Haochen Sun

University of Waterloo, 200 University Avenue West, Waterloo, Ontario, N2L 3G1, Canada
haochen.sun@uwaterloo.ca | July 6th, 2000 | jvhs0706.github.io | github.com/jvhs0706 | **Haochen Sun**

Education

University of Waterloo, *PhD in Computer Science* | Waterloo, Canada — Sept 2022 - Present

- Supervisor: Prof. Xi He.
- Research focus: Security and privacy in machine learning and data management.

The Hong Kong University of Science and Technology (HKUST), *BSc in Data Science and Technology, and in Computer Science* | Hong Kong, China — Sept 2018 - July 2022

- GPA: 3.888/4.3, Major GPA: 4.041/4.3.
- Awards: Chern Class Scholarship (Department of Mathematics), Zhiyuan Scholarship (China Soong Ching Ling Foundation), University's Scholarship Scheme for Continuing Undergraduate Students, Dean's List.
- Link to the diploma and the official transcript.

Research Experience

Zero-knowledge Deep Learning, *with Prof. Hongyang Zhang* | Univeristy of Waterloo — Sept 2022 - April 2024

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

Adversarial Example Tracing, *Independent Study (with Prof. Minhao Cheng)* | HKUST — Jan 2022 - Jul 2022

- Zero-shot tracing the origin of adversarial examples via watermarking.

Air Pollution Forecast with Deep Learning, *Undergraduate Research and Research Assistantship (with Profs. Jimmy Fung and Xingcheng Lu)* | HKUST — Jan 2020 - Nov 2022

- Specialized deep-learning architecture for modelling the spatial-temporal distribution of air pollutants.
- Improving the accuracy of regional air-pollution forecast by 30%.

Papers

1. Haochen Sun, Jason Li, and Hongyang Zhang. "zkLLM: Zero Knowledge Proofs for Large Language Models." *ACM Conference on Computer and Communications Security (CCS)*, 2024.
2. Haochen Sun, Tonghe Bai, Jason Li, and Hongyang Zhang. "zkDL: Efficient Zero-Knowledge Proofs of Deep Learning Training." *Under Review at IEEE Transactions on Information Forensics and Security (TIFS)*, 2023.
3. Minhao Cheng, Rui Min, Haochen Sun, Pin-Yu Chen. "Identification of the Adversary from a Single Adversarial Example." *International Conference on Machine Learning (ICML)*, 2023.
4. 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.
5. Haochen Sun, Jimmy C.H. Fung, Yiang Chen, Wanying Chen, Zhenning Li, Yeqi Huang, Changqing Lin, Mingyun Hu, 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

Conference Reviewer

- Reviewer for NeurIPS 2023, AISTATS 2024.
- Subreviewer for SaTML 2023, ALT 2023, ACM CCS 2023.

Teaching Assistantship, University of Waterloo

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