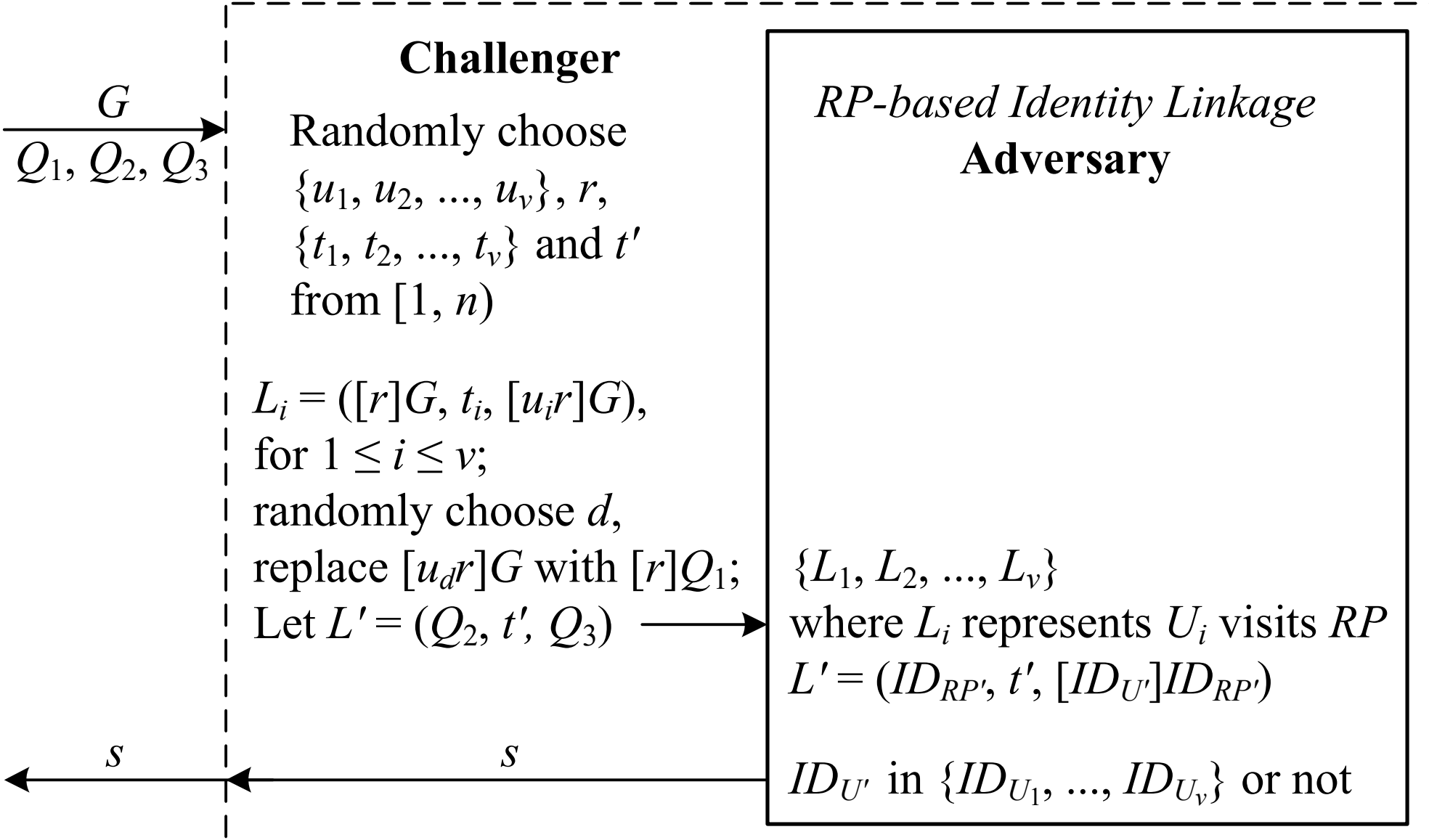
Challenger
RP-based Identity Linkage Adversary
G
Q_1, Q_2, Q_3
Randomly choose $\{u_1, u_2, ..., u_v\}$, r, $\{t_1, t_2, ..., t_v\}$ and t' from [1, n)
$L_i = ([r]G, t_i, [u_i r]G)$, for $1 \le i \le v$;
randomly choose d,
replace $[u_d r]G$ with $[r]Q_1$;
Let $L' = (Q_2, t', Q_3)$
$\{L_1, L_2, ..., L_v\}$
where L_i represents U_i visits RP
$L' = (ID_{RP'}, t', [ID_{U'}]ID_{RP'})$
$ID_{U'}$ in $\{ID_{U_1}, ..., ID_{U_v}\}$ or not
s
s