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 PhD student at 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 and lattice-based post-quantum cryptography.

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: Prof. Jung Hee, Cheon
  - Focus: Cryptography (Homomorphic Encryption, Lattice-based Post Quantum Cryptography)
- B.S. in Mathematical Sciences   Mar 2013 – Aug 2019

Seoul Science High School, Seoul, Republic of Korea   Mar 2010 – Feb 2013

PUBLICATIONS

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

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

[M01] Hyeongmin Choe, Saebyul Jung, Duhyeong Kim, Dah Hoon Lee and Jai Hyun Park, "Arithmetic PCA for Encrypted Data,"
Encouragement Prize, National Cryptography Contest 2022

AWARDS & HONORS

AWARDS

- Encouragement Prize (4th, Top ??), National Cryptography Contest   Oct 2022
  "Arithmetic PCA for Encrypted Data"
  National Security Research Institute (NSRI)
  $1,250

- First Place Prize, iDASH Secure Genome Analysis Competition   Dec 2020
  Track I: Secure multi-label Tumor classification using Homomorphic Encryption
  IDASH Privacy & Security Workshop 2020
  National Institutes of Health (NIH)

- Excellence Prize (2nd, Top 21), Final Korean Mathematical Olympiad (FKMO)   Apr 2012
  Korean Mathematical Society

- Gold Prize (1st, Top 28), Korean Mathematical Olympiad (KMO)   Sep 2011
  Korean Mathematical Society

HONORS

- BK 21+ Scholarship   Sep 2019 – Present
  Ministry of Education of Korea
  $7,500/year for M.S. and $12, 000/year for Ph.D.

- Presidential Science Scholarship   Mar 2013 – Dec 2018
  Korea Student Aid Foundation
  Tuition + $5, 000/year for 4 years

CONFERENCE PRESENTATIONS	▪ Efficient, Round-optimal Blind Signatures from Standard Assumptions 2022 KMS Spring Meeting, virtual Korean Mathematical Society	Apr 2022
	▪ Security Analysis on NIST PQC Lattice-based Finalists 3rd KpqC Workshop, PyeongChang, South Korea National Security Research Institute (NSRI)	Nov 2021
	▪ Conversion between Two RLWE-based FHE Schemes and its Application 2020 KMS Fall Meeting, virtual Korean Mathematical Society	Oct 2020

EXPERIENCES

TEACHING

▪ Seoul National University, Math Courses TA

• Differential & Integral Calculus Practice 1	2022
• Differential & Integral Calculus Practice 1, Number Theory, Honor Calculus Practice 2	2021
• Calculus Practice 1, Honor Calculus Practice 2, Calculus TA Seminar	2020

▪ Korean Mathematical Olympiad (KMO) Winter/Summer School TA	Jan 2013 – Aug 2014

• 2013 Winter & Summer Schools
• 2014 Winter & Summer Schools

MILITARY

▪ Republic of Korea Air Force (ROKAF) Intelligence System Management Group, Gyeryong Mandatory military service Discharged as a Sergeant	Jul 2015 – Jul 2017

INTERNSHIPS

▪ Undergraduate Research Internships

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

LANGUAGES

▪ Korean: Native language

▪ English: Fluent

SKILLS

▪ LaTeX, Matlab, Python: Proficient

▪ C/C++, HEaaN, HElib, Mathematica, HTML, SageMath: Working Knowledge

▪ HTML, R, PyTorch, TensorFlow: Basic

Last updated on 2022-10-05