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

Exercise (Soundness of the QNR-ZK protocol). *Let n be a composite number with a factorisation $n = pq$ known to the prover $\mathcal{P}$. Let $v \in \mathbb{Z}_n^*$ be a number for which the prover wants to prove that it is quadratic non-residue. Show that the the following zero-knowledge protocol*

$$\begin{array}{lcl}
 & \mathcal{P} \qquad\qquad\qquad\qquad\qquad\qquad \mathcal{V} & \\
 & & b \xleftarrow[u]{} \{0,1\}\,, \\
 & \xleftarrow{\qquad\qquad c = r^2 v^b \qquad\qquad} & r \xleftarrow[u]{} \mathbb{Z}_n^* \\
 & \xleftarrow{\qquad\qquad\qquad \alpha \qquad\qquad\qquad} & \alpha \leftarrow \mathcal{P}_{\mathrm{POK}} \\
\beta \leftarrow \mathcal{B} & \xrightarrow{\qquad\qquad\qquad \beta \qquad\qquad\qquad} & \\
\mathsf{Ver}(\alpha, \beta, \gamma) \overset{?}{=} 1 & \xleftarrow{\qquad\qquad\qquad \gamma \qquad\qquad\qquad} & \gamma \leftarrow \mathcal{P}_{\mathrm{POK}}(\beta) \\
\bar{b} \leftarrow \mathsf{IsQnr}_{p,q}(c) & \xrightarrow{\qquad\qquad\qquad \bar{b} \qquad\qquad\qquad} & \bar{b} \overset{?}{=} b
\end{array}$$

where the verifier $\mathcal{V}$ uses disjunctive sigma protocol $\mathrm{POK}[\exists r : c = r^2] \vee \mathrm{POK}[\exists r : c = r^2 v]$ to prove the knowledge of b and r is sound. For that write down the disjunctive proof and show that the distribution of $(c, \alpha, \beta, \gamma)$ messages is independent of b when v is a quadratic residue. After that generalise proof using witness indistinguishability defined as follows. The interactive proof of knowledge $\mathrm{POK}[\exists r, b : c = r^2 v^b]$ is witness indistinguishable if the distributions of (α, β, γ) are independent of (r, b) pairs that satisfy $c = r^2 v^b$.

Solution. The construction of disjunctive sigma protocol $\mathrm{POK}[\exists r : c = r^2] \vee \mathrm{POK}[\exists r : c = r^2 v]$ can be based solely on the standard Fiat-Shamir sigma protocol $\mathrm{POK}[\exists r : c = r^2]$. Indeed, note that v is public value and thus the knowledge of $\exists r : c = r^2 v$ is equivalent to the knowledge of $\exists r : c' = r^2$ for $c' = c/v$.

Before we specify the sigma protocol $\mathrm{POK}[\exists r : c = r^2]$ note that there is a naming clash due to the structure of the zero knowledge protocol. The verifier in the zero-knowledge proof acts as a prover and the prover of the zero-knowledge proof acts as a verifier in the Fiat-Shamir protocol. To simplify the presentation, we align the diagram with the high-level protocol, i.e., the prover of the Fiat-Shamir protocol is on the right. The Fiat-Shamir sigma protocol for $\mathrm{POK}[\exists r : c = r^2]$ is defined through the following diagram:

$$\begin{array}{lcl}
 & \mathcal{V} \qquad\qquad\qquad\qquad\qquad\qquad \mathcal{P} & \\
 & \xleftarrow{\qquad\qquad \alpha = u^2 \qquad\qquad} & u \xleftarrow[u]{} \mathbb{Z}_n^* \\
\beta \xleftarrow[u]{} \{0,1\} & \xrightarrow{\qquad\qquad\qquad \beta \qquad\qquad\qquad} & \\
 & \xleftarrow{\qquad\qquad \gamma = ur^\beta \qquad\qquad} &
\end{array}$$

where the verifying party $\mathcal{V}$ accepts the proof only if $\gamma^2 = \alpha c^\beta$. The protocol is functional as

$$\alpha c^\beta = u^2 (r^2)^\beta = u^2 r^{2\beta} = (ur^\beta)^2 = \gamma^2 \ .$$

The canonical simulator for the Fiat-Shamir protocol, which includes the global parameter c as an explicit argument, is following:

```
$\mathcal{S}(c, \beta)$
    $\gamma \xleftarrow[u]{} \mathbb{Z}_n^*$
    $\alpha \leftarrow \gamma^2 / c^\beta$
    **return** $(\alpha, \beta, \gamma)$ .
```

Recall that for uniformly chosen $\beta \xleftarrow[u]{} \{0,1\}$ the distribution of (α, β, γ) output by the simulator is identical to the distribution of (α, β, γ) generated by the real world execution of between honest $\mathcal{P}$ and $\mathcal{V}$. For the brief proof, note that, even for fixed $b \in \mathbb{Z}_2$, uv^{β} is uniformly distributed over $\mathbb{Z}_n^*$ whenever $u \xleftarrow[u]{} \mathbb{Z}_n^*$ and v is invertible. Consequently, (β, γ) is uniformly distributed over $\mathbb{Z}_2 \times \mathbb{Z}_n^*$ in the real protocol execution. As for fixed β, γ there is only one valid α value, the simulation where we first sample the pair (β, γ) and then compute α must lead to the same distribution as in the real protocol execution.

To be explicit, we specify disjunctive sigma protocol $\textsc{pok}[\exists r : c = r^2] \vee \textsc{pok}[\exists r : c = r^2 v]$ first for the case where $\mathcal{P}$ knows r such that $r^2 = c$ and then for the case where $\mathcal{P}$ knows r such that $vr^2 = c$. In the first case, the prover behaves as follows:

$$\begin{array}{lcl}
\mathcal{V} & & \mathcal{P} \\
 & & \beta_1 \xleftarrow[u]{} \{0,1\} \\
 & & (\alpha_1, \beta_1, \gamma_1) \leftarrow \mathcal{S}(c/v, \beta_1) \\
 & \xleftarrow{\qquad \alpha_0, \alpha_1 \qquad} & u_0 \leftarrow \mathbb{Z}_n^*,\ \alpha_0 \leftarrow u_0^2 \\
\beta \xleftarrow[u]{} \{0,1\} & \xrightarrow{\qquad \beta \qquad} & \beta_0 \leftarrow \beta - \beta_1 \\
 & \xleftarrow{\qquad \beta_0, \beta_1, \gamma_0, \gamma_1 \qquad} & \gamma_0 \leftarrow u_0 r^{\beta_0}
\end{array}$$

In the second case, the prover behaves as follows:

$$\begin{array}{lcl}
\mathcal{V} & & \mathcal{P} \\
 & & \beta_0 \xleftarrow[u]{} \{0,1\} \\
 & & (\alpha_0, \beta_0, \gamma_0) \leftarrow \mathcal{S}(c, \beta_0) \\
 & \xleftarrow{\qquad \alpha_0, \alpha_1 \qquad} & u_1 \leftarrow \mathbb{Z}_n^*,\ \alpha_1 \leftarrow u_1^2 \\
\beta \xleftarrow[u]{} \{0,1\} & \xrightarrow{\qquad \beta \qquad} & \beta_0 \leftarrow \beta - \beta_1 \\
 & \xleftarrow{\qquad \beta_0, \beta_1, \gamma_0, \gamma_1 \qquad} & \gamma_1 \leftarrow u_1 r^{\beta_1}
\end{array}$$

In both cases, the verifier checks that v and c are invariable and the following conditions hold:

$$\beta = \beta_0 + \beta_1, \quad \gamma_0^2 = \alpha_0 c^{\beta_0}, \quad \gamma_1^2 = \alpha_1 \left(\frac{c}{v}\right)^{\beta_1} \quad .$$

To prove the soundness, we must show that malicious prover will gain no useful information during the disjunctive proof of knowledge. First of all, we can assume that the verifier in the zero-knowledge protocol halts if $v \notin \mathbb{Z}_n^*$. Consequently, the only way for the malicious prover to succeed is to send a quadratic residue $v \in \mathbb{Z}_n^*$ instead of quadratic non-residue. Consequently, it is sufficient to show that the distribution of $(c, \alpha, \beta, \gamma)$ is independent of b if v is quadratic residue.

First of all, note that if $v \in \mathbb{Z}_n^*$ is quadratic residue then the verifier in the zero-knowledge proof can get c in two ways: $c = r_0^2$ and $c = r_1^2 v$, which are both equiprobable. Hence, the value c is distributed independently of b. More precisely, c is uniformly distributed over quadratic residues.

As c has two equiprobable decompositions, the verifier of the zero-knowledge uses either the upper or lower specification of $\textsc{pok}[\exists r : c = r^2] \vee \textsc{pok}[\exists r : c = r^2 v]$ to proceed. Next, we will show that even if $\mathcal{V}$ chooses β maliciously based on the commitment message α_0, α_1, the distribution of $\beta_0, \beta_1, \gamma_1, \gamma_2$ is independent of b.

To show that we first give an intuitive claim and then make it explicit through game rewriting argument. For the decomposition $c = r_0^2$, it is easy to see that α_0 and α_1 are uniformly distributed quadratic residues: α_0 by the construction and α_1 by the definition of canonical simulation. They are also independent as they are computed from independent random values. The same claims holds also for the decomposition $c = r_1^2 v$. Consequently, $\mathcal{V}$ chooses β independently from b. Similarly, we can show that the final response message is also independent from b although the analysis must consider the way α_0 and α_1 are computed.

For the formal analysis, we first show that the following games have identical output distributions:

$$\begin{array}{ll}
\mathcal{V}_\circ^{\mathcal{S}} & \mathcal{V}_\circ^{\mathcal{P}} \\
\left[\begin{array}{l}
\beta_1 \xleftarrow[u]{} \{0,1\} \\
(\alpha_1, \beta_1, \gamma_1) \leftarrow \mathcal{S}(c/v, \beta_1) \\
\textbf{return } (\alpha_1, \beta_1, \gamma_1)
\end{array}\right. \qquad\qquad &
\left[\begin{array}{l}
u_1 \leftarrow \mathbb{Z}_n^*, \alpha_1 \leftarrow u_1^2 \\
\beta_1 \leftarrow \{0,1\}, \gamma_1 \leftarrow u_1 r_1^{\beta_1} \\
\textbf{return } (\alpha_1, \beta_1, \gamma_1) \ .
\end{array}\right.
\end{array}$$

The claim is almost evident, except for a small wrinkle – the decomposition is not unique: $c/v = r_1^2 = (-r_1)^2$. However, the latter does not matter. By the definition of the canonical simulator the output distributions must coincide for fixed decomposition. By the transitivity, the output distributions of right games are the same regardless, which of the decompositions we use. This allows us to rewrite the following game that captures the interaction between $\mathcal{P}$ and $\mathcal{V}$ in the disjunctive proof of knowledge:

$$
\begin{array}{l}
\mathcal{V}^{\mathcal{P}_0}(\phi)\\
\left[\begin{array}{l}
\beta_1 \xleftarrow[u]{} \{0,1\}\\
(\alpha_1, \beta_1, \gamma_1) \leftarrow \mathcal{S}(c/v, \beta_1)\\
u_0 \leftarrow \mathbb{Z}_n^*, \alpha_0 \leftarrow u_0^2\\
\beta \leftarrow \mathcal{V}(\phi, \alpha_0, \alpha_1)\\
\beta_0 \leftarrow \beta - \beta_1\\
\gamma_0 \leftarrow u_0 r_0^{\beta_0}\\
\textbf{return } (\alpha_0, \alpha_1, \beta_0, \beta_1, \gamma_0, \gamma_1)
\end{array}\right.
\end{array}
\quad\rightsquigarrow\quad
\begin{array}{l}
\mathcal{V}^{\mathcal{P}_0}(\phi)\\
\left[\begin{array}{l}
u_1 \leftarrow \mathbb{Z}_n^*, \alpha_1 \leftarrow u_1^2\\
\beta_1 \xleftarrow[u]{} \{0,1\}, \gamma_1 \leftarrow u_1 r_1^{\beta_1}\\
u_0 \leftarrow \mathbb{Z}_n^*, \alpha_0 \leftarrow u_0^2\\
\beta \leftarrow \mathcal{V}(\phi, \alpha_0, \alpha_1)\\
\beta_0 \leftarrow \beta - \beta_1\\
\gamma_0 \leftarrow u_0 r_0^{\beta_0}\\
\textbf{return } (\alpha_0, \alpha_1, \beta_0, \beta_1, \gamma_0, \gamma_1)
\end{array}\right.
\end{array}
$$

where the auxiliary input ϕ captures the external knowledge of $\mathcal{V}$ gained before starting the Fiat-Shamir protocol and $c = r_1^2 v$ is one of two possible decompositions. Similarly, we can rewrite the interaction corresponding to the other execution scheme:

$$
\begin{array}{l}
\mathcal{V}^{\mathcal{P}_1}(\phi)\\
\left[\begin{array}{l}
\beta_0 \xleftarrow[u]{} \{0,1\}\\
(\alpha_0, \beta_0, \gamma_0) \leftarrow \mathcal{S}(c, \beta_0)\\
u_1 \leftarrow \mathbb{Z}_n^*, \alpha_1 \leftarrow u_0^2\\
\beta \leftarrow \mathcal{V}(\phi, \alpha_0, \alpha_1)\\
\beta_1 \leftarrow \beta - \beta_0\\
\gamma_1 \leftarrow u_1 r_1^{\beta_1}\\
\textbf{return } (\alpha_0, \alpha_1, \beta_0, \beta_1, \gamma_0, \gamma_1)
\end{array}\right.
\end{array}
\quad\rightsquigarrow\quad
\begin{array}{l}
\mathcal{V}^{\mathcal{P}_1}(\phi)\\
\left[\begin{array}{l}
u_0 \leftarrow \mathbb{Z}_n^*, \alpha_0 \leftarrow u_0^2\\
\beta_0 \xleftarrow[u]{} \{0,1\}, \gamma_0 \leftarrow u_0 r_0^{\beta_0}\\
u_1 \leftarrow \mathbb{Z}_n^*, \alpha_1 \leftarrow u_0^2\\
\beta \leftarrow \mathcal{V}(\phi, \alpha_0, \alpha_1)\\
\beta_1 \leftarrow \beta - \beta_1\\
\gamma_1 \leftarrow u_1 r_1^{\beta_0}\\
\textbf{return } (\alpha_0, \alpha_1, \beta_0, \beta_1, \gamma_0, \gamma_1)
\end{array}\right.
\end{array}
\ .
$$

By simple rearranging it is easy to see that simplified games differ only in the way β_0 and β_1 are sampled:

$$
\begin{array}{l}
\mathcal{V}^{\mathcal{P}_0}(\phi)\\
\left[\begin{array}{l}
u_0 \leftarrow \mathbb{Z}_n^*, \alpha_0 \leftarrow u_0^2\\
u_1 \leftarrow \mathbb{Z}_n^*, \alpha_1 \leftarrow u_1^2\\
\beta \leftarrow \mathcal{V}(\phi, \alpha_0, \alpha_1)\\
\beta_1 \xleftarrow[u]{} \{0,1\}\\
\beta_0 \leftarrow \beta - \beta_1\\
\gamma_0 \leftarrow u_0 r_0^{\beta_0}, \gamma_1 \leftarrow u_1 r_1^{\beta_1}\\
\textbf{return } (\alpha_0, \alpha_1, \beta_0, \beta_1, \gamma_0, \gamma_1)
\end{array}\right.
\end{array}
\qquad\qquad
\begin{array}{l}
\mathcal{V}^{\mathcal{P}_1}(\phi)\\
\left[\begin{array}{l}
u_0 \leftarrow \mathbb{Z}_n^*, \alpha_0 \leftarrow u_0^2\\
u_1 \leftarrow \mathbb{Z}_n^*, \alpha_1 \leftarrow u_0^2\\
\beta \leftarrow \mathcal{V}(\phi, \alpha_0, \alpha_1)\\
\beta_0 \xleftarrow[u]{} \{0,1\}\\
\beta_1 \leftarrow \beta - \beta_1\\
\gamma_0 \leftarrow u_0 r_0^{\beta_0}, \gamma_1 \leftarrow u_1 r_1^{\beta_1}\\
\textbf{return } (\alpha_0, \alpha_1, \beta_0, \beta_1, \gamma_0, \gamma_1)
\end{array}\right.
\end{array}
\ .
$$

As both ways to sample β_0, β_1 are equivalent the outputs of both games are identical. Hence, we have formally shown that the disjunctive proof $\textsc{pok}[\exists r : c = r^2] \vee \textsc{pok}[\exists r : c = r^2 v]$ is indeed witness indistinguishable.

The latter provides us the necessary handle for showing soundness. In brief, as a malicious prover in the zero-knowledge protocol receives messages $\alpha_0, \alpha_1, \beta_0, \beta_1, \gamma_0, \gamma_1$ that are independent of b, he or she can guess b with probability $\frac{1}{2}$. For the formal proof, we could define the game measuring the success of a malicious prover and then use the rearrangement we obtained for proving witness indistinguishability.

Witness indistinguishability as an intermediate security notions provides a way to hide some details. Since c is guaranteed to have a decomposition $c = r^2$ and the proof is witness indistinguishable, the real world interaction is identical to the interaction where the verifier of the zero-knowledge protocol proves the claim $c = r^2$. As we have obtained that c is uniformly distributed over quadratic residues, we can replace the interaction with code that is independent of b and thus obtain the soundness error $\frac{1}{2}$.