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

Exercise (Pseudorandom generator based on hard-core bits). *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*

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

If a function $f : \{0,1\}^n \to \{0,1\}^{n+\ell}$ is (t, ε_1)-pseudorandom generator and $\pi : \{0,1\}^n \to \{0,1\}$ is efficiently computable predicate (t, ε_1)-hardcore , then a concatenation $f_*(s) = f(s)||\pi(s)$ is $(t, \varepsilon_1 + \varepsilon_2)$-pseudorandom generator.

Solution.