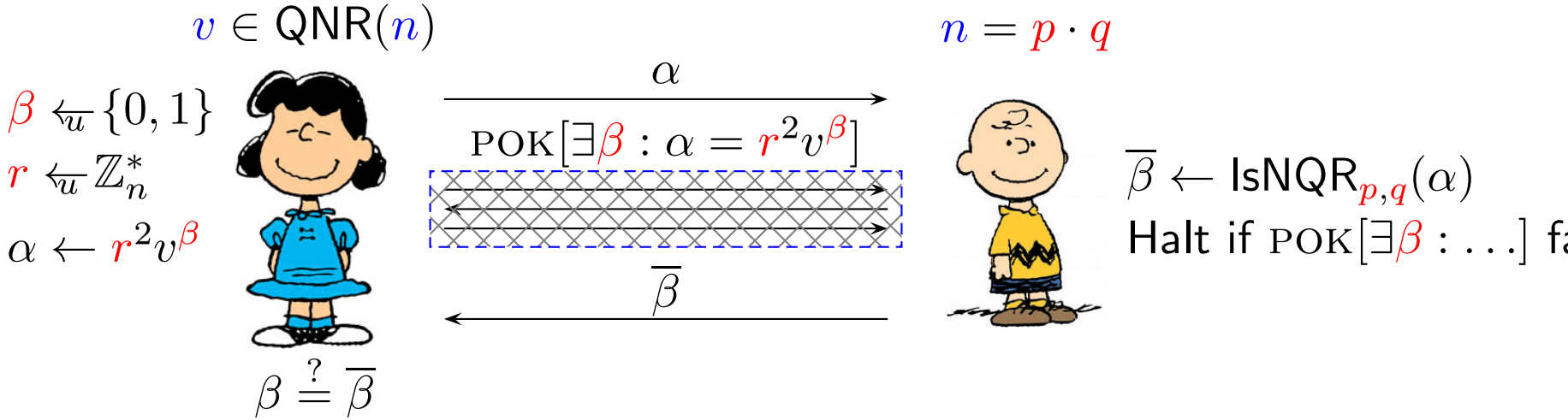
$v \in \mathsf{QNR}(n)$
$n = p \cdot q$
$\beta \xleftarrow{u} \{0,1\}$
$r \xleftarrow{u} \mathbb{Z}_n^*$
$\alpha \leftarrow r^2 v^\beta$
α
$\textsc{pok}[\exists \beta : \alpha = r^2 v^\beta]$
$\overline{\beta}$
$\beta \stackrel{?}{=} \overline{\beta}$
$\overline{\beta} \leftarrow \mathsf{IsNQR}_{p,q}(\alpha)$
Halt if $\textsc{pok}[\exists \beta : \ldots]$ fa