Homework 1

Deadline: Oct 3, 2016

1. **Negligible and Noticeable Functions**

   (a) (5 points) If μ_1 and μ_2 are negligible functions, then prove that μ is also a negligible function, where $\mu(n) = \mu_1(n) + \mu_2(n)$ for any $n \in \mathbb{N}$.

   (b) (5 points) If μ_1 is a noticeable function and μ_2 is a negligible function, then prove that μ is also a noticeable function, where $\mu(n) = \mu_1(n) - \mu_2(n)$ for any $n \in \mathbb{N}$.

   (c) (5 points) Construct a function μ that is neither negligible, nor noticeable.

2. **One-way Functions (I):** Let $f : \{0,1\}^n \to \{0,1\}^n$ be any one-way function. Prove (via reduction) or disprove (by building an efficient inverter) each of the following statements:

   (a) (10 points) Let $f' : \{0,1\}^{2n} \to \{0,1\}^{2n}$ be s.t. for every $x_1 \| x_2 \in \{0,1\}^{2n}$, $|x_1| = |x_2|$, $f'(x_1 \| x_2) = f(x_1) \| x_2$. Then f' is also a one-way function.

   (b) (10 points) Let $f' : \{0,1\}^{2n} \to \{0,1\}^{n}$ be s.t. for every $x_1 \| x_2 \in \{0,1\}^{2n}$, $|x_1| = |x_2|$, $f'(x_1 \| x_2) = f(x_1) \oplus x_2$. Then f' is also a one-way function.

3. **One-way Functions (II):** For any one-way functions f_1 and f_2 with the same domains and codomains, define:

$$f(x_1 \| x_2) = f_1(x_1) \oplus f_2(x_2).$$

(a) (15 points) Let $g : \{0,1\}^n \to \{0,1\}^n$ be a one-way function. Define $f_1(x_1\|x_2) = g(x_1)\|(x_1 \oplus x_2)\|0^{2n}$ and $f_2(x_1\|x_2) = (x_1 \oplus x_2)\|g(x_1)\|0^{2n}$

i. Prove that f_1 and f_2 are one-way functions.

ii. Prove that f (as defined above) is not a one-way function.

(b) (15 points) Construct f_1 and f_2 such that if they are one-way functions, then f (as defined above) is also a one-way function.

4. **Pseudorandom Generators:** (15 points) Let $G : \{0,1\}^n \to \{0,1\}^{2n}$ be a pseudorandom generator with n-bit stretch. Prove that G is a one-way function.

5. **Hardcore Predicates:** (20 points) Give the full proof of the Goldreich-Levin theorem stated below:

Theorem 1 (Goldreich-Levin) *Let f be a OWF (OWP). Define function $g(x,r) = (f(x),r)$, where $|x| = |r|$. Then g is a OWF (OWP) and $h(x,r) =< x,r >$ is a hard-core predicate for f. Here, $< x,r >$ denotes the inner product of x and r, i.e., $\sum_i x_i r_i \bmod 2$.*

(Note: For this question you are allowed to look for the proof online. However, you must write all the details in your own words.)