Jeonghyun **Woo**

PH.D. STUDENT · ELECTRICAL AND COMPUTER ENGINEERING · 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

My research broadly spans the area of **computer architecture/systems, security, memory systems, and AI/ML**, with specific emphasis on the following areas:

- **Memory Security:** Developing techniques to secure memory systems, with a focus on RowHammer attacks and defenses. Investigating novel security attacks, performance degradation (Denial-of-Service) attacks, and timing-side channel vulnerabilities. Actively developing secure and low-overhead RowHammer mitigations, including per-row activation counting (PRAC)-based solutions, which are expected to become standard RowHammer mitigations for future DRAM products.
- **AI/ML Security:** Investigating emerging threats in AI/ML security, including LLM Jailbreaking attacks, and developing robust defenses to mitigate these risks.
- **Microarchitecture Designs:** Designing high-performance, energy-efficient microarchitectures by leveraging advanced compression techniques for prefetching, branch prediction, and cache replacement policies to optimize system efficiency.

Education

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

PH.D. IN ELECTRICAL AND COMPUTER ENGINEERING — *Sep. 2022 - Nov. 2026 (Expected)*

- Advisor: Prof. Prashant Nair
- 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
- **Dissertation: Row-hammering Mitigation Architecture for High 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
- **Dissertation: 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.1] Zachary Coalson, **Jeonghyun Woo**, Shiyang Chen, Yu Sun, Lishan Yang, Prashant Nair, Bo Fang, and Sanghyun Hong. **"PrisonBreak: Jailbreaking Large Language Models with Fewer Than Twenty-Five Targeted Bit-flips"**. *In 34th USENIX Security Symposium **(USENIX SEC'25)***. 2025. **[Arxiv]**

CONFERENCE PUBLICATIONS

[C.5] **Jeonghyun Woo**, Joyce Qu, Gururaj Saileshwar, and Prashant Nair. **"When Mitigations Backfire: Timing Channel Attacks and Defense for PRAC-Based Rowhammer Mitigations"**. *In 52nd Annual International Symposium on Computer Architecture **(ISCA'25)***. To Appear. (Acceptance Rate: 23.1%).

[C.4] **Jeonghyun Woo**, Shaopeng (Chris) Lin, Prashant 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]**
[Distinguished Artifact Award]

[C.3] **Jeonghyun Woo** and Prashant 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 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]**
[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.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**	*Las Vegas, USA*
2023, 2025	HPCA 2023 Student Travel Grant	*Canada, USA*
2022-2024	Faculty of Applied Science Graduate Award, University of British Columbia (UBC) → $16,600 CAD in Total	*Canada*
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	Hanyang Academic Excellence Award → Top 3% 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, University of British Columbia (UBC)
Vancouver, BC, Canada

Graduate Research Assistant *Sep. 2022 - Present*

- Advisor: Prof. Prashant Nair
- Conducting research on computer architecture, memory systems, security, and AI/ML.
- Publishing papers in top-tier architecture and security venues and delivering presentations.

University of British Columbia (UBC)
Vancouver, BC, Canada

Graduate Teaching Assistant *Sep. 2022 - Present*

- 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 and Mentor: Dr. Aamer Jaleel
- Explored secure and low-overhead Per Row Activation Counting (PRAC)-based RowHammer mitigations.

Vertical Systems Research (VSR), Micron Technology
Folsom, CA, USA

Sytems Research Engineering Intern *May. 2023 - Aug. 2023*

- Manager: Ameen Akel and Mentor: Dr. Chun-Yi Liu
- Explored RowHammer solutions for future High-Bandwidth Memory (HBM).

Systems Platform Research Group, University of Illinois Urbana-Champaign (UIUC) *Champagin, IL, USA*

Graduate Research Assistant *Aug. 2020 - Jan. 2021*

- Advisor: Prof. Jian Huang
- Integrated Non-Volatile Memory (NVM) into programmable switch data planes, achieving 2× lower packet latency than the prior TEA approach while maintaining line-rate packet processing.
- Explored crash consistency challenges in integrating NVM into GPUs, demonstrating inefficiencies in existing solutions via architectural simulations.

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 a reliable, low-overhead probabilistic RowHammer mitigation surpassing the state-of-the-art PARA and PRoHIT.
- Designed a new efficient retention-aware refresh scheme for highly scaled-down 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*

- Led labs/tutorials, implemented auto graders for assignments, 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 - Jun. 2018*

- Developed lab assignments on Altera FPGA boards, led labs, and graded exams and assignments.

Talks

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*

Service

Sep. 2024 **Student Volunteer**, at ISSWC’24 *Vancouver, Canada*

Mar. 2023 **Student Volunteer**, at ASPLOS’23 *Vancouver, Canada*

Academic Projects

Investigating the Potential of Data Compression for Optimized LLC Replacement *Advanced Computer Architecture*

University of British Columbia (UBC), Instructor: Prof. Mieszko Lis *Jan. 2023 - Apr. 2023*

- Conducted a comprehensive evaluation of existing LLC replacement methods to assess their effectiveness and limitations.
- Demonstrated 72.7% of cache lines are compressible by 10B or more, showing the potential of using compression for better replacement policies.
- Proposed a preliminary compression-assisted replacement method to optimize performance while minimizing storage overhead.

Revisiting Address Translation on Intel Optane DC PMEM using Big-Memory Applications

Graduate Operating Systems

University of British Columbia (UBC), Instructor: Prof. Margo Seltzer

Sep. 2022 - Dec. 2022

- Quantified address translation overhead in Optane DC PMEM systems using graph processing, HPC, and genomics workloads.
- Showed significant overhead with 4KB pages and demonstrated huge pages reduce overhead for applications sized tens of GB.

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 five optimized forward-pass of convolutional layers using CUDA by leveraging shared memory, constant memory, and loop unrolling.
- Performed performance analysis with GPU performance profiling tools Nsight-Systems and Nsight-Compute.
- Source Code: https://github.com/jeonghyunwoo0306/ece408PJ_Fa2020

32-Bit 5-Stage Pipelined MIPS Processor

Computer Architecture

Hanyang University (HYU)

Apr. 2016 - Jun. 2016

- Implemented a 32-bit 5-stage pipelined MIPS processor using Verilog.
- Performed an FPGA demonstration on Xilinx ZedBoard.

8-Bit LCD Password Timer

Microprocessor

Hanyang University (HYU)

Nov. 2013 - Dec. 2013

- Implemented an 8-bit LCD password timer using Assembly Language.

Skills

Programming Languages	C/C++, Python, Perl, CUDA, Verilog, Bash Script, 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
- Embedded System Design, HYU
- VLSI Engineering, HYU
- Computer Architecture, HYU
- Operating Systems, HYU
- Microprocessor, HYU
- Data Structures, HYU
- Digital Logic Design, HYU