Ihyun Nam

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

EDUCATION

Ph.D. in Computer Science Fall 2025–3030 (expected)
Stanford University
- Cryptography and Systems Security

M.S. in Computer Science (Computer and Network Security) Fall 2024–Winter 2025
Stanford University
- **CS:** Cryptography, Computer Security, Operating Systems, and Distributed Systems

B.S. in Mathematics & Computer Science with Honors (Systems) Fall 2020–Spring 2024
Stanford University
- **CS:** Computational Complexity, Algorithms, Mathematical Foundations of Computing
- **Math:** Linear Algebra, Group Theory, Number Theory, Probability, and Metalogic

PUBLICATIONS

1. **Ihyun Nam**, "The Avg-Act Swap and Plaintext Overflow Detection in Fully Homomorphic Operations Over Deep Circuits," in the Proceedings of the 14th ACM Conference on Data and Application Security and Privacy, June 2024 (pdf)
2. 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)
**Alphabetical author listing, as is conventional in Mathematics.*

RESEARCH EXPERIENCE

A Sparse Polynomial Commitment Scheme from Lattices (pdf) Winter 2024–Present
Advisor: Professor Dan Boneh Stanford CS
- Built the first sparse polynomial commitment scheme from lattices based on a prior field-based scheme, and proved perfect completeness and knowledge soundness
- Standardized the scheme to use any (non-sparse) lattice-based PCS in the commit phase and achieve optimal prover costs linear in the polynomial sparsity

Authentication Logging to a Public Blockchain (pdf) Winter 2024–Present
Advisor: Professors David Mazières & Emma Dauterman Stanford CS
- Designed a privacy-preserving authentication logging protocol that (1) does not require a trusted log server during enrollment and audit for correct service and (2) guarantees user privacy against a colluding log server and relying party, unlike the state-of-the-art solution larch
- Log server does not learn anything about the RP from users' logged records, and a malicious log server cannot authenticate on behalf of a user.
- Implemented protocol in Rust, including a bare metal blockchain; <1 second login time expected

Faster Fully Homomorphic Encryption with Plaintext Overflow Detection (pdf) Spring–Fall 2023
Advisor: Professor John Mitchell Stanford CS
- Designed 'Swap', a method to transform any traditional neural network to achieve faster encrypted inference on FHE-encrypted data, by averaging data before applying activation functions
- Applied the Swap to two neural networks I built for a 25% speedup with 98% accuracy, and to the Lenet-5 neural network for a 28% speedup with 90% accuracy
- Devised the first plaintext overflow detection protocol for fixed-point arithmetic FHE and showed applicability to the Cheon-Kim-Kim-Song and BFV/GV schemes
- Published and presented results as the solo author at the ACM Conference on Data and Application Security and Privacy (Porto, Portugal, 21% acceptance rate)
- Poster presentation at the Symposia for Undergraduate Research and Public Service (Stanford, CA – October 2023)

Identifying TLS Clients via Unsupervised Learning on Domain Names (pdf) Spring–Summer 2023
Advisor: Professor Zakir Durumeric Stanford CS
- Built and evaluated Clid: a TLS client identification tool that uses unsupervised learning to map clients to domain names that are most informative of their identity, among prior connections
- Designed a client-domain algorithm based on frequency and exclusivity of connections, and clustering to abstract out errors in real data
- Clid identifies the most associated domain names for >60% of clients in all test TLS sets

A Survey of Multivariate Polynomial Commitment Schemes (pdf) Fall–Winter 2023

Advisor: Professor Dan Boneh — Stanford CS

- Wrote a survey of eight multivariate polynomial commitments schemes and their security analyses

Shuffle Squares and Reverse Shuffle Squares (pdf) — Summer–Fall 2021
Advisor: Professor Pawel Grzegrzolka — Stanford Math

- Proved the Henshall-Rampersad-Shallit conjecture on enumerating shuffle squares (words containing identical disjoint strings) that was previously only shown with empirical evidence
- Disproved a companion conjecture on *reverse* shuffle squares and proved a novel alternative, contributing to efficient error correcting codes in deletion channels
- Published results at the European Journal of Combinatorics (February 2024)
- Poster presentation at the Symposia for Undergraduate Research and Public Service (Stanford, CA – October 2021)

TEACHING

Math 19 (Calculus) – Stanford University — Fall 2024
Instructor: Zachary Wickham

- **Teaching Assistant:** Led office hours (5hrs/week), held exam review sessions, and graded exams for 230 students

Hack Lab (Introduction to Cybersecurity) – Stanford University — Fall 2023
Instructor: Alex Stamos

- **Teaching assistant:** Led lab sections (1hr/week) on exploiting and defending web vulnerabilities, held office hours (1hr/week), and wrote and graded exams for 100 students
- **Lab assistant:** Transitioned GCP virtual Kali attack machines and targets to host in a new on-prem Proxmox cluster, to be used by Stanford CS classes and computer security labs

Stanford University Mathematics Camp – Stanford University — Summer 2023
Instructor: Rick Sommer

- **Teaching Assistant:** Advised five crypto research projects (8hrs/week) and led group theory problem sessions (3hrs/day)
- **Residential Counselor:** Led social activities and counselled 40 high school students

Paschar Consulting – Seoul, South Korea — Summer 2021

- **Tutor:** Mentored high school seniors for college admissions via daily meetings and essay editing

Bloomsbury Education – Jeju, South Korea — Summer 2020

- **Math Tutor:** Taught International Baccalaureate Higher Level Math to Year 3–12 students
- **Latin Tutor:** Taught iGCSE Latin to Year 9 students

ACCOLADES

School of Engineering Fellowship — Fall 2025
Organization: Stanford University

- Fellowship for top incoming PhD students.

The Hoefer Prize for Writing in the Major — Spring 2024
Organization: Stanford University

- One of seven annual recipients chosen for quality of writing in thesis work, nominated by faculty
- Recognized for CS Honors Thesis on novel research on fully homomorphic encryption

IORH Blockchain Research Grant — Spring 2024
Organization: Stanford IOG Research Hub

- Received a $118K grant for proposed research on authentication logging to a public blockchain
- Pitched grant to principal investigator and drafted proposal

Computer Science Honors Program — Spring 2023–2024
Organization: Stanford CS Department

- One of 16 students accepted to the Honors program in the CS major, through research proposal and faculty recommendation
- Presented thesis on fully homomorphic encryption to CS faculty at the department colloquium

Conference Grant — Spring 2024
Organization: Stanford University

- One of eight recipients of a $1.5K travel grant to present accepted research at CODASPY ’24

Presidential Science Scholarship — 2020–2024

Organization: Korea Student Aid Foundation
- One of 20 annual recipients of a $200K college scholarship awarded by the President of Korea
- Selected for excellence in Math and interest in studying cryptography in university

Scholarship for the Richard Tapia Conference for Diversity in Computing Summer 2023
Organization: Stanford CS Department
- One of 18 annual recipients to represent Stanford's CS department through booth

Major Grant Spring 2023
Organization: Stanford University
- Received a $7.5K grant (largest grant for undergraduates, 68% acceptance rate) for 10-week research on fully homomorphic encryption advised by Professor Dan Boneh

Talent Award of Korea Winter 2022
Organization: Deputy Prime Minister & Minister of Education of Korea
- One of 50 annual recipients under 34, selected by a faculty committee for excellence in chosen field
- Recognized for academic work in cryptography and community service for gender minorities

LEADERSHIP AND SERVICE

Board Member (2024); Mentee (2020-23) 2020–2024
Organization: Stanford Women in Math Mentoring
- Led recruiting of 80 members, hosted faculty talks on diversity in Math, and organized three socials

Community Outreach Intern 2021–2022
Organization: Stanford Women's Community Center
- Hosted welcome for 200 minority students and interviewed 10 women leaders at Stanford for project

Volunteer 2017–2018, 2024
Organization: Jeju Women's Association
- Helped organize their annual feminist film festival by translating Korean materials to English

INDUSTRY

Research Intern (Mobile Game Industry) Summer 2022
Organization: Devsisters – Seoul, South Korea
- As an intern on blockchain game team, developed a math model for predicting token prices at decentralized cryptocurrency exchanges (DEX) based on two months of data I collected
- Presented results and advised C-level team on the quarterly pricing of blockchain game tokens

LANGUAGES AND TOOLS

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