Yijun Yang, Ph.D.

Email: yjyang@cse.cuhk.edu.hk
Tel: +852 59862685
Shatin, Hong Kong, China

Education

The Chinese University of Hong Kong — Hong Kong, China
Ph.D. of Computer Science and Engineering — *Aug. 2019 - Jul. 2024*

Tsinghua, University — Beijing, China
M.Phil. in School of Integrated Circuit Engineering — *Aug. 2016 - Jul. 2019*

North China Research Institute of Electro-Optics — Beijing, China
Drop out Master in Electric Engineering — *Aug. 2013 - Sept. 2015*

Central South University — Chang Sha, China
B.Eng. of Department of Automation — *Aug. 2009 - Jul. 2013*

Experience

Research Intern — Dec. 2023 – Jul. 2024
AI Theory, Huawei Noah's Ark Lab — *Hong Kong, China*
- Multimodal Large Model Project

Research Intern — Jul. 2023 – Nov. 2023
Institute of Automation, Chinese Academy of Sciences — *Beijing, China*
- Wenge·YaYi Large Language Model Project

Research Intern — Mar. 2022 – Jun. 2023
Foundation Model Group, Megvii — *Beijing, China*
- Conducted research on data synthesis for perception in autonomous vehicles.

Research Intern — Mar. 2020 – Jun. 2020
EDA group, Huawei 2012 Lab — *Shenzhen, China*
- Conducted research on EDA software design.

Publication

[1] **Yijun Yang**, Ruiyuan Gao, Xiaosen Wang, Tsung-Yi Ho, Nan Xu, and Qiang Xu. "MMA-Diffusion: MultiModal Attack on Diffusion Models". In: *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (**CVPR**)*. 2024. URL: https://arxiv.org/abs/2311.17516.

[2] **Yijun Yang**, Ruiyuan Gao, Xiao Yang, Jianyuan Zhong, and Qiang Xu. "GuardT2I: Defending Text-to-Image Models from Adversarial Prompts". In: *Conference on Neural Information Processing Systems (**NeurIPS**)*. 2024. URL: https://arxiv.org/abs/2403.01446.

[3] Zhiyuan He*, **Yijun Yang***, Pin-yu Chen, Qiang Xu, and Tsung-Yi Ho. "Be Your Own Neighborhood: Detecting Adversarial Example by the Neighborhood Relations Built on Self-Supervised Learning, * co-first author." In: *International Conference on Machine Learning (**ICML**)*. 2024. URL: https://arxiv.org/abs/2209.00005.

[4] **Yijun Yang**, Ruiyuan Gao, Xiaosen Wang, Xiangyu Wen, Xiangyu Zhang, and Qiang Xu. "Bridging Perception Gaps: A Generative Approach to Thwarting Adversarial Hiding Attacks". In: ***Under review***. 2023.

[5] **Yijun Yang**, Ruiyuan Gao, Yu Li, Qiuxia Lai, and Qiang Xu. "What You See is Not What the Network Infers: Detecting Adversarial Examples Based on Semantic Contradiction". In: *Network and Distributed System Security Symposium (**NDSS**)*. 2022. URL: https://arxiv.org/pdf/2201.09650.

[6] **Yijun Yang**, Ruiyuan Gao, and Qiang Xu. "Out-of-Distribution Detection with Semantic Mismatch under Masking". In: *European Conference on Computer Vision (**ECCV**)*. Springer. 2022. URL: https://arxiv.org/abs/2208.00446.

[7] **Yijun Yang**, Ruiyuan Gao, Yu Li, Qiuxia Lai, and Qiang Xu. "Mixdefense: A Defense-in-Depth Framework for Adversarial Example Detection". In: *The International Symposium on Computer Architecture (**ISCA Workshop**)*. 2021. URL: https://arxiv.org/pdf/2104.10076.

[8] **Yijun Yang**, Liji Wu, Ye Yuan, and Xiangmin Zhang. "A General Hardware Trojan Technique Targeted on Lightweight Cryptography with Bit-serial Structure". In: *EAI International Conference on Security and Privacy in New Computing Environments (**SPNCE**)*. 2019. URL: https://eudl.eu/pdf/10.1007/978-3-030-21373-2_54.

[9] **Yijun Yang**, Ye Yuan, Liji Wu, and Xiangmin Zhang. "A High PSRR Low Drop-out Linear Regulator without Output Capacitor". In: *IEEE International Conference on Electron Devices and Solid State Circuits (**EDSSC**)*. 2018. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8487175.

[10] Ye Yuan, **Yijun Yang**, Liji Wu, and Xiangmin Zhang. "A High PSRR Low Drop-out Linear Regulator without Output Capacitor". In: *Security and Communication Networks (**SCN**)*. 2018. URL: https://www.hindawi.com/journals/scn/2018/2483619/.

[11] **Yijun, Yang**, Liji Wu, Xiangmin Zhang, and Jianben He. "A Novel Hardware Trojan Detection with ChipID Based on Relative Time Delay". In: *IEEE International Conference on Anticounterfeiting Security and Identification (**ASID**)*. 2017. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8285766.

Competition

International Algorithm Case Competition (Huangpu) | *Adversarial Training* Aug. 2022 – Nov. 2022

- As the **team leader** on the team of CURE Lab from CUHK.
- **2nd place** in competition problem of Adversarial Robustness Defense Algorithm of Deep Learning Models.

Awards & Scholarships

- Full Postgraduate Studentship, The Chinese University of Hong Kong.
- Outstanding Graduate, Tsinghua University (Top 2%).
- Outstanding Thesis Award, Tsinghua University (Top 3%).
- Outstanding Graduate, Central South University (Top 3%).
- Outstanding Thesis, Central South University (Top 5%).
- Second-class Undergraduate Merit Scholarship, Central South University (Top 10%).

Services

I have served as a reviewer of academic conferences: **ECCV 2024**, **ICML 2024**, **ICASSP 2023**, **NeurIPS 2024**, **ICLR 2024**, **CVPR 2024**, **Neural Computing**, **AAAI 2025**, **ICLR 2025**, and **ICASSP 2025**.

Technical Skills and Other

Languages: Python, C/C++, Java, Verilog/VHDL
Frameworks: Pytorch, Tensorflow, Rails
Developer Tools: Linux and shell, Git, Docker, VS Code, Visual Studio, PyCharm, LaTeX