Intak Hwang

Email: intak.hwang@snu.ac.kr **Website**: sp301415.com **GitHub**: sp301415

I'm a Ph.D. student in Cryptography & Privacy Lab at Seoul National Unversity, advised by Yongsoo Song. I'm interested in post-quantum cryptographic protocols based on lattices, including but not limited to Fully Homomorphic Encryption and Zero-Knowledge Proofs.

Education

Seoul National University 2023 — Present
Integrated M.S./Ph.D. in Computer Science & Engineering
Advised by Yongsoo Song

DGIST 2018 — 2022
B.S. in School of Undergraduate Studies *Summa Cum Laude*

Publications

[C09] 2025/1804
HELIOS: Multi-Key Fully Homomorphic Encryption with Sublinear Bootstrapping
Binwu Xiang, Seonhong Min, Intak Hwang, Zhiwei Wang, Haoqi He, Yuanju Wei, Kang Yang, Jiang Zhang, Yi Deng, Yu Yu
Eurocrypt 2026

[C08] 2024/2032
Carousel: Fully Homomorphic Encryption with Bootstrapping over Automorphism Group
Intak Hwang, Seonhong Min, Yongsoo Song
Asiacrypt 2025

[C07] 2025/382
On the Security and Privacy of CKKS-based Homomorphic Evaluation Protocols
Intak Hwang, Seonhong Min, Jinyeong Seo, Yongoo Song
Asiacrypt 2025

[C06] 2025/216
Practical TFHE Ciphertext Sanitization for Oblivious Circuit Evaluation
Intak Hwang, Jinyeong Seo, Seonhong Min, Yongsoo Song
ACM CCS 2025

[C05] 2024/1879
Practical Zero-Knowledge PIOP for Maliciously Secure Multiparty Homomorphic Encryption
Intak Hwang, Hyeonbum Lee, Jinyeong Seo, Yongsoo Song
ACM CCS 2025

[C04] 2025/1255

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

[C03] 2024/1502
MatriGear: Accelerating 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

[C02] 2024/306
Concretely Efficient Lattice-based Polynomial Commitment from Standard Assumptions
Intak Hwang, Jinyeong Seo, Yongsoo Song
Crypto 2024

[C01] 2023/1328
Optimizing HE via Level-aware Key-switching
Intak Hwang, Jinyeong Seo, Yongsoo Song
WAHC 2023

[J01] **A Privacy-Preserving HLA Imputation Method with Homomorphic Encryption**
Hakin Kim, Intak Hwang, Yongsoo Song, Buhm Han
iScience

PREPRINTS

[P03] 2026/044
Jindo: Practical Lattice-Based Polynomial Commitment for Zero-Knowledge Arguments
Intak Hwang, Hyeonbum Lee, Jinyeong Seo, Yongsoo Song

[P02] 2025/395
Provably Secure Approximate Computation Protocols from CKKS
Intak Hwang, Yisol Hwang, Miran Kim, Dongwon Lee, Yongsoo Song

[P01] 2025/203
Ciphertext-Simulatable HE from BFV with Randomized Evaluation
Intak Hwang, Seonhong Min, Yongsoo Song

PROJECTS

TFHE-go (GitHub Repository)
TFHE-go is an implementation of (MK)TFHE scheme, written in Go and Go Assembly. Currently, it is one of the fastest and most feature-complete TFHE implementaion available open-source.

Ringo-SNARK (GitHub Repository)
Ringo-SNARK is a Zero-Knowledge PIOP toolkit for efficiently proving Ring-LWE relations, written in Go. It supports simple, gnark-like circuit design and compilation.

Presentations

Practical TFHE Ciphertext Sanitization for Oblivious Circuit Evaluation
ACM CCS 2025 — Taipei, Taiwan
FHE.org — Online

MatriGear: Accelerating Authenticated Matrix Triple Generation with Scalable Prime Fields via Optimized HE Packing
IEEE S&P 2025 — San Fransisco, USA

Optimizing HE via Level-aware Key-switching
WAHC 2023 — Copenhagen, Denmark

Honors and Scholarships

National Cryptographic Contest

Excellence Award, Encouragement Award	2025
Best Award, Excellence Award	2024
Special Award	2023

CTF Security Competitions 2020 — 2022

SSTF Hacker's Playground 2022	*5th place*
WhiteHat Contest 2021	*3rd place*
DEFCON CTF 2021	*Finalist*
PlaidCTF 2021	*5th place*
Real World CTF 2020/2021 (Media Coverage)	*1st place*
Midnight Sun CTF 2020 Finals	*7th place*
TokyoWesterns CTF 2020 Finals	*3rd place*
DEFCON CTF 2020	*Finalist*

DGIST Dean's List 2020

Skills

Languages
Korean (native), English (fluent)

Programming Languages
Go, Python (SageMath), C/C++, C#, Rust, LaTeX

Other Activities

Member of CTF Team CodeRed 2020 — 2022
I participated in CTF competitions from time to time, mostly solving crypto challenges.

Developer & Writer of Team Invertible 2020 — Present
I am actively working on *Shards of Time*, a sokoban puzzle game. We are planning to release the game on Steam.

Other Interests

I love watching films. I also wrote and directed several short films.