Foundation of Cryptography, Fall 2010 — Ran Canetti and Iftach Haitner

Problem Set 4

January 27, 2011 — Due: February 17

Section 4.4.2 in Goldreich's book (Volume I) and the following two scribe notes could be a useful read towards solving this problem set.

`http://www.cs.tau.ac.il/~ canetti/f09-materials/f09-scribe3.pdf`
`http://www.cs.tau.ac.il/~ canetti/f08-materials/scribe11.pdf`

1. (a) [**30 points**] Prove that no commitment scheme can be both perfectly binding and perfectly hiding.

   (b) [**Bonus: 30 points**] Extend the proof in 1(a) to show impossiblity of commitment schemes that are both *statistically binding* and *statistically hiding.*

2. Consider the basic Blum protocol for Graph Hamiltonicity (Section 3.4 in the second notes), where the commitments are instantiated with Pedersen commitments (see first scribe notes, Section 2.4.2).

   (a) [**30 points**] Show that this protocol is statistical zero knowledge. (Bonus 10 points: Show that this protocol is in fact *perfect* zero knowledge.)

   (b) [**40 points**] Show that the protocol is **computationally sound** with soundness error $1/2 + \nu(n)$, where $\nu()$ is a negligible function, under the Discrete Log assumption in the group G used for the Pedersen commitments.

   (c) [**Bonus: 50 points**] Let n be the input length, and consider the n-fold sequential composition of the basic Blum protocol. That is, the basic three-message protocol is repeated sequentially n times, where the verifier uses fresh random coins for each instance of the basic protocol, and accepts only if all n instances accept. Show that this protocol is a proof of knowledge (see Section 3.6 of the second scribe notes), under the Discrete Log assumption in G.