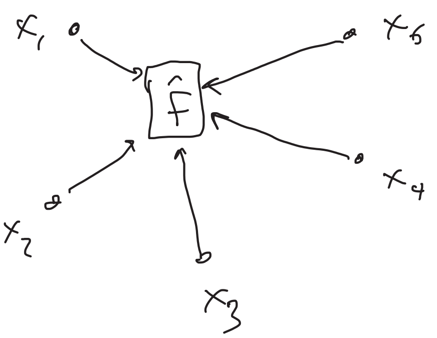
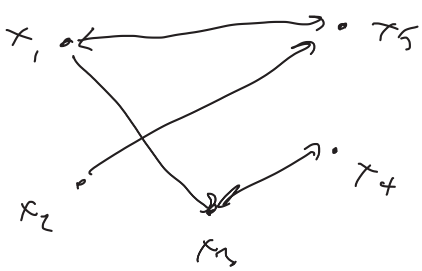
- Scribes?
- lecture recording



Want to compute $f(x_1, \dots, x_n) = \sum x_i$

- instead compute approximation $\hat{f}(\vec{x}) = f(\vec{x}) + Lap(1/\varepsilon)$
- To avoid a central authority, use MPC to compute $\hat{f}$

$\Longrightarrow$ protocol Π that computes a d.p. approx to f



Info.-theoretic diff. privacy of Π:
For any set of t parties & any neighboring inputs $\vec{x}, \vec{x}'$ (that are equal for the t corrupted), & any set of views V

$$\Pr\left[\mathrm{View}_t^{\Pi}(\vec{x}) \in V\right] \le e^{\varepsilon} \cdot \Pr\left[\mathrm{View}_t^{\Pi}(\vec{x}') \in V\right]$$

Computational version of diff privacy of Π
For all efficient distinguishers D:

$$\Pr\left[D\left(\mathrm{view}_t^{\Pi}(\vec{x})\right) = 1\right] \le e^{\varepsilon} \cdot \Pr\left[D\left(\mathrm{view}_t^{\Pi}(\vec{x}')\right) = 1\right] + \underline{\delta(n)}$$

Centralized protocol for summation: $\sum_i x_i + Lap(1/\varepsilon)$

Local protocol for summation: $\sum_i (x_i + Lap(1/\varepsilon))$

(HT): Computationally D.P. protocol for summation:

- Parties set up a threshold homomorphic encryption scheme
  - public key pk

    given $Enc_{pk}(x_1)$, $Enc_{pk}(x_2) \Rightarrow Enc_{pk}(x_1 + x_2)$
  - threshold: every party holds a share sk_i of secret key sk
- Every party sets $\hat{x}_i = x_i + \text{noise}$

  publish $Enc_{pk}(\hat{x}_i)$
- Parties compute $Enc_{pk}(\sum \hat{x}_i)$
- Parties collectively decrypt to get $\sum \hat{x}_i$

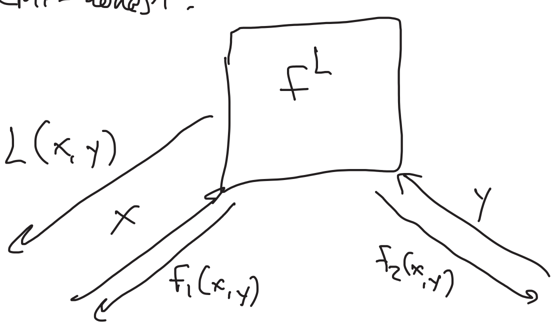
$\Rightarrow$ noise per party can be much lower than in the LDP

Here: use MPC to compute a diff private functionality $\hat{f}$

Another possibility: Could we a (ε, δ)-DP MPC protocol to compute $\hat{f}$

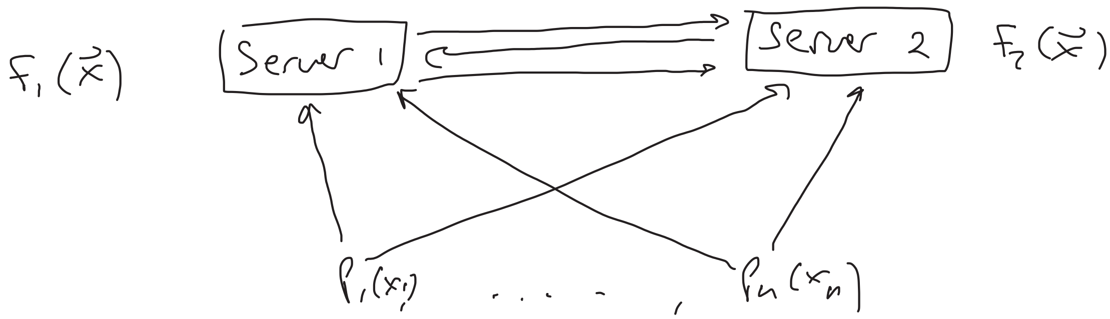
3rd possibility: use a (ε, δ)-DP MPC protocol to compute f

Semi-honest:

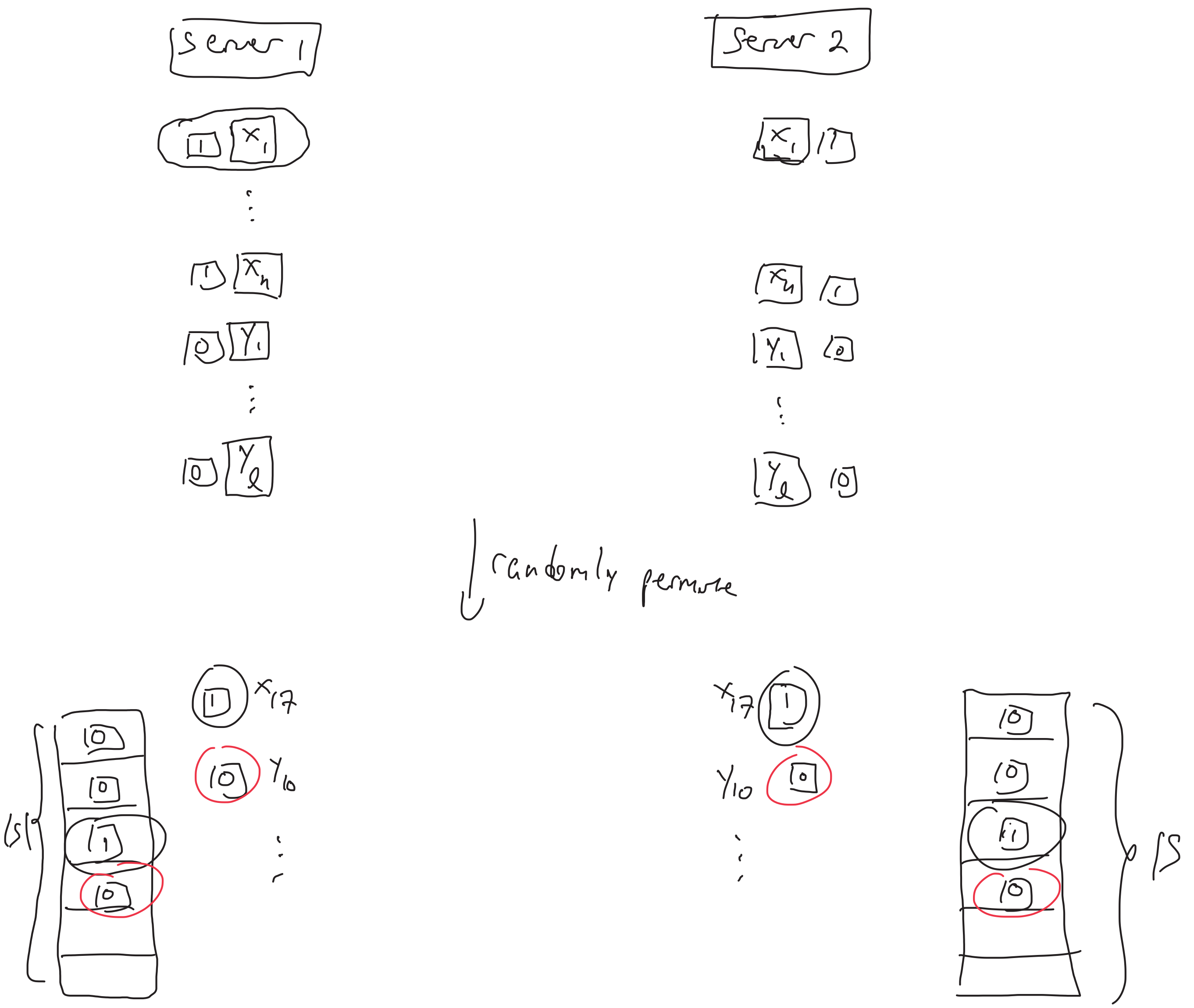


Protocol ε-diff privately computes f:

- π securely computes f^L
- L is ε-d.p.

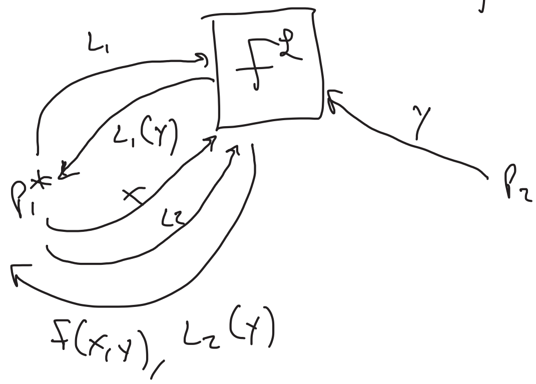


$$f_1(\vec{x}) \oplus f_2(\vec{x}) = f(\vec{x})$$



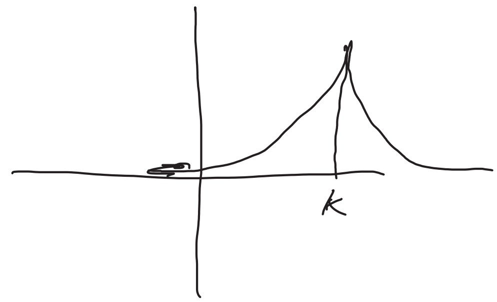
diff. private computation, malicious case

$\mathcal{L} = \{(L_1, L_2)\}$



Protocol π is ε-d.p. if

- $\boxed{\pi \text{ securely realizes } F^{\mathcal{L}}}$
- Every $(L_1, L_2) \in \mathcal{L}$ is ε-diff. private



$\underline{P_1}(x_1, \ldots, x_n)$		$\underline{P_2}(y_1, \ldots, y_n)$
$d'_2, d'_1, x_1, x_{12}, x_{25}$	$\longleftrightarrow$	$y_1, y_2, d_1, d_2.$
x_2, x_7, x_{20}		y_6, y_{21}, y_{30}
$\vdots$		y_3