Seonhong Min

Email: me@minsh.info **Website**: minsh.info

Research Interests

Lattice–based Cryptography, especially Fully Homomorphic Encryption (FHE).

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.

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

2025/216
Practical TFHE Ciphertext Sanitization for Oblivious Circuit Evaluation
Intak Hwang, Seonhong Min, Jinyeong Seo, Yongsoo Song
In Submission

2025/203
Ciphertext-Simulatable HE from BFV with Randomized Evaluation
Intak Hwang, Seonhong Min, Yongsoo Song
In Submission

2024/2032
Carousel: Fully Homomorphic Encryption from Slot Blind Rotation Technique
Intak Hwang, Seonhong Min, Yongsoo Song
In Submission

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

AsiaCCS 2025

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
In Submission

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
S&P 2025

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, under revision

2024/181
Funtional Bootstrapping for Packed Ciphertexts via Homomorphic LUT Evaluation
Dongwon Lee, Seonhong Min, Yongsoo Song
In Submission

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

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

PRESENTATION

Youtube
Faster TFHE Bootstrapping with Block Binary Keys
FHE.org Meetup

Faster TFHE Bootstrapping with Block Binary Keys
AsiaCCS 2023

Youtube
Functional Bootstrapping for Packed Ciphertexts via Homomorphic LUT Evaluation
FHE.org Meetup

Youtube

Towards Practical MK-TFHE: Parallelizable, Key-Compatible, Quasi-Linear Complexity
PKC 2024

Posters

Practical MK-TFHE: Parallelizable, Key-Compatible, Quasi-Linear Complexity
FHE.org 2023

Fully Homomorphic Encryption from Slot Blind Rotation Technique
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

Experiences

Cryptolab Inc. (Intern) 2024.11 – 2025.02

Github Repositories

Multi-key TFHE
https://github.com/SNUCP/MKTFHE

Carousel.jl
https://github.com/SNUCP/Carousel.jl

HIENAA.jl
https://github.com/snu-lukemin/HIENAA.jl

Ciphertext Simulatable BFV
https://github.com/SNUCP/simct

Skills

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

Programming Languages
Julia, Python, Java, Go, LaTeX

Other Interests

My hobby is to write songs and to draw digital paintings. I have a few albums and singles released; I would love to share them if you contact me personally.