Dissertation Defense
Doctor of Philosophy in Computer Science

“Improving Performance and Space Efficiency of Secure Memory with ORAM” by Mehrnoosh Raoufi

Date: March 29, 2024
Time: 11:00 a.m. – 2:00 p.m.
Place: Room 6329, Sennott Square, 210 S Bouquet St, Pittsburgh, PA 15213

Committee:
- Dr. Youtao Zhang, Professor, Department of Computer Science, School of Computing and Information
- Dr. Xulong Tang, Assistant Professor, Department of Computer Science, School of Computing and Information
- Dr. Stephen Lee, Assistant Professor, Department of Computer Science, School of Computing and Information
- Dr. Jun Yang, Professor, Department of Electrical and Computer Engineering, Swanson School of Engineering

Abstract:
In modern computing, safeguarding user privacy has become a major challenge. Data content can be protected via encryption. However, encryption cannot hide the location of the data being accessed, hence exposing the access pattern to the adversary. Studies have shown that the access pattern can leak sensitive information about the user such as medical records, user identity, financial information, etc. In contemporary computer systems, the processor chip integrates a memory controller on-chip and transmits memory addresses and device commands in cleartext on memory buses. Therefore, even if the data is encrypted, one can snoop on the bus and untrusted off-chip memory and infer sensitive information via observing the memory address trace of a user program. ORAM (Oblivious RAM) is an expensive cryptographic technique that obfuscates access patterns. When ORAM is implemented in the processor, it converts each off-chip memory request from a user program into tens to hundreds of memory accesses. While ORAM provably hides the access pattern, thereby bringing privacy protection, from the system perspective, it incurs significant overhead. ORAM requires continuously shuffling user data in the memory. Not only does it slow down the execution of user programs, but it also imposes substantial memory space demand.

This dissertation aims to minimize ORAM overhead from different aspects by introducing various architectural techniques. The goal is to make ORAM more desirable for wide adoption, thereby enabling modern computing systems with efficient, privacy-preserving secure memory. The dissertation analyzes the most popular ORAM implementations and their latest optimizations in the literature to expose ORAM inefficiencies in terms of performance, and space demand. Then, it strives to alleviate these inefficiencies. It reduces the memory intensity of ORAM by decreasing the number of memory accesses needed per user request, thereby reducing bandwidth overhead and improving ORAM performance. It also reduces ORAM memory space demand by reclaiming invalidated memory blocks in ORAM and saving further DRAM space through the introduction of a hybrid-memory ORAM design.