



NTNU

Norwegian University of
Science and Technology

PARAMETER ESTIMATION UNDER DIFFERENT MODELS OF TRUST

NKS 2025

Espen Sund

October 30, 2025

Contents

Differential Privacy

Trust relations

Ongoing research

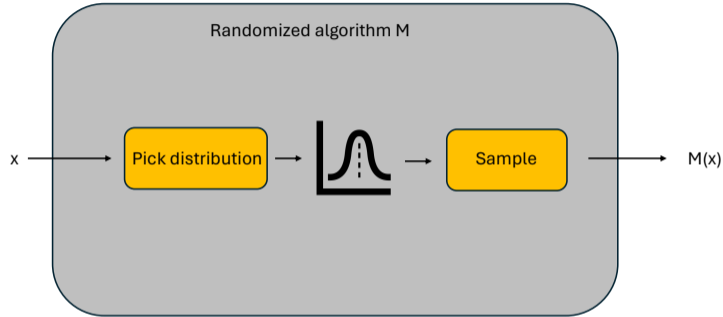
Differential Privacy

- ▶ Data drives everything
- ▶ Privacy/ Utility
- ▶ Overall trends
- ▶ Calibrated randomness

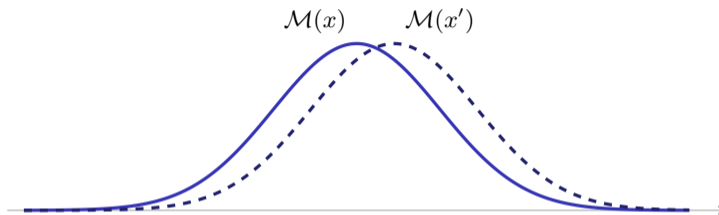


Randomized algorithm

- ▶ Two parts
- ▶ Pick
- ▶ Sample



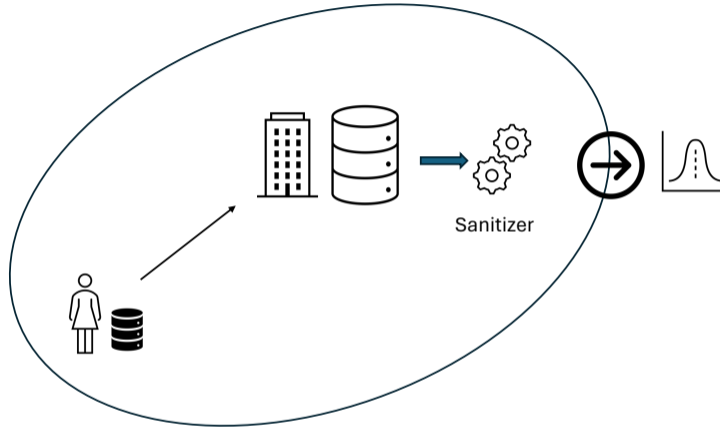
Indistinguishable output distributions



Two neighboring datasets x and x' (differing by one record) yield output distributions that are almost indistinguishable.

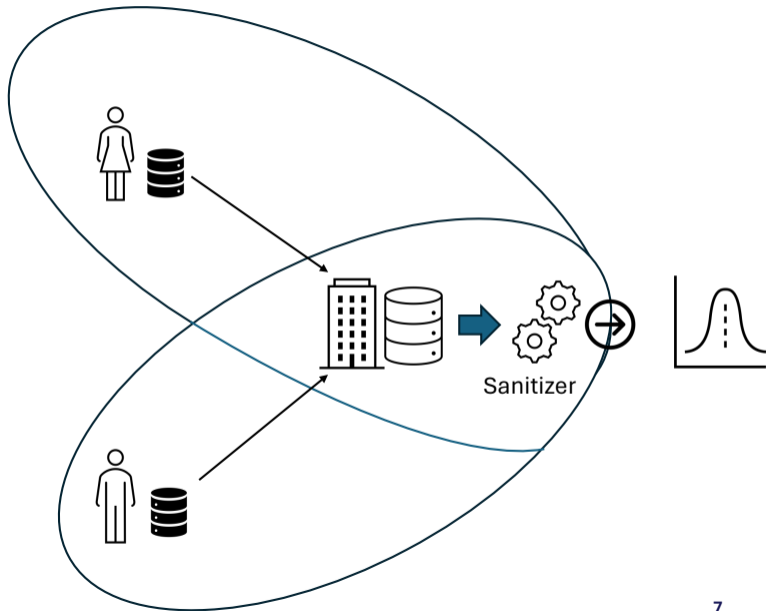
Trust relations

- ▶ How and where
- ▶ Circles of trust
- ▶ Sanitizers



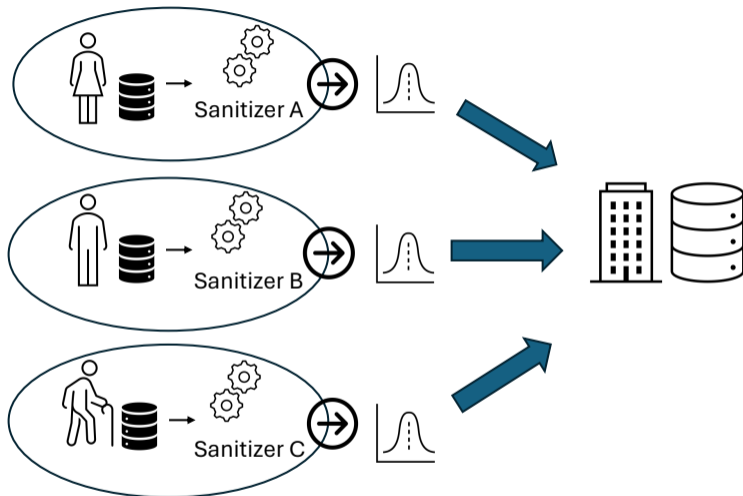
Central model

- ▶ Original setting
- ▶ Trusted data collector



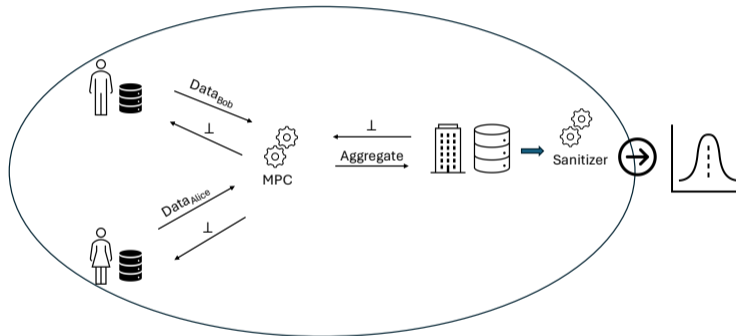
Local model

- ▶ No trusted entity
- ▶ Strong protection
- ▶ More noise



Intermediate trust models

- ▶ Cryptography
- ▶ Best of both worlds
- ▶ Additional costs



Randomized response

- ▶ 1965
- ▶ Reduce evasive bias
- ▶ Plausible deniability
- ▶ $P(\text{"Yes"})$
 $= qp + (1 - q)(1 - p)$
 $= (2q - 1)p + (1 - q)$
- ▶ Estimator $\frac{\bar{Y} - (1 - q)}{2q - 1}$

