0368.4162 Foundations of Cryptography Fall 2017 Nir Bitansky

Final Exam, Moed B

March 28 2018

Duration: 3 hours.

Structure: 3 questions, 2 items each.

Grading: Each item is worth 17 points. Grades above 100 will be rounded to 100.

Instructions:

- You can use any written materials.
- You can use statements shown in the lectures or home assignments as long as you state them clearly.
- If you don't know the answer, you can write "I don't know" and you will get 5/17 points.
- Write in any language you wish, but write clearly.
- Recommendation: each answer (including both items) shouldn't take much longer than half a page.

1. In the following question, let $f : \{0,1\}^* \to \{0,1\}^*$ be a one-way function and let $\langle \cdot, \cdot \rangle$ denote the inner product modulo 2. Prove the following statements or give a counter example:

   (a)
   $$\{f(x), r_1, r_2, \langle x, r_1 \rangle, \langle x, r_2 \rangle\}_{n \in \mathbb{N}} \approx_c \{f(x), r_1, r_2, u_1, u_2\}_{n \in \mathbb{N}} \ ,$$
   where x, r_1, r_2 are each sampled uniformly and independently from $\{0,1\}^n$, and u_1, u_2 are uniform and independent bits.

   (b)
   $$\{f(x), r_1, \dots, r_{2n}, \langle x, r_1 \rangle, \dots, \langle x, r_{2n} \rangle\}_{n \in \mathbb{N}} \approx_c \{f(x), r_1, \dots, r_{2n}, u_1, \dots, u_{2n}\}_{n \in \mathbb{N}} \ ,$$
   where $x, r_1, \dots, r_{2n}$ are each sampled uniformly and independently from $\{0,1\}^n$, and $u_1, \dots, u_{2n}$ are uniform and independent bits.

2. Let (E, D) be a CPA-secure secret-key bit-encryption scheme. Assume there exists a PPT algorithm R so that for any $sk \in \{0,1\}^n$, any $b \in \{0,1\}$, and any randomness $r \in \{0,1\}^n$ for the encryption algorithm E, the distribution $R(E_{sk}(b; r))$ is identical to $E_{sk}(b; U_n)$, where U_n denotes the uniform distribution. (In other words, R is perfectly rerandomizes any ciphertext).

   (a) Consider the following candidate (G', E', D') for a public-key bit-encryption scheme:
      - $G'(1^n)$ outputs (sk, pk) where $sk \leftarrow \{0,1\}^n$ and $pk = (ct_0, ct_1)$ where $ct_b \leftarrow E_{sk}(b)$.
      - $E'_{pk}(b)$ outputs $ct' \leftarrow R(ct_b)$.
      - $D'_{sk}(ct') = D_{sk}(ct')$.

      Prove that (G', E', D') is a secure public-key bit encryption, or give a counter example.

   (b) Construct from (E, D, R) a two-message $(1, 2)$-oblivious-transfer against semi-honest adversaries. No need to prove its security.

3. Let L be an NP language and for every $x \in L$, denote by $W(x)$ its set of valid witnesses.
   An interactive proof (P, V) is witness-indistinguishable if for any non-uniform PPT malicious V^*
   $$\{(P(w_0), V^*)(x)\}_{x \in L, w_0, w_1 \in W(x)} \approx_c \{(P(w_1), V^*)(x)\}_{x \in L, w_0, w_1 \in W(x)} \ ,$$
   where for any $x \in L$ and $w \in W(x)$, $(P(w), V^*)(x)$ denotes an interaction with common input x, and prover additional input w.
   Prove or give a counter example for each of the following statements:

   (a) If an interactive proof (P, V) is zero knowledge then it is also witness indistinguishable.

   (b) If an interactive proof (P, V) is witness indistinguishable, then so is its two-fold repetition $(P^{\otimes 2}, V^{\otimes 2})$.
   In the two-fold repetition of a protocol, the original protocol is executed twice in parallel on the same inputs x, w, but with independent randomness.