

Intak Hwang

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

RESEARCH INTERESTS

Lattice-Based Cryptography, 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
Advisor: Prof. Yongsoo Song

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

PUBLICATIONS

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

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

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

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

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

2025/1255

Efficient Full Domain Functional Bootstrapping from Recursive LUT Decomposition

Intak Hwang, Shinwon Lee, Seonhong Min, Yongsoo Song

SAC 2025

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

2025/395

Provably Secure Approximate Computation Protocols from CKKS

Intak Hwang, Yisol Hwang, Miran Kim, Dongwon Lee, Yongsoo Song

2025/203

Ciphertext-Simulatable HE from BFV with Randomized Evaluation

Intak Hwang, Seonhong Min, Yongsoo Song

2024/306

Concretely Efficient Lattice-based Polynomial Commitment from Standard Assumptions

Intak Hwang, Jinyeong Seo, Yongsoo Song

Crypto 2024

2023/1328

Optimizing HE via Level-aware Key-switching

Intak Hwang, Jinyeong Seo, Yongsoo Song

WAHC 2023

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.

HONORS AND SCHOLARSHIPS

National Cryptographic Contest

Excellence Award, Encouragement Award 2025

Best Award, Excellence Award 2024

Special Award 2023

CTF Security Competitions

SSTF Hacker's Playground 2022 2020 — 2022

5th place

WhiteHat Contest 2021	<i>3rd place</i>
DEF CON CTF 2021	<i>Finalist</i>
PlaidCTF 2021	<i>5th place</i>
Real World CTF 2020/2021 (Media Coverage)	<i>1st place</i>
Midnight Sun CTF 2020 Finals	<i>7th place</i>
TokyoWesterns CTF 2020 Finals	<i>3rd place</i>
DEF CON CTF 2020	<i>Finalist</i>
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 — Present

I participate 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.