

Exploring Utility and Attackability Trade-offs in Local Differential Privacy (LDP)

GitHub 



Contact

 haoying.zhang@inria.fr
 <https://haoyingzhang.github.io>

Haoying Zhang^{1,2} Abhishek K. Mishra¹ Héber H. Arcolezi¹

¹ Inria

² INSA CVL

Motivation

- Selecting ϵ in (L)DP → open challenge
- Balancing privacy vs. utility is difficult
- Practitioners lack tools for tuning & evaluation

Our Solution: LDP-Toolbox

- First web-based benchmarking system for LDP
- Visualizations for utility & attackability
- Flexible parameter tuning across 8 protocols
- Customizable data loader

ϵ -LDP: For any two inputs $x, x' \in \text{Domain}(\Psi)$ and for any output $y \in \text{Range}(\Psi)$:

$$\Pr[\Psi(x) = y] \leq e^\epsilon \Pr[\Psi(x') = y]$$

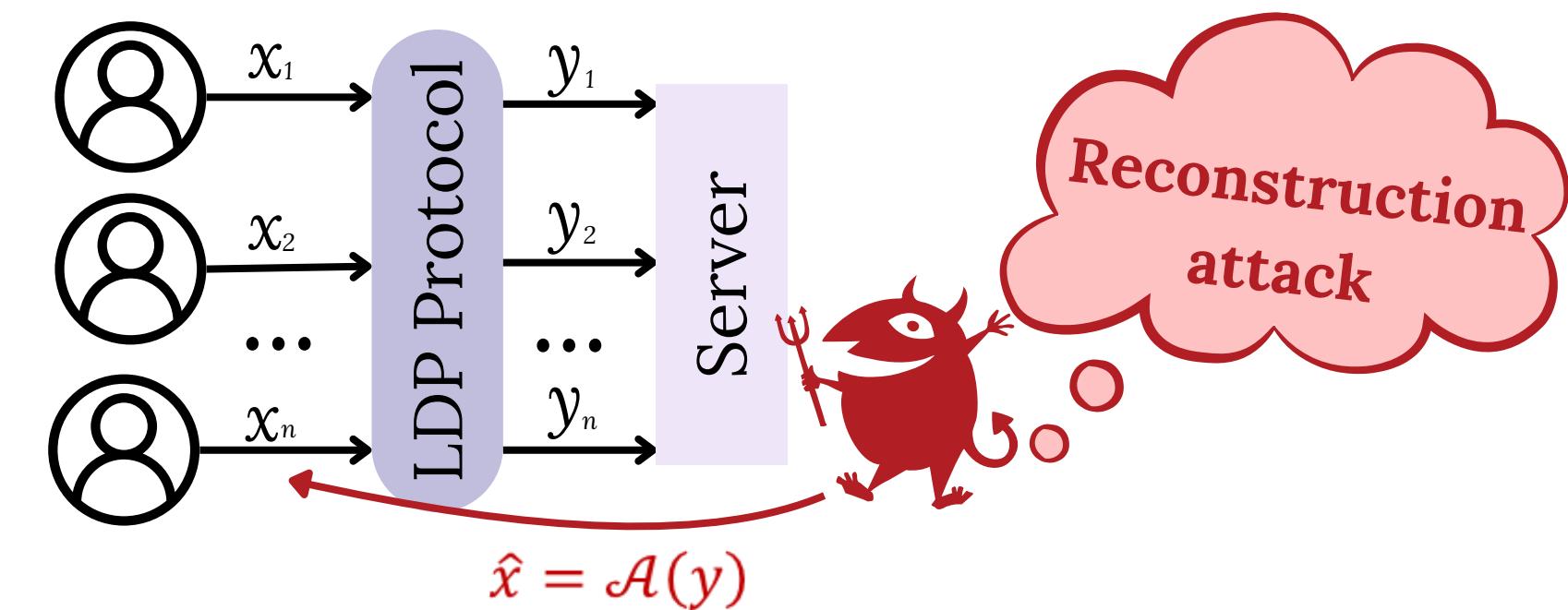
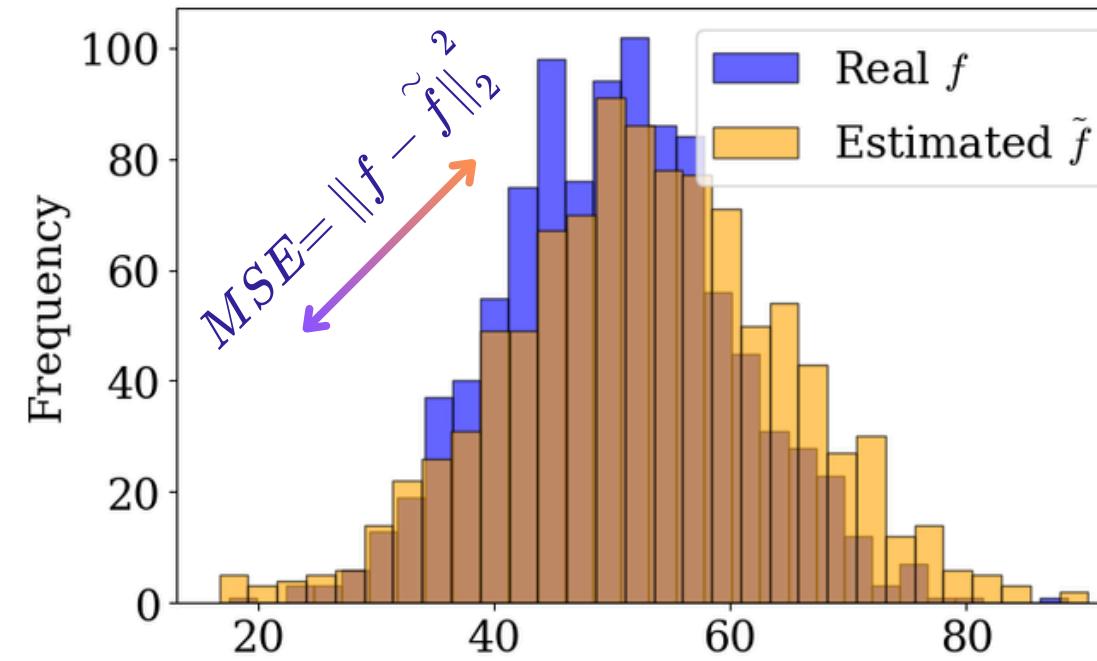


LDP-Toolbox is available on PyPI
`pip install ldp-toolbox`



Core Metrics

- Utility loss [1]
 - Estimation error (e.g., MSE)
- Attackability [2, 3]
 - Reconstruction risk



LDP-Toolbox Modules

- Analytical Visualization
 - Compare theoretical utility vs. attackability
- Custom Upload
 - Explore trade-offs with your own dataset
- Protocol & ϵ Selection (Future Work)
 - Automatic protocol and ϵ recommendation

Workflow Example (Custom Upload)

- Upload dataset and set parameters
 - ϵ -range, protocols, ...
- Compare trade-offs
 - Attackability vs. utility results
- Visualize estimated vs. real distribution
 - Select best protocol

LDP Toolbox

Analytical Visualization

Custom Upload

Upload Custom Dataset

Drag and Drop or Select CSV File
38477 users loaded | 70 attributes

Select attribute: day 0 12h
Define value range

Is this a location dataset? (Heatmap visualization)
Yes

Percentage of users to sample: 1% 20 100%
Select All

Select Protocol(s):
 Generalized Randomized Response (GRR)
 Binary Local Hashing (BLH)
 Optimized Local Hashing (OLH)
 Symmetric Unary Encoding (SUE)
 Optimized Unary Encoding (OUE)
 Subset Selection (SS)
 Summation with HE (SHE)
 Thresholding with HE (THE)

ϵ Range: 2.5 4 6 8 10 12 14 16 18 20
Compute

Attackability

Attackability for Low $\epsilon = 2.50$
Attackability for Medium $\epsilon = 6.25$
Attackability for High $\epsilon = 10.00$

Utility Loss

Choose a Utility Metric:
smaller is better | higher is better
MSE

Utility Loss for Low $\epsilon = 2.50$
Utility Loss for Medium $\epsilon = 6.25$
Utility Loss for High $\epsilon = 10.00$

Distribution & Heatmap

Choose a protocol: GRR
Choose an epsilon range between low, medium and high:
high

Real vs Estimated Distribution for High $\epsilon = 10.00$ with MSE = 0.73

Original Grid Heatmap
Estimated Heatmap for High $\epsilon = 10.00$

References

- G. Cormode, S. Maddock, C. Maple. "Frequency estimation under local differential privacy". VLDB 2021.
- H.H. Arcolezi, S. Gambs. "Revisiting LDP Protocols: Towards Better Trade-offs in Privacy, Utility, and Attack Resistance". ArXiv 2025.
- M.E. Gursoy, et al. "An adversarial approach to protocol analysis and selection in local differential privacy". IEEE TIFS 2022.