Hyewon Sung

Research Profile

I am a Ph.D. candidate in Cryptography at Ewha Womans University, advised by Prof. Hyang-Sook Lee.
Building on my background in mathematics, I focus my research on cryptography, particularly ***fully homomorphic encryption, privacy-preserving protocols, and post-quantum cryptography.***

Contact Information

- **Address :** Ewha Womans University, Seoul, Republic of Korea
- **E-mail :** hyewonsung@ewha.ac.kr
- **Contact :** +82 10-2615-3194
- **Personal Website :** Google Scholar/Hyewon Sung
, github.com/HyewonSung

Education

Integrated MS/Ph.D. Ewha Womans University, Cryptography — March 2021 – Present

- *Integrated Master's and Ph.D. Program in Mathematics with a specialization in Cryptography*
- Advisor: Prof. Hyang-Sook Lee
- GPA: 4.1 / 4.3

BS **Ewha Womans University**, Mathematics — March 2017 – February 2021

- *Double Major in Information Security, Minor in Computer Engineering*
- GPA: 3.49 / 4.3

Experiences

Research Intern	NTT Social Information Laboratories, Japan	July 2026 – Present
Research Intern	NTT Social Information Laboratories, Japan	October 2025 – April 2026

Publications

sPAR : (Somewhat) Practical Anonymous Router — 2026

- Debajyoti Das, Jeongeun Park and **Hyewon Sung**
- Accepted by ACM CCS 2026

Cryptanalysis of an Unbounded Fully Homomorphic Encryption Scheme — 2026

- **Hyewon Sung** and Mehdi Tibouchi
- Accepted by ACISP 2026

EvalRound+ Bootstrapping and its Rigorous Analysis for CKKS Scheme — 2024

- **Hyewon Sung**, Sieun Seo, Taekyung Kim and Chohong Min
- Published in IEEE Access (Volume : 13)
- DOI : 10.1109/ACCESS.2025.3595177

Preprints

Traveling Salesman-Based Token Ordering Improves Stability in Homomorphically Encrypted Language Models 2025

- Donghwan Rho, Sieun Seo, **Hyewon Sung**, Chohong Min and Ernest K. Ryu
- arxiv.org/abs/2510.12343

Private Information Retrieval based on Homomorphic Encryption, Revisited 2025

- Jaeseon Kim, Jeongeun Park and **Hyewon Sung**
- eprint.iacr.org/2025/729

Projects

CKKS Reference Implementation for ISO Standardization April 2023

- **Hyewon Sung**, Sieun Seo and Chohong Min
- Implemented the complete CKKS scheme in pure C, without using external libraries, as reference code submitted for ISO standardization.

Presentations

Group Signatures from Lattices

- Summer Sinchon Seminar of Graduates in Mathematics (SSG), Yonsei University, Republic of Korea, 22 June 2023

Efficient Scalr Multiplications over Twisted Edwards Curves of Isogeny-based PQC

- East Asian Core Doctoral Forum on Mathematics (EACDFM), Fudan University, Shanhai, 7-11 January 2024

Homomorphic Encryption and Error Analysis of CKKS

- Winter Sinchon Seminar of Graduates in Mathematics (SSG), Ewha Womans University, Republic of Korea, 27 December 2024

Cryptanalysis of an Unbounded Fully Homomorphic Encryption Scheme

- Internship Presentation, NTT Social Informatics Laboratories, Japan, 8 April 2026

Cryptanalysis of an Unbounded Fully Homomorphic Encryption Scheme

- 31st Australasian Conference on Information Security and Privacy (ACISP), Perth, Australia, 6-9 July 2026

Invited Talks

EvalRound+ Bootstrapping and its Rigorous Analysis for CKKS Scheme

- Crypto Winter Camp, Seoul National University, Republic of Korea, 3-4 January 2025

Patents

APPARATUS FOR BOOTSTRAP PROCESSING HOMOMORPHIC ENCRYPTED MESSAGES AND METHODS THEREOF August 19, 2024

- **Hyewon Sung**, Sieun Seo, Sunghak Kim, Taekyung Kim, and Chohong Min.
- Korean Patent Application No.1020250032963

Electronic Device and Controlling Method Thereof. Feburary 05, 2026

- Donghwan Rho, Sieun Seo, **Hyewon Sung**, Chohong Min and Ernest K. Ryu
- Korean Patent Application No.10-2025-0014625

Languages

Korean: Native proficiency
English: Professional working proficiency
Programming Languages: Python (Advanced), C++ (Advanced), C (Advanced), Go (Intermediate), Matlab (Advanced)