MEET UDESHI

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

NYU Tandon School of Engineering
PhD Student, ECE, CGPA: 3.965
Control/Robotics Research Lab, Center for Cybersecurity
Advisors: Prof Farshad Khorrami and Prof Ramesh Karri

Research Interests: cyber-physical systems security, hardware security, reverse engineering, LLM agents

SELECTED PUBLICATIONS

M. Udeshi, P. Krishnamurthy, H. Pearce, R. Karri, and F. Khorrami. 2024. "REMaQE: Reverse Engineering Math Equations from Executables." ACM Transactions on Cyber-Physical Systems 8, 4

M. Shao, S. Jancheska, **M. Udeshi**, B. Dolan-Gavitt, K. Milner, B. Chen, M. Yin et al. "NYU CTF Bench: A scalable open-source benchmark dataset for evaluating LLMs in offensive security." In Advances in Neural Information Processing Systems 37

T. Abramovich, **M. Udeshi**, M. Shao, K. Lieret, H. Xi, K. Milner, S. Jancheska et al. "EnIGMA: Interactive Tools Substantially Assist LM Agents in Finding Security Vulnerabilities." In International Conference on Machine Learning.

RESEARCH EXPERIENCE

Reverse Engineering Math Equations Aug'22 to Present
Control/Robotics Research Lab, Center for Cybersecurity

- Designed REMaQE: reverse engineering math equations from binary executables
- Designed REMEND: neural decompilation for math equations
- Leveraged `angr` symbolic execution and `capstone` for binary analysis
- REMaQE obtains *100% accuracy* on C and Simulink binaries
- REMEND obtains *89.8% to 92.4% accuracy* on C and Fortran binaries

LLMs for Cybersecurity Automation Mar'24 to Present
Center for Cybersecurity

- Curated NYU-CTF-Bench with 200 CTF challenges for LLM automation testing
- Developed EnIGMA with interactive debugging tools for LLMs for vulnerabilities
- Developed D-CIPHER: LLM multi-agent framework to solve CTFs
- Hosted the LLM Attack Challenge at Cybersecurity Awareness Week (CSAW)

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

- Worked on key aspects of AI100 compiler like multi-core, multi-thread data tiling, memory management, graph scheduling and operator fusion
- Innovated various **graph optimization techniques** applicable to 2D and 3D computer vision models, recommendation systems and autonomous driving tasks
- Contributed to the open-source **Pytorch Glow** compiler framework
- Deployed power efficient object tracking pipeline using **Kernelized Correlation Filters (KCF)** algorithm on AI100

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**
- Implemented confidence measurement for **Gem5** stride and DCPT prefetcher

ACHIEVEMENTS

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

Awarded the **Recognition of Outstanding Contributions (ROCStar)** for work on the AI100 compiler and KCF

Awarded **Gold Medal** in the Indian National Physics Olympiad

MENTORSHIP

Organizer for the CSAW LLM Attack Challenge '24 and '25

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

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/Capstone	★★★★★
ReAct LLM agents	★★★★★
ROS2	★★★★☆

Tools

Ghidra	★★★★★
Binary Ninja	★★★★☆
Vivado HLS	★★★★☆