Introduction to Cryptography
Courant, Fall 2016

Homework 5

Instructor: Oded Regev
Student: YOUR NAME HERE

Homework is due by **7am of Oct 24**. Send by email to both "regev" (under the cs.nyu.edu domain) and "avt237@nyu.edu" 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!

Instructions. Solutions must be typeset in LaTeX (a template for this homework is available on the course web page). Your work will be graded on *correctness*, *clarity*, and *conciseness*. You should only submit work that you believe to be correct; if you cannot solve a problem completely, you will get significantly more partial credit if you clearly identify the gap(s) in your solution. It is good practice to start any long solution with an informal (but accurate) "proof summary" that describes the main idea.

You are expected to read all the hints either before or after submission, but before the next class.

You may collaborate with others on this problem set and consult external sources. However, you must ***write your own solutions***. You must also ***list your collaborators/sources*** for each problem.

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 $\mathcal{X} \overset{c}{\approx} \mathcal{Y}$, then $\{X_n^{m(n)}\} \overset{c}{\approx} \{Y_n^{m(n)}\}$. (Where do you use that X_n, Y_n are efficiently sampleable?)

2. (2 points) *(PRG)* For a PRG f, define $g(x) = f(x)|f(\bar{x})$, where $\bar{x}$ is the bit-wise negation of x. Show that g is not necessarily a PRG.

3. (5 points) *(Prediction vs distinguishing)* A function $h : \{0,1\}^* \to \{0,1\}$ is *hard-core* for a function f if for all non-uniform 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

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

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

4. *(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.

5. (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