# Ihyun Nam

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

## EDUCATION

**M.S. in Computer Science** (Computer and Network Security) Fall 2024–Winter 2025
**Stanford University** (GPA: 3.9/4.3)
- **CS:** Cryptography, Computer Security, Operating Systems, and Distributed Systems

**B.S. in Mathematics & Computer Science with Honors** (Systems) Fall 2020–Spring 2024
**Stanford University** (GPA: 3.7/4.3)
- **CS:** Computational Complexity, Algorithms, Mathematical Foundations of Computing
- **Math:** Linear Algebra, Group Theory, Number Theory, Probabilistic Analysis, and Metalogic

## PUBLICATIONS

1. **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)
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)
**Authors are listed in alphabetical order by last name, as is conventional in Mathematics*

## RESEARCH EXPERIENCE

**Lasso Lookup Arguments on Lattices** (In Progress) Winter 2024–Present
**Advisor:** Professor Dan Boneh Stanford CS
- Building sparse polynomial commitments for lattices using the LaBRADOR compact proof system
- Building post-quantum Lasso-style lookup arguments from standard lattice assumptions

**Authentication Logging to a Public Blockchain** (In Progress) Winter 2024–Present
**Advisor:** Professors David Maziéres & Emma Dauterman Stanford CS
- Designed, built, and evaluated a privacy-preserving authentication logging system that (1) does not require a trusted log server and (2) guarantees user privacy against colluding log server and relying party, unlike the state-of-the-art solution Larch
- Leveraged lightweight crypto primitives like blind signatures and verifiable encryption to achieve zero cost in all involved parties
- Devised efficient auditing methods leveraging a public blockchain, even with a dishonest log server
- Implemented protocol in Rust, including a bare metal blockchain; achieved <1 second login time
- Received the IORH Grant for Blockchain Research (pitched grant to P.I. and drafted proposal)
- (Note to professors) Paper in preparation for submission to IEEE S&P or USENIX Security

**Faster Fully Homomorphic Encryption with Plaintext Overflow Detection** Spring–Fall 2023
**Advisor:** Professor John Mitchell Stanford CS
- Designed the Avg-Act Swap (the Swap): averaging FHE-encrypted data before applying activation function in deep circuits for faster encrypted inference, with minimal loss in accuracy
- Modified Lenet-5 with the Swap to achieve a 28% faster encrypted inference speed
- Designed the first plaintext overflow detection protocol for floating-point arithmetic FHE schemes; showed applicability to Cheon-Kim-Kim-Song and BFV/GV schemes and proved IND-CPA security
- Published & presented results at the 14th ACM Conference on Data and Application Security and Privacy (pdf) (2024)
- Poster presentation at Stanford's Symposium for Undergraduate Research and Public Service
- Received Stanford's Major Grant and Conference Travel Grant for undergraduate research

**TLS Client Identification with Unsupervised Learning on Domain Names** Spring–Summer 2023
**Advisor:** Professor Zakir Durumeric Stanford CS
- Used BigQuery statistics tools to show current client identification tools identify <20% of network clients due to their reliance on hardcoded databases that grow outdated
- Built Clid: an improved TLS client identification tool using unsupervised learning, Bayesian optimization, and DBSCAN clustering on domain names
- Showed Clid identifies the most associated domain names for >60% of clients in all test TLS sets
- Uploaded preprint to arXiv (pdf)

**Shuffle Squares and Reverse Shuffle Squares** Summer–Fall 2021
**Advisor:** Professor Pawel Grzegrzolka Stanford Math
- Proved the Henshall-Rampersad-Shallit conjecture on enumerating shuffle squares; disproved their conjecture on reverse shuffle squares and proved a novel alternative
- Contributed to efficient error-correcting codes for deletion channels

- 1 of 7 projects in Stanford Undergraduate Research Institute in Mathematics (selection by application)
- Published results in the European Journal of Combinatorics (pdf) (2024)
- Poster presentation at Stanford's Symposium for Undergraduate Research and Public Service

**TEACHING**

**Math 19** (Calculus) – Stanford University — Fall 2024
**Instructor:** Zachary Wickham
- Teaching Assistant: Led office hours & exam review sessions for 230 students and graded exams

**Hack Lab** (Introduction to Cybersecurity) – Stanford University — Fall 2023
**Instructor:** Alex Stamos
- **Teaching assistant:** Led lab sections on exploiting & defending web vulnerabilities, held office hours for 120 students, and wrote exams
- **Lab assistant:** Transitioned virtual machine from GCP virtual Kali attack machines and targets to hosting in a new on-prem Proxmox cluster, to be used by Stanford CS classes and security labs

**Stanford University Mathematics Camp** — Summer 2023
**Instructor:** Rick Sommer
- **Teaching Assistant:** Advised 5 crypto research projects; led group theory problem sessions
- **Residential Counselor:** Led daily dorm meetings for 40 high school students

**Bloomsbury Education** — 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**

**The Hoefer Prize for Excellence in Undergraduate Writing** — Spring 2024
**Organization:** Stanford University
- 7 selected theses through faculty nomination; recognized for quality of writing in chosen field (CS)

**Presidential Science Scholarship** — 2020–2024
**Organization:** Korea Student Aid Foundation
- 20 annual recipients; $200K college scholarship awarded by the President of Korea
- Selected for excellence in Math and interest in studying cryptography in university

**Conference Scholarship for the Richard Tapia Conference for Diversity in CS** — Summer 2023
**Organization:** Stanford CS
- 18 annual recipients; represented Stanford's CS department through boothing

**Talent Award of Korea** — Winter 2022
**Organization:** Deputy Prime Minister & Minister of Education of Korea
- 50 annual recipients; selection by a faculty committee on excellence in chosen field (CS)
- Recognized for study in cryptography and community service

**LEADERSHIP AND SERVICE**

**Board Member (2023); Mentee (2020-22)** — 2020–2024
**Organization:** Stanford Women in Math Mentoring
- Led recruiting of 80 members, hosted faculty talks in diversity in Math, and organized 3 socials

**Community Outreach Intern** — 2021–2022
**Organization:** Stanford Women's Community Center
- Hosted event for 200 students and interviewed women leaders at Stanford for intern project

**INDUSTRY**

**Research Intern** (Mobile Game Industry) — Summer 2022
**Organization:** Devsisters Corporation – Seoul, South Korea
- Collected 3 months of data and developed mathematical models to predict token prices at 6 cryptocurrency exchanges
- Advised C-level team on the launching and 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