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 Coursework [SP26]: CS194-198(Network Theory), CS189(ML), CS294–308(Sum-of-Squares & Semidefinite Programming)

TCS: CS270(Graduate Algorithms), CS294-180(Partition Functions: **A+**), CS174(Randomized Algorithms), CS170(Algorithms: **A+**), CS177(Algorithmic Economics), CS294-284(Constraint Satisfaction Problems & PCP Theorem)

Computational Science: CS194-302(Comp. Immunology: **A+**), EECS249B(Cyber-Physical Systems), CS176(Comp. Bio), CS188(AI/RL)

Fundamentals: CS61A/B(SCIP, Data Structures: **A+**), CS70(Discrete & Probability: **A+**), EECS16A/B (Circuits, Control & Lin. Alg: **A+**)

Research Interests

Theoretical computer science (Approximations, Statistics, Sublinear Algorithms) and computational sciences (Comp. Bio, ML-Physics)

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
- In progress of proposing a simple extension to a Multiplicative Auction algorithm to accommodate fully dynamic matching

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
- Implemented and experimenting 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

JLK Group Seoul, South Korea

Research Intern, First Author *Feb. 2024 - May. 2024*

- Developed Federated Learning models reaching near identical performance to commercially deployed U-Net models using Python
- Collaborated with four M.D. professionals to investigate the use of Federated Learning in medicine; advised by Dr. Wi-Sun Ryu

Keimyung University Daegu, South Korea

Independent Researcher *Feb. 2023 - Jul. 2024*

- Proposed a randomized masking Federated Learning algorithm as an obfuscation technique against Deep Leakage for images
- Designed experiments to compare performance-privacy trade-offs amongst SOTA defense algorithms; advised by Prof. Sejin Park

Studio.geo @ UC Berkeley Berkeley, CA

Undergraduate Researcher *Feb. 2022 - May. 2022*

- Experimented Progressive-GAN on the Savio cluster to generate artificial maps using Python; advised by Prof. Clancy Wilmott
- Pictures of 4x4 grid of generated maps of 256x256 pixels trained on real colored maps included in Prof. WIlmott's book proposal

Independent Biomedical Research Seoul, South Korea
Independent Researcher *Jan. 2020 - Jun. 2020*

- 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
- Verbally presented research findings at the 2020 Society of Interdisciplinary Business Research Conference as a representative

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 Projects & Technical Reports

- **CS294-180**: Final Report and 70-minute lecture on Sublinear Sampling of Spanning Trees via Entropic Independence
- **CS 194-302**: Final Project on modeling drug-induced resistance continuum with a Hill-function modulated CTMC
- **CS 194-302**: Class presentation on Cohort Studies; explained MrVI, a double-layered VAE model for single-cell biology
- **EECS 249B**: Final Project on the runtime monitoring of stochastic contracts; mainly researched Scenario Optimization
- **CS176**: Literature Review on Cassiopeia, a parsimony-based phylogeny algorithm hybridizing ILP and Greedy methods

Professional Experience

Impact AI Seoul, South Korea
Data Engineering Intern *Jul. 2022 - Aug. 2022*

- Developed a data preprocessing pipeline to pattern-match raw datasets of various formats from multiple companies using Python
- Contributed in designing SQL-like UI/UX features for the main page of web and native applications deployed to client companies

Teaching Experience

CS70 Course Staff Berkeley, CA
UCS1 *Jan. 2026 - Current*

- 4 hours of grading and 4 hours of discussion section assistance and office hours for CS70 (Discrete Mathematics and Probability)

Computer Science Mentors Berkeley, CA
CS70 Junior Mentor *Aug. 2025 - Dec. 2025*

- Lead a group of five undergraduates in hour-long review sessions twice a week for CS70 (Discrete Mathematics and Probability)

Awards

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

Technical Skills

- LaTeX, Python, Java, C, PyTorch, TensorFlow, Flower(Federated Learning Framework), Docker, AWS