Foundation of Cryptography (0368-4162-01), Fall 2011 — Iftach Haitner

Problem set 3. Exercises 6

December 6, 2011 — Due: Dec 18

- Send your solutions in a PDF format to foc.exc@gmail.com.
- Solution for each exercise should be emailed *separately*, title: Exe # (e.g., 3), Id (Israel id) (write the same details in the body of the attached file).
- Please *don't* write your name in the email/attached file.
- 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.
- In case you work in (small) groups, please write the id list of your partners in the solution file. I stress that each student should write his solution by *himself* (joint effort is only allowed in the "thinking phase")
- The notation we use appear in the first lecture (www.cs.tau.ac.il/∼iftachh/Courses/FOC/Fall11/Introduction_admin.pdf), section "Notation"

Exe 6

- **a. Proving proposition 9 in Lecture 4 (3 points):** The *view* of random algorithm in a given execution, consists of its input and random coins. In case of an oracle-aided algorithm, this view contains also the answers to its oracle calls.[1]

  Let D be an oracle-aided algorithm making queries in $\{0,1\}^n$. Let Π_n be the set of all functions from $\{0,1\}^n$ to $\{0,1\}^n$, and let D^{Π_n} be the distribution induced by D's view, given oracle access to a uniformly chosen $\pi \in \Pi_n$ (D's coins are chosen at random). Let B be an interactive algorithm that on message (i.e., query) $q \in \{0,1\}^n$, returns a random value in $\{0,1\}^n$ if q was not asked before, and returns the same answer otherwise, and let D^{B} be the distribution induced by D's view, given "oracle access" to B (the coins of D and B are chosen at random).[2] Prove that D^{Π_n} and D^{B} are equivalent.

- **b. PRF combiner (7 points):** 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.).

[1] We omit the (oracle) queries form the view, since they are determined by the other values.

[2] That is, D's questions are forwarded to B, and B's answers are sent back to D as the oracle answers.