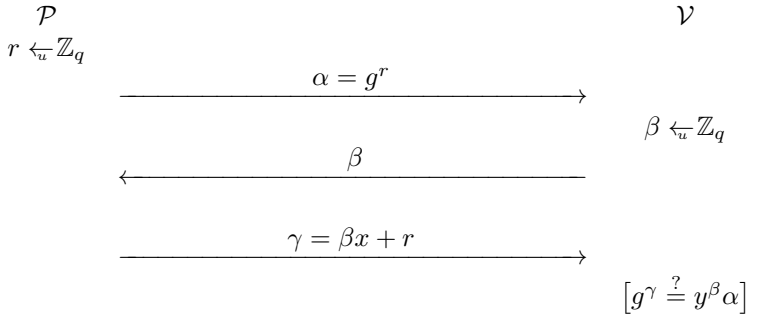
MTAT.07.003 Cryptology II
Spring 2012 / Exercise session ?? / Example Solution

Exercise (Knowledge-extraction for 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.*



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. We can define a knowledge extractor $\mathcal{K}^{\mathcal{P}^*}(y)$ for finding discrete logarithm and then a self-randomised algorithm that uses $\mathcal{K}^{\mathcal{P}^*}$ on re-randomised problem instance. Consider the success probability for fixed time-bound on the running-time $\mathcal{K}^{\mathcal{P}^*}$.

Hint. Take the standard knowledge extraction construction with success probability one and expected running-time $\Theta(1/(\varepsilon - \kappa))$. Fix a time-bound such that the extractor would succeed with probability $1/2$ when the ε is the average success probability of $\mathcal{P}^*$. Now note that for each y the success probability of $\mathcal{P}^*$ ε_y can be different. Estimate what is the success probability of the knowledge extractor $\mathcal{K}$ with the fixed time-bound. Use random self reducibility to even this into average value for each challenge y.