

Zijian HUANG

Phone: (1)2172003699 Email: zijianh@umich.edu

EDUCATION

University of Michigan Ann Arbor, Ann Arbor, US

08/2023-present

PhD in Electrical and Computer Engineering

GPA: 3.94 / 4.0

- **Advisor:** Prof. Jiasi Chen

- **Research interests:** Trustworthy and Efficient LLM, Reinforcement Learning, XR Security

University of Illinois at Urbana-Champaign, Urbana, US

01/2021-05/2023

Master of Science in Computer Science

GPA: 4.0 / 4.0

- **Advisor:** Prof. Bo Li (Secure Learning Lab)

- **Research interests:** robust machine learning, reinforcement learning, computer vision

The Hong Kong University of Science and Technology, Hong Kong, China

09/2016-07/2020

B.Sc in Computer Science, double major in General Math

Major GPA: 3.838

Ecole Polytechnique Fédérale de Lausanne (EPFL), Lausanne, Switzerland

02/2019-06/2019

Exchange Student in Computer Science (Informatique)

GPA: 5.34 / 6.0

PUBLICATIONS

- **Zijian Huang**, Wenda Chu, Linyi Li, Chejian Xu, Bo Li, “COMMIT: Certifying Robustness of Multi-Sensor Fusion Systems against Semantic Attacks”, accepted by *the Thirty-Ninth AAAI Conference on Artificial Intelligence (AAAI 2025)* (PDF)
- **Zijian Huang***, Xuechen Zhang*, Chenshun Ni, Ziyang Xiong, Jiasi Chen, Samet Oymak, “Efficient Small Reasoning Models through Length Penalized Reinforcement Learning”, submitted to *the 2nd Conference ON Language Modeling (COLM 2025)* (PDF)
- **Zijian Huang***, Xuechen Zhang*, Chenshun Ni, Yingcong Li, Jiasi Chen, Samet Oymak, “BREAD: Enhancing SLM Reasoning by Bridging Supervised and Reinforcement Learning”, submitted to *the Thirty-Ninth Annual Conference on Neural Information Processing Systems (NeurIPS 2025)*
- **Zijian Huang**, Yicheng Zhang, Sophie Chen, Nael Abu-Ghazaleh, Jiasi Chen, “Siren Song: Manipulating Pose Estimation in XR Headsets Using Acoustic Attacks”, submitted to *the 24th IEEE International Symposium on Mixed and Augmented Reality (ISMAR 2025)* (PDF)
- **Zijian Huang***, Cary Shu*, Hang Qiu, Jiasi Chen, “ReplayAR: A Tool for Visual Evaluation of Mixed Reality”, accepted by *the 2nd ACM Workshop on Mobile Immersive Computing, Networking, and Systems (ImmerCom 2024)*
- Xuechen Zhang, **Zijian Huang**, Ege Onur Taga, Samet Oymak, Carlee Joe-Wong, Jiasi Chen, “Efficient Contextual LLM Cascades through Budget-Constrained Policy Learning”, accepted by *the Thirty-eighth Annual Conference on Neural Information Processing Systems (NeurIPS 2024)* (PDF)
- Fan Wu, Linyi Li, **Zijian Huang**, Yevgeniy Vorobeychik, Ding Zhao, Bo Li. “CROP: Certifying Robust Policies for Reinforcement Learning through Functional Smoothing”, accepted at *the Tenth International Conference on Learning Representations (ICLR 2022)* (PDF) (Website) (code)
- Xuanchi Ren, Haoran Li, **Zijian Huang**, Qifeng Chen. “Self-supervised dance video synthesis conditioned on music”, accepted at *the 28th ACM International Conference on Multimedia (ACM MM 2020)* as Full Oral Presentation (PDF)
- Tristan McCarty, Weijia Zhang, **Zijian Huang**, Jiasi Chen, Elena Kokkoni, “An Adaptive Difficulty Algorithm to Personalize Mixed Reality Pediatric Motor Rehabilitation”, accepted by *the 2025 World Conference of the International Society for Virtual Rehabilitation (WCISVR 2025)*
- Tristan McCarty, Smrithi Surender, Cary Shu, **Zijian Huang**, Jiasi Chen, Elena Kokkoni, “Integrating Mixed Reality and Body Weight Support Technology for Immersive Pediatric Rehabilitation”, accepted by *the 46th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC 2024)*

SELECTED PUBLICATIONS

- COMMIT: Certifying Robustness of Multi-Sensor Fusion Systems against Semantic Attacks
 - Propose the first framework for certifying the robustness of 3D object detection fusion models against rotation transformation and colorization
 - Propose two robustness certification criteria for 3D object detection models, together with corresponding certification algorithms based on median smoothing
 - Propose the first algorithm to compute the lower bound of 3D IoU given the range of bounding box parameters

- Theoretically prove the certification radius for inputs and lower bound of detection confidence score and IoU between prediction and ground truth under bounded physical transformation
- Efficient Contextual LLM Cascades through Budget-Constrained Policy Learning
 - Characterize the accuracy, monetary cost, and latency of LLMs
 - Propose an adaptive LLM and prompt selection policy based on reinforcement learning
 - Conduct extensive evaluations on robustness to different budgets, question difficulty, price changes, new LLMs, and new unseen task types
- CROP: Certifying Robust Policies for Reinforcement Learning through Functional Smoothing
 - Propose the first framework for certifying the robustness of Q-learning algorithms against adversarial attacks
 - Propose two robustness certification criteria for Q-learning algorithms, together with corresponding certification algorithms based on global and local smoothing strategies
 - Theoretically prove the certification radius for input state and lower bound of perturbed cumulative reward under bounded adversarial state perturbations
- Self-supervised dance video synthesis conditioned on music
 - Propose a pipeline to generate dance video, given music
 - Propose a creative GAN model with modified Local Temporal Discriminator
 - Propose Pose Perceptual Loss to generate verisimilitude dance pose sequence
 - Propose a metric to assess the difference between dance pose sequences using MMD-NCA loss and K-means

JOB EXPERIENCE & RESEARCH EXPERIENCE

- | | |
|--|------------------------------|
| • UMich Mavens Lab | 08/2023-present |
| Research Assistant (Trustworthy and Efficient Machine Learning) | <i>Ann Arbor, MI</i> |
| • UIUC Secure Learning Lab | 01/2021-05/2023 |
| Research Assistant (Adversarial Machine Learning) | <i>Urbana-Champaign, IL</i> |
| • Reality Lab at Meta | 05/2022-08/2022 |
| Machine Learning Engineer summer intern (Face expression classifier and face tracker) | <i>Menlo Park, US</i> |
| • AI Lab in ByteDance | 09/2020-12/2020 |
| Computer Vision Research Intern (Unsupervised 3D human pose estimation with Autoencoder) | <i>Beijing, China</i> |
| • Visual Interlligence Lab in HKUST | 06/2019-05/2020 |
| Computer Vision Research Assistant (Video Generation with GAN) | <i>Hong Kong, China</i> |
| • Computer Vision lab in EPFL | 02/2019-06/2019 |
| Computer Vision Research Assistant (Type Design Project with GAN) (code) | <i>Lausanne, Switzerland</i> |
| • Tencent Youtu X-lab | 12/2018-01/2019 |
| Computer Vision Research Intern (Destroyed Audio Reconstruction with GAN) | <i>Shenzhen, China</i> |
| • HKUST RIPS-HK Project | 06/2018-08/2018 |
| Machine Learning Research Assistant (Music Generation with GAN) | <i>Hong Kong, China</i> |
| • Sustainable Smart Campus as a Living Lab | 02/2018-06/2018 |
| Software Engineer (Indoor Localization APP) | <i>Hong Kong, China</i> |

TEACHING EXPERIENCES

- | | |
|--|-------------|
| • UMich EECS 498 AI-Enabled Mixed Reality | Fall 2025 |
| • UIUC CS 442 Trustworthy Machine Learning | Spring 2023 |
| • UIUC CS 562 Advanced Topics in Security, Privacy, and Machine Learning | Fall 2022 |
| • UIUC AE 504 Optimal Aerospace Systems | Spring 2022 |

AWARDS & SCHOLARSHIPS

- | | |
|---|---------------------------------|
| • University's Scholarship Scheme for Continuing Undergraduate Students from The Hong Kong University of Science and Technology | 2016, 2017, 2018 and 2019 |
| • Dean's List from The Hong Kong University of Science and Technology | 2016, 2017, 2018, 2019 and 2020 |
| • Reaching Out Award from HKSAR Government Scholarship Fund | 2019 |
| • Study Abroad Sponsorship from The Hong Kong University of Science and Technology | 2019 |
| • Admission Scholarship from The Hong Kong University of Science and Technology | 2016 |

SERVICE

- **Conference Reviewer:** ICLR, NeurIPS, ICML, AISTAT, CVPR, ICCV, ECCV, INFOCOM

LANGUAGE & TECHNICAL SKILLS

- **Programming Skills:** Python, C++, R, JAVA, JavaScript, HTML, CSS
- **Familiar Software:** MS office, MATLAB