CSC 5440: Cryptography
The Chinese University of Hong Kong

Homework 2
due Wednesday 2 March

Problem 1

In this problem you will explore perfectly secure analogues of MACs for fixed length messages. Let k be the key length and m be the message length.

(a) Say a scheme is perfectly q-secure against chosen message attacks if it is secure against chosen message attacks, provided that the adversary can make at most q queries to the tagging oracle. Give a formal definition of perfect q-security against chosen message attacks of MACs for messages of fixed length m.

(b) Show that there exists a MAC that is perfectly 0-secure (against chosen message attack) if and only if $k \geq m$.

(c) Show that if $k < qm$, then no MAC is perfectly q-secure against chosen message attack.

(d) (Optional) Show that if $k \geq 2m$, then there exists a MAC that is perfectly 2-secure against chosen message attack.

Problem 2

Consider the following encryption scheme, where $\{F_K\}$ is a pseudorandom function family:

$$Enc((K_1, K_2), M) = (S, F_{K_1}(S) + M, F_{K_2}(S + M)) \quad \text{where } S \text{ is a random string}$$

$$Dec((K_1, K_2), (S, C, T)) = \begin{cases} C + F_{K_1}(S), & \text{if } F_{K_2}(S + C + F_{K_1}(S)) = T \\ \texttt{error}, & \text{otherwise.} \end{cases}$$

(a) Show that if (Enc, Dec) is used with the same key $K_1 = K_2$, the scheme is not message indistinguishable, even for one encryption.

(b) Now assume that K_1 and K_2 are independent. Consider the ideal scheme $(REnc, RDec)$ which is a variant of (Enc, Dec) where F_{K_1} and F_{K_2} are replaced with truly random independent functions R_1 and R_2, respectively. Show that if $\{F_K\}$ is pseudorandom and $(REnc, RDec)$ is CPA-secure, than (Enc, Dec) is CPA secure (for an appropriate choice of the parameters).

(c) Show that $(REnc, RDec)$ is CPA-secure (for an appropriate choice of the parameters).

(d) (Optional) Can you show that (Enc, Dec) is CCA-secure?

Problem 3

Let $\{h_S\colon \{0,1\}^{2k} \to \{0,1\}^k\}$ be a cryptographic hash family for input length $2k$. Let $h_S^{(t)}\colon \{0,1\}^{2^t k} \to \{0,1\}^k$ be the function recursively defined by the formula

$$h_S^{(t)}(M_1 M_2) = h_S(h_S^{(t-1)}(M_1), h_S^{(t-1)}(M_2)), \quad M_1, M_2 \in \{0,1\}^{2^{t-1}k}$$

with $h_S^{(1)} = h_S$. Show that $\{h_S^{(t)}\}$ is a cryptographic hash family for input length $2^t k$ (for appropriate parameters).

Problem 4

Suppose $\{F_K\colon \{0,1\}^k \to \{0,1\}^k \mid K \in \{0,1\}^k\}$ is a family of functions. Consider the following family of functions $\{G_{K,S}\colon \{0,1\}^k \to \{0,1\}^k \mid K, S \in \{0,1\}^k\}$:

$$G_{K,S}(x) = \begin{cases} F_K(x), & \text{if } x \neq S \\ F_K(0^k), & \text{if } x = S. \end{cases}$$

You will argue that $\{G_{K,S}\}$ is a pseudorandom function family, but not a cryptographic hash family.

(a) Show that if $\{F_K\}$ is a pseudorandom function family, so is $\{G_{K,S}\}$ (with appropriate parameters).

(b) Show that $\{G_{K,S}\}$ is not a cryptographic hash family.