

## Personal

- **Full Name:** Hyeongmin Choe
- **Contact Details:**
  - **Email:** hyeongmin.choe528@gmail.com
- **Nationality:** Republic of Korea (South Korea)
- **Date of Birth:** May 28th, 1994
- **Personal Links:**
  - **Personal Website:** <https://hmchoe0528.github.io/>
  - **Google Scholar:** <https://scholar.google.co.kr/citations?user=Ih2nebEAAAAJ>

## Education

- **Ph.D. in Mathematical Sciences—Cryptography**
  - **Institution:** Department of Mathematical Sciences, Seoul National University, Seoul, Korea
  - **Adviser:** Professor Jung Hee Cheon
  - **Period:** September 1st, 2019 - February 26th, 2025
  - **Thesis Title:** Accelerating Homomorphic Computation through Machine-Efficient Arithmetic
  - **Note:** Integrated MA/PhD, 2 years for M.S. and 3+ years for Ph.D.
- **B.S. in Mathematical Sciences**
  - **Institution:** Department of Mathematical Sciences, Seoul National University, Seoul, Korea
  - **Period:** March 2nd, 2013 - August 29th, 2019
  - **Grade of Qualification:** Cum Laude.

## Awards & Honors

### Awards

- **Korean Post-Quantum Cryptography Standardization Competition (KpqC)**, National Security Research Institute (NSR) and National Intelligence Service (NIS). A three-year competition (Sept. 2021 – Jan. 2025) for standardizing Korean PQC Algorithms: KEM/PKE and Digital Signature.
  - **Winner in KEM/PKE:** *SMAUG-T* Key Encapsulation Mechanism, based on [C01, J05].
    - \* website: <https://www.kpqc.cryptolab.co.kr/smaug-t>.
  - **Winner in Digital Signature:** HAETAE Digital Signature scheme, based on [C02].
    - \* website: <https://www.kpqc.cryptolab.co.kr/haetae>.
- **Korean National Cryptography Contest**, National Security Research Institute (NSR). An annual contest that awards cryptography research papers to encourage (under)graduate students and post-doctoral researchers in Korea.
  - **Grand Prize** for C03, **Honorable Mention** for M03, and **Special Award** for J05, Oct. 2024.
  - **Honorable Mention** for M01, Oct. 2022.
- **TA Awards**, Seoul National University, Dept. of Mathematical Sciences
  - **Excellence in Teaching:** for teaching “Honor Calculus Practice 1 (2023 Spring),” Aug. 2023.
- **2020 iDASH Genomic Data Privacy and Security Protection Competition**, American National Institutes of Health
  - **First Place Prize** in Track I: “Secure Multi-label Tumor Classification using Homomorphic Encryption,” Dec. 2020. Latter published as \*J04

### Honors

- **BK 21+ Scholarship**, Ministry of Education of Korea

- **Period:** Sep. 2019 – Present
- **Presidential Science Scholarship** (Undergraduate), Korea Student Aid Foundation
  - **Period:** Mar. 2013 – Dec. 2018.

## Experiences

---

- **Cryptography Engineer**
  - **Institution:** CryptoLab Inc., Seoul, Korea.
  - **Period:** March 2025 - Present
  - **Topic:** Homomorphic Encryption (HE) and Lattice-based Post-Quantum Cryptography (PQC), focusing on improving HE, implementing practical HE applications, and improving and standardizing KpqC schemes.
- **Visiting Researcher**
  - **Institution:** École Normale Supérieure de Lyon, Lyon, France.
  - **Period:** September 1st - October 31st, 2023 (2 months, during PhD studies)
  - **Topic:** Lattice-based cryptography, focusing on new concrete constructions of digital signatures.
- **Sergeant**
  - **Organization:** Intelligence System Management Group, Republic of Korea Air Force (ROKAF)
  - **Period:** July 19th, 2015 to July 19th, 2017 (2-year mandatory military service)

## Public & Professional Services

---

### Invited Talks

- **Invited Talk, Conference:** 2025 KMS Spring Meeting, Korean Mathematical Society (KMS), Korea Advanced Institute of Science & Technology (KAIST), Korea
  - **Title:** HAETAE and SMAUG-T: Korean PQC Standards
  - **Date:** April 25th, 2025.
- **Invited Talk, Graduate Seminar** at Faculty of Computer Science, Security Engineering, Ruhr University Bochum (RUB), Germany
  - **Title:** Recent Advances in Fully Homomorphic Encryption
  - **Date:** January 21st, 2025 (1.5h), during a research visit on Jan. 16-21st.
- **Invited Talk, Graduate Seminar** at Dept. of Convergence Security Engineering, Sungshin Women's University, Korea
  - **Title:** HAETAE: Shorter Lattice-based Fiat-Shamir Signatures
  - **Date:** May 21st, 2024 (1.5h)
- **Invited Talk, Research Camp:** 2024 Algebra Camp, Center for Quantum Structures in Modules and Spaces (QSMS), Yangpyeong Bloomvista, Korea
  - **Title:** Bridging Algebraic Number Theory to Post-Quantum Digital Signatures
  - **Date:** February 5th, 2024 (0.5h)
- **Invited Talk, Lecture Series:** 2nd 10-10 Gauss Distinguished Lecture, Industrial & Mathematical Data Analytics Research Center (IMDARC), Seoul National University (SNU), Korea
  - **Title:** Mathematical Foundation of Lattice Crypto (jointly with Prof. Jung Hee Cheon, 1.25h in total), A Pre-study of Damien Stehlé's Distinguished Lecture on NIST PQC Standards
  - **Date:** September 15th, 2023 (0.5h)
- **Invited Talk, Graduate Seminar** at School of Cybersecurity, Korea University, Korea
  - **Title:** HAETAE, a Post-Quantum Signature Scheme
  - **Date:** July 24th, 2023 (2h)
- **Invited Talk, Workshop:** KIAS-JBNU KpqC Workshop, Korea Institute for Advanced Study (KIAS), Jeonbuk National University, Korea
  - **Title:** HAETAE: Rejecting on Hyperballs
  - **Date:** May 19th, 2023 (2h)

## Invited Lectures & Training

- **Invited Lectures:** *Cryptography Training for Information Security Professionals*, Korea Cryptography Forum.
  - **Details:** The course was jointly organized by Korea Institute of Information Security and Cryptology (KIISC) and Korea Cryptography Forum (KCF). Delivered pre-recorded lectures of a total of 3 hours on lattice-based PQC, as part of a one-week training course.
  - **Date:** Pre-recorded in May, scheduled in June 2025.
- **Invited Lecture:** Undergraduate Course at Dongguk University, Korea
  - **Title:** Security in the Post-Quantum Era: Post-Quantum Cryptography and Standardizations (Translated)
  - **Date:** May 29th, 2025.
- **Invited Lectures:** *PQC Training Course*, CryptoLab Inc., Seoul National University (SNU), Korea
  - **Details:** The course was jointly conducted by Dr. Damien Stehlé (CryptoLab Inc.) and Dr. Inkwon Yu (CryptoLab Inc.). Delivered two half-day lectures (7 hours total) as part of a 3-week PQC training course, focusing on the concrete security of lattice-based PQC schemes. The course was given in English and attended by researchers from a governmental organization, with a daily schedule of 7-9 hours of lectures and hands-on training.
  - **Material:** Available at [https://github.com/hmchoe0528/PQC\\_training](https://github.com/hmchoe0528/PQC_training)
  - **Date:** July 16-17th, 2024

## Journal & Conference Reviewing

- **Journals:** Design, Codes and Cryptography (DCC), Journal of Cryptology (JoC).
- **Conferences:** Sub/External reviewer for ANTS 2020, MathCrypt 2021, PQCrypto 2021, Asiacrypt 2021, 2022, ACM CCS 2022, FHE.org 2022, PQCrypto 2023, PKC 2024, Eurocrypt 2024, PQCrypto 2024, Asiacrypt 2025.

## Publications

---

Authors are listed in alphabetical order by last name, unless an asterisk(\*) is indicated. A dagger (†) indicates the corresponding author, when applicable.

### Conferences (refereed)

- C04 Hyeongmin Choe<sup>†</sup>, “Toward Practical Threshold FHE: Low Communication, Computation and Interaction,” *ACM CCS 2024 Doctoral Symposium*, 3-Page Extended Abstract.
- C03 Jung Hee Cheon, Hyeongmin Choe<sup>†</sup>, Alain Passelègue, Damien Stehlé, and Elias Suvanto, “Attacks Against the IND-CPA<sup>D</sup> Security of Exact FHE Schemes,” *The ACM Conference on Computer and Communications Security 2024 (ACM CCS 2024)*.
- 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,” *The annual Conference on Cryptographic Hardware and Embedded Systems 2024 (CHES 2024)*.
- C01 Jung Hee Cheon, Hyeongmin Choe<sup>†</sup>, Dongyeon Hong, and MinJune Yi, “SMAUG: Pushing Lattice-based Key Encapsulation Mechanisms to the Limits,” *Selected Areas in Cryptography 2023 (SAC 2023)*.

### Journals (refereed)

- J06 Jung Hee Cheon, Hyeongmin Choe, and Jai Hyun Park, “Tree-based Lookup Table on Batched Encrypted Queries using Homomorphic Encryption,” *Accepted to Journal of the Korean Mathematical Society*.
- J05 Jung Hee Cheon, Hyeongmin Choe<sup>†</sup>, 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<sup>†</sup>, “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<sup>†</sup>, “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,” *Journal of Computational Analysis and Applications*, vol. 18(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,” *Journal of Computational Analysis and Applications*, vol. 15(6), pp. 1138–1149, Oct. 2013.

## Manuscripts (non-refereed)

Manuscripts that are archived or near completion.

- M03 Jung Hee Cheon, Hyeongmin Choe, Yongdong Yeo, “Reusable Dynamic Multi-Party Homomorphic Encryption.” *Cryptology ePrint Archive, Paper 2025/581*, April 2025.
- M02 Jung Hee Cheon, Hyeongmin Choe, Minsik Kang, Jaehyung Kim, Seonghak Kim, Johannes Mono, Taeyeong Noh “Grafting: Decoupled Scale Factors and Modulus in RNS-CKKS,” *Cryptology ePrint Archive, Paper 2024/1014*, June 2024. *In submission*.
- 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 (3341.781)**
  - **Institute:** Dept. of Mathematical Sciences, Seoul National University
  - **Semester(s):** 2024 Spring
  - **Responsibility:** TA. Guiding new TAs in teaching skills and student management.
- **(i-TAP) Post-Quantum Cryptography**
  - **Institute:** SK Hynix Inc.
  - **Period:** April to May (5 weeks), 2021.
  - **Responsibility:** TA and Co-lecturer (8 among 26 hours). Develop course materials (Introduction to PQC) and engage with participants in discussions and Q&A sessions.
- **(Differential & Integral / Honor) Calculus Practice 1 & 2 (L0442.200, 400, 600, 800, 1000, 1200)**
  - **Institute:** College of Natural Sciences, Seoul National University
  - **Semester(s):** 2020 Spring & Fall, 2021 Spring & Fall, 2022 Spring, and 2023 Spring & Fall, respectively
  - **Responsibility:** TA and Lecturer, assisting the main courses by conducting the lectures (2 hours weekly) with summarized contents and practice sessions.
  - **Teaching evaluations:** (student survey, averaged) 27.7/30, 34.0/35, 33.4/35, 32.0/35, 33.4/35, 34.6/35, and 32.7/35, respectively. Received “Excellence in Teaching” from the TA Awards, for teaching Honor Calculus Practice 1 (2023 Spring).
- **Korean Mathematical Olympiad (KMO) Winter/Summer Schools**
  - **Institute:** The Korean Mathematical Society
  - **Period:** 2013 January, 2013 August, 2014 January, and 2014 August.
  - **Responsibility:** Residential TA. Manage and support gifted elementary/high school students during 2 weeks of residential Winter/Summer schools, including preparing and conducting problem-solving exercise sessions and assessments.

## Patents

---

- Jung Hee Cheon, Hyeongmin Choe, “Apparatus for conversion of homomorphic encrypted message and method thereof,”
  - Korea Patent No. KR1027825570000, Granted, Feb. 2025.
- Jung Hee Cheon, Hyeongmin Choe, “Apparatus for generating blind signature and method thereof,”
  - Applications No. KR20230127905A and US20230291573A1, Pending.
- Jung Hee Cheon, Hyeongmin Choe, Dongyeon Hong, “Electronic device for encrypting data by public key and methods thereof,”
  - Applications No. KR20240081407A and US20240178992A1, Pending.
- Jung Hee Cheon, Hyeongmin Choe, Jai Hyun Park, “Electronic device for searching encrypted data and methods thereof,”
  - Applications No. KR20240118024A and US20240354343A1, Pending.
- Jung Hee Cheon, Hyeongmin Choe, Jai Hyun Park, “Electronic device for making decision and methods thereof,”

- Applications No. KR20240118 025A and US20240289650A1, Pending.

## Contributed Talks

---

Contributed and Conference Talks.

- **Contributed Talk, Affiliated Workshop:** ACM CCS 2024 Doctoral Symposium, Salt Lake City, US
  - **Title:** Toward Practical Threshold FHE: Low Communication, Computation and Interaction
  - **Date:** October 2024.
- **Team Presenter, Colloquium:** KpqC Contest 2nd Round Colloquium, KpqC Research Group, Hansung University, Korea
  - **Title:** HAETAE v3.0
  - **Date:** August 2024.
- **Contributed Talk, Research Camp:** 2024 Crypto Winter Camp, SNU Cryptography Lab, Vivaldi Park, Korea
  - **Title:** IND-CPA<sup>D</sup> and KR<sup>D</sup> security of FHE and application to Threshold-FHE
  - **Date:** January 2024.
- **Contributed Talk, Conference:** Selected Areas in Cryptography (SAC) 2023, University of New Brunswick, Canada
  - **Title:** SMAUG: Pushing Lattice-based Key Encapsulation Mechanisms to the Limits
  - **Date:** October 2023
- **Team Presenter, Research Camp:** 2023 KpqC Winter Camp, KpqC Research Group, Chung-Ang University, South Korea
  - **Title:** Introduction to HAETAE
  - **Date:** February 2023
- **Contributed Talk, Research Camp:** 2023 Crypto Winter Camp, SNU Cryptography Lab, Konjiam Resort, Korea
  - **Title:** Introduction to SMAUG KEM and HAETAE signature schemes
  - **Date:** January 2023