Yanan Guo

Address: 250 Hutchison Rd, Rochester, NY 14620
Mobile: +1 412-773-0553
E-mail: yanan.guo@rochester.edu
Home Page: yananguo.com

Professional Experience

University of Rochester — Rochester, NY
Assistant Professor — July 2024 - Present

NVIDIA — Santa Clara, CA
Hardware Security Intern — May 2022 - August 2022

NIO — San Jose, CA
Cybersecurity Consultant Intern — February 2021 - July 2021

Education

University of Pittsburgh — Pittsburgh, PA
Ph.D. in Electrical and Computer Engineering — 2024
M.S. in Electrical and Computer Engineering — 2020
Ph.D. Thesis: Cache Side Channel Attacks on Modern Processors
Advisor: Prof. Jun Yang

Xidian University — Xi'an, China
B.S. in Telecommunications Engineering — 2018

Publications

Peer-reviewed Conference Papers

- Behind Bars: A Side-Channel Attack on NVIDIA MIG Cache Partitioning Using Memory Barriers
  Cheng Gu, Reese Levine, Zhenkai Zhang, Tyler Sorensen, and **Yanan Guo**
  35th USENIX Security Symposium ***(USENIX Security'26)***
- CuSafe: Capturing Memory Corruption on NVIDIA GPUs
  Hongyi Lu, Fengwei Zhang, Zhenkai Zhang, Shuai Wang, and **Yanan Guo**
  35th USENIX Security Symposium ***(USENIX Security'26)***
- Exploiting TLBs in Virtualized GPUs for Cross-VM Side-Channel Attacks
  Hongyue Jin, **Yanan Guo**, and Zhenkai Zhang
  The Network and Distributed System Security Symposium 2026. ***(NDSS'26)***
- Demystifying and Exploiting ASLR on NVIDIA GPUs
  Ruofan Zhu, Ganhao Chen, Wenbo Shen, Lyuye Zhang, Dakun Shen, Rui Chang, and **Yanan Guo**
  47th IEEE Symposium on Security and Privacy. ***(S&P'26)***
- Chekhov's Gun: Uncovering Hidden Risks in macOS Application-Sandboxed PID-Domain Services
  Minghao Lin, Jiaxun Zhu, Tingting Yin, Zechao Cai, Guanxing Wen, **Yanan Guo**, and Mengyuan Li
  32nd ACM Conference on Computer and Communications Security. ***(CCS'25)***
- Security and Performance Implications of GPU Cache Eviction Priority Hints
  Qizhong Wang, Xiangyue Huang, **Yanan Guo**, and Yuanchao Xu
  58th IEEE/ACM International Symposium on Microarchitecture. ***(MICRO'25)***
- SCREME: A Scalable Framework for Resilient Memory Design
  Fan Li, Mimi Xie, **Yanan Guo**, Huize Li and Xin Xin
  34th ACM/IEEE International Conference on Parallel Architectures and Compilation Techniques. ***(PACT'25)***

- GPU Memory Exploitation for Fun and Profit
  Yanan Guo*, Zhenkai Zhang*, and Jun Yang
  33rd USENIX Security Symposium ***(USENIX Security'24)***
- Invalidate+Compare: A Timer-Free GPU Cache Attack Primitive
  Zhenkai Zhang, Kunbei Cai, **Yanan Guo**, Fan Yao, and Xing Gao
  33rd USENIX Security Symposium ***(USENIX Security'24)***
- Integrated Qubit Reuse and Circuit Cutting for Large Quantum Circuit Evaluation
  Aditya Pawar, Yingheng Li, Zewei Mo, **Yanan Guo**, Youtao Zhang, Xulong Tang, and Jun Yang
  30th ACM International Conference on Architectural Support for Programming Languages and Operating Systems ***(ASPLOS'24)***
- RTT-UAF: Reuse Time Tracking for Use-After-Free Detection
  Yubo Du, **Yanan Guo**, Youtao Zhang, and Jun Yang
  38th ACM International Conference on Supercomputing ***(ICS'24)***
- Uncore Encore: Covert Channels Exploiting Uncore Frequency Scaling
  Yanan Guo*, Dingyuan Cao*, Xin Xin, Youtao Zhang, and Jun Yang
  56th IEEE/ACM International Symposium on Microarchitecture. ***(MICRO'23)***
- IDYLL: Enhancing Page Translation in Multi-GPUs via Light Weight PTE Invalidations
  Bingyao Li, **Yanan Guo**, Yueqi Wang, Aamer Jaleel, Jun Yang, and Xulong Tang
  56th IEEE/ACM International Symposium on Microarchitecture. ***(MICRO'23)***
- Understanding and Defending Patch-Based Adversarial Attacks for Vision Transformer
  Liang Liu, **Yanan Guo**, Youtao Zhang, and Jun Yang
  40th International Conference on Machine Learning. ***(ICML'23)***
- Orchestrating Measurement-Based Quantum Computation over Photonic Quantum Processors
  Yingheng Li, Aditya Pawar, Mohadeseh Azari, **Yanan Guo**, Youtao Zhang, Jun Yang, Kaushik Parasuram Seshadreesan, and Xulong Tang
  60th ACM/IEEE Design Automation Conference. ***(DAC'23)***
- Leaky Way: A Conflict-Based Cache Covert Channel Bypassing Set Associativity
  Yanan Guo, Xin Xin, Youtao Zhang, and Jun Yang
  55th IEEE/ACM International Symposium on Microarchitecture. ***(MICRO'22)***
- Adversarial Prefetch: New Cross-Core Cache Side Channel Attacks
  Yanan Guo, Andrew Zigerelli, Youtao Zhang, and Jun Yang
  43rd IEEE Symposium on Security and Privacy. ***(S&P'22)***
  Shortlisted for Top Picks in Hardware and Embedded Security 2023.
- Q-GPU: A Recipe of Optimizations for Quantum Circuit Simulation Using GPUs
  Yilun Zhao, **Yanan Guo**, Yuan Yao, Amanda Dumi, Devin Mulvey, Shiv Upadhyay, Youtao Zhang, Kenneth Jordan, Jun Yang, and Xulong Tang
  28th IEEE International Symposium on High-Performance Computer Architecture. ***(HPCA'22)***
- Performance-Enhanced Integrity Verification for Large Memories
  Yanan Guo, Andrew Zigerelli, Yueqiang Cheng, Youtao Zhang, and Jun Yang
  2021 IEEE International Symposium on Secure and Private Execution Environment Design. ***(SEED'21)***
- SAM: Accelerating Strided Memory Accesses
  Xin Xin, **Yanan Guo**, Youtao Zhang, and Jun Yang
  54th IEEE/ACM International Symposium on Microarchitecture. ***(MICRO'21)***
- ModelShield: A Generic and Portable Framework Extension for Defending Bit-Flip Based Adversarial Weight Attacks
  Yanan Guo, Liang Liu, Yueqiang Cheng, Youtao Zhang, and Jun Yang
  39th IEEE International Conference on Computer Design. ***(ICCD'21)***
- IVcache: Defending Cache Side Channel Attacks via Invisible Accesses
  Yanan Guo, Andrew Zigerelli, Youtao Zhang, and Jun Yang
  31st Great Lakes Symposium on VLSI. ***(GLSVLSI'21)***

Journal Articles

- Generating Robust DNN with Resistance to Bit-Flip Based Adversarial Weight Attack
  Liang Liu, **Yanan Guo**, Yueqiang Cheng, Youtao Zhang, and Jun Yang
  IEEE Transactions on Computers, 72(2). ***(TC'22)***
  TC Featured Paper of the Month.

Posters & Workshops

- Adversarial Attacks on Adaptive Cruise Control Systems
  Yanan Guo, Takami Sato, Yulong Cao, Qi Alfred Chen, and Yueqiang Cheng
  IEEE/ACM Workshop on the Internet of Safe Things co-located with Cyber-Physical Systems and Internet of Things Week 2023. ***(SafeThings'23)***
- Prefetch-Based Cache Side Channel Attacks
  Yanan Guo, Andrew Zigerelli, Youtao Zhang, and Jun Yang
  Career Workshop for Inclusion and Diversity in Computer Architecture co-located with 55th IEEE/ACM International Symposium on Microarchitecture. ***(CWIDCA'22)***

External Funding

- NSF Award: CICI: UCSS: Securing GPU Computing for AI-Driven Scientific Workflows
  PI: Yanan Guo. Amount: $599,943.00
- Research Gift from Hydrox AI.
  PI: Yanan Guo. Amount: $50,000.00

Teaching Experience

Instructor, University of Rochester — Rochester, NY
CSC 276 - Computer Architecture and Security — Fall 2025
CSC 252 - Computer Organization — Fall 2024, Fall 2025

Teaching Assistant, University of Pittsburgh — Pittsburgh, PA
ECE 1541 - Introduction to Computer Architecture — Spring 2020, Spring 2019
ECE 0401 - Analytical Methods — Fall 2019
ECE 1552 - Signals and Systems Analysis — Fall 2018

Guest Lecturer, University of Pittsburgh — Pittsburgh, PA
ECE 2162 - Computer Architecture — Fall 2021
ECE 3162 - Advanced Computer Architecture — Spring 2020

Invited Talks

Threads of Trouble: Unveiling GPU Hardware and Software Security Flaws
SC 2025 — 2025

Behind the Pixels: Unveiling GPU Hardware and Software Security Flaws
Intel — 2025
Rochester Institute of Technology — 2025
Temple University — 2025
UC Santa Cruz — 2024

Speeding into Trouble: Side Channel Attacks on Modern Processors
WISE 2024 — 2024

GPU Memory Exploitation for Fun and Profit
USENIX Security 2024 — 2024

Leaky Hardware: Side Channel Attacks on Modern Processors
ByteDance 2023

Adversarial Prefetch: New Cross-Core Cache Side Channel Attacks
Top Picks in Hardware and Embedded Security 2023 2023
NVIDIA 2022
S&P 2022 2022

Adversarial Attacks on Adaptive Cruise Control Systems
SafeThings 2023 2023
NIO 2021

Cache Side Channel Attacks on Modern Processors
Southeast University 2022
University of Pittsburgh 2022

Leaky Way: A Conflict-Based Cache Covert Channel Bypassing Set Associativity
MICRO 2022 2022

Prefetch-Based Cache Side Channel Attacks
CWIDCA 2022 2022

Q-GPU: A Recipe of Optimizations for Quantum Circuit Simulation Using GPUs
HPCA 2022 2022

ModelShield: A Generic and Portable Framework Extension for Defending Bit-Flip Based Adversarial Weight Attacks
ICCD 2021 2021

Performance-Enhanced Integrity Verification for Large Memories
SEED 2021 2021

IVcache: Defending Cache Side Channel Attacks via Invisible Accesses
GLSVLSI 2021 2021

Mentoring Experience

Ph.D. students:

Cheng Gu at the University of Rochester
Yihan Jin at the University of Rochester
Yubo Du at the University of Pittsburgh, with Prof. Jun Yang

Undergraduate students:

Luke He, UG student at the University of Rochester
Chengrui Wang, UG student at the University of Rochester
Jeffery Li, UG student at the University of Rochester

Honors & Awards

Best Ph.D. Dissertation Award from IEEE HOST 2025
Top Picks in Hardware and Embedded Security (Shortlisted) 2023
University of Pittsburgh Travel Grant 2022
MICRO Travel Grant 2022
S&P Travel Grant 2022
Outstanding Graduate of Xidian University (Top 1%) 2018
China National Scholarship (Top 1%) 2017

Academic Service

Program Committee

ASPLOS 2026, USENIX Security 2026, HPCA 2026, CCS 2026

ISCA 2025, HPCA 2025, GLSVLSI 2025

SEED 2024, GLSVLSI 2024, HASP 2024

External Program Committee

MICRO 2025, MICRO 2024

Journal Reviewer

IEEE Transactions on Dependable and Secure Computing (TDSC)

IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD)