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 \((s,q,\varepsilon)\)-universal CPA simulatability against 1-of-2 leaked keys. (Hint: Eve gets an input.)

Solution: The encryption scheme \((\text{Enc}, \text{Dec})\) is \((s,q,\varepsilon)\)-universal CPA simulatable (by size \(t\)) if for every \(b \in \{0,1\}\), the view of any size-\(s\), \(q\)-query oracle circuit \(A\) there exists a simulator \(\text{Sim}\) (of size \(t\)) such that the view of \(A\) on input \(K_b\) when interacting with the encryption oracle \(\text{Enc}(K_0 K_1, \cdot)\) is \((s,q,\varepsilon)\)-indistinguishable from the output of \(\text{Sim}(K_b)\).

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

Solution: One such scheme is \(\text{Enc}(K_0 K_1, M) = \text{Enc}'(K_0 + K_1, M)\) and \(\text{Dec}(K_0 K_1, C) = \text{Dec}'(K_0 + K_1, C)\), where \((\text{Enc}', \text{Dec}')\) is the CPA secure private key encryption scheme from Lecture 3 (based on the PRF \(F_K\)). We argue that if \((\text{Enc}', \text{Dec}')\) is simulatable against standard adversaries then \((\text{Enc}, \text{Dec})\) is simulatable with the same parameters against 1-of-2 leaked keys. Since \(K_0 + K_1\) is independent of \(K_b\), so are the CPA oracle answers of \(\text{Enc}(K_0 K_1, \cdot)\). Therefore the view of \(D(K_b)\) when interacting with \(\text{Enc}(K_0 K_1, \cdot)\) is identically distributed with its view when interacting with \(\text{Enc}'(K', \cdot)\), when \(K'\) is a key independent of \(K_b\). As \(K_b\) is independent of the oracle answers we may view is at internal randomness of the distinguisher \(D\) and so its view is identical to that of an adversary for \((\text{Enc}', \text{Dec}')\) and therefore simulatable with the same parameters. By Theorem 8 in Lecture 3 the value of these parameters can be taken as \((s' = s - O(mq), q' = q, \varepsilon' = \varepsilon + \left(\frac{t}{2}\right) \cdot 2^{-n})\).

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

Solution: Consider the “hybrid” function \(R \circ H_{K'}\) given by \(R(H_{K'}(x))\) where \(R\) is a random function. The view of any distinguisher \(D(K')\) when querying \(R \circ H_{K'}\) is identical to its view when querying a truly random function, unless it happened to query two inputs \(x \neq x'\) that collide under \(H_{K'}\). In case this event happens, a collision for \(H_{K'}\) can be found by going over all \({\binom{q}{2}}\) pairs of queries and reporting the colliding one, which takes \(O(q^2 t)\) gates to implement. Assuming \(H_{K'}\) is \((s + O(q^2 t), \varepsilon)\)-collision resistant, \(R \circ H_{K'}\) is therefore \((s, q, \varepsilon)\)-pseudorandom.

On the other hand, if \(R \circ H_{K'}\) is \((s, q, \varepsilon)\)-distinguishable from \(F'_{K,K'} = F_K \circ H_{K'}\) then \(R\) is \((s + qt, q, \varepsilon)\)-distinguishable from \(F_K\). When the latter distinguisher queries \(x\), the former queries \(H_{K'}(x)\) accounting for the additional \(qt\) gates. As \(R \circ H_{K'}\) is \((s, q, \varepsilon)\)-pseudorandom and \((s, q, \varepsilon)\)-indistinguishable from \(F'\), by the triangle inequality \(F'\) is \((s, q, 2\varepsilon)\)-pseudorandom.
b) Show that if $H$ is not $(s, \varepsilon)$-collision resistant then $F'$ is not an $(s + O(t), 2, \varepsilon - 2^{-m})$-pseudorandom function, where $m$ is the output length of $F$.

**Solution:** Suppose $C(K')$ finds a collision $x \neq x'$ for $H_{K'}$. Then the circuit $D$ that queries its oracle on $x$ and $x'$ and accepts iff their answers are equal distinguishes $F'$ from a random function $R'$ except when $R'(x) = R'(x')$, an event of probability $2^{-m}$. As $C$ finds a collision with probability more than $\varepsilon$, $D$ distinguishes with probability more than $\varepsilon - 2^{-m}$.

**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 $M$.

**Solution:** Alice and Bob output $\text{Dec}((A, B), (h, c)) = h^{-A-B} \cdot c$. Then

\[
\text{Dec}((A, B), (g^R, PK_A^R \cdot PK_B^R \cdot M)) = (g^R)^{-A-B} \cdot g^{AR} \cdot g^{BR} \cdot M = M.
\]

(b) Show that under the $(s, \varepsilon)$-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.

**Solution:** Alice’s view is $(A, g^B, g^R, g^{AR} \cdot g^{BR} \cdot M)$. The simulator outputs $(A, g^B, g^R, g^Z)$ where $B, R, Z$ are independent random exponents. Suppose some $D$ of size $s$ distinguishes these two views with advantage $\varepsilon$ for some $M$. Then the distinguisher $D'$ that on input $(b, r, z)$ outputs $D(A, b, r, z^A \cdot M^{-1})$ for a random exponent $A$ produces Alice’s view when $b = g^B, r = g^B, z = g^{BR}$ and the output of the sampler when $z$ is independent of $b$ and $r$, thereby invalidating the $(s+O(t), \varepsilon)$-DDH assumption.

**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).

**Solution:** No. Let $(h, k)$ be Bob’s view on inputs $(x = 1, y = 0)$ and $(h', k')$ be Bob’s view on inputs $(x = 2, y = 0)$. Then $(h, k)$ and $(h', k')$ are $(O(\log q), 1 - O(1/q))$-distinguishable because $h$ equals $k$ with probability one while $h'$ equals $k'$ only when $R = 0$, an event with probability $O(1/q)$. Bob’s input and output are the same in both cases $(y = 0$ and $f(x, y) = 0$, so by the triangle inequality at least one of them is not $O(\log q, 1/2 - O(1/q))$-simulatable (by a simulator of any size) from Bob’s input and output.