Faster Squaring in the Cyclotomic Subgroup of Sixth Degree Extensions

Robert Granger and Michael Scott[⋆]

Claude Shannon Institute
School of Computing, Dublin City University
Glasnevin, Dublin 9, Ireland
{rgranger,mike}@computing.dcu.ie

Abstract. This paper describes an extremely efficient squaring operation in the so-called 'cyclotomic subgroup' of $\mathbb{F}_{q^6}^{\times}$, for $q \equiv 1 \bmod 6$. Our result arises from considering the Weil restriction of scalars of this group from $\mathbb{F}_{q^6}$ to $\mathbb{F}_{q^2}$, and provides efficiency improvements for both pairing-based and torus-based cryptographic protocols. In particular we argue that such fields are ideally suited for the latter when the field characteristic satisfies $p \equiv 1 \pmod 6$, and since torus-based techniques can be applied to the former, we present a compelling argument for the adoption of a single approach to efficient field arithmetic for pairing-based cryptography.

Keywords: Pairing-based cryptography, torus-based cryptography, finite field arithmetic.

1 Introduction

Pairing-based cryptography has provoked a wealth of research activity since the first cryptographically constructive application of pairings was proposed by Joux in 2000 [21]. Since then, numerous further applications of pairings have been proposed and their place in the modern cryptographers' toolkit is now well established. As a result, much research activity has focused on algorithmic, arithmetic and implementation issues in the computation of pairings themselves, in order to ensure the viability of such systems [3, 12, 2, 18].

In practise, pairings are typically instantiated using an elliptic or a hyperelliptic curve over a finite field, via the Weil or Tate pairing (see [6]) - or a variant of the latter such as the ate [18], or R-ate pairing [25]. These pairings map pairs of points on such curves to elements of a subgroup of the multiplicative group of an extension field, which is contained in the so-called cyclotomic subgroup.

Properties of the cyclotomic subgroup can be exploited to obtain faster arithmetic or more compact representations than are possible for general elements of the extension field. Cryptosystems such as LUC [33] and XTR [26], and the observations of Stam and Lenstra [34] and Granger, Page and Stam [16], all exploit

[⋆] Research supported by the Claude Shannon Institute, Science Foundation Ireland Grant No. 06/MI/006.

membership of this subgroup to achieve fast exponentiation. Many pairing-based protocols require exponentiation in the cyclotomic subgroup, as does the 'hard' part of the final exponentiation of a pairing computation, and so these ideas can naturally be applied in this context [31, 17].

Currently there is a huge range of parametrisation options and algorithmic choices to be made when implementing pairings, and in order to facilitate a simple and unified approach to the construction of extension fields used in pairings, in 2005 Koblitz and Menezes introduced the concept of Pairing-Friendly Fields (PFFs) [24]. These are extension fields $\mathbb{F}_{p^k}$ with $p \equiv 1 \pmod{12}$ and $k = 2^a 3^b$, with $a \geq 1$ and $b \geq 0$. Such specialisation enables algorithms and implementations to be highly optimised. Indeed for ordinary elliptic curves the 2008 IEEE 'Draft Standard for Identity-based Public-key Cryptography using Pairings' (P1636.3/D1) deals exclusively with fields of this form [19].

In 2006 Granger, Page and Smart proposed a method for fast squaring in the cyclotomic subgroup of PFFs [15]. However even for degree six extensions the method was almost 50% slower than the Stam-Lenstra result [34]; the latter however does not permit the use of the highly efficient sextic twists available to the former, and so is not practical in this context. Both of these methods rely on taking the Weil restriction of scalars of the equation that defines membership of the cyclotomic subgroup, in order to obtain a variety over $\mathbb{F}_p$. The defining equations of this variety are then exploited to improve squaring efficiency. Rather than descend to the base field $\mathbb{F}_p$, in this paper we show that descending to only a cubic subfield enables one to square with the same efficiency as Stam-Lenstra for degree six extensions, and for between 60% and 75% the cost of the next best method for the cryptographically interesting extension degrees $12, 18$ and 24.

In tandem with the results of [5] which show that PFFs are not always the most efficient field constructions for pairing-based cryptography, we present a compelling argument for the adoption of a single approach to efficient field arithmetic for pairing-based cryptography, based on the use of fields of the form $\mathbb{F}_{q^6}^{\times}$, for $q \equiv 1 \bmod 6$. While these fields intersect with those listed in [19] - lending strong support to their possible standardisation - since these recommendations can be improved upon and since in the latest draft of this standard the recommended security parameters section is empty [20], we believe that our proposed fields should now be given serious consideration for inclusion.

The sequel is organised as follows. In §2 we describe our field construction and in §3 present our fast squaring formulae. Then in §4 we compare our approach with previous results, and in §5 and §6 apply our result to pairing-based and torus-based cryptography respectively. We conclude in §7.

2 Pairing, Towering and Squaring-Friendly Fields

Pairing-friendly fields were introduced to allow the easy construction of, and efficient arithmetic within extension fields relevant to pairing-based cryptography (PBC), and are very closely related to Optimal Extension Fields [1]. In particular we have the following result from [24]:

Theorem 1. *Let $\mathbb{F}_{p^k}$ be a PFF, and let β be an element of $\mathbb{F}_p$ that is neither a square nor a cube in $\mathbb{F}_p$. Then the polynomial $X^k - \beta$ is irreducible over $\mathbb{F}_p$.*

Observe that for 'small' β, reduction modulo $X^k - \beta$ can be implemented very efficiently. Observe also that the form of the extension degree is important for applications. When $6 \mid k$ the presence of sextic twists for elliptic curves with discriminant $D = 3$ allows for very efficient pairing computation, while for $4 \mid k$ one can use the slightly less efficient quartic twists. Such extensions also permit the use of compression methods based on taking traces [33, 26], or utilising the rationality of algebraic tori [30]. Furthermore $\mathbb{F}_{p^k}$ may be constructed as a sequence of Kummer extensions, by successively adjoining the square or cube root of β, then the square or cube root of that, as appropriate, until the full extension is reached.

As shown in [5], the condition $p \equiv 1 \pmod{12}$ is somewhat spurious in that PFFs do not always yield the most efficient extension towers, and does not allow for families of pairing-friendly curves that have since been discovered [22]. For the Barreto-Naehrig curves for example [4], which have embedding degree twelve, $p \equiv 3 \bmod 4$ is preferred since one can use the highly efficient quadratic subfield $\mathbb{F}_{p^2} = \mathbb{F}_p[x]/(x^2 + 1)$. To allow for the inclusion of such fields, Benger and Scott introduced the following concept [5]:

Definition 1. *A Towering-Friendly Field (TFF) is a field of the form $\mathbb{F}_{q^m}$ for which all prime divisors of m also divide $q - 1$.*

As with PFFs, TFFs allow a given tower of field extensions to be constructed via successive root extractions, but importantly stipulate less exclusive congruency conditions on the base field cardinality. For example, as above for BN-curves with $p \equiv 3 \pmod 4$, the extension $\mathbb{F}_{p^{12}}$ is not a PFF, whereas the degree six extension of $\mathbb{F}_{p^2}$ is towering-friendly, since $p^2 - 1 \equiv 0 \pmod 6$, cf. §5.2. This definition thus captures those considerations relevant to pairing-based cryptography (PBC). We refer the reader to [5] for details of the construction of efficient TFFs.

All of the fields for PBC that follow shall be TFFs of special extension degree $k = 2^a 3^b$, with $a, b \geq 1$, i.e., with $6 \mid k$. Should it not cause confusion, we also refer to any field of the form $\mathbb{F}_{q^6}$ for which $q \equiv 1 \bmod 6$ as a *Squaring-Friendly Field (SFF)*, a name whose aptness will become clear in §3. Thus all SFFs are TFFs and all TFFs used for PBC in this paper are SFFs.

3 New Fast Squaring in the Cyclotomic Subgroup

In this section we derive efficient squaring formulae for elements of the cyclotomic subgroup of TFFs, when the extension degree is of the form $k = 2^a 3^b$, with $a, b \geq 1$, i.e., for SFFs. This is the subgroup of $\mathbb{F}_{p^k}^{\times}$ of order $\Phi_k(p)$, where Φ_k is the k-th cyclotomic polynomial, which for $6 \mid k$ is always of the form:

$$\Phi_{2^a 3^b}(x) = x^{2 \cdot 2^{a-1} 3^{b-1}} - x^{2^{a-1} 3^{b-1}} + 1.$$

We denote the cyclotomic subgroup by $G_{\Phi_k(p)}$, the membership of which can be defined as follows:

$$G_{\Phi_k(p)} = \{\alpha \in \mathbb{F}_{p^k} \mid \alpha^{\Phi_k(p)} = 1\}. \tag{1}$$

The condition on α in (1) defines a variety V over $\mathbb{F}_{p^k}$. For $d \mid k$ let $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^k}$. We write $\mathrm{Res}_{\mathbb{F}_{p^k}/\mathbb{F}_{p^d}} V$ for the Weil restriction of scalars of V from $\mathbb{F}_{p^k}$ to $\mathbb{F}_{p^d}$. Then $\mathrm{Res}_{\mathbb{F}_{p^k}/\mathbb{F}_{p^d}} V$ is a variety defined over $\mathbb{F}_{p^d}$ for which we have a morphism

$$\eta : \mathrm{Res}_{\mathbb{F}_{p^k}/\mathbb{F}_{p^d}} V \to V$$

defined over $\mathbb{F}_{p^k}$ that induces an isomorphism

$$\eta : (\mathrm{Res}_{\mathbb{F}_{p^k}/\mathbb{F}_{p^d}} V)(\mathbb{F}_{p^d}) \to V(\mathbb{F}_{p^k}).$$

We refer the reader to Section 1.3 of [37] for more on the restriction of scalars.

While not stated explicitly, all prior results for fast squaring in $G_{\Phi_k(p)}$ exploit the form of the Weil restriction of this variety to a subfield. Stam and Lenstra restrict $G_{\Phi_6(p)}$ from $\mathbb{F}_{p^6}$ to $\mathbb{F}_p$ and $G_{\Phi_2(p)}$ from $\mathbb{F}_{p^2}$ to $\mathbb{F}_p$ [34], and similarly Granger *et al.* restrict $G_{\Phi_k(p)}$ from $\mathbb{F}_{p^k}$ to $\mathbb{F}_p$ [15].

Observe that $\Phi_{2^a 3^b}(x) = \Phi_6(x^{2^{a-1}3^{b-1}})$ and so we have the following simplification:

$$G_{\Phi_k(p)} = G_{\Phi_6(p^{k/6})}.$$

We therefore need only consider $G_{\Phi_6(q)}$ where $q = p^{k/6}$. Observe also that $\Phi_6(q) \mid \Phi_2(q^3)$ and so

$$G_{\Phi_6(q)} \subset G_{\Phi_2(q^3)}.$$

Hence one can alternatively employ the simplest non-trivial restriction of $G_{\Phi_6(q)}$, or rather of $G_{\Phi_2(q^3)}$, from $\mathbb{F}_{q^6}$ to $\mathbb{F}_{q^3}$, as in [34]. This reduces the cost of squaring in $G_{\Phi_2(q^3)}$, and hence in $G_{\Phi_6(q)}$, from two $\mathbb{F}_{q^3}$-multiplications to two $\mathbb{F}_{q^3}$-squarings, as we shall see in §3.1.

Our simple idea is to use the next non-trivial Weil restriction of $G_{\Phi_6(q)}$, which is from $\mathbb{F}_{q^6}$ to $\mathbb{F}_{q^2}$. This rather fortuitously provides the fastest squaring formulae yet discovered for the cyclotomic subgroups of SFFs, making an even greater efficiency gain than the Stam-Lenstra formulae for $G_{\Phi_2(q^3)}$ (cf. Table 1), while providing a systematic and more general framework than the more ad-hoc method of [34]. Restrictions to other subfields for higher extension degrees of interest do not seem to yield better results, however we leave this as an open problem.

3.1 Fast squaring in $\mathrm{Res}_{\mathbb{F}_{q^2}/\mathbb{F}_q} G_{\Phi_2(q)}$

Let $\mathbb{F}_{q^2} = \mathbb{F}_q[x]/(x^2 - i)$ with i a quadratic non-residue in $\mathbb{F}_q$, and consider the square of a generic element $\alpha = a + bx$:

$$\alpha^2 = (a+xb)^2 = a^2+2abx+b^2x^2 = a^2+ib^2+2abx = (a+ib)(a+b)-ab(1+i)+2abx.$$

This operation can be performed at the cost of two $\mathbb{F}_q$-multiplications, and a few additions.

If however $\alpha \in G_{\Phi_2(q)}$, we have $\alpha^{q+1} = 1$, or $\alpha^q \cdot \alpha = 1$. Observe that:

$$\alpha^q = (a + xb)^q = a + bx^q = a + bx^{2(q-1)/2} \cdot x = a + bi^{(q-1)/2} \cdot x = a - bx,$$

since i is a quadratic non-residue. Hence the variety defined by the cyclotomic subgroup membership equation (1) is $(a + xb)(a - xb) = 1$, or $a^2 - x^2 b^2 = 1$, or $a^2 - ib^2 = 1$. Note that this results in just one equation over $\mathbb{F}_q$, rather than two. Substituting from this equation into the squaring formula, one obtains

$$\alpha^2 = (a + xb)^2 = 2a^2 - 1 + [(a + b)^2 - a^2 - (a^2 - 1)/i]x,$$

where now the main cost of computing this is just two $\mathbb{F}_q$-squarings. Observe that if i is 'small' (for example if $i = -1$ for $p \equiv 3 \pmod 4$ when $\mathbb{F}_q = \mathbb{F}_p$), then the above simplifies considerably.

3.2 Fast squaring in $\mathbf{Res}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}} G_{\Phi_6(q)}$

Let $\mathbb{F}_{q^6} = \mathbb{F}_q[z]/(z^6 - i)$, with $i \in \mathbb{F}_q$ a sextic non-residue. The standard representation for a general element of this extension is

$$\alpha = \alpha_0 + \alpha_1 z + \alpha_2 z^2 + \alpha_3 z^3 + \alpha_4 z^4 + \alpha_5 z^5.$$

However, in order to make the subfield structure explicit, we write elements of $\mathbb{F}_{q^6}$ in two possible ways, each of which will be convenient depending on the context: firstly as a compositum of $\mathbb{F}_{q^2}$ and $\mathbb{F}_{q^3}$, and secondly as cubic extension of a quadratic extension.

$\mathbb{F}_{q^6}$ as a compositum: Let

$$\alpha = (a_0 + a_1 y) + (b_0 + b_1 y)x + (c_0 + c_1 y)x^2 = a + bx + cx^2, \tag{2}$$

where $\mathbb{F}_{q^2} = \mathbb{F}_q[y]/(y^2 - i)$ with $y = z^3$, and $\mathbb{F}_{q^3} = \mathbb{F}_q[x]/(x^3 - i)$ with $x = z^2$. Note that $a, b, c \in \mathbb{F}_{q^2}$. One can therefore regard this extension as the compositum of the stated degree two and degree three extensions of $\mathbb{F}_q$:

$$\mathbb{F}_{q^6} = \mathbb{F}_q(z) = \mathbb{F}_{q^3}(y) = \mathbb{F}_{q^2}(x),$$

with the isomorphisms as given above. Viewing α in the latter form its square is simply:

$$\begin{aligned}\alpha^2 &= (a + bx + cx^2)^2 = a^2 + 2abx + (2ac + b^2)x^2 + 2bcx^3 + c^2x^4 \\ &= (a^2 + 2ibc) + (2ab + ic^2)x + (2ac + b^2)x^2 = A + Bx + Cx^2 \end{aligned} \tag{3}$$

As before we use the characterising equation (1) for membership of $G_{\Phi_6(q)}$, which in this case is $\alpha^{q^2-q+1} = 1$. To Weil restrict to $\mathbb{F}_{q^2}$, we first calculate how the Frobenius automorphism acts on our chosen basis. Firstly, since i is a quadratic non-residue, we have

$$y^q = y^{2(q-1)/2} \cdot y = i^{(q-1)/2} \cdot y = -y.$$

Hence $a^q = (a_0 + a_1 y)^q = a_0 - a_1 y$, which for simplicity we write as $\bar{a}$, and similarly for b^q and c^q. Furthermore, since i is a cubic non-residue we have

$$x^q = x^{3(q-1)/3} \cdot x = i^{(q-1)/3} \cdot x = \omega x,$$

where ω is a primitive cube root of unity in $\mathbb{F}_q$. Applying the Frobenius again gives $x^{q^2} = \omega^2 x$. Note that the above computations necessitate $q \equiv 1 \pmod 6$, which is satisfied thanks to the definition of SFFs.

The cyclotomic subgroup membership equation, rewritten as $\alpha^{q^2} \cdot \alpha = \alpha^q$ is therefore:

$$(a + b\omega^2 x + c\omega^4 x^2)(a + bx + cx^2) = \bar{a} + \bar{b}\omega x + \bar{c}\omega^2 x^2,$$

which upon expanding, reducing modulo $x^3 - i$, and modulo $\Phi_3(\omega) = \omega^2 + \omega + 1$, becomes

$$(a^2 - \bar{a} - bci) + \omega(ic^2 - \bar{b} - ab)x + \omega^2(b^2 - \bar{c} - ac)x^2 = 0. \tag{4}$$

This equation defines the variety $\mathrm{Res}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}} G_{\Phi_6(q)}$, as each $\mathbb{F}_{q^2}$ coefficient of x^i equals zero. Solving for bc, ab, ac, one obtains:

$$\begin{aligned} bc &= (a^2 - \bar{a})/i \\ ab &= ic^2 - \bar{b} \\ ac &= b^2 - \bar{c} \end{aligned}$$

Substituting these into the original squaring formula (3) then gives

$$\begin{aligned} A &= a^2 + 2ibc = a^2 + 2i(a^2 - \bar{a})/i = 3a^2 - 2\bar{a}, \\ B &= ic^2 + 2ab = ic^2 + 2(ic^2 - \bar{b}) = 3ic^2 - 2\bar{b}, \\ C &= b^2 + 2ac = b^2 + 2(b^2 - \bar{c}) = 3b^2 - 2\bar{c}. \end{aligned}$$

$\mathbb{F}_{q^6}$ as a cubic over a quadratic extension: As before let $\mathbb{F}_{q^6} = \mathbb{F}_q[z]/(z^6 - i)$, with $i \in \mathbb{F}_q$ a sextic non-residue. Let the tower of extensions be given explicitly by $\mathbb{F}_{q^2} = \mathbb{F}_q[y]/(y^2 - i)$, and $\mathbb{F}_{q^6} = \mathbb{F}_{q^2}[x]/(x^3 - \sqrt{i})$, with elements represented in the basis:

$$\alpha = (a_0 + a_1 y) + (b_0 + b_1 y)x + (c_0 + c_1 y)x^2 = a + bx + cx^2,$$

which is superficially the same as equation (2), but where now the isomorphism is given by $y = z^3, x = z$. The squaring formula is identical to (3) with $i \leftarrow \sqrt{i}$.

With this representation one can see that the Frobenius automorphism acts on x as multiplication by a sixth root of unity in $\mathbb{F}_q$, which we shall also call ω. Noting that $q \equiv 1 \pmod 6$ observe that:

$$x^q = x^{q-1} \cdot x = x^{3(q-1)/3} \cdot x = \sqrt{i}^{(q-1)/3} \cdot x = i^{(q-1)/6} \cdot x.$$

Since i is a sextic non-residue in $\mathbb{F}_q$, we have that $\omega = i^{(q-1)/6}$ is a primitive sixth root of unity in $\mathbb{F}_q$. Hence $x^q = \omega x$, and similarly $x^{q^2} = (\omega x)^q = \omega^2 x$.

This simplifies the cyclotomic subgroup membership equation (1) to:

$$(a + b\omega^2 x + c\omega^4 x^2)(a + bx + cx^2) = \bar{a} + \bar{b}\omega x + \bar{c}\omega^2 x^2,$$

which upon expanding, reducing modulo $x^3 - \sqrt{i}$, and modulo $\Phi_6(\omega) = \omega^2 - \omega + 1$, becomes

$$(a^2 - \bar{a} - bc\sqrt{i}) - \omega(\sqrt{i}c^2 + \bar{b} - ab)x + \omega^2(b^2 - \bar{c} - ac)x^2 = 0. \qquad (5)$$

Solving for bc, ab, ac, one obtains:

$$\begin{aligned} bc &= (a^2 - \bar{a})/\sqrt{i} \\ ab &= \sqrt{i}c^2 + \bar{b} \\ ac &= b^2 - \bar{c} \end{aligned}$$

Substituting these into the revised squaring formula gives

$$\begin{aligned} A &= a^2 + 2\sqrt{i}bc = a^2 + 2\sqrt{i}(a^2 - \bar{a})/\sqrt{i} = 3a^2 - 2\bar{a} \\ B &= \sqrt{i}c^2 + 2ab = \sqrt{i}c^2 + 2(\sqrt{i}c^2 + \bar{b}) = 3\sqrt{i}c^2 + 2\bar{b} \\ C &= b^2 + 2ac = b^2 + 2(b^2 - \bar{c}) = 3b^2 - 2\bar{c} \end{aligned}$$

3.3 Observations

Both sets of formulae for these degree six extensions are remarkably simple, requiring just three $\mathbb{F}_{q^2}$-squarings to square an element of $G_{\Phi_6(q)}$, which is analogous to the result in §3.1 that requires two $\mathbb{F}_q$-squarings to square an element of $G_{\Phi_2(q)}$. Combining the result from §3.1 for squaring a generic element of $\mathbb{F}_{q^2}$, means that for SFFs squaring in $G_{\Phi_6(q)}$ requires only six $\mathbb{F}_q$-multiplications, which matches the result of Stam and Lenstra.

Strictly speaking, the formulae require knowledge of the action of the Frobenius on elements of $\mathbb{F}_{q^2}$, which although as simple as it is, does entail Weil restriction of equations (4) and (5) to $\mathbb{F}_q$. However, if one ignores the arithmetic of $\mathbb{F}_{q^2}$ and restricts directly to $\mathbb{F}_q$ as in [15], then the above formulae are obscured and indeed were missed by Granger *et al.* So it is in the sense that the formulae were discovered in this way that we mean the restriction is to $\mathbb{F}_{q^2}$ only.

Observe also that for the extension tower, one needs to multiply by $\sqrt{i} \in \mathbb{F}_{q^2}$, whereas for the compositum one has $i \in \mathbb{F}_q$. The cost of the former is however not much more than the latter since the basis for $\mathbb{F}_{q^2}/\mathbb{F}_q$ is $\{1, \sqrt{i}\}$ and so multiplication by $\sqrt{i}$ of a value in $\mathbb{F}_{q^2}$ involves just a component swap and a multiplication by i.

4 Comparison with Prior Work

In this section we compare the efficiency of the squaring formulae derived in §3 with the most efficient results in the literature.

4.1 Operation counts

Let m and s be the time required to perform an $\mathbb{F}_q$-multiplication and an $\mathbb{F}_q$-squaring respectively. Since the cost of computing a squaring using our formulae or others reduces to computing squarings in a subfield, we use the notation S_d and M_d to denote the time required to compute the square of one or the product of two generic elements of $\mathbb{F}_{q^d}$. In our estimates we do not include the time for modular additions and subtractions since although not negligible, are not the dominant operations. This assumes that multiplication by the elements i, j used in §3.1 and §3.2 can be effected with very few modular shifts and additions when needed, see [5] for justification of this assumption.

We focus on TFFs with extension degrees $6, 12, 18$ and 24 over $\mathbb{F}_q$, which are the main extension degrees of interest in PBC. However one can easily extrapolate cost estimates for any field whose extension degree is of the form $k = 2^a3^b$. To estimate the cost of a multiplication in $\mathbb{F}_{q^k}$, we use the function $\nu(k)m$ where $\nu(k) = 3^a6^b$. The 3 and 6 in this estimate arise from the use of Karatsuba-Ofman multiplication [23] for each quadratic and each cubic extension respectively. Our cost function differs from that in [24] and [15], which is 3^a5^b, because these assume that the Toom-Cook multiplication [36] of two degree three polynomials is more efficient than Karatsuba-Ofman multiplication, however this is not usually the case [9]. Hence the cost of an $\mathbb{F}_{q^k}$ multiplication for the given extension degrees is $18m, 54m, 108m, 162m$ respectively.

The cost of squaring a generic element of $\mathbb{F}_{q^k}$ is more complicated, since there are several squaring techniques and one needs to determine which is faster for a given application. Using the observation in [34], one can deduce that $S_k = 2M_{k/2} = 2 \cdot 3^{a-1}6^b$. In addition, the results due to Chung and Hasan [8] give three alternative formulae for squaring using the final degree three polynomial at a cost of $3M_{k/3} + 2S_{k/3}$, $2M_{k/3} + 3S_{k/3}$ and $M_{k/3} + 4S_{k/3}$. For simplicity we use the second of the Chung-Hasan formulae, which incidentally for the above extension degrees requires exactly the same number of $\mathbb{F}_q$-multiplications as when using [34].

Table 1 contains counts of the number of $\mathbb{F}_q$-multiplications and $\mathbb{F}_q$-squarings that are required to perform a squaring in $\mathbb{F}_{q^k}$ and $G_{\Phi_k(q)}$, via the methods arising from Weil restriction to the quadratic, cubic and $\mathbb{F}_q$ subfields respectively.

As is clear from the table, with the present result we have reduced the squaring cost for generic elements in each of these fields by a factor of two for every degree, which greatly improves the speed of an exponentiation. If we assume for the moment also that $m \approx s$, then our squaring takes approximately 2/3-rds the time of the Stam-Lenstra result in the third column. In comparison with the final column, one sees that we beat this comprehensively; indeed for $k = 24$ the result from [15] is worse than when using $\mathrm{Res}_{\mathbb{F}_{q^k}/\mathbb{F}_{q^{k/2}}} G_{\Phi_2(q^{k/2})}$, and is barely

Table 1. Operation counts for squaring in various Weil restrictions of $G_{\Phi_k(q)}$ for $6 \mid k$.

k	$\mathbb{F}_{q^k}$	$\mathrm{Res}_{\mathbb{F}_{q^k}/\mathbb{F}_{q^{k/2}}} G_{\Phi_2(q^{k/2})}$	$\mathrm{Res}_{\mathbb{F}_{q^k}/\mathbb{F}_{q^{k/3}}} G_{\Phi_6(q^{k/6})}$	$\mathrm{Res}_{\mathbb{F}_{q^k}/\mathbb{F}_q} G_{\Phi_6(q^{k/6})}$
		(Stam-Lenstra [34])	(Present result)	(Granger *et al.* [15])
6	$12m$	$2S_3 = 4m + 6s$	$3S_2 = 6m$	$3m + 6s$
12	$36m$	$2S_6 = 24m$	$3S_4 = 18m$	$18m + 12s$
18	$72m$	$2S_9 = 24m + 30s$	$3S_6 = 36m$	
24	$108m$	$2S_{12} = 72m$	$3S_8 = 54m$	$84m + 24s$

better than Karatsuba-Ofman. Hence restricting to the cubic subfield is clearly the most efficient for fields of this form.

Remark 1. Note that we have not included the Stam-Lenstra squaring cost for $k = 6$ because this requires $q \equiv 2$ or $5 \pmod 9$ whereas the use of the sextic twist requires $D = 3$ and hence $p \equiv q \equiv 1 \pmod 3$, thus making them less desirable for pairings. An open problem posed in [15] asked for a generalisation of the Stam-Lenstra result to cyclotomic fields of degree different from six, for pairings. We have shown that our formula for squaring in the cyclotomic subgroup of $\mathbb{F}_{q^6}^{\times}$ when $q \equiv 1 \pmod 6$ matches the extremely efficient degree six squaring of [34] (while also permitting the use of sextic twists), and extends efficiently to higher degree extensions. Hence in the sense that we have provided an efficient tailor-made solution for pairings, we believe we have answered this question affirmatively.

4.2 Applicability of method to higher powerings

As we have shown, all of the techniques to date for producing faster arithmetic in the cyclotomic subgroup result from an application of the Weil restriction of scalars of the equation defining membership of this group. A natural question to ask is whether this will work for extensions of any other degree? The answer is that it does, but that it appears very unlikely to provide a faster alternative to squaring.

Let $\delta(k)$ be the degree of the equation $\alpha^{\Phi_k(q)} = 1$, once expanded and the linear Frobenius operation has been incorporated. If $\delta = 2$, then the variety resulting from the Weil restriction down to any intermediate subfield may help with squaring. If $\delta > 2$ then the resulting equations may help when raising an element of the cyclotomic subgroup to the δ-th power [34]. However this is unlikely to be faster than sequential squaring for an exponentiation, even when squaring is slow. For example, for $G_{\Phi_3(q)}$, one finds that $\delta = 3$ and the resulting equations aid cubing. However the ratio of the cost of a cubing to a squaring is $> \log_2 3$, and thus it better to square than cube during an exponentiation in this case.

Complementary to this is the fact that $\delta \leq 2$ only for extensions of degree $k = 2^a 3^b$ for $a \geq 1, b \geq 0$. Hence pairings with embedding degrees of this form are ideally suited to exploit our, and the Stam-Lenstra fast squaring technique.

5 Application to Pairing-Based Cryptography

In this section we apply our squaring formula to extension field arithmetic required in the final exponentiation of a pairing computation, and post-pairing exponentations, for two concrete examples. We here assume that $\mathbb{F}_q = \mathbb{F}_p$.

The use of our formulae is possible because for any pairing, the codomain is a subgroup of $G_{\Phi_k(p)} \subset \mathbb{F}_{p^k}^\times$ where k is the embedding degree of the curve. For instance, the Tate pairing on an elliptic curve has the following form: for r coprime to p we have

$$e_r : E(\mathbb{F}_p)[r] \times E(\mathbb{F}_{p^k})/rE(\mathbb{F}_{p^k}) \to \mathbb{F}_{p^k}^\times/(\mathbb{F}_{p^k}^\times)^r.$$

In order to obtain a unique coset representative the output is usually powered by $(p^k - 1)/r$. Since

$$(p^k - 1)/r = (p^k - 1)/\Phi_k(p) \cdot \Phi_k(p)/r,$$

the first term $(p^k - 1)/\Phi_k(p)$ can be computed easily using the Frobenius and a few multiplications and a division, while the remaining 'hard' part must be computed as a proper exponentiation. Since for any element $\alpha \in \mathbb{F}_{p^k}^\times$, we have $\alpha^{(p^k-1)/\Phi_k(p)} \in G_{\Phi_k(p)}$, fast arithmetic for this group can be used.

5.1 MNT curves

MNT curves were discovered in 2001 by Miyaji *et al.* and consist of three families of ordinary elliptic curves with embedding degrees $3, 4$ and 6 [28]. For efficiency reasons, of most interest are the latter, for which the parametrisation of the base field, group cardinality and trace of Frobenius are given by:

$$\begin{aligned} p(x) &= x^2 + 1 \\ r(x) &= x^2 - x + 1 \\ t(x) &= x + 1 \end{aligned}$$

Using the method of Scott *et al.* [32] the final exponentiation reduces to the powering of an element of G_{p^2-p+1} by x. The maximum twist available has degree two and so for efficiency one would like to use $\mathbb{F}_{p^3}$ arithmetic with a quadratic extension of this field to give $\mathbb{F}_{p^6}$. This implies that one should use the composite construction of §3.2. One can alternatively use a quadratic extension of a cubic extension for the Miller loop computation, and then switch to the isomorphic tower construction of §3.2 for the final exponentiation. This isomorphism is just a permutation of basis elements, and so switching between representations, even during the Miller loop, is viable, and therefore permits the use of the fast multiplication results of [9].

The one condition that must be satisfied in order for our method to apply is that $p \equiv 1 \pmod 6$ which requires $x \equiv 0 \pmod 6$, which eliminates 2/3-rds of potential MNT curves. While this is restrictive, the benefits of ensuring this condition are clear.

5.2 BN curves

The Barreto-Naehrig family of pairing-friendly curves were reported in 2005 and have embedding degree 12 [4]. The parametrisation of the base field, group cardinality and trace of Frobenius are given by:

$$\begin{aligned} p(x) &= 36x^4 + 36x^3 + 24x^2 + 6x + 1 \\ r(x) &= 36x^4 + 36x^3 + 18x^2 + 6x + 1 \\ t(x) &= 6x^2 + 1 \end{aligned}$$

Note that for odd x, $\mathbb{F}_{p^{12}}$ is not pairing-friendly. However, choosing $p \equiv 3 \pmod 4$ enables the use of the initial extension $\mathbb{F}_{p^2} = \mathbb{F}_p[x]/(x^2+1)$ which permits highly efficient arithmetic. Since BN curves possess a sextic twist, such efficient subfield arithmetic is very desirable. With this choice of extension, $\mathbb{F}_{q^6}$ is towering-friendly with $\mathbb{F}_q = \mathbb{F}_{p^2}$ since $p^2 \equiv 1 \pmod 6$ for all primes $p > 3$, and is also squaring-friendly.

Again the efficient final exponentiation of Scott *et al.* [32] can be applied to reduce the final powering to essentially just three exponentiations by x. In practise, it is recommended that x should be chosen to have as low a Hamming weight as possible, to minimise the resulting cost of the Miller loop [10]. Hence for the final exponentiation, the entries in Table 1 imply that this cost will be $\approx 75\%$ the cost of the previous fastest. Indeed using our squaring method with the degree six extension of $\mathbb{F}_{p^2}$ given by the tower in §3.2 - i.e., a tower having extensions of $\mathbb{F}_p$ of degrees $1-2-4-12$ - a simple estimate of the cost of performing the final powering with Scott *et al.*'s method for a 256-bit prime, i.e., at AES 128-bit security, is 4856 $\mathbb{F}_p$-multiplications. In contrast using the tower extension with degrees $1-2-6-12$ and using the Stam-Lenstra result of §3.1 for the final extension, this figure is 5971 $\mathbb{F}_p$-multiplications, so our method should be approximately 20% faster in practise. Furthermore by excluding $p \equiv 3 \pmod 4$, the arithmetic for PFFs would be even slower for both towers.

With regard to post-pairing exponentiation, one is free to use the method of [13] which uses a clever application of the GLV decomposition [14]. For BN curves one obtains a four-dimensional decomposition and hence uses quadruple exponentiation to achieve this speed-up. Since there will be more multiplications than for the final powering the impact of our squaring formulae on the cost of exponentiation will be less pronounced, but still significant.

Another factor to consider for post-pairing exponentiations is that the trace-based methods of LUC [33], XTR [26, 35] and XTR over extension fields [27], are known to be faster than [34] and [16] for a single exponentiation. However we expect the Galbrith-Scott method to be superior since the resulting exponents in the quadruple exponentiation are one quarter the size, and for the trace-based methods efficient algorithms appear to be known only for single and double exponentiation [13], ruling out their application in this context. The same reasoning applies to schemes that require a product of pairings each with individual post-pairing exponentiation, such as [7].

The trace methods are also ruled out of Scott *et al.*'s final-powering method since many multiplications are required, whereas the trace methods only permit exponentiation. Hence, barring any improvements in trace-based multi-exponentiation algorithms, we expect our formulae to feature in the most efficient way to implement pairings, their products and exponentiation.

6 Application to Torus-Based Cryptography

Our central result may also be applied to torus-based cryptography (TBC), which is based on the mathematics of algebraic tori, which were introduced to cryptography by Rubin and Silverberg in 2003 [30]. While for degree six extensions of prime fields, our squaring formulae only match the fastest implementation of CEILIDH [16] - which uses [34] - for nearly all sixth degree extensions of non-prime fields our squaring method is the most efficient known.

The implementation of $T_{30}(\mathbb{F}_p) = G_{\Phi_{30}(p)}$ by van Dijk *et al.* used the Stam-Lenstra result for $p \equiv 2$ or $5 \pmod 9$ [11]. This condition implies that $q = p^k \equiv 2$ or $5 \pmod 9$ whenever $k = 5^m$. Hence the family of fields of extension degree $6 \cdot 5^m$ over $\mathbb{F}_q$ for $q \equiv 2$ or $5 \pmod 9$ matches our squaring efficiency for the cyclotomic subgroup. On the other hand, the condition $q \equiv 1 \pmod 6$ for SFFs is far less restrictive and in fact can be said to apply to $3/4$'s of all finite fields.

With regard to compression of torus elements, which is the central function of torus-based cryptography, let $p \equiv 1 \pmod 6$ and let the field construction for $\mathbb{F}_{q^6}$ be the compositum given in §3.2. We reorder the basis as so:

$$\alpha = (a_0 + a_1 x + a_2 x^2) + (b_0 + b_1 x + b_2 x^2)y = a + by.$$

Assuming $\alpha \in G_{q^2-q+1}$, then as in [17] and explicitly in [29], a straightforward analysis of condition (1) yields that such elements - excepting the identity - can be represented by two elements of $\mathbb{F}_q$. To compress, one writes $\alpha \neq 1$ as

$$\alpha = a + by = \frac{c - y}{c + y},$$

where $c = -(a+1)/b$ for $b \neq 0$ and $c = 0$ if $b = 0$. Condition (1) now becomes

$$\left(\frac{c-y}{c+y}\right)^{q^2-q+1} = 1,$$

and leads to the equation $3c_0^2 + i - 3ic_1c_2 = 0$, where $c = c_0 + c_1 x + c_2 x^2$. Therefore there is redundancy between the c_i's. One can eliminate c_2 for instance which can be recovered from c_0 and c_1. The decompression map is just the inverse of this:

$$\psi : \mathbb{A}^2(\mathbb{F}_q) \to T_6(\mathbb{F}_q) \setminus \{1\} : (c_0, c_1) \mapsto \frac{3ic_0c_1 + 3ic_1^2 x + (3c_0^2 + i)x^2 - 3ic_1 y}{3ic_0c_1 + 3ic_1^2 x + (3c_0^2 + i)x^2 + 3ic_1 y},$$

with the condition $c_1 \neq 0$, which therefore represents all $q^2 - q$ non-identity elements in G_{q^2-q+1}.

Since this compression method works for all fields for which $p \equiv 1 \pmod 6$, achieves the maximum known compression for any algebraic torus, and has the fastest squaring available, we propose that such fields should be considered ideal candidates TBC.

Furthermore, as stated in [13], TBC parameters can be easily generated from pairing-friendly elliptic curves. The multi-exponentiation techniques stated in §5.2 that one acquires from PBC when TBC parameters are generated in this way mean that exponentiation in $T_6(\mathbb{F}_q)$ should be extremely efficient, and indeed faster than all other known methods.

Therefore while it could be argued that the main application of TBC is to PBC - in terms of offering faster arithmetic and compression mechanisms for systems that may be used in practise - here TBC really benefits from PBC, thus demonstrating a neat symbiosis between the two application areas.

7 Conclusion

We have presented a method to perform squaring extremely efficiently in the cyclotomic subgroup of $\mathbb{F}_{q^6}^{\times}$, for $q \equiv 1 \pmod 6$. We have shown how to apply this result to fields of interest in pairing-based cryptography to obtain the fastest final- and post-pairing exponentiation algorithms, and also detailed why these fields are ideally suited for torus-based cryptography, when $p \equiv 1 \pmod 6$.

Since these fields include those listed in the IEEE's P1363.3/D1 draft standard for identity-based public-key cryptography, which use pairings over ordinary elliptic curves that permit the fastest pairing via a maximal twist, our result strongly supports their standardisation, but also demonstrates that the more general squaring-friendly fields introduced here warrant serious consideration for inclusion.

We leave it as an open problem to find similarly efficient squaring formulae for the remaining case $q \equiv -1 \bmod 6$.

Acknowledgements

The authors would like to thank Martijn Stam for answering some questions.

References

1. D.V. Bailey and C. Paar. *Optimal Extension Fields for Fast Arithmetic in Public-Key Algorithms.* In Advances in Cryptology (CRYPTO 1998), Springer LNCS 1462, 472–485, 1998.
2. P. Barreto, S.D. Galbraith, C. Ó hÉigeartaigh, and M. Scott. *Efficient Pairing Computation on Supersingular Abelian Varieties.* In Designs, Codes and Cryptography, Volume 42, Number 3: 239–271, 2007.
3. P. Barreto, H. Kim, B. Lynn and M. Scott. *Efficient Algorithms for Pairing-Based Cryptosystems.* In Advances in Cryptology (CRYPTO 2002), Springer LNCS 2442, 354–368, 2002.

4. P. Barreto and M. Naehrig. *Pairing-Friendly Elliptic Curves of Prime Order.* In Selected Areas in Cryptography, Springer LNCS 3897, 319–331, 2005.
5. N. Benger and M. Scott. *Constructing Tower Extensions for the implementation of Pairing-Based Cryptography.* Preprint.
6. I.F. Blake, G. Seroussi and N.P. Smart. *Advances in Elliptic Curves in Cryptography.* Cambridge University Press, 2005.
7. D. Boneh, X. Boyen and H. Shacham. *Short Group Signatures.* In Advances in Cryptology (CRYPTO 2004), Springer LNCS 3152, 41–55, 2004.
8. J. Chung and M.A. Hasan. *Asymmetric Squaring Formulae.* In IEEE Symposium on Computer Arithmetic, 113–122, 2007.
9. A.J. Devegili, C. Ó hÉigeartaigh, M. Scott and R. Dahab. *Multiplication and Squaring on Pairing-Friendly Fields.* Available at `http://eprint.iacr.org/2006/471`
10. A.J. Devegili, M. Scott and R. Dahab. *Implementing Cryptographic Pairings over Barreto-Naehrig Curves.* In Pairing, Springer LNCS 4575, 197–207, 2007.
11. M. van Dijk, R. Granger, D. Page, K. Rubin, A. Silverberg, M. Stam and D. Woodruff. *Practical cryptography in high dimensional tori.* In Advances in Cryptology (EUROCRYPT 2005), Springer LNCS 3494, 234–250, 2005.
12. S.D. Galbraith, K. Harrison and D. Soldera. *Implementing the Tate pairing.* In Algorithmic Number Theory Symposium (ANTS-IV) Springer LNCS 2369, 324–337, 2002.
13. S.D. Galbraith and M. Scott. *Exponentiation in Pairing-Friendly Groups Using Homomorphisms.* In Pairing, Springer LNCS 5209, 211–224, 2008.
14. R. Gallant, J. Lambert and S. Vanstone. *Faster Point Multiplication on Elliptic Curves with Efficient Endomorphisms.* In Advances in Cryptology (CRYPTO 2001), Springer LNCS 2139, 190–200, 2001.
15. R. Granger, D. Page and N.P. Smart. *High Security Pairing-Based Cryptography Revisited.* In Algorithmic Number Theory Symposium (ANTS-VII), Springer LNCS 4076, 480–494, 2006.
16. R. Granger, D. Page and M. Stam. *A Comparison of CEILIDH and XTR.* In Algorithmic Number Theory Symposium (ANTS-VI) Springer LNCS 3076, 235–249, 2004.
17. R. Granger, D. Page and M. Stam. *On Small Characteristic Algebraic Tori in Pairing-based Cryptography.* In LMS Journal of Computation and Mathematics, Volume 9: 64–85, 2006.
18. F. Hess, F. Vercauteren and N.P. Smart. *The Eta Pairing Revisited.* In IEEE Transactions on Information Theory, Volume 52, Issue 10: 4595–4602, 2006.
19. *IEEE Draft Standard for Identity-based Public-key Cryptography using Pairings (P1636.3/D1)*, 2008. Available from `http://grouper.ieee.org/groups/1363/IBC/material/P1363.3-D1-200805.pdf`
20. *IEEE Draft Standard for identity-based cryptographic techniques using pairings (P1363.3/D3),* 2009. Available from `http://grouper.ieee.org/groups/1363/IBC/index.html`
21. A. Joux. *A One Round Protocol for Tripartite Diffie-Hellman.* In Algorithmic Number Theory Symposium (ANTS-IV), Springer LNCS 1838, 385–394, 2000.
22. E.J. Kachisa, E.F. Schaefer and M. Scott. *Constructing Brezing-Weng Pairing-Friendly Elliptic Curves Using Elements in the Cyclotomic Field.* In Pairing, Springer LNCS 5209, 126–135, 2008.
23. A. Karatsuba and Y. Ofman. *Multiplication of Many-Digital Numbers by Automatic Computers.* In Soviet Physics Doklady **7**, 595–596, 1963.

24. N. Koblitz and A. J. Menezes. *Pairing-Based Cryptography at High Security Levels.* In Cryptography and Coding, Springer LNCS 3796, 13–36, 2005.
25. E. Lee, H.S. Lee and C.M. Park. *Efficient and Generalized Pairing Computation on Abelian Varieties.* In IEEE Transactions on Information Theory, Volume 55, Number 4: 1793–1803, 2009.
26. A. K. Lenstra and E. Verheul. *The XTR Public Key System.* In Advances in Cryptology (CRYPTO 2000), Springer LNCS 1880, 1–19, 2000.
27. S. Lim, S. Kim, I. Yie, J. Kim and H. Lee. *XTR extended to GF(p^{6m}).* In Selected Areas in Cryptography (SAC 2001), Springer LNCS 2259, 301–312, 2001.
28. A. Miyaji, M. Nakabayashi and S. Takano. *New explicit conditions of elliptic curve traces for FR-reduction.* IEICE Trans. Fundamentals **E84-A (5)**, 1234–1243, 2001.
29. M. Naehrig, P.S.L.M. Barreto and P. Schwabe. *On Compressible Pairings and their Computation.* In Africacrypt 2008, Springer LNCS, 371–388, 2008.
30. K. Rubin and A. Silverberg. *Torus-Based Cryptography.* In Advances in Cryptology (CRYPTO 2003), Springer LNCS 2729, 349–365, 2003.
31. M. Scott and P. Barreto. *Compressed Pairings.* In Advances in Cryptology (CRYPTO 2004), Springer LNCS 3152, 140–156, 2004.
32. M. Scott, N. Benger, M. Charlemagne, L.J.D. Perez and E.J. Kachisa. *On the Final Exponentiation for Calculating Pairings on Ordinary Elliptic Curves.* In Pairing, Springer LNCS 5671, 78–88, 2009.
33. P. Smith and C. Skinner. *A public-key cryptosystem and a digital signature system based on the Lucas function analogue to discrete logarithms.* In Advances in Cryptology (ASIACRYPT 1995), Springer LNCS 917, 357–364, 1995.
34. M. Stam and A. K. Lenstra. *Efficient Subgroup Exponentiation in Quadratic and Sixth Degree Extensions.* In Cryptographic Hardware and Embedded Systems (CHES 2002), Springer LNCS 2523, 318–332, 2002.
35. M. Stam and A. K. Lenstra. *Speeding Up XTR.* In Advances in Cryptology (ASIACRYPT 2001), Springer LNCS 2248, 125–143, 2001.
36. A.L. Toom. *The Complexity of a Scheme of Functional Elements realizing the Multiplication of Integers.* Soviet Mathematics, 4(3): 714–716, 1963.
37. A. Weil. *Adeles and algebraic groups.* Progress in Mathematics **23**, Birkhäuser, Boston, 1982.