Department of Electrical Engineering
香港城市大學
City University of Hong Kong

CityU Architecture Lab for Arithmetic and Security (CALAS) Seminar Series

ConBOOM: A Configurable CPU Microarchitecture for Speculative Execution Attack Mitigation

Candice Zhewen ZHANG, Ph.D. Candidate
Supervisor: Prof. Ray C.C. CHEUNG

Abstract:

Speculative execution attacks are serious security problems that cause information leakage in computer systems by building speculative covert channels. Hardware defenses mitigate speculative covert channels through microarchitectural changes. However, existing hardware defenses have limitations in terms of either security or performance. The limitations indicate that it is difficult to achieve better security and performance of a processor against speculative execution attacks using a single defense method. In this paper, we propose ConBOOM, a configurable central processing unit (CPU) microarchitecture that provides optimized switchable hardware defensive modes, including the high-security eager delay mode and two proposed performance-optimized modes based on the anticipated attack scenarios. Compared to the existing representative work with the fixed performance overhead of 39.1%, ConBOOM has the lower performance overhead ranging between 15.1% and 39.1% to mitigate different attack scenarios. ConBOOM provides more defensive flexibility with negligible hardware resource overhead about 2.0% and good security.

Biography:

Candice Zhewen ZHANG received the B.Eng. degree in electronics information science and technology from the School of Astronautics, Harbin Institute of Technology, Harbin, in 2020. She is currently working towards the Ph.D. degree in the Department of Electrical Engineering, City University of Hong Kong, Hong Kong, under the supervision of Prof. Ray C.C. Cheung. Her research interests include computer system, RISC-V processor designs, and hardware security.

25 Aug 2025 (Mon); 2pm - 4pm; G4302; https://cityu.zoom.us/j/96742093029