Cryptography & Complexity

Spring 2005 - Home exercise #4

Instructor: Dr. Erez Petrank, T.A.: Benny Appelbaum

Exercise 4 on the web: http://www.cs.technion.ac.il/~erez/courses/cc/ex4.pdf

Question 1:

Provide (computational) zero-knowledge interactive proofs for the following NP-Complete language. Do not use reductions to other NP-Complete languages, but provide "direct" interactive-proofs for the languages in the question.

- Vertex-Cover = { (G,k) : Graph G has a vertex cover of size at most k }

Prove that you provided an interactive proof for the language, and then provide an efficient simulator and argue that it simulates the interactive proof.

Question 2:

Show that it is possible to construct a bit commitment scheme from a psuedo-random bit generator. This implies that bit commitment may be constructed from any one-way-function. Guidance:

1. Use a simulator G that expands strings of length n to strings of length 3n.
2. The commitment phase is interactive. First, the receiver chooses uniformly at random a string r in $\{0,1\}^{3n}$ and sends r to the sender. The sender then picks a random string s in $\{0,1\}^{n}$. To commit on the bit 0, the sender sends G(s). To commit on 1, the sender sends G(s)+r, where + denotes bitwise exclusive or.
3. To reveal, the sender sends s to the receiever and the receiver verifies that the commitment was correct.
4. Prove that if the output of the pseudo-random generator is pseudo-random, then no efficient receiever R* can distinguish between a commitment on 0 and a commitment on 1.
5. Prove that there is a negligible fraction of the possible r's in $\{0,1\}^{3n}$ that allow the sender to send a commitment that it can later open both as 0 and as 1.

Question 3:

Prove that the existence of bit commitment schemes implies the existence of one-way functions.