Kevin Nam (남기빈)

Seoul, South Korea | rallyk3vin@gmail.com | +82 10 2443 7250 | rallykevin.github.io
github.com/SNUSOR-PECT

Contents

Research Summary

My research path began with hardware security, including monitoring mechanisms and Trusted Execution Environments (TEE), and has since expanded to privacy-enhancing technologies (PETs). In particular, my recent works are focused on enabling efficient and accurate Machine Learning as a Service over Fully Homomorphic Encryption (FHE).

My research vision is to ***design efficient Security and Privacy Enhancing Computing Systems***. While PETs have achieved significant theoretical and mathematical progress, they are still far from widespread deployment due to their inherent limitations such as high computational complexity. To make them acceptable, I seek wisdom in not only mathematical optimizations, but in efficient implementation -— algorithm–system co-design & optimizations and integration with system security measurements–to mitigate the performance bottlenecks of domain-specific security and privacy-preserving solutions. Ultimately, my goal is to make privacy-preserving computation as conventional and accessible as everyday computing.

Research Interests

- Applied Cryptography
- Systems for PETs & Cryptography
- HW/SW Security (including confidential computing)
- Security/Privacy for AI Services
- Platform Specific Security/Privacy (e.g., V2X)
- AI for Security (e.g., AVR)

Education

Seoul National University, MS/Ph.D in Electrical and Computer Engineering — Mar 2020 – Feb 2026 (expected)

Advisor : Prof. Yunheung Paek
Dissertation Title (tentative) : Optimizations for Fast and Precise Privacy-Preserving Machine Learning as a Service over Encrypted Data

Seoul National University, BS in Electrical and Computer Engineering — Mar 2014 – Feb 2020

Left for military service during 2017-2019

Experience

Seoul National University. Seoul, Korea — Mar 2020 – Feb 2026*

Research Assistant
Advisor: Yunheung Paek

CryptoLab. Seoul, Korea — Mar 2023 – April 2024

Guest Researcher (industry–academia joint research)
Manager : Dr. Junbum Shin (Ex CTO)
Topic : Secure FHE key management mechanisms and protocols w. TEEs

Yale University. New Haven, CT, USA — Mar 2023 – Oct 2023

Research Collaborator (remote from Seoul)
Advisor: Jakub Szefer
Topic : PQC (Sphincs+) HW implementation design, side-channel attacks on FHE

Visiting Researcher (Dunham Laboratory) — Jan 2023 – Feb 2023

Advisor: Jakub Szefer
Topic : Side-channel attack resillient Post-Quantum-Cryptography algorithm design

Seoul National University. Seoul, Korea — Jun 2018 – Dec 2018

Research Intern
Advisor: Yunheung Paek
Topic : LSTM based Anomalous Branch Behavior Monitoring

Publications

Refereed Conference Publications

KIISE score refers to those from the '정보과학회 제정 2024년도 우수학술대회' list.

[1] **[ASPLOS'26]** (To Appear) "HEPIC: Private Inference over Homomorphic Encryption with Client Intervention". *Kevin Nam, Youyeon Joo, Seungjin Ha, Hyungon Moon**, Yunheung Paek**. (** co-correspondance) In the 31st International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS'26), March 2026.*
(KIISE S, BK21 IF: 4, CSRankings).

[2] [HiPC'25] "An Accelerator for Low-computational Overhead Privacy-Preserving GNN Inference". *Heonhui Jung*, Whoiree Ha*, Kevin Nam, Youyeon Joo, Lucas Oros, and Yunheung Paek. (* co-first authors) In the 32nd IEEE International Conference on High Performance Computing, Data, and Analytics (HiPC'25), December 2025.*
(BK21 IF: 1).

[3] **[Security'25]** "SLOTHE: Lazy Approximation of Non-Arithmetic Neural Network Functions over Encrypted Data". *Kevin Nam*, Youyeon Joo*, Seungjin Ha, and Yunheung Paek. (* co-first authors) In USENIX Security Symposium (Security'25), August 2025.*
(KIISE S, BK21 IF: 3, CSRankings).

[4] **[ASPLOS'25]** "Affinity-based Optimizations for TFHE on Processing-in-DRAM". *Kevin Nam, Heonhui Jung, Hyunyoung Oh**, Yunheung Paek**. (** co-correspondance) In the 30th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS'25), April 2025.*
(KIISE S, BK21 IF: 4, CSRankings).

[5] **[Security'25]** "LOHEN: Layer-wise Optimizations for Neural Network Inferences over Encrypted Data with High Performance or Accuracy". *Kevin Nam, Youyeon Joo, Dongju Lee, Seungjin Ha, Hyunyoung Oh, Hyungon Moon**, Yunheung Paek**. (** co-correspondance) In USENIX Security Symposium (Security'25), August 2025.*
(KIISE S, BK21 IF: 3, CSRankings).

[6] **[ICCAD'22]** "Accelerating N-bit Operations over TFHE on Commodity CPU-FPGA". *Kevin Nam, Hyunyoung Oh, Hyungon Moon**, Yunheung Paek**. (** co-correspondance) In IEEE/ACM International Conference on Computer-Aided Design (ICCAD'22), November 2022.*
(KIISE A, BK21 IF: 3, CSRankings).

[7] "Area-Efficient Accelerator for the Full NTRU-KEM Algorithm". *Yongseok Lee, Kevin Nam, Youyeon Joo, Jeehwan Kim, Hyunyoung Oh, Yunheung Paek. In International Conference on Computational Science and Its Applications, Lecture Notes in Computer Science (LNCS), vol. 14106, Springer Nature Switzerland, 2023.*
(SCOPUS indexed).

Refereed Journal Publications

[8] "An Efficient Hardware/Software Co-design for FALCON on Low-End Embedded Systems". *Yongseok Lee, Jonghee Youn, Kevin Nam, Heon Hui Jung, Myunghyun Cho, Jimyung Na, Jong-Yeon Park, Seungsu Jeon, Bo Gyeong Kang, Hyunyoung Oh, Yunheung Paek. In IEEE Access, 2024.*

[9] "MeetGo: A trusted execution environment for remote applications on FPGA". *Hyunyoung Oh, Kevin Nam, Seongil Jeon, and Yeongpil Cho, Yunheung Paek. In IEEE Access, 2021.*

Refereed Poster Publications

[10] "Affinity-based Optimizations of Homomorphic Encryption Operations on Processing-in-DRAM". *Kevin Nam, Heonhui Jung, Hyunyoung Oh, and Yunheung Paek. In the 61th ACM/IEEE Design Automation Conference Work-in-Progress (DAC'24 WiP), 2024.*

[11] "Implementing Efficient, Precise N-bit Operations of TFHE on Commodity CPU-FPGA". *Kevin Nam, Youyeon Joo, Dongju Lee, Seungjin Ha, Hyunyoung Oh, Hyungon Moon, and Yunheung Paek. In the 59th ACM/IEEE Design Automation Conference Work-in-Progress (DAC'22 WiP), 2022.*

Domestic Papers *(Representative Ones)*

[12] "A Study on the TEE-based On-device Inference for Protecting Model Privacy". *Seungjin Ha, Kevin Nam, Yunheung Paek. Annual Symposium of KIPS, 2025*

[13] "A Comparative Study of CUDA Optimisation Techniques for Accelerating TFHE". *Seungjin Ha, Kevin Nam, Yunheung Paek. Annual Conference of KIPS, 2024*

[14] "Intermediate Data Guided Approximation for Fast and Accurate Encrypted Neural Networks". *Kevin Nam, Youyeon Joo,*

Seungjin Ha, Yunheung Paek. Annual Conference of KIPS, 2024.

[15] "Proxy Encryption with Trusted Execution Environments to Reduce the Communication Overhead of Cloud Services over Encrypted Data". *Youyeon Joo, Kevin Nam, Seungjin Ha, Yunheung Paek. Annual Conference of KIPS, 2024.*

[16] "Quantization of Non-Arithmetics to Optimize CNNs over TFHE". *Kevin Nam, Heonhui Jung, Dongju Lee, Yunheung Paek. Annual Symposium of KIPS, 2024.*

[17] "Side-Channel Attacks on Homomorphic Encryption and Their Mitigation Methods". *Kevin Nam, Youyeon Joo, Yunheung Paek. Annual Symposium of KIPS, 2023* **(NIPA Director Award)**

[18] "Realization of Homomorphic Encrypted Deep Learning Models". *Kevin Nam, Myunghyun Cho, Hyunjun Kim, Yunheung Paek. Annual Conference of KIPS, 2021,* **(Undang Academic Award)**

Patents

[19] "METHOD OF PROCESSING NON-ARITHMETIC FUNCTIONS FOR ARTIFICIAL NEURAL NETWORKS AND CRYPTOGRAPHIC APPARATUS USING THE SAME". *Yunheung Paek, Youyeon Joo, Kevin Nam. Oct 2025. KS Patent No. 10-2025-0147837, Applied*

[20] "METHOD FOR PROCESSING HOMOMORPHIC CIPHIERTEXT AND ELECTRONIC APPARATUS". *Yunheung Paek, Heonhui Jung, Kevin Nam, Seungjin Ha, Junbum Shin, Inkwan Yu, Sunchul Jung, Jungjoo Seo. Feb 2025. US Patent No. 19/052442, Applied*

[21] "METHOD FOR PROCESSING HOMOMORPHIC CIPHIERTEXT AND ELECTRONIC APPARATUS". *Yunheung Paek, Heonhui Jung, Kevin Nam, Seungjin Ha, Junbum Shin, Inkwan Yu, Sunchul Jung, Jungjoo Seo. Jan 2025. KR Patent No. 10-2025-0008424, Applied*

[22] "METHOD AND APPRATUS FOR COMPUTING ENCRYPTED DATA USING MULTI-HOMOMORPHIC ENCRYPTION SYSTEM". *Yunheung Paek, Kevin Nam, Youyeon Joo. Nov 2024. KR Patent No. 10-2024-0153707, Applied*

[23] "TEE ENVIRONMENT PROVIDING APPARATUS AND METHOD USING FPGA". *Yunheung Paek, Hyunyoung Oh, Kevin Nam, Yeongpil Cho. Jan 2021. KR Patent No. 10-2021-0006281, Applied*

Research Projects Involved

w. fundings, Principal Investigator : Yunheung Paek.

Copyright Protection/Management of On-Device AI *funded by MCST and KOCCA* Apr 2025 – current
- Role : Designing protocols to bind the model on the device.

Development of Automotive Security Platform *funded by NRF (RS-2024-00406121)* Apr 2024 – current
- Role : Devising a TrustZone based security SoC platform for autodrive systems

Neural Network Program to FHE Transpiler *funded by ETRI, South Korea* Oct 2023 – Nov 2023
- Role : Designing a transpiler that translates tensorflow/Pytorch programs into FHE programs

Zero-Error AI Inference over Encrypted Data *funded by NRF (RS-2023-00277326)* Sep 2023 – current
- Role : Integrating non-mathematical methods (e.g., compiler) to enhance the performance of cryptographic backends

Secure FHE Key Management System *funded by CryptoLab, South Korea* Mar 2023 – April 2024
- Role : Designing efficient TEE-based FHE key management system within SGX restrictions

FHE for Cloud-based DL *funded by the KIISC Cryptography Research* Mar 2023 – Nov 2023
- Role : Developing a framework that analyzes normal codes and suggest FHE programs with the identical functionality.

Multi-Scheme FHE based DL *funded by the KIISC Cryptography Research* Mar 2022 – Nov 2022
- Role : Developing a framework that fuses the use of FHE and TEE for multi-scheme computation.

FPGA Accelerator for CKKS *funded by CryptoLab, South Korea* Mar 2022 – Nov 2022
- Role : Analyzing the algorithm and design the overall operation mapping and pipeline for CKKS on FPGA

Design HW/SW-based Computing Base for Secure Boxes *funded by IITP (2021-0-00528)* Sep 2021 – current
- Role : Implementing HW/SW-based isolated VMs with TEEs and HE

FPGA Accelerator for TFHE *funded by the KIISC Cryptography Research* Mar 2021 – Nov 2021
- Role : Designing an FPGA-based TFHE accelerator exploiting the double parallelism of TFHE

Designing PQC Accelerators *funded by Samsung Electronics, South Korea* Sep 2020 – Sep 2024
- Role : Integrating and optimize the HW modules

FPGA-based Trusted Execution Environments *funded by NRF (2020R1A2B5B03095204)* Mar 2020 – July 2022

- Role : Implementing TEE isolation systems on FPGAs

Teaching Experience

Seoul National University (TA)

Logic Circuit Design Course, 430.201A

- Period : 2020-1, 2022-2, 2023-2, 2024-2
- Role : Developed a comprehensive set of lab materials from the ground up. Served as a primary lecturer of the lab classes and parts of the theory classes. Authored, administered, and graded midterm and final exams of the main lecture.

Data Security & Privacy, 430.658

- Period : 2024-2, 2025-2
- Role : Authored a set of lecture materials and notes on applied cryptography and confidential computing. Served as a primary lecturer, independently delivering approximately half of the course lectures throughout the semester.

Creative Design Project (Graduation Project), 430.405

- Period : from 2022-1 to current
- Role : Mentored undergraduate students on their final-year graduation projects, guiding them through the entire lifecycle from topic selection to implementation.

Honors & Awards

Excellence Paper Award, *from ACK 2024* May 2024

Award for Excellence in Teaching Assistant, *from Seoul National University* Mar 2024
Logic circuit Design Course

NIPA Director Award *from ASK 2023* May 2023

Undang Academic Award *from KIPS, Best Graduate Student Paper Award* Dec 2021

Best Paper Award *from ASK 2021* May 2021

Scholarship
BK 21+ Scholarship *by the Ministry of Education of Korea* Sep 2020 - Feb 2021
Mar 2023 - present

Services & Activities

USENIX Security Symposium 2026 *Artifact Evaluation Committee*

IEEE Symposium on Security and Privacy 2026 *Artifact Evaluation Committee*

EuroSys 2025 *Shadow Program Committee*

CES 2017 *Exihibitor (BOM Team)*

Secondary-Reviewer

IEEE Transactions on Computers 2025
IEEE Transactions on Very Large Scale Integration Systems 2024

Domestic Activities

Secondary reviewer of Korea Cryptography Forum Paper Submissions 2022, 2023

Talks & Seminars

[1] *"Zero-Error Privacy-Preserving Machine Learning as a Service" presented at Seoul National University AI Health & Care Center Symposium, December 2023*

[2] *"Fully Homomorphic Encryption based Neural Network Inference" presented at Ewha Women University, September 2022*

Skills

Languages: English, French, Korean

Programming Languages: C/C++, Python, various HDL, CUDA, JAVA, Kotlin, etc

Tools/Frameworks/APIs: Vitis, Vivado, Xcellium, Synopsys DC, Tensorflow, Pytorch, Keras, Hydra, Docker, Git, LLVM

References

Prof. Yunheung Paek (Ph.D. Advisor)
Professor, Department of Electrical and Computer Engineering
Seoul National University
Email: ypaek@snu.ac.kr
Phone: +82-10-6409-3472

Prof. Hyungon Moon
Professor, Department of Computer Science and Engineering
Ulsan National Institute of Science and Technology (UNIST)
Email: hyungon@unist.ac.kr / hyungon.moon@gmail.com

Prof. Hyunyoung Oh
Assistant Professor, Dept. of AI · Software
Gachon University
Email: hyoh@gachon.ac.kr / ongban123@gmail.com
Phone: +82-10-9755-8497

Cansu Karakuzu Aslan
Researcher, Hasso Plattner Institute
Email: cansu.karakuzu@hpi.de

Prof. Jakub Szefer
Associate Professor, Dept. of Electrical and Computer Engineering
Northwestern University
Email: jakub.szefer@northwestern.edu

Prof. Mingyu Gao
Associate Professor, Institute for Interdisciplinary Information Sciences
Tsinghua University
Email: gaomy@tsinghua.edu.cn

Dr. Junbum Shin
Executive Advisor
CryptoLab Inc.
Phone: +82-10-9985-4275