Constructing Tower Extensions of Finite Fields for Implementation of Pairing-Based Cryptography

Naomi Benger and Michael Scott,[1]

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

17th May 2010

Claude Shannon Institute
Discrete Mathematics, Coding, Cryptography and Information Security
www.shannoninstitute.ie

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

Pairing-Based Cryptography (PBC) is fundamentally different to most other Public-Key Cryptography: we can not write a generic implementation which will perform reasonably well for varying security levels.

For each security level we need to be able to automatically generate:

- curve,
- pairing,
- finite field representation.

Notation

- $\mathbb{F}_q$ be a finite field, $q = p^n$ for some prime p and integer n.
- E is an elliptic curve defined over a prime field $\mathbb{F}_p$; r is a large prime divisor of the number of points of E over $\mathbb{F}_p$.
- The *embedding degree* of E with respect to r: smallest positive integer k such that $r \mid p^k - 1$.

All points of E or order r defined over $\overline{\mathbb{F}}_p$ are defined over $\mathbb{F}_{p^k}$;

- $\mathbb{G}_1, \mathbb{G}_2$ disjoint additive groups of order r in $E(\mathbb{F}_{p^k})$;

A *Pairing*: $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mu_r \in \mathbb{F}_{p^k}$. To compute the pairing, need a lot of extension field arithmetic...

The most efficient way to implement an extension field is using towers:

A *Tower extension* is an extension of a field, constructed by continually adjoining roots of a certain element.

$\mathbb{F}_{p^k} \equiv \mathbb{F}_p[x]/f(x)\mathbb{F}_p[x]$ for some irreducible binomial $f(x)$.

Why Towers?

- IEEE draft standard "P1363.3: Standard for Identity-Based Cryptographic Techniques using Pairings": extensions of odd primes should be constructed using a tower of extensions created using irreducible binomials at each stage.
- Implementation advantages...

Theorem

The binomial $x^m - \alpha \in \mathbb{F}_q[x]$ $(m \geq 2)$ is irreducible if and only if the following are true:

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

Problems:

1. Can't use this if $q \not\equiv 1 \mod 4$ ... we don't want to add extra constraints on p.
2. Need to compute the order of elements in $\mathbb{F}_q$ ... don't really want to do this either.

Avoid computing the Order

Easier method to construct $\mathbb{F}_{q^m}$ if all primes dividing m also divide $p-1$

Theorem

The binomial $x^m - \alpha \in \mathbb{F}_q[x]$ $(m \geq 2)$ is irreducible if the following two conditions are satisfied:

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

Solves the problem of computing orders of elements in $\mathbb{F}_q$.

The condition $q \equiv 1 \mod 4$ when $m \equiv 0 \mod 4$...?

Avoid adding extra constraints

If $q \not\equiv 1 \mod 4 \Rightarrow q \equiv 3 \mod 4$.

Construct a *Base Tower* of degree 2 (using a binomial) then a tower of degree $m/2$ over the base tower.

If $p = q$ this can be done by adjoining $\sqrt{-1}$.

What these results mean to PBC

We extend the recommendation: $k = 2^i 3^j$ $(i > 0, j \geq 0)$.

We like to use curves curves supporting higher degree twists:

- Quartic Twists: CM discriminant $D = 1$ and have equations of the form $E : y^2 = x^3 + Ax \Rightarrow p \equiv 1 \mod 4$

  $\Rightarrow$We can use the general method

- Sextic Twists: CM discriminant $D = 3$ and have equations of the form $E : y^2 = x^3 + B \Rightarrow p \equiv 1 \mod 3$

  $\Rightarrow$We can use the general method if $p \equiv 1 \mod 4$

Towers in PBC

Now we need to automatically generate these towers.

We will construct the towers using two tools:

- Theorem which gives sufficient and necessary conditions for irreducibility of a binomial in PBC;
- Euler's conjectures for cubic residues and the polynomial parameterisation of the primes.

Euler's Conjectures

Fermat: primes $p \equiv 1 \mod 3$, p can be written as the sum $p = a^2 + 3b^2$ for $a, b \in \mathbb{Z}$.

- 2 is a cubic residue $\Leftrightarrow 3 \mid b$.
- 3 is a cubic residue $\Leftrightarrow 9 \mid b$; or $9 \mid (a \pm b)$.
- 5 is a cubic residue $\Leftrightarrow 15 \mid b$; or $3 \mid b$ and $5 \mid a$; or $15 \mid (a \pm b)$; or $3 \mid (2a \pm b)$.
- ...

The primes used in PBC are parameterised by univarite polynomials.

Theorem for BN Towers:

BN primes: $k = 12 \rightarrow$ we can use a sextic twist defined over $\mathbb{F}_{p^2}$.
Consider the case $p \equiv 3 \mod 4$.

Corollary

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

Maybe more efficient than using a field with $p \equiv 1 \mod 4$: arithmetic in $\mathbb{F}_p(\sqrt{-1})$ can be performed faster than in $\mathbb{F}_p(\sqrt{\tau})$ for some other quadratic non-residue $\tau \in \mathbb{F}_p$.

Using Euler's Conjectures for BN Towers:

BN curves are defined over $\mathbb{F}_p$ where $p = 36x^4 + 36x^3 + 24x^2 + 6x + 1$.

- $a(x) = 6x^2 + 3x + 1$
- $b(x) = x$

$p(x) = a(x)^2 + 3b(x)^2$ (Shirase)

Let $p = 36x_0^4 + 36x_0^3 + 24x_0^2 + 6x_0 + 1$ for some x_0.

BN Towers

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

- 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 $\mathbb{F}_{p^2} = \mathbb{F}_p(\sqrt{-1})$.

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.

KSS $k = 18$ Towers

KSS $k = 18$ curves are defined over $\mathbb{F}_p$ where

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

for some $x \equiv 14 \mod 42$.

Substitute $x = 42x' + 14$ to get:

- $a(x') = 444528x'^4 + 629748x'^3 + 333396x'^2 + 78321x' + 6908$
- $b(x') = 296352x'^4 + 407484x'^3 + 209916x'^2 + 48091x' + 4143$

$$p(x') = a(x')^2 + 3b(x')^2$$

Let x'_0 be the value determining p.

KSS $k = 18$ Towers

- 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 $\mathbb{F}_p$,

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

- If $x_0' \equiv 2 \mod 7$ then $x^{18} - 7$ is irreducible over $\mathbb{F}_p$.

Which tower to chose...?

When there is more than one option...

- Twist isomorphism
- Fast arithmetic...

Summary

Automatic constructions of finite extension fields used in PBC using:

- Euler's conjectures,
- polynomial parametrisation of p,
- new sufficient and necessary conditions for irreducibility of polynomials over certain fields.

The resulting constructions are efficient and can contribute to the development of a cryptographic compiler specialised for pairing-based cryptography.