# Hyeongmin Choe
### PHD, CRYPTOGRAPHER

✉ hyeongmin (dot) choe528 (at) gmail.com | ⌂ hmchoe0528.github.io | ⊙ hmchoe0528 | ⊞ hyeongmin-choe

## Personal

- **Full Name:** Hyeongmin Choe
- **Contact Details:**
    - **Email:** hyeongmin.choe528@gmail.com
- **Personal Links:**
    - **Personal Website:** `https://hmchoe0528.github.io/`
    - **Google Scholar:** `https://scholar.google.co.kr/citations?user=Ih2nebEAAAAJ`

## Research Interests

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

## Education

- **Ph.D. in Mathematical Sciences—Cryptography**
    - **Institution:** Department of Mathematical Sciences, Seoul National University, Seoul, Korea
    - **Adviser:** Professor Jung Hee Cheon
    - **Period:** Sep. 2019 - Feb. 2025
    - **Thesis Title:** Accelerating Homomorphic Computation through Machine-Efficient Arithmetic
    - **Note:** Integrated MS/PhD, 2 years for MS and 3+ years for PhD.
- **B.S. in Mathematical Sciences**
    - **Institution:** Department of Mathematical Sciences, Seoul National University, Seoul, Korea
    - **Period:** March 2013 - Aug. 2019
    - **Grade of Qualification:** Cum Laude.

## Awards & Honors

### Awards

- **Korean Post-Quantum Cryptography Standardization (KpqC) Competition**, National Security Research Institute (NSR) and National Intelligence Service (NIS). A three-year competition (Sep. 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. The result was later published as J04

## Honors

- **BK 21+ Scholarship**, Ministry of Education of Korea
    - **Period:** Sep. 2019 – Feb. 2025.
- **Presidential Science Scholarship** (Undergraduate), Korea Student Aid Foundation
    - **Period:** March 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.
- **Research Visit**
    - **Institution:** École Normale Supérieure de Lyon, Lyon, France.
    - **Period:** Sep. - Oct. 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 2015 - July 2017 (2 years, mandatory military service)

# Public & Professional Services

## Invited Talks

### Conferences and Workshops

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

### Research Camps and Seminars

- **Kookmin University, Korea**, Dept. of Information Security, Cryptography, and Mathematics
    - **Title:** Security in the Post-Quantum Era: Post-Quantum Cryptography and Standardizations (Translated)
    - **Date:** June 13, 2025 (1h)
- **Ruhr Univ. Bochum, Germany**, Faculty of Computer Science, Security Engineering
    - **Title:** Recent Advances in Fully Homomorphic Encryption
    - **Date:** Jan. 21, 2025 (1.5h), during a week of research visit
- **Sungshin Women's Univ., Korea**, Dept. of Convergence Security Engineering
    - **Title:** HAETAE: Shorter Lattice-based Fiat-Shamir Signatures
    - **Date:** May 21, 2024 (1.5h)
- **2024 KpqC Winter Camp**, KpqC Research Group, Sogang Univ., Korea
    - **Title:** HAETAE
    - **Date:** Feb. 27, 2024 (1h)
- **2024 Algebra Camp**, QSMS, Yangpyeong Bloomvista, Korea

- **Title:** Bridging Algebraic Number Theory to Post-Quantum Digital Signatures
  - **Date:** Feb. 5, 2024 (30m)
- **Korea University, Korea**, School of Cybersecurity
  - **Title:** HAETAE, a Post-Quantum Signature Scheme
  - **Date:** July 24, 2023 (2h)
- **2023 KpqC Winter Camp**, KpqC Research Group, Chung-Ang Univ., Korea
  - **Title:** Introduction to HAETAE
  - **Date:** Feb. 22, 2023 (1h)

### Lectures and Training Programs

- **Cryptography Training for Information Security Professionals**, Korea Cryptography Forum.
  - **Details:** Pre-recorded lectures on lattice-based PQC, as part of a one-week training program.
  - **Date:** Pre-recorded in May, scheduled in June 2025 (3h)
- **Dongguk University, Korea**, Undergraduate Course at Dept. of CS & AI
  - **Title:** Security in the Post-Quantum Era: Post-Quantum Cryptography and Standardizations (Translated)
  - **Date:** May 29, 2025 (1.5h)
- **PQC Training Course**, CryptoLab Inc.
  - **Details:** The course was conducted by Dr. Damien Stehlé and Dr. Inkwan Yu. Two half-day lectures on the concrete security of lattice-based PQC were provided in English, as part of a 3-week training course.
  - **Material:** Available at `https://github.com/hmchoe0528/PQC_training`
  - **Date:** July 16-17, 2024 (7h)
- **2nd 10-10 Gauss Distinguished Lecture Series**, IMDARC, SNU
  - **Details:** A Pre-study of Damien Stehlé's Distinguished Lecture on NIST PQC Standards, focusing on the mathematical foundations of Lattice Crypto (jointly with Prof. Jung Hee Cheon)
  - **Date:** Sep. 15, 2023 (30m)

## 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 alphabetically by last name (see AMS 2004 statement), unless marked with an asterisk (*). A dagger (†) indicates the corresponding author, when applicable.

## Conferences (refereed)

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," *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[†], 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[†], 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, April 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, April 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**, Dept. of Mathematical Sciences, SNU, 2024 Spring
  - **Role:** TA. Guided new TAs on teaching skills and student management strategies.
- **Calculus Practice Sessions**, College of Natural Sciences, SNU, 2020 - 2023 (7 semesters)
  - **Role:** TA and Lecturer. Delivered 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**, SK Hynix Inc., April - May (5 weeks), 2021
  - **Role:** TA and Co-lecturer. Delivered 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**, Korean Mathematical Society, 2013-2014
  - **Period:** Jan. & Aug., 2013, and Jan. & Aug., 2014 (each 2-3 weeks)
  - **Role:** Residential TA. Managed and supported gifted students during intensive camps. Led problem-solving exercises and evaluations.

# 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**

**Conferences and Workshops**

- **ACM CCS 2024 Doctoral Symposium**, Salt Lake City, US
  - **Title:** Toward Practical Threshold FHE: Low Communication, Computation and Interaction
  - **Date:** Oct. 14, 2024
- **Selected Areas in Cryptography (SAC) 2023**, Univ. of New Brunswick, Canada
  - **Title:** SMAUG: Pushing Lattice-based Key Encapsulation Mechanisms to the Limits
  - **Date:** Aug. 16, 2023

**Research Camps and Colloquiums**

- **KpqC Contest 2nd Round Colloquium**, KpqC Research Group, Hansung Univ., Korea
  - **Title:** HAETAE v3.0
  - **Date:** Aug. 28, 2024 (20m)
- **2024 KMS Spring Meeting**, Korean Mathematical Society (KMS), Daejeon Convention Center, Korea
  - **Title:** IND-CPA$^D$ and KR$^D$ Security of Exact (F)HEs
  - **Date:** April 19, 2024 (20m)
- **2024 Crypto Winter Camp**, SNU Cryptography Lab, Vivaldi Park, Korea
  - **Title:** IND-CPA$^D$ and KR$^D$ security of FHE and application to Threshold-FHE
  - **Date:** Jan. 4, 2024 (1h)
- **2023 Crypto Winter Camp**, SNU Cryptography Lab, Konjiam Resort, Korea
  - **Title:** Introduction to SMAUG KEM and HAETAE signature schemes
  - **Date:** Jan. 5, 2023 (1h)
- **2022 KMS Spring Meeting**, Korean Mathematical Society (KMS), Virtual
  - **Title:** Efficient, round-optimal blind signatures from standard assumptions
  - **Date:** April 28, 2022 (20m)
- **2020 KMS Annual Meeting**, Korean Mathematical Society (KMS), Virtual
  - **Title:** Conversion between two RLWE-based FHE schemes and its application
  - **Date:** Oct. 24, 2020 (20m)