Curriculum Vitae

Hyeongmin **Choe**

CRYPTOGRAPHER

27-441, Gwanak-ro 1, Gwanak-gu, Seoul, South Korea

☎ (+82) 10-3509-4726 | ✉ sixtail528@snu.ac.kr | ⌂ hmchoe0528.github.io | hmchoe0528 | hyeongmin-choe

Personal

- **Full Name:** Hyeongmin Choe
- **Contact Details:**
  - **Email:** sixtail528@snu.ac.kr
  - **Phone:** 82-10-3509-4726 (cell phone), 82-02-880-6272 (office)
- **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
  - **Date:** February 28th, 2025 (fully expected)
  - **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
  - **Date:** August 29th, 2019
  - **Grade of Qualification:** Cum Laude.

Experiences

- **Sergeant**
  - **Organization:** Intelligence System Management Group, Republic of Korea Air Force (ROKAF)
  - **Period:** July 19th, 2015 to July 19th, 2017 (discharged as a Sergeant)
- **Visiting Researcher**
  - **Institution:** École Normale Supérieure de Lyon, Lyon, France.
  - **Period:** September 1st - October 31st, 2023
  - **Topic:** Lattice-based cryptography, focusing on new concrete construction of digital signatures.

Teaching Record

- **Calculus TA Seminar (3341.781)**
  - **Institute:** Department 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.

Public & Professional Services

Invited Talks & Lectures

- **Invited Speaker**, Seminar at Faculty of Computer Science, Security Engineering, Ruhr University Bochum, Germany
  - **Title:** Recent Advances in Fully Homomorphic Encryption
  - **Date:** January 21st, 2025 (1.5h), during research visit (Jan. 16-21.)
- **Invited Lecturer**, PQC Training Course, Korea
  - **Details:** The course was jointly conducted by Dr. Damien Stehlé (CryptoLab Inc.) and Dr. Inkwan 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`
  - **Date:** July 16-17th, 2024
- **Invited Speaker**, Seminar at Department of Convergence Security Engineering, Sungshin Women's University, Korea
  - **Title:** HAETAE: Shorter Lattice-based Fiat-Shamir Signatures
  - **Date:** May 21st, 2024 (1.5h)
- **Invited Speaker**, 2024 Algebra Camp, Yangpyeong Bloomvista, Korea
  - **Title:** Bridging Algebraic Number Theory to Post-Quantum Digital Signatures
  - **Date:** February 5th, 2024 (0.5h)
- **Invited Speaker**, 2nd 10-10 Gauss Distinguished Lecture, 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 Speaker**, Seminar at School of Cybersecurity, Korea University, Korea
  - **Title:** HAETAE, a Post-Quantum Signature Scheme
  - **Date:** July 24th, 2023 (2h)

Reviewer

- **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.

Research Grants

Funded Projects

Selected Funded Projects participated in as a PhD Researcher (Graduate Research Assistant).

- **Sensitive Data Protection using HE and its Acceleration (Samsung Elec.)**

  - **Period:** From September 2020 to present
- **Industrial & Mathematical Data Analytics Research Center (NRF, MSIT)**
  - **Period:** From September 2019 to present
- **Development and Library Implementation of Fully Homomorphic ML Algorithms supporting Neural Network Learning over Encrypted Data (IITP)**
  - **Period:** From September 2020 to December 2023
- **DARPA Data Protection in Virtual Environments** (DPRIVE)
  - **Period:** From December 2022 to December 2023
- **HE Technology for 6G Security** (LG Elec.)
  - **Period:** From March 2022 to March 2023

Publications

Authors are listed in alphabetical order by last name, unless an asterisk(*) is indicated.

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)

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," *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 archived or near completion.

M04 Jung Hee Cheon, Hyeongmin Choe, Yongdong Yeo, "Reusable Dynamic Multi-Party Homomorphic Encryption."

M03 Jung Hee Cheon, Hyeongmin Choe, Minsik Kang, Jaehyung Kim, "Grafting: Complementing RNS in CKKS," *Cryptology ePrint Archive, Paper 2024/1014*, June 2024. *In submission.*

M02 Jung Hee Cheon, Hyeongmin Choe, and Jai Hyun Park, "Tree-based Lookup Table on Batched Encrypted Queries using Homomorphic Encryption," *Cryptology ePrint Archive, Paper 2024/087*, Jan. 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.

Specifications (non-refereed)

Specifications submitted to standardization processes.

- **HAETAE** (based on C02), available at `https://www.kpqc.cryptolab.co.kr/haetae`.
  - KpqC Competition, Round 2 (Feb. 2024), selected as final winner.
  - NIST Additional Digital Signature Schemes, Round 1 (May 2023)
  - KpqC Competition, Round 1 (Dec. 2022)
- **SMAUG(-T)** (based on C01 and J05), available at `https://www.kpqc.cryptolab.co.kr/smaug-t`.
  - KpqC Competition, Round 2 (Feb. 2024), selected as final winner.
  - KpqC Competition, Round 1 (Dec. 2022)

Awards & Honors

Awards

- **Korean Post-Quantum Cryptography Standardization Competition**, National Security Research Institute (NSRI) and National Intelligence Service (NIS)
  Three-year competition (Sept. 2021 – Jan. 2025) for standardizing Korean PQC Algorithms: KEM/PKE and Digital Signature.
  - *Selected Algorithm* in KEM/PKE: SMAUG-T Key Encapsulation Mechanism scheme [C01, J05].
  - *Selected Algorithm* in Digital Signature: HAETAE Digital Signature scheme [C02].
- **Korean National Cryptography Contest**, National Security Research Institute (NSRI)
  An annual contest that awards cryptography research papers to encourage undergraduate/graduate students in Korea.
  - *Grand Prize* for C03, Oct. 2024.
  - *Encouragement Prize* for M04, Oct. 2024.
  - *Special Prize* for J05 (with a slightly different working title), Oct. 2024.
  - *Encouragement Prize* for M01, Oct. 2022.
- **TA Awards**, Seoul National University, Department 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.

Contributed Talks

Selected Contributed and Conference Talks.

- **Toward Practical Threshold FHE: Low Communication, Computation and Interaction**
  - **ACM CCS 2024 Doctoral Symposium** (affiliated with ACM CCS 2024), Salt Lake City, USA, Oct. 2024.
- **IND-CPA^D and KR^D security of FHE and application to Threshold-FHE**
  - 2024 Crypto Winter Camp, Vivaldi Park, South Korea, Jan. 2024.
- **SMAUG: Pushing Lattice-based Key Encapsulation Mechanisms to the Limits**
  - SAC 2023, University of New Brunswick, Canada, Oct. 2023.
- **HAETAE: Rejecting on Hyperballs**
  - KIAS-JBNU KpqC Workshop, Jeonbuk National University, South Korea, May 2023.
- **Introduction to HAETAE**
  - 2023 KpqC Winter Camp, Chung-Ang University, South Korea, Feb. 2023.
- **Introduction to SMAUG KEM and HAETAE signature schemes**
  - 2023 Crypto Winter Camp, Konjiam Resort, South Korea, Jan. 2023.