Minsik Kang

minsik.kang0503@gmail.com | mskang0503.github.io

Research Interests

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

Education

Seoul National University, Seoul, Republic of Korea — Mar 2018 – Feb 2026

- Ph.D. in Mathematical Sciences
- Focus: Cryptography (Homomorphic Encryption)
- Advisor: Prof. Jung Hee Cheon

Seoul National University, Seoul, Republic of Korea — Mar 2013 – Feb 2018

- B.S. in Mathematical Sciences

Experience

CryptoLab Inc., Lyon, France — June 2024 – Aug 2024

- Advisor: Prof. Damien Stehlé

Publications

Authors are listed in alphabetical order by last name, unless an asterisk(*) is indicated. A dagger (†) indicates the corresponding author, when applicable.

Conferences

[C05] **Towards Lightweight CKKS: On Client Cost Efficiency**
Jung Hee Cheon, Minsik Kang, Jai Hyun Park
ACM ASIA Conference on Computer and Communications Security (ACM ASIACCS 2026)

[C04] **Grafting: Decoupled Scale Factors and Modulus in RNS-CKKS**
Jung Hee Cheon, Hyeongmin Choe, Minsik Kang, Jaehyung Kim, Seonghak Kim, Johannes Mono, Taeyeong Noh
ACM Conference on Computer and Communications Security (ACM CCS 2025)

[C03] **High-Throughput AES Transciphering using CKKS: Less than 1ms**
Youngjin Bae, Jung Hee Cheon, Minsik Kang, Taeseong Kim
Workshop on Encrypted Computing & Applied Homomorphic Cryptography (WAHC 2025)

[C02] **NeuJeans: Private Neural Network Inference with Joint Optimization of Convolution and FHE Bootstrapping**
Jae Hyung Ju*, Jaiyoung Park*, Jongmin Kim, Minsik Kang, Donghwan Kim, Jung Hee Cheon, Jung Ho Ahn
ACM Conference on Computer and Communications Security (ACM CCS 2024)

[C01] **High-precision RNS-CKKS on fixed but smaller word-size architectures: theory and application**
Rashmi Agrawal, Jung Ho Ahn, Flavio Bergamaschi, Ro Cammarota, Jung Hee Cheon, Fillipe DM de Souza, Huijing Gong, Minsik Kang, Duhyeong Kim, Jongmin Kim, Hubert De Lassus, Jai Hyun Park, Michael Steiner, Wen Wang
Workshop on Encrypted Computing & Applied Homomorphic Cryptography (WAHC 2023)

Journals

[J01] **Batch Inference on Deep Convolutional Neural Networks With Fully Homomorphic Encryption Using Channel-By-Channel Convolutions**
Jung Hee Cheon, Minsik Kang†, Taeseong Kim, Junyoung Jung, Yongdong Yeo
IEEE Transactions on Dependable and Secure Computing 2024

Manuscripts

[M02] **Fast Batch Matrix Multiplication in Ciphertexts**
Jung Hee Cheon, Minsik Kang, Junho Lee
Cryptology ePrint Archive, Available at https://eprint.iacr.org/2025/1957

[M01] **Algorithms for CRT-variant of Approximate Greatest Common Divisor Problem**
Jung Hee Cheon, Wonhee Cho, Minsik Kang, Jiseung Kim, and Changmin Lee
Cryptology ePrint Archive, Available at https://eprint.iacr.org/2019/195

Honors & Awards

National Cryptography Contest, National Security Research Institute

- Grand Prize ($10,000) for [M01] Oct 2017
- Best Prize ($3,000) for [C04] Oct 2025
- Excellence Prize ($2,000) for [C02] Oct 2024
- Special Prize ($1,000) for [M02] Oct 2024
- Special Prize ($1,000) for [J01] Oct 2023

University Students Contest for Mathematics, Korean Mathematical Society

- Bronze Medal Nov 2016
- Bronze Medal Nov 2014

Invited Talks

Homomorphic Encryption from Mathematical Backgrounds

- East Asian Core Doctorial Forum in Mathematics (EACDFM) 2026, Seoul, Korea Jan 2026

Presentations

Grafting: Decoupled Scale Factors and Modulus in RNS-CKKS

- ACM CCS 2025, Taipei, Taiwan, co-presented with Hyeongmin Choe Oct 2025

Towards Lightweight CKKS: On Client Cost Efficiency

- 2025 KMS Spring Meeting, Daejeon, Korea Apr 2025

Skills

Programming: C, C++, Python, Sage, LaTeX

Languages: Korean (native), English (fluent)