CS 601.442/642 – Modern Cryptography Instructor: Abhishek Jain

Homework 4

Deadline: October 12; 2022, 1:30 PM EST

1 Hard Core Predicate

1. (10 points) Consider the following definition of a **2-bit hard core function**, which says that given the output of a OWF on an input x, it should be hard for the adversary to guess the 2-bit output of this hard core function on x:

   A function $h : \{0,1\}^* \to \{0,1\}^2$ is a 2-bit hard-core function for $f(\cdot)$, if h is efficiently computable given x and there exists a negligible function ν s.t. for every non-uniform PPT adversary $\mathcal{A}$ and $\forall n \in \mathbb{N}$:

   $$\Pr\left[x \leftarrow \{0,1\}^n : \mathcal{A}(1^n, f(x)) = h(x)\right] \leq \frac{1}{4} + \nu(n).$$

   Let $f : \{0,1\}^{2n} \to \{0,1\}^{2n}$ be a OWF. Then we know that $g(x,r) = (f(x), r)$, where $|x| = |r|$ is also a OWF. Explain using a counterexample that $h(x,r) = \langle x[0:n], r\rangle \| \langle x[n:2n], r\rangle$, where $x[0:n]$ (and resp. $x[n:2n]$) denote the first n bits (and resp. last n bits) of x, is **NOT** a 2-bit hard core function for f.

2 Pseudorandom 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 via reduction 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 via reduction or give a counterexample.

3. (15 points) Let $\{f_k\}_{k\in\{0,1\}^n}$ be a family of PRFs, where $f_k : \{0,1\}^n \to \{0,1\}^n$. Let $g : \{0,1\}^n \to \{0,1\}^{2n}$ be a PRG. Show via reduction that $\{h_k\}_{k\in\{0,1\}^n}$, where $h_k(x) = g(f_k(x))$ is also a family of PRFs.

3 Discrete Log

1. (10 points) Let $(G, \cdot)$ be a cyclic group with generator g. Suppose you are given $X \in G$. You are allowed to choose any $X' \neq X$ and learn the discrete log of X' (with respect to base g). Show that you can use this ability to learn the discrete log of X.

4 Diffie Hellman

1. (10 points) Explain what is wrong with the following argument:

In Diffie-Hellman key agreement, Alice sends $A = g^a$ and Bob sends $B = g^b$. Their shared key is g^{ab}. To break the scheme, the eavesdropper can simply compute $A \cdot B = (g^a) \cdot (g^b) = g^{ab}$

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 $a, b, r \xleftarrow{\$} \{0, \ldots, p-1\}$, the following distributions are computationally indistinguishable:

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

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

$$D_1 = \{g, g^{a_1}, g^{a_2}, g^{a_1 \cdot b}, g^{a_2 \cdot b}\}$$
$$D_2 = \{g, g^{a_1}, g^{a_2}, g^{r_1}, g^{r_2}\}$$