Number Theory & Cryptography - Weekly meetings

Curso en Zacatecas [Q1 2015]

Luis J. Dominguez Perez

CIMAT-Zac, Junio 10 de 2015

Contenido, sección 1

Emparejamiento de Weil

Emparejamiento de Weil

Sea $r > 1$ un número entero, y sean $\mathcal{D}_1$, y $\mathcal{D}_2$ divisores en una curva elíptica E con soportes disjuntos, es decir,

$$\text{supp}(\mathcal{D}_1) \cap \text{supp}(\mathcal{D}_2) = \emptyset,$$

existen dos funciones racionales f_1, y f_2 en E, tales que $\text{div}(f_1) = r\mathcal{D}_1$, y $\text{div}(f_2) = r\mathcal{D}_2$. El emparejamiento de Weil definido como

$$e_W(\mathcal{D}_1, \mathcal{D}_2) = \frac{f_1(\mathcal{D}_2)}{f_2(\mathcal{D}_1)},$$

es un emparejamiento bilineal no degenerado . . .

emparejamiento de Weil

Específicamente, dados los puntos $P \in \mathbb{G}_1$, y $Q \in \mathbb{G}_2$, f_1, y f_2 son funciones racionales en $\mathbb{F}_{p^k}(E)$ con divisores $\text{div}(f_1) = r[P] - r[\mathcal{O}]$, y $\text{div}(f_2) = r[Q] - r[\mathcal{O}]$, respectivamente, tal que $\mathcal{D}_1 \sim [P] - [\mathcal{O}]$, y $\mathcal{D}_2 \sim [Q] - [\mathcal{O}]$. Por lo tanto, el cálculo de $f_i(\mathcal{D}_i)$ toma valores en el grupo multiplicativo $\mathbb{F}^*_{p^k}$, y además, a través de la reciprocidad de Weil, se cumple que

$$\left(\frac{f_1(\mathcal{D}_2)}{f_2(\mathcal{D}_1)}\right)^r = \frac{f_1(r\mathcal{D}_2)}{f_2(r\mathcal{D}_1)} = \frac{f_1(\text{div}(f_2))}{f_2(\text{div}(f_1))} = 1,$$

es decir, $g = e_W(\mathcal{D}_1, \mathcal{D}_2)$ es un elemento en el subgrupo de las r-ésimas raíces primitivas de la unidad en $\mathbb{F}^*_{p^k}$.

emparejamiento de Weil

En los últimos años se han hecho distintas mejoras a los emparejamientos bilineales, por un lado, se ha demostrado que el cálculo de $f_1(\mathcal{D}_2)$ puede ser reemplazado por $f_1(Q)$, y del mismo modo $f_2(\mathcal{D}_1)$ por $f_2(P)$. Por otro lado, si p, y Q son puntos de torsión r, entonces:

$$\text{div}(f_1) = r[P] - r[\mathcal{O}] = r[P] - [rP] - (r-1)[\mathcal{O}]$$

y

$$\text{div}(f_2) = r[Q] - r[\mathcal{O}] = r[Q] - [rQ] - (r-1)[\mathcal{O}]$$

es decir, f_1, y f_2 se pueden expresar como las funciones de Miller $f_{r,P}$, y $f_{r,Q}$.

emparejamiento de Weil

Finalmente,

$$e_W : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T,$$

$$(Q, P) \mapsto \frac{f_{r,P}(Q)}{f_{r,Q}(P)}$$

Contenido, sección 2

Emparejamiento de Weil

Emparejamiento de Tate

Emparejamiento de ate

Tate-Lichtenbaum pairing

The Tate pairing was introduced by Tate as a rather general pairing on Abelian varieties over local fields. Lichtenbaum gave an application of this pairing to the Jacobians of curves over local fields. The Tate-Lichtenbaum pairing is hereafter referred to as the Tate pairing

Tate pairing

- Let $P \in E(\mathbb{F}_p)[r]$ and let $Q \in E(\mathbb{F}_p)$. Q can be used for representing an equivalence class in $E(\mathbb{F}_p)/rE(\mathbb{F}_p)$.
- Since $[r]P = \mathcal{O}$ it follows that there is a function f such that $(f) = r(P) - r(\mathcal{O})$.
- Let D be any degree zero divisor equivalent to $(Q) - (\mathcal{O})$ such that D is defined over $\mathbb{F}_p$ and the support of D is disjoint from the support of (f).
- In most cases such a divisor can easily be constructed by choosing an arbitrary point $S \in E(\mathbb{F}_p)$ and defining $D = (Q + S) - (S)$.
- Since f and D are defined over $\mathbb{F}_p$, the value $f(D)$ is an element of $\mathbb{F}_p$.
- Since the supports of (f) and D are disjoint, we have $f(D) \neq 0$ and so $f(D) \in \mathbb{F}_p^*$.

Simplificando

- Let $P \in E(\mathbb{F}_p)[r]$ and $Q \in E(\mathbb{F}_{p^k})$, and consider the divisor $D = (Q + S) - (S)$ with S a random point in $E(\mathbb{F}_{p^k})$. Let $f_{a,P}$ be a function with a divisor

$$(f_{a,P}) = a(P) - (aP) - (a-1)(0)$$

for $a \in \mathbb{Z}$. A non degenerate, bilinear Tate pairing is the map:

$$e_r : E(\mathbb{F}_p)[r] \times E(\mathbb{F}_{p^k})/rE(\mathbb{F}_{p^k}) \to \mathbb{F}^*_{p^k}/(\mathbb{F}^*_{p^k})^r$$
$$(P, Q) \mapsto f_{r,P}(Q)$$

A “small” map at the end

- The value of the pairing is in an equivalence class, $\mathbb{F}_{p^k}^* / (\mathbb{F}_{p^k}^*)^r$.
- For practical purposes it is preferred to raise the value of the pairing to the power of $(p^k - 1)/r \in \mathbb{F}_{p^k}^*$ to obtain a unique representative of the class, and to make it bilinear.
- This exponentiation is known as the *final exponentiation*, and the pairing is referred to as the *Reduced Tate Pairing*.

The Tate pairing

- The Tate pairing becomes:

$$e_r(P,Q) : (P,Q) \mapsto f_r, P(Q)^{(p^k-1)/r}$$

- We define the $\mathbb{G}_1 \in E(\mathbb{F}_p)[r]$ as the group of points of order r on E over the base field $\mathbb{F}_p$
- $\mathbb{G}_2$ as the group on $E(\mathbb{F}_{p^k})/rE(\mathbb{F}_{p^k})$.
- Let P be a point in $\mathbb{G}_1$ and Q a point in $\mathbb{G}_2$.

Contenido, sección 3

Emparejamiento de Weil

Emparejamiento de Tate

Emparejamiento de ate

ate pairing

- The ate pairing is a variant of the Tate pairing and it is a generalization of the Eta pairing, a pairing that can be used with supersingular elliptic curves (now defunct).
- The ate pairing is particularly suitable for pairing-friendly curves with small values of t.

ate pairing

- We take
  - $\mathbb{G}_1 = E[r] \cap Ker(\pi_p - [1])$,
  - $\mathbb{G}_2 = E[r] \cap Ker(\pi_p - [p])$,
  - and let $T = t - 1$.

- Let $N = \mathsf{GCD}(T^k - 1, p^k - 1)$,
- and $T^k - 1 = LN$.

ate pairing

For $Q \in \mathbb{G}_2$ and $P \in \mathbb{G}_1$, the ate pairing is defined as:

$$e_T : (Q, P) \longmapsto f_{T,Q}(P)^{c_T(p^k-1)/N},$$

where $c_T = \sum_{i=0}^{k-1-i} p^i \equiv kp^{k-1} \bmod r$.

The ate pairing is a bilinear, non-degenerate pairing if $r \nmid L$.

We can use the Tate's final exponentiation $(p^k - 1)/r$ if $T^k \not\equiv 1 \bmod r^2$, since $r|N$ and $r \nmid c$ the function is always bilinear, and non-degenerate