Introduction to Cryptography
Courant, Fall 2017

Homework 5

Instructor: Oded Regev
Student: YOUR NAME HERE

Homework is due by **11pm of Oct 22**. Send by email to both "regev" (under the cs.nyu.edu domain) and "ry849" (under the nyu.edu domain) with subject line "CSCI-GA 3210 Homework 5" and name the attachment "YOUR NAME HERE HW5.tex/pdf". There is no need to print it. Start early!

1. (4 points) *(More indistinguishability)* For a probability distribution D over Ω and positive integer m, let D^m denote the *product distribution* over Ω^m, obtained by drawing a tuple of m independent samples from D. Let $\mathcal{X} = \{X_n\}$ and $\mathcal{Y} = \{Y_n\}$ be ensembles of distributions that are efficiently sampleable (in PPT), and let $m(n) = \text{poly}(n)$. Prove that if $\mathcal{X} \stackrel{c}{\approx} \mathcal{Y}$, then $\{X_n^{m(n)}\} \stackrel{c}{\approx} \{Y_n^{m(n)}\}$. (Where do you use that X_n, Y_n are efficiently sampleable?)

2. (5 points) *(Prediction vs distinguishing)* A function $h : \{0,1\}^* \to \{0,1\}$ is *hard-core* for a function f if for all PPT algorithms $\mathcal{A}$,

$$\Pr_{x \leftarrow \{0,1\}^n}[\mathcal{A}(f(x)) = h(x)] \leq \frac{1}{2} + \text{negl}(n) \ .$$

   Show that this definition is equivalent to requiring that

$$(f(U_n), h(U_n)) \stackrel{c}{\approx} (f(U_n), U_1),$$

   where U_n is a uniform n-bit string, and U_1 is a uniform bit. Simplify the right hand side when f is a *permutation* (i.e., a bijection). Once you're done, I recommend reading Goldreich's Section 3.3.5

3. *(Hard core.)*[1] Prove or disprove (giving the simplest counterexample you can find) the following statements. In constructing a counterexample, you may assume the existence of another OWF / PRG.
   (a) (1 point) If an efficiently-computable function f has a hard-core predicate h, then f is one-way.
   (b) (3 points) If an efficiently-computable injective (one-to-one) function f has a hard-core predicate h, then f is one-way.

4. (2 points) (Pseudorandom functions♣) We would like to extend the definition of a pseudorandom generator so that its output length is exponential. Can you think of a definition that makes sense?

[1] A question from Peikert's class