

CAS CS 538. Problem Set 6

Due in class Wednesday, November 3, 2010.

In the two problems below, suppose $\{F_k\}$ is a pseudorandom function family from n -bit inputs to n -bit outputs, with a n -bit key k . Also, let \circ denote concatenation, \bar{x} denote the bit-by-bit negation of x , and 0^n denote the string of n zeroes.

Problem 1. (40 points, 10 for each part) We are trying to construct a function family with $2n$ -bit outputs out of $\{F_k\}$. Which of the following are pseudorandom function families? Prove your answers.

(a) $F_k^1(x) = F_k(0^n) \circ F_k(x)$.

(b) $F_k^2(x) = F_k(x) \circ F_k(\bar{x})$.

(c) $F_k^3(x) = F_{0^n}(x) \circ F_k(x)$.

(d) $F_k^4(x) = G(F_k(x))$, where G is a length-doubling PRG.

Problem 2. (20 points, 10 for each part)

(a) Consider the following function family $\{G_s\}$: if $s = 0^k$, output 0^k ; else output $F_s(x)$. Show that it is pseudorandom (a simple reduction works here).

(b) Consider the family $H_s(x) = G_x(s)$. Show that it is **not** pseudorandom.

Thus, swapping the seed and the input in a PRF does not always result in a PRF!

Problem 3. (20 points) In class we showed that two-round Luby-Rackoff is not a pseudorandom permutation by exhibiting a two-query distinguisher: ask for two queries on the same R and different L s and observe that the changes in S will be the same as the changes in L . Show that three-round Luby-Rackoff, as described in the lecture notes, is not super pseudorandom. Namely, exhibit a three-query distinguisher (two forward queries followed by one reverse query), and explain why it distinguishes with high probability. (Hint: recall that our in-class distinguisher found a way to XOR a predictable value into S by varying L . You can similarly XOR a predictable value into S with a reverse query (think about how). Using this, you can get S in a reverse query to be equal to S in a different forward query. This will lead to non-random-looking relationship among the inputs and outputs.)

Problem 4. (20 points) Here is the correct definition of strongly universal hash functions (Wegman-Carter 1991, Stinson 1994).

Definition 1. A family of efficient functions $\mathcal{H} = \{h_i : \{0, 1\}^n \rightarrow \{0, 1\}^\ell\}_{i \in I}$ is δ -almost strongly universal if for all distinct $x \neq x', y, y'$ (a) $\Pr_{i \leftarrow I}[h_i(x) = y] = 2^{-\ell}$ and (b) $\Pr_{i \leftarrow I}[h_i(x) = y \wedge h_i(x') = y'] \leq \delta 2^{-\ell}$. Families with $\delta = 2^{-\ell}$ are called *strongly universal* or *pairwise independent*.

Consider now the following hash function family. Let $p > 2^n$ be a prime. The key i is a random value $a \in \mathbb{Z}_p$ and a random value $b \in \mathbb{Z}_{2^\ell}$. The function is $h_i(x) = ((ax \bmod p) + b) \bmod 2^\ell$. Prove that it is $2^{-\ell+1}$ -almost strongly universal.