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

Exercise (Malleability of Schnorr identification scheme). *The Schnorr identification scheme is directly based on the discrete logarithm problem. The identification scheme is a honest verifier zero-knowledge proof that the prover knows x such that $g^x = y$ in a group $\mathbb{G}$ of size q. The protocol itself is following.*

$$
\begin{array}{ccc}
\mathcal{P} & & \mathcal{V} \\
r \xleftarrow{u} \mathbb{Z}_q & & \\
& \xrightarrow{\qquad \alpha = g^r \qquad} & \\
& & \beta \xleftarrow{u} \mathbb{Z}_q \\
& \xleftarrow{\qquad \beta \qquad} & \\
& \xrightarrow{\qquad \gamma = \beta x + r \qquad} & \\
& & [g^\gamma \stackrel{?}{=} y^\beta \alpha]
\end{array}
$$

Show that if an honest t-time prover $\mathcal{P}^*$ that can convince the honest verifier with probability ε on average over all $y \in \mathbb{G}$ can also solve the discrete logarithm problem well enough.

Solution. Consider a modified prover $\mathcal{P}^{**}$ that re-randomises the statement to be proven. That is it gets a statement $\text{POK}_y[\exists x : g^x = y]$ and then asks $\mathcal{P}^*$ to prove $\text{POK}_{y'}[\exists x' : g^{x'} = y']$ for $y' = yg^\delta$. Show how it can use the repies of $\mathcal{P}^*$ to pass $\text{POK}_y[\exists x : g^x = y]$. What does this mean on the success rate of $\mathcal{P}^{**}$ – can there be more successful statements.