CSCI 5440: Cryptography — Take Home Midterm
The Chinese University of Hong Kong, Spring 2018 — due Tuesday 13 March

Please turn in your solutions in class on Tuesday 13 March. You must work on the problems and write the solutions on your own. You are free to consult the lecture notes and homework solutions. You are not allowed to discuss the exam or use external sources such as books, other lecture notes, and the internet. Work out the quantitative dependencies between the parameters.

Question 1

Assume that exactly one among F and F' is a pseudorandom function. Show that (a) $F_K(x) \oplus F'_{K'}(x)$ with independent K, K' is a pseudorandom function, but (b) $F_K(x) \oplus F'_K(x)$ might not be one.

Question 2

Consider the following DDH-based protocol for Alice, Bob, and Charlie to sample a shared secret key.

0. Alice samples $A \sim \mathbb{Z}_q$. Bob samples $B \sim \mathbb{Z}_q$. Charlie samples $C \sim \mathbb{Z}_q$.
1. Alice sends $h_{AB} = g^A$ to Bob. Bob sends $h_{BC} = g^B$ to Charlie. Charlie sends $h_{CA} = g^C$ to Alice.
2. Alice sends $k_{AB} = h_{CA}^A$ to Bob. Bob sends $k_{BC} = h_{AB}^B$ to Charlie. Charlie sends $k_{CA} = h_{BC}^C$ to Alice.
3. Alice (privately) outputs $PK_A = k_{CA}^A$. Bob outputs $PK_B = k_{AB}^B$. Charlie outputs $PK_C = k_{BC}^C$.

As usual, $p = 2q + 1$ is a safe prime and $g \in \mathbb{G}$ is a quadratic residue modulo p. Show the following.

(a) PK_A, PK_B, and PK_C are all equal and identically distributed to a random element of $\mathbb{G}$.

(b) Under the DDH assumption, (T, PK_A) is simulatable by a pair of independent random variables, where T is the transcript.

Question 3

Assuming pseudorandom functions exist, show that there is a private-key identification scheme that is (a) secure against eavesdropping but (b) insecure against impersonation. (**Hint:** Modify the challenge-response protocol from Lecture 5.)

Question 4

Consider a two-party protocol by which Alice and Bob compute $f(x, y)$ (x is Alice's input, y is Bob's input, and $f(x, y)$ is Bob's output). Assume the protocol is simulatable against honest-but-curious parties. Eve, who knows neither x nor y, observes the transcript $T(x, y)$. Which of the following is true? Give a proof or a counterexample.

(a) For all x, y, and y', $T(x, y)$ and $T(x, y')$ are indistinguishable.

(b) For all x, x', and y, $T(x, y)$ and $T(x', y)$ are indistinguishable.

(c) For all x, x', y and y', $T(x, y)$ and $T(x', y')$ are indistinguishable when $f\colon \{0, 1, 2\} \times \{0, 1, 2\} \to \{0, 1\}$ is the equality function $f(x, y) = 1$ if $x = y$ and 0 if $x \neq y$.