Seongkwang Kim

56, Seongchon-gil, Seocho-gu, Seoul, Korea
seongkwang.kim23@gmail.com
sgk1m.github.io

Last updated: 2024. Sep. 3

Summary of Skills

- Design & analysis of symmetric ciphers
- Knowledge of PETs (MPC, HE)
- Post-quantum signature (MPC-in-the-Head)
- Implementation skills (e.g. x86 intrinsics)
- Proficiency on PET libraries
- Scientific and technical writing

Professional Experience

- Senior Engineer in Samsung SDS, Seoul, Korea — Mar. 2022 - Present
  - Research on MPCitH-based signature
    - The principal submitter of AIMer submission to NIST PQC standardization of additional digital signature schemes
    - A submitter of AIMer submission to KpqC competition
  - 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

- K. Han, **S. Kim**, and Y. Son. “Private Computation on Common Fuzzy Records”. Proceedings on Prviacy Enhancing Technologies (PoPETs 2025), to appear.
- 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), to appear.
- **S. Kim**, B. Lee, and M. Son. “Relaxed Vector Commitment for Shorter Signature”. IACR Cryptology ePrint Archive. https://eprint.iacr.org/2024/1004.
- *__S. Kim__, J. Ha, M. Son, and B. Lee. “Efficacy and Mitigation of the Cryptanalysis on AIM”. The 5th NIST PQC Standardization Conference.
- *__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).
- 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).
- 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).
- *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.
- **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).

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. 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-research-papers/AIMer/ AIMer

Talks and Posters

- "AIMer". KpqC Contest Colloquium. Aug. 2024. Seoul, Korea.
- (Invited, 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.
- (Invited) "The AIMer Signature Scheme". 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.
- (Invited) "Signature Schemes based on the MPC-in-the-Head Paradigm". Ewha-KMS International Cryptography Workshop 2023. Jul. 2023. Seoul, Korea.
- (Invited) "Reducing the Overhead of Approximate Homomorphic Encryption". 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).
- (Invited) "Transciphering Framework for Approximate Homomorphic Encryption". 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

- Y. Son, K. Han, **S. Kim**. "Method for Generating Common Identifier and Apparatus Therefor". (US18396442, EP232189712). Dec. 2023.
- **S. Kim**, D. Moon, J. Kwon, S. Lee, J. Lee, M. Son, B. Lee, and J. Ha. "Method for Calculating using One-Way Function Efficient in a Zero Knowledge Proof, and Apparatus Implementing Same Method". US18387520. Nov. 2023.

- Y. Son, K. Han, **S. Kim**. “Method for Generating Common Identifier and Apparatus Therefor”. KR1020230122560. Sep. 2023.
- Y. Son, K. Han, **S. Kim**. “Method for Protecting Data Based on Private Set Union Protocol, and Apparatus Implementing the Same Method”. (US18216223, EP231846056). Jun. 2023.
- D. Moon, J. Lee, J. Lee, Y. Son, **S. Kim**, J. Ha, M. Son, and B. Lee. "Calculating Method Using Zero Knowledge Proof-Friendly One-Way Function, and Apparatus for Implementing the Same". (US18198667, EP231728221, SG10202301388U). May 2023.
- 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". US17081862. Jan. 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". KR1020220155427. Nov. 2022.
- Y. Son, K. Han, **S. Kim**. “Method for Protecting Data Based on Private Set Union Protocol, and Apparatus Implementing the Same Method”. KR1020220141508. Oct. 2022.
- D. Moon, J. Lee, J. Lee, Y. Son, **S. Kim**, J. Ha, M. Son, and B. Lee. "Apparatus and Method for Constructing ZKP-friendly One-way Functions with Single Rounds". KR1020220060914. May 2022.
- J. Lee, D. Moon, H. Yoon, J. Cho, **S. Kim**, J. Lee, and J. Ha. “Method and Apparatus for Generating Key Stream”. US17514135. Oct. 2021.
- J. Lee, D. Moon, H. Yoon, J. Cho, **S. Kim**, J. Lee, and J. Ha. “Method and Apparatus for Generating Key Stream”. KR1020210052987. Apr. 2021.
- D. Moon, H. Yoon, and J. Cho, **S. Kim**, J. Lee, J. Ha, and W. Choi. “Symmetric Cipher Suitable for Homomorphic Encryption Schemes over Modular Domains”. KR1020200103887. Aug. 2020.
- J. Lee, H. Yoon, D. Moon, J. Cho, E. Kim, **S. Kim**, J. Lee, J. Ha, and W. Choi. “Method for Converting Symmetric Key Encryption Based Ciphertext into Homomorphic Encryption Based Ciphertext”. KR1020200047585. Apr. 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:

- ICISC 2023, 2024

External reviewer:

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

Honors and Awards

- The bronze award at Samsung Paper Award in 2023
- 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

Other Experiences

- Exchange student at NUS, Singapore in 2015
- Cellist in POSTECH orchestra (Mar. 2012 - Feb. 2016) / KAIST orchestra (Mar. 2016 - Feb. 2020)
- Have traveled to dozens of countries