CS 601.442/642 – Modern Cryptography Instructor: Abhishek Jain

Homework 2

Deadline: October 8; 2017, 11:59 PM

1 Hardcore Predicates and One-way Functions

1. (15 points) Prove that every one-to-one function that has a hardcore predicate is also a one-way function. Recall that a function f is one-to-one if every element in the codomain of f has a unique pre-image in the domain of f.

2 Pseudo-random Generators

1. (10 points) Let G_1 and G_2 be PRGs. Is $G(s) = G_1(s)||G_2(s)$ also a PRG? Prove or give a counterexample.

3 Pseudo-random Functions

1. (10 points) Let $\{f_k\}_k$ be a family of PRFs. Is $\{g_k\}_k$ also a family of PRFs, where $g_k(x) = f_k(x)||f_k(\bar{x})$. Prove or give a counterexample.
2. (10 points) Let $\{f_k\}_k$ be a family of PRFs. Is $\{g_k\}_k$ also a family of PRFs, where $g_k(x) = f_k(0||x)||f_k(1||x)$. Prove or give a counterexample.

4 Hybrid Arguments

1. (10 points) For integers $a \leq b$, let $U_{a,b}$ denote the uniform distribution over the integers x, $a \leq x \leq b$. Now consider the following two distributions: (a) $U_{0,2^n-1}$, (b) $U_{2^n,2^{n+1}-1}$.

   Consider the following proof via hybrid argument to establish that $U_{0,2^n-1}$ and $U_{2^n,2^{n+1}-1}$ are indistinguishable: For $0 \leq i \leq 2^n$, let $H_i = U_{i,2^n-1+i}$. Clearly, $H_0 = U_{0,2^n-1}$ and $H_{2^n} = U_{2^n,2^{n+1}-1}$. Also, for every i, $H_i \approx H_{i+1}$ because they are statistically close. Therefore, $U_{0,2^n-1} \approx U_{2^n,2^{n+1}-1}$.
   Is the above a valid proof? Explain your answer.

2. (15 points) Let G be a cyclic group of prime order p with a generator g. Recall that Decisional Diffie Hellman (DDH) assumption states that for $a, b, r \stackrel{\$}{\leftarrow} \{0, \ldots, p-1\}$, the following distributions are computationally indistinguishable:

   $$\{g, g^a, g^b, g^{a.b}\} \approx_c \{g, g^a, g^b, g^r\}$$

   Prove that for $a_1, a_2, b, r_1, r_2 \stackrel{\$}{\leftarrow} \{0, \ldots, p-1\}$, the following two distributions are indistinguishable under the DDH assumption:

   $$\{g, g^{a_1}, g^{a_2}, g^{a_1.b}, g^{a_2.b}\} \approx_c \{g, g^{a_1}, g^{a_2}, g^{r_1}, g^{r_2}\}$$