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

# Problem set 4. Exercises 7-9

*December 22, 2011* Due: January 5

- 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/Slides/OWF.pdf), section "Notation"

**Exe 7 (10 points):** Let $g\colon \{0,1\}^n \mapsto \{0,1\}^{3n}$ be a PRG and consider the following commitment scheme:

**Protocol 1** $((\mathsf{S},\mathsf{R}))$**.**
***Commit stage:***

**Common input:** $1^n$

**S's input:** $b \in \{0,1\}$

**Commit:**

1. R *chooses* $r \leftarrow \{0,1\}^{3n}$ *and sends it to* S
2. S *chooses* $x \leftarrow \{0,1\}^n$*. Sends* $c = g(x)$ *to* S *in case* $b = 0$*, and* $c = g(x) \oplus r$ *otherwise.*

***Reveal stage:***

**Common input:** $1^n$ *and* $r, c \in \{0,1\}^{3n}$

**S's input:** $b \in \{0,1\}$ *and* $x \in \{0,1\}^{3n}$.

S *sends* $(b,x)$ *to* R*, and* R *accepts iff* $(b,x)$ *is consistent with* $r$ *and* $c$ *(i.e.,* $c = g(x)$ *in case* $b = 0$*, and* $c = g(x) \oplus r$ *otherwise).*

Prove the the above scheme is statistically-binding and computationally-hiding (bit) commitment scheme.

Hint: for the binding part, prove that for most fixing of $r$, the scheme is *perfectly* binding.

**Exe 8, (10 points):** Prove Claim 1 in Lecture 6.

**Exe 9, (10 points):** Prove the ZK part of Claim 12 in Lecture 6. That is, assuming that $\mathsf{S}_H$ is a good simulator for $\mathcal{L}$ in the hidden bit model (HBM), and that $b$ is an hardcore predicate for the family $(G, f, \mathsf{Inv})$,[1] then S of Algorithm 13 is a good simulator for $\mathcal{L}$ in the standard model (according to Definition 2).

Recall that in the HBM, we require that $\{(x, \{c_i\}_{i\in\mathcal{I}}, \pi_H, \mathcal{I})_{c\leftarrow\{0,1\}^{p(|x|)},(\pi_H,\mathcal{I})\leftarrow \mathsf{P}_H(x,c)}\}_{x\in\mathcal{L}} \approx_c \{x, \mathsf{S}_H(x)\}_{x\in\mathcal{L}}$, where the set $\{c_i\}_{i\in\mathcal{I}}$ is ordered (i.e., given as ordered list $c_{i_1}, \ldots, c_{i_k}$, where $i_j$ is the $j$'th smallest element in $\mathcal{I}$) and $p \in$ poly is a parameter of the proof system.

[1] I.e., for any PPT A and $p \in$ poly, it holds that $\mathsf{Pr}_{sk\leftarrow\{0,1\}^n, pk=G(sk), x\leftarrow\{0,1\}^n}[\mathsf{A}(pk, f(pk,x)) = b(x)] < \frac{1}{2} + \frac{1}{p(n)}$ for large enough $n$.