Foundation of Cryptography (0368-4162-01), Fall 2016 Applebaum and Haitner

Final Exam

28.02.2017

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. Best two contribute 40 points each, and the lesser one contributes 20 points.

Good Luck!

1. Let $f\colon \{0,1\}^n \mapsto \{0,1\}^n$ be a (length-preserving) polynomial-time computable function.

   Prove/disprove each of the following statements:

   (a) If $\Pr_{y \leftarrow U_m}[\mathsf{A}(y) \in f^{-1}(y)] = \operatorname{neg}(n)$ for any PPT A, then f is one-way.

   (b) If f is one-way, then $\Pr_{y \leftarrow U_m}[\mathsf{A}(y) \in f^{-1}(y)] = \operatorname{neg}(n)$ for any PPT A.

2. For a function ensemble $\mathcal{F} = \{\mathcal{F}_n\colon \{0,1\}^n \mapsto \{0,1\}^n\}$, let $\mathcal{F}^2 = \{\mathcal{F}_n^2\colon \{0,1\}^{2n} \mapsto \{0,1\}^{2n}\}$ be the function ensemble in which each function $g \in \mathcal{F}_n^2$ is associated with a pair of functions (f_1, f_2) of $\mathcal{F}_n$, and for $x_1, x_2 \in \{0,1\}^n$:

$$g(x_1, x_2) = (f_1(x), f_2(x_2)).$$

   Let $\mathcal{F} = \{\mathcal{F}_n\colon \{0,1\}^n \mapsto \{0,1\}^n\}$ be a PRF, prove/disprove each of the following statements:

   (a) $\mathcal{F}^2$ is a PRF (over the domain $\{0,1\}^{2n}$).

   (b) Let Π_n be the family of all functions from n-bits to n-bits, then $\mathcal{F}^2$ is "indistinguishable" from Π_n^2. That is,

$$\Big| \Pr_{g \leftarrow \mathcal{F}_n^2}[\mathsf{D}^g(1^n) = 1] - \Pr_{\pi \leftarrow \Pi_n^2}[\mathsf{D}^\pi(1^n) = 1] \Big| = \operatorname{neg}(n)$$

   for any oracle-aided PPT D.

3. Assuming the existence of one-way functions, prove each of the following statements:

   (a) There exists an encryption scheme that has indistinguishable encryptions in the private-key model under CPA attack, but not under CCA**2** attack.

   (b) There exists an encryption scheme that has indistinguishable encryptions in the private-key model under CPA attack, but not under CCA**1** attack.