User U_i ($i \in [1, N]$)

Tally

$x_i \in_r G,\ y_i = g^{x_i} \bmod q$

y_i →

$k_{ij} = \sum_{j \neq i} H\left(y_j^{x_i} \parallel \ell \parallel s\right) \cdot (-1)^{i>j} \bmod 2^{32}$

← $\{y_j\}_{j \in [1,N]}$

$b_{i\ell} = X_{i\ell} + k_{i\ell} \bmod 2^{32}$

$\{b_{i\ell}\}_{\ell \in [1,L]}$ →

Fault recovery (if needed)

← U^{on}

$k'_{ij} = \sum_{\substack{j \neq i \\ j \notin U^{on}}} H\left(y_j^{x_i} \parallel \ell \parallel s\right) \cdot (-1)^{i>j} \bmod 2^{32}$

$\{k'_{i\ell}\}_{\ell \in [1,L]}$ →

$C'_\ell = \left(\sum_{i \in U^{on}} b_{i\ell} - \sum_{i \in U^{on}} k'_{i\ell}\right) \bmod 2^{32}$


SLOW

User U_i ($i \in [1, N]$)

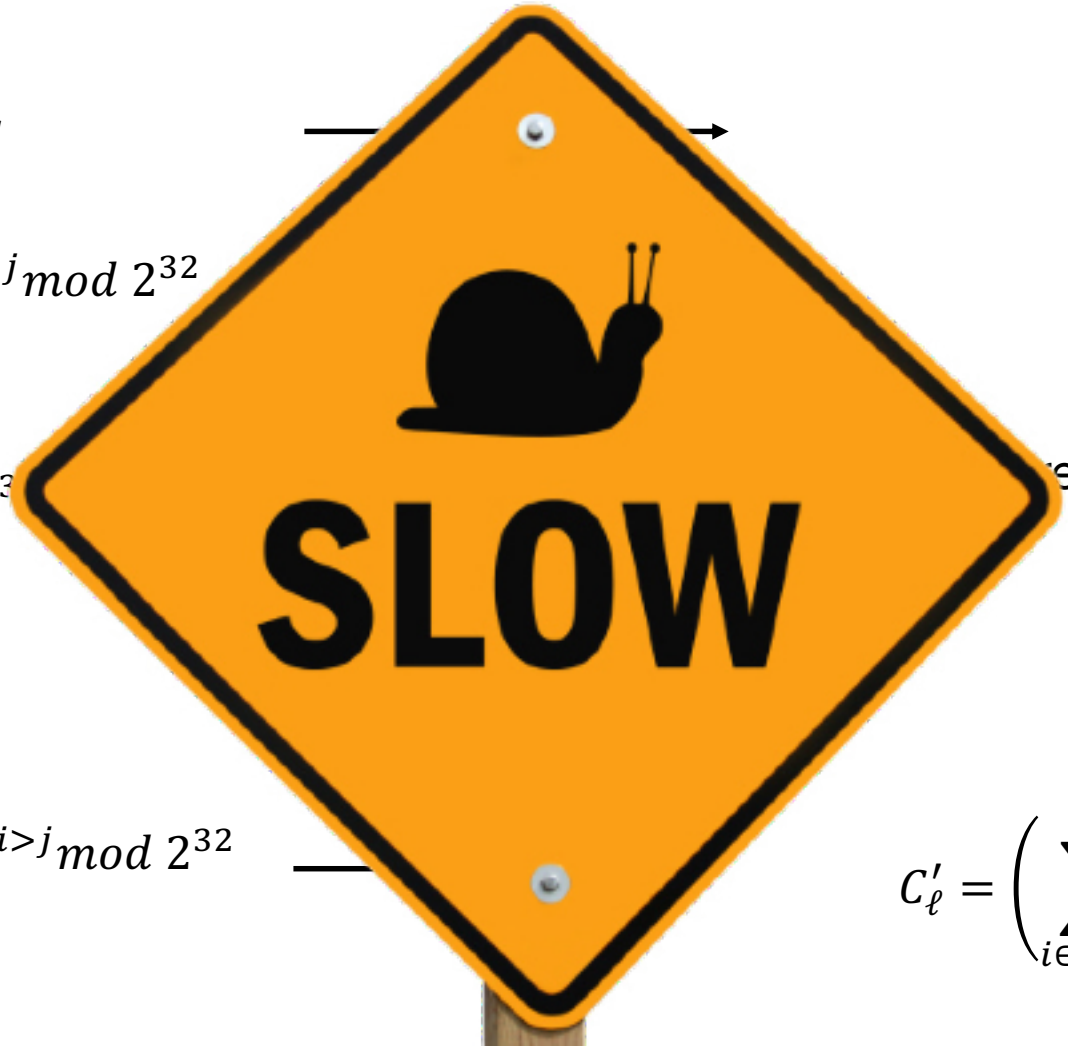
Tally

$$x_i \in_r G,\ y_i = g^{x_i} \bmod q$$

$$k_{ij} = \sum_{j \neq i} H\left(y_j^{x_i} \parallel \ell \parallel s\right) \cdot (-1)^{i>j} \bmod 2^{32}$$

$$b_{i\ell} = X_{i\ell} + k_{i\ell} \bmod 2^{3}$$

ecovery (if needed)



$$k'_{ij} = \sum_{\substack{j \neq i \\ j \notin U^{on}}} H\left(y_j^{x_i} \parallel \ell \parallel s\right) \cdot (-1)^{i>j} \bmod 2^{32}$$

$$C'_\ell = \left(\sum_{i \in U^{on}} b_{i\ell} - \sum_{i \in U^{on}} k'_{i\ell}\right) \bmod 2^{32}$$

So what now?