

Challenger

G
 Q_1, Q_2, Q_3

Randomly choose $u_i, r_j, t_{i,j}$ in $[1, n)$
 for $1 \leq i \leq v$ and $1 \leq j \leq c$,
 assemble $L_{i,j}^m = ([r_j]G, t_{i,j}, [u_i r_j]G)$.

Randomly choose a in $[1, c]$, t' in $[1, n)$,
 assemble $L' = ([r_a]G, t', [r_a]Q_1)$.

Randomly choose b in $[1, c]$ and $b \neq a$,
 replace $L_{i,b}^m$ with $(Q_2, t_{i,b}, [u_i]Q_2)$.

Randomly choose u_k'', t_k'' in $[1, n)$
 for $1 \leq k \leq w$,
 assemble $L_k'' = (Q_2, t_k'', [u_k'']Q_2)$.

Randomly choose d in $[1, w]$,
 replace L_d'' with (Q_2, t_d'', Q_3) .

e

e

RP-based Linkage Adversary

$$\mathcal{L}^m = \{L_{i,j}^m; 1 \leq i \leq v, 1 \leq j \leq c\}$$

$$L_{i,b}^m = (Q_2, t_{i,b}, [u_i]Q_2)$$

$$L' = ([r_a]G, t', [r_a]Q_1)$$

$$\begin{aligned} \mathcal{L}'' &= \{L_k''; 1 \leq k \leq w\} \\ &= \{(Q_2, t_k'', [u_k'']Q_2)\} \end{aligned}$$

$$L_d'' = (Q_2, t_d'', Q_3)$$

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