Fei Wang

Current Position

Recent Ph.D. Graduate
Edward S. Rogers Sr. Department of Electrical and Computer Engineering
University of Toronto
10 King's College Road
Toronto, Ontario M5S 3G4, Canada

☎ +1 (437) 988-5917
✉ silviafey.wang@utoronto.ca
🏠 silviafeiwang.github.io
linkedin.com/feiwang
github.com/silviafeiwang
🎓 Google Scholar Citations

Research Interests

Privacy-preserving distributed machine learning, especially federated learning, foundation model adaptation, and reinforcement learning for network optimization and robotic control, advancing toward trustworthy AI systems, privacy-aware agentic AI, and embodied AI.

Education

University of Toronto, Toronto, Ontario, Canada
Edward S. Rogers Sr. Department of Electrical and Computer Engineering

- ◇ **Ph.D.**, Computer Engineering, January 2026
  - ▷ *Advisor:* Baochun Li
  - ▷ *Cumulative GPA:* 3.88/4.00

Wuhan University, Wuhan, Hubei, P. R. China
Hongyi Honor College

- ◇ **B.Engr.** (with honors), Computer Science and Technology, June 2020
  - ▷ *Thesis Advisor:* Yanjiao Chen
  - ▷ *Cumulative GPA:* 3.80/4.00
  - ▷ *Rank:* 4/34 (selected from 587 students in the School of Computer Science, Wuhan University)

Honours and Awards

- ◇ *Mary H. Beatty Fellowship*, University of Toronto, September 2024–April 2025.
- ◇ *School of Graduate Studies Conference Grant*, University of Toronto, May 2024.
- ◇ *Best Paper Award for IEEE INFOCOM 2023*, for the paper co-authored with Ethan Hugh and Baochun Li, titled "More than Enough is Too Much: Adaptive Defenses against Gradient Leakage in Production Federated Learning," May 2023.
- ◇ *IEEE INFOCOM 2023 Student Travel Grant*, sponsored by the IEEE Communications Society (ComSoc) and US National Science Foundation (NSF), May 2023.
- ◇ *Farid and Diana Najm Graduate Fellowship*, competitive faculty-nominated award for academic excellence, Department of Electrical and Computer Engineering, University of Toronto, March 2023.
- ◇ *IEEE ICNP 2022 Travel Grant*, September 2022.
- ◇ *The Edward S. Rogers Sr. Graduate Scholarships*, Department of Electrical and Computer Engineering, University of Toronto, 2020–2025.

◇ *Distinguished Graduate Award*, Wuhan University, June 2020.

◇ *Overseas Exchange Scholarships*, Wuhan University, 2018–2020.

◇ *Outstanding Student Leader Award*, recognition for exceptional leadership and service contributions to the student union, Wuhan University, December 2018.

◇ *Academic Excellence Scholarships*, Wuhan University, 2016–2019.

Publications

◇ Refereed Journal Articles

[J4] **Fei Wang**, Baochun Li. "Data Reconstruction and Protection in Federated Learning for Fine-Tuning Large Language Models," in *IEEE Transactions on Big Data*, Special Section on Pre-Trained Large Language Models, December 2024.

[J3] **Fei Wang**, Ethan Hugh, Baochun Li. "More than Enough is Too Much: Adaptive Defenses against Gradient Leakage in Production Federated Learning," in *IEEE/ACM Transactions on Networking*, vol. 32, no. 4, pp. 3061-3075, March 2024.

[J2] **Fei Wang**, Baochun Li. "Harnessing the Power of Local Supervision in Federated Learning," in *IEEE Transactions on Big Data*, Special Issue on Federated Learning for Big Data Applications, vol. 11, no. 5, pp. 2162-2173, May 2024.

[J1] Salma Emara, **Fei Wang**, Baochun Li, Timothy Zeyl. "Pareto: Fair Congestion Control with Online Reinforcement Learning," in *IEEE Transactions on Network Science and Engineering*, vol. 9, no. 5, pp. 3731-3748, September–October 2022.

◇ Refereed Magazine Articles

[M2] **Fei Wang**, Baochun Li, and Bo Li. "Federated Unlearning and Its Privacy Threats," in *IEEE Network*, vol. 38, no. 2, pp. 294-300, June 2023.

[M1] **Fei Wang**, Baochun Li, and Bo Li. "Quality-Oriented Federated Learning on the Fly," in *IEEE Network*, Special Issue on Federated Optimizations and Networked Edge Intelligence, vol. 36, no. 5, pp. 152-159, September–October 2022.

◇ Refereed Conference Papers

[C6] **Fei Wang**, Yan Zhu, Baochun Li. "Unraveling Elevated Data Leakage in Split Learning for Fine-Tuning Stable Diffusion Models," in the Proceedings of *the 20th ACM ASIA Conference on Computer and Communications Security (ACM ASIACCS 2025)*, Hanoi, Vietnam, August 25–29, 2025 (acceptance ratio: 15%). ASIACCS'25

[C5] Salma Emara, Daniel Liu, **Fei Wang**, Baochun Li, "Cascade: Enhancing Reinforcement Learning with Curriculum Federated Learning and Interference Avoidance — A Case Study in Adaptive Bitrate Selection," in the Proceedings of *IEEE INFOCOM 2024 Workshop on Distributed Machine Learning and Fog Networks (FOGML)*, Vancouver, Canada, May 20–23, 2024. INFOCOM'24

[C4] Baochun Li, Ningxin Su, Chen Ying, **Fei Wang**. “Plato: An Open-Source Research Framework for Production Federated Learning,” in the Proceedings of *ACM Turing Award Celebration Conference (TURC)*, Wuhan, China, July 29–30, 2023. TURC’23

[C3] **Fei Wang**, Salma Emara, Isidor Kaplan, Baochun Li, Timothy Zeyl. “Multi-Agent Deep Reinforcement Learning for Cooperative Edge Caching via Hybrid Communication,” in the Proceedings of *IEEE International Conference on Communications (ICC 2023)*, Selected Areas in Communications — Machine Learning for Communications and Networking Track, Rome, Italy, May 28–June 1, 2023. ICC’23

[C2] **Fei Wang**, Ethan Hugh, Baochun Li. “More than Enough is Too Much: Adaptive Defenses against Gradient Leakage in Production Federated Learning,” in the Proceedings of *IEEE INFOCOM 2023*, New York Area, U.S.A., May 17–20, 2023 (acceptance ratio: 19%, **Best Paper Award**). INFOCOM’23

[C1] Salma Emara, **Fei Wang**, Isidor Kaplan, and Baochun Li. “Ivory: Learning Network Adaptive Streaming Codes,” in the Proceedings of *the 29th IEEE/ACM International Symposium on Quality of Service (IWQoS 2022)*, Online, June 10–12, 2022 (acceptance ratio: 24%). IWQoS’22

◇ Preprints / Papers Under Review

[P4] Salma Emara, Baochun Li, Timothy Zeyl, Daniel Liu, **Fei Wang**. “Lethe: Interference-Based Forgetting for Continual Reinforcement Learning in Robotic Agents,” 2025.

[P3] **Fei Wang**, Baochun Li, Bo Li. “Expert Pathway Recovery through Structural Memorization in Fine-Tuned Mixture-of-Experts Large Language Models,” 2025.

[P2] **Fei Wang**, Baochun Li. “Leaner Training, Lower Leakage: Revisiting Memorization in LLM Fine-Tuning with LoRA,” 2025.

[P1] **Fei Wang**, Baochun Li. “Hear No Evil: Detecting Gradient Leakage by Malicious Servers in Federated Learning,” 2025.

Professional Experience

The Hong Kong University of Science and Technology, Hong Kong, P. R. China
Department of Computer Science and Engineering

◇ *Research Assistant* July–August 2024

▷ Co-supervised by Professor Wei Wang and Professor Baochun Li.

▷ Investigated memorization and training data extraction risks in parameter-efficient fine-tuning of large language models.

City University of Hong Kong, Hong Kong, P. R. China
Department of Computer Science

◇ *Research Assistant* June–August 2023

- ▷ Co-supervised by Professor Cong Wang and Professor Baochun Li.
- ▷ Investigated data reconstruction attacks in fine-tuned large language models, revealing privacy risks in parameter-efficient adaptation.

The Hong Kong University of Science and Technology, Hong Kong, P. R. China
Department of Computer Science and Engineering

◇ *Research Assistant* May–August 2021

- ▷ Co-supervised by Professor Bo Li and Professor Baochun Li.
- ▷ Conducted research on reinforcement learning-based adaptive aggregation mechanisms for federated learning in heterogeneous environments, optimizing convergence efficiency.

University of Toronto, Toronto, Ontario, Canada
Edward S. Rogers Sr. Department of Electrical and Computer Engineering

◇ *Teaching Assistant*, ECE1724 – Advanced Web Development: React Ecosystem and Modern Frameworks Winter 2026

- ▷ Developed autograders for assignments and evaluated course projects across multiple milestones.
- ▷ Provided responsive support on course discussion platforms and conducted in-person evaluation of project presentations.

◇ *Teaching Assistant*, APS105 – Computer Fundamentals Winter 2022/23/24/25/26

- ▷ Delivered weekly in-person tutorials on C programming fundamentals to 50+ undergraduate engineering students.
- ▷ Conducted weekly lab sessions for 20+ students, guiding them through practical implementation and debugging in VSCode and Git workflows.
- ▷ Handled student Q&A on Piazza with detailed explanations and graded programming assignments, midterms, and finals.

◇ *Teaching Assistant*, ECE1724 – Performant Software Systems with Rust Fall 2024/25

- ▷ Developed automated grading framework for bi-weekly assignments, reducing manual grading while maintaining consistency for 120+ students.
- ▷ Evaluated group course projects from proposal to final report and presentation, providing detailed feedback and recommendations.

◇ *Teaching Assistant*, ECE1771 – Quality of Service Fall 2023

- ▷ Graded bi-weekly assignments, final papers, and exams for 100+ students.

◇ *Software Development Assistant*, ECE Department Project March–April 2022

- ▷ Developed a research database web application built with Node.js and PostgreSQL.

◇ *Undergraduate Research Assistant* September 2019–August 2020

- ▷ Supervised by Professor Baochun Li and mentored by Dr. Salma Emara (now Assistant Professor, Teaching Stream, Department of Electrical and Computer Engineering, University of Toronto, Canada).
- ▷ Developed reinforcement learning solutions for network optimization, including congestion control, edge caching, and adaptive error control.

Wuhan University, Wuhan, Hubei, People's Republic of China
Department of Computer Science

◇ *Undergraduate Research Assistant* December 2018–August 2019

- ▷ Supervised by Professor Yanjiao Chen (now Bairen Researcher and Doctoral Supervisor, College of Electrical Engineering, Zhejiang University, P. R. China).
- ▷ Developed a reinforcement learning-based congestion control algorithm for wireless networks, including algorithm design, implementation, and empirical evaluation.

Scholarly Activities

- ◇ *"Is Federated Learning Ready for Real-World Deployment?,"* Invited Talk, Distinguished Lecture Series, Department of Computing, Hong Kong Polytechnic University, Hong Kong, P. R. China, July 7, 2023.

Professional Service Activities

- ◇ **Student Volunteer**
  - ▷ 43rd IEEE International Conference on Distributed Computing Systems (ICDCS), Hong Kong, P. R. China, July 18–21, 2023.
- ◇ **Journal Reviewer**
  - ▷ IEEE Transactions on Dependable and Secure Computing (TDSC), Information Forensics and Security (TIFS), Network Science and Engineering (TNSE), Mobile Computing (TMC), Cloud Computing (TCC), ACM Transactions on Sensor Networks (TOSN).

Professional Society Memberships

- ◇ *Graduate Student Member*, the Institute of Electrical and Electronic Engineers (IEEE)
- ◇ *Student Member*, the Association for Computing Machinery (ACM)

Undergraduate Mentoring

- ◇ **Engineering Science Thesis Projects (ESC499)**

Name	*Graduation Date*	*Thesis Title*
Yi Lin Luo	June 2025	Evaluating the Effectiveness of Data Extraction Attacks in Fine-Tuned Large Language Models
Tom Nguyen	June 2025	Privacy Risks of Large Language Models from Training Data Memorization
Arjun Sharma	June 2024	Investigating Techniques of Data Reconstruction From Language Model Gradients: Methods & Vulnerabilities
David Chu	June 2023	Preventing Privacy Leakage against Malicious Server Gradient Magnification in Federated Learning

- ◇ **Undergraduate Research Interns**

Name	*Starting and Ending Date*	*Research Topic*
Eric Kim	May–October 2025	Privacy Risks of Fine-Tuning Mixture-of-Experts Large Language Models

Yan Zhu	May–August 2024	Fine-Tuning Data Reconstruction in Privacy Backdoored LLMs
Yan Zhu	May–August 2023	Data Leakage in Split Learning for Fine-Tuning Stable Diffusions
Ethan Hugh	May–August 2022	Defending against Gradient Leakage in Federated Learning
Isidor Kaplan	May–August 2020	Multi-Agent Reinforcement Learning for Edge Caching