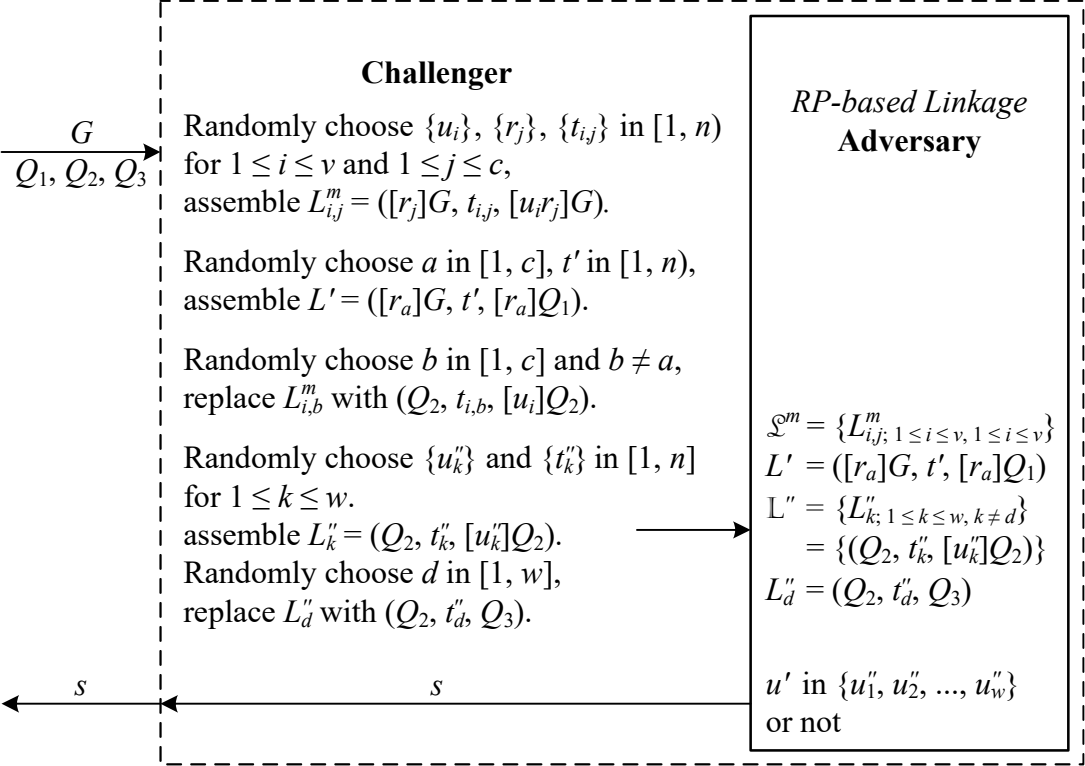
Challenger
RP-based Linkage
Adversary
G
Q1, Q2, Q3
Randomly choose {ui}, {rj}, {ti,j} in [1, n)
for 1 ≤ i ≤ v and 1 ≤ j ≤ c,
assemble L^m_{i,j} = ([rj]G, ti,j, [uirj]G).
Randomly choose a in [1, c], t′ in [1, n),
assemble L′ = ([ra]G, t′, [ra]Q1).
Randomly choose b in [1, c] and b ≠ a,
replace L^m_{i,b} with (Q2, ti,b, [ui]Q2).
Randomly choose {u″k} and {t″k} in [1, n]
for 1 ≤ k ≤ w.
assemble L″k = (Q2, t″k, [u″k]Q2).
Randomly choose d in [1, w],
replace L″d with (Q2, t″d, Q3).
𝕃^m = {L^m_{i,j; 1 ≤ i ≤ v, 1 ≤ i ≤ v}}
L′ = ([ra]G, t′, [ra]Q1)
𝕃″ = {L″k; 1 ≤ k ≤ w, k ≠ d}
= {(Q2, t″k, [u″k]Q2)}
L″d = (Q2, t″d, Q3)
u′ in {u″1, u″2, ..., u″w}
or not
s
s