Kevin Nam

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

About Me

 I am currently pursuing a combined MS/PhD in the Security Optimization Research Lab at Seoul National University. I hold a Bachelor of Science in Electrical and Computer Engineering from the same university, with a focus on hardware/system/AI security and privacy. But my research fields are not limitied to them. Back when I was an undergraduate student, I had been deeply passionate about hardware design and computer architecture. My first research topics were naturally related to efficient system integration (including hardware designs) for high-performance domain-specific computation. My research interests have expanded since then, including security and privacy-preserving computation. My current focused research topics are homomorphic encryption, multi-party computation, and trusted execution environments. As I deepen my expertise in these areas, I remain open to exploring new challenges and interdisciplinary fields within broader scopes.

Education

Seoul National University, BS in Electrical and Computer Engineering   Mar 2014 – Feb 2020
- Left for military service for 2017-2019

Seoul National University, MS/Ph.D in Electrical and Computer Engineering   Mar 2020 – present
- MS/Ph.D Combined course (currently Ph.D candidate status)

Publications

- "Affinity-based Optimizations for TFHE on Processing-in-DRAM". (To Appear) *In the 30th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS'25), April 2025*
  <u>*Kevin Nam*</u>, *Heonhui Jung, Hyunyoung Oh, and Yunheung Paek*

- "LOHEN: Layer-wise Optimizations for Neural Network Inferences over Encrypted Data with High Performance or Accuracy". (To Appear) *In USENIX Security Symposium (Security'25), August 2025*
  <u>*Kevin Nam*</u>, *Youyeon Joo, Dongju Lee, Seungjin Ha, Hyunyoung Oh, Hyungon Moon, and Yunheung Paek*

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

- "Accelerating N-bit Operations over TFHE on Commodity CPU-FPGA". *In IEEE/ACM International Conference on Computer-Aided Design (ICCAD'22), November 2022*
  <u>*Kevin Nam*</u>, *Hyunyoung Oh, Hyungon Moon, and Yunheung Paek*

- "MeetGo: A trusted execution environment for remote applications on FPGA". *In IEEE Access, 2021*
  Hyunyoung Oh, <u>*Kevin Nam*</u>, *Seongil Jeon, and Yeongpil Cho, Yunheung Paek*

Research Experience (w. fundings)

Zero-Error Privacy-Preserving Neural Networks *funded by NRF, South Korea*   Oct 2023 – present
- Research on desining efficient and accurate neural network services over encrypted data
- Integrate non-mathematical methods (e.g., compiler) with the mathematical cryptosystems
- Currently participating as **the project leader**

Secure FHE Key Management System *funded by CryptoLab, South Korea*   Mar 2023 – April 2024
- Designed TEE-based FHE key management system
- Developed the protocol to publish and depricate keys to users specifically adapted for FHE
- Participated as the TEE software engineer

Neural Network Program to FHE Transpiler *funded by ETRI, South Korea*   Oct 2023 – Nov 2023
- Designed a transpiler that changes a tensorflow, Pytorch program to FHE programs

- Developed the FHE routines that corresponds to the kernels used in tensorflow (e.g., convolution, activations)
- **Solely participated in the whole project**

PEC Platform *funded by the National Intelligence Service, South Korea*   Mar 2022 – Nov 2023
- Designed a Privacy-Enhancing-Computation (PEC) platform that exploits the use of various privacy-preserving techniques (e.g., FHE, MPC, TEE)
- Developed a framework that transpiles a normal code into privacy-preserving one, suggesting appropriate privacy-preserving technique for each partitions
- Participated as **the project leader** (designing the dataflow of the platform/framework)

FPGA Accelerator for CKKS *funded by CryptoLab, South Korea*   Mar 2022 – Nov 2022
- Designed an FPGA-based CKKS Accelerator for its bootstrapping algorithm
- Participated as **the algorithm analyzer** - designed the overall operation mapping and pipeline

FPGA Accelerator for FHE *funded by the National Intelligence Service*   Mar 2021 – Nov 2021
- Designed an FPGA-based TFHE accelerator exploiting the double parallelism of TFHE
- Developed a methodology to find the optimal setup of parallelism considering the system's memory bandwidth
- **Solely participated in the whole project**, from algorithm analysis to system integration

Post-Quantum-Cryptography Hardware Design *funded by Samsung LSI*   Mar 2020 – Feb 2021
- Designed PQC hardware modules to be implemented in various devices (e.g., smartphones, IPTV)
- Participated as a **hardware engineer**

Honors & Awards

Undang Academic Award *from KIPS, Best Graduate Student Paper Award*	Dec 2021
NIPA Director Award *from ASK 2023*	Jun 2023
Award for Excellence in Teaching Assistant, *from Seoul National University*	Jan 2024

Logic circuit Design Course

Scholarship
BK 21+ Scholarship *by the Ministry of Education of Korea*   Mar 2020 - present
SNU graduate student scholarship *by Seoul National University*   Mar 2022 - Feb 2024

Activities

EuroSys'25 *Shadow Program Committee*   2025

Teaching (Assistant) Experience

Seoul National University
Logic Circuit Design Course   Sep 2023 - Dec 2023
Data Security & Privacy   Sep 2024 - Dec 2024

Skills

Languages: English (IBT TOEFL 108), French (mother tongue), Korean (native)

Programming Languages: C/C++, Python, HDL, JAVA

Tools/Frameworks: Vitis, Vivado, Xcellium, Synopsys DC, Tensorflow, Pytorch, Docker, Git, Linux

Privacy-Preserving Tools: MS SEAL, OpenFHE, HeaaN, TFHE-rs, OpenCheetah, and much more