ERGUTE BAO

13 Computing Drive, 117417, Singapore

baoergute8@gmail.com | https://erguteb.github.io | +86 18126160962

RESEARCH INTEREST

Privacy-preserving data analysis, with a focus on Differential Privacy (DP) for machine learning and distributed computing.

EDUCATION

National University of Singapore (NUS) 2024
Ph.D. in Computer Science
Thesis: Algorithms for Differential Privacy under Distributed Settings.
Advisor: Xiaokui Xiao

The Chinese University of Hong Kong (CUHK) 2018
B.Sc. in Computer Science (First Class Honours), Minor in Mathematics

PUBLICATIONS

1. Fei Wei, **Ergute Bao**, Xiaokui Xiao, Yin Yang, and Bolin Ding.
   AAA: an Adaptive Mechanism for Locally Differential Private Mean Estimation.
   Proceedings of the VLDB Endowment (PVLDB), 2024.

2. **Ergute Bao**, Dawei Gao, Xiaokui Xiao, Yaliang Li.
   Communication Efficient and Differentially Private Logistic Regression under the Distributed Setting.
   Proceedings of the SIGKDD Conference on Knowledge Discovery and Data Mining (SIGKDD), 2023.

3. Jianxin Wei, **Ergute Bao**, Xiaokui Xiao, Yin Yang.
   DPIS: an Enhanced Mechanism for Differentially Private SGD with Importance Sampling.
   Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS), 2022.

4. **Ergute Bao**, Yizheng Zhu, Xiaokui Xiao, Yin Yang, Beng Chin Ooi, B.H.M. Tan, K.M.M. Aung.
   Skellam Mixture Mechanism: a Novel Approach to Federated Learning with Differential Privacy.
   Proceedings of the VLDB Endowment (PVLDB), 2022.

5. **Ergute Bao**, Yin Yang, Xiaokui Xiao, and Bolin Ding.
   CGM: An Enhanced Mechanism for Streaming Data Collection with Local Differential Privacy
   Proceedings of the VLDB Endowment (PVLDB), 2021.

6. **Ergute Bao**, Xiaokui Xiao, Jun Zhao, Dongping Zhang and Bolin Ding.
   Synthetic Data Generation with Differential Privacy via Bayesian Networks
   Journal of Privacy and Confidentiality (JPC), 2021, 11(3).
   Invited paper, based on our solution for 2018 NIST DP challenge.

MANUSCRIPTS

1. **Ergute Bao**, Fei Wei, Xiaokui Xiao, Yin Yang, Tianyu Pang, and Du Chao.
   Secure and Effective Federated Learning with Distributed Differential Privacy for Vertically Partitioned Data.

2. Jianxin Wei, Yizheng Zhu, Xiaokui Xiao, **Ergute Bao**, Yin Yang, and Beng Chin Ooi.
   GCON: Differentially Private Graph Convolutional Network via Objective Perturbation.

SERVICES

Reviewer for ICML (2022), DASFAA (Demo 2023-24), IEEE TKDE (2022-24), IEEE Transactions on Information Forensics and Security (2024), International Journal of Information Security (2024), IEEE Transactions on Privacy (2024).
Subreviewer or external reviewer for VLDB, SIGMOD, and ICDE.

INTERNSHIPS

Tongyi, Alibaba — Summer 2024
Project: LLMs with multi-intelligence agents.
Host: Fei Wei and Yaliang Li.

Sea AI Lab (SAIL) — Spring 2023
Project: DP algorithms for Vertical Federated Learning.
Host: Tianyu Pang and Chao Du.

DAMO Academy, Alibaba — Summer 2022
Project: DP algorithms for Horizontal Federated Learning.
Host: Yaliang Li.

Faculty of Engineering, CUHK — Summer 2017, Summer 2016
Project: Dimensionality Reduction algorithms for distributed systems.
Host: James Cheng

AWARDS AND HONORS

First place (out of 88 competitors) in the 2020 NIST Differential Privacy Temporal Map Challenge.
Third place (out of 87 competitors) in the 2018 NIST Differential Privacy Synthetic Data Challenge.
Dean's Graduate Research Excellence Award 2023 by NUS School of Computing.
Research Achievement Award 2021 & 2022 by NUS School of Computing.
Research Scholarship 2018-2022 by NUS.
Dean's list in 2015/16, 16/17, 17/18 by CUHK.
The Cheng Foundation Scholarships 2016/17 by CUHK.
ELITE Scholarships 2016/17 by CUHK.
Engineering Faculty Alumni Association Scholarships 2017/18 by CUHK.
George Lam Tse Cheung Scholarships 2016/17, awarded by Lee Woo Sing College, CUHK.

INVITED TALKS

Talk on *Additive Discrete Noise Mechanisms for Differential Privacy*, Privacy reading group, Michigan State University, (2024).

Talk on *the Skellam Mechanism for Distributed Differential Privacy*, Privacy Innovation Lab, TikTok (2023).
Talk on *Protecting Data with Differential Privacy*, DAMO Academy, Alibaba (2022).