

# JOON KIM

joonkim1@berkeley.edu • (510)-529-6091 • [Homepage](#)

## EDUCATION

---

### University of California, Berkeley

May 2027 (Expected)

B.S. Electrical Engineering & Computer Science, GPA: 4.00/4.00

Current: CS270(Grad Algo.), CS294-180(Partition Functions: A+), EECS249B(Cyber-Physical Systems), CS194-302(Comp. Immunology)

CS174(Randomized Algo.), CS176(Comp. Bio), CS170(Algorithms: A+), CS188(AI), CS177(Algo. Econ), CS294-284(CSP & PCP Theorem), CS61B(Data Structures: A+), CS70(Discrete Math & Probability: A+), EECS16A/B (Circuits, Control, & Lin. Alg: A+), CS61A(Python: A+)

## RESEARCH INTERESTS

---

Bridging the gap between theoretical computer science and computational sciences; algorithms, statistics, and heuristic methods

## PUBLICATIONS

---

- **Network-Level Bit-Flipping Attacks on Cooperative Adaptive Cruise Control in 5G Environment** (*Submitted to VTC2026-Spring*); C. Duan, J. Kim, S. Ray; Proposed an efficient message recovery algorithm that defends the previous paper on 5G network bit-flipping attack for Cooperative Adaptive Cruise Control (CACC) systems; developed a novel pattern-matching mechanism
- **Bit-Flipping Attack Exploration and Countermeasure in 5G Network** ([IEEE MASS 2025](#)); J. Kim, C. Duan, S. Ray; Identified the vulnerability of 5G networks without costly integrity protection and designed a man-in-the-middle that either succeeds in flipping one bit or denies service; implemented a keystream-based method as a runtime-efficient alternative defense compared to NIA
- **In-Silo Federated Learning vs. Centralized Learning for Segmenting Acute and Chronic Ischemic Brain Lesions** ([Intelligence-Based Medicine](#)); J. Kim, H. Lee, W. Ryu, et al.; Comparative analysis of Federated and Centralized Learning on real-life non-i.i.d. brain lesion datasets of ~10,000 patients over 9 medical institutions; Poster at International Conference STROKE UPDATE 2024
- **Random Gradient Masking as a Defensive Measure to Deep Leakage in Federated Learning** ([Arxiv](#)); J. Kim, S. Park; Compared the efficacy of randomly masking gradients from Federated Learning submissions against other defenses against Deep Leakage from Gradients such as Pruning, Compression, and Noising on Convolution Neural Networks; Proposed masking as an effective defense

## RESEARCH EXPERIENCE

---

### Independent Theoretical CS Research

Berkeley, CA

Independent Researcher

Dec. 2025 - Current

- Investigating approximate Maximum Weighted Matching (MWM) and its dynamic matching variant; advised by Prof. Satish Rao

### Lawrence Berkeley Laboratory - Perlmutter Group

Berkeley, CA

Undergraduate Researcher

Sep. 2025 - Current

- Modeling the Carousel Lens to constrain cosmology using the multi-GPU node implementation of GIGA-Lens, an ML pipeline
- Investigating numerical instability of Stochastic Variational Inference with Gaussian Mixtures; advised by Prof. Xiaosheng Huang

### University of Florida REU: Secure and Sustainable Transportation

Gainesville, FL

Undergraduate Researcher, First Author

May. 2025 - Aug. 2025

- Explored network-level bit flipping attacks on 5G Connected and Automated Vehicles (CAV); advised by Prof. Sandip Ray
- Verified bit-flipping attack feasibility; proposed a keystream based shuffling defense that drastically lowers attack success rate
- Simulated CAV in OpenAirInterface (OAI) and proposed an error correction based defense; preparing conference submission

### Berkeley Artificial Intelligence Research - C.H.E.N. Lab

Berkeley, CA

Undergraduate Researcher

Jul. 2024 - Feb. 2025

- Designed zero-shot LLM pseudo-label pipeline to improve semi-supervised learning accuracy; advised by Prof. Irene Chen
- Experimented mainly on images; investigated LLM agents for image labeling such as CLIP and ViT, showed results on CIFAR-100
- Worked on RadQA dataset; implemented FixMatch and our new proposed method on a non-inference task for comparison

<b>JLK Group</b>	Seoul, South Korea
<i>Research Intern, First Author</i>	<i>Feb. 2024 - May. 2024</i>
<ul style="list-style-type: none"> <li>• Developed Federated Learning models reaching near identical performance to commercially deployed U-Net models using Python</li> <li>• Collaborated with four M.D. professionals to investigate the use of Federated Learning in medicine; advised by Dr. Wi-Sun Ryu</li> </ul>	
<b>Keimyung University</b>	Daegu, South Korea
<i>Independent Researcher</i>	<i>Feb. 2023 - Jul. 2024</i>
<ul style="list-style-type: none"> <li>• Proposed a randomized masking Federated Learning algorithm as an obfuscation technique against Deep Leakage for images</li> <li>• Designed experiments to compare performance-privacy trade-offs amongst SOTA defense algorithms; advised by Prof. Sejin Park</li> </ul>	
<b>Studio.geo @ UC Berkeley</b>	Berkeley, CA
<i>Undergraduate Researcher</i>	<i>Feb. 2022 - May. 2022</i>
<ul style="list-style-type: none"> <li>• Experimented Progressive-GAN on the Savio cluster to generate artificial maps using Python; advised by Prof. Clancy Wilmott</li> <li>• Pictures of 4x4 grid of generated maps of 256x256 pixels trained on real colored maps included in Prof. Wilmott's book proposal</li> </ul>	
<b>Independent Biomedical Research</b>	Seoul, South Korea
<i>Independent Researcher</i>	<i>Jan. 2020 - Jun. 2020</i>
<ul style="list-style-type: none"> <li>• Proposed a microarray analysis model for screening early schizophrenia with RNA genetic samples; overcame the lack of public RNA data with oversampling techniques and elected a Deep Neural Network model for inference; advised by Ph.D. Taehyun Kim</li> <li>• Verbally presented research findings at the 2020 Society of Interdisciplinary Business Research Conference as a representative</li> </ul>	

## PROFESSIONAL EXPERIENCE

---

<b>Impact AI</b>	Seoul, South Korea
<i>Data Engineering Intern</i>	<i>Jul. 2022 - Aug. 2022</i>
<ul style="list-style-type: none"> <li>• Developed a data preprocessing pipeline to pattern-match raw datasets of various formats from multiple companies using Python</li> <li>• Contributed in designing SQL-like UI/UX features for the main page of web and native applications deployed to client companies</li> </ul>	

## TEACHING EXPERIENCE

---

<b>CS70 Course Staff</b>	Berkeley, CA
<i>UCS1</i>	<i>Jan. 2026 - Current</i>
<ul style="list-style-type: none"> <li>• 4 hours of grading and 4 hours of discussion section assistance and office hours for CS70 (Discrete Mathematics and Probability)</li> </ul>	
<b>Computer Science Mentors</b>	Berkeley, CA
<i>CS70 Junior Mentor</i>	<i>Aug. 2025 - Dec. 2025</i>
<ul style="list-style-type: none"> <li>• Leading a group of five undergraduates in hour-long review sessions twice a week for CS70 (Discrete Mathematics and Probability)</li> </ul>	

## AWARDS

---

- **Korean Honor Scholarship 2025:** Received \$1500, selected 71 out of 356 students based on academic achievements