Jincheol Ha

Updated November 1, 2025

Research Interests

homomorphic encryption, CKKS, TFHE, HE-friendly cipher, post-quantum digital signature, MPC-in-the-Head, symmetric-key encryption, algebraic analysis

Professional Experience

CryptoLab Inc. in Seoul, Korea — 2025. 2. – Present
HE Research Engineer

Education

Ph.D. in Computer Science (GSIS), KAIST — 2021. 3. – 2025. 2.
Research area: Cryptography
Thesis title: Practical and Efficient Methods to Use the TFHE Scheme
Advisor: Jooyoung Lee

M.S. in Computer Science (GSIS), KAIST — 2019. 3. – 2021. 2.
Research area: Cryptography
Thesis title: An HE-friendly Cipher Using Modular Arithmetic
Advisor: Jooyoung Lee

B.S. in Mathematical Science, KAIST — 2015. 3. – 2019. 2.
Double Major in Computer Science

Publications[1]

– Conferences

Refined TFHE Leveled Homomorphic Evaluation and Its Application
*R. Wang†, **J. Ha**†, X. Shen, X. Lu, C. Chen, K. Wang, and J. Lee.
To appear ACM CCS 2025.

Polocolo: A ZK-Friendly Hash Function Based on S-boxes Using Power Residues
J. Ha, S. Hwang, J. Lee, S. Park, and M. Son.
The 44th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2025).

Efficacy and Mitigation of the Cryptanalysis on AIM
*S. Kim, **J. Ha**, M. Son, and B. Lee.
The 5th NIST PQC Standardization Conference, 2024.

AIM: Symmetric Primitive for Shorter Signatures with Stronger Security
*S. Kim†, **J. Ha**†, M. Son, B. Lee, J. Lee, S. Lee, J. Kwon, J. Cho, H. Yoon, and J. Lee.
The 30th ACM Conference on Computer and Communications Security (CCS 2023).

[1] Authors are listed in alphabetical order by last name, unless an asterisk(∗) is indicated. Daggers (†) indicate co-first authors.

Rubato: Noisy Ciphers for Approximate Homomorphic Encryption
J. Ha, S. Kim, B. Lee, J. Lee, and M. Son.
The 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2022).

Transciphering Framework for Approximate Homomorphic Encryption
J. Cho, **J. Ha**, S. Kim, B. Lee, J. Lee, J. Lee, D. Moon, and H. Yoon.
International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2021).

– Journals

FRAST: TFHE-friendly Cipher Based on Random S-boxes
M. Cho, W. Chung, **J. Ha**, J. Lee, E. Oh, and M. Son.
Transactions on Symmetric Cryptology (ToSC), 2024, Issue 3.

MPCitH 기반 영지식 증명과 대칭키 프리미티브 기반 일방향 함수를 결합 양자내성 전자서명 AIMer 소개
***하진철**, 김성광, 손민철
The Korea Institute of Information Security and Cryptology. 2024.

Masta: An HE-friendly Cipher Using Modular Arithmetic
***J. Ha**, S. Kim, W. Choi, J. Lee, D. Moon, H. Yoon, and J. Cho.
IEEE Access. 2020.

– Tech. Report

The AIMer Signature Scheme (Ver. 2.0)
*J. Lee, J. Cho, **J. Ha**, S. Kim, J. Kwon, B. Lee, J. Lee, S. Lee, D. Moon, M. son, and H. Yoon.
Submission to Korean Post-Quantum Cryptography (KpqC) Competition 2nd Round. 2024. https://aimer-signature.org

The AIMer Signature Scheme (Ver. 1.0)
*S. Kim, J. Cho, M. Cho, **J. Ha**, J. Kwon, B. Lee, J. Lee, J. Lee, S. Lee, D. Moon, M. son, and H. Yoon.
Submission to NIST Call for Additional Signature Schemes. 2023. https://aimer-signature.org

The AIMer Signature Scheme (Ver. 0.9)
*S.Kim[†], **J. Ha**[†], M. Son, B. Lee, D. Moon, J. Lee, S. Lee, J. Kwon, J. Cho, H. Yoon, and J. Lee.
Submission to Korean Post-Quantum Cryptography (KpqC) Competition. 2022. https://aimer-signature.org

Talk

(Invited) **Refined TFHE Leveled Homomorphic Evaluation and Its Application**
2025 KMS Annual Meeting, Oct 2025, Seoul, Korea

Refined TFHE Leveled Homomorphic Evaluation and Its Application
2025 ACM CCS, Oct 2025, Taipei, Taiwan

FRAST: TFHE-Friendly Cipher Based on Random S-Boxes
The 31st Fast Software Encryption Conference (FSE 2025), Mar 2025, Rome, Italy

AIMer
2024 KpqC Winter Camp, Feb 2024, Seoul, Korea (slide)

AIM에 대한 분석 및 대응
KpqC 연구단 7차 워크숍, Nov 2023, Seoul, Korea (slide)

FRAST: Ciphers for Homomorphic Encryption over Torus
2023 KMS Annual Meeting, Oct 2023, Seoul, Korea

FRAST: Ciphers for Homomorphic Encryption over Torus
2023 KSIAM Spring Conference, May 2023, Pyeong Chang, Korea

AIMer: ZKP-based Digital Signature
2023 KpqC Winter Camp, Feb 2023, Seoul, Korea (slide)

(Invited) **On the Number of Linearly Independent Boolean Equations of Power Mapping Based S-boxes**
KIAS, Nov 2022, Online

Masta: An HE-friendly Cipher Using Modular Arithmetic
2020 KMS Fall Meeting, Oct 2020, Online

Programming

– Languages: C/C++, Python, Golang, Rust, SageMath, Magma, Mathematica, LaTeX

– Repositories: Refined TFHE Leveled Homomorphic Evaluation and Its Application
https://github.com/KAIST-CryptLab/refined-tfhe-lhe

FRAST: TFHE-friendly Cipher Based on Random S-boxes
https://github.com/KAIST-CryptLab/FRAST

Boolean Quadratic Equations of Power Mappings
https://github.com/KAIST-CryptLab/BoolQuadEqs

RtF Transciphering Framework with HERA and Rubato
https://github.com/KAIST-CryptLab/RtF-Transciphering

CKKS-FV Hybrid Transciphering Framework with HERA
https://github.com/smilecjf/CKKS-FV-HERA