Ihyun Nam

ihyun@stanford.edu • Cell: (650) 695-3723 • Web: ihyunnam.github.io

Education

M.S. in Computer Science, Computer and Network Security Track — Jan 2023–Jun 2025
Stanford University (GPA: 3.9/4.3) — Stanford, CA

- Relevant coursework: Cryptography, Network Security, Operating Systems, and Distributed Systems

B.S. in Computer Science with Honors, Systems Track; B.S. in Mathematics — Sep 2020–Jun 2024
Stanford University (GPA: 3.7/4.3) — Stanford, CA

- Relevant coursework in Computer Science: Computational Complexity, Algorithms, and Mathematical Foundations of Computing
- Relevant coursework in Mathematics: Linear Algebra, Metalogic, Group Theory, Number Theory, Advanced Probability, and Combinatorics

Publications

Ihyun Nam, "The Avg-Act Swap and Plaintext Overflow Detection in Fully Homomorphic Operations Over Deep Circuits," appeared in the 14th ACM Conference on Data and Application Security and Privacy, June 2024 (pdf)

Xiaoyu He, Emily Huang, **Ihyun Nam**, Rishubh Thaper, "Shuffle Squares and Reverse Shuffle Squares," appeared in the European Journal of Combinatorics (Vol 116), February 2024 (pdf)
**Authors are listed in alphabetical order by last name, as is conventional in Mathematics*

Research

Title: Lasso Over Rings — Winter 2024–Present
Advisor: Professor Dan Boneh — Stanford, CA
Computer Science Department at Stanford University

- (In progress) Building a sparse polynomial commitment from Greyhound to create the Lasso proof system over rings

Title: Authentication Logging to a Public Blockchain — Winter 2024–Present
Advisor: Professor David Mazieres — Stanford, CA
Computer Science Department at Stanford University

- Proposed an improvement of the Larch authentication logging system that is secure against an untrusted log server and collusion between the log server and a relying party
- Proposed and implemented a bare metal blockchain in Rust with a t-out-of-n agreement protocol to log immutable records
- Implemented the core zero-knowledge proofs of the protocol in zkSNARK circuits; achieved a 1.2 second login time
- Received the IORH Grant for Blockchain Research

Title: The Avg-Act Swap and Plaintext Overflow Detection in Fully Homomorphic Operations Over Deep Circuits — Spring–Fall 2023
Stanford, CA
Advisor: Professor John Mitchell
Computer Science Department at Stanford University

- Proposed the Avg-Act Swap, which embeds an activation function at the end of AvgPool in neural networks over encrypted data with fully homomorphic encryption (FHE) for faster encrypted inference
- Designed and trained two FHE-friendly neural networks; optimized neural and cryptographic parameters to reduce encrypted inference time by 39%
- Used the Avg-Act Swap in Lenet-5 to reduce encrypted inference time by 28% when classifying encrypted MNIST images
- Proposed the first formalized plaintext overflow detection protocol for the Cheon-Kim-Kim-Song FHE scheme with IND-CPA security
- **Published and presented results at the 14th ACM Conference on Data and Application Security and Privacy (pdf)**
- **Presented results at the Symposium for Undergraduate Research and Public Service at Stanford**

Title: Client Identification Using Unsupervised Learning on Server Name Indication — Spring–Summer 2023

Advisor: Professor Zakir Durumeric Stanford, CA
Computer Science Department at Stanford University

- Proposed and built a novel client identification tool based on unsupervised learning on server name indication and clustering
- Proposed an optimized mapping between clients and domain names based on frequency and exclusivity of connections
- Showed that state-of-the-art client identification tools fail to identify up to 90% of clients in real networks
- Showed that our tool identifies the most associated domain names for at least 60% of clients
- Uploaded preprint to arXiv (pdf)

Title: A Survey of Multivariate Polynomial Commitment Schemes Winter–Spring 2022
Advisor: Professor Dan Boneh Stanford, CA
Computer Science Department at Stanford University

- Developed a survey of 8 multivariate polynomial commitment schemes including Dew, Dory, and Orion
- Analyzed correctness and security properties of each scheme
- Uploaded survey to arXiv (pdf)

Title: Shuffle Squares and Reverse Shuffle Squares Summer 2021
Advisor: Dr. Pawel Grzegrzolka Stanford, CA
Stanford Undergraduate Research Institute in Mathematics

- Proved the Henshall-Rampersad-Shallit conjecture to enumerate shuffle squares
- Disproved a companion conjecture on reverse shuffle squares, and proposed and proved a novel alternative
- Suggested applications in deletion channel error correcting codes
- **Published results at the European Journal of Combinatorics (pdf)**
- **Presented results at the Symposium for Undergraduate Research and Public Service at Stanford**

Talks

"The Avg-Act Swap and Plaintext Overflow Detection in Homomorphic Operations Over Deep Circuits," presentation at the 14th ACM Conference on Data and Application Security and Privacy — Jun 2024, Porto, Portugal

"The Avg-Act Swap: Towards Faster Machine Learning Applications of Fully Homomorphic Encryption," poster presentation at the Symposium for Undergraduate Research and Public Service at Stanford University — Fall 2023, Stanford, CA

"Shuffle Squares and Reverse Shuffle Squares," poster presentation at the Symposium for Undergraduate Research and Public Service at Stanford University — Fall 2022, Stanford, CA

Teaching

Teaching Assistant for Math 19 (Calculus) Fall 2024
Stanford University Stanford, CA

- Led office hours (5hrs/week) for 300 students, held exam review sessions, and wrote and graded midterm and final exams

Teaching Assistant for Hack Lab (Introduction to Cybersecurity) Fall 2023
Stanford University Stanford, CA

- Led lab sections on exploiting and defending various web vulnerabilities (1hr/week), held office hours (1hr/week) for 120 students, and wrote and proctored exams
- Transitioned virtual machine from GCP virtual Kali attack machines and targets to hosting in a new on-prem Proxmox cluster

Teaching Assistant and Residential Counselor Summer 2023
Stanford University Mathematics Camp Stanford, CA

- Led cryptography research sessions (7hrs/week), led problem sessions on group theory (3hrs/day), graded daily assignments, and organized recreational activities for 130 high school students

Honors

The Hoefer Prize for Excellence in Undergraduate Writing Spring 2024
Stanford University Stanford, CA

- One of 7 theses for the "writing in the major" program recognized for the quality of writing

Conference Scholarship for the Richard Tapia Conference — Summer 2023, Dallas, Texas
CMD-IT/ACM Richard Tapia Celebration of Diversity in Computing Conference
- One of 18 students to represent Stanford's CS department through boothing

Major Grant — Summer 2023, Stanford, CA
Stanford University Vice Provost for Undergraduate Education
- Received a $8K grant for a 10-week independent research on the Avg-Act Swap

Presidential Science Scholarship — Fall 2020–Spring 2024
Korea Student Aid Foundation — Seoul, South Korea
- One of 20 recipients of a $200k college scholarship granted annually by the President of Korea

Talent Award of Korea
Deputy Prime Minister and Minister of Education of Korea
- One of 50 annual recipients; recognized for demonstrated interest in cryptography and social service

Leadership & Service

Board Member (2023); Mentee (2020-22) — Fall 2020–Spring 2024
Stanford Women in Math Mentoring — Stanford, CA
- Organized quarterly socials for 70 members, hosted talks on diversity and gender equity in Math, managed the alumni network, and led recruiting

Community Outreach Intern — Fall 2021 – Spring 2022
Stanford Women's Community Center — Stanford, CA
- Hosted a welcome for 200 students, organized a spotlight series for 10 women leaders at Stanford, and did social media takeovers to promote intern activities

Industry

Research Intern — Summer 2022
Devsisters Corporation — Seoul, South Korea
- Developed mathematical models to predict token prices at six decentralized exchanges
- Advised the C-level team on the launching and quarterly pricings of new game token

Languages Rust, Python, C, C++, Java, Javascript, Rust, SQL
Tools BigQuery, Compute Engine, Git, Docker, Vim, Tmux, Wireshark