Curriculum Vitae

Hyeongmin **Choe**

PhD, Cryptographer

hyeongmin (dot) choe (at) uni.lu | hmchoe0528.github.io | hmchoe0528 | hyeongmin-choe | Scholar

Research Interests

- Post-Quantum Cryptography (PQC) and Lattice-based Cryptography
- Fully Homomorphic Encryption (FHE), including Threshold FHE
- Privacy Enhancing Technologies (PETs)

Education

- **Ph.D. in Mathematical Sciences—Cryptography**, *Dept. of Mathematical Sciences, Seoul National University* (*SNU*), *Korea*, Sep. 2019–Feb. 2025
  - **Adviser:** Prof. Jung Hee Cheon
  - **Thesis Title:** Accelerating Homomorphic Computation through Machine-Efficient Arithmetic
- **B.S. in Mathematical Sciences**, *Dept. of Mathematical Sciences, SNU, Korea*, Mar. 2013–Aug. 2019

Selected Publications

Selected recent publications. The complete list is available on Google Scholar.

- Hyeongmin Choe, Jaehyung Kim, Damien Stehlé, Elias Suvanto, "Leveraging Discrete CKKS to Bootstrap in High Precision," ACM CCS 2025
- Jung Hee Cheon, Hyeongmin Choe, Minsik Kang, Jaehyung Kim, Seonghak Kim, Johannes Mono, Taeyeong Noh, "Grafting: Decoupled Scale Factors and Modulus in RNS-CKKS," ACM CCS 2025
- Jung Hee Cheon, Hyeongmin Choe†, Alain Passelègue, Damien Stehlé, Elias Suvanto, "Attacks Against the IND-CPA^D Security of Exact FHE Schemes," ACM CCS 2024
- Jung Hee Cheon, Hyeongmin Choe, Julien Devevey, Tim Güneysu, Dongyeon Hong, Markus Krausz, Georg Land, Marc Möller, Damien Stehlé, MinJune Yi, "HAETAE: Shorter Lattice-Based Fiat–Shamir Signatures," CHES 2024

Awards & Honors

Awards

- **Korean National Cryptography Contest**, *National Security Research Institute* (*NSR*).
  - **Excellence Prize**, Oct. 2025
  - **Grand Prize**, **Honorable Mention**, and **Special Prize**, Oct. 2024
  - **Honorable Mention**, Oct. 2022
- **Korean PQC Standardization (KpqC)**, *NSR and National Intelligence Service* (*NIS*), Sep. 2021–Jan. 2025.
  - **Winner in KEM/PKE**: SMAUG-T Key Encapsulation Mechanism
  - **Winner in Digital Signature**: HAETAE Digital Signature scheme
- **TA Awards**, *Dept. of Mathematical Sciences, SNU*, Aug. 2023
  - **Excellence in Teaching**: for teaching "Honor Calculus Practice 1 (2023 Spring)."
- **2020 iDASH Genomic Data Privacy & Security Protection**, *American National Institutes of Health* (*NIH*), Dec. 2020
  - **First Place (Track I)**. The result was later published as .

Honors

- **ACM CCS 2024 Doctoral Symposium Travel Grant**, *ACM SIGSAC*, Oct. 2024
- **BK 21+ Scholarship**, *Ministry of Education of Korea*, Sep. 2019–Feb. 2025
- **Presidential Undergraduate Science Scholarship**, *Korea Student Aid Foundation*, Mar. 2013–Dec. 2018

Experiences

- **Postdoctoral Researcher**, *University of Luxembourg, Luxembourg*, Nov. 2025–Present
- **Cryptography Engineer**, *CryptoLab Inc., Korea*, Mar.–Oct. 2025
- **Research Visit**, *École Normale Supérieure de Lyon, France*, Sep.–Oct. 2023 (during PhD studies)
- **Sergeant**, *Republic of Korea Air Force* (*ROKAF*), July 2015–July 2017 (mandatory military service)

Public & Professional Services

Invited Talks: *Selected invited talks.*

Conference Invited Talks

- **2025 KMS Spring Meeting**, "HAETAE and SMAUG-T: Korean PQC Standards," *organized by Korean Mathematical Society* (*KMS*), KAIST, Korea, Apr. 25, 2025 (1h)
- **KIAS-JBNU KpqC Workshop**, "HAETAE: Rejecting on Hyperballs," *organized by Korea Institute for Advanced Study* (*KIAS*), Jeonbuk National Univ., Korea, May 19, 2023 (2h)

Seminar Invited Talks

- **Ruhr Univ. Bochum, Germany**, "Recent Advances in Fully Homomorphic Encryption," *at Faculty of Computer Science, Security Engineering*, Jan. 21, 2025 (1.5h)
- **2024 KpqC Winter Camp**, "HAETAE," *organized by KpqC Research Group, at Sogang Univ., Korea*, Feb. 27, 2024 (1h)
- **2024 Algebra Camp**, "Bridging Algebraic Number Theory to Post-Quantum Digital Signatures," *organized by QSMS, at Yangpyeong Bloomvista, Korea*, Feb. 5, 2024 (30m)
- **2023 KpqC Winter Camp**, "Introduction to HAETAE," *organized by KpqC Research Group, at Chung-Ang Univ., Korea*, Feb. 22, 2023 (1h)

Invited Lectures

- **Lecture Series at PQC Migration Platform Seminar**, *jointly organized by LG U+, NIA, and CryptoLab Inc.*, Introductory lectures on PQC and lattice-based KEMs and digital signatures, July 25, Sep. 30, Oct. 29, and Nov. 25, 2025 (8h)
- **Cryptography Training for Information Security Professionals**, *organized by Korea Cryptography Forum*, Pre-recorded lectures on lattice-based PQC, May–Jun. 2025 (3h)
- **PQC Training Course**, *organized by CryptoLab Inc.*, Two half-day lectures on the concrete security of lattice-based PQC, July 16-17, 2024 (7h)
  Material: `https://github.com/hmchoe0528/PQC_training`.
- **2nd 10-10 Gauss Distinguished Lecture Series**, *organized by IMDARC, SNU*, Pre-study on Damien Stehlé's Distinguished Lecture on NIST PQC Standards, Sep. 15, 2023 (0.5h)

Editorial & Academic Service

- **Co-Editor**, CKKS.org , Dec. 2025 – Present
- **Program Committee Member:** ICISC 2025 and ACM CCS 2026
- **Journal Reviewing:** Journal of Cryptology (JoC) in 2023, 2026, and Design, Codes and Cryptography (DCC) in 2024, 2025.
- **Conference Reviewing:** Asiacrypt 2022, 2025, ACM CCS 2022, FHE.org 2022, 2026, PQCrypto 2023–2024, PKC 2024, and Eurocrypt 2024, 2026.

Teaching Record

- **Calculus TA Seminar**, TA, *at Dept. of Mathematical Sciences, SNU*, 2024 Spring
- **Calculus Practice Sessions**, TA & Lecturer, *at College of Natural Sciences, SNU*, 2020–2023 (7 semesters)
- **(i-TAP) Post-Quantum Cryptography**, TA & Co-lecturer, *at SK Hynix Inc.*, Apr.–May (5 weeks), 2021
- **Korean Mathematical Olympiad (KMO) Winter/Summer Schools**, Residential TA, *organized by KMS*, 2013–2014

Contributed Talks

Selected contributed talks.

Conferences and Workshops

- **ACM CCS 2025**, *at Taipei, Taiwan*, Oct. 14, 2025
  - **Title:** Leveraging Discrete CKKS to Bootstrap in High Precision
- **ACM CCS 2025**, *at Taipei, Taiwan*, Oct. 14, 2025 (jointly with Minsik Kang)
  - **Title:** Grafting: Decoupled Scale Factors and Modulus in RNS-CKKS
- **ACM CCS 2024 Doctoral Symposium**, *at Salt Lake City, US*, Oct. 14, 2024
  - **Title:** Toward Practical Threshold FHE: Low Communication, Computation and Interaction
- **Selected Areas in Cryptography (SAC) 2023**, *at Univ. of New Brunswick, Canada*, Aug. 16, 2023
  - **Title:** SMAUG: Pushing Lattice-based Key Encapsulation Mechanisms to the Limits

Research Camps and Colloquiums

- **KpqC Contest 2nd Round Colloquium**, *organized by KpqC Research Group, at Hansung Univ., Korea*, Aug. 28, 2024 (0.5h)
  - **Title:** HAETAE v3.0
- **2024 KMS Spring Meeting**, *organized by KMS*, *at Daejeon Convention Center, Korea*, Apr. 19, 2024 (0.5h)
  - **Title:** IND-CPA^D and KR^D Security of Exact (F)HEs
- **2022 KMS Spring Meeting**, *organized by KMS*, *Virtual*, Apr. 28, 2022 (0.5h)
  - **Title:** Efficient, Round-optimal Blind Signatures from Standard Assumptions