MURS: Practical and Robust Privacy Amplification with Multi-Party Differential Privacy

Tianhao Wang, Min Xu, Bolin Ding, Jingren Zhou, Cheng Hong, Zhicong Huang, Ninghui Li, Somesh Jha
Purdue University, University of Chicago, Alibaba Group, University of Wisconsin-Madison

Background

- **Multi-Party Differential Privacy: Better trust than DP and better utility than LDP**

  ![Multi-Party Differential Privacy System Model](image)

  *Figure 1: Multi-Party Differential Privacy System Model*

- Existing work either provides poor utility [5, 3, 2, 6] or high communication overhead [1, 4].
- The system model in Figure 1 is weak.

System Analysis of MPDP

- The server colluding with all other users.
- The server with \( t \geq 1 \) auxiliary servers.
- The auxiliary servers may poison the result.

SLH

- Utilizing the Local Hashing idea, we improve the utility of existing work.

MURS

- Utilizing Onion Encryption and Oblivious Shuffle, we improve the threat model of existing work.

![System Model of MURSS: Sequential Shuffle.](image)

*Figure 2: System Model of MURSS: Sequential Shuffle.*

- The auxiliary servers may poison the result.

Evaluation Results

- Reasonable communication and computation overhead.
- Utility (mean absolute error) is orders of magnitudes better.

![Utility Comparison. SH is from [2], AUE is from [1] (but communication cost is much larger), Base is uniform guess, and Lap is centralized DP.](image)

*Figure 4: Utility Comparison. SH is from [2], AUE is from [1] (but communication cost is much larger), Base is uniform guess, and Lap is centralized DP.*

References