AARHUS UNIVERSITY - COMPUTER SCIENCE

Protocol Theory - Handin 3

Peter Burgaard -201209175

February 22, 2017

EXERCISE 9

Prove the rewinding lemma. Does the results also hold for statistical and computational zero-knowledge.

LEMMA 3.1 *The rewinding lemma: Let (P, V) be a proof system for language L, and let M be a perfect honest-verifier simulator for (P, V). Assume that conversations have the form (a, b, z), where P sends a, V responds with a random bit b, and P replies with z. Then (P, V) is perfect zero-knowledge.*

We say that a prover P and a Verifier V for a language L is **HVZK** if there exists a polynomial time simulator M, which $\forall x \in L$ outputs a transcript (a, b, z), which will have the same probability distrubtion as the honest P, V on a input $x \in L$.

We define our simualtor M as follows:

1. The verifier is given the input x, maybe some auxiliary input, and the random input bits
2. Simulation of a iteration is as follows
   a) Draw a uniform random challenge c and response z, and compute a from these, and send the commitment to the verifier V
   b) We receive challenge b from V. If $c = b$ then it outputs (a, b, z) and we exit the loop, else reset V to the state right after step 1, and we'll start the simulation over from step 2.a.

Assume we're given a malicious verifier V^*, we have to be able to perfectly simulate a conversation between P and V^* using our simulation as subroutine. This means we will prove **ZK**, since our V^* is malicious.

Since V^* is malicious we have no idea how it will choose its challenge b^*. It might well, not be uniformly chosen and therefor dependent on maybe the initial message a. So we use our simulation M to "guess" the b^* in advance and chose c, and compute matching a and z for it. If we receive $b^* = c$, then M finishes the transcript succefully, otherwise it restarts anew.

We should be able to design our M in such a fashion that, if $x \in L$, we choose a such a way, we don't reveal any information about which answer we have prepared. This would mean $P(b = c) = \frac{1}{2}$, and M should succed after expected 2 tries, (polynomial). This gives us a transcript in polynomial time which statistically close to that of P and V^*, with the difference being the negligible, in the chance of M failling being 2^{-n} in n tries, which is were M "mis-guesses" all of its tries.