SHUWEN DENG

Address: Yale University, 10 Hilllhouse Avenue, New Haven, CT, 06511 Email: shuwen.deng@aya.yale.edu
Webpage: https://caslab.csl.yale.edu/~shuwen/ Phone Number: +1 (475) 655-5336

RESEARCH INTERESTS

My research interests lie in computer architecture and security, especially focusing on developing and verifying secure processor microarchitectures by building side-channel vulnerability checking schemes and security attack analysis, as well as proposing tools for practical and scalable security hardware and architectures defense and verification.

EDUCATION

Yale University August 2016 - May 2022
Ph.D. in Electrical Engineering
Research Assistant, Computer Architecture and Security (CAS) Lab.

Yale University August 2016 - June 2019
M.S., M.Phil. in Electrical Engineering

Shanghai Jiao Tong University September 2012 - June 2016
B.S. in Microelectronics

SELECTED HONORS AND AWARDS

- **Top Picks** in Hardware and Embedded Security — December 2021
- Selected for 2020 UC Berkeley Rising Stars in EECS Workshop — November 2020
- **2020 Google Fellowship in Privacy and Security** — April 2020
- **Elihu Elias Dickerman Fellowship** — Jan 2020
- Security and Privacy IEEE Symposium Student Scholarship — May 2018
- Yale New Student Fellowship — September 2016
- **Merit Student of Shanghai, China** (Top **1%**) — June 2016
- **China National Scholarship** (Top **1%**) — September 2015
- Academic Excellence Scholarship (**First-Class**) (Top **1%**) — September 2015
- **Meritorious Winner**, ICM/MCM American College Students' Mathematical Contest in Modeling — February 2015
- Neil Shen Scholarship (**20** among **12,000** SJTU undergraduates) — July 2014

PUBLICATIONS

- **Shuwen Deng**, Bowen Huang, and Jakub Szefer. "Leaky Frontends: Micro-Op Cache and Processor Frontend Vulnerabilities". Accepted by the the 28th IEEE International Symposium on High-Performance Computer Architecture (**HPCA**), 2022.
- **Shuwen Deng**, Nikolay Matyunin, Wenjie Xiong, Stefan Katzenbeisser, and Jakub Szefer. "Evaluation of Cache Attacks on Arm Processors and Secure Caches". Accepted by IEEE Transactions on Computers (**IEEE TC**), 2021.

- **Shuwen Deng** and Jakub Szefer. "New Predictor-Based Attacks in Processors". Accepted by the 58th Design Automation Conference (**DAC**), 2021. Acceptance rate of **23%**.
- **Shuwen Deng**, Wenjie Xiong, and Jakub Szefer. "A Benchmark Suite for Evaluating Caches' Vulnerability to Timing Attacks". Proceedings of the 25th International Conference on Architectural Support for Programming Languages and Operating Systems (**ASPLOS**), 2020. Acceptance rate of **18.10%**.
- **Shuwen Deng**, Wenjie Xiong, and Jakub Szefer. "Secure TLBs". Proceedings of the 46th International Symposium on Computer Architecture (**ISCA**), 2019. Acceptance rate of **16.98%**. **(Top Picks in Hardware and Embedded Security 2021)**
- **Shuwen Deng**, Wenjie Xiong, and Jakub Szefer. "Understanding Insecurity of Processor Caches Due to Cache Timing-Based Vulnerabilities". In Journal of IEEE Security & Privacy, 2021.
- **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 (**JHSS**), 2019.
- **Shuwen Deng**, et al. "SecChisel Framework for Security Verification of Secure Processor Architectures". Proceedings of the 8th International Workshop on Hardware and Architectural Support for Security and Privacy (**HASP**), 2019.
- **Shuwen Deng**, Wenjie Xiong, and Jakub Szefer. "Cache Timing Side-Channel Vulnerability Checking with Computation Tree Logic". Proceedings of the 7th International Workshop on Hardware and Architectural Support for Security and Privacy (**HASP**), 2018.
- Ferhat Erata, **Shuwen Deng**, Faisal Zaghloul, Wenjie Xiong, Onur Demir, and Jakub Szefer, "Survey of Approaches and Techniques for Security Verification of Computer Systems". Journal on Emerging Technologies in Computing Systems, 2022.
- Allen Mi, **Shuwen Deng**, and Jakub Szefer, "Securing Reset Operations in NISQ Quantum Computers". Proceedings of the Conference on Computer and Communications Security (CCS), 2022.
- Allen Mi, **Shuwen Deng**, and Jakub Szefer. "Device- and Locality-Specific Fingerprinting of Shared NISQ Quantum Computers". the 10th International Workshop on Hardware and Architectural Support for Security and Privacy (**HASP**), 2021.
- Wen Wang, Bernhard Jungk, Julian Walde, **Shuwen Deng**, Naina Gupta, Jakub Szefer, and Ruben Niederhagen. "XMSS and Embedded Systems - XMSS Hardware Accelerators for RISC-V". Proceedings of the 34th International Conference on Selected Areas in Cryptography (**SAC**), 2019.
- Guoyong Shi, Hanbin Hu, and **Shuwen Deng**. "Topological Approach to Automatic Symbolic Macromodel Generation for Analog Integrated Circuits". ACM Transactions on Design Automation of Electronic Systems (**TODAES**) 22.3 (2017):47.

PROFESSIONAL EXPERIENCE

- **Research Intern**, ARG, NVIDIA Research, New Haven, CT, Remote June - August 2021
  Study of high-speed and high-fidelity GPU covert-channel attacks under multi-tenancy features.
- **Security Research Intern**, Intel Labs, New Haven, CT, Remote June - August 2020
  Formal verification of Security Protocol and Data Model standard.
- **Visiting Student**, Princeton University, Princeton, NJ June - July 2019
  Under Prof. Ruby B. Lee's group, secure architecture design and evaluation.

TEACHING AND ADVISING EXPERIENCE

- **Research Advising**, Yale University, New Haven, CT, USA — January 2021 - Now
  Allen Mi, Bachelor's Thesis
- **Teaching Fellow**, Yale University, New Haven, CT, USA — January 2019 - May 2019
  Introduction to Computer Engineering (EE201).
- **Teaching Fellow**, Yale University, New Haven, CT, USA — January 2018 - May 2018
  Introduction to Computer Engineering (EE201).
- **Research Advising**, Yale University, New Haven, CT, USA — June 2017 - August 2017
  Corine Lu, Bachelor's Thesis

RESEARCH EXPERIENCE

- Micro-Op Cache and Processor Frontend Vulnerabilities, lead student — 2020 - Now
- Fingerprinting and Crosstalk on Quantum Computers, participating student — 2021 - Now
- Value Predictor Based Attacks and Defenses, lead student — 2020 - Now
- Cache Timing-Based Side-Channel Vulnerability Checking and Secure Caches Verification, lead student — 2017 - Now
- TLB Timing-Based Side-Channel Vulnerability Modeling, Secure TLBs Design and Evaluation, lead student — 2018 - 2020
- Language and Tool for Security Hardware Formal Verification, lead student — 2016 - 2019
- XMSS Accelerators for RISC-V, participating student — 2018 - 2019
- Design of Mini Dafny and SAT Solver, lead student, two-people group — 2017
- Design of Tiger Compiler, lead student, three-people group — 2017
- Design of a Five-Pipeline-Stage MIPS Processor, lead student, three-people group — 2014 - 2015

TUTORIAL

- Jakub Szefer, Wenjie Xiong, and **Shuwen Deng**, "Secure Processor Architectures in the Era of Spectre and Meltdown", responsible for the third part tutorial (about secure cache architectures) at IEEE International Symposium on Hardware Oriented Security and Trust (HOST) 2019.

PRESENTATIONS

- "Security Attacks and Defenses of the Micro-Op Cache and the Processor Frontend", talk for National Microelectronics Security Training Center (MEST), December 2021
- "Secure TLBs", virtual talk for research lab at Department of Computer Science of Peking University, December 2021
- "Value Predictor Attacks in Professors", virtual lightning talk, 7th Career Workshop for Inclusion and Diversity in Computer Architecture, October 2021
- "Zen of Security: Processor Microarchitecture Security Design and Verification", virtual talk on th third Youth Forum on the Next Generation Computer Sciences hosted by the Department of Computer Science and Technology of Peking University, October 2021

- "Secure Professor Caches", virtual talk for research lab at Research Institute of Information Technology of Tsinghua University, September 2021
- "Evaluation of Cache Attacks on Secure Caches", virtual SRC TECHCON, September 2021
- "Securing Modern Memory Systems: Secure TLBs, Caches and Beyond", virtual 2020 Rising Stars workshop, November 2020
- "Secure TLBs", virtual 2020 Google PhD Fellowship Summit, July 2020
- "A Benchmark Suite for Evaluating Caches' Vulnerability to Timing Attacks", virtual ASPLOS talk, March 2020
- "A Benchmark Suite for Evaluating Caches' Vulnerability to Timing Attacks", invited talk for Intel labs, January 2020
- "Secure TLBs", ISCA conference talk, AZ, USA, June 2019
- "SecChisel Framework for Security Verification of Secure Processor Architectures", SRC TECHCON 2019, TX, USA, September 2019
- "SecChisel Framework for Security Verification of Secure Processor Architectures", HASP workshop talk, AZ, USA, June 2019
- "Cache Timing Side-Channel Vulnerability Checking with Computation Tree Logic", invited talk for Intel labs, August 2018
- "Cache Timing Side-Channel Vulnerability Checking with Computation Tree Logic", HASP workshop talk, CA, USA, June 2018

SERVICE AND TECHNICAL REVIEWING

- Reviewer for IEEE Transactions on Dependable and Secure Computing — December 2021
- Hosting Computer Systems Seminars at Yale — February - May 2021
- Reviewer for ACM Digital Threats: Research and Practice — February - September 2021
- Reviewer for IEEE Transactions on Computers — September 2020
- Reviewer for IEEE Access — September 2019

HARDWARE DEMOS AND POSTERS

- "Value Predictor Attacks in Professors", virtual 7th Career Workshop for Inclusion and Diversity in Computer Architecture, October 2021
- "New Predictor-Based Attacks in Processors", virtual 2021 Google PhD Fellowship Summit, September 2021
- "RISC-V Secure Caches Demo on FPGA", hardware demo at IEEE International Symposium on Hardware Oriented Security and Trust (HOST), September 2019
- "Framework for Security Verification of Secure Processor Architectures", poster presentation at IEEE Symposium on Security and Privacy (S&P), May 2018
- "SecChisel: Language and Tool for Practical and Scalable Security Verification of Security-Aware Hardware Architectures", poster presentation at Women in Cybersecurity (WiCyS), April 2017