

Challenger

\xrightarrow{G}
 Q_1, Q_2, Q_3

Randomly choose $\{u_1, u_2, \dots, u_v\}$,
 $\{r_1, r_2, \dots, r_c\}$, $\{t_{1,1}, t_{1,2}, \dots, t_{v,c}\}$ in $[1, n)$,
assign $L_{ij} = ([r_j]G, t_{ij}, [u_i r_j]G)$
for $1 \leq i \leq v$ and $1 \leq j \leq c$

Randomly choose j' in $[1, c]$, t' in $[1, n)$,
assign $L' = ([r_{j'}]G, t', [r_{j'}]Q_1)$

Randomly choose j'' in $[1, c]$,
replace $L_{ij''}$ with $(Q_2, t_{ij''}, [u_i]Q_2)$
for $1 \leq i \leq v$

Randomly choose $\{u''_1, u''_2, \dots, u''_w\}$,
 $\{t''_1, t''_2, \dots, t''_w\}$ in $[1, n)$,
assign $L''_k = (Q_2, t''_k, [u''_k]Q_2)$, for $1 \leq k \leq w$
randomly choose d in $[1, w]$,
replace L''_d with (Q_2, t''_d, Q_3)



RP-based Linkage **Adversary**

$L_{ij}; 1 \leq i \leq v, 1 \leq j \leq c$
 $L' = ([r_{j'}]G, t', [r_{j'}]Q_1)$
 $L''_k; 1 \leq k \leq w = (Q_2, t''_k, [u''_k]Q_2)$

$ID_{U'}$ in $\{u_1, u_2, \dots, u_w\}$
or not

\xleftarrow{S}

\xleftarrow{S}