NJIT

# Department of Computer Science

## Understanding and Enhancing Microarchitecture Security in the Era of AI and Emerging Hardware

**Fan Yao**
University of Central Florida

**Hosted by: Cong Shi**

**Date:** Tuesday, March 25, 2025
**Coffee:** 2:15 PM – 2:30 PM
**Time:** 2:30 PM – 3:30 PM (Eastern Time (US and Canada)
**Location:** GITC 4402 (4th floor Seminar Lecture Hall)

**Zoom Link:** https://njit-edu.zoom.us/j/95903616720?pwd=UrsFtzLWaZFP0ePgVmqLxAOES8ECNn.1

**Abstract:**

Recent developments of adversarial exploitation rooting in hardware (e.g., microarchitectural information leakage and fault attacks) have forcibly opened a new chapter for computing system security, highlighting the fact that the underlying hardware (i.e., internal threats) is at the center of future attacks and defenses. The security prospect of future computing is even more concerning with the rapid advances of artificial intelligence and machine learning (ML) techniques, which are ubiquitously integrated into our daily lives to perform many security-sensitive tasks.

In this talk, I will first present our investigations into novel attacks that exploit hardware vulnerabilities (i.e., memory fault attacks and side channels) to subvert key security primitives of state-of-the-art deep learning models. Our research for the first time reveals the feasibility of compromising ML systems (model extraction and tampering) by directly targeting model parameters (in contrast to inputs), which opens a new avenue for understanding the ML system security through the lens of hardware threats. Meanwhile, trusted execution environments (TEE) have emerged as a promising solution for trustworthy computing, offering data confidentiality and integrity protection. In my talk, I will further present our recent studies on security issues in secure processor architectures (i.e., the foundation for TEE) when considering the more practical multi-faceted attack surfaces, with the objective to provide holistic protection for data in compute/transit and at rest.

**Bio:** Dr. Fan Yao is an Associate Professor in the Department of Electrical and Computer Engineering at the University of Central Florida. His research interests lie in the areas of computer architecture and security. His recent research focuses include microarchitecture security (microarchitectural attacks and defenses), hardware security for robust and trustworthy AI systems (hardware-based model extraction and tampering), secure processor architectures and trusted computing. His works has been frequently published in top-tier conference venues in the respective field (ISCA, MICRO, HPCA, S&P, USENIX Security, CCS etc.). His research papers have been recognized several times in the Top Picks in Hardware and Embedded Security (HES). Dr. Yao is the program co-chair of ICCD 2025, TPC subcommittee chair of DAC 2025, general co-chair of SEED 2024 and artifact evaluation chair of IISWC 2023. He has been actively serving in the technical program committees and organizing committees for many leading computer architecture and security conferences. Dr. Yao is a recipient of the National Science Foundation CAREER Award.