Cryptography: Homework 5

(Deadline: 11:59am, 2019/10/30)

1. (20 points) Let $G : \{0,1\}^n \to \{0,1\}^{l(n)}$ be a PRG with expansion factor $l(n) > n$. Let $\mathrm{Im}(G) = \{G(k) : k \in \{0,1\}^n\}$. For any $m \in \{0,1\}^{l(n)}$, define $m \oplus \mathrm{Im}(G) = \{m \oplus s : s \in \mathrm{Im}(G)\}$.

   (1) Show that for any $m_0 \in \{0,1\}^{l(n)}$, there exists an $m_1 \in \{0,1\}^{l(n)}$ such that $(m_1 \oplus \mathrm{Im}(G)) \not\subseteq (m_0 \oplus \mathrm{Im}(G))$.

   (2) Based on the results of (1), show that the fixed-length encryption from PRG (page 6, lec8.pptx) is not perfectly secret.

2. (30 points) Let F be a length-preserving PRF. Let $H : \{0,1\}^n \times \{0,1\}^{n-1} \to \{0,1\}^{2n}$ be a keyed function such that $H_k(x) = F_k(0\|x)\|F_k(x\|1)$ for any $k \in \{0,1\}^n$ and $x \in \{0,1\}^{n-1}$. Determine if H is a PRF. Explain your answer.