

Keewoo Lee

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

OVERVIEW

I am a postdoctoral researcher studying cryptography 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) and their applications (e.g., privacy-preserving machine learning).

EMPLOYMENT

University of California, Berkeley, United States

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

CryptoLab Inc., Seoul, Republic of Korea

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

EDUCATION

Seoul National University, Seoul, 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 Crypto)
 - 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.

CONFERENCES

- [C09] Leo de Castro, K. Lee, “VeriSimplePIR: Verifiability in SimplePIR at No Online Cost for Honest Servers,” *USENIX Security Symposium (USENIX Security 2024)*
- [C08] 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
- [C07] *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)*
- [C06] Jung Hee Cheon, Dongwoo Kim, K. Lee, “MH2k: 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
- [C05] *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)*
- [C04] 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)
- [C03] *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)*
- [C02] 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)*

- [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

JOURNALS

- [J06] K. Lee, “Bit Security as Cost to Demonstrate Advantage,” *Communications in Cryptology (IACR CiC)*, 2024
- Best Award, National Cryptography Contest 2022
- [J05] *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
- [J04] 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
- [J03] *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
- [J02] *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
- [J01] *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

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

MANUSCRIPTS

- [M02] Jung Hee Cheon, K. Lee, Jai Hyun Park, Yongdong Yeo, “Private Database Query with SIMD-Aware Homomorphic Compression,” 2023
- Special Prize, National Cryptography Contest 2023
- [M01] Jung Hee Cheon, K. Lee, Jaehyun Nam, “Privacy-preserving Median Selection and Secure Aggregation in Federated Learning,” 2021
- Special Prize, National Cryptography Contest 2021

HONORS & AWARDS

- Doctoral Dissertation Award
Korean Mathematical Society
Apr 2024
 - Best Award (\$1000)
“A Study on Homomorphic Packing: Definitions, Constructions, and Limitations”
- Doctoral Dissertation Award
College of Natural Sciences, Seoul National University
Aug 2023
 - Best Award (\$2000)
“A Study on Homomorphic Packing: Definitions, Constructions, and Limitations”
- Global PhD Fellowship
National Research Foundation of Korea
Full Tuition and \$20000/year
2018–2023
 - Award for Top 10% of Global PhD Fellowship (\$4000)
May 2022
 - Award for Top 10% of Global PhD Fellowship (\$4000)
Mar 2020
- National Cryptography Contest
National Security Research Institute
 - Special Prize (\$1000)
“Private Database Query with SIMD-Aware Homomorphic Compression”
Oct 2023
 - Best Award (\$3000)
“Bit Security as Cost to Observe Advantage”
Oct 2022

	<ul style="list-style-type: none"> • Best Award (\$3000) “Limits of Polynomial Packings for \mathbb{Z}_{p^k} and \mathbb{F}_{p^k}” 	Oct 2021
	<ul style="list-style-type: none"> • Special Prize (\$1000) “Privacy-preserving Median Selection and Secure Aggregation on Federated Learning” 	Oct 2021
	<ul style="list-style-type: none"> • Excellence Award (\$2000) “MHZ2k: MPC from HE over \mathbb{Z}_{2^k}” 	Oct 2020
	<ul style="list-style-type: none"> • Excellence Award (\$1500) Problem-solving Track 	Nov 2017
	<ul style="list-style-type: none"> • Excellence Award (\$1500) “Privacy-Preserving Computation of Predictive Medical Models with Minimax Approximation” 	Nov 2016
	<ul style="list-style-type: none"> ▪ Best Paper Runner-up, Asiacrypt 2019 International Association for Cryptologic Research “Numerical Methods for Comparison on Homomorphically Encrypted Numbers” Invited to <i>Journal of Cryptology</i> (Top 3 of 71 accepted papers among 307 submissions) 	Dec 2019
	<ul style="list-style-type: none"> ▪ First Place Prize, iDASH Genomic Data Privacy and Security Protection Competition Track 3: Homomorphic Encryption (HME) based Logistic Regression Model Learning 	Oct 2017
INVITED TALKS	<ul style="list-style-type: none"> ▪ On the Bit Security of Cryptographic Primitives 2022 Korean Mathematical Society International Conference, Seoul, Korea Invited Speaker of Focus Session on “Discrete Mathematics and Mathematics of Computer Science” 	Oct 2022
	<ul style="list-style-type: none"> ▪ Introduction to Secure Computation BK21 Colloquium (Rookies Pitch) @ Seoul National University, Seoul, Korea Invited as an Outstanding Graduate Student of Math@SNU 	Mar 2022
PRESENTATIONS	<ul style="list-style-type: none"> ▪ VeriSimplePIR: Verifiability in SimplePIR at No Online Cost for Honest Servers Bay Area Crypto Day 	Apr 2024
	<ul style="list-style-type: none"> ▪ Limits of Polynomial Packings for \mathbb{Z}_{p^k} and \mathbb{F}_{p^k} Eurocrypt 2022, Trondheim, Norway 	May 2022
	<ul style="list-style-type: none"> ▪ MHZ2k: MPC from HE over \mathbb{Z}_{2^k} with New Packing, Simpler Reshare, and Better ZKP Crypto 2021, Virtual 	Aug 2021
	<ul style="list-style-type: none"> ▪ Microsoft Private AI Bootcamp 2020 Korean Mathematical Society Spring Meeting, Virtual 	Oct 2020
	<ul style="list-style-type: none"> ▪ Microsoft Private AI Bootcamp 2020 Korean Mathematical Society Spring Meeting, Virtual 	Jul 2020
	<ul style="list-style-type: none"> ▪ Numerical Methods for Comparison on Homomorphically Encrypted Numbers 2019 Korean Mathematical Society Spring Meeting 	Apr 2019
	<ul style="list-style-type: none"> ▪ Privacy-preserving Predictive Models with Minimax Approx. and Non-adjacent Form WAHC 2017, Sliema, Malta 	Apr 2017
EXPERIENCES	<ul style="list-style-type: none"> ▪ Visiting Student (Prof. Vinod Vaikuntanathan) MIT, Boston, Massachusetts, USA 	Oct 2022–Dec 2022
	<ul style="list-style-type: none"> ▪ Research Intern On privacy-preserving machine learning Microsoft Research, Redmond, Washington, USA 	Cancelled due to COVID-19
	<ul style="list-style-type: none"> ▪ Private AI Bootcamp Team Project: <i>Ensuring Trust when Trading ML Models</i> Microsoft Research, Redmond, Washington, USA 	Dec 2019
SERVICES	<ul style="list-style-type: none"> ▪ Reviewer (Conferences) Crypto (2024), Asiacrypt (2019, 2021, 2022, 2023), PKC (2019), AsiaCCS (2023), CT-RSA (2019, 2020), PQCrypto (2020, 2023, 2024), ANTS (2020), FHE.org Workshop (2022), Mathcrypt Workshop (2023) 	
	<ul style="list-style-type: none"> ▪ Reviewer (Journals) Journal of Cryptology (JoC), Transactions on Dependable and Secure Computing (TDSC), Designs, Codes and Cryptography (DCC) 	

[Last update : 2024-04-06]