

Minsik Kang

minsik.kang0503@gmail.com | scholar.google.com

Publications

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

Conferences

[C05] Towards Lightweight CKKS: On Client Cost Efficiency

Jung Hee Cheon, Minsik Kang, Jai Hyun Park

Accepted at ACM ASIACCS 2026, Available at <https://eprint.iacr.org/2025/720>

[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

Proceedings of the 2025 on ACM SIGSAC Conference on Computer and Communications Security, pp. 1098-1112, 2025.

[C03] High-Throughput AES Transciphering using CKKS: Less than 1ms

Youngjin Bae, Jung Hee Cheon, Minsik Kang, Taeseong Kim

Proceedings of the 13th Workshop on Encrypted Computing & Applied Homomorphic Computing, pp. 1-12, 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
Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security, pp. 4361-4375, 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

Proceedings of the 11th Workshop on Encrypted Computing & Applied Homomorphic Cryptography, pp. 23-34, 2023.

Journals

[J01] Batch Inference on Deep Convolutional Neural Networks With Fully Homomorphic Encryption Using Channel-By-Channel Convolutions

Jung Hee Cheon, Minsik Kang \dagger , Taeseong Kim, Junyoung Jung, Yongdong Yeo

IEEE Transactions on Dependable and Secure Computing, vol. 22, No. 2, pp. 1674-1685, 2025.

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