

Kyungmi Lee

6100 Main St., Duncan Hall 3103
Houston, TX 77005

✉ {firstname}.{lastname}@rice.edu 🏠 kyungmi-lee.github.io 🔗 Google Scholar

ACADEMIC POSITIONS

Assistant Professor, Rice University, Houston, TX 2026 - Current
Department of Computer Science

Postdoctoral Associate, Massachusetts Institute of Technology, Cambridge, MA 2024 - 2026
Research Laboratory of Electronics (Host: Anantha P. Chandrakasan)

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

PUBLICATIONS

Journals

- [J1] Kyungmi Lee, Gaurab Das, Donghyeon Han, Anantha P. Chandrakasan, **Securing DNN Acceleration From Off-Chip Memory Vulnerabilities With Low-Overhead Authenticated Encryption**, IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 34, no. 3, pp. 953–966, 2026. DOI: 10.1109/TVLSI.2025.3650411.
- [J2] Kyungmi Lee, Maitreyi Ashok, Saurav Maji, Rashmi Agrawal, Ajay Joshi, Mengjia Yan, Joel S. Emer, Anantha P. Chandrakasan, **Secure Machine Learning Hardware: Challenges and Progress**, IEEE Circuits and Systems Magazine, vol. 25, no. 1, pp. 8–34, 2025. DOI: 10.1109/MCAS.2024.3509376.
- [J3] Saurav Maji, Kyungmi Lee, 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. DOI: 10.1109/LCA.2024.3397730.
- [J4] Saurav Maji, Kyungmi Lee, Cheng Gongye, Yungsi Fei, 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. DOI: 10.1109/JSSC.2024.3374638.
- [J5] Gabrielle Cahill, Annette A. Wang, Kyungmi Lee, Masaharu Sakagami, D. Bradley Welling, Konstantina M. Stankovic, **Association of Stapedotomy Volume and Patient Sex With Better Outcome**, JAMA Otolaryngology–Head & Neck Surgery, Aug. 2022. DOI: 10.1001/jamaoto.2022.2142.
- [J6] Kyungmi Lee, Anantha P. Chandrakasan, **Understanding the Energy vs. Adversarial Robustness Trade-Off in Deep Neural Networks**, IEEE Open Journal of Circuits and Systems, vol. 2, pp. 843–855, 2021. DOI: 10.1109/OJCS.2021.3116244.

Conferences & Peer-Reviewed Workshop Proceedings

- [C1] Kyungmi Lee, Zhiye Song, Eun Kyung Lee, Xin Zhang, Tamar Eilam, Anantha P. Chandrakasan, **EnergAIzer: Fast and Accurate GPU Power Estimation Framework for AI Workloads**, in 2026 IEEE International Symposium on Performance Analysis of Systems and Software (ISPASS), 2026, pp. 435–447. DOI: 10.1109/ISPASS69572.2026.00049.

[C2] Jan Strzeszynski, Jianming Tong, [Kyungmi Lee](#), Nathan Xiong, Angshuman Parashar, Joel S. Emer, Tushar Krishna, Mengjia Yan, **SquareLoop: Explore Optimal Authentication Block Strategy for ML**, in International Workshop on Hardware and Architectural Support for Security and Privacy, ser. HASP '25, Association for Computing Machinery, 2025, pp. 37–45. DOI: 10.1145/3768725.3768732.

[C3] [Kyungmi Lee](#), Mengjia Yan, Joel Emer, Anantha Chandrakasan, **SecureLoop: Design Space Exploration of Secure DNN Accelerators**, in IEEE/ACM International Symposium on Microarchitecture, ser. MICRO '23, Toronto, ON, Canada: Association for Computing Machinery, 2023, pp. 194–208. DOI: 10.1145/3613424.3614273.

[C4] Saurav Maji, [Kyungmi Lee](#), Cheng Gongye, Yungsi Fei, Anantha P. Chandrakasan, **An Energy-Efficient Neural Network Accelerator with Improved Protections Against Fault-Attacks**, in IEEE 49th European Solid State Circuits Conference (ESSCIRC), **Student Research Preview (ISSCC'23) Best Poster**, 2023, pp. 233–236. DOI: 10.1109/ESSCIRC59616.2023.10268746.

[C5] [Kyungmi Lee](#), 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 (ICASSP), 2022, pp. 4208–4212. DOI: 10.1109/ICASSP43922.2022.9747337.

[C6] [Kyungmi Lee](#), Anantha P. Chandrakasan, **Understanding the Energy vs. Adversarial Robustness Trade-Off in Deep Neural Networks**, in IEEE International Workshop on Signal Processing Systems (SiPS), **Bob Owens Best Student Paper Award**, 2021, pp. 46–51.

HONORS & AWARDS

MIT MTL Doctoral Dissertation Award	2024
Bob Owens Best Student Paper Award, IEEE International Workshop on Signal Processing Systems	2021
Siebel Scholars, Class of 2020	2020
MIT Jacobs Presidential Fellowship	2018
Korea Foundation for Advanced Studies, Doctoral Fellowship	2018-2023

TEACHING

Teaching Assistant

- **Hardware Architecture for Deep Learning** (MIT 6.5930/1) Spring 2021
Graduate & senior undergraduate level course with ~30 students (Instructor: Vivienne Sze, Joel S. Emer)
Covers design and implementation of hardware architectures of accelerators and processors for deep learning algorithms. As a TA, I was responsible for developing lab assignments and mentoring final projects.

Related Program

- **MIT Kaufman Teaching Certificate** Fall 2025
A semester-long workshop for developing teaching skills offered by MIT Teaching + Learning Lab

MENTORING

Undergraduate/Master's Students at MIT

• Andrea Leang (Master of Engineering)	2026
• Jan Strzeszynski (Master of Engineering)	2026
• Arul Kolla (Undergraduate, MIT EECS Citadel Undergraduate Research and Innovation Scholar)	2026
• Christopher Mejia (Undergraduate)	2025
• Nathan Xiong (Undergraduate)	2025
• Steven Reyes (Undergraduate)	2025
• Kenneth Chap (Undergraduate)	2025
• Gaurab Das (Undergraduate)	2024

Other Mentoring Experiences

- MIT Research Mentoring Certificate 2025
- Mentor for MIT EECS Graduate Application Assistance Program 2024 - 2025

PROFESSIONAL SERVICE

Paper Review

- IEEE Transactions on Circuits and Systems 1: Regular Papers
- ACM Transactions on Architecture and Code Optimization
- IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems
- IEEE Transactions on Very Large Scale Integration Systems
- IEEE Open Journal of Circuits and Systems
- IEEE Journal of Solid-State Circuits
- IEEE Transactions on Circuits and Systems for Artificial Intelligence
- Journal of Signal Processing Systems

Program Committee

- IEEE International Symposium on Hardware Oriented Security and Trust (HOST) 2027
- IEEE International Symposium on High Performance Computer Architecture (HPCA) 2027
- ACM/IEEE International Symposium on Machine Learning for CAD (MLCAD) 2026
- IEEE International Conference on Cloud Engineering (IC2E), Industry Track 2025

Volunteering

- Bingo Networking Night at the IEEE CICC 2025, organized by the SSCS Women in Circuits

TALKS

- Securing AI from the Hardware Up: Efficient Designs from Architecture to Silicon
 - Arizona State University, Department of Electrical, Computer, and Energy Engineering Apr 2026
 - University of Pennsylvania, Department of Electrical and Systems Engineering Apr 2026
 - University of Minnesota Twin Cities, Department of Electrical and Computer Engineering Mar 2026
 - Columbia University, Department of Computer Science Mar 2026
 - Rice University, Department of Computer Science Mar 2026
 - University of Massachusetts Amherst, Department of Electrical and Computer Engineering Feb 2026
 - North Carolina State University, Department of Electrical and Computer Engineering Feb 2026
 - University of Washington, Department of Electrical and Computer Engineering Feb 2026
- Towards Secure Machine Learning Acceleration: Threats and Defenses Across Algorithms, Architecture, and Circuits
 - Worcester Polytechnic Institute ECE Graduate Seminar Course Feb 2025
 - MIT Microsystems Technology Laboratory Doctoral Dissertation Seminar Dec 2024
- Securing DNN Acceleration from Off-chip Vulnerabilities with Low-overhead Authenticated Encryption
 - MIT MTL - Samsung Semiconductor Research Fund Workshop Sept 2024
- SecureLoop: Design Space Exploration of Secure DNN Accelerators
 - SRC ACE Center Liaison Meetings June 2024
 - MIT AI Hardware Program Symposium (Poster) May 2024
 - New England Hardware Security Day (Short Talk) Apr 2024
 - MIT Research Review for Center for Integrated Circuits and Systems (CICS) Nov 2023
 - MIT MTL - Samsung Semiconductor Research Fund Workshop Sept 2023
- SparseBFA: Attacking Sparse Deep Neural Networks with the Worst-case Bit Flips on Coordinates
 - MIT Research Review for Center for Integrated Circuits and Systems (CICS) May 2022

MEDIA

- A faster way to estimate AI power consumption, MIT News Apr 2026
<https://news.mit.edu/2026/faster-way-to-estimate-ai-power-consumption-0427>
- Accelerating AI tasks while preserving data security, MIT News Oct 2023
<https://news.mit.edu/2023/accelerating-ai-tasks-while-preserving-data-security-1030>

INDUSTRY EXPERIENCE

Analog Devices, Boston, MA

2023

Advanced Algorithms Research Intern at AI Solutions

Developed generative AI model for speech enhancement and audio bandwidth extension