Homework 11 in Cryptography II

Prof. Dr. Rudolf Mathar, Wolfgang Meyer zu Bergsten, Steven Corroy

20.07.2010

Exercise 31. Describe how the DSA signature scheme can be carried out in a group of $\mathbb{F}_p$-rational points on an elliptic curve $E/\mathbb{F}_p$.

Exercise 32. Implementation cost of elliptic curve arithmetic is often expressed in terms of the number of multiplications, squarings and inversions in the underlying field K. Determine how many of each of these operations are needed for a point addition and for a point doubling, respectively.

Exercise 33. Given the following curve:

$$E_a : y^2 = x^3 + ax + (a + 1).$$

Let E_a be defined over $\mathbb{F}_{11}$, i.e. $a \in \mathbb{F}_{11}$.

(a) For which values of a does E_a describe an elliptic curve over $\mathbb{F}_{11}$?

(b) How many points are in $E_4(\mathbb{F}_{11})$? Determine all points.

(c) Find the inverse to each point $P \in E_4(\mathbb{F}_{11})$.