Haochen Sun

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

Education

- **University of Waterloo** Sep 2022 – Present
  PhD in Computer Science *Waterloo, Canada*
  - Supervisor: Prof. Xi He
  - Research interests: data privacy and machine learning security.
  - Honors and awards: **SIGMOD 2026 Best Paper Award**; David R. Cheriton Graduate Scholarship.
- **The Hong Kong University of Science and Technology (HKUST)** Sep 2018 – Jul 2022
  BSc in Data Science and Technology, and in Computer Science *Hong Kong, China*
  - 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, and Dean's List.

Research Experience

- **Faithfulness of Differential Privacy Mechanism Execution** May 2024 – Present
  PhD Research Project (with Prof. Xi He) *University of Waterloo*
  - Discovered an undetectable backdoor attack against DP mechanisms that can arbitrarily compromise the privacy guarantee.
  - Developed defenses against such malicious deviations in a distributed DP setting.
  - Awarded the **SIGMOD 2026 Best Paper Award**.
- **Zero-Knowledge Deep Learning** Sep 2022 – Apr 2024
  University of Waterloo
  - Developed specialized zero-knowledge proof (ZKP) protocols for deep learning, implemented with CUDA.
  - The first working ZKP scheme for 13B-parameter LLMs and for training 10M-parameter neural networks.
- **Air Pollution Forecasting with Deep Learning** Jan 2020 – Nov 2022
  Undergraduate Research and RA (with Profs. Jimmy Fung and Xingcheng Lu) *HKUST*
  - Designed deep learning architectures to model the spatiotemporal distribution of air pollutants.
  - Improved regional air pollution forecasting accuracy by 30%.

Publications

Only (co-)first-author publications are listed below.

1. **(SIGMOD 2026 Best Paper Award)** Haochen Sun and Xi He. "GPM: The Gaussian Pancake Mechanism for Planting Undetectable Backdoors in Differential Privacy." *Proceedings of the ACM on Management of Data (PACMMOD)*, 2026.
2. Haochen Sun and Xi He. "VDDP: Verifiable Distributed Differential Privacy under the Client–Server–Verifier Setup." *Theory and Practice of Differential Privacy (TPDP)*, 2026.
3. Shufan Zhang[*], Haochen Sun[*], 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." *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, TKDE.
- **Teaching Assistant, University of Waterloo:** Courses: CS 116, CS 135, CS 246, CS 330, CS 480.