Foundation of Cryptography, Spring 2013 Iftach Haitner

Problem set 3

June 1, 2013 Due: June 4

- Please submit the handout in class.
- Write clearly and shortly using sub claims if needed. The emphasize in most questions is on the proofs (no much point is writing a "solution" w/o proving its correctness)
- For Latex users, a solution example can be found in the course web site.
- In case you work in (small) groups, please write the id list of your partners in the solution file. I stress that each student should write his solution by *himself* (joint effort is only allowed in the "thinking phase")
- The notation we use appear in the first lecture (www.cs.tau.ac.il/∼iftachh/Courses/FOC/Fall11/Slides/OWF.pdf), section "Notation"

Exe 1, CRH to OWF. (10 points) Prove that the existence of collision-resistance hash function family (definition 12, lecture 5) implies the existence of one-way functions.

Exe 2, Birthday paradox (10 points). Prove that $\mathsf{Pr}_{\pi \leftarrow \Pi_n}[\exists x \neq x' \in \mathcal{S} \colon \pi(x) = \pi(x')] \in \Omega(1)$, where $\mathcal{S} \subset \{0,1\}^n$ is of size $2^{n/2}$ (n is a power two).

You might find the following inequality useful: $e^{-x} \geq (1-x)$ for $x \in [0,1]$

Exe 3, Interactive Proofs, Goldreich, Chapter 5, exe 2, (10 points) Prove that if $\mathcal{L}$ has an interactive proof system with *deterministic* verifier, then $\mathcal{L} \in$ NP.

Guideline: note that if the verifier is deterministic, then the entire interaction between the prover and verifier can be determined by the prover.

Exe 4, Zero knowledge (10 points) Prove that the interactive proof presented in class for graph non-isomorphism is *honest-verifier* perfect zero-knowledge (i.e., the ZK definition is restricted to $\mathsf{V}^* = \mathsf{V}$).

Bonus (5 points): Is the above protocol (full fledged) zero knowledge? justify your answer as good as you can.