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

Exercise (Signatures $\Rightarrow$ Entity authentication). *Let* $(\mathsf{Gen}, \mathsf{Sign}, \mathsf{Ver})$ *be a signature scheme that is* (t, ε)*-secure against universal one-more signature attack where the message distribution is uniform distribution over the message space* $\mathcal{M}$*. Prove that the entity authentication protocol where the verifier* $\mathcal{V}$ *chooses* $m \xleftarrow[u]{} \mathcal{M}$ *and the prover sends back the signature* $s \leftarrow \mathsf{Sign}_{\mathsf{sk}}(m)$ *there can be no black-box knowledge extractors for the secret key that is also efficient.*

Solution. Let $\mathcal{K}^{\mathcal{P}_*}$ be a black-box knowledge extractor algorithm that succeeds in time t_2 and with probability ε_2 for all provers $\mathcal{P}_*$ that run in time t_1 and are at least ε_1 successful. Then we can construct an adversary $\mathcal{B}$ can conduct successful one-more signature attacks....