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

Haoying Zhang [1,2] **Abhishek K. Mishra** [1] **Héber H. Arcolezi** [1]

[1] Inria [2] INSA CVL

Contact

haoying.zhang@inria.fr

https://haoyingzhang.github.io

GitHub ★

ACM CCS 2025

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 $x, x' \in$ Domain(Ψ) and for any output $y \in$ Range(Ψ):

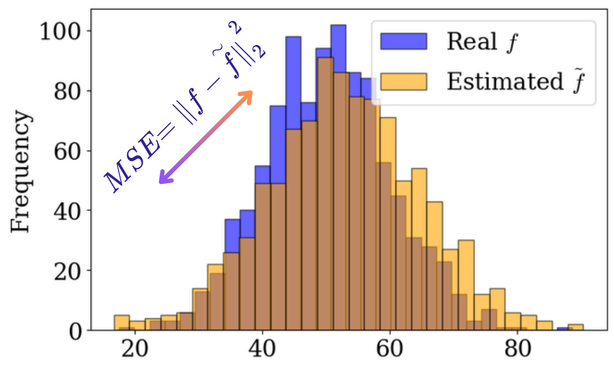
$$Pr[\Psi(x) = y] \leqslant e^{\varepsilon} Pr[\Psi(x') = y]$$

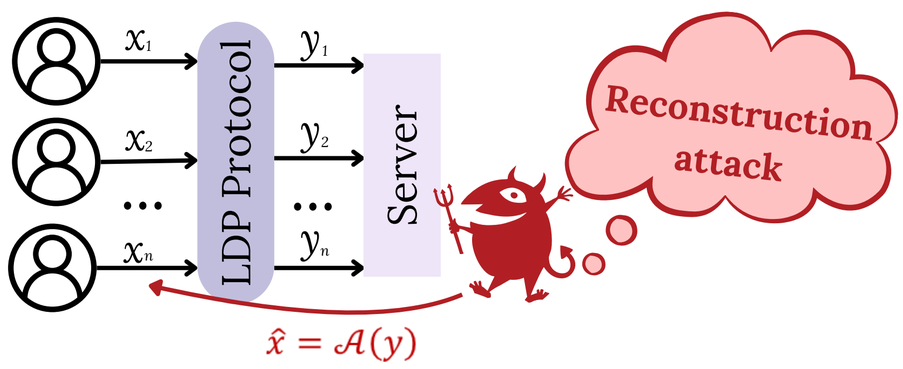
LDP-Toolbox is available on PyPI

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)

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

References

[1] G. Cormode, S. Maddock, C. Maple. "*Frequency estimation under local differential privacy*". VLDB 2021.

[2] H.H. Arcolezi, S. Gambs. "*Revisiting LDP Protocols: Towards Better Trade-offs in Privacy, Utility, and Attack Resistance*". ArXiv 2025.

[3] M.E. Gursoy, et al. "*An adversarial approach to protocol analysis and selection in local differential privacy*". IEEE TIFS 2022.