Constructing Tower Extensions of Finite Fields for 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 of a finite 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 classes of finite fields than previous methods, some of which allow faster arithmetic.
We also show that for some families of pairing-friendly elliptic curves defined over $\mathbb{F}_p$ there are a large number of instances for which an efficient tower extension $\mathbb{F}_{p^k}$ is given immediately if the parameter defining the prime characteristic of the field satisfies a few easily checked equivalences.
Keywords: Extension Fields, Pairing implementation, pairing-based cryptosystems, Euler's Conjectures.

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 is fundamentally different. An efficient implementation at the 80-bit level of security using the Tate pairing on

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

a Cocks-Pinch pairing-friendly curve [10] will be completely different from an implementation at the 128-bit level using the 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 [9].

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 first contribution of this work is to prove a result which gives a method of checking if a binomial defined over an extension field is irreducible by testing a single element in the base field. This result gives a new method which complements the existing method and gives a means for automatically constructing efficient towers of extensions of finite fields in the cases for which the existing method can not be used or do not give the most efficient algorithms. The resulting constructions are efficient and the usefulness of these results will be shown by the specific application to pairing-based cryptography. The second contribution of this work is to give some constant constructions for the tower extensions for classes of families of pairing-friendly curves.

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 will be presented. Some existing ideas for constructing tower extensions are briefly explained in §4. A general result to use in the construction of tower extensions for general fields is given in §5 which is applied to the context of PBC in §6. In §6.2 Euclid's conjectures will be presented and used to give concrete tower constructions for some specific families of pairing-friendly curves. In §7 the selection of appropriate polynomials for implementation will be discussed. In §8 we draw some conclusions.

2 Extension Fields

Consider the implementation of the extension field $\mathbb{F}_{p^k}$. The natural representation of the 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 [10]. 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 of 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. [8].

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 (PBC) would be to fix the tower for a particular k. This 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-friendly 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.

Motivating this work is our ambition to contribute to a "cryptographic compiler" [9], that is, a compiler which when given as input the parameters for a pairing-friendly curve, should be able to automatically 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 $e(P,Q)$, evaluates as 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 endomorphism [23].

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 $\overline{\mathbb{F}}_p$ are contained in $\mathbb{F}_{p^k}$, the codomain of the pairing. 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) [7].

For the Tate pairing the point Q is commonly represented as a point over some twist $E'(\mathbb{F}_{p^{k/d}})$, where $d \mid k$, as opposed to being on the curve defined over the full extension field $E(\mathbb{F}_{p^k})$. When k is even, the quadratic twist ($d = 2$) can always be used, when the pairing-friendly curve has a CM discriminant of $D = 1$ and $4 \mid k$, the quartic twist ($d = 4$) can be used, if $D = 3$, $3 \mid k$ and k is odd, cubic twists ($d = 3$) can be used and when the CM discriminant is $D = 3$ and $6 \mid k$, the sextic twist ($d = 6$) 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 [10], 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 $k = 2^i \cdot 3^j$ for $i, j \geq 0$. 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 general towers

Let p be an odd prime, and let $n, m > 0$ 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 $\mathbb{F}_{p^n}$ and successively adjoin roots of the previously adjoined root until the tower has been constructed (we refer to this as 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 $p^n \equiv 1 \mod 4$.*

The *order* of $\gamma \in \mathbb{F}_{p^n}$ is the smallest positive integer e such that $\gamma^e = 1$ in $\mathbb{F}_{p^n}$ and the order is a divisor of $p^n - 1$.

By Theorem 1 we see that the general method above works for all $m \not\equiv 0 \mod 4$. 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 cubic and quadratic 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 $p \equiv 1 \mod 12$ 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 neither a square not a cube in $\mathbb{F}_p$. The extension 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 $j = 0$ then it is sufficient that $p \equiv 1 \mod 4$ 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 $\alpha \in \mathbb{F}_p$ 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 [8]). Having to skip a nice curve just because $p \equiv 3 \mod 4$ 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 $k = 18$ [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 arises 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 instead refer to these fields as *towering-friendly* as this gives a more accurate description of these fields – the towers over such fields are easily constructed. This definition is not specific to pairings, but in this setting we would like to use towering-friendly fields for the most efficient implementation possible.

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 $q-1$.

In essence, towering-friendly fields are fields for which the tower of sub-extensions can be easily (and most efficiently) constructed; that is, using binomials. The OEFs of Bailey and Paar [3] are by definition towering-friendly fields with characteristic a prime of a special form. The fields said to be pairing-friendly by Koblitz and Menezes are indeed towering-friendly, but these are not the only towering-friendly fields which occur in the context of pairing-based cryptography.

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 finite field $\mathbb{F}_{p^{nm}}$ over $\mathbb{F}_{p^n}$. The general method uses a binomial $x^m - \alpha$ which is irreducible in $\mathbb{F}_{p^n}[x]$ and successively adjoins roots of the previously adjoined root until the tower has been constructed, as in [19]. By Theorem 1 the only restriction on α is that α should not be a qth power in $\mathbb{F}_{p^n}$ for any prime divisor q of m. This method works for all m, $m \not\equiv 0 \bmod 4$. When $m \equiv 0 \bmod 4$, this method will work if $p^n \equiv 1 \bmod 4$ (which is always true for even n).

The two issues to address now are:

- we need a method to build a tower when $m \equiv 0 \bmod 4$ and $p^n \equiv 3 \bmod 4$;
- we need to find a suitable irreducible binomial $x^m - \alpha \in \mathbb{F}_{p^n}[x]$ to construct the tower.

The first problem has a relatively simple solution. We construct first a quadratic extension of $\mathbb{F}_{p^n}$, $\mathbb{F}_{p^{2n}}$, which we will refer to as a *base tower*, using a binomial. We now have $p^{2n} \equiv 1 \bmod 4$ so we can use the general method to build the rest of the tower above $\mathbb{F}_{p^{2n}}$ using a binomial $x^{m/2} - \alpha$, where $\alpha \in \mathbb{F}_{p^{2n}}$ (not

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

Remark 3. *The idea of a base tower can be generalised: Suppose $\mathbb{F}_{p^{nm}}$ over $\mathbb{F}_{p^n}$ is not a towering-friendly field. Write $m = m_1 m_2$ such that $gcd(p^n - 1, m_2) = 1$ and all the primes dividing m_1 divide $p^n - 1$. If all the primes dividing m_2 divide $p^{nm_1} - 1$ then the tower of $\mathbb{F}_{p^{nm}}$ over $\mathbb{F}_{p^n}$ can be constructed in two parts using the general method. First $\mathbb{F}_{p^{nm_1}}$ over $\mathbb{F}_{p^n}$ is constructed using a binomial, this is the base-tower. Then $\mathbb{F}_{p^{nm}} = \mathbb{F}_{p^{nm_1 m_2}}$ over $\mathbb{F}_{p^{nm_1}}$ is constructed using a binomial defined over $\mathbb{F}_{p^{nm_1}}$ (not over any subfield of $\mathbb{F}_{p^{nm_1}}$). This method can be implemented recursively to achieve an efficient tower for a non-towering-friendly extension.*

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 then computing their order in the extension field and verifying that the conditions hold is quite cumbersome, the order could be quite large and this could require a lot of extension field computation for a single element. Using Theorem 1, however, we are able to prove a theorem which results in a simpler method for checking the irreducibility of a polynomial $x^m - \alpha$ in certain cases and hence a more practical method for finding irreducible polynomials to construct the towering-friendly field extensions, particularly in the context of PBC.

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* of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$ 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 $\gamma_1, \gamma_2 \in \mathbb{F}_{p^n}$,

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

and so for any $\ell \in \mathbb{Z}^+$ we have $N_{\mathbb{F}_{p^n}/\mathbb{F}_p}(\gamma^\ell) = N_{\mathbb{F}_{p^n}/\mathbb{F}_p}(\gamma)^\ell$.

Theorem 4. *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. *each prime factor q of m divides $p - 1$ 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 4 implies condition 1 of Theorem 1. We assume that condition 1 of Theorem 4 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 4 is satisfied.

Using Theorem 4 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 of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$ of α – a much simpler task than computing the order of an element in $\mathbb{F}_{p^n}$. Theorem 4 can be used in all cases for which the prime divisors of m also divide $p - 1$ to automatically generate towers of extensions over all towering-friendly fields to build an efficient tower of extensions for the extension field $\mathbb{F}_{p^{nm}}$. As already mentioned, if condition 2 of Theorem 1 is not satisfied, the towers can still be easily constructed by first constructing a base tower, a quadratic extension, then using the theorem to construct the tower over the base tower.

We now illustrate the usefulness of Theorem 4 by adapting it to the context of PBC as outlined in §3.

6 Towers in Pairing-Based Cryptography

Given the constraints outlined in §3, it is clear that the tower of extensions can be built 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 [21, 12]. 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]. Starting with a quadratic extension where possible is preferred (in case a base tower is needed). Taking all these constraints into account, in Table 1 we make the towering recommendations for the curves recommended in [10].

Table 1. Suggested Towers for Curves with Efficient Arithmetic

k	ρ	D	Twist d	Construction	Tower
4	2	1	4	FST [10]	1-2-4
6	2	3	6	FST [10]	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

The ρ-value is given by $\frac{\log(p)}{\log(r)}$ for p the characteristic of the field over which the curve is defined and r the cardinality of the group of points on the elliptic curve.

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

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 extension field is a 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 the 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 $p \equiv 3 \mod 4$ [7]) and so $p \equiv 1 \mod 4$. This means that the field is towering-friendly as all $D = 1$ cases in Table 1 have $k = 2^n$ so the Koblitz-Menezes strategy appears to be optimal. Indeed, in the case of $p \equiv 5 \bmod 8$ 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 be supersingular [23] and so $p \equiv 1 \mod 3$ 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 $p \not\equiv 1 \mod 4$ then we 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 actually be more efficient than an implementation using a pairing-friendly field as the arithmetic in $\mathbb{F}_p(\sqrt{-1})$ can be performed faster than in $\mathbb{F}_p(\sqrt{\tau})$ for some other quadratic non-residue $\tau \in \mathbb{F}_p$ [11]. The following Corollary (drawing on ideas from Barreto and Naehrig in [6]) gives a method for finding an appropriate 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 5. *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. For any element $a \pm b\sqrt{-1}$, $N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(a \pm b\sqrt{-1}) = (a + b\sqrt{-1})(a - b\sqrt{-1}) = a^2 + b^2$. The integer m is of the form $2^i 3^j$ and so by Theorem 4 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 $\mathbb{F}_{p^2}$.

This Corollary is basically Theorem 4 in the case $p \equiv 3 \mod 4$, $n = 2$ and $m = k/2$, this is the case of most concern in PBC. 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 [6].

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

Construction 6. *For approximately 2/3 of the primes $p \equiv 3$ modulo 8 the polynomial $x^m - (1 + \sqrt{-1})$ is irreducible in $\mathbb{F}_{p^2}[x]$ for $m = 2^i 3^j$, $i, j > 0$.*

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 p for approximately 2/3 of the values of p.

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

Construction 7. *For approximately* 2/3 *of the primes* $p \equiv 2$ *or* 3 *modulo* 5 *the polynomial* $x^m - (2 + \sqrt{-1})$ *is irreducible in* $\mathbb{F}_{p^2}[x]$ *for* $m = 2^i 3^j$, $i, j > 0$.[1]

Proof. The values of a and b in Corollary 5 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 $15 \mid a$, or $3 \mid a$ and $5 \mid b$, or $15 \mid (a \pm b)$, or $15 \mid (a \pm 2b)$ [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 p for approximately 2/3 of the values of p.

The result of Constructions 6 and 7 is that for around 2/3 of the fields not considered pairing-friendly we have a more automatic and often more efficient implementation than is possible for pairing-friendly fields.

6.2 Using Euler's Conjectures

For primes which are equivalent to $2 \mod 3$ it is easily shown that every element is a cubic residue modulo p. For primes which are $1 \mod 3$ Fermat showed that p can be written as the sum $p = a^2 + 3b^2$ for some integers a and b. Euler conjectured (and Gauss proved) that using this form we can easily determine if some small elements are cubic residues [17]:

1. 2 is a cubic residue $\Leftrightarrow 3 \mid b$.
2. 3 is a cubic residue $\Leftrightarrow 9 \mid b$; or $9 \mid (a \pm b)$.
3. 5 is a cubic residue $\Leftrightarrow 15 \mid b$; or $3 \mid b$ and $5 \mid a$; or $15 \mid (a \pm b)$; or $3 \mid (2a \pm b)$.
4. 6 is a cubic residue $\Leftrightarrow 9 \mid b$; or $9 \mid (a \pm 2b)$.
5. 7 is a cubic residue $\Leftrightarrow 21 \mid b$; or $3 \mid b$ and $7 \mid a$; or $21 \mid (a \pm b)$; or $7 \mid (a \pm 4b)$; or $7 \mid (2a \pm b)$.

These conjectures can be used once p has been constructed to decide if constructions 6 or 7 can be used. For some cases we have this information already.

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

BN Towers The prime characteristic p of the field over which a BN curve is defined is parameterised by the polynomial $p(x) = 36x^4 + 36x^3 + 24x^2 + 6x + 1$; an appropriate value x_0 is chosen to give $p = p(x_0)$. It was noticed by Shirase [22] that this parameterisation can be written in the form $p(x) = a(x)^2 + 3b(x)^2$ thus giving us more information about the towers we can construct for certain values of x_0 without having to perform the quadratic and cubic residue tests modulo p. We have $a(x) = 6x^2 + 3x + 1$ and $b(x) = x$. With this additional information, we now see that we are able to use Theorem 4 to put conditions on the values of x_0, which, when satisfied, give an immediate construction for the tower of fields of degree 12 over BN primes.

Considering first BN primes $p \equiv 3 \mod 4$ we know that $x_0 \equiv \pm 1 \mod 4$ and that we have a towering friendly field which requires a base tower $\mathbb{F}_{p^2}$ which can be constructed by adjoining $\sqrt{-1}$ to $\mathbb{F}_p$. We now need to find an element $a+b\sqrt{-1} \in \mathbb{F}_{p^2}$ such that $x^6-(a+b\sqrt{-1})$ is irreducible to construct the remaining extensions. From Corollary 5 we know that $x^6 - (a + b\sqrt{-1})$ is irreducible if $a^2 + b^2$ is neither a square nor a cube in $\mathbb{F}_p$. We know from the conjecture 1 that if $x_0 \equiv \pm 1 \mod 3$ then 2 is a cubic non-residue modulo p. For 2 to be a non-quadratic residue also we need $p \equiv 3 \mod 8$, this implies that $x_0 \equiv 3 \mod 4$. Together, these two constraints give the following:

- If $x_0 \equiv 7$ or $11 \mod 12$ then $x^6 - (1 + \sqrt{-1})$ is irreducible over $\mathbb{F}_{p^2} = \mathbb{F}_p(\sqrt{-1})$.

In [22] the same conclusion is drawn, but using a much more elaborate method. We see that this result supports the claim in Construction 6 as 2/3 of the possible values of x_0 (for $p \equiv 3 \mod 8$) give a p for which 2 is a quadratic non-residue.

Using Theorem 4 we are also able to classify more constructions than those given in [22]. Using a similar method as above:

- If x_0 is odd and $x_0 \equiv 1, 3, 7, 11, 12$ or $13 \mod 15$ then $x^6 - (1 + 2\sqrt{-1})$ is irreducible over $\mathbb{F}_{p^2} = \mathbb{F}_p(\sqrt{-1})$.

Using Euler's conjectures it is also straight forward to set construction for BN primes $p \equiv 1 \mod 4$ not needing a base tower.

- If $x_0 \not\equiv 0 \mod 3$ and $x_0 \equiv 2, 6 \mod 8$ then $x^{12} - 2$ is irreducible;
- If $x_0 \equiv 1, 3, 7, 11, 12$ or $13 \mod 15$ then $x^{12} - 5$ is irreducible;
- If $x_0 \not\equiv 0, 2$ or $4 \mod 9$ and $x_0/2$ is odd then $x^{12} - 6$ is irreducible.

BN curves are quite plentiful and easy to find. Using BN curves in pairing-based protocols means that we need an efficient implementation of $\mathbb{F}_{p^{12}}$ and also of $\mathbb{F}_{p^2}$ as we would use a degree 6 twist. It may be favourable to choose $x_0 \equiv 1 \mod 2$ and x_0 satisfying one of the equivalences above so that $\mathbb{F}_{p^2}$ can be constructed as $\mathbb{F}_p(\sqrt{-1})$ and the tower for $\mathbb{F}_{p^{12}}$ can be constructed using one of Constructions 6 or 7, though these fields would not have originally been considered pairing-friendly. Given that BN curves are so plentiful, this restriction would not impede finding curves appropriate for use.

KSS Towers When $k = 18$ the parameterisation of $p(x)$ can also be written in the form $a(x)^2 + 3b(x)^2 = p(x)$ where $a(x)$ and $b(x)$ have integer coefficients. In these cases we are also able to give the tower construction if the value x_0 satisfies some easily checked conditions.

KSS $k = 18$ The polynomial parameterisation of p for a KSS $k = 18$ curve is given by

$$p(x) = (x^8 + 5x^7 + 7x^6 + 37x^5 + 188x^4 + 259x^3 + 343x^2 + 1763x + 2401)/21.$$

We also know that $x \equiv 14 \mod 42$ so substituting $x = 42x' + 14$ we obtain the equation

$$p(x') = 461078666496x'^8 + 1284433428096x'^7 + 1564374047040x'^6 + 1088278335648x'^5 + 473078255328x'^4 + 131624074008x'^3 + 22896702948x'^2 + 2277529014x' + 99213811.$$

Using Euclid's algorithm and interpolation we find

$$a(x') = 444528x'^4 + 629748x'^3 + 333396x'^2 + 78321x' + 6908,$$

and

$$b(x') = 296352x'^4 + 407484x'^3 + 209916x'^2 + 48091x' + 4143,$$

such that $a(x')^2 + 3b(x')^2 = p(x')$. Using Euler's Conjectures we see that:

- If $x'_0 \equiv 1, 4, 5, 8 \mod 12$ then $x^{18} - 2$ is irreducible over $\mathbb{F}_p$;
- If $x'_0 \not\equiv 2, 3, 4 \mod 9$ then $x^{18} - 3$ is irreducible over $\mathbb{F}_p$;
- If $x'_0 \equiv 7, 9, 12, 14 \mod 15$ then $x^{18} - 5$ is irreducible over $\mathbb{F}_p$;
- If $x'_0 \equiv a \mod 42$ then $x^{18} - 6$ is irreducible over $\mathbb{F}_p$,

where $a = \{2, 3, 4, 9, 10, 11, 12, 13, 18, 20, 21, 22, 27, 28, 30, 31, 35, 36, 37, 38, 38, 40, 44, 45, 46, 48, 49, 53, 54, 55, 56, 57, 58, 62, 63, 64, 65, 66\}$;

- If $x'_0 \equiv 2 \mod 7$ then $x^{18} - 7$ is irreducible over $\mathbb{F}_p$.

7 Twists and choosing α

When choosing a particular value of α to construct the tower we may find that there are more than one potential values we could use. In this case we must decide which value α is best for implementation. This is illustrated in the following example.

Example 1 The value $x_0 = 4008804000000009_{16}$ generates suitable parameters for a BN curve. Using this x_0 we see that $p \equiv 3 \mod 4$ and we first need a base tower $\mathbb{F}_{p^2} = \mathbb{F}_p(\sqrt{-1})$ before we use the general construction method. We see also that $x_0 \equiv 3 \mod 15$ and x_0 is odd so, as shown in section 6.2, we know immediately that 5 is a cubic and quadratic non-residue in $\mathbb{F}_p$ and so $x^6 - (1 + 2\sqrt{-1})$ is irreducible over $\mathbb{F}_{p^2} = \mathbb{F}_p(\sqrt{-1})$. Using the same reasoning, however, we also know that $x^6 - (2 + 1\sqrt{-1})$, $x^6 - (2 - 1\sqrt{-1})$, $x^6 - (-2 - 1\sqrt{-1})$ and $x^6 - (-2 + 1\sqrt{-1})$ are all irreducible over $\mathbb{F}_{p^2} = \mathbb{F}_p(\sqrt{-1})$. Using this particular value of x_0 we also see that $a^2 + b^2$ is neither a square nor a cube for the (unordered and unsigned) pairs $(a, b) = (1, 3)$, $(1, 5)$, $(2, 3)$ as well as for $(1, 2)$. This example raises an important question:

How do we decide which value will be the best for implementation?

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. There is another important point to take into account when choosing α and that is the construction of the twists of the elliptic curve used when computing the pairing.

In §3 it was mentioned that twists are used to improve the efficiency of the pairing computation. To construct a twist of degree d and the isomorphism from the twist to the curve we need an element $i \in \mathbb{F}_{p^{k/d}}$ which is a qth non-residue for all divisors q of k/d. Clearly, for the tower construction we already have such an element. In fact, it would make sense to use the same element to define the twist as we use to construct the tower; though we will have to be slightly more careful in our selection of the element α. An elliptic curve with a twist of degree d actually has $\phi(d)$ twists of degree d, with different numbers of points. The twists used for the curves specified above are of degrees $d = 4$ or 6, both having $\phi(6) = \phi(4) = 2$ possible twists.

For $E(F_p) : y^2 = x^3 + Ax$, the quartic twists are given by $E_1'(\mathbb{F}_{p^{k/t}}) : y^2 = x^3 + Ax/i$ and $E_2'(\mathbb{F}_{p^{k/t}}) : y^2 = x^3 + Ax/i^3$, the twist used for the pairing is the twist with the correct number of points. The respective isomorphisms are given as [20]:

$$E_1' \to E : (x, y) \to (i^{1/2}x, i^{3/4}y)$$

and

$$E_2' \to E : (x, y) \to (i^{1/2}x/i, i^{1/4}y/i).$$

Similarly, for $E(F_p) : y^2 = x^3 + B$, the sextic twists are given by $E_1'(\mathbb{F}_{p^{k/t}}) : y^2 = x^3 + B/i$ and $E_2'(\mathbb{F}_{p^{k/t}}) : y^2 = x^3 + B/i^5$, the twists must then be tested to find the one with the correct number of points. The respective isomorphisms are given as:

$$E_1' \to E : (x, y) \to (i^{1/3}x, i^{1/2}y)$$

and

$$E_2' \to E : (x, y) \to (i^{2/3}x/i, i^{1/2}y/i).$$

We see here how important it is to choose the element i to be of the simplest form as the isomorphism will be effected. If we select α such that $i = \alpha^{(1/e)}$, where $e = k/d$, then the isomorphism is basically a free computation [8]. If the curve defined choosing $i = \alpha^{(1/e)}$ does not give the correct number of points, then we must take $i = \alpha^{(3/e)}$ if E' is a quartic twist or $i = \alpha^{(5/e)}$ if E' is a sextic twist. In these cases the isomorphism will be slightly more expensive. This is also discussed in [13].

To summarise, when selecting the element α to define the tower, both $\omega(\alpha)$ and the structure of the twist should be taken into account.

8 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 an efficient method of construction for fields which occur in pairing-based cryptography and which were not originally considered to be "pairing-friendly" and could not be constructed using general method discussed in [15]. Using Theorem 5 along with the general construction method 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 [9]. We have used our results, Euclid's conjectures and an observation by Shirase [22] to give immediate constructions for a large class of towering-friendly fields used with BN curves. Using Euclid's conjectures we have also given an immediate construction for a large group of towering-friendly fields used with KSS $k = 18$ curves. We are confident that these methods can be extended to other families of pairing-friendly elliptic curves and other embedding degrees to generate automatic tower structures for these curves.

9 Acknowledgements

The authors thank Rob Granger for his insightful comments and encouraging discussions and thank Paulo Barreto for his helpful comments. We would also like to thank the anonymous reviewers for their constructive 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 *LNCS*, 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 *LNCS*, 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 *LNCS*, 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 *LNCS*, pages 319–331. Springer-Verlag, 2006.
7. H. Cohen and G. Frey, editors. *Handbook of elliptic and hyperelliptic curve cryptography*. CRC Press, 2005.
8. A. J. Devegili, M. Scott, and R.Dahab. Implementing cryptographic pairings over Barreto-Naehrig curves. In *Pairing 2007*, volume 4575 of *LNCS*, pages 197–207. Springer-Verlag, 2007.
9. 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.
10. D. Freeman, M. Scott, and E. Teske. A taxonomy of pairing-friendly elliptic curves. In *Journal of Cryptology*, volume 23. Springer, 2010.
11. 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.
12. 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.
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 *LNCS*, 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 *LNCS*, 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. *Reciprocity Laws: From Euler to Eisenstein*. 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. A note on twists for pairing friendly curves. `ftp://ftp.computing.dcu.ie/pub/resources/crypto/twists.pdf`.

21. M. Scott and P. Barreto. Compressed pairings. In *Advances in Cryptology – Crypto' 2004*, volume 3152 of *LNCS*, pages 140–156. Springer-Verlag, 2004. Also available from `http://eprint.iacr.org/2004/032/`.
22. Masaaki Shirase. Universally constructing 12-th degree extension field for ate pairing. Cryptology ePrint Archive, Report 2009/623, 2009. `http://eprint.iacr.org/`.
23. J. H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, New York, 1986.