

Student Research Seminar

Secure kNN Computation on Encrypted Databases

Mr Wong Wai Kit

Date & Time:
January 5, 2009
Monday
5:00pm

Venue:
Room 313
Chow Yei Ching Building
The University of Hong Kong

Abstract:

Service providers like Google and Amazon are moving into the SaaS (Software as a Service) business. They turn their huge infrastructure into a cloud-computing environment and aggressively recruit businesses to run applications on their platforms. To enforce security and privacy on such a service model, we need to protect the data running on the platform. Unfortunately, traditional encryption methods that aim at providing "unbreakable" protection are often not adequate because they do not support the execution of applications such as database queries on the encrypted data. In this talk, I will discuss the general problem of secure computation on an encrypted database and propose a SCONEDB (Secure Computation ON an Encrypted DataBase) model, which captures the execution and security requirements. As a case study, we focus on the problem of k-nearest neighbor (kNN) computation on an encrypted database. We develop a new asymmetric scalar-product-preserving encryption (ASPE) that preserves a special type of scalar product. We use ASPE to construct two secure schemes that support kNN computation on encrypted data; each of these schemes is shown to resist practical attacks of a different background knowledge level, at a different overhead cost. Extensive performance studies are carried out to evaluate the overhead and the efficiency of the schemes.

About the Speaker:

Wong Wai Kit is a Ph.D candidate at the University of Hong Kong (HKU). He is supervised by Professor David Cheung. His research interests include secure database applications and cloud computing.

All are welcome!

**For enquiries, please call 2859-2180 or email enquiry@cs.hku.hk
Department of Computer Science
The University of Hong Kong**

