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

Exercise (Disjunctive POP is witness indistinguishable). *Let* $(\mathsf{sk}_0, \mathsf{pk}_0)$ *and* $(\mathsf{sk}_1, \mathsf{pk}_1)$ *be private and public keys of an encryption scheme* $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$*. Then a disjunctive proof for the possession of secret keys* sk_0 *and* sk_1 *is defined as follows:*

1. *The verifier* $\mathcal{V}$ *chooses* $m \xleftarrow{u} \mathcal{M}$ *and sends the corresponding challenge* $\mathsf{Enc}_{\mathsf{sk}_0}(m; r_0)$ *for* $r_0 \leftarrow \mathcal{R}$*, and* $\mathsf{Enc}_{\mathsf{sk}_1}(m; r_1)$ *for* $r_1 \leftarrow \mathcal{R}$ *together with encryptions of random nonces* $\mathsf{Enc}_{\mathsf{sk}_0}(r_1)$ *and* $\mathsf{Enc}_{\mathsf{sk}_1}(r_0)$ *to* $\mathcal{P}$*.*
2. *Given challenge ciphertexts* c_1, c_2, c_3, c_4*, the prover* $\mathcal{P}$ *uses one of the secret keys* sk_i *to decrypt a challenge* $\overline{m}$ *and the nonce* $r_{\neg i}$ *used to randomise the other encryption* $c_{\neg i}$*. If* $c_{\neg i} = \mathsf{Enc}_{\mathsf{pk}_{\neg i}}(\overline{m}; r_{\neg i})$*, the prover* $\mathcal{P}$ *sends* $\overline{m}$ *to* $\mathcal{V}$*, otherwise* $\mathcal{P}$ *can halt as* $\mathcal{V}$ *cheats.*
3. *The verifier* $\mathcal{V}$ *accepts if* $\overline{m} = m$*.*

Prove that even an unbounded cheating verifier cannot learn whether the prover possesses sk_0 *or* sk_1

Solution. Let us first formalise by games $\mathcal{G}_0$ and $\mathcal{G}_1$ what happens if the prover knows sk_0 or sk_1.... Let us now modify the games so that the game pair encodes indistinguishability advantage ... Now we can prove that in both games the honest prover rejects exactly the same challenges ... Next note that for a valid challenge the response is the same in both games. ...