Efficient Tate Pairing Computation for Elliptic Curves over Binary Fields

Soonhak Kwon

Inst. of Basic Science and Dept. of Mathematics, Sungkyunkwan University,
Suwon 440-746, Korea
shkwon@skku.edu

Abstract. In this paper, we present a closed formula for the Tate pairing computation for supersingular elliptic curves defined over the binary field $\mathbb{F}_{2^m}$ of odd dimension. There are exactly three isomorphism classes of supersingular elliptic curves over $\mathbb{F}_{2^m}$ for odd m and our result is applicable to all these curves.

Keywords: supersingular elliptic curve, Tate pairing, divisor, automorphism, roots of unity.

1 Introduction

Many cryptographic schemes are based on the bilinear pairings arising from the rank two abelian group structure of the points of prescribed order of the given elliptic curve. Bilinear pairings were originally used as tools for attacking discrete logarithm problem for supersingular elliptic curves by Menezes et al. [1] and also by Frey and Rück [2], and they become popular these days for efficient encryption and signature schemes. Examples of such cryptographic protocols are, to name just a few, identity based encryption scheme by Boneh and Franklin [3], short signature scheme by Boneh et al. [4], tripartite Diffie-Hellman key agreement protocol by Joux [5], identity based authenticated key agreement protocol by Smart [7], and identity based signature schemes by Sakai et al. [6], Hess [16], Cha and Cheon [19], Baek and Zheng [28]. In most of these applications, the Tate pairing of supersingular elliptic curves (or curves of small embedding degrees) is an essential tool. Therefore efficient computation of the Tate pairing is a crucial factor for practical applications of the above mentioned cryptographic protocols.

Recently many progresses have been made on the computation of the Tate pairing. A few refined techniques and ideas to speed up the computation of the Tate pairing are suggested in [8,9,10,14,21,24]. The notion of the squared Tate pairing is introduced by Eisenträger [11]. Barreto et al. [14] showed that the algorithm of Miller [22] can be modified to a new algorithm where division in a finite field can be omitted since the denominator becomes one after final powering. Also Duursma and Lee [10] presented a closed formula for the computation of the Tate pairing for a finite field with characteristic *three*, which significantly reduces the cost of computation.

C. Boyd and J.M. González Nieto (Eds.): ACISP 2005, LNCS 3574, pp. 134–145, 2005.

In this paper, we show that an efficient closed formula can also be obtained for the computation of the Tate pairing for supersingular elliptic curves over a binary field $\mathbb{F}_{2^m}$ with odd dimension m. There are exactly three isomorphism classes of supersingular elliptic curves over $\mathbb{F}_{2^m}$ with m odd [17] and our method is applicable to all these curves. Also we present a method of avoiding inverse Frobenius operations in our and Duursma-Lee's algorithms. When one wants to use a polynomial basis, inverse Frobenius operation is not at all trivial unlike the case of a normal basis. We propose new modified algorithms which avoid the inverse Frobenius map without affecting the computational merits of the original algorithms.

A preliminary version of this work was posted through e-print archive, http://eprint.iacr.org/2004/303.pdf. Subsequently, the author was informed that a similar work was already presented by Barreto, Galbraith, O hEigeartaigh and Scott in ECC 2004 (slides are available through http://www.cacr.math.uwaterloo.ca/conferences/2004/ecc2004/barreto.pdf). Their preprint containing generalization to hyperelliptic case has appeared through http://eprint.iacr.org/2004/375.pdf.

2 Elliptic Curves and Miller's Algorithm

Let E be an elliptic curve over a finite field $\mathbb{F}_q$ where q is a power of a prime. We may express E as the standard Weierstrass form, $E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$, where the coefficients a_1, a_2, a_3, a_4, a_6 are in $\mathbb{F}_q$. Let $E(\mathbb{F}_q)$ be the additive group of all points $P = (x, y)$, $x, y \in \mathbb{F}_q$, on the curve with the point at infinity O. Let l be a positive integer and let $E[l]$ (resp. $E[l](\mathbb{F}_q)$) be the set of points $P \in E(\overline{\mathbb{F}}_q)$ (resp. $P \in E(\mathbb{F}_q)$) satisfying $lP = O$, where $\overline{\mathbb{F}}_q$ is an algebraic closure of $\mathbb{F}_q$. Let k be the minimal degree of the extension satisfying $E[l] \subset E(\mathbb{F}_{q^k})$. Such k is called the embedding degree (or the security multiplier) of $E[l]$ [17,25] and is dependent on E and l. If l is prime to q, then it is well known [13] that $E[l] \cong \mathbb{Z}/l \oplus \mathbb{Z}/l$.

A divisor D on E is a formal (finite) sum of the points P on the curve $D = \sum n_p(P)$, $n_p \in \mathbb{Z}$. We call D a degree 0 divisor if $\sum n_p = 0$. A principal divisor is a divisor of the form $(f) = \sum n_p(P)$, where f is a rational function on E and P is a point of E with n_P the order of multiplicity of f at P, i.e. $n_P > 0$ if f has a zero at P and $n_P < 0$ if f has a pole at P. We say two divisors D and D' are equivalent if $D - D'$ is a principal divisor. It is well known [13,17] that a principal divisor (f) is a degree 0 divisor, and a divisor $D = \sum n_p(P)$ is a principal divisor if D is a degree 0 divisor and $\sum n_pP = O$ in the abelian group $E(\overline{\mathbb{F}}_q)$. More precisely, there is an isomorphism

$$Div_0/Div_{prin} \longrightarrow E, \quad \text{with} \quad D = \sum n_p(P) \longmapsto \sum n_pP, \tag{1}$$

where the summation in the right side is the addition of points on the elliptic curve E and Div_0 (resp. Div_{prin}) is a free abelian group generated by the degree 0 divisors (resp. principal divisors). Now suppose that $P \in E[l]$. Then the divisor $l(P) - l(O)$ is a principal divisor so that there is a rational function f_P such that $(f_P) = l(P) - l(O)$. For any rational function f and any divisor $D = \sum n_p(P)$

having disjoint supports, one naturally defines $f(D) = \prod f(P)^{n_p}$. The Tate pairing τ_l on the set $E[l]$ is defined as follows.

Definition 1. *Let $P \in E[l](\mathbb{F}_q)$ and $Q \in E[l](\mathbb{F}_{q^k})$. The Tate pairing is a map*

$$\tau_l : E[l](\mathbb{F}_q) \times E[l](\mathbb{F}_{q^k}) \longrightarrow \{\zeta_l\}, \quad \text{with} \quad \tau_l(P,Q) = f_P(D_Q)^{\frac{q^k-1}{l}},$$

where f_P is a rational function satisfying $(f_P) = l(P) - l(O)$ and D_Q is a degree 0 divisor equivalent to $(Q) - (O)$ such that D_Q and (f_P) have disjoint supports. Also $\{\zeta_l\}$ is the group of l-th roots of unity in $\mathbb{F}_{q^k}^{\times}$.

It is well known that τ_l is a non-degenerate bilinear pairing and a proof can be found in [2,15]. It is also easy to verify $\tau_{ld}(P,Q) = \tau_l(P,Q)$ for $P, Q \in E[l]$ and $d > 0$ with ld dividing $|E(\mathbb{F}_q)|$.

An effective algorithm for finding a rational function f_P satisfying $(f_P) = l(P) - l(O)$ with $P \in E[l]$ is found by Miller [17,22]. Let us briefly explain the idea of Miller. For any degree 0 divisor D and D', the isomorphism in (1) implies that there exist points P and P' such that $D = (P) - (O) + (f)$ and $D' = (P') - (O) + (f')$ for some rational functions f and f'. Then one has the following formula due to Miller,

$$D + D' = (P + P') - (O) + (ff' \frac{\ell_{P,P'}}{\ell_{P+P'}}), \tag{2}$$

where $\ell_{P,P'}$ is an equation of a line intersecting P and P', and ℓ_P is an equation of a vertical line intersecting P and $-P$. This can be verified using the relation $(\frac{\ell_{P,P'}}{\ell_{P+P'}}) = (\ell_{P,P'}) - (\ell_{P+P'}) = (P) + (P') + (-P - P') - 3(O) - \{(P + P') + (-P - P') - 2(O)\} = (P) + (P') - (P + P') - (O)$.

An elliptic curve E over $\mathbb{F}_q$ is called supersingular if $Tr(\varphi) \equiv 0 \pmod{p}$ where φ is the Frobenius map and p is the characteristic of $\mathbb{F}_q$. If an elliptic curve E over $\mathbb{F}_q$ is supersingular, then it is well known [17] that for any l dividing $|E(\mathbb{F}_q)|$, the embedding degree k is bounded by 6. More precisely, we have $E[l] \subset E(\mathbb{F}_{q^k})$ with $k = 2, 3, 4, 6$. It is also well known that the embedding degree $k = 6$ is attained when the characteristic of $\mathbb{F}_q$ is *three* and the embedding degree $k = 4$ is attained when the characteristic of $\mathbb{F}_q$ is *two*. It should be mentioned that non-supersingular curves of low embedding degrees (≤ 6) are found by Miyaji et al. [12], which have some potential security advantage over supersingular curves.

3 Review of Previous Works

For some families of supersingular curves with embedding degree $k = 2, 4, 6$, Barreto et al. [14] showed that one can speed up the computation of the Tate pairing by observing that the denominators ℓ_Q appearing in the Miller's algorithm can be omitted using the idea of the distortion map ϕ introduced by Verheul [25], where ϕ is a suitably chosen nontrivial automorphism of the given supersingular elliptic curve. That is, since the line $X - \alpha$ intersecting $Q = (\alpha, \beta) \in \mathbb{F}_q$ and $-Q$

has only X-coordinate and since this X-coordinate has the value in $\mathbb{F}_{q^{k/2}}$ after applying ϕ to Q, it becomes one after taking the final power by $\frac{q^k-1}{l}$ because $l|q^{k/2}+1$ and $q^k-1=(q^{k/2}-1)(q^{k/2}+1)$. By the similar reasoning, they also showed that it is not necessary to evaluate the Tate pairing at the point at infinity O. To summarize, one may twist the pairing in Definition 1 such as $\tau_l(P,Q)=f_P(\phi(Q))^{\frac{q^k-1}{l}}$, which simplifies all the necessary computations.

For a field with characteristic *three*, $\mathbb{F}_q$ with $q=3^m$, Duursma and Lee [10] noticed that one can obtain a faster Tate pairing computation if one uses $l=q^3+1=3^{3m}+1$, since the ternary expansion of q^3+1 is trivial. That is, if one write g_Q as a rational function satisfying $3(Q)-3(O)=(3Q)-(O)+(g_Q)$, then, by repeated applications of the above equation, one has

$$3^{3m}(P)-3^{3m}(O)=(3^{3m}P)-(O)+(g_P^{3^{3m-1}}g_{3P}^{3^{3m-2}}\cdots g_{3^{3m-2}P}^{3}g_{3^{3m-1}P}).$$

It is shown [10] that the rational function $f=\prod_{i=1}^{3m}g_{3^{i-1}P}^{3^{3m-i}}$ can be used for a computation of the Tate pairing as $\tau_l(P,Q)=f(\phi(Q))^{3^{3m}-1}$. Duursma and Lee [10] showed that the value $f(\phi(Q))=\prod_{i=1}^{3m}\{g_{3^{i-1}P}(\phi(Q))\}^{3^{3m-i}}$ has certain cyclic property with regard to the polynomials $g_{3^{i-1}P}^{3^{3m-i}}$ so that they found a nice closed formula for f as a product of m (not $3m$) polynomials.

4 Tate Pairing Computation for Binary Fields

4.1 Supersingular Elliptic Curves over Binary Fields

For cryptographic purposes, it is natural to think of elliptic curves defined over $\mathbb{F}_{2^m}$ with m odd or more strongly a prime. There are exactly three isomorphism classes of supersingular elliptic curves over $\mathbb{F}_{2^m}$ when m is odd [17]. Namely they are $Y^2+Y=X^3+X$, $Y^2+Y=X^3+X+1$ and $Y^2+Y=X^3$. Among them, the curves

$$E_b: Y^2+Y=X^3+X+b, \quad b=0,1 \tag{3}$$

have the embedding degree (or security multiplier) $k=4$ while the curve $Y^2+Y=X^3$ has $k=2$. Thus we are mainly interested in the curves E_b though our method is also applicable to the curve $Y^2+Y=X^3$. The Frobenius map $\varphi: E_b \longrightarrow E_b$ with $\varphi(x,y)=(x^2,y^2)$ is a root of the characteristic polynomial $h(X)=X^2\pm 2X+2=(X-\varphi)(X-\bar{\varphi})$. We also have the order $|E_b(\mathbb{F}_{2^m})|$ of the group of rational points $E_b(\mathbb{F}_{2^m})$ as $|E_b(\mathbb{F}_{2^m})|=2^m+1-Tr(\varphi^m)$, where $Tr(\varphi^m)=\varphi^m+\bar{\varphi}^m$ and $\varphi^m(x,y)=(x^{2^m},y^{2^m})$. Letting $c_j=Tr(\varphi^j)$, one can find the values of c_j using the second order linear recurrence relations (or Lucas type sequences) arising from the characteristic polynomial $h(X)$, $c_j=2(\mp c_{j-1}-c_{j-2})$, $j\geq 0$, with $c_0=2$ and $c_1=\mp 2$. From these relations, it is straightforward to see [17] that $E_b(\mathbb{F}_{2^m})$ is a cyclic group of order

$$\begin{aligned} |E_b(\mathbb{F}_{2^m})| &= 2^m+1+(-1)^b\sqrt{2\cdot 2^m}, \quad \text{if} \quad m\equiv 1,7 \pmod 8 \\ &= 2^m+1-(-1)^b\sqrt{2\cdot 2^m}, \quad \text{if} \quad m\equiv 3,5 \pmod 8. \end{aligned} \tag{4}$$

4.2 Closed Formula of the Tate Pairing for $Y^2 + Y = X^3 + X + b$

As in the characteristic three case of Duursma and Lee [10], we want to derive a closed formula for the Tate pairing computation using the simple equality for our binary case, $2^{2m} + 1 = (2^m + 1 + 2^{\frac{m+1}{2}})(2^m + 1 - 2^{\frac{m+1}{2}})$. Let $P = (\alpha, \beta)$ be a point on the curve $E_b : Y^2 + Y = X^3 + X + b$, $b = 0, 1$. Then one has $-P = (\alpha, \beta + 1)$ and $2P = (\alpha^4 + 1, \alpha^4 + \beta^4)$. Thus we get $2^2P = (\alpha^{2^4}, \beta^{2^4} + 1) = -\varphi^4(P)$, $2^3P = (\alpha^{2^6} + 1, \alpha^{2^6} + \beta^{2^6} + 1)$, $2^4P = (\alpha^{2^8}, \beta^{2^8})$, where $\varphi^4 + 4 = 0$, i.e. $h(X) = X^2 \pm 2X + 2$ divides $X^4 + 4$. Using this cyclic property, one finds easily

$$\begin{aligned} 2^{i-1}P &= (\alpha^{2^{2i-2}} + i - 1, \beta^{2^{2i-2}} + (i-1)\alpha^{2^{2i-2}} + \epsilon_i) \\ &= (\alpha^{(2i-2)} + i - 1, \beta^{(2i-2)} + (i-1)\alpha^{(2i-2)} + \epsilon_i), \end{aligned} \tag{5}$$

where $\alpha^{(j)}$ (resp. $\beta^{(j)}$) is defined as $\alpha^{(j)} = \alpha^{2^j}$ (resp. $\beta^{(j)} = \beta^{2^j}$) and ϵ_i is defined as

$$\epsilon_i = 0 \quad \text{if } i \equiv 1, 2 \pmod 4 \quad \text{and} \quad \epsilon_i = 1 \quad \text{if } i \equiv 3, 4 \pmod 4. \tag{6}$$

For an effective Tate pairing computation, the following distortion map (non-trivial automorphism) $\phi : E_b \longrightarrow E_b$ with $\phi(x, y) = (x + s^2, y + sx + t)$ is chosen [14], where $s^2 + s + 1 = 0$ and $t^2 + t + s = 0$. That is, $\mathbb{F}_2(s) = \mathbb{F}_{2^2}$, $\mathbb{F}_2(t) = \mathbb{F}_{2^4}$, $s = t^5$, $t^4 + t + 1 = 0$, and t is a generator of the group $\mathbb{F}_{2^4}^{\times}$ of order 15.

For any point Q on the curve E_b, let us write g_Q as a rational function satisfying $2(Q) - 2(O) = (2Q) - (O) + (g_Q)$. By the Miller's formula in (2), we have $g_Q = \ell_{Q,Q}/\ell_{2Q}$ and the denominator ℓ_{2Q} can be omitted by the result in [14]. Now for a given point $P \in E_b(\mathbb{F}_{2^m})$, one repeatedly has

$$\begin{aligned} 2(P) - 2(O) &= (2P) - (O) + (g_P), \\ 2^2(P) - 2^2(O) &= 2\{(2P) - (O)\} + (g_P^2) = (2^2P) - (O) + (g_P^2 g_{2P}), \\ &\cdots \\ 2^{2m}(P) - 2^{2m}(O) &= (2^{2m}P) - (O) + (g_P^{2^{2m-1}} g_{2P}^{2^{2m-2}} \cdots g_{2^{2m-2}P}^2 g_{2^{2m-1}P}). \end{aligned}$$

Letting

$$f_P = \prod_{i=1}^{2m} g_{2^{i-1}P}^{2^{2m-i}} = g_P^{2^{2m-1}} g_{2P}^{2^{2m-2}} \cdots g_{2^{2m-2}P}^2 g_{2^{2m-1}P}, \tag{7}$$

we have $2^{2m}(P) - 2^{2m}(O) = (2^{2m}P) - (O) + (f_P)$ and $(P) - (O) = (P) - (O) + (1)$. Thus the equation (2) of the Miller's formula again says $(2^{2m} + 1)\{(P) - (O)\} = (f_P \ell_P)$ because $2^{2m}P = -P$. Note that the line ℓ_P can also be omitted in the actual computation in view of [14]. Therefore after adjusting the irrelevant factors, we can say that

$$(f_P) = (2^{2m} + 1)\{(P) - (O)\} = \tfrac{2^{2m}+1}{l} \cdot \{l(P) - l(O)\} = \tfrac{2^{2m}+1}{l}(f'_P), \tag{8}$$

where f'_P is a rational function satisfying $l(P) - l(O) = (f'_P)$. Thus we have the Tate pairing

$$\tau_l(P, Q) = f'_P(\phi(Q))^{\frac{2^{4m}-1}{l}} = f'_P(\phi(Q))^{\frac{2^{2m}+1}{l}(2^{2m}-1)} = f_P(\phi(Q))^{2^{2m}-1}. \tag{9}$$

From the equation (7), the rational function f_P is just a product of the functions of the form $g_{2^{i-1}P}$ which can be regarded as the tangent line at the point $2^{i-1}P$. Thus all we have to do is to find an explicit expression of $f_P = \prod_{i=1}^{2m} g_{2^{i-1}P}^{2^{2m-i}}$.

Lemma 2. *Let $P = (\alpha, \beta), Q = (x, y)$ be points in $E_b(\mathbb{F}_{2^m})$. Then one has the value of $\{g_{2^{i-1}P}(\phi(Q))\}^{2^{2m-i}} = \{g_{2^{i-1}P}(x + s^2, y + sx + t)\}^{2^{2m-i}}$ as*

$$\{g_{2^{i-1}P}(\phi(Q))\}^{2^{2m-i}} = \alpha^{(i-1)}x^{(-i)} + \beta^{(i-1)} + y^{(-i)} + s(\alpha^{(i-1)} + x^{(-i)}) + t + b,$$

where $g_R(X, Y) = \ell_{R,R}$ is an equation of the tangent line at R.

Proof. The tangent line at $P = (\alpha, \beta)$ on the curve $E_b : Y^2 + Y = X^3 + X + b$ is $Y = (\alpha^2 + 1)X + \beta^2 + b$. Thus we have $2(P) - 2(O) = (2P) - (O) + (\frac{g_P}{\ell_{2P}})$ where

$$g_P(x, y) = (\alpha^2 + 1)x + \beta^2 + b - y, \tag{10}$$

and ℓ_{2P} is the vertical line intersecting $2P$ and $-2P$. Since ℓ_{2P} can be removed without affecting the pairing value, we are mainly interested in the computations of the lines $g_{2^{i-1}P}$. Using the equation (5), one has $g_{2^{i-1}P}(x, y) = (\alpha^{(2i-1)} + i)x + \beta^{(2i-1)} + (i-1)\alpha^{(2i-1)} + \epsilon_i + b - y$. Therefore, by applying the distortion map ϕ to the point $Q = (x, y)$, we get

$$\begin{aligned} g_{2^{i-1}P}(x + s^2, y + sx + t) = (\alpha^{(2i-1)} + i)(x + s^2) + \beta^{(2i-1)} \\ + (i-1)\alpha^{(2i-1)} + \epsilon_i + b - (y + sx + t). \end{aligned} \tag{11}$$

Taking 2^{2m-i}-th power of both sides of the above equality,

$$\begin{aligned} &\{g_{2^{i-1}P}(\phi(Q))\}^{2^{2m-i}} \\ &= (\alpha^{(i-1)} + i)(x^{(2m-i)} + s^{(2m-i+1)}) + \beta^{(i-1)} + (i-1)\alpha^{(i-1)} + \epsilon_i + b \\ &\quad - (y^{(2m-i)} + s^{(2m-i)}x^{(2m-i)} + t^{(2m-i)}) \\ &= \alpha^{(i-1)}x^{(2m-i)} + \{i - s^{(2m-i)}\}x^{(2m-i)} + \{s^{(2m-i+1)} + i - 1\}\alpha^{(i-1)} \\ &\quad + \beta^{(i-1)} + b - y^{(2m-i)} + \{is^{(2m-i+1)} + \epsilon_i - t^{(2m-i)}\}. \end{aligned} \tag{12}$$

From $s^2 + s + 1 = 0$, we have $s^{(2)} = s^4 = s, s^{(3)} = s + 1, s^{(4)} = s, \cdots$. That is,

$$s^{(j)} = s + j. \tag{13}$$

The coefficients $i - s^{(2m-i)}$ (resp. $i - 1 + s^{(2m-i+1)}$) of $x^{(2m-i)}$ (resp. $\alpha^{(i-1)}$) in the equation (12) have a unique value equal to s independent of the choices of i because i and $2m - i$ always have the same parity and we are in the binary field. In other words, for any $i \geq 0$, we get

$$i - s^{(2m-i)} = i + 2m - i + s = s. \tag{14}$$

From $t^2 = t+s$, we have $t^{(2)} = t^{2^2} = t+s+s^2 = t+1, t^{(3)} = t^{2^3} = t+s+1, t^{(4)} = t+s+s^2+1 = t, t^{(5)} = t^2 = t+s, \cdots$. Therefore, for any $j \geq 0$, we have

$$t^{(4j)} = t, \quad t^{(4j+1)} = t+s, \quad t^{(4j+2)} = t+1, \quad t^{(4j+3)} = t+s+1. \tag{15}$$

Now using the equations (6),(13),(15), it is trivial to show that the last term of the equation (12) has the value

$$is^{(2m-i+1)} + \epsilon_i - t^{(2m-i)} = t \tag{16}$$

independent of the choices of i. This can be proved as follows. Since the extension degree m is odd, we may write $m = 2j+1$ for some j. Therefore one has $is^{(2m-i+1)} + \epsilon_i - t^{(2m-i)} = is^{(4j+3-i)} + \epsilon_i - t^{(4j+2-i)}$. By taking $i \pmod 4$ and noticing that our field has characteristic *two*, we easily get the equation (16). Since x, y, α, β are all in $\mathbb{F}_{2^m}$, the values $x^{(j)}, y^{(j)}, \alpha^{(j)}, \beta^{(j)}$ are determined up to the residue classes of $j \pmod m$ and $x^{(j)}$ with $j \in \mathbb{Z}$ (resp. $y^{(j)}, \alpha^{(j)}, \beta^{(j)}$) is understood as $x^{(j)} = x^{2^{j'}}$ where j', $0 \leq j' \leq m-1$, is a unique integer satisfying $j' \equiv j \pmod m$. Therefore, using (14) and (16) in the equation (12), we are done. □

Theorem 3. *One has the Tate pairing* $\tau_l(P,Q) = f_P(\phi(Q))^{2^{2m}-1}$ *where*

$$f_P(\phi(Q)) = \prod_{i=1}^{m} \{\alpha^{(i)} x^{(-i+1)} + \beta^{(i)} + y^{(-i+1)} + s^2(\alpha^{(i)} + x^{(-i+1)}) + t^2 + b\}.$$

Proof. Lemma 2 implies that $\{g_{2^{i-1}P}(\phi(Q))\}^{2^{2m-i}}$ is depending only on the residue classes of $i \pmod m$. Thus, from (7) and (9), we have $f_P(\phi(Q)) = \prod_{i=1}^{2m} \{g_{2^{i-1}P}(\phi(Q))\}^{2^{2m-i}} = \prod_{i=1}^{m} \{g_{2^{i-1}P}(\phi(Q))\}^{2^{2m-i} \cdot 2} = \prod_{i=1}^{m} \{\alpha^{(i)} x^{(-i+1)} + \beta^{(i)} + y^{(-i+1)} + s^2(\alpha^{(i)} + x^{(-i+1)}) + t^2 + b\}$. □

4.3 Closed Formula of the Tate Pairing for $Y^2 + Y = X^3$

The curve $E : Y^2 + Y = X^3$ has the embedding degree $k = 2$ and is not so interesting in terms of the bandwidth. However using the same techniques in the previous section, we can derive a similar closed formula for the pairing computation. That is, by defining the distortion map $\phi : E \longrightarrow E$ as $\phi(x,y) = (x+1, y+x+t)$ with $t^2+t+1 = 0$, we have $\{g_{2^{i-1}P}(\phi(Q))\}^{2^{m-i}} = \alpha^{(i-1)} x^{(-i)} + (\alpha+\beta)^{(i-1)} + (x+y)^{(-i)} + t$, where $P = (\alpha, \beta)$ and $Q = (x,y)$ are the points in $E(\mathbb{F}_{2^m})$. Therefore

Theorem 4. *One has the Tate pairing* $\tau_l(P,Q) = f_P(\phi(Q))^{2^m-1}$ *where*

$$f_P(\phi(Q)) = \prod_{i=1}^{m} \{\alpha^{(i-1)} x^{(-i)} + (\alpha+\beta)^{(i-1)} + (x+y)^{(-i)} + t\},$$

and f_P *is a rational function satisfying* $(2^m+1)\{(P) - (O)\}$.

5 Field Arithmetic for the Computation of $f_P(\phi(Q))$

In Theorem 3, using $s^2 = t^2 + t + 1$, we may write $\alpha^{(i)}x^{(-i+1)} + \beta^{(i)} + y^{(-i+1)} + s^2(\alpha^{(i)} + x^{(-i+1)}) + t^2 + b = w + zt + (z+1)t^2$, where

$$z = \alpha^{(i)} + x^{(-i+1)}, \quad w = z + \alpha^{(i)}x^{(-i+1)} + \beta^{(i)} + y^{(-i+1)} + b. \tag{17}$$

Letting $C = c_0 + c_1t + c_2t^2 + c_3t^3$, $c_i \in \mathbb{F}_{2^m}$, be the partial product in the computation of $f_P(\phi(Q))$, we have $C \cdot (w+zt+(z+1)t^2) = c'_0 + c'_1t + c'_2t^2 + c'_3t^3$, where $c'_0 = c_0w+(c_2+c_3)(z+1)+c_3$, $c'_1 = c_0w+(c_1+c_2+c_3)w+(c_0+c_2+c_3)(w+z+1)+c_3(z+1)+c_0+c_3$, $c'_2 = c_0w+(c_1+c_2+c_3)w+(c_0+c_2+c_3)(w+z+1)+(c_1+c_2)(w+z+1)+c_1$ and $c'_3 = (c_1+c_2+c_3)w+(c_1+c_2)(w+z+1)+c_2$. Therefore one needs 6 $\mathbb{F}_{2^m}$-multiplications for the computation of $C \cdot (w + zt + (z+1)t^2)$ with respect to the basis $\{1, t, t^2, t^3\}$. One may also use the basis $\{1, s, t, st\}$ to get the same result.

Table 1. An algorithm for computing $f_P(\phi(Q))$

Input: $P = (\alpha, \beta), Q = (x, y)$
Output: $C = f_P(\phi(Q))$
$C \leftarrow 1$
for ($i = 1$ to m ; $i++$)
$\alpha \leftarrow \alpha^2, \quad \beta \leftarrow \beta^2$
$z \leftarrow \alpha + x, \quad w \leftarrow z + \alpha x + \beta + y + b$
$C \leftarrow C \cdot (w + zt + (z+1)t^2)$
$x \leftarrow x^{2^{m-1}}, \quad y \leftarrow y^{2^{m-1}}$
end for

If we ignore the costs of (inverse) Frobenius maps and $\mathbb{F}_{2^m}$-additions, we find that exactly 7 $\mathbb{F}_{2^m}$-multiplications are needed in each round of the for-loop, where the computation of w needs one multiplication in $\mathbb{F}_{2^m}$ and the computation of C needs 6 multiplications in $\mathbb{F}_{2^m}$. Compare our result with the similar result in $\mathbb{F}_{3^m}$ case of Duursma and Lee where each step of the algorithm in [10] requires 14 $\mathbb{F}_{3^m}$-multiplications [8,9] with loop unfolding technique.

6 Algorithms Without Inverse Frobenius Operations

Many computational evidence [8,23] imply that a more efficient field arithmetic can be obtained for small characteristic finite fields by using a polynomial basis than a normal basis, especially for software purposes. Though a Gaussian normal basis of low complexity [27] is a good choice for a fast arithmetic, such basis does not appear quite frequently when compared with a polynomial basis of low hamming weight (like trinomial or pentanomial). Granger et al. [8] showed that, even though a cube root operation (inverse Frobenius operation for characteristic *three*) in a polynomial basis is tricky, an algorithm for the

Tate pairing computation with a polynomial basis outperforms a method with a normal basis since the cost of a multiplication with a normal basis is quite expensive than that of a polynomial basis in general situations. Based on the idea of Vercauteren [8], Granger et al. showed that a cube root operation in $\mathbb{F}_{3^m}$ has roughly the same cost as 2/3 multiplication in $\mathbb{F}_{3^m}$ with a small amount of precomputation. A similar method for the characteristic *two* case is discussed by Fong et al. [26] so that one can show that the cost of one square root operation is roughly equal to the cost of 1/2 multiplication with a precomputation. In fact, as pointed out by Harrison [18], the cost of one inverse Frobenius (square or cube root) operation is almost equal to the cost of one Frobenius operation when the given irreducible polynomial is a trinomial. However for a general case where no irreducible trinomial exists, the computation is not so simple and even in the case of pentanomial basis, inverse Frobenius operation is quite costly compared with Frobenius operation.

6.1 Avoiding Square Root Operation

Let us define A_i as $A_i = \{\alpha^{(i)}x^{(-i+1)} + \beta^{(i)} + y^{(-i+1)} + s^2(\alpha^{(i)} + x^{(-i+1)}) + t^2 + b\}^{2^{3m+i}} = \alpha^{(2i)}x^2 + \beta^{(2i)} + y^2 + s^{(i)}(\alpha^{(2i)} + x^2) + t^{(m-1+i)} + b$, where we used the fact that $s^{(j)}$ is determined up to $j \pmod 2$ with $3m+1 \equiv 0 \pmod 2$ and $t^{(j)}$ is determined up to $j \pmod 4$ with $3m+1 \equiv m-1 \pmod 4$ as is clear from the equations (13) and (15). Then the expression of $f_P(\phi(Q))$ in Theorem 3 can be rewritten as $f_P(\phi(Q)) = \prod_{i=1}^{m} A_i^{2^{m-i}} = (\cdots(((A_1)^2A_2)^2A_3)^2\cdots)^2A_m$. Using the cyclic property of $t^{(j)}$ in the equation (15), it is not difficult to see that, for all indices $1 \le i \le m$, A_i can be written as $A_i = A_i(t) = w + zt + (z+1)t^2$ for some z and w in $\mathbb{F}_{2^m}$. Thus, similarly as in the previous section, one needs 6 $\mathbb{F}_{2^m}$-multiplications for computing $C \cdot A_i(t)$ with respect to the basis $\{1, t, t^2, t^3\}$ for any $C \in \mathbb{F}_{2^{4m}}$. We now have the following algorithm for computing $f_P(\phi(Q))$ which avoids inverse Frobenius operations.

Table 2. An algorithm for computing $f_P(\phi(Q))$ without square root operations

Input: $P = (\alpha, \beta), Q = (x, y)$
Output: $C = f_P(\phi(Q))$
$C \leftarrow 1$
$u \leftarrow x^2, \quad v \leftarrow u, \quad y \leftarrow y^2$
for ($i = 1$ to m ; $i++$)
$\alpha \leftarrow \alpha^4, \quad \beta \leftarrow \beta^4$
$A(t) \leftarrow \alpha(v+1) + u + \beta + y + b + \frac{m-1}{2} + (\alpha + v)t + (\alpha + v + 1)t^2$
$C \leftarrow C^2 \cdot A(t)$
$u \leftarrow u + v + 1, \quad v \leftarrow v + 1$
end for

Note that the coefficients of $A_i(t)$ depend on the values of $s^{(i)}$ and $t^{(m-1+i)}$ and they are recursively computed by the relation (13) and (15). We also have the initial values $s^{(1)} = s^2 = t^2 + t + 1$ and $t^{(m)} = t^2 + \frac{m-1}{2}$. In each step of the above

algorithm, one needs 7 $\mathbb{F}_{2^m}$-multiplications which is same to the algorithm in Table 1. Since the operation $C \leftarrow C^2$ needs 4 squaring operations in $\mathbb{F}_{2^m}$ and since the operations $\alpha \leftarrow \alpha^4$, $\beta \leftarrow \beta^4$ also need 4 squaring operations, the total number of necessary squaring is 8 in this new algorithm. On the other hand, the algorithm in Table 1 needs 2 squaring and 2 square root operations. Therefore our new algorithm in Table 2 is a more optimal choice if one is interested in the implementation with arbitrary polynomial basis (especially for hardware purpose) since this new algorithm uses 6 Frobenius operations instead of using 2 inverse Frobenius operations.

6.2 Avoiding Cube Root Operation from the Algorithm of Duursma and Lee

Duursma and Lee [10] found a closed formula for the following supersingular elliptic curves defined over $\mathbb{F}_{3^m}$ with m prime to 6, $E_b : Y^2 = X^3 - X + b$, $b = \pm 1$. For the above mentioned curves, the following nontrivial automorphism $\phi : E_b \longrightarrow E_b$ with $\phi(x, y) = (\rho - x, \sigma y)$ is used, where $\sigma^2 + 1 = 0$ and $\rho^3 - \rho - b = 0$. That is, $\mathbb{F}_3(\sigma) = \mathbb{F}_{3^2}$ and $\mathbb{F}_3(\rho) = \mathbb{F}_{3^3}$. A closed formula of Duursma and Lee says that, for $P = (\alpha, \beta)$ and $Q = (x, y)$ in $E[l](\mathbb{F}_{3^m})$, the Tate pairing can be written as $\tau_l(P, Q) = f_P(\phi(Q))^{3^{3m}-1}$ with $f_P(\phi(Q)) = \prod_{i=1}^{m} B_i$ where $B_i = -\sigma\beta^{(i)}y^{(-i+1)} - (\alpha^{(i)} + x^{(-i+1)} - \rho + b)^2$ and f_P is a rational function satisfying $(f_P) = (3^{3m} + 1)\{(P) - (O)\}$. Now let us define $A_i \in \mathbb{F}_{3^{6m}}$ as $A_i = B_i^{3^{5m+i}} = -\sigma^{(5m+i)}\beta^{(2i)}y^{(1)} - (\alpha^{(2i)} + x^{(1)} - \rho^{(5m+i)} + b)^2 = (-1)^{i+1}\sigma\beta^{(2i)}y^{(1)} - (\alpha^{(2i)} + x^{(1)} - \rho + (m + 1 - i)b)^2$, where we used the relations $\sigma^{(j)} = (-1)^j\sigma$ and $\rho^{(j)} = \rho + jb$. Thus, from $B_i = A_i^{3^{m-i}}$, we get $f_P(\phi(Q)) = \prod_{i=1}^{m} A_i^{3^{m-i}} = (\cdots(((A_1)^3A_2)^3A_3)^3\cdots)^3A_m$. Letting $\mu = \alpha^{(2i)} + x^{(1)} + (m+1-i)b \in \mathbb{F}_{3^m}$ and $\lambda = (-1)^{i+1}\sigma\beta^{(2i)}y^{(1)} - \mu^2 \in \mathbb{F}_{3^{2m}}$, one finds $A_i = \lambda - \mu\rho - \rho^2$. Therefore the modified algorithm is given as follows.

Table 3. A modified Duursma-Lee algorithm without cube root operations

Input: $P = (\alpha, \beta), Q = (x, y)$
Output: $C = f_P(\phi(Q))$
$C \leftarrow 1$
$x \leftarrow x^3, \quad y \leftarrow y^3, \quad d \leftarrow mb$
for ($i = 1$ to m ; $i++$)
$\alpha \leftarrow \alpha^9, \quad \beta \leftarrow \beta^9$
$\mu = \alpha + x + d, \quad \lambda = \sigma\beta y - \mu^2$
$C \leftarrow C^3 \cdot (\lambda - \mu\rho - \rho^2)$
$y \leftarrow -y, \quad d \leftarrow d - b$
end for

In each step of the above algorithm, the number of necessary multiplications in $\mathbb{F}_{3^m}$ is same to that of the original algorithm of Duursma and Lee. Since the cube operation $C \leftarrow C^3$ with respect to the basis $\{1, \rho, \rho^2\}$ over $\mathbb{F}_{3^{2m}}$ costs 6 cube operations in $\mathbb{F}_{3^m}$ and since the operations $\alpha \leftarrow \alpha^9$, $\beta \leftarrow \beta^9$ cost 4 cube

operations in $\mathbb{F}_{3^m}$, the total number of necessary Frobenius operations in each step of the above algorithm is 10. Note that the original Duursma-Lee algorithm needs 2 Frobenius operations plus 2 inverse Frobenius operations. Therefore our modified algorithm uses 8 Frobenius operations instead of using 2 inverse Frobenius operations. With arbitrary polynomial basis, it is safe to believe that the cost of 4 cube operations is cheaper than the cost of one cube root operation.

7 Conclusions

In this paper we showed that an efficient closed formula can be derived for the Tate pairing computation for supersingular elliptic curves over a binary field $\mathbb{F}_{2^m}$ of odd dimension. There are exactly three isomorphism classes of supersingular elliptic curves over $\mathbb{F}_{2^m}$ with m odd and our method is applicable to all these curves. Each step of our algorithm requires two inverse Frobenius operations like the characteristic three case of Duursma and Lee. To overcome the computational complexity of the inverse Frobenius operation with arbitrary polynomial basis, we modified our algorithm and the algorithm of Duursma and Lee, and presented another closed formula which does not need any inverse Frobenius operation, which is especially useful for polynomial basis arithmetic.

Acknowledgements: The author would like to thank Robert Granger and Keith Harrison who made valuable suggestions on the preprint version of this paper. Also thanks are due to the anonymous referees for their many helpful comments. Finally, this work was supported by grant No. R01-2005-000-11261-0 from Korea Science and Engineering Foundation in Ministry of Science & Technology.

References

1. A.J. Menezes, T. Okamoto, and S.A. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite field," *IEEE Trans. Information Theory*, vol. 39, pp. 1639–1646, 1993.
2. G. Frey and H. Rück, "A remark concerning m-divisibility and the discrete logarithm in the divisor class groups of curves," *Math. Comp.*, vol. 62, pp. 865–874, 1994.
3. D. Boneh and M. Franklin, "Identity based encryption from the Weil pairing," *Crypto 2001, Lecture Notes in Computer Science*, vol. 2139, pp. 213–229, 2001.
4. D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing," *Asiacrypt 2001, Lecture Notes in Computer Science*, vol. 2248, pp. 514–532, 2002.
5. A. Joux, "A one round protocol for tripartite Diffie-Hellman," *ANTS 2000, Lecture Notes in Computer Science*, vol. 1838, pp. 385–394, 2000.
6. R. Sakai, K. Ohgishi, and M. Kasahara, "Cryptosystems based on pairing," *SICS 2000, Symposium on Cryptography and Information Security*, pp. 26–28, 2000.
7. N.P. Smart, "An identity based authentication key agreement protocol based on pairing," *Electronics Letters*, vol. 38, pp. 630–632, 2002.
8. R. Granger, D. Page, and M. Stam, "Hardware and software normal basis arithmetic for pairing based cryptography in characteristic three," preprint, *available at* http://eprint.iacr. org/2004/157.pdf, 2004.

9. R. Granger, D. Page, and M. Stam, "On small characteristic algebraic tori in pairing based cryptography," preprint *available at* http://eprint.iacr.org/2004/132.pdf, 2004.
10. I. Duursma and H. Lee, "Tate pairing implementation for hyperelliptic curves $y^2 = x^p - x + d$," *Asiacrypt 2003, Lecture Notes in Computer Science*, vol. 2894, pp. 111–123, 2003.
11. K. Eisenträger, K. Lauter, and P.L. Montgomery, "Improved Weil and Tate pairing for elliptic and hyperelliptic curves," preprint, 2004.
12. A. Miyaji, M. Nakabayashi, and S. Takano, "New explicit conditions of elliptic curve trace for FR-reduction," *IEICE Trans. Fundamentals*, vol. E84 A, pp. 1–10, 2001.
13. J.H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, 1985.
14. P. Barreto, H. Kim, B. Lynn, and M. Scott, "Efficient algorithms for pairing based cryptosystems," *Crypto 2002, Lecture Notes in Computer Science*, vol. 2442, pp. 354–368, 2002.
15. F. Hess, "A Note on the Tate pairing of curves over finite fields," *Arch. Math.* vol. 82, pp. 28–32, 2004.
16. F. Hess, "Efficient identity based signature schemes based on pairings," *SAC 2002, Lecture Notes in Computer Science*, vol. 2595, 310-324, 2003.
17. A.J. Menezes, *Elliptic Curve Public Key Cryptosystems*, Kluwer Academic Publisher, 1993.
18. K. Harrison, *Personal Communications*, 2004.
19. J.C. Cha and J.H. Cheon, "An identity-based signature from gap Diffie-Hellman groups," *PKC 2003, Lecture Notes in Computer Science*, vol. 2567, 18-30, 2003.
20. K. Rubin and A. Silverberg "Torus based cryptography," *Crypto 2003, Lecture Notes in Computer Science*, vol. 2729, pp. 349–365, 2003.
21. S. Galbraith, K. Harrison, and D. Soldera, "Implementing the Tate pairing," *ANTS 2002, Lecture Notes in Computer Science*, vol. 2369, pp. 324–337, 2002.
22. V. Miller, "Short programs for functions on curves," *unpublished manuscript*, 1986.
23. D. Hankerson, J.L. Hernandez, and A.J. Menezes, "Software implementation of elliptic curve cryptography over binary fields," *CHES 2000, Lecture Notes in Computer Science*, vol. 1965, pp. 1–24 , 2000.
24. S. Galbraith, "Supersingular curves in cryptography," *Asiacrypt 2001, Lecture Notes in Computer Science*, vol. 2248, pp. 495–513, 2001.
25. E.R. Verheul, "Evidence that XTR is more secure than supersingular elliptic curve cryptosystems," *Eurocrypt 2001, Lecture Notes in Computer Science*, vol. 2045, pp. 195–210, 2001.
26. K. Fong, D. Hankerson, J. López, and A. Menezes, "Field inversion and point halving revisited," *Technical Report CORR 2003-18*, Univ. of Waterloo, 2003.
27. S. Gao, J. von zur Gathen, and D. Panario, "Gauss periods and fast exponentiation in finite fields," *Latin 1995, Lecture Notes in Computer Science*, vol. 911, pp. 311–322, 1995.
28. J. Baek and Y. Zheng, "Identity-based threshold signature scheme from the bilinear pairings," *ITCC 2004, Proceedings of International Conference on Information Technology*, vol 1, pp. 124–128, 2004.
29. P. Gaudry, F. Hess, and N.P. Smart, "Constructive and destructive facets of Weil descent on elliptic curves," *J. of Cryptology*, vol. 15, pp. 19–46, 2002.
30. N. Koblitz, A. Menezes, and S. Vanstone, "The state of elliptic curve cryptography," *Design, Codes and Cryptography*, vol. 19, pp. 173–193, 2000.