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

Exercise (Hard-core bits and regularity). *A predicate* $\pi : \mathcal{S} \to \{0,1\}$ *is said to be a* ε-regular *if the output distribution for uniform input distribution is nearly uniform:*

$$\Delta(\pi) = \left|\Pr\left[s \xleftarrow{u} \mathcal{S} : \pi(s) = 0\right] - \Pr\left[s \xleftarrow{u} \mathcal{S} : \pi(s) = 1\right]\right| \leq \varepsilon \enspace .$$

A predicate π *is a* (t,ε)-unpredictable *also known as* (t,ε)-hardcore predicate *for a function* $f : \mathcal{S} \to \mathcal{X}$ *if for any* t*-time adversary*

$$\mathsf{Adv}^{\mathsf{hc\text{-}pred}}_{f,\pi}(\mathcal{A}) = 2 \cdot \left|\Pr\left[s \xleftarrow{u} \mathcal{S} : \mathcal{A}(f(s)) = \pi(s)\right] - \tfrac{1}{2}\right| \leq \varepsilon \enspace .$$

Let us first define two sets:

$$\mathcal{S}_0 = \{s \in \mathcal{S} : \pi(s) = 0\}$$
$$\mathcal{S}_1 = \{s \in \mathcal{S} : \pi(s) = 1\} \enspace .$$

Then we can define following distinguishing games:

$$\begin{array}{ll}
\mathcal{G}_0 & \mathcal{G}_1 \\
\left[\begin{array}{l} s \xleftarrow{u} \mathcal{S}_0 \\ x \leftarrow f(s) \\ \textbf{\textit{return}}\ \mathcal{A}(x) \end{array}\right. &
\left[\begin{array}{l} s \xleftarrow{u} \mathcal{S}_1 \\ x \leftarrow f(s) \\ \textbf{\textit{return}}\ \mathcal{A}(x) \end{array}\right.
\end{array}$$

Show that even if $\mathcal{S}_0$ *and* $\mathcal{S}_1$ *are completely indistinguishable, the predicate does not have to be* (t,ε)*-unpredictable if the predicate* π *is not regular.*

Solution.