

SEMINAR NOTICE:



Differentially Private Data Publication and Analysis

Yin “David” Yang

Research Scientist at the Advanced Digital
Sciences Center in Singapore

**Thursday, May 17
2:00 p.m.
CSL 368**



Abstract:

Data privacy has been an important research topic in the security, theory and database communities in the last few decades. However, many existing studies have restrictive assumptions regarding the adversary’s prior knowledge, meaning that they preserve individuals’ privacy only when the adversary has rather limited background information about the sensitive data, or only uses certain kinds of attacks. Recently, differential privacy has emerged as a new paradigm for privacy protection with very conservative assumptions about the adversary’s prior knowledge. Since its proposal, differential privacy had been gaining attention in many fields of computer science and is considered among the most promising paradigms for privacy-preserving data publication and analysis. In this talk, I will motivate its introduction as a replacement for other paradigms, present the basics of the differential privacy model from a database perspective and describe several state-of-the-art methods in differential privacy research.

Biosketch:

Yin "David" Yang is a research scientist at the Advanced Digital Sciences Center in Singapore. His research interests lie in database security and query optimization. He has published several papers in renowned venues about query authentication in outsourced databases. In addition, he has designed efficient query processing methods in various contexts, including data streams, relational keyword search, spatial databases, web portals, and wireless sensor networks. Currently, David is working on a project related to differentially private databases, led by University of Illinois at Urbana-Champaign Computer Science Professor Marianne Winslett.