Foundation of Cryptography, Fall 2016 Beny Applebaum and Iftach Haitner

Problem set 4

December 31, 2016 Due: January 5

- 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. The question is about the signature scheme described in Construction 32, of Lecture 5.

   Does the construction remain secure when $\boldsymbol{r}$ is set to $g(m)$ (rather than to $\pi(h(m))_{1,\ldots,n}$), where g is part of the singing key, and chosen at random by Gen' from a family of pair-wise independent hash functions from $\{0,1\}^*$ to $\{0,1\}^n$?

   $*$ The random function π is still used for generating the randomness for Gen, in Step 1.1.

2. Prove that if $\mathcal{L}$ has an interactive proof system with *deterministic* verifier, then $\mathcal{L} \in \mathcal{NP}$.

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

3. 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 $\mathsf{V}^* = \mathsf{V}$).

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

4. The question is about the $\mathcal{CZK}$ protocol for $3\mathrm{COL}$ presented in class (Protocol 20 of Lecture 6). Explain how to modify the Simulator given in class, so that the resulting simulator handles also aborting verifiers.