Haochen Sun

University of Waterloo, 200 University Avenue West, Waterloo, Ontario, N2L 3G1, Canada
haochen.sun@uwaterloo.ca | jvhs0706.github.io | github.com/jvhs0706 | Google Scholar

Education

University of Waterloo *PhD in Computer Science* | Waterloo, Canada — Sep 2022 – Present

- Supervisor: Prof. Xi He
- Research Focus: Security and privacy in machine learning and data management
- Honors and Awards: David R. Cheriton Graduate Scholarship

The Hong Kong University of Science and Technology (HKUST) *BSc in Data Science and Technology, and in Computer Science* | Hong Kong, China — Sep 2018 – Jul 2022

- GPA: 3.888/4.3 | Major GPA: 4.041/4.3
- Honors and Awards: Chern Class Scholarship (Department of Mathematics), Zhiyuan Scholarship (China Soong Ching Ling Foundation), HKUST Scholarship Scheme for Continuing Undergraduates, Dean's List

Research Experience

Faithfulness of Differential Privacy Mechanism Execution *PhD Research Project (with Prof. Xi He)* | University of Waterloo — May 2024 – Present

- Investigating vulnerabilities from unfaithful execution of differential privacy mechanisms, focusing on additional privacy leakage incurred, and defenses to ensure execution integrity.

Zero-Knowledge Deep Learning *with Prof. Hongyang Zhang* | University of Waterloo — Sep 2022 – Apr 2024

- Specialized zero-knowledge proof (ZKP) protocols for deep learning with CUDA implementations.
- The first working ZKP scheme for 13B-parameter LLMs and for training 10M-parameter neural networks.

Air Pollution Forecasting with Deep Learning *Undergraduate Research and RA (with Profs. Jimmy Fung and Xingcheng Lu)* | HKUST — Jan 2020 – Nov 2022

- Designed deep learning architectures for modeling the spatio-temporal distribution of air pollutants.
- Improved regional air pollution forecasting accuracy by 30%.

Publications

1. Haochen Sun and Xi He. "GPM: The Gaussian Pancake Mechanism for Planting Undetectable Backdoors in Differential Privacy." *Preprint*, 2025.
2. Haochen Sun and Xi He. "VDDP: Verifiable Distributed Differential Privacy under the Client–Server–Verifier Setup." *Preprint*, 2025.
3. Haochen Sun*, Shufan Zhang*, Karl Knopf*, Shubhankar Mohapatra, Wei Pang, Calvin Wang, Yingke Wang, Masoumeh Shafieinejad, David Emerson, and Xi He. "FedDPSyn: Federated Tabular Data Synthesis with Computational Differential Privacy." *Theory and Practice of Differential Privacy (TPDP)*, 2025.
4. Haochen Sun, Jason Li, and Hongyang Zhang. "zkLLM: Zero-Knowledge Proofs for Large Language Models." *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2024.
5. Haochen Sun, Tonghe Bai, Jason Li, and Hongyang Zhang. "zkDL: Efficient Zero-Knowledge Proofs of Deep Learning Training." *IEEE Transactions on Information Forensics and Security (TIFS)*, 2024.
6. Haochen Sun, Jimmy C. H. Fung, Yiang Chen, Zhenning Li, Dehao Yuan, Wanying Chen, and Xingcheng Lu. "Development of an LSTM broadcasting deep-learning framework for regional air pollution forecast improvement." *Geoscientific Model Development (GMD)*, 2022.
7. Haochen Sun, Jimmy C. H. Fung, Yiang Chen, Wanying Chen, Zhenning Li, Yeqi Huang, Changqing Lin, Mingyun Hu, and Xingcheng Lu. "Improvement of $PM_{2.5}$ and O_3 forecasting by integration of 3D numerical simulation with deep learning techniques." *Sustainable Cities and Society (SCS)*, 2021.

Academic Services

(Sub)Reviewer

- Conferences: CCS, SIGMOD, VLDB, NeurIPS, SaTML, AISTATS
- Journals: TDSC, TMLR

Teaching Assistant, University of Waterloo

- Head TA for CS 480/680: Introduction to Machine Learning (Spring 2023, Winter 2024)
- CS 116, CS 135, CS 246, CS 330