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

**Exercise (Weak knowledge-extractor for Schnorr protocol).** *Let $\mathbb{G}$ be a discrete logarithm group with a prime number $q$ elements. Show that the following knowledge-extractor constructor*

$$
\begin{array}{l}
\mathcal{K}^{\mathcal{P}_*(\cdot)}(\phi) \\
\left[\begin{array}{l}
\omega \leftarrow \Omega \\
\alpha \leftarrow \mathcal{P}_*(\phi, \omega) \\
\beta_1 \xleftarrow{u} \mathbb{Z}_q \\
\gamma_1 \leftarrow \mathcal{P}_*(\beta_1) \\
\alpha \leftarrow \mathcal{P}_*(\phi, \omega) \\
\beta_2 \xleftarrow{u} \mathbb{Z}_q \\
\gamma_2 \leftarrow \mathcal{P}_*(\beta_2) \\
\hat{x} \leftarrow \dfrac{\gamma_2 - \gamma_1}{\beta_2 - \beta_1} \\
\textbf{\textit{return}}\ \hat{x}
\end{array}\right.
\end{array}
$$

*that restarts the prover with the same input and randomness only once is suitable for the Schnorr protocol*

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

*and satisfies the following weak knowledge-extraction guarantee:*

$$
\forall \phi \in \{0,1\}^* \ \forall x \in \mathbb{Z}_q : \quad \Pr\left[\mathcal{K}^{\mathcal{P}_*(\cdot)}(\phi) = 1\right] \geq \Pr\left[\mathcal{V}^{\mathcal{P}_*(\phi)}(g^x) = 1\right]^2 - \frac{1}{q} \ .
$$

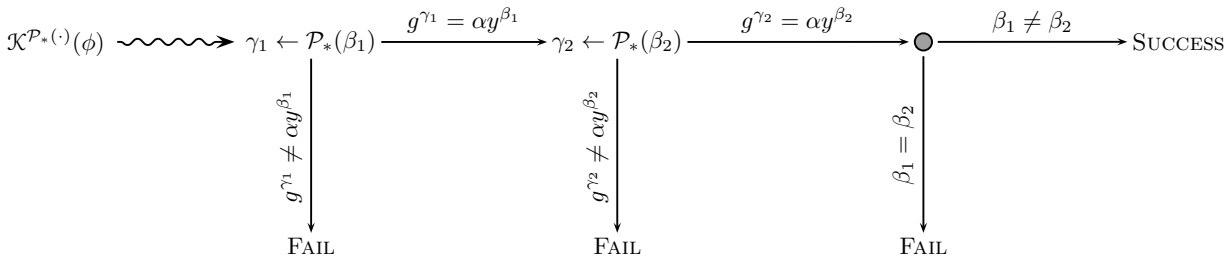
*Estimate the running time of the knowledge extractor and show that Schnorr identification protocol is secure if the underlying group is $(t, \varepsilon)$-secure Diffie-Hellman group.*

**Solution.** For the proof let us first establish the weak knowledge-extraction bound and then use this bound for estimating the probability that a malicious prover without the explicit knowledge of $x$ will succeed in the Schnorr identification protocol on average over all possible values of $x$.

Weak knowledge-extraction. Let $\varepsilon(\phi, x)$ denote the probability of successful deception for fixed $\phi$ and $x$, i.e., the function $\varepsilon(\phi, x)$ is defined as follows

$$
\varepsilon(\phi, x) = \Pr\left[\mathcal{V}^{\mathcal{P}_*(\phi)}(g^x) = 1\right] = \Pr\left[\alpha \leftarrow \mathcal{P}_*(\phi), \beta \xleftarrow{u} \mathbb{Z}_q, \gamma \leftarrow \mathcal{P}_*(\beta) : g^\gamma = \alpha y^\beta\right] \ .
$$

Now lets look what has to happen for the knowledge extractor to succeed. The extraction succeeds only if both transcripts produced by $\mathcal{K}$ are valid and $\beta_1 \neq \beta_2$. If one of those conditions is not met, the extraction might succeed due to share luck but we cannot count on it. See the event tree depicted below.




As $\mathcal{K}$ executes two independent protocol runs between honest verifier and malicious prover $\mathcal{P}_*$

$$\Pr\left[g^{\gamma_1} = \alpha y^{\beta_1}\right] = \varepsilon(\phi, x) = \Pr\left[g^{\gamma_2} = \alpha y^{\beta_2}\right] \ .$$

It is important to note that the event $[\beta_1 \neq \beta_2]$ is not independent of the event $[g^{\gamma_1} = \alpha y^{\beta_1}] \wedge [g^{\gamma_2} = \alpha y^{\beta_2}]$. For instance, the prover might succeed only if $\beta_i = 0$ then obviously $\beta_1 \neq \beta_2$ can be never met when the event $[g^{\gamma_1} = \alpha y^{\beta_1}] \wedge [g^{\gamma_2} = \alpha y^{\beta_2}]$ occurs while the event $\beta_1 \neq \beta_2$ is quite probable without restrictions:

$$\Pr\left[\beta_1 \neq \beta_2 | g^{\gamma_1} = \alpha y^{\beta_1} \wedge g^{\gamma_2} = \alpha y^{\beta_2}\right] \neq \Pr\left[\beta_1 \neq \beta_2\right]$$

Consequently, we cannot use the standard decomposition for estimating the success:

$$\Pr\left[\textsc{Success}\right] = \varepsilon(\phi, x)\varepsilon(\phi, x) \Pr\left[\beta_1 \neq \beta_2 | g^{\gamma_1} = \alpha y^{\beta_1} \wedge g^{\gamma_2} = \alpha y^{\beta_2}\right] \ ,$$

since we have no idea how to lower bound the last conditional probability. Thus, we have to rely on much cruder formula

$$\Pr\left[\textsc{Success}\right] = \Pr\left[g^{\gamma_1} = \alpha y^{\beta_1}\right] \Pr\left[g^{\gamma_2} = \alpha y^{\beta_2} \wedge \beta_1 \neq \beta_2 | g^{\gamma_1} = \alpha y^{\beta_1}\right] \ .$$

Due to the basic property of probabilities

$$\Pr\left[A \wedge B\right] \geq \Pr\left[A\right] - \Pr\left[\neg B\right]$$

we can lower bound the second term

$$\Pr\left[g^{\gamma_2} = \alpha y^{\beta_2} \wedge \beta_1 \neq \beta_2 | g^{\gamma_1} = \alpha y^{\beta_1}\right] \geq \Pr\left[g^{\gamma_2} = \alpha y^{\beta_2} | g^{\gamma_1} = \alpha y^{\beta_1}\right] - \Pr\left[\beta_1 = \beta_2 | g^{\gamma_1} = \alpha y^{\beta_1}\right] \ .$$

The latter allows us to proceed as by the construction the event $[g^{\gamma_2} = \alpha y^{\beta_2}]$ is independent of $[g^{\gamma_1} = \alpha y^{\beta_1}]$. Similarly the event $[\beta_1 = \beta_2]$ is independent of $[g^{\gamma_1} = \alpha y^{\beta_1}]$. Consequently, we get

$$\Pr\left[g^{\gamma_2} = \alpha y^{\beta_2} \wedge \beta_1 \neq \beta_2 | g^{\gamma_1} = \alpha y^{\beta_1}\right] \geq \Pr\left[g^{\gamma_2} = \alpha y^{\beta_2}\right] - \Pr\left[\beta_1 = \beta_2\right] \geq \varepsilon(\phi, x) - \frac{1}{q}$$

and

$$\Pr\left[\mathcal{K}^{\mathcal{P}_*(\cdot)}(\phi) = 1\right] \geq \Pr\left[\textsc{Success}\right] \geq \varepsilon(\phi, x)\left(\varepsilon(\phi, x) - \frac{1}{q}\right) \geq \varepsilon(\phi, x)^2 - \frac{1}{q} \ .$$

As a result, we have proved the desired claim

$$\forall \phi \in \{0,1\}^* \ \forall x \in \mathbb{Z}_q : \quad \Pr\left[\mathcal{K}^{\mathcal{P}_*(\cdot)}(\phi) = 1\right] \geq \varepsilon(\phi, x)^2 - \frac{1}{q} = \Pr\left[\mathcal{V}^{\mathcal{P}_*(\phi)}(g^x) = 1\right]^2 - \frac{1}{q} \ .$$

Security. Let $\varepsilon(\phi)$ denote the average success rate of a malicious prover $\mathcal{P}_*$ that does not have access to the uniformly chosen exponent $x$. Then the weak knowledge extractor succeeds with the average probability

$$\begin{aligned}
\Pr\left[x \xleftarrow{u} \mathbb{Z}_q : \mathcal{K}^{\mathcal{P}_*(\cdot)}(\phi, x) = 1\right] &= \sum_{x \in \mathbb{Z}_q} \frac{1}{q} \cdot \Pr\left[\mathcal{K}^{\mathcal{P}_*(\cdot)}(\phi, x) = 1\right] \\
&\geq \sum_{x \in \mathbb{Z}_q} \frac{1}{q} \cdot \left(\Pr\left[\mathcal{V}^{\mathcal{P}_*(\phi)}(g^x) = 1\right]^2 - \frac{1}{q}\right) \\
&\geq \sum_{x \in \mathbb{Z}_q} \frac{1}{q} \cdot \Pr\left[\mathcal{V}^{\mathcal{P}_*(\phi)}(g^x) = 1\right]^2 - \frac{1}{q} \ .
\end{aligned}$$

As squaring is convex-cup function, we can apply Jensen's inequality

$$\Pr\left[x \xleftarrow{u} \mathbb{Z}_q : \mathcal{K}^{\mathcal{P}_*(\cdot)}(\phi) = 1\right] \geq \left(\sum_{x \in \mathbb{Z}_q} \frac{1}{q} \cdot \Pr\left[\mathcal{V}^{\mathcal{P}_*(\phi)}(g^x) = 1\right]\right)^2 - \frac{1}{q} \geq \varepsilon(\phi)^2 - \frac{1}{q} \ .$$

The latter gives us handle to limit the average success $\varepsilon(\phi)$. Recall that the security of discrete logarithm problem is defined through the following game:

$$\begin{array}{l} \mathcal{Q} \\ \left[\begin{array}{l} x \xleftarrow{u} \mathbb{Z}_q \\ \textbf{return } \left[\mathcal{B}(g, g^x) \stackrel{?}{=} x\right] \end{array}\right. . \end{array}$$

If the weak knowledge extractor has reasonable success peobability, we can use it as an adversary against discrete logarithm problem:

$$\begin{array}{l} \mathcal{B}(g, g^x) \\ \left[\begin{array}{l} \phi \leftarrow (g, g^x) \\ \textbf{return } \mathcal{K}^{\mathcal{P}_*(\cdot)}(\phi) \end{array}\right. \end{array}$$

By the construction, the running time of $\mathcal{B}$ is $2t_{\mathcal{P}} + \mathrm{O}(1)$, where $t_{\mathcal{P}}$ is the running time of malicious prover $\mathcal{P}_*$ and the advantage against discrete logarithm is

$$\mathsf{Adv}^{\mathsf{dl}}_{\mathbb{G}}(\mathcal{B}) \geq \Pr\left[x \leftarrow \mathbb{Z}_q : \mathcal{V}^{\mathcal{P}_*(\phi)}(g^x) = 1\right]^2 - \frac{1}{q} \ .$$

By imitting constant terms, we obtain the following security claim. If the underlying DL group is $(t, \varepsilon)$-secure then Schnorr identification protocol is $\left(\frac{t}{2}, \sqrt{\varepsilon + \frac{1}{q}}\right)$-secure.

Comment on the security proof. The presented reduction is not unique, as we could to $\ell$ rewindings instead of two in the weak knowledge extractor. Each choice of $\ell$ provides a different security guarantee. However, these are not directly comparable as the bounds on running times are different. Still, one could utilise all of them if instead of single security assumption $(t, \varepsilon)$ we look hypothetical success profile:

$$\varepsilon(t) = \max_{\mathcal{B} \text{is } t\text{-time}} \mathsf{Adv}^{\mathsf{dl}}_{\mathbb{G}}(\mathcal{B}) \ .$$

The result would be several competing upper bounds $\varepsilon^*_\ell(t)$ on the maximal average success against the Schnorr protocol on average. By combining them all we get a better bound.