Hyeongmin Choe

📍27-441, Gwanak-ro 1, Gwanak-gu, Seoul, South Korea
✉sixtail528@snu.ac.kr ☎+82-2-880-6272 🏠https://hmchoe0528.github.io

OVERVIEW

I am an Integrated Ph.D. student at the Department of Mathematical Sciences, Seoul National University (SNU), Republic of Korea. My advisor is Prof. Jung Hee Cheon. I work on cryptography, currently focusing on Homomorphic Encryption (HE) and Lattice-based Post-Quantum Cryptography (PQC). I am a member of *Team SMAUG(-T)* and *Team HAETAE*, participating in PQC standard efforts in KpqC competition and NIST Additional Signatures.

EDUCATION

Seoul National University, Seoul, Republic of Korea

- Integrated Ph.D. in Mathematical Sciences — Sep 2019 – Present
  - Consists of a two-year M.S. course and a three-year Ph.D. course
  - Adviser: Jung Hee Cheon
  - Focus: Cryptography (Homomorphic Encryption, Lattice-based Post-Quantum Cryptography)
- B.S. in Mathematical Sciences — Mar 2013 – Aug 2019

PUBLICATIONS

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

CONFERENCES

C03 Jung Hee Cheon, Hyeongmin Choe, Alain Passelègue, Damien Stehlé, and Elias Suvanto, "Attacks Against the IND-CPA$^{\mathrm{D}}$ Security of Exact FHE Schemes," *Accepted to 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," *Accepted to CHES 2024, Issue 3.*

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 (SAC) 2023.* Feb 2024.

JOURNALS

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

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

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.

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

Specifications submitted to standardization processes.

- HAETAE (based on C02), submitted to *KpqC Competition Round 2* (Feb 2024), *NIST Additional Digital Signature Schemes Round 1* (May 2023), and *KpqC Competition Round 1* (Dec 2022).

- SMAUG(-T) (based on C01), submitted to *KpqC Competition Round 2* (Feb 2024) and *KpqC Competition Round 1* (Dec 2022).

AWARDS & HONORS

AWARDS

- Excellence in Teaching Aug 2023
  Seoul National University, Department of Mathematical Sciences
  for teaching "Honor Calculus Practice 1 (2023 Spring)"
- Encouragement Prize (4th, Top 15) Oct 2022
  (Korean) National Cryptography Contest, National Security Research Institute (NSRI)
  for the manuscript "Arithmetic PCA for Encrypted Data"
- First Place Prize, iDASH Secure Genome Analysis Competition Dec 2020
  iDASH Genomic Data Privacy and Security Protection Competition, National Institutes of Health (NIH)
  in Track I: Secure Multi-label Tumor Classification using Homomorphic Encryption

HONORS

- BK 21+ Scholarship Sep 2019 – Aug 2022, Feb 2023 – Present
  Ministry of Education of Korea
- Presidential Science Scholarship Mar 2013 – Dec 2018
  Korea Student Aid Foundation

TALKS

2024

- HAETAE: Shorter Lattice-based Fiat-Shamir Signatures May 2024
  Invited Talk, Sungshin Women's University, South Korea
- Bridging Algebraic Number Theory to Post-Quantum Digital Signatures Feb 2024
  2024 Algebra Camp, Bloomvista, South Korea
- IND-CPA^{D} and KR^{D} security of FHE and application to Threshold-FHE Jan 2024
  2024 Crypto Winter Camp, Vivaldi Park, South Korea

2023

- Mathematical Foundation of Lattice Crypto (jointly with Jung Hee Cheon) Sep 2023
  Pre-study of Damien Stehlé's talk, "CRYSTALS-KYBER, CRYSTALS-DILITHIUM and Beyond"
  Distinguished Lecture on NIST PQC Standards, Seoul National University, South Korea
- SMAUG: Pushing Lattice-based Key Encapsulation Mechanisms to the Limits Aug 2023
  SAC 2023, University of New Brunswick, Canada
- HAETAE, a Post-Quantum Signature Scheme Jul 2023
  Invited Talk, Korea University, South Korea
- HAETAE: Rejecting on Hyperballs May 2023
  KIAS-JBNU KpqC Workshop, Jeonbuk National University, South Korea
- Introduction to HAETAE Feb 2023
  2023 KpqC Winter Camp, Chung-Ang University, South Korea
- Introduction to SMAUG KEM and HAETAE signature schemes Jan 2023
  2023 Crypto Winter Camp, Konjiam Resort, South Korea

2022 & BEFORE

- Efficient, Round-optimal Blind Signatures from Standard Assumptions Apr 2022
  2022 KMS Spring Meeting, virtual
- Blind Signatures from HE Jan 2022
  2022 Crypto Winter Camp, Konjiam Resort, South Korea
- Security Analysis on NIST PQC Lattice-based Finalists Nov 2021
  3rd KpqC Workshop, Alpensia Resort, South Korea
- Conversion between Two RLWE-based FHE Schemes and its Application Oct 2020
  2020 KMS Fall Meeting, virtual

PROJECTS

List of selective projects.

- DARPA Data Protection in Virtual Environments (DPRIVE) 2022 – 2023
- HE Technology for 6G Security (LG Elec.) 2022 – 2023
- Security Analysis on NIST PQC Finalists (NSR) 2021
- Sensitive Data Protection using HE and its Acceleration (Samsung Elec.) 2020 – 2024

- Development and Library Implementation of Fully Homomorphic ML Algorithms supporting Neural Network Learning over Encrypted Data (IITP) 2020 – 2023

EXPERIENCES

TEACHING

- Invited Lecturer for PQC Training Course, conducted by CryptoLab Inc. 2024
  Concrete Security of Lattice-based PQC Schemes–Lectures and Tutorials (7h)
- Seoul National University, Math Courses TA
  - Calculus TA Seminar 2024
  - Computational Number Theory, Honor Calculus Practice 1, 2 2023
  - Differential & Integral Calculus Practice 1 2022
  - Number Theory, Differential & Integral Calculus Practice 1, Honor Calculus Practice 2 2021
  - Calculus TA Seminar, Calculus Practice 1, Honor Calculus Practice 2 2020
- Korean Mathematical Olympiad (KMO) Winter/Summer School TA Jan 2013 – Aug 2014
  - 2013 & 2014 Winter/Summer Schools

MILITARY

- Republic of Korea Air Force (ROKAF) Jul 2015 – Jul 2017
  Intelligence System Management Group, Gyeryong, discharged as a Sergeant

INTERNSHIPS

- Undergraduate Research Internships
  - Stochastic Representations of the Hyperbolic PDEs 2019
    Seoul National University, advised by Prof. Seung Yeal Ha
  - Homomorphic Signature Schemes and Threshold Cryptosystems 2018 – 2019
    Sejong University, advised by Prof. Ji Sun Shin
  - Lattice Reductions and Homomorphic Encryption with C++ 2018 – 2019
    Seoul National University, advised by Prof. Jung Hee Cheon
  - Machine Learning (Image Processing) with Python, Matlab 2017
    Seoul National University, advised by Prof. Myungjoo Kang

SKILLS

- LaTeX, Matlab, Python: Proficient
- C/C++, Mathematica, SageMath, HTML: Working Knowledge
- R, PyTorch, TensorFlow: Basic

SERVICES

REVIEWER (JOURNALS)

- Design, Codes and Cryptography (DCC), Journal of Cryptology (JoC).

REVIEWER (CONFERENCES)

- ANTS 2020, MathCrypt 2021, PQCrypto 2021, Asiacrypt 2021, 2022, ACM CCS 2022, FHE.org 2022, PQCrypto 2023, PKC 2024, Eurocrypt 2024, PQCrypto 2024.

Last Updated: Jul 2024