Bilinear Pairings - study

arnaucube

August 2022

Abstract

Notes taken from Matan Prsma math seminars and also while reading about Bilinear Pairings. Usually while reading papers and books I take handwritten notes, this document contains some of them re-written to $LaTeX$.

The notes are not complete, don't include all the steps neither all the proofs. I use these notes to revisit the concepts after some time of reading the topic.

Contents

1 Weil reciprocity

2 Generic Weil Pairing

Def 2.1. Divisor

$$D = \sum_{P \in E(\mathbb{K})} n_p \cdot [P]$$

Def 2.2. Degree & Sum

$$deg(D) = \sum_{P \in E(\mathbb{K})} n_p$$

$$sum(D) = \sum_{P \in E(\mathbb{K})} n_p \cdot P$$

Def 2.3. Principal divisor iff $deg(D) = 0$ and $sum(D) = 0$

$D \sim D'$ iff $D - D'$ is principal.

Def 2.4. Evaluation of a rational function

$$r(D) = \prod r(P)^{n_p}$$

2.1 Generic Weil Pairing

Let $E(\mathbb{K})$, with $\mathbb{K}$ of char p, n s.t. $p \nmid n$.

$\mathbb{K}$ large enough: $E(\mathbb{K})[n] = E(\overline{\mathbb{K}}) = \mathbb{Z}_n \oplus \mathbb{Z}_n$ (with n^2 elements).

$P, Q \in E[n]$:

$$D_P \sim [P] - [0]$$

$$D_Q \sim [Q] - [0]$$

We need them to have disjoint support:

$$D_P \sim [P] - [0]$$

$$D_Q \sim [Q+T] - [T]$$

$$\Delta D = D_Q - D'_Q = [Q] - [0] - [Q+T] + [T]$$

3 Exercises

An Introduction to Mathematical Cryptography, 2nd Edition - Section 6.8. Bilinear pairings on elliptic curves

6.29. $div(R(x) \cdot S(x)) = div(R(x)) + div(S(x))$, where $R(x), S(x)$ are rational functions.
proof:
Norm of f: $N_f = f \cdot \overline{f}$, and we know that $N_{fg} = N_f \cdot N_g \ \forall \ \mathbb{K}[E]$,
then

$$deg(f) = deg_x(N_f)$$

and

$$deg(f \cdot g) = deg(f) + deg(g)$$

Proof:

$$deg(f \cdot g) = deg_x(N_{fg}) = deg_x(N_f \cdot N_g)$$

$$= deg_x(N_f) + deg_x(N_g) = deg(f) + deg(g)$$

So, $\forall P \in E(\mathbb{K}),\ ord_P(rs) = ord_P(r) + ord_P(s)$.
As $div(r) = \sum_{P \in E(\mathbb{K})} ord_P(r)[P]$, $div(s) = \sum ord_P(s)[P]$.
So,

$$div(rs) = \sum ord_P(rs)[P]$$

$$= \sum ord_P(r)[P] + \sum ord_P(s)[P] = div(r) + div(s)$$

6.31.

$$e_m(P,Q) = e_m(Q,P)^{-1} \forall P, Q \in E[m]$$

Proof: We know that $e_m(P,P) = 1$, so:

$$1 = e_m(P+Q, P+Q) = e_m(P,P) \cdot e_m(P,Q) \cdot e_m(Q,P) \cdot e_m(Q,Q)$$

and we know that $e_m(P,P) = 1$, then we have:

$$1 = e_m(P,Q) \cdot e_m(Q,P)$$

$$\implies e_m(P,Q) = e_m(Q,P)^{-1}$$