Jai Hyun PARK

✉ jaihyunp@gmail.com 🏠 https://jaihyunp.github.io 📍 Lyon, France

Overview

I am a full-time researcher at CryptoLab in Lyon, France. 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. I received my Ph.D. in Mathematical Sciences from Seoul National University, where I was advised by Prof. Jung Hee Cheon.

Employment

- **CryptoLab Inc.** — *Sep 2024 – Present*
  Junior Researcher — Lyon, France
  - Research on fully homomorphic encryption and its application
  - Permanent full-time position (CDI)

Education

- **Seoul National University** — *Mar 2020 – Aug 2024*
  Ph.D. in Mathematical Sciences — Seoul, Korea
  - Focus: Cryptography (Homomorphic Encryption)
  - Thesis: Matrix Multiplication on Encrypted Data
  - Advisor: Prof. Jung Hee Cheon
- **Seoul National University** — *Mar 2013 – Feb 2020*
  B.S. in Mathematical Sciences — Seoul, Korea

Publications

C=Conference, J=Journal, M=Manuscript, P=Patent

Authors are listed in **alphabetical order by last name**, except where an asterisk (*) indicates (co-)first authorship. The corresponding author is marked with a dagger (†) for journal papers.

Conference

[C06] "Ciphertext-Ciphertext Matrix Multiplication: Fast for Large Matrices"
Jai Hyun Park
EUROCRYPT 2025

[C05] "Plaintext-Ciphertext Matrix Multiplication and FHE Bootstrapping: Fast and Fused"
Youngjin Bae, Jung Hee Cheon, Guillaume Hanrot, Jai Hyun Park, Damien Stehlé
CRYPTO 2024

[C04] "High-precision RNS-CKKS on fixed but smaller word-size architectures: theory and application"
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
WAHC 2023

[C03] "HERMES: Efficient Ring Packing using MLWE Ciphertexts and Application to Transciphering"
Youngjin Bae, Jung Hee Cheon, Jaehyung Kim, Jai Hyun Park, Damien Stehlé
CRYPTO 2023

[C02] "Privacy-Preserving Text Classification on BERT Embeddings with Homomorphic Encryption"
*Garam Lee, *Minsoo Kim, *Jai Hyun Park, Seung-won Hwang, Jung Hee Cheon
NAACL 2022, short

[C01] "Towards a Practical Cluster Analysis over Encrypted Data"
Jung Hee Cheon, Duhyeong Kim, Jai Hyun Park
SAC 2019

Journal

[J06] "Tree-based Lookup Table on Batched Encrypted Queries using Homomorphic Encryption"
Jung Hee Cheon, Hyeongmin Choe, Jai Hyun Park†
JKMS

[J05] "Efficient Homomorphic Evaluation on Large Intervals"
Jung Hee Cheon, Wootae Kim, Jai Hyun Park†
IEEE TIFS (2022)

[J04] "Efficient verifiable computation over quotient polynomial rings"
*Jai Hyun Park, Jung Hee Cheon, Dongwoo Kim†
IJIS (2022)

[J03] "Secure tumor classification by shallow neural network using homomorphic encryption"
*Seungwan Hong†, Jai Hyun Park, Wonhee Cho, Hyeongmin Choe, Jung Hee Cheon
BMC Genomics (2022)

[J02] "Noise Removal using Support Vector Regression in Noisy Document Images"
*Heehoon Kim†, Seunghyo Kang, Jai Hyun Park, Hyunho Ha, Donghoon Lim
The Korean Journal of Applied Statistics (2012)

[J01] "Robust Image Fusion Using Stationary Wavelet Transform"
*Heehoon Kim†, Seunghyo Kang, Jai Hyun Park, Hyunho Ha, Jinsoo Lim, Donghoon Lim
The Korean Journal of Applied Statistics (2011)

Manuscript

[M04] "Towards Lightweight CKKS: On Client Cost Efficiency"
Jung Hee Cheon, Minsik Kang, Jai Hyun Park†
Available at https://eprint.iacr.org/2025/720

[M03] "Fast Homomorphic Linear Algebra with BLAS"
Youngjin Bae, Jung Hee Cheon, Guillaume Hanrot, Jai Hyun Park†, Damien Stehlé
Available at https://arxiv.org/abs/2503.16080

[M02] "Private Database Query with SIMD-Aware Homomorphic Compression"
Jung Hee Cheon, Keewoo Lee†, Jai Hyun Park, Yongdong Yeo
Available at https://arxiv.org/abs/2408.17063

[M01] "Arithmetic PCA for Encrypted Data"
Jung Hee Cheon, Hyeongmin Choe, Saebyul Jung, Duhyeong Kim, Dah Hoon Lee, Jai Hyun Park
Available at https://eprint.iacr.org/2023/1544

Patent

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

Honors & Awards

- **Korea Cryptography Contest**
  National Security Research Institute
  - Special Prize for [M04] — *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
- **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**
  Samsung Electronics
  - Silver Award for [J01] *Feb 2012*
  - Bronze Award for [J02] *Feb 2012*
- **Silver Medal, Korean Mathematical Olympiad** *Sep 2010*
  Korean Mathematical Society

Talks

- **Plaintext-Ciphertext Matrix Multiplication and FHE Bootstrapping: Fast and Fused**
  - Invited talk at École polytechnique, France *Feb 2025*
  - CRYPTO 2024, UC Santa Barbara, USA *Aug 2024*
- **HERMES: Efficient Ring Packing using MLWE Ciphertexts and Application to Transciphering**
  - Crypto Winter Camp 2024, Vivaldi Park, Korea *Jan 2024*
  - Invited talk at Dongguk University, Korea *Dec 2023*
  - CRYPTO 2023, UC Santa Barbara, USA *Aug 2023*
- **Tree-based Lookup Table on Batched Encrypted Queries using Homomorphic Encryption**
  - Tech talk at CryptoLab, Korea *Jun 2022*
  - 2022 KMS Spring Meeting, Virtual *Apr 2022*
- **Efficient Homomorphic Evaluation on Large Intervals**
  - Crypto Winter Camp 2022, Virtual *Jan 2022*
  - 2020 KMS Fall Meeting, Virtual *Oct 2020*
- **Towards a Practical Cluster Analysis over Encrypted Data**
  - 2019 KMS Fall Meeting, Hong-ik University, Korea *Oct 2019*
  - SAC 2019, University of Waterloo, Canada *Aug 2019*

Teaching

- **FHE School**
  Organized by Seoul National University and CryptoLab Jan 2025
  - Delivered 9 invited lectures on fully homomorphic encryption over a 3-week program.
- **ENS de Lyon**
  - Fully Homomorphic Encryption (M2) *Fall 2024*
    Co-lecturer with Alain Passelègue and Damien Stehlé.
- **Seoul National University (TA)**
  - Computational Number Theory *Spring 2023*
  - Number Theory *Spring 2021*
  - Differential and Integral Calculus *Spring 2020 – Spring 2023*

PROJECTS

- **Data Protection in Virtual Environments (DPRIVE)** *Dec 2022 – Sep 2023*
  Supported by the DARPA
  - Collaborated with Intel Labs
- **A Study on Cryptographic Primitives for SNARK** *Apr 2021 – Aug 2024*
  Supported by the IITP Grant through the Korean Government
- **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. (FHELab)** *Jan 2024 – Mar 2024*
  Main project: [C05] Lyon, France
- **CryptoLab Inc.** *Jan 2023 – Feb 2023*
  Main Project: [C03] Seoul, Korea

MILITARY

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

REVIEWER / EXTERNAL REVIEWER

Journals: Design, Codes and Cryptography (DCC); Journal of Cryptology (JoC); Information Sciences; IEEE Access
Conferences: EUROCRYPT 2025, 2024, 2023; PQCrypto 2023; ASIACRYPT 2022, 2021; FHE.org 2022; ANTS 2020

[Last update: 2025-05-01]