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

Exercise (Existence of hard-core bits). *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:*

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

*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*

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

Prove that any (t,ε)-hardcore predicate is 2ε-regular. Let $f : \mathcal{S} \to \{0,1\}^n$ be a deterministic function and let $\pi_k(s)$ denote the kth bit of $f(s)$ and $f_k(s)$ denote the output of $f(s)$ without the kth bit. Show that if f is a (t,ε)-secure pseudorandom generator, then π_k is (t,ε)-hardcore predicate for f_k.

Solution. Regularity. As the first step, we first unroll the game inlined into the probability formula that defines advantage against hard-core predicates:

$$\begin{array}{l}\mathcal{G}\\ \left[\begin{array}{l} s \xleftarrow{u} \mathcal{S}\\ x \leftarrow f(s)\\ b \leftarrow \pi(s)\\ \textbf{return } [b \stackrel{?}{=} \mathcal{A}(x)] \enspace . \end{array}\right.\end{array}$$

This representation highlights that $\mathcal{A}$ must choose between two complex hypotheses $[\pi(s) \stackrel{?}{=} 0]$ and $[\pi(s) \stackrel{?}{=} 1]$. If one of these hypotheses is significantly more probable than the other, then the adversary $\mathcal{A}_*$ abuse this fact and output the most probable hypothesis without looking at the input. Let

$$\begin{aligned}\alpha_0 &= \Pr[s \xleftarrow{u} \mathcal{S} : \pi(s) = 0]\\ \alpha_1 &= \Pr[s \xleftarrow{u} \mathcal{S} : \pi(s) = 1]\end{aligned}$$

the corresponding probabilities for hypotheses. Then it is straightforward to see that

$$\begin{aligned}\mathsf{Adv}^{\mathsf{hc\text{-}pred}}_{f,\pi}(\mathcal{A}_*) &= \left|\alpha_0 - \tfrac{1}{2}\right| = \left|\alpha_1 - \tfrac{1}{2}\right| = \tfrac{1}{2} \cdot |\alpha_0 - \alpha_1|\\ &= \tfrac{1}{2} \cdot |\Pr[s \xleftarrow{u} \mathcal{S} : \pi(s) = 0] - \Pr[s \xleftarrow{u} \mathcal{S} : \pi(s) = 1]| \enspace .\end{aligned}$$

Consequently, any predicate that is not 2ε-regular can be predicted without looking at the input with advantage at least ε. Thus, the first claim is proved.

Indistinguishability. Although the definition of hard-core predicate is given through a single guessing game, we can represent it also in terms of indistinguishability. Let us first define two sets:

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

Then we can define following distinguishing games:

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

If the sizes of sets are equal $|\mathcal{S}_0| = |\mathcal{S}_1|$, then the game $\mathcal{G}$ can be thought as simple guessing between equiprobable seed distributions $\mathcal{S}_0$ and $\mathcal{S}_1$ and thus

$$\mathsf{Adv}^{\mathsf{hc\text{-}pred}}_{f,\pi}(\mathcal{A}) = \left|\Pr\left[\mathcal{G}_0^{\mathcal{A}} = 1\right] - \Pr\left[\mathcal{G}_1^{\mathcal{A}} = 1\right]\right| \enspace .$$

In general, the probability of seed distributions $\mathcal{S}_0$ and $\mathcal{S}_1$ is slightly off balance and thus

$$\begin{aligned}\left|\Pr\left[\mathcal{G}_0^{\mathcal{A}} = 1\right] - \Pr\left[\mathcal{G}_1^{\mathcal{A}} = 1\right]\right| &= 2\cdot\left|\Pr\left[s \xleftarrow{u} \mathcal{S} : \mathcal{A}(f(s)) = \pi(s)\right] - \max\{\alpha_0,\alpha_1\}\right| \\ &\le 2\cdot\left|\Pr\left[s \xleftarrow{u} \mathcal{S} : \mathcal{A}(f(s)) = \pi(s)\right] - \tfrac{1}{2}\right| + 2\cdot\left|\alpha_0 - \tfrac{1}{2}\right| \\ &\le \mathsf{Adv}^{\mathsf{hc\text{-}pred}}_{f,\pi}(\mathcal{A}) + 2\cdot\Delta(\pi) \enspace .\end{aligned}$$

Consequently, we could define hard-core predicates in terms of indistinguishability games as long as we require that the predicate is nearly regular. For regular predicates, these two notions coincide.

Analysis of a standard construction. Let k be fixed and let $x_\bullet$ denote a bitstring $x_n \ldots x_{k+1}x_{k-1}x_1$ that is obtained by dropping the kth bit form n-bit string $x = x_n \ldots x_1$. To show that π_k is an hardcore bit, we have to analyse the following game:

$$\begin{array}{l}\mathcal{G}_0\\ \left[\begin{array}{l} s \xleftarrow{u} \mathcal{S}\\ x \leftarrow f(s)\\ \textbf{return } [x_k \stackrel{?}{=} \mathcal{A}(x_\bullet)]\end{array}\right. \enspace .\end{array}$$

By our assumption $f(s)$ is indistinguishable from uniformly chosen string $x \xleftarrow{u} \{0,1\}^n$. Let $\mathcal{G}_1$ be the corresponding game:

$$\begin{array}{l}\mathcal{G}_1\\ \left[\begin{array}{l} s \xleftarrow{u} \mathcal{S}\\ x \xleftarrow{u} \{0,1\}^n\\ \textbf{return } [x_k \stackrel{?}{=} \mathcal{A}(x_\bullet)]\end{array}\right. \enspace .\end{array}$$

For the formal proof, we need to estimate the computational difference of $\mathcal{G}_0$ and $\mathcal{G}_1$ interns of security games:

$$\begin{array}{l}\mathcal{Q}_0^{\mathcal{B}}\\ \left[\begin{array}{l} s \xleftarrow{u} \{0,1\}^n\\ x \xleftarrow{u} f(s)\\ \textbf{return } [\mathcal{B}(x) \stackrel{?}{=} 1]\end{array}\right.\end{array} \qquad\qquad \begin{array}{l}\mathcal{Q}_1^{\mathcal{B}}\\ \left[\begin{array}{l} x \xleftarrow{u} \{0,1\}^n\\ \textbf{return } [\mathcal{B}(x) \stackrel{?}{=} 1]\end{array}\right.\end{array}$$

through which the notion of pseudorandomness is defined. Now if we define the adversary as follows:

$$\begin{array}{l}\mathcal{B}(x)\\ \left[\,\textbf{return } [x_k \stackrel{?}{=} \mathcal{A}(x_\bullet)]\right.\end{array}$$

then $\mathcal{Q}_0^{\mathcal{B}} \equiv \mathcal{G}_0^{\mathcal{A}}$ and $\mathcal{Q}_1^{\mathcal{B}} \equiv \mathcal{G}_1^{\mathcal{A}}$. As $\mathcal{B}$ is a valid program and its running time is only by a constant slower than the running time of $\mathcal{A}$, games $\mathcal{G}_0$ and $\mathcal{G}_1$ are (t,ε)-indistinguishable. As the bit x_k is completely independent form $\boldsymbol{x}_\bullet$ in the game $\mathcal{G}_1$, we get the desired result:

$$\mathsf{Adv}^{\mathsf{hc\text{-}pred}}_{f,\pi}(\mathcal{A}) = \left|\Pr\left[\mathcal{G}_0^{\mathcal{A}} = 1\right] - \tfrac{1}{2}\right| = \left|\Pr\left[\mathcal{G}_0^{\mathcal{A}} = 1\right] - \Pr\left[\mathcal{G}_1^{\mathcal{A}} = 1\right]\right| \le \varepsilon \enspace .$$