

Jai Hyun Park

✉ jhyunp@snu.ac.kr

🌐 <https://jaihyunp.github.io>

📍 27-441, Gwanak-ro 1, Gwanak-gu, Seoul, Republic of Korea, 08826 📞 +82-2-880-6272

OVERVIEW

I am a PhD student majoring in cryptography at Department of Mathematical Sciences, Seoul National University (SNU), Republic of Korea. My advisor is Prof. Jung Hee Cheon. I am interested in a broad range of topics in cryptography from theory to practice. Currently my research focus is on homomorphic encryption, verifiable computation, and their applications.

EDUCATION

Seoul National University, Seoul, Republic of Korea

- Ph.D. in Mathematical Sciences Mar 2020 – Present
 - Advisor: Prof. Jung Hee Cheon
 - Focus: Cryptography (Homomorphic Encryption, Verifiable Computation)
- B.S. in Mathematical Sciences Mar 2013 – Feb 2020

PUBLICATIONS

In the list below, first authors are indicated by asterisks (*) when authors are ordered by contribution; the symbol = indicates a paper with alphabetically-ordered authors.

CONFERENCES

- = [C04] Rashmi Agrawal, Jung Ho Ahn, Flavio Bergamaschi, Ro Cammarota, Jung Hee Cheon, Fillipe D. M. de Souza, Huijing Gong, Minsik Kang, Duhyeong Kim, Jongmin Kim, Hubert de Lassus, Jai Hyun Park, Michael Steiner, Wen Wang, “High-precision RNS-CKKS on fixed but smaller word-size architectures: theory and application,” *11th Workshop on Encrypted Computing & Applied Homomorphic Cryptography (WAHC 2023)*
- = [C03] Youngjin Bae, Jung Hee Cheon, Jaehyung Kim, Jai Hyun Park, Damien Stehlé, “HERMES: Efficient Ring Packing using MLWE Ciphertexts and Application to Transciphering,” *Annual International Cryptology Conference (CRYPTO 2023)*
- [C02] *Garam Lee, *Minsoo Kim, *Jai Hyun Park, Seung-won Hwang, Jung Hee Cheon, “Privacy-Preserving Text Classification on BERT Embeddings with Homomorphic Encryption,” *Annual Conference of the North American Chapter of the Association for Computational Linguistics (NAACL 2022, short)*
- = [C01] Jung Hee Cheon, Duhyeong Kim, and Jai Hyun Park, “Towards a Practical Cluster Analysis over Encrypted Data,” *International Conference on Selected Areas in Cryptography (SAC 2019)*

JOURNALS

- = [J05] Jung Hee Cheon, Wootae Kim, Jai Hyun Park, “Efficient Homomorphic Evaluation on Large Intervals,” *IEEE Transactions on Information Forensics and Security*, 2022
 - Excellence Award, National Cryptography Contest 2020
- [J04] *Jai Hyun Park, Jung Hee Cheon, Dongwoo Kim, “Efficient verifiable computation over quotient polynomial rings,” *International Journal of Information Security*, 2022
- [J03] *Seungwan Hong, Jai Hyun Park, Wonhee Cho, Hyeongmin Choe, Jung Hee Cheon, “Secure tumor classification by shallow neural network using homomorphic encryption,” *BMC Genomics*, 2022
 - First Place Prize, iDASH Genomic Data Privacy and Security Protection Competition 2020
- [J02] *Heehoon Kim, Seunghyo Kang, Jai Hyun Park, Hyunho Ha, Donghoon Lim, “Noise Removal using Support Vector Regression in Noisy Document Images,” *The Korean Journal of Applied Statistics*, 2012
 - Bronze Award, 18th Samsung Humantech Paper Award for High Schools
- [J01] *Heehoon Kim, Seunghyo Kang, Jai Hyun Park, Hyunho Ha, Jinsoo Lim, Donghoon Lim, “Robust Image Fusion Using Stationary Wavelet Transform,” *The Korean Journal of Applied Statistics*, 2011
 - Silver Award, 18th Samsung Humantech Paper Award for High Schools

PROJECTS

- “Data Protection in Virtual Environments (DPRIVE)”. Supported by the *DARPA* Nov 2022 – Present
- “A Study on Cryptographic Primitives for SNARK”. Supported by the *IITP* Grant through the *Korean Government* Apr 2021 – Present

	<ul style="list-style-type: none"> ▪ “Development and Library Implementation of Fully Homomorphic Machine Learning Algorithms supporting Neural Network Learning over Encrypted Data”. Supported by the <i>IITP</i> Grant through the <i>Korean Government</i> Apr 2020 – Present 	
PATENTS	<p>[P01] Jung Hee Cheon, <u>Jai Hyun Park</u>, Wootae Kim, “Apparatus for Processing Non-polynomial Operation on Homomorphic Encrypted Messages and Methods Thereof,”</p> <ul style="list-style-type: none"> • KOR 10-2304992 <i>granted</i>, US 17/499793 	
HONORS & AWARDS	<ul style="list-style-type: none"> ▪ Encouragement Prize, National Cryptography Contest National Security Research Institute “Arithmetic PCA for Encrypted Data” Oct 2022 ▪ First Place Prize, iDASH Genomic Data Privacy and Security Protection Competition National Institutes of Health Track I: Secure multi-label Tumor classification using Homomorphic Encryption Dec 2020 ▪ Excellence Award, National Cryptography Contest National Security Research Institute “Polynomial Approximation on Wide Domain and Logistic Regression over Encrypted Data” Oct 2020 ▪ Award for Excellence in Teaching Seoul National University For teaching Differential and Integral Calculus Sep 2020 ▪ BK 21+ Scholarship Ministry of Education of Korea \$7,500/year for M.S. and \$12,000/year for Ph.D. Mar 2020 – Present ▪ The Presidential Science Scholarship Korea Student Aid Foundation Academic Grant: Tuition + \$5, 000/year for 4 years Mar 2013 – Dec 2018 ▪ Silver Award, 18th Samsung Humantech Paper Award for High School Samsung Electronics “Robust Image Fusion Using Stationary Wavelet Transform” Feb 2012 ▪ Bronze Award, 18th Samsung Humantech Paper Award for High School Samsung Electronics “Noise Removal using Support Vector Regression in Noisy Document Images” Feb 2012 ▪ Silver Medal, Korean Mathematical Olympiad Korean Mathematical Society Sep 2011 	
CONFERENCE PRESENTATIONS	<ul style="list-style-type: none"> ▪ HERMES: Efficient Ring Packing using MLWE Ciphertexts and Application to Transciphering CRYPTO 2023, UC Santa Barbara, USA Aug 2023 ▪ Secure Lookup Table with Homomorphic Encryption 2022 Korean Mathematical Society Spring Meeting, Virtual Apr 2022 ▪ Polynomial Approximation on Wide Domain and Logistic Regression over Encrypted Data 2022 Korean Mathematical Society Fall Meeting, Virtual Oct 2020 ▪ Towards a Practical Cluster Analysis over Encrypted Data 2019 Korean Mathematical Society Fall Meeting, Hong-ik University, Republic of Korea Oct 2019 Selected Areas in Cryptography (SAC) 2019, University of Waterloo, Canada Aug 2019 	
EXPERIENCES	<p>INTERN CryptoLab Inc. Jan 2023 – Feb 2023</p> <p>MILITARY Republic of Korea Army Sergeant Jul 2016 – Apr 2018</p>	
SERVICES	<p>TEACHING ASSISTANT Seoul National University</p> <ul style="list-style-type: none"> • Computational Number Theory Mar 2023 – Aug 2023 • Number Theory Mar 2021 – Aug 2021 • Differential and Integral Calculus Mar 2020 – Present <p>Summer Research Program in Industrial and Applied Mathematics</p>	

- Academic Mentor

Jun 2019 – Aug 2019

REVIEWER / EXTERNAL REVIEWER

- Design, Codes and Cryptography (DCC); Journal of Cryptology (JoC); Information Sciences; IEEE Access
- ANTS 2020; ASIACRYPT 2021, 2022; FHE.org 2022, PQCrypto 2023

SKILLS

- C/C++, \LaTeX , HEaaN: Proficient
- Python: Working Knowledge

LANGUAGES

- Korean: Native language
- English: Fluent

[Last update : 2023-09-28]