**The Department of Computer Science and Engineering**

**Distinguished Speakers Series Presents**



**Michael T. Goodrich, University of California - Irvine**

**Title: Using Data-Oblivious Algorithms for Private Cloud Storage Access**

Abstract: We study data-oblivious algorithms as a natural way to model privacy-preserving data outsourcing where a client, Alice, stores sensitive data at an honest-but-curious cloud storage server, Bob. The general approach involves obscuring the access patterns to a remote storage so that the manager of that storage, Bob, cannot infer information about its contents. Previous solutions typically involve costly amortized overheads for achieving this goal and involve

potentially huge variations in access times, depending on when they occur. We show that efficient privacy-preserving data access is possible using a combination of probabilistic encryption, which directly hides data values, stateless oblivious RAM simulation, which hides the pattern of data accesses, and algorithms that are explicitly data oblivious.

Short Biography:

Speaker Bio: Prof. Goodrich received his B.A. in Mathematics and Computer Science from Calvin College in 1983 and his PhD in Computer Sciences from Purdue University in 1987. He is a Chancellor's Professor at the University of California, Irvine, where he has been a faculty member in the Department of Computer Science since 2001. In addition, he currently serves as Chair of the Department of Computer Science. Dr. Goodrich's research is directed at the design of high performance algorithms and data structures for solving large-scale

problems motivated from information assurance and security, the Internet, Bioinformatics, and geometric computing. With over 250 publications, including several widely-adopted books, his recent work includes contributions to efficient and secure distributed data structures, information privacy, social networks, and cloud security. He is an ACM Distinguished Scientist, a Fellow of the American

Association for the Advancement of Science (AAAS), a Fulbright

Scholar, a Fellow of the IEEE, and a Fellow of the ACM.

**The talk will be held in Clemens 120 from 3:30 – 4:30 pm. Refreshments are immediately following talk in 338A Davis Hall.**