Solutions

ENEE/CMSC/MATH 456: Cryptography PRF
Class Exercise 2/16/22

Let F be a length-preserving pseudorandom function. For the following constructions of a keyed function $F': \{0,1\}^n \times \{0,1\}^{n-1} \to \{0,1\}^{2n}$, state whether F' is a pseudorandom function. If yes, prove it; if not, show an attack.

1. $F'_k(x) := F_k(0||x)||F_k(x||1)$. No.

Distinguisher $D^{\mathcal{O}}(1^n)$:
1. query $\mathcal{O}$ on input $x_1 = 0^{n-1}$, get back y_1
2. query $\mathcal{O}$ on input $x_2 = 0^{n-2}1$, get back y_2

Note $F'_k(x_1) = F'_k(0^{n-1}) = F_k(0^n)||F_k(0^{n-1}1)$
$F'_k(x_2) = F'_k(0^{n-2}1) = F_k(0^{n-1}1)||F_k(0^{n-2}1^2)$

3. If second half of y_1 is equal to first half of y_2, output 1. O/w output 0.

$\Pr\left[D^{F'_k(\cdot)}(1^n) = 1\right] = 1$

$\Pr\left[D^{f(\cdot)}(1^n) = 1\right] = \frac{1}{2^n}$

Therefore

$\left|\Pr\left[D^{F'_k(\cdot)}(1^n) = 1\right] - \Pr\left[D^{f(\cdot)}(1^n) = 1\right]\right| = 1 - \frac{1}{2^n}$

contradicting security of F'.

Clearly, D is ppt.

2. $F'_k(x) := F_k(0||x)||F_k(1||x)$. Yes

Idea of proof: for any set of queries $x_1 \ldots x_q$ the responses $f(0||x_i)||f(1||x_i)$ are completely independent and uncorrelated when f is a truly random function.

Therefore, by security of PRF, $F'_k(\cdot)$ remains secure when truly random f is replaced with pseudorandom F_k.