Keewoo Lee

✉ keewoole@gmail.com 🌐 https://keewoolee.github.io

OVERVIEW

I am a cryptography researcher in the Privacy Cluster at the Ethereum Foundation. Previously, I was a postdoctoral researcher at UC Berkeley, hosted by Prof. Sanjam Garg. I obtained my Ph.D. in Mathematical Sciences at Seoul National University, advised by Prof. Jung Hee Cheon. I am broadly interested in cryptography from theory to practice. Currently, my research focus is on cryptographic primitives for secure computation (e.g., homomorphic encryption, secure multiparty computation, zero-knowledge proof) and their applications (e.g., private database query), with emphasis on privacy in the Ethereum ecosystem.

EMPLOYMENT

Ethereum Foundation, Remote

- Scientific Advisor (Full-time) Dec 2025 – Present
  - Privacy Stewards of Ethereum (PSE) Team
- Scientific Advisor (Part-time) Feb 2025 – Nov 2025
  - Privacy Stewards of Ethereum (PSE) Team

University of California, Berkeley, United States

- Postdoctoral Researcher Nov 2023 – Nov 2025
  - Host: Prof. Sanjam Garg

CryptoLab Inc., Republic of Korea

- Research Scientist (Freelancer), HealthcareAI Division Sep 2023 – Oct 2023
  - Focus: Privacy-preserving Machine Learning on Biomedical Data

EDUCATION

Seoul National University, Republic of Korea

- Ph.D. in Mathematical Sciences Sep 2017 – Aug 2023
  - Advisor: Prof. Jung Hee Cheon
  - Focus: Cryptography (Homomorphic Encryption, Secure Multiparty Computation, Lattice-based Cryptography)
  - Thesis: “A Study on Homomorphic Packing: Definitions, Constructions, and Limitations”
- B.S. in Mathematical Sciences Mar 2014 – Aug 2017

PUBLICATIONS

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

CONFERENCE & JOURNAL

[C18] K. Lee, Yongdong Yeo, “SophOMR: Improved Oblivious Message Retrieval from SIMD-Aware Homomorphic Compression,” *USENIX Security Symposium (USENIX Security 2026)*

[C17] *Mayank Rathee, K. Lee, Raluca Ada Popa, “Verifiable PIR with Small Client Storage,” *IEEE Symposium on Security and Privacy (S&P 2026)*

[C16] *Grant Bosworth, K. Lee, Sunwoong Kim, “Leveraging FPGAs for Homomorphic Matrix-Vector Multiplication in Oblivious Message Retrieval,” *Asilomar Conference on Signals, Systems, and Computers (ACSSC 2025)*

[C15] Leo de Castro, K. Lee, “VeriSimplePIR: Verifiability in SimplePIR at No Online Cost for Honest Servers,” *USENIX Security Symposium (USENIX Security 2024)*

[C14] K. Lee, “Bit Security as Cost to Demonstrate Advantage,” *Communications in Cryptology (IACR CiC)*, 2024

- Best Award, National Cryptography Contest 2022

[C13] *Seoyoung Ko, K. Lee, Hyunhum Cho, Yoonjae Hwang, Huisu Jang, “Asynchronous Federated Learning with Directed Acyclic Graph-based Blockchain in Edge Computing: Overview, Design, and Challenges,” *Expert Systems with Applications*, 2023

[C12] Jung Hee Cheon, K. Lee, “Limits of Polynomial Packings for $\mathbb{Z}_{p^k}$ and $\mathbb{F}_{p^k}$,” *Annual International Conference on the Theory and Applications of Cryptographic Techniques (Eurocrypt 2022)*

- Best Award, National Cryptography Contest 2021

[C11] Jung Hee Cheon, Dongwoo Kim, Duhyeong Kim, K. Lee, “On the Scaled Inverse of $(x^i - x^j)$ modulo Cyclotomic Polynomial of the form $\Phi_{p^s}(x)$ or $\Phi_{p^s q^t}(x)$,” *Journal of the Korean Mathematical Society*, 2022

[C10] *Michael Cho, K. Lee, Sunwoong Kim, "HELPSE: Homomorphic Encryption-based Lightweight Password Strength Estimation in a Virtual Keyboard System," *Great Lakes Symposium on VLSI (GLSVLSI 2022)*

[C09] Jung Hee Cheon, Dongwoo Kim, K. Lee, "MHz2k: MPC from HE over $\mathbb{Z}_{2^k}$ with New Packing, Simpler Reshare, and Better ZKP," *Annual International Cryptology Conference (Crypto 2021)*

- Excellence Award, National Cryptography Contest 2020

[C08] *Wonkyung Jung, Eojin Lee, Sangpyo Kim, K. Lee, Namhoon Kim, Chohong Min, Jung Hee Cheon, Jung Ho Ahn, "Accelerating Fully Homomorphic Encryption Through Architecture-Centric Analysis and Optimization," *IEEE Access*, 2021

[C07] *Sunwoong Kim, K. Lee, Wonhee Cho, Yujin Nam, Jung Hee Cheon, Rob A. Rutenbar, "Hardware Architecture of a Number Theoretic Transform for a Bootstrappable RNS-based Homomorphic Encryption Scheme," *2020 IEEE 28th Annual International Symposium on Field-Programmable Custom Computing Machines (FCCM 2020)*

[C06] Jung Hee Cheon, Dongwoo Kim, Duhyeong Kim, Hun Hee Lee, K. Lee, "Numerical Methods for Comparison on Homomorphically Encrypted Numbers," *International Conference on the Theory and Applications of Cryptology and Information Security (Asiacrypt 2019)*

- Invited to *Journal of Cryptology* (Top 3 of 71 accepted papers among 307 submissions)

[C05] *Sunwoong Kim, K. Lee, Wonhee Cho, Jung Hee Cheon, Rob A. Rutenbar, "FPGA-based Accelerators of Fully Pipelined Modular Multipliers for Homomorphic Encryption," *2019 International Conference on ReConFigurable Computing and FPGAs (ReConFig 2019)*

[C04] *Sungjoon Park, Minsu Kim, Seokjun Seo, Seungwan Hong, Kyoohyung Han, K. Lee, Jung Hee Cheon, Sun Kim, "A Secure SNP Panel Scheme using Homomorphically Encrypted K-mers without SNP Calling on the User Side," *BMC Genomics*, 2019

[C03] Jung Hee Cheon, Haejin Cho, Jaewook Jung, Joohee Lee, K. Lee, "Efficient Identity-Based Encryption from LWR," *Annual International Conference on Information Security and Cryptology (ICISC 2019)*

[C02] *Andrey Kim, Yongsoo Song, Miran Kim, K. Lee, Jung Hee Cheon, "Logistic Regression Model Training based on the Approximate Homomorphic Encryption," *BMC Medical Genomics*, 2018

- First Place Prize, iDASH Genomic Data Privacy and Security Protection Competition 2017

[C01] Jung Hee Cheon, Jinhyuck Jeong, Joohee Lee, K. Lee, "Privacy-preserving Computations of Predictive Medical Models with Minimax Approximation and Non-adjacent Form," *International Conference on Financial Cryptography and Data Security (WAHC 2017)*

- Excellence Award, National Cryptography Contest 2016

BOOK CHAPTERS

[B01] Laia Amorós, Syed Mahbub Hafiz, K. Lee, M. Caner Tol, "Gimme That Model!: A Trusted ML Model Trading Protocol," In *Protecting Privacy through Homomorphic Encryption*, 2021

PREPRINTS

[P04] Jaiden Fairoze, Sanjam Garg, K. Lee, Mingyuan Wang, "Bypassing Prompt Guards in Production with Controlled-Release Prompting," https://arxiv.org/abs/2510.01529

[P03] K. Lee, "Barely Doubly-Efficient SimplePIR," https://eprint.iacr.org/2025/1305

[P02] Leo de Castro, Duhyeong Kim, Miran Kim, K. Lee, Seonhong Min, Yongsoo Song, "More Efficient Lattice-based OLE from Circuit-private Linear HE with Linear Overhead," https://eprint.iacr.org/2024/1534

[P01] Jung Hee Cheon, K. Lee, Jai Hyun Park, Yongdong Yeo, "Private Database Query with SIMD-Aware Homomorphic Compression," https://arxiv.org/abs/2408.17063

HONORS & AWARDS

- Sejong Science Fellowship — 2024–2025
  National Research Foundation of Korea
  ≈$50,000/year
- Doctoral Dissertation Award — Apr 2024
  Korean Mathematical Society
  - Best Award ($1,000)

"A Study on Homomorphic Packing: Definitions, Constructions, and Limitations"

- Doctoral Dissertation Award — Aug 2023
  College of Natural Sciences, Seoul National University
  - Best Award ($2,000)
    "A Study on Homomorphic Packing: Definitions, Constructions, and Limitations"
- Global PhD Fellowship — 2018–2023
  National Research Foundation of Korea
  Full Tuition and ≈$15,000/year
  - Award for Top 10% of Global PhD Fellowship ($4,000) — May 2022
  - Award for Top 10% of Global PhD Fellowship ($4,000) — Mar 2020
- National Cryptography Contest
  National Security Research Institute
  - Best Award ($3,000) — Oct 2022
    "Bit Security as Cost to Observe Advantage"
  - Best Award ($3,000) — Oct 2021
    "Limits of Polynomial Packings for $\mathbb{Z}_{p^k}$ and $\mathbb{F}_{p^k}$"
  - Excellence Award ($2,000) — Oct 2020
    "MHz2k: MPC from HE over $\mathbb{Z}_{2^k}$"
  - Excellence Award ($1,500) — Nov 2017
    Problem-solving Track
  - Excellence Award ($1,500) — Nov 2016
    "Privacy-Preserving Computation of Predictive Medical Models with Minimax Approximation"
- Best Paper Runner-up, Asiacrypt 2019 — Dec 2019
  International Association for Cryptologic Research
  "Numerical Methods for Comparison on Homomorphically Encrypted Numbers"
  Invited to *Journal of Cryptology* (Top 3 of 71 accepted papers among 307 submissions)
- First Place Prize, iDASH Genomic Data Privacy and Security Protection Competition — Oct 2017
  Track 3: Homomorphic Encryption (HME) based Logistic Regression Model Learning

INVITED TALKS

- Oblivious Compression for Homomorphic Encryption and Its Applications — Feb 2025
  EIMS-KMS International Workshop on Cryptography, Virtual
- Homomorphic Encryption: An Introduction to Secure Computation — Nov 2024
  ESL GCI Seminar Series @ Rochester Institute of Technology, New York, USA
- On the Bit Security of Cryptographic Primitives — Oct 2022
  2022 Korean Mathematical Society International Conference, Seoul, Korea
  Invited Speaker of Focus Session on "Discrete Mathematics and Mathematics of Computer Science"
- Introduction to Secure Computation — Mar 2022
  BK21 Colloquium (Rookies Pitch) @ Seoul National University, Seoul, Korea
  Invited as an Outstanding Graduate Student of Math@SNU

PRESENTATIONS

- Privacy & Scaling Explorations at Ethereum Foundation — May 2025
  Silicon Valley Private AI Forum (K-PAI), Santa Clara, CA
- Oblivious Message Retrieval for ZCash — Jul 2024
  MPC & FHE Primer @ EDCON2024, Tokyo, Japan
- VeriSimplePIR: Verifiability in SimplePIR at No Online Cost for Honest Servers — Apr 2024
  Bay Area Crypto Day
- Homomorphic Packing: Constructions and Lower Bounds — Feb 2023
  UC Berkeley Cryptography Seminar, Virtual
- Limits of Polynomial Packings for $\mathbb{Z}_{p^k}$ and $\mathbb{F}_{p^k}$
  Eurocrypt 2022, Trondheim, Norway — May 2022
  2022 Korean Mathematical Society Spring Meeting, Virtual — Apr 2022
- MHz2k: MPC from HE over $\mathbb{Z}_{2^k}$ with New Packing, Simpler Reshare, and Better ZKP
  Crypto 2021, Virtual — Aug 2021
  2020 Korean Mathematical Society Fall Meeting, Virtual — Oct 2020
- Microsoft Private AI Bootcamp — Jul 2020
  2020 Korean Mathematical Society Spring Meeting, Virtual

- Numerical Methods for Comparison on Homomorphically Encrypted Numbers — Apr 2019
  2019 Korean Mathematical Society Spring Meeting
- Privacy-preserving Predictive Models with Minimax Approx. and Non-adjacent Form — Apr 2017
  WAHC 2017, Sliema, Malta

EXPERIENCES

- Visiting Student (Prof. Vinod Vaikuntanathan) — Oct 2022–Dec 2022
  MIT, Boston, Massachusetts, USA
- Private AI Bootcamp — Dec 2019
  Team Project: *Ensuring Trust when Trading ML Models*
  Microsoft Research, Redmond, Washington, USA

SERVICES

- Program Committee
  Asiacrypt (2025), S&P (2026), ISC (2025)
- Editorial Board
  IACR CiC (2025)
- Reviewer (Conferences)
  Crypto (2024, 2025), Eurocrypt (2025, 2026), Asiacrypt (2019, 2021, 2022, 2023, 2024), TCC (2024), PKC (2019), AsiaCCS (2023), CT-RSA (2019, 2020), PQCrypto (2020, 2023, 2024), ANTS (2020), FHE.org Workshop (2022), Mathcrypt Workshop (2023)
- Reviewer (Journals)
  Journal of Cryptology (JoC), Transactions on Dependable and Secure Computing (TDSC), Transactions on Information Theory (TIT), Designs, Codes and Cryptography (DCC)