

Computer Science and Engineering Department  
Michigan State University  
East Lansing, MI 48824, USA

Mobile: (+1)-517-402-8258  
Email: yaoyugua@msu.edu  
Website: <https://cse.msu.edu/~yaoyugua>

---

## RESEARCH FOCUS

---

**Deep Learning:** Prompt Learning, Model Compression, Adversarial Machine Learning.

**Optimization:** Zeroth-order Optimization, Bi-level Optimization.

---

## EDUCATION

---

**Ph.D. student** in CSE, Michigan State University (MSU)    Advisor: [Sijia Liu](#)    Jan. 2021 – now  
**Ph.D. student** in CSE, Tsinghua University/MSU    Advisor: [Yunhao Liu](#)    Aug. 2018 – Dec. 2020  
**B.S.** in Automation, Tsinghua University    Advisor: Hong Wang    Aug. 2014 – July. 2018  
**Exchange** in CSE, École Polytechnique Fédérale de Lausanne    Aug. 2016 – Feb. 2017

---

## WORK

---

**Research Intern** in Cisco Research    Feb. 2023 – now  
**Research Intern** in MIT-IBM Watson AI Lab    May. 2021 – Aug. 2021  
**Research Intern** in DiDi AI Lab    Nov. 2017 – Feb. 2018  
**Research Intern** in Hong Kong Univ. of Science and Technology    June. 2017 – Sep. 2017

---

## SELECTED PUBLICATION

---

- [1] **Y. Yao\***, J. Liu\*, Y. Gong\*, X. Liu, Y. Wang, X. Lin, S. Liu, [Can Adversarial Examples Be Parsed to Reveal Victim Model Information?](#), *preprint*.
- [2] A. Chen, **Y. Yao**, P. Chen, Y. Zhang, S. Liu, [Understanding and Improving Visual Prompting: A Label-Mapping Perspective](#), *CVPR'23*.
- [3] **Y. Yao\***, Y. Zhang\*, P. Ram, P. Zhao, T. Chen, M. Hong, Y. Wang, S. Liu, [Advancing Model Pruning via Bi-level Optimization](#), *NeurIPS'22*.
- [4] A. Chen\*, P. Lorenz\*, **Y. Yao**, P. Chen, S. Liu, [Visual Prompting for Adversarial Robustness](#), *ICASSP'22*.
- [5] **Y. Yao\***, Y. Gong\*, 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 Spotlight*.
- [7] P. Zhao, P. Ram, S. Lu, **Y. Yao**, D. Bouneffouf, X. Lin, S. Liu, [Learning to Generate Image Source-Agnostic Universal Adversarial Perturbations](#), *IJCAI'22*.
- [8] L. Liu, **Y. Yao**, Z. Cao, M. Zhang, [DeepLoRa: Learning Accurate Path Loss Model for Long Distance Links in LPWAN](#), *INFOCOM'21*.
- [9] L. Li\*, M. Liu\*, **Y. Yao**, F. Dang, Z. Cao, Y. Liu, [Patronus: Preventing Unauthorized Speech Recordings with Support for Selective Unscrambling](#), *SenSys'20*.
- [10] **Y. Yao**, Z. Ma, Z. Cao, [LoSee: Long-Range Shared Bike Communication System Based On LoRaWAN Protocol](#), *EWSN'19*.

---

**PROJECT**

---

**Bi-level Optimization-based Pruning**Supervisor: [Sijia Liu](#) (MSU) Collaborator: [Parikshit Ram](#) (IBM), [Mingyi Hong](#) (UMN)

- Devise the model pruning algorithm through the lens of bi-level optimization.
- Build the new bi-level pruning (BiP) pipeline, achieving SOTA performance.
- **Publications:** [\[3\]](#)

**Reverse Engineering of Adversarial Examples**Supervisor: [Sijia Liu](#) (MSU) Collaborator: [Xiaoming Liu](#) (MSU), [Xue Lin](#) (NEU)

- Build Reverse Engineering of Deceptions (RED) to recover adversarial noise.
- Build evaluation pipeline for RED in pixel, logit, and attribution space.
- **Publications:** [\[1, 5\]](#)

**Scalable Optimization for Adversarial Learning**Supervisor: [Sijia Liu](#) (MSU) Collaborator: [Shiyu Chang](#) (UCSB), [Pin-Yu Chen](#) (IBM)

- Build the query-based optimization system to ensure certified robustness.
- Integrate the bi-level optimization into the backdoor example generation.
- Build the MAML-based few-shot universal adversarial perturbation generation.
- **Publications:** [\[6, 7\]](#)

---

**SKILL**

---

- Python, PyTorch, C++, MATLAB, Git, SQL

---

**HONOR**

---

- **Travel Grant** at Neurips 2022, CVPR 2023.
- **Winner of Best Poster Award** at EWSN 2019.
- **Outstanding Undergraduate** of Automation Department, Tsinghua University, 2018.
- **Excellent Academic Scholarship** of Tsinghua University, 2015, 2016, 2017.
- **Chinese University Entrance Exam Rank 25/341642** of Shanxi Province, 2014.
- **Chinese Mathematics Olympics 1st Prize** of Shanxi Province, 2014.

---

**TEACH**

---

- **CSE 801: Big Data Analysis** of MSU, Spring. 2023.
- **CSE 232: C++ Programming** and **CSE 231: Python Programming** of MSU, Fall. 2021.
- **CSE 477: Web Applications** of MSU, Spring. 2021.
- **CSE 480: Database Systems** of MSU, Fall. 2020, Fall. 2023.
- **CSE 891: Artificial Intelligence and Internet of Things (AIOT)** of MSU, Apr. 2020.

---

**SERVICE**

---

- **Workshop Activity Student Chair** of [AdvML Frontiers](#) at ICML'22 and ICML'23.
- **Workshop TPC** of [AdvML](#) at KDD'22, [TSRML](#) at Neurips'22.
- **Reviewers** of Neurips'22, ICASSP'23, ICML'23.