Jinsheng Zhang

alexanderzjs@gmail.com
https://www.linkedin.com/in/alexanderzjs/
https://github.com/alexanderzjs
alexanderzjs
+86-18738327320

Education

2010 – 2016 Ph.D. Computer Science, Iowa State University
Thesis: Data access pattern protection in cloud storage
GPA: 3.82/4.0

2006 – 2010 B.S. Information Security, University of Science and Technology of China
Thesis: Research on Trusted Routing Protocol of Mobile Ad Hoc Networks
GPA: 3.62/4.3

Employment

- Technique Expert (P7) in Secure Multiparty Computation group of Blockchain Department at Ant Financial (Alibaba Group) July 2018 – April 2019
  - Participate in desigining private query project of China Mobile.
    - Research and re-design existing Private Set Intersection scheme for China Mobile's project.
    - Participate in developing new Private Set Intersection scheme to support privacy-preserving intersection query on 100-million level dataset.
  - Participate in designing and developing privacy-preserving Logistic Regression model for over 20 finanacial institutions.
    - Design Secret Sharing scheme to protect the privacy of Logisitic Regression model.
    - Enhance the existing model to support over 10,000 sample size and over 1000 feature size.
    - Develop the Garbled Circuit module to reduce modeling time by one magnitude.
  - Participate in designing and developing privacy-preserving GBDT model for over 20 finanacial institutions.
    - Research and design Garbled Circuit based scheme to protect the privacy of GBDT model.
    - Independently research and develop core Garbled Circuit primitives.
    - Design Garbled Circuit and Homomophic Encryption based privacy-preserving GBDT model.
  - Design the compiler for Secure Multiparty Computation.
    - Design the compiler to support both Garbled Circuit and Secret Sharing.
    - Design the corresponding virtual machine to connect to the compiler.
- Software Engineer III in Trust and Identity Management team at Ebay Inc. May 2016 – July 2018
  - Design and develop push notification based multi-factor authentication.
    - Develop the push notification multi-factor authentication and integrate to Ebay FIDO server.
  - Participate in developing Single Sign On support for password-less access to Ebay.
  - ★ Participate in designing and developing RESTful services to migrate existing sign-in system for better system isolation.
    - Research on existing sign-in system services based on different user types and service types.
    - Developing Cookie library for different type of users.
  - Developing commercial RESTful serivce to track user sign-in activities for data analysis.
- Software Engineer Internship at Nok Nok Labs. Jan 2015 – Dec 2015
  - Designed and implemented multi-factor authentication functionality with IBM Tivoli Server.
  - Implemented and productized a multi-tenant access control and multi-factor authentication system.
  - Developed a bootstrap web application for multi-factor authentication system to bootstrap an end-user with email registration.
- Head Teaching Assistant at Com S Department, Iowa State University. Sep 2013 – Dec 2014
  - COM S 106: Introduction to Web Programming (Instructor: Dr. Susan (Shu-Hui) Chang)

- Teaching Assistant at Com S Department, Iowa State University. Jan 2012 – Sep 2013
  - COM S 103: Computer Applications (Instructor: Dr. Susan (Shu-Hui) Chang)
- Teaching Assistant at Com S Department, Iowa State University. Jan 2012 – May 2012
  - COM S 552: Principles of Operating Systems (Instructor: Dr. Wensheng Zhang)
- Research Assistant at Com S Department, Iowa State University. Sep 2010 – Dec 2011
  - I worked with Dr. Wensheng Zhang (Com S Department) and Dr. Daji Qiao (ECE Department) from Iowa State University. My research interests are applied cryptography and computer security/privacy, including but not only restricted to security and privacy system and algorithm designs in systems, databases, networking.
- Research Internship at State Key Laboratory of Information Security, Chinese Academy of Sciences. Jun 2009 – Aug 2009
  - I worked with Dr. Yuqing Zhang on summer intern project “Research on the Impact of RepTrap Attack to Trust Management System”.

Publications

1. Qiumao Ma and Jinsheng Zhang and Yang Peng and Wensheng Zhang and Daji Qiao. (2016). SE-ORAM: a Storage-efficient Oblivious RAM for Privacy-preserving Access to Cloud Storage. In Cyber Security and Cloud Computing (CSCloud), 2016 IEEE 3rd International Conference on. IEEE.
2. Qiumao Ma and Wensheng Zhang and Jinsheng Zhang. (2016). DF-ORAM: A Practical Dummy Free Oblivious RAM to Protect Outsourced Data Access Pattern. In International Conference on Network and System Security. Springer.
3. Jinsheng Zhang. (2016). Data Access Pattern Protection in Cloud Storage (Doctoral dissertation). Iowa State University.
4. Jinsheng Zhang and Qiumao Ma and Wensheng Zhang and Daji Qiao. (2016a). MSKT-ORAM: A Constant Bandwidth ORAM without Homomorphic Encryption (tech. rep.). IACR Cryptology ePrint Archive, Report 2016/882.
5. Jinsheng Zhang and Qiumao Ma and Wensheng Zhang and Daji Qiao. (2016b). TSKT-ORAM: A Two-server K-ary Tree ORAM for Access Pattern Protection in Cloud Storage. In Military Communications Conference, MILCOM 2016-2016 IEEE. IEEE.
6. Jinsheng Zhang and Wensheng Zhang and Daji Qiao. (2016). MU-ORAM: Dealing with Stealthy Privacy Attacks in Multi-User Data Outsourcing Services. IACR Cryptology ePrint Archive, 2016, 73.
7. Ka Yang and Jinsheng Zhang and Wensheng Zhang and Daji Qiao. (2015). Privacy-Preserving Accountable Cloud Storage.
8. Jinsheng Zhang and Qiumao Ma and Wensheng Zhang and Daji Qiao. (2015). TSKT-ORAM: A Two-Server k-ary Tree Oblivious RAM without Homomorphic Encryption. Future Internet, 9(4), 57. https://doi.org/10.3390/fi9040057
9. Jinsheng Zhang and Wensheng Zhang and Daji Qiao. (2015). GP-ORAM: A Generalized Partition ORAM. In International Conference on Network and System Security. Springer.
10. Jinsheng Zhang and Qiumao Ma and Wensheng Zhang and Daji Qiao. (2014). KT-ORAM: A Bandwidth-efficient ORAM Built on K-ary Tree of PIR Nodes.
11. Jinsheng Zhang and Wensheng Zhang and Daji Qiao. (2014). S-ORAM: A Segmentation-based Oblivious RAM. In Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security. ACM.
12. Ka Yang and Jinsheng Zhang and Wensheng Zhang and Daji Qiao. (2013). Light-weight Preservation of Access Pattern Privacy in Un-trusted Storage. IEIE Transactions on Smart Processing & Computing, 2(5), 282–296.

13 Ka Yang and Jinsheng Zhang and Wensheng Zhang and Daji Qiao. (2011a). A Light-weight Solution to Preservation of Access Pattern Privacy in Un-trusted Clouds. In European Symposium on Research in Computer Security. Springer.

Formal Presentations

- "S-ORAM: A Segmentation-based Oblivious RAM" at ASIACCS, Kyoto, Japan, 2014
- "GP-ORAM: A Generalized Partition ORAM" at NSS, New York, USA, 2015

Posters and Demos

1 Ka Yang and Jinsheng Zhang and Wensheng Zhang and Daji Qiao. (2011b). Intrustion Detection in the Cloud.

2 Ka Yang and Jinsheng Zhang and Wensheng Zhang and Daji Qiao. (2011c). Privacy and Secrecy Preservation in Un-trusted Clouds.

3 Jinsheng Zhang and Wensheng Zhang. (2011). Protecting Access Pattern Privacy in Cloud Computing.

Awards and Achievements

2014 National Science Foundation #1422402,
NSF Org: CNS Division Of Computer and Network Systems
Title: TWC: Small: Building Efficient and Accountable Multi-User ORAM Systems for Protecting Data Access Patterns
Program Manager: Nan Zhang, CSE Direct For Computer & Info Scie & Enginr
Period: Sep. 1, 2014 - Aug. 31, 2016
Awarded Amount: $100,000.00
Investigator(s): Wensheng Zhang (Principal Investigator), Daji Qiao (Co-Principal Investigator)
Sponsor: Iowa State University, 1138 Pearson, Ames
NSF Programs(s): Secure & Trustworthy Cyberspace
Program Reference Code(s): 7434, 7923, 9150
Program Element Code(s): 8060

2009 Certificate of Award, Outstanding University Project of Summer Internship of "Research on the Impact of RepTrap Attack to Trust Management System".

Professional Services

I have been a reviewer/external reviewer of the following journals/conferences:
International Journal of Distributed Sensor Networks,
IEEE/ACM International Symposium on Quality of Service,
IEEE Communications Letters,
IEEE International Conference on Computer Communications,
IEEE International Conference on Distributed Computing Systems,
IEEE Wireless Communications,
ACM Transactions on Sensor Networks,
Mobile Adhoc and Sensor Systems.