

Homework is due by **11pm of Oct 1**. 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 3” and name the attachment “YOUR NAME HERE HW3.tex/pdf”. There is no need to print it. Start early!

1. <sup>1</sup> By definition, a one-way function is a deterministic function. But we can also consider a “randomized one-way function,” namely, a randomized function  $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$  satisfying

1. Easy to evaluate: there exists a PPT algorithm  $F$  such that for all  $x \in \{0, 1\}^n$ , the distribution of  $F(x)$  is identical to that of  $f(x)$ ;
2. Hard to invert: for any PPT  $I$ ,

$$\Pr_{x \leftarrow \{0, 1\}^n, y \leftarrow f(x)} [I(y) \in f^{-1}(y)] = \text{negl}(n),$$

where  $f^{-1}(y)$  denoted the set of all  $x$  that  $f$  maps to  $y$  with positive probability.

- (a) (1 point) Show that the existence of a one-way function implies the existence of a randomized one-way function.
  - (b) (5 points) Show that the existence of a randomized one-way function implies the existence of a one-way function.
2. <sup>2</sup> A *collection of one-way functions* is a family  $F = \{f_s : D_s \rightarrow R_s\}_{s \in S}$  satisfying:

1. Easy to sample function: there exists a PPT algorithm  $\text{Gen}$  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 PPT  $I$ ,

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

(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  $\{f_s : \{0, 1\}^n \rightarrow \{0, 1\}^n\}_{s \in \{0, 1\}^n}$  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  $\text{Gen}$  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).

<sup>1</sup> A question asked in class by Emil Goldsmith Olesen.

<sup>2</sup> A question from Peikert’s class

3. (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  $\text{poly}(n)$  output length. If you feel adventurous, try to suggest a way to prove its correctness.
4. (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  $f : \{0, 1\}^n \rightarrow \{0, 1\}^n$ . Explain why  $g : \{0, 1\}^n \rightarrow \{0, 1\}^{2n}$  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.
5. (2 points) Prove that there is no “statistical PRG”, i.e., a (deterministic) function  $g : \{0, 1\}^n \rightarrow \{0, 1\}^{\ell(n)}$  for some  $\ell(n) > n$  such that  $g(U_n)$  is within negligible total variation distance (also known as statistical distance) of  $U_{\ell(n)}$ .

---

♣ 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.