~ MathDefs ~

CS 127: Cryptography / Boaz Barak

Homework 2

Total of 128 points.

Exercises from Lecture 3

1. (impossibility of statistically testing randomness, 15 points) Let $T_1, \ldots, T_M : \{0,1\}^n \rightarrow \{0,1\}$ be a collection of function that are supposed to be statistical tests for randomness. Prove that if n is large enough and $M < 2^{100n}$ there exists a distribution X that passes all these tests but is very far from the uniform distribution. Concretely, show that there exists a random variable X over $\{0,1\}^n$ such that:

- For every $i \in [M]$, $|\mathbb{E}[T_i(X)] - \mathbb{E}[T_i(U_n)]| < 0.001$ where U_n is the uniform distribution over n bits.
- But, there exists some $T^* : \{0,1\}^n \rightarrow \{0,1\}$ such that $|\mathbb{E}[T^*(X)] - \mathbb{E}[T^*(U_n)]| > 0.999$.

(No points, just food for thought.) Based on this exercise, what do you believe can we say about a distribution X if it passes the FIPS 140-2 testing suite for randomness?

2. (20 points) We call a sequence $\{X_n\}_{n \in \mathbb{N}}$ where X_n is a distribution over $\{0,1\}^n$ *pseudorandom* if it's computationally indistinguishable from the sequence $\{U_n\}$ where U_n is the uniform distribution over $\{0,1\}^n$. Are the following sequences pseudorandom? prove or refute.

a. (10 points) $\{X_n\}$ where X_n be the following distribution: we pick $x_1, \ldots, x_{n-1}$ uniformly at random in $\{0,1\}^{n-1}$, and let x_n be the parity (i.e. XOR) of $x_1, \ldots, x_{n-1}$, we output $x_1, \ldots, x_n$.

b. (10 points) $\{Z_n\}$ where for n large enough, with probability $2^{-n/10}$ we output an n bit string encoding the text `"This is not a pseudorandom distribution"` (say encode in ASCII and pad with zeros), and with probability $1 - 2^{-n/10}$ pick a random string. For n that is not large enough to encode the text, Z_n always outputs the all zeroes string.

3. (24 points) Suppose that $G : \{0,1\}^n \rightarrow \{0,1\}^{3n}$ is a secure pseudorandom generator. For each one of the constructions G^1, G^2, G^3 below either prove that they are necessarily a secure pseudorandom generator or give a counterexample (which is a construction, based on the Cipher, PRG or PRG conjectures, of a generator G such that G_i would not be secure.)

a. (8 points) $G^1(s) = G(s)_{1,\ldots,2n}$ (i.e., the first $2n$ bits of $G(s)$).

b. (8 points) $G^2(s) = G(0, s_2, \ldots, s_n)$ (i.e., the output of $G(s)$ but setting the first seed bit to zero)

c. (8 points) $G^3(s_1, \ldots, s_n) = G(s_n, \ldots, s_1)$ (i.e., the output of $G(s')$ where s' is obtained by reversing s).

Exercises from Lecture 4

4. (24 points) In these three questions you'll show that if we have a pseudorandom function family with particular input and output sizes, we can easily obtain a family that handles different inputs and outputs.

a. (Padding inputs and outputs, 8 points) Suppose that $\{f_s\}$ is a pseudorandom function collection where for every $s \in \{0,1\}^n$, f_s maps $\{0,1\}^n$ to $\{0,1\}^n$. Prove that if we define f'_s to be function that on input $i \in [2^{n/2}]$ outputs the first bit of $f_s(2^{n/2} + i)$ then $\{f'_s\}$ is a pseudorandom function collection (with one bit output).

b. (Increasing output size, 8 points) Prove that if there exists a collection $\{f_s\}$ where $f_s : \{0,1\}^{|s|} \rightarrow \{0,1\}$ (i.e., one bit output), then then there exists a collection $\{f'_s\}$ with $f'_s : \{0,1\}^{|s|} \rightarrow \{0,1\}^{|s|}$. See footnote for hint.[1]

c. (Changing PRFs input size, 8 points) Prove that if there exists a collection $\{f_s\}$ of pseudorandom functions with $f_s : \{0,1\}^{|s|} \rightarrow \{0,1\}^{|s|}$ then there exists a collection $\{f'_s\}$ with $f'_s : \{0,1\}^* \rightarrow \{0,1\}^{|s|}$ (i.e., f'_s for a random $s \in \{0,1\}^n$ is indistinguishable from a random function from $\{0,1\}^*$ to $\{0,1\}^n$. (If it makes your life easier, it's fine to construct a collection $\{f'_s\}$ with a single output bit.)

5. (20 points) Suppose that $\{f_s\}$ is a collection of secure pseudorandom functions where f_s maps $\{0,1\}^{|s|+1}$ to $\{0,1\}$. For each of the following constructions f^1,f^2 below of function collections mapping $\{0,1\}^{|s|}$ to $\{0,1\}^2$, either prove that they are necessarily secure or show a counterexample (i.e., a construction of PRF's $\{f_s\}$ based on the PRF conjecture such that the corresponding construction f^i is insecure)

a. (10 points) $f^1_s(x) = f_s(0 \circ x) \circ f_s(1 \circ x)$

b. (10 points) $f^2_s(x) = f_s(0 \circ x) \circ f_s(x \circ 1)$

6. (25 points) For the sake of this question, let's say that a pair of algorithms (S, V) is an *enhanced message authentication code* if it is a secure message authentication code (as per the definition given in the lecture notes) with the following addition— in the attack game Mallory is given not just oracle (i.e., black box) access to the signing oracle S but also to the verification

[1] First come up with a pseudorandom family with output longer than 1 but shorter than $|s|$. For example, if $s \in \{0,1\}^{n^2}$ then the output can be n. Then show that existence of PRF implies existence of pseudorandom generators and use that to expand your output.

oracle V. That is, Mallory can put forward a pair (m, σ) to the oracle and find out whether or not the pair passes verification. Prove that every (S, V) that is a secure message authentication code is also an enhance message authentication code.