Self-pairings on Hyperelliptic Curves

Steven D. Galbraith[1], Chang-An Zhao[2]

[1] Mathematics Department, University of Auckland,
Private Bag 92019, Auckland 1142, New Zealand
[2] School of Computer Science and Educational Software,
Guangzhou University, Guangzhou 510006, P.R. China
S.Galbraith@math.auckland.ac.nz
changanzhao@gzhu.edu.cn

Abstract. A self-pairing is a pairing computation where both inputs are the same group element. Self-pairings are used in some cryptographic schemes and protocols. In this paper, we show how to compute the Tate-Lichtenbaum pairing $\langle D, \phi(D)\rangle$ on a curve more efficiently than the general case. The speedup is obtained by requiring a simpler final exponentiation. We also discuss how to use this pairing in cryptographic applications.

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

1 Introduction

A pairing is a non-degenerate bilinear map

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \mapsto \mathbb{G}_T$$

where $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ are cyclic groups of prime order r (the first two are usually written additively, and the third multiplicatively). Such groups are found from elliptic or hyperelliptic curves and the pairing is usually the Tate-Lichtenbaum pairing or one of its variants. Pairings have found many applications in cryptography.

This paper restricts to the case $\mathbb{G}_2 = \mathbb{G}_1$, which is usually implemented using supersingular curves and distortion maps. The goal of the paper is to give fast methods for computing $e(P, P)$, in other words, for computing the Tate-Lichtenbaum pairing in the special case when both points are equal. We call this special case a "self-pairing". For cryptographic purposes, the self-pairing should be non-degenerate, i.e., for all non-zero $P \in \mathbb{G}$ we have $e(P, P) \neq 1_T \in \mathbb{G}_T$.

Several cryptographic applications involve computing pairings in the form $e(P, P)$. For example, on-line/off-line signature scheme of Zhang et al [15] (we discuss this scheme in Section 6) and the designated confirmer signature [16].

It is natural to hope that the case $e(P, P)$ might be simpler to compute than the general case $e(P, Q)$. Our result, which may be surprising, is that the final

exponentiation can be simplified in this case. This extends the previous work of Zhao, Zhang and Xie [17].

There has been a lot of work on efficient implementations of the general bilinear pairing $e(P, Q)$. Motivated by the idea of Miller loop shortening [2], many optimizations have been proposed [6, 9, 14, 7]. On the other hand, pairings on hyperelliptic curves have been also investigated. Some excellent surveys can be found in [3, 1]. It should be remarked that the Eta and Ate pairings on hyperelliptic curves have been also presented in [2] and [5] respectively. However, there is little work on the performance of self-pairings [12, 17].

In this paper, we study self-pairing computation on curves with a single point at infinity. Since we need a distortion map ϕ, we restrict to supersingular curves. Our pairing is the twisted Tate-Lichtenbaum pairing $\tau(P, \phi(Q))$. We instantiate our general result with supersingular hyperelliptic curves of genus two over large prime fields and finite fields with even characteristic.

The remainder of this paper is structured as follows. In Section 2, we provide some fundamental definitions. Section 3 presents the main result. Section 4 and Section 5 show how the main result can be achieved using hyperelliptic curves over large prime fields and finite fields with even characteristic respectively. In Section 6, we show how the pairings can be used in a real protocol, and we discuss the efficiency in comparison with other methods.

2 Preliminaries

In this section, we briefly recall the arithmetic on hyperelliptic curves and the definition of the Tate-Lichtenbaum and Weil pairings.

Let C be a nonsingular curve of genus g defined over a finite field $\mathbb{F}_q$ with $q = p^n$ elements. In the remainder of the paper, we will assume that C has a unique point ∞ at infinity. Our concrete examples will be hyperelliptic curves with affine part given by

$$y^2 + h(x)y = f(x)$$

where $h, f \in \mathbb{F}_q[x]$, $\deg(h) \leq g$, f monic and $\deg(f) = 2g + 1$.

For any algebraic extension K of $\mathbb{F}_q$, denote by $C(K) := \{(x, y) \in K \times K \mid y^2 + h(x)y = f(x)\} \bigcup \{\infty\}$, the set of $K-$rational points on C. Although the set $C(K)$ for $g \geq 2$ does not form a group, we can embed C into an abelian variety of dimension g called the Jacobian of C and denoted by J_C. As usual, we will represent elements of $J_C(K)$ by elements of the divisor class group of degree 0 divisors $Div_C^0(K)/Prin_C(K)$.

2.1 The Tate-Lichtenbaum and Weil Pairings

Let r be a prime with $r \mid \#J_C(\mathbb{F}_q)$ and $\gcd(r, q) = 1$ and let k be the smallest integer such that $r \mid (q^k - 1)$, then k is called the embedding degree with respect to r. Note that this implies that the r-th roots of unity μ_r are contained in $\mathbb{F}_{q^k}$ and in no strictly smaller extension of $\mathbb{F}_q$. Note that $r > k$, since k is the order

of q modulo r and hence $k \mid (r-1)$ holds. Denote by $J_C(\mathbb{F}_{q^k})[r]$ the r-torsion points on J_C defined over $\mathbb{F}_{q^k}$.

For $D_1 \in J_C(\mathbb{F}_{q^k})[r]$, the divisor rD_1 is linearly equivalent to zero, hence there is some rational function whose divisor is rD_1, namely the Miller function f_{r,D_1} [10, 11]. Let D_2 be a divisor class, with representative $D_2 = \Sigma_P \mathrm{ord}_P D_2(P)$ having support disjoint from D_1. We define a pairing called the Tate-Lichtenbaum pairing as follows:

$$J_C(\mathbb{F}_{q^k})[r] \times J_C(\mathbb{F}_{q^k})/rJ_C(\mathbb{F}_{q^k}) \to \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r;$$
$$(D_1, D_2) \mapsto f_{r,D_1}(D_2) = \prod_P f_{r,D_1}(P)^{\mathrm{ord}_P D_2}.$$

This pairing is bilinear, non-degenerate and the result is independent of the choice of representatives of the divisor classes.

Note that another way to compute $f(P)$ when f is non-zero and defined at P is as the leading coefficient of a series expansion of f with respect to a local uniformizer of the curve at P.

If the Miller function f_{r,D_1} is properly normalised [5], one can compute $f_{r,D_1}(D_2)$ as $f_{r,D_1}(\epsilon(D_2))$ where $\epsilon(D_2)$ is the effective part of the unique reduced divisor in the class of D_2. All Miller functions will be normalised in the remainder of the paper.

For cryptographic applications, one will require a unique pairing value in the group $\mu_r \subseteq \mathbb{F}_{q^k}$ of r-th roots of unity. Thus one can define the reduced Tate-Lichtenbaum pairing as

$$\tau(D_1, D_2) = f_{r,D_1}(D_2)^{\frac{(q^k-1)}{r}} = f_{r,D_1}(\epsilon(D_2))^{\frac{(q^k-1)}{r}}.$$

For our proof we need to use the Weil pairing. The crucial feature of the Weil pairing is that the pairing value already lies in $\mu_r \subset \mathbb{F}_{q^k}^*$ and so no final exponentiation is required. Recall that the Weil pairing is a non-degenerate and bilinear map of the form

$$e_r : J_C(\mathbb{F}_{q^k})[r] \times J_C(\mathbb{F}_{q^k})[r] \to \mu_r.$$

Howe [8] has proved that one may compute the Weil pairing as follows. Let $D_1,\ D_2 \in J_C(\mathbb{F}_{q^k})[r]$ be degree zero divisors (representing divisor classes). Howe's result does not require the supports of D_1 and D_2 to be disjoint. Let f_1 and f_2 be functions such that $rD_1 = \mathrm{div}(f_1)$ and $rD_2 = \mathrm{div}(f_2)$. Then

$$e_r(D_1, D_2) = (-1)^{r \sum_{P \in C} \mathrm{ord}_P(D_1)\mathrm{ord}_P(D_2)} \frac{f_{r,D_2}(D_1)}{f_{r,D_1}(D_2)}.$$

Lemma 1. *Let $D_1, D_2 \in J_C(\mathbb{F}_{q^k})[r]$ be degree zero divisors and let f_1 and f_2 be normalised functions such that $rD_1 = div(f_1)$ and $rD_2 = div(f_2)$. For $i = 1, 2$ denote by $\epsilon(D_i)$ the effective part of D_i and d_i its degree, so that $D_i = \epsilon(D_i) - d_i(\infty)$. Suppose that the supports of $\epsilon(D_1)$ and $\epsilon(D_2)$ are disjoint. Then*

$$e_r(D_1, D_2) = (-1)^{rd_1d_2} \frac{f_{r,D_2}(\epsilon(D_1))}{f_{r,D_1}(\epsilon(D_2))}.$$

Proof. We note that

$$(-1)^{rd_1d_2}e_r(D_1,D_2)=\frac{f_2(D_1)}{f_1(D_2)}=\frac{f_2(\epsilon(D_1))}{f_1(\epsilon(D_2))}\left(\frac{f_1^{d_2}}{f_2^{d_1}}\right)(\infty).$$

Since the leading term of the series expansion at infinity of the function $f_1^{d_2}/f_2^{d_1}$ is one, the result follows.

3 Main Results

We now give our main result, which is that one can simplify the final exponentiation of the Tate-Lichtenbaum pairing and still get a value in μ_r, in the case of self-pairings. An interesting feature of the proof is that it uses the Weil pairing, but the result itself is about the Tate-Lichtenbaum pairing.

Theorem 1. *Let C be a curve over $\mathbb{F}_q$. Let r be a large prime such that $r \mid \#J_C(\mathbb{F}_q)$. Let $k=2d$ be the embedding degree with respect to r. Let $\sigma(x)=x^{q^d}$ be the q^d-power Frobenius map (i.e., σ generates $Gal(\mathbb{F}_{q^k}/\mathbb{F}_{q^d})$). Suppose that $\phi \in Aut(C)$ satisfies*

1. *$\tau(D,\phi(D)) \neq 1$ where $D \in J_C(\mathbb{F}_q)[r]$ is non-zero,*
2. *$\sigma(\phi)=\hat{\phi}=\phi^{-1}$ and $\sigma(\hat{\phi})=\phi$, where $\hat{\phi}\circ\phi=\phi\circ\hat{\phi}=[1]$.*

Then $f_{r,D}(\epsilon(\phi(D)))^{2(q^d-1)} \in \mu_r$.

Proof. According to the definition of the Weil pairing, we have (here we are actually using the inverse of the Weil pairing, which is more suitable for our application)

$$(-1)^{r\deg(\epsilon(D))\deg(\epsilon(\phi(D)))}\frac{f_{r,D}(\epsilon(\phi(D)))}{f_{r,\phi(D)}(\epsilon(D))} \in \mu_r.$$

Note that

$$\mathrm{div}(f_{r,D}\circ\hat{\phi})=\mathrm{div}(\hat{\phi}^*(f_{r,D}))=\hat{\phi}^*(rD)=r\phi(D)=\mathrm{div}(f_{r,\phi(D)}).$$

It follows that

$$f_{r,\phi(D)}(\epsilon(D))=f_{r,D}(\epsilon(\hat{\phi}(D))).$$

By condition (2) and $f_{r,D} \in \mathbb{F}_q(C)$ where $\mathbb{F}_q(C)$ is the algebraic function field of C over $\mathbb{F}_q$, we get

$$\sigma\Big(f_{r,D}(\epsilon(\phi(D)))\Big)=f_{r,D}(\epsilon(\sigma(\phi)(D)))=f_{r,D}(\epsilon(\hat{\phi}(D)))$$

and

$$\sigma\Big(f_{r,D}(\epsilon(\hat{\phi}(D)))\Big)=f_{r,D}(\epsilon(\sigma(\hat{\phi})(D)))=f_{r,D}(\epsilon(\phi(D))).$$

This implies that

$$\sigma\Big(f_{r,D}(\epsilon(\phi(D)))f_{r,D}(\epsilon(\hat{\phi}(D)))\Big)=f_{r,D}(\epsilon(\phi(D)))f_{r,D}(\epsilon(\hat{\phi}(D))).$$

That is,

$$\left(f_{r,D}(\epsilon(\phi(D)))f_{r,D}(\epsilon(\hat{\phi}(D)))\right)^{q^d-1} = 1.$$

Therefore,

$$\left(f_{r,D}(\epsilon(\hat{\phi}(D)))\right)^{q^d-1} = \left(1/f_{r,D}(\epsilon(\phi(D)))\right)^{q^d-1}.$$

Note that if the characteristic of $\mathbb{F}_q$ is odd then q^d-1 is even, this gives $(-1)^{q^d-1} = 1$; if the characteristic of $\mathbb{F}_q$ is even, the fact that $-1 = 1$ also gives $(-1)^{q^d-1} = 1$. By raising the inverse of the Weil pairing to the power q^d-1, we get

$$\left((-1)^{r\deg(\epsilon(D))^2}\frac{f_{r,D}(\epsilon(\phi(D)))}{f_{r,\phi(D)}(\epsilon(D))}\right)^{q^d-1} = f_{r,D}(\epsilon(\phi(D)))^{2(q^d-1)} \in \mu_r.$$

This completes the proof of Theorem 1.

The main achievement of this result is to replace the usual Tate-Lichtenbaum final exponentation, to the power $(q^d-1)(q^d+1)/r$, with the final exponentiation to the power $2(q^d-1)$. Note that raising to the power $2(q^d-1)$ is simply one action of q^d-power Frobenius (which is applying a linear map), one inversion, one multiplication, and one squaring (all in $\mathbb{F}_{q^k}$). In contrast, the $(q^d+1)/r$ term in the usual final exponentiation may require a very large number of field operations, especially if r is small compared with q^d.

4 Hyperelliptic curves over Large Prime Fields

We first show how the self-pairing can be computed on the curve defined by the equation

$$C : y^2 = x^5 + a,\ a \in \mathbb{F}_p^*,\ p \equiv 2, 3 \pmod 5.$$

It is easy to see that the genus of the hyperelliptic curve is two. Although the case $g = 2$ is considered here, we should point out that our result also applies to the curves $y^2 = x^{2g+1} + a$ over $\mathbb{F}_p$ with genus g.

The order of Jacobian of the hyperelliptic curve C is p^2+1. Note that this curve is supersingular and its embedding degree is $k = 4$. There exists an automorphism ϕ of C defined by $\phi(x, y) = (\zeta x, y)$ where $\zeta \in \mathbb{F}_{p^4} \setminus \mathbb{F}_p$ is a primitive 5-th root of unity. Let $D \in J_C(\mathbb{F}_q)[r]$. The automorphism ϕ induces an efficient automorphism on the Jacobian, which with the customary abuse of notation we also call ϕ:

$$\begin{gathered}\phi : [x^2 + u_1x + u_0, v_1x + v_0] \mapsto [x^2 + \zeta u_1 x + \zeta^2 u_0, \zeta^4 v_1 x + v_0] \\ [x + u_0, v_0] \mapsto [x + \zeta u_0, v_0] \\ \infty \mapsto \infty.\end{gathered}$$

There exists another automorphism $\hat{\phi} : C \to C$ defined by $\phi(x, y) = (\zeta^4 x, y)$. Note that $\hat{\phi} \circ \phi$ is the identity on C. Similarly, this automorphism also induces an efficient automorphism on the Jacobian as follows:

$$\begin{aligned}\hat{\phi} : [x^2 + u_1 x + u_0, v_1 x + v_0] &\mapsto [x^2 + \zeta^4 u_1 x + \zeta^3 u_0, \zeta v_1 x + v_0] \\ [x + u_0, v_0] &\mapsto [x + \zeta^4 u_0, v_0] \\ \infty &\mapsto \infty.\end{aligned}$$

It is easy to check $\phi \circ \hat{\phi} = \hat{\phi} \circ \phi = [1]$ on $J_C(\mathbb{F}_{p^k})$.

Lemma 2. *With notation as above, condition (1) is satisfied.*

Proof. According to Proposition 4.8 of [4], there exists a distortion map of the form $\pi_p^i \phi^j$ where π_p is the p-power Frobenius map and $0 \leq i, j \leq 3$. Since D is in $J_C(\mathbb{F}_p)$, then $\pi_p^i \phi^j(D) = \phi^{j'}$ for some $0 \leq j' \leq 3$. Assume that $\tau(D, \phi(D)) = 1$ for some non-zero D. It follows from Galois theory that $\tau(D, \pi_p^i \phi^j(D)) = 1$ with $0 \leq i, j \leq 3$ which leads to a contradiction to Proposition 4.8 of [4]. Therefore, $\tau(D, \phi(D)) \neq 1$, i.e., condition (1) is satisfied for ϕ.

Note that one can also obtain this result using Theorem 4 of Takashima [13].

Lemma 3. *With notation as above, condition (2) is satisfied.*

Proof. Let $D = [x^2 + u_1 x + u_0, v_1 x + v_0] \in J_C(\mathbb{F}_q)[r]$ in Mumford representation. Then $\phi(D) = [x^2 + \zeta u_1 x + \zeta^2 u_0, \zeta^4 v_1 x + v_0]$ and $\hat{\phi}(D) = [x^2 + \zeta^4 u_1 x + \zeta^3 u_0, \zeta v_1 x + v_0]$. Let σ be the generator in the Galois group $Gal(\mathbb{F}_{p^4}/\mathbb{F}_{p^2})$. Since $p^2 \equiv 4 \pmod 5$ and the order of ζ is 5, it follows that $\sigma(\zeta) = \zeta^4$. This implies that

$$\begin{aligned}\sigma(\phi(D)) &= [x^2 + \zeta^4 u_1 x + (\zeta^2)^4 u_0, (\zeta^4)^4 v_1 x + v_0] \\ &= [x^2 + \zeta^4 u_1 x + \zeta^3 u_0, \zeta v_1 x + v_0] \\ &= \hat{\phi}(D)\end{aligned}$$

and

$$\begin{aligned}\sigma(\hat{\phi}(D)) &= [x^2 + (\zeta^4)^4 u_1 x + (\zeta^3)^2 u_0, \zeta^4 v_1 x + v_0] \\ &= [x^2 + \zeta u_1 x + \zeta^2 u_0, \zeta^4 v_1 x + v_0] \\ &= \phi(D).\end{aligned}$$

This completes the proof.

Since all conditions are satisfied, we can apply Theorem 1. Hence, we have

$$f_{r,D}(\epsilon(\phi(D)))^{2(p^2-1)} \in \mu_r.$$

This shows that we can compute the self-pairing with a simple final exponentiation.

5 Hyperelliptic curves in Characteristic Two

Since the curves over finite fields with even characteristic have larger embedding degree and may be preferred in hardware implementations, we will discuss the self-pairing computation on hyperelliptic curves over finite fields with even characteristic in this section.

Let m be a positive integer coprime to 6. Let $\mathbb{F}_q$ be a finite field with $q = 2^m$. Assume that C is a hyperelliptic curve over $\mathbb{F}_q$ with equation

$$C : y^2 + y = x^5 + x^3 + d, \quad d = 0 \text{ or } 1. \tag{1}$$

Note that this curve is supersingular and its embedding degree is $k = 12$. We use the same notation for the representation of $\mathbb{F}_{q^{12}}$ as in Section 7.1 of [2], i.e., $\mathbb{F}_{q^6} \simeq \mathbb{F}_q[w]/(w^6 + w^5 + w^3 + w^2 + 1)$ and $\mathbb{F}_{q^{12}} \simeq \mathbb{F}_{q^6}[s_0]/(s_0^2 + s_0 + w^5 + w^3)$. Denote $s_1 = w^2 + w^4$ and $s_2 = w^4 + 1$. There exists an automorphism on C given as follows.

$$\begin{aligned} &\phi : C \to C \\ &(x, y) \mapsto (x + w, y + s_2 x^2 + s_1 x + s_0). \end{aligned}$$

It induces an automorphism on the Jacobian as follows:

$$\begin{aligned} \phi : [x^2 + u_1 x + u_0, v_1 x + v_0] &\mapsto [x^2 + u_1 x + u_0 + w u_1 + w^2, \\ &(v_1 + s_2 u_1 + s_1)x + v_0 + s_0 + v_1 w + s_2 u_0 + s_2 u_1 w + s_1 w] \\ [x + u_0, v_0] &\mapsto [x + u_0 + w, v_0 + s_2 u_0^2 + s_1 u_0 + s_0] \\ \infty &\mapsto \infty. \end{aligned}$$

The inverse of ϕ can be defined as follows.

$$\begin{aligned} &\hat{\phi} : C \to C \\ &(x, y) \to (x + w, y + s_2 x^2 + s_1 x + s_0 + 1). \end{aligned}$$

One can verify that $\hat{\phi} \circ \phi$ is the identity map on C. Similarly, $\hat{\phi}$ induces an automorphism on the Jacobian as follows:

$$\begin{aligned} \hat{\phi} : [x^2 + u_1 x + u_0, v_1 x + v_0] &\mapsto [x^2 + u_1 x + u_0 + w u_1 + w^2, \\ &(v_1 + s_2 u_1 + s_1)x + v_0 + s_0 + v_1 w + s_2 u_0 + s_2 u_1 w + s_1 w + 1] \\ [x + u_0, v_0] &\mapsto [x + u_0 + w, v_0 + s_2 u_0^2 + s_1 u_0 + s_0 + 1] \\ \infty &\mapsto \infty. \end{aligned}$$

Let $D \in J_C(\mathbb{F}_q)[r]$. We show that condition (1) and (2) are also satisfied in this case.

Lemma 4. *With notation as above, condition (1) is satisfied.*

Proof. By Theorem 10 of [13], and since the other distortion maps in that Theorem are all defined over proper subfields of $\mathbb{F}_{q^{12}}$, we know that all the maps $\phi\pi_q^j$ with $0 \leq j \leq 3$ are distortion maps. In particular, it follows that $\phi = \phi\pi_q^0$ is a distortion map. Therefore, we have $\tau(D, \phi(D)) \neq 1$ in this case.

Lemma 5. *Let notation be as above, then condition (2) is satisfied.*

Proof. Let $D \in J_C(\mathbb{F}_q)[r]$ be written $D = [x^2 + u_1x + u_0, v_1x + v_0]$ in Mumford representation. Then $\phi(D)$ and $\hat{\phi}(D)$ can be determined as above. Let σ be the generator in the Galois group $Gal(\mathbb{F}_{q^{12}}/\mathbb{F}_{p^6})$. Note that $\sigma(s_2) = s_2$, $\sigma(s_1) = s_1$ and $\sigma(w) = w$. Since $\sigma(s_0) = s_0 + 1$ and $\sigma(s_0 + 1) = s_0$, it follows that

$$\begin{aligned}
&\sigma(\phi(D)) \\
=&\sigma([x^2+u_1x+u_0+wu_1+w^2,(v_1+s_2u_1+s_1)x + v_0+v_1w+s_2u_0+s_2u_1w+s_1w+s_0]) \\
=&[x^2+u_1x+u_0+wu_1+w^2,(v_1+s_2u_1+s_1)x+v_0+s_0+v_1w+s_2u_0+s_2u_1w+s_1w+1] \\
=&\hat{\phi}(D)
\end{aligned}$$

and

$$\begin{aligned}
&\sigma(\hat{\phi}(D)) \\
=&\sigma([x^2+u_1x+u_0+wu_1+w^2,(v_1+s_2u_1+s_1)x+v_0+s_0+1+v_1w+s_2u_0+s_2u_1w+s_1w]) \\
=&[x^2+u_1x+u_0+wu_1+w^2,(v_1+s_2u_1+s_1)x+v_0+s_0+v_1w+s_2u_0+s_2u_1w+s_1w] \\
=&\phi(D).
\end{aligned}$$

This completes the proof.

Since all conditions are satisfied, we can apply Theorem 1 on the curve. Hence, we have

$$f_{r,D}(\epsilon(\phi(D)))^{2(q^6-1)} \in \mu_r.$$

This shows that we can compute the self-pairing with a simple final exponentiation.

6 Applications

In this section, we will consider how to use our results in pairing-based cryptosystems. We assume that the Tate-Lichtenbaum pairing is being used to implement the protocol. As we have noted, the main contribution of our result is to require a much simpler final exponentiation.

In many cases it is more efficient to use the hyperelliptic ate pairing or twisted hyperelliptic ate pairing [5], especially since that pairing requires no final exponentiation, but this is not always the case. Recall that the ate pairing has a Miller function of the form $f_{q,D_2}(D_1)$ where q is the field of definition of the curve and where $r \mid (q^2+1)$ or, in the case $q = 2^n$, when $r \mid (2^{2n} \pm 2^{(3n+1)/2} + 2^n \pm 2^{(n+1)/2} + 1)$. In both cases, for high security levels, one needs q^k very large

compared with r and so it is quite often the case that $r < q$. Hence, there is no loop shortening from using the ate pairing at high security levels. Since our pairing has a very simple final exponentiation, the motivation for using the ate pairing disappears in these cases.

A further issue with the ate pairing in this setting is that it requires a distortion map from the 1-eigenspace of Frobenius to the q-eigenspace. Such a distortion map may be more expensive to compute than the distortion maps used in our method. For example, neither of the automorphisms from Sections 4 and 5 map to the q-eigenspace.

Now we discuss some details about the implementation for cryptographic schemes. In [15], the authors proposed a new short signature scheme. The full details are given in [15], but here we only note that a signature on message m is a pair (σ, r) and the verification equation is

$$e(\sigma, \sigma) = e(uv^{\pm m}g^r, g).$$

Section 3.2 of [15] shows how to speed up verification by using a pre-computation: one computes and stores $a = e(u, g)$, $b = e(v, g)$ and $c = e(g, g)$ and verifies the signature as

$$e(\sigma, \sigma) = ab^{\pm m}c^r,$$

which requires only one self-pairing computation.

It is natural to use our method to compute the self-pairing $e(\sigma, \sigma)$ for that protocol. However, there is one subtlety that must be addressed: The Tate-Lichtenbaum pairing is the value

$$\tau(D, \phi(D)) = f_{r,D}(\phi(D))^{(q^d-1)(q^d+1)/r}$$

whereas we are computing the function

$$e(D, D) = f_{r,D}(\phi(D))^{2(q^d-1)}.$$

It follows that $\tau(D, \phi(D)) \neq e(D, D)$ in general. Instead,

$$\tau(D, \phi(D)) = e(D, D)^t$$

where, when q is odd, $t \equiv (q^d+1)/(2r) \pmod r$ (we now require that $r^2 \nmid (q^d+1)$) and when $q = 2^m$ is even then $t = 2^{m-1}\big((q^d + 1)/r \pmod r\big)$.

For the signature scheme, we can incorporate this extra exponentiation into the precomputation. Let $s = 2\big(r/(q^d + 1) \pmod r\big)$ and define $a = \tau(u, \phi(g))^s$, $b = \tau(v, \phi(g))^s$ and $c = \tau(g, \phi(g))^s$. Then the protocol works correctly and the verification is faster than previous methods. These ideas can be also applied in the designated confirmer signature scheme proposed by Zhang *et. al* [16].

Acknowledgement

We would like to appreciate Jingwei Zhang and Fangguo Zhang for their helpful discussions.

References

1. Balakrishnan, J., Belding, J., Chisholm, S., Eisentraeger, K., Stange, K., Teske, E.: Pairings on hyperelliptic curves. ArXiv e-prints, 0908.3731 (2009)
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. Galbraith, S., Hess, F., Vercauteren, F.: Hyperelliptic pairings. In: Takagi, T., Okamoto, T., Okamoto, E., Okamoto, T. (eds.) Pairing-Based Cryptography Pairing 2007, Lecture Notes in Computer Science, vol. 4575, pp. 108–131. Springer Berlin / Heidelberg (2007)
4. Galbraith, S.D., Pujols, J., Ritzenthaler, C., Smith, B.: Distortion maps for supersingular genus two curves. Journal of Mathematical Cryptology 3(1), 1–18 (2009)
5. 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)
6. Hess, F., Smart, N., Vercauteren, F.: The eta pairing revisited. IEEE Transactions on Information Theory 52, 4595–4602 (2006)
7. Hess, F.: Pairing lattices. In: Galbraith, S., Paterson, K. (eds.) Pairing-Based Cryptography C Pairing 2008, Lecture Notes in Computer Science, vol. 5209, pp. 18–38. Springer Berlin / Heidelberg (2008)
8. Howe, E.W.: The Weil pairing and the Hilbert symbol. Mathematische Annalen 305, 387–392 (1996)
9. 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)
10. Miller, V.S.: Short programs for functions on curves (1986), http://crypto.stanford.edu/miller/miller.ps.
11. Miller, V.S.: The Weil pairing, and its efficient calculation. J. Cryptology 17(4), 235–261 (2004)
12. Park, C., Kim, M., Yung, M.: A remark on implementing the Weil pairing. In: Feng, D., Lin, D., Yung, M. (eds.) Information Security and Cryptology, Lecture Notes in Computer Science, vol. 3822, pp. 313–323. Springer Berlin / Heidelberg (2005)
13. Takashima, K.: Efficiently computable distortion maps for supersingular curves. In: van der Poorten, A., Stein, A. (eds.) Algorithmic Number Theory, Lecture Notes in Computer Science, vol. 5011, pp. 88–101. Springer Berlin / Heidelberg (2008), $http://dx.doi.org/10.1007/978-3-540-79456-1_5$, $10.1007/978-3-540-79456-1_5$
14. Vercauteren, F.: Optimal pairings. IEEE Transactions on Information Theory 56(1), 455–461 (2010)
15. 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)
16. 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, New York, NY, USA (2008)
17. Zhao, C.A., Zhang, F., Xie, D.: Faster computation of self-pairings. IEEE Transactions on Information Theory 58(5), 3266 –3272 (2012)