0368.4162 Foundations of Cryptography Fall 2017 Nir Bitansky

Final Exam, Moed B, Solution

March 28 2018

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.

   Solution: We argue that
   $$f(x), r_1, r_2, \langle x, r_1\rangle, \langle x, r_2\rangle \approx_c f(x), r_1, r_2, \langle x, r_1\rangle, u_2 \approx_c f(x), r_1, r_2, u_1, u_2 \ .$$
   For the first indistinguishability, note that x is unpredictable from $(f(x), r_1, \langle x, r_1\rangle)$ (note that an adversary could just guess $\langle x, r_1\rangle$ with probability half). Thus, indistinguishability follows by applying the Goldreich-Levin lemma. The second follows from the fact that x is unpredictable from $f(x), r_2, u_2$, and again the GL lemma.

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

   Solution: For any OWF, the two are distinguishable — we can efficiently invert $f(x)$ in the left distribution, whereas we cannot on the right. Specifically, with overwhelming probability $r_1, \ldots, r_{2n}$ contain n linearly independent vectors, and we can thus obtain x.

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.

   Solution: To see that the scheme is secure, consider a fake public key $\widetilde{pk} = (\widetilde{ct}_0, \widetilde{ct}_1)$ where both ciphertexts are sampled as encryptions of zero. Then, by the CPA security $\widetilde{pk} \approx_c pk$, and thus it suffices to show that $\widetilde{pk}, E'_{\widetilde{pk}}(0) \approx_c \widetilde{pk}, E'_{\widetilde{pk}}(1)$. This holds since both $E'_{\widetilde{pk}}(0)$ and $E'_{\widetilde{pk}}(1)$ are rerandomizations of encryptions $\widetilde{ct}_0, \widetilde{ct}_1$ and are thus distributed identically (as $E_{sk}(0, U_n)$).

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

Solution: The receiver $R(b)$ samples two public keys (pk_0, pk_1). pk_b is a real public key, sampled using G' and pk_{1-b} is a fake public key sampled as $\widetilde{pk}$ above. The sender $S(\sigma_0, \sigma_1, (pk_0, pk_1)$ sends encryptions $E'_{pk_0}(\sigma_0), E'_{pk_1}(\sigma_1)$.

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.

Solution: Both distributions are indistinguishable from the same simulated distribution $S(x)$ (which doesn't depend on any witness) and are thus indistinguishable from each other.

(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.

Solution: This statement follows from a simple hybrid argument. Concretely consider the distribution where the first proof is given using the first witness, and the second is given using the second witness. Then by the witness indistinguishability property this hybrid distribution is indistinguishable from both the distribution where both proofs use the first witness as from the distribution where both use the second witness.