Advanced cryptography: Pairing-based cryptography
winter term 2012/13

DANIEL LOEBENBERGER AND MICHAEL NÜSKEN

4. Exercise sheet
Hand in solutions until Monday, 19 November 2012, 23:59:59

In cryptography we typically need the size of an elliptic curve to implement our primitives. The following exercise shall give you a tiny little more insight into this business.

Exercise 4.1. (10 points)

Analogously to the lecture, describe detailed the differences between classical signature schemes and ID-based signature schemes. $\boxed{10}$

Exercise 4.2 (Count it!). (15 points)

Let $E\colon y^2 = x^3 + ax + b$ be an elliptic curve defined over $\mathbb{F}_q$ with characteristic neither 2 nor 3. Denote by $E(\mathbb{F}_q)$ the set of $\mathbb{F}_q$-rational points on the curve E and write $\#E(\mathbb{F}_q)$ for the number of $\mathbb{F}_q$-rational points on the curve.

(i) Show that $\#E(\mathbb{F}_q) \leq 2q + 1$. $\boxed{2}$

(ii) Show that we always have $\#E(\overline{\mathbb{F}}_q) = \infty$. $\boxed{2}$

(iii) Consider the (generalized) Legendre symbol $\boxed{3}$

$$\left(\frac{a}{\mathbb{F}_q}\right) := \begin{cases} 0 & \text{if } a = 0, \\ 1 & \text{if there is } b \in \mathbb{F}_q \text{ with } b^2 = a, \\ -1 & \text{if there is no } b \in \mathbb{F}_q \text{ with } b^2 = a. \end{cases}$$

Prove that $\#E(\mathbb{F}_q) = q + 1 + \sum_{x \in \mathbb{F}_q} \left(\frac{x^3+ax+b}{\mathbb{F}_q}\right)$.

(iv) Consider the curve $E\colon x^3 + x + 1$ over $\mathbb{F}_5$. Compute $\#E(\mathbb{F}_5)$ using the formula from (iii). $\boxed{3}$

(v) Consider the same situation over $\mathbb{F}_{5^2} = \mathbb{F}_5[x]/(x^2 + x + 1)$. Compute $\#E(\mathbb{F}_{5^2})$ using the formula from (iii). $\boxed{5}$

For the next exercise you need the following

Theorem (Group structure of an elliptic curve). *Let E be an elliptic curve over $\mathbb{F}_q$. Then*

$$E(\mathbb{F}_q) \simeq \mathbb{Z}_n \text{ or } E(\mathbb{F}_q) \simeq \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$$

for some integer $n \geq 1$, or for integers $n_1, n_2 \geq 1$ with n_1 dividing n_2.

Exercise 4.3 (Group order and structure). (0+10 points)

Consider $q = 73$.

+1 (i) Determine the Hasse interval of possible group sizes $\#E(\mathbb{F}_q)$.

+1 (ii) Consider the elliptic curve $E_1\colon y^2 = x^3 - 2x + 2$ defined over $\mathbb{F}_q$. The point $(-36, 24)$ on E_1 has order 23. Determine $\#E_1(\mathbb{F}_q)$ and the possible group structure of E_1.

+2 (iii) Consider the elliptic curve $E_2\colon y^2 = x^3 - 2x + 1$ defined over $\mathbb{F}_q$. The point $(20, 2)$ has order 5 and the point $(-23, -12)$ has order 8. Determine $\#E_2(\mathbb{F}_q)$ and the possible group structure of E_2.

+2 (iv) Consider the elliptic curve $E_3\colon y^2 = x^3 - 3x + 5$ defined over $\mathbb{F}_q$. The point $(25, 15)$ has order 9 and the point $(17, -7)$ has order 15. Determine $\#E_3(\mathbb{F}_q)$ and the possible group structure of E_3.

+4 (v) Consider the elliptic curve $E_4\colon y^2 = x^3 + 16$ defined over $\mathbb{F}_q$. Both points $P := (-5, 16)$ and $Q := (-35, -24)$ have order 9. Determine $\#E_4(\mathbb{F}_q)$ and conclude the group structure. Hint: Show that there is no k such that $Q = kP$ or $3Q = kP$ and use Hasse.

Exercise 4.4 (Distribution of sizes of elliptic curves). (0+8 points)

In this exercise we will explore how the sizes of elliptic curves over some particular small finite field are distributed.

+4 (i) Write a small program that counts the number of points of all elliptic curves in Weierstraß form over $\mathbb{F}_{11}$. To do so, generate all possible equations of the form $y^2 = x^3 + ax + b$ with $a, b \in \mathbb{F}_{11}$ and count for each choice of a and b using for example the formula from exercise 7.1 (iii) how many pairs $(x, y) \in \mathbb{F}_{11}^2$ exist that fullfill that equation. Do not forget to count the point at infinity!

+2 (ii) Nicely plot the statistics and compare your results to Hasse's bound $|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}$.

+2 (iii) Explain the symmetry of the plot.