Sijia Liu

Assistant Professor
Department of Computer Science & Engineering
Michigan State University, East Lansing, MI
[Personal Website] [OPTML Lab] [Google Scholar]

Emails: lsjxjtu@gmail.com
liusiji5@msu.edu
Tel: (315)-744-6778 (Mobile)

PRIMARY RESEARCH AREAS

Trustworthy ML: Adversarial attack & defense, model explanation, verification, fairness

Scalable ML: Black-box optimization, distributed learning, model compression, automated ML

EDUCATION

Ph.D., Electrical and Computer Engineering, Syracuse University Mar. 2016
All University Doctoral Prize; Advisor: Pramod Varshney

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

Best Paper Runner-Up Award at the 38th Conference on Uncertainty in Artificial Intelligence (UAI), 2022

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

Winner of Best Student Paper Award (3rd place), the 42nd IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2017

Best Student Paper Nominee (among the seven finalists) at Asilomar Conference on Signals, Systems, and Computers, CA, Pacific Grove, CA, 2013

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

First Class Award in National Mathematics Olympiad, 2004
— Exempted from National College Entrance Examination in China

TEACHING

1. SS'21, SS'22, FS'22, *CSE 891: Adversarial Machine learning*, Michigan State University

SELECTED PUBLICATIONS

Full list of publications can be found at **Google Scholar**.

$*$ denotes equal contribution; † denotes authors under my supervision/mentorship.

Survey Paper:

1. **S. Liu**, P.-Y. Chen, B. Kailkhura, G. Zhang, A. O. Hero III, , P. K. Varshney, "A Primer on Zeroth-Order Optimization in Signal Processing and Machine Learning", **IEEE Signal Processing Magazine**, 37(5), 43-54.

Conference Papers:

1. G. Zhang*, S. Lu*, Y. Zhang†, 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", **UAI'22 (Oral, the Best Paper Runner-Up Award)**
2. Y. Zhang†,*, G. Zhang*, P. Khanduri, M. Hong, S. Chang, **S. Liu**, "Revisiting and advancing fast adversarial training through the lens of bi-level optimization", **ICML'22**
3. T. Chen, Z. Zhang, **S. Liu**, Y. Zhang, S. Chang, Z. Wang, "Data-Efficient Double-Win Lottery Tickets from Robust Pre-training", **ICML'22**
4. T. Chen*, Z. Zhang*, Y. Zhang†,*, S. Chang, **S. Liu**, Z. Wang, "Quarantine: Sparsity Can Uncover the Trojan Attack Trigger for Free", **CVPR'22**
5. Y. Gong†,*, Y. Yao†,*, Y. Li, Y. Zhang, X. Liu, X. Lin, **S. Liu**, "Reverse Engineering of Imperceptible Adversarial Image Perturbations", **ICLR'22**
6. Y. Zhang†, Y. Yao†, J. Jia†, J. Yi, M. Hong, S. Chang, **S. Liu**, "How to Robustify Black-Box ML Models? A Zeroth-Order Optimization Perspective", **ICLR'22**
7. L. Fan†, **S. Liu**, P.-Y. Chen, G. Zhang, C. Gan, "When does Contrastive Learning Preserve Adversarial Robustness from Pretraining to Finetuning?", **NeurIPS'21**
8. J. Wang†,*, T. Zhang†,*, **S. Liu**, P.-Y. Chen, J. Xu, M. Fardad, B. Li, "Adversarial Attack Generation Empowered by Min-Max Optimization", **NeurIPS'21**
9. R. Wang†, K. Xu†, **S. Liu**, P.-Y. Chen, T.-W. Weng, C. Gan, M. Wang,"On Fast Adversarial Robustness Adaptation in Model-Agnostic Meta-Learning", **ICLR'21**
10. S. Srikant†, **S. Liu**, T. Mitrovska, S. Chang, Q. Fan, G. Zhang, U.-M. O'Reilly, "Generating Adversarial Computer Programs using Optimized Obfuscations", **ICLR'21** (MIT News)
11. K. Xu†, G. Zhang†, **S. Liu**, Q. Fan, M. Sun, H. Chen, P.-Y. Chen, Y. Wang, X. Lin, "Adversarial T-shirt! Evading Person Detectors in A Physical World", **ECCV'20 (spotlight)** [demo, **over 200 media coverage on the web**]
12. R. Wang†, G. Zhang†, **S. Liu**, P.-Y. Chen, J. Xiong, M. Wang, "Practical Detection of Trojan Neural Networks: Data-Limited and Data-Free Cases", **ECCV'20**
13. A. Boopathy†, **S. Liu**, G. Zhang, C. Liu, P.-Y. Chen, S. Chang, L. Daniel, "Proper Network Interpretability Helps Adversarial Robustness in Classification", **ICML'20**
14. **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", **ICML'20**
15. **S. Liu***, P. Ram*, D. Vijaykeerthy, D. Bouneffouf, G. Bramble, H. Samulowitz, D. Wang, A. Conn, A. Gray, "An ADMM Based Framework for AutoML Pipeline Configuration", **AAAI'20**
16. **S. Liu**, P.-Y. Chen, X. Chen, M. Hong, "signSGD via Zeroth-Order Oracle", **ICLR'19**