YUXI LI

Address: No.195, Chuangxin Road, Hunnan District, Shenyang, Liaoning, China, 116024
Birthdate: 03/03/1990 Gender: Female Nationality: Chinese
Phone: (+ 86) 180-0421-9988 Email: eliyuxi@gmail.com

EDUCATION BACKGROUND

Northeastern University **Shenyang, China**
Ph.D. Candidate in Software Engineering (Supervisor: Prof. Fucai Zhou) Sept. 2014 - Jul. 2018 (expected)
Northeastern University **Shenyang, China**
M.S. in Computer Application Technology Sept. 2012 - Jul. 2014
Sichuan University **Chengdu, China**
B.E. in Computer Science and Technology Sept. 2008 - Jul. 2012
B.Ec. in International Economics and Trade Sept. 2008 - Jul. 2012

RESEARCH INTERESTS

My research interests are cryptography, security and data privacy with a special focus in searchable encryption, cloud security and electronic cash.

ACADEMIC EXPERIENCE

Searchable Unstructured Data Encryption in Cloud Computing (Ph.D. Topic) (Nov. 2013 - Mar. 2016)

Description: The objective is to design secure and efficient schemes to address essential data utilization functions over encrypted data in cloud computing. To this end, we studied three problems in this research area. Detailed topics:

- **Integrity Preserving Multi-keyword Searchable Encryption** (completed)
  We investigated a multi-keyword searchable encryption scheme with an authentication mechanism that can efficiently verify the integrity of search results.
  -adopt the bilinear map accumulator to prove the correctness of set operations
  -supports multiple keywords as input for conjunctive search
  -gives the server the ability to prove the integrity of the search result to the user
  -efficient, unforgeable and adaptive secure against chosen-keyword attacks
- **Multi-Keyword Fuzzy Search over Encrypted Data** (completed)
  We proposed a multi-keyword fuzzy search method on the encrypted data, on the study of the method of multi-keyword fuzzy search.
  -based on the bloom filter, dual coding function and the position sensitive hash function
  -uses the distance recoverable encryption arithmetic to encrypt file index
  -no need to set index storage space in advance, which greatly reduces the complexity of the search
  -no need of predefined dictionary library
  -compared with the existing solutions, lower the storage overhead in consequence

Searchable Structured Data Encryption in Cloud Computing (Ph.D. Topic) (Nov. 2015 - Present)

Description: In previous, I proposed different ways to search on encrypted data. However, I am also focused on how to search on encrypted structured data which are gaining a lot of popularity. Detailed topics:

- **Privacy-preserving queries on encrypted Graph** (in progress)
  To solve the privacy-preserving problem for cloud computing when querying in large-scale graph structure, we are trying to propose a novel solution for encrypted graph structure with support for various graph queries.

-transform a graph into a special encrypted structure
-perform efficient approximate privacy preserving query
-encrypt the graph by inverted index and homomorphic encryption scheme

- **Privacy-Preserving Pattern Matching over Encrypted Genetic Data** (in progress)
  We investigate an important privacy-sensitive data application in cloud computing, i.e., genetic testings over DNA sequences. To provide secure and efficient genetic testings in the cloud, we are trying to utilize structured encryption and design a secure pattern matching scheme to achieve strong privacy guarantee while fulfilling the functionality requirement efficiently.

Privacy-Preserving Electronic Cash System (M.S. Topic) **(Sep. 2012 - Mar. 2014)**
Description: We study new electronic cash system by the utilization of non-interactive zero-knowledge proof and dynamic group signature that avoids the limitations of (1) relying on a random oracle, (2) not supporting multiple bank setting and users dynamically joining or (3) prohibitively expensive.
-anonymous against chosen-ciphertext attack (CCA) in the standard model
-supports multiple banks enrolling and users dynamically joining
-achieves CCA anonymity, unforgeability, traceability and no double-spending
-compared with the existing systems, ours has advantages of both the efficiency and security

PUBLICATIONS

[1] Fucai Zhou, **Yuxi Li**, Qingshi Zhou, Jingwei Miao, Jian Xu, The Electronic Cash System Based on Non-Interactive Zero-Knowledge Proofs. International Journal of Computer Mathematics. Vol. 93, No. 2, 2016.

[2] Fucai Zhou, **Yuxi Li**, Alex X Liu, Muqing Lin, Zifeng Xu, Integrity Preserving Multi-keyword Searchable Encryption for Cloud Computing. The Tenth International Conference on Provable Security(ProvSec 2016).

[3] **Yuxi Li**, Fucai Zhou, Alex X Liu, Muqing Lin, Zifeng Xu, Integrity-Verifiable Conjunctive Keywords Searchable Encryption in Cloud Storage. Soft Computing (Submitted).

[4] FuCai Zhou, MuQing Lin, Yang Zhou and **YuXi Li**, Efficient Anonymous Broadcast Encryption with Adaptive Security. KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS VOL. 9, NO. 11, Nov. 2015.

[5] Jian Xu, **Yuxi Li**, Jingwei Miao, Fucai Zhou, The Electronic Cash Protocol Based on Dynamic Group Signature. JoWUA, VOL. 4, NO. 4, 2013.

[6] Kaixuan Wang, **Yuxi Li**, Fucai Zhou, Quanqi Wang, Multi-Keyword Fuzzy Search over Encrypted Data. Journal of Computer Reasearch and Development, VOL. 54, NO. 4, 2017.

[7] **Yuxi Li**, Kaixuan Wang, Muqing Lin, Fucai Zhou, A P2P network privacy protection system based on anonymous broadcast encryption scheme. Journal of Shandong University(Natural Science), VOL. 51, NO. 9, 2016.

[8] Sifei Wang, Xiaohan Yue, **Yuxi Li**, Fucai Zhou, Dynamic Short Group Signature with Provable Security in Standard Model. Journal of Northeastern University(Natural Science), VOL. 34, NO. 8, 2013.

[9] Xuegang Huang, Tianhan Gao, **Yuxi Li**, Research on Chameleon Certification Tree Algorithm for Streaming Data Authentication. Journal of Sichuan University(ENGINEERING SCIENCE EDITION), VOL. 48, NO. 8, 2016.

PRESENTATIONS

Integrity Preserving Multi-keyword Searchable Encryption for Cloud Computing
-The 10th International Conference on Provable Security (ProvSec 2016); Nanjing; November, 2016

An electronic Survey System based on Non-Interactive Zero Knowledge proofs
-The 10th Chinese Conference on Trust Computing and Information Security, Chengdu; October, 2016

Research on Chameleon Certification Tree Algorithm for Streaming Data Authentication
-The 9th Chinese Conference on Trust Computing and Information Security, Xi'an; October, 2015

The Electronic Cash Protocol Based on Dynamic Group Signature
-Security Protocol Workshop; Institute of Information Engineering, Beijing; July, 2013

AWARDS

Northeastern University Scholarship (2 times)	2013 - 2014
Sichuan University Scholarship (3 times)	2009 - 2012

INTERESTS

Chinese Calligraphy, Marathon, Mountain Climbing.

REFERENCES PERSONS

Prof. Fucai Zhou, Northeastern University, China. Contact: fczhou@mail.neu.edu.cn
Prof. Jian Xu, Northeastern University, China. Contact: xuj@mail.neu.edu.cn