1 Fun with PRFs

Suppose that \( \{ F_s : \{0,1\}^k \to \{0,1\}^k \mid s \in \{0,1\}^k \} \) is a family of pseudorandom functions from \( k \)-bit inputs to \( k \)-bit outputs, indexed by a \( k \)-bit key seed \( s \). We would like to construct a new PRF family.

For each of the following constructions, say whether the specified family is pseudorandom or not, for the appropriate domain and range. If your answer is yes, give an outline of a reduction. If your answer is no, give a counterexample \( F \), convincing evidence that your \( F \) is a PRF, and an attack on \( F \) when it is based on your \( F \).

a. \( F_a^s(x) = F_{0^k}(x) \circ F_s(x) \)

b. \( F_b^s(x) = G(s) \oplus x \), where \( G : \{0,1\}^k \to \{0,1\}^{2k} \) is a PRG.

c. \( F_c^s(x) = F_{s_1}(x) \oplus s_2 \), where \( s = s_1 \circ s_2 \) and \( |s_1| = |s_2| = k \).

d. \( F_d^s(x) = \begin{cases} F_s(x) & \text{when } x \neq 0^k \\ a \circ b & \text{when } x = 0^k, \end{cases} \)

where we define \( a \) to be the first \( \lfloor k/2 \rfloor \) bits of \( s \), and \( b \) to be the last \( \lfloor k/2 \rfloor \) bits of \( F_s(x) \).

e. \( F_e^s(x) = F_s(0 \circ x) \circ F_s(1 \circ x) \)

2 Pseudorandom Fun(ctions)

Given a pseudorandom function \( F_s : \{0,1\}^{k+\log k} \to \{0,1\} \), construct a pseudorandom function \( F'_s : \{0,1\}^k \to \{0,1\}^k \) and prove that it is secure.
3 PRFs as MACs

A message authentication code (MAC) is a method for ensuring that the data received over a network came from the right person. More precisely, it is an object that satisfies the following properties: Suppose Alice and Bob share a secret $s$, and Bob wants to send message $m$ to Alice. Then a MAC $M_s(m)$ is an efficiently computable function such that even if an active attacker Eve queries it on a set of messages of Eve’s choice, Eve still cannot authenticate any message not explicitly queried.

To give a more formal definition, we first extend our notation. If $A(\cdot)$ is an oracle Turing machine, then by $Q \leftarrow A^O(i)$, we denote the contents of $A$’s query tape upon termination with oracle $O$ and input $i$. Now, a function family $\{M_s(\cdot)\}$ is a MAC family if for all p.p.t. $A$, there exists a negligible function $\nu(k)$ such that:

$$\Pr[s \leftarrow \{0,1\}^k; ((m,x),Q) \leftarrow A^{M_s(1^k)}: x = M_s(m) \text{ and } (m,x) \notin Q] \leq \nu(k)$$

a. Let $\{F_s : \{0,1\}^{|s|} \rightarrow \{0,1\}^{|s|}\}$ be a PRF family. Show that it is a MAC family.

b. Is it the case that a MAC is a PRF? Prove your answer.

c. Is it true that if MACs exist then PRFs exist? Briefly defend your answer.