CSCI 5440: Cryptography
The Chinese University of Hong Kong

Midterm Exam
due Wednesday 14 November

Please turn in your solutions on **Wednesday 14 November** in the beginning of class. If you are not coming to class that day please send me the solutions by email before 10.30am.

You must work on the problems and write up the solutions individually. No collaboration is allowed. You are free to consult the lecture notes, homework solutions, and references listed on the course web page. However, you are not allowed to look for solutions in external sources, including textbooks, other lecture notes, and the internet.

Use asymptotic definitions of security. All schemes are private key.

Problem 1

Let $\{F_K \colon \{0,1\}^k \to \{0,1\}^n\}$ be a pseudorandom function family. Let $G_K \colon \{0,1\}^{k-1} \to \{0,1\}^{2n}$ be the function

$$G_K(x) = (F_K(x0), F_K(x1)).$$

Show that $\{G_K\}$ is a pseudorandom function family.

Problem 2

A bit encryption scheme is an encryption scheme in which there are only two messages, $M = 0$ and $M = 1$. Let $\{F_K \colon \{0,1\}^{k+1} \to \{0,1\}^k\}$ be a pseudorandom function family. Consider the following bit encryption scheme:[1]

$$Enc(K, M) = (R, F_K(R, M)) \quad \text{where } R \sim \{0,1\}^k \text{ is random}$$

$$Dec(K, (R, C)) = \begin{cases} 0, & \text{if } F_K(R, 0) = C \\ 1, & \text{if } F_K(R, 1) = C \\ \texttt{error}, & \text{otherwise.} \end{cases}$$

(a) Show that this bit encryption scheme is CPA-secure.

(b) **(Extra credit)** Is the scheme CCA-secure?

[1] The scheme does not technically meet our definition of functionality because it is not well-defined in the case $F_K(R, 0) = F_K(R, 1)$, but this event has negligible probability if F_K is pseudorandom.

Problem 3

Assume (Tag, Ver) is a secure MAC for message length m. Is the following MAC secure for message length $2m$?

$$Tag'(K, M_1M_2) = (Tag(K, M_1), Tag(K, M_1 + M_2))$$

$$Ver'(K, M_1M_2, (T_1, T_2)) = \begin{cases} 1, & \text{if } Ver(K, M_1, T_1) = Ver(K, M_1 + M_2, T_2) = 1 \\ 0, & \text{otherwise.} \end{cases}$$

Here, M_1 and M_2 are in $\{0,1\}^m$.

Problem 4

Let $f, f' \colon \{0,1\}^n \to \{0,1\}^n$ be two efficiently computable permutations. Assume that at least one of f and f' is a one-way permutation. Show that $g(x, x') = (f(x), f'(x'))$ is a one-way permutation.