6.875J/18.425J Cryptography and Cryptanalysis	October 13, 2001

Handout 9: Problem Set 5

Instructor: Anna Lysyanskaya — *Teaching Assistant: Moses Liskov*

This problem set is due on Wednesday, October 24.

Problem 1: Fun with primitives

(35 points) Let $F : \{0,1\}^* \to \{0,1\}^*$ be a one-way function. Let $G : \{0,1\}^* \to \{0,1\}^*$ be a pseudorandom generator. Finally, let $P : \{0,1\}^* \to \{0,1\}^*$ be a one-way permutation. (Refer to lecture notes from lecture 10 for rigorous definitions of these primitives.) For each of the following, answer either "yes" or "no." If you answer "yes" give an intuitive argument to support your answer. If you answer "no" give a counterexample.[1] For at least *one* of your "yes" answers, if you give any, give an actual proof (5 points) of your answer.

(a) Is $G \circ G$ a PRG?[2]

(b) Is $F \circ F$ a OWF?

(c) Is $P \circ P$ a OWP?

(d) Is $P \circ F$ a OWP?

(e) Is $G \circ P$ a PRG?

(f) Is $G \circ F$ a PRG?

Problem 2: Hard-core bits

(20 points) Let $b : \{0,1\}^* \to \{0,1\}$ be an efficiently computable, nontrivial predicate (with respect to sampling with the uniform distribution).

(a) Prove that if OWP's exist, there is a OWP $P : \{0,1\}^* \to \{0,1\}^*$ such that b is a hard-core predicate of P. Here you may assume that b is of the form $b_r(x) = r \cdot x \bmod 2$, where $|r| = |x|$.

(b) Prove that if $P : \{0,1\}^* \to \{0,1\}^*$ is an efficiently computable permutation, and b is a hard-core predicate of P, then P is a OWP. Also, prove that if $F : \{0,1\}^* \to \{0,1\}^*$ and $b(x)$ is hard to compute given only access to $F(x)$, then F is not necessarily a OWF.

[1] To give a counterexample, you may need to assume the existence of some other F', G', or P', and then describe how F, G, or P could be constructed from them such that F, G, or P is still a OWF (or PRG or OWP) but the answer to the question is no for that F, G, and P.

[2] $f \circ g$ refers to the *composition* of functions f and g, that is $f \circ g(x) = f(g(x))$

Problem 3: OWP $\Rightarrow$ PRG

(20 points) Let $P : \{0,1\}^* \rightarrow \{0,1\}^*$ be a OWP, and let b be a hard-core predicate of P. Consider the following construction, due to Blum and Micali, of a PRG. To generate a key PK, just use the key generation algorithm for P. Let s denote the input, where $|s| = k$.

Let $x_0 = s$, and let $x_i = P(x_{i-1})$ for all $i > 0$. Define

$$G(s) = b(s = x_0) \circ b(x_1) \circ \ldots \circ b(x_k)$$

(a) Prove that G is *next-bit unpredictable*. That is, that

$$\forall \{A\}_n\ \exists f \in neg\ \forall k$$
$$\Pr[(\alpha, j) \leftarrow A_k; s \leftarrow \{0,1\}^k;$$
$$r \leftarrow G(s); b \leftarrow A_k(\alpha, r_1 \circ \ldots \circ r_j) : b = r_{j+1}] \leq 1/2 + f(k)$$

where $r = r_1 \circ r_2 \circ \ldots \circ r_{k+1}$.

(b) Prove that for *any* G, if G is next-bit unpredictable then it is a pseudorandom generator (in the sense we used in lecture - that G is indistinguishable from random).

Problem 4: Pumping Pseudorandomness

(20 points) Suppose you are given a PRG G such that $|G(x)| = |x| + 1$, and a polynomial p. Construct a G' such that $|G'(x)| = p(|x|)$, and prove that G' is also a PRG. Your proof should be along similar lines to the proof you use in problem 3. A certain level of informality is acceptable.

Problem 5: Predictable OWFs

(5 points)[3] Let $F : \{0,1\}^* \rightarrow \{0,1\}^*$ be a length-preserving one-way function. Let $b_i(x)$ be a predicate which returns the i^{th} bit of x. Construct a length preserving function F', and prove that F' is (1) a one-way function, and (2) for any $1 \leq i \leq k$, it is easy for random x of length k to compute $b_i(x)$, given only $F'(x)$ as input.

[3] Consider this a challenge problem. At only 5 points it should not seriously impact your grade whether you do this problem or not.