

# Yijun Yang, Ph.D. Candidate

✉ yjyang@cse.cuhk.edu.hk    ✉ yangyj16@tsinghua.org.cn  
🏠 Yijun's Homepage    🐙 Github  
🔍 Google Scholar    📄 Research Gate  
☎ +86 18613370368



## Short Bio

- 📌 I am a fourth-year Ph.D. student of [CUhk RELiable Laboratory \(CURE\)](#), in the Department of Computer Science and Engineering, [The Chinese University of Hong Kong](#), supervised by [Prof. Qiang Xu](#). Our lab focuses on AI security and AI robustness related tasks. Before that, I received my M.Phil in EE from [Tsinghua University](#) in 2019. My current research interests span the fields of AI security and Deep Learning, including Adversarial Example defense, Out-of-distribution detection, Deep Generative Models, and self-supervised learning.

## Education

- 📌 **Ph.D., The Chinese University of Hong Kong**, Hong Kong S.A.R.  
*CUhk RELiable Computing Laboratory (CURE),  
Department of Computer Science and Engineering. GPA: 3.7/4.0*
- 📌 **M.Phil., Tsinghua University**, Beijing, China.  
*Department of Integrated Circuit Engineering. GPA: 3.7/4.0, Ranking: 3/45*
- 📌 **B.Eng, Central South University**, Changsha, China.  
*Department of Automation. GPA: 3.7/4.0*

## Experiences

- Research intern    📌 Mar. 2022 - Present, Foundation Model, Megvii, Beijing, China  
                              📌 Mar. 2020 - June. 2020, 2012 Lab, Huawei, Shenzhen, China

## Selected Research Publications

- 1 **Yijun, Yang**, Ruiyuan, G., & Qiang, X. (2022). Out-of-distribution detection with semantic mismatch under masking. *European Conference on Computer Vision (ECCV 2022)*. Retrieved from <https://arxiv.org/abs/2208.00446>
- 2 **Yijun, Yang**, Ruiyuan, G., Yu, L., Qiuxia, L., & Qiang, X. (2022). What you see is not what the network infers: Detecting adversarial examples based on semantic contradiction. *Network and Distributed Systems Security (NDSS 2022)*. Retrieved from <http://arxiv.org/abs/2201.09650>
- 3 Zhiyuan, He\*, **Yijun, Yang\***, Pin-yu, C., Qiang, X., & Tsung, H. (2022). Be your own neighborhood: Detecting adversarial example by the neighborhood relations built on self-supervised learning. *European Conference on Computer Vision Workshop (ECCV 2022 AWOR)* \* co-first author.
- 4 **Yijun, Yang**, Ruiyuan, G., Yu, L., Qiuxia, L., & Qiang, X. (2021). Mixdefense: A defense-in-depth framework for adversarial example detection. *The International Symposium on Computer Architecture (ISCA 2021) Workshop*. Retrieved from <https://sites.google.com/usc.edu/spsl/home>
- 5 **Yijun, Yang**, Liji, W., Ye, Y., & Xiangmin, Z. (2019). A general hardware trojan technique targeted on lightweight cryptography with bit-serial structure. *EAI International Conference on Security and Privacy in New Computing Environments (SPNCE 2019)*.
- 6 **Yijun, Yang**, Ye, Y., Liji, W., & Xiangmin, Z. (2017). A novel hardware trojan detection with chipid based on relative time delay. *IEEE International Conference on Anticounterfeiting Security and Identification (ASID 2017)*.

## Selected Award and Honors

---

- **Full Postgraduate Studentship**, The Chinese University of Hong Kong.
- **Outstanding Master Graduate**, Tsinghua University (Top 2%).
- **Outstanding Thesis Award**, Tsinghua University (Top 3%).
- **Scholarship for Advancement in Academic Work**, Tsinghua University (Top 5%).
- **Scholarship for Advancement in Academic Work**, Tsinghua University (Top 5%).
- **Outstanding Bachelor Graduate**, Central South University (Top 3%).
- **Outstanding Thesis Award**, Central South University (Top 5%).