Title: Looking Beyond Microarchitectural-Only Side Channels

Speaker: Mengjia Yan, Assistant Professor, MIT

Abstract:
Modern systems are becoming increasingly complex, exposing a large attack surface with vulnerabilities in both software and hardware. Today, it is common for security researchers to explore software and hardware vulnerabilities separately, considering these vulnerabilities in disjoint threat models. In this talk, I will discuss the importance of considering a broader threat model when studying microarchitectural side channels and looking beyond microarchitecture-only side channels. A broader threat model considers the combined effects of exploiting vulnerabilities residing in different system layers. I will use a few examples to demonstrate how a broader threat model can help advance our hardware security research in multiple ways.

Bio:
Mengjia Yan is an Assistant Professor in the EECS department at MIT. She received her Ph.D. degree from the University of Illinois at Urbana-Champaign (UIUC). Her research interest lies in the areas of computer architecture and hardware security, with a focus on microarchitectural attacks and defenses. Mengjia received the NSF CAREER Award, Intel Rising Star Faculty Award, ACM SIGARCH/IEEE CS TCCA Outstanding Dissertation Award Honorable Mention, multiple MICRO TopPicks in Computer Architecture and a MICRO best paper award.