On the Selection of Pairing-Friendly Groups

Paulo S. L. M. Barreto[1], Ben Lynn[2], and Michael Scott[3]

[1] Universidade de São Paulo, Escola Politécnica.
Av. Prof. Luciano Gualberto, tr. 3, 158.
BR 05508-900, São Paulo(SP), Brazil.
pbarreto@larc.usp.br
[2] Computer Science Department, Stanford University, USA.
blynn@cs.stanford.edu
[3] School of Computer Applications
Dublin City University
Ballymun, Dublin 9, Ireland.
mscott@indigo.ie

Abstract. We propose a simple algorithm to select group generators suitable for pairing-based cryptosystems. The selected parameters are shown to favor implementations of the Tate pairing that are at once conceptually simple and very efficient, with an observed performance about 2 to 10 times better than previously reported implementations.
Keywords: pairing-based cryptosystems, group generators, elliptic curves, Tate pairing.

1 Introduction

Pairing-based cryptosystems are currently one of the most active areas of research in elliptic curve cryptography, as we see from the abundance of recent literature on the subject. Computation of the Tate pairing over certain elliptic curve groups is a central operation — and often a bottleneck — in such systems.

A subgroup G of (the group of points of) an elliptic curve $E(\mathbb{F}_q)$ is said to have *embedding degree* k if its order r divides $q^k - 1$, but does not divide $q^i - 1$ for all $0 < i < k$. Given a curve $E(\mathbb{F}_q)$ known to contain a subgroup of prime order r with embedding degree k, we investigate the problem of finding suitable points $P \in E(\mathbb{F}_q)$ of order r and $Q \in E(\mathbb{F}_{q^k})$ linearly independent from P, such that the restricted Tate pairing $e : \langle P \rangle \times \langle Q \rangle \to \mathbb{F}_{q^k}^*$ is efficiently computable.

Efficient algorithms for supersingular curves have been proposed [1, 8, 11]. However, there is a widespread feeling that supersingular curves should be avoided whenever possible, as they may be more susceptible to attacks than ordinary curves. Additionally, choices of k are very limited for supersingular curves, and the larger values only occur over fields of small characteristic [15, section 5.2.2], which are more vulnerable to Coppersmith's discrete logarithm attack [6]. Protecting against this attack increases bandwidth requirements (larger fields), and while this may not be an issue in some situations, it is a central concern in many cases (e.g. short BLS signatures [5]). Thus we would like to find

similar optimizations for ordinary curves over fields of large characteristics containing subgroups of manageable embedding degree [2, 7, 17].

We show how to select groups in nonsupersingular curves where many optimizations proposed for supersingular curves [1] have a counterpart. In particular, we show how to perform elimination of irrelevant factors and denominators during the computation of the Tate pairing, which is rendered conceptually simpler and substantially more efficient.

This paper is organized as follows. Section 2 recalls some concepts essential to the discussion of pairings. Section 3 describes our group selection algorithm. Section 4 examines how the selected groups lead to efficient implementation of the Tate pairing. We present our results in section 5.

2 Preliminaries

We briefly review the most relevant concepts underlying pairing-based cryptography. In what follows, let $E(\mathbb{F}_q)$ be a curve containing a subgroup of prime order r with embedding degree k.

2.1 The Frobenius endomorphism

The *Frobenius endomorphism* is the mapping $\Phi : E(\mathbb{F}_{q^k}) \to E(\mathbb{F}_{q^k})$, $(X, Y) \mapsto (X^q, Y^q)$. Thus a point $P \in E(\mathbb{F}_{q^k})$ is defined over $\mathbb{F}_{q^i}$ if and only if $\Phi^i(P) = P$; in particular, $\Phi^k(P) = P$ for any $P \in E(\mathbb{F}_{q^k})$.

The characteristic polynomial of the Frobenius endomorphism is the polynomial $\pi(u) = u^2 - tu + q$. The value t is called the trace of the Frobenius endomorphism, not to be confused with the trace map defined below. The polynomial π factorizes as $\pi(u) = (u-1)(u-q) \pmod r$, so the Frobenius admits an eigenvector Q of order r associated to $q \pmod r$, i.e. $\Phi(Q) = [q]Q$ and $[r]Q = O$. Since, by definition, $r \mid q^k - 1$ but $r \nmid q^i - 1$ for any $0 < i < k$, clearly $r \mid (q^k - 1)/(q-1)$ and hence $[(q^k - 1)/(q - 1)]Q = O$.

2.2 The trace map

The *trace map* is the mapping $\mathrm{tr} : E(\mathbb{F}_{q^k}) \to E(\mathbb{F}_q)$ defined as $\mathrm{tr}(P) = P + \Phi(P) + \Phi^2(P) + \cdots + \Phi^{k-1}(P)$. We have $\mathrm{tr}(\Phi(P)) = \Phi(\mathrm{tr}(P)) = \mathrm{tr}(P)$ for any $P \in E(\mathbb{F}_{q^k})$, (which shows that the the range of the map is indeed $E(\mathbb{F}_q)$).

Lemma 1. *If k is coprime to the order of $E(\mathbb{F}_{q^k})$, $E(\mathbb{F}_q)$ is the eigenspace of the trace map with eigenvalue k.*

Proof. Clearly, all points $R \in E(\mathbb{F}_{q^k})$ defined over $\mathbb{F}_q$ satisfy $\mathrm{tr}(R) = [k]R$, hence we only need to show that all points $R \in E(\mathbb{F}_{q^k})$ such that $\mathrm{tr}(R) = [k]R$ are defined over $\mathbb{F}_q$. Indeed, if $\mathrm{tr}(R) = [k]R$, then $\Phi(\mathrm{tr}(R)) = \Phi([k]R) = [k]\Phi(R)$, but since $\Phi(\mathrm{tr}(R)) = \mathrm{tr}(R)$, it follows that $[k]\Phi(R) = \mathrm{tr}(R) = [k]R$ and thus $[k](\Phi(R) - R) = O$. As k is coprime to the order of R, necessarily $\Phi(R) - R = O$, hence R must be defined over $\mathbb{F}_q$, that is, $R \in E(\mathbb{F}_q)$. Therefore, $E(\mathbb{F}_q)$ is the eigenspace of the trace map with eigenvalue k. □

For an eigenvector Q of order r associated to the eigenvalue $q \pmod r$ of the Frobenius, the trace map satisfies $\mathrm{tr}(Q) = Q + [q]Q + [q^2]Q + \cdots + [q^{k-1}]Q = [(q^k - 1)/(q - 1)]Q = O$, as we pointed out above.

2.3 The twist of a curve

The *twist* of a curve given in short Weierstraß form $E : y^2 = x^3 + ax + b$ is the curve $E' : y^2 = x^3 + a'x + b'$ with $a' = v^2a$ and $b' = v^3b$ for some quadratic non-residue $v \in \mathbb{F}_q$. The orders of the groups of rational points of these curves satisfy the relation $\#E(\mathbb{F}_q) + \#E'(\mathbb{F}_q) = 2q + 2$ [3, section III.3].

2.4 Divisors and the Tate pairing

Let $E(\mathbb{F}_q)$ be an elliptic curve containing a subgroup of prime order r with embedding degree k. A *divisor*[4] on E is a formal sum $D = \sum_{P \in E(\mathbb{F}_{q^k})} n_P(P)$ where $n_P \in \mathbb{Z}$.

The set of points $P \in E(\mathbb{F}_{q^k})$ such that $n_P \neq 0$ is called the support of D. The degree of D is the value $\deg(D) = \sum_P n_P$. The null divisor, denoted 0, has all $n_P = 0$. The sum of two divisors $D = \sum_P n_P(P)$ and $D' = \sum_P n'_P(P)$ is the divisor $D + D' = \sum_P (n_P + n'_P)(P)$.

Given a rational function $f : E(\mathbb{F}_{q^k}) \to \mathbb{F}_{q^k}$, the *divisor of* f is the divisor $(f) = \sum_P \mathrm{ord}_P(f)(P)$ where $\mathrm{ord}_P(f)$ is the multiplicity of f at P. It follows from this definition that $(fg) = (f) + (g)$ and $(f/g) = (f) - (g)$ for any two functions f and g defined on E; moreover, $(f) = 0$ if and only if f is a nonzero constant.

We say two divisors D and D' are equivalent, $D' \sim D$, if there exists a function g such that $D' = D + (g)$. For any function f and any divisor $D = \sum_P n_P(P)$ of degree zero, we define $f(D) = \prod_P f(P)^{n_P}$.

The *Tate pairing* is a bilinear, non-degenerate mapping $e : E(\mathbb{F}_q) \times E(\mathbb{F}_{q^k}) \to \mathbb{F}^*_{q^k}$. Specifically, let $P \in E(\mathbb{F}_q)$ be a point of order r, let f_r be a function whose divisor satisfies $(f_r) \sim r(P) - r(O)$, let $Q \in E(\mathbb{F}_{q^k})$, and let $D \sim (Q) - (O)$ be a divisor whose support is disjoint from the support of (f_r). We define the (reduced) Tate pairing as

$$e(P, Q) = f_r(D)^{(q^k-1)/r}.$$

One can show [10] that this mapping is indeed bilinear, and also non-degenerate for linearly independent P and Q.

The Tate pairing is usually defined as simply $f_r(D)$, but this is only defined up to r-th powers. Raising $f(D)$ to $(q^k - 1)/r$ not only produces a unique value in $\mathbb{F}^*_{q^k}$, it also ensures that the result is either 1 or an element of order r. This property is useful in efficiently preventing small subgroup attacks [14]. Indeed,

[4] Divisors are usually defined over the algebraic closure $\overline{\mathbb{F}_q}$ of $\mathbb{F}_q$ subject to additional condition that only finitely many n_P are nonzero. However, we restrict our attention to divisors defined over $\mathbb{F}_{q^k}$, so the total number of n_P coefficients is itself finite.

in several protocols Q is computed as the hash of some data and thus its order is *a priori* unknown. In general this would necessitate multiplying Q by a large cofactor to avoid small subgroup attacks. However, checking the pairing value alone is sufficient.

3 Parameter Generation

The method we propose to select pairing-friendly groups is based upon the following observation.

Theorem 1 (Group selection). *Suppose $E(\mathbb{F}_q)$ has a subgroup of prime order $r > 2$ with even embedding degree $k = 2d$ for some $d > 0$, such that r and k are coprime. Let R be a random point of order r on $E(\mathbb{F}_{q^k})$ such that $\mathrm{tr}(R) \neq O$, and let $Q = [k]R - \mathrm{tr}(R)$, so that $\mathrm{tr}(Q) = O$. If $Q = (X, Y)$, then $X^{q^d-1} = 1$ (i.e. $X \in \mathbb{F}_{q^d}$) and $Y^{q^d-1} = -1$.*

Proof. Our strategy is to compute and analyze the properties of the eigenvalues and eigenvectors of the Frobenius endomorphism Φ.

As we saw in section 2.1, the characteristic polynomial of the Frobenius π factorizes mod r as $\pi(u) = (u-1)(u-q) \pmod r$. Let P_0 be a point of order r over $\mathbb{F}_q$ and let Q_0 be a point of order r over $\mathbb{F}_{q^k}$ such that $\Phi(P_0) = P_0$ and $\Phi(Q_0) = [q]Q_0$. The points P_0 and Q_0 form a basis for $E(\mathbb{F}_{q^k})[r]$. As we saw in section 2.2, $\mathrm{tr}(P_0) = [k]P_0$ and $\mathrm{tr}(Q_0) = O$.

Now let $R = [m_1]P_0 + [m_2]Q_0$. Then $\mathrm{tr}(R) = [m_1]\,\mathrm{tr}(P_0) + [m_2]\,\mathrm{tr}(Q_0) = [m_1][k]P_0$, and $[k]R - \mathrm{tr}(R) = [k][m_1]P_0 + [k][m_2]Q_0 - [m_1][k]P_0 = [k][m_2]Q_0$. In other words, $\{\mathrm{tr}(R), [k]R - tr(R)\}$ is a basis equivalent to $\{P_0, Q_0\}$.

Finally, $q^d \equiv -1 \pmod r$, because $q^{2d} \equiv 1 \pmod r$ and $2d = k$ is the smallest integer for which this holds. Thus $\Phi^d(Q_0) = -Q_0$, and for $Q = [k]R - \mathrm{tr}(R)$ it follows that $\Phi^d(Q) = \Phi^d([k][m_2]Q_0) = -[k][m_2]Q_0 = -Q$. Writing $Q = (X, Y)$ so that $-Q = (X, -Y)$ for a suitable Weierstraß form, we conclude that $\Phi^d(X, Y) = (X^{q^d}, Y^{q^d}) = (X, -Y)$. Therefore, $X^{q^d-1} = 1$ (i.e. $X \in \mathbb{F}_{q^d}$) and $Y^{q^d-1} = -1$. □

Theorem 1 suggests this algorithm:

Group selection algorithm:

1. Randomly generate a point $R \in E(\mathbb{F}_{q^k})$ of order r.
2. Compute $P \leftarrow \mathrm{tr}(R)$.
3. Compute $Q \leftarrow [k]R - P$.
4. If $P = O$ or $Q = O$, goto step 1.

We view the domain of the Tate pairing as $\langle P \rangle \times \langle Q \rangle$. Notice that $P = O$ or $Q = O$ occurs in step 4 with negligible probability, so for curves used in practice it may be safe to skip this step. We note that Boneh and Franklin [4] also propose hashing to points of trace zero according to the formula in step 3.

An efficiency bottleneck seems to arise in step 1 of algorithm 3, in that the point R must be of order r. This usually means that a random point on $E(\mathbb{F}_{q^k})$ must be multiplied by a large cofactor $h = \#E(\mathbb{F}_{q^k})/r^2 \approx q^{k-2}$. In fact, in most cases a much smaller cofactor can be be used, as established by the following theorem.

Theorem 2 (Small cofactors). *Let R_0 be a random point on $E(\mathbb{F}_{q^k})$ where $k = 2d$, and let $h' = \#E(\mathbb{F}_{q^d})/r$. Assume that $\gcd(r, h') = 1$. Then $R' = [h']R_0$ can be used instead of a random point $R \in E(\mathbb{F}_{q^k})$ of order r in step 1 of algorithm 3.*

Proof. Let $t_m = \alpha^m + \beta^m$, where α and β satisfy $\alpha + \beta = t$, $\alpha\beta = q$ (t being the trace of the Frobenius, defined below). It is known [15, Theorem 2.15] that $\#E(\mathbb{F}_{q^m}) = q^m + 1 - t_m$ for any $m > 0$. A simple inspection shows that $t_{2m} = t_m^2 - 2q^m$ and thus $\#E(\mathbb{F}_{q^k}) = (q^d+1-t_d)(q^d+1+t_d)$. Therefore any $R_0 \in E(\mathbb{F}_{q^k})$ can be written as $R_0 = U + V$, where U is in a subgroup of order $q^d + 1 - t_d$ and V is in a subgroup of order $q^d + 1 + t_d$.

The Frobenius equation for Φ^m is [3, section III.3]:

$$\Phi^{2m} - [t_m]\Phi^m + [q^m] = [0],$$

meaning that, for any point $P \in E(\overline{\mathbb{F}_q})$, $\Phi^{2m}(P) - [t_m]\Phi^m(P) + [q^m]P = O$. Hence for $k = 2d$ the Frobenius equation is $\Phi^k - [t_d]\Phi^d + [q^d] = [0]$, which, since $\Phi^k(Q) = Q$ for all $Q \in E(\mathbb{F}_{q^k})$, reduces to:

$$[t_d]\Phi^d = [q^d + 1].$$

In other terms, $[t_d](\Phi^d(Q) \pm Q) = [q^d+1 \pm t_d]Q$ for any $Q \in E(\mathbb{F}_{q^k})$. Therefore $\Phi^d(U) = U$ and $\Phi^d(V) = -V$, given the orders of their respective subgroups, so we can write $U = (X_U, Y_U)$ and $V = (X_V, iY_V)$, where $X_U, Y_U, X_V, Y_V \in \mathbb{F}_{q^d}$ and $i^2 \in \mathbb{F}_{q^d}$ is a quadratic non-residue in $\mathbb{F}_{q^d}$ (and thus satisfies $\Phi^d(i) = -i$). Notice that $\mathrm{tr}(V) = O$.

Let $h' = \#E(\mathbb{F}_{q^d})/r = (q^d + 1 - t_d)/r$, and let $R' = [h']R_0 = [h']U + [h']V$. This establishes that $U' = [h']U$ is an element of order r, and thus either $\Phi(U') = U'$ or $\Phi(U') = [q]U'$. But $\Phi^d([h']U) = [h']U$, so necessarily $\Phi(U') = U'$, that is, $U \in E(\mathbb{F}_q)$, which implies that $\mathrm{tr}(U') = [k]U'$. Notice that $V' = [h']V$ satisfies $\Phi^d(V') = -V'$.

Therefore, $Q' = [k]R' - \mathrm{tr}(R') = [k]U' - \mathrm{tr}(U') + [k]V' - \mathrm{tr}(V') = [k]V'$, and hence $\Phi^d(Q') = -Q'$. Besides, $[r]Q' \neq O$ unless $Q' = O$. This establishes that Q' is a suitable replacement for Q in algorithm 3; equivalently, R' is a suitable replacement for R as defined in step 1 of that algorithm. □

According to this result, the actual cofactor can be $h' \approx q^{k/2-1}$, thus halving the cofactor multiplication time as compared to the full $h = \#E(\mathbb{F}_{q^k}) \approx q^{k-2}$.

A nice observation is that, if d is odd (so that a quadratic non-residue chosen from $\mathbb{F}_q$ exists in $\mathbb{F}_{q^d}$), multiplication by h' maps onto a group isomorphic to the twist $E'(\mathbb{F}_{q^d})$. This suggests the strategy of creating and manipulating Q'

directly as a point on $E'(\mathbb{F}_{q^d})$ for operations like key pair generation and point transmission over a communications channel, and mapping back to a pair of coordinates in $\mathbb{F}_{q^k}$ for immediate consumption by the pairing algorithm. This avoids $E(\mathbb{F}_{q^k})$ arithmetic altogether and halves bandwidth requirements. For instance, if $k = 2$ pairing-based protocols can be implemented using only standard $E(\mathbb{F}_q)$ arithmetic, readily available in optimized form in many program libraries, plus support for simple $\mathbb{F}_{q^2}$ arithmetic.

We note that although we see no potential weakness in the derivation of both generators from a single parameter R, if this is a concern any other P' such that $e(P', Q) \neq 1$ can be used in step 2.

4 Tate Pairing Computation

We now review Miller's algorithm [16] for computing the Tate pairing and describe how to optimize it for the subgroups constructed according to our algorithm.

Assume that curve $E(\mathbb{F}_q)$ has a subgroup of prime order r and embedding degree $k > 1$. Let $P \in E(\mathbb{F}_q)[r]$ and $Q \in E(\mathbb{F}_{q^k})$ be linearly independent points. The Tate pairing of order r is defined as $e(P, Q) = f(D)^{(q^k-1)/r}$, where $D \sim (Q) - (O)$ and $(f) = r(P) - r(O)$. Computation of the Tate pairing is helped by the following observations.

Lemma 2. *For any $d > 1$ such that $d \mid k$, $q^{k/d} - 1$ is a factor of $(q^k - 1)/r$.*

Proof. We start with the factorization $q^k - 1 = (q^{k/d} - 1) \sum_{i=0}^{d-1} q^{ik/d}$. Since the embedding degree is $k > 1$,we have $r \mid q^k - 1$ and $r \nmid q^{k/d} - 1$. Thus $r \mid \sum_{i=0}^{d-1} q^{ik/d}$, and hence $q^{k/d} - 1$ survives as a factor of $(q^k - 1)/r$. □

The next theorem generalizes a result originally established only for certain supersingular curves [1, Theorem 1]:

Theorem 3. *$e(P, Q) = f(Q)^{(q^k-1)/r}$ for $Q \neq O$.*

Proof. Suppose $R \notin \{O, -P\}$ is some point on the curve. Let f' be a function with divisor $(f') = r(P + R) - r(R) \sim (f)$, so that $e(P, Q) = f'((Q) - (O))^{(q^k-1)/r}$. Since P has coordinates in $\mathbb{F}_q$, and because f' does not have a zero or pole at O, we know that $f'(O) \in \mathbb{F}_q^*$. Thus $f'((Q) - (O)) = f'(Q)/f'(O)$. By Fermat's Little Theorem for finite fields [13, lemma 2.3], $f'(O)^{q-1} = 1$. Lemma 2 then ensures that $f'(O)^{(q^k-1)/r} = 1$. Hence, $f'(O)$ is an irrelevant factor and can be omitted from the Tate pairing computation, i.e. $e(P, Q) = f'(Q)^{(q^k-1)/r}$. Now consider P, Q to be fixed and R to be variable. Since the above statement holds for all $R \notin \{O, -P\}$ we have that $f'(Q)$ is a constant when viewed as a function of R, coinciding with the value of $f(Q)$. Therefore, $e(P, Q) = f(Q)^{(q^k-1)/r}$. □

Notice that the special case $Q = O$ where theorem 3 does not apply is trivially handled, since $e(P, O) = 1$. But of greater importance is the next corollary:

Corollary 1 (Irrelevant factors). *One can freely multiply or divide $f(Q)$ by any nonzero $\mathbb{F}_{q^{k/d}}$ factor without affecting the pairing value.*

In what follows, which we quote directly from Barreto et al. [1, Theorem 2], for each pair $U, V \in E(\mathbb{F}_q)$ we define $g_{U,V} : E(\mathbb{F}_{q^k}) \to \mathbb{F}_{q^k}$ to be (the equation of) the line through points U and V (if $U = V$, then $g_{U,V}$ is the tangent to the curve at U, and if either one of U, V is the point at infinity O, then $g_{U,V}$ is the vertical line at the other point). The shorthand g_U stands for $g_{U,-U}$. In affine coordinates, for $U = (x_U, y_U)$, $V = (x_V, y_V)$ and $Q = (x, y)$, we have:

$$\begin{aligned} g_{U,V}(O) &= 1. \\ g_{U,U}(Q) &= \lambda_1(x - x_U) + y_U - y,\ Q \neq O. \\ g_{U,V}(Q) &= \lambda_2(x - x_U) + y_U - y,\ Q \neq O,\ U \neq V. \\ g_U(Q) &= x - x_U,\ Q \neq O. \end{aligned}$$

where

$$\lambda_1 = \frac{3x_U^2 + a}{2y_U},\quad \lambda_2 = \frac{y_V - y_U}{x_V - x_U}.$$

Lemma 3 (Miller's formula). *Let P be a point on $E(\mathbb{F}_q)$ and f_c be a function with divisor $(f_c) = c(P) - (cP) - (c-1)(O)$, $c \in \mathbb{Z}$. For all $a, b \in \mathbb{Z}$, $f_{a+b}(Q) = f_a(Q) \cdot f_b(Q) \cdot g_{aP,bP}(Q)/g_{(a+b)P}(Q)$.*

Proof. See Barreto et al. [1, Theorem 2]. □

Notice that $(f_0) = (f_1) = 0$, so that by corollary 1 we can set $f_0(Q) = f_1(Q) = 1$. Furthermore, $f_{a+1}(Q) = f_a(Q) \cdot g_{aP,P}(Q)/g_{(a+1)P}(Q)$ and $f_{2a}(Q) = f_a(Q)^2 \cdot g_{aP,aP}(Q)/g_{2aP}(Q)$. Recall that $r \geqslant 0$ is the order of P. Let its binary representation be $r = (r_t, \ldots, r_1, r_0)$ where $r_i \in \{0, 1\}$ and $r_t \neq 0$. Miller's algorithm computes $f(Q) = f_r(Q), Q \neq O$ by coupling the above formulas with the double-and-add method to calculate rP:

Miller's algorithm:

set $f \leftarrow 1$ and $V \leftarrow P$
for $i \leftarrow t-1, t-2, \ldots, 1, 0$ do {
    set $f \leftarrow f^2 \cdot g_{V,V}(Q)/g_{2V}(Q)$ and $V \leftarrow 2V$
    if $r_i = 1$ then set $f \leftarrow f \cdot g_{V,P}(Q)/g_{V+P}(Q)$ and $V \leftarrow V + P$
}
return f

Miller's algorithm can be simplified even further if k is even, as established by the following generalization of a previous result [1, Theorem 2]:

Theorem 4 (Denominator elimination). *If k is even and coprime to r and $P \in E(\mathbb{F}_q)[r]$, the g_{2V} and g_{V+P} denominators in Miller's algorithm can be discarded altogether without changing the value of $e(P, Q)$ for any $Q \in E(\mathbb{F}_{q^k})$ such that $\Phi^{k/2}(Q) = -Q$ and r divides the order of Q.*

Proof. We will show that the denominators become unity at the final powering in the Tate pairing. The denominators in Miller's formula have the form $g_U(Q) \equiv x-u$, where $x \in \mathbb{F}_{q^{k/2}}$ (Theorem 1) is the abscissa of Q and $u \in \mathbb{F}_q$ is the abscissa of U. Hence $g_U(Q) \in \mathbb{F}_{q^{k/2}}$. These denominators are raised to the exponent $(q^k - 1)/r$ at the final powering. But by Lemma 2, this exponent contains a factor $q^{k/2} - 1$, causing all denominators to become unity. Therefore, they can be discarded without changing the pairing value. □

To illustrate the effectiveness of our method for the computation of the Tate pairing, we compare our results with those of Izu and Takagi [12] for non-supersingular curves with $k = 2$ and $k = 6$.

The computation of $e(P, Q)$ requires all of the intermediate points computed during the scalar multiplication $[r]P$. If P is fixed, these can be precalculated and stored, with considerable savings. In this case affine coordinates are faster, and require less storage. Otherwise we follow [12] and use projective coordinates. Additional savings could be obtained with the method of Eisentraeger et al. [9], but we have not implemented it.

Table 1 summarizes the results, where M denotes the computing time of a multiplication in $\mathbb{F}_q$, and assuming that the time taken by one squaring is about $0.8M$.

Table 1. Complexity of computing the Tate pairing.

algorithm	coordinates	$k = 2$, $\|q\| = 512$	$k = 6$, $\|q\| = 171$
[12]	projective	20737.6M	33078.3M
ours, w/o precomp.	projective	4153.2M	15633.0M
ours, with precomp.	projective	2997.6M	14055.4M
ours, with precomp.	affine	1899.6M	11110.2M

5 Conclusions

We have shown how to select cryptographically significant groups where the Tate pairing can be efficiently implemented. Our algorithm is faster than previously reported implementations [12] by a factor of 2 to 10.

Specifically, we have argued that the Tate Pairing $e(P, Q)$ is most efficiently calculated when $P \in E(\mathbb{F}_q)[r]$ and $Q \in E(\mathbb{F}_q^k)$ satisfies $\Phi^{k/2}(Q) = -Q$. We have also provided an algorithm to choose such P and Q so that $e(P, Q)$ is non-degenerate.

An interesting line of further research is the extension of our methods to hyperelliptic curves, possibly with enhancements. This has already been done for the supersingular case [8].

We wish to thank Florian Heß for suggesting the elegant proof of theorem 1, and Steven Galbraith for his valuable comments about this work.

References

1. P.S.L.M. Barreto, H.Y. Kim, B. Lynn, and M. Scott, *Efficient algorithms for pairing-based cryptosystems*, Advances in Cryptology – Crypto'2002, Lecture Notes in Computer Science, vol. 2442, Springer-Verlag, 2002, pp. 377–87.
2. P.S.L.M. Barreto, B. Lynn, and M. Scott, *Constructing elliptic curves with prescribed embedding degrees*, Security in Communication Networks – SCN'2002, Lecture Notes in Computer Science, vol. 2576, Springer-Verlag, 2002, pp. 263–273.
3. I. Blake, G. Seroussi, and N. Smart, *Elliptic curves in cryptography*, Cambridge University Press, London, 1999.
4. D. Boneh and M. Franklin, *Identity-based encryption from the Weil pairing*, SIAM Journal of Computing **32** (2003), no. 3, 586–615.
5. D. Boneh, B. Lynn, and H. Shacham, *Short signatures from the Weil pairing*, Advances in Cryptology – Asiacrypt'2001, Lecture Notes in Computer Science, vol. 2248, Springer-Verlag, 2002, pp. 514–532.
6. D. Coppersmith, *Fast evaluation of logarithms in fields of characteristics two*, IEEE Transactions on Information Theory, vol. 30, 1984, pp. 587–594.
7. R. Dupont, A. Enge, and F. Morain, *Building curves with arbitrary small MOV degree over finite prime fields*, Cryptology ePrint Archive, Report 2002/094, 2002, `http://eprint.iacr.org/2002/094`.
8. I. Duursma and H.-S. Lee, *Tate-pairing implementations for tripartite key agreement*, Cryptology ePrint Archive, Report 2003/053, 2003, `http://eprint.iacr.org/2003/053`.
9. K. Eisentraeger, K. Lauter, and P.L. Montgomery, *Fast elliptic curve arithmetic and improved Weil pairing evaluation*, Topics in Cryptology – CT-RSA'2003, Lecture Notes in Computer Science, vol. 2612, Springer-Verlag, 2003, pp. 343–354.
10. G. Frey and H.-G. Rueck, *A remark concerning m-divisibility and the discrete logarithm problem in the divisor class group of curves*, Mathematics of Computation, vol. 62, 1994, pp. 865–874.
11. S. Galbraith, K. Harrison, and D. Soldera, *Implementing the Tate pairing*, Algorithm Number Theory Symposium – ANTS V, Lecture Notes in Computer Science, vol. 2369, Springer-Verlag, 2002, pp. 324–337.
12. 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), Lecture Notes in Computer Science, vol. 2587, Springer-Verlag, 2003, pp. 283–297.
13. R. Lidl and H. Niederreiter, *Finite fields*, 2nd ed., Encyclopedia of Mathematics and its Applications, no. 20, Cambridge University Press, 1997.
14. C.H. Lim and P.J. Lee, *A key recovery attack on discrete log-based schemes using a prime order subgroup*, Advances in Cryptology – Crypto'97, Lecture Notes in Computer Science, vol. 1294, Springer-Verlag, 1997, pp. 249–263.
15. A.J. Menezes, *Elliptic curve public key cryptosystems*, Kluwer Academic Publishers, 1993.
16. V. Miller, *Short programs for functions on curves*, unpublished manuscript, 1986.
17. A. Miyaji, M. Nakabayashi, and S. Takano, *New explicit conditions of elliptic curve traces for FR-reduction*, IEICE Transactions on Fundamentals **E84-A** (2001), no. 5, 1234–1243.