Instructor: Adam O'Neill
adamo@cs.umass.edu

CS-690C: Homework 4

Problem 1. (20 points.) Find a popular news article about cryptography and provide a link to it. Critique it from a technical perspective. Did they do a good job explaining the main ideas? Is there anything they got wrong? Anything they did well? Anything they should have added?

Problem 1. (80 points.)

Let $\mathsf{AE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be a public-key encryption scheme with message space MsgSp. For $n \in \mathbb{N}$ define the *n-fold parallel composition of* AE as $\mathsf{AE}^n = (\mathcal{K}^n, \mathcal{E}^n, \mathcal{D}^n)$ with message space MsgSp^n as follows. Algorithm $\mathcal{K}^n$ outputs

$$((pk_1, \ldots, pk_n), (sk_1, \ldots, sk_n))$$

where $(pk_i, sk_i) \leftarrow\!\!\$\, \mathcal{K}$ for all $i \in [n]$. Algorithm $\mathcal{E}^n$ on inputs $(pk_1, \ldots, pk_n), (m_1, \ldots, m_n)$ outputs $(c_1, \ldots, c_n)$ where $c_i \leftarrow\!\!\$\, \mathcal{E}(pk_i, m_i)$ for all $i \in [n]$. Algorithm $\mathcal{D}^n$ is defined accordingly. Show that AE^n is IND-CPA if AE is. You should formulate and prove a corresponding concrete security statement.