Exercise 8  
Friday, December 22, 2017

Problem 1. *(Feige-Fiat-Shamir-signature)* Zero-knowledge-protocols can also be used to construct signature schemes. Construct a signature scheme from the Feige-Fiat-Shamir identification protocol by replacing the challenge \((b_1, ..., b_k)\) with a hash value \(h(m, x)\). Specify the signing and the verification algorithm.

Problem 2. *(zero-knowledge factorization)* James Bond (JB) wants to prove to the British secret service (MI5) that he knows the factorization of a composite number \(n\) without revealing the factors. These factors are two distinct primes \(p\) and \(q\) fulfilling the congruences \(p, q \equiv 3 \pmod{4}\). JB suggests the following protocol:

(i) The MI5 chooses an arbitrary quadratic residue \(y\) modulo \(n\), and sends \(y\) to JB.

(ii) JB computes the square root \(x\) of \(y\), and sends \(x\) to the MI5.

(iii) The MI5 checks whether \(x^2 \equiv y \pmod{n}\).

These steps are repeated 20 times. If JB can compute the square roots modulo \(n\) in all 20 attempts, the MI5 believes him.

a) Show that the MI5 can factor \(n\) with very high probability.

b) Does this protocol satisfy the requirements of a zero-knowledge protocol?

c) Is a third party able to derive useful information about the factorization of \(n\) by intercepting the communication between JB and the MI5?

Problem 3. *(working with elliptic curves I)* Consider the equation

\[ Y^2 = X^3 + X + 1. \]

a) Show that this equation describes an elliptic curve \(E\) over the field \(\mathbb{F}_7\).

b) Determine all points in \(E(\mathbb{F}_7)\) and compute the trace \(t\) of \(E\).

c) Show that \(E(\mathbb{F}_7)\) is cyclic and give a generator.