Dr. Michael Reyer

Tutorial 9

Friday, January 11, 2019

Problem 1. *(Schnorr Identification Scheme)* Consider a Schnorr Identification Scheme with system parameters $p = 71$, $q = 7$, $\beta = 20$, $t = 2$. Suppose Alice chooses the private key $a = 5$, during the protocol the random number $r = 3$, and Bob issues the challenge $e = 4$.

a) Check that the parameters fulfill the requirements except for the sizes of p and q.

b) Compute the public parameter v.

c) Execute all steps in the protocol.

Problem 2. *(Threshold Cryptography)* There are four people $i = 1, \dots, 4$ working on a project. They want to allow to access the project only if all four people are together. A trusted authority (TA) applies the construction from the lecture for hiding a secret to get to the project and uses the polynomial over $\mathbb{F}_7$

$$q(X) = X^3 + 5.$$

a) What is the secret?

b) Help the TA. Determine appropriate partial information for all people such that only all of them may calculate the secret to access the project.

The TA has produced a new secret, (a new polynomial) and issued new pieces of information. The issued pieces are $(1, 6)$, $(2, 2)$, $(3, 5)$, and $(4, 0)$.

c) What is the secret?

Problem 3. *(Elliptic Curve Double-and-Add)* In analogy to the *Square-and-Multiply* algorithm in a ring $\mathbb{Z}_n$, the k-th multiple of P can be algorithmically computed based on doubling and addition on an elliptic curve over a field $\mathbb{F}_q$. You may use the binary representation of factor $k = (k_m, \dots, k_0)_2 = \sum_{i=0}^{m} k_i \, 2^i$.

a) Describe $45P$ in terms of doublings and additions of P only.

b) Formulate an *iterative Double-and-Add* algorithm $f_{\text{it}}(P, k)$ to calculate $k\,P$.

c) Give a *recursive* version $f_{\text{rec}}(P, k)$ of the above *Double-and-Add* algorithm.