ZIHAO ZHU （朱梓豪）

Address: 2001 Longxiang Road, Shenzhen, China

zihaozhu@link.cuhk.edu.cn | Homepage | Google Scholar

EDUCATION

The Chinese University of Hong Kong, Shenzhen *2021.09 - Present*
School of Data Science
Ph.D. of Data Science
Advisor: Baoyuan Wu

University of Chinese Academy of Sciences *2018.09 - 2021.06*
Institute of Information Engineering
Master of Science in Engineering
Advisor: Yue Hu, Jing Yu

China University of Mining and Technology *2014.09 - 2018.06*
School of Computer Science and Technology
Bachelor of Engineering

RESEARCH INTERESTS

AI security & privacy, Backdoor attack and defense, Multimodal machine learning

RESEARCH EXPERIENCE

Tencent AILab Shenzhen, China
Research Intern *2024.03 - Present*

Shenzhen Research Institute of Big Data Shenzhen, China
Research Assistant at Secure Computing Lab of Big Data *2021.06 - 2024.01*

PUBLICATIONS

Journal (1 PR)

1. Cross-Modal Knowledge Reasoning for Knowledge-based Visual Question Answering
   Jing Yu*, **Zihao Zhu**, Yujing Wang, Weifeng Zhang, Yue Hu, Jianlong Tan (*Advisor)
   In Pattern Recognition (PR), 2020

Conference (1 ICLR, 1 NeruIPS, 2 IJCAI, 1 AAAI, 2 ICASSP)

1. VDC: Versatile Data Cleanser for Detecting Dirty Samples via Visual-Linguistic Inconsistency
   Zihao Zhu, Mindda Zhang, Shaokui Wei, Bingzhe Wu, Baoyuan Wu
   In International Conference on Learning Representations (ICLR), 2024

2. Learning to Optimize Permutation Flow Shop Scheduling via Graph-based Imitation Learning
   Longkang Li, Siyuan Liang, **Zihao Zhu**, Xiaochun Cao, Chris Ding, Hongyuan Zha, Baoyuan Wu
   In AAAI Conference on Artificial Intelligence (AAAI), 2024

3. BackdoorBench: A Comprehensive Benchmark of Backdoor Learning
   Baoyuan Wu, Hongrui Chen, Mingda Zhang, **Zihao Zhu**, Shaokui Wei, Danni Yuan, Hongyuan Zha
   In Thirty-sixth Conference on Neural Information Processing Systems (NeurIPS), 2022

4. From Shallow to Deep: Compositional Reasoning over Graphs for Visual Question Answering
   Zihao Zhu
   In IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2022

5. MCR-NET: A Multi-Step Co-Interactive Relation Network for Unanswerable Questions on Machine Reading Comprehension
   Wei Peng, Yue Hu, Luxi Xing, Yuqiang Xie, **Zihao Zhu**, Yajing Sun
   In IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2021

6. Mucko: Multi-Layer Cross-Modal Knowledge Reasoning for Fact-based Visual Question Answering
   Zihao Zhu, Jing Yu, Yujing Wang, Yajing Sun, Yue Hu, Qi Wu
   In Proceedings of the 29th International Conference on Joint Artificial Intelligence (IJCAI), 2020

7. DAM: Deliberation, Abandon and Memory Networks for Generating Detailed and Non-repetitive Responses
   Xiaoze Jiang, Jing Yu, Zengchang Qin, **Zihao Zhu**, Qi Wu
   In Proceedings of the 29th International Conference on Joint Artificial Intelligence (IJCAI), 2020

Preprints (4 arXiv)

1. Boosting Backdoor Attack with A Learnable Poisoning Sample Selection Strategy
   Zihao Zhu, Mingda Zhang, Shaokui Wei, Li Shen, Yanbo Fan, Baoyuan Wu
   arXiv, 2023

2. BlackboxBench: A Comprehensive Benchmark of Black-box Adversarial Attacks
   Meixi Zheng, Xuanchen Yan, **Zihao Zhu**, Hongrui Chen, Baoyuan Wu
   arXiv, 2023

3. Robust Backdoor Attack with Visible, Semantic, Sample-Specific, and Compatible Triggers
   Ruotong Wang, Hongrui Chen, **Zihao Zhu**, Li Liu, Yong Zhang, Yanbo Fan, Baoyuan Wu
   arXiv, 2023

4. Attacks in Adversarial Machine Learning: A Systematic Survey from the Life-cycle Perspective
   Baoyuan Wu, **Zihao Zhu**, Li Liu, Yanbo Fan, Siwei Lyu, Hongyuan Zha
   arXiv, 2023

5. Defenses in Adversarial Machine Learning: A Survey
   Baoyuan Wu, Shaokui Wei, Mingli Zhu, Meixi Zheng, **Zihao Zhu**, Mingda Zhang, Hongrui Chen, Danni Yuan, Li Liu, Qingshan Liu
   arXiv, 2023

PATENTS

- Graph Visualization Method based on Graph Convolution Network
  Zihao Zhu, Chuan Zhou, YaNan Cao, Peng Zhang, Li Guo
  China, CN109753589A

SERVICE

Reviewer:

AAAI 2020, CVPR 2024, IEEE TIP

TEACHING

MFE5260 Data Sciences in Financial Engineering — 2022 Spring
Teaching Assistant

DDA6309 Probabilistic Graphical Models — 2021 Fall
Teaching Assistant

AWARDS

AIRS Talent of PhD Research Program — 2021.09
University of Chinese Academy of Sciences Merit Student — 2020.10
Outstanding Undergraduate Thesis Award — 2018.06
The First Prize Scholarship of CUMT — 2016.10
The First Prize Scholarship of CUMT — 2015.10