Jinyeong Seo

jinyeong.seo@protonmail.com | LinkedIn | GitHub | jin-yeong-seo.github.io

Research Interests

Practical instantiation of cryptographic protocols using techniques from lattice-based cryptography, specifically 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 (Advisor: Yongsoo Song) — *Mar. 2022 – Present*

KAIST — Daejeon, South Korea
B.S. in Mathematical Science (Double Major: Computer Science) — *Mar. 2016 – Aug. 2021*

Experience

Apple — Cupertino, United States
Ph.D. Intern (Mentor: Nicholas Genise) — *Jun. 2025 – Aug. 2025*

CryptoLab Inc. — Seoul, South Korea
Researcher — *Sep. 2019 – Mar. 2020*

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

Intern — *Jun. 2019 – Aug. 2019*

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 Multiparty 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*

[C01] **Faster TFHE Bootstrapping with Block Binary Keys**
Changmin Lee, Seonhong Min, Jinyeong Seo, Yongsoo Song. *ACM ASIACCS 2023*

Journals

[J01] ***HEaaN-STAT: a privacy-preserving statistical analysis toolkit for large-scale numerical, ordinal, and categorical data**
Younho Lee, Jinyeong Seo, Yujin Nam, Jiseok Chae, Jung Hee Cheon. *IEEE TDSC 2023*

Honors & Awards

Student Travel Grant ($1,000) Dec. 2025
ASIACRYPT 2025

Korea Cryptography Contest - 2nd Place ($3,000) Oct. 2024
National Security Research Institute

Student Travel Grant ($1,000) Oct. 2024
ACM CCS 2024

Korea Cryptography Contest - 1st Place ($10,000) Oct. 2023
National Security Research Institute

Samsung Humantech Paper Award - Silver Award ($7,000) Feb. 2023
Samsung Electronics

Korea Cryptography Contest - 3rd Place ($2,000) Oct. 2022
National Security Research Institute

Projects

level-aware-ksw | github.com/SNUCP/level-aware-ksw
- PoC Implementation of [C05]: Optimizing HE operations via Level-aware Key-switching.

snu-mghe | github.com/SNUCP/snu-mghe
- PoC Implementation of [C04]: Multi-key homomorphic encryption from gadget decomposition.

fast-ksw | github.com/SNUCP/fast-ksw
- PoC Implementation of [C02]: Accelerating HE Operations from Key Decomposition.

blockkey-tfhe | github.com/SNUCP/blockkey-tfhe
- PoC Implementation of [C01]: Faster TFHE Bootstrapping with Block Binary Keys.

Technical Skills

Programming Languages: C, C++, Go, Python

Selected Presentations

On the Security and Privacy of CKKS-based Homomorphic Evaluation Protocols (ASIACRYPT 2025, Dec 2025)

Practical Zero-Knowledge PIOP for Maliciously Secure Multiparty HE (ACM CCS 2025, Oct 2025)

Simpler and faster BFV Bootstrapping for Arbitrary Plaintext Modulus from CKKS (ACM CCS 2024, Oct 2024)

Concretely Efficient Lattice-based Polynomial Commitment (CRYPTO 2024, Aug 2024)

Practical Lattice-based Private Stream Aggregation (PPML Workshop, Aug 2023)