YUJIN NAM

✉ yujinnam@ucsd.edu Personal Webpage Linkedin

EDUCATION

University of California, San Diego Sep. 2021 - present
Ph.D in Computer Science
Advisor: Tajana Šimunić Rosing

Seoul National University Mar. 2015 - Aug. 2020
B.S. in Electrical and Computer Engineering
GPA: 3.80/4.30 *(Cum Laude)*

RESEARCH EXPERIENCES/ PROJECTS

[DATE'25] Privacy-Preserving Federated Learning
UCSD, Yale, IBM Jun. 2023 - Sep. 2024
- Privacy-preserving federated learning framework based on FHE
- Design space exploration of FHE schemes, parameters and model parameters for communication and computational efficiency

[ePrint 2024/2012] Private Similarity Search
UCSD, Intel Labs (Summer Internship) Jun. 2023 - Sep. 2024
- Fully homomorphic encryption (FHE) based private similarity search protocol for graph-like database
- Design of FHE friendly graph data structure and graph operations

[ISLPED'23] Fully Homomorphic Encrypted Hyperdimensional Computing
UCSD Nov. 2021 - Apr. 2023
- Advisor: Tajana Šimunić Rosing
- Secure hyper-dimensional training based on fully homomorphic encryption
- Investigated fully homomorphic encryption parameters for hyper-dimensional computing training and tested training performance.

Fully Homomorphic Encryption Workload
UCSD, Intel Corp. (Summer Internship) Jun. 2022 - Sep. 2022
- Design and implementation of a private machine learning model
- HW accelerator simulation

[CyberHunt'24] Efficient Host-based Intrusion Detection System
UCSD, collaboration with UW-Madison Apr. 2023 - Present
- Efficient real-time IDS using lightweight hyperdimensional computing

[TDSC'24] Privacy-Preserving Statistical Analysis ToolKit
Crypto Lab Inc. Jul. 2019 - Apr. 2020
- Advisor: Younho Lee, Jung Hee Cheon
- Privacy-preserving statistical analyzing toolkit development using the CKKS scheme.
- Proposed efficient data arrangement in ciphertext and analyzing functions.
- Implemented the toolkit, optimized codes, and evaluated the toolkit.

[FCCM' 20] Hardware Architecture of a Number Theoretic Transform
Crypto Lab Inc. Aug. 2019 - Oct. 2019
- Advisor: Sunwoong Kim, Jung Hee Cheon
- Hardware accelerator design for NTT in the RNS-variant of the CKKS scheme.
- Generated test bench and debugged HW architecture.

PUBLICATION

1. Duhyeong Kim, **Yujin Nam**, Wen Wang, Huijing Gong, Ishwar Bhati, Rosario Cammarota, Tajana S. Rosing, Mariano Tepper, and Theodore L. Willke. GraSS: Graph-based similarity search on encrypted query. Cryptology ePrint Archive, Paper 2024/2012, 2024.
2. S. Kim, K. Lee, W. Cho, **Y. Nam**, J. H. Cheon, and R. A. Rutenbar. Hardware architecture of a number theoretic transform for a bootstrappable rns-based homomorphic encryption scheme. In *2020 IEEE 28th Annual International Symposium on Field-Programmable Custom Computing Machines (FCCM)*, pages 56–64, 2020.
3. Younho Lee, Jinyeong Seo, **Nam, Yujin**, Jiseok Chae, and Jung Hee Cheon. Heaan-stat: a privacy-preserving statistical analysis toolkit for large-scale numerical, ordinal, and categorical data. *IEEE Transactions on Dependable and Secure Computing*, pages 1–18, 2023.
4. **Nam, Yujin**, Minxuan Zhou, Saransh Gupta, Gabrielle De Micheli, Rosario Cammarota, Chris Wilkerson, Daniele Micciancio, and Tajana Rosing. Efficient machine learning on encrypted data using hyperdimensional computing. In *2023 IEEE/ACM International Symposium on Low Power Electronics and Design (ISLPED)*, pages 1–6, 2023.
5. **Yujin Nam**, Abhishek Moitra, Yeshwanth Venkatesha, Xiaofan Yu, Gabrielle De Micheli, Xuan Wang, Minxuan Zhou, Augusto Vega, Priyadarshini Panda, and Tajana Rosing. Rhychee-fl: Robust and efficient hyperdimensional federated learning with homomorphic encryption. DATE, 2025.
6. Minxuan Zhou, **Yujin Nam**, Pranav Gangwar, Weihong Xu, Arpan Dutta, Kartikeyan Subramanyam, Chris Wilkerson, Rosario Cammarota, Saransh Gupta, and Tajana Rosing. Fhemem: A processing in-memory accelerator for fully homomorphic encryption, 2023.
7. Minxuan Zhou, **Yujin Nam**, Xuan Wang, Youhak Lee, Chris Wilkerson, Raghavan Kumar, Sachin Taneja, Sanu Mathew, Rosario Cammarota, , and Tajana Rosing. Ufc: A unified accelerator for fully homomorphic encryption. In *57th IEEE/ACM Inter-national Symposium on Microarchitecture (MICRO)*, 2024.

WORK EXPERIENCES

Graduate Intern, *Intel Labs* Jun. 2023 - Sep. 2023
- Fully Homomorphic Encryption based private similarity search algorithm

Graduate Intern, *Intel Corp.* Jun. 2022 - Sep. 2022
- Fully homomorphic encryption based machine learning implementation

Researcher, *Crypto Lab Inc.* Aug. 2019 - Sep. 2020
- Software and hardware design of fully homomorphic encryption based application

Summer Intern, *Crypto Lab Inc.* Jun. 2019 - Aug. 2019

HONORS and AWARDS

National Scholarship For Science and Engineering (fully funded), Korea Student Aid Foundation 2017 - 2019
SNU Merit-Based Scholarship, SNU 2015, 2016

SKILLS

Programming Languages	C/C++, Python, Verilog, MATLAB, R
Frameworks	PyTorch
Developer Tools	Git, VS Code, Vivado

EXTRA-CURRICULAR ACTIVITIES

SNU's Tomorrow's Engineers Membership (STEM) 2017 Fall - 2019 Fall
honor society of college of engineering, SNU

Student Council of College of Engineering 2016 Spring
member of the department of human rights

Student Council of Department of Electrical and Computer Engineering 2015 Fall
member