Program

Date: 6th, May, 2013
Locate: Room #401, Technical Building, HBUT

8:45-8:55 Opening Speech
   Professor and Dean: Chunzhi Wang

8:55-9:00 Photo

Session 1: Secret Sharing and Primitives in Cloud Storage
Mediator: Professor Caiquan Xiong

9:00-9:45 Title: Secret Sharing, Proof of Plaintext Knowledge, and Their Applications to Secure Cloud Storages
   Professor Kirill Morozov, Kyushu University

9:45-10:30 Title: A New Publicly Verifiable Secret Sharing Scheme without Dealer
   Professor Zhenhua Chen, Shaanxi Normal University

10:30-10:45 Break

Session 2: Data Outsourcing and Computation in Cloud Computing
Mediator: Professor Zhiwei Ye

10:45-11:30 Title: Secure k-NN query on encrypted cloud database
   Dr. Youwen Zhu, JSPS doctoral fellow, and Institute of Mathematics for Industry Kyushu University

11:30-12:15 Title: Fairness of Secure Multi-Party Computation
   Dr. Ou Yuan, Hubei University of Technology

12:30-14:00 Lunch and break
Session 3: Secure Computation and Privacy Preservation in Open Cloud Application

Mediator: Professor Kirill Morozov

14:00-14:45 Title: Privacy-Preserving Data Aggregation in Smart-Grid Cloud Systems
   Professor Mingwu Zhang, Hubei University of Technology

14:45-15:30 Title: Secure Set Comparison and its Applications
   Mr. Wei Shi, Hubei University of Technology

15:30-15:45 Break

Session 4: Intelligence Process and Optimization Algorithms and Applications

Mediator: Professor Hongwei Chen

15:45-16:30 Title: P2P Traffic Identification based on Trust Sample Model
   Mr. Dongyang YU, Hubei University of Technology

16:30-17:15 Title: Fuzzy Clustering Image Segmentation Method Based on Bat Algorithm
   Mr. Mingwei Wang, Hubei University of Technology

18:00 Dinner
Title: **Secret Sharing, Proof of Plaintext Knowledge, and Their Applications to Secure Cloud Storage**

**ABSTRACT:** In this talk, I will present some recent results in the two areas of cryptography: cheater-identifiable secret sharing and (postquantum) code-based cryptographic protocols, putting them into the context of providing security and privacy for cloud storage services.

First, I will present secret sharing as a tool for simultaneously achieving security and availability for cloud storage. Here, a private data can be split between n servers in such a way that only a threshold k of them (for instance k=n/2) can reconstruct the data, but any k-1 servers provably have no information about it.

Then, I will introduce our ongoing work on preventing corrupt servers from causing the honest servers to reconstruct an incorrect data. We obtain an improvement over existing results in terms of the share size for the case when up to t<k/3 servers misbehave.

Second, I will present the cryptographic protocol called "proof of plaintext knowledge" (PPK) for public-key encryption (PKE). We suggest its application to secure cloud storage. Then, we present PPK for code-based McEliece and Niederreiter PKE. One particular advantage of these schemes is their security even against attacks using quantum computation.

This result will be presented at AsiaCCS 2013.

Title: **Secure k-NN Query on Encrypted Cloud Database**

**ABSTRACT:** In recent years, secure outsourcing and query on encrypted database receives much attention, as cloud computing becomes a more and more prevalent computing model. Among them, secure k-nearest neighbors (k-NN) computation on encrypted cloud data is a significant topic, and several solutions for it have been put forward. In this talk, we review the existing secure k-NN query schemes, and it shows that most previous schemes assume query users are fully trusted and all query users share the full key to encrypt and decrypt the outsourced database of data owner, which is not feasible in lots of real-world applications.

To deal with the problems of key-sharing, we present a new approach in which query users can access only partial information about the key instead of the full one. At last, we introduce our future work, such as a new scheme to support offline data owner and key confidentiality.
Title: **A new Publicly Verifiable Secret Sharing Scheme without Dealer**

**ABSTRACT:** Most publicly verifiable secret sharing schemes without dealer are based on the traditional public-key systems such as the discrete logarithm problem or the integer factoring problem so far.

In this talk, we propose a new publicly verifiable secret sharing scheme without dealer. It is shown how to avoid the dealer who selects and distributes the private share and to allow the each participant of the group can publicly verify whether the share is correct. This scheme is efficient and with unconditional verifiability. Furthermore, the verification process in this scheme is made non-interactive without using the Fiat-Shamir technique or any additional Zero Knowledge proof, which make it simple than that in the other known schemes.

Title: **Secure Set Comparison and its Applications**

**ABSTRACT:** In cloud systems, secure multi-party computation has been extensively applied to privacy preserving information retrieval, scientific computation, effective application of privacy data, etc., and has become a research focus in international cryptographic community. This talk focuses on secure multi-party computation on set equality test, comparing set through matching of set and natural number and comparison of natural numbers. The simulations show that these multi-party solutions are secure.

Title: **Privacy-Preserving Data Aggregation in Smart-Grid Cloud Systems**

**ABSTRACT:** The concept of smart grid has emerged as a convergence of traditional power system engineering and information and communication technology. It is vital to the success of next generation of power grid, which is expected to be featuring reliable, efficient, flexible, clean, friendly and secure characteristics.

In this talk, we present and discuss the data aggregations in smart grids without revealing any additional information about the individual meter readings. We also give the basic ideas and solutions for aggregating the data via cryptographic primitives.
Title: **Fuzzy Clustering Image Segmentation Method Based on Bat Algorithm**

**ABSTRACT:** Fuzzy c-means (FCM) algorithm is a dynamic cluster algorithm, which is suitable for the uncertain and ambiguous characteristic in the intensity image segment, however, it is too sensitive to provide a good solution for initial clustering center and membership matrix, and likely converged into the locally optimal solution. There often exists insignificant clustering in the result of Fuzzy c-means algorithm when traditional union, intersection and inclusion work in fuzzy set.

In this talk, we propose a new image segmentation method, which combines Bat algorithm with FCM clustering. The results indicate that our method is efficient in clustering of image segmentation, and it has a faster convergence speed and higher accuracy of segmentation.

Title: **P2P Traffic Identification based on Trust Sample Model**

**ABSTRACT:** In P2P network, trust sample traffic identification, based on Deep-Package-Inspection (DPI), is a kind of purpose sample method. During the whole procedure of sampling identification, the sampling ratio will adjust by the history estimators of the traffic, dynamically. In this presentation, we propose a trust degree model that the trust degree is updated by the logarithm of previous estimator of traffic ratio. We also give the simulation of traffic identification on a host machine. The experimental results show that, compared with non-trust sample model, the cumulative amount of the sampled traffic packets in cycles has an obvious decreasing tendency. The results also indicate that the trust sample is fine-purposed, and it can reduce the time complexity and consumption of system resource, without expanding the absolute error of the estimator.

Title: **Fairness of Secure Multi-Party Computation**

**ABSTRACT:** With the development of modern Internet, mobile networks and cloud computing, there is an increasing demand for privacy-preserving cooperative computation, such as data outsourcing, delegate computation, database storage and digital copyright protect etc. Secure multi-party computation (SMPC) provides a general solution to these applications and has become a hot topic in cloud computing.

In this presentation, we will focus on the security, privacy and fairness of secure multiparty computation, and give the fine-grained suggestions for the problems.