ERGUTE BAO

13 Computing Drive, 117417, Singapore

ergute@comp.nus.edu.sg | https://erguteb.github.io

RESEARCH INTEREST

Privacy-preserving data analysis, with a focus on Differential Privacy (DP) under distributed settings.

EDUCATION

National University of Singapore (NUS)   2024 (expected)
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

PEER-REVIWED PUBLICATIONS

1. Fei Wei, **Ergute Bao**, Xiaokui Xiao, Yin Yang, and Bolin Ding.
   AAA: an Adaptive Mechanism for Locally Differential Private Mean Estimation.
   50th International Conference on Very Large Data Bases (VLDB), 2024.

2. **Ergute Bao**, Dawei Gao, Xiaokui Xiao, Yaliang Li.
   Communication Efficient and Differentially Private Logistic Regression under the Distributed Setting.
   29th ACM SIGKDD Conference on Knowledge Discovery and Data Mining (KDD), 2023.

3. Jianxin Wei, **Ergute Bao**, Xiaokui Xiao, Yin Yang.
   DPIS: an Enhanced Mechanism for Differentially Private SGD with Importance Sampling.
   29th ACM 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.
   48th International Conference on Very Large Data Bases (VLDB), 2022.

5. **Ergute Bao**, Yin Yang, Xiaokui Xiao, and Bolin Ding.
   CGM: An Enhanced Mechanism for Streaming Data Collection with Local Differential Privacy
   47th International Conference on Very Large Data Bases (VLDB), 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, Tianyu Pang, and Du Chao.
   Differentially Private Principal Component Analysis for Vertically Partitioned Data.

SERVICES

Reviewer for ICML 2022, DASFAA 2023 2024, TKDE.
Subreviewer or external reviewer for VLDB, SIGMOD, and ICDE.

INTERNSHIPS

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

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

Student Intern. Faculty of Engineering, CUHK   Summer 2017, Summer 2016
Project: Dimensionality Reduction algorithms for distributed systems.
Host: James Chung

HONORS

NUS School of Computing Dean's Graduate Research Excellence Award, 2023.
NUS School of Computing Research Achievement Award, 2021 & 2022.
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.
NUS Research Scholarship, 2018-2022.
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 *the Skellam Mechanism for Distributed Differential Privacy*, Privacy Innovation Lab, TikTok (2023).
Talk on *Protecting Data with Differential Privacy*, DAMO Academy, Alibaba (2022).