The Eta Pairing Revisited

F. Hess[1], N. Smart[2], and Frederik Vercauteren[3]

[1] Technische Universität Berlin,
Fakultät II, Institut für Mathematik, MA 8-1,
Strasse des 17. Juni 136, D-10623 Berlin, Germany.
hess@math.tu-berlin.de
[2] Dept. Computer Science, University of Bristol
MVB, Woodland Road, Bristol, BS8 1UB, United Kingdom
nigel@cs.bris.ac.uk
[3] Department of Electrical Engineering, University of Leuven
Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium
frederik.vercauteren@esat.kuleuven.be

Abstract. In this paper we simplify and extend the Eta pairing, originally discovered in the setting of supersingular curves by Barreto et al., to ordinary curves. Furthermore, we show that by swapping the arguments of the Eta pairing, one obtains a very efficient algorithm resulting in a speed-up of a factor of around six over the usual Tate pairing, in the case of curves which have large security parameters, complex multiplication by an order of $\mathbb{Q}(\sqrt{-3})$, and when the trace of Frobenius is chosen to be suitably small. Other, more minor savings are obtained for more general curves. [1] [2]

1 Introduction

A bilinear pairing (or simply pairing) is a map of the form

$$\hat{t} : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T$$

where $\mathbb{G}_1, \mathbb{G}_2$ are additive groups and $\mathbb{G}_T$ is a multiplicative group. By bilinear we mean that the map is linear in each component, i.e.

$$\hat{t}(P_1 + P_2, Q) = \hat{t}(P_1, Q) \cdot \hat{t}(P_2, Q),$$
$$\hat{t}(P, Q_1 + Q_2) = \hat{t}(P, Q_1) \cdot \hat{t}(P, Q_2).$$

[1] The work described in this paper has been supported in part by the European Commission through the IST Programme under Contract IST-2002-507932 ECRYPT. The information in this document reflects only the author's views, is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability

[2] © 2006 IEEE. personal use of this material is permitted. however, permission to reprint/republish this material for advertising or promotional purposes or for creating new collective works for resale or redistribution to servers or lists, or to reuse any copyrighted component of this work in other works must be obtained from the ieee.

We only consider pairings, between groups of large prime order r, which are non-degenerate, i.e. for which there exists $P \in \mathbb{G}_1$ and $Q \in \mathbb{G}_2$ such that $\hat{t}(P,Q) \neq 1$.

Pairings on elliptic curves have, in recent years, become of great research interest in the cryptographic community. This is due to their application in a number of protocols with cryptographic functionality that cannot be achieved using other mathematical primitives, e.g. [6, 7, 16].

Traditionally two types of pairings have been considered, the Weil pairing and the Tate pairing. It is now accepted that for general curves providing common levels of security, the Tate pairing is more efficient, [14, 19]. However, other related pairings are available which in certain situations are more efficient, for example the Eta-pairing [1] on certain supersingular elliptic curves, which in itself extended and optimized the Duursma-Lee techniques introduced in [9].

In this paper we present a new pairing, which is closely related to the Eta-pairing but which can be used efficiently with ordinary elliptic curves. In addition we show that for the types of curves for which our new pairing applies, one achieves further performance improvements due to the fact that one can represent the group $\mathbb{G}_2$ more efficiently than one can normally.

We call our new pairing the Ate pairing, pronounced *eight*. This is for two reasons, firstly it is like the Tate pairing, but faster (hence the missing 'T'), it is also like the Eta pairing but it reverses the order of the arguments (and Ate is Eta spelled backwards).

Much of the results in this paper are based on the use of properties of twists of elliptic curves. Many of the results we use are well known to the experts, but we have been unable to locate them in the literature. Hence, we will also present these results related to twists.

2 Background on Tate Pairing

This section briefly recalls the definition of the Tate pairing and sets notation used in the remainder of the paper. An excellent survey of pairings can be found in [11].

Let $\mathbb{F}_q$ be a finite field with $q = p^n$ elements where p is prime and let E be an elliptic curve defined over $\mathbb{F}_q$. Consider a large prime r such that $r \mid \#E(\mathbb{F}_q)$ and denote the embedding degree by k, i.e. the smallest positive integer such that r divides $q^k - 1$. For technical reasons we assume that r^2 does not divide $q^k - 1$, which is not a problem in practice. The embedding degree k is chosen in this way so as to ensure that the full r-torsion $E[r]$ of the elliptic curve is defined over the field $\mathbb{F}_{q^k}$, i.e. $E[r] \subset E(\mathbb{F}_{q^k})$.

Let $P \in E[r]$ and $Q \in E(\mathbb{F}_{q^k})$, and consider the divisor $D = (Q + R) - (R)$ with R a random point in $E(\mathbb{F}_{q^k})$. For every integer s, let $f_{s,P}$ be a function with divisor

$$(f_{s,P}) = s(P) - ([s]P) - (s-1)\mathcal{O}\,,$$

then the Tate pairing is a well-defined, non-degenerate, bilinear pairing

$$\langle \cdot, \cdot \rangle_r : \begin{cases} E[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) \to & \mathbb{F}^*_{q^k}/(\mathbb{F}^*_{q^k})^r \\ (P,Q) & \mapsto \langle P,Q\rangle_r = f_{r,P}(D). \end{cases}$$

The output of this pairing is only defined up to a coset of $(\mathbb{F}_{q^k}^*)^r$, however for protocols we will require a unique element of $\mathbb{F}_{q^k}^*$. Hence to obtain a unique representative, one defines the reduced Tate pairing as

$$e(P,Q) = \langle P,Q\rangle_r^{(q^k-1)/r} = f_{r,P}(D)^{(q^k-1)/r} \in \mathbb{G}_T.$$

It is not difficult to show [2] that if $k > 1$ one can in fact ignore working with the divisor D and simply work with the point Q, i.e. one can define the reduced Tate pairing as $e(P,Q) = f_{r,P}(Q)^{(q^k-1)/r}$. A second useful property [12] is that r can be replaced by any integer N such that $r \mid N \mid q^k - 1$, i.e. $e(P,Q) = f_{N,P}(Q)^{(q^k-1)/N}$.

To compute the function $f_{s,P}$ for $s > 0$, one can simply use Miller's algorithm [17]. For $s < 0$ it suffices to remark that $(f_{s,P}) = -(f_{-s,P}) - (v_{sP})$ with v_{sP} the vertical line through sP, so we can take $f_{s,P} = 1/(f_{-s,P}v_{sP})$. If k is even, then v_{sP} can be ignored due to the final powering operation.

3 The Ate Pairing

In this section we introduce the Ate pairing and show that it extends and simplifies the Eta pairing introduced in [1]. Indeed, the conditions stated in [1, Theorem 1] are in fact automatically satisfied.

Although the Tate pairing as defined in the previous section allows arguments $P \in E[r]$ and $Q \in E(\mathbb{F}_{q^k})$, in practice one often works with specific subgroups to speed-up the pairing computation. Let π_q be the Frobenius endomorphism, i.e. $\pi_q : E \to E : (x,y) \mapsto (x^q, y^q)$, then the following choice seems to be optimal:

- the group $\mathbb{G}_1 = E[r] \cap \mathrm{Ker}(\pi_q - [1])$,
- the group $\mathbb{G}_2 = E[r] \cap \mathrm{Ker}(\pi_q - [q])$.

Although in practice one has always used the Tate pairing on $\mathbb{G}_1 \times \mathbb{G}_2$, from a theoretical point of view, the Tate pairing on $\mathbb{G}_2 \times \mathbb{G}_1$ has a much nicer structure.

3.1 The Ate Pairing on $\mathbb{G}_2 \times \mathbb{G}_1$

The main result of this section is summarised in the following theorem.

Theorem 1. *Let E be an elliptic curve over $\mathbb{F}_q$, r a large prime with $r \mid \#E(\mathbb{F}_q)$ and denote the trace of Frobenius with t, i.e. $\#E(\mathbb{F}_q) = q+1-t$. For $T = t-1$, $Q \in \mathbb{G}_2 = E[r] \cap \mathrm{Ker}(\pi_q - [q])$ and $P \in \mathbb{G}_1 = E[r] \cap \mathrm{Ker}(\pi_q - [1])$, we have the following:*

- *$f_{T,Q}(P)$ defines a bilinear pairing, which we call the Ate pairing*
- *let $N = \gcd(T^k - 1, q^k - 1)$ and $T^k - 1 = LN$, with k the embedding degree, then*

$$e(Q,P)^L = f_{T,Q}(P)^{c(q^k-1)/N} \tag{1}$$

  where $c = \sum_{i=0}^{k-1} T^{k-1-i}q^i \equiv kq^{k-1} \bmod r$
- *for $r \nmid L$, the Ate pairing is non-degenerate*

The proof of Theorem 1 follows immediately from the following three short lemma's.

Lemma 1. *Using the notation of Theorem 1, we have*

$$e(Q,P)^L = f_{T^k,Q}^{(q^k-1)/N}\,.$$

PROOF: By definition of the reduced Tate pairing, we have to compute

$$e(Q,P) = f_{r,Q}(P)^{(q^k-1)/r} = f_{N,Q}(P)^{(q^k-1)/N}\,,$$

for any N with $r \mid N \mid q^k-1$. Note that indeed $r \mid N$: by definition of t we have $\#E(\mathbb{F}_q) = q+1-t$, therefore $q \equiv t-1 \bmod r$ and thus $(t-1)^k \equiv 1 \bmod r$. Consider the equalities

$$\begin{aligned} e(Q,P)^L &= f_{N,Q}(P)^{L(q^k-1)/N} = f_{LN,Q}(P)^{(q^k-1)/N} \\ &= f_{T^k-1,Q}(P)^{(q^k-1)/N}\,, \end{aligned}$$

where the first follows from the definition of the reduced Tate pairing, the second holds since we can take $f_{LN,Q} = f_{N,Q}^L$ and the third equality follows from the definition of L and N. Furthermore, note that $(f_{T^k-1,Q}) = (f_{T^k,Q})$ since $Q \in E[r]$, so without loss of generality we can take $f_{T^k-1,Q} = f_{T^k,Q}$, which ends the proof. □

An easy calculation [1, Lemma 2] proves the following lemma.

Lemma 2. *Using the notation of Theorem 1 we can choose $f_{T^k,Q}$ such that*

$$f_{T^k,Q} = f_{T,Q}^{T^{k-1}} f_{T,TQ}^{T^{k-2}} \cdots f_{T,T^{k-1}Q}\,. \tag{2}$$

The crucial point is now that each of the factors in the right hand side of (2) can be expressed in terms of $f_{T,Q}$. To see this, note that since $Q \in \mathbb{G}_2$, we have $\pi_q(Q) = [q]Q = [t-1]Q = [T]Q$ and similarly $\pi_q^i(Q) = [T^i]Q$, so it suffices to relate $f_{T,\pi_q^i(Q)}$ with $f_{T,Q}$ as in the following lemma.

Lemma 3. *For all $Q \in \mathbb{G}_2$, we can take $f_{T,\pi_q^i(Q)} = f_{T,Q}^{\sigma^i}$, with σ the q-th power Frobenius automorphism of $\overline{\mathbb{F}}_q$.*

PROOF: By definition we have $(f_{T,\pi_q^i(Q)}) = T(\pi_q^i(Q)) - (\pi_q^{i+1}(Q)) - (T-1)(\mathcal{O})$ and since π_q is purely inseparable of degree q we have

$$\begin{aligned} (\pi_q^i)^*(f_{T,\pi_q^i(Q)}) &= q^i T(Q) - q^i(\pi_q(Q)) - q^i(T-1)(\mathcal{O}) \\ &= (f_{T,Q}^{q^i})\,. \end{aligned}$$

Furthermore, $(\pi_q^i)^*(f_{T,\pi_q^i(Q)}) = (f_{T,\pi_q^i(Q)} \circ \pi_q^i)$, so we can take

$$f_{T,\pi_q^i(Q)} \circ \pi_q^i = f_{T,Q}^{q^i}\,.$$

Rewriting $f_{T,Q}^{q^i} = f_{T,Q}^{\sigma^i} \circ \pi_q^i$ then shows that we can take $f_{T,\pi_q^i(Q)} = f_{T,Q}^{\sigma^i}$. □

Note that there is also a much easier proof of the above lemma; however the technique in the above proof will be used later, which is why we have given the more complicated version above. For completeness, the easier proof goes as follows: the coefficients of $f_{T,Q}$ are polynomial functions of the coefficients of the curve and the coordinates of Q. Since the curve is defined over $\mathbb{F}_q$, the q-th power Frobenius σ only acts on the coordinates of Q, so we can indeed take $f_{T,\pi_q^i(Q)} = f_{T,Q}^{\sigma^i}$.

PROOF OF THEOREM 1: since $P \in \mathbb{G}_1$ and in particular, $P \in \mathrm{Ker}(\pi_q - 1)$, Lemma 3 implies

$$f_{T,\pi_q^i(Q)}(P) = f_{T,Q}^{\sigma^i}(P) = (f_{T,Q}(P))^{q^i},$$

and using Lemma 2, we obtain

$$f_{T^k,Q}(P) = f_{T,Q}(P)^{\sum_{i=0}^{k-1} T^{k-1-i} q^i}.$$

Substituting the above in Lemma 1, we recover Equation (1)

$$e(Q,P)^L = f_{T,Q}(P)^{c(q^k-1)/N}$$

with $c = \sum_{i=0}^{k-1} T^{k-1-i} q^i \equiv k q^{k-1} \bmod r$. This equation shows that $f_{T,Q}(P)$ defines a bilinear pairing (since $e(Q,P)$ is bilinear), which is non-degenerate if $r \nmid L$, since $e(Q,P)$ itself is non-degenerate. □

For $T^k - 1 \neq 0$, the Ate pairing will be non-degenerate since then $r \nmid L$. Indeed, since $q \equiv T \bmod r$ and since we assumed that $r^2 \nmid q^k - 1$, we also have $r^2 \nmid T^k - 1$ and thus $r \nmid L$, since $r \mid N$. The condition $T^k - 1 \neq 0$ is easily seen to be equivalent with $t \neq 2$ or $t \neq 0$ for k even. In this case, the Ate pairing $f_{T,Q}(P)$ defines a non-degenerate, bilinear pairing on $\mathbb{G}_2 \times \mathbb{G}_1 \longrightarrow \mathbb{G}_T$. Similarly, we have the reduced Ate pairing $f_{T,Q}(P)^{(q^k-1)/r}$, which by (1) equals a fixed power of the reduced Tate pairing. Indeed, let $N = rs$ then $r \nmid s$ since this would again imply $r^2 \mid T^k - 1$. Note that $r \nmid c$ since $r > k$ and $r \nmid q$, so we conclude that the reduced Ate pairing equals $e(Q,P)^M$ with $M \equiv Lsc^{-1} \bmod r$. Also note that the Ate pairing requires a Full-Miller operation, but with a shorter loop than the Miller-lite operation in the Tate pairing.

3.2 The Ate Pairing on $\mathbb{G}_1 \times \mathbb{G}_2$

In this section we study whether the same technique applies to $\mathbb{G}_1 \times \mathbb{G}_2$. Denote with $\hat{\pi}_q$ the dual of the Frobenius endomorphism π_q (also called Verschiebung), then since $\hat{\pi}_q \circ \pi_q = [q]$, we conclude that $\hat{\pi}_q$ acts as

- $\hat{\pi}_q(P) = [q]P = [t-1]P = [T]P$ for $P \in \mathbb{G}_1$, so $\mathbb{G}_1 = E[r] \cap \mathrm{Ker}(\hat{\pi}_q - [q])$,
- $\hat{\pi}_q(Q) = Q$ for $Q \in \mathbb{G}_2$, so $\mathbb{G}_2 = E[r] \cap \mathrm{Ker}(\hat{\pi}_q - [1])$.

It is clear that Lemma 1 and 2 remain valid when P and Q are swapped. The main problem arises in Lemma 3 when we try to work with Verschiebung instead of Frobenius. We now have to make an explicit distinction between supersingular and ordinary curves, since $\hat{\pi}_q$ has fundamentally different properties in these cases.

Supersingular Case In the supersingular case, we have $E[q^i] = \{\mathcal{O}\}$ and $\hat{\pi}_q^i$ is purely inseparable of degree q^i. The same proof as in Lemma 3 shows that we can take

$$f_{T,\hat{\pi}_q^i(P)} \circ \hat{\pi}_q^i = f_{T,P}^{q^i}\,.$$

Since $\hat{\pi}_q$ acts trivially on $Q \in \mathbb{G}_2$, we conclude that in fact

$$(f_{T,\hat{\pi}_q^i(P)} \circ \hat{\pi}_q^i)(Q) = f_{T,\hat{\pi}_q^i(P)}(Q) = (f_{T,P}(Q))^{q^i}\,.$$

Since this is exactly the same as in the previous section, we conclude that

$$e(P,Q)^L = f_{T,P}(Q)^{c(q^k-1)/N}\,,$$

with $c = \sum_{i=0}^{k-1} T^{k-1-i}q^i \equiv kq^{k-1} \bmod r$. Note that this result corresponds to [1, Theorem 1], but without the need for an automorphism.

Ordinary Case In the ordinary case, we have $E[q^i] \simeq \mathbb{Z}/q^i\mathbb{Z}$ and $\hat{\pi}_q^i$ separable with kernel $\mathrm{Ker}(\hat{\pi}_q^i) = E[q^i]$. If we now try to mimic the proof of Lemma 3, we run into the following problem. By definition of the pull back on a divisor and since $\hat{\pi}_q$ is unramified, we have

$$(\hat{\pi}_q^i)^*(\hat{\pi}_q^i P) = \sum_{R \in E[q^i]} (P+R)\,,$$

and thus

$$\begin{aligned}(\hat{\pi}_q^i)^*(f_{T,\hat{\pi}_q^i(P)}) = T \sum_{R\in E[q^i]} (P+R) - \sum_{R\in E[q^i]} (TP+R)\\ -(T-1)\sum_{R\in E[q^i]} (R)\,.\end{aligned}$$

By properties of the pull back we also have

$$(\hat{\pi}_q^i)^*(f_{T,\hat{\pi}_q(P)}) = (f_{T,\hat{\pi}_q(P)} \circ \hat{\pi}_q^i)\,.$$

So we have explicitly computed the divisor of $f_{T,\hat{\pi}_q(P)} \circ \hat{\pi}_q^i$ and as before, would like to relate this to the divisor of $f_{T,P}$, but this seems difficult since $\hat{\pi}_q$ has non-trivial kernel. Furthermore, it is not very surprising that no easy relation exists, since any explicit example shows that in the ordinary case $f_{T,P}(Q)^{(q^k-1)/r}$ does not define a bilinear pairing.

The failure of the above technique also suggest a partial solution: as we will show in Section 6, for some elliptic curves, there exists an integer e such that $\hat{\pi}_q^e$ acts as an automorphism on $\mathbb{G}_1$. In this case, we will be able to relate $e(P,Q)$ to $f_{T^e,P}(Q)$ using the theory of twists.

4 Twists of Ordinary Elliptic Curves over $\mathbb{F}_{p^n}$, $p \geq 5$

In this section we study the twists of an ordinary elliptic curve E over a finite field $\mathbb{F}_q$ with $q = p^n$ and $p \geq 5$. We will derive their group orders and show how the structure of $E(\mathbb{F}_{q^d})$ relates to the various twists of degree d. Much of what follows is well known to the experts but we have been unable to find a location where all these relevant facts and proofs are located. Hence, we present the facts we need and some extensions here.

4.1 Existence of Twists

We begin with the following definition.

Definition 1. *Let E and E' be two elliptic curves over $\mathbb{F}_q$, then E' is called a twist of degree d of E if there exists an isomorphism $\phi_d : E' \to E$ defined over $\mathbb{F}_{q^d}$ and d is minimal.*

Although not immediate from the above definition, there are only a very limited number of possible degrees d. To see why, let σ be the q-th power Frobenius automorphism of $\overline{\mathbb{F}}_q$, then $\phi_d^\sigma \circ \phi_d^{-1} \in \mathrm{Aut}(E)$, with ϕ_d^σ the isomorphism obtained by applying σ to the coefficients of ϕ_d. Furthermore, since d was chosen minimal, the order of this automorphism is d. So, if E' is a degree d twist of E, then $\mathrm{Aut}(E)$ must contain an element of order d. However, $\mathrm{Aut}(E)$ always is a finite group of order dividing 24 [20, Theorem III.10.1] and if $p \geq 5$, we have $\#\mathrm{Aut}(E) \mid 6$. So for $p \geq 5$, only $d = 2, 3, 4, 6$ are possible. Furthermore, all twists can be described explicitly as in [20, Proposition X.5.4]

Proposition 1. *Assume that $p \geq 5$, then the set of twists of E is canonically isomorphic with $\mathbb{F}_q^*/(\mathbb{F}_q^*)^d$ with $d = 2$ if $j(E) \neq 0, 1728$, $d = 4$ if $j(E) = 1728$ and $d = 6$ if $j(E) = 0$.*

Note that in the above cases we have that $\mathrm{Aut}(E) \cong \mu_d$, with μ_d the d-th roots of unity. If we assume that E is given by a short Weierstrass equation $E : y^2 = x^3 + ax + b$ with $a, b \in \mathbb{F}_q$, then an isomorphism is given by

$$[\cdot] : \mu_d \to \mathrm{Aut}(E) : \xi \mapsto [\xi] \quad \text{with} \quad [\xi](x, y) = (\xi^2 x, \xi^3 y)\,.$$

Also it is rather easy to find an equation for the twists given an equation for E. Let $D \in \mathbb{F}_q^*$, then the twists corresponding to D mod $(\mathbb{F}_q^*)^d$ are given by

$$\begin{array}{ll} d = 2 & : y^2 = x^3 + a/D^2 x + b/D^3, \ \phi_d : E' \to E : (x, y) \mapsto (Dx, D^{3/2} y) \\ d = 4 & : y^2 = x^3 + a/Dx, \qquad\quad \phi_d : E' \to E : (x, y) \mapsto (D^{1/2} x, D^{3/4} y) \\ d = 3, 6 & : y^2 = x^3 + b/D, \qquad\quad \phi_d : E' \to E : (x, y) \mapsto (D^{1/3} x, D^{1/2} y) \end{array}$$

An alternative representation of the quadratic twists, which may be more convenient from an implementation perspective, is given by

$$d = 2 : Dy^2 = x^3 + ax + b,\ \phi_d : E' \to E : (x, y) \mapsto (x, D^{1/2} y)$$

Note that if we want to construct a twist of degree d, then $\mathbb{F}_q^*/(\mathbb{F}_q^*)^d$ has to have d elements or equivalently, $q \equiv 1 \bmod d$.

4.2 Group Orders of Twists

Recall that the number of $\mathbb{F}_q$-rational points on an elliptic curve E over $\mathbb{F}_q$ is related to the Frobenius endomorphism $\pi_q : E \to E : (x, y) \mapsto (x^q, y^q)$, since $E(\mathbb{F}_q) = \mathrm{Ker}(\pi_q - 1)$. The following theorem summarises the result.

Theorem 2. *Let E be an elliptic curve over $\mathbb{F}_q$, then there exists $t \in \mathbb{Z}$, called the trace of Frobenius, with $|t| \leq 2\sqrt{q}$ such that $\pi_q^2 - [t] \circ \pi_q + [q] = [0]$ in $\mathrm{End}(E)$ and $\#E(\mathbb{F}_q) = q + 1 - t$. Furthermore, let $\alpha \in \mathbb{C}$ be a root of $X^2 - tX + q$, then*

$$\forall k \in \mathbb{N}_0 : \#E(F_{q^k}) = q^k + 1 - \alpha^k - \bar{\alpha}^k \,.$$

Let E be an elliptic curve over $\mathbb{F}_q$ admitting a twist E' of degree d. Then by definition E and E' become isomorphic over $\mathbb{F}_{q^d}$, and in particular $\#E(\mathbb{F}_{q^d}) = \#E'(\mathbb{F}_{q^d})$. The above theorem shows that $\alpha = \xi\alpha'$ for some $\xi \in \mu_d$, so there are only d possibilities for $\#E'(\mathbb{F}_q)$. In fact, since E' is a twist of degree d (and not smaller), there are only $\varphi(d)$ possibilities, namely for ξ a primitive d-th root of unity.

Proposition 2. *Let E be an ordinary elliptic curve over $\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = q + 1 - t$, admitting a twist E' of degree d, then the possible group orders of $E'(\mathbb{F}_q)$ are given by the following:*

$$\begin{array}{ll}
\underline{d = 2} : \#E'(\mathbb{F}_q) = q + 1 + t & \\
\underline{d = 3} : \#E'(\mathbb{F}_q) = q + 1 - (3f - t)/2 & \text{with } t^2 - 4q = -3f^2 \\
\#E'(\mathbb{F}_q) = q + 1 - (-3f - t)/2 & \text{with } t^2 - 4q = -3f^2 \\
\underline{d = 4} : \#E'(\mathbb{F}_q) = q + 1 + f & \text{with } t^2 - 4q = -f^2 \\
\#E'(\mathbb{F}_q) = q + 1 - f & \text{with } t^2 - 4q = -f^2 \\
\underline{d = 6} : \#E'(\mathbb{F}_q) = q + 1 - (-3f + t)/2 & \text{with } t^2 - 4q = -3f^2 \\
\#E'(\mathbb{F}_q) = q + 1 - (3f + t)/2 & \text{with } t^2 - 4q = -3f^2
\end{array}$$

Proof:

- $d = 2$: since -1 is the only 2-nd primitive root, we get $\alpha' = -\alpha$ or $t' = -t$ and the result follows.
- $d = 3$: note that $\mu_3 \subset \mathrm{End}(E)$ and since E is assumed ordinary, $\mathrm{End}(E)$ is an order in the imaginary quadratic field $\mathbb{Q}(\sqrt{\Delta})$ with $\Delta = t^2 - 4q$. However, the only imaginary quadratic field containing μ_3 is $\mathbb{Q}(\sqrt{-3})$ and thus $t^2 - 4q = -3 \cdot f^2$ for some $f \in \mathbb{N}_0$. It follows that we can take $\alpha = (t + f\sqrt{-3})/2$. The two possibilities for α' then are $\alpha' = \xi_3\alpha$ and $\alpha' = \xi_3^2\alpha$ with $\xi_3 = (-1 + \sqrt{-3})/2$. The result follows since $t' = \alpha' + \bar{\alpha'}$.
- $d = 4$: here we have $\mu_4 \subset \mathrm{End}(E)$ and since the only imaginary quadratic field containing μ_4 is $\mathbb{Q}(i)$, we can write $t^2 - 4q = -f^2$ with $f \in \mathbb{N}_0$. Also, we can take $\alpha = (t + fi)/2$ and the only possibilities for α' are $\alpha' = i\alpha$ and $\alpha' = -i\alpha$. Again the result follows.
- $d = 6$: the reasoning is entirely the same as for $d = 3$, but now $\alpha' = \xi_6\alpha$ or $\alpha' = \xi_6^5\alpha$ with $\xi_6 = (1 + \sqrt{-3})/2$.

□

4.3 A Structure Theorem

Let E be an elliptic curve over $\mathbb{F}_q$ admitting a twist E' of degree d. In this section we prove a "folklore" result about $E(\mathbb{F}_{q^d})$ being essentially a direct sum of the $\mathbb{F}_q$-rational points on its d twists over $\mathbb{F}_q$. Whilst we shall only require a much weaker result, we feel it may be of some independent interest to those working in elliptic curve cryptography.

Let π_q (resp. π'_q) be the Frobenius endomorphism on E (resp. E'). Note that the isomorphism $\phi_d : E' \to E$ gives rise to a ring isomorphism

$$\Phi_d : \mathrm{End}(E') \to \mathrm{End}(E) : f \mapsto \Phi_d(f) = \phi_d \circ f \circ \phi_d^{-1} .$$

Since for any rational map $h : E \to E'$ we clearly have $\pi'_q \circ h = h^\sigma \circ \pi_q$, we conclude that

$$\Phi_d(\pi'_q) = \phi_d \circ \pi'_q \circ \phi_d^{-1} = \phi_d \circ (\phi_d^{-1})^\sigma \circ \pi_q .$$

Again since the degree is d, we conclude that $\phi_d \circ (\phi_d^{-1})^\sigma \in \mathrm{Aut}(E)$ of order precisely d, i.e. is a primitive d-th root of unity. Since we have an isomorphism $[\cdot] : \mu_d \to \mathrm{Aut}(E)$, we can label the twists E_i (degree dividing d) of E for $i = 0, \ldots, d-1$ by $\Phi_i(\pi_{q,i}) = [\xi_d^i]\pi_q$ with ξ_d a fixed primitive d-th root of unity, $\pi_{q,i}$ the Frobenius endomorphism on E_i and Φ_i the ring isomorphism induced by the isomorphism $\phi_i : E_i \to E$.

Given the d twists E_i of E of degree dividing d, we would like to know whether

$$E(\mathbb{F}_{q^d}) \cong \bigoplus_{i=0}^{d-1} E_i(\mathbb{F}_q) .$$

To see why this is a sensible question, note that the $\mathbb{F}_{q^d}$-rational points on E are precisely the fixed points of π_q^d, i.e. $E(\mathbb{F}_{q^d}) = \mathrm{Ker}(\pi_q^d - 1)$. Similarly, we have $E_i(\mathbb{F}_q) = \mathrm{Ker}(\pi_{q,i} - 1)$. Since by the labelling $\Phi_i(\pi_{q,i}) = [\xi_d^i]\pi_q$, we have an immediate isomorphism

$$E_i(\mathbb{F}_q) \simeq \mathrm{Ker}([\xi_d^i]\pi_q - 1) .$$

Furthermore, we can factor $\pi_q^d - 1 = (-1)^{d-1} \prod_{i=0}^{d-1} ([\xi_d^i]\pi_q - 1)$. Since $\pi_q^d - 1$ is separable, we simply take the degree of both sides and conclude $\#E(\mathbb{F}_{q^d}) = \prod_{i=0}^{d-1} E_i(\mathbb{F}_q)$.

A necessary condition for $E(\mathbb{F}_{q^d}) \cong \oplus_{i=0}^{d-1} E_i(\mathbb{F}_q)$ to hold, clearly is

$$\mathrm{Ker}([\xi_d^i]\pi_q - 1) \cap \mathrm{Ker}([\xi_d^j]\pi_q - 1) = \mathcal{O} \quad \text{for all } i \neq j , \tag{3}$$

which is equivalent with $E(\mathbb{F}_{q^d}) \cap \mathrm{Ker}([\xi_d^k] - 1) = \mathcal{O}$ for $k = 1, \ldots, d-1$. By taking degrees, it is easy to see that $\mathrm{Ker}([\xi_d^k] - 1) \subset E[d]$, with $E[d]$ the d-torsion points on E. However, a more detailed analysis shows that (3) holds if and only if:

- $d = 2, 4$: $E(\mathbb{F}_{q^d}) \cap E[2] = \mathcal{O}$
- $d = 3$: $E(\mathbb{F}_{q^d}) \cap \mathrm{Ker}([\xi_3] - 1) = \mathcal{O}$ with $\mathrm{Ker}([\xi_3] - 1) \subsetneq E[3]$

– $d = 6$: $E(\mathbb{F}_{q^d}) \cap E[2] = \mathcal{O}$ and $E(\mathbb{F}_{q^d}) \cap \mathrm{Ker}([\xi_3] - 1) = \mathcal{O}$

Furthermore, translating these conditions back to $E(\mathbb{F}_q)$, we get the following very natural condition: (3) holds if and only if

$$\forall p_i \mid d,\ p_i \text{ prime } : \#E(\mathbb{F}_q) \not\equiv 0 \bmod p_i\,. \tag{4}$$

The following theorem shows that this is in fact also a sufficient condition.

Theorem 3. *Let E be an ordinary elliptic curve over $\mathbb{F}_q$ admitting a twist of degree d and let E_i for $i = 0, \ldots, d-1$ be the twists of E of degree dividing d. Assume that $\#E(\mathbb{F}_q)$ satisfies condition (4), then*

$$E(\mathbb{F}_{q^d}) \cong \bigoplus_{i=0}^{d-1} E_i(\mathbb{F}_q)\,.$$

Proof: Let $f_i = [\xi_d^i]\pi_q - 1$ for $i = 0, \ldots, d-1$, then as shown above we have $\mathrm{Ker}(f_i) \cap \mathrm{Ker}(f_j) = \mathcal{O}$ for $i \neq j$ and $\#E(\mathbb{F}_{q^d}) = \prod_{i=0}^{d-1} \#\,\mathrm{Ker}(f_i)$. Furthermore, since the curve is ordinary, we have $f_i \circ f_j = f_j \circ f_i$ for all i, j. Now apply Lemma 4, which finalises the proof. □

Lemma 4. *Let G be a finite abelian group and let f_i for $i = 0, \ldots, d-1$ be d endomorphisms such that $f_i \circ f_j = f_j \circ f_i$, $\mathrm{Ker}(f_i) \cap \mathrm{Ker}(f_j) = 0_G$ with 0_G the neutral element of G and $\#G = \prod_{i=0}^{d-1} \#\,\mathrm{Ker}(f_i)$, then $G = \bigoplus_{i=0}^{d-1} \mathrm{Ker}(f_i)$.*

Proof: Since by assumption the kernels have intersection $\{0_G\}$ and $\#G = \prod_{i=0}^{d-1} \#\,\mathrm{Ker}(f_i)$, it suffices to prove that each element $g \in G$ can be written uniquely as $g = \sum_{i=0}^{d-1} e_i$ with $e_i \in \mathrm{Ker}(f_i)$. Equivalently, if $0_G = \sum_{i=0}^{d-1} e_i$ with $e_i \in \mathrm{Ker}(f_i)$, then $e_i = 0_G$.

To see this, first note that f_j restricted to $\mathrm{Ker}(f_i)$ is an isomorphism for all $i \neq j$. Indeed, $f_j \circ f_i = f_i \circ f_j$ implies that $f_j(\mathrm{Ker}(f_i)) \subset \mathrm{Ker}(f_i)$ and $\mathrm{Ker}(f_i) \cap \mathrm{Ker}(f_j) = 0_G$ implies that f_j is injective on $\mathrm{Ker}(f_i)$ and thus also surjective.

Let $g_i = \circ_{j \neq i} f_j$, i.e. the composition of all f_j without f_i, then $g_i(e_j) = 0_G$ for $i \neq j$ and thus also $g_i(e_i) = 0_G$. However, by the above g_i is an isomorphism on $\mathrm{Ker}(f_i)$ and thus $e_i = 0_G$ which finishes the proof. □

In practice however, we only need the following result: since the intersection $\mathrm{Ker}([\xi_d^i]\pi_q - 1) \cap \mathrm{Ker}([\xi_d^j]\pi_q - 1)$ for $i \neq j$ is contained in $E[d]$, we conclude immediately that if $l > d$ is a prime with $l \mid\mid \#E(\mathbb{F}_q)$ and $l^2 \mid\mid \#E(\mathbb{F}_{q^d})$ with d minimal, then there exists a *unique* twist E_i of degree d such that $l \mid\mid \#E_i(\mathbb{F}_q)$.

5 Representing the Group $\mathbb{G}_2$

Recall that the group $\mathbb{G}_2$ was defined as $\mathbb{G}_2 = E[r] \cap \mathrm{Ker}(\pi_q - q)$, i.e. the q-eigenspace of Frobenius on $E[r]$. Assume that E admits a twist of degree d and

let $m = \gcd(k, d)$ and $e = k/m$. Since k is the minimal value such that r divides $q^k - 1$, we know that the group $E(\mathbb{F}_{q^e})$ has order divisible by r, but not r^2. Furthermore, since $r \geq 7$, we know that there is a unique degree m twist E' of E over $\mathbb{F}_{q^e}$ such that $r \mid \#E'(\mathbb{F}_{q^e})$. This unique degree m twist can be easily found using Proposition 2, since there will only be one possible group order divisible by r.

By the analysis in the previous section, there exists a unique primitive m-th root of unity ξ_m such that

$$E'(\mathbb{F}_{q^e}) \simeq \mathrm{Ker}([\xi_m]\pi_q^e - 1)\,.$$

Since $\mathrm{Ker}([\xi_m]\pi_q^e - 1)$ is stable under π_q, we conclude $\mathbb{G}_2 = E[r] \cap \mathrm{Ker}([\xi_m]\pi_q^e - 1)$. As such, we obtain a much more efficient representation of $\mathbb{G}_2$ as the unique subgroup $\mathbb{G}_2'$ of $E'(\mathbb{F}_{q^e})$ of order r. Furthermore, as shown above, there is a monomorphism

$$\phi_m : E'(\mathbb{F}_{q^e}) \rightarrow E(\mathbb{F}_{q^k})\,,$$

so we in fact obtain a modified pairing $\hat{e}$ of an element $P \in \mathbb{G}_1$ and an element in $Q' \in \mathbb{G}_2'$ via

$$\hat{e}(P, Q') = e(P, \phi_m(Q'))\,.$$

When k is even and $d = 2$ we recover the standard trick of representing $\mathbb{G}_2$ as the quadratic twist of E over $\mathbb{F}_{q^{k/2}}$. For $k = 12, d = 6$ and $q \equiv 1 \pmod 6$ we recover the representation of $\mathbb{G}_2$ as an elliptic curve of $\mathbb{F}_{q^2}$ as presented by Barreto and Naehrig [4].

However, we achieve similar savings for other values of k which are of practical interest. For example, all curves given by Brezing and Weng [8] have either $d = 4$ or $d = 6$ and so one can use the above technique to significantly improve the performance of arithmetic in $\mathbb{G}_2$ over the standard quadratic twist technique.

It is common to implement the finite fields in pairing based systems via so-called pairing friendly fields [19]. These are finite fields defined by a polynomial

$$f(X) = X^k + f_0$$

where $f_0 \in \mathbb{F}_q$. These fields offer good arithmetic, in particular they enable fast reduction and also enable faster squaring in the cyclotomic subgroup in which μ_r is embedded [14]. They also enable the subfields to be implemented relatively efficiently via the polynomial

$$X^{k/i} + f_0$$

for a subfield of index i.

Calculation on the d-th twist can be made simpler by choosing the polynomial $f(X)$ such that in the subfield defined by the polynomial

$$g(X) = X^{k/d} + f_0$$

the value of D which defines the twist is given by the formal root of $g(X)$, i.e. we take the twist defined by $D = (-f_0)^{d/k}$. This enables multiplication by D to be performed by a simple coefficient shift in the polynomial basis.

Using pairing friendly fields we can naively quantify the improvement. If we write $k = 2^i 3^j$ and use Karatsuba and/or Toom-Cook multiplication/squaring in the extension field, then point addition in $E(\mathbb{F}_{q^k})$ requires time proportional to $3^i 5^j$ multiplications in $\mathbb{F}_q$.

If one used the standard quadratic twist representation of $\mathbb{G}_2$, then point addition in $\mathbb{G}_2'$ would require time proportional to $3^{i-1}5^j$. However, if we use the representation using sextic twists then arithmetic in $\mathbb{G}_2$ would require time proportional to $3^{i-1}5^{j-1}$. Hence, a five fold performance improvement in the basic group operations.

If one selects q to maximise d then one achieves the performance improvement indicated in Table 1 for various practical values of k, when comparing the degree m twist representation with the standard quadratic twist representation. Note, in this table we assume that optimal curves can be produced, i.e. curves whose parameters balance the security of the DLP in the elliptic curve and the finite field. In practice such curves may not be able to be generated, so the improvement may not be so pronounced in selecting $m = 4$ or 6 over $m = 2$.

Further performance improvements can be made in the case of point multiplication in $\mathbb{G}_2'$ via the use of the endomorphism coming from the small CM discriminant, using the techniques of [13]. When performing cofactor multiplication to generate random elements in $\mathbb{G}_2$ the performance improvement is even greater since the cofactor we need to multiply by also shrinks by a factor of around $(k-1)/(e-1)$.

Table 1. Performance Improvement For Various k and m

k	$m = 4$	$m = 6$
6	1	5
8	3	1
10	1	1
12	3	5
24	3	5

6 Twisted Ate Pairing

In Section 3, we studied the relation between $e(P, Q)$ and $f_{T,P}(Q)$, by exploiting the definitions of $\mathbb{G}_1 = E[r] \cap \mathrm{Ker}(\pi_q - 1)$ and $\mathbb{G}_2 = E[r] \cap \mathrm{Ker}(\pi_q - q)$. For ordinary curves, we concluded that there was no such relation, basically due to the non-trivial kernel of the dual of Frobenius $\hat{\pi}_q$.

In this section, we will assume that E admits a twist of degree d and again we set $m = \gcd(k, d)$ and $e = k/m$. In this case, we have the alternative representation of $\mathbb{G}_2$ as

$$\mathbb{G}_2 = E[r] \cap \mathrm{Ker}([\xi_m]\pi_q^e - 1)\,,$$

for a unique primitive m-th root of unity ξ_m. Since π_q acts as multiplication by q on $\mathbb{G}_2$, we conclude that $[\xi_m]$ acts as multiplication by q^{-e} on $\mathbb{G}_2$. Since $E[r] = \mathbb{G}_1 \times \mathbb{G}_2$ and $[\xi_m]$ has degree 1, we conclude that $[\xi_m]$ acts as multiplication by q^e on $\mathbb{G}_1$.

As in Section 3, let $T = t - 1$ and recall that $T \equiv q \bmod r$. Note that for $P \in \mathbb{G}_1$ we have

$$[q^e]P = [T^e]P = [\xi_m]P\,.$$

Since $[\xi_m]$ is an automorphism of the curve and thus has trivial kernel, we are able to prove the following lemma.

Lemma 5. *For all $P \in \mathbb{G}_1$, we can take $f_{T^e,[\xi_m]P} \circ [\xi_m] = f_{T^e,P}$.*

Proof: Since $[\xi_m]$ is an automorphism of the curve and thus separable of degree 1, we have

$$\begin{aligned}(f_{T^e,[\xi_m]P} \circ [\xi_m]) &= [\xi_m]^*(f_{T^e,[\xi_m]P}) \\ &= [\xi_m]^*\left(T^e([\xi_m]P) - (T^e[\xi_m]P) - (T-1)(\mathcal{O})\right) \\ &= T^e(P) - (T^eP) - (T-1)(\mathcal{O}) \\ &= (f_{T^e,P}).\end{aligned}$$

Which ends the proof. □

Since $f_{T^e,P}$ is defined over $\mathbb{F}_q$, we have $f_{T^e,[\xi_m]P} \circ [\xi_m] \circ \pi_q^e = f_{T^e,P}^{q^e}$ and thus for $Q \in \mathbb{G}_2$, $f_{T^e,T^eP}(Q) = f_{T^e,[\xi_m]P}(Q) = f_{T^e,P}(Q)^{q^e}$. A similar reasoning as in Section 3, then finally shows that

$$e(P,Q)^L = f_{T^e,P}(Q)^{c(q^k-1)/N}\,, \tag{5}$$

with $N = \gcd(T^k - 1, q^k - 1)$, $T^k - 1 = LN$, $c = \sum_{i=0}^{m-1} T^{e(m-1-i)}q^{ei} \equiv mq^{e(m-1)} \bmod r$.

For $T^k - 1 \neq 0$, we have $r \nmid L$ and Equation (5) shows that $f_{T^e,P}(Q)$ defines a non-degenerate bilinear pairing on $\mathbb{G}_1 \times \mathbb{G}_2$, which we call the *twisted Ate pairing*. Similarly, the reduced twisted Ate pairing is defined by $f_{T^e,P}(Q)^{(q^k-1)/r}$. Note that this pairing can only be faster than the Tate pairing when $|T^e| \leq r$, so especially when the trace is small compared to r.

7 Efficiency Comparison

We now turn to quantifying the performance of our different pairing algorithms, for different types of curves and extension degrees. As before we assume E is an ordinary elliptic curve over $\mathbb{F}_q$ with group order divisible by a large prime r, and we let k denote the embedding degree such that r divides $q^k - 1$. We let d denote the size of the set of possible twists of the curve over $\mathbb{F}_q$, i.e. $d = 6$ if E has complex multiplication by an order of $\mathbb{Q}(\sqrt{-3})$, $d = 4$ if it has complex multiplication by an order of $\mathbb{Q}(\sqrt{-1})$ and $d = 2$ otherwise. We set $m = \gcd(k, d)$,

which denotes the size of the twist available to us in our system and we let $e = k/m$ which denotes the degree of the field over which the twisted curve will be defined so as to produce the group $\mathbb{G}'_2$. To save space however, we only focus on the cases which produce $m = 2$ (as in standard implementations) and $m = 6$ which produces the greatest performance improvement.

We follow the analysis of [19], which was extended in [14]. We have three different pairings we need to compare, and since all involve the same final powering step, we need only focus on the Miller-like part of the algorithm. The final powering step can be computed efficiently using multi-exponentiation techniques and the Frobenius map, a technique introduced for pairings in [15] for $k = 6$ and applied in [14] to arbitrary k. Our three pairings are given by:

1. The standard Tate pairing, $f_{r,P}(Q)$.
2. The standard Ate pairing $f_{T,Q}(P)$, with $T = t - 1$.
3. The twisted Ate pairing $f_{T^e,P}(Q)$, with $T = t - 1$.

However, we also need to consider the size of t, for most curves this is of size $\sqrt{q}$, however it could possibly be as small as $r^{1/\varphi(k)}$. See [3, 10] for methods to construct curves for pairing based systems with $k \geq 12$ and such a small value of t. Hence, we also quantify the size in this case as well.

We let M_s, S_s, I_s denote the cost of multiplication, squaring and inversion in the finite field $\mathbb{F}_{q^s}$. As alluded to earlier, if we are using pairing friendly fields and $s = 2^i 3^j$ then we have

$$M_s = 3^i 5^j M_1 \text{ and } S_s = 3^i 5^j S_1.$$

Inversion costs can also be computed via a combination of the rules

$$I_{2s} = 2S_s + 2M_s + I_s \text{ and } I_{3s} = 3S_s + 11M_s + I_s.$$

We now turn to estimating the cost of evaluating the functions

$$f_{N,P}(Q) \text{ and } f_{N,Q}(P).$$

Following [19] we refer to the former as a Miller-Lite operation and the latter as the Full-Miller operation. We denote the cost of the Miller-Lite algorithm by C_{Lite}. Note, a Full-Miller operation can be performed either using projective coordinates or using affine coordinates, the exact choice as to which is more efficient depending on the ratio M_1/I_1. We denote the two different costs of the Full-Miller algorithm, by C^P_{Full} for the projective version and C^A_{Full} for the affine version. In computing the cost we only count, again following [19] and [14], the cost of the doubling part of Miller's algorithm. This part always needs to be computed irrespective of the signed Hamming weight of the multiplier N, and so can be used as a way of comparing algorithms independent of optimisations on N.

We assume that the elliptic curves are of the form

$$Y^2 = X^3 + AX + B$$

where $A = -3$ if $d = 2$ and $A = 0$ when $d = 6$. A careful analysis of the Miller-operations then reveals the following costs for each operation

$$C_{\text{Lite}} = \begin{cases} (4S_1 + (2e+7)M_1 + S_k + M_k)\log_2 N & \text{when } A = -3, \\ (5S_1 + (2e+6)M_1 + S_k + M_k)\log_2 N & \text{when } A = 0. \end{cases}$$

$$C^P_{\text{Full}} = \begin{cases} (4S_e + 6M_e + 2eM_1 + S_k + M_k)\log_2 N & \text{when } A = -3, \\ (5S_e + 6M_e + 2eM_1 + S_k + M_k)\log_2 N & \text{when } A = 0. \end{cases}$$

$$C^A_{\text{Full}} = (2S_e + 3M_e + I_e + eM_1 + S_k + M_k)\log_2 N \quad \text{any } A.$$

Table 2 represents the costs, in terms of multiplications/squarings in $\mathbb{F}_q$, of the different algorithms for various security levels. An average trace t is defined to be $t \sim \sqrt{q}$, whereas a small t is defined as $t \sim r^{1/\varphi(k)}$. Ate(P) refers to the Ate pairing implemented with projective coordinates, Ate(A) refers to the Ate pairing implemented with affine coordinates and Ate(T) refers to the twisted Ate pairing implemented with projective coordinates. The security levels are the same as those considered in [19]. In the table we made the assumption that $I_1/M_1 \approx 10$. We see that when $d = 2$ and for general t, the fastest method is almost always the traditional Tate pairing. For other values of d and t we see that the best choice of algorithm depends on the exact choice of k, p and n. However, at the high security levels we find that if one can select a trace which is relatively small one can achieve significant advantages.

Acknowledgements

We would like to thank Jasper Scholten for pointing out that f_j defines an isomorphism on $\text{Ker}(f_i)$ in Lemma 4, Steven Galbraith for several comments on an earlier version of this article, Rob Granger for pointing out an error in the program that generated Table 2 and the anonymous referees for various improvements.

References

1. P.S.L.M. Barreto, S. Galbraith, C. O'hEigeartaigh and M. Scott. Efficient pairing computation on supersingular abelian varieties. Preprint 2005, to appear in Designs, Codes and Cryptography.
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*, Springer LNCS 2442, 354–369, 2002.
3. P.S.L.M. Barreto, B. Lynn and M. Scott. Constructing elliptic curves with prescribed embedding degrees. Preprint, 2002.
4. P.S.L.M. Barreto and M. Naehrig. Pairing-friendly elliptic curves of prime order. In *Selected Areas in Cryptography – SAC 2005*, Springer-Verlag LNCS 3897, 319–331, 2006.
5. I.F. Blake, G. Seroussi and N.P. Smart. *Elliptic curves in cryptography.* Cambridge University Press, 1999.

Table 2. Cost of the various Miller algorithms for the different pairings

Security Level	Method	$d=2$ t		$d=6$ t	
		Average	Small	Average	Small
$k=6$	Tate	7520	7520	6880	6880
$p \approx 2^{160}$	Ate(P)	6880	6880	3440	3440
$r \approx 2^{160}$	Ate(A)	6560	6560	3680	3680
	Ate(T)	11280	11280	3440	3440
$k=6$	Tate	12032	12032	11008	11008
$p \approx 2^{512}$	Ate(P)	22016	11008	11008	5504
$r \approx 2^{256}$	Ate(A)	20992	10496	11776	5888
	Ate(T)	36096	18048	11008	5504
$k=12$	Tate	28928	28928	26880	26880
$p \approx 2^{256}$	Ate(P)	32256	16128	16256	8128
$r \approx 2^{256}$	Ate(A)	27520	13760	15488	7744
	Ate(T)	86784	43392	26880	13440
$k=6$	Tate	18048	18048	16512	16512
$p \approx 2^{1365}$	Ate(P)	58695	16512	29347	8256
$r \approx 2^{384}$	Ate(A)	55965	15744	31395	8832
	Ate(T)	96232	27072	29347	8256
$k=12$	Tate	43392	43392	40320	40320
$p \approx 2^{683}$	Ate(P)	86058	24192	43370	12192
$r \approx 2^{384}$	Ate(A)	73422	20640	41321	11616
	Ate(T)	231537	65088	71715	20160
$k=6$	Tate	24064	24064	22016	22016
$p \approx 2^{2560}$	Ate(P)	110080	22016	55040	11008
$r \approx 2^{512}$	Ate(A)	104960	20992	58880	11776
	Ate(T)	180480	36096	55040	11008
$k=12$	Tate	57856	57856	53760	53760
$p \approx 2^{1280}$	Ate(P)	161280	32256	81280	16256
$r \approx 2^{512}$	Ate(A)	137600	27520	77440	15488
	Ate(T)	433920	86784	134440	26880
$k=24$	Tate	156160	156160	147968	147968
$p \approx 2^{640}$	Ate(P)	238080	47616	120640	24128
$r \approx 2^{512}$	Ate(A)	195520	39104	110400	22080
	Ate(T)	1171200	234240	369920	73984

6. D. Boneh and M. Franklin. Identity based encryption from the Weil pairing. *SIAM Journal of Computing*, **32**, 586–615, 2003.
7. D. Boneh, B. Lynn and H. Shacham. Short signatures from the Weil pairing. *Advances in Cryptology – Asiacrypt 2001*, Springer-Verlag LNCS 2248, 514–532, 2001.
8. F. Brezing and A. Weng. Elliptic curves suitable for pairing based cryptography. *Designs, Codes and Cryptography*, **37**, 133–141, 2005.

9. I. M. Duursma and H.-S. Lee. Tate Pairing Implementation for Hyperelliptic Curves $y^2 = x^p - x + d$. In *Advances in Cryptology – ASIACRYPT 2003*, Springer-Verlag LNCS 2894, 111–123, 2003.
10. P. Duan, S. Cui and C.W. Chan. Special polynomial families for generating more suitable elliptic curves for pairing-based cryptosystems. Preprint, 2005.
11. S. Galbraith. Pairings. *Advances in elliptic curve cryptography*, London Math. Soc. Lecture Note Ser. **317**, 183–213, Cambridge Univ. Press, 2005.
12. S. Galbraith, K. Harrison and S. Soldera. Implementing the Tate pairing. In *Algorithmic Number Theory Symposium – ANTS V*, Springer LNCS 2369, 324–337, 2002.
13. R.P. Gallant, R.J. Lambert and S.A. Vanstone. Faster point multiplication on elliptic curves with efficient endomorphisms. In *Advances in Cryptology – CRYPTO 2001*, Springer-Verlag LNCS 2139, 190–200, 2001.
14. R. Granger, D. Page and N.P. Smart. High security pairing-based cryptography revisited. Preprint, 2006.
15. L. Hu, J.-W. Dong and D.-Y. Pei. Implementation of cryptosystems based on Tate pairing. *Journal of Computer Science and Technology*, **20**, 264–269, 2005.
16. A. Joux. A one round protocol for tripartite Diffie–Hellman. In *Algorithmic Number Theory Symposium – ANTS IV*, Springer-Verlag LNCS 1838, 385–394, 2000.
17. V. S. Miller. Short programs for functions on curves. Unpublished manuscript 1986 `http://crypto.stanford.edu/miller/miller.pdf`
18. A. Lenstra and E. Verheul. The XTR public key system. In *Advances in Cryptology – CRYPTO 2000*, Springer-Verlag LNCS 1880, 1–19, 2000.
19. A.J. Menezes and N. Koblitz. Pairing-based cryptography at high security levels. In *Cryptography and Coding*, Springer-Verlag LNCS 3796, 13–36, 2005.
20. J. H. Silverman. *The arithmetic of elliptic curves*. Springer-Verlag, New York, 1992.
21. N.P. Smart and F. Vercauteren. On computable isomorphisms in efficient pairing based systems. Preprint, 2005.