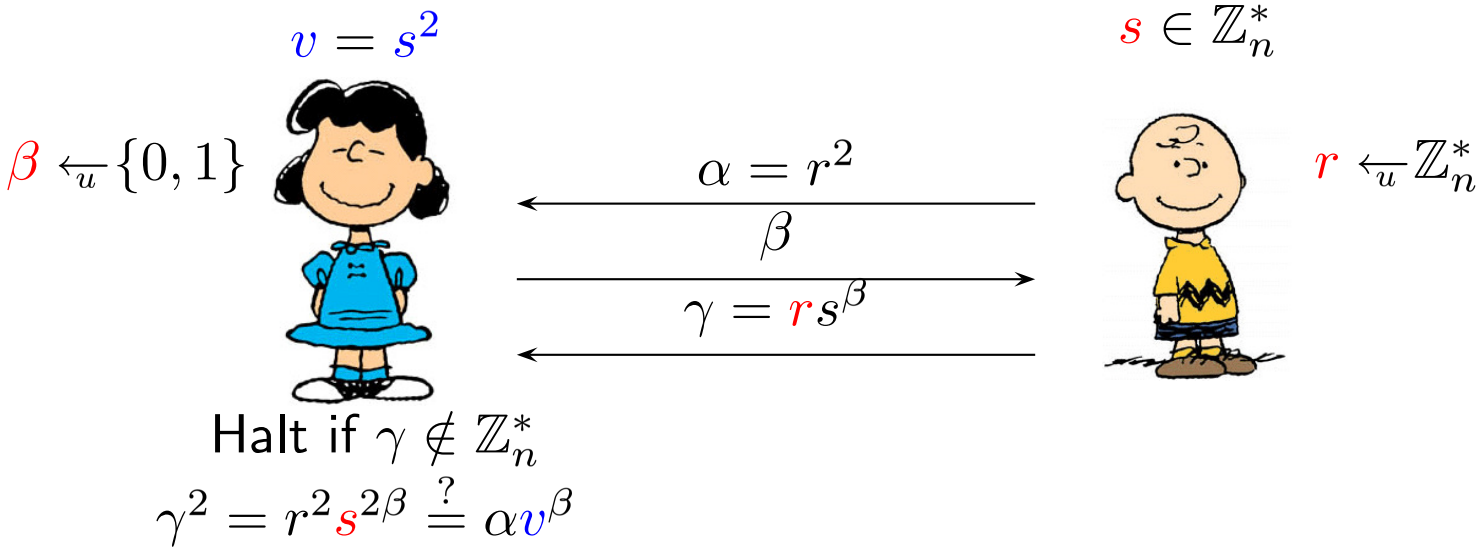
$v = s^2$
$s \in \mathbb{Z}_n^*$
$\beta \leftarrow_u \{0,1\}$
$\alpha = r^2$
β
$\gamma = rs^\beta$
$r \leftarrow_u \mathbb{Z}_n^*$
Halt if $\gamma \notin \mathbb{Z}_n^*$
$\gamma^2 = r^2 s^{2\beta} \stackrel{?}{=} \alpha v^\beta$