KYUNGMI LEE

kyungmi@mit.edu | kyungmi-lee.github.io

EDUCATION

Massachusetts Institute of Technology, Cambridge, MA *2020-2024*
Ph.D. in Electrical Engineering & Computer Science

Thesis: Towards Secure Machine Learning Acceleration: Threats and Defenses Across Algorithms, Architecture, and Circuits
Thesis Advisor: Anantha P. Chandrakasan
Thesis Committee: Mengjia Yan, Joel S. Emer

Massachusetts Institute of Technology, Cambridge, MA *2018-2020*
S.M. in Electrical Engineering & Computer Science

Thesis: Improved Methodology for Evaluating Adversarial Robustness in Deep Neural Networks
Thesis Advisor: Anantha P. Chandrakasan

Seoul National University, Seoul, South Korea *2014-2018*
B.S. in Electrical & Computer Engineering

Summa Cum Laude, Rank: 1 / 118, GPA: 4.19 / 4.30

PROFESSIONAL EXPERIENCE

Postdoctoral Associate, Massachusetts Institute of Technology, Cambridge, MA June 2024 - Present
Research Laboratory of Electronics (Advisor: Anantha P. Chandrakasan)

Advanced Algorithms Research Intern, Analog Devices, Boston, MA June 2023 - Aug 2023
AI Solutions (Supervisor: Tao Yu)

Undergraduate Research Assistant, Seoul National University, Seoul, South Korea Mar 2018 - July 2018
Design Automation Lab (Advisor: Kiyoung Choi)

HONORS & AWARDS

MIT MTL Doctoral Dissertation Seminar, Winner, Fall 2024	2024
Bob Owens Best Student Paper Award, IEEE International Workshop on Signal Processing Systems (SiPS)	2021
Siebel Scholars, Class of 2020	2020
MIT Jacobs Presidential Fellowship	2018
Korea Foundation for Advanced Studies, Doctoral Fellowship	2018-2023
Undergraduate Fellowship, Semiconductor Industry Association	2017

PUBLICATIONS

Journals

[5] **Lee**, **Kyungmi** and Ashok, Maitreyi and Maji, Saurav and Agrawal, Rashmi and Joshi, Ajay and Yan, Mengjia and Emer, Joel S. and Chandrakasan, Anantha P., "Secure Machine Learning Hardware: Challenges and Progress," *IEEE Circuits and Systems Magazine*, vol. 25, no. 1, pp. 8–34, 2025.

[4] Saurav Maji, **Kyungmi Lee**, and Anantha P. Chandrakasan, "SparseLeakyNets: Classification Prediction Attack Over Sparsity-Aware Embedded Neural Networks Using Timing Side-Channel Information," *IEEE Computer Architecture Letters*, vol. 23, no. 1, pp. 133–136, 2024.

[3] Saurav Maji, **Kyungmi Lee**, Cheng Gongye, Yunsi Fei, and Anantha P. Chandrakasan, "An Energy-Efficient Neural Network Accelerator With Improved Resilience Against Fault Attacks," *IEEE Journal of Solid-State Circuits*, vol. 59, no. 9, pp. 3106–3116, 2024.

[2] Gabrielle Cahill, Annette A. Wang, **Kyungmi Lee**, Masaharu Sakagami, D. Bradley Welling, and Konstantina M. Stankovic, "Association of Stapedotomy Volume and Patient Sex With Better Outcome," *JAMA Otolaryngology–Head & Neck Surgery*, Aug. 2022.

[1] **Kyungmi Lee** and Anantha P. Chandrakasan, "Understanding the Energy vs. Adversarial Robustness Trade-Off in Deep Neural Networks," *Open Journal of Circuits and Systems*, vol. 2, pp. 843–855, 2021.

Conferences & Peer-reviewed Workshops

[4] **Kyungmi Lee**, Mengjia Yan, Joel S. Emer, and Anantha P. Chandrakasan, "SecureLoop: Design Space Exploration of Secure DNN Accelerators," in *56th Annual IEEE/ACM International Symposium on Microarchitecture*, 2023.

[3] Saurav Maji, **Kyungmi Lee**, Cheng Gongye, Yunsi Fei, and Anantha P. Chandrakasan, "An Energy-Efficient Neural Network Accelerator with Improved Protections against Fault-Attacks," in *IEEE 49th European Solid-State Circuits Conference, Student Research Preview (ISSCC 2023) Poster Award*, 2023.

[2] **Kyungmi Lee** and Anantha P. Chandrakasan, "SparseBFA: Attacking Sparse Deep Neural Networks With the Worst-case Bit Flips On Coordinates," in *IEEE International Conference on Acoustics, Speech and Signal Processing*, 2022.

[1] **Kyungmi Lee** and Anantha P. Chandrakasan, "Understanding the Energy vs. Adversarial Robustness Trade-Off in Deep Neural Networks," in *IEEE Workshop on Signal Processing Systems (SiPS), Bob Owens Best Student Paper Award*, 2021, pp. 46–51.

Preprints

[2] **Kyungmi Lee** and Anantha P. Chandrakasan, *Rethinking Empirical Evaluation of Adversarial Robustness Using First-Order Attack Methods*, 2020. arXiv: `2006.01304 [cs.LG]`.

[1] Euntae Choi, **Kyungmi Lee**, and Kiyoung Choi, *Autoencoder-Based Incremental Class Learning without Retraining on Old Data*, arXiv:1907.07872, 2019. eprint: `1907.07872` (cs.LG).

Under Review

[1] **Kyungmi Lee**, Gaurab Das, Donghyeon Han, and Anantha P. Chandrakasan, *Securing dnn acceleration from dram vulnerabilities with low-overhead authenticated encryption*, In Preparation, 2025.

Theses

[2] Kyungmi Lee, "Towards Secure Machine Learning Acceleration: Threats and Defenses Across Algorithms, Architecture, and Circuits," PhD thesis, Massachusetts Institute of Technology, Cambridge, MA, May 2024.

[1] Kyungmi Lee, "Improved Methodology for Evaluating Adversarial Robustness in Deep Neural Networks," M.S. thesis, Massachusetts Institute of Technology, Cambridge, MA, May 2020.

TEACHING

Hardware Architecture for Deep Learning MIT 6.812/825 (Currently 6.5930/1)
Teaching Assistant, Spring 2021 (Instructors: Vivienne Sze, Joel S. Emer)

PROFESSIONAL ACTIVITY

Reviewer

- IEEE Transactions on Circuits and Systems for Artificial Intelligence
- Journal of Signal Processing Systems

MENTORING

Undergraduate Students at MIT

- Gaurab Das, SuperUROP, 2023-2024 → M.Eng. at MIT (2024-2025)

Mentor for MIT EECS Graduate Application Assistance Program 2024

TALKS & PRESENTATIONS

- MIT Microsystems Technology Laboratory Doctoral Dissertation Seminar, “Towards Secure Machine Learning Acceleration: Threats and Defenses Across Algorithms, Architecture, and Circuits", Dec 2024
- ACE Center Liaison Meetings, “SecureLoop: Design Space Exploration of Secure DNN Accelerators", June 2024
- MIT AI Hardware Program Symposium, “SecureLoop: Design Space Exploration of Secure DNN Accelerators", Poster, May 2024
- New England Hardware Security Day, “SecureLoop: Design Space Exploration of Secure DNN Accelerators", Short Talk, Apr 2024
- MIT Research Review for Center for Integrated Circuits and Systems (CICS), “SecureLoop: Design Space Exploration of Secure DNN Accelerators", Nov 2023
- MIT Research Review for Center for Integrated Circuits and Systems (CICS), “SparseBFA: Attacking Sparse Deep Neural Networks with the Worst-case Bit Flips on Coordinates", May 2022