Negar Neda

New York University, Tandon School of Engineering, Brooklyn, New York, 11201

negar@nyu.edu negarnd.github.io negarnd

Education

New York University, Tandon School of Engineering *Sep. 2021 -present*
PhD in Electrical and Computer Engineering
Thesis title: Accelerating Homomorphic Encryption Implementation

University of Tehran (UT), Tehran, Iran *Sep. 2018 - Feb. 2021*
M.Sc. in Computer Architecture
Cumulative GPA: 17.26/20 (3.63/4)
Thesis title: FPGA-based Multi-precision Accelerator for Deep Neural Networks

Amirkabir University of Technology (AUT), Tehran, Iran *Sep. 2014 - Sep. 2018*
B.Sc. in Computer Engineering, Computer Architecture Systems
Cumulative GPA: 17.2/20 (3.62/4)
Thesis title: Implementation of a Tracking System Using LoRaWAN Protocol

Research Interest

- Cybersecurity
- Privacy-preserving ML Alg.
- FPGA
- Homomorphic Encryption
- Hardware Accelerators
- Deep Neural Networks

Publications

• "CiFlow: Dataflow Analysis and Optimization of Key Switching for Homomorphic Encryption", ISPASS, N. Neda, A. Ebel, B. Reynwar, B. Reagen, 2024.

• "Quantifying the Overheads of Modular Multiplication", IEEE International Symposium on Low Power Electronics and Design (ISLPED), D. Soni, M. Nabeel, N. Neda, et al., 2023.

• "Towards fast and scalable private inference", Proceedings of the 20th ACM International Conference on Computing Frontiers, J. Mo, K. Garimella, N. Neda, A. Ebel, B. Reagen, 2023.

• "RPU: The Ring Processing Unit", IEEE International Symposium on Performance Analysis of Systems and Software (ISPASS), D. Soni*, N. Neda*, et al., 2023.

• "Multi-Precision Deep Neural Network Acceleration on FPGAs", Asia and South Pacific Design Automation Conference (ASP-DAC), N. Neda, S. Ullah, Az. Ghanbari, H. Mahdiani, M. Modarressi, A. Kumar, 2022.

Research Experience

• **Research Assistant in BAAHL Lab**, New York University. 2022 - present
- Supervised by Prof. Brandon Reagen

My research involves exploring hardware accelerators for privacy-preserving machine learning algorithms, mainly homomorphic encryption (HE). HE allows computation on encrypted data without the need to decrypt the input. However, the main challenge in HE lies in the substantial computational demands on encrypted data and the large encrypted data size compared to plaintext. This leads to a significant increase in latency and energy consumption, limiting its potential applications. Therefore, our goal is to enhance the performance of HE workloads. During the first two years of my research, I concentrated on designing a vector processor tailored for RLWE-based algorithms, which includes HE, and evaluated the performance of (i)NTT on the designed accelerator. This research was funded by **DARPA**, under the Data Protection in Virtual Environments **(DPRIVE)** program, contract HR0011-21-9-0003.

Currently my focus has shifted towards exploring TFHE, and I am planning on designing a hardware to accelerate it's implementation.

• **Research Assistant in Network on Chip Laboratory**, University of Tehran 2018 - 2021
- Supervised by Dr. Mehdi Modarressi

For my master's thesis I worked on implementing an FPGA-based Multi-precision Accelerator for Deep Neural Networks. My research was published in ASP-DAC 2022.

• **Researcher in Digital System Design Lab**, Amirkabir University of Technology 2017 - 2018
- Supervised by Dr.Mahmoud Momtazpour and Dr.Morteza Saheb Zamani

In this laboratory, we worked on the Amirkabir University of Technology IoT Gateway Project.

Teaching Experience

- **Computing Systems Architecture**, T.A. (Prof. Brandon Reagen) 2023
- **Computer Aided Digital System Design**, T.A. (Prof. Mehdi Modarressi) 2019 & 2020
- **Logic Circuit Laboratory**, Lab Instructor 2018
- **Computer Networks**, T.A. (Prof. Siavash Khorsandi) 2017
- **Digital Design Automation**, T.A. (Prof. Morteza Saheb Zamani) 2017
- **Electrical Circuit1**, T.A. (Prof. Siavash Khorsandi) 2016
- **Logic Circuits**, T.A. (Prof. Mehdi Sedighi & Prof. Mahmoud Momtazpour) 2016

HONOR & AWARDS

- Received **Travel Grant** for ISPASS conference. 2023 & 2024
- Earned **Future Leader Fellowship** at NYU Tandon. 2022-2024
- **Ranked Top 3 in terms of GPA**, among Computer Architecture Students in AUT 2019
- **Ranked top 0.6%** out of 222,500, Nationwide University Entrance Exam, Mathematics 2014

Technical skills

Programming	Python(Tensorflow, PyTorch), Rust, C/C++, Java, VHDL, Verilog, Co-Design, CUDA, OpenMP, Assembly LaTeX
Tools	Visual Studio, Qt, MATLAB, Jupyter Notebook, Arduino IDE, Git
Hardware CAD Tools	Vivado Design Suite, Xilinx ISE Design Suite, PSPICE, HSPICE, Modelsim, Proteus, Keil
Language	English (IELTS Overal Score: 7.5), Persian (Native)

Talks

- "CiFlow: Dataflow Analysis and Optimization of Key Switching for Homomorphic Encryption", ISPASS 2024
- "RPU: The Ring Processing Unit", ISPASS 2023
- "Summary of RPU: The Ring Processing Unit ", Princeton Computer Architecture day 2023
- "A Novel Vector ISA for Accelerating Homomorphic Encryption", TECHCON 2022