Foundation of Cryptography, Spring 2013 | Iftach Haitner

Problem set 4

June 5, 2013 | Due: June 18

- 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, One-message ZK proof. (10 points) Prove Claim 1 in Lecture 7: Assume that $\mathcal{L} \subseteq \{0,1\}^*$ has a *one-message* ZK proof (even computational), with standard completeness and soundness,[1] then $\mathcal{L} \in \text{BPP}$.

Bonus*: prove the above for 2-message protocols.

[1] That is, the completeness is $\frac{2}{3}$ and soundness error is $\frac{1}{3}$.