JIAYUAN YE

Home page: https://www.comp.nus.edu.sg/~jiayuan/ ◇ Email: jiayuan@comp.nus.edu.sg

EDUCATION

Ph.D. in Computer Science — National University of Singapore
Advisor: Reza Shokri
Research Interest: Data Protection and Privacy in Machine Learning
Thesis: Privacy Analysis of Machine Learning Algorithms — August 2020 - current

B.S. in Mathematical Sciences — University of Science and Technology of China
Division: Computational Mathematics — July 2016 - June 2020

AWARDS

Apple Scholars in AIML PhD fellowship — *2024-2026*
(Among 21 recipients in the 2024 cohort)
Google PhD Fellowship — *2023-2024*
(Among 4 recipients in the 2023 Privacy and Security Track)
NUS SoC Dean's Graduate Research Excellence Award — *Jan 2024*
(Among 11 recipients - senior PhD students who have made significant research achievements)
NeurIPS 2023 Scholar Award — *Oct 2023*
NUS SoC Research Achievement Award — *Aug 2022, 2023*
(Among ∼30 recipients - PhD students for continuous research achievement during their candidature)
Outstanding Student Scholarship in USTC — *Oct 2019*
Yuanqing Yang Education Fund Scholarship — *Sep 2018*
Meritous Winnner Prize (**10%**) in the Interdisciplinary Contest in Modeling — *Feb 2018*
China National Scholarship (**1%**) — *Sep 2017*

RESEARCH EXPERIENCES

Research Intern — Feb 2024 - June 2024
Worked with Kunal Talwar and Vitaly Feldman — *Apple MLR*

Research Intern — Jun 2023 - Aug 2023
Worked with Shruti Tople and Lukas Wutschitz — *Azure Research - MSR Cambridge*

PUBLICATIONS

Preprints

- Identifying Optimal Output Sets for Differential Privacy Auditing
  Jiayuan Ye, Yao Tong, Reza Shokri

Conference

- How much of my dataset did you use? Quantitative Data Usage Inference in Machine Learning
  In International Conference on Learning Representations (**ICLR**) 2025
  Yao Tong*, Jiayuan Ye*, Sajjad Zarifzadeh, Reza Shokri
  (Acccepted as **oral**, among less than 2% of submissions)
- Leave-one-out Distinguishability in Machine Learning [Paper]
  Jiayuan Ye, Anastasia Borovykh, Soufiane Hayou, Reza Shokri
  In International Conference on Learning Representations (**ICLR**) 2024
  Also Presented at the Symposium on Foundations of Responsible Computing (**FORC**) 2024

- Initialization Matters: Privacy-Utility Analysis of Overparameterized Neural Networks [Paper]
  Jiayuan Ye, Zhenyu Zhu, Fanghui Liu, Reza Shokri, Volkan Cevher
  In Advances in Neural Information Processing Systems (**NeurIPS**) 2023
  Also Presented at the Theory and Practice of Differential Privacy (**TPDP**) 2023

- Unified Enhancement of Privacy Bounds for Mixture Mechanisms via f-Differential Privacy [Paper]
  Chendi Wang*, Buxin Su*, Jiayuan Ye, Reza Shokri, Weijie J Su
  In Advances in Neural Information Processing Systems (**NeurIPS**) 2023

- Share Your Representation Only: Guaranteed Improvement of the Privacy-Utility Tradeoff in Federated Learning [Paper]
  Zebang Shen, Jiayuan Ye, Anmin Kang, Hamed Hassani, Reza Shokri
  In International Conference on Learning Representations (**ICLR**) 2023

- Differentially Private Learning Needs Hidden State (Or Much Faster Convergence) [Paper]
  Jiayuan Ye, Reza Shokri
  In Advances in Neural Information Processing Systems (**NeurIPS**) 2022
  Also Presented at the Symposium on Foundations of Responsible Computing (**FORC**) 2022

- Enhanced Membership Inference Attacks Against Machine Learning Models [Paper] [Code]
  Jiayuan Ye, Aadyaa Maddi, Sasi Kumar Murakonda, Vincent Bindschaedler, Reza Shokri
  In the ACM SIGSAC conference on computer and communications security (**CCS**) 2022

- Differential Privacy Dynamics of Langevin Diffusion and Noisy Gradient Descent [Paper]
  Rishav Chourasia*, Jiayuan Ye*, Reza Shokri
  In Advances in Neural Information Processing Systems (**NeurIPS**) 2021
  (Acccepted as **spotlight**, among less than 3% of submissions)

TOOL

Privacy Meter (https://github.com/privacytrustlab/ml_privacy_meter) is an open-source library to audit data privacy in statistical and machine learning algorithms via membership inference

- Worked on incorporating the various attack algorithms for membership inference in our paper (Ye et al. CCS 2022) to the privacy meter tool, as well as their efficiency testing.

TEACHING ASSISTANCE

CS5562: Trust-worthy Machine Learning *Fall 2021, 2022, 2023*
National University of Singapore Lecturer: Prof. Reza Shokri

PROFESSIONAL EXPERIENCES

- Journal Reviewer: JMLR (2022), SICOMP (2023)

- Conference & Workshop Program Commitee/Reviewer: NeurIPS 2022, 2023, 2024; ICLR 2023, 2024, 2025; ICML 2023, 2024, 2025; AISTATS 2023, 2025; ACM CCS 2024; IEEE SaTML 2025; AAAI 2024; PPAI-2022; FL-ICML 2023; PRIVATE ML @ ICLR 2024; SYNTHDATA @ ICLR 2025; DATA-FM @ ICLR 2025.

- Conference & Workshop Subreviewer: IEEE S&P 2020, 2021, 2022, 2023, 2024. ACM CCS 2021, 2022, 2023.