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

Exercise (Signatures ⇒ 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* $s \leftarrow \mathsf{Sign}_{\mathsf{sk}}(m)$ *is secure in the most powerful setting where the adversary can run several identification protocols concurrently in order to impersonate true signer.*

Solution. Hint