Cryptography: Homework 8

(Nov 22, 2018)

1. (10 points) Prove that if F is a length-preserving PRF, then the function $G : \{0,1\}^n \to \{0,1\}^{2n}$ defined by $G(k) = F_k(1)\|F_k(2)$ is a PRG with expansion factor $2n$, where the 1 and 2 in $F_k(1), F_k(2)$ are considered as the decimal representations of some n-bit strings.

2. (20 points) Let F be a length-preserving PRF. Let $P : \{0,1\}^{2n} \times \{0,1\}^{2n} \to \{0,1\}^{2n}$ be a keyed function defined by a 2-round Feistel network:

   - key: $k = (k_1, k_2) \in \{0,1\}^n \times \{0,1\}^n$; input: $x = (L_0, R_0) \in \{0,1\}^n \times \{0,1\}^n$
   - $L_1 = R_0, R_1 = L_0 \oplus F_{k_1}(R_0)$; $L_2 = R_1, R_2 = L_1 \oplus F_{k_2}(R_1)$; output $P_k(x) = (L_2, R_2)$

   Show that P is not a PRP.