Introduction to Cryptography | **Instructor: Oded Regev**
Courant, Fall 2013 | **Student: YOUR NAME HERE**

Homework 5

Homework is due by **noon of Oct 21**. Send by email to both "regev" and "tess" under the cs.nyu.edu domain with subject line "CSCI-GA 3210 Homework 5" and name the attachment "YOUR NAME HERE HW5.tex/pdf". Please also bring a printed copy to class. 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 may collaborate with others on this problem set and consult external sources. However, you must ***write your own solutions*** and ***list your collaborators/sources*** for each problem.

1. (3 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 $m(n) = \mathrm{poly}(n)$.

   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. (2 points) *(PRG)*[1] For PRGs f_1 and f_2, define $g(x) = f_1(x)|f_2(\bar{x})$, where $\bar{x}$ is the bit-wise negation of x. Show that g is not necessarily a PRG. (For extra credit of 2 point, show it when $f_1 = f_2$.)

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

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

   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

4. *(Hard core.)*[2] 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 a function f has a hard-core predicate h, then f is one-way.
   (b) (3 points) If an injective (one-to-one) function f has a hard-core predicate h, then f is one-way.

5. (3 points) (Extra credit) Complete the proof from class, showing that "$x \geq (p-1)/2$" is a hard-core predicate for modular exponentiation.

6. (2 points) (Pairwise independence) Assume $r_1, \ldots, r_t$ are independent uniform strings in $\{0,1\}^n$. Show that the collection of all $2^t - 1$ nontrivial XORs, $\{\bigoplus_{i \in S} r_i\}_{\emptyset \neq S \subset [t]}$ is pairwise independent, i.e., any two of them are jointly distributed like an independent uniform pair of strings in $\{0,1\}^n$.

7. (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 Dodis's class
[2] A question from Peikert's class