

Hanbin Hong

Department of Computer Science and Engineering,
University of Connecticut, Storrs, CT 06269
hanbin.hong@uconn.com
<https://youbin2014.github.io>

EDUCATION

- Ph.D. Student, University of Connecticut** Storrs, Connecticut
Department of Computer Science and Engineering September 2022 – May 2025 (expected)
Area: Computer Science
- Ph.D. Student, Illinois Institute of Technology** Chicago, Illinois
Department of Computer Science January 2021 – May 2022
Area: Computer Science
- Research Internship, Rochester Institute of Technology** Rochester, New York
Golisano College of Computing and Information Sciences September 2019 – December 2020
Area: Computer Vision
- Graduate School, Xi'an Jiaotong University** Xi'an, China
School of Economics and Finance September 2018 – July 2019
Major: Financial Engineering
- Xi'an Jiaotong University** Xi'an, China
Qian Xuesen School September 2014 – July 2018
Major: Honor Science Program (Physics)

PUBLICATION

- Xinyu Zhang, **Hanbin Hong**, Yuan Hong, Peng Huang, Binghui Wang, Zhongjie Ba, and Kui Ren. Text-CRS: A Generalized Certified Robustness Framework against Textual Adversarial Attacks. 45th IEEE Symposium on Security and Privacy (IEEE S&P), 2024
- Hanbin Hong**, and Yuan Hong. Certifiable Black-Box Attack: Ensuring Provably Successful Attack for Adversarial Examples. arXiv preprint arXiv:2304.04343, 2023
- Han Wang, **Hanbin Hong**, Li Xiong, Zhan Qin, and Yuan Hong. PrivLBS: Local Differential Privacy for Location-Based Services with Staircase Randomized Response. Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS), 2022.
- Hanbin Hong**, and Yuan Hong. Certified Adversarial Robustness via Anisotropic Randomized Smoothing. arXiv preprint arXiv:2207.05327, 2022.
- Hanbin Hong**, Binghui Wang, and Yuan Hong. UniCR: Universally Approximated Certified Robustness via Randomized Smoothing. Computer Vision European Conference (ECCV), 2022
- Hanbin Hong**, Yuan Hong, and Yu Kong. An Eye for an Eye: Defending against Gradient-based Attacks with Gradients. arXiv preprint arXiv:2202.01117, 2022.
- Hanbin Hong**, Wentao Bao, Yuan Hong, and Yu Kong. Privacy Attributes-aware Message Passing Neural Network for Visual Privacy Attributes Classification. 2020 25th International Conference on Pattern Recognition (ICPR). IEEE, 2021.
- Junwen Chen, Haiting Hao, **Hanbin Hong**, and Yu Kong, RIT-18: A Novel Dataset for Composi-

tional Group Activity Understanding, IEEE Conference on Computer Vision and Pattern Recognition (CVPR) Workshops, 2020.

RESEARCH
INTERESTS

Machien Learning Security, Adversarial Learning, Adversarial Attacks, Adversarial Robustness, Certifiable Robustness, Differential Privacy, and Privacy-preserving Machine Learning.

SERVICES

Program Committee

Association for the Advancement of Artificial Intelligence (AAAI) 2023

Association for the Advancement of Artificial Intelligence (AAAI) 2022

Reviewer

Computer Vision and Pattern Recognition Conference (CVPR) 2023

International World Wide Web Conference (Web) 2023

IEEE Transactions on Dependable and Secure Computing (TDSC) 2023

IEEE Internet of Things Journal (IoTJ) 2023

International Conference on Machine Learning (ICML) 2023

International Conference on Computer Vision (ICCV) 2023

Conference on Neural Information Processing Systems (NeurIPS) 2022

International Conference on Machine Learning (ICML) 2022

European Conference on Computer Vision (ECCV) 2022

External Reviewer

ACM Conference on Computer and Communications Security (CCS) 2023

International Conference on Autonomous Agents and Multiagent Systems (AAMAS) 2023

USENIX Security Symposium (USENIX) 2023

ACM Conference on Computer and Communications Security (CCS) 2022

USENIX Security Symposium (USENIX) 2022

International Symposium on Research in Attacks, Intrusions and Defenses (RAID) 2022

Special Interest Group on Knowledge Discovery and Data Mining (KDD) 2022

SOFTWARE
COMPETENCIES

Programming

Python, Matlab, C\C++, Java

Software Library

PyTorch, Keras, Tensorflow

Operating Systems

Windows, Linux

HONORS AND
AWARDS

General Electric Graduate Fellowship for Excellence 2023

Predoctoral Fellowship with Excellent Research Award	2023
Synchrony Financial Cybersecurity Graduate Fellowship	2023
Student Travel Grant for CCS'22	2022
Certificate of Honors Graduate awarded by Qian Xuesen School	2018
2nd Class Zhufeng Scholarship (Top 10 in 120 students)	2017
Si Yuan Scholarship awarded by Xi'an Jiaotong University	2016
The 2nd Prize in China Undergraduate Mathematical Contest in Modeling (Top 5% in 1821 teams)	2015
The 2nd Prize in Mathematical Contest in Modeling at Xi'an Jiaotong University	2015