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.

**Solution:** Assume $F$ is $(s, q, \varepsilon)$-pseudorandom and has size $t$. We show $F_K \oplus F'_{K'}$ is $(s - t, q, \varepsilon)$-pseudorandom. For part (a), suppose $D$ distinguishes it from a random function and take the distinguisher $D'$ that makes the same oracle queries as $D$ but shifts the answer by $F_{K'}(x)$ for a random key $K'$. The views $D'^{F_K}$ are identical to $D^{F_K \oplus F'_{K'}}$, and so are their views when given a random function as an oracle (because a random function shifted by $F'$ is still random. So $D'$ distinguishes the two with the same advantage.
For part (b) let $F'$ be the same function as $F$ except that $F'_K(0) = 0$ and $F'_K(1) = F_K(1)$. Then $F'_K$ is not pseudorandom because of the first condition, and $F_K \oplus F'_K$ is not because of the second 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 $O(1/q)$-close to a random element of $\mathbb{G}$.

**Solution:** $PK_A = k_{CA}^A = h_{BC}^{CA} = g^{BCA}$. This equals $g^{ABC}$, and by symmetry so do the others. $g^{ABC}$ can be distinguished from $g^R$ for a random $R$ only if one of $A$, $B$, $C$ is zero. By a union bound event has probability at most $3/q$.

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

**Solution:** We show that under $(s, \varepsilon)$-DDH, $(T, PK_A)$ is $(s - 8t, 2\varepsilon)$ indistinguishable from a pair of independent random variables, where $t$ is the time it takes to exponentiate. Consider the three random variables

$$\begin{aligned}(T, PK_A) = &(g^A, g^B, g^C, g^{AB}, g^{BC}, g^{AC}, g^{ABC})\\ &(g^A, g^B, g^C, g^X, g^{BC}, g^{AC}, g^{XC})\\ &(g^A, g^B, g^C, g^X, g^{BC}, g^{AC}, g^Y).\end{aligned}$$

If the first two can be distinguished then so can $(g^A, g^B, g^{AB})$ and $(g^A, g^B, g^X)$ at the cost of raising four inputs to the $C$-th power for a random $C$. If the last two can be distinguished so can $(g^C, g^X, g^{XC})$ and $(g^C, g^X, g^Y)$ at the cost of raising four inputs to the $A$-th/$B$-th power for random $A/B$. In the last random variable $g^Y$ is independent of the rest as desired.

## 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.)

**Solution:** Consider the challenge-response mechanism but first modify the pseudorandom function so that $F_K(0) = K$. An impersonator can challenge the prover on input 0, find the secret key $K$ and pass validation. On the other hand, if the unmodified PRF was $(s, q, \varepsilon)$-secure then the view of a $q$-query eavesdropper on the modified and unmodified PRFs are $q \cdot 2^{-n}$-indistinguishable so the scheme is still $(s, q+1, \varepsilon + q \cdot 2^{-n})$-secure against eavesdropping.

## 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.

**Solution:** Yes. Since Alice's view is $(s, \varepsilon)$-simulatable from her input $x$, her views when Bob uses any two inputs $y, y'$ are both $(s, \varepsilon)$-simulatable so they are $(s, 2\varepsilon)$-indistinguishable. If Eve could distinguish the two transcripts then Alice could distinguish her two views.

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

**Solution:** No. Consider the trivial XOR protocol by which Alice sends $x$ and Bob outputs $x \oplus y$. This is perfectly secure for Bob, but Eve can distinguish the views $T(0, y)$ and $T(1, y)$.

(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 $x \neq y$.

**Solution:** Yes. The views in part (b) are indistinguishable for Bob (and therefore for Eve) under the additional assumption $f(x, y) = f(x', y)$ because then Bob can simulate both from his input and output. For the equality function and every pair $x, x'$ there always exists $y^*$ such that $f(x, y^*) = f(x', y^*)$. By part (a), $T(x, y)$ and $T(x, y^*)$ are $(s, 2\varepsilon)$-indistinguishable, and so are $T(x', y')$ and $T(x', y^*)$. Since $f(x, y^*)$ and $f(x', y^*)$, $T(x, y^*)$ and $T(x', y^*)$ are also $(s, 2\varepsilon)$-indistinguishable. By the triangle inequality, $T(x, y)$ and $T(x', y')$ are $(s, 6\varepsilon)$-indistinguishable.