Seongkwang Kim

Jung Woonoh IT & General Education Center, Korea University, 145 Anam-ro, Seongbuk-gu, Seoul 02841, Republic of Korea

seongkwang-kim@korea.ac.kr

seongkwang.kim23@gmail.com

sgk1m.github.io

Last updated: 2026. Mar. 1

Professional Experience

- Assistant Professor in Korea University, Seoul, Korea — Mar. 2026 - Present
- Senior Engineer in Samsung SDS, Seoul, Korea — Mar. 2022 - Feb. 2026
  - Research on MPCitH/VOLEitH-based signature
    - Main contributor in AIMer team (NIST R1 candidate, KpqC selected)
    - Vector semi-commitment applied to MPCitH/VOLEitH-based signature schemes
  - Research on authenticated encryption with associated data (AEAD)
    - Design and security proof of efficient beyond-birthday-bound AEAD
    - Design and security proof of nonce-misuse resistant AEAD
  - Research on privacy-preserving protocols
    - Privacy-preserving record linkage using circuit-based private set intersection
    - Oblivious pseudorandom function based on oblivious key-value store

Education

- Ph.D. in Information Security — Mar. 2018 - Feb. 2022
  - Where: KAIST, Daejeon, Korea
  - Advisor: Jooyoung Lee
  - Research Area: HE-friendly ciphers, transciphering framework, provable security
- M.Sc. in Mathematical Science — Mar. 2016 - Feb. 2018
  - Where: KAIST, Daejeon, Korea
  - Advisor: Sanggeun Han
  - Research Area: cryptanalysis of LWE
- B.Sc. in Mathematics — Mar. 2012 - Feb. 2016
  - Where: POSTECH, Pohang, Korea

Publications

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

Academic Papers

1. W. Chung, S. Hwang, **S. Kim**, B. Lee, and J. Lee. "Making GCM Great Again: Toward Full Security and Longer Nonces". The 44th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2025).

2. **S. Kim**, B. Lee, and M. Son. "Relaxed Vector Commitment for Shorter Signatures". The 44th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2025).

3. K. Han, **S. Kim**, and Y. Son. "Private Computation on Common Fuzzy Records". Proceedings on Privacy Enhancing Technologies Symposium (PoPETs 2025).

4. K. Han, **S. Kim**, B. Lee, and Y. Son. "Revisiting OKVS-based OPRF and PSI: Cryptanalysis and Better Construction". The 30th Annual International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2024).

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

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

7. J. Cho, J. Ha, **S. Kim**, B. Lee, J. Lee, J. Lee, D. Moon, and H. Yoon. "Transciphering Framework for Approximate Homomorphic Encryption". The 27th Annual International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2021).

8. *J. Ha, **S. Kim**, W. Choi, J. Lee, D. Moon, H. Yoon, and J. Cho. "Masta: An HE-friendly Cipher Using Modular Arithmetic". IEEE Access 10.1109/ACCESS.2020.3033564, 2020.

9. **S. Kim**, B. Lee, and J. Lee. "Tight Security Bounds for Double-Block Hash-then-Sum MACs". The 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2020).

Preprints

- S. Kim, B. Lee, and M. Son. "Shorter VOLE-in-the-Head-based Signatures from Vector Semi-Commitment". Cryptology ePrint Archive. Report 2025/1077. 2025. https://eprint.iacr.org/2025/1077.

Technical Report

- *J. Lee, J. Cho, J. Ha, **S. Kim**, J. Kwon, B. Lee, J. Lee, S. Lee, D. Moon, M. Son, and H. Yoon. "The AIMer Signature Scheme (Ver. 2.1)". 2024. https://aimer-signature.org.

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

- *__S. Kim__, J. Ha, M. Son, and B. Lee. "Efficacy and Mitigation of the Cryptanalysis on AIM". The 5th NIST PQC Standardization Conference. 2024. https://eprint.iacr.org/2023/1474.

- *__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. “The AIMer Signature Scheme (Ver. 1.0)”. Submission to NIST Call for Additional Signature Schemes. 2023. https://aimer-signature.org.
- *__S. Kim__†, J. Ha†, M. Son, B. Lee, D. Moon, J. Lee, S. Lee, J. Kwon, J. Cho, H. Yoon, and J. Lee. “The AIMer Signature Scheme (Ver. 0.9)”. Submission to Korean Post-Quantum Cryptography (KpqC) Competition. 2022. https://aimer-signature.org.

Ph.D. Dissertation

- __S. Kim__. "On Homomorphic Encryption, Transciphering Frameworks, and HE-friendly Ciphers". 2022. KAIST.

Repositories

- https://github.com/KAIST-CryptLab/RtF-Transciphering RtF framework with HERA, Rubato
- https://github.com/samsungsds-opensource/AIMer AIMer

Talks and Posters

- “The AIMer Signature Scheme”. KpqC Winter Camp 2026. Feb. 2026. Seoul, Korea.
- “Relaxed Vector Commitment for Shorter Signatures”. Invited Talk, ICISC 2025. Nov. 2025. Seoul, Korea.
- “AIMer Standard Format”. 2025 KpqC Conference. Nov. 2025. Seoul, Korea.
- “Hash-based Signatures”. KIISC Cryptography Education Program. Nov. 2025. Online.
- “AIMer Standardization Document Writing Plan”. 2025 KpqC Workshop. Jul. 2025. Taean, Korea.
- “Secure Multiparty Computation, MPC-in-the-Head, and AIMer”. KIISC Cryptography Education Program. Jul. 2025. Online.
- “AIMer v2.1 and Beyond”. Cryptography Research Society (in KIISC) 2025 Mid-term Workshop. Jun. 2025. Busan, Korea.
- “AIMer v2.1 and Beyond”. Invited Talk, KMS Spring Meeting 2025. Apr. 2025. Daejeon, Korea.
- “Revisiting OKVS-based OPRF and PSI: Cryptanalysis and Better Construction”. Asiacrypt 2024. Dec. 2024. Kolkata, India.
- “Updates on AIMer”. KpqC 9th Workshop. Oct. 2024. Seoul, Korea.
- “Circuit-PSI and Applications”. NIST Workshop on Privacy Enhancing Cryptography. Sep. 2024. Online.
- “AIMer”. KpqC Contest Colloquium. Aug. 2024. Seoul, Korea.
- (Poster) “The AIMer Signature Scheme”. NIST 5th PQC Standardization Conference. Apr. 2024. Rockville, MD, US. https://csrc.nist.gov/Events/2024/fifth-pqc-standardization-conference.

- "Efficacy and Mitigation of the Cryptanalysis on AIM". NIST 5th PQC Standardization Conference. Apr. 2024. Rockville, MD, US.
- "AIM: Symmetric Primitive for Shorter Signatures and Stronger Security". ACM CCS 2023. Nov. 2023. Copenhagen, Denmark.
- "The AIMer Signature Scheme". Invited Talk, 2nd Oxford PQC Summit. Sep. 2023. Oxford, United Kingdom. https://www.maths.ox.ac.uk/events/conferences/past-events/oxford-post-quantum-cryptography-workshop-2023.
- "Signature Schemes based on the MPC-in-the-Head Paradigm". Invited Talk, Ewha-KMS International Cryptography Workshop 2023. Jul. 2023. Seoul, Korea.
- "Reducing the Overhead of Approximate Homomorphic Encryption". Invited Talk, KMS Fall Meeting 2022. Oct. 2022. Seoul, Korea.
- "Rubato: Noisy Ciphers for Approximate Homomorphic Encryption". Eurocrypt 2022. Jun. 2022. Trondheim, Norway. https://youtu.be/TE_sYzJtZQc (in English).
- "Transciphering Framework for Approximate Homomorphic Encryption". Invited Talk, CryptoLab. Dec. 2021. Seoul, Korea.
- "Transciphering Framework for Approximate Homomorphic Encryption". Asiacrypt 2021. Dec. 2021. Online. https://youtu.be/r3_07fWqOas (in English).
- "Transciphering Framework for Approximate Homomorphic Encryption". Security @ KAIST. Nov. 2021. Online. https://youtu.be/xKEgtZeMTaw?t=6434 (in Korean).
- "Hybrid Framework for Approximate Computation over Encrypted Data". KMS Spring Meeting 2021. Apr. 2021. Online.

Patents

- K. Han, **S. Kim**, B. Lee, Y. Song, J. Seo, and I. Hwang. "Method, apparatus and computer program for bypassing verification in homomorphic encryption". KR1020250193693. Dec. 2025.
- **S. Kim**, K. Han, and B. Lee. "Method for Multiple Applications of an Oblivious Pseudo-Random Function Protocol between a Receiving Device and a Sending Device based on an Oblivious Key-Value Store Algorithm, and Device using the Same". KR1020250091679. Jul. 2025.
- B. Lee and **S. Kim**. "Method, Apparatus, System and Computer Program for Generating Variable-Output-Length Pseudo-Random Function based on Block Cipher". KR1020250059321. May. 2025.
- **S. Kim**, B. Lee, M. Son. "Method, Apparatus, System and Computer Program for Zero-Knowledge Proof based on Binary Tree". (KR1020250156598, US19189453, EP25172274). Feb. 2025.
- Y. Son, **S. Kim**, B. Lee, and K. Han. "Method for implementing a private set intersection protocol using an oblivious pseudorandom function based on minicrypt, and a terminal device using the same". (KR1020250109577, US19005316). Jan. 2024.
- Y. Son, K. Han, **S. Kim**. "Method for Generating Common Identifier and Apparatus Therefor". (KR1020240153894, US18396442, EP232189712). Sep. 2023.
- **S. Kim**, D. Moon, J. Kwon, S. Lee, J. Lee, M. Son, B. Lee, and J. Ha. "Method for Calculating using an One-Way Function Efficient in a Zero Knowledge Proof, and Apparatus Implementing the Same Method". (KR1020240073510, US18387520, EP232031583). Nov. 2022.

- Y. Son, K. Han, **S. Kim**. “Method for Protecting Data Based on Private Set Union Protocol, and Apparatus Implementing the Same Method”. (KR1020240029490, US18216223, EP231846056). Oct. 2022.
- D. Moon, J. Lee, J. Lee, Y. Son, **S. Kim**, J. Ha, M. Son, and B. Lee. “Method for Calculating Using a Zero Knowledge Proof-Friendly One-Way Function, and Apparatus Implementing the Same Method”. (KR1020230161195, US18198667, EP231728221, SG10202301388U). May 2022.
- J. Lee, D. Moon, H. Yoon, J. Cho, **S. Kim**, J. Lee, and J. Ha. “Method and Apparatus for Generating Key Stream”. (KR1020220146115, US17514135). Apr. 2021.
- J. Lee, D. Moon, H. Yoon, J. Cho, E. Kim, **S. Kim**, J. Lee, J. Ha, W. Choi. “Apparatus and Method for Encryption, Apparatus and Method for Converting Ciphertext”. (KR20210129573, US17081862). Oct. 2020.
- D. Moon, H. Yoon, and J. Cho, **S. Kim**, J. Lee, J. Ha, and W. Choi. “Apparatus and Method for Symmetric-key Cryptography”. KR1020220022826. Oct. 2020.

Skills

- I speak Korean as a native and English fluently as a second language.
- Familiar with C/C++ (with x86 intrinsics), Python, Mathmatica and LaTeX
- Proficient to use PET libraries (e.g. SEAL, HElib, LibOTe)

Teaching Experiences

- Counseling assistant: Sep. 2016 - Feb. 2021
- Teaching assistant
  - IS511 Information security: 2018 Spring, 2019 Spring
  - CS204 Discrete mathematics: 2019 Fall, 2021 Spring

Services

Program committee:

- ISC 2025
- ICISC 2023, 2024, 2025

External reviewer:

- PKC 2024
- Eurocrypt 2023, 2026
- Asiacrypt 2019, 2020, 2024
- ICISC 2018
- ProvSec 2018

Honors and Awards

- The final selected digital signature algorithm (AIMer) in KpqC Competition (2025)
- The bronze award at Samsung Paper Award in 2023, 2025
- The best dissertation award at Korean Mathematical Society in 2023
- The 3rd award at iDash Competition (Track 4: Secure Record Linkage) in 2022
- The 2nd award at Korea Cryptography Contest (hosted by Korea Cryptography Forum) in 2018, 2024

Other Experiences

- Exchange student at NUS, Singapore in 2015
- Cellist in POSTECH orchestra (Mar. 2012 - Feb. 2016) / KAIST orchestra (Mar. 2016 - Feb. 2020)
- I have traveled to ...
  - Asia: KR, JP, CN, TW, MY, ID, VN, SG, TH, LA, MM, IN, NP, MV, MN, KZ, IL
  - Europe: NO, CZ, PL, DE, NL, CH, IT, FR, ES, UK, DK, AT, VA, RU
  - America & Oceania & Africa: US (MD, NY, DC, GU), NZ, MA

Previous Email Addresses

- sk39.kim@samsung.com
- ksg0923@kaist.ac.kr
- ksg0923@postech.ac.kr