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

Exercise (Classical hybrid argument). *Let $\mathcal{X}_0$ and $\mathcal{X}_1$ efficiently samplable distributions that are (t,ε)-indistinguishable. Show that distributions $\mathcal{X}_0$ and $\mathcal{X}_1$ remain computationally indistinguishable even if the adversary can get n samples. As the first step, estimate computational distances between following games*

$$\begin{array}{lll}
\mathcal{G}_{00}^{\mathcal{A}} & \mathcal{G}_{01}^{\mathcal{A}} & \mathcal{G}_{11}^{\mathcal{A}} \\
\left[\begin{array}{l} x_0 \leftarrow \mathcal{X}_0 \\ x_1 \leftarrow \mathcal{X}_0 \\ \textbf{\textit{return}}\ \mathcal{A}(x_0,x_1) \end{array}\right. &
\left[\begin{array}{l} x_0 \leftarrow \mathcal{X}_0 \\ x_1 \leftarrow \mathcal{X}_1 \\ \textbf{\textit{return}}\ \mathcal{A}(x_0,x_1) \end{array}\right. &
\left[\begin{array}{l} x_0 \leftarrow \mathcal{X}_1 \\ x_1 \leftarrow \mathcal{X}_1 \\ \textbf{\textit{return}}\ \mathcal{A}(x_0,x_1) \end{array}\right.
\end{array}$$

and then generalise the argumentation to the case, where the adversary $\mathcal{A}$ gets n samples from a distribution $\mathcal{X}_i$. Why do we need to assume that distributions $\mathcal{X}_0$ and $\mathcal{X}_1$ are efficiently samplable?

Solution. Let us examine computational distances between following games:

$$\begin{array}{ll}
\mathcal{G}_{00}^{\mathcal{A}} & \mathcal{G}_{01}^{\mathcal{A}} \\
\left[\begin{array}{l} x_0 \leftarrow \mathcal{X}_0 \\ x_1 \leftarrow \mathcal{X}_0 \\ \textbf{return}\ \mathcal{A}(x_0,x_1) \end{array}\right. &
\left[\begin{array}{l} x_0 \leftarrow \mathcal{X}_0 \\ x_1 \leftarrow \mathcal{X}_1 \\ \textbf{return}\ \mathcal{A}(x_0,x_1) \end{array}\right. .
\end{array}$$

Note that we can define the next adversary:

$$\begin{array}{l}
\mathcal{B}(x) \\
\left[\begin{array}{l} x_0 \leftarrow \mathcal{X}_0 \\ x_1 \leftarrow x \\ \textbf{return}\ \mathcal{A}(x_0,x_1) \end{array}\right.
\end{array}$$

against indistinguishability games

$$\begin{array}{ll}
\mathcal{Q}_{0}^{\mathcal{B}} & \mathcal{Q}_{1}^{\mathcal{B}} \\
\left[\begin{array}{l} x \leftarrow \mathcal{X}_0 \\ \textbf{return}\ \mathcal{B}(x) \end{array}\right. &
\left[\begin{array}{l} x \leftarrow \mathcal{X}_1 \\ \textbf{return}\ \mathcal{B}(x) \end{array}\right. .
\end{array}$$

Inserting our concrete adversary $\mathcal{B}$ into the indistinguishability games yields:

$$\begin{array}{ll}
\mathcal{Q}_{0}^{\mathcal{B}} & \mathcal{Q}_{1}^{\mathcal{B}} \\
\left[\begin{array}{l} x \leftarrow \mathcal{X}_0 \\ x_0 \leftarrow \mathcal{X}_0 \\ x_1 \leftarrow x \\ \textbf{return}\ \mathcal{A}(x_0,x_1) \end{array}\right. &
\left[\begin{array}{l} x \leftarrow \mathcal{X}_1 \\ x_0 \leftarrow \mathcal{X}_0 \\ x_1 \leftarrow x \\ \textbf{return}\ \mathcal{A}(x_0,x_1) \end{array}\right. ,
\end{array}$$

from which we can easily see that games $\mathcal{Q}_0^{\mathcal{B}}$ is equivalent to $\mathcal{G}_0^{\mathcal{A}}$ and $\mathcal{Q}_1^{\mathcal{B}}$ is equivalent to $\mathcal{G}_1^{\mathcal{A}}$ (denoted by $\mathcal{Q}_0^{\mathcal{B}} \equiv \mathcal{G}_0^{\mathcal{A}}$ and $\mathcal{Q}_1^{\mathcal{B}} \equiv \mathcal{G}_1^{\mathcal{A}}$). That leads to the next inequality

$$\left|\Pr\left[\mathcal{G}_{00}^{\mathcal{A}} = 1\right] - \Pr\left[\mathcal{G}_{01}^{\mathcal{A}} = 1\right]\right| = \left|\Pr\left[\mathcal{Q}_{0}^{\mathcal{B}} = 1\right] - \Pr\left[\mathcal{Q}_{1}^{\mathcal{B}} = 1\right]\right| \leq \mathsf{Adv}^{\mathsf{ind}}_{\mathcal{X}_0,\mathcal{X}_1}(\mathcal{B}) \enspace .$$

Let t_{s} denote the time needed to take a sample form $\mathcal{X}_0$ and $t_{\mathcal{A}}$ the running time of $\mathcal{A}$. Then the running time of $\mathcal{B}$ is $t_s + t_{\mathcal{A}}$. Now if if $t_{\mathcal{A}} \leq t - t_{\mathrm{s}}$, the running time of $\mathcal{B}$ is at most t and we can bound

$$\mathsf{Adv}^{\mathsf{ind}}_{\mathcal{X}_0,\mathcal{X}_1}(\mathcal{B}) \leq \varepsilon \enspace .$$

More formally, note that (t, ε)-indistinguishability of $\mathcal{X}_0$ and $\mathcal{X}_1$ implies that this equation must hold for any t-time adversary $\mathcal{B}$ and thus it must hold for the particular construction of $\mathcal{B}$.

In a similar way, we can analyse the computational distances between the games:

$$\begin{array}{ll}
\mathcal{G}_{01}^{\mathcal{A}} & \mathcal{G}_{11}^{\mathcal{A}} \\
\left[\begin{array}{l} x_0 \leftarrow \mathcal{X}_0 \\ x_1 \leftarrow \mathcal{X}_1 \\ \textbf{return } \mathcal{A}(x_0, x_1) \end{array}\right. & \left[\begin{array}{l} x_0 \leftarrow \mathcal{X}_1 \\ x_1 \leftarrow \mathcal{X}_1 \\ \textbf{return } \mathcal{A}(x_0, x_1) \ . \end{array}\right.
\end{array}$$

In this case, we obtain reduction to the indistinguishability by considering the following adversary

$$\begin{array}{l}
\mathcal{C}(x) \\
\left[\begin{array}{l} x_0 \leftarrow x \\ x_1 \leftarrow \mathcal{X}_1 \\ \textbf{return } \mathcal{A}(x_0, x_1) \ . \end{array}\right.
\end{array}$$

Direct substitution into the games $\mathcal{Q}_0$ and $\mathcal{Q}_1$ allows us to prove that $\mathcal{Q}_0^{\mathcal{C}} \equiv \mathcal{G}_0^{\mathcal{A}}$ and $\mathcal{Q}_1^{\mathcal{C}} \equiv \mathcal{G}_1^{\mathcal{A}}$. Thus,

$$\left|\Pr\left[\mathcal{G}_{01}^{\mathcal{A}}\right] = 1\right] - \Pr\left[\mathcal{G}_{11}^{\mathcal{A}} = 1\right]\right| = \mathsf{Adv}_{\mathcal{X}_0, \mathcal{X}_1}^{\mathsf{ind}}(\mathcal{C})$$

Again, it is easy to see that if we can sample an element from $\mathcal{X}_1$ in time t_{s}, then

$$\left|\Pr\left[\mathcal{G}_{01}^{\mathcal{A}}\right] = 1\right] - \Pr\left[\mathcal{G}_{11}^{\mathcal{A}} = 1\right]\right| \le \varepsilon$$

for all $(t - t_{\mathrm{s}})$-time adversaries $\mathcal{A}$. Finally, we can use triangular inequality to combine both bounds:

$$\left|\Pr\left[\mathcal{G}_{00}^{\mathcal{A}}\right] = 1\right] - \Pr\left[\mathcal{G}_{11}^{\mathcal{A}} = 1\right]\right| \le \left|\Pr\left[\mathcal{G}_{00}^{\mathcal{A}}\right] = 1\right] - \Pr\left[\mathcal{G}_{01}^{\mathcal{A}} = 1\right]\right| + \left|\Pr\left[\mathcal{G}_{01}^{\mathcal{A}}\right] = 1\right] - \Pr\left[\mathcal{G}_{11}^{\mathcal{A}} = 1\right]\right| \le 2\varepsilon \ .$$

As the bound holds for any $(t - t_{\mathrm{s}})$-time adversary $\mathcal{A}$, we have established that game $\mathcal{G}_{00}$ and $\mathcal{G}_{11}$ are $(t - t_{\mathrm{s}}, 2\varepsilon)$-indistinguishable.

Genralisation. To generalise the result, we must consider the following set of games

$$\begin{array}{l}
\mathcal{G}_{b_{n-1}\dots b_1 b_0}^{\mathcal{A}} \\
\left[\begin{array}{l} x_0 \leftarrow \mathcal{X}_{b_0} \\ x_1 \leftarrow \mathcal{X}_{b_1} \\ \dots \\ x_{n-1} \leftarrow \mathcal{X}_{b_{n-1}} \\ \textbf{return } \mathcal{A}(x_0, x_1, \dots, x_{n-1}) \ . \end{array}\right.
\end{array}$$

It is easy to see that for any two games $\mathcal{G}_{b_{n-1}\dots b_1 b_0}$ and $\mathcal{G}_{c_{n-1}\dots c_1 c_0}$ where indices differ only in the i^{th} position we can define a reduction adversary $\mathcal{B}$ which samples all other elements according to the description of $\mathcal{G}_{b_{n-1}\dots b_1 b_0}$ and uses the sample x in the place of x_i. If $b_i = 0$ then by the construction $\mathcal{Q}_0^{\mathcal{B}} \equiv \mathcal{G}_{b_{n-1}\dots b_1 b_0}^{\mathcal{A}}$ and $\mathcal{Q}_1^{\mathcal{B}} \equiv \mathcal{G}_{c_{n-1}\dots c_1 c_0}^{\mathcal{A}}$. Otherwise, $\mathcal{Q}_0^{\mathcal{B}} \equiv \mathcal{G}_{c_{n-1}\dots c_1 c_0}^{\mathcal{A}}$ and $\mathcal{Q}_1^{\mathcal{B}} \equiv \mathcal{G}_{b_{n-1}\dots b_1 b_0}^{\mathcal{A}}$. As the running time of $\mathcal{B}$ is $t_{\mathcal{A}} + (n-1)t_{\mathrm{s}}$, we get that for all $(t - (n-1)t_{\mathrm{s}})$-time adversaries $\mathcal{A}$:

$$\left|\Pr\left[\mathcal{G}_{b_{n-1}\dots b_1 b_0}^{\mathcal{A}} = 1\right] - \Pr\left[\mathcal{G}_{c_{n-1}\dots c_1 c_0}^{\mathcal{A}} = 1\right]\right| \le \varepsilon.$$

To bound the computational distance between $\mathcal{G}_{0\dots 0}$ and $\mathcal{G}_{1\dots 1}$, we have to find a path from $0\dots 0$ to $1\dots 1$ where adjacent points in the path differ only by single bit. The longest such paths goes through all 2^n bitstrings while the simplest one has only n alterations. Since each edge in this path adds ε to the estimate on the computational distance, we should use the shortest path. As a consequence, we can prove that games $\mathcal{G}_{0\dots 0}$ and $\mathcal{G}_{1\dots 1}$ are $(t - (n-1)t_{\mathrm{s}}, n\varepsilon)$-indistinguishable. Figure 1 illustrates the derivation when $n = 3$.

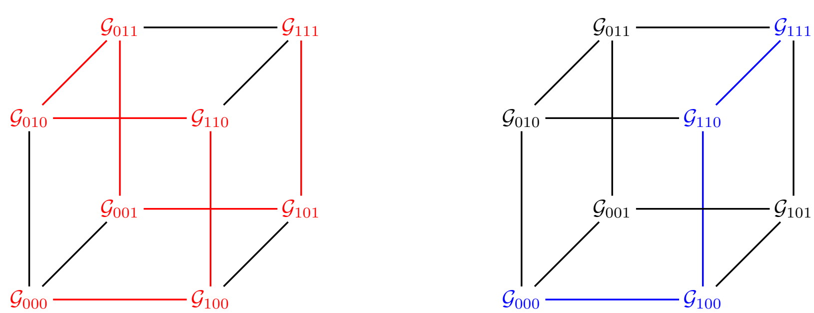

Figure 1: Game space when the number of samples is three with the longest and the shortest path