

Student Research Seminar

Query and Access Control over Encrypted Databases

Mr. Zhang Ye

Date:

November 19, 2010

**Friday
3:00 pm**

Venue:

**Room 313
Chow Yei Ching Building
The University of Hong Kong**

Abstract:

Due to limited computation, storage and human resources or just for pursuing a lower management cost, a data owner may wish to outsource its data to a third party, the service provider. Such a paradigm is called outsourcing database. However, in an outsourcing database, there are several security and privacy issues raised, which cannot resort to traditional techniques.

For example, (1) the data owner may not trust the service provider which motivates the data owner to encrypt its valuable data before outsourcing them to the service provider. The service provider still needs to perform data management tasks (e.g., answering a query) over encrypted databases; (2) the data owner may trust the service provider but the clients who consume data (e.g., retrieve data records) do not trust the service provider. In this case, a privacy-preserving protocol should allow the client to retrieve a data record from the service provider while preventing the service provider from learning which record is being accessed and what attributes are associated with the client who retrieved that record. The protocol should also ensure the client can retrieve a data record if and only if the attributes associated with her are consistent with the access policy of that record.

To address problem (1), we devised an encryption scheme which allows the service provider to do Hamming-distance based similarity search over encrypted databases. It turns out that Hamming-distance based similarity search is useful in database, bioinformatics and many other areas. Compared to a generic construction from the previous literature, the ciphertext size in our new encryption scheme is smaller.

To address problem (2), we devised a privacy-preserving protocol. A previous construction for the same problem used a duplication strategy to achieve a disjunction of attributes access policy, which lets the same data record to appear multiple times each with a different conjunction of attributes access policy. Our new protocol realizes disjunction of attributes access policy without duplication, which leads to encrypted data records of a smaller size.

About the Speaker:

Zhang Ye is a full-time M.Phil. student in Department of Computer Science, The University of Hong Kong, under the supervision of Dr. Nikos Mamoulis and Prof. David W. Cheung. His research interests include cryptography and data privacy.

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

