CSCI 5440: Cryptography — Take Home Midterm
The Chinese University of Hong Kong, Fall 2020 — due Tuesday 3 November

Please submit your solutions here by Tuesday 3 November. You must work on the problems and write the solutions on your own; collaboration is not allowed. You are free to consult the lecture notes and homework solutions. Please avoid using external references but if you must do provide the source. If you have questions please contact the instructor privately.

Question 1

Alice and Bob have two independent random shared secret keys $K_0, K_1 \in \{0,1\}^k$, one of which has been leaked to Eve, but they don't know which one.

(a) Define (s, q, ε)-universal CPA simulatability against 1-of-2 leaked keys. (**Hint:** Eve gets an input.)

(b) Given an (s, q, ε)-pseudorandom function F_K of circuit size t, describe a secret-key encryption scheme and prove it is (s', q', ε')-simulatable against 1-of-2 leaked keys for a suitable choice of s', q', and ε'.

Question 2

Let F_K be a pseudorandom function and $H_{K'}$ be a hash function, both of size t. Let $F'_{K,K'}(x) = F_K(H_{K'}(x))$. Assume K, K' are independent and K' is public (it is given to the PRF distinguisher as input).

(a) Show that if F is $(s + t, q, \varepsilon)$-pseudorandom and H is $(s + O(q^2 t), \varepsilon)$-collision resistant then F' is an $(s, q, 2\varepsilon)$-pseudorandom function.

(b) Show that if H is not (s, ε)-collision resistant then F' is not an $(s + O(t), 2, \varepsilon - 2^{-m})$-pseudorandom function, where m is the output length of F.

Question 3

Alice and Bob have private keys A, B and public keys $PK_A = g^A, PK_B = g^B$, respectively, where g is a quadratic residue modulo a safe prime. Charlie encrypts his message M by $(g^R, PK_A^R \cdot PK_B^R \cdot M)$ with a random exponent R.

(a) Explain how together Alice and Bob can decrypt M.

(b) Show that under the (s, ε)-DDH assumption, Alice's view $(A, PK_B, g^R, PK_A^R \cdot PK_B^R \cdot M)$ is $(s - O(t), \varepsilon)$-simulatable (without knowing M), where t is the circuit size of a group operation.

Question 4

Consider the following two-party computation for the equality function ($f(x, y) = 1$ if $x = y$ and 0 if not), where x, y are base-g exponents (i.e., they are considered equal if $g^x = g^y$):

1. Alice sends (g^R, g^{xR}) for a random R.
2. Upon receiving (h, k), Bob outputs 1 if $h^y = k$ and 0 otherwise.

Assuming base-g DDH, is this computation simulatable against honest-but-curious parties? Prove your claim (with a suitable choice of parameters).