Cryptanalytic world records, summer 2014

DANIEL LOEBENBERGER, KONSTANTIN ZIEGLER

5. Exercise sheet
Hand in solutions until Sunday, 11 May 2014, 23:59:59

Exercise 5.1 (Re-doing relation finding). (8 points)

Show how to perform the following task: $\boxed{8}$

Find the logarithm of $h_1(X)$ and the logarithm of all elements of K that are represented by linear polynomials $X + a$ for $a \in \mathbb{F}_{q^2}$.

To do so, repeat the proof from the lecture by setting $P(X) = X$. Explain detailed how you set up you linear system at the end and argue why you can solve the above stated task.

Exercise 5.2 (Number of suitable relations). (3 points)

In the lecture we observed that the number of relations in the quasi-polynomial time algorithm for computing discrete logarithms corresponds (heuristically) to the number of elements in the set $P_q = \mathrm{PGL}_2(\mathbb{F}_{q^2}) / \mathrm{PGL}_2(\mathbb{F}_q)$.

(i) Prove that for any integer $i \geq 1$, we have $\# \mathrm{PGL}_2(\mathbb{F}_{q^i}) = q^{3i} - q^i$. $\boxed{2}$

(ii) Show that $\# P_q = q^3 + q$. $\boxed{1}$

Exercise 5.3 (Filling a gap). (8 points)

Prove that there are $q + 1$ transformations $m \in \mathrm{PGL}_2(\mathbb{F}_{q^2}) / \mathrm{PGL}_2(\mathbb{F}_q)$ whose image sets of $\mathbb{P}^1(\mathbb{F}_q)$ contain two given points (say $(0 : 1)$ and $(1 : 0)$). $\boxed{8}$

Exercise 5.4 (Experimental science: On the heuristic). (0+14 points)

For the following task you might want to employ a computer algebra system of your choice. Consider the matrix $\mathcal{H}$ defined in the lecture. Its rows consist of incidence vectors of the image sets of $\mathbb{P}^1(\mathbb{F}_q)$ of all the $q^3 + q$ transformations $m \in \mathrm{PGL}_2(\mathbb{F}_{q^2}) / \mathrm{PGL}_2(\mathbb{F}_q)$.

(i) For $q = 3$ write down the matrix. Hint: You need to think about first which $m \in \mathrm{PGL}_2(\mathbb{F}_{q^2})$ you want to take, such that pairwise two of them do not differ by an element of $\mathrm{PGL}_2(\mathbb{F}_q)$ only! $\boxed{+6}$

(ii) Verify that the sum of all rows is the vector $(q^2+q, q^2+q, \ldots, q^2+q)$. $\boxed{+1}$

$\boxed{+1}$ (iii) Verify that the sum of all rows whose first coordinate is 1 is the vector $(q^2+q, q+1, \ldots, q+1)$.

$\boxed{+6}$ (iv) Now perform the following experiment: Randomly select q^2+1 rows and compute the rank (over $\mathbb{Z}$) of the resulting $(q^2+1) \times (q^2+1)$ matrix. What do you observe? Interpret your result.