

# Jinyeong Seo

**Email:** jinyeong.seo@snu.ac.kr

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

## Overview

I am a Ph.D. 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

<b>Seoul National University</b>	Seoul, South Korea
<b>Ph.D.</b> in Computer Science	Mar. 2022 – Present
Advisor: Prof. Yongsoo Song	
 <b>KAIST</b>	 Daejeon, South Korea
<b>B.S.</b> 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.

## Conferences

[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*

	<p><b>[C03] Toward Practical Lattice-based Proof of Knowledge from Hint-MLWE</b>  Duhyeong Kim, Dongwon Lee, <u>Jinyeong Seo</u>, Yongsoo Song.  <i>CRYPTO 2023</i></p>
	<p><b>[C02] Accelerating HE Operations from Key Decomposition Technique</b>  Miran Kim, Dongwon Lee, <u>Jinyeong Seo</u>, Yongsoo Song.  <i>CRYPTO 2023</i></p>
	<p><b>[C01] Faster TFHE Bootstrapping with Block Binary Keys</b>  Changmin Lee, Seonhong Min, <u>Jinyeong Seo</u>, Yongsoo Song.  <i>ACM ASIACCS 2023</i></p>
Journals	<p><b>[J01] *HEaaN-STAT: a privacy-preserving statistical analysis toolkit for large-scale numerical, ordinal, and categorical data</b>  Younho Lee, <u>Jinyeong Seo</u>, Yujin Nam, Jiseok Chae, Jung Hee Cheon  <i>IEEE TDSC 2023</i></p>
Experiences	<p><b>CryptoLab Inc.</b> <span style="float: right;">Seoul, South Korea</span>  - Researcher <span style="float: right;">Sep. 2019 – Mar. 2020</span>  - Intern <span style="float: right;">Jun. 2019 – Aug. 2019</span>  - Developed HEaaN-STAT, homomorphic encryption-based statistical analysis toolkit.</p> <p><b>eWBM Inc.</b> <span style="float: right;">Seoul, South Korea</span>  - Intern <span style="float: right;">Jun. 2018 – Aug. 2018</span>  - Developed ECDH PKI protocols for secure communication on LoRa devices.</p>
Presentations	<p><b>Simpler and faster BFV Bootstrapping for Arbitrary Plaintext Modulus from CKKS</b> <span style="float: right;">Oct. 2024</span>  <i>ACM CCS 2024</i></p> <p><b>Concretely Efficient Lattice-based Polynomial Commitment from Standard Assumptions</b> <span style="float: right;">Aug. 2024</span>  <i>CRYPTO 2024</i></p> <p><b>Practical Lattice-based Private Stream Aggregation and Application to Federated Learning</b> <span style="float: right;">Aug. 2023</span>  <i>The 5th Privacy-Preserving Machine Learning Workshop 2023</i></p>
Honors & Awards	<p><b>Korea Cryptography Contest</b> <span style="float: right;">Oct. 2024</span>  2nd Place (\$3, 000) <span style="float: right;">National Security Research Institute</span></p> <p><b>Student Travel Grants</b> <span style="float: right;">Oct. 2024</span>  Travel Grant (\$1,000) <span style="float: right;">ACM CCS 2024</span></p>

**Korea Cryptography Contest**

Oct. 2023

1st Place (\$10, 000)

National Security Research Institute

**29th Samsung Humantech Paper Award**

Feb. 2023

Silver Award (\$7, 000)

Samsung Electronics

**Korea Cryptography Contest**

Oct. 2022

3rd Place (\$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