MTAT.07.003 Cryptology II
Spring 2012 / Exercise session ?? / Example Solution

Exercise (Prediction of randomised functions). *Let $g : \mathcal{S} \times \Omega \to \mathcal{Y}$ be a randomised function and let $f : \mathcal{S} \to \mathcal{X}$ be a function such that any two states $s_0, s_1 \in \mathcal{S}$ are (t, ε)-indistinguishable given the output $f(s_i)$. Prove that a function $f^* : \mathcal{S} \times \Omega \to \mathcal{X}$ defined as $f_*(s, \omega) = f(s)$ is also such that any two states $(s_0, \omega_0), (s_1, \omega_1) \in \mathcal{S} \times \Omega$ are (t, ε)-indistinguishable given the output $f_*(s_i, \omega_i)$ and that*

$$\mathsf{Adv}^{\mathsf{sem}}_{f,g}(\mathcal{A}) = \mathsf{Adv}^{\mathsf{sem}}_{f_*,g_*}(\mathcal{A})$$

where $g_*(s, \omega) = g(s, \omega)$ is a deterministic function over extended state space $\mathcal{S} \times \Omega$.

Solution. Indistinguishability of states. For the first part of the proof we must estimate the computational distance of following games:

$$\mathcal{G}_{s_0,\omega_0}\ \left[\begin{array}{l} x \leftarrow f_*(s_0, \omega_1) \\ \textbf{return } \mathcal{A}(x) \end{array}\right. \qquad \mathcal{G}_{s_1,\omega_1}\ \left[\begin{array}{l} x \leftarrow f_*(s_1, \omega_1) \\ \textbf{return } \mathcal{A}(x) \end{array}\right. .$$

By the definition of function f_*, we can simplify these games:

$$\mathcal{G}_{s_0,\omega_0}\ \left[\begin{array}{l} x \leftarrow f(s_0) \\ \textbf{return } \mathcal{A}(x) \end{array}\right. \qquad \mathcal{G}_{s_1,\omega_1}\ \left[\begin{array}{l} x \leftarrow f(s_1) \\ \textbf{return } \mathcal{A}(x) \end{array}\right. .$$

Since these games do not depend on ω_0 and ω_1, we can observe the following games:

$$\mathcal{G}_{s_0}\ \left[\begin{array}{l} x \leftarrow f(s_0) \\ \textbf{return } \mathcal{A}(x) \end{array}\right. \qquad \mathcal{G}_{s_1}\ \left[\begin{array}{l} x \leftarrow f(s_1) \\ \textbf{return } \mathcal{A}(x) \end{array}\right. .$$

By the security assumption for f, the games $\mathcal{G}_{s_0}$ and $\mathcal{G}_{s_1}$ is (t, ε)-indistinguishable. Hence, for any t-time adversary $\mathcal{A}$, the advantage of distinguishing games $\mathcal{G}_{s_0,\omega_0}$ and $\mathcal{G}_{s_1,\omega_1}$ is bounded:

$$\begin{aligned}\mathsf{Adv}^{\mathsf{ind}}_{(s_0,\omega_0),(s_1,\omega_1)}(\mathcal{A}) &= \left|\Pr\left[\mathcal{G}^{\mathcal{A}}_{s_0,\omega_0} = 1\right] - \Pr\left[\mathcal{G}^{\mathcal{A}}_{s_1,\omega_1} = 1\right]\right| \\ &= \left|\Pr\left[\mathcal{G}^{\mathcal{A}}_{s_0} = 1\right] - \Pr\left[\mathcal{G}^{\mathcal{A}}_{s_1} = 1\right]\right| = \mathsf{Adv}^{\mathsf{ind}}_{s_0,s_1}(\mathcal{A}) \leq \varepsilon \ .\end{aligned}$$

This proves the desired claim about indictinguishability of extended states.

Guessing advantage. Recall that the advantage $\mathsf{Adv}^{\mathsf{sem}}_{f,g}(\mathcal{A})$ can be expressed as the distance between the following games

$$\mathcal{G}_0\ \left[\begin{array}{l} s \leftarrow \mathcal{S} \\ x \leftarrow f(s) \\ \textbf{return } [g(s) \stackrel{?}{=} \mathcal{A}(x)] \end{array}\right. \qquad \mathcal{G}_1\ \left[\begin{array}{l} s \leftarrow \mathcal{S} \\ x \leftarrow f(s) \\ \textbf{return } [g(s) \stackrel{?}{=} y_\circ] \end{array}\right.$$

where $y_\circ$ is the must probable outcome of $g(s)$. Analogously, $\mathsf{Adv}^{\mathsf{sem}}_{f_*,g_*}(\mathcal{A})$ can be expressed as the distance between the following games

$$\mathcal{Q}_0\ \left[\begin{array}{l} s \leftarrow \mathcal{S} \\ \omega \leftarrow \Omega \\ x \leftarrow f_*(s, \omega) \\ \textbf{return } [g_*(s, \omega) \stackrel{?}{=} \mathcal{A}(x)] \end{array}\right. \qquad \mathcal{Q}_1\ \left[\begin{array}{l} s \leftarrow \mathcal{S} \\ \omega \leftarrow \Omega \\ x \leftarrow f_*(s, \omega) \\ \textbf{return } [g_*(s, \omega) \stackrel{?}{=} y_*] \end{array}\right.$$

where y_* is the must probable outcome of $g_*(s,\omega)$. First, note that $y_\circ$ coincides with y_*, since by definition

$$y_\circ = \operatorname*{argmax}_{y\in\mathcal{Y}} \Pr\left[s \leftarrow \mathcal{S} : g(s) \stackrel{?}{=} y\right] = \operatorname*{argmax}_{y\in\mathcal{Y}} \Pr\left[s \leftarrow \mathcal{S}, \omega \leftarrow \Omega : g(s,\omega) \stackrel{?}{=} y\right] = y_* \ .$$

Second, note that we can explicitly sample the randomness used to evaluate g in the first set of games:

$$\begin{array}{ll}
\mathcal{G}_0 & \qquad\qquad \mathcal{G}_1 \\
\left[\begin{array}{l} s \leftarrow \mathcal{S} \\ \omega \leftarrow \Omega \\ x \leftarrow f(s) \\ \textbf{return } [g(s,\omega) \stackrel{?}{=} \mathcal{A}(x)] \end{array}\right. & \qquad\qquad \left[\begin{array}{l} s \leftarrow \mathcal{S} \\ \omega \leftarrow \Omega \\ x \leftarrow f(s) \\ \textbf{return } [g(s,\omega) \stackrel{?}{=} y_\circ] \ . \end{array}\right.
\end{array}$$

Now if we substitute the definitions of f_* and g_* into the second set of games, we get games

$$\begin{array}{ll}
\mathcal{Q}_0 & \qquad\qquad \mathcal{Q}_1 \\
\left[\begin{array}{l} s \leftarrow \mathcal{S} \\ \omega \leftarrow \Omega \\ x \leftarrow f(s) \\ \textbf{return } [g(s,\omega) \stackrel{?}{=} \mathcal{A}(x)] \end{array}\right. & \qquad\qquad \left[\begin{array}{l} s \leftarrow \mathcal{S} \\ \omega \leftarrow \Omega \\ x \leftarrow f(s) \\ \textbf{return } [g(s,\omega) \stackrel{?}{=} y_\circ] \end{array}\right.
\end{array}$$

that are identical to the first set of games. Hence,

$$\mathsf{Adv}^{\mathsf{sem}}_{f,g}(\mathcal{A}) = \left|\Pr\left[\mathcal{G}_0^{\mathcal{A}} = 1\right] - \Pr\left[\mathcal{G}_1^{\mathcal{A}} = 1\right]\right| = \left|\Pr\left[\mathcal{Q}_0^{\mathcal{A}} = 1\right] - \Pr\left[\mathcal{Q}_1^{\mathcal{A}} = 1\right]\right| = \mathsf{Adv}^{\mathsf{sem}}_{f_*,g_*}(\mathcal{A})$$

as desired. The claim about prediction success follows.