Gururaj Saileshwar — *Georgia Institute of Technology*

Contact

Electrical and Computer Engineering
266 Ferst Dr. NW, KACB 1210
Atlanta, GA USA 30332

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

Education

Georgia Institute of Technology, Atlanta, Georgia USA
Ph.D., Electrical and Computer Engineering, August 2022 *(expected)*
Dissertation: "Principled Yet Practical Security for Memory Systems"
Advisor: Moinuddin K. Qureshi

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

Awards and Honors

- ◇ **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

Conference Publications

1. 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%*
2. **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%*
3. 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)**
4. **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)**

5. **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%*

6. **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%*

7. **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%*

8. **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%*

9. **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**, 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)** *To Appear*

Workshop Publications

1. 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 Supplemental Volume (Industry Track)*, 2021. **(DSN-S’21)**
   **equal contribution lead authors*

2. 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. Martin Schwarzl, Pietro Borrello, **Gururaj Saileshwar**, Hanna Muller, Michael Schwarz, Daniel Gruss. “Practical Timing Side Channel Attacks on Memory Compression”, *arXiv: 2111.08404*, 2021.

2. **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. **Gururaj Saileshwar** and Muntaquim Chowdhury. (submitted). “Speculative Information Flow Tracking”. 62/894,657. USA.

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

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

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

Research Talks

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

Research Experience

Graduate Research Assistant, Georgia Tech, USA Fall 2016 - Present

Advised by Prof. Moinuddin Qureshi, my research enabled new cache attacks and principled defenses for caches against side-channels, for memory-systems against transient leakage, and for DRAM against data-tampering and rowhammer attacks. Published 7 papers, 2 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. 2 papers in submission.

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 2 papers (DSN-S'21, TACO'22) and 1 patent.

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.

Teaching Experience

- ◇ **Co-Instructor, Reliable & Secure Architectures - Georgia Tech** (CS7292) Fall 2021
  Delivered >30% course lectures. Co-designed curriculum, labs and exams, and supervised student projects. Students rated the course 4.5 out of 5 in anonymous midterm evaluation.
- ◇ **Guest Lecturer - Georgia Tech**
  Advanced Hardware Oriented Security & Trust (ECE 8873) Fall 2018
  Advanced Memory Systems (ECE 7103) Spring 2018
- ◇ **Graduate Teaching Assistant - IIT Bombay**
  Advanced Computing for EE (EE 717) Spring 2014
  VLSI Design (EE-671) Fall 2013
- ◇ **Undergraduate Teaching Assistant - IIT Bombay**
  Introduction to Programming (CS 101) Fall 2011, Spring 2012

Students Mentored

- ◇ **Yonghae Kim (Georgia Tech, Ph.D.)** 2020 - 2021
  Hardware Support for Improving Fuzzing Performance and Precision. *Paper in CCS'21*
- ◇ **Bolin Wang (University of British Columbia, M.Sc.)** 2020 - 2021
  Hot-Data Aware Dynamic Merkle-Trees for Scalable Secure Memories. *(under submission)*
- ◇ **Anish Saxena (Georgia Tech, Ph.D.)** 2021
  Transparent Protection for Page-Tables against Rowhammer Attacks. *(under submission)*
- ◇ **Aditya Rohan (Georgia Tech, Ph.D.)**, 2021
  Scalable Defenses against Rowhammer Attacks with in-DRAM Counters. *Paper in ISCA'22*
- ◇ **Anurag Kar and Xueyang Liu (Georgia Tech, M.S./Ph.D.)** 2021
  Secure Network-On-Chip Design for Side-Channel Resilience.

Academic Service

- ◇ **Program-Committee Member:** IEEE 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 - Present
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

References

Prof. Moinuddin Qureshi
Georgia Institute of Technology
School of Computing Science

266 Ferst Dr. NW
KACB 2312
Atlanta, GA 30318, USA
✉ moin@gatech.edu
🏠 https://www.cc.gatech.edu/∼moin/

Prof. Christopher W. Fletcher
University of Illinois - Urbana Champaign
Department of Computing Science

201 N Goodwin Ave,
4106 Siebel Center for Comp Sci
Urbana, IL 61801, USA
✉ cwfletch@illinois.edu
🏠 http://cwfletcher.net/

Prof. Daniel Gruss
Graz University of Technology (TU Graz)
Institute of Applied Information Processing and Communications (IAIK)

Inffeldgasse 16a,
8010 Graz, Austria
✉ daniel.gruss@iaik.tugraz.at
🏠 https://gruss.cc/

Prof. Milos Prvulovic
Georgia Institute of Technology
School of Computing Science

266 Ferst Dr. NW
KACB 2332
Atlanta, GA 30318, USA
✉ milos@cc.gatech.edu
🏠 https://www.cc.gatech.edu/∼milos/

Prof. Taesoo Kim
Georgia Institute of Technology
School of Computing Science

756 West Peachtree Street NW
CODA E1062B,
Atlanta, GA 30332, USA
✉ taesoo@gatech.edu
🏠 https://taesoo.kim/