0368.4162 Foundations of Cryptography November 16, 2017

Problem Set 2

Due: November 30

Instructions:

- Type your solution and email it to "focf17hw@gmail.com", with subject "HW#, ID#, Name".
- You're encouraged to use latex. You can find on the webpage the assignment's tex file to help you.
- You can cooperate. However, you should write the solution by yourself, and list all collaborators for each question. Same goes for any external sources that you may use.
- Do not discuss solutions over the course's forum. You are more than welcome though to ask for clarifications regarding the questions themselves.

1. (30 pts) Let ℓ, ℓ' be two 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 poly-time algorithm $f(1^n, x)$ that given 1^n and $x \in \{0,1\}^{\ell(n)}$ outputs $f_n(x)$, and for every n.u. PPT A there exists a negligible 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 any such ensemble implies OWFs as defined in class; namely, a function f that is defined on every input length n, and not just $\ell(n)$.

2. Let G be a PRG with stretch ℓ (that is, G maps n bits to $n + \ell(n)$ pseudorandom bits).
   (a) (15 pts) Show that if $\ell(n) = \omega(\log n)$, then G is a OWF.
   (b) (15 pts) Actually, show that even if $\ell(n) = 1$, then G is a OWF.
   (c) (**Bonus:** 10 pts) Assume $\ell(n) = 1$. Define an ensemble of functions $f = \left\{f_n : \{0,1\}^{2n} \to \{0,1\}^{n+1}\right\}$ by $(s_0, s_1) \xmapsto{f_n} G(s_1) \oplus G(s_2)$. Prove that f is one way or give a counter example.

3. 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) (10 pts) Show that if there exist OWFs, then there also exist weak OWFs that are not OWFs.
   (b) 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. (12 pts) Show that there exists an $i \in [t]$ such that

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

ii. (12 pts) Show that there exists a n.u. adversary A' (depending on A and i) whose running time is

$$time(A') = O\left(time(A) \cdot \frac{t}{2\varepsilon} \cdot n\right)$$

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