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 efficient, with an observed performance about 2 to 10 times better than previously reported implementations, depending on the embedding degree. Our algorithm has beneficial side effects: various non-pairing operations become faster, and bandwidth may be saved.

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. This interest is not unfounded, as previously unsolved problems have been cracked by using pairings.

To date, most suitable pairings are based on the Tate pairing over certain elliptic curve groups, a notable exception being that of Boneh, Mironov and Shoup [6] based on the String RSA assumption. Unfortunately, the Tate pairing is an expensive operation and is often the bottleneck in such systems.

Efficient pairings for supersingular curves have been proposed [2, 9, 12]. 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. Moreover, for technical reasons, one is often forced to use fields of small characteristic [16, section 5.2.2], which are more vulnerable to Coppersmith's discrete logarithm attack [7]. 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]).

M. Matsui and R. Zuccherato (Eds.): SAC 2003, LNCS 3006, pp. 17–25, 2004.

Thus we would like to find similar optimizations for ordinary curves over fields of large characteristics containing subgroups of manageable embedding degree [3, 8, 18].

We show how to select groups in nonsupersingular curves where many optimizations proposed for supersingular curves [2] have a counterpart, and obtain running times that are up to ten times better than previously reported results [13]. 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. Additionally, it turns out that operations of pairing-based schemes that do not rely on pairings, such as key generation, become more efficient with our choice of groups.

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 explains how the selected groups lead to efficient implementation of the Tate pairing. We compare our results with previous work in Section 5, and present our conclusions in Section 6.

2 Preliminaries

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 $0 < i < k$. We assume $k > 1$. The group $E[r] \cong \mathbb{F}_r \times \mathbb{F}_r$ of r-torsion points lies in $E(\mathbb{F}_{q^k})$ [1].

In what follows, let $\mathbb{F}_q$ be a field of odd characteristic and $E(\mathbb{F}_q)$ an elliptic curve containing a subgroup of prime order r with embedding degree k, and assume that r and k are coprime.

2.1 The Twist of a Curve

Let $E(\mathbb{F}_q)$ given by the short Weierstraß equation $y^2 = x^3 + ax + b$, let d be a factor of k and let $v \in \mathbb{F}_{q^d}$ be some quadratic non-residue. The *twist* of E over $\mathbb{F}_{q^d}$ is the curve $E'(\mathbb{F}_{q^d}) : y^2 = x^3 + v^2 a\, x + v^3 b$. The orders of the groups of rational points of these curves satisfy the relation $\#E(\mathbb{F}_{q^d}) + \#E'(\mathbb{F}_{q^d}) = 2q^d + 2$ [4, section III.3].

In the above equation, if v is instead a quadratic residue, then it is easy to check that an isomorphism $E \to E'$ given by $(X, Y) \mapsto (vX, v\sqrt{v}Y)$ exists.

2.2 Divisors and the Tate Pairing

For our purposes, a *divisor* 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 nonzero 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 nonzero rational 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 mapping $e : E(\mathbb{F}_q)[r] \times E(\mathbb{F}_{q^k}) \to \mathbb{F}_{q^k}^*$. Specifically, let $P \in E(\mathbb{F}_q)$ be a point of order r, let f be a function whose divisor satisfies $(f) = r(P) - r(O)$, 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). We define the (reduced) Tate pairing as

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

One can show [11] that this mapping is indeed bilinear, and also nondegenerate for linearly independent P and Q if r divides the order of Q.

More generally, if D' is a divisor satisfying $D' \sim (P) - (O)$ then we can substitute any f' for f such that $(f') = rD'$, so long as the support of D' is disjoint to that of D.

Note that raising $f(D)$ to $(q^k - 1)/r$ ensures that the result is either 1 or an element of order r. This property is useful in efficiently preventing small subgroup attacks [15]. There is no need to multiply Q by a large cofactor to avoid these attacks, as checking the pairing value is sufficient.

2.3 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 $P \in E(\mathbb{F}_{q^k})$.

2.4 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 range of the map is indeed $E(\mathbb{F}_q)$).

We describe the two eigenspaces of the trace map on $E[r]$. The eigenvalues are k and 0.

Lemma 1. *The k-eigenspace of the trace map is $E(\mathbb{F}_q)[r]$.*

Proof. Clearly, all points $R \in E(\mathbb{F}_q)[r]$ satisfy $\mathrm{tr}(R) = [k]R$, hence we only need to show that all points $R \in E[r]$ 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, $R \in E(\mathbb{F}_q)[r]$. □

It is easy to verify that for any $R \in E(\mathbb{F}_{q^k})$ the point $Q = R - \Phi(R)$ satisfies $\mathrm{tr}(Q) = O$. This provides a way of generating points of trace zero. Since at least one finite point Q can be constructed in this fashion (provided $k > 1$), we see that the other eigenvalue of the trace map is indeed zero. We know that this space must be one-dimensional, since the other dimension has been accounted for by $E(\mathbb{F}_q)[r]$.

We now describe the eigenspaces of the Frobenius map on $E[r]$. 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. The polynomial π factorizes as $\pi(u) = (u-1)(u-q) \pmod{r}$, so the eigenvalues are 1 and q.

Lemma 2. *The* 1*-eigenspace of* Φ *is* $E(\mathbb{F}_q)[r]$*.*

Proof. A point of $E(\mathbb{F}_{q^k})$ is fixed under Φ if and only if it lies in $E(\mathbb{F}_q)$. □

Lemma 3. *The* q*-eigenspace of* Φ *consists of all points* $R \in E[r]$ *satisfying* $\mathrm{tr}(R) = O$*.*

Proof. If a point R satisfies $\mathrm{tr}(R) = (1 + \Phi + ... + \Phi^{k-1})R = O$, then $\mathrm{tr}(\Phi(R)) = (\Phi + ... + \Phi^k)R = O$. In other words, the points of trace zero are mapped to points of trace zero under Φ and hence must constitute an eigenspace. As the 1-eigenspace has already been accounted for, the set of points of trace zero must be the q-eigenspace of Φ. □

3 Parameter Generation

Assume k is even and set $d = k/2$. We propose a method for selecting group generators that makes the pairing more efficient, and additionally improves the performance of operations in pairing-based schemes that do not use the pairing, such as key generation.

Let E be given by $y^2 = x^3 + ax + b$, and consider its twist over $\mathbb{F}_{q^d}$, namely, the curve $E'(\mathbb{F}_{q^d}) : y^2 = x^3 + v^2 a\ x + v^3 b$ for some quadratic non-residue $v \in \mathbb{F}_{q^d}$. In $\mathbb{F}_{q^k}$, v is a quadratic residue, which means the map $\Psi : (X, Y) \mapsto (v^{-1}X, (v\sqrt{v})^{-1}Y)$ is an isomorphism that maps the group of points of $E'(\mathbb{F}_{q^d})$ to a subgroup of points of $E(\mathbb{F}_{q^k})$.

Let $Q' = (X, Y) \in E'(\mathbb{F}_{q^d})$, and set $Q = \Psi(Q') = (v^{-1}X, (v\sqrt{v})^{-1}Y) \in E(\mathbb{F}_{q^k})$. By construction, the x-coordinate of Q is an element of $\mathbb{F}_{q^d}$, allowing the denominator elimination optimization that will be described in the next section. This suggests the following group selection algorithm.

Group Selection Algorithm:

1. Randomly generate a point $P \in E(\mathbb{F}_q)$ of order r.
2. Randomly generate a point $Q' \in E'(\mathbb{F}_{q^d})$.

We view the domain of the Tate pairing as $\langle P\rangle \times \langle Q\rangle$, where $Q = \Psi(Q')$. It may be desirable to explicitly check that $e(P, Q) \neq 1$, but as this occurs with overwhelming probability, in some situations it could be safe to skip this check. Note that only P is required to have order r.

Operations that do not use the pairing such as key generation and point transmission can be performed using only arithmetic on $\mathbb{F}_{q^d}$. Points of $E'(\mathbb{F}_{q^d})$ are mapped back to points on $E(\mathbb{F}_{q^k})$ only when needed for a pairing computation. This avoids many $\mathbb{F}_{q^k}$ operations and halves bandwidth requirements.

For instance, if $k = 2$, pairing-based protocols can be implemented using $E(\mathbb{F}_q)$ arithmetic, readily available in a highly optimized form in many code libraries, along with support for simple $\mathbb{F}_{q^2}$ operations for the pairing computation. For higher k, we suggest implementing $\mathbb{F}_{q^k}$ as $\mathbb{F}_q[x]/R_k(x)$, where $R_k(x)$ is the sparsest possible polynomial containing only terms of even degree. In this case, elements in $\mathbb{F}_{q^d}$ are polynomials lacking any term of odd degree.

3.1 Some Remarks on the Selected Groups

We mention a few observations on the groups selected by our algorithm.

Lemma 4. *Let $Q = (X, Y) \in E(\mathbb{F}_{q^k})$ be a finite point. Then $\Phi^d(Q) = -Q$ if and only if $X^{q^d-1} = 1$ (i.e. $X \in \mathbb{F}_{q^d}$) and $Y^{q^d-1} = -1$.*

Proof. Since $-Q = (X, -Y)$ (for a suitable Weierstraß form), we conclude that $\Phi^d(X, Y) = (X^{q^d}, Y^{q^d}) = (X, -Y)$ if and only if $X^{q^d-1} = 1$ (i.e. $X \in \mathbb{F}_{q^d}$) and $Y^{q^d-1} = -1$. □

Thus $\Psi(E'(\mathbb{F}_{q^d}))$ is precisely the group of points in $E(\mathbb{F}_{q^k})$ satisfying $\Phi^d(Q) = -Q$, which is a subgroup of the trace zero points of $E(\mathbb{F}_{q^k})$.

Hence an alternative way to pick Q in our algorithm is to choose a random $R \in E(\mathbb{F}_{q^k})$ and set $Q \leftarrow R - \Phi^d(R)$. However this is slower than finding points of $E'(\mathbb{F}_{q^d})$, and we also do not obtain the bonus of speeding up non-pairing operations.

Lastly, we note that the above lemma can be used to show that r-torsion points of trace zero have a special form.

Corollary 1. *Let $Q = (X, Y) \in E(\mathbb{F}_{q^k})[r]$ be a finite point with $\mathrm{tr}(Q) = O$. Then $X \in \mathbb{F}_{q^d}$ and $Y^{q^d-1} = -1$.*

Proof. As $\mathrm{tr}(Q) = O$, the point Q lies in the q-eigenspace of the Frobenius map Φ, that is, $\Phi(Q) = [q]Q$. We have $q^d \equiv -1 \pmod{r}$, because $q^{2d} \equiv 1 \pmod{r}$ and $2d = k$ is the smallest integer for which this holds. Thus $\Phi^d(Q) = -Q$. By Lemma 4 we have $X^{q^d-1} = 1$ and $Y^{q^d-1} = -1$. □

4 Tate Pairing Computation

We review Miller's algorithm [17] for computing the Tate pairing and describe how to optimize it for the subgroups constructed according to our algorithm.

Let $P \in E(\mathbb{F}_q)[r]$ and $Q \in E(\mathbb{F}_{q^k})$ be linearly independent points. Let f be the rational function with divisor $(f) = r(P) - r(O)$. We wish to compute the Tate pairing $e(P, Q) = f(D)^{(q^k-1)/r}$, where D satisfies $D \sim (Q) - (O)$, and the support of D does not contain P or O.

For this section, instead of requiring k to be even and setting $d = k/2$, we generalize so that d now represents any proper factor of k, that is, $d \mid k$ and $d < k$.

Lemma 5. *$q^d - 1$ is a factor of $(q^k - 1)/r$.*

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

Corollary 2 (Irrelevant factors). *One can multiply $f(D)$ by any nonzero $x \in \mathbb{F}_{q^d}$ without affecting the pairing value.*

Proof. To compute the pairing, $f(D)$ is raised to the exponent $(q^k - 1)/r$. By Lemma 5, this exponent contains a factor $q^d - 1$, thus by Fermat's Little Theorem for finite fields [14, lemma 2.3], $x^{(q^k-1)/r} = 1$. □

The next theorem generalizes a result originally established only for certain supersingular curves [2, Theorem 1]:

Theorem 1. *Let $P \in E(\mathbb{F}_q)[r]$ and $Q \in E(\mathbb{F}_{q^k})$ be linearly independent points. Then $e(P, Q) = f(Q)^{(q^k-1)/r}$.*

Proof. Suppose $R \notin \{O, -P, Q, Q - P\}$ is some point on the curve. Let f' be a function with divisor $(f') = r(P + R) - r(R) \sim (f)$, so that $e(P, Q) = f'((Q) - (O))^{(q^k-1)/r}$. Because f' does not have a zero or pole at O, we have $f'((Q) - (O)) = f'(Q)/f'(O)$, and since P has coordinates in $\mathbb{F}_q$, we know that $f'(O) \in \mathbb{F}_q^*$. Corollary 2 then ensures that $f'(O)$ 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 $(f') = r((P + R) - (R)) = r((P) - (O) + (g)) = (f) + r(g)$ for some rational function g, since $(P + R) - (R) \sim (P) - (O)$. Thus $f' = fg^r$, and because Q is not a zero or pole of f or f' (so that $g(Q) \in \mathbb{F}_{q^k}^*$ is well defined) it follows that $f'(Q)^{(q^k-1)/r} = f(Q)^{(q^k-1)/r} g(Q)^{q^k-1} = f(Q)^{(q^k-1)/r}$. □

The case of linearly dependent P and Q is trivially handled, as then we have $e(P, Q) = 1$.

In what follows, which we quote directly from Barreto et al. [2, 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, $E : y^2 = x^3 + ax + b$, for $U = (x_U, y_U)$, $V = (x_V, y_V)$ and $Q = (x, y)$, we have:

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

where

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

Lemma 6 (Miller's formula). *Let P be a point on $E(\mathbb{F}_q)$ and f_c be a function with divisor $(f_c) = c(P) - ([c]P) - (c-1)(O)$, $c \in \mathbb{Z}$. For all $a, b \in \mathbb{Z}$, $f_{a+b}(Q) = f_a(Q) \cdot f_b(Q) \cdot g_{[a]P,[b]P}(Q)/g_{[a+b]P}(Q)$.*

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

Notice that $(f_0) = (f_1) = 0$, so that by corollary 2 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 $f_{2a}(Q) = f_a(Q)^2 \cdot g_{[a]P,[a]P}(Q)/g_{[2a]P}(Q)$. Recall that $r > 0$ 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 $f(Q) = f_r(Q)$, $Q \notin \{O, P\}$, by coupling the above formulas with the double-and-add method to calculate $[r]P$:

Miller's Algorithm:

```
set $f \leftarrow 1$ and $V \leftarrow P$
for $i \leftarrow t-1, t-2, \ldots, 1, 0$ do {
    set $f \leftarrow f^2 \cdot g_{V,V}(Q)/g_{[2]V}(Q)$ 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 further if k is even, as established by the following generalization of a previous result [2, Theorem 2]:

Theorem 2 (Denominator elimination). *Let $P \in E(\mathbb{F}_q)[r]$. Suppose $Q = (X, Y) \in E(\mathbb{F}_{q^k})$ and $X \in \mathbb{F}_{q^d}$. Then the $g_{[2]V}$ and g_{V+P} denominators in Miller's algorithm can be discarded without changing the value of $e(P, Q)$.*

Proof. The denominators in Miller's formula have the form $g_U(Q) \equiv x - u$, where $x \in \mathbb{F}_{q^d}$ is the abscissa of Q and $u \in \mathbb{F}_q$ is the abscissa of U. Hence $g_U(Q) \in \mathbb{F}_{q^d}$. By corollary 2, they can be discarded without changing the pairing value. □

Table 1. Complexity of computing the Tate pairing

algorithm	coordinates	$k = 2$, $\|q\| = 512$	$k = 6$, $\|q\| = 171$
[13]	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 Results

To illustrate the effectiveness of our method for the computation of the Tate pairing, we compare our results with those of Izu and Takagi [13] 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 Izu and Takagi [13] and use projective coordinates. Additional savings could be obtained with the method of Eisentraeger, Lauter and Montgomery [10], 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 $0.8M$.

6 Conclusions

We have shown how to select cryptographically significant groups where the Tate pairing can be efficiently implemented.

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 nondegenerate.

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 [9].

Acknowledgements

We wish to thank Waldyr Benits, Steven Galbraith, and Florian Heß for valuable comments about this work.

References

[1] R. Balasubramanian and N. Koblitz. The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm. *Journal of Cryptology*, 11(2):141–145, 1998. 18

[2] P. S. L. M. Barreto, H. Y. Kim, B. Lynn, and M. Scott. Efficient algorithms for pairing-based cryptosystems. In *Advances in Cryptology – Crypto'2002*, volume 2442 of *Lecture Notes in Computer Science*, pages 377–87. Springer-Verlag, 2002. 17, 18, 22, 23

[3] P. S. L. M. Barreto, B. Lynn, and M. Scott. Constructing elliptic curves with prescribed embedding degrees. In *Security in Communication Networks – SCN'2002*, volume 2576 of *Lecture Notes in Computer Science*, pages 263–273. Springer-Verlag, 2002. 18

[4] I. Blake, G. Seroussi, and N. Smart. *Elliptic Curves in Cryptography.* Cambridge University Press, London, 1999. 18

[5] D. Boneh, B. Lynn, and H. Shacham. Short signatures from the Weil pairing. In *Advances in Cryptology – Asiacrypt'2001*, volume 2248 of *Lecture Notes in Computer Science*, pages 514–532. Springer-Verlag, 2002. 17

[6] D. Boneh, I. Mironov, and V. Shoup. A secure signature scheme from bilinear maps. In *Topics in Cryptology – CT-RSA'2003*, volume 2612 of *Lecture Notes in Computer Science*, pages 98–110, San Francisco, USA, 2003. Springer-Verlag. 17

[7] D. Coppersmith. Fast evaluation of logarithms in fields of characteristics two. In *IEEE Transactions on Information Theory*, volume 30, pages 587–594, 1984. 17

[8] 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. 18

[9] 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. 17, 24

[10] K. Eisentraeger, K. Lauter, and P. L. Montgomery. Fast elliptic curve arithmetic and improved Weil pairing evaluation. In *Topics in Cryptology – CT-RSA'2003*, volume 2612 of *Lecture Notes in Computer Science*, pages 343–354. Springer-Verlag, 2003. 24

[11] G. Frey and H.-G. Rück. A remark concerning m-divisibility and the discrete logarithm problem in the divisor class group of curves. In *Mathematics of Computation*, volume 62, pages 865–874, 1994. 19

[12] S. Galbraith, K. Harrison, and D. Soldera. Implementing the Tate pairing. In *Algorithm Number Theory Symposium – ANTS V*, volume 2369 of *Lecture Notes in Computer Science*, pages 324–337. Springer-Verlag, 2002. 17

[13] T. Izu and T. Takagi. Efficient computations of the Tate pairing for the large MOV degrees. In *5th International Conference on Information Security and Cryptology (ICISC 2002)*, volume 2587 of *Lecture Notes in Computer Science*, pages 283–297. Springer-Verlag, 2003. 18, 24

[14] R. Lidl and H. Niederreiter. *Finite Fields.* Number 20 in Encyclopedia of Mathematics and its Applications. Cambridge University Press, 2nd edition, 1997. 22

[15] C. H. Lim and P. J. Lee. A key recovery attack on discrete log-based schemes using a prime order subgroup. In *Advances in Cryptology – Crypto'97*, volume 1294 of *Lecture Notes in Computer Science*, pages 249–263. Springer-Verlag, 1997. 19

[16] A. J. Menezes. *Elliptic Curve Public Key Cryptosystems.* Kluwer Academic Publishers, 1993. 17

[17] V. Miller. Short programs for functions on curves. unpublished manuscript, 1986. 22

[18] A. Miyaji, M. Nakabayashi, and S. Takano. New explicit conditions of elliptic curve traces for FR-reduction. *IEICE Transactions on Fundamentals*, E84-A(5):1234–1243, 2001. 18