

Seonhong Min

Email: me@minsh.info, minsh@snu.ac.kr | Website: minsh.info

Research Focus: FHE

Conferences: 10 | Journals: 2 | Preprints: 4

RESEARCH INTERESTS

Lattice based cryptography. Mainly Fully Homomorphic Encryption (FHE) and its multiple party variants.

EDUCATION

Seoul National University Mar. 2022 – Present
Integrated M.S./Ph.D. in Computer Science & Engineering
Advisor: Prof. Yongsoo Song

Seoul National University Mar. 2018 - Feb. 2022
B.S. in Mathematics

Daegu Science High School Mar. 2015 – Feb. 2018

PUBLICATIONS

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

Conferences

C11 2025/2057
Distributed Key Generation for Efficient Threshold-CKKS

Seonhong Min, Guillaume Hanrot, Jai Hyun Park, Alain Passelègue, Damien Stehlé
ACM CCS 2026

C10 2026/322
Multi-key Fully Homomorphic Encryption with Non-Interactive Setup in the Plain Model
Seonhong Min, Jeongeun Park, Yongsoo Song
IACR CRYPTO 2026

C9 2025/1804
***HERDS: Multi-Key Fully Homomorphic Encryption with Sublinear Bootstrapping**
Binwu Xiang, Seonhong Min, Intak Hwang, Zhiwei Wang, Haoqi He, Yuanju Wei, Yi Deng, Jiang Zhang, Kang Yang, Yu Yu
IACR EUROCRYPT 2026

C8 2025/382
On the Security and Privacy of CKKS-based Homomorphic Evaluation Protocols
Intak Hwang, Seonhong Min, Jinyeong Seo, Yongsoo Song

IACR ASIACRYPT 2025

C7 2024/2032
Carousel: Fully Homomorphic Encryption with Bootstrapping over Automorphism Group
Intak Hwang, Seonhong Min, Yongsoo Song
IACR ASIACRYPT 2025

C6 2025/216
Practical (Malicious) Circuit Privacy / Sanitization for TFHE
Intak Hwang, Seonhong Min, Jinyeong Seo, Yongsoo Song
ACM CCS 2025

C5 2025/1255
Efficient Full Domain Functional Bootstrapping from Recursive LUT Decomposition
Intak Hwang, Shinwon Lee, Seonhong Min, Yongsoo Song
SAC 2025

C4 2024/1502
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

C3 2025/429
***Enhanced CKKS Bootstrapping with Generalized Polynomial Composites Approximation**
Seonhong Min, Joon-woo Lee, Yongsoo Song
ACM ASIACCS 2025

C2 2023/958
Faster TFHE Bootstrapping with Block Binary Keys
Changmin Lee, Seonhong Min, Jinyeong Seo, Yongsoo Song
ACM ASIACCS 2023

C1 2022/1460
Towards Practical MK-TFHE: Parallelizable, Key-Compatible, Quasi-Linear Complexity
Hyesun Kwak, Seonhong Min, Yongsoo Song
IACR PKC 2024

Journals

J2 2024/1534
More Efficient Lattice-based OLE from Circuit-private Linear HE with Polynomial Overhead

Leo de Castro, Duhyeong Kim, Miran Kim, Keewoo Lee,
Seonhong Min, Yongsoo Song
ACR COMMUNICATIONS IN CRYPTOLOGY

J1 2406.14372

***Ring-LWE based encrypted controller with unlimited number of recursive multiplications and effect of error growth**

Yeongjun Jang, Joowon Lee, Seonhong Min, Hyesun Kwak, Junsoo Kim, Yongsoo Song

IEEE TRANS. ON CONTROL OF NETWORK SYSTEMS

Preprints

P3 2026/1585 **Proving Threshold Regev PKE from Adaptive Hint-MLWE: Efficient, Non-interactive, and CCA Secure**

Yisol Hwang, Shuichi Katsumata, Seonhong Min, Guilhem Niot, Yongsoo Song

P2 2025/203

Ciphertext-Simulatable HE from BFV with Randomized Evaluation

Intak Hwang, Seonhong Min, Yongsoo Song

P1 2024/181

Functional Bootstrapping for Packed Ciphertexts via Homomorphic LUT Evaluation

Dongwon Lee, Seonhong Min, Yongsoo Song

PRESENTATIONS

- **Enhanced CKKS Bootstrapping with Generalized Polynomial Composites Approximation** - AsiaCCS 2025
- **Faster TFHE Bootstrapping with Block Binary Keys** - FHE.org Meetup ([Video](#))
- **Faster TFHE Bootstrapping with Block Binary Keys** - AsiaCCS 2023
- **Functional Bootstrapping for Packed Ciphertexts via Homomorphic LUT Evaluation** - FHE.org Meetup ([Video](#))
- **Towards Practical MK-TFHE: Parallelizable, Key-Compatible, Quasi-Linear Complexity** - PKC 2024 ([Video](#))

POSTERS

- **Practical MK-TFHE: Parallelizable, Key-Compatible, Quasi-Linear Complexity** - FHE.org 2023
- **Carousel: Blind Rotation Over the Automorphism Group** - FHE.org 2024

- **Practical Sanitization for TFHE** - FHE.org 2024
- **MatriGear: Accelerated Authenticated Matrix Triple Generation with Scalable Prime Fields via Optimized HE Packing** - FHE.org 2024

HONORS & AWARDS

- **Korea Cryptography Contest 2025** - 3rd Place, 4th Place
- **Korea Cryptography Contest 2024** - 3rd Place
- **Korea Cryptography Contest 2023** - 4th Place

EXPERIENCES

FHElab Lyon (Cryptolab Inc.) (Intern) 2024.11 – 2025.02

OPEN-SOURCE REPOSITORIES

- **Multi-key TFHE:** [SNUCP/MKTFHE](#)
- **Carousel.jl:** [SNUCP/Carousel.jl](#)
- **HIENAA.jl:** [snu-lukemin/HIENAA.jl](#)
- **Ciphertext Simulatable BFV:** [SNUCP/simct](#)
- **CRS-less MKFHE:** [SNUCP/crsless](#)

ACADEMIC SERVICES

Reviewer at TCS (Theoretical Computer Science), DCC (Designs, Codes and Cryptography)

SKILLS

Languages: Korean (native), English (fluent), Japanese (conversational)

Programming Languages: Julia, Python, Java, Go, $\text{\LaTeX}$