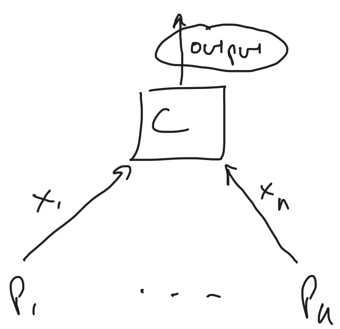
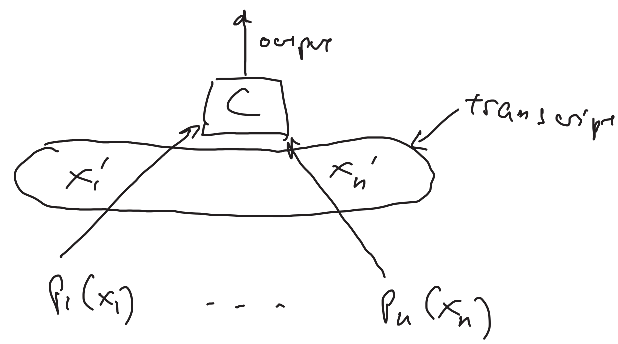
- exam
- scribes?
- lecture recording

Centralized model:



local model:



$R(x_1) \to x_1'$

$x_i \in \{0,1\}$

want to estimate $\sum x_i$

Centralized model: Laplace mechanism $\quad \sum x_i + Lap(1/\varepsilon)$

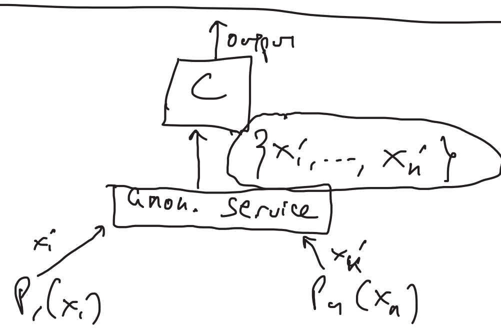
- ε-diff. private
- noise $O(1/\varepsilon)$

local model: local Laplace mechanism: each party sends $x_i' = x_i + Lap(1/\varepsilon)$

Curator releases $\sum x_i'$

- ε-diff private
- noise $O(\sqrt{n}/\varepsilon)$ — optimal

- Shuffle model



I.e., to generate a noisy histogram:

- each party applies randomized response
  - w/ prob. $1-\gamma$, $x_i' = x_i$
  - w/ prob γ, $x_i' \leftarrow \{1, \ldots, k\}$
- each party sends x_i' to anonymous bulletin board
- Curator gets $\{x_1', \ldots x_n'\}$ & generates histogram from that

In expectation, γ-fraction of the parties replace their inputs by random value

Consider changing input of P_1

Case 1: P_1 sends uniform value in $\{1, \ldots, k\}$

view is independent of P_1's input

Case 2: P_1 sends its input (either x_1 or $\hat{x}_1$)

Still a privacy benefit in shuffle model,

b/c w/ some probability, other parties send $x_1 / \hat{x}_1$ due to randomized response

Fix any view of the curator – including bit-vector indicating which parties sent random values

Let V denote the values sent by P_1 & the values sent by the parties sending random values

$$\Pr[M(1, \ldots, x_n) = V] = \binom{|B|}{\underbrace{n_1-1}, n_2, \ldots, n_k} \cdot \underline{\Pr(|B| \text{ parties send random values})}$$

$$\Pr[M(2, x_2, \ldots, x_n) = V] = \binom{|B|}{n_1, n_2-1, \ldots, n_k} \cdot \underline{\Pr(|B| \text{ parties send random values})}$$

$$\binom{|B|}{n_1-1, n_2, \ldots, n_k} = \binom{|B|}{n_1-1} \cdot \binom{|B|-n_1+1}{n_2} \cdot \underline{\binom{|B|-n_1-n_2+1}{n_3} \cdots}$$

$$\binom{|B|}{n_1, n_2-1, \ldots, n_k} = \binom{|B|}{n_1} \cdot \binom{|B|-n_1}{n_2-1} \cdot \underline{\binom{|B|-n_1-n_2+1}{n_3} \cdots}$$

$$\frac{\Pr[M(1, x_2, \dots, x_n) = v]}{\Pr[M(2, x_2, \dots, x_n) = v]} = \frac{\binom{B}{n_1 - 1} \cdot \binom{|B| - n_1 + 1}{n_2}}{\binom{|B|}{n_1} \cdot \binom{|B| - n_1}{n_2 - 1}}$$

$$= \frac{\dfrac{\cancel{|B|!}}{(n_1-1)!\,(B - \cancel{n_1+1})!} \quad \dfrac{(|B| - \cancel{n_1+1})!}{n_2!\,(B - \cancel{n_1 - n_2 + 1})!}}{\dfrac{\cancel{|B|!}}{n_1!\,(B - \cancel{n_1})!} \quad \dfrac{(|B| - \cancel{n_1})!}{(n_2-1)!\,(|B| - \cancel{n_1 - n_2 + 1})!}}$$

$$= \frac{n_1!\,(n_2 - 1)!}{n_2!\,(n_1 - 1)!} = \frac{n_1}{n_2}$$

Application to summation

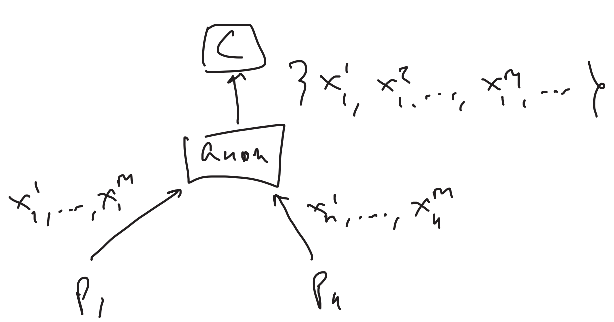
- use this protocol to generate a histogram
- Compute the sum of the contributed values

$\implies$ noise $O(n^{1/3})$

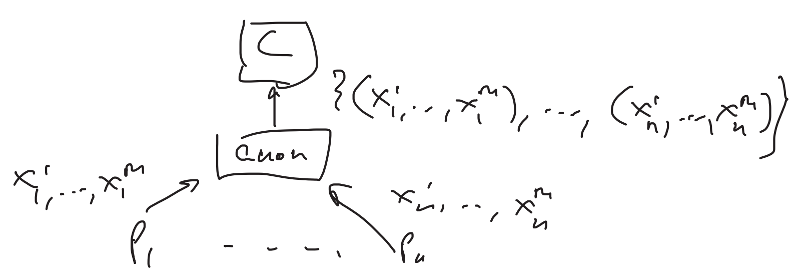
assuming $\varepsilon_0 = O\left(\log\left(\frac{n}{\log 1/\delta}\right)\right)$

Amplification result: Take any R that is ε_0-LDP and run it through the shuffle mechanism, the result is $O\left(\min\{\varepsilon_0, 1\} \cdot e^{\varepsilon_0} \cdot \sqrt{\frac{\log 1/\delta}{n}}, \delta\right)$-DP

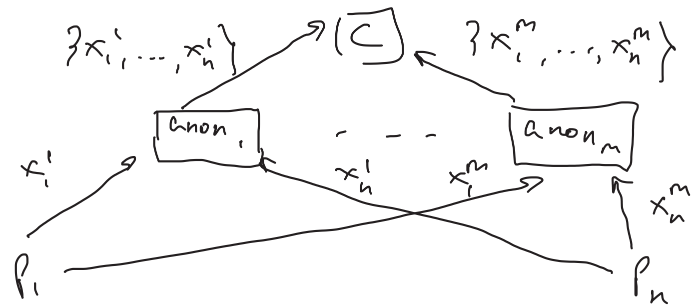
Multi-message shuffle model



single-msg shuffle model



parallel multi-message shuffling



Exact summation using anonymization layer

- want to learn the sum exactly, w/o revealing parties inputs

$$\text{View}(\vec{x}) \approx \text{View}(\vec{x}') \quad \text{for any } \vec{x}, \vec{x}' \text{ w/ the same sum}$$

Protocol: each party P_i w/ input x_i chooses m values $\underline{x_i^1, \dots, x_i^m}$ uniformly subject to $\sum_j x_i^j = x_i \mod q$

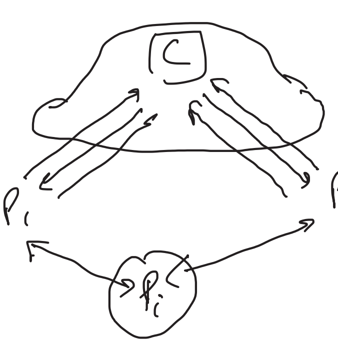
Send $x_i^1, \dots, x_i^m$ to the anon. service

Curator gets $\{x_1^1, \dots, x_1^m, \dots, x_n^1, \dots, x_n^m\}$ and outputs the sum

To achieve differential privacy, apply this protocol to $x_i + \text{noise}_i$

$$\text{final result}: \sum x_i + \underbrace{\sum \text{noise}_i}_{O(1/\varepsilon)}$$

Interactive local model



General protocols