# Wenjie Xiong

(203)393 8968 • wenjie.xiong@yale.edu • http://caslab.csl.yale.edu/~wenjie
10 Hillhouse Avenue, Room 505, New Haven, CT 06511

## Research Interest

I am broadly interested in hardware security. I am working on designs of new Physically Unclonable Functions (PUFs), designs of schemes leveraging physical properties of hardware for new cryptographic and security applications, security verification of processor architectures, and analysis of attacks and mitigations of timing channels in caches and TLBs.

## Education

**Yale University** — **New Haven, CT, USA**
***Ph.D. Candidate & Master of Science in Electrical Engineering*** — *Aug. 2014 – present*
Department of Electrical Engineering
*Advisor: Prof.* Jakub Szefer

**Peking University** — **Beijing, China**
***Bachelor of Science in Microelectronics*** — *Sep. 2010 – Jul. 2014*
School of Electronics Engineering and Computer Science
*Cumulative GPA:* **3.76/4.0** (Rank: **4/45**), *Major GPA:* **3.86/4.0** (Rank: **3/45**)

**Peking University** — **Beijing, China**
***Bachelor of Science in Psychology*** — *Sep. 2010 – Jul. 2014*
Department of Psychology

## Publications

### Peer-reviewed Publications

- Shuwen Deng, **Wenjie Xiong**, and Jakub Szefer, "Secure TLBs", in Proceedings of the International Symposium on Computer Architecture (ISCA), June 2019.
- **Wenjie Xiong**, André Schaller, Stefan Katzenbeisser, and Jakub Szefer, "Dynamic Physically Unclonable Functions", in Proceedings of the Great Lakes Symposium on VLSI (GLSVLSI), May 2019.
- **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), March 2019.
- 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, vol. 2, no. 3, June 2018.
- 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), June 2018.
- 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), 2018.
- 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), May 2017. (Best Student Paper Finalist)
- **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), pp. 432-453, 2016.
- 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, no. 5 (2014): 1025-1035.

- 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), pp. 9-12, 2014.
- **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, vol. 609, pp. 1459-1463, 2014.
- 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, no. 12 (2013): 121102.

† The authors contributed equally to the work.

### Technical Reports

- Shuwen Deng, **Wenjie Xiong**, and Jakub Szefer, "Analysis of Secure Caches and Timing-Based Side-Channel Attacks", February 2019.
- Shuwen Deng, Doğuhan Gümüşoğlu, **Wenjie Xiong**, Y. Serhan Gener, Onur Demir, and Jakub Szefer. "SecChisel: Language and Tool for Practical and Scalable Security Verification of Security-Aware Hardware Architectures." IACR Cryptology ePrint Archive 2017 (2017): 193.
- 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.

### News

- **Wenjie Xiong**, and Jakub Szefer. "Memristive fingerprints prove key destruction." Nature Electronics 1.10 (2018): 527.

## Research Experience

Computer Architecture and Security Laboratory (CASLab), Yale University *Aug. 2014 – present*

**Practical DRAM PUFs in Commodity Devices and its Application**

*Advisors: Prof. Jakub Szefer and Prof. Stefan Katzenbeisser (TU Darmstadt, Germany)*

- Demonstrated a novel type of PUFs (physical unclonable functions) using DRAM (Dynamic Random Access Memory)
- Implemented two practical DRAM PUF access methods in firmware as well as a Linux kernel module in Intel Galileo and Pandaboard
- Designed and evaluated new authentication and key storage schemes based on the proposed DRAM PUFs
- Exploited inherent DRAM features for advanced cryptographic protocols
- Improved the DRAM PUF readout time with Rowhammer effect
- Designed schemes to protect user programs with the PUFs in the hardware at system runtime

**Security Modeling of Cache and TLBs**

*Advisor: Prof. Jakub Szefer*

- Formulated a three-step model of cache and TLB side channel attacks covering all possible cache and TLB timing-based side-channel vulnerabilities.
- Designed reduction rules and cache three-step simulator to automatically derive the exhaustive list of all the three steps which map to effective vulnerabilities.

**Security Verification of Processor Architectures**

*Advisors: Prof. Jakub Szefer and Prof. Onur Demir (Yeditepe University, Turkey)*

- Developed new methods and framework to model hardware and verify the security of processor architectures by adding new annotations in hardware description language, leveraging current functional verification tools

**Design and Simulation of Secure Architecture with DIFT**

*Advisor: Prof. Jakub Szefer*

- Designed and simulated a secure architecture with Dynamic Information Flow Tracking (DIFT) to protect database
- Implemented information flow tracking features into GEM5, which is an open-source simulator
- Tested and evaluated the DIFT approach to database computation protection
- Modified two database applications, SQLite and Redis, to demonstrate the usability of the architecture

Institute of Microelectronics, Peking University *Apr. 2012 – Jun. 2014*

**Design of Neural Stimulation System for Insect Cyborg (Senior Project)**

*Advisor: Prof. Zhihong Li*

- A new design of neural stimulation system for insect flight control.
- Designed and simulated the circuit, including digital logic, DC-DC converter, and output array in Cadence IC.

**Design, Simulation, Fabrication and Test of cuff electrodes**

*Advisor: Prof. Zhihong Li*

- Built 3D finite element model and Simulated electric field distribution of working cuff electrodes in COMSOL
- Fabrication: photolithography, oxygen plasma etching, wet etching of Si, $SiO_2$ and metals, Ni and Au electroplating

## Professional Experience

**Intel Labs, Hillsboro, OR, USA** Security Research Intern *Jun.- Aug. 2018*

"Micro-architecture level mitigation of speculative timing side channel attacks in cache and TLB"

Investigated existing Spectre-like attacks and analyzed each component of the attack and possible mitigation in micro-architecture. Implemented mitigation of speculative timing side channel attacks in cache and TLB in a cycle-accurate simulator and evaluated the performance overhead.

**Intel Labs, Hillsboro, OR, USA** Security Research Intern *Jun.- Aug. 2017*

"Data integrity in memory with minimal bandwidth overhead"

Evaluated bandwidth overhead of real-world workloads with functional simulator. Implemented algorithms in RTL and evaluated the delay and area overhead.

**TU Darmstadt, Germany** Graduate Researcher *Nov.- Dec. 2016*

Designed and evaluated rowhammer DRAM PUF.

## Teaching Experience

**EENG 201** Teaching Assistent, Introduction to Computer Engineering, Yale University *2017 Spring*

**EENG 201** Teaching Assistent, Introduction to Computer Engineering, Yale University *2016 Spring*

Topics include boolean algebra, digital design, and basic computer architecture principles. I assisted Prof. Szefer in preparing lab materials, leading lab sessions, and grading.

## Presentations

- "Run-time Accessible DRAM PUFs in Commodity Devices", TU Darmstadt, Nov. 2016
- "Run-time Accessible DRAM PUFs in Commodity Devices", CHES, Santa Barbara, CA, USA, Aug. 2016

## Service

- Reviewer for IEEE Transactions on Embedded Computing Systems (TECS)
- Reviewer for Nature Electronics
- Reviewer for IEEE Transactions on Dependable and Secure Computing (TDSC)
- Student Program Committee of 39th IEEE Symposium on Security and Privacy (S&P 2018)

## Selected Honors and Awards

- 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
- First Prize of High School Biology Olympiad, Zhejiang Province, China 2009