香港浸會大學理學院
HKBU Faculty of Science

for favour of posting

DEPARTMENT OF COMPUTER SCIENCE

PhD Degree Oral Presentation

PhD Candidate:	Mr Zhe FAN
Supervisor:	Dr Koon Kau CHOI
External Examiner:	Prof Hong CHENG Prof Wook Shin HAN
Time:	7 Aug 2015 (Friday) 10:00 am – 12:00 nn (35 mins presentation and 15 mins Q & A)
Venue:	RRS 732, Sir Run Run Shaw Bldg., HSH Campus

"Secure Subgraph Query Services"

Abstract

Graphs are powerful tools for a wide range of real applications, from Biological and Chemical Databases, Social Networks, Citation Networks to Knowledge Bases. Large graph data repositories have been consistently found in recent applications. Due to the high complexity of graph queries, e.g., NP-Completeness of subgraph query, and the lack of IT expertise, hosting efficient graph query services for the owners of graph data has been a technically challenging task. And hence, they may prefer to outsource their services to third-party service providers (SPs) for scalability, elasticity and efficiency.

Unfortunately, SPs may not always be trusted. Security, typically the integrity and confidentiality, of the data, has been recognized as one of the critical attributes of Quality of Services (QoS). This directly influences the willingness of both data owners and query clients to use SP's services. To address these concerns, this thesis proposes novel techniques to solve both authentication-aware and privacy-aware subgraph query.

Firstly, we study authenticated subgraph query services (Chapter 3). To support the service, we propose Merkle IFTree (MIFTree) where Merkle hash trees are applied into our Intersection-aware Feature-subgraph Tree (IFTree). IFTree aims to minimize I/O in a well-received subgraph query paradigm namely the filtering-and-verification framework. The structures required to be introduced to verification objects (VOs) and the authentication time are minimized. Subsequently, the overall response time is minimized. For optimizations, we propose an enhanced authentication method on MIFTree.

Secondly, we propose structure-preserving subgraph query services (Chapter 4). A crucial step of this part is to transform the seminal subgraph isomorphism algorithm (the Ullmann's algorithm) into a series of matrix operations. We propose a novel cyclic group based encryption (CGBE) method for private matrix operations. We propose a protocol that involves the query client and static indexes for optimizations. We prove that the structural information of both query graph and data graph are preserved under CGBE and analyze the privacy preservation in the presence of the optimizations.

Thirdly, we propose asymmetric structure-preserving subgraph query processing (Chapter 5), where the data graph is publicly known and the query structure/topology is kept secret. Unlike other previous methods for subgraph queries, this part proposes a series of novel optimizations that only exploit graph structures, not the queries. Further, we propose a robust query encoding and adopt our proposed cyclic group based encryption method, so that the query processing can be transformed into a series of private matrix operations and performed securely.

The effectiveness and efficiency of all the techniques presented in this thesis are experimentally evaluated with both real-world and synthetic dataset.

***** ALL INTERESTED ARE WELCOME *****