# Jinyeong Seo

**Email**: jinyeong.seo@snu.ac.kr        **Homepage**: https://isaac-seo.github.io/

## Overview

I am a graduate student at Seoul National University, advised by Prof. Yongsoo Song. My research interest lies in (but is 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
**M.S.** in Computer Science                                  Mar. 2022 – Present
Advisor: Prof. Yongsoo Song

**Korea Advanced Institute of Science & Technology** Daejeon, South Korea
**B.S.** in Mathematical Science                              Mar. 2016 – Aug. 2021
(double major: computer science)

## Publications

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

## Conference

[C05] **Optimizing HE operations via Level-aware Key-switching Framework**
Intak Hwang, Jinyeong Seo, Yongsoo Song.
To appear at *WAHC 2023.*

[C04] **Asymptotically faster multi-key homomorphic encryption from homomorphic gadget decomposition**
Taechan Kim, Hyesun Kwak, Dongwon Lee, Jinyeong Seo, Yongsoo Song.
To appear at *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, <u>Jinyeong Seo</u>, Yongsoo Song.
*ACM ASIA CCS 2023.*

| | |
|---|---|
| Journal | **[J01] \*HEaaN-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
*IEEE TDSC 2023.*

| | | |
|---|---|---|
| Experiences | **CryptoLab Inc.** | Seoul, South Korea |
| | - Researcher | Sep. 2019 – Mar. 2020 |
| | - Intern | Jun. 2019 – Aug. 2019 |
| | - Developed HEaaN-STAT, 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. | |

| | | |
|---|---|---|
| Talks | **Practical Lattice-based Private Stream Aggregation and Application to Federated Learning** | Aug. 2023 |
| | The 5th Privacy-Preserving Machine Learning Workshop 2023 | |

| | | |
|---|---|---|
| Awards | **29th Samsung Humantech Paper Award** | Feb. 2023 |
| | Silver Award ($7, 000) | Samsung Electronics |
| | | |
| | **Korea Cryptography Contest** | Oct. 2022 |
| | Excellence Award ($2, 000) | National Security Research Institute |

| | | |
|---|---|---|
| GitHub 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 |