Constructing Tower Extensions for the implementation of Pairing-Based Cryptography

Naomi Benger and Michael Scott*

School of Computing
Dublin City University
Ballymun, Dublin 9, Ireland.
nbenger, mike@computing.dcu.ie

Abstract. A cryptographic pairing evaluates as an element in an extension field, and the evaluation itself involves a considerable amount of extension field arithmetic. It is recognised that organising the extension field as a "tower" of subfield extensions has many advantages. Here we consider criteria that apply when choosing the best towering construction, and the associated choice of irreducible polynomials for the implementation of pairing-based cryptosystems. We introduce a method for automatically constructing efficient towers for more congruency classes than previous methods, some of which allow faster arithmetic.
Keywords: Pairing implementation, pairing-based cryptosystems.

1 Introduction

When considering the software implementation of a cryptographic scheme such as RSA, or schemes based on the discrete logarithm problem, an implementation can be written which performs reasonably efficiently for any level of security. For example, an RSA implementation with a 1024-bit modulus can easily be modified to use a 4096-bit modulus, maybe by just changing a single parameter within the program. The same applies to elliptic curve cryptography where a generic implementation will perform reasonably well for a curve with a subgroup of points of size 160-bits, 192-bits or 256-bits. Of course an implementation specially tailored for, and hard-wired to, a particular level of security will perform somewhat better, but not spectacularly so.

The situation for pairing-based cryptography (PBC) is fundamentally different. An efficient implementation at the 80-bit level of security using the Tate pairing on a Cocks-Pinch pairing-friendly curve [9] will be completely different from an implementation at the 128-bit level using the

* Research supported by the Claude Shannon Institute, Science Foundation Ireland Grant 06/MI/006

R-ate [16] pairing on a BN curve [6] and very little code will be reusable between the two implementations. In this situation the development and maintenance of good quality pairing code becomes difficult and there is a compelling case for the development of some kind of automatic tool – a *cryptographic compiler* – which can generate good quality code for each case [8].

When using pairing-based protocols, it is necessary to perform arithmetic in fields of the form $\mathbb{F}_{q^k}$, for moderate values of k, so it is important that the field is represented in such a way that the arithmetic can be performed as efficiently as possible. It is this aspect of the implementation of pairing-based protocols which is the focus of this paper.

The remainder of the paper is organised as follows: in §2 the motivation for the work in this paper will be reinforced. In §3 the specific context of focus will be presented. Some existing ideas for the field construction are briefly explained in §4. A general result is proved in §5 which is then applied to the context of pairing-based cryptography in in §6, including the main contribution of this paper to PBC in §6.1. In §7 we draw some conclusions.

2 Extension Fields

Consider the implementation of the extension field $\mathbb{F}_{q^k}$. The obvious representation of elements of this field is as polynomials of degree $k-1$, $\mathbb{F}_{p^k} = \mathbb{F}_p[x]/f(x)\mathbb{F}_p[x]$ where $f(x)$ is an irreducible polynomial in $\mathbb{F}_p[x]$ of degree k. For efficiency reasons some effort might be made to choose $f(x)$ to have a minimal number of terms and small coefficients. For example, for the field $\mathbb{F}_{p^2}$, where p is a prime and $p \equiv 3 \mod 4$, a good choice for $f(x)$ would be x^2+1, and elements can be represented as $ax+b$, with $a, b \in \mathbb{F}_p$. For the case $p \equiv 5 \mod 8$, a good choice for $f(x)$ would be x^2-2. For the final case $p \equiv 1 \mod 8$ there is no immediately obvious way to choose a suitable irreducible binomial, but for some small value i which is a quadratic non-residue in $\mathbb{F}_p$, x^2-i would be appropriate.

In some settings the value of the extension degree k might be much greater than 2, in which case the direct polynomial representation becomes more arithmetically complex. For elliptic curve cryptography implemented over "Optimal Extension Fields", (OEFs) as suggested by Bailey and Paar [3], extensions as high as $\mathbb{F}_{p^{30}}$ are considered; in pairing-based cryptosystems, an extension degree of up to 50 is reasonable [9]. OEFs are usually defined as extensions with respect to a small single-word pseudo-mersenne prime. The extension fields that arise in the context of efficient

implementations of pairing-based cryptography, however, are rather different.

If the extension degree is a parameter of the implementation then the potentially uncomfortable situation arises where, if the extension degree changes, an optimal implementation must be re-written again, largely "from scratch". The alternative seems to be to use generic polynomial code to construct the extension field, making the implementation slow and bulky. A nice compromise that applies when the extension k is smooth (that is has only small factors) is to use a "tower" of extensions, where one layer builds on top on the last, and ideally where each sub-extension is quite small. For example, $\mathbb{F}_{p^{12}}$ could be implemented as a quadratic extension, of a cubic extension, of a very efficiently implemented (and reusable) quadratic extension field $\mathbb{F}_{p^2}$, as implemented by Devegili et al. [7].

This idea of using a tower of extensions was suggested by Baktir and Sunar [19] as a better way of implementing OEFs, and in the process of doing this they discovered that the resulting simpler implementation resulted in an asymptotically improved method for performing field inversion. The point is that it is relatively easy to implement quadratic and cubic extensions efficiently, whereas the complexity of implementing generic methods over large extensions might result in the inadvertent use of sub-optimal methods.

It is also proposed in the IEEE draft standard "P1363.3: Standard for Identity-Based Cryptographic Techniques using Pairings" that extensions of odd primes are constructed using a tower of extensions created using irreducible binomials at each stage [1].

Clearly it is advantageous to use this towering method when implementing a pairing-based protocol. One issue remains: finding the best tower for a particular value of k. Obviously, for different values of k, we will need to use different towers; a very reasonable approach in the context of pairing-based cryptography would be to fix the tower for a particular k which will be made clear in §6.

The construction does not only depend on k however, but also on p, the characteristic of the base field. There is an existing method for constructing such towers given by Koblitz and Menezes in [15] which can only be used for some p with specific properties, so relying on this method alone places unnecessary restrictions on the parameters of a pairing-based curve. Given that pairing-friendly elliptic curves are quite rare, it is clear that we should aim to reduce the number of constraints on the parameters that may compromise the efficiency of the implementation.

The main contribution of this work is to give a new method, which complements the existing method and gives a means for automatically constructing efficient towers in the cases for which the existing method can not be used. In some cases, the towers given using this new method give more efficient arithmetic than would be possible using the towers over fields for which the Koblitz and Menezes method can be used.

Motivating this work is our ambition to contribute to a "cryptographic compiler" [8], that is, a compiler which when given as input the parameters for a pairing-friendly curve, should be automatically able to generate the optimal pairing code, including the optimal field arithmetic implementation.

3 Pairings and pairing-friendly elliptic curves

The Tate pairing of two linearly independent points P and Q on an elliptic curve $E(\mathbb{F}_{q^k})$, denoted $e(P,Q)$, is an element of the extension field $\mathbb{F}_{q^k}$. If P is of prime order r, then the pairing evaluates as an element of order r. Here we focus on the case of non-supersingular elliptic curves over prime fields, that is, $q = p$. In practice it is common to choose P as a point on the elliptic curve over the base field, $E(\mathbb{F}_p)$. As is well known, the number of points on this elliptic curve is $p+1-t$, where $\mid t \mid \leq 2\sqrt{p}$ (Hasse bound) is the trace of the Frobenius [12].

The Tate pairing is only of interest if it is calculated on a "pairing-friendly" elliptic curve. This pairing-friendliness entails that $r \mid p^k - 1$ for some reasonably small value of k, that is, the rth roots of unity in $\bar{\mathbb{F}}_p$, the codomain of the pairing, are contained in $\mathbb{F}_{p^k}$. To find the actual parameters of the curve, however, it is also required that the integer $4p-t^2$ (always positive as a consequence of the Hasse condition), has a relatively small non-square part D (the CM discriminant), that is it factors as Dv^2 for small D. Such curves can then be found using the method of complex multiplication (CM) [12].

For the Tate pairing the point Q is commonly represented as a point over some twist $E'(\mathbb{F}_{p^{k/t}})$, where $t \mid k$, as apposed to being on the curve defined over the full extension field, $E(\mathbb{F}_{p^k})$. When k is even the quadratic twist $t = 2$ can always be used, when the pairing-friendly curve has a CM discriminant of $D = 1$ and $4 \mid k$, the quartic twist $t = 4$ can be used, and when the CM discriminant is $D = 3$ and $6 \mid k$, the sextic twist $t = 6$ can be used. It is preferable to use the highest order twist available, as this leads to a faster more compact implementation [13].

Variants of the Tate pairing have recently been discovered (the ate pairing [13], and the R-ate pairing [16]) that are more efficient in some cases, but which require the roles of P and Q to be reversed. This makes it even more important to use the highest order twist available as a significant part of the pairing calculation is a point multiplication of the first parameter (now Q), which is more expensive than in the Tate pairing.

In their taxonomy of pairing-friendly curves [9], Freeman Scott and Teske, following a recommendation from Koblitz and Menezes [15, §8.3], particularly recommend curves for which the embedding degree k is of the form $k = 2^i \cdot 3^j$. Here we further restrict that $i \geq 1$, $j \geq 0$ as an even value for k facilitates the important "denominator elimination" optimization for the pairing calculation [4]. In each case we prefer curves which support the maximal twist.

4 Existing ideas for constructing towers

Let p be an odd prime, and let $n > 0$ and $m > 1$ be integers. The most obvious way to construct the tower of sub-extensions of the field $\mathbb{F}_{p^{nm}}$ over $\mathbb{F}_{p^n}$ would be to use a binomial $x^m - \alpha$ which is irreducible over $\mathbb{F}_{p^n}[x]$ and successively adjoin roots of the previously adjoined root until the tower has been constructed (call this the 'general method'). We are able to test $x^m - \alpha$ for irreducibility using the following theorem:

Theorem 1. *[18, Theorem 3.75] Let $m \geq 2$ be an integer and $\alpha \in \mathbb{F}_{p^n}^{\times}$. Then the binomial $x^m - \alpha$ is irreducible in $\mathbb{F}_{p^n}[x]$ if and only if the following two conditions are satisfied:*

1. *each prime factor of m divides the order e of $\alpha \in \mathbb{F}_{p^n}^{\times}$, but not $(p^n - 1)/e$;*
2. *If $m \equiv 0 \mod 4$ then $p^n \equiv 1 \mod 4$.*

By theorem 1 we see that the general method above works for all m, $m \not\equiv 0 \mod 4$. When $m \equiv 0 \mod 4$, this method works if $p^n \equiv 1 \mod 4$.

Given the constraints outlined in §3, it is clear that the tower of extensions used in pairing-based cryptography can be built using a sequence of quadratic and cubic sub-extensions. This was recognised by Koblitz and Menezes in [15]. They called a field $\mathbb{F}_{p^k}$ *pairing-friendly* (not to be confused with a pairing-friendly elliptic curve) if $p \equiv 1 \bmod 12$ and k is of the form $k = 2^i 3^j$, in which case by [15, Theorem 2] (which is derived from Theorem 1 above) the polynomial $x^k - \alpha$ is irreducible over $\mathbb{F}_p$ if α is neither a square nor a cube in $\mathbb{F}_p$. The extension tower can be constructed

using the general method by simply adjoining a cube or square root of some small such α and then successively adjoining a cube or square root of the previously adjoined root until the tower has been constructed. If $b = 0$ then it is sufficient that $p = 1 \bmod 4$, and that α be a quadratic non-residue in $\mathbb{F}_p$. This result gives us an easy method for building towers over pairing-friendly fields: simply find an element α in $\mathbb{F}_p$ which is a quadratic and (when necessary) cubic non-residue and adjoin successive cube and square roots of α to $\mathbb{F}_p$.

There is one major issue remaining, the strict condition that $p \equiv 1 \mod 12$ to give a pairing-friendly field. When searching for pairing-friendly curves of a suitable size there are typically other criteria that we wish to meet (for example, it is preferred that the Hamming weight of the variable that controls the Miller loop in the pairing calculation should be as small as possible [7]). Having to skip a nice curve just because $p \not\equiv 1 \mod 12$ seems unnecessarily restrictive. Since the publication of [15], new families of pairing-friendly elliptic curves have been discovered which the results of [15] could not have taken into account. In particular, the KSS curves with embedding degree 18 [14] are good for implementation given the many optimisations possible using these curves. The condition that $p \equiv 1 \mod 12$ here is completely unnecessary as this condition comes from condition 2 of Theorem 1 which is not applicable when $k = 18$.

Given the many applications of pairings in cryptography and the fact that the parameters of a pairing-based protocol are already subject to quite strict constraints, it is clear that there is a necessity for a method to construct towers for fields which would not be considered pairing-friendly (in the sense of Koblitz and Menezes) but would otherwise be favourable for implementation of a pairing-based protocol. The term 'pairing-friendly field' is slightly misleading, as there are families of pairing-friendly elliptic curves attractive for implementation which are defined over fields which do not necessarily satisfy $p \equiv 1 \bmod 12$. In a sense, the pairing-friendly fields of [15] are the fields, in the context of pairings, over which it is easy to build the towers. We introduce a new definition:

Definition 2. A *towering-friendly* field is a field of the form $\mathbb{F}_{q^m}$, where q is a prime power, for which all prime divisors of m also divide $q - 1$.

Essentially, towering-friendly fields are fields for which the tower of sub-extensions can be easily (and most efficiently) constructed; that is, using irreducible binomials. The OEFs of Bailey and Paar [3] are by definition towering-friendly fields (where q a prime of a special form). The fields said to be pairing-friendly by Koblitz and Menezes are also

towering-friendly, but these are not the only towering-friendly fields which occur in the context of pairing based cryptography.

The contribution of this paper is to give a simple, general method for testing the irreducibility of a binomial $x^m - \alpha$ in $\mathbb{F}_{p^n}[x]$ to construct the tower of sub-extensions of the field $\mathbb{F}_{p^{nm}}$ over $\mathbb{F}_{p^n}$. This results in a method for constructing general towers for towering-friendly fields when $m \equiv 0 \mod 4$ and $p^n \not\equiv 1 \mod 4$. In the context of pairing-based cryptography this gives a method for constructing towers for towering-friendly fields not considered pairing-friendly.

5 General tower construction method

Considering first the general case where p is an odd prime, $n > 0$ and $m > 1$ are integers and we want to construct the tower of sub-extensions of the towering-friendly field $\mathbb{F}_{p^{nm}}$ over $\mathbb{F}_{p^n}$. The two issues to address are:

- we need a method to construct towers over $\mathbb{F}_{p^n}$ when $m \equiv 0 \mod 4$ and $p^n \not\equiv 1 \mod 4$, and
- we need to find an appropriate irreducible binomial $x^m - \alpha$ in $\mathbb{F}_{p^n}[x]$ to construct the tower.

The first issue has a relatively simple solution. As $p^n \not\equiv 1 \mod 4$ and p is an odd prime, we know that n is odd and $p \equiv 3 \mod 4$. In order to be able to use the straightforward construction method we construct first a quadratic extension $\mathbb{F}_{p^{2n}}$ of $\mathbb{F}_{p^n}$, which we will refer to as a *base tower*, using a binomial. Over the base tower we can use the general method to build the rest of the tower using the binomial $x^{m/2} - \alpha$, where $\alpha \in \mathbb{F}_{p^{2n}} \setminus \mathbb{F}_{p^n}$, as now $p^{2n} \equiv 1 \mod 4$.[1]

In the particular case of $n = 1$ this can be done by simply adjoining a square root of -1. This idea is a generalisation of the approach taken by Barreto and Naehrig in [6] to construct the field $\mathbb{F}_{p^{12}}$ over $\mathbb{F}_p$. They first implement an efficient quadratic extension over the base field, and then

[1] The idea of a base tower can be generalised: Suppose a given $\mathbb{F}_{p^n}$ and m do not form a towering friendly field. Write $m = m_1 m_2$ such that $gcd(p^n - 1, m_2) = 1$ and all primes dividing m_1 divide $p^n - 1$. If all primes dividing m_2 divide $p^{nm_1} - 1$ then the tower of $\mathbb{F}_{p^{nm}}$ over base tower $\mathbb{F}_{p^n}$ can be constructed in two parts. The base tower $\mathbb{F}_{p^{nm_1}}$ over $\mathbb{F}_{p^n}$ can be constructed using the general method. Now, $\mathbb{F}_{p^{nm_1 m_2}}$ over $\mathbb{F}_{p^{nm_1}}$ is towering-friendly and the general method can be used to implement the remaining subfield extensions (using a binomial $x^{m_2} - \alpha$ where $\alpha \in \mathbb{F}_{p^{nm_1}} \setminus \mathbb{F}_{p^n}$). This gives a procedure for deciding whether or not, given input (p, n, m), any subfields of $F_{p^{nm}}/F_{p^n}$ are towering-friendly.

look for irreducible polynomials of the from $x^6 - \alpha$ where $\alpha \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ is neither a square nor a cube.

As to the problem of finding a suitable α for constructing the tower (and also the base tower when necessary), Theorem 1 provides a means for determining whether a given binomial is irreducible, but it does not give an efficient method for constructing the towers: taking random small elements of $\mathbb{F}_{p^n}$ then computing their order and verifying that the conditions hold is quite cumbersome – especially as n grows. Using this result, however, we are able to prove a theorem which results in a more efficient method for finding a suitable α.

We first recall some definitions and properties which will be used in the following theorems and proof: Let $\gamma \in \mathbb{F}_{p^n}$. The *Norm* from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ of γ, denoted $N_{\mathbb{F}_{p^n}/\mathbb{F}_p}(\gamma)$, is the product of all its conjugates,

$$N_{\mathbb{F}_{p^n}/\mathbb{F}_p}(\gamma) = \prod_{i=0}^{n-1} (\gamma)^{p^i} \in \mathbb{F}_p.$$

The norm is multiplicative, that is, for $\gamma_1, \gamma_2 \in \mathbb{F}_{p^n}$,

$$N_{\mathbb{F}_{p^n}/\mathbb{F}_p}(\gamma_1 \cdot \gamma_2) = N_{\mathbb{F}_{p^n}/\mathbb{F}_p}(\gamma_1) \cdot N_{\mathbb{F}_{p^n}/\mathbb{F}_p}(\gamma_2).$$

Using induction this gives us that $N_{\mathbb{F}_{p^n}/\mathbb{F}_p}(\gamma^\ell) = N_{\mathbb{F}_{p^n}/\mathbb{F}_p}(\gamma)^\ell$ for some $\ell \in \mathbb{Z}^+$. The *order* of γ is the smallest positive integer e such that $\gamma^e = 1$ in $\mathbb{F}_{p^n}$. The order is a divisor of $p^n - 1$.

Theorem 3. *Let $m > 1$, $n > 0$ be integers, p an odd prime and $\alpha \in \mathbb{F}_{p^n}^\times$. The binomial $x^m - \alpha$ is irreducible in $\mathbb{F}_{p^n}[x]$ if the following two conditions are satisfied:*

1. *for each prime factor q of m: q divides $p^n - 1$ and $N_{\mathbb{F}_{p^n}/\mathbb{F}_p}(\alpha) \in \mathbb{F}_p$ is not a qth residue in $\mathbb{F}_p$;*
2. *If $m \equiv 0 \mod 4$ then $p^n \equiv 1 \mod 4$.*

Proof. To prove this theorem, we show that condition 1 of Theorem 3 implies condition 1 of Theorem 1. We assume that condition 1 of Theorem 3 is true. Let e denote the order of α in $\mathbb{F}_{p^n}$ and q denote a prime divisor of m.

Suppose that $q \mid (p^n - 1)/e$. This implies that $e \mid (p^n - 1)/q$ and so α is a qth power in $\mathbb{F}_{p^n}$. Let $\delta \in \mathbb{F}_{p^n}$ be such that $\delta^q = \alpha$. Taking the norm of α we see that $N_{\mathbb{F}_{p^n}/\mathbb{F}_p}(\alpha) = N_{\mathbb{F}_{p^n}/\mathbb{F}_p}(\delta^q) = N_{\mathbb{F}_{p^n}/\mathbb{F}_p}(\delta)^q$ where $N_{\mathbb{F}_{p^n}/\mathbb{F}_p}(\delta) \in \mathbb{F}_p$ and thus $N_{\mathbb{F}_{p^n}/\mathbb{F}_p}(\alpha)$ is a qth residue in $\mathbb{F}_p$, a contradiction, so $q \nmid (p^n - 1)/e$.

We have also assumed that $q \mid (p^n - 1)$ and since $q \nmid (p^n - 1)/e$ it is clear that $q \mid e$ and so condition 1 of theorem 3 is satisfied.

Using Theorem 3 we are able to verify the irreducibility of a binomial $x^m - \alpha$ over an extension field $\mathbb{F}_{p^n}[x]$, where α is an element of $\mathbb{F}_{p^n}$, by checking the properties of just one particular element of the base field, namely the norm from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ of α - a much simpler task than computing the order of an element in $\mathbb{F}_{p^n}$. Theorem 3 can be applied in all contexts to find the binomial for automatically generating towers of extensions over all towering-friendly fields.

We now illustrate the usefulness of Theorem 3 by adapting it to the particular context of pairing-based cryptography as outlined in §3.

6 Towers for PBC

Following the constraints in §3, we will consider the tower of extensions as a sequence of quadratic and cubic sub-extensions. There is some freedom as to the best way to order the extensions. The choice here may be influenced by whether or not it is intended to compress the value of the pairing [20, 11]. This compressed value can then be further efficiently exponentiated in its compressed form by using Lucas or XTR based methods for times 2 and times 3 compression respectively. This is facilitated by terminating with a quadratic or a cubic extension respectively.

Consider for example the BN curves [6], which have an embedding degree of 12 and which support the sextic twist $t = 6$. In this case $E(\mathbb{F}_{p^2})$ arithmetic must be supported, and so it makes sense that the tower should start with a quadratic extension over the base field. This can be followed by a cubic extension and then a quadratic, or indeed the other way around. Assuming that the highest possible compression should be supported, the tower of choice in this case is $1 - 2 - 4 - 12$. This particular tower construction is given as an example by the IEEE draft standard [1]. For reasons that will become clear, starting with a quadratic extension where possible is preferred. In general, to have an efficient implementation we chose the tower which supports the highest possible compression rate and highest degree twist. Taking these constraints into account we make the following towering recommendations for the curves recommended in [9], in Table 1.

There have been some advances in arithmetic performance in $\mathbb{F}_{p^k}$ based on the final extension being a quadratic extension [2] and such towers can also be constructed using our method.

Table 1. Suggested Towers for Curves with Efficient Arithmetic

k	ρ	D	Twist t	Construction	Tower
4	2	1	4	FST [9]	1-2-4
6	2	3	6	FST [9]	1-2-6
8	1.5	1	4	KSS [14]	1-2-4-8
12	1	3	6	BN [6]	1-2-4-12
16	1.25	1	4	KSS [14]	1-2-4-8-16
18	1.333	3	6	KSS [14]	1-3-6-18
24	1.25	3	6	BLS [5]	1-2-4-8-24
32	1.125	1	4	KSS [14]	1-2-4-8-16-32
36	1.167	3	6	KSS [14]	1-2-6-12-36
48	1.125	3	6	BLS [5]	1-2-4-8-16-48

6.1 Tower construction for PBC

From the definition of towering-friendly fields we are only able to distinguish on a specific case-to-case basis if a general field is towering-friendly field. In the PBC setting we have a little more information. We are able to determine information about some of the parameters for particular curves in advance by making some observations. We see from the following discussion that all fields $\mathbb{F}_{p^k}$ arising when using the families of pairing friendly curves in Table 1 are towering-friendly.

Elliptic curves with CM discriminant $D = 1$ Elliptic curves from Table 1 with CM discriminant $D = 1$ have equations of the form $E : y^2 = x^3 + Ax$. We know that these curves are not supersingular (which is the case for curves with such equations defined over a prime field with characteristic $p \equiv 3 \mod 4$ [12]) and so $p \equiv 1 \mod 4$. This means that the field is towering-friendly (also pairing-friendly) as all $D = 1$ cases in Table 1 have $k = 2^n$ so the general method appears to be optimal. Only a small quadratic non-residue $\alpha \in \mathbb{F}_p$ is needed to construct the tower. Indeed, in the case of $p = 5 \bmod 8$ we can always choose $\alpha = 2$, which leads to fast reduction. An implementation can simply tower up quadratically, by adjoining the square root of the last adjoined element to build the next extension at each step.

Elliptic curves with CM discriminant $D = 3$ For elliptic curves with CM discriminant $D = 3$, p will not always be a pairing-friendly prime in the sense of the Koblitz and Menezes definition, but we do have some information which will aid us in the construction of the towers over

$\mathbb{F}_p$. Given that the CM discriminant $D = 3$, we know that the elliptic curve must have an equation of the form $E : y^2 = x^3 + B$. If $p \equiv 2 \mod 3$ then such a curve would supersingular [12] and so we know that $p \equiv 1 \mod 3$ must be true. We see then that all the fields resulting from this construction are towering-friendly.

For the KSS $k = 18$ curves and FST $k = 6$ curves we are able to use the general method in every case without a base tower (as $k \not\equiv 0 \mod 4$ and both 2 and 3 divide $p - 1$). We simply adjoin successive cubic and quadratic roots of some cubic and quadratic non-residue $\alpha \in \mathbb{F}_p$ in the recommended order.

For all other families of curves, if the prime p is not $1 \mod 4$ then we will need to use a base tower to construct the tower. One advantage in this case is that we know $p \equiv 3 \mod 4$ and so the base tower $\mathbb{F}_{p^2}$ over $\mathbb{F}_p$ can be efficiently constructed by adjoining a square root of -1. This may be more efficient than an implementation using a towering-friendly prime which satisfies $p \equiv 1 \mod 4$ as the arithmetic in $\mathbb{F}_p(\sqrt{-1})$ can be faster than $\mathbb{F}_p(\sqrt{\tau})$ for some other base field quadratic non-residue τ [10].

The following Corollary (drawing on ideas from Barreto and Naehrig in [6]) gives a method for finding appropriate candidates for the value α such that the polynomial $x^m - \alpha$ is irreducible over a finite field of the form $\mathbb{F}_{p^2} = \mathbb{F}_p(\sqrt{-1})$.

Corollary 4. *The polynomial $x^m - (a \pm b\sqrt{-1})$ is irreducible over $\mathbb{F}_{p^2}$, for $m = 2^i 3^j$, $i, j > 0$, if $a^2 + b^2$ is neither a square nor a cube in $\mathbb{F}_p$.*

Proof. The norm for any element $a \pm b\sqrt{-1}$ is $N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(a \pm b\sqrt{-1}) = (a + b\sqrt{-1})(a - b\sqrt{-1}) = a^2 + b^2$. The integer m is of the form $2^i 3^j$ and so by Theorem 3 if $a^2 + b^2$ is neither a quadratic nor a cubic residue modulo p, then $x^m - (a \pm b\sqrt{-1})$ is irreducible over $\mathbb{F}_{p^2}$.

Using this corollary, in order to construct the tower, small values of a and b can be tested until a combination is found such that $a^2 + b^2$ is neither a square nor a cube in $\mathbb{F}_p$. This process only requires a few cubic and quadratic non-residue tests to be performed on elements of the base field. Small values for a and b can be found to help improve efficiency.

As $\frac{1}{2}$ of the non-zero elements of $\mathbb{F}_p$ are non-squares and $\frac{2}{3}$ of the non-zero elements are non-cubes, such an element must exist; in fact, on heuristic grounds it is expected that $\frac{1}{3}$ of the elements will be neither squares nor cubes, which the experimental evidence supports.

Using corollary 4 we can now simply construct the towers for all curves from Table 1 with $D = 3$ for primes $p \equiv 7 \mod 12$.

BN $k = 12$ $\mathbb{F}_p \to \mathbb{F}_{p^2} \to \mathbb{F}_{p^4} \to \mathbb{F}_{p^{12}}$:

$$\mathbb{F}_p \subset \mathbb{F}_p(\sqrt{-1}) \subset \mathbb{F}_p(\sqrt{-1}, (a - b\sqrt{-1})^{1/2}) \subset \mathbb{F}_p(\sqrt{-1}, (a - b\sqrt{-1})^{1/6}) = \mathbb{F}_{p^{12}}.$$

BLS $k = 24$ $\mathbb{F}_p \to \mathbb{F}_{p^2} \to \mathbb{F}_{p^4} \to \mathbb{F}_{p^8} \to \mathbb{F}_{p^{24}}$:

$$\mathbb{F}_p \subset \mathbb{F}_p(\sqrt{-1}) \subset \mathbb{F}_p(\sqrt{-1}, (a - b\sqrt{-1})^{1/2}) \subset \mathbb{F}_p(\sqrt{-1}, (a - b\sqrt{-1})^{1/4}) \subset \mathbb{F}_p(\sqrt{-1}, (a - b\sqrt{-1})^{1/12}) = \mathbb{F}_{p^{24}}.$$

KSS $k = 36$ $\mathbb{F}_p \to \mathbb{F}_{p^2} \to \mathbb{F}_{p^6} \to \mathbb{F}_{p^{12}} \to \mathbb{F}_{p^{36}}$:

$$\mathbb{F}_p \subset \mathbb{F}_p(\sqrt{-1}) \subset \mathbb{F}_p(\sqrt{-1}, (a - b\sqrt{-1})^{1/3}) \subset \mathbb{F}_p(\sqrt{-1}, (a - b\sqrt{-1})^{1/6}) \subset \mathbb{F}_p(\sqrt{-1}, (a - b\sqrt{-1})^{1/18}) = \mathbb{F}_{p^{36}}.$$

BLS $k = 48$ $\mathbb{F}_p \to \mathbb{F}_{p^2} \to \mathbb{F}_{p^4} \to \mathbb{F}_{p^8} \to \mathbb{F}_{p^{16}} \to \mathbb{F}_{p^{48}}$:

$$\mathbb{F}_p \subset \mathbb{F}_p(\sqrt{-1}) \subset \mathbb{F}_p(\sqrt{-1}, (a - b\sqrt{-1})^{1/2}) \subset \mathbb{F}_p(\sqrt{-1}, (a - b\sqrt{-1})^{1/4}) \subset \mathbb{F}_p(\sqrt{-1}, (a - b\sqrt{-1})^{1/8}) \subset \mathbb{F}_p(\sqrt{-1}, (a - b\sqrt{-1})^{1/24}) = \mathbb{F}_{p^{48}}.$$

Once a suitable pair (a, b) has been found the tower can be constructed automatically.

Given a little more information about p, which is easily found, we are able to give some more specific constructions.

Construction 5. *For a prime $p \equiv 3$ modulo 8 the function $x^m - (1 + \sqrt{-1})$ is irreducible over $\mathbb{F}_{p^2}[x]$ for $m = 2^i 3^j$, $i, j > 0$, for approximately $2/3$ of the values of p.*

Proof. In this case $a^2 + b^2 = 2$. The polynomial will be irreducible if 2 is neither a square nor a cube modulo p. We know that 2 is a quadratic non-residue modulo p when $p \equiv 3 \mod 8$. The only remaining condition is that 2 is not a cube modulo p.

All primes $p \equiv 1 \mod 3$ can be written in the form $p = 3u^2 + v^2$. As Euler conjectured (proved by Gauss [17]) 2 is a cubic residue modulo p if and only if $3 \mid u$. Instinctively we would presume that this occurs $1/3$ of the time. There is currently no proof concerning the number of primes in a quadratic sequence but this is supported by experimental results. So 2 is a cubic non-residue modulo for approximately $2/3$ of the values of p for which $p \equiv 3$ modulo 8.

When $p \equiv 7 \mod 8$ the following corollary may be useful:

Construction 6. *For a prime $p \equiv 2$ or 3 modulo 5 the function $x^m - (2 + \sqrt{-1})$ is irreducible over $\mathbb{F}_{p^2}[x]$ for $m = 2^i 3^j$, $i, j > 0$ for approximately 2/3 of the values of p.*[2]

Proof. The values of a and b in theorem 4 in this case are 2 and 1 respectively, so $a^2 + b^2 = 5$. The polynomial will be irreducible if 5 is neither a square nor a cube modulo p. When $p \equiv 2$ or 3 modulo 5 we know that 5 is a quadratic non-residue modulo p and so the only condition left is that 5 should not be a cube in $\mathbb{F}_p$. With p written in the form $p = 3u^2 + v^2$, we know that 5 is a cube if $15 \mid u$, or $3 \mid u$ and $5 \mid v$, or $15 \mid (u \pm v)$, or $15 \mid (u \pm 2v)$ [17]. Again, there is currently no proof concerning the number of primes in a quadratic sequence but as supported by experimental results we expect that this occurs 1/3 of the time. So 5 is a cubic non-residue modulo for approximately 2/3 of the values of p for which $p \equiv 2$ or 3 modulo 5.

The results of Corollaries 5 and 6 is that for around 2/3 of the primes not considered pairing-friendly, we have a more automatic and often more efficient implementation than is possible for pairing-friendly fields. To construct the tower for a pairing-friendly field we must find a small quadratic and cubic non-residue in $\mathbb{F}_p$ - which will be at least 5.

Example 1 The value $x = 4008804000000009_{16}$ generates suitable parameters for a BN curve. Using this x we see that $p \equiv 3 \mod 4$ we first need a base tower before we use the general construction method. We can see that $p \equiv 3 \mod 5$ and running a few tests we verify that $a^2 + b^2$ is neither a square nor a cube for the (unordered) pairs $(a, b) = (1, 2)$ as given in Construction 6. Here we can construct the tower as:

$$\mathbb{F}_p \xrightarrow{2} \mathbb{F}_p(\sqrt{-1}) \xrightarrow{2} \mathbb{F}_p(\sqrt{-1}, (1 - 2\sqrt{-1})^{1/2}) \xrightarrow{3} \mathbb{F}_p(\sqrt{-1}, (1 - 2\sqrt{-1})^{1/6}).$$

Given that $a^2 + b^2 = b^2 + a^2$ we could also use:

$$\mathbb{F}_p \xrightarrow{2} \mathbb{F}_p(\sqrt{-1}) \xrightarrow{2} \mathbb{F}_p(\sqrt{-1}, (2 - \sqrt{-1})^{1/2}) \xrightarrow{3} \mathbb{F}_p(\sqrt{-1}, (2 - \sqrt{-1})^{1/6}).$$

Trivially we could also use the conjugates $a + b\sqrt{-1}$ and $b + a\sqrt{-1}$, or the negatives $-a + b\sqrt{-1}$ and $-b + a\sqrt{-1}$. Not only $(1, 2)$ could be used, also $(1, 3)$, $(1, 5)$, $(2, 3)$ would be suitable. This example raises some questions about the choice of pairs (a, b). A simple analysis indicates that the optimal choice is the one which minimises $\omega(a) + \omega(b)$, where $\omega(n)$ is the number of additions required to perform a multiplication by n.

[2] In this case, the polynomial $x^m - (1 + 2\sqrt{-1})$ is also irreducible.

Example 2 Comparing now our method with that given in [6], for the security level of 196 bits, the authors suggest the BN curve with prime

$$p = 627710171953126940051704371006089286231860471313967450972 3.$$

The tower suggested in [6] would then be

$$\mathbb{F}_p \xrightarrow{2} \mathbb{F}_p(\sqrt{-1}) \xrightarrow{6} \mathbb{F}_p(\sqrt{-1}, (-8 + 8\sqrt{-1})^{1/6}).$$

Using our method, we see that 2 is neither a cube, nor a square modulo p and so the tower can be constructed:

$$\mathbb{F}_p \xrightarrow{2} \mathbb{F}_p(\sqrt{-1}) \xrightarrow{6} \mathbb{F}_p(\sqrt{-1}, (1 + \sqrt{-1})^{1/6}),$$

which is equivalent to:

$$\mathbb{F}_p \xrightarrow{2} \mathbb{F}_p(\sqrt{-1}) \xrightarrow{2} \mathbb{F}_p(\sqrt{-1}, (1 + \sqrt{-1})^{1/2}) \xrightarrow{3} \mathbb{F}_p(\sqrt{-1}, (1 + \sqrt{-1})^{1/6}).$$

Example 3 Using the parameterisation of the KSS $k = 18$ curves [14] and the value $x = 17592186050810$, we find a suitable value for p where $p \equiv 3 \mod 4$, so according to the constraints given by the Koblitz and Menezes (predating the discovery of such curves) the extension field $\mathbb{F}_{p^k}$ would not be pairing-friendly. We can construct these towers using the general method and after very few tests we discover that 3 is neither a square nor a cube modulo p so the tower for this particular prime can be given by:

$$\mathbb{F}_p \xrightarrow{3} \mathbb{F}_p(3^{1/3}) \xrightarrow{2} \mathbb{F}_p(3^{1/6}) \xrightarrow{3} \mathbb{F}_p(3^{1/18}).$$

7 Conclusion

In this paper we proved a theorem which leads to a method to determine if a binomial defined over an extension field is irreducible by performing a few tests on one element of the base field. This results in a method to construct the towers of extension fields of towering-friendly fields $\mathbb{F}_{p^m}$ for which the general method could not be used.

Using Theorem 4 along with the general construction method and base towers we are now able to automatically construct towers of extensions for the implementation of the finite fields used in pairing-based cryptography by performing a few cubic and quadratic non-residue tests on elements of $\mathbb{F}_p$. The resulting constructions are efficient and can contribute to the development of a cryptographic compiler specialised for pairing-based cryptography as described in [8].

8 Acknowledgements

The authors thank Rob Granger for his insightful comments and encouraging discussions. The authors also thank Paulo Barreto for his helpful comments.

References

1. IEEE P1363.3: Standard for identity-based cryptographic techniques using pairings. Draft 3:Section 5.3.2. `http://grouper.ieee.org/groups/1363/IBC/index.html`.
2. C. Arène, T. Lange, M. Naehrig, and C. Ritzenthaler. Faster computation of the Tate pairing. Cryptology ePrint Archive, Report 2009/155, 2009. `http://eprint.iacr.org/`.
3. D. Bailey and C. Paar. Optimal extension fields for fast arithmetic in public-key algorithms. In *Advances in Cryptology – Crypto' 1998*, volume 1462 of *Lecture Notes in Computer Science*, pages 472–485. Springer-Verlag, 1998.
4. 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 354–368. Springer-Verlag, 2002.
5. 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.
6. P.S.L.M. Barreto and M. Naehrig. Pairing-friendly elliptic curves of prime order. In *Selected Areas in Cryptography – SAC'2005*, volume 3897 of *Lecture Notes in Computer Science*, pages 319–331. Springer-Verlag, 2006.
7. A. J. Devegili, M. Scott, and R.Dahab. Implementing cryptographic pairings over Barreto-Naehrig curves. In *Pairing 2007*, volume 4575 of *Lecture Notes in Computer Science*, pages 197–207. Springer-Verlag, 2007.
8. L. J. Dominguez Perez and M. Scott. Automatic generation of optimised cryptographic pairing functions. *SPEED-CC Workshop Record– Software Performance Enhancement for Encryption and Decryption and Cryptographic Compilers*, 1:55–71, 2009.
9. D. Freeman, M. Scott, and E. Teske. A taxonomy of pairing-friendly elliptic curves. Cryptology ePrint Archive, Report 2006/372, 2006. `http://eprint.iacr.org/2006/372`.
10. S. Galbraith, X. Lin, and M. Scott. Endomorphisms for faster elliptic curve cryptography on a large class of curves. In *EUROCRYPT '09: Proceedings of the 28th Annual International Conference on Advances in Cryptology*, pages 518–535, Berlin, Heidelberg, 2009. Springer-Verlag.
11. R. Granger, D. Page, and M. Stam. On small characteristic algebraic tori in pairing based cryptography. *LMS Journal of Computation and Mathematics*, 9:64–85, 2006.
12. D. Hankerson, A. Menezes, and S. Vanstone. *Guide to Elliptic Curve Cryptography*. Springer, 2003.
13. F. Hess, N. Smart, and F. Vercauteren. The eta pairing revisited. *IEEE Trans. Information Theory*, 52:4595–4602, 2006.

14. E. Kachisa, E. Schaefer, and M. Scott. Constructing Brezing-Weng pairing friendly elliptic curves using elements in the cyclotomic field. In *Pairing 2008*, volume 5209 of *Lecture Notes in Computer Science*, pages 126–135. Springer-Verlag, 2008.
15. N. Koblitz and A. Menezes. Pairing-based cryptography at high security levels. In *Cryptography and Coding: 10th IMA International Conference*, volume 3796 of *Lecture Notes in Computer Science*, pages 13–36. Springer-Verlag, 2005.
16. E. Lee, H. Lee, and C. Park. Efficient and generalized pairing computation on abelian varieties. *IEEE Trans. Information Theory*, 55:1793–1803, 2009.
17. F. Lemmermeyer. Springer Monographs in Mathematics. Springer-Verlag, 2000.
18. R. Lidl and H. Niederreiter. *Finite Fields*. Number 20 in Encyclopedia of Mathematics and its Applications. Cambridge University Press, Cambridge, UK, 2nd edition, 1997.
19. Selçuk Baktır and Berk Sunar. Optimal tower fields. *IEEE Transactions on Computers*, 53(10):1231–1243, October 2004.
20. M. Scott and P. Barreto. Compressed pairings. In *Advances in Cryptology – Crypto' 2004*, volume 3152 of *Lecture Notes in Computer Science*, pages 140–156. Springer-Verlag, 2004. Also available from `http://eprint.iacr.org/2004/032/`.