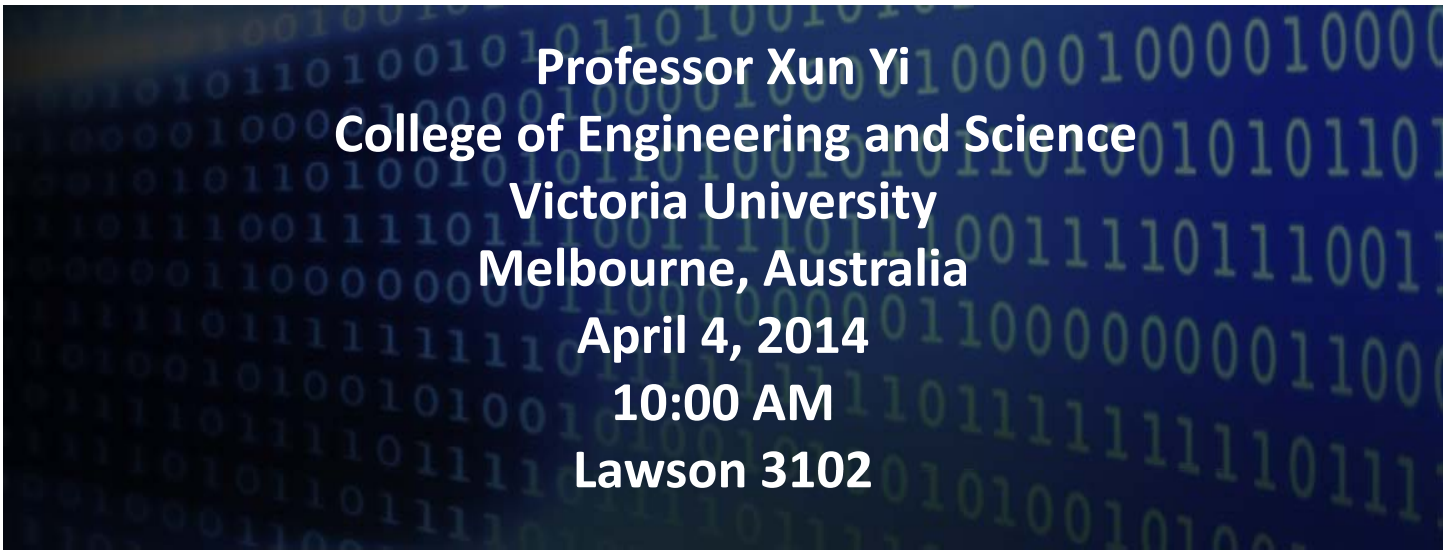
CYBER CENTER SEMINAR SERIES

Practical k Nearest Neighbor Queries with Location Privacy



Speaker Bio

Dr. Xun Yi is a professor with the College of Engineering and Science, Victoria University, Australia. His research interests include database security, computer and network security, mobile and wireless communication security, and privacy-preserving data mining and applied cryptograph. He has published more than 100 research papers in international journals, such as IEEE Trans. Knowledge and Data Engineering, IEEE Trans. Wireless Communication, IEEE Trans. Dependable and Secure Computing, IEEE Trans. Circuit and Systems, IEEE Trans. Vehicular Technologies, IEEE Communication Letters, IEE Electronic Letters, and conference proceedings. He is leading a few of Australia Research Council (ARC) Discovery Projects. He is currently serving as editor of IEEE Transactions on Dependable and Secure Computing.

Presentation Abstract

In mobile communication, spatial queries pose a serious threat to user location privacy because the location of a query may reveal sensitive information about the mobile user. In this talk, we consider k nearest neighbor (kNN) queries where the mobile user queries the location-based service (LBS) provider about k nearest points of interest (POIs) on the basis of his current location. We present a solution for the mobile user to preserve his location privacy in kNN queries. The proposed solution is built on the Paillier public-key cryptosystem and can provide both location privacy and data privacy. In particular, our solution allows the mobile user to retrieve one type of POIs, for example, k nearest car parks, without revealing to the LBS provider what type of points is retrieved. For a cloaking region with nxn cells and m types of points, the total communication complexity for the mobile user to retrieve a type of k nearest POIs is O(n+m) while the computation complexities of the mobile user and the LBS provider are O(n+m) and O(n^2m), respectively. Compared with existing solutions for kNN queries with location privacy, our solutions are more efficient. Experiments have shown that our solutions are practical for kNN queries.