CS-690C: Homework 3

Do NOT look at Boneh-Shoup for this assignment.

Problem 1. (100 points.)

(Part A - 40 points.) Let $t, q \in \mathbb{N}$ and $\varepsilon = \varepsilon(t, q)$ where $0 \leq \varepsilon \leq 1$. Define an appropriate notion of (t, q, ε)-UF-CMA-secure message authentication code. Here t is the bound on the running-time of the adversary, q is the bound on its number of queries, and ε is the bound on its advantage.

(Part B - 60 points.) For $k, m, n \in \mathbb{N}$, let $H\colon \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^m$ be pairwise independent. Show that H is a $(\infty, 1, 2^{-m})$-UF-CMA secure message authentication code. Here '∞' indicates an unbounded running-time.

(Part C - 50 points extra credit.) Extend the definition of pairwise independence to t-wise independence for arbitrary $t \in \mathbb{N}$. (Do not look up the definition; write the natural extension.) Give two equivalent definitions for it, as we gave in class for pairwise independence. Appropriately strengthen and prove the result from Part B in the case H is t-wise independent.