Jeonghyun **Woo**

Ph.D. Student · Electrical and Computer Engineering · The University of British Columbia (UBC)

4025, 2332 Main Mall, Vancouver, BC, Canada V6T 1Z4

(+1) 778-929-7902 | jhwoo36@ece.ubc.ca | jeonghyunwoo0306.github.io | jeonghyunwoo0306 | LinkedIn | Google Scholar

Research Interests

Hardware/Systems Security, Computer Architecture, Memory Systems, and AI/ML Systems, with specific emphasis on:

- **Memory System Security:** Uncovering fundamental vulnerabilities (e.g., RowHammer, Denial-of-Service, timing side-channels) in memory systems to drive the design of secure and scalable mitigations. I am also interested in extending these robust security guarantees to emerging memory technologies, including CXL and Processing-in-Memory (PIM).
- **Trustworthy AI & LLM Security:** Investigating hardware-induced privacy risks in high-performance LLM serving systems. My research targets LLM jailbreaking and side-channel leakage arising from model- and system-level optimizations, such as Mixture-of-Experts (MoE) and speculative decoding, and develops lightweight, cross-layer defenses that eliminate these threats without compromising inference efficiency.
- **Memory Systems for ML:** Designing high-performance, energy-efficient memory architectures for scalable ML inference and training. I focus on hardware- and system-level optimizations, including KV cache management and intelligent memory controller designs, to address power and bandwidth bottlenecks in modern AI platforms.

Education

The University of British Columbia (UBC) — *Vancouver, BC, Canada*

Ph.D. in Electrical and Computer Engineering — *Sep. 2022 - May 2026 (Expected)*

- Advisor: Prof. Prashant Nair
- **Dissertation: Secure and Low-Overhead RowHammer Mitigations for Scalable Memory Systems**
- GPA: 4.00/4.00

Hanyang University (HYU) — *Seoul, South Korea*

M.S. in Electronics and Computer Engineering — *Mar. 2018 - Feb. 2020*

- Advisor: Prof. Ki-Seok Chung
- **Thesis: RowHammer Mitigation Architecture for Highly Reliable DRAM**
- GPA: 4.00/4.00

Hanyang University (HYU) — *Seoul, South Korea*

B.S. in Electronic Engineering — *Mar. 2012 - Feb. 2018*

- Advisor: Prof. Ki-Seok Chung
- **Senior Thesis: Implementation of an FPGA-based CNN Accelerator using SDSoC**
- GPA: 3.89/4.00 **(Graduating with Honors - Summa Cum Laude)**

Publications

Preprints and In Submission

[P.2] **Jeonghyun Woo**, Junsu Kim, Aamer Jaleel, and Prashant J. Nair. **"Loaded Dices: Solving the Non-Selection Problem for Scalable Probabilistic RowHammer Defense"**. *Submitted to 53rd Annual International Symposium on Computer Architecture **(ISCA'26)***. 2025.

[P.1] Zachary Coalson, **Jeonghyun Woo**, Chris S. Lin, Joyce Qu, Yu Sun, Shiyang Chen, Lishan Yang, Gururaj Saileshwar, Prashant J. Nair, Bo Fang, and Sanghyun Hong. **"PrisonBreak: Jailbreaking Large Language Models with at Most Twenty-Five Targeted Bit-flips"**. *arXiv Preprint*. 2025. [arXiv]

Conference Publications

[C.5] **Jeonghyun Woo**, Joyce Qu, Gururaj Saileshwar, and Prashant J. Nair. **"When Mitigations Backfire: Timing Channel Attacks and Defense for PRAC-Based RowHammer Mitigations"**. *In 52nd Annual International Symposium on Computer Architecture **(ISCA'25)***. June 2025. (Acceptance Rate: 23.1%). [Paper] [Code] [Slides]
[Artifact Evaluated: Available, Functional, Reproduced]

[C.4] **Jeonghyun Woo**, Shaopeng (Chris) Lin, Prashant J. Nair, Aamer Jaleel, and Gururaj Saileshwar. **"QPRAC: Towards Secure and Practical PRAC-based Rowhammer Mitigation using Priority Queues"**. *In 31st International Symposium on High-Performance Computer Architecture **(HPCA'25)***. Mar. 2025. (Acceptance Rate: 21.0%). [Paper] [Code] [Slides]
[Artifact Evaluated: Available, Functional, Reproduced]
[Distinguished Artifact Award]

[C.3] **Jeonghyun Woo** and Prashant J. Nair. **"DAPPER: A Performance-Attack-Resilient Tracker for RowHammer Defense"**. *In 31st International Symposium on High-Performance Computer Architecture **(HPCA'25)***. Mar. 2025. (Acceptance Rate: 21.0%). [Paper] [Slides]

[C.2] **Jeonghyun Woo**, Gururaj Saileshwar, and Prashant J. Nair. **"Scalable and Secure Row-Swap: Efficient and Safe Row Hammer Mitigation in Memory Systems"**. *In 29th International Symposium on High-Performance Computer Architecture **(HPCA'23)***. Feb. 2023. (Acceptance Rate: 25.0%). [Paper] [Code] [Slides]
[Artifact Evaluated: Available, Functional, Reproduced]
[Best Paper Award: One of Two Best Papers in 364 Submissions]

[C.1] Kwangrae Kim, **Jeonghyun Woo**, Junsu Kim, and Ki-Seok Chung. **"HammerFilter: Robust Protection and Low Hardware Overhead Method for RowHammer"**. *In 39th International Conference on Computer Design **(ICCD'21)***. Oct. 2021. (Acceptance Rate: 24.4%). [Paper] [Slides] [Video]

Workshop Publications and Posters

[W.3] Chris S. Lin, **Jeonghyun Woo**, Prashant J. Nair, Gururaj Saileshwar. **"CnC-PRAC: Coalesce, not Cache, Per Row Activation Counts for an Efficient in-DRAM Rowhammer Mitigation"**. *Fifth Workshop on DRAM Security **(DRAMSec'25)** co-located with **ISCA 2025***. June 2025. [Paper]

[W.2] Shih-Lien Lu, **Jeonghyun Woo**, Prashant J. Nair. **"Counterpoint: One-Hot Counting for PRAC-Based RowHammer Mitigation"**. *Fifth Workshop on DRAM Security **(DRAMSec'25)** co-located with **ISCA 2025***. June 2025. [Paper]

[W.1] Kwangrae Kim, Junsu Kim, **Jeonghyun Woo**, and Ki-Seok Chung. **"HammerFilter: Robust Protection and Low Hardware Overhead Method for Row-Hammering"**. *Work-in-Progress (WIP) poster in 58th Design Automation Conference **(DAC'21)***. Dec. 2021. [Poster]

Domestic (Korean) Conference Publications

[D.2] **Jeonghyun Woo** and Ki-Seok Chung. **"A Method to Find the Optimal Probability for Probability-driven Additional Row Refresh to Prevent DRAM Row Hammering"**. *In The Korean Institute of Communications and Information Sciences Winter Conference*. Jan. 2019.

[D.1] Changwoo Lee*, **Jeonghyun Woo***, Sang-Soo Park, and Ki-Seok Chung. **"Implementation of an FPGA-based CNN Accelerator using SDSoC"**. *In The Korean Institute of Communications and Information Sciences Fall Conference*. Nov. 2017. (*Equal Contribution). [Code: 300+ Stars]
[Outstanding Paper Award]

Honors and Awards

2023	**HPCA 2023 Best Paper Award** → One of Two Best Papers in 364 Submissions	*Canada*
2025	**HPCA 2025 Distinguished Artifact Award**	*USA*
2022-2025	Faculty of Applied Science Graduate Award, The University of British Columbia (UBC) → $24,800 CAD in Total	*Canada*
2025	ISCA Student Travel Grant	*Japan*
2023, 2025	HPCA Student Travel Grant	*Canada and USA*
2018-2019	Hanyang Graduate School Scholarship → 70% of Tuition (≈ $9,200 CAD per Year)	*South Korea*
2016, 2017	Hanyang Academic Excellence Award → Top 1% ranked in University (≈15,000 Students)	*South Korea*
2016-2017	Hanyang Alumni Association Scholarship → Full Tuition (≈$10,000 CAD per Year)	*South Korea*
2016	Excellent Tutor Award in Engineering Mathematics Tutoring Program, Hanyang University (HYU)	*South Korea*
2012-2013	Hanyang University Scholarship → Full Tuition (≈$10,000 CAD per Year)	*South Korea*

Experience

Systems and Architectures (STAR) Lab, The University of British Columbia (UBC) — *Vancouver, BC, Canada*
Graduate Research Assistant — *Sep. 2022 - Present*
- Advisor: Prof. Prashant Nair
- Leading research on hardware security, scalable memory systems, and Trustworthy AI, resulting in publications at top-tier venues (**ISCA** and **HPCA**).

The University of British Columbia (UBC) — *Vancouver, BC, Canada*
Graduate Teaching Assistant — *Sep. 2022 - Apr. 2025*
- Computer Architecture (CPEN 411): Fall 2022, Fall 2023, and Fall 2024
- Digital Systems and Microcomputers (CPEN 312): Spring 2025

Architecture Research Group (ARG), NVIDIA Research — *Westford, MA, USA*
Research Intern — *May 2024 - Aug. 2024*
- Manager: Dr. David Nellans | Mentor: Dr. Aamer Jaleel
- Investigated secure and low-overhead Per Row Activation Counting (PRAC)-based RowHammer mitigations, resulting in publication at **HPCA 2025**.

Vertical Systems Research (VSR), Micron Technology — *Folsom, CA, USA*
Systems Research Engineering Intern — *May 2023 - Aug. 2023*
- Manager: Ameen Akel | Mentor: Dr. Chun-Yi Liu
- Investigated RowHammer solutions for future High-Bandwidth Memory (HBM).

Systems Platform Research Group, University of Illinois Urbana-Champaign (UIUC) — *Champaign, IL, USA*
Graduate Research Assistant — *Aug. 2020 - Jan. 2021*
- Advisor: Prof. Jian Huang
- Explored integration of Non-Volatile Memory (NVM) into programmable switches and GPUs.

Embedded System on Chip (ESoC) Lab, Hanyang University (HYU) *Seoul, South Korea*
Graduate Research Assistant *Mar. 2018 - Feb. 2020*

- Advisor: Prof. Ki-Seok Chung
- Proposed reliable and low-overhead mechanisms for RowHammer mitigation and retention-aware refresh in highly scaled DRAMs.
- Implemented an FPGA-based Foveated Rendering decoder using Verilog for an industry-funded project with LG Display.

Hanyang University (HYU) *Seoul, South Korea*
Graduate Teaching Assistant *Mar. 2018 - Dec. 2019*

- VLSI Engineering (ELE 3081): Fall 2019
- SoC Design (ITE 4003): Spring 2018

Teaching and Mentoring Experience

Teaching Experience

Computer Architecture (CPEN 411) *University of British Columbia (UBC)*
Teaching Assistant *2022 - 2024*

- Redesigned the laboratory curriculum by migrating assignments from SimpleScalar to the state-of-the-art **ChampSim** simulator.
- Led labs and tutorials, implemented auto-graders, held office hours, and graded exams.

Digital Systems and Microcomputers (CPEN 312) *University of British Columbia (UBC)*
Teaching Assistant *Jan. 2025 - Apr. 2025*

- Led labs, held office hours, and graded exams and assignments.

VLSI Engineering (ELE 3081) *Hanyang University (HYU)*
Teaching Assistant *Sep. 2019 - Dec. 2019*

- Led labs, held office hours, and graded exams and assignments.

SoC Design (ITE 4003) *Hanyang University (HYU)*
Teaching Assistant *Mar. 2018 - June 2018*

- Designed and deployed comprehensive lab assignments for Altera FPGA boards.
- Led labs and graded exams and assignments.

Mentoring Experience

Junsu Kim *University of British Columbia (UBC)*
Ph.D. Student *Jan. 2020 - Current*

- Mentored undergraduate research on RowHammer security, resulting in a Work-in-Progress poster at **DAC'21** and a full paper at **ICCD'21**.
- Currently mentoring Ph.D. research on efficient LLM inference.

Kwangrae Kim *Hanyang University (HYU)*
Ph.D. Student *Jan. 2019 - Dec. 2021*

- Guided Ph.D. research on RowHammer security, resulting in a Work-in-Progress poster at **DAC'21** and a full paper at **ICCD'21**.

Talks

Nov. 2025	**Towards Secure and Scalable Memory Systems: From RowHammer Attacks to Hardware-Induced LLM Jailbreaks**, CASYS Seminar @ KAIST	*Remote*
June 2025	**When Mitigations Backfire: Timing Channel Attacks and Defense for PRAC-Based RH Mitigations**, ISCA'25	*Tokyo, Japan*
Mar. 2025	**QPRAC: Towards Secure and Practical PRAC-based Rowhammer Mitigation using Priority Queues**, HPCA'25	*Las Vegas, USA*
Mar. 2025	**DAPPER: A Performance-Attack-Resilient Tracker for RowHammer Defense**, HPCA'25	*Las Vegas, USA*
Aug. 2024	**Towards Secure and Low-Overhead PRAC-Based RowHammer Mitigations**, End-of-Intern Talk at NVIDIA	*Westford, USA*
Aug. 2023	**RowHammer Mitigations for Future High-Bandwidth Memory**, End-of-Intern Talk at MICRON	*Folsom, USA*
Feb. 2023	**Scalable and Secure Row-Swap: Efficient and Safe Row Hammer Mitigation in Memory Systems**, HPCA'23	*Montreal, Canada*
Nov. 2017	**Implementation of an FPGA-based CNN Accelerator using SDSoC**, KICS'17 Fall Conference	*Daegu, South Korea*

Academic Service

Program Committee Member

- 2026 IEEE International Symposium on High-Performance Computer Architecture (HPCA 2026) – Light PC

Artifact Evaluation Committee Member

- 2025 IEEE International Symposium on Workload Characterization (IISWC 2025)

Invited Reviewer

- IEEE Transactions on Very Large Scale Integration (VLSI) Systems (TVLSI) 2025

Student Volunteer

- SPICE Workshop Co-Located with MICRO 2025
- 2024 IEEE International Symposium on Workload Characterization (IISWC 2024)
- 2023 International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS 2023)

Academic Projects

Investigating the Potential of Data Compression for Optimized LLC Replacement *Advanced Computer Architecture*
The University of British Columbia (UBC), Instructor: Prof. Mieszko Lis *Jan. 2023 - Apr. 2023*

- Conducted a comprehensive evaluation of existing Last-Level Cache (LLC) replacement policies.
- Demonstrated that 72.7% of cache lines are compressible by 10B or more, highlighting the potential for compression-aware replacement.
- Proposed a preliminary compression-assisted replacement policy to optimize hit rates while minimizing metadata storage overhead.

Revisiting Address Translation on Intel Optane DC PMEM using Big-Memory Applications *Graduate Operating Systems*
The University of British Columbia (UBC), Instructor: Prof. Margo Seltzer *Sep. 2022 - Dec. 2022*

- Quantified address translation overheads in Optane DC PMEM systems using graph processing, HPC, and genomics workloads.
- Identified significant 4KB page bottlenecks and demonstrated that Transparent Huge Pages reduce overhead for memory-intensive applications.

Implementing Forward Operation of a Modified LeNet-5 in CUDA *Applied Parallel Programming*
University of Illinois at Urbana-Champaign (UIUC) *Nov. 2020 - Dec. 2020*

- Implemented optimized convolutional forward passes in CUDA leveraging shared memory tiling, constant memory, and loop unrolling.
- Conducted performance analysis using Nsight Systems and Nsight Compute to identify and eliminate memory bottlenecks.
- Source Code: https://github.com/jeonghyunwoo0306/ece408PJ_Fa2020

Skills

Programming Languages C/C++, Python, Perl, CUDA, Verilog, Bash, Assembly Language, Go
Simulators Ramulator, ChampSim, Gem5, DRAMSim2, GPGPU-Sim, MGPUSim
Tools Pin, SimPoint, Xilinx Vivado, Xilinx SDSoC, Intel Quartus

Relevant Coursework

- Advanced Computer Architecture (UBC)
- Graduate Operating Systems (UBC)
- Applied Parallel Programming (UIUC)
- SoC Design (HYU)
- VLSI Engineering (HYU)
- Embedded System Design (HYU)