Exercise (Lottery game with distributions). Consider the following game, where an adversary $A$ gets three values $x_1, x_2$ and $x_3$. Two of them are sampled from the efficiently samplable distribution $X_0$ and one of them is sampled from the efficiently samplable distribution $X_1$. The adversary wins the game if it correctly determines which sample is taken from $X_1$. Find an upper bound to the success probability if distributions $X_0$ and $X_1$ are $(t, \varepsilon)$-indistinguishable.

Solution. Any such problem can be split into three conceptual parts: formalisation of the attack scenario, game manipulation, and final probability computations. One possible formalisation of the attack scenario is given below

\[
\begin{aligned}
G^A_0 & \quad \begin{cases}
  x_1 \leftarrow X_0 \\
  x_2 \leftarrow X_0 \\
  x_3 \leftarrow X_1 \\
  \pi \leftarrow \text{Perm}(\{1, 2, 3\}) \\
  i \leftarrow A(x_{\pi(1)}, x_{\pi(2)}, x_{\pi(3)}) \\
  \text{return } [\pi(i) \neq 3]
\end{cases} \\
G^A_1 & \quad \begin{cases}
  x_1 \leftarrow X_0 \\
  x_2 \leftarrow X_0 \\
  x_3 \leftarrow X_1 \\
  \pi \leftarrow \text{Perm}(\{1, 2, 3\}) \\
  i \leftarrow A(x_{\pi(1)}, x_{\pi(2)}, x_{\pi(3)}) \\
  \text{return } [\pi(i) \neq 3]
\end{cases}
\end{aligned}
\]

The fourth line in the game models random shuffling of the values $x_1, x_2, x_3$. If we choose uniformly a permutation $\pi$ over $\{1, 2, 3\}$, the elements $x_{\pi(1)}, x_{\pi(2)}, x_{\pi(3)}$ are in a random order. Obviously, the guess of $A$ is correct if and only if $\pi(i) = 3$. As a second step, we modify the game in the following way

\[
\begin{aligned}
G^A_0 & \quad \begin{cases}
  x_1 \leftarrow X_0 \\
  x_2 \leftarrow X_0 \\
  x_3 \leftarrow X_1 \\
  \pi \leftarrow \text{Perm}(\{1, 2, 3\}) \\
  i \leftarrow A(x_{\pi(1)}, x_{\pi(2)}, x_{\pi(3)}) \\
  \text{return } [\pi(i) \neq 3]
\end{cases} \\
G^A_1 & \quad \begin{cases}
  x_1 \leftarrow X_0 \\
  x_2 \leftarrow X_0 \\
  x_3 \leftarrow X_1 \\
  \pi \leftarrow \text{Perm}(\{1, 2, 3\}) \\
  i \leftarrow A(x_{\pi(1)}, x_{\pi(2)}, x_{\pi(3)}) \\
  \text{return } [\pi(i) \neq 3]
\end{cases}
\end{aligned}
\]

Note that the games differ only in a single line: $x_3$ is chosen either from $X_0$ or from $X_1$ depending on the game. The latter allows us to use the entire game as a distinguisher for $X_0$ and $X_1$. Namely, let us define a new adversary

\[
B(x) \quad \begin{cases}
  x_1 \leftarrow X_0 \\
  x_2 \leftarrow X_0 \\
  x_3 \leftarrow x \\
  \pi \leftarrow \text{Perm}(\{1, 2, 3\}) \\
  i \leftarrow A(x_{\pi(1)}, x_{\pi(2)}, x_{\pi(3)}) \\
  \text{return } [\pi(i) \neq 3]
\end{cases}
\]

against the indistinguishability games

\[
\begin{aligned}
Q^B_0 & \quad \begin{cases}
  x \leftarrow X_0 \\
  \text{return } B(x)
\end{cases} \\
Q^B_1 & \quad \begin{cases}
  x \leftarrow X_1 \\
  \text{return } B(x)
\end{cases}
\end{aligned}
\]
By the \((t, \varepsilon)\)-indistinguishability assumptions
\[
\text{Adv}^{\text{ind}}_{X_0, X_1}(B) = |\Pr [Q_0^B = 1] - \Pr [Q_1^B = 1]| \leq \varepsilon
\]
for any \(t\)-time adversary \(B\). Let us estimate the behaviour of our concrete adversary by inserting its definition into the games \(Q_0\) and \(Q_1\):

\[
\begin{align*}
Q_0^B & : x \leftarrow X_0 \\
x_1 & \leftarrow X_0 \\
x_2 & \leftarrow X_0 \\
x_3 & \leftarrow x \\
\pi & \leftarrow \text{Perm}(\{1, 2, 3\}) \\
i & \leftarrow A(x_{\pi(1)}, x_{\pi(2)}, x_{\pi(3)}) \\
\text{return} & \left[\pi(i) \neq 3\right]
\end{align*}
\]

\[
\begin{align*}
Q_1^B & : x \leftarrow X_1 \\
x_1 & \leftarrow X_0 \\
x_2 & \leftarrow X_0 \\
x_3 & \leftarrow x \\
\pi & \leftarrow \text{Perm}(\{1, 2, 3\}) \\
i & \leftarrow A(x_{\pi(1)}, x_{\pi(2)}, x_{\pi(3)}) \\
\text{return} & \left[\pi(i) \neq 3\right]
\end{align*}
\]

By doing simple syntactic changes that do not alter the behaviour of games, we can convert \(Q_0^B\) to \(G_1^A\) and \(Q_1^B\) to \(G_0^A\). Hence, we have established that
\[
|\Pr [G_0^A = 1] - \Pr [G_1^A = 1]| = |\Pr [Q_0^B = 1] - \Pr [Q_1^B = 1]| \leq \varepsilon
\]
provided that the running-time of \(B\) is less than \(t\). Let \(t_A\) be the running-time of \(A\) and \(t_s\) time needed to get a sample from \(X_0\) or \(X_1\). Then the running time of \(B\) is \(2t_s + t_A + O(1)\). Hence, for all \(t - 2t_s - O(1)\) time adversaries
\[
|\Pr [G_0^A = 1] - \Pr [G_1^A = 1]| \leq \varepsilon.
\]

By doing syntactic changes that do not alter the behaviour of the game, we can rewrite the game \(G_1\) even further

\[
\begin{align*}
G_1^A & : x_1 \leftarrow X_0 \\
x_2 & \leftarrow X_0 \\
x_3 & \leftarrow X_0 \\
\pi & \leftarrow \text{Perm}(\{1, 2, 3\}) \\
i & \leftarrow A(x_{\pi(1)}, x_{\pi(2)}, x_{\pi(3)}) \\
\text{return} & \left[\pi(i) \neq 3\right]
\end{align*}
\]

\[
\begin{align*}
G_2^A & : x_1 \leftarrow X_0 \\
x_2 & \leftarrow X_0 \\
x_3 & \leftarrow X_0 \\
i & \leftarrow A(x_1, x_2, x_3) \\
\pi & \leftarrow \text{Perm}(\{1, 2, 3\}) \\
\text{return} & \left[\pi(i) \neq 3\right]
\end{align*}
\]

Note that the behaviour of the game does not change since \(A\) gets the same input distribution \(X_0 \times X_0 \times X_0\) in both games. As the output of \(A\) is fixed before the permutation is chosen, we get
\[
\Pr [G_2^A = 1] = \frac{1}{3}.
\]

By compering (1) and (2) we obtain
\[
\Pr [G_0^A = 1] \leq \frac{1}{3} + \varepsilon
\]
provided that the running-time of \(A\) is \(t - 2t_s - O(1)\).

**Comments.** if distributions \(X_0\) and \(X_1\) are \((t, \varepsilon)\)-indistinguishable, it is always possible to change the game by replacing a line \(x \leftarrow X_0\) with a line \(x \leftarrow X_1\). The total time-complexity of the game sets limitations on the overall running time of the adversary, as the corresponding distinguisher \(B\) must simulate the game inside its code. By applying such rewriting rules long enough, we can prove computational closeness of many complex games.