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

Problem set 2. Exercises 4–5

November 21, 2011 Due: Dec 4

- 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. Each student, however, should write his solution by *himself* (joint effort is only allowed in the "thinking phase")
- The notation we use appears in the first lecture (www.cs.tau.ac.il/∼iftachh/Courses/FOC/Fall11/Introduction_admin.pdf), section "Notation"

Exe 4 a. (5 points) Let $\{X_n\}_{n\in\mathbb{N}}$ be a Boolean distribution ensemble (i.e., $\mathrm{Supp}(X_n) = \{0,1\}$ for every n), let $\varepsilon : \mathbb{N} \mapsto [0,1]$ and let A be a PPT such that

$$\mathsf{Pr}_{x\leftarrow X_n}[\mathsf{A}(1^n) = x] \geq \frac{1}{2} + \varepsilon(n)$$

for every $n \in \mathbb{N}$. Prove that there exists a PPT B such that

$$\mathsf{Pr}_{x\leftarrow X_n}[\mathsf{B}(1^n, x) = 1] - \mathsf{Pr}_{x\leftarrow\{0,1\}}[B(1^n, x) = 1] \geq \varepsilon(n),$$

for every $n \in \mathbb{N}$.[1]

b. (5 points) Let $f\colon \{0,1\}^n \mapsto \{0,1\}^n$ be a one-way function. Prove that for any PPT A, it holds that

$$\mathsf{Pr}_{x\leftarrow\{0,1\}^n, i\leftarrow[n]}\left[\mathsf{A}(f(x), i) = x[i]\right] \leq 1 - \frac{1}{2n^2},$$

for large enough $n \in \mathbb{N}$, where $x[i]$ is the i'th bit of x.

Exe 5 (10 point) Prove Claim 18 in lecture 2.

[1] Both probabilities are also over the algorithms' random coins.