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 thorugh 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 (S$ 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 2^{nd} Young Architect Workshop at ASPLOS'20, Switzerland.
Feb. 2019 President's Graduate Fellowship, the most prestigious doctoral fellowship in Singapore.
Sep. 2014 Ranked **164**th 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
VMScape: Exposing and Exploiting Incomplete Branch Predictor Isolation in Cloud Environments.
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

CCS'25 | **Ali Hajiabadi**, Michele Marazzi, Kaveh Razavi
CHaRM: Checkpointed and Hashed Counters for Flexible and Efficient Rowhammer Mitigation.
Proceedings of 32^{nd} ACM Conference on Computer and Communications Security (CCS 2025), October 2025.
▶ *Enabling a flexible in-CPU Rowhammer mitigation that secures any DRAM device, with arbitrary Rowhammer 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
One Flew over the Stack Engine's Nest: Practical Microarchitectural Attacks on the Stack Engine.
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
Cassandra: *Efficient Enforcement of Sequential Execution for Cryptographic Programs*.
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
Paradise: *Criticality-Aware Instruction Reordering for Power Attack Resistance*.
∗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
Conjuring: *Leaking Control Flow via Speculative Fetch Attacks*.
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
Levioso: *Efficient Compiler-Informed Secure Speculation*.
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 | Yun Chen*, **Ali Hajiabadi***, Trevor E. Carlson
GadgetSpinner: *A New Transient Execution Primitive using the Loop Stream Detector*.
Proceedings of 30^{th} IEEE International Symposium on High-Performance Computer Architecture (HPCA 2024), March 2024. Acceptance rate: 75/410 = 18.3%
∗Joint first-authors with equal contribution.
▶ *Analyzing and discovering vulnerabilities of the Loop Stream Detector (LSD) in Intel CPUs that enables cross-core transient execution attacks without requiring branch mistraining/poisoning.*
Paper | Artifact

HPCA'24 | Yun Chen, **Ali Hajiabadi**, Lingfeng Pei, Trevor E. Carlson
PREFETCHX: *Cross-Core Cache-Agnostic Prefetcher-Based Side-Channel Attacks.*
Proceedings of 30^{th} IEEE International Symposium on High-Performance Computer Architecture (HPCA 2024), March 2024. Acceptance rate: 75/410 = 18.3%
▶ *Extensive reverse-engineering of an undocumented Intel prefetcher, called XPT (an LLC miss predictor) that enables cross-core cache-agnostic side and covert channels.*
Paper | Artifact

ICCAD'23 | Arash Pashrashid, **Ali Hajiabadi**, Trevor E. Carlson
HIDFIX: *Efficient Mitigation of Cache-based Spectre Attacks through Hidden Rollbacks.*
Proceedings of 42^{nd} IEEE/ACM International Conference on Computer-Aided Design (ICCAD 2023), November 2023. Acceptance rate: 172/768 = 22.4%
▶ *Co-designing detection and mitigation to defend cache-based Spectre with no performance overhead; extensive study of existing detection/mitigation combinations and proposing attacks to bypass them.*
Paper

ICCAD'22 | Arash Pashrashid, **Ali Hajiabadi**, Trevor E. Carlson
Fast, Robust and Accurate Detection of Cache-based Spectre Attack Phases.
Proceedings of 41^{st} IEEE/ACM International Conference on Computer-Aided Design (ICCAD 2022), November 2022. Acceptance rate: 132/586 = 22.5%
▶ *(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.*
Paper | Github

ASPLOS'21 | **Ali Hajiabadi**, Andreas Diavastos, Trevor E. Carlson
NOREBA: *A Compiler-Informed Non-speculative Out-of-Order Commit Processor.*
Proceedings of 26^{th} ACM International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS 2021). April 2021. Acceptance rate: 75/398 = 18.8%
▶ *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.*
Paper | Extended Abstract | Short Slides | Short Talk | Slides | Full Talk

TOCS'21 | Mohammad Sadrosadati, Amirhossein Mirhosseini, **Ali Hajiabadi**, Seyed Borna Ehsani, Hajar Falahati, Hamid Sarbazi-Azad, Mario Drumond, Babak Falsafi, Rachata Ausavarungnirun, Onur Mutlu
Highly Concurrent Latency-tolerant Register Files for GPUs.
In ACM Transactions on Computer Systems (TOCS), 2021.
▶ *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.*
arXiv Paper

CGO'21 | Harish Patil, Alexander Isaev, Wim Heirman, Alen Sabu, **Ali Hajiabadi**, Trevor E. Carlson
ELFies: Executable Region Checkpoints for Performance Analysis and Simulation.
Proceedings of 19^{th} IEEE International Symposium on Code Generation and Optimization (CGO 2021), March 2021. Acceptance rate: 31/89 = 34.8%
▶ *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.*
Paper | Github

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

▶ **Sharif University of Technology, Tehran, Iran**

SPRING 2017 **Teaching Assistant** (assignments and projects), *CE323 Computer Architecture* (BSc) – Lecturer: Prof. Hamid Sarbazi-Azad
FALL 2017/2018 **Teaching Assistant** (tutorial instructor, assignments and projects), *CE453 Real-Time Systems* (BSc) – 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** *2^{nd} Young Architect Workshop at the 25^{th} 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:	LaTeX, Microsoft Word