Wenjie Xiong

Assistant Professor
The Bradley Department of Electrical and Computer Engineering
Virginia Tech

E-mail: wenjiex@vt.edu
Website: https://computing.ece.vt.edu/~wenjiex/

Last update: Sept. 2023.

BIOGRAPHICAL NOTE

Wenjie Xiong is an Assistant Professor at Virginia Tech since Jan 2022. She was a postdoctoral researcher at Meta (formerly "Facebook") AI Research. She received her Ph.D. in the Department of Electrical Engineering at Yale University in May 2020, advised by Prof. Jakub Szefer. Her research interests are in computer architecture and hardware security, where she leverages hardware features to enhance the security of computer systems as well as identify and mitigate security vulnerabilities that are rooted in the hardware designs. Her work on covert channel attacks on cache replacement states was selected as an Honorable Mention of IEEE Micro Top Picks 2021 and the featured paper of IEEE Transactions on Computers (TC). Her earlier work on run-time accessible DRAM PUFs was selected as the Top Picks in Hardware and Embedded Security 2019.

Education

Yale University, New Haven, CT, USA

Ph.D., Electrical Engineering **2020**
M.Phil., Electrical Engineering **2017**
M.S., Electrical Engineering **2016**

Advisor: *Prof.* Jakub Szefer
Thesis: Hardware Security in DRAMs and Processor Caches

Peking University, Beijing, China

B.S., Microelectronics Thesis: Microelectrode and Circuit for Peripheral Nerve Stimulation **2014**
B.S., Psychology **2014**

Professional Experience

Assistant Professor **1/2022 – Present**
CCI fellow
The Bradley Department of Electrical and Computer Engineering
Virginia Tech, Blacksburg, VA

Postdoctoral Researcher **8/2020 – Present**
Meta AI (previously Facebook), Cambridge, MA

Postdoctoral Associate **6/2020 – 7/2020**
Yale University, New Haven, CT

Security Research Intern **6/2018 – 8/2018**
Intel Labs, Hillsboro, OR
"Microarchitecture level mitigation of speculative timing side-channel attacks in cache and TLB."

Security Research Intern **6/2017 – 8/2017**
Intel Labs, Hillsboro, OR
"Data integrity in memory with low bandwidth overhead."

Graduate Researcher **11/2016 – 12/2016**
TU Darmstadt, Germany
"Rowhammer DRAM PUF."

Selected Honors and Awards

- Featured Paper in the April 2021 issue of IEEE Transactions on Computers (TC) 2021
- Honorable Mention of IEEE Micro Top Picks 2021
- Top Picks in Hardware and Embedded Security 2021
- Top Picks in Hardware and Embedded Security 2019
- Participant of 3rd Heidelberg Laureate Forum 2015
- Microsoft Research Graduate Women's Scholars 2015
- National Scholarship, China 2013
- Merit Student of Peking University 2012
- Wusi Scholarship of Peking University 2011
- Merit Student of Zhejiang Province 2010

Publications

Peer-reviewed Publications

1. Maximilian Lam, Jeff Johnson, **Wenjie Xiong**, Kiwan Maeng, Udit Gupta, Minsoo Rhu, Hsien-Hsin S. Lee, Vijay Janapa Reddi, Gu-Yeon Wei, David Brooks, and G. Edward Suh "GPU-based Private Information Retrieval for On-Device Machine Learning Inference" in Proceedings of the International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS), 2024
2. Wenxuan Zeng, Meng Li, **Wenjie Xiong**, Tong Tong, Wen-jie Lu, Jin Tan, Runsheng Wang, and Ru Huang "MPCViT: Searching for Accurate and Efficient MPC-Friendly Vision Transformer with Heterogeneous Attention" in International Conference on Computer Vision (ICCV), 2023
3. Shuwen Deng, Wenjie Xiong, and Jakub Szefer "Secure TLBs" in IEEE Design & Test, 2023
4. Sanjay Kariyappa, Chuan Guo, Kiwan Maeng, **Wenjie Xiong**, G. Edward Suh, Moinuddin K Qureshi, and Hsien-Hsin S. Lee "Cocktail Party Attack: Breaking Aggregation-Based Privacy in Federated Learning using Independent Component Analysis" in Proceedings of The International Conference on Machine Learning (ICML), 2023.
5. Jiaxun Cui, Xiaomeng Yang[†], Mulong Luo[†], Geunbae Lee[†], Peter Stone, Hsien-Hsin S. Lee, Benjamin Lee, Edward Suh, **Wenjie Xiong**[‡], Yuandong Tian[‡] "MACTA: A Multi-agent Reinforcement Learning Approach for Cache Timing Attacks and Detection" in Proceedings of the 11th International Conference on Learning Representations (ICLR), 2023. [†]Equal Second-author Contribution, [‡]Equal Supervising
6. Mulong Luo[†], **Wenjie Xiong**[†], John Lee, Yueying Li, Xiaomeng Yang, Yuandong Tian, Amy Zhang, Hsien-Hsin Sean Lee, and G. Edward Suh. "AutoCAT: Reinforcement Learning for Automated Exploration of Cache-Timing Attacks" to be appear in Proceedings of the 29th IEEE International Symposium on High Performance Computer Architecture (HPCA), 2023. [†] The authors contributed equally.
7. Hanieh Hashemi, **Wenjie Xiong**, Liu Ke, Kiwan Maeng, Murali Annavaram, G. Edward Suh, and Hsien-Hsin Lee, "Private Data Leakage via Exploiting Access Patterns of Sparse Features in Deep Learning-based Recommendation Systems", Workshop on Trustworthy and Socially Responsible Machine Learning (TSRML), December 2022.
8. Ferhat Erata, Shuwen Deng, Faisal Zaghloul, **Wenjie Xiong**, Onur Demir, and Jakub Szefer, "Survey of Approaches and Techniques for Security Verification of Computer Systems", in Journal on Emerging Technologies in Computing Systems, 2022.
9. Yuan Liang, Xing Gao, Kun Sun, **Wenjie Xiong**, and Haining Wang, "An Investigation on Data Center Cooling Systems Using FPGA-based Temperature Side Channels" in Proceedings of the 41st International Symposium on Reliable Distributed Systems (SRDS), Sep 2022.
10. Yongqin Wang, G. Edward Suh, **Wenjie Xiong**, Benjamin Lefaudeux, Brian Knott, Murali Annavaram, Hsien-Hsin S. Lee, "Characterization of MPC-based Private Inferences for Transformer-based Models", to appear in Proceedings of the IEEE International Symposium on Performance Analysis of Systems and Software (ISPASS), May 2022.
11. **Wenjie Xiong**, Liu Ke, Dimitrije Jankov, Michael Kounavis, Xiaochen Wang, Eric Northup, Jie Amy Yang, Bilge Acun, Carole-Jean Wu, Ping Tak Peter Tang, G. Edward Suh, Xuan Zhang, and Hsien-Hsin S. Lee, "SecNDP: Secure Near-Data Processing with Untrusted Memory", Proceedings of the 28th IEEE International Symposium on High Performance Computer Architecture (HPCA), April 2022.

12. Yongqin Wang, G. Edward Suh, **Wenjie Xiong**, Brian Knott, Benjamin Lefaudeux, Murali Annavaram, and Hsien-Hsin Lee, "Characterizing and Improving MPC-based Private Inference for Transformer-based Models", NeurIPS 2021 Workshop on Privacy in Machine Learning, December 2021.
13. Shuwen Deng, Nikolay Matyunin, **Wenjie Xiong**, Stefan Katzenbeisser, and Jakub Szefer, "Evaluation of Cache Attacks on Arm Processors and Secure Caches", in IEEE Transactions on Computers, November 2021.
14. Shuwen Deng, **Wenjie Xiong**, and Jakub Szefer, "Secure TLBs", in Top Picks in Hardware and Embedded Security, November 2021.
15. **Wenjie Xiong**, and Jakub Szefer, "Survey of Transient Execution Attacks and their Mitigations", in ACM Computing Surveys, vol. 54, no. 3, Article 54, May 2021.
16. Shuwen Deng, **Wenjie Xiong**, and Jakub Szefer, "Understanding Insecurity of Processor Caches due to Cache Timing-Based Vulnerabilities", in IEEE Security & Privacy, vol. 19, no. 3, pp. 42-49, May-June 2021.
17. Shanquan Tian, Ilias Giechaskiel, **Wenjie Xiong**, and Jakub Szefer, "Cloud FPGA Cartography using PCIe Contention", in Proceedings of the International Symposium on Field-Programmable Custom Computing Machines (FCCM), May 2021.
18. **Wenjie Xiong**, André Schaller, Nikolaos A. Anagnostopoulos, Muhammad Umair Saleem, Sebastian Gabmeyer, Stefan Katzenbeisser, and Jakub Szefer, "DRAM PUFs in Commodity Devices", in IEEE Design & Test, 2021.
19. **Wenjie Xiong**, Stefan Katzenbeisser, and Jakub Szefer, "Leaking Information Through Cache LRU States in Commercial Processors and Secure Caches", in IEEE Transactions on Computers, vol. 70, no. 04, pp. 511-523, 2021. (**Featured Paper in the April 2021 issue**)
20. Shuwen Deng, **Wenjie Xiong**, and Jakub Szefer, "A Benchmark Suite for Evaluating Caches' Vulnerability to Timing Attacks", in Proceedings of the International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS), 2020.
21. Shanquan Tian, **Wenjie Xiong**, Ilias Giechaskiel, Kasper Rasmussen, and Jakub Szefer, "Fingerprinting Cloud FPGA Infrastructures", in Proceedings of the International Symposium on Field-Programmable Gate Arrays (FPGA), 2020.
22. **Wenjie Xiong**, and Jakub Szefer, "Leaking Information Through Cache LRU States", in Proceedings of the 26th International Symposium on High-Performance Computer Architecture (HPCA), 2020. (**IEEE Micro Top Picks 2021 Honorable Mention**)
23. **Wenjie Xiong**, André Schaller, Stefan Katzenbeisser, and Jakub Szefer, "Software Protection using Dynamic PUFs", in IEEE Transactions on Information Forensics and Security (TIFS), 2019.
24. Shuwen Deng, **Wenjie Xiong**, and Jakub Szefer, "Analysis of Secure Caches using a Three-Step Model for Timing-Based Attacks", in Journal of Hardware and Systems Security, 2019.
25. Shuai Chen, **Wenjie Xiong**, Yehan Xu, Bing Li, and Jakub Szefer, "Thermal Covert Channels Leveraging Package-On-Package DRAM", in Proceedings of the International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2019.
26. Shuwen Deng, **Wenjie Xiong**, and Jakub Szefer, "Secure TLBs", in Proceedings of the International Symposium on Computer Architecture (ISCA), 2019.
27. Shuwen Deng, Doğuhan Gümüşoğlu, **Wenjie Xiong**, Y. Serhan Gener, Onur Demir, and Jakub Szefer, "SecChisel Framework for Security Verification of Secure Processor Architectures", in Proceedings of the Workshop on Hardware and Architectural Support for Security and Privacy (HASP), 2019.
28. **Wenjie Xiong**, André Schaller, Stefan Katzenbeisser, and Jakub Szefer, "Dynamic Physically Unclonable Functions", in Proceedings of the Great Lakes Symposium on VLSI (GLSVLSI), 2019.
29. **Wenjie Xiong**, Nikolaos Athanasios Anagnostopoulos, André Schaller, Stefan Katzenbeisser, and Jakub Szefer, "Spying on Temperature using DRAM", in Proceedings of the Design, Automation, and Test in Europe (DATE), 2019.
30. Nikolaos Athanasios Anagnostopoulos, Tolga Arul, Yufan Fan, Christian Hatzfeld, André Schaller, **Wenjie Xiong**, Manishkumar Jain, Muhammad Umair Saleem, Jan Lotichius, Sebastian Gabmeyer, Jakub Szefer, and Stefan Katzenbeisser, "Intrinsic Run-Time Row Hammer PUFs: Leveraging the Row Hammer Effect for Run-Time Cryptography and Improved Security", in Cryptography, 2(3), p.13, 2018.
31. Shuwen Deng, **Wenjie Xiong** and Jakub Szefer, "Cache Timing Side-Channel Vulnerability Checking with Computation Tree Logic", in Proceedings of the Workshop on Hardware and Architectural Support for Security and Privacy (HASP), 2018.

32. André Schaller†, **Wenjie Xiong**†, Nikolaos Athanasios Anagnostopoulos, Muhammad Umair Saleem, Sebastian Gabmeyer, Boris Skoric, Stefan Katzenbeisser, and Jakub Szefer, "Decay-Based DRAM PUFs in Commodity Devices", in IEEE Transactions on Dependable and Secure Computing (TDSC), 16(3), pp.462-475, 2019. † The authors contributed equally.
33. André Schaller, **Wenjie Xiong**, Nikolaos Athanasios Anagnostopoulos, Muhammad Umair Saleem, Sebastian Gabmeyer, Stefan Katzenbeisser, and Jakub Szefer, "Intrinsic Rowhammer PUFs: Leveraging the Rowhammer effect for improved security", in Proceedings of the International Symposium on Hardware Oriented Security and Trust (HOST), 2017. (**Best Student Paper Finalist**)
34. **Wenjie Xiong**, André Schaller, Nikolaos A. Anagnostopoulos, Muhammad Umair Saleem, Sebastian Gabmeyer, Stefan Katzenbeisser, and Jakub Szefer, "Run-time accessible DRAM PUFs in commodity devices", in Proceedings of the Conference on Cryptographic Hardware and Embedded Systems (CHES), 2016. (**Top Picks in Hardware and Embedded Security 2019**)
35. Huaiqiang Yu, **Wenjie Xiong**, Hongze Zhang, Wei Wang, and Zhihong Li, "A parylene self-locking cuff electrode for peripheral nerve stimulation and recording", in Journal of Microelectromechanical Systems, 23(5), pp.1025-1035, 2014.
36. Huaiqiang Yu, **Wenjie Xiong**, Hongze Zhang, Wei Wang, and Zhihong Li, "A cable-tie-type parylene cuff electrode for peripheral nerve interfaces", in IEEE 27th International Conference on Micro Electro Mechanical Systems (MEMS), 2014.
37. **Wen Jie Xiong**, Huai Qiang Yu, and Zhi Hong Li, "Design and Simulation of a Parylene-based Three-Dimensional Cuff Electrode for peripheral nerve stimulation", in Key Engineering Materials, 609, pp.1459-1463, 2014.
38. Linbo Shao, Li Wang, **Wenjie Xiong**, Xue-Feng Jiang, Qi-Fan Yang, and Yun-Feng Xiao, "Ultrahigh-Q, largely deformed microcavities coupled by a free-space laser beam", in Applied Physics Letters, 103(12), p.121102, 2013.

Technical Reports

- Onur Demir, **Wenjie Xiong**, Faisal Zaghloul, and Jakub Szefer, "Survey of Approaches for Security Verification of Hardware/Software Systems", IACR Cryptology ePrint Archive 2016 (2016): 846, Sep. 2016.

News

- **Wenjie Xiong**, and Jakub Szefer, "Memristive fingerprints prove key destruction", Nature Electronics 1(10), p.527, 2018.

Patent

- Kounavis, Michael, et al. "Security-oriented compression." U.S. Patent Application No. 16/674,346.

Presentations and Tutorials

- "RL for computer architecture and security", RL4CAS tutorial at ISCA, June, 2023.
- "Reinforcement Learning for Automated Exploration and Detection of Cache-Timing Attacks", Security & Trustworthy Data & Technology workshop, Virginia Tech, Apr. 2023.
- "Reinforcement Learning for Automated Exploration and Detection of Cache-Timing Attacks", Yale University, Feb. 2023.
- "Secure Data Processing in Heterogeneous Systems", Intel, Aug. 2022.
- "Secure Data Processing in Heterogeneous Systems", IBM, Jun. 2022.
- "Designing Secure Computing Systems: from caches to DRAMs", University of North Carolina at Chapel Hill, 2021.
- "Designing Secure Computing Systems: from caches to DRAMs", Virginia Tech, 2021.
- "Designing Secure Computing Systems: from caches to DRAMs", Arizona State University, 2021.
- "Run-time Accessible DRAM PUFs in Commodity Devices", at Top Picks in Hardware and Embedded Security, Westminster, CO, USA, Nov. 2019.
- Jakub Szefer, **Wenjie Xiong** and Shuwen Deng, Tutorial "Secure Processor Architectures in the Era of Spectre and Meltdown", at IEEE International Symposium on Hardware Oriented Security and Trust (HOST), May 2019.
- "Dynamic PUFs and Software Protection", CASLAB Day, at Yale University, May 2019.
- "Run-time Accessible DRAM PUFs in Commodity Devices", at TU Darmstadt, Nov. 2016.
- "Run-time Accessible DRAM PUFs in Commodity Devices", at Conference on Cryptographic Hardware and Embedded Systems (CHES), Santa Barbara, CA, USA, Aug. 2016.

Teaching

ECE5504 Computer Architecture Virginia Tech
2023 Fall: 60 students
ECE5504 Computer Architecture Virginia Tech
2022 Fall: 49 students
ECE2564 Embedded Systems Virginia Tech
2022 Spring: 98 students
EENG 201 Introduction to Computer Engineering Teaching Assistant, Yale University
2017 Spring and *2016 Spring*

Professional Service

Conference/Workshop Organizing

- Workshop and Program Chairs of International Workshop on Hardware and Architectural Support for Security and Privacy (HASP 2020),
- Proceedings co-Chair for the 41th IEEE International Conference on Computer Design (ICCD 2023),
- Organizer of Tutorial: (RL4CAS) Reinforcement Learning for Computer Architecture and Systems Research, with ISCA 2023,
- Publicity Chair for the 29th IEEE International Symposium on High-Performance Computer Architecture (HPCA 2023),
- Proceedings co-Chair for the 40th IEEE International Conference on Computer Design (ICCD 2022),
- Session Chair for session 1B: "Security I" in the 28th IEEE International Symposium on High-Performance Computer Architecture (HPCA-28),
- Publicity Chair for the 28th IEEE International Symposium on High-Performance Computer Architecture (HPCA 2022),
- Session Chair for session 1: "the eternal war of side channels" in the IEEE International Symposium on Secure and Private Execution Environment Design (SEED 2021),
- Publications Chair for the IEEE International Symposium on Secure and Private Execution Environment Design (SEED 2021),
- Proceedings co-Chair for the 39th IEEE International Conference on Computer Design (ICCD) 2021,
- Served on the Organizing Committee of Secure and Private Systems for machine Learning (SPSL) workshop, co-located with ISCA 2021.

Paper Review

Served on the Program Committees of the conferences/workshops:

- 29th Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS'24),
- Young Architect Workshop (YArch'23) ,
- ERC for the 50th International Symposium on Computer Architecture (ISCA'23),
- 28th Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS'23),
- Cryptographic Hardware and Embedded Systems 2023 (TCHES),
- Cryptographic Hardware and Embedded Systems 2022 (TCHES),
- Young Architect Workshop (YArch'22) ,
- ERC for Architectural Support for Programming Languages and Operating Systems 2022 (ASPLOS'22),
- the 39th IEEE International Conference on Computer Design (ICCD 2021),
- ERC for Architectural Support for Programming Languages and Operating Systems 2021 (ASPLOS'21),
- 9th International Workshop on Hardware and Architectural Support for Security and Privacy (HASP 2020),
- 8th International Workshop on Hardware and Architectural Support for Security and Privacy (HASP 2019).

Served as a reviewer for journals:

- ACM Computing Surveys (CSUR),
- IEEE Computer Architecture Letters (CAL),
- Design Automation for Embedded Systems (DAEM),
- IEEE Security & Privacy,

- IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD),
- IEEE Transactions on Circuits and Systems I,
- IEEE Transactions on Computers (TC),
- Advanced Electronic Materials,
- Design Automation for Embedded Systems (DAEM),
- ACM Transactions on Architecture and Code Optimization (TACO),
- IEEE Design & Test,
- Nature Electronics,
- IEEE Access,
- International Journal of Circuit Theory and Applications (CTA),
- IEEE Consumer Electronics Magazine,
- ACM Transactions on Embedded Computing Systems (TECS),
- IEEE Transactions on Dependable and Secure Computing (TDSC).

Diversity and Inclusion Events

- Rising Stars in EECS 2020
- Career Workshop for Women and Minorities in Computer Architecture (CWWMCA) 2020
- Career Workshop for Women and Minorities in Computer Architecture (CWWMCA) 2019
- Improving the Diversity of Faculty in Electrical and Computer Engineering (iREDEFINE ECE) 2018
- Equity in the Job Search at Yale 2018
- Workshop for Women in Hardware and Systems Security (WISE) 2017
- CRA-W Grad Cohort 2016
- Workshop for women and underrepresented groups interested in computer security research (GREPSEC) II 2015