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

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

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

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

where $g_\omega : S \rightarrow \mathcal{Y}$ 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 $\text{Adv}_{f,g}^{\text{sem}}(A)$ can be expressed as the distance between the following games

$\mathcal{G}_0$

- $s \leftarrow S$
- $x \leftarrow f(s)$
- $\text{return } [g(s) \overset{?}{=} A(x)]$

$\mathcal{G}_1$

- $s \leftarrow S$
- $x \leftarrow f(s)$
- $\text{return } [g(s) \overset{?}{=} y_*]$

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

$\mathcal{G}_{0\omega}$

- $s \leftarrow S$
- $x \leftarrow f(s)$
- $\text{return } [g(s, \omega) \overset{?}{=} A(x)]$

$\mathcal{G}_{1\omega}$

- $s \leftarrow S$
- $x \leftarrow f(s)$
- $\text{return } [g(s, \omega) \overset{?}{=} y_\omega]$

where $y_\omega$ is the most probable outcome of $g_\omega(s) = g(s, \omega)$. 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 $y_\omega$ does not have to be equal to $y_*$. Consequently, we need yet another pair of games

$\mathcal{G}_{0\omega}^*$

- $s \leftarrow S$
- $x \leftarrow f(s)$
- $\text{return } [g(s, \omega) \overset{?}{=} A(x)]$

$\mathcal{G}_{1\omega}^*$

- $s \leftarrow S$
- $x \leftarrow f(s)$
- $\text{return } [g(s, \omega) \overset{?}{=} y_*]$

to define the semantical advantage as the average:

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

The coin-fixing argument tells us that by taking

$$\omega_* = \arg \max_{\omega \in \Omega} \Pr[\mathcal{G}_{0\omega}^* = 1] - \Pr[\mathcal{G}_{1\omega}^* = 1]$$

we guarantee

$$\text{Adv}_{f,g}^{\text{sem}}(A) \leq \Pr[\mathcal{G}_{0\omega_*}^* = 1] - \Pr[\mathcal{G}_{1\omega_*}^* = 1] \leq \Pr[g_{\omega_*}^A = 1] - \Pr[\mathcal{G}_{1\omega_*}^A = 1],$$

since the game $\mathcal{G}_{0\omega_*}^*$ is identical to $g_{\omega_*}^A$. The same claim does not hold for the games $\mathcal{G}_{1\omega_*}^A$ is identical to $G_{1\omega_*}^A$, since $y_*$ can be different form $y_\omega$. In fact, it is straightforward to show that the inequality (1) does not
hold. As a concrete example, consider a randomised function $g(s)$ that returns uniformly chosen integer 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

$$\Delta(\omega) = \Pr[G_A \omega \ast = 1] - \Pr[G_{A^c} \omega \ast = 1]$$

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

![Figure 1: Counter example that shows that the inequality (1) cannot be satisfied by coin-fixing argument](image1.png)

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

$$\text{Adv}_{f,g}(A) \leq \max_{\omega \in \Omega} \{\text{Adv}_{f,g_\omega}(A)\}$$

it just shows that there is no easy way to find such coins. To show impossibility of other more clever choice of $\omega$ 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 $A$ is deterministic with the outputs depicted on the figure. Note that guesses of $A$ 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.](image2.png)

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

$$\text{Adv}_{f,g}(A) = \frac{8}{12} - \frac{1}{2} = \frac{1}{6}.$$

As $A$ guesses correctly only two values in each row, $\Pr[G_A \omega = 1] = \frac{2}{7}$. If the randomness is fixed then the best choice for $y_\omega$ can be determined by majority voting and thus $\Pr[G_{A^c} \omega = 1] \geq \frac{4}{7}$. The latter implies that $\text{Adv}_{f,g_\omega}(A) \leq 0$ for any $\omega \in \{0, 1, 2, 3\}$ and thus $\text{Adv}_{f,g}(A) > \text{Adv}_{f,g_\omega}(A)$. 

2