Dr. Michael Reyer

Tutorial 8

Friday, December 21, 2018

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. *(Zero Knowledge Protocol Example)* Consider the Zero Knowledge Protocol Example from the lecture. Let $n = p \cdot q$, $p \neq q$ primes. A selects random s, computes $y = s^2 \mod n$ with $\gcd(y, n) = 1$ and publishes y. The protocol is:

1. A chooses r_1, r_2 randomly with $r_1 \cdot r_2 \equiv s \pmod n$ by choosing r_1 with $\gcd(r_1, n) = 1$ and calculating $r_2 = s \cdot r_1^{-1} \mod n$. Let $x_1 = r_1^2 \mod n$ and $x_2 = r_2^2 \mod n$.
   $A \to B : (x_1, x_2)$. (Witness)
2. B checks if $x_1 \cdot x_2 \equiv y \pmod n$ and chooses x_1 or x_2 randomly. B asks A to supply a square root of it. (Challenge)
3. A sends the square root to B and B checks, if $r_1^2 \equiv x_1 \mod n$.

Discuss that the protocol works by particularly answering the following questions.

a) O does not know a square root of y modulo n. How should O produce a witness for B to maximize his chances? Why cannot O answer all potential challenges?

b) How often should this protocol be repeated to ensure that O has a success rate of less than 10^{-3}.

c) Why is it important that B checks $x_1 \cdot x_2 \equiv y \pmod{n}$?

d) What should A avoid while creating the random numbers r_1?

e) May O learn from listening to the protocol between A and B repeatedly.