Private Data Aggregation (PDA)

Goal: Learn aggregate counts (237 users have watched a and b), not who has watched what

Use additively homomorphic encryption

$$Enc_{PK}(x) * Enc_{PK}(y) = Enc_{PK}(x+y)$$

Distribute keys adding up to 0

User $U_1, U_2, \cdots, U_N \longrightarrow k_1 + k_2 + \cdots + k_N = 0$

$Enc_{ki}(x_i) = x+k_i \bmod 2^{32}$

$\Pi_{i=1,..,N} Enc_i(x_i) = \Sigma_{i=1,..,N} (x_i+k_i) = \Sigma_{i=1,..,N} x_i$

Private Data Aggregation (PDA)

Goal: Learn aggregate counts (237 users have watched a and b), not who has watched what

Use additively homomorphic encryption

$Enc_{PK}(x)*Enc_{PK}(y) = Enc_{PK}(x+y)$

Distribute keys adding up to 0

User $U_1, U_2, \cdots, U_N \longrightarrow k_1 + k_2 + \cdots + k_N = 0$

$Enc_{ki}(x_i) = x+k_i \bmod 2^{32}$

$\Pi_{i=1,..,N} Enc_i(x_i) = \Sigma_{i=1,..,N} (x_i+k_i) = \Sigma_{i=1,..,N} x_i$

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}

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

$\{k'_{i\ell}\}_{\ell \in [1,L]}$ →

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