Homework 2′

This problem set is due in class on **Thursday, March 23.**

Do only the problems that you got wrong on Homework 2. (See the ones listed under "Try again:" on the front page of your returned solution to HW2.) This time, prove all statements carefully and in full detail. Do not skip any steps. Make sure you give a fully specified reduction. Define all adversaries precisely. Define all events, random variables, and probabilities clearly and unambiguously, and show your work when calculating advantages and probabilities. Use standard notation. Double-check the details to make sure that all steps are fully justified.

Reprise of 3(a)

Prove the following theorem.

Theorem 1. *If $F : \mathcal{K} \times \mathcal{M} \to \mathcal{S}$ is a (t, q, ϵ)-PRF, then $H : \mathcal{K} \times (\mathcal{M} \times \mathcal{S}) \to \mathcal{S}$ defined by $H_k(x, y) = F_k(x) \oplus y$ is $\epsilon + \frac{1}{|\mathcal{S}|}$-weakly 2-universal.*

Reminder: We say that $H : \mathcal{K} \times \mathcal{M} \to \mathcal{S}$ is *ϵ-weakly 2-universal* if $\Pr[K \xleftarrow{\$} \mathcal{K}; H_K(x) = H_K(x')] \le \epsilon$ for all $x, x' \in \mathcal{M}$ with $x \ne x'$.

Reprise of 3(b)

Prove the following theorem.

Theorem 2. *If H is ϵ-weakly 2-universal and F is a (t, q, ϵ')-PRF, then F' defined by $F_{k,k'}(x) = F_k(H_{k'}(x))$ is a $(t - O(q), q, \epsilon' + \binom{q}{2}\epsilon)$-PRF.*

Reprise of 5(b)

Let (E, D) be a symmetric-key encryption scheme. Define V by

$$V_k(c) = \begin{cases} \text{false} & \text{if } D_k(c) = \perp \\ \text{true} & \text{otherwise.} \end{cases}$$

Say that (E, D) is (t, q_s, q_v, ϵ)-*secure against reaction attacks* if, for all adversaries A running in time t and making at most q_s queries to their first oracle and at most q_v queries to their second oracle, we have

$$\left|\Pr[K \xleftarrow{\$} \mathcal{K}; A^{E_K, V_K} = 1] - \Pr[K \xleftarrow{\$} \mathcal{K}; A^{E_K \circ \$, V_K} = 1]\right| \le \epsilon.$$

Prove the following theorem:

Theorem 3. *If (E, D) is (t, q_s, q_v, ϵ)-IND-CCA2 secure, then (E, D) is $(t - O(q_v), q_s, q_v, \epsilon)$-secure against reaction attacks.*