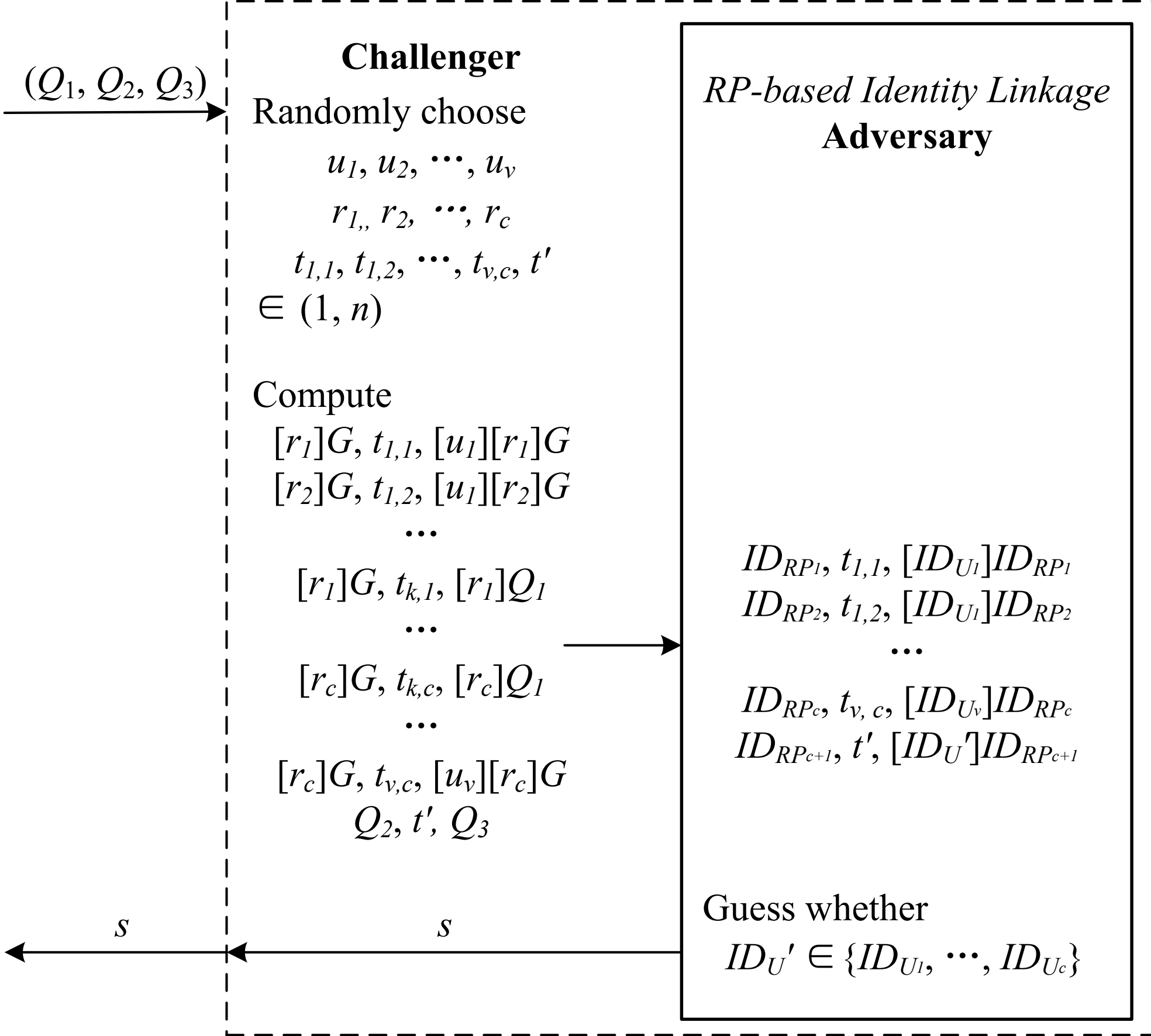
(Q_1, Q_2, Q_3)
Challenger
Randomly choose
$u_1, u_2, \cdots, u_v$
$r_{1,}, r_2, \cdots, r_c$
$t_{1,1}, t_{1,2}, \cdots, t_{v,c}, t'$
$\in (1, n)$
Compute
$[r_1]G, t_{1,1}, [u_1][r_1]G$
$[r_2]G, t_{1,2}, [u_1][r_2]G$
$\cdots$
$[r_1]G, t_{k,1}, [r_1]Q_1$
$\cdots$
$[r_c]G, t_{k,c}, [r_c]Q_1$
$\cdots$
$[r_c]G, t_{v,c}, [u_v][r_c]G$
Q_2, t', Q_3
RP-based Identity Linkage
Adversary
$ID_{RP1}, t_{1,1}, [ID_{U1}]ID_{RP1}$
$ID_{RP2}, t_{1,2}, [ID_{U1}]ID_{RP2}$
$\cdots$
$ID_{RPc}, t_{v,c}, [ID_{Uv}]ID_{RPc}$
$ID_{RPc+1}, t', [ID_U']ID_{RPc+1}$
Guess whether
$ID_U' \in \{ID_{U1}, \cdots, ID_{Uc}\}$
s
s