Foundation of Cryptography (0368-4162-01), Spring 2014 Iftach Haitner

Final Exam, Moed B

1.9.2014

Time Limit: 3 hours
Instructions:

- The exam is with open books — you might use any written material.
- Please write clearly, and prove your answers. In case you are using an unproven “fact", please state the fact clearly, and explain why you are not proving it (“lack of time",“easy to see", etc.).
- There are three questions, each contributes up to 33 points (hence, the minimal grade is 1).

Good Luck!

1. Given two function families $\mathcal{F}$ and $\mathcal{G}$, let $\mathcal{F} \oplus \mathcal{G}$ be the function family $\{(f,g) \in \mathcal{F} \times \mathcal{G}\}$, where $(f,g)(x) := f(x) \oplus g(x)$.

   Let $\mathcal{F} = \{\mathcal{F}_n \colon \{0,1\}^n \mapsto \{0,1\}^n\}_{n\in\mathbb{N}}$ and $\mathcal{G} = \{\mathcal{G}_n \colon \{0,1\}^n \mapsto \{0,1\}^n\}_{n\in\mathbb{N}}$ be two efficient, length-preserving function ensembles (i.e., each $f \in \mathcal{F}_n$ maps strings of length n to strings of length n). Prove that if $\mathcal{F}$ or $\mathcal{G}$ (or both) is a PRF, then $\mathcal{F} \oplus \mathcal{G} := \{\mathcal{F}_n \oplus \mathcal{G}_n\}_{n\in\mathbb{N}}$ is a PRF.

   Hint: consider the function families $\mathcal{F} \oplus \Pi := \{\mathcal{F}_n \oplus \Pi_n\}_{n\in\mathbb{N}}$ and $\mathcal{G} \oplus \Pi := \{\mathcal{G}_n \oplus \Pi_n\}_{n\in\mathbb{N}}$, where Π_n is as in (a.).

2. (a) Give an example of an encryption scheme that has indistinguishable encryptions in the public-key model, and is *not* CPA secure.

   (b) Give an example of a CCA1-secure public-key encryption scheme, that is *not* CCA2-secure.

3. Consider the following definition of "part-wise" zero-knowledge proof.

   Definition 1 (part-wise $\mathcal{ZK}$)**.** *An interactive proof* (P,V) *is* part-wise zero-knowledge proof *for* $\mathcal{L}$*, if for any* PPTM V^* *there exist two* PPTM*'s* S_1 *and* S_2 *such that* $\{\langle(\mathsf{P},\mathsf{V}^*)(x)\rangle_{\text{trans}}\}_{x\in\mathcal{L}} \approx_c \{\mathsf{S}_1(x)\}_{x\in\mathcal{L}}$*, and* $\{\langle(\mathsf{P},\mathsf{V}^*)(x)\rangle_{\mathsf{rand}}\}_{x\in\mathcal{L}} \approx_c \{\mathsf{S}_2(x)\}_{x\in\mathcal{L}}$*, where* e_{trans} *is the communication transcript of the execution* e*, and* e_{rand} *are* V^**'s random-coins used in* e*.*

   Is any part-wise zero-knowledge proof is also computational zero-knowledge according to definition given in class? Prove your answer.