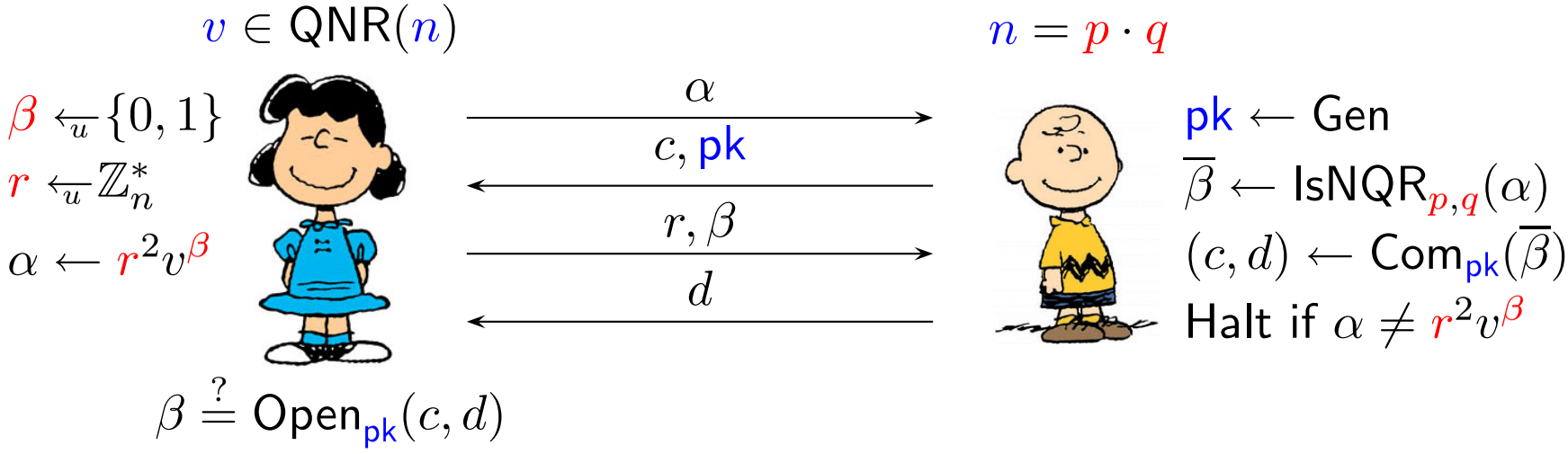
$v \in \mathsf{QNR}(n)$
$n = p \cdot q$
$\beta \leftarrow_u \{0,1\}$
$r \leftarrow_u \mathbb{Z}_n^*$
$\alpha \leftarrow r^2 v^\beta$
α
c, pk
r, β
d
$\mathsf{pk} \leftarrow \mathsf{Gen}$
$\overline{\beta} \leftarrow \mathsf{IsNQR}_{p,q}(\alpha)$
$(c, d) \leftarrow \mathsf{Com}_{\mathsf{pk}}(\overline{\beta})$
Halt if $\alpha \neq r^2 v^\beta$
$\beta \stackrel{?}{=} \mathsf{Open}_{\mathsf{pk}}(c, d)$