Jai Hyun PARK

jaihyunp@gmail.com https://jaihyun.com/ Lyon, France

Overview

I develop scalable privacy-enhancing technologies, primarily focusing on high-performance FHE and protocols for secure, large-scale data analysis.

Highlights

- Consistently published in top-tier cryptography venues, including **CRYPTO**, **EUROCRYPT** (including 1 single-authored paper), and **Journal of Cryptology**.
- Pioneered high-performance FHE algorithms; achieved a breakthrough in encrypted matrix multiplication, reducing the performance gap to cleartext matrix multiplication within a small constant factor.
- Leading practical FHE deployments as a Senior Researcher at CryptoLab, specifically for large-scale applications such as **Llama inference** and **Threshold ML-DSA**.
- Contributed to the academic community through teaching at **ENS de Lyon**, delivering **invited talks**, and serving as a reviewer for CRYPTO, EUROCRYPT, STOC, TCC, etc.

Research Interests

- **Fully Homomorphic Encryption (FHE)**
  - *Fast FHE*: Pioneered fast encrypted linear algebra [C05, C06, J05], advanced ring packing [C03], batch bootstrapping [C05], and non-polynomial function evaluation [J03, J04].
  - *Lightweight FHE*: Reduced communication costs for FHE ciphertexts [C03] and public keys [C07].
  - *Threshold FHE*: Developed distributed key generation (DKG) protocols for threshold FHE systems [M03].
- **Privacy-Preserving Applications**
  - On secure language models [M04, C02], private bioinformatic analysis [J01], and encrypted cluster analysis [C01].
- **Post-Quantum and Lattice-based Cryptography**
  - Introduced efficient threshold ML-DSA [M05].

Education

Seoul National University — *Seoul, Korea*

- **Ph.D. in Mathematical Sciences** — Mar 2020 – Aug 2024
  - **Research Focus:** Cryptography (homomorphic encryption)
  - **Thesis:** Matrix Multiplication on Encrypted Data
  - **Advisor:** Prof. Jung Hee Cheon
- **B.S. in Mathematical Sciences** — Mar 2013 – Feb 2020
  - **Undergraduate Research Intern:** SNU Crypto Lab (Jul 2018 – Jan 2020)
    - Research on [C01, J02].
  - Fulfilled two years of mandatory military duty in Republic of Korea Army (Jul 2016 – Apr 2018)

Employment

CryptoLab Inc. — *France & Korea*

- **Senior Researcher**, *Lyon, France* — Jan 2026 – Present
  - Promoted to Senior Researcher in recognition of contributions to FHE optimization.
- **Junior Researcher**, *Lyon, France* — Sep 2024 – Jan 2026
  - Full-time research (CDI) on efficiency of fully homomorphic encryption (FHE).
  - Authored papers including [C06, C07, J04, J05, M03].
- **PhD Research Intern**, *Lyon, France & Seoul, Korea*
  - Lyon (Jan – Mar, 2024): Presented at CRYPTO 2024 for [C05] based on intern research.
  - Seoul (Jan – Feb, 2023): Presented at CRYPTO 2023 for [C03] based on intern research.

Selected Publications

C=Conference, J=Journal, M=Manuscript

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.

[M05] THED: Threshold Dilithium from FHE
Jai Hyun Park, Alain Passelègue, Damien Stehlé
Available at https://eprint.iacr.org/2026/638

As the migration to post-quantum (PQ) cryptography accelerates, protecting sensitive signing keys through threshold schemes has become a critical necessity. This paper proposes THED, an interaction-efficient threshold ML-DSA (NIST standard) framework leveraging FHE. In this work, I designed the underlying FHE algorithms, including an improved threshold decryption protocol, and led the full-scale implementation using CryptoLab's high-performance library.

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

Matrix multiplication on encrypted data (CCMM) is traditionally considered to be several orders of magnitude slower than cleartext operations. This paper makes large-scale CCMM as fast as cleartext multiplication up to a small constant factor, by reducing CCMM into a series of cleartext matrix operations. As the sole author, I proposed and implemented all the underlying algorithms. This work has been accepted to EUROCRYPT 2025, and a portion is featured in my Ph.D. thesis.

[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

Both plaintext-ciphertext matrix multiplication (PCMM) and bootstrapping have traditionally been the primary bottlenecks in high-throughput FHE computations. This work addresses both challenges, particularly achieving PCMM algorithms that are nearly as fast as cleartext matrix multiplication, within a small constant factor. In this work, I proposed and implemented all the PCMM algorithms. I presented this research at CRYPTO 2024, and the linear algebra components are included in my Ph.D. thesis.

Other Selected Publications:

[J05] Fast Homomorphic Linear Algebra with BLAS
Youngjin Bae, Jung Hee Cheon, Guillaume Hanrot, Jai Hyun Park †, Damien Stehlé
Journal of Cryptology 2026

[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

[J03] Efficient Homomorphic Evaluation on Large Intervals
Jung Hee Cheon, Wootae Kim, Jai Hyun Park †
TIFS 2022

Honors & Awards

- **Korea Cryptography Contest**
  National Security Research Institute
  - Special Prize for [C07] — *Nov 2024*
  - Best Award for [C03]; Special Prize for [M02] — *Oct 2023*
  - Encouragement Prize for [M01] — *Oct 2022*
  - Excellence Award for [J03] — *Oct 2020*
- **BK 21+ Scholarship** — *Mar 2020 – Aug 2023*
  Ministry of Education of Korea
- **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
- **The Presidential Science Scholarship** — *Mar 2013 – Feb 2019*
  Korea Student Aid Foundation

Teaching

- **ENS de Lyon**
  - Privacy-preserving Machine Learning with Homomorphic Encryption (M2) — *Fall 2025*
    - *Co-instructor with Guillaume Hanrot.*
  - Fully Homomorphic Encryption (M2) — *Fall 2024*
    - *Co-instructor with Alain Passelègue and Damien Stehlé.*

- **FHE School** — Jan 2025
  Organized by Seoul National University and CryptoLab
  - Delivered 9 invited lectures on fully homomorphic encryption over a 3-week program.

- **Seoul National University (TA)**
  - Computational Number Theory — *Spring 2023*
  - Number Theory — *Spring 2021*
  - Differential and Integral Calculus — *Spring 2020 – Spring 2023*

Selected Talks

- **Threshold Dilithium** [M05]
  - Invited talk at Seoul National University, Korea — *Feb 2026*

- **Ciphertext-Ciphertext Matrix Multiplication: Fast for Large Matrices** [C06]
  - Invited talk at NTNU, Norway — *Nov 2025*
  - Invited Talk at FHE.org, Virtual — *Jun 2025*
  - **EUROCRYPT 2025**, Madrid, Spain — *May 2025*
  - Invited talk at Seoul National University, Virtual — *Feb 2025*

- **Plaintext-Ciphertext Matrix Multiplication and FHE Bootstrapping: Fast and Fused** [C05]
  - 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** [C03]
  - 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** [J04]
  - 2022 KMS Spring Meeting, Virtual — *Apr 2022*

- **Efficient Homomorphic Evaluation on Large Intervals** [J03]
  - 2020 KMS Fall Meeting, Virtual — *Oct 2020*

- **Towards a Practical Cluster Analysis over Encrypted Data** [C01]
  - 2019 KMS Fall Meeting, Hong-ik University, Korea — *Oct 2019*
  - **SAC 2019**, University of Waterloo, Canada — *Aug 2019*

Research 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** — Apr 2020 – Dec 2023
  Supported by the IITP Grant through the Korean Government

Patents

[P02] Electronic device for searching encrypted data and methods thereof
Jung Hee Cheon, Hyeongmin Choe, Jai Hyun Park
US 12367404, granted

[P01] Apparatus for Processing Non-polynomial Operation on Homomorphic Encrypted Messages and Methods Thereof
Jung Hee Cheon, Wootae Kim, Jai Hyun Park
KR 10-2304992, US 11757618, JP 7449911, CN 115208548, granted

Academic Service

- **Journal Reviewer:** Journal of Cryptology (JoC); Design, Codes and Cryptography (DCC); Information Sciences; IEEE Access
- **Conference External Reviwer:** CRYPTO 2026; EUROCRYPT 2026, 2025, 2024, 2023; STOC 2026; ASIACRYPT 2025, 2022, 2021; TCC 2025; PQCrypto 2023; FHE.org 2022; ANTS 2020

Publications (Full List)

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.

Conferences

[C07] Towards Lightweight CKKS: On Client Cost Efficiency
Jung Hee Cheon, Minsik Kang, Jai Hyun Park
ASIACCS 2026

[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 (short) 2022

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

Journals

[J05] Fast Homomorphic Linear Algebra with BLAS
Youngjin Bae, Jung Hee Cheon, Guillaume Hanrot, Jai Hyun Park †, Damien Stehlé
Journal of Cryptology 2026

[J04] Tree-based Lookup Table on Batched Encrypted Queries using Homomorphic Encryption
Jung Hee Cheon, Hyeongmin Choe, Jai Hyun Park †
Journal of the Korea Mathematical Society 2025

[J03] Efficient Homomorphic Evaluation on Large Intervals
Jung Hee Cheon, Wootae Kim, Jai Hyun Park †
TIFS 2022

[J02] Efficient verifiable computation over quotient polynomial rings
Jai Hyun Park*, Jung Hee Cheon, Dongwoo Kim †
International Journal of Information Security 2022

[J01] 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

Preprints

[M05] THED: Threshold Dilithium from FHE
Jai Hyun Park, Alain Passelègue, Damien Stehlé
Available at https://eprint.iacr.org/2026/638

[M04] Scaling up Privacy-Preserving ML: A CKKS Implementation of Llama-2-7B
Jaiyoung Park*, Sejin Park, Jai Hyun Park, Jung Ho Ahn, Jung Hee Cheon, Guillaume Hanrot, Jung Woo Kim, Minje Park, Damien Stehlé
Available at https://arxiv.org/abs/2601.18511

[M03] Distributed Key Generation for Efficient Threshold-CKKS
Seonhong Min*, Guillaume Hanrot, Jai Hyun Park, Alain Passelègue, Damien Stehlé
Available at https://eprint.iacr.org/2025/2057

[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

[Last update: 2026–04–30]