KAICHEN YANG

kaicheny@mtu.edu
+1 3523281128
EERC Building 712, 1400 Townsend Dr. Houghton, Michigan 49931-1295

EDUCATION

University of Florida, Gainesville, Florida, USA *May 2021 -May 2022*
Ph.D in Electrical and Computer Engineering Department
Advisor: Dr. Shuo Wang.

University of Florida, Gainesville, Florida, USA *August 2016 -May 2021*
Ph.D candidate in Electrical and Computer Engineering Department
Advisor: Dr. Yuguang Fang & Dr. Yier Jin.

University of Science and Technology of China (USTC), Hefei, Anhui, China *Sept 2013 -July 2016*
M.S. in Engineering at Department of Electrical Engineering & information science
Advisor: Dr. Chi Zhang.

University of Science and Technology of China (USTC), Hefei, Anhui, China *Sept 2009 - July 2013*
B.S. in Information Security at Department of Electrical Engineering & information science

RESEARCH INTERESTS

1. Deep learning security
2. Network Security
3. Cyber-Physical System Security
4. Deep learning assisted Hardware Security
5. 2D and 3D computer vision

PUBLICATIONS

- Weimin Fu, Shijie Li, Yifang Zhao, Haocheng Ma, Raj Dutta, Xuan Zhang, **Kaichen Yang**, Yier Jin and Xiaolong Guo, "Hardware phi-1.5 b: A large language model encodes hardware domain specific knowledge", 2024 29th Asia and South Pacific Design Automation Conference (ASP-DAC). (Published)
- Fan, Cheng, Zhaohui Wang, and **Kaichen Yang**. "Energy-efficient underwater acoustic communication based on Dyna-Q with an adaptive action space." Physical Communication 61 (2023): 102218. (Published)
- Weimin Fu, **Kaichen Yang**, Raj Gautam Dutta, Xiaolong Guo, Gang Qu, "LLM4SecHW: Leveraging domain-specific large language model for hardware debugging", 2023 Asian Hardware Oriented Security and Trust Symposium (AsianHOST), 2023. (Published)
- Honggang Yu, Shuo Wang, Haoqi Shan, Maximillian Panoff, Michael Lee, **Kaichen Yang** and Yier Jin, "Dual-Leak: Deep Unsupervised Active Learning for Cross-Device Profiled Side-Channel Leakage Analysis", IEEE International Symposium on Hardware Oriented Security and Trust (HOST), 2023. (Published)
- Honggang Yu, Mei Wang, Xiyu Song, Haoqi Shan, Hongbing Qiu, Junyi Wang, **Kaichen Yang**, "Noise2Clean: Cross-Device Side-Channel Traces Denoising with Unsupervised Deep Learning", *Electronics*. (Published)

- Weimin Fu, Honggang Yu, Orlando Arias, **Kaichen Yang**, Yier Jin, Tuba Yavuz, Xiaolong Guo, “Graph Neural Network based Hardware Trojan Detection at Intermediate Representative for SoC Platforms”, GLSVLSI 2022, 2022. (Published)
- Max Panoff, Raj Gautam Dutta, Yaodan Hu, **Kaichen Yang** and Yier Jin, “On Sensor Security in the Era of IoT and CPS”, SN Computer Science, 2021.
- **Kaichen Yang**, Tzungyu-Tsai, Honggang Yu, Max Panoff, Tsung-yi Ho and Yier Jin, “Robust Roadside Physical Adversarial Attack Against Deep Learning in Lidar Perception Modules”, 16th ACM ASIA Conference on Computer and Communications Security (ACM ASIACCS 2021). (19% acceptance ratio)
- **Kaichen Yang**, Xuanyi-Lin, Yixi Sun, Tsung-Yi Ho and Yier Jin, “3D-Adv: Black-Box Physical Adversarial Attacks against Deep Learning Models through 3D Sensors”, 58th Design Automation Conference (DAC), 2021. (To Appear) (23% acceptance ratio)
- Honggang Yu, Haocheng Ma, **Kaichen Yang**, Yiqiang Zhao and Yier Jin, “DeepEM: Deep Neural Networks Model Recovery through EM Side-Channel Information Leakage”, IEEE International Symposium on Hardware Oriented Security and Trust (HOST), 2020.
- **Kaichen Yang**, Tzungyu Tsai, Honggang Yu, Tsung-Yi Ho and Yier Jin, “Beyond Digital Domain: Fooling Deep Learning Based Recognition System in Physical World”, Proceedings of the AAAI Conference on Artificial Intelligence, 2020. (20.6% acceptance ratio)
- Tzungyu Tsai, **Kaichen Yang**, Tsung-Yi Ho and Yier Jin, “Robust adversarial objects against deep learning models”, Proceedings of the AAAI Conference on Artificial Intelligence, 2020. **Oral Presentation**. (20.6% acceptance ratio)
- Honggang Yu, **Kaichen Yang**, Teng Zhang, Yun-Yun Tsai, Tsung-Yi Ho and Yier Jin,“Cloudleak: Large-scale deep learning models stealing through adversarial examples”, Proceedings of Network and Distributed Systems Security Symposium (NDSS) /Blackhat USA, 2020. (17.4% acceptance ratio)
- **Kaichen Yang**, Jianqing Liu, Chi Zhang and Yuguang Fang, “Adversarial examples against the deep learning based network intrusion detection systems”, IEEE Military Communications Conference (MILCOM), 2018.
- **Kaichen Yang**, Chi Zhang and Nenghai Yu, “Economic costs of multi-sever private information retrieval in cloud computing”, International Conference on Cloud Computing and Big Data (CCBD), 2015.
- Mengke Yu, **Kaichen Yang**, Lingbo Wei and Jinyuan Sun, “Practical private information retrieval supporting keyword search in the cloud”, Sixth International Conference on Wireless Communications and Signal Processing (WCSP), 2014.

PROJECTS

NSF CICI: UCSS: Safeguarding AI in Bioinformatics: Enhancing Cybersecurity in Biological Data Infrastructure.

2024 - 2027

NSF ERI: Towards Robust and Secure Intelligent 3D Sensing Systems

2024 - 2026

NSF Travel Grant: Travel: Travel support for SmartSP 2023

2023 - 2024

DoD-Intel State-of-the-Art Heterogeneous Integrated Packaging (SHIP) Prototype Project

2020 - 2022

Analyze the gate-level chip design from the hypergraph perspective, partition the netlist into small sub-netlist and conduct security evaluation using hypergraph neural network.

STAMP Project

2020 - 2022

Collecting and processing the Trojan inserted gate-level netlist file for Trojan detection research.

PROFESSIONAL EXPERIENCES AND SERVICES

Journal Reviewer

- ACM Journal on Emerging Technologies in Computing Systems, 2021
- IEEE Internet of Things Journal, 2021, 2023
- IEEE Transactions on Big Data, 2024
- IEEE Transactions on Circuits and Systems, 2024
- Transactions on Information Forensics & Security, 2024
- IEEE Transactions on Mobile Computing (TMC), 2023, 2024
- IEEE Transactions on Knowledge Discovery from Data, 2023
- ACM Journal on Emerging Technologies in Computing Systems, 2021
- IEEE Transactions on Industrial Informatics, 2024

Panel Reviewer

- NSF SaTc Hardware track, 2023

Chair

- Sponsorship & Exhibits Chair of the EAI SmartSP 2023 Conference.

Tutorials

- “Adversarial Input Manipulation Attacks against Deep Learning Applications”, UF-TH Summer AI Security Training sessions, 2018
- Helping down-scaling audio recognition model into small one using tensorflow-lite and deploy it in MSP432 board for AI Lab MicroP 2, 2020

Member

- ACM Member 2022 -
- IEEE Member 2022 -

PRESENTATIONS

Oral Presentations

- “Adversarial examples against the deep learning based network intrusion detection systems”, in IEEE Military Communications Conference (MILCOM), Los Angeles, USA, Oct 2018
- “Robust adversarial objects against deep learning models”, in AAAI Conference on Artificial Intelligence, New York, USA, Feb 2020
- “Robust Roadside Physical Adversarial Attack Against Deep Learning in Lidar Perception Modules”, in ACM Asia Conference on Computer and Communications Security (AsiaCCS), Hongkong, China, June 2021

- “3D-Adv: Black-Box Physical Adversarial Attacks against Deep Learning Models through 3D Sensors”, in Design Automation Conference (DAC), San Francisco, USA, Dec 2021
- “LLM4SecHW: Leveraging domain-specific large language model for hardware debugging”, 2023 Asian Hardware Oriented Security and Trust Symposium (AsianHOST), 2023.

Poster Presentations

- “Beyond Digital Domain: Fooling Deep Learning Based Recognition System in Physical World”, in AAAI Conference on Artificial Intelligence, New York, USA, Feb 2020

TEACHING EXPERIENCES

EE4800&5900 - AI Engineeing Applications *MTU Spring 2023, 2024*
Instructor of the course. Answering student’s questions, teaching lessons, recording demos,

EE4173 - Computer System Engineering and Performance *MTU Fall 2022, 2023, 2024*
Instructor of the course. Answering student’s questions, teaching lessons, recording demos,

EEL4745C - Microprocessor Applications *UF Spring 2021*
Answering student’s questions, teaching lessons, recording demos, supervise lab experiments, assign grades and give quizzes.

Summer Undergraduate Research at Florida (SURF) *UF Summer 2021*
Supervising undergraduate student in researching activities, including hosting weekly meeting, checking progress, selecting research topics, providing reading materials and answering questions.

RESEARCH EXPERIENCES

Assistant Professor

- At the Michigan Technology University, Houghton, MI, US *Fall 2022 - Present*

Graduate Research Assistant

- At the University of Florida, Gainesville, FL, US *Fall 2016 - 2022*
- At the University of Science and Technology of China (USTC), Hefei, China *Fall 2013 - Summer 2016*

HONORS

- Student Travel grant from University of Florida to attend the MILCOM 2018, Los Angeles.
- Student Travel grant from University of Florida to attend the AAAI 2020, New York.
- Student Travel grant from University of Florida to attend the Design Automation Conference (DAC) 2021, San Francisco.

COURSES

Network Science and Applications; Noise in Linear Systems; Computer Communications; Digital Signal Processing; Computer Architecture; Wireless Communications; Machine Learning; Wireless Networks; Applied Cryptography; Queuing Theory/Data Communication; Online Pedagogy for Engineers; Multimedia Signal Processing; Wireless Multimedia; Multimedia Systems; Image and Video Processing; Software Engineering; Interactive Media Design and Production; Internet Protocols; Signal and System Theorem; Matrix Theory And Methods; Probability Theory and Stochastic Process

SKILLS

Verilog; C/C++ Language (including the developing programs in embedded system, such as ARM); MATLAB; Python; Java; Latex; Web-programming (PHP); Photoshop; Caffe; PyTorch; Tensorflow; Tensorflow-lite; Unity engine; 3D modeling and printing related software and devices; Network simulation.