(P)}$ at the infinity point is

$$f_{m,\psi(P)} = t_{P_\infty}^h + \cdots = (x/y)^h + \cdots .$$

As $t_{P_\infty} \circ \psi = (\frac{1}{b(a\beta)^p})(\frac{x}{y})^p$, this implies that the local expansion of $f_{m,\psi(P)} \circ \psi$ at the infinity point is

$$f_{m,\psi(P)} \circ \psi = (\frac{1}{b(a\beta)^p})^h (\frac{x}{y})^{hp} + \cdots .$$

As $f_{m,P}$ is normalized, it follows that $f_{m,P}^p = (x/y)^{hp} + \cdots$. Comparing the expression of $f_{m,\psi(P)} \circ \psi$ with that of $f_{m,P}^p$ gives $\gamma_m = (b(a\beta)^p)^{-h}$ which concludes the proof of Lemma 2. □

We will show that $f_{m,P}(\phi(P))$ can be related to $f_{m,P}(\psi(P))^{p^2}$ in the following Lemma 3. This observation is simple but useful for constructing the new self-pairings.

Lemma 3. *Using the notation defined as previous, we have*

$$f_{m,P}(\phi(P)) = f_{m,P}(\psi(P))^{p^2}.$$

Proof. Note that the rational function $f_{m,P}$ in the function field $\mathbb{F}_{p^2}(E)$ can be written as

$$f_{m,P} = c_0 + c_1 x + c_2 x^2$$

where c_0, c_1 and c_2 are the rational functions over $\mathbb{F}_{p^2}$ in terms of y. Put $P = (x_0, y_0)$ where $x_0, y_0 \in \mathbb{F}_{p^2}$. Then $\psi(P) = ((a\beta)^{-p} x_0^p, by_0^p)$ and $\phi(P) = (a\beta x_0^p, by_0^p)$. By abuse of notation, the valuation of the rational function c_i at the points $\phi(P)$ and $\psi(P)$ can be also denoted by c_i with $i = 0, 1, 2$. It follows that

$$f_{m,P}(\phi(P)) = c_0 + c_1(a\beta x_0^p) + c_2(a\beta x_0^p)^2. \tag{2}$$

On the other hand,

$$f_{m,P}(\psi(P)) = c_0 + c_1(a\beta)^{-p} x_0^p + c_2(a\beta)^{-2p}(x_0^p)^2. \tag{3}$$

Raising to the power p^2 at both sides of (3), we have

$$(f_{m,P}(\psi(P)))^{p^2} = c_0 + c_1(a\beta)^{-p^3} x_0^p + c_2(a\beta)^{-2p^3}(x_0^p)^2. \tag{4}$$

To prove the assertion of this lemma, it suffices to show that $a\beta = (a\beta)^{-p^3}$ by comparing (2) with (4). As $\beta = \rho^{1/3}$ and $\alpha = \rho^{-(2p-1)/3}$, it follows that

$$(\alpha\beta)^{3(p+1)} = (\rho^{-(2p-1)}\rho)^{p+1} = \rho^{-2(p^2-1)} = 1.$$

Note that $p^3 + 1 = (p+1)(p^2 - p + 1)$ and $3 \mid (p^2 - p + 1)$. It follows that $3(p+1) | (p^3 + 1)$ and then $(a\beta)^{p^3+1} = 1$. This completes the proof. □

By combining Lemma 2 and 3, we can establish the relationships between $f_{m,\psi(P)}(P)$ and $f_{m,P}(\psi(P))$.

Lemma 4. *Using the notation defined as previous, we have*

$$f_{m,\psi(P)}(P) = \gamma_m f_{m,P}(\psi(P))^{p^3},$$

where $\gamma_m = (b(a\beta)^p)^m$ *if* $r|m$ *and* $\gamma_m = (b(a\beta)^p)^{(m-1)}$ *otherwise.*

Proof. Now we consider the evaluation of $f_{m,\psi(P)}$ at point P. Note that $\langle P\rangle \neq \langle\psi(P)\rangle$ and P is not a 2-torsion point. Thus $f_{m,\psi(P)}(P)$ makes sense. Since $P \in E(\mathbb{F}_{p^2}) = Ker(\pi_{p^2} - [1])$, we obtain

$$f_{m,\psi(P)}(P) = (f_{m,\psi(P)} \circ \pi_{p^2})(P) = (f_{m,\psi(P)} \circ \psi \circ \phi)(P).$$

It follows from Lemma 2 that

$$(f_{m,\psi(P)} \circ \psi \circ \phi)(P) = (f_{m,\psi(P)} \circ \psi)(\phi(P)) = \gamma_m(f_{m,P}(\phi(P)))^p.$$

Therefore,

$$f_{m,\psi(P)}(P) = \gamma_m(f_{m,P}(\phi(P)))^p.$$

By Lemma 3, we have

$$f_{m,P}(\phi(P)) = (f_{m,P}(\psi(P)))^{p^2}.$$

It also gives that

$$f_{m,\psi(P)}(P) = \gamma_m(f_{m,P}(\psi(P)))^{p^3}.$$

□

Proof (of Theorem 1). Without loss of generality, we only prove the case $T = T_1$. Since $r^2 \nmid (T^3 - 1)$, it follows that the pairing $\hat{e}(P, \psi(P))^{(T^3-1)/r}$ keeps non-degeneracy. It is obvious from the definition of the Weil pairing that

$$\hat{e}(P, \psi(P))^{(T^3-1)/r} = (-1)^{(T^3-1)} \frac{f_{T^3-1,\psi(P)}(P)}{f_{T^3-1,P}(\psi(P))} = (-1)^{(T^3-1)} \frac{f_{T^3,\psi(P)}(P)}{f_{T^3,P}(\psi(P))}.$$

It follows from Lemma 4 that

$$f_{T^3,\psi(P)}(P) = \gamma_m(f_{T^3,P}(\psi(P)))^{p^3},$$

where $\gamma_m = (b(a\beta)^p)^{(T^3-1)p}$ and $m = T^3$. Hence

$$\hat{e}(P, \psi(P))^{(T^3-1)/r} = (-1)^{T^3-1}\gamma_m f_{T^3,P}(\psi(P))^{p^3-1}. \tag{5}$$

Note that $P \in \mathbb{G}_1 = E[r] \cap Ker(\hat{\pi}_{p^2} - [p^2])$ and $\psi(P) \in \mathbb{G}_2 = E[r] \cap Ker(\hat{\pi}_{p^2} - [1])$ by Lemma 1. Due to the discussion in Section 3.2 of [13] (or see the proof of Theorem 1 in [2]), we see that

$$f_{T^3,P}(\psi(P)) = (f_{T,P}(\psi(P)))^{T^2+Tp^2+p^4}. \tag{6}$$

Substituting (6) into the equation (5), we have

$$\hat{e}(P,\psi(P))^{(T^3-1)/r} = (-1)^{T^3-1}\gamma_m(f_{T,P}(\psi(P)))^{(p^3-1)c}, \tag{7}$$

where $c = T^2 + Tp^2 + p^4 \equiv 3p^4 \pmod{r}$. As $b^{(p+1)} = 1$, $(a\beta)^{3(p+1)} = 1$ and $p+1 \equiv 0 \pmod{2}$, then $((-1)\cdot\gamma_m)^{3(p+1)} = 1$. Since r does not divide $3(p+1)$, both sides of (7) can be raised to the power $3(p+1)$ and the left hand side still keeps non-degeneracy. Therefore,

$$\hat{e}(P,\psi(P))^{3(p+1)(T^3-1)/r} = (f_{T,P}(\psi(P)))^{3(p+1)(p^3-1)c}. \tag{8}$$

Following the argument of Theorem 2 in [14], we can ignore the exponent c from the final exponentiation. In fact, it is seen that

$$f_{r^2,P}(\psi(P))^{3(p+1)(p^3-1)} = \hat{e}(P,\psi(P))^{r\cdot 3(p+1)} = 1.$$

By the Chinese Remainder Theorem, we can find $T' = T + \tau r^2$ for some integer τ such that $T' \equiv 0 \pmod{r'}$ for all prime numbers $r' \neq r$ dividing $p^6 - 1$. Then $c' = {T'}^2 + T'p^2 + p^4 \equiv 3p^4 \pmod{r}$ and $(c', p^6-1) = 1$. By replacing T by T' in Equation (8), we obtain

$$\hat{e}(P,\psi(P))^{3(p+1)({T'}^3-1)/r} = (f_{T',P}(\psi(P)))^{3(p+1)(p^3-1)c'}. \tag{9}$$

Let $\bar{c'}$ be an integer $\bar{c'}c' \equiv 1 \pmod{p^6-1}$. Raising Equation (9) to the power $\bar{c'}$ we get

$$\begin{aligned}\hat{e}(P,\psi(P))^{3\bar{c'}(p+1)(T^3-1)/r} &= f_{T+\tau r^2,P}(\psi(P))^{3(p+1)(p^3-1)} \\ &= f_{T,P}(\psi(P))^{3(p+1)(p^3-1)} f_{\tau r^2,P}(\psi(P))^{3(p+1)(p^3-1)} \\ &= f_{T,P}(\psi(P))^{3(p+1)(p^3-1)}.\end{aligned}$$

It follows that

$$e_s(P,P) \triangleq f_{T,P}(\psi(P))^{3(p+1)(p^3-1)}$$

is a well-defined self-pairing. This completes the whole proof of Theorem 1. □

Remark 1. In implementations, the parameter T_1 can be chosen to have a low Hamming weight and be possibly as small as $r^{1/\varphi(k)}$ by Algorithm 1 [8]. This also shows that the parameter T_1 is optimal in efficiency.

Remark 2. The main advantage of the proposed self-pairings on curves with $k = 3$ is that the final exponentiation $3(p+1)(p^3-1)$ has a simple expression

in terms of p. Note that the final exponentiation for the reduced Tate pairing or its variants is

$$(p^6 - 1)/r = (p^3 - 1)(p + 1)(l_0 + l_1 p),$$

where l_0 and l_1 are two small positive integers. We will also give efficiency comparisons between the proposed self-pairings and the self-pairings based on the Eta/Ate pairings in later sections.

Remark 3. It should be remarked that the final exponentiation for the self-pairings on E_2 of [28] is $6(p-1)$, not $4(p-1)$. Here we give a brief explanation. Let ϕ be the distortion map on E_2 of [28], i.e. $\phi : E_2 \to E_2 : (x, y) \to (\beta x, y)$ where $\beta^3 = 1$. Then $t_{P_\infty} \circ \phi = \beta x/y$. For eliminating the non-zero constant in terms of β, the final exponentiation should be divided by 3. The authors of [10] have also noticed this.

4 Efficiency comparison

Now the performance of the proposed self-pairings is considered in this section. We first analyze the efficiency of the different self-pairings on the supersingular elliptic curves with $k = 3$. Then we compare the efficiency of the self-pairings on elliptic curves with $k = 2$ and $k = 3$ at AES 80-bit security level.

It is obvious that another choice for implementing the self-pairings on supersingular curves with $k = 3$ is the Eta/Ate pairing $f_{T_1,P}(\psi(P))^{(p^6-1)/r}$. The final exponentiation of the proposed self-pairings equals $3(p + 1)(p^3 - 1)$, and that of the Eta/Ate pairing equals $(p^6 - 1)/r$. After computing $(p^3 - 1)(p + 1)$, one cube is required for the proposed self-pairings. This is faster than computing the exponent $(p^2 - p + 1)/r$ for the self-pairings based on the Eta/Ate pairing. Since the Miller loop step in both cases is identical, we conclude that the proposed self-pairings are faster than the previous fastest self-pairings on the curves with $k = 3$.

Now we compare the efficiency of self-pairings on supersingular elliptic curves over large different prime fields at AES 80-bit security level since discrete logarithms in small characteristic are more vulnerable than that in large characteristic [16]. By Algorithm 1 of [8], we can generate the corresponding curves for efficiency comparison.

We denote by M_i, S_i and I_i the cost of multiplication, squaring, and inversion in $\mathbb{F}_{p^i}$ for $i = 1, 2, 6$. For purposes of comparison, the cost of these operations

should be expressed in terms of the multiplication in the base prime field. Let $S_1 = M_1$, $I_1 = 10M_1$, $S_2 = 2M_1$, $M_2 = 3M_1$, $I_2 = 14M_1$, $S_6 = 11M_1$, $M_6 = 15M_1$ and $I_6 = 53M_1$ as assumed in [13, 8].

Let $\mathbb{F}_{p_1^2}$ be a finite field with p_1^2 elements where p_1 is a 192-bit prime number. We consider self-pairing computations on supersingular elliptic curve E over $\mathbb{F}_{p_1^2}$ with $k = 3$. let M_1 denote the cost of a multiplication in $\mathbb{F}_{p_1}$. Since the corresponding parameters can be generated with a low Hamming weight, we will count the doubling steps in the Miller loop roughly. the cost of each doubling step in projective coordinates is $7S_2+(5+3\cdot 3)M_2+2S_6+M_6 = 93M_1$ according to [5]. Assume that the bit length of the parameter T_1 equals 86. Then the total cost for the Miller loop is $85 \cdot 93 = 7905M_1$. the cost for computing the exponent $3(p+1)(p^3-1)$ equals $109M_1$ provided that we neglect the cost of the Frobenius map in finite fields. Thus the total cost for computing the self-pairings is $8014M_1$.

Let $\mathbb{F}_{p_2}$ be a finite field with p_2 elements where p_2 is a 512-bit prime number. We consider the computation of self-pairings on the curve E_1 in [28] with $k = 2$. let $M_1^{'}$ denote the cost of a multiplication in $\mathbb{F}_{p_2}$ where the bit-length of p_2 is 512. For comparison purposes the cost of a multiplication in $\mathbb{F}_{p_2}$ should be expressed in terms of the number of $\mathbb{F}_{p_1}$ multiplications. Using basic Karatsuba trick, we estimate $1M_1^{'} = (512/192)^{1.58} \approx 4.7M_1$. the cost of each doubling step in projective coordinates is $19M_1^{'}$ according to [5]. Assume that the bit length of the order of the corresponding subgroup equals 160. Then the total cost for the Miller loop is $159 \cdot 19 = 3021M_1^{'} \approx 14198M_1$. the cost for computing the exponent $4(p-1)$ equals $21M_1^{'} \approx 99M_1$. Thus the total cost for computing the self-pairings proposed in [28] is $14297M_1$.

We summarize the above estimations into Table 1. We can see that the proposed self-pairings on supersingular curves with $k = 3$ are more efficient than that of [28] on supersingular curves with $k = 2$.

Table 1. Cost of self-pairing computations on different curves

Curves	Size of p	Cost of Miller Loop	Cost of Final Exponentiation	Total Cost
$E(\mathbb{F}_{p_1^2})$ $k = 3$	192	$7905M_1$	$109M_1$	$8014M_1$
$E'(\mathbb{F}_{p_2})$ $k = 2$	512	$14198M_1$	$99M_1$	$14297M_1$

5 Conclusion

In this paper, we showed how to speed up the computation of the self-pairings on supersingular elliptic curves with $k = 3$. We demonstrated that the proposed self-pairings can be the fastest on supersingular curve with $k = 3$. We indicated that the proposed self-pairings on curves with $k = 3$ require 44% less field multiplications than the fastest ones on curves with $k = 2$ at AES 80-bit security level.

References

1. Balasubramanian, R., Koblitz, N.: The improbability that an elliptic curve has subexponential discrete log problem under the menezes-okamoto-vanstone algorithm. Journal of Cryptology 11(2), 141–145 (1998)
2. Barreto, P.S.L.M., Galbraith, S.D., O'Eigeartaigh, C., Scott, M.: Efficient pairing computation on supersingular abelian varieties. Des. Codes Cryptography 42(3), 239–271. (2007)
3. Barreto, P., Kim, H., Lynn, B., Scott, M.: Efficient algorithms for pairing-based cryptosystems. In: Yung, M. (ed.) Advances in Cryptology - CRYPTO 2002, Lecture Notes in Computer Science, vol. 2442, pp. 354–369. Springer Berlin / Heidelberg (2002)
4. Barreto, P.S., Lynn, B., Scott, M.: On the selection of pairing-friendly groups. In: Matsui, M., Zuccherato, R. (eds.) Selected Areas in Cryptography, Lecture Notes in Computer Science, vol. 3006, pp. 17–25. Springer Berlin Heidelberg (2004)
5. Boxall, J., Mrabet, N., Laguillaumie, F., Le, D.P.: A variant of miller's formula and algorithm. In: Joye, M., Miyaji, A., Otsuka, A. (eds.) Pairing-Based Cryptography - Pairing 2010, Lecture Notes in Computer Science, vol. 6487, pp. 417–434. Springer Berlin Heidelberg (2010)
6. Duursma, I., Lee, H.S.: Tate pairing implementation for hyperelliptic curves $y^2 = x^p - x + d$. In: Laih, C.S. (ed.) Advances in Cryptology - ASIACRYPT 2003, Lecture Notes in Computer Science, vol. 2894, pp. 111–123. Springer Berlin / Heidelberg (2003)
7. Galbraith, S.D.: Pairings-Advances in Elliptic Curve Cryptography. Cambridge University Press (2005)
8. Galbraith, S.D., Lin, X., Mireles Morales, D.J.: Pairings on hyperelliptic curves with a real model. In: Galbraith, S., Paterson, K. (eds.) Pairing-Based Cryptography - Pairing 2008, Lecture Notes in Computer Science, vol. 5209, pp. 265–281. Springer Berlin Heidelberg (2008)

9. Galbraith, S.D., Verheul, E.R.: An analysis of the vector decomposition problem. In: Cramer, R. (ed.) Public Key Cryptography - PKC 2008, Lecture Notes in Computer Science, vol. 4939, pp. 308–327. Springer Berlin Heidelberg (2008)
10. Galbraith, S.D., Zhao, C.A.: Self-pairings on hyperelliptic curves. Preprint, to appear in J. Math. Crypt. (2012)
11. Göloğlu, F., Granger, R., McGuire, G., Zumbrägel, J.: On the function field sieve and the impact of higher splitting probabilities. In: Canetti, R., Garay, J. (eds.) Advances in Cryptology - CRYPTO 2013, Lecture Notes in Computer Science, vol. 8043, pp. 109–128. Springer Berlin Heidelberg (2013)
12. Granger, R., Hess, F., Oyono, R., Theriault, N., Vercauteren, F.: Ate pairing on hyperelliptic curves. In: Naor, M. (ed.) Advances in Cryptology - EUROCRYPT 2007, Lecture Notes in Computer Science, vol. 4515, pp. 430–447. Springer Berlin / Heidelberg (2007)
13. Hess, F., Smart, N., Vercauteren, F.: The eta pairing revisited. IEEE Transactions on Information Theory 52, 4595–4602 (Oct, 2006)
14. Hess, F.: Pairing lattices. In: Galbraith, S., Paterson, K. (eds.) Pairing-Based Cryptography-Pairing 2008, Lecture Notes in Computer Science, vol. 5209, pp. 18–38. Springer Berlin / Heidelberg (2008)
15. Howe, E.W.: The Weil pairing and the Hilbert symbol. Mathematische Annalen 305, 387–392 (1996)
16. Joux, A.: A new index calculus algorithm with complexity $L(1/4 + o(1))$ in very small characteristic. Cryptology ePrint Archive, Report 2013/095 (2013)
17. Joux, A., Vitse, V.: Cover and decomposition index calculus on elliptic curves made practical. In: Advances in Cryptology–EUROCRYPT 2012, pp. 9–26. Springer (2012)
18. Lee, E., Lee, H.S., Park, C.M.: Efficient and generalized pairing computation on abelian varieties. IEEE Transactions on Information Theory 55(4), 1793–1803 (2009)
19. Lei, H., Jun-Wu, D., Ding-Yi, P.: An implementation of cryptosystems based on tate pairing. Journal of Computer Science and Technology 20(2), 264 – 269 (2005)
20. Lin, X., Zhao, C.A., Zhang, F., Wang, Y.: Computing the ate pairing on elliptic curves with embedding degree k = 9. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences 91(9), 2387–2393 (2008)
21. Miller, V.S.: Short programs for functions on curves (Aug 26, 1986), http://crypto.stanford.edu/miller/miller.ps.
22. Miller, V.S.: The Weil pairing, and its efficient calculation. J. Cryptology 17(4), 235–261 (2004)
23. Paterson, K.G.: Cryptography from Pairings - Advances in Elliptic Curve Cryptography. Cambridge University Press (2005)

24. Vercauteren, F.: Optimal pairings. IEEE Transactions on Information Theory 56(1), 455–461 (2010)
25. Verheul, E.: Evidence that XTR is more secure than supersingular elliptic curve cryptosystems. In: Pfitzmann, B. (ed.) Advances in Cryptology - EUROCRYPT 2001, Lecture Notes in Computer Science, vol. 2045, pp. 195–210. Springer Berlin / Heidelberg (2001)
26. Zhang, F., Chen, X., Wei, B.: Efficient designated confirmer signature from bilinear pairings. In: Proceedings of the 2008 ACM symposium on Information, computer and communications security. pp. 363–368. ASIACCS '08, ACM (2008)
27. Zhang, F., Chen, X., Susilo, W., Mu, Y.: A new signature scheme without random oracles from bilinear pairings. In: Nguyen, P. (ed.) Progress in Cryptology - VIETCRYPT 2006, Lecture Notes in Computer Science, vol. 4341, pp. 67–80. Springer Berlin / Heidelberg (2006)
28. Zhao, C.A., Zhang, F., Xie, D.: Faster computation of self-pairings. IEEE Transactions on Information Theory 58(5), 3266 –3272 (2012)
29. Zhao, C., Xie, D., Zhang, F., Zhang, J., Chen, B.L.: Computing bilinear pairings on elliptic curves with automorphisms. Des. Codes Cryptography 58(1), 35–44 (2011)