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

Exercise (Hard-core predicate based on Decisional Diffie-Hellman problem). *A predicate* π *is a* (t, ε)-unpredictable *for a function* $f : \mathcal{S} \to \mathcal{X}$ *if for any* t*-time adversary*

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

Such predicates are also known as (t, ε)-hardcore predicates. *Let* $\mathbb{G}$ *be a* q*-element* (t, ε_1)*-secure Decisional Diffie-Hellman group with a generator* g*. Let* $\rho : \mathbb{G} \to \{0, 1\}$ *be* ε_2*-regular:*

$$\left|\Pr\left[h \leftarrow \mathbb{G} : \rho(h) = 0\right] - \Pr\left[h \leftarrow \mathbb{G} : \rho(h) = 1\right]\right| \leq \varepsilon_2 \enspace .$$

Show that the function $f : \mathbb{Z}_q \times \mathbb{Z}_q \to \mathbb{G} \times \mathbb{G}$ *and the predicate* $\pi : \mathbb{Z}_q \times \mathbb{Z}_q \to \{0, 1\}$ *defined as follows*

$$f(x, y) = (g^x, g^y)$$
$$\pi(x, y) = \rho(g^{xy})$$

gives a rise to an hard-core predicate. Find exact security quantifications. When does this imply that the individual bits of g^{xy} *are unpredictable for the adversaries in the Diffie-Hellman key exchange protocol.*

Solution.