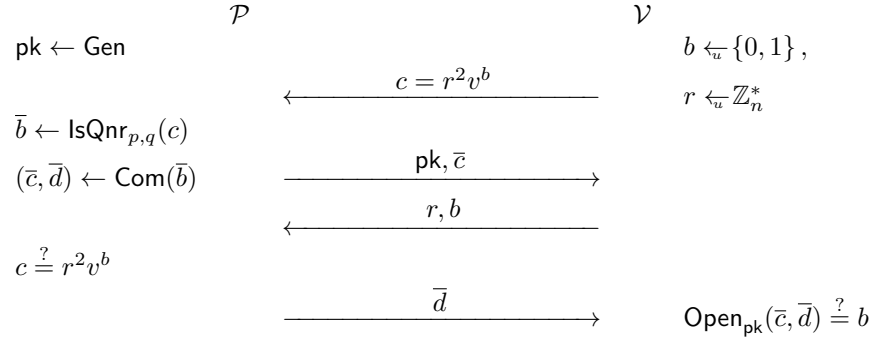


**Exercise (Simulator for the QNR-ZKD protocol).** Let  $n$  be a composite number with a factorisation  $n = pq$  known to the prover  $\mathcal{P}$ . Let  $v \in \mathbb{Z}_n^*$  be a number for which the prover wants to prove that it is quadratic non-residue. Let  $(\text{Gen}, \text{Com}, \text{Open})$  be a perfectly binding and computationally hiding commitment. Show that the the following zero-knowledge protocol



where the verifier  $\mathcal{V}$  releases  $r, b$  is simulatable. For that construct first a semi-efficient algorithm  $\mathcal{K}^{\mathcal{V}_*}$  for extracting  $r, b$  that correspond to initial message  $c$ . Next show that the following simulator construction

$\mathcal{V}_o(\phi)$

[

$\omega \leftarrow \Omega$   
 $c \leftarrow \mathcal{V}_*(\phi; \omega)$   
 $(b_*, r_*) \leftarrow \mathcal{K}^{\mathcal{V}_*}(\phi; \omega)$   
 $\alpha \leftarrow \mathcal{V}_*$   
 $\beta \xleftarrow{u} \mathcal{B}$   
 $\gamma \leftarrow \mathcal{V}_*(\beta)$   
 if  $\text{Ver}(\alpha, \beta, \gamma) = 0$  then **return**  $\mathcal{V}_*(\perp)$   
 if  $\beta_* \neq \perp$  then **return**  $\mathcal{V}_*(b_*)$   
 else **return**  $\perp$

can create an output distribution  $\psi_o$  that is computationally  $(t_o, \varepsilon_o)$ -distant from the output distribution of malicious verifier  $\mathcal{V}_*$  that interacts with the honest prover. Also, estimate how the running-time of the simulator depends on the desired distance  $\varepsilon_o$ .

**Solution.**