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

# Problem set 5. Exercises 10-11

*January 4, 2012* Due: January 16

- 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 10**

**a. (5 points):** Prove Claim 14 in Lecture 7.

**b. (5 points):** Prove Claim 35 in Lecture 7. You can use the fact that the existence of OWFs yield that of one-time length-restricted signature schemes, and that of an efficient target collision-resistant family $\mathcal{H} = \{\mathcal{H}_n \colon \{0,1\}^* \mapsto \{0,1\}^n\}$.

**Exe 11**

**a. (7 points):** Prove Claim 37 in Lecture 7.

**b. (3 points):** Is the converse true? Namely, is any random one-time existential unforgeable signature scheme also target one-time existential unforgeable?