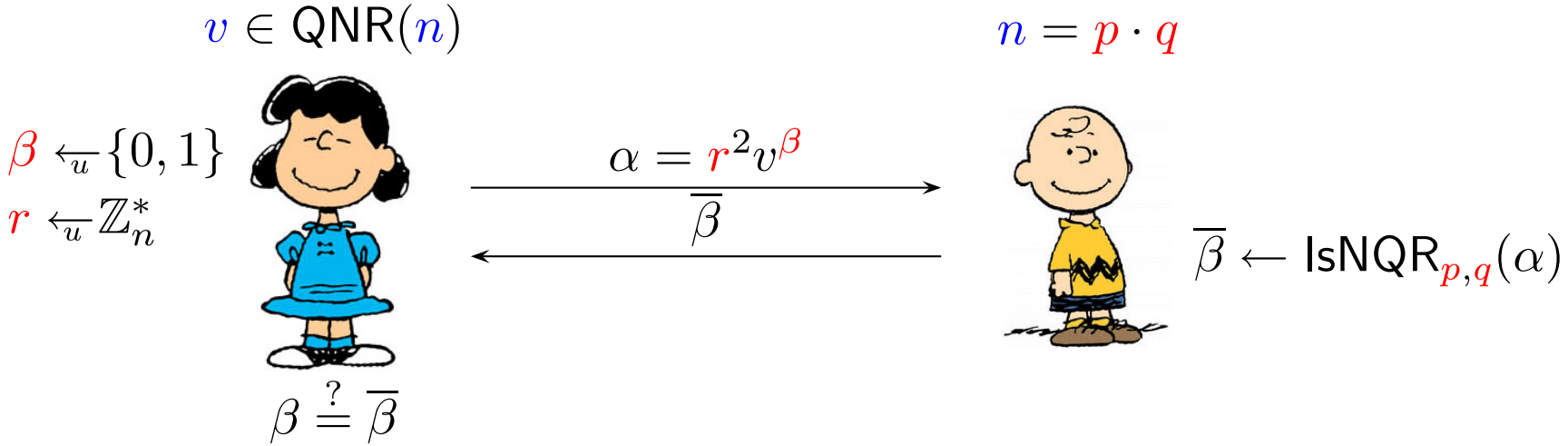
$v \in \mathsf{QNR}(n)$
$n = p \cdot q$
$\beta \leftarrow_u \{0,1\}$
$r \leftarrow_u \mathbb{Z}_n^*$
$\alpha = r^2 v^\beta$
$\overline{\beta}$
$\overline{\beta} \leftarrow \mathsf{IsNQR}_{p,q}(\alpha)$
$\beta \stackrel{?}{=} \overline{\beta}$