# Sijia Liu

Assistant Professor
Department of Computer Science & Engineering
Michigan State University, East Lansing, MI
Affiliated Professor
MIT-IBM Watson AI Lab, IBM Research

Email: liusiji5@msu.edu
Tel: (315)-744-6778 (Mobile)
[Personal Website]
[OPTML Lab Website]
[Google Scholar]

## PRIMARY RESEARCH AREAS

**Trustworthy ML:** Adversarial ML, model explanation, fairness, security & privacy

**Scalable ML:** Zeroth-order optimization, deep model compression, distributed ML, automated ML

## EDUCATION

**Ph.D.**, Electrical and Computer Engineering, Syracuse University — Mar. 2016
**All University Doctoral Prize**; Advisors: Pramod Varshney and Makan Fardad

**M. A. Sc.**, Electrical Engineering, Xi'an Jiaotong University — May 2011

**B.S.**, Electrical Engineering, Xi'an Jiaotong University — May 2008

## PROFESSIONAL EXPERIENCE

**Assistant Professor**, CSE, Michigan State University — Jan. 2021 – present

**Affiliated Professor**, MIT-IBM Watson AI Lab, IBM Research — Oct. 2021 – present

**Research Staff Member**, MIT-IBM Watson AI Lab, IBM Research — Jan. 2018 – Dec. 2020

**Postdoc Research Fellow**, University of Michigan, Ann Arbor — July 2016 – Dec. 2017
Supervisors: Alfred Hero (EECS) and Indika Rajapakse (Computational Medicine & Bioinformatics)

## HONORS AND RECOGNITION

**National Science Foundation (NSF) CAREER Award**, 2024
*— For the project titled "Zeroth-Order Machine Learning: Foundations and Emerging AI Applications"*

**Top 3% Paper Recognition** at the 48th IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP), 2023 *— For the paper titled "Visual Prompting for Adversarial Robustness"*

**AAAI'23 New Faculty Highlights** on "*General and Scalable Optimization for Robust AI*", 2023

**Best Paper Runner-Up Award** at 38th Conference on Uncertainty in Artificial Intelligence (UAI), 2022
*— For the paper titled "Distributed Adversarial Training to Robustify Deep Neural Networks at Scale"*

**IBM Pat Goldberg Best Paper Award Finalist**, 2020
*— For the AAAI'20 paper titled "An ADMM Based Framework for AutoML Pipeline Configuration", the key enabling technique in the IBM Watson Studio Automated ML System*

**Three IBM Outstanding Research Accomplishments**, 2019
*— Trustworthy AI; Toward Automating the AI Lifecycle with AutoAI; Deep Learning on Graphs*

**Best Student Paper Award** at 42nd ICASSP, 2017
*— For the paper titled "Ultra-fast Robust Compressive Sensing Based on Memristor Crossbars"*

**Best Student Paper Award Finalist** at Asilomar Conference on Signals, Systems, and Computers, CA, 2013
*— For the paper titled "Adaptive Non-myopic Quantizer Design for Target Tracking in Wireless Sensor Networks"*

**Winner of Best Poster Award** at Nunan Poster Competition, Syracuse University, 2012

**First Class Award in National Mathematics Olympiad**, 2004

## SELECTED PUBLICATIONS

Full list of publications can be found at **Google Scholar** (8509 citations as of July 16, 2024). **CSRanking** score: **72**
∗ denotes equal contribution; † denotes student authors **under my supervision**.

**Five Representative Publications in *Trustworthy ML*:**

P5. Y. Zhang$^{\dagger,*}$, J. Jia$^{\dagger,*}$, X. Chen, A. Chen$^{\dagger}$, Y. Zhang$^{\dagger}$, J. Liu$^{\dagger}$, K. Ding, **S. Liu**, “ To Generate or Not? Safety-Driven Unlearned Diffusion Models Are Still Easy To Generate Unsafe Images ... For Now.” *European Conference on Computer Vision (ECCV)*, 2024

P4. C. Fan$^{\dagger,*}$, J. Liu$^{\dagger,*}$, Y. Zhang$^{\dagger}$, E. Wong, D. Wei, **S. Liu**, “SalUn: Empowering Machine Unlearning via Gradient-based Weight Saliency in Both Image Classification and Generation.” *International Conference on Learning Representations (ICLR)*, 2024 (**Spotlight**)

P3. J. Jia$^{\dagger,*}$, J. Liu$^{\dagger,*}$, P. Ram, Y. Yao$^{\dagger}$, G. Liu, Y. Liu, P. Sharma, **S. Liu**, “Model Sparsity Can Simplify Machine Unlearning.” *Advances in Neural Information Processing Systems (NeurIPS)*, 2023, pp.51584-51605 (**Spotlight**)

P2. Y. Zhang$^{\dagger,*}$, G. Zhang$^{\dagger,*}$, P. Khanduri, M. Hong, S. Chang, **S. Liu**, “Revisiting and advancing fast adversarial training through the lens of bi-level optimization.” *International Conference on Machine Learning (ICML)*, 2022, pp.26693-26712

P1. Y. Zhang$^{\dagger}$, Y. Yao$^{\dagger}$, J. Jia$^{\dagger}$, J. Yi, M. Hong, S. Chang, **S. Liu**, “How to Robustify Black-Box ML Models? A Zeroth-Order Optimization Perspective.” *International Conference on Learning Representations (ICLR)*, 2022 (**Spotlight**)

**Five Representative Publications in *Scalable ML*:**

P5. Y. Zhang$^{\dagger}$, P. Khanduri, I. Tsaknakis, Y. Yao$^{\dagger}$, M. Hong, **S. Liu**, “An Introduction to Bi-level Optimization: Foundations and Applications in Signal Processing and Machine Learning.” *IEEE Signal Processing Magazine*, 2024, pp.38-59 (**Feature Article**)

P4. Y. Zhang$^{\dagger,*}$, Y. Zhang$^{\dagger,*}$, Aochuan Chen$^{\dagger,*}$, J. Jia$^{\dagger}$, J. Liu$^{\dagger}$, G. Liu, M. Hong, S. Chang, **S. Liu**, “Selectivity Drives Productivity: Efficient Dataset Pruning for Enhanced Transfer Learning.” *Advances in Neural Information Processing Systems (NeurIPS)*, 2023, pp.36913-36937

P3. Y. Zhang$^{*,\dagger}$, Y. Yao$^{*,\dagger}$, P. Ram, P. Zhao, T. Chen, M. Hong, Y. Wang, **S. Liu**, Advancing Model Pruning via Bi-level Optimization, *Advances in Neural Information Processing Systems (NeurIPS)*, 2022, pp.18309-18326

P2. G. Zhang$^{\dagger,*}$, S. Lu$^{*}$, Y. Zhang$^{\dagger}$, X. Chen, P.-Y. Chen, Q. Fan, L. Martie, L. Horesh, M. Hong, **S. Liu**, “Distributed Adversarial Training to Robustify Deep Neural Networks at Scale.” *Conference on Uncertainty in Artificial Intelligence (UAI)*, 2022, pp.2353-2363 (**the Best Paper Runner-Up Award**)

P1. **S. Liu**$^{*}$, S. Lu$^{*}$, X. Chen$^{*}$, Y. Feng, K. Xu, A. Al-Dujaili, M. Hong, U.-M. O’Reilly, “Min-Max Optimization without Gradients: Convergence and Applications to Adversarial ML.” *International Conference on Machine Learning (ICML)*, 2020, pp.6282-6293

## SELECTED TALKS/PRESENTATIONS

T1. “Machine Unlearning in Computer Vision: Foundations and Applications.” *CVPR’24 Tutorial*, 06/2024

T2. “Zeroth-Order Machine Learning: Fundamental Principles and Emerging Applications in Foundation Models.” *AAAI’24 Tutorial*, 02/2024

T3. “DeepZero: Scaling Up Zeroth-Order Optimization for Deep Model Training.” *Invited Talk in Special Session on Sustainable AI Training at the Large and Tiny Scales, ICCAD’23*, 10/2023

T4. “Empowering Machine Unlearning through Model Sparsity.” *Invited Talk at TrustML Workshop@UBC*, 06/2023

T5. “Reverse Engineering of Deceptions: Foundations and Applications”, *CVPR’23 Tutorial*, 06/2023

T6. “Bi-level Optimization in Machine Learning: Foundations and Applications.” *AAAI’23 Tutorial*, 02/2023

T7. “Foundational Robustness of Foundation Models”, *NeurIPS’22 Tutorial*, 12/2022