NYU COMPUTER SCIENCE FALL 2026

Introduction to Cryptography

CSCI-GA.3210-001 Instructor: Nir Bitansky

Problem Set 2

Due: Wednesday, October 7, 2026, at 11:59 p.m.

Instructions:

- Turn in your solutions in LaTeX and submit a PDF through Gradescope.
(You don't have to know latex, can use AI tools like Prism.)
- Solutions will be graded for both correctness and clarity. If you do not know how to solve a question, you may write "I don't know how to do this" to receive 15% credit for that question.
- Discussion with peers is strongly encouraged, but you must write up your solutions on your own and list your discussion partners. Cite any external sources you use.
- AI use is permitted. If you use AI to solve the homework, list the exact model as a collaborator and include your prompts in an appendix. We strongly recommend solving the questions yourself: the final exam will mostly contain variants of homework questions.
- Use the course forum for clarification questions, but do not post solutions there.

1. Let S_0 and S_1 be two non-uniform PPT algorithms, and let $X = \{X_n\}_{n\in\mathbb{N}}$ be a distribution ensemble. Assume that

$$(X, S_0(X)) \approx_c (X, S_1(X)) \ .$$

Here, $(X, S_b(X))$ denotes the distribution ensemble $\{(X_n, S_b(X_n))\}_{n\in\mathbb{N}}$, where a sample (x, y) is obtained by first sampling $x \leftarrow X_n$ and then sampling $y \leftarrow S_b(x)$. Note that S_b is randomized and may toss additional coins of its own.

Let p be any polynomial. For $b \in \{0, 1\}$, consider a new ensemble $Y_b = \{Y_{b,n}\}_{n\in\mathbb{N}}$, given by

$$Y_{b,n} = (X_n, \overbrace{S_b(X_n), \ldots, S_b(X_n)}^{p(n) \text{ times}}) \ ,$$

where a sample $(x, y_1, \ldots, y_{p(n)})$ is given by sampling $x \leftarrow X_n$ and then independently sampling each $y_i \leftarrow S_b(x)$.

   (a) (15 pts) Show that $Y_0 \approx_c Y_1$.

   (b) (10 pts) Show that if S_0 and S_1 are allowed to be **inefficient**, then, assuming computationally secure secret-key encryption exists, the previous claim is false.

2. (25 pts) Let ℓ and ℓ' be polynomials. An ensemble of functions $\left\{f_n : \{0,1\}^{\ell(n)} \to \{0,1\}^{\ell'(n)}\right\}_{n\in\mathbb{N}}$ is one-way if there exists a polynomial-time algorithm that, given 1^n and $x \in \{0,1\}^{\ell(n)}$, outputs $f_n(x)$, and if for every n.u. PPT adversary A there exists a negligible function μ such that, for all $n \in \mathbb{N}$,

$$\Pr_{x\leftarrow\{0,1\}^{\ell(n)}}\left[A(f_n(x)) \in f_n^{-1}(f_n(x))\right] \leq \mu(n) \ .$$

Show that the existence of such an ensemble implies the existence of a OWF as defined in class; namely, a function $f : \{0,1\}^* \to \{0,1\}^*$ that is defined at every input length, rather than only at lengths of the form $\ell(n)$.

3. Let G be a PRG with stretch ℓ (that is, G maps n bits to $n + \ell(n)$ pseudorandom bits).

   (a) (10 pts) Show that if $\ell(n) = \omega(\log n)$, then G is a OWF.

   (b) (10 pts) Actually, show that even if $\ell(n) = 1$, then G is a OWF.

   (c) (5 pts) Assume $\ell(n) = 1$. Define an ensemble of functions $f = \left\{f_n : \{0,1\}^{2n} \to \{0,1\}^{n+1}\right\}$ by $(s_0, s_1) \xmapsto{f_n} G(s_0) \oplus G(s_1)$. Prove that f is one way or give a counter example.

4. We say that f is a weak one-way function if there exists a polynomial p such that for any n.u. PPT A and all $n \in \mathbb{N}$:

$$\Pr_{x\leftarrow\{0,1\}^{n}}\left[A(f(x)) \in f^{-1}(f(x))\right] \leq 1 - \Omega\left(\frac{1}{p(n)}\right) \ .$$

This question aims to show that *weak* OWFs may be strictly weaker than OWFs, but can always be amplified to OWFs.

   (a) (4 pts) Show that if there exist OWFs, then there also exist weak OWFs that are not OWFs.

   (b) (21 pts) Let f be a weak OWF with respect to some polynomial p (as in the above definition), and let $t(n) = \log^2 n \cdot p(n)$. We define the t-fold direct product $f_n^{\otimes t} : (\{0,1\}^n)^{t(n)} \to \{0,1\}^*$ as:

$$f_n^{\otimes t}(x_1, \ldots, x_{t(n)}) = f(x_1), f(x_2), \ldots, f(x_{t(n)}) \ .$$

   We will show that the ensemble $\{f_n^{\otimes t}\}_n$ is one-way. In what follows, let A be an adversary that inverts $f_n^{\otimes t}$ with probability $\varepsilon = \varepsilon(n)$.
   For $i \in [t]$, let $G_i \subseteq \{0,1\}^n$ be the set of inputs x such that

$$\Pr_{x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_t}\left[A \text{ inverts } f^{\otimes t}(x_1, \ldots, x_{i-1}, x, x_{i+1} \ldots, x_t))\right] \geq \varepsilon/2t \ .$$

      i. (7 pts) Show that there exists an $i \in [t]$ such that

$$\Pr_{x\leftarrow\{0,1\}^{n}}\left[x \in G_i\right] \geq 1 - \frac{\log(2/\varepsilon)}{t} \ .$$

      ii. (7 pts) Show that there exists a n.u. adversary A' (depending on A and i) whose running time is

$$time(A') = O\left(time(A) \cdot time(f) \cdot \frac{t}{\varepsilon} \cdot n\right)$$

      and which inverts f with probability at least $1 - \frac{\log(2/\varepsilon)}{t} - 2^{-n}$. (You can use the previous item even if you didn't manage to prove it.)

      iii. (7 pts) Deduce that $\varepsilon(n) = n^{-\omega(1)}$. That is, $f^{\otimes t}$ is a OWF.