

# Zeliang Zhang

Portfolio: [zhangai.github.io](https://github.com/zhangai)  
Github: [github.com/zhangai](https://github.com/zhangai)

Email: [hust0426@gmail.com](mailto:hust0426@gmail.com)  
Mobile: +1-585-410-8957

## EDUCATION

- Huazhong University of Science and Technology** Wuhan, Hubei, China  
*Bachelor, Computer Science; GPA: 3.89*  
Sep 2018 - June 2022
- University of Rochester** Rochester, New York State, US  
*Ph.D. student, Computer Science; GPA: 3.55*  
Sep 2022 - Present

## PERSONAL STATEMENT

My research interests fall on high-performance **scientific tensor computations** and applications (quantum neural networks, big data analysis, and quantum circuits), **responsible AI**, and **optimization theory**. I am an expert in **Python and C programming**, and familiar with popular deep learning frameworks, including Pytorch/TensorFlow, and basic **CUDA programming**, including the use of **GPU tensor cores**.

## WORKING EXPERIENCE

- Machine Learning Group, Microsoft Research Asia** Beijing, China  
*Research intern*  
Oct. 2021 - Jun. 2022
  - HPC for AI4Science**: Work on using GPU to accelerate the DFT computation for the automatic material design, and molecular chemistry computation.

## TEAMWORK EXPERIENCE

- AI4Finance programming team** Remote  
*Student research assistant*  
Advised by Xiao-Yang Liu
  - Stable RL**: Involved in an open source project, ElegantRL (over 1,500 starts on Github), and developed a Hamiltonian regularization term to stable the RL training, <https://github.com/AI4Finance-Foundation/ElegantRL>.
  - HPC for tensor network-based methods**: Study on the design of high-performance tensor computations and applications, including tensor networks, DMRG, and the classical simulation of quantum circuits.

## PUBLICATIONS

(\* indicates the **equal contribution** with random order, which may be different from literature order.)

- [**Trustworthy**] **Zeliang Zhang**, Wei Yao, Susan Liang, Chenliang Xu. "Random Smooth-based Certified Defense against Text Adversarial Attack." **EACL Findings** 2024.
- [**Trustworthy**] **Zeliang Zhang\***, Mingqian Feng\*, Zhiheng Li, Chenliang Xu. "Multiple Unknown Biased Subclass Discovery in Latent Space." **CVPR** 2024.
- [**Trustworthy**] Rongyi Zhu\*, **Zeliang Zhang\***, Susan Liang\*, Zhuo Liu, Chenliang Xu. "Learning to Transform Dynamically for Better Adversarial Transferability." **CVPR** 2024.
- [**Optimization**] Jinyang Jiang\*, **Zeliang Zhang\***, Chenliang Xu, Zhaoifei Yu, Yijie Peng. "Breaking the chain rule: learning with only forward using the likelihood ratio method." **ICLR** 2024.
- [**LLM**] Yunlong Tang, ..., **Zeliang Zhang**, ..., Chenliang Xu. "Video Understanding with Large Language Models: A Survey." Technical report 2024.
- [**Trustworthy**] **Zeliang Zhang**, Rongyi Zhu, Wei Yao, Xiaosen Wang, Chenliang Xu. "Bag of tricks to boost adversarial transferability." Technical report 2024.
- [**Quantum computation**] Xiao-Yang Liu, **Zeliang Zhang**. "Classical Simulation of Quantum Circuits Using Reinforcement Learning: Parallel Environments and Benchmark." **NeurIPS** dataset and benchmark track 2023.
- [**Trustworthy**] Xiaosen Wang, **Zeliang Zhang**, and Jianping Zhang. "Structure Invariant Transformation for better Adversarial Transferability." **ICCV** 2023.
- [**Trustworthy**] **Zeliang Zhang\***, Zhiyuan Wang\*, Siyuan Liang, and Xiaosen Wang. "Diversifying the High-level Features for better Adversarial Transferability." **BMVC** 2023.
- [**Quantum computation**] **Zeliang Zhang\***, Xiao-Yang Liu\*, Zhiyuan Wang, Han Lu, Xiaodong Wang, and Anwar Walid. "High-Performance Tensor Learning Primitives Using GPU Tensor Cores." **IEEE Transactions on Computers** 2022. (Top journal in System area)
- [**Quantum computation**] **Zeliang Zhang**, Junzhe Zhang, Guoping Lin, Zeyuan Yin, and Kun He. "Parallel TTr1-Tensor: Randomized Compression-based Scheme for Tensor Train Rank-1 Decomposition." **NeurIPS** 2020 QTNMLW.

- **[Trustworthy]** Xiaosen Wang, **Zeliang Zhang**, Kangheng Tong, Dihong Gong, Kun He, Zhifeng Li, and Wei Liu. "Triangle attack: A query-efficient decision-based adversarial attack." **ECCV** 2022.
- **[Optimization]** Xiao Li, **Zeliang Zhang**, Jinyang Jiang, and Yijie Peng. "Noise optimization in artificial neural networks." **CASE** 2022.
- **[Optimization]** **Zeliang Zhang**, Zhuo Liu, Susan Liang, Zhiyuan Wang, Yifan Zhu, Chen Ding, Chenliang Xu. "Scalable CP Decomposition for Tensor Learning using GPU Tensor Cores." Technical report 2024.
- **[Reinforcement Learning]** **Zeliang Zhang**, Yipeng Wang, Zeqi Liu, and Xiao-Yang Liu, "DHN: Deep Hamiltonian Network for Variational Reinforcement Learning." **NeurIPS** 2021 QTNMLW.
- **[Quantum computation]** **Zeliang Zhang**, Xiao-Yang Liu, and Pan Zhou. "Trillion-Tensor: Trillion-Scale CP Tensor Decomposition." **IJCAI** 2020 TNRMWL.

## PROJECTS

---

### Are large models always better? Understanding audio-visual model robustness under corruptions

Daiki Shimada, **Zeliang Zhang**, Chenliang Xu

- **[Trustworthy/Robustness]** This paper presents a benchmarking framework to evaluate the robustness of audio-visual models against common corruptions.
- Under review.

### A Forward-Only and Parallel Framework for Boosting Neural Network Training

**Zeliang Zhang\***, Jinyang Jiang\*, Zhuo Liu\*, Yijie Peng, Chenliang Xu

- **[Optimization]** We propose an approximated likelihood ratio method for gradient estimation and pipeline the training.
- Under review.

### Revisit Audio-Visual Adversarial Robustness from Temporal and Modality Correlation Perspectives

**Zeliang Zhang\***, Susan Liang\*, Daiki Shimada\*, Chenliang Xu

- **[Trustworthy AI]** We propose a powerful audio-visual adversarial attack to benchmark the robustness performance of audio-visual models and strong defense adversarial defense methods.
- Under review.

### High-performance Tensor-Train Primitives Using GPU Tensor Cores

Xiao-Yang Liu, Hao Hong, **Zeliang Zhang**, Weiqing Tong, Xiaodong Wang, Anwar Walid

- **[Tensor computation]** We present high-performance tensor-train primitives using GPU tensor cores and demonstrate three applications.
- Under review.

## HONORS AND AWARDS

---

### Individual Scholarship on Arts and Sports

Recognition for students with good performance in arts and sports activities

Apr. 2019

### Scholarship for Scientific and Technological Innovation

Recognition for students with good performance in scientific and technological innovation

Dec. 2020

### The SANGFOR scholarship

Recognition by Sangfor Technologies Inc for students in both study and academics

Apr. 2021

### Excellent graduate

Recognition for excellent graduate in HUST.

Jun. 2022