Yanan (Lana) Guo

Address: 3700 O'Hara St, Pittsburgh, PA 15213
Mobile: +1 412-773-0553
E-mail: yag45@pitt.edu
Home Page: yananguo.com

Research Interests

My research interests lie in computer architecture and cybersecurity, with a focus on the following areas:

- Side channel attacks and countermeasures.
- Memory encryption and authentication.
- Memory exploits and defenses.

I also have research experience in various areas of computer architecture, including GPU memory optimization.

Education

University of Pittsburgh Pittsburgh, PA
Ph.D. in Electrical and Computer Engineering August 2018 - April 2024 *(expected)*
M.S. in Electrical and Computer Engineering August 2018 - April 2020

Ph.D. Thesis: Side Channel Attacks on Modern Processors
Advisor: Prof. Jun Yang

Xidian University Xi'an, China
B.S. in Telecommunications Engineering August 2014 - June 2018

Publications

Peer-reviewed Conference Papers

1. 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)***
2. 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)***
3. 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)***
4. 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)***
5. 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)***
6. 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.
7. 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)***

8. 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)***

9. SAM: Accelerating Strided Memory Accesses
Xin Xin, **Yanan Guo**, Youtao Zhang, and Jun Yang
54th IEEE/ACM International Symposium on Microarchitecture. ***(MICRO'21)***

10. 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)***

11. 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

1. 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

1. 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)***

2. 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)***

Ongoing Research

1. GPU Memory Exploitation for Fun and Profit
Yanan Guo, Zhenkai Zhang, and Jun Yang
Under submission, developed the first GPU return-oriented programming attack.

2. Invalidate+Compare: A Timer-Free GPU Cache Attack Primitive
Zhenkai Zhang, Kunbei Cai, **Yanan Guo**, Fan Yao, and Xing Gao
Under submission, developed the first GPU timer-free cache attack.

Professional Experience

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

NIO — San Jose, CA
Research Intern — February 2021 - July 2021

Teaching Experience

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

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

Yubo Du, Ph.D. student at the University of Pittsburgh, with Prof. Jun Yang

Liang Liu, Ph.D. student at the University of Pittsburgh, with Prof. Jun Yang

Aditya Pawar, Ph.D. student at the University of Pittsburgh, with Prof. Youtao Zhang

Kaiwen Zhao, Ph.D. student at the University of Pittsburgh, with Prof. Xulong Tang

Landon Colaresi, high school student at the Pittsburgh Allderdice High School, with Prof. Jun Yang

Honors & Awards

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
SEED 2024

Secondary Reviewer
ASPLOS 2023, ISCA 2023, MICRO 2023, HPCA 2024

Volunteer
Student Assistant: MICRO 2020

References

Prof. Jun Yang
Department of Electrical and
Computer Engineering
University of Pittsburgh
Email: juy9@pitt.edu

Prof. Wenjie Xiong
Bradley Department of
Electrical and Computer Engineering
Virginia Tech
Email: wenjiex@vt.edu

Prof. Riccardo Paccagnella
Software and Societal
Systems Department
Carnegie Mellon University
Email: rpaccagn@cs.cmu.edu

Prof. Youtao Zhang
Department of Computer Science
University of Pittsburgh
Email: zhangyt@cs.pitt.edu

Prof. Yuval Yarom
Computer Science
Ruhr University Bochum
Email: yuval.yarom@rub.de

Dr. Aamer Jaleel
NVIDIA Research
Email: ajaleel@nvidia.com