Introduction to Cryptography
Courant, Fall 2016

Homework 3

Instructor: Oded Regev
Student: YOUR NAME HERE

Homework is due by **7am of Oct 3**. Send by email to both "regev" (under the cs.nyu.edu domain) and "avt237@nyu.edu" with subject line "CSCI-GA 3210 Homework 3" and name the attachment "YOUR NAME HERE HW3.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. [1] A *collection of one-way functions* is a family $F = \{f_s : D_s \to R_s\}_{s \in S}$ satisfying:

   1. Easy to sample function: there exists a PPT algorithm Gen that outputs some $s \in S$ (according to some distribution);
   2. Easy to sample from domain: there exists a PPT algorithm D such that $D(s)$ outputs some $x \in D_s$ (according to some distribution);
   3. Easy to evaluate: there exists a PPT algorithm F such that for all $s \in S, x \in D_s$ we have $F(s, x) = f_s(x)$;
   4. Hard to invert: for any (non-uniform) PPT I,

   $$\Pr_{s \leftarrow S(1^n),\, x \leftarrow D(s)} [I(s, f_s(x)) \in f_s^{-1}(f_s(x))] = \mathrm{negl}(n) \ .$$

   (The only significant change here compared to the definition of OWF is the introduction of s.) In this question we prove that there exists a collection $\{f_s\}$ of one-way functions if and only if there exists a one-way function f.

   (a) (2 points) Prove the "if" part.

   (b) (3 points) Prove the "only if" part. We recommend you make the simplifying assumption that the set of keys S is $\{0,1\}^n$ with the uniform distribution and also that the domain of all the functions in the collection is $\{0,1\}^n$, again with the uniform distribution. So the collection of OWFs is $\{f_s : \{0,1\}^n \to \{0,1\}^n\}_{s \in \{0,1\}^n}$ and we are given just one deterministic algorithm F that takes a key $s \in \{0,1\}^n$ and an input $x \in \{0,1\}^n$ and outputs $f_s(x)$ (there is no need anymore for Gen and D). Once you are done with this, you can try to extend it to the general setting (but start your solution with the simpler case).

2. (2 points) *(Expanding a PRG.♣)* Suggest a construction that we can use to show that the existence of a PRG with output length $\ell(n) = n + 1$ implies the existence of a PRG with any $\mathrm{poly}(n)$ output length. If you feel adventurous, try to suggest a way to prove its correctness.

[1] A question from Peikert's class

♣Another "food-for-thought" question; you are not required to solve it fully, but you are required to demonstrate that you thought about it seriously.

3. (2 points) *(Constructing a PRG.♣)* Try to suggest ways to build a PRG from a OWF. For instance, say we take a one-way function $f : \{0,1\}^n \to \{0,1\}^n$. Explain why $g : \{0,1\}^n \to \{0,1\}^{2n}$ defined by $g(x) = (f(x), x)$ is not a PRG. How about $g(x) = (f(x), x_1)$, where x_1 is the first bit of x? Explain how taking f to be a one-way *permutation* helps a bit, but still does not give us a PRG. Suggest a way one can try to fix the problem.

4. (2 points) Prove that there is no "statistical PRG", i.e., a (deterministic) function $g : \{0,1\}^n \to \{0,1\}^{\ell(n)}$ for some $\ell(n) > n$ such that $g(U_n)$ is within negligible total variation distance (also known as statistical distance) of $U_{\ell(n)}$.