Lecture 06 ()

TIL: People print lecture PDFs :O

1 (Final) Solution to Question 04.02

Consider probabilities p_0 and p_1 such that adversary guesses 0 in world 0 and 1 respectively. Consider hybrid world where $(enc(m_0, k_1), enc(m_1, k_2))$ is sent, let the probability of guessing 0 is p_h.

We have two cases for p_h:

1.1 Case 1

$$|p_h - p_0| = \delta$$

B sends $(enc(m_0, k_1), ct)$. If p_h is larger, then we guess $\neg\hat{b}$ else $\hat{b}$, where $\hat{b}$ is the guess of A.

1.2 Case 2

$$|p_h - p_1| = \delta$$

B sends $(ct, enc(m_0, k_2))$. If p_h is larger, then we guess $\neg\hat{b}$ else $\hat{b}$, where $\hat{b}$ is the guess of A.

2 Security of E_G

Assume that $\exists A$ which breaks E_G, then $\exists B$ which breaks G (assuming E is secure)