Number Theory & Cryptography - Weekly meetings

Curso en Zacatecas [Q1 2015]

Luis J. Dominguez Perez

CIMAT-Zac, Junio 03 de 2015

Contenido, sección 1

Tower extensions of finite fields

Twists

Divisores

Towers

- An element $\alpha \in \mathbb{F}_{p^k}$ can be represented as a polynomial up to degree $k-1$ with coefficients in $\mathbb{F}_p$ modulo an irreducible polynomial $\in \mathbb{F}_p[X]$.
- For efficiency purposes, this irreducible polynomial should be simple.

- One method to construct the $\mathbb{F}_{p^k}$ is using towers of extensions.
- Baktir and Sunar introduced the concept of tower field representation, which facilitates the finite field operations, in particular the inversion.
- They defined a *tower field* as a field obtained by extending its ground field with several irreducible polynomials.

Towering-friendly field

- Benger and Scott in presented a method to construct a tower, using towering-friendly fields.

Definition

A *towering-friendly* field is a field of the form $\mathbb{F}_{q^m}$, where q is a prime power, where $q-1$ is divisible by all of the prime divisors of m.

Construction

- These fields are constructed using a tower of sub-extensions using binomials as irreducible polynomials.
- Each sub-extension is a layer constructed by adjoining the roots of the previous level (every other sub-extension is represented with elements of the previous sub-extension).
- The tower can be constructed using quadratic and cubic extensions of the previous base field until we reach the desired extension field ($\mathbb{F}_{p^k}$).

Towering examples

The table presents the recommended choice of sub-extensions for selected embedding degrees:

k	Construction	Tower
8	KSS	1-2-4-8
12	6.8	1-2-4-12
18	6.12	1-3-6-18
24	6.6	1-2-4-8-24
36	6.14	1-2-6-12-36

BN example

- Barreto and Naehrig proposed the use of a polynomial $X^6 - \xi$, where $1/\xi = \lambda^2\mu^3$ with $\lambda \in \mathbb{F}_p$ a non-cube, and $\mu \in \mathbb{F}_{p^2}$ a non-square.
- Corollary 5 from the Benger and Scott method says that a polynomial $x^m - (a \pm b\sqrt{-1})$ is irreducible over $\mathbb{F}_{p^2}$ if $a^2 + b^2$ is neither a square nor a cube in $\mathbb{F}_p$.
- We can trivially find either a small (a, b) or (λ, μ) pair with a linear search. . .

Irreducible polynomials

Fortunately, some of the values for (a, b) in the Benger and Scott paper are already calculated and are based on some values of p, the parameter defining the base field.

$\mathbb{F}_{p^n}$	X^m	Test	(a, b)
2	$2^i 3^j$	$p \equiv 3 \bmod 8$	(1,1)
2	$2^i 3^j$	$p \equiv 2, 3 \bmod 5$	(2,1)
Construction	X^m	**Test**	(a, b)
6.8	6	$x \equiv 7, 11 \bmod 12$	(1,1)
6.8	6	$x \equiv 1, 3, 7, 11, 12, 13 \bmod 15$	(1,2)
6.8	12	$x \equiv 1, 3, 7, 11, 12, 13 \bmod 15$	(5,0)
6.12	18	$x_0 \equiv 1, 4, 5, 8 \bmod 12$	(2,0)
6.12	18	$x_0 \equiv 7, 9, 12, 14 \bmod 15$	(5,0)
6.12	18	$x_0 \not\equiv 2, 3, 4 \bmod 9$	(3,0)

Contenido, sección 2

Tower extensions of finite fields

Twists

Divisores

Twist of a curve

Definition

A twist curve E' defined over $\mathbb{F}_{p^e}$, with $e = \frac{k}{d}$, is another elliptic curve isomorphic to E defined over $\mathbb{F}_{p^k}$.

Degree of a twist

We define d as the degree of the twist of the curve E. The values of d, with a CM field defined as $\mathbb{Q}(\sqrt{D})$ are as follows:

- $d = 6$ if the curve E has CM discriminant $D = -3$, and $j(E) = 0$.
- $d = 4$ if the discriminant is $D = -1$, and $j(E) = 1728$.
- $d = 2$ for any other value of D, and $j(E) \neq 0, 1728$.

When $d = 2$, the curves is said to have or support a quadratic twist, when $d = 3$: cubic twist, when $d = 4$: quartic twist, and when $d = 6$: sextic twist.

Form of the twisted curve

The formulae for an elliptic curve E is $y^2 = x^3 + a.x + b$, defined over $\mathbb{F}_p$, whereas the formulae for the twisted curve E' depends on the degree of the twist, and are as follows:

$$E' : y^2 = x^3 + \frac{ax}{D^2} + \frac{b}{D^3}b \qquad \text{for } d = 2$$

$$E' : y^2 = x^3 + \frac{ax}{D} \qquad \text{for } d = 4$$

$$E' : y^2 = x^3 + \frac{b}{D} \qquad \text{for } d = 6$$

where $D \in \mathbb{F}_{p^e}$ such that $W^d - D$ is irreducible over $\mathbb{F}_{p^e}[W]$.

One isomorphism

Furthermore, if $\delta \in \mathbb{F}_{p^k}$ is a root of $W^d - D$, then there exists a homomorphism which maps points on the twist E' to the points of the curve E as follows:

$\psi : E'(F_{p^{k/d}}) \to E(\mathbb{F}_{p^k})$ defined by: $(x', y') \to (x'.\delta^{1/3}, y'.\delta^{1/2})$,

with an isomorphism given by:

$\phi : \mu_d \to Aut(E) : \delta \mapsto [\delta]$ with $[\delta](x, y) = (x.\delta^2, y.\delta^3)$.

Contenido, sección 3

Tower extensions of finite fields

Twists

Divisores

Funciones racionales de la curva

Dada una curva elíptica E definida sobre un campo finito $\mathbb{F}_q$, donde $q = p^n$, y $n \in \mathbb{Z}^+$, con $\bar{\mathbb{F}}_q$ como la cerradura de $\mathbb{F}_q$, se dice que $f(x, y)$ es una función racional en $E/\mathbb{F}_q$, si existe un punto $P = (x_P, y_P) \in E(\bar{\mathbb{F}}_q)$, tal que $f(x_P, y_P) \neq \infty$

El conjunto de funciones racionales en $E/\mathbb{F}_q$ está denotado por $\bar{\mathbb{F}}_q(E)$, y para todo $f \in \bar{\mathbb{F}}_q(E)$ se cumple que $f(P)$ es un elemento en el conjunto $\{\bar{\mathbb{F}}_q \cup \infty\}$

funciones racionales de la curva

Sean P y Q puntos en la curva elíptica $E/\mathbb{F}$, una función racional $f \in \bar{\mathbb{F}}_q(E)$ tiene un **cero** en P, y un **polo** en Q, si y sólo sí $f(P) = 0$, y $f(Q) = \infty$, respectivamente. En general, la evaluación de f en un punto P puede ser representada a partir de la siguiente igualdad:

$$f(P) = (u(P))^m \cdot g(P)$$

donde $m \in \mathbb{Z}$, $u(P) = 0$, y $g(P) \neq 0, \infty$. Si $m > 0$, entonces f tiene un cero en P, y si $m < 0$, entonces f tiene un polo (en P). cabe mencionar que $u(P)$ es llamada la función "*uniformadora*", y el número m es el **orden** de f en P, denotado como:

$$\text{ord}_P(f) = m.$$

Divisores

Sea $E/\mathbb{F}_q$ una curva elíptica, a cada punto $P \in E(\bar{\mathbb{F}}_q)$ se le asigna el símbolo formal $[P]$. Un divisor $\mathcal{D}$ sobre $E/\mathbb{F}_q$ es una combinación lineal finita de dichos símbolos con coeficientes en $\mathbb{Z}$

$$\mathcal{D} = \sum_j a_j [P_j], \quad a_j \in \mathbb{Z}.$$

divisores

Los operadores que definen a un divisor son:

- El grado

$$\deg\left(\sum_j a_j[P_j]\right) = \sum_j a_j \in \mathbb{Z}$$

- La suma

$$\text{sum}\left(\sum_j a_j[P_j]\right) = \sum_j a_j P_j \in E$$

- El soporte

$$\text{supp}\left(\sum_j a_j[P_j]\right) = \{P_j \in E | a_j \neq 0\}$$

Divisores principales

Un divisor $\mathcal{D}$ sobre la curva elíptica $E/\mathbb{F}_q$ con $\deg(\mathcal{D}) = 0$, y $\text{sum}(\mathcal{D}) = \mathcal{O}$, es llamado **"principal"** si existe una función racional $f \in \bar{\mathbb{F}}_q(E)$, tal que $\mathcal{D} = \text{div}(f)$, donde

$$\text{div}(f) = \sum_{P_j \in E} \text{ord}_{P_j}(f)[P_j].$$

ejemplos

Las funciones racionales $\ell_{P,P}$, y $\ell_{P,Q}$

- $\mathbf{div}(\ell_{P,P}) = 2[P] + [-2P] - 3[\mathcal{O}]$
- $\mathbf{div}(\ell_{P,Q}) = [P] + [Q] + [-(P+Q)] - 3[\mathcal{O}]$

Propiedades

En general, dadas las funciones f y $g \in \bar{\mathbb{F}}_q(E)$, los divisores principales cumplen con las siguientes propiedades:

- $\text{div}(f \cdot g) = \text{div}(f) + \text{div}(g)$
- $\text{div}(f/g) = \text{div}(f) - \text{div}(g)$
- La función f es una constante, sí y sólo si $\text{div}(f) = 0$

propiedades

Una función racional f puede ser evaluada en un divisor $\mathcal{D} = \sum_j a_j[P_j]$, a través de la siguiente fórmula:

$$f(\mathcal{D}) = \prod_{P_j \in \text{supp}(\mathcal{D})} f(P_j)^{a_j},$$

de tal manera que, para todo $n \in \mathbb{Z}$,

$$f(\mathcal{D})^n = f(n\mathcal{D}),$$

donde $n\mathcal{D} = \sum_j n \cdot a_j[P_j]$.

Definiciones varias

Reciprocidad de Weil

Sea $E/\mathbb{F}_q$ una curva elíptica, y $f, g \neq 0$ funciones racionales en $\bar{\mathbb{F}}_q(E)$ con soportes disjuntos, entonces:

$$f(\mathsf{div}(g)) = g(\mathsf{div}(f))$$

definiciones varias

Relación de equivalencia

Dos divisores $\mathcal{D}_1$, y $\mathcal{D}_2$ son linealmente equivalentes, $\mathcal{D}_1 \sim \mathcal{D}_2$, sí y sólo si $\mathcal{D}_1 - \mathcal{D}_2$ es un divisor principal, esto es,

$$\mathcal{D}_1 - \mathcal{D}_2 = \mathsf{div}(f), \quad \text{o bien} \mathcal{D}_1 = \mathcal{D}_2 + \mathsf{div}(f)$$

Miller

Función de Miller

Una función de Miller de longitud $s \in \mathbb{Z}$ denotada por $f_{s,R}$, es una función racional en $\bar{\mathbb{F}}_q(E)$ con divisor
$\text{div}(f_{s,R}) = s[R] - [sR] - (s-1)[\mathcal{O}]$.

. . . Miller

Lemma

Sea $f_{s,R}$ una función de Miller, y sea v_R la función vertical que corta a la curva elíptica E en el punto R, para todo $a, b \in \mathbb{Z}$ se cumple que:

- $f_{a+b,R} = f_{a,R} \cdot f_{b,R} \cdot \ell_{aR,bR}/v_{(a+b)R}$
- $f_{ab,R} = f_{b,R}^{a} \cdot f_{a,bR}$
- $f_{1,R} = c$, donde c es una constante