CS 435: Introduction to Cryptography **2012 Fall**

Homework 3

Professor Somesh Jha **Due:** November 5

1. (Problem 3.3) Prove that Definition 3.8 cannot be satisfied if Π can encrypt arbitrary-length messages and the adversary is *not* restricted to outputting equal-length messages in experiment $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}$.

   Hint. Let $q(n)$ be a polynomial upper-bound on the length of the ciphertext when Π is used to encrypt a single bit. Then consider an adversary who outputs $m_0 \in \{0,1\}$ and a random $m_1 \in \{0,1\}^{q(n)+2}$.

2. (Problem 3.6) Let G be a pseudorandom generator where $|G(s)| > 2 \cdot |s|$.

   (a) Define $G'(s) := G(s0^{|s|})$. Is G' necessarily a pseudorandom generator?

   Note. You don't need to be totally rigorous here.

   (b) Define $G'(s) := G(s_1 s_2 \cdots s_{n/2})$, where $s = s_1 s_2 \cdots s_n$. Is G' necessarily a pseudorandom generator?

   Hint. Think about this problem in terms of "reducing" the pseudorandomness of G' to the pseudorandomness of G. If G' is not a pseudorandom generator, does this produce a contradiction?

3. (Problem 3.16) Consider a variant of CBC-mode encryption where the sender simply imcrements the IV by 1 each time a message is encrypted (rather than choosing IV at random each time). Show that the resulting scheme is *not* CPA-secure.

4. In class, we drew a decryption diagram for Cipher Block Chaining mode that corresponds to the encryption diagram (Figure 3.6) in the text. Draw the corresponding decryption diagrams for Output Feedback (Figure 3.7) and Counter (Figure 3.8) modes. Can encryption and decryption be parallelized easily for these two modes?