Ingab Kang

PhD Candidate @University of Michigan, CSE
mojomojo53@gmail.com | Homepage | Google Scholar | LinkedIn

SHORT SKILLSET AND RESEARCH INTRODUCTION

In my research, I am examining the susceptibility of real systems to Rowhammer attacks. My research provided me with a solid understanding of the memory system, the processor, and the OS. I have studied JEDEC DDR memory specifications, Intel and AMD processor documentations, and the Linux Kernel source code to knit together the necessary information to create the appropriate tool-chains for my research work. Furthermore, I have written micro architectural benchmarks testing out-of-order execution, memory operations, and used perf access MSRs to verify that the expected behavior of the machine matches the actual behavior (Intel 6th to 13th gen. AMD Zen 4,5). Most of my experiments were implemented in C/C++ with bits of Rust, as well as Python to automate experiments and parse results.
Prior to my PhD, I interned at Kakao Enterprise in South Korea where I was tasked with the optimization of transformer based NLP translation on the cloud and mobile devices. Moreover, I have benchmarked the app's permanence with CuDNN, ONNX, Apple ML, and Pytorch frameworks. During my Masters, my research focus was in computer architecture. I researched efficient memory deduplication and compression designs, as well as low overhead Rowhammer defenses. To measure the performance gain / overhead of the designs, I used architectural timing simulators(McSimA+, ZSim) to benchmark the designs and instrumentation tools to create benchmark traces for the simulation.

EDUCATION

- **Doctor of Philosophy, Computer Science and Engineering** Sep. 2020 - Summer 2025 (Expected)
  University of Michigan.
  Courses:
  Advanced Compilers - Used program profile to have LLVM insert lookup tables to cache values

- **Master of Science, Intelligent Systems** Mar. 2018 - Feb. 2020
  Seoul National University
  Courses:
  SoC Design Automation - Used System C to create custom hardware running MNIST Classifier
  Computer Interconnection Networks - Interconnect network fundamentals (Bisection bandwidth, mesh, ring, dragonfly, torus)

- **Bachelor of Science, Electrical and Computer Engineering** Mar. 2011 - Feb. 2018
  Seoul National University ∗ 2-year leave due to military service

SKILLS

- **Computer Architecture:** Memory Architecture
- **Reverse Engineering:** Micro architecture testing, Physical probing through logic analyzer
- **Proficient Programming Languages:** C/C++, Python, Rust, Assembly, Javascript
- **Instrumentation:** Intel Pin
- **Architectural Simulator:** McSimA+, ZSim
- **Performance Monitoring:** Perf
- **AI Framework** Pytorch, ONNX, CuDNN, Core ML

EXPERIENCE

- **Graduate Researcher, Hardware Security Lab, University of Michigan** Sep. 2020 – Current
  - Advisor: Daniel Genkin
  - Assessing and enhancing the severity of Rowhammer vulnerabilities in modern DDR4 DRAM
    - Created a new hammering pattern leveraging Bank-level parallelism on DDR4 memory, generating 7× more bit flips than SOTA [1].
    - Created a novel self-evicting hammering pattern, where every memory access causes an eviction in cache and hammers the memory. My work yielded 100× more bit flips than previous work in browsers and demonstrated significant degradation in DRAM integrity [1].
  - Testing the plausibility of Rowhammer bit flips on DDR5 DRAM and lastest systems (Intel 12th, 13th gen, AMD Zen4, 5)
    - Used logic analyzers attached to the memory bus to verify commands sent to the momory matches expected behavior.
    - Used memory access latency to reverse engineer the memory controller's DRAM refresh implementation.
  - Proof of concept exploits that leverage memory bit flips
    - Demonstrated that Rowhammer bit flips on DRAM can be leveraged to gain root privilege in under 5 minutes on Linux by flipping opcodes in Sudo binary[1].
    - Demonstrated how Rowhammer can be combined with the Spectre vulnerabilities to defeat previous Spectre mitigations and read arbitrary data using gadgets in the Linux kernel[3].
    - Created a novel cache side-channel to infer contiguous physical memory allocation. This resulted in the first Rowhammer attack in the browser (Firefox, Chrome) on default OS settings.
- **Intern, Context Part, Kakao Enterprise** Mar. 2020 – Aug. 2020
  - Optimized Mobile Neural Machine Translator (NMT)
    - Optimized NMT by modifying the transformer to cache values between model layers, which removed redundent computation. This reduced complexity from $O(n^3)$ to $O(n^2)$ and gained 2× speedup on average.
    - Deployed NMT using different ML frameworks (Apple Core ML, ONNX, Tensorflow, Pytorch)
- **Visiting Scholar, Computer Systems Laboratory, Cornell University** Oct. 2019 – Dec. 2019
  - Advisor: G. Edward Suh
  - Combining memory deduplication & compression [4]
    - Used Intel Pin to extract accessed memory data from executed benchmarks.
    - Ran ZSim architecture simulator to measure the speedup from the proposed scheme.
- **Graduate Researcher, SCALE, Seoul National University** Mar. 2019 – Feb. 2020
  - Advisor: Jung Ho Ahn
  - Created novel space-efficient in-DRAM Rowhammer mitigation mechanisms
    - TWiCe [6] reduces the need to count all ACTs to DRAM by pruning benign ACTs. Guarantees data integrity with no false positives.
    - CAT-TWO [5] optimizes the CAT mitigation scheme by 55% reduction in size and guarantees a mathematical bound for perfect mitigation. First work to propose rank-level mitigation technique.
- **Intern, Mobile Communications Business, Samsung Electronics** Jul. 2017 – Aug. 2017

  - Worked in the Mobile display division, aided in testing mobile phone displays.

PATENT

1. **US Patent 11,037,618**, Eojin Lee, **Ingab Kang**, and Jung Ho Ahn, Row hammer prevention circuit, a memory module including the row hammer prevention circuit, and a memory system including the memory module

PUBLICATIONS

1. **Ingab Kang**, Walter Wang, Jason Kim, Stephan van Schaik, Youssef Tobah, Daniel Genkin, Andrew Kwong, and Yuval Yarom, SledgeHammer: Amplifying Rowhammer via Bank-level Parallelism, *USENIX Security*, 2024
2. Youssef Tobah, Andrew Kwong, **Ingab Kang**, Daniel Genkin, and Kang G. Shin, Go Go Gadget Hammer: Flipping Nested Pointers for Arbitrary Data Leakage, *USENIX Security*, 2024
3. Youssef Tobah, Andrew Kwong, **Ingab Kang**, Daniel Genkin, and Kang G. Shin, SpecHammer: Combining Spectre and Rowhammer for new speculative attacks, *IEEE S&P*, 2022
4. Sungbo Park, **Ingab Kang**, Yaebin Moon, Jung Ho Ahn, and G. Edward Suh, BCD Deduplication: Effective Memory Compression Using Partial Cache-Line Deduplication, *ASPLOS* , 2021
5. **Ingab Kang**, Eojin Lee, and Jung Ho Ahn, CAT-TWO: Counter-based Adaptive Tree, Time Window Optimized, *IEEE Access*, 2020.
6. Eojin Lee, **Ingab Kang**, Sukhan Lee, G. Edward Suh, and Jung Ho Ahn, TWiCe: Preventing Row-hammering by Exploiting Time Window Counters, *ISCA*, 2019.
7. Kangjin Yoon, Taejun Park, Jihoon Kim, Weiping Sun, Sunwook Hwang, **Ingab Kang**, and Sunghyun Choi, COTA: Channel occupancy time adaptation for LTE in unlicensed spectrum, *DySPAN*, 2017.

SERVICES

· **Peer Review** USENIX Security 2022, IEEE Transactions on Computers 2023, 2024