

Daehyun Jang

CV Ver:
Jun. 29. 2026

📍 Seoul, Republic of Korea ✉ jadh0309@snu.ac.kr

ABOUT ME

I am a Ph.D. student in Mathematical Sciences at Seoul National University, advised by Prof. **Jung Hee Cheon**. My research focuses on Cryptography, particularly Homomorphic Encryption.

EDUCATION

- | | |
|--|-----------------------|
| Integrated M.S./Ph.D. Program in Mathematical Sciences
Seoul National University, Seoul, Republic of Korea | Sep. 2024 – Present |
| B.S. in Mathematical Sciences
Seoul National University, Seoul, Republic of Korea | Mar. 2019 – Aug. 2024 |
| <ul style="list-style-type: none">GPA: 3.86/4.3 (Overall)<ul style="list-style-type: none">– Major: Mathematical Sciences (3.99/4.3)– Minor: Philosophy (3.80/4.3)Military Service at Republic of Korea Army | |
| | Dec. 2020 – Jun. 2022 |

PUBLICATIONS

Published

- Jung Hee Cheon, **Daehyun Jang**, "Cryptanalysis on Lightweight Verifiable Homomorphic Encryption," *Asiacrypt 2025*.
Author order is alphabetical by surname.

Preprint(s)

- Jung Hee Cheon, **Daehyun Jang**, Jaehee Kang, Hanee Rhee, "Private Embedding Lookup with Encrypted Compact Queries under Fully Homomorphic Encryption"
Author order is alphabetical by surname.
- Jung Hee Cheon, **Daehyun Jang**, Jaehee Kang, Hanee Rhee, "SWIFT: Shallow and SIMD-Aware CKKS Functional Bootstrapping for Low-Latency"
Author order is alphabetical by surname.

TALKS

- Korean Mathematical Society (KMS) 2024 Fall Meeting
"Cryptanalysis on Lightweight Verifiable Homomorphic Encryption"
- Asiacrypt 2025
"Cryptanalysis on Lightweight Verifiable Homomorphic Encryption"
- International Conference for the 80th Anniversary of the Korean Mathematical Society
Jun. 23, 2026
"SWIFT: Shallow and SIMD-Aware CKKS Functional Bootstrapping for Low-Latency"
- PACOH Workshop: Homomorphic Encryption 2026
Jun. 29, 2026, Sokcho, Republic of Korea
"SWIFT: Shallow and SIMD-Aware CKKS Functional Bootstrapping for Low-Latency"

POSTERS

- FHE.org Conference 2026, "Efficient Private Embedding Lookup via Independent Vector Evaluation"

RESEARCH INTERNSHIP

Graduate Research Fellow

Korea Institute for Advanced Study (KIAS), Seoul, Republic of Korea

- Homomorphic Encryption Jan. 2025 – Present
 - Theoretical study on the CKKS scheme
 - Advised by Prof. Jeong Han Kim

Undergraduate Research Internship

Seoul National University, Seoul, Republic of Korea

- Homomorphic Encryption Oct. 2023 – Aug. 2024
 - Study on the CKKS scheme and its recent advances
 - Advised by Prof. Jung Hee Cheon
- Homogeneous Dynamics Jun. 2023 – Aug. 2023
 - Study on the Quantitative version of the Oppenheim conjecture
 - Advised by Prof. Seonhee Lim

TEACHING EXPERIENCE

Teaching Assistant

- Abstract Algebra I Spring 2026
- Engineering Mathematics I Spring 2026
- Mathematical Exercises II Fall 2024, Fall 2025
- Advanced Mathematical Exercises I Spring 2025

Undergraduate Tutor

- Mathematics I Spring 2020, Spring 2024
- Mathematics II Fall 2020
- Mathematics for Life Sciences I Spring 2023
- Calculus II Fall 2023

HONORS & AWARDS

- 3rd Place, Korea Crypto Contest Oct. 2025
- Outstanding Teaching Assistant Award, Seoul National University Dec. 2024
- Outstanding Tutor Award, Seoul National University Dec. 2023
- Outstanding Student Award, Seoul National University Dec. 2020