NATIONAL UNIVERSITY OF SINGAPORE

School of Computing

PH.D DEFENCE - PUBLIC SEMINAR

Title: **Differentially Private Online Collaborative Recommendation Systems**

Speaker: Mr Liu Xiao

Date/Time: 21 March 2016, Monday, 09:00 AM to 10:30 AM

Venue: Executive Classroom, COM2-04-02

Supervisor : Dr Yu Haifeng, Associate Professor, School of Computing
Dr Seth Lewis Gilbert, Assistant Professor, School of Computing

Abstract:

In this seminar, we discuss the protection of privacy in collaborative recommendation system (a.k.a. collaborative filtering). Collaborative recommendation system is one of the most important types of recommendation systems, and today it is widely deployed in large websites such as Amazon, Netflix and YouTube.

Since a collaborative recommendation system works by sharing users' personal opinions on objects, a sensitive user may worry that his/her private opinions will be leaked. We adopt differential privacy as our notion of privacy and we consider an online collaborative recommendation system model.

The challenge of preserving differential privacy mainly comes from two facts: i) the system runs for a long time and it generates many recommendations, therefore the privacy leakage may accumulate; ii) the attackers may collude, and they collectively probe more information than a single attacker.

We address this challenge by two steps. In the first step, we assume that the attackers are non-colluding. We then show a lower bound on the best achievable privacy for any algorithm with non-trivial recommendation quality, and we also propose recommendation algorithms with near-optimal recommendation quality/privacy. In the second step, we consider colluding attackers in a simplified setting.

Counter-intuitively, we are able to achieve the same level of differential privacy as the case of non-colluding attackers, even if there is an unbounded number of colluding attackers. We get this strong result using a "forking" idea, and an interesting topic of future work is how this idea can be modified to protect privacy against colluding attackers in the general setting.