Foundations of Cryptography : Home assignment (submission date 30/9/2008)

Teacher: Ronen Shaltiel

July 29, 2008

Instructions

General:

- You must hand in printed solutions. (I'm willing to accept calculations in handwriting if you don't know how to print them but the rest must be printed).
- Please write clearly and precisely!
- I will not accept solutions that are longer than 10 pages.

Rules:

- This is a test! You are not allowed to collaborate with other people and must do the work on your own. For some of the questions it may be the case that there are solutions on-line. Don't use them!
- Please include in your submission a **signed statement** saying that: I (*include name and ID*) hereby declare that I did not discuss this project with any other people and the solution that I am submitting is my own work. If you submit electronically (which is preferred) make sure to place such a statement in my mailbox. Note that I may want to set up a date in which I will spend 10-20 minutes with every student and have him explain his solutions to me.

Relevant material: You are encouraged to read the relevant topics in the two references that appear in the course's webpage. Specifically, if you are not sure regarding precise definitions you can find them in any of these two references.

Grading:

- There are 9 questions and you are supposed to answer only 4 of them. Each question i comes with two numbers (a_i, b_i). The final score will be given by summing the a_i's of the questions you answer to compute a, summing the b_i's of the questions you answer to compute b and the final score is $min(a, 70) + b$.
- Write clear and full answers! A 10 point bonus will be given to submissions which are clear and well written.
- You are allowed to answer one additional question over the 4 questions required (that is you can answer 5 questions), and I will base the scoring on the best 4 questions.

Good Luck!

Definitions:

In this section I include definitions for concepts that *were not* defined in class and appear in the questions below.

Definition 1 (Honest verifier zero knowledge)**.** *We say that an interactive proof system (P, V) is* honest verifier zero knowledge *for a language L if there exists a probabilistic polynomial time machine S such that for every sufficiently large n, and every input $x \in L$ of length n:*

$$(P, V)(x) \equiv_c S(x)$$

Questions:

1. $(18, 0)$ Prove that there does not exist a function f such that both f and f^{-1} are OWP.

2. $(22, 0)$ Let $X = \{X_n\}$ be an ensemble such that X_n is a random variable that takes values in $\{0,1\}^n$. Assume that X is a pseudorandom ensemble. Let $f : \{0,1\}^* \to \{0,1\}^*$ be a polynomial time computable length preserving function (that is $|f(x)| = |x|$). Let $Y = \{Y_n\}$ be the ensemble defined by $Y_n = f(X_n)$. Let $Z = \{Z_n\}$ be the ensemble defined as follows: Z_n is the random variable in which we choose a string $a \in \{0,1\}^n$ uniformly at random and set $Z_n = f(a)$. Show that $Y \equiv_c Z$.

3. Let f be a one-way function. Define f' as follows. When given a string x of length $2n$ think about it as two strings x_1, x_2 and define $f'(x) = 0^n \circ f(x_1)$.

   - $(20, 2)$ Show that f' is a one-way function.
   - $(5, 3)$ In class we gave a construction of pseudorandom generators from any one-way permutation f. Show that assuming that there exists a one-way function f, there also exists a one-way function f' such that if we apply the construction of pseudorandom generators that we saw in class (say for stretch $\ell(n) = 10n$) then what we get is not a pseudorandom generator.

4. (Candidate Generators) Let G_1 and G_2 be polynomial time computable functions with stretch $\ell(n) = n^2$. Suppose that G_1 is a pseudorandom generator and G_2 is an arbitrary function that may (or may not) be a pseudorandom generator. Define a function G' as follows: When given a string x of length $2n$ think about it as two strings x_1, x_2 each of length n and define $G'(x) = G_1(x_1) \oplus G_2(x_2)$ (here $y_1 \oplus y_2$ means that we take strings y_1, y_2 and compute the exclusive or in a bit-wise fashion).

   - $(20, 2)$ Show that for every function G_2 the function G' is a pseudorandom generator.
   - $(5, 3)$ Let f_1, f_2 be two length preserving functions. Suppose that we know that one of them is a OWP, we don't know which one is a OWP and the other function may be any permutation. Show how to construct a pseudorandom generator that stretches $2n$ bits to n^2 bits.

5. Let G be a pseudorandom generator with stretch function $\ell(n) = 2n$. Define $G'(x)$ as follows. When given a string x of length n^2 think about it as n strings $x_1, \ldots, x_n$ each of length n and define $G'(x) = G(x_1) \circ G(x_2) \circ \ldots G(x_n)$.

   - $(20, 10)$ Show that G' is a pseudorandom generator. (Hint: use the technique of hybrids that we developed when we constructed pseudorandom generators).
   - $(5, 0)$ What is the stretch function of G'?

6. (ZK proof for Clique). Consider the language

$$L = \{G : G \text{ is a graph that has a clique that contains at least half the vertices}\}$$

The goal of this question is to design an interactive proof system for L that is zero knowledge *directly*. That is without relying on the fact that $L \in NP$. We will use the assumption that there exist one-way permutations. (Hint: the protocol I have in mind resembles the one for Graph Hamiltonicity).

- $(20, 5)$ Design an interactive proof system for L with completeness 1 and soundness $1/2$ and show that it is honest verifier zero knowledge.
- $(5, 5)$ Explain how to modify the construction of your simulator to show that the protocol is zero knowledge. Give a high level explanation why your simulator works. (It is not necessary to give a detailed formal proof).

7. (Parallel repetition of ZK with an honest verifier) In class we showed an interactive proof system for *Hamiltonian Cycle* and showed that it has completeness 1, soundness 1/2 and Zero Knowledge assuming the existence of one-way permutations.

- $(10, 0)$ Consider the protocol (P', V') which on input x of length n repeats the protocol (P, V) n times *in parallel*. Describe this protocol (what does each party sends at every step?)
- $(15, 12)$ Show that this protocol is honest verifier zero knowledge. Does your proof works for any verifier V^*?

8. Consider the following attempt at constructing a bit-commitment protocol from a OWP f. In the commit phase the committer has a bit b that he wants to put in the box. He chooses at random a string r of length n such that the first bit of r equals b and then sends $m = f(r)$ as the "box". In the reveal phase the committer sends r and the receiver checks that $f(r) = m$ and decides that b is the first bit of r.

   $(25, 15)$ Show that if there exists a OWP then there exists a OWP f such that following the commit phase the receiver can know what is the bit b.

9. Let f_1, f_2 be two length preserving polynomial time computable functions. Define $g(x) = f_2(f_1(x))$. Which of the following statements are true? Prove your answers.

- $(10, 2)$ If f_1, f_2 are both one-way functions then g is a OWF.
- $(10, 8)$ If f_1 is a OWP then g is a OWP for any choice of f_2 that is a permutation (but not necessarily one-way).
- $(10, 10)$ If f_2 is a OWP then g is a OWP for any choice of f_1 that is a permutation (but not necessarily one-way).