

Ali HAJIABADI

Postdoctoral Researcher and Lecturer
ETH Zürich

CONTACT INFORMATION

ADDRESS: ETZ G 78.2, Gloriastr. 35, 8092 Zürich, Switzerland
EMAIL: ahajiabadi@ethz.ch
HOMEPAGE: ahajiabadi.github.io

RESEARCH INTERESTS

Systems Security, Hardware/Software Co-design, Computer Architecture, Optimizing Compilers, Formal Methods, Secure Architectures and Software, Microarchitectural Side Channels, Trusted Execution Environments

EDUCATION

-
- 2019 - 2024 Doctor of Philosophy in Computer Science
National University of Singapore (NUS), Singapore
Thesis: "*Building Efficient and Secure Processors thorough Hardware/Software Co-design*"
Advisor: Prof. Trevor E. CARLSON
- 2014 - 2019 Bachelor of Science in Computer Engineering
Sharif University of Technology, Tehran, Iran
Thesis: "*High Concurrency Latency Tolerant Register Files for GPUs*"
Advisor: Prof. Hamid SARBAZI-AZAD
- 2009 - 2013 Diploma in Physics and Mathematics Discipline
Shahid Beheshti High School, Birjand, Iran
Affiliated with the National Organization for the Development of Exceptional Talents (NODET)

HONORS & AWARDS

-
- AUG. 2024 DEAN'S GRADUATE RESEARCH EXCELLENCE AWARD.
- JUL. 2024 SCHOOL OF COMPUTING CS PHD THESIS AWARD (Honorable Mention), selected as top five theses.
- JUN. 2024 BEST PAPER AWARD nomination at DAC '24.
- OCT. 2023 NUSGS RESEARCH INCENTIVE AWARD from School of Computing, NUS (\$\$ 2,500 award).
- JAN. 2022 STUDENT TRAVEL AWARD from ASPLOS'22 conference.
- AUG. 2021 RESEARCH ACHIEVEMENT AWARD from School of Computing, NUS.
- MAR 2020 Invited talk and travel grant for the 2nd Young Architect Workshop at ASPLOS'20, Switzerland.
- FEB. 2019 PRESIDENT'S GRADUATE FELLOWSHIP, the most prestigious doctoral fellowship in Singapore.
- SEP. 2014 Ranked 164th in Iranian National University Entrance Exam among more than 250,000 students.
- 2006/2009 Recognized as talented student in entry exam of NODET for middle school and high school.

PROFESSIONAL EXPERIENCE

-
- JUL. 2024 - PRESENT Postdoctoral Researcher at ETH ZÜRICH, Switzerland
Computer Security (COMSEC) Group
Group Lead: Prof. Kaveh RAZAVI
Research: CPU and DRAM security, novel attacks and defenses for computing systems
- AUG. 2019 - JUN. 2024 Graduate Research Assistant at NATIONAL UNIVERSITY OF SINGAPORE, Singapore
NUS Computer Architecture (CompArch) Group
Group Lead: Prof. Trevor E. CARLSON
Research: hardware/software co-design for efficient and secure modern processors
- JUL. 2016 - JUN. 2019 Research Assistant at SHARIF UNIVERSITY OF TECHNOLOGY, Tehran, Iran
High Performance Computer Architectures and Networks (HPCAN) Lab
Group Lead: Prof. Hamid SARBAZI-AZAD
Research: GPU register prefetching via HW/SW co-design and compiler optimizations
- SUMMER 2018 Research Intern at NATIONAL UNIVERSITY OF SINGAPORE, Singapore
Group Lead: Prof. Trevor E. CARLSON
Research: exploring new implementations for out-of-order commit processors

PEER-REVIEWED PUBLICATIONS

S&P'26	Jean-Claude Graf*, Sandro Rüegge*, Ali Hajiabadi , Kaveh Razavi <i>VMScape: Exposing and Exploiting Incomplete Branch Predictor Isolation in Cloud Environments.</i> Proceedings of 47 th IEEE Symposium on Security and Privacy (S&P, Oakland 2026), May 2026. Acceptance rate: 118/925 = 12.8% ► A systematic analysis of Branch Target Injection (BTI) across virtualization boundaries, with the first attack on AMD CPUs where a KVM guest leaks secrets from an unmodified QEMU process on the host. Paper GitHub Website
HPCA'26	Hritvik Taneja, Ali Hajiabadi , Michele Marazzi, Kaveh Razavi, Moinuddin K. Qureshi <i>MIRZA: Efficiently Mitigating Rowhammer with Randomization and ALERT.</i> Proceedings of 32 nd IEEE International Symposium on High-Performance Computer Architecture (HPCA 2026), February 2026. Acceptance rate: 119/602 = 19.8% ► <i>ALERT Is All You Need:</i> proposing a reactive and efficient Rowhammer mitigation without per row activation counters, using probabilistic and securely filtered ALERTs.
CCS'25	Ali Hajiabadi , Michele Marazzi, Kaveh Razavi <i>CHaRM: Checkpointed and Hashed Counters for Flexible and Efficient Rowhammer Mitigation.</i> Proceedings of 32 nd ACM Conference on Computer and Communications Security (CCS 2025), October 2025. Acceptance rate: 316/2186 = 14.5% ► An in-CPU Rowhammer mitigation breaking counter-threshold dependency to protect DRAM devices with arbitrary threshold, while using a fixed storage budget and efficient tagless SRAM counters. Paper Artifact GitHub Website
MICRO'25	Silvan Niederer, Sandro Rüegge, Ali Hajiabadi , Kaveh Razavi <i>One Flew over the Stack Engine's Nest: Practical Microarchitectural Attacks on the Stack Engine.</i> Proceedings of 58 th IEEE/ACM International Conference on Microarchitecture (MICRO 2025), October 2025. Acceptance rate: 124/597 = 20.8% ► Providing an extensive reverse engineering of the stack engine in modern AMD and Intel CPUs, and proposing novel and practical stack engine side channel attacks, leaking sensitive information. Paper Artifact Website
ISCA'25	Ali Hajiabadi , Trevor E. Carlson <i>CASSANDRA: Efficient Enforcement of Sequential Execution for Cryptographic Programs.</i> Proceedings of 52 nd ACM/IEEE International Symposium on Computer Architecture (ISCA 2025), June 2025. Acceptance rate: 132/570 = 23.1% ► A hardware/software mechanism to protect constant-time cryptographic code against Spectre by disabling speculation and recording-and-replaying sequential control flow. Paper
TACO'25	Yun Chen*, Ali Hajiabadi *, Romain Poussier, Yaswanth Tavva, Andreas Diavastos, Shivam Bhasin, Trevor E. Carlson <i>PARADISE: Criticality-Aware Instruction Reordering for Power Attack Resistance.</i> *Joint first-authors with equal contribution. In ACM Transactions on Architecture and Code Generation (TACO), 2024 ► Proposing a novel criticality-aware and non-deterministic instruction scheduling for out-of-order processors to resist power analysis attacks. Paper
DAC'24	Ali Hajiabadi , Trevor E. Carlson <i>CONJURING: Leaking Control Flow via Speculative Fetch Attacks.</i> Proceedings of 61 st ACM/IEEE Design Automation Conference (DAC 2024), June 2024. Acceptance rate: 337/1465 = 23.0% ★ Best Paper Award Nominee (5/337 = 1.5%) ► Proposing a new and practical variant of speculative fetch attacks that enables unprivileged attackers to leak control flow information of victims, without requiring priming a side channel. Paper Talk
DAC'24	Ali Hajiabadi , Archit Agarwal, Andreas Diavastos, Trevor E. Carlson <i>LEVIOSO: Efficient Compiler-Informed Secure Speculation.</i> Proceedings of 61 st ACM/IEEE Design Automation Conference (DAC 2024), June 2024. Acceptance rate: 337/1465 = 23.0% ► Efficient and comprehensive mitigation for speculative execution attacks through compiler-informed hints about true branch dependencies to restrict execution of speculative instructions only if necessary. Paper Github Talk

HPCA'24	<p>Yun Chen*, Ali Hajiabadi*, Trevor E. Carlson GADGETSPINNER: A New Transient Execution Primitive using the Loop Stream Detector. Proceedings of 30th IEEE International Symposium on High-Performance Computer Architecture (HPCA 2024), March 2024. Acceptance rate: 75/410 = 18.3% *Joint first-authors with equal contribution. ► <i>Analyzing and discovering vulnerabilities of the Loop Stream Detector (LSD) in Intel CPUs that enables cross-core transient execution attacks without requiring branch prediction unit mistraining.</i></p>
HPCA'24	<p>Yun Chen, Ali Hajiabadi, Lingfeng Pei, Trevor E. Carlson PREFETCHX: Cross-Core Cache-Agnostic Prefetcher-Based Side-Channel Attacks. Proceedings of 30th IEEE International Symposium on High-Performance Computer Architecture (HPCA 2024), March 2024. Acceptance rate: 75/410 = 18.3% ► <i>Extensive reverse-engineering of an undocumented Intel prefetcher, called XPT (an LLC miss predictor) that enables cross-core cache-agnostic covert and side channels.</i></p>
ICCAD'23	<p>Arash Pashrashid, Ali Hajiabadi, Trevor E. Carlson HIDFIX: Efficient Mitigation of Cache-based Spectre Attacks through Hidden Rollbacks. Proceedings of 42nd IEEE/ACM International Conference on Computer-Aided Design (ICCAD 2023), November 2023. Acceptance rate: 172/768 = 22.4% ► <i>Extensive study of existing detection/mitigation combinations and proposing attacks to bypass them; co-designing detection and mitigation to defend cache-based Spectre with no performance overhead.</i></p>
ICCAD'22	<p>Arash Pashrashid, Ali Hajiabadi, Trevor E. Carlson Fast, Robust and Accurate Detection of Cache-based Spectre Attack Phases. Proceedings of 41st IEEE/ACM International Conference on Computer-Aided Design (ICCAD 2022), November 2022. Acceptance rate: 132/586 = 22.5% ► <i>(1) Demonstrating different attacks bypassing ML-based detectors for Spectre attacks; (2) proposing an efficient, accurate, robust, and timely mechanism to detect cache-based Spectre attack phases.</i></p>
ASPLOS'21	<p>Ali Hajiabadi, Andreas Diavatos, Trevor E. Carlson NOREBA: A Compiler-Informed Non-speculative Out-of-Order Commit Processor. Proceedings of 26th ACM International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS 2021). April 2021. Acceptance rate: 75/398 = 18.8% ► <i>A hardware/software co-design that compiler informs the hardware about true branch dependencies enabling safe and non-speculative out-of-order commit of instructions improving efficiency.</i></p>
TOCS'21	<p>Mohammad Sadrosadati, Amirhossein Mirhosseini, Ali Hajiabadi, Seyed Borna Ehsani, Hajar Falahati, Hamid Sarbazi-Azad, Mario Drumond, Babak Falsafi, Rachata Ausavarungnirun, Onur Mutlu <i>Highly Concurrent Latency-tolerant Register Files for GPUs.</i> In ACM Transactions on Computer Systems (TOCS), 2021. ► <i>A hardware/software co-operative design for register prefetching in GPUs. The compiler constructs the prefetch sets and ensures minimal register bank conflicts via register renumbering.</i></p>
CGO'21	<p>Harish Patil, Alexander Isaev, Wim Heirman, Alen Sabu, Ali Hajiabadi, Trevor E. Carlson ELFies: Executable Region Checkpoints for Performance Analysis and Simulation. Proceedings of 19th IEEE International Symposium on Code Generation and Optimization (CGO 2021), March 2021. Acceptance rate: 31/89 = 34.8% ► <i>Proposing a set of tools to generate checkpoint executables of the regions of interest of applications, called ELFies. ELFies run natively and can be used for detailed analysis in other tools and simulators.</i></p>

TEACHING EXPERIENCE

► ETH Zürich, Switzerland

- FALL 2025 Lecturer, Computer Security (BSc) [New Course]
- SPRING 2025 Lecturer, Capture the Flag - Introduction to Cybersecurity (P&S BSc) [New Course]
- SPRING 2025 Co-lecturer with Prof. Kaveh Razavi, Computer Engineering (BSc)

► National University of Singapore, Singapore

- SPRING 2020 Teaching Assistant (tutorial instructor), CS2106 Introduction to Operating Systems (BSc)
- SPRING 2021 Lecturer: Prof. Djordje Jevdjic

► Sharif University of Technology, Tehran, Iran

- SPRING 2017 **Teaching Assistant** (assignments & projects), *CE323 Computer Architecture (BSc)*
Lecturer: Prof. Hamid Sarbazi-Azad
- FALL 2017 **Teaching Assistant** (tutorial instructor, assignments & projects), *CE453 Real-Time Systems (BSc)*
FALL 2018 Lecturer: Prof. Amirhossein Jahangir

TALKS

- Nov. 2025 **The Hidden and Ugly Faces of Spectre: Unexplored and Unmitigated Threat Models**
IC, EPFL, Lausanne, Switzerland.
- OCT. 2025 **CHaRM: Checkpointed and Hashed Counters for Flexible and Efficient Rowhammer Mitigation**
Conference on Computer and Communication Security (CCS 2025), Taipei, Taiwan.
- JUN. 2025 **CASSANDRA: Efficient Enforcement of Sequential Execution for Cryptographic Programs**
Int. Symposium on Computer Architecture (ISCA 2025), Tokyo, Japan.
- MAR. 2024 **Will CPUs Be Free of Spectre? Dark Side and Light Side of the Battle**
ETH Zürich, COMSEC Group, Zürich, Switzerland.
- MAR. 2024 **GADGETSPINNER: A New Transient Execution Primitive using the Loop Stream Detector**
Int. Symposium on High-Performance Computer Architecture (HPCA 2024), Edinburgh, Scotland.
- AUG. 2021 **NOREBA: A Compiler-Informed Non-speculative Out-of-Order Commit Processor**
Computing Research Week, School of Computing (NUS), Virtual.
- APR. 2021 **NOREBA: A Compiler-Informed Non-speculative Out-of-Order Commit Processor**
Int. Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS 2021), Virtual.
- FEB. 2021 **Accelerating HPC applications with Out-of-Order Commit Processors**
Free and Open source Software Developers' European Meeting (FOSDEM 2021), HPC, Big Data, and Data Science track, Virtual.
- MAR. 2020 **Speculation-Free Out-of-Order Commit**
2nd Young Architect Workshop at the 25th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS 2020), Virtual.

PROFESSIONAL SERVICES

- Program Committee** ISCA 2026, HPCA 2026, MICRO 2025, EuroS&P 2026, AsiaCCS 2026
- Sub-reviewer** USENIX Security 2025
- Reviewer (journals)** IEEE CAL, ACM TACO, ACM TRETS
- Shadow PC** EuroSys 2024, EuroSys 2023
- Student Volunteer** PLDI 2021

RESEARCH MENTORING

- MAR 2025 - PRESENT *Sandro Rüegge* PhD thesis at COMSEC, ETH Zürich
- JUL. 2024 - PRESENT *Silvan Niderer* PhD thesis at COMSEC, ETH Zürich
- MAR 2025 - SEP. 2025 *Maximilian Mosler* Master thesis at ETH Zürich
- MAR 2025 - JUN. 2025 *Jonas Buchholz* Master semester project at ETH Zürich
- DEC. 2024 - JUN. 2025 *Chenfei Liu* Master thesis at ETH Zürich
- SEP. 2024 - FEB. 2025 *Mounir Raki* Master semester project at ETH Zürich
- AUG. 2020 - MAR. 2024 *Yun Chen* PhD thesis at NUS CompArch
- JAN. 2021 - DEC. 2023 *Arash Pashrashid* PhD thesis at NUS CompArch
- JUL. 2021 - JUL. 2023 *Archit Agarwal* Research assistant at NUS CompArch
- SEP. 2020 - SEP. 2021 *Vernon Pang* BSc final-year project at NUS

SKILLS

- PROGRAMMING LANGUAGES:** C, C++, Python, bash, and familiar with Java, Matlab, Scala
- INSTRUCTION SET ARCHITECTURES:** x86, Arm, RISC-V
- SCIENTIFIC TOOLS:** LLVM Compiler Infrastructure, gem5 Simulator, Sniper Simulator, Ramulator, Intel Pin, Dynamorio
- TYPESETTING:** L^AT_EX, Microsoft Word