Gururaj Saileshwar *University of Toronto*

CONTACT

Dept of Computer Science, University of Toronto,
40 St. George Street, Room 4283
Toronto, ON M5S 2E4, Canada

☎ +1(470) 263-4332
✉ gururaj@cs.toronto.edu
https://gururaj-s.github.io/

EDUCATION

Georgia Institute of Technology, Atlanta, Georgia USA
Ph.D., Electrical and Computer Engineering, August 2022
Dissertation: "Architecting Secure Processor Caches"
Advisor: Moinuddin K. Qureshi

Indian Institute of Technology - Bombay (IIT-B), Mumbai, India
B.Tech. and M.Tech., Electrical Engineering, August 2014

RESEARCH

Interests **Computer Architecture and Systems Security:** Cache Side-channels, Transient Execution Attacks, Rowhammer Attacks and Memory Integrity, Software Reliability and Memory Safety.

Impact Published 12+ conference papers in top-tier venues in computer architecture (ISCA, MICRO, HPCA, ASPLOS) and security (USENIX Security, S&P (Oakland), CCS).

AWARDS AND HONORS

- ◇ **ACM-SIGMICRO Dissertation Award** (Honorable Mention) 2023
- ◇ **ACM-SIGARCH/IEEE-TCCA Outstanding Dissertation Award** (Hon. Mention) 2023
- ◇ **Best Paper Award, IEEE HPCA'23 Conference** 2023
  Joint work with Jeonghyun Woo (UBC) and Prashant Nair (UBC).
- ◇ **Best PhD Dissertation Award, IEEE Hardware Oriented Security & Trust** 2022
- ◇ **Distinguished Reviewer, Shadow PC, IEEE Security & Privacy'21 (Oakland)** 2021
  One of 7 honored out of 70+ Shadow PC; Invited to IEEE S&P'22 Program Committee
- ◇ **Awarded Georgia Tech Information Security & Privacy (IISP) Fellowship** 2021
  Awarded by Georgia Tech IISP for pursuing innovative cybersecurity research
- ◇ **Finalist at the Qualcomm Innovation Fellowship** (one of 43 finalists) 2021
- ◇ **Selected for 8th Heidelberg Laureate Forum** (one of 100 students worldwide) 2020
- ◇ **IEEE-Micro Top-Picks Honorable Mention** 2019
  Among Top-22 out of 200+ papers in top computer architecture conferences in 2018
- ◇ **Invited Speaker, FOCA Visioning Workshop at IBM Research** (one of 7 students) 2019
- ◇ **Finalist for Microsoft Ph.D. Fellowship** (one of 20 finalists from 600+ applicants) 2019
- ◇ **Finalist at the Qualcomm Innovation Fellowship** (one of 37 finalists) 2019
- ◇ **Awarded M&H Bourne Fellowship, Georgia Tech** (to exceptional new students) 2016
- ◇ **Recipient of Undergraduate Research Award, IIT-Bombay** 2013

Work Experience

Assistant Professor, University of Toronto, Computer Science Fall 2023 - Present
Assistant Professor, University of Toronto Mississauga, MCS Fall 2023 - Present
Tenure-track faculty leading a research group focused on hardware and systems security in the Department of Computer Science. Involved in undergraduate and graduate teaching in the areas of Computer Security and Computer Architecture.

Postdoctoral Researcher, NVIDIA Research, USA Fall 2022 - Summer 2023
In the Architecture Research Group, my research analyzed emerging security threats for CPUs, GPUs, and System on Chip components.

Graduate Research Assistant, Georgia Tech, USA Fall 2016 - Summer 2022
Advised by Prof. Moinuddin Qureshi, I enabled new attacks and defenses for caches against side-channels and for DRAM against data-tampering. Published 8 papers, 1 submitted.

Visiting Researcher, IAIK, TU Graz, Austria Summer 2021
Working with Prof. Daniel Gruss, I contributed to new side-channel attacks on memory compression in Linux and on Multi-Threading in AMD processors. Published 2 papers.

Research Intern, IBM Research (Security Group), NY, USA Summer 2020
Working with Rick Boivie, Alper Buyuktosunoglu and Tong Chen, I enabled always-on memory safety for C/C++ with HW support. Published 3 papers and 2 patents.

Research Intern, Microsoft, Redmond, WA, USA Summer 2019
Working with Muntaquim Chowdhury, I enabled principled security solutions for transient execution attacks like Spectre, using information-flow tracking. Submitted 2 patents.

Research Intern, Intel Labs (Security Group), Hillsboro, OR, USA Summer 2018
Working with Ken Grewal, enabled low-cost memory safety for C/C++ programs by designing hardware support for software-based sanitizers.

Research Intern, ARM Research (Memory Group), Austin, TX, USA Summer 2017
Working with Prakash Ramrakhyani, Wendy Elsasser and Jose Joao, I enabled low-cost DRAM integrity to prevent data tampering. Published 2 papers (HPCA'18, MICRO'18), 1 patent.

Conference Publications

1. Anish Saxena, **Gururaj Saileshwar**, Jonas Juffinger, Andreas Kogler, Daniel Gruss, and Moinuddin Qureshi. "PT-Guard: Integrity-Protected Page Tables to Defend Against Breakthrough Rowhammer Attacks", In *53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks 2023*. **(DSN'23)** *Acceptance rate: 19.6%*

2. Martin Schwarzl, Pietro Borrello, **Gururaj Saileshwar**, Hanna Mller, Michael Schwarz, and Daniel Gruss. "Practical Timing Side-Channel Attacks on Memory Compression", In *44th IEEE Symposium on Security and Privacy*, 2023. **(S&P'23)** *Acceptance rate: 17%*

3. Stefan Gast, Jonas Juffinger, Martin Schwarzl, **Gururaj Saileshwar**, Andreas Kogler, Simone Franza, Markus Kstl, and Daniel Gruss. "SQUIP: Exploiting the Scheduler Queue Contention Side Channel", In *44th IEEE Symposium on Security and Privacy*, 2023. **(S&P'23)** *Acceptance rate: 17%*

4. Jeonghyun Woo, **Gururaj Saileshwar** and Prashant J Nair. "Scalable and Secure Row-Swap: Efficient and Safe Row Hammer Mitigation in Memory Systems", In *29th IEEE International Symposium on High Performance Computer Architecture*, 2023. **(HPCA'23)** *Acceptance rate: 25.3%*
2023 IEEE HPCA Best Paper Award

5. Anish Saxena, **Gururaj Saileshwar**, Prashant J Nair and Moinuddin Qureshi. "AQUA: Scalable Rowhammer Mitigation by Quarantining Aggressor Rows at Runtime", In *55th ACM/IEEE International Symposium on Microarchitecture*, 2022. **(MICRO'22)** *Acceptance rate: 23.8%*

6. Moinuddin Qureshi, Aditya Rohan, **Gururaj Saileshwar** and Prashant J Nair. "Hydra: Enabling Low-Overhead Mitigation of Row-Hammer at Ultra-Low Thresholds via Hybrid Tracking", In *49th ACM/IEEE International Symposium on Computer Architecture*, 2022. **(ISCA'22)** *Acceptance rate: 16.8%*

7. **Gururaj Saileshwar**, Bolin Wang, Moinuddin Qureshi and Prashant J Nair. "Randomized Row-Swap: Mitigating Rowhammer by Breaking Spatial Correlation Between Aggressor and Victim Rows", In *27th ACM International Conference on Architectural Support for Programming Languages and Operating Systems*, 2022. **(ASPLOS'22)** *Acceptance rate: 20.2%*

8. Rick Boivie, **Gururaj Saileshwar**, Tong Chen, Benjamin Segal, and Alper Buyuktosunoglu. "On the Scalability of HeapCheck", In *52nd IEEE/IFIP International Conference on Dependable Systems and Networks (Industry Track)*, 2022. **(DSN'22)**

9. Ren Ding, Yonghae Kim, Fan Sang, Wen Xu, **Gururaj Saileshwar**, Taesoo Kim. "Hardware Support to Improve Fuzzing Performance and Precision", In *28th ACM Conference on Computer and Communications Security*, 2021. **(CCS'21)**

10. **Gururaj Saileshwar**, Sanjay Kariyappa, Moinuddin Qureshi. "Bespoke Cache Enclaves: Fine-Grained and Scalable Isolation from Cache Side-Channels via Flexible Set-Partitioning", In *1st IEEE International Symposium on Secure and Private Execution Environment Design*, 2021. **(SEED'21)**

11. **Gururaj Saileshwar** and Moinuddin Qureshi. "MIRAGE: Mitigating Conflict-Based Cache Attacks with a Practical Fully-Associative Design", In *30th USENIX Security Symposium*, 2021. **(SEC'21)** *Acceptance rate: 21.7%*

12. **Gururaj Saileshwar**, Christopher W Fletcher, and Moinuddin Qureshi. "Streamline: A Fast, Flushless Cache Covert-channel Attack by Enabling Asynchronous Collusion", In *26th ACM International Conference on Architectural Support for Programming Languages and Operating Systems*, 2021. **(ASPLOS'21)** *Acceptance rate: 18.9%*

13. Rick Boivie*, **Gururaj Saileshwar***, Tong Chen, Benjamin Segal, and Alper Buyuktosunoglu. "Hardware Support for Low-Cost Memory Safety", In *51st IEEE/IFIP International Conference on Dependable Systems and Networks (Industry Track)*, 2021. **(DSN'21)** **equal contribution*

14. **Gururaj Saileshwar** and Moinuddin Qureshi. "CleanupSpec: An "Undo" Approach to Safe Speculation", In *52nd ACM/IEEE International Symposium on Microarchitecture*, 2019. **(MICRO'19)** *Acceptance rate: 22.9%*

15. **Gururaj Saileshwar**, Prashant J Nair, Prakash Ramrakhyani, Wendy Elsasser, Jose A Joao, and Moinuddin Qureshi. "Morphable Counters: Enabling Compact Integrity Trees for Low-Overhead Secure Memories.", In *51st ACM/IEEE International Symposium on Microarchitecture*, 2018. **(MICRO'18)** *Acceptance rate: 21.3%*

16. **Gururaj Saileshwar**, Prashant J Nair, Prakash Ramrakhyani, Wendy Elsasser, and Moinuddin Qureshi. "Synergy: Rethinking Secure-memory Design for Error-Correcting Memories.", In *24th IEEE International Symposium on High Performance Computer Architecture*, 2018. **(HPCA'18)** *Acceptance rate: 20.8%*
IEEE MICRO Top Picks 2019 Honorable Mention

JOURNALS

1. **Gururaj Saileshwar** and Moinuddin Qureshi. "The Mirage of Breaking MIRAGE: Analyzing the modeling pitfalls in emerging attacks on MIRAGE". In *IEEE Computer Architecture Letters*, 2023. **(CAL'23)**

2. Anurag Kar, Xueyang Liu, Yonghae Kim, **Gururaj Saileshwar**, Hyesoon Kim, and Tushar Krishna. "Mitigating Timing-Based NoC Side-Channel Attacks With LLC Remapping". In *IEEE Computer Architecture Letters*, 2023. **(CAL'23)**

3. **Gururaj Saileshwar**, Rick Boivie, Tong Chen, Benjamin Segal, and Alper Buyuktosunoglu. "HeapCheck: Low-Cost Hardware-Support for Memory-Safety", In *ACM Transactions on Architecture and Code Optimization*, 2022. **(TACO'22)**

Workshop Publications

1. Elba Garza, **Gururaj Saileshwar**, Udit Gupta, Tianyi Liu, Abdulrahman Mahmoud, Saugata Ghose, and Joel Emer. "Mentoring Opportunities in Computer Architecture: Analyzing the Past to Develop the Future", In *21st Workshop on Computer Architecture Education held in conjunction with ISCA 2021*, 2021. **(WCAE'21)**
   Highest Peer-Review Scores in the Workshop

arXiv Publications

1. **Gururaj Saileshwar** and Moinuddin Qureshi. "Lookout for Zombies: Mitigating Flush+Reload Attack on Shared Caches by Monitoring Invalidated Lines", *arXiv:1906.02362*, 2019.

Patents

1. Tong Chen, Alper Buyuktosunoglu, Richard Boivie, and **Gururaj Saileshwar**. (submitted). "Safe execution of programs that make out-of-bounds references". 17/236,748.

2. **Gururaj Saileshwar** and Muntaquim Chowdhury. (submitted). "Hybrid Mitigation of Speculation Attacks based on Program Behavior". 62/899,549. USA.

3. Richard Boivie, Tong Chen, Alper Buyuktosunoglu, and **Gururaj Saileshwar**. (granted). "Protecting against invalid memory references.". 11,429,590. USA.

4. **Gururaj Saileshwar** and Muntaquim Chowdhury. (granted). "Speculative Information Flow Tracking". 11,301,591. USA.

5. **Gururaj Saileshwar**, Prakash Ramrakhyani, Wendy Elsasser. (granted). Memory Organization for Security and Reliability. 10,540,297. USA.

6. Sanket Thakur, **Gururaj Saileshwar**, Kadayanti Naveen, Ayesha Mudassir, Priyanka Kabara, Maryam Baghini, Dinesh Sharma. (granted). Differential Impedance to Frequency Converter. 2794/MUM/2011. India.

Invited Talks

Securing Processors from Side-Channel Attacks: Caches, Schedulers, and Beyond!

- ◇ Intel Labs - Bangalore, India 2023
- ◇ IISc Bangalore, Bengaluru, India 2023
- ◇ IIT-Kanpur, Kanpur, India 2023
- ◇ IIT-Madras, Chennai, India 2023
- ◇ IIT-Delhi, Delhi, India 2023
- ◇ IIT-Bombay, Mumbai, India 2023
- ◇ University of Waterloo (Computer Science), Waterloo, Canada 2023

Rethinking Security for Computing Hardware through Principled Randomization

- ◇ University of Toronto, Toronto, Canada 2022
- ◇ University of Wisconsin-Madison, Madison, USA 2022
- ◇ University of British Columbia, Vancouver, Canada 2022
- ◇ University of Waterloo, Waterloo, Canada 2022
- ◇ Simon Fraser University, Burnaby, Canada 2022
- ◇ UC-Irvine, Irvine, USA 2022
- ◇ University of Maryland, College Park, USA 2022

◇ NVIDIA Research, USA 2022
◇ AMD Research, USA 2022

Practical CPU-Driven Defenses for DRAM Rowhammer Attacks
◇ Intel Labs (Security and Privacy Research Group) 2022

Streamline: A Fast, Flushless Cache Covert-channel Attack
◇ SRC CRISP Program Industry Liaison Meeting (virtual) 2021
◇ ASPLOS 2021, Virtual. 2021

MIRAGE: Mitigating Cache Attacks with a Practical Fully-Associative Design
◇ USENIX Security Symposium 2021, Vancouver, BC, Canada. (virtual) 2021
◇ TU Graz - IAIK, Graz, Austria. 2021
◇ IBM Research - Security Group, TJ Watson Center, NY, USA. (virtual) 2020
◇ 5th Future of Computing Architecture Workshop (virtual), IBM Research, NY, USA 2020

CleanupSpec: An Undo Approach to Safe Speculation
◇ MICRO 2019, Fukuoka, Japan 2019
◇ Intel Labs Security & Privacy Research, Hillsboro, OR, USA. (virtual) 2019

SIFT: Speculative Information Flow Tracking to Mitigate Speculation-Attacks
◇ Microsoft Research, Redmond, WA, USA. 2019

Enabling Low-Cost Security against Micro-Architectural Side Channels
◇ 4th Future of Computing Architecture Workshop, IBM Research, NY, USA 2019
◇ Microsoft Research, Redmond, WA, USA. 2019
◇ Qualcomm Research, San Diego, CA, USA. 2019

Architecting Secure Memories with Commodity DRAM
◇ Intel Labs - Processor Architecture Research, Bangalore, India. 2018
◇ ARM Research, Austin, TX, USA. 2017

Morphable Counters: Compact Integrity Trees for Secure Memories
◇ MICRO 2018, Cambridge, MA, USA. 2018

Effective Memory Safety for Small Objects with Low Overheads
◇ Intel Labs Security & Privacy Research, Hillsboro, OR, USA. 2018

Synergy: Rethinking Secure Memory Design for Error Correcting Memories
◇ HPCA 2018, Vienna, Austria. 2018

Teaching Experience

University of Toronto - Canada, Assistant Professor
◇ CSC427: Computer Security Winter 2024
◇ CSC2231: Secure Computer Systems and Hardware Fall 2023

Georgia Institute of Technology - USA, Co-Instructor
◇ CS7292: Reliable & Secure Architecture Fall 2021
Delivered 30% course lectures. Co-designed curriculum, labs and exams.

Georgia Institute of Technology - USA, Guest Lecturer
◇ ECE8873: Advanced Hardware Oriented Security & Trust Fall 2018
◇ ECE7103: Advanced Memory Systems Spring 2018

Indian Institute of Technology (IIT) Bombay - India, Teaching Assistant
◇ EE717: Advanced Computing for EE Spring 2014
◇ EE671: VLSI Design Fall 2013
◇ CS101: Introduction to Programming Fall 2011, Spring 2012

Students Supervised

- **Brian Fu (University of Toronto, MSc. Thesis)** 2023 - Current
  Fuzzing Hardware to Discover Side-Channels at Design-Time
- **Gary Wei (University of Toronto, BASc. Thesis)** 2023 - Current
  Privacy-Leaks in Machine Learning via GPU Side-Channels

Academic Service

- **Workshop & Tutorials Co-Chair, MICRO'24**
- **Co-Chair, Artifact Evaluation Committee, ISCA'24**
- **Tutorials Chair, MICRO'23**
- **Co-Chair, Artifact Evaluation Committee, ASPLOS'23**
- **Program-Committee Member:**
  - International Symposium on Microarchitecture (MICRO), 2023.
  - International Conference on Dependable Systems and Networks (DSN), 2023.
  - International Symposium on Research in Attacks, Intrusions & Defenses (RAID), 2023
  - Top Picks in Hardware and Embedded Security (HES), 2022
  - International Symposium on Research in Attacks, Intrusions & Defenses (RAID), 2022
  - European Symposium on Research in Computer Security (ESORICS), 2022.
  - IEEE Symposium on Security & Privacy (Oakland), 2022.
- **External Review Committee Member:** ISCA 2022.
- **Shadow PC Member:** IEEE S&P (Oakland) 2021. *Recognized as Distinguished Reviewer.*
- **Reviewer:** IEEE CAL, IEEE MICRO, IEEE TCAD, IEEE Trans. Computers, IEEE TVLSI.
- **Artifact Evaluation Committee Member:** USENIX Security 2020, ASPLOS 2020.
- **Steering Committee Member, Computer Architecture Students Association (CASA)**
  - Co-organized mentorship programs Meet-A-Senior Architect at ASPLOS'21, ISCA'21, and Meet-a-Senior-Student at MICRO'20, ASPLOS'21, enabling 500+ mentoring sessions.
  - Moderated panel on "Long-Term Mentorship in Computer Architecture" at WCAE'21.

University Service

Chief Justice, Graduate Judiciary Cabinet, Georgia Tech. 2021 - 2022
Chair of the 9-member graduate student judiciary panel adjudicating graduate student misconduct and academic violations at Georgia Tech. Served on the panel for 2+ years.

Head, Institute Student Mentor Program, IIT-Bombay. 2013 - 2014
Led a team of 200+ student mentors, forming a support system for 1000+ freshmen and 300+ academically weak students; created an inclusive environment for new & existing students.

Professional Memberships

ACM, IEEE, USENIX