

# MASTERS FINAL ORAL EXAMINATION

**Wednesday, November 2<sup>nd</sup>  
12:00p.m. @ 223 Atanasoff**

**Daolin Cheng**

**Major Professor: Wensheng Zhang**

## **Implementation of a Privacy-Preserving Cloud Storage System Based on Storage-Efficient Oblivious RAM**

Cloud-based storage services have been popular. Individual and organization users have widely adopted cloud-based storage services to enjoy the unprecedented convenience and cost-effectiveness brought by this new storage paradigm. Meanwhile, concerns about the security of the data outsourced to the cloud storage and the privacy of the users' accesses to the outsourced data have arised. Technologies such as data encryption and encrypted data protection have been proposed to secure the data. Recently, oblivious RAM (ORAM) based algorithms have been developed to protect users' privacy in accessing the data. However, the existing works on ORAM have focused on theoretical design and analysis, while very few study has been conducted on how to apply the ORAM algorithms to build practical cloud storage systems.

This creative component aims to fill this gap by implementing a cloud storage prototype system with the following features:

- (i) protecting data secrecy (through data encryption);
- (ii) protecting data access pattern privacy (through incorporating an ORAM scheme);
- (iii) providing user friendliness (through offering the major functions a state-of-the-art cloud storage system can offer, while hiding the details about how to protect data secrecy and access pattern protection);
- (iv) cost-efficiency.

**IOWA STATE UNIVERSITY**  
Department of Computer Science