CS60084: Foundations of Cryptography
Spring 2019

April 12, 2019

Tutorial 6: One-way Functions

Submission Guidelines All problems must be solved in class today. Searching on the internet for solutions is strictly discouraged.

1. Show that any IND-EAV-secure private-key encryption scheme implies the existence of a one-way function.

2. Suppose $f : \{0,1\}^n \rightarrow \{0,1\}^n$ is a one-way function. Prove that the function $g : \{0,1\}^{2n} \rightarrow \{0,1\}^{2n}$ defined as $g(x_1, x_2) = (f(x_1), x_2)$ for $x_1, x_2 \in \{0,1\}^n$ is also one-way.

3. Show (formally) that if a one-to-one function has a hard-core predicate, then it is one-way. Where exactly do you need the one-to-one property?