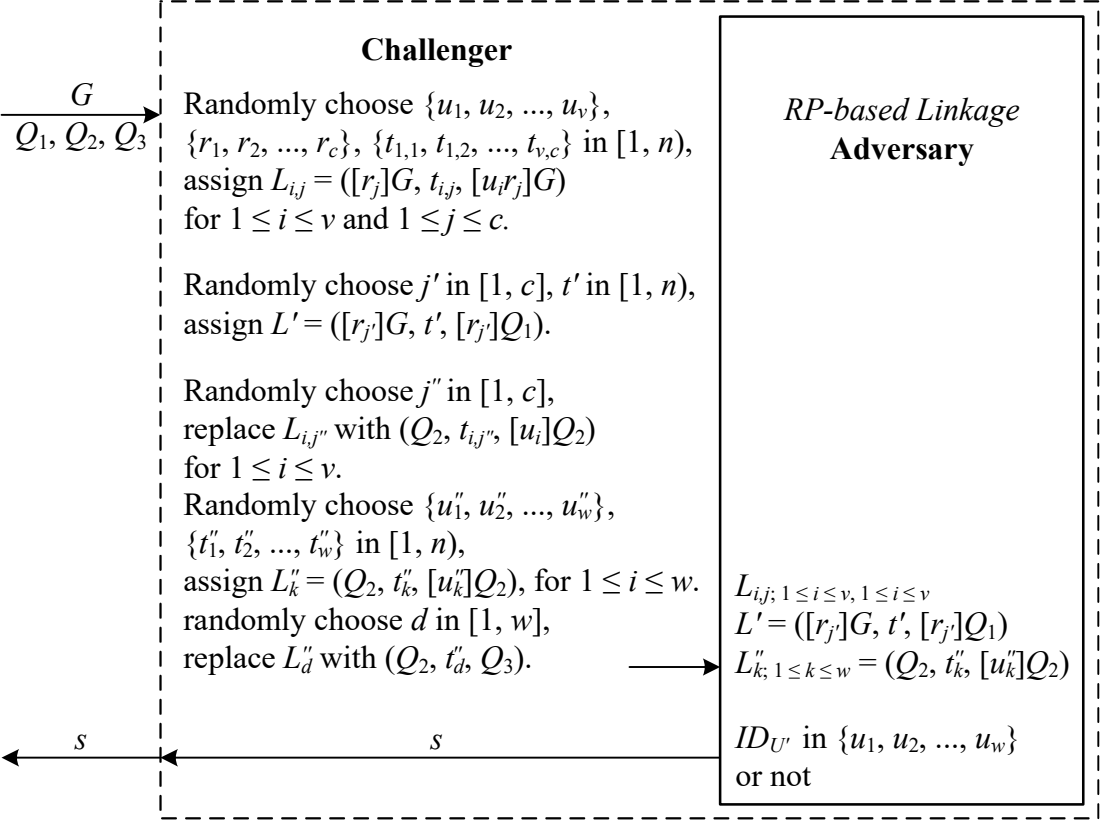
Challenger
G
Q1, Q2, Q3
Randomly choose {u1, u2, ..., uv},
{r1, r2, ..., rc}, {t1,1, t1,2, ..., tv,c} in [1, n),
assign Li,j = ([rj]G, ti,j, [uirj]G)
for 1 ≤ i ≤ v and 1 ≤ j ≤ c.
Randomly choose j′ in [1, c], t′ in [1, n),
assign L′ = ([rj′]G, t′, [rj′]Q1).
Randomly choose j″ in [1, c],
replace Li,j″ with (Q2, ti,j″, [ui]Q2)
for 1 ≤ i ≤ v.
Randomly choose {u1″, u2″, ..., uw″},
{t1″, t2″, ..., tw″} in [1, n),
assign Lk″ = (Q2, tk″, [uk″]Q2), for 1 ≤ i ≤ w.
randomly choose d in [1, w],
replace Ld″ with (Q2, td″, Q3).
RP-based Linkage
Adversary
Li,j; 1 ≤ i ≤ v, 1 ≤ i ≤ v
L′ = ([rj′]G, t′, [rj′]Q1)
Lk″; 1 ≤ k ≤ w = (Q2, tk″, [uk″]Q2)
IDU′ in {u1, u2, ..., uw}
or not
s
s