

# Jai Hyun Park

✉ jaihyunp@cryptolab.co.kr

🌐 <https://jaihyunp.github.io>

## OVERVIEW

I am a full-time researcher at CryptoLab in Lyon, France. I obtained my Ph.D. in Mathematical Sciences at Seoul National University, advised by 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 fully homomorphic encryption and its applications.

## EMPLOYMENT

**CryptoLab**, Lyon, France

▪ Junior Researcher

Sep 2024 – Present

## EDUCATION

**Seoul National University**, Seoul, Republic of Korea

▪ Ph.D. in Mathematical Sciences

Mar 2020 – Aug 2024

- Advisor: Prof. Jung Hee Cheon
- Focus: Cryptography (Homomorphic Encryption)
- Thesis: Matrix Multiplication on Encrypted Data

▪ B.S. in Mathematical Sciences

Mar 2013 – Feb 2020

## PUBLICATIONS

In the list below, the symbol = indicates papers with alphabetically-ordered authors. The corresponding author is indicated by a dagger (†) for the journal papers.

### CONFERENCES

- = [C05] Youngjin Bae, Jung Hee Cheon, Guillaume Hanrot, Jai Hyun Park, Damien Stehlé, “Plaintext-Ciphertext Matrix Multiplication and FHE Bootstrapping: Fast and Fused,” *Annual International Cryptology Conference (CRYPTO 2024)*
- = [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 Transcipherring,” *Annual International Cryptology Conference (CRYPTO 2023)*
  - Best Award, Korea Cryptography Contest 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)*
  - The authors with the asterisk symbol (\*) contributed equally.
- = [C01] Jung Hee Cheon, Duhyeong Kim, 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<sup>†</sup>, “Efficient Homomorphic Evaluation on Large Intervals,” *IEEE Transactions on Information Forensics and Security*, 2022
  - Excellence Award, Korea Cryptography Contest 2020
- [J04] Jai Hyun Park, Jung Hee Cheon, Dongwoo Kim<sup>†</sup>, “Efficient verifiable computation over quotient polynomial rings,” *International Journal of Information Security*, 2022
- [J03] Seungwan Hong<sup>†</sup>, 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<sup>†</sup>, 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, 18<sup>th</sup> Samsung Humantech Paper Award for High Schools
- [J01] Heehoon Kim<sup>†</sup>, 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, 18<sup>th</sup> Samsung Humantech Paper Award for High Schools

#### MANUSCRIPTS

- = [M03] Jung Hee Cheon, Hyeongmin Choe, Jai Hyun Park<sup>†</sup>, “Tree-based Lookup Table on Batched Encrypted Queries using Homomorphic Encryption,” Available at <https://eprint.iacr.org/2024/087>, 2024
- = [M02] Jung Hee Cheon, Keewoo Lee<sup>†</sup>, Jai Hyun Park, Yongdong Yeo, “Private Database Query with SIMD-Aware Homomorphic Compression,” 2023
- Special Prize, Korea Cryptography Contest 2023
- = [M01] Jung Hee Cheon, Hyeongmin Choe, Saebyul Jung, Duhyeong Kim, Dah Hoon Lee, Jai Hyun Park, “Arithmetic PCA for Encrypted Data,” Available at <https://eprint.iacr.org/2023/1544>, 2023
- Encouragement Prize, Korea Cryptography Contest 2022

#### HONORS & AWARDS

- Korea Cryptography Contest  
*National Security Research Institute*
  - Special Prize Nov 2024
  - Best Award for [C03] Oct 2023
  - Special Prize for [M02] Oct 2023
  - Encouragement Prize for [M01] Oct 2022
  - Excellence Award for [J05] Oct 2020
- First Place Prize, iDASH Genomic Data Privacy and Security Protection Competition Dec 2020  
*National Institutes of Health*  
Track I: Secure multi-label Tumor classification using Homomorphic Encryption
- Award for Excellence in Teaching Sep 2020  
*Seoul National University*  
For teaching Differential and Integral Calculus
- Scholarship
  - BK 21+ Scholarship Mar 2020 – Aug 2023  
*Ministry of Education of Korea*  
\$7,500/year for M.S. and \$12,000/year for Ph.D.
  - The Presidential Science Scholarship Mar 2013 – Feb 2019  
*Korea Student Aid Foundation*  
Academic Grant: Tuition + \$5, 000/year for 4 years
- Samsung Humantech Paper Award for High School
  - Silver Award for [J01] Feb 2012
  - Bronze Award for [J02] Feb 2012
- Silver Medal, Korean Mathematical Olympiad Sep 2011  
*Korean Mathematical Society*

#### TALKS

- Plaintext-Ciphertext Matrix Multiplication and FHE Bootstrapping: Fast and Fused Aug 2024  
CRYPTO 2024, UC Santa Barbara, USA
- HERMES: Efficient Ring Packing using MLWE Ciphertexts and Application to Transciphering Aug 2023  
CRYPTO 2023, UC Santa Barbara, USA
- Tree-based Lookup Table on Batched Encrypted Queries using Homomorphic Encryption Apr 2022  
2022 KMS Spring Meeting, Virtual
- Efficient Homomorphic Evaluation on Large Intervals Oct 2020  
2020 KMS Fall Meeting, Virtual
- Towards a Practical Cluster Analysis over Encrypted Data Oct 2019  
2019 KMS Fall Meeting, Hong-ik University, Republic of Korea

**TEACHING****LECTURER**

- ENS de Lyon
  - Fully Homomorphic Encryption Fall 2024 (M2)
  - Co-lecturer with Alain Passelègue and Damien Stehlé.*
  - Delivered two sessions focusing on homomorphic linear algebra.

**TEACHING ASSISTANT**

- Seoul National University
  - Computational Number Theory Spring 2023
  - Number Theory Spring 2021
  - Differential and Integral Calculus Spring 2020 – Spring 2023

**PATENTS**

- [P01] Jung Hee Cheon, Jai Hyun Park, Wootae Kim, “Apparatus for Processing Non-polynomial Operation on Homomorphic Encrypted Messages and Methods Thereof,”
- KOR 10-2304992, US 11757618, JPN 7449911, *granted*

**PROJECTS**

- “Data Protection in Virtual Environments (DPRIVE)”. Supported by the *DARPA* Dec 2022 – Sep 2023
- “A Study on Cryptographic Primitives for SNARK”. Supported by the *IITP* Grant through the *Korean Government* Apr 2021 – Aug 2024
- “Development and Library Implementation of Fully Homomorphic Machine Learning Algorithms supporting Neural Network Learning over Encrypted Data”. Supported by the *IITP* Grant through the *Korean Government* Apr 2020 – Dec 2023

**EXPERIENCES****RESEARCH INTERN**

- CryptoLab Inc., Lyon, France Jan 2024 – Mar 2024
- CryptoLab Inc., Seoul, Korea Jan 2023 – Feb 2023

**MILITARY**

- Republic of Korea Army Jul 2016 – Apr 2018
- Discharged as a Sergeant

**SERVICES****REVIEWER / EXTERNAL REVIEWER**

- Design, Codes and Cryptography (DCC); Journal of Cryptology (JoC); Information Sciences; IEEE Access
- ANTS 2020; ASIACRYPT 2022, 2021; FHE.org 2022; PQCrypto 2023; EUROCRYPT 2023, 2024

[Last update : 2024-11-20]