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 in the Publications section.

- Hyeongmin Choe, Jaehyung Kim, Damien Stehlé, Elias Suvanto, "Leveraging Discrete CKKS to Bootstrap in High Precision," ACM CCS 2025 (C06)
- 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 (C05)
- 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 (C03)
- 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 (C02)

Awards & Honors

Awards

- **Korean National Cryptography Contest**, *National Security Research Institute* (*NSR*). A national annual competition for outstanding cryptography research papers, co-authored by undergraduates to postdocs. Grand/Excellence Prize: best paper from all/each track(s).
  - **Excellence Prize** (for C05), Oct. 2025
  - **Grand Prize** (for C03), **Honorable Mention** (for M02), and **Special Prize** (for J05), Oct. 2024
  - **Honorable Mention** (for M01), Oct. 2022
- **Korean PQC Standardization (KpqC)**, *NSR and National Intelligence Service* (*NIS*). A three-year competition for standardizing Korean PQC Algorithms (Sep. 2021–Jan. 2025).
  - **Winner in KEM/PKE:** SMAUG-T Key Encapsulation Mechanism
  - **Winner in Digital Signature**: HAETAE Digital Signature scheme

  Website: `https://www.kpqc.cryptolab.co.kr`
- **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)**: "Secure Multi-label Tumor Classification using Homomorphic Encryption." The result was later published as J04.

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
  - Topic: Broadly on Lattice-based Cryptography, FHE, PQC, and PETs
- **Cryptography Engineer**, *CryptoLab Inc., Korea*, Mar.–Oct. 2025
  - Topic: FHE (applications, implementation, and cryptoanalysis) and PQC (applications, implementation, and standardization)
- **Research Visit**, *École Normale Supérieure de Lyon, France*, Sep.–Oct. 2023 (during PhD studies)
  - Topic: Concrete construction of a new digital signature scheme.
- **Sergeant**, *Intelligence System Management Group*, *Republic of Korea Air Force* (*ROKAF*), July 2015–July 2017 (mandatory military service)

Public & Professional Services

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

- **Kookmin Univ., Korea**, "Security in the Post-Quantum Era: Post-Quantum Cryptography and Standardizations (Translated)," *at Dept. of Information Security, Cryptography, and Mathematics*, June 13, 2025 (1h)
- **Ruhr Univ. Bochum, Germany**, "Recent Advances in Fully Homomorphic Encryption," *at Faculty of Computer Science, Security Engineering*, Jan. 21, 2025 (1.5h)
- **Sungshin Women's Univ., Korea**, "HAETAE: Shorter Lattice-based Fiat-Shamir Signatures," *at Dept. of Convergence Security Engineering*, May 21, 2024 (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)
- **Korea Univ., Korea**, "HAETAE, a Post-Quantum Signature Scheme," *at School of Cybersecurity*, July 24, 2023 (2h)
- **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)
- **Sungshin Women's Univ., Korea**, "HAETAE: Lattice-based Digital Signature (Translated)," Graduate Course *at Dept. of Convergence Security Engineering*, Sep. 23, 2025 (2h)
- **Cryptography Training for Information Security Professionals**, *organized by Korea Cryptography Forum*, Pre-recorded lectures on lattice-based PQC, May–Jun. 2025 (3h)
- **Dongguk Univ., Korea**, "Security in the Post-Quantum Era: Post-Quantum Cryptography and Standardizations (Translated)," Undergraduate Course, *at Dept. of CS & AI*, May 29, 2025 (1.5h)

- **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

Journal & Conference Reviewing

- **Program Committee Member:** ICISC 2025 and ACM CCS 2026
- **Journals:** (Sub/External) Reviewer for
  - Journal of Cryptology (JoC) 2023,
  - Design, Codes and Cryptography (DCC) in 2024–2025.
- **Conferences:** Sub/External reviewer for
  - Asiacrypt 2022, 2025,
  - ACM CCS 2022,
  - FHE.org 2022, 2026,
  - PQCrypto 2023–2024,
  - PKC 2024,
  - Eurocrypt 2024, 2026.

Publications

Authors are listed alphabetically by last name, per the AMS 2004 authorship statement, unless marked with an asterisk (*).
A dagger (†) *denotes the corresponding author when applicable.*

Conferences

C06 Hyeongmin Choe, Jaehyung Kim, Damien Stehlé, Elias Suvanto, "Leveraging Discrete CKKS to Bootstrap in High Precision," **ACM CCS 2025** (ACM Conference on Computer and Communications Security).

C05 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** (ACM Conference on Computer and Communications Security).

C04 Hyeongmin Choe†, "Toward Practical Threshold FHE: Low Communication, Computation and Interaction," **ACM CCS 2024 Doctoral Symposium.** 3-Page Extended Abstract.

C03 Jung Hee Cheon, Hyeongmin Choe†, Alain Passelègue, Damien Stehlé, and Elias Suvanto, "Attacks Against the IND-CPA^{D} Security of Exact FHE Schemes," **ACM CCS 2024** (ACM Conference on Computer and Communications Security).

C02 Jung Hee Cheon, Hyeongmin Choe, Julien Devevey, Tim Güneysu, Dongyeon Hong, Markus Krausz, Georg Land, Marc Möller, Damien Stehlé, and MinJune Yi, "HAETAE: Shorter Lattice-Based Fiat-Shamir Signatures," **CHES 2024** (Conference on Cryptographic Hardware and Embedded Systems).

C01 Jung Hee Cheon, Hyeongmin Choe†, Dongyeon Hong, and MinJune Yi, "SMAUG: Pushing Lattice-based Key Encapsulation Mechanisms to the Limits," **SAC 2023** (Selected Areas in Cryptography).

Journals

J06 Jung Hee Cheon, Hyeongmin Choe, and Jai Hyun Park, "Tree-based Lookup Table on Batched Encrypted Queries using Homomorphic Encryption," **JKMS** (Journal of the Korean Mathematical Society), vol. 62, pp. 1237–1263, Sep. 2025.

J05 Jung Hee Cheon, Hyeongmin Choe†, Jungjoo Seo, Hyoeun Seong, "SMAUG(-T), Revisited: Timing-secure, More Compact, Less Failure," **IEEE ACCESS**, vol. 12, pp. 188386–188397, Dec. 2024.

*J04 Seungwan Hong, Jai Hyun Park, Wonhee Cho, Hyeongmin Choe and Jung Hee Cheon†, "Secure tumor classification by shallow neural network using homomorphic encryption," **BMC Genomics**, vol. 23, no. 284, Apr. 2022.

J03 Jung Hee Cheon, Hyeongmin Choe, Donghwan Lee and Yongha Son†, "Faster Linear Transformations in **HElib**, revisited," **IEEE Access**, vol. 7, pp. 50595–50604, Apr. 2019.

*J02 Siyul Lee and Hyeongmin Choe, "On Fourth-order Iterative Methods for Multiple Roots of Nonlinear Equations with High Efficiency," **JoCAAA** (Journal of Computational Analysis and Applications), vol. 18, no. 1, pp. 109–120, Jan. 2015.

*J01 Siyul Lee and Hyeongmin Choe, "Multiplicational Combinations and A General Scheme of Single-step Iterative Methods for Multiple Roots," **JoCAAA** (Journal of Computational Analysis and Applications), vol. 15, no. 6, pp. 1138–1149, Oct. 2013.

Technical Articles & Specifications (non-refereed)

T04 Hyeongmin Choe, Jeongdae Hong, "Korean Post-Quantum Cryptography Algorithm HAETAE: Lattice-based Digital Signature Scheme,"[1] Invited Technical Article, **Review of KIISC** (Korea Institute of Information Security and Cryptology), vol. 35, no. 3, pp. 15–20, June 2026.

T03 Hyeongmin Choe, Jeongdae Hong, "Korean Post-Quantum Cryptography Algorithm SMAUG-T: Lattice-based Key Encapsulation Mechanism,"[2] Invited Technical Article, **Review of KIISC** (Korea Institute of Information Security and Cryptology), vol. 35, no. 3, pp. 21–27, June 2026.

T02 Jung Hee Cheon, Hyeongmin Choe, Julien Devevey, Tim Güneysu, Dongyeon Hong, Markus Krausz, Georg Land, Marc Möller, Junbum Shin, Damien Stehlé and MinJune Yi, "HAETAE: Hyperball bimodAl modulE rejecTion signAture schemE," Algorithm Specification v0.9–v3.0, along with **KpqC Competition** and **NIST PQC Additional Signatures.**

T01 Jung Hee Cheon, Hyeongmin Choe, Joongeun Choi, Dongyeon Hong, Jeongdae Hong, Chi-Gon Jung, Honggoo Kang, Janghyun Lee, Seonghyuck Lim, Aesun Park, Seunghwan Park3, Jungjoo Seo, Hyoeun Seong, and Junbum Shin, "SMAUG(-T): the Key Exchange Algorithm based on Module-LWE and Module-LWR," Algorithm Specification v0.9–v4.0, for **KpqC Competition**.

Manuscripts (non-refereed)

Manuscripts that are archived or near completion.

M02 Jung Hee Cheon, Hyeongmin Choe, Yongdong Yeo, "Multi-Party Homomorphic Encryption with Dynamicity and Ciphertext Reusability." **Cryptology ePrint Archive, Paper 2025/581**, Apr. 2025.

M01 Jung Hee Cheon, Hyeongmin Choe, Saebyul Jung, Duhyeong Kim, Dah Hoon Lee, and Jai Hyun Park, "Arithmetic PCA for Encrypted Data," **Cryptology ePrint Archive, Paper 2023/1544**, Oct. 2023.

Teaching Record

- **Calculus TA Seminar**, *at Dept. of Mathematical Sciences, SNU*, 2024 Spring
  - **Role:** TA, guiding new TAs on teaching skills and student management strategies.
- **Calculus Practice Sessions**, *at College of Natural Sciences, SNU*, 2020–2023 (7 semesters)
  - **Role:** TA and Lecturer, delivering 2-hour weekly practice sessions with summarized content and guided students.
  - **Teaching Evaluation (Student Survey):** Avg. 94.6 / 100. Awarded "*Excellence in Teaching*" in 2023 Spring.
- **(i-TAP) Post-Quantum Cryptography**, *at SK Hynix Inc.*, Apr.–May (5 weeks), 2021
  - **Role:** TA and Co-lecturer, for i-TAP (Innovative Technology Advancement Program), delivering 8 of 26 total hours as a co-lecturer. Also contributed to course material development and led Q&A and discussion sessions on lattice-based PQC.
- **Korean Mathematical Olympiad (KMO) Winter/Summer Schools**, *organized by KMS*, 2013–2014
  - **Period:** Jan. & Aug., 2013, and Jan. & Aug., 2014 (each 2–3 weeks)
  - **Role:** Residential TA, managing and supporting elementary to high school students during intensive camp; delivering exercise sessions.

Contributed Talks

Conferences and Workshops

- **ACM CCS 2025**, *at Taipei, Taiwan*, Oct. 14, 2025

[1] Title translated. Original title is "한국형 양자내성암호 HAETAE: 격자기반 전자서명 스킴."
[2] Title translated. Original title is "한국형 양자내성암호 SMAUG-T: 격자기반 키 캡슐화 메커니즘 스킴."

  - **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
- **2024 Crypto Winter Camp**, *organized by SNU Cryptography Lab, at Vivaldi Park, Korea*, Jan. 4, 2024 (1h)
  - **Title:** IND-CPA^{D} and KR^{D} Security of FHE and Application to Threshold-FHE
- **2023 Crypto Winter Camp**, *organized by SNU Cryptography Lab, at Konjiam Resort, Korea*, Jan. 5, 2023 (1h)
  - **Title:** Introduction to SMAUG KEM and HAETAE Signature Schemes
- **2022 KMS Spring Meeting**, *organized by KMS*, *Virtual*, Apr. 28, 2022 (0.5h)
  - **Title:** Efficient, Round-optimal Blind Signatures from Standard Assumptions
- **2020 KMS Annual Meeting**, *organized by KMS*, *Virtual*, Oct. 24, 2020 (0.5h)
  - **Title:** Conversion between Two RLWE-based FHE Schemes and its Application