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

Exercise (Coin-fixing and semantic-security). *Let $\mathcal{S}$ be a distribution of secret values. Then the semantic security of a function f against predicting a function g is defined through an advantage*

$$\mathsf{Adv}^{\mathsf{sem}}_{f,g}(\mathcal{A}) = \Pr\left[s \leftarrow \mathcal{S} : \mathcal{A}(f(s)) = g(s)\right] - \max_{y_* \in \mathcal{Y}} \Pr\left[s \leftarrow \mathcal{S} : g(s) = y_*\right] \quad .$$

Show that we cannot a priory postulate that deterministic functions are easier to predict. In particular, show that there may exist $\mathcal{A}$ and a randomised function $g : \mathcal{S} \times \Omega \to \mathcal{Y}$ such that

$$\mathsf{Adv}^{\mathsf{sem}}_{f,g}(\mathcal{A}) \leq \max_{\omega \in \Omega} \left\{\mathsf{Adv}^{\mathsf{sem}}_{f,g_\omega}(\mathcal{A})\right\} \tag{1}$$

where $g_\omega : \mathcal{S} \to \mathcal{Y}$ is a deterministic function defined as $g_\omega(s) = g(s, \omega)$.

Solution. Let us first express definitions in terms of corresponding security games. The advantage $\mathsf{Adv}^{\mathsf{sem}}_{f,g}(\mathcal{A})$ can be expressed as the distance between the following games

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

where y_* is the must probable outcome of $g(s)$. Now for a fixed random value ω, the advantage $\mathsf{Adv}^{\mathsf{sem}}_{f,g_\omega}(\mathcal{A})$ can be expressed as the distance between the following games

$$\begin{array}{ll}
\mathcal{G}_{0\omega} & \mathcal{G}_{1\omega} \\
\left[\begin{array}{l} s \leftarrow \mathcal{S} \\ x \leftarrow f(s) \\ \textbf{return } [g(s,\omega) \stackrel{?}{=} \mathcal{A}(x)] \end{array}\right. & \left[\begin{array}{l} s \leftarrow \mathcal{S} \\ x \leftarrow f(s) \\ \textbf{return } [g(s,\omega) \stackrel{?}{=} y_\circ] \end{array}\right.
\end{array}$$

where $y_\circ$ is the must probable outcome of $g_\omega(s) = g(s, w)$. Note that while y_* might be the most probable outcome of $g(s)$ it does not have to be the most probable outcome of $g_\omega(s)$. Hence $y_\circ$ does not have to be equal to y_*. Consequently, we need yet another pair of games

$$\begin{array}{ll}
\overline{\mathcal{G}}_{0\omega} & \overline{\mathcal{G}}_{1\omega} \\
\left[\begin{array}{l} s \leftarrow \mathcal{S} \\ x \leftarrow f(s) \\ \textbf{return } [g(s,\omega) \stackrel{?}{=} \mathcal{A}(x)] \end{array}\right. & \left[\begin{array}{l} s \leftarrow \mathcal{S} \\ x \leftarrow f(s) \\ \textbf{return } [g(s,\omega) \stackrel{?}{=} y_*] \end{array}\right.
\end{array}$$

to define the semantical advantage as the average:

$$\mathsf{Adv}^{\mathsf{sem}}_{f,g}(\mathcal{A}) = \sum_{\omega \in \Omega} \Pr\left[\omega\right] \cdot \left(\Pr\left[\overline{\mathcal{G}}^{\mathcal{A}}_{0\omega} = 1\right] - \Pr\left[\overline{\mathcal{G}}^{\mathcal{A}}_{1\omega} = 1\right]\right) \quad .$$

The coin-fixing argument tells us that by taking

$$\omega_* = \operatorname*{argmax}_{\omega \in \Omega} \Pr\left[\overline{\mathcal{G}}^{\mathcal{A}}_{0\omega_*} = 1\right] - \Pr\left[\overline{\mathcal{G}}^{\mathcal{A}}_{1\omega_*} = 1\right]$$

we guarantee

$$\mathsf{Adv}^{\mathsf{sem}}_{f,g}(\mathcal{A}) \leq \Pr\left[\overline{\mathcal{G}}^{\mathcal{A}}_{0\omega_*} = 1\right] - \Pr\left[\overline{\mathcal{G}}^{\mathcal{A}}_{1\omega_*} = 1\right] \leq \Pr\left[\mathcal{G}^{\mathcal{A}}_{0\omega_*} = 1\right] - \Pr\left[\overline{\mathcal{G}}^{\mathcal{A}}_{1\omega_*} = 1\right] \quad ,$$

since the game $\overline{\mathcal{G}}^{\mathcal{A}}_{0\omega_*}$ is identical to $\mathcal{G}^{\mathcal{A}}_{0\omega_*}$. However, the game $\overline{\mathcal{G}}^{\mathcal{A}}_{1\omega_*}$ does not have to be identical to $\mathcal{G}^{\mathcal{A}}_{1\omega_*}$, since y_* can be different form $y_\circ$. In fact, it is straightforward to show that the inequality (1) does not hold in general. As a concrete example, consider a randomised function $g(s)$ that returns uniformly chosen integer ω form the range $\{0,\ldots,7\}$. Then obviously the knowledge of $f(s)$ does not help in predicting and thus the best strategy is to output a fixed guess say 3. Figure 1 depicts the distribution of differences

$$\Delta(\omega) = \Pr\left[\overline{\mathcal{G}}^{\mathcal{A}}_{0\omega_*} = 1\right] - \Pr\left[\overline{\mathcal{G}}^{\mathcal{A}}_{1\omega_*} = 1\right]$$

that are averaged to get the advantage $\mathsf{Adv}^{\mathsf{sem}}_{f,g}(\mathcal{A})$. Note that for fixed $\omega = 3$, the output of g_3 is also fixed and thus the advantage $\mathsf{Adv}^{\mathsf{sem}}_{f,g}(\mathcal{A}) = 0$.

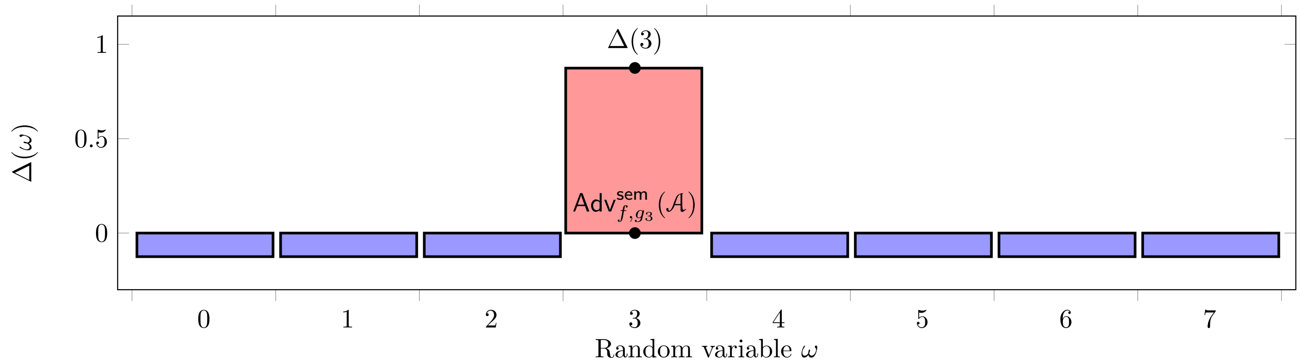

Figure 1: Counter example that shows that the inequality (1) cannot be satisfied by coin-fixing argument

The presented counter example does not show that it is impossible to choose $\omega \in \Omega$ such that

$$\mathsf{Adv}^{\mathsf{sem}}_{f,g}(\mathcal{A}) \leq \max_{\omega\in\Omega}\left\{\mathsf{Adv}^{\mathsf{sem}}_{f,g_\omega}(\mathcal{A})\right\}$$

it just shows that there is no easy way to find such coins. To show impossibility of other more clever choice of ω consider the counter example depicted on Figure 2. In this example, the three secrets $\mathcal{S} = \{0, 1, 2\}$ and four equiprobable random values $\Omega = \{0, 1, 2, 3\}$. The function f is deterministic and the adversary $\mathcal{A}$ is deterministic with the outputs depicted on the figure. Note that guesses of $\mathcal{A}$ must coincide on the same row.

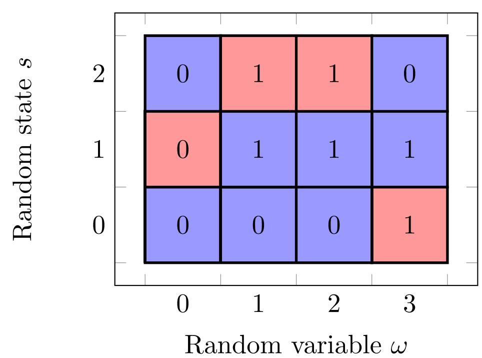

Figure 2: Counter example that shows that the inequality (1) cannot be satisfied at all. All squares are equiprobable in the experiment. The number inside the square marks the output of $g(s,\omega)$. Correct guesses are marked with blue and incorrect guesses are marked with red squares.

Since $\mathcal{A}$ guesses the value $g(s,\omega)$ on eight squares and there are equal number of ones and zeros, we get

$$\mathsf{Adv}^{\mathsf{sem}}_{f,g}(\mathcal{A}) = \tfrac{8}{12} - \tfrac{1}{2} = \tfrac{1}{6}\ .$$

As $\mathcal{A}$ guesses correctly only two values in each row, $\Pr\left[\mathcal{G}^{\mathcal{A}}_{0\omega_*} = 1\right] = \frac{2}{3}$. If the randomness is fixed then the best choice for $y_\circ$ can be determined by majority voting and thus $\Pr\left[\mathcal{G}^{\mathcal{A}}_{1\omega_*} = 1\right] \geq \frac{2}{3}$. The latter implies that $\mathsf{Adv}^{\mathsf{sem}}_{f,g_\omega}(\mathcal{A}) \leq 0$ for any $\omega \in \{0, 1, 2, 3\}$ and thus $\mathsf{Adv}^{\mathsf{sem}}_{f,g}(\mathcal{A}) > \mathsf{Adv}^{\mathsf{sem}}_{f,g_\omega}(\mathcal{A})$.