Foundation of Cryptography, Fall 2016 Beny Applebaum and Iftach Haitner

Problem set 5

January 5, 2017 Due: January 19

- Please submit the handout in class, or email me, in case you write in LaTeX.
- 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.
- It is ok to work in (small) groups, but please write the id list of your partners in the solution file, and each student should write her solution by *herself* (joint effort is only allowed in the “thinking phase").
- The notation we use appears in the introduction part of the first lecture (*Notation* section).

1. Prove Claim 1 in Lecture 7.

2. Assuming trapdoor permutation, construct an adaptively secure NIZK for Hamiltonicity. Prove your answer. Hint: Amplify the soundness of the protocol described in class, and show that the resulting protocol is adaptive NIZK.

3. Prove that any $\mathcal{CZK}$ protocol is also WI (Witness Indistinguishability). See definition in Slide 3 of Lecture 7.