张晋升

alexanderzjs@gmail.com
https://www.linkedin.com/in/alexanderzjs/
https://github.com/alexanderzjs
alexanderzjs
+86-18768199334

教育经历

2010 – 2016 博士学位，计算机科学系，Iowa State University
博士论文：云存储数据访问模式保护
课程绩点：3.82/4.0

2006 – 2010 学士学位，信息安全专业，中国科学技术大学
学士论文：研究移动 Ad Hoc 网络的可信路由协议
课程绩点：3.62/4.3

工作经历

蚂蚁金服 (阿里巴巴) 技术专家 (P7) 安全多方计算组区块链团队 2018 年七月 – 2019 年四月

- 参与并负责设计中国移动隐私保护查询项目
  - 调研并设计改进的 PSI（隐私保护的集合查询）技术以支撑移动的基本需求
  - 参与开发改进的 PSI（隐私保护的集合查询）技术实现亿级别数据查询
- 参与并负责设计 20 多家银行、基金、消金和互金的隐私保护逻辑回归模型 LR 建模方案
  - 设计秘密共享技术实现进行隐私保护 LR 建模
  - 改进设计的隐私保护建模方案来支持万级别数据和千级别特征的隐私保护 LR 建模
  - 引入混淆电路技术进一步改进 LR 建模方案以实现分钟级别隐私保护 LR 建模
- 参与并负责设计 20 多家银行、基金、消金和互金的隐私保护树模型 GBDT 预测方案
  - 设计基于混淆电路技术实现的隐私保护 GBDT 树模型预测方案
  - 独立开发实现混淆电路以及相关核心技术
  - 提出并设计基于混淆电路和同态加密的隐私保护 GBDT 树模型预测方案
- 设计多方安全计算编译器
  - 设计基于混淆电路和秘密共享技术的编译器
  - 设计基于混淆电路和秘密共享技术的虚拟机来完成编译内容的运行

Ebay 中级软件工程师, 信任和身份管理组 2016 年五月 – 2018 年七月

- 实现基于消息推送的双重认证机制
  - 利用 Ebay 的 FIDO 服务来实现消息推送认证机制
- 实现跨平台单点认证模型来支持任意设备的无密码访问
- 设计并实现已有登录系统到 REST 服务的迁移来明确登录系统中各服务的分离性和易维护性
  - 深入研究现有登录系统的各个服务以及不同用户类型的不同服务分支的区别
  - 实现不同类别用户（10 个类别）的 Cookie 管理（一共 80 多个 Cookie）
- 实现一个商用标准的 REST 服务，该服务用于追踪消费者登陆行为并提供数据给其他数据分析组使用

Nok Nok Labs 软件工程师实习 2015 年一月 – 2015 年十二月

- 设计并整合 IBM Tivoli 服务器与已有的多重认证服务器
- 实现商用化多租户的访问控制并整合已有的多重认证服务器
- 实现多重认证服务器的用户邮件注册功能

Iowa State University 计算机科学系首席助教 2013 年九月 – 2014 年十二月

- COM S 106: 网页编程导论 (主讲教授: Dr. Susan (Shu-Hui) Chang)
  - 参与课程讲义编制、课程作业设计以及课程项目的设计

Iowa State University 计算机科学系首席助教 2012 年一月 – 2013 年九月

- COM S 103: 计算机应用导论 (主讲教授: Dr. Susan (Shu-Hui) Chang)

- 参与学生答疑，课程作业的以及课程项目的批改

Iowa State University 计算机科学系助教 2012 年一月 – 2012 年五月

- ★ COM S 552: 操作系统原理 (主讲教授: Dr. Wensheng Zhang)
  - 参与学生答疑，课程作业的以及课程项目的批改

Iowa State University 计算机科学系助研 2010 年九月 – 2011 年十二月

★ 在助研阶段，我和我的导师 Dr. Wensheng Zhang (计算机科学系) 以及 Dr. Daji Qiao (计算机电气工程系) 紧密合作来完成博士学业。我的科研方向是应用密码学，计算机安全 / 隐私保护，包括相关算法，系统，数据库，网络的设计以及更多方向的研究。

中科院信息安全国家重点实验室助研 2009 年六月 – 2009 年八月

★ 在实习阶段，我和我的导师 Dr. Yuqing Zhang 紧密合作来完成大学生研究计划课题“研究 RepTrap 攻击对信任管理系统的影响”。

学术论文列表

1. Jinsheng Zhang. (2016). Data Access Pattern Protection in Cloud Storage (Doctoral dissertation, Iowa State University).
2. Jinsheng Zhang and Qiumao Ma and Wensheng Zhang and Daji Qiao. (2016a). MSKT-ORAM: A Constant Bandwidth ORAM without Homomorphic Encryption. IACR Cryptology ePrint Archive, Report 2016/882.
3. 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 军事通信会议) (pp. 527–532). IEEE.
4. 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.
5. 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 (pp. 20–25). IEEE.
6. 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 (pp. 415–432). Springer.
7. 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. doi:10.3390/fi9040057
8. Jinsheng Zhang and Wensheng Zhang and Daji Qiao. (2015). GP-ORAM: A Generalized Partition ORAM. In International Conference on Network and System Security (pp. 268–282). Springer.
9. Ka Yang and Jinsheng Zhang and Wensheng Zhang and Daji Qiao. (2015). Privacy-Preserving Accountable Cloud Storage.
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 (pp. 147–158). 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 (pp. 528–547). Springer.

演讲列表

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

学术海报和演示

1 Jinsheng Zhang and Wensheng Zhang. (2011). Protecting Access Pattern Privacy in Cloud Computing. Poster Day at Department of Computer Science, Iowa State University.

2 Ka Yang and Jinsheng Zhang and Wensheng Zhang and Daji Qiao. (2011b). Intrustion Detection in the Cloud. Security and Software Engineering Research Center (S2ERC) Showcase.

3 Ka Yang and Jinsheng Zhang and Wensheng Zhang and Daji Qiao. (2011c). Privacy and Secrecy Preservation in Un-trusted Clouds. Security and Software Engineering Research Center (S2ERC) Showcase.

荣誉和获奖证书

2014 美国国家自然科学基金 #1422402,
基金颁发下属机构: 计算机网络系统分部
标题: TWC: Small: Building Efficient and Accountable Multi-User ORAM Systems for Protecting Data Access Patterns
基金项目经理: Nan Zhang, CSE Direct For Computer & Info Scie & Enginr
时间: 2014 年 9 月 1 日 - 2016 年 8 月 31 日
基金总额: $100,000.00
赞助方: Iowa State University, 1138 Pearson, Ames
基金领域: 安全可信的网络空间
基金编号: 7434, 7923, 9150
基金代码: 8060

2009 大学生暑期研究计划优秀项目 “研究 RepTrap 攻击对信任管理系统的影响”。

学术服务

我曾经担任过以下学术杂志和会议的评审 / 外部评审：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.