

Jinyeong Seo

Email: jinyeong.seo@protonmail.com

LinkedIn: <https://linkedin.com/in/jinyeong-seo-4bb505328/>

GitHub: <https://github.com/jin-yeong-seo>

Website: <https://jin-yeong-seo.github.io/>

Overview

I am a Ph.D. student at Seoul National University, advised by Prof. Yongsoo Song. My research interests lie in (but are not limited to) the practical instantiation of cryptographic protocols using techniques from lattice-based cryptography. Specifically, my recent research focuses on improving the performance of lattice-based proof systems and homomorphic encryption schemes. I also have broad interests in the theoretical foundations of cryptographic proofs.

Education

Seoul National University

Seoul, South Korea

Ph.D. in Computer Science

Mar. 2022 – Present

Advisor: Yongsoo Song

KAIST

Daejeon, South Korea

B.S. in Mathematical Science

Mar. 2016 – Aug. 2021

(double major: Computer Science)

Experiences

Apple

Cupertino, United States

Ph.D. Intern

Jun. 2025 – Aug. 2025

Mentor: Nicholas Genise

CryptoLab Inc.

Seoul, South Korea

Researcher

Sep. 2019 – Mar. 2020

Intern

Jun. 2019 – Aug. 2019

Developed HEaaS-STAT, a homomorphic encryption-based statistical analysis toolkit.

eWBM Inc.

Seoul, South Korea

Intern

Jun. 2018 – Aug. 2018

Developed ECDH PKI protocols for secure communication on LoRa devices.

Publications

Authors are listed in alphabetical order by last name, unless an asterisk (*) is indicated.

Conferences

[C11] On the Security and Privacy of CKKS-based Homomorphic Evaluation Protocols

Intak Hwang, Seonhong Min, Jinyeong Seo, Yongsoo Song

ASIACRYPT 2025

[C10] Practical TFHE Ciphertext Sanitization for Oblivious Circuit Evaluation

Intak Hwang, Seonhong Min, Jinyeong Seo, Yongsoo Song
ACM CCS 2025

[C09] Practical Zero-Knowledge PIOP for Maliciously Secure Multi-party Homomorphic Encryption

Intak Hwang, Hyeonbum Lee, Jinyeong Seo, Yongsoo Song
ACM CCS 2025

[C08] MatriGear: Accelerated Authenticated Matrix Triple Generation with Scalable Prime Fields via Optimized HE Packing

Hyunho Cha, Intak Hwang, Seonhong Min, Jinyeong Seo, Yongsoo Song
IEEE S&P 2025

[C07] Simpler and faster BFV Bootstrapping for Arbitrary Plaintext Modulus from CKKS

Jaehyung Kim, Jinyeong Seo, Yongsoo Song
ACM CCS 2024

[C06] Concretely Efficient Lattice-based Polynomial Commitment from Standard Assumptions

Intak Hwang, Jinyeong Seo, Yongsoo Song.
CRYPTO 2024

[C05] Optimizing HE operations via Level-aware Key-switching Framework

Intak Hwang, Jinyeong Seo, Yongsoo Song.
WAHC 2023

[C04] Asymptotically faster multi-key homomorphic encryption from homomorphic gadget decomposition

Taechan Kim, Hyesun Kwak, Dongwon Lee, Jinyeong Seo, Yongsoo Song.
ACM CCS 2023

[C03] Toward Practical Lattice-based Proof of Knowledge from Hint-MLWE

Duhyeong Kim, Dongwon Lee, Jinyeong Seo, Yongsoo Song.
CRYPTO 2023

[C02] Accelerating HE Operations from Key Decomposition Technique

Miran Kim, Dongwon Lee, Jinyeong Seo, Yongsoo Song.
CRYPTO 2023

	<p>[C01] Faster TFHE Bootstrapping with Block Binary Keys Changmin Lee, Seonhong Min, <u>Jinyeong Seo</u>, Yongsoo Song. <i>ACM ASIACCS 2023</i></p>	
Journals	<p>[J01] *HEaN-STAT: a privacy-preserving statistical analysis toolkit for large-scale numerical, ordinal, and categorical data Younho Lee, <u>Jinyeong Seo</u>, Yujin Nam, Jiseok Chae, Jung Hee Cheon <i>IEEE TDSC 2023</i></p>	
Presentations	<p>On the Security and Privacy of CKKS-based Homomorphic Evaluation Protocols <i>ASIACRYPT 2025</i></p>	Dec. 2025
	<p>Practical Zero-Knowledge PIOP for Maliciously Secure Multiparty Homomorphic Encryption <i>ACM CCS 2025</i></p>	Oct. 2025
	<p>Simpler and faster BFV Bootstrapping for Arbitrary Plaintext Modulus from CKKS <i>ACM CCS 2024</i></p>	Oct. 2024
	<p>Concretely Efficient Lattice-based Polynomial Commitment from Standard Assumptions <i>CRYPTO 2024</i></p>	Aug. 2024
	<p>Practical Lattice-based Private Stream Aggregation and Application to Federated Learning <i>The 5th Privacy-Preserving Machine Learning Workshop 2023</i></p>	Aug. 2023
Honors & Awards	<p>Student Travel Grants Travel Grant (\$1,000)</p>	Dec. 2025 ASIACRYPT 2025
	<p>Korea Cryptography Contest 2nd Place (\$3,000)</p>	Oct. 2024 National Security Research Institute
	<p>Student Travel Grants Travel Grant (\$1,000)</p>	Oct. 2024 ACM CCS 2024
	<p>Korea Cryptography Contest 1st Place (\$10,000)</p>	Oct. 2023 National Security Research Institute
	<p>29th Samsung Humantech Paper Award Silver Award (\$7,000)</p>	Feb. 2023 Samsung Electronics

Korea Cryptography Contest

Oct. 2022

3rd Place (\$2,000)

National Security Research Institute

Repositories

<https://github.com/SNUCP/level-aware-ksw>

PoC Implementation of [C05]

<https://github.com/SNUCP/snu-mghe>

PoC Implementation of [C04]

<https://github.com/SNUCP/fast-ksw>

PoC Implementation of [C02]

<https://github.com/SNUCP/blockkey-tfhe>

PoC Implementation of [C01]

Skills

Programming : C, C++, Go, Python