MEET UDESHI

NYU Tandon School of Engineering
PhD Student, ECE, CGPA: 3.958
Advisors: Prof Farshad Khorrami and Prof Ramesh Karri

+1-607-216-5524 m.udeshi@nyu.edu
mudeshi.in udiboy1209

Research Interests: embedded and cyber-physical systems security, hardware security, machine learning

PUBLICATIONS

M. Udeshi, P. Krishnamurthy, H. Pearce, R. Karri, F. Khorrami, "REMaQE: Reverse Engineering Math Equations from Executables," in ACM Transactions on Cyber-Physical Systems, 2024

M. Shao, S. Jancheska, **M. Udeshi**, B. Dolan-Gavitt, H. Xi, K. Milner, B. Chen, M. Yin, S. Garg, P. Krishnamurthy, F. Khorrami, R. Karri, M. Shafique, "NYU CTF Bench: A Scalable Open-Source Benchmark Dataset for Evaluating LLMs in Offensive Security," in Neural Information Processing Systems, 2024

M. Udeshi, P. Krishnamurthy, R. Karri, F. Khorrami, "Tamper-Proof Network Traffic Measurements on a NIC for Intrusion Detection," in IEEE Transactions on Network and Service Management, 2024

N. K. Boran, S. Rathore, **M. Udeshi**, V. Singh, "Fine-Grained Scheduling in Heterogeneous-ISA Architectures," in IEEE Computer Architecture Letters, 2020

RESEARCH AND WORK EXPERIENCE

PhD project - Reverse engineering math equations Aug'22 - Present
Control/Robotics Research Lab, Center for Cybersecurity

- Designed REMaQE, an automated framework based on **dynamic analysis** and **symbolic execution** to reverse engineer math equations from binaries
- Designed REMEND, a **neural decompilation** based static analysis framework to reverse engineer math equations from binaries

PhD project – LLM agents for cybersecurity Mar'24 - Present
Control/Robotics Research Lab, Center for Cybersecurity

- Compiled the **NYU CTF Bench,** a benchmark of **200 CTF challenges** to evaluate LLM security capabilities
- Developed the **EnIGMA agent** that achieves **13.5%** on NYU CTF Bench

Senior Engineer – Qualcomm R&D Jul'19 - Jul'22
ML Compiler Team for Cloud AI100 Accelerator

- Contributed to key aspects of AI100 compiler like multi-core, multi-thread data tiling, memory management, and graph scheduling
- Innovated various **graph optimization techniques** for computer vision models, recommendation systems and autonomous driving tasks

Master's Thesis – Hardware security Aug'18 - Jun'19
Guide: Prof. Virendra Singh, CADSL, IIT Bombay

- Designed a **prefetcher disabling attack** to amplify cache side-channel leakage
- Achieved **99%** reduction in prefetches generated by **AES program**

ACHIEVEMENTS

Awarded the **DAC Young Fellowship** to present a poster at DAC'23

Awarded the **Recognition of Outstanding Contributions** at Qualcomm

Received a **Gold Medal** in Indian National Physics Olympiad

MENTORSHIP

Mentor for a hardware security project in the Qualcomm Innovation Fellowship from Aug'20 to May'21

Teaching Assistant for Microprocessor course (EE309) and VLSI Design lab (EE705) from Aug'18 to Apr'19

Manager of Electronics Club, IIT Bombay from May'16 to May'17

Reviewer in the 46th International Physics Olympiad

SKILLS

Relevant Courses

Hardware Security & Trust
Advanced Computer Architecture
Advanced Hardware Design
Deep Learning

Programming

Embedded C/C++ ★★★★★
Python ★★★★★
Verilog/VHDL ★★★★☆

Frameworks

Angr Symbolic Exec ★★★★★
LLVM Compiler ★★★★☆

Tools

Ghidra ★★★★★
Vivado HLS ★★★★☆
Gem5 ★★★★☆