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.

   A: Refer to Katz-Lindell book (section 6.7) for the proof.

2. Suppose $f : \{0,1\}^n \to \{0,1\}^n$ is a one-way function. Prove that the function $g : \{0,1\}^{2n} \to \{0,1\}^{2n}$ 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.

   A: Let $\mathscr{A}_g$ be an inverting adversary for g. We construct an adversary $\mathscr{A}_f$ that inverts f.

   Description of $\mathscr{A}_f$:

   - $\mathscr{A}_f$ received $f(x)$ for some $x \xleftarrow{\text{U}} \{0,1\}^n$.
   - It then picks $x_2 \xleftarrow{\text{U}} \{0,1\}^n$ and provides $g(x, x_2) = (f(x), x_2)$ to $\mathscr{A}_g$.
   - $\mathscr{A}_q$ sends some $x', x_2' \in \{0,1\}^n$ and halts.
   - $\mathscr{A}_f$ just relays x' to its challenger and terminates.

   Clearly,
   $$\Pr[\mathscr{A}_f \text{ wins}] = \Pr[f(x') = f(x)] = \Pr[g(x', x_2') = g(x, x_2')] = \Pr[\mathscr{A}_g \text{ wins}]$$
   thus implying that if f is one-way, then so is g.

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?

   A: Let $f : X \to Y$ be a 1-1 function and let hc be a hard-core predicate for f. Let $\mathscr{A}$ be an adversary inverting f. We show how to build a prediction adversary $\mathscr{B}$ for hc.

   Description of $\mathscr{B}$:

   - Receives from its challenger $y = f(x)$ for some $x \xleftarrow{\text{U}} X$.
   - Provides y to $\mathscr{A}$ and receives $x' \in X$ in return.
   - Returns $\mathsf{hc}(\mathsf{x}')$ and halts.

   If $\mathscr{A}$ wins, then $f(x') = f(x)$. f is 1-1 implies that $x = x'$ and hence $\mathsf{hc}(\mathsf{x}) = \mathsf{hc}(\mathsf{x}')$. In this case, $\mathscr{B}$ wins. We therefore can conclude that hc is (ε, t)-hardcore predicate for f implies that f is $(\varepsilon, t - O(1))$ one-way.