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

Exercise (Sigma protocol for Pedersen commitment). *Let $\mathbb{G}$ be a discrete logarithm group with a prime number q elements. Then public parameters of the Pedersen commitments are two group elements g_1 and g_2. To commit an element $m \in \mathbb{Z}_q$, the commiter has to choose a random element $x \in \mathbb{Z}_q$ and compute a corresponding commitment $c = g_1^m g_2^x$. As the commitment is perfectly hiding, the committer can only prove that he or she knows m and x such that $c = g_1^m g_2^x$. Prove that the sigma protocol depicted below is a sigma protocol for proving knowledge* $\textsc{pok}[\exists m \exists x : c = g_1^m g_2^x]$.

$$
\begin{array}{ccc}
\mathcal{P} & & \mathcal{V} \\
r_1, r_2 \xleftarrow{u} \mathbb{Z}_q & & \\
& \xrightarrow{\alpha = g_1^{r_1} g_2^{r_2}} & \\
& & \beta \xleftarrow{u} \mathbb{Z}_q \\
& \xleftarrow{\beta} & \\
& \xrightarrow{\gamma_1 = m\beta + r_1, \gamma_2 = x\beta + r_2} & \\
& & [g_1^{\gamma_1} g_2^{\gamma_2} \stackrel{?}{=} y^\beta \alpha]
\end{array}
$$

Solution. As the protocol has the right message structure, we must show only that the protocol is functional and has special soundness and zero-knowledge property.

FUNCTIONALITY. If both parities are honest then $y = g_1^m g_2^x$. Consequently,

$$g_1^{\gamma_1} g_2^{\gamma_2} = g_1^{m\beta + r_1} g_2^{x\beta + r_2} = g_1^{m\beta} g_1^{r_1} g_2^{x\beta} g_2^{r_2} = (g_1^m g_2^x)^\beta g_1^{r_1} g_2^{r_2} = y^\beta \alpha$$

and thus the verifier always reaches the accepting state.

SPECIAL SOUNDNESS. Let $(\alpha, \beta, \gamma_1, \gamma_2)$ and $(\alpha, \bar{\beta}, \bar{\gamma}_1, \bar{\gamma}_2)$ two accepting protocol transcripts. To get the extraction formulae, we first express secrets m and x in terms of $\beta, \bar{\beta}, \ldots, \bar{\gamma}_2$ under the assumption that the prover is honest. This leads us to the system of linear equations:

$$
\begin{aligned}
\gamma_1 &= m\beta + r_1 \enspace, & \gamma_2 &= x\beta + r_2 \enspace, \\
\bar{\gamma}_1 &= m\bar{\beta} + r_1 \enspace, & \bar{\gamma}_2 &= x\bar{\beta} + r_2 \enspace,
\end{aligned}
$$

which has the following solution

$$m = \frac{\gamma_1 - \bar{\gamma}_1}{\beta - \bar{\beta}} \enspace, \qquad x = \frac{\gamma_2 - \bar{\gamma}_2}{\beta - \bar{\beta}} \enspace.$$

Next, we have to show that this holds for any accepting transcript pair. Let us verify this by direct algebraic manipulation:

$$g_1^m g_2^x = g_1^{\frac{\gamma_1 - \bar{\gamma}_1}{\beta - \bar{\beta}}} g_2^{\frac{\gamma_2 - \bar{\gamma}_2}{\beta - \bar{\beta}}} = \left(\frac{g_1^{\gamma_1}}{g_1^{\bar{\gamma}_1}} \cdot \frac{g_2^{\gamma_2}}{g_2^{\bar{\gamma}_2}}\right)^{\frac{1}{\beta - \bar{\beta}}} = \left(\frac{\alpha y^\beta}{\alpha y^{\bar{\beta}}}\right)^{\frac{1}{\beta - \bar{\beta}}} = \left(y^{\beta - \bar{\beta}}\right)^{\frac{1}{\beta - \bar{\beta}}} = y \enspace.$$

ZERO-KNOWLEDGE PROPERTY. Recall that the sigma protocol satisfies the zero-knowledge property if the protocol transcript can be simulated as follows:

$$
\begin{array}{l}
\mathsf{Sim} \\
\left[\begin{array}{l}
\beta \leftarrow \mathbb{Z}_q \\
(\alpha, \gamma_1, \gamma_2) \leftarrow \mathcal{S}(\beta) \\
\textbf{return } (\alpha, \beta, \gamma_1, \gamma_2) \enspace.
\end{array}\right.
\end{array}
$$

To show the existence of such simulator, let us first analyse the distribution of γ_1 and γ_2 for a fixed β value. If the prover is honest then

$$\gamma_1 = m\beta + r_1$$
$$\gamma_2 = x\beta + r_2$$

for randomly chosen $r_1, r_2 \xleftarrow[u]{} \mathbb{Z}_q$ and thus γ_1 and γ_2 are independently and uniformly distributed over $\mathbb{Z}_q$. Hence, we know how to sample γ_1 and γ_2 for a fixed β. It remains to derive the value of α. As the valid transcript must satisfy the verification condition

$$g_1^{\gamma_1} g_2^{\gamma_2} = y^\beta \alpha \quad \Leftrightarrow \quad \alpha = g_1^{\gamma_1} g_2^{\gamma_2} \cdot y^{-\beta}$$

we get the following simulator construction

$$\begin{array}{l}\mathcal{S}(\beta) \\ \left[\begin{array}{l}\gamma_1, \gamma_2 \xleftarrow[u]{} \mathbb{Z}_q \\ \alpha \leftarrow g_1^{\gamma_1} g_2^{\gamma_2} \cdot y^{-\beta} \\ \textbf{return } (\alpha, \gamma_1, \gamma_2)\end{array}\right. .\end{array}$$

For the complete proof, we should show that the simulation creates the same distribution as in the real protocol execution. The latter follows from two observations proved above:

- For fixed $\beta, \gamma_2, \gamma_2$ there exists only one α such that $(\alpha, \beta, \gamma_1, \gamma_2)$ is accepting protocol transcript.
- In the protocol execution, the distribution of $(\beta, \gamma_1, \gamma_2)$ is uniform over $\mathbb{Z}_q \times \mathbb{Z}_q \times \mathbb{Z}_q$.

Indeed, the simulator Sim generates first $(\beta, \gamma_1, \gamma_2)$ by uniform sampling and then picks the only possible α value. Thus, it must get the same message distribution.