Tate pairing implementation for hyperelliptic curves $y^2 = x^p - x + d$

Iwan Duursma[1] and Hyang-Sook Lee[2] *

[1] Department of Mathematics, University of Illinois at Urbana-Champaign
Urbana IL 61801, USA, duursma@math.uiuc.edu
[2] Department of Mathematics, Ewha Womans University
Seoul, 120-750, Korea, hsl@ewha.ac.kr

Abstract. The Weil and Tate pairings have been used recently to build new schemes in cryptography. It is known that the Weil pairing takes longer than twice the running time of the Tate pairing. Hence it is necessary to develop more efficient implementations of the Tate pairing for the practical application of pairing based cryptosystems. In 2002, Barreto et al. and Galbraith et al. provided new algorithms for the fast computation of the Tate pairing in characteristic three. In this paper, we give a closed formula for the Tate pairing on the hyperelliptic curve $y^2 = x^p - x + d$ in characteristic p. This result improves the implementations in [BKLS02], [GHS02] for the special case $p = 3$.

1 Introduction

Pairings were first used in cryptography as a cryptanalytic tool for reducing the discrete log problem on some elliptic curves to the discrete log problem in a finite field. There are two reduction types. One uses the Weil pairing and is called the MOV reduction [MOV93], the other uses the Tate pairing and is called the FR reduction [FR94]. Positive cryptographic applications based on pairings arose from the work of Joux [J00], who gave a simple one round tripartite Diffie-Hellman protocol on supersingular curves. Curve based pairings, such as the Weil pairing and Tate pairing, provide a good setting for the so-called bilinear Diffie-Hellman problem. Many cryptographic schemes based on the pairings have been developed recently, such as identity based encryption [BF01], identity based signature schemes [SOK00], [CC03], [H02a], [P02], and identity based authenticated key agreement [S02]. For the practical application of those systems it is important to have efficient implementations of the pairings. According to [G01], the Tate pairing can be computed more efficiently than the Weil pairing. The recent papers [BKLS02], [GHS02] provide fast computations of the Tate pairing in characteristic three.

Our main result in this paper is a closed expression for the Tate pairing on the hyperelliptic curve defined by the equation $C^d/k : y^2 = x^p - x + d$, for a prime number p congruent to 3 modulo 4 (Theorem 5). We assume that k is

* Supported by Korea Research Foundation Grant (KRF-2002-070-C00010)

a finite extension of degree n of the prime field F_p with n coprime to $2p$. The formula assigns to a pair (P, Q) of k-rational points on the curve an element $\{P, Q\} \in K^*$, where K/k is an extension of degree $2p$. By a general property of the Tate pairing the map is bilinear. Following Joux [J00], we can use the map to construct a tripartite key agreement protocol: If A, B, C are three parties with private keys a, b, c, and public keys aP, bP, cP, respectively, they can establish a common secret key $\alpha \in K^*$ via

$$\alpha = \{aP, bP\}^c = \{bP, cP\}^a = \{cP, aP\}^b \in K^*.$$

The computation of the Tate pairing can be performed using an algorithm first presented by Miller [M86]. For a general elliptic curve in characteristic three, the computation can be improved. For the elliptic curve $E^b/k : y^2 = x^3 - x + b$, techniques specific to the curve yield further improvements [BKLS02], [GHS02]. We describe these algorithms and we show that the evaluation of our closed expression, for the special case $p = 3$, uses fewer logical and arithmetic operations.

This paper is organized as follows. In the next section, we recall the general formulation of the Tate pairing. Section 3 gives useful properties of the elliptic curve $E^b : y^2 = x^3 - x + b$ and gives Miller's algorithm in base 3. We also describe the algorithm for computing the Tate pairing due to Barreto et al. [BKLS02]. For comparison, we derive a closed expression for the output of the algorithm proposed by Barreto et al. in Section 4. Section 5 gives useful properties of the curve $C^d : y^2 = x^p - x + d$ and we give a first algorithm to evaluate the Tate pairing for the curve C^d. Our main result in Section 6 gives the output of this algorithm in closed form. The expression is then used to formulate a second faster algorithm.

2 Tate pairing

Let X/k be an algebraic curve over a finite field k. Let **Div** be the group of divisors on X, $\mathbf{Div_0}$ the subgroup of divisors of degree zero, **Prin** the subgroup of principal divisors, and $\Gamma = \mathbf{Div_0}/\mathbf{Prin}$ the group of divisor classes of degree zero. For $m > 0$ prime to char k, let

$$\Gamma[m] = \{[D] \in \Gamma : mD \text{ is principal}\}.$$

For a rational function f and a divisor $E = \sum n_P P$ with $(f) \cap E = \emptyset$, let

$$f(E) = \prod f(P)^{n_P} \in k^*.$$

Theorem 1 ([FR94], [H02b]). *The Tate pairing*

$$\begin{aligned} \{-,-\}_m :\ & \Gamma[m] \times \Gamma/m\Gamma \longrightarrow k^*/k^{*m}, \\ & \{[D], [E]\}_m = f_D(E), \end{aligned}$$

is well-defined on divisor classes. The pairing is non-degenerate if and only if the constant field k of X contains the m-th roots of unity. Here, f_D is such that $(f_D) = mD$, and we assume that the classes are represented by divisors with disjoint support: $D \cap E = \emptyset$.

For an elliptic curve E/k we can identify Γ with the group of rational points on the curve using an isomorphism $E(k) \simeq \Gamma$, $P \mapsto [P - O]$. For an elliptic curve E/k, and for $D = [P - O]$, efficient computation of $f_D(Q)$ in the Tate pairing is achieved with a square-and-multiply strategy using Miller's algorithm in base 2 [M86].

3 The BKLS-Algorithm

Let $E^+ : y^2 = x^3 - x + 1$ and $E^- : y^2 = x^3 - x - 1$ be twisted elliptic curves over the field F_3 of three elements. Their cryptographic applications have been studied in [K98], [DS98]. Let N be the number of points on E^+ or E^- over an extension field $k = F_{3^n}$ such that $\gcd(n, 6) = 1$. Then the Tate pairing

$$\begin{aligned} \{-,-\}_N :\ & \Gamma[N] \times \Gamma/N\Gamma \longrightarrow K^*/K^{*N}, \\ & \{[D],[E]\}_N = f_D(E), \end{aligned}$$

is non-degenerate for an extension K/k of degree $[K : k] = 6$. For the extension K/k, $E(K)$ contains the full N-torsion and the Weil pairing is also non-degenerate [MOV93].

For the curves E^b, $b = \pm 1$, multiplication $V \mapsto 3V$ is particularly simple. For $V = (\alpha, \beta)$, $3V = (\alpha^9 - b, -\beta^9)$. Also, taking the cube of a scalar $f \mapsto f^3$ in characteristic three has linear complexity on a normal basis. Thus, Miller's algorithm will perform faster for these curves in a cube-and-multiply version (Algorithm 1).

Next we describe further improvements to Algorithm 1 proposed in [BKLS02], [GHS02]. We consider the curve $E^b/k : y^2 = x^3 - x + b$, for $b = \pm 1$. We assume k is of finite degree $[k : F_3] = n$ with $\gcd(n, 6) = 1$. And we let F/k and K/k be extensions of degree $[F : k] = 3$ and $[K : k] = 6$, respectively. The following theorem and lemma are similar to Theorem 1 and Lemma 1, respectively, in [BKLS02].

Theorem 2. *Let $N = |E(k)|$. Let $P, O \in E(k)$ be distinct points, and let g_P be a k-rational function with $(g_P) = N(P - O)$. For all $Q \in E(K)$, $Q \neq P, O$,*

$$\{[P - O], [Q - O]\}_N{}^{|K^*|/N} = g_P(Q)^{|K^*|/N} \in K^*.$$

Proof. Taking a power of the Tate pairing gives a non-degenerate pairing with values in K^* instead of K^*/K^{*N}. We give a different proof to show that the point O in $Q - O$ can be ignored. Let t_O be a k-rational local parameter for O, i.e. t_O vanishes to the order one in O. We may assume that $(t_O) \cap P = \emptyset$. Thus $Q - O + (t_O) \sim Q - O$, such that $Q - O + (t_O) \cap P - O = \emptyset$. With the following lemma, $g_P(Q - O + (t_O)) = g_P(Q) \in K^*/K^{*N}$. □

Algorithm 1 Miller's algorithm, cube-and-multiply [GHS02], [BKLS02]

INPUT: $P, Q \in E(K), (a_i) \in \{0, \pm 1\}^s$.

$\{a = 3^s + a_1 3^{s-1} + \cdots + a_{s-1}3 + a_s.\}$

OUTPUT: $f_a(Q)$.

$\{(f_a) = a(P) - (aP) - (a-1)O,\ (l_{A,B}) = A + B + (-A-B) - 3O.\}$

$a \leftarrow 1,\ V \leftarrow P,\ f \leftarrow 1$
for $i = 1$ to s **do**
  $g \leftarrow l_{V,V}/l_{2V,O} \cdot l_{V,2V}/l_{3V,O}(Q)$
  $a \leftarrow 3a,\ V \leftarrow 3V,\ f \leftarrow f^3 \cdot g$
  if $a_i = \pm 1$ **then**
    $g \leftarrow l_{\pm P,V}/l_{V \pm P,O}(Q)$
    $a \leftarrow a \pm 1,\ V \leftarrow V \pm P,\ f \leftarrow f \cdot g$
  end if
  $\{a \leftarrow 3^i + a_1 3^{i-1} + \cdots + a_{i-1}3 + a_i,\ V \leftarrow aP,\ f \leftarrow f_a(Q).\}$
end for

Algorithm 2 $E/k : y^2 = x^3 - x + b$ [BKLS02]

INPUT: $P \in E(k), Q = (x, y) \in F \times K, a = 3^{2m-1} \pm 3^m + 1$.

$\{[k : F_3] = 2m - 1, [F : k] = 3, [K : k] = 6, a = |E(k)|.\}$

OUTPUT: $f_a(Q)$.

$\{(f_a) = a(P) - (aP) - (a-1)O,\ (l_{A,B}) = A + B + (-A-B) - 3O.\}$

$V \leftarrow P,\ a \leftarrow 1,\ f \leftarrow 1$
for $i = 1$ to $m - 1$ **do**
  $g \leftarrow l_{V,V} l_{V,-3V}(Q)$
  $a \leftarrow 3a,\ V \leftarrow 3V,\ f \leftarrow f^3 \cdot g\ \{a = 3, \ldots, 3^{m-1}\}$
end for
$g \leftarrow l_{\pm P,V}(Q)$
$a \leftarrow a \pm 1,\ V \leftarrow V \pm P,\ f \leftarrow f \cdot g\ \{a = 3^{m-1} \pm 1\}$
for $i = 1$ to m **do**
  $g \leftarrow l_{V,V} l_{V,-3V}(Q)$
  $a \leftarrow 3a,\ V \leftarrow 3V,\ f \leftarrow f^3 \cdot g\ \{a = 3^m + 3, \ldots, 3^{2m-1} \pm 3^m\}$
end for
$g \leftarrow l_{P,V}(Q)$
$a \leftarrow a + 1,\ V \leftarrow V + P,\ f \leftarrow f \cdot g\ \{a = 3^{2m-1} \pm 3^m + 1\}$

Lemma 1. *Let $N = |E(k)|$. For a F-rational function f and for a F-rational divisor R such that $(f) \cap R = \emptyset$,*

$$f(R) = 1 \in K^*/{K^*}^N.$$

Proof. We have $f(R) \in F^*$. The group order N is an odd divisor of $3^{3n} + 1$. Therefore, the group order N is coprime to $3^{3n} - 1$. And $F^* = {F^*}^N \subset {K^*}^N$. □

Definition 1 ([BKLS02]). Let $\rho \in F_{3^3}$ be a root of $\rho^3 - \rho - b = 0$. Let $\sigma \in F_{3^2}$ be a root of $\sigma^2 + 1 = 0$. Define the distortion map

$$\phi : E(K) \to E(K), \quad \phi(x, y) = (\rho - x, \sigma y). \tag{1}$$

Combine the distortion map with Theorem 2 to obtain a pairing

$$E(k) \times E(k) \longrightarrow K^*, \quad (P, Q) \mapsto g_P(\phi(Q))^{|K^*|/N} \in K^*. \tag{2}$$

The curve $y^2 = x^3 - x + b$ has complex multiplication by -1 and the distortion map corresponds to multiplication by $\sqrt{-1}$. Indeed, ϕ is an automorphism of E,

$$(\sigma y)^2 = -y^2 = -x^3 + x - b = (\rho - x)^3 - (\rho - x) + b.$$

And $\phi^2 = -1$. The following remark is used in Theorem 3 [BKLS02] to discard contributions of the form $l_{P,O}(\phi(Q))$ in the evaluation of the Tate pairing.

Remark 1. Let $P \in E(k)$, $Q \in F \times K$, and let $l_{P,O}$ be the vertical line through P. Then $l_{P,O}(\phi(Q)) = 1 \in K^*/{K^*}^N$.

We summarize the differences between Algorithm 1 and Algorithm 2.

1. The distortion map gives a non-degenerate pairing on $E(k) \times E(k)$.
2. Because of the simple ternary expansion of N, a single loop of length $2m - 1$ containing an if statement for the adding can be replaced with two smaller loops each followed by an unconditional addition.
3. The denominators in $l_{V,V}/l_{2V,O} \cdot l_{V,2V}/l_{3V,O}$ are omitted. For $P \in E(k), x_Q \in F$, they do not affect the value of the Tate pairing.
4. The line $l_{V,2V}$ is written $l_{V,-3V}$. Since the points $V, 2V$ and $-3V$ lie on a line, the expressions are the same, but $-3V$ is easier to compute than $2V$. For $V = (\alpha, \beta)$, $-3V = (\alpha^9 - b, \beta^9)$.

We give a further analysis of Algorithm 2 in the following section.

4 A closed formula for the BKLS-Algorithm

Let $E^b/k : y^2 = x^3 - x + b$ be an elliptic curve as in Section 3. Recall from Definition 1 in Section 3 the pairing $E(k) \times E(k) \longrightarrow K^*$,

$$(P, Q) \mapsto g_P(\phi(Q))^{|K^*|/N} \in K^*.$$

For the efficient evaluation of $g_P(\phi(Q))$ we use Algorithm 2.

Remark 2. We make three remarks. They all reflect that the lines that are computed by the algorithm can be precomputed.

1. After the first loop, we have, for $P = (\alpha^3, \beta^3)$,
$$l_{\pm P,V} = \pm y - \beta(x - \alpha + b).$$
2. After the second loop $V = (3^{2m-1} \pm 3^m)P = -P$, and multiplication by $l_{P,-P}(Q) = l_{P,0}(Q)$ can be omitted.
3. Inside each loop, if we omit only the denominator $l_{3V,O}$, we find
$$(l_{V,V} l_{V,-3V}/l_{2V,O}) = 3V + (-3V) - 4O.$$
For $V = (\alpha, \beta)$, the function $h_V : \beta^3 y - (\alpha^3 - x + 1)^2$ has the same divisor. We claim that using h_V in place of $l_{V,V} l_{V,-3V}$ uses fewer operations.

Theorem 3 (Algorithm 2 in closed form). *Let*
$$P = (\alpha^3, \beta^3) \in E(k), \quad Q = (x, y) \in E(k), \quad \phi(Q) = (\rho - x, \sigma y).$$
Then, for g_P with $(g_P) = N(P - Q)$, $g_P(\phi(Q))$ is the product of
$$\prod_{i=1}^{m-1} (\sigma\beta^{(i)} y^{(n-i)} - (\alpha^{(i)} + x^{(n-i)} - \rho + mb)^2),$$
$$\prod_{i=m}^{2m-1} (\sigma\beta^{(i)} y^{(n-i)} - (\alpha^{(i)} + x^{(n-i)} - \rho)^2),$$
$$(\pm\sigma y - \beta(\rho - x - \alpha + b))^{(m)}.$$

The second remark is clear. In the remainder of this section we first prove the third remark, then the first remark and finally the theorem.

Lemma 2. *Let $l_{A,B}$ be the line through A and B. For $V = (\alpha, \beta) \in E(K)$,*
$$\begin{aligned}
&l_{V,V} : (x - \alpha) - \beta(y - \beta) = 0,\\
&l_{2V,O} : x - \alpha - 1/\beta^2 = 0,\\
&l_{2V,V} : (\beta^4 - 1)(x - \alpha) - \beta(y - \beta) = 0,\\
&l_{3V,O} : x - \alpha^9 + b = 0.
\end{aligned}$$

The lines $l_{V,V}, l_{2V,V}$ correspond to l_1 and l_1', respectively, in [GHS02], up to a slight difference to reduce the number of operations. For the third remark, we compare the number of operations (Multiplication, Squaring, Addition, Frobenius).

$g \leftarrow l_{V,V} l_{V,-3V}, f \leftarrow f^3 \cdot g$	(4M,4A,1F)
$g \leftarrow h_V, f \leftarrow f^3 \cdot g$	(2M,1S,2A,2F)

To establish the first remark we use the following lemma.

Lemma 3. *Let $(\alpha,\beta)\in E^b(\bar F_3)$. The line $l: by-\beta(x-\alpha+b)=0$ has divisor*

$$(\alpha,\beta)\ +\ (\alpha+b,-\beta)\ +\ (\alpha^3,b\beta^3)\ -\ 3O.$$

Let $(\alpha,\beta)\in E^b(k)$, for k of degree $[k:F_3]=n=2m-1$ with $\gcd(6,n)=1$.

$$\begin{array}{ll} n=1(\mathrm{mod}\ 3): & 3^n(\alpha+b,-\beta)=(\alpha,\beta),\ \ 3^m(\alpha+b,-\beta)=(\alpha^3,(-1)^{m+1}\beta).\\ n=2(\mathrm{mod}\ 3): & 3^n(\alpha,\beta)=(\alpha+b,-\beta),\ \ 3^m(\alpha,\beta)=(\alpha^3,(-1)^m\beta).\end{array}$$

Proof. The first claim is obvious. The last claim uses

$$V=(\alpha,\beta)\Rightarrow 3V=(\alpha^9-b,-\beta^9).$$

□

We summarize in a table.

	$n=1(\mathrm{mod}\ 3), m=1(\mathrm{mod}\ 3)$	$n=2(\mathrm{mod}\ 3), m=0(\mathrm{mod}\ 3)$
(α,β)	3^nW	W
$(\alpha+b,-\beta)$	W	3^nW
$(\alpha^3,b\beta^3)$	$\epsilon 3^mW$	$\epsilon 3^mW$
ϵ	$(-1)^{m-1}b$	$(-1)^mb$

With the value of ϵ from the table, $|E(k)|=3^n+1+\epsilon 3^m$.

Proposition 1. *We apply the lemma. Let $P=(\alpha^3,\beta^3)\in E^b(k)$, for k of degree $[k:F_3]=n=2m-1$ with $\gcd(6,n)=1$. The line through ϵP and $V=3^{m-1}P$ has equation*

$$l_{\epsilon P,V}:\epsilon y-\beta(x-\alpha+b)=0.$$

The third point on the line $l_{\epsilon P,V}$ is $(\alpha+mb,(-1)^m\beta)$.

Proof. Write $P=3^mW$, so that $V=3^nW$. Then W is the third point on the line through ϵP and V. And W can be obtained as the unique solution to $3^mW=P$.

□

This proves the first remark. We can now prove Theorem 3.

Proof. The contribution of the first loop to $g_P(\phi(Q))$ is

$$\begin{aligned}
&\prod_{i=1}^{m-1}((-1)^{i-1}\beta^{(2i)}(\sigma y)-(\alpha^{(2i)}-(i-1)b-(\rho-x)+b)^2)^{(2m-1-i)}\\
&=\prod_{i=1}^{m-1}((-1)^{i-1}\beta^{(i)}(\sigma^{(n-i)}y^{(n-i)}\\
&\qquad-(\alpha^{(i)}-(i-1)b-(\rho+(2m-1-i)b-x^{(n-i)})+b)^2)\\
&=\prod_{i=1}^{m-1}(\beta^{(i)}y^{(n-i)}\sigma-(\alpha^{(i)}+x^{(n-i)}-\rho+mb)^2).
\end{aligned}$$

The second loop starts with $V=(\alpha+mb,(-1)^m\beta)$ instead of $V=P=(\alpha^3,\beta^3)$ and is of length m instead of length $m-1$. It gives a contribution

$$\begin{aligned}
&\prod_{i=1}^{m}((-1)^{i+m}\beta^{(2i-1)}(\sigma y)-(\alpha^{(2i-1)}+(m+1-i)b-(\rho-x)+b)^2)^{(m-i)}\\
&=\prod_{i=1}^{m}((-1)^{i+m}\beta^{(m-1+i)}\sigma^{(m-i)}y^{(m-i)}\\
&\qquad-(\alpha^{(m-1+i)}+(m+1-i)b-(\rho+(m-i)b-x^{(m-i)})+b)^2)\\
&=\prod_{i=m}^{2m-1}(\beta^{(i)}y^{(n-i)}\sigma-(\alpha^{(i)}+x^{(n-i)}-\rho-b)^2).
\end{aligned}$$

The contribution from $l_{\epsilon P,V}$ follows directly from the proposition 1. This proves Theorem 3. $\square$

5 The curve $C^d: y^2 = x^p - x + d$

Let C^d/k be the hyperelliptic curve $y^2=x^p-x+d$, $d=\pm1$, for $p\equiv 3 \pmod 4$. We assume that k is of degree $[k:F_p]=n$, for $\gcd(2p,n)=1$, and we let F/k and K/k be the extensions of degree $[F:k]=p$ and degree $[K:k]=2p$, respectively. Thus C^d is a direct generalization of the elliptic curve E^b studied in the previous sections. Over the extension field K, the curve is the quotient of a hermitian curve, hence is Hasse-Weil maximal. And the class group over K is annihilated by $p^{pn}+1$. The last fact can be seen also from the following lemma. It shows that for $P\in C^d(K)$, $(p^{pn}+1)(P-O)$ is principal. We write $x^{(i)}$ for x^{p^i}.

Lemma 4 ([D96],[DS98]). *Let $P=(\alpha,\beta)\in C^d$. The function*

$$h_P=\beta^p y-(\alpha^p-x+d)^{(p+1)/2}$$

has divisor $(h_V)=p(V)+(V')-(p+1)O$, where

$$V'=(\alpha^{(2)}+d^p+d,\beta^{(2)}).$$

We will write V also for the divisor class $V-O$, so that $V'=-pV$. In particular $p^{pn}P=-P$, for $P\in C(K)$ and for $\mathrm{Trace}_{K/F_p}d=0$. Let $M=p^{pn}+1=|K^*|/|F^*|$. Thus, the order of $P-O$ in the divisor class group Γ is a divisor of M. The precise order N of the class group can be obtained from the zeta functions for C^d in [D96], [DS98]. We will only need the following lemma.

Lemma 5. *Let Γ^d denote the class group of the curve C^d/k.*

$$|\Gamma^+(k)||\Gamma^-(k)|=(p^{pn}+1)/(p^n+1)$$

In particular, $N=|\Gamma(k)|$ is an odd divisor of $M=p^{pn}+1$.

We include the size of the class group for $p = 7$. Let $[k : F_7] = n$ and $m = (n+1)/2$. Then

$$|\Gamma^+(k)| = (1+7^n)^3 + (\frac{7}{n})7^m(1+7^n+7^{2n}).$$
$$|\Gamma^-(k)| = (1+7^n)^3 - (\frac{7}{n})7^m(1+7^n+7^{2n}).$$

And $|\Gamma^+(k)||\Gamma^-(k)| = (1+7^{7n})/(1+7^n)$.

6 Main theorem

Miller's algorithm for the Tate pairing on an elliptic curve E/k uses lines as building blocks to construct other rational functions. In our version of the Tate pairing implementation, we will not rely on lines but on the functions described in Lemma 4. So that we can generalize from elliptic curves $E^b/k : y^2 = x^3 - x + b$, $b = \pm 1$, to hyperelliptic curves $C^d/k : y^2 = x^p - x + d$, $d = \pm 1$, for $p \equiv 3 \pmod 4$. Generalization of the results in Section 3 poses no problem.

Theorem 4. *Let $N = |\Gamma(k)|$, so that N divides $M = p^{pn} + 1 = |K^*|/|F^*|$. Let $P, O \in C(k)$ be distinct points. Let f_P be a k-rational function with $(f_P) = M(P - O)$. For all $Q \in C(K)$, $Q \neq P, O$,*

$$\{[P - O], [Q - O]\}_M{}^{|K^*|/M} = f_P(Q)^{|F^*|} \in K^*.$$

Proof. The argument that shows that the contribution by O can be omitted is the same as in Theorem 2. □

The difference with Theorem 2 is that f_P is computed with a multiple M of N instead of with N itself. The multiple M has trivial expansion in base p and this leads to Algorithm 3 which has no logical decisions (only point multiplication by p and no adding). See also Remark in Section 6 of [GHS02]. But it has pn iterations compared to n iterations in Algorithm 2 (for the case $p = 3$). After Theorem 5, we will reduce this to n iterations in Algorithm 4. The following generalizations of Lemma 1 and Remark 1 are straightforward.

Lemma 6. *Let $N = |\Gamma(k)|$. For a F-rational function f and for a F-rational divisor E such that $(f) \cap E = \emptyset$,*

$$f(E) = 1 \in K^*/K^{*N}.$$

Proof. We have $f(E) \in F^*$. The group order N is an odd divisor of $p^{pn} + 1$. Therefore, the group order N is coprime to $p^{pn} - 1$. And $F^* = F^{*N} \subset K^{*N}$. □

Remark 3. Let $P \in E(F)$, $Q \in F \times K$, and let $l_{P,O}$ be the vertical line through P. Then $l_{P,O}(\phi(Q)) = 1 \in K^*/K^{*N}$.

Algorithm 3 $C/k : y^2 = x^p - x + d.$

INPUT: $P \in C(k), Q \in C(K), a = p^{pn} + 1$

$\{[k : F_p] = n, [K : k] = 2p, a = |K^*|/|F^*|.\}$

OUTPUT: $f_a(Q) \in K^*/F^*$

$\{(f_a) = a(P) - (aP) - (a-1)O,\ (h_V) = p(V) + (-pV) - (p+1)O.\}$

$V \leftarrow P,\ a \leftarrow 1,\ n \leftarrow 1,\ d \leftarrow 1$
for $i = 1$ to pn **do**
  $g \leftarrow h_V(Q)$
  $a \leftarrow pa,\ V \leftarrow pV,\ f \leftarrow f^p \cdot g$
end for

Definition 2. *Let $\rho \in F$ be a root of $\rho^p - \rho + 2d = 0$. Let $\sigma, \bar\sigma \in K$ be the roots of $\sigma^2 + 1 = 0$. Define the distortion map*

$$\phi : C(K) \to C(K), \quad \phi(x, y) = (\rho - x, \sigma y). \tag{3}$$

Combine the distortion map with Theorem 4 to obtain a pairing

$$C(k) \times C(k) \longrightarrow K^*, \quad (P, Q) \mapsto f_P(\phi(Q))^{|F^*|} \in K^*. \tag{4}$$

Indeed, $(\sigma v)^2 = -v^2 = -u^p + u - d = (\rho - u)^p - (\rho - u) + d.$

Theorem 5 (Main Theorem). *For $P = (\alpha, \beta), Q = (x, y) \in C(k)$,*

$$f_P(\phi(Q)) = \prod_{i=1}^{n} (\beta^{(i)} y^{(n+1-i)} \bar\sigma - (\alpha^{(i)} + x^{(n+1-i)} - \rho + d)^{(p+1)/2}).$$

Proof. From Algorithm 3, we see that

$$f_P(\phi(Q)) = \prod_{i=1}^{pn} (h_{p^{i-1}P}(\phi(Q))^{(pn-i)}.$$

Substitution of

$$\begin{aligned} h_P(Q) &= \beta^p y - (\alpha^p - x + d)^{(p+1)/2} \\ p^{i-1}P &= (\alpha^{(2i-2)} + (i-1)2d, (-1)^{i-1}\beta^{(2i-2)}) \\ \phi(Q) &= (\rho - x, \sigma y) \end{aligned}$$

yields

$$\begin{aligned} &\prod_{i=1}^{pn} ((-1)^{i-1}\beta^{(2i-1)}(\sigma y) - (\alpha^{(2i-1)} + (i-1)2d - (\rho - x) + d)^{(p+1)/2})^{(pn-i)} \\ &= \prod_{i=1}^{pn} ((-1)^{i-1}\beta^{(i-1)}\sigma^{(pn-i)}y^{(pn-i)} \\ &\qquad - (\alpha^{(i-1)} + (i-1)2d - (\rho - (pn-i)2d - x^{(pn-i)}) + d)^{(p+1)/2}). \end{aligned}$$

Or, since $\alpha, \beta, x, y \in k$, and since $(-1)^{i-1}\sigma^{(pn-i)} = \sigma$, for both i odd and i even,

$$\prod_{i=1}^{n} (\beta^{(i-1)} y^{(n-i)} \sigma - (\alpha^{(i-1)} - \rho + x^{(n-i)} - d)^{(p+1)/2})^p$$
$$= \prod_{i=1}^{n} (\beta^{(i)} y^{(n+1-i)} \bar{\sigma} - (\alpha^{(i)} + x^{(n+1-i)} - \rho^p - d)^{(p+1)/2}).$$

Finally, $-\rho^p - d = -\rho + d$. □

Note that $f_P(\phi(Q)) = f_Q(\phi(P))$, as it should.

Algorithm 4 $C/k : y^2 = x^p - x + d$.

INPUT: $P = (\alpha, \beta) \in C(k)$, $Q = (\rho - x, \sigma y), (x, y) \in C(k)$, $a = p^{pn} + 1$

$\{[k : F_p] = n, \rho^p - \rho + 2d = 0, \sigma^2 + 1 = 0.\}$

$\{[F : F_p] = pn, [K : F_n] = 2pn, a = |K^*|/|F^*|.\}$

OUTPUT: $f_a(Q) \in K^*/F^*$

$\{(f_a) = a(P) - (aP) - (a-1)O.\}$

```
for i = 1 to n do
  α ← α^3, β ← β^3
  g ← (βyσ̄ − (α + x − ρ + d)^((p+1)/2))
  f ← f · g
  x ← x^(1/3), y ← y^(1/3)
end for
```

Summarizing, using a Tate pairing $\{-,-\}_M$ instead of $\{-,-\}_N$ removes all logic and all additions from Algorithm 2. When using the version Algorithm 4 the number of iterations is similar to Algorithm 2. Which gives the following advantages for Algorithm 4.

1. Uniform algorithm that applies to all $p \equiv 3 \pmod 4$.
2. Expressing $N = |\Gamma(k)|$ in base p can be omitted.
3. Expressing $|K^*|/N$ in base p, for raising $g_P(Q)$ to the power $|K^*|/N$, can be omitted. It is replaced with raising to the power $|F^*|$.
4. At each iteration, only multiplication by p is required, no additions.
5. Multiplication by p using the function h_P is faster than using a product of lines (case $p = 3$).

7 Concluding remarks

Theorem 3 for elliptic curves and its generalization Theorem 5 for hyperelliptic curves give closed formulae to evaluate the Tate pairing on curves of the form

$y^2 = x^p - x + d$. The complexity estimate after Lemma 3 indicates a speed-up by a factor two over algorithms described in [BKLS02] and [GHS02] when using Theorem 3 to evaluate the Tate pairing. Timing comparisons by Keith Harrison confirm this estimate. A running time comparison for the closed formula for hyperelliptic curves remains to be done. We thank Steven Galbraith, Paulo Barreto, Doug Kuhlman, Keith Harrison and anonymous referees for their helpful feedback on the preprint version.

References

[PBCL] The Pairing-Based Crypto Lounge, http://planeta.terra.com.br/informatica/paulobarreto/pblounge.html

[BKLS02] P. S. L. M. Barreto, H. Y. Kim, B. Lynn, M. Scott, "Efficient Algorithms for Pairing-Based Cryptosystems." Advances in Cryptology – Crypto 2002, Lecture Notes in Computer Science, Vol. 2442, Springer-Verlag, pp. 354–368, (2002).

[BSS99] I. Blake, G. Seroussi, and N.P. Smart, Elliptic curves in cryptography. London Mathematical Society LNS, 265. Cambridge University Press, Cambridge, 1999 (reprinted 2000).

[BF01] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing." Advances in Cryptology, Crypto 2001, Lecture Notes in Computer Science, Vol. 2139, Springer-Verlag, pp. 213-229, (2001).

[BS02] D. Boneh and A. Silverberg, "Applications of multilinear forms to cryptography." Contemporary Mathematics, Vol. 324, American Mathematical Society, pp. 71-90, (2003).

[CC03] J. C. Cha, J. H. Cheon, "An Identity-Based Signature from Gap Diffie-Hellman Groups." Proceedings of PKC, Lecture Notes in Computer Science, Vol. 2567, pp. 18-30, (2003).

[DH76] W. Diffie and M. Hellman. "New direction in cryptography." IEEE Trans. Information Theory, IT-22(6), pp. 644-654, (1976).

[D96] I. Duursma, "Class numbers for hyperelliptic curves." In: "Arithmetic, Geometry and Coding Theory." eds. Pellikaan, Perret, Vladuts, pp. 45-52, publ. deGruyter, Berlin, 1996.

[DS98] I. Duursma, K. Sakurai, "Efficient algorithms for the Jacobian variety of hyperelliptic curves $y^2 = x^p - x + 1$ over a finite field of odd characteristic p." Coding theory, cryptography and related areas (Guanajuato, 1998), pp. 73–89, Springer, Berlin, 2000.

[FR94] G. Frey, H.-G. Rück, "A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves." Math. Comp. 62, no. 206, pp. 865–874, (1994).

[G01] S.D. Galbraith, "Supersingular curves in cryptography." Asiacrypt 2001, Springer, Lecture Notes in Computer Science, Vol. 2248, 495–513, (2001).

[GHS02] S. D. Galbraith, K. Harrison, D. Soldera, "Implementing the Tate pairing." Algorithmic Number Theory Symposium, ANTS-V, Lecture Notes in Computer Science, Vol. 2369, Springer-Verlag, pp. 324–337, (2002).

[H02a] F. Hess, Exponent group signature schemes and efficient identity based signature schems based on pairing, Proceedings of the Workshop Selected Areas in Cryptology, SAC, Aug. 2002.

[H02b] F. Hess, “A Note on the Tate Pairing of Curves over Finite Fields,” 2002. Available on http://www.math.tu-berlin.de/ hess.

[IT02] T. Izu and T. Takagi, “Efficient Computations of the Tate Pairing for the Large MOV degrees.” 5th International Conference on Information Security and Cryptology, ICISC 2002, Springer-Verlag, Lecture Notes in Computer Science, Vol. 2587, pp. 283-297, (2003).

[J00] A. Joux, “A one round protocol for tripartite Diffie-Hellman.” Proceedings of Algorithmic Number Theory Symposium, Lecture Notes in Computer Science, Vol. 1838, Springer-Verlag, pp. 385-394, (2000).

[K98] N. Koblitz, “An elliptic curve implementation of the finite field digital signature algorithm.” Advances in cryptology, Crypto 1998, Lecture Notes in Computer Science, Vol. 1462, Springer, Berlin, pp. 327–337, 1998.

[M86] V. Miller, “Short Programs for Functions on Curves.” Unpublished manuscript, 1986.

[MOV93] A. Menezes, T. Okamoto and S. Vanstone, “Reducing elliptic curve logarithms to logarithms in a finite field.” IEEE Trans. on Inform. Theory 39, pp. 1639–1646, (1993).

[P02] K.G. Paterson, ID-based signature from pairings on elliptic curves, Electronics Letters, Vol. 38 (18), pp. 1025-1026, (2002).

[SOK00] R. Sakai, K. Ohgishi and M. Kasahara, “Cryptosystems based on pairing.” Symposium on cryptography and Information Security, Okinawa, Japan, pp. 26-28, (2000)

[S02] N.P. Smart, An identity based authentication key agreement protocol based on pairing, Electronics Letters, Vol 38, pp 630-632, (2002).