University of Pittsburgh | School of Computing and Information

# Proposal Defense

***Doctor of Philosophy in Computer Science***

"**Improving Performance and Space Efficiency of Secure Memory with ORAM**" by
**Mehrnoosh Raoufi**

**Date:** May 31, 2022
**Time:** 9:00AM – 11:00AM
**Place:** https://pitt.co1.qualtrics.com/jfe/form/SV_3RiLQTsfIVUHy0m

**Committee:**

- Dr. Youtao Zhang, Professor, Department of Computer Science, School of Computing and Information
- Dr. Jun Yang, Professor, Department of Electrical and Computer Engineering, Swanson School of Engineering
- 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

**Abstract:**
Modern computer systems widely adopt the detached-memory architecture, i.e., the processor chip integrates a memory controller on-chip and sends memory addresses and device commands in cleartext on memory buses. Studies have shown that, even if the user data may be secured with strong encryption and authentication schemes, it is possible to leak sensitive information from access patterns in memory address traces. To ensure high-level protection of user privacy, it is necessary to adopt expensive ORAM (Oblivious RAM) primitive that obfuscates memory requests from the user program. ORAM converts each off-chip memory request from user program to tens to hundreds of memory accesses. While several schemes have been proposed to mitigate the total number of memory accesses. ORAM remains a highly memory intensive primitive that leads to large memory bandwidth and space occupation and performance degradation.

In this thesis, we study the most popular ORAM implementations and their latest optimizations proposed in the literature. We perform extensive analyses to expose ORAM inefficiencies in terms of bandwidth, performance and space demand. We then propose a set of techniques to address these inefficiencies. In particular, we present schemes to improve the performance of ORAM by reducing its memory intensity. Moreover, we propose to reduce the space demand of ORAM to make it more desirable for wide adoption.