

# 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](mailto:jhwoo36@ece.ubc.ca) | 🏠 [jeonghyunwoo0306.github.io](https://jeonghyunwoo0306.github.io) | 📄 [jeonghyunwoo0306](https://jeonghyunwoo0306.github.io) | 🔗 [LinkedIn](#) | 📖 [Google Scholar](#)

## Research Interests

Computer Architecture/Systems, Security, Memory Systems, and AI/ML, with specific emphasis on the following areas:

- **Memory Security:** Developing techniques for secure and reliable memory systems by exploring new attack vectors and unexplored vulnerabilities, such as denial-of-service (DoS) and timing side channels, and designing defenses against them. With a particular focus on RowHammer, I investigate both novel RowHammer-based attacks and practical mitigations, including low-overhead Per Row Activation Counting (PRAC)-based approaches that are expected to become standard in future DRAM products.
- **AI/ML Security:** Developing techniques to secure machine learning systems by investigating unexplored security risks caused by system- and hardware-level vulnerabilities. My research examines threats such as side-channel leakage from system-level optimizations (e.g., speculative decoding) and emerging vulnerabilities in large language models, and develops defenses to mitigate these risks.
- **Systems for ML:** Improving the efficiency of large language model (LLM) inference through techniques such as optimized speculative decoding and batching management.

## Education

### The University of British Columbia (UBC)

PH.D. IN ELECTRICAL AND COMPUTER ENGINEERING

- Advisor: [Prof. Prashant Nair](#)
- GPA: 4.00/4.00

Vancouver, BC, Canada

Sep. 2022 - Jul. 2026 (Expected)

### Hanyang University (HYU)

M.S. IN ELECTRONICS AND COMPUTER ENGINEERING

- Advisor: [Prof. Ki-Seok Chung](#)
- **Dissertation:** Row-hammering Mitigation Architecture for High Reliable DRAM
- GPA: 4.00/4.00

Seoul, South Korea

Mar. 2018 - Feb. 2020

### Hanyang University (HYU)

B.S. IN ELECTRONIC ENGINEERING

- 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)

Seoul, South Korea

Mar. 2012 - Feb. 2018

## 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 submission. 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)*. June 2025. (Acceptance Rate: 23.1%). [\[Paper\]](#) [\[Code\]](#) [\[Slides\]](#)
- [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.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	<b>HPCA 2023 Best Paper Award</b> → One of Two Best Papers in 364 Submissions	Canada
2025	<b>HPCA 2025 Distinguished Artifact Award</b>	USA
2025	ISCA Student Travel Grant	Japan
2023, 2025	HPCA Student Travel Grant	Canada and 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, The 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.

### The 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

#### SYSTEMS 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)

Champaign, 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.

### 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 - Jun. 2018

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

# Talks

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

# Academic Service

- 2026 **Light Program Committee Member**, IEEE International Symposium on High-Performance Computer Architecture (HPCA)
- 2025 **Artifact Evaluation Committee Member**, IEEE International Symposium on Workload Characterization (IISWC)
- 2025 **Invited Reviewer**, IEEE Transactions on Very Large Scale Integration (VLSI) Systems (TVLSI)
- 2024 **Student Volunteer**, IEEE International Symposium on Workload Characterization (IISWC)
- 2023 **Student Volunteer**, International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS)

# 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 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

THE 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](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, MGPU-Sim

**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