Motivation

No defense against both privacy and robustness attacks

Can we use DP (Central and/or Local) as a defense?

Intuition:

CDP should limit information exposed about a specific participant

LDP same for records in a participant's dataset

In both cases, the impact of poisonous data should be reduced while simultaneously protecting against inference attacks

50

Motivation

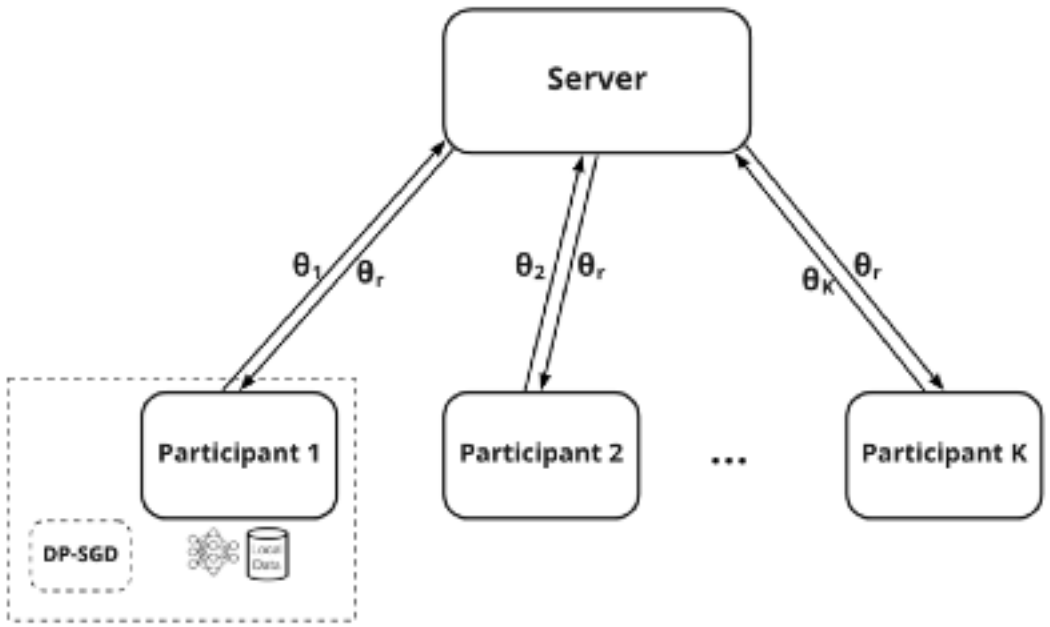
No defense against both privacy and robustness attacks

Can we use DP (Central and/or Local) as a defense?

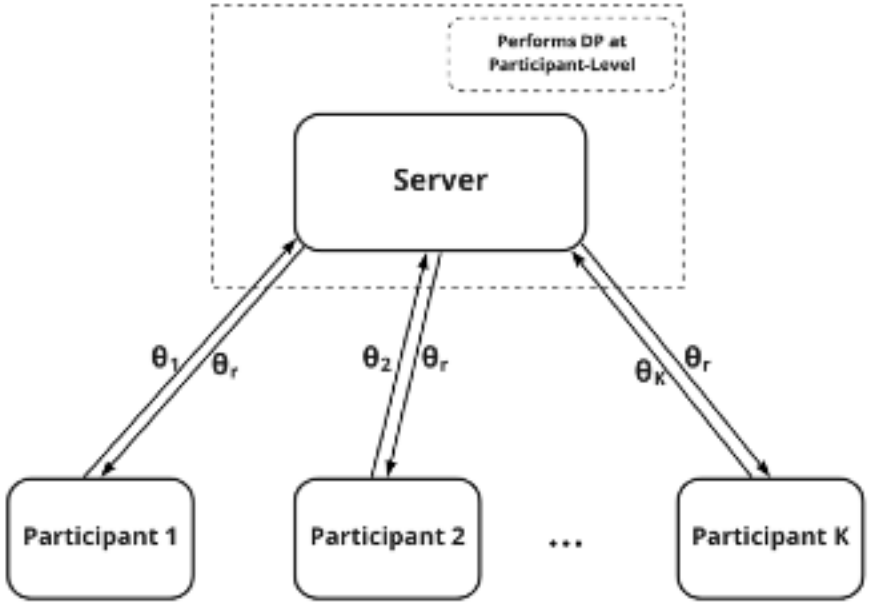
Intuition:

- CDP should limit information exposed about a specific participant
- LDP same for records in a participant's dataset
- In both cases, the impact of poisonous data should be reduced while simultaneously protecting against inference attacks

Local vs Central DP



Local Differential Privacy (LDP)



Central Differential Privacy (CDP)