A. BIOGRAPHICAL INFORMATION

1. **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/

2. **Degrees**

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

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

3. **Employment**

Sept 2023 – present:	**Assistant Professor**, University of Toronto Mississauga, Dept of Mathematical and Computational Sciences, Mississauga ON, Canada.
Sept 2023 – present:	**Assistant Professor**, University of Toronto, Dept of Computer Science, Toronto ON, Canada.
Aug 2022 – Aug 2023:	**Postdoctoral Research Scientist**, NVIDIA Research, Seattle, USA
Aug 2016 – July 2022:	**Graduate Research Assistant**, Georgia Tech, Atlanta, USA
May 2021 – Aug 2021:	**Visiting Researcher**, CoreSec Group, Graz University of Technology, Graz, Austria
May 2020 – Aug 2020:	**Research Intern**, IBM Research (T.J. Watson Center), New York, USA
May 2019 – Aug 2019:	**Research Intern**, Microsoft Azure Research, Redmond, USA
May 2018 – Aug 2018:	**Research Intern**, Intel Labs (Security & Privacy), Hillsboro, USA
May 2017 – Aug 2017:	**Research Intern**, ARM Research, Austin, USA

4. **Honours**

- **University of Toronto Dean's Excellence Award 2025,** for outstanding research achievements 2025
- **IEEE HPCA Distinguished Artifact Award** for HPCA 2025 paper, QPRAC 2025
- **IEEE Top Pick in Hardware and Embedded Security Award** for SEC 2021 paper, MIRAGE 2024
  Top pick among top-tier architecture, security and CAD conferences of the last 5 years.
- **ACM-SIGMICRO Dissertation Award** (Honorable Mention) 2023
- **ACM-SIGARCH/IEEE-TCCA Outstanding Dissertation Award** (Honorable Mention) 2023
- **Best Paper Award, IEEE HPCA 2023 Conference** 2023
- **Best PhD Dissertation Award, IEEE Hardware Oriented Security & Trust** 2022
- **Distinguished Reviewer, Shadow PC, IEEE Security & Privacy'21 (Oakland)** 2021
- **Awarded Georgia Tech Information Security & Privacy (IISP) Fellowship** 2021
- **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 Workshop at IBM Research** (one of 7 students invited) 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

B. ACADEMIC HISTORY

5. A. **Research Endeavours**

Research Interests: Computer Architecture and Systems Security, focusing on microarchitectural security (cache side-channels, transient execution attacks, Rowhammer attacks), system security (memory safety and fuzzing) and security for machine learning systems (LLM side channels, data isolation).

Impact: Published **18** conference papers in **top-tier venues in computer architecture** (ISCA, MICRO, HPCA, ASPLOS) and **computer security** (USENIX Security, S&P-Oakland, CCS).

B. **Research Awards**

1. **NSERC Discovery Grant:** *Automated Testing Techniques for Hardware Security and Reliability* (sole PI), 2023-2028. CAD 185,000.
2. **NSERC Discovery Launch Supplement:** *Automated Testing Techniques for Hardware Security and Reliability* (sole PI), 2023-2028. CAD 12,500.
3. **NSERC CSE Research Communities Grant:** *An End-to-End Approach to Safe and Secure AI Systems* (co-PI), 2024-2028. CAD 240,000.

C. **Patents** awarded (in reverse chronological order)

1. Tong Chen, Alper Buyuktosunoglu, Richard Boivie, and **Gururaj Saileshwar**. "Safe execution of programs that make out-of-bounds references". US PTO 12,204,460. USA.
2. Richard Boivie, Tong Chen, Alper Buyuktosunoglu, and **Gururaj Saileshwar**. "Protecting against invalid memory references". US PTO 11,966,382. USA.
3. Richard Boivie, Tong Chen, Alper Buyuktosunoglu, and **Gururaj Saileshwar**. "Protecting against invalid memory references". US PTO 11,429,590. USA.
4. **Gururaj Saileshwar** and Muntaquim Chowdhury. "Speculative Information Flow Tracking". US PTO 11,301,591. USA.
5. **Gururaj Saileshwar**, Prakash Ramrakhyani, Wendy Elsasser. "Memory Organization for Security and Reliability". US PTO 10,540,297. USA.

C. SCHOLARLY AND PROFESSIONAL WORK

6. **Refereed Publications**

In computer science, peer-reviewed conferences are more prestigious than journals, with top-tier conferences such as ISCA, MICRO, HPCA, ASPLOS in computer architecture, and S&P, SEC, and CCS in computer security being the most prestigious, with typical acceptance rates below 20%.

My research has resulted in 18 top-tier publications: 3 x ISCA, 3 x MICRO, 3 x HPCA, 3 x ASPLOS, 3 x SEC, 2 x S&P, 1 x CCS papers.

A. **Conferences** (in reverse chronological order)

1. Chris S. Lin*, Joyce Qu*, and **Gururaj Saileshwar**. "GPUHammer: Rowhammer Attacks on GPU Memories are Practical", In *34th USENIX Security Symposium*, 2025. **(SEC'25)**
   Media Coverage: ArsTechnica, Tom's Hardware, The Register, Mashable, TechRadar, The Hacker News, BleepingComputer, SecurityWeek, CybersecurityNews, SCMedia, Fudzilla, SDXCentral, PC Perspective, CyberPress, GBHackers, ITNews, Guru3D, WebProNews, WCCFTech, Security Brief Australia, Red Hot Cyber.

2. Yuqin Yan, Wei Huang, Ilya Grishchenko, **Gururaj Saileshwar**, Aastha Mehta, and David Lie. "Title under embargo", In *34th USENIX Security Symposium*, 2025. **(SEC'25)**

3. Jeonghyun Woo, Joyce Qu, **Gururaj Saileshwar** and Prashant J Nair. "When Mitigations Backfire: Timing Channel Attacks and Defense for PRAC-Based Rowhammer Mitigations", In *51st ACM/ IEEE International Symposium on Computer Architecture*, 2025. **(ISCA'25)**

4. Jules Drean, Fisher Jepsen, Edward Suh, Srini Devadas, Aamer Jaleel, and **Gururaj Saileshwar**. "Teaching an Old Dog New Tricks: Verifiable FHE Using Commodity Hardware", In *25th Proceedings on Privacy Enhancing Technologies Symposium*, 2025. **(PoPETS'25)**

5. Bo Fu*, Leo Tenenbaum*, David Adler, Assaf Klein, Arpit Gogia, Alaa R. Alameldeen, Marco Guarnieri, Mark Silberstein, Oleksii Oleksenko, and **Gururaj Saileshwar**. "AMuLeT: Automated Design-Time Testing of Secure Speculation Countermeasures", In *30th ACM International Conference on Architectural Support for Programming Languages and Operating Systems*, 2025. **(ASPLOS'25)**

6. Jeonghyun Woo, Shaopeng Lin, Prashant J Nair, Aamer Jaleel, and **Gururaj Saileshwar**. "QPRAC: Towards Secure and Practical PRAC-based Rowhammer Mitigation using Priority Queues", In *31st IEEE International Symposium on High Performance Computer Architecture*, 2025. **(HPCA'25)**
   🏆 **IEEE HPCA Distinguished Artifact Award 2025**

7. Aamer Jaleel, **Gururaj Saileshwar**, Steve Keckler, and Moinuddin Qureshi. "PrIDE: Achieving Secure Rowhammer Mitigation with Low-Cost In-DRAM Trackers", In *51st ACM/ IEEE International Symposium on Computer Architecture*, 2024. **(ISCA'24)** *Acceptance rate: 19.6%*

8. 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%*

9. Martin Schwarzl, Pietro Borrello, **Gururaj Saileshwar**, Hanna Muller, 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%*

10. Stefan Gast, Jonas Juffinger, Martin Schwarzl, **Gururaj Saileshwar**, Andreas Kogler, Simone Franza, Markus Kostl, 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%*
Media Coverage: Phoronix, Tom's Hardware, SecurityWeek, HackDay, Neowin, HotHardware, NotebookCheck, WCCFTech, TechRadar, The Hacker News, NextPlatform.

11. 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%*
🏆 **IEEE HPCA Best Paper Award 2023**

12. 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%*

13. 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%*

14. **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%*

15. 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)**

16. 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)**

17. **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)**

18. **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%*
🏆 **IEEE Top Pick in Hardware and Embedded Security 2024**

19. **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%*

20. 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*

21. **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%*

22. **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%*

23. **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 Honorable Mention 2019

B. **Journals** (in reverse chronological order)

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)**

C. **Workshops**

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)**

7. **Non-Refereed Publications** (in reverse chronological order)

1. Tianchen Zhang, **Gururaj Saileshwar** and David Lie. "Time Will Tell: Timing Side Channels via Output Token Count in Large Language Models", *arXiv:2412.15431*, 2024.
2. Jiankun Wei, Abdulrahman Abdulrazzag, Tianchen Zhang, Adel Muursepp, and **Gururaj Saileshwar**. "Privacy Risks of Speculative Decoding in Large Language Models", *arXiv:2411.01076*, 2024.
3. **Gururaj Saileshwar** and Moinuddin Qureshi. "Lookout for Zombies: Mitigating Flush+ Reload Attack on Shared Caches by Monitoring Invalidated Lines", *arXiv:1906.02362*, 2019.

8. **Invited Lectures**

A Good Offense is the Best Defense: Robustly Mitigating Spectre and Rowhammer in Future Systems
- ETH Zurich, Zurich, Switzerland 2025
- Google Hardware Security Workshop, Zurich, Switzerland 2025
- Intel IPAS Tech Sharing Seminar, Virtual 2025
- CISPA Helmholtz Center for Information Security, Germany 2025

Learning to Trust DRAM in the Era of Worsening Rowhammer Attacks
- Carnegie Mellon University (CMU), USA (virtual). 2024
- ZTHA Workshop co-located with CHES, Halifax, Canada. 2024

Microarchitectural Side-Channels: Attacks, Defenses, and Ending the Arms Race
- Microsoft Research, Redmond, USA. 2024

Rowhammer: Learnings from Designing Defenses and Outlook For the Future
- Dagstuhl Seminar on "Micro-architectural Attacks and Defenses", Germany. 2023

Mitigating DRAM Rowhammer Attacks in the Era of Breakthrough Attacks
- Invited talk at HASP Workshop co-located with MICRO, Toronto, Canada. 2023

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
- Top Picks in Hardware and Embedded Security Workshop, Newark, NJ, USA. 2025
- 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

D. TEACHING AND MENTORING

9. A. **Undergraduate courses taught**

University of Toronto - Mississauga
- CSC427-0201 : Computer Security Winter 2025
  Enrollment: 31. Introduced new topics like Spectre and Rowhammer, and instructor delivered lectures.
- CSC427-0101 : Computer Security Winter 2024
  Enrollment: 54. Revamped assignments that formed 30% of the overall assessment.

B. **Graduate courses taught**

University of Toronto
- CSC2231: Special Topics in Computer Systems - Secure Computer Systems and Hardware Fall 2024
  Enrollment: 11.
- CSC2231: Special Topics in Computer Systems - Secure Computer Systems and Hardware Fall 2023
  Enrollment: 11.

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

C. **Theses supervised**
1. **Shaopeng Lin (University of Toronto, PhD. Thesis)** Sept 2024 - Current
   Thesis: *Rowhammer Attacks and Defenses for CPUs and GPUs*
2. **Raghav Sharma (University of Toronto, MSc. Thesis)** Sept 2024 - Current
   Thesis: *Fully-Homomorphic Encryption Systems*
3. **Bo Fu (University of Toronto, MSc. Thesis)** Sept 2023 - April 2025
   Thesis: *Automated Design-Time Testing of Secure Speculation Countermeasures*
4. **Gary Wei (University of Toronto, BASc. Thesis)** Sept 2023 - Apr 2024
   Thesis: *Side-Channels via Sparsity and Caching in Machine Learning Systems*

D. **Undergraduate students supervised**
1. **Joyce Qu** (3rd year), *Rowhammer Attacks and Defenses*
   University of Toronto Excellence Award (UTEA), Summer 2025
   Research Volunteer, Fall 2024 - Winter 2025.
2. **David Wei** (4th year), *Side Channel Attacks on Speculative Decoding in LLMs*
   NSERC Undergraduate Student Research Award, Summer 2025
   CSC494, Summer 2024 - Winter 2025
3. **Allison Lau** (4th year), *Prompt Injection Attacks on AI Agentic Systems*
   NSERC Undergraduate Student Research Award, Summer 2025
4. **Anthony Dimaggio** (4th year), *GPU Confidential Computing*
   DCS Research Award, Summer 2025 CSC494, Summer 2024

5. **Louis Ryan Tan** (3rd year), *Prompt Injection Attacks on AI Agentic Systems*
   DCS Research Award, Summer 2025
6. **Henry Chen** (3rd year), *Fuzzing RISC-V CPUs for Side-Channels*
   DCS Research Award, Summer 2025
7. **Leo Tanenbaum** (4th year), *Automated Leakage Testing of CPU Speculation Defenses*
   NSERC Undergraduate Student Research Award, Summer 2024; CSC494, Winter 2024
   🏆 First Place at ACM Student Research Competition (Undergraduate), MICRO 2024
   🏆 CRA Outstanding Undergraduate Researcher Award 2024-25 (Honorable Mention)
8. **Abdulrahman Abdulrazzaq** (4th year), *Side-Channel Attacks on Speculative Decoding in LLMs*
   NSERC Undergraduate Student Research Award, Summer 2024
9. **Shaopeng Lin** (4th year), *GPU Rowhammer Attacks*
   University of Toronto Excellence Award (UTEA), Summer 2024; CSCD94H3, Winter 2024
10. **Richard Shi** (3rd year), *ML Pruning in Secure Federated Learning*
    University of Toronto Excellence Award (UTEA), Summer 2024
11. **Adel Mursuup** (3rd year), *Side-Channel Attacks on Speculative Decoding in LLMs*
    CSC494, Summer 2024
12. **Mathew Toohey** (4th year), *Formal Verification of CPU Speculation Defenses*
    CSC494, Fall 2024
13. **Leonid Nediak** (4th year), *Formal Verification of CPU Speculation Defenses*
    CSC494/495, Fall 2024 - Winter 2025
14. **Theodore Preduta** (4th year), *Fuzzing RISC-V CPUs on FPGAs for Vulnerabilities*
    CSC494/495, Fall 2024 - Winter 2025
15. **Yifu Zhu** (4th year), *Fuzzing RISC-V CPUs for Vulnerabilities*
    CSC494/495, Summer 2024 - Winter 2025
16. **David Adler** (3rd year), *Automated Leakage Testing of CPU Speculation Defenses*
    CSC494, Summer 2024
17. **Shubh Bapna** (4th year), *RowPress Attacks on DDR3 DRAM*
    CSC492H5, Winter 2024
18. **Warren Liu** (4th year), *DRAM Rowhammer Attacks on Apple iPhones*
    CSC494, Winter 2024
19. **Juan Yi Loke** (4th year), *Latency and Accuracy Trade-off in Private ML Inference*
    CSC494, Winter 2024
20. **Harshkumar Patel** (3rd year), *Latency and Accuracy Trade-off in Private ML Inference*
    CSC494, Winter 2024
21. **Ahmad Islah** (4th year), *Privacy and Performance Trade-Offs in Federated Learning*
    CSC494, Winter 2024
22. **Chenika Bukes** (3rd year), *Privacy and Performance Trade-Off in Federated Learning*
    CSC494, Winter 2024
23. **Yinuo Zhao** (3rd year), *Side-Channels in LLM Speculative Decoding*
    CSC494, Winter 2024
24. **Sophia Abolore** (4th year), *Side-Channels in LLM Speculative Decoding*
    CSC494, Winter 2024

E. **Other teaching and lectures given**

- **University of Toronto - Mississauga, Toronto, Guest Lecturer**
  - CSC148: Introduction to Computer Science — Winter 2025
- **Georgia Institute of Technology - USA, Guest Lecturer**
  - ECE8873: Advanced Hardware Oriented Security & Trust — Fall 2018
  - ECE7103: Advanced Memory Systems — Spring 2018

E. ADMINISTRATIVE POSITIONS

10. A. **Positions held and service on committees and organizations within the University**

- **Faculty Recruitment Committee (Tenure Stream)**, Dept of Computer Science, UofT. 2024-2025
- **Faculty Recruitment Committee (Tenure Stream)**, Dept of Computer Science, UofT. 2023-2024

B. **Positions held and service on committees and organizations outside the University**

- **Co-Chair, Artifact Evaluation Committee, ISCA'25**
- **Workshop & Tutorials Co-Chair, MICRO'24**
- **Co-Chair, Artifact Evaluation Committee, ISCA'24**
- **Workshop & Tutorials Co-Chair, MICRO'23**
- **Co-Chair, Artifact Evaluation Committee, ASPLOS'23**
- **Program-Committee Member:**
  - USENIX Security Symposium, 2026.
  - International Symposium on Microarchitecture (MICRO), 2025.
  - International Symposium on Computer Architecture (ISCA), 2025.
  - International Symposium on High Performance Computer Architecture (HPCA), 2025.
  - International Symposium on Microarchitecture (MICRO), 2024.
  - International Symposium on Research in Attacks, Intrusions & Defenses (RAID), 2024
  - 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.