Xiaochen Zhu

https://xczhu.com/ • xczhu@mit.edu • xczhu@proton.me • he/him

Education

Massachusetts Institute of Technology, Cambridge, MA
PhD in Electrical Engineering and Computer Science, currently pursuing since September 2024
SM in Electrical Engineering and Computer Science, currently pursuing since September 2024
Research focus: data privacy and machine learning, advised by Prof Srinivas Devadas

National University of Singapore, Singapore
BComp with Honours (Highest Distinction) in Computer Science, June 2023
BSc with Honours (Highest Distinction) in Mathematics, June 2023
GPA: 4.78/5.0 for BComp in computer science, 4.79/5.0 for BSc in mathematics
Thesis: Graph Neural Networks with Local Differential Privacy (Outstanding Undergraduate Research Prize), advised by Prof Xiaokui Xiao and Prof Vincent Y. F. Tan
BComp focus areas: Algorithms and Theory, Artificial Intelligence

Research Interests

Computer security, data privacy and machine learning, in particular, differential privacy, federated learning, security and privacy of machine learning

Publications

Xiaochen Zhu, Xinjian Luo, Yuncheng Wu, Yangfan Jiang, Xiaokui Xiao, Beng Chin Ooi. Passive Inference Attacks on Split Learning via Adversarial Regularization. *Proceedings of the 32nd Annual Network and Distributed System Security Symposium (NDSS)*, to appear, San Diego, CA, Feburary 2025

Yangfan Jiang, Xinjian Luo, Yuncheng Wu, **Xiaochen Zhu**, Xiaokui Xiao, Beng Chin Ooi. On Data Distribution Leakage in Cross-Silo Federated Learning. *IEEE Transactions on Knowledge and Data Engineering (TKDE), 36*(7), 3312–3328, 2024

Xiaochen Zhu, Vincent Y. F. Tan and Xiaokui Xiao. Blink: Link Local Differential Privacy in Graph Neural Networks via Bayesian Estimation. *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2651–2664, Copenhagen, Denmark, November 2023 (AR=19.15%)

Xiaochen Zhu. Link Local Differential Privacy in GNNs via Bayesian Estimation. *Companion of the 2023 International Conference on Management of Data (SIGMOD)*, 265–267, Seattle, WA, June 2023
(First Place in SIGMOD Student Research Competition, Undergraduate Category)

Professional Experience

Research Assistant, Dept. of Computer Science / Institute of Data Science, NUS, Singapore
July 2023 – July 2024
Worked with Prof Vincent Y. F. Tan and Prof Xiaokui Xiao and performed research in differential privacy, federated learning and machine learning theory

Student Researcher, Department of Computer Science, NUS, Singapore
August 2021 – June 2023
Advised by Prof Xiaokui Xiao and worked on data privacy and federated learning

Software Engineering Intern, Privacy and Data Protection Office, TikTok, Singapore
May 2022 – August 2022
Worked on Records of Processing Activities generation, maintained a project for A/B testing and access control, and led a team of interns to develop a pandas-like data frame Go package

Research Intern, Institute of Mathematical Sciences, Sponsored by Google, Singapore
May 2021 – July 2021
Led a team of four undergraduate researchers, developed a privacy-preserving vertical federated learning protocol with homomorphic encryption, and demonstrated its financial applications

Teaching	Teaching Assistant, DSA3102, Convex Optimization, at NUS (Fall 2023)
	Teaching Assistant, CS3230, Design and Analysis of Algorithms, at NUS (Fall 2022, Spring 2022)
	Teaching Assistant, CS1231S, Discrete Structures, at NUS (Fall 2021, Spring 2021, Fall 2020)
	Grader, CS3243, Introduction to Artificial Intelligence, at NUS (Fall 2020)
	Teaching Assistant, CS2030(S), Programming Methodology II, at NUS (Spring 2021, Spring 2020)
Service	Member of the Artifact Evaluation Committee, USENIX Security 2025
	Reviewer, ICLR 2025
	Member of the Artifact Evaluation Committee, ACM CCS 2023 – 2024
	Reviewer, ACL ARR 2024
	Reviewer, IEEE TSC
Research Awards	Grand Final Candidate, ACM Student Research Competition, 2024
	First-Place, SIGMOD Student Research Competition (Undergraduate Category), 2023
	SIGMOD 2023 Travel Award, ACM SIGMOD, 2023
	Outstanding Undergraduate Researcher Prize, National University of Singapore, 2023
	Turing Program, NUS School of Computing, 2023
	Outstanding Computing Project Prize, NUS School of Computing, 2022
	Science and Technology Scholarship, Ministry of Education (Singapore) and NUS, 2018 (full funding for undergraduate studies at NUS)
Teaching Awards	Honor List of Student Tutors for Academic Year 2022–2023, NUS School of Computing, 2024