0368.4162 Foundations of Cryptography November 2, 2017

Problem Set 1

Due: November 16

Instructions:

- Type your solution and email it to me. Include FOCF17HW in the subject. You're encouraged to do so in latex. You can find on the webpage the assignment's tex file to help you.
- You can cooperate. However, you should write the solution by yourself, and list all collaborators for each question. Same goes for any external sources that you may use.
- Do not discuss solutions over the course's forum. You are more than welcome though to ask for clarifications regarding the questions themselves.

1. (25 pts) In class, we saw that for any encryption scheme (E, D) for messages of length ℓ, with keys of length $n \leq \ell - 10$, if E is deterministic, there exist two messages m_0, m_1 and an inefficient A such that

$$\Pr\left[A(ct) = m_b \;\middle|\; \begin{array}{l} sk \leftarrow \{0,1\}^n \\ b \leftarrow \{0,1\} \\ ct \leftarrow E_{sk}(m_b) \end{array} \right] > 0.99 \ .$$

   Show that the same holds even if E also tosses, say n, coins (on top of the key). That is, an encryption of any message $m \in \{0,1\}^\ell$ is drawn from a distribution $\{ct \mid sk \leftarrow \{0,1\}^n, r \leftarrow \{0,1\}^n, ct = E_{sk}(m;r)\}$.

2. In this question, let X_0, X_1 be two distributions with the same finite support S. Recall that:

$$\Delta_A(X_0, X_1) := \left|\Pr\left[A(X_0) = 1\right] - \Pr\left[A(X_1) = 1\right]\right| \ .$$

   (a) (15 pts) Show that for any function A (efficient or not):

$$\left|\Pr\left[A(x) = b \;\middle|\; \begin{array}{l} b \leftarrow \{0,1\} \\ x \leftarrow X_b \end{array} \right] - \frac{1}{2}\right| = \frac{\Delta_A(X_0, X_1)}{2} \ .$$

   (b) (15 pts) Show that

$$\max_A \Delta_A(X_0, X_1) = \frac{1}{2}\sum_{x \in S} \left|\Pr\left[X_0 = x\right] - \Pr\left[X_1 = x\right]\right| = \max_{T \subseteq S} \left|\Pr\left[X_0 \in T\right] - \Pr\left[X_1 \in T\right]\right| \ .$$

   (c) (15 pts) let A be a randomized distinguisher that uses n random coins. That is, $A(x;r)$ is given a sample x and a random string $r \leftarrow \{0,1\}^n$ (and as usually outputs a bit). Prove that there exists a fixed string $r \in \{0,1\}^n$ such that

$$\Delta_A((X_0;r),(X_1;r)) \geq \Delta_A((X_0;U_n),(X_1;U_n)) \ ,$$

   where U_n is the uniform distribution on $\{0,1\}^n$.
   (This means that for non-uniform algorithms, we can often assume w.l.o.g that they're deterministic.)

3. Let S_0 and S_1 be two non-uniform PPT algorithms, and let $X = \{X_n\}_{n\in\mathbb{N}}$ be a distribution ensemble. Assume that

$$X, S_0(X) \approx_c X, S_1(X) \ ,$$

Here $(X, S_b(X))$ denotes the distribution ensemble $\{X_n, S_b(X_n)\}_{n\in\mathbb{N}}$, where a sample (x, y) is given by first sampling $x \leftarrow X_n$ and then sampling $y \leftarrow S_b(x)$ (note that S_b is randomized and may toss additional coins of its own).

Let p be any polynomial. For $b \in \{0, 1\}$, consider a new ensemble $Y_b = \{Y_{b,n}\}_{n\in\mathbb{N}}$, given by

$$Y_{b,n} = (X_n, \overbrace{S_b(X_n), \ldots, S_b(X_n)}^{p(n) \text{ times}}) \ ,$$

where a sample $(x, y_1, \ldots, y_{p(n)})$ is given by sampling $x \leftarrow X_n$ and then independently sampling each $y_i \leftarrow S_b(x)$.

(a) (30 pts) Show that $Y_0 \approx_c Y_1$.

(b) (**Bonus**: 10 pts) show that if S_0, S_1 may be **inefficient**, and there exists computationally-secure (secret-key) encryption, the previous claim is not true.