The 40th Annual AAAI Conference on Artificial Intelligence

Private Frequency Estimation Via Residue Number Systems

Héber H. Arcolezi

heber.hwang-arcolezi@inria.fr

Inria, France

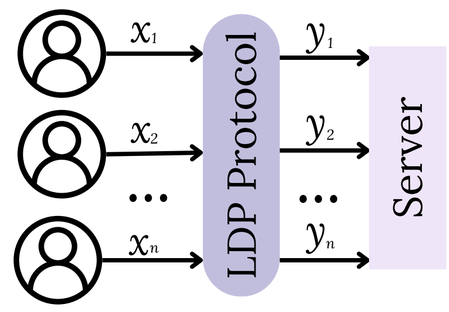
https://hharcolezi.github.io/

Paper

Code

Motivation

- Local Differential Privacy (**LDP**) → allows to privatize data before sharing
- Highly adopted by **Big Tech** → large-scale frequency monitoring systems
- Real-world AI systems operate on **very large alphabets**
- **Challenge:** four-way trade-off
  - Utility (↑), Communication cost (↓), Server runtime (↓), Robustness to reconstruction attacks (↑)
  - Existing protocols optimize only **subsets** of these constraints



We need LDP protocols that are accurate, lightweight, fast, and attack-resistant

Our Contribution: Modular Subset Selection (MSS)

User: Report one noisy modular view

x = 17

RNS

mod 5	mod 7	mod 11
r_0=17→2	r_1=17→3	r_2=17→6

Randomly select **one** modulus $j \in \{0,1,2\}$

Privatization via ε-LDP(r_j)

y = (modulus index, privatized residue)

Example ("top-20 URL"):
- domain size = 20
- Moduli: {5, 7, 11}

Residue Number System (RNS): split a large alphabet into few small modular views

Randomized modular view (single report)

Server: Aggregation & decoding

Reports:

(j=0, Y) (j=1, Y) (j=2, Y)

group by modulus *j*

j=0 *j*=1 *j*=2

Weighted least squares (CRT-based)

Estimated frequency vector

Why MSS Works (Results & Takeaway)

Near-optimal utility 🎯

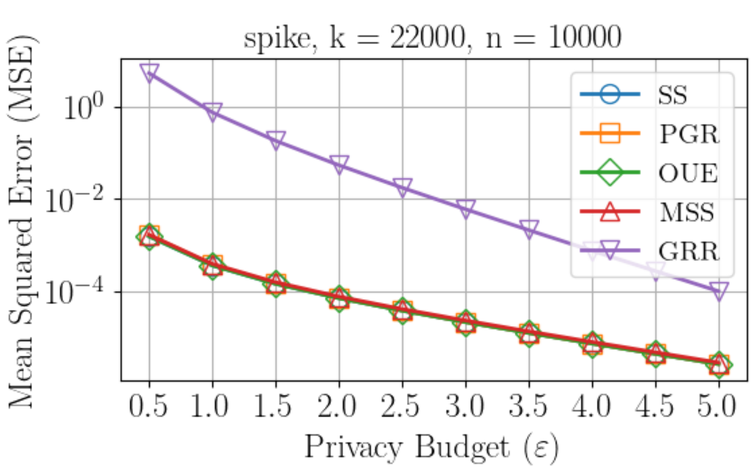
Matches state-of-the-art
Stable across privacy budgets
No collapse for large alphabets

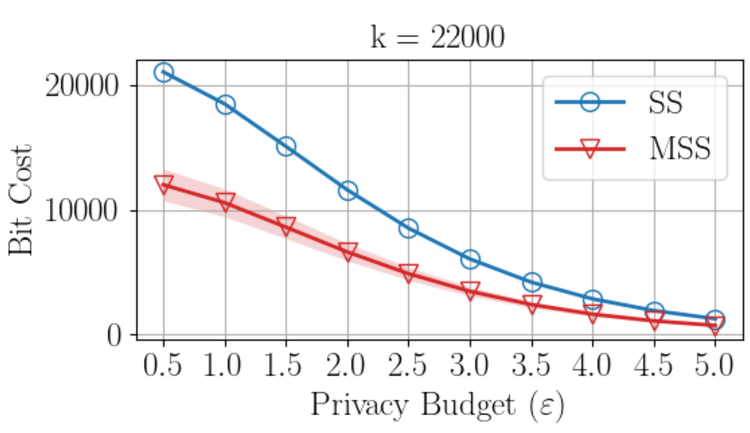
System efficiency ⚡📦

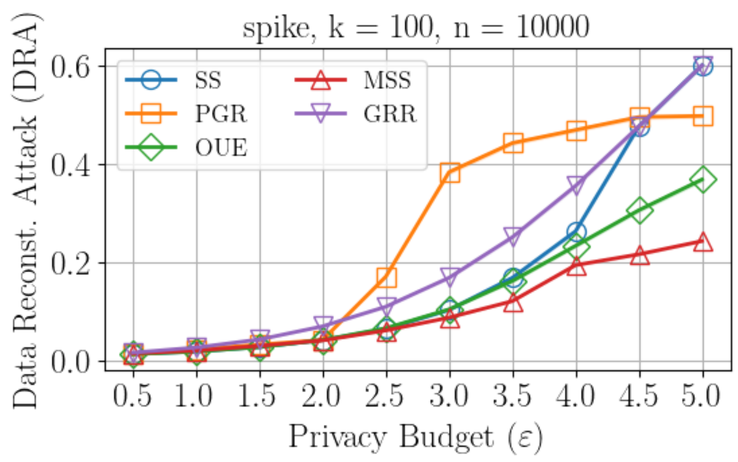
Short messages (few bits)
Fast server-side decoding
Scales to very large domains

Practical privacy 🛡️

Randomized modular view
Lowest reconstruction risk
Stronger protection in practice







MSS shows that large-alphabet LDP can be both practical and robust to reconstruction attacks

References

[1] Kasiviswanathan, Shiva Prasad, et al. "What can we learn privately?." SIAM Journal on Computing 40.3 (2011): 793-826..

[2] Szabo, Nicholas S., and Richard I. Tanaka. "Residue arithmetic and its applications to computer technology." (1967).

[3] Ye, Min, and Alexander Barg. "Optimal schemes for discrete distribution estimation under locally differential privacy." IEEE Transactions on Information Theory 64.8 (2018): 5662-5676.