

# 李宇溪

✉ eliyuxi@gmail.com

📍 辽宁省沈阳市东北大学浑南校区  
ℹ 1990年3月3日出生于辽宁省朝阳市



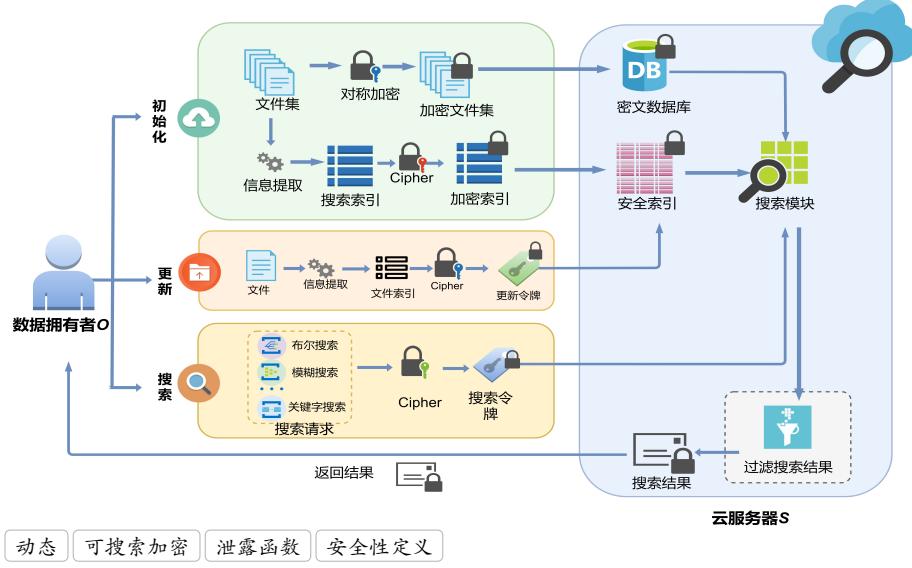
**简介** 李宇溪，女，东北大学-佐治亚理工学院联合培养软件工程专业博士。主要研究方向是**网络空间安全、应用密码学、可搜索加密及其应用**。参与国家重大专项、国家自然科学基金面上项目以及辽宁省自然科学基金等多项课题。近些年来，在 International Journal of Information Security、International Journal of Computer Mathematics、IEEE Access 和计算机研究与发展等国内外相关领域的期刊和 ProvSecurity 和 SciSec 等国际会议上发表 SCI、EI 检索论文数 10 余篇；申请国家发明专利 2 项；与国内外同领域知名学者和研究机构开展持续的研究合作，包括 Alex X. Liu (美国 Michigan State University) 和 Alexandra Boldyreva 教授 (美国 Georgia Institute of Technology) 等学者。

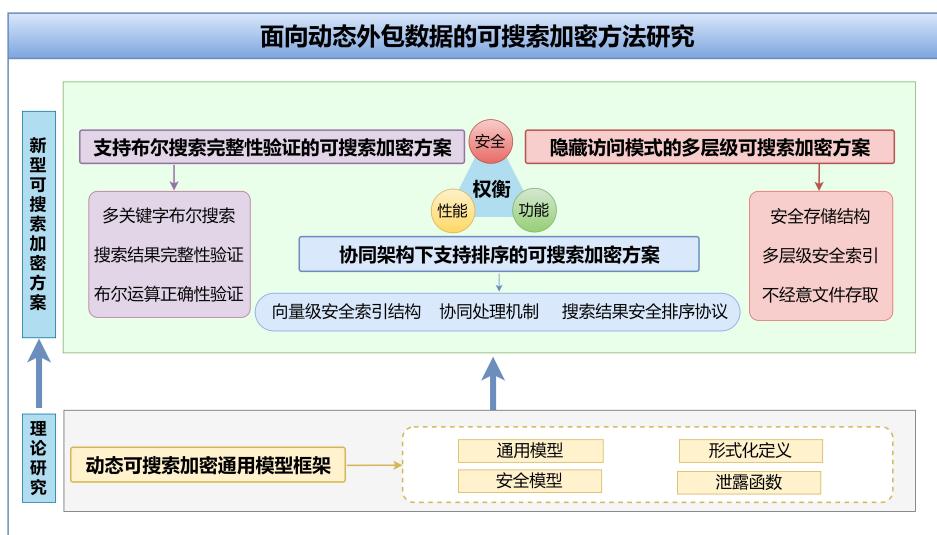
## 🎓 教育背景

2014 年 9 月 -2020 年 1 月	博士，软件工程，软件学院，东北大学，沈阳 研究方向：“可搜索加密及相关应用” 导师： <a href="#">周福才教授</a>
2017 年 10 月 -2018 年 10 月	访问学者，信息安全系，计算机学院，佐治亚理工学院，美国 研究方向：“Searchable Encryption” 导师： <a href="#">Alexandra Boldyreva 教授</a>
2012 年 9 月 -2014 年 7 月	硕士，计算机应用技术，信息科学与工程学院，东北大学，沈阳 毕业设计题目：“基于可追踪动态群签名的公平离线电子现金系统” 导师： <a href="#">周福才教授</a>
2008 年 9 月 -2012 年 7 月	本科，计算机科学与技术，计算机学院，四川大学，成都 本科，国际经济与贸易，经济学院，四川大学，成都

## 📖 学术经历

2016 年 7 月 -2014 年 9 月	<b>动态可搜索加密通用模型框架研究，东北大学，博士课题</b> 在可搜索加密技术进行深入研究的基础上，设计动态可搜索加密通用模型框架。提出一种动态可搜索加密通用模型，并对模型进行形式化定义。提出动态可搜索加密安全模型，对敌手的攻击能力进行安全假设，分析在特定安全假设下的安全目标，定义不同阶段的泄露函数，针对自适应性敌手给出动态自适应选择关键字安全性定义。并给出模型的扩展分类和潜在现实应用场景。
---------------------------	--





聚焦于动态外包数据的特征和数据安全的多元需求,在安全、功能以及性能三个方面研究可搜索加密关键技术,利用对称加密机制、双线性累加器、同态加密方法、安全多方计算、广播加密方法以及安全性与复杂度分析理论等密码学和数学理论,提出面向动态外包数据的三种可搜索加密方案,为可搜索加密在动态外包数据环境中真正部署应用提供理论基础。

#### > 支持布尔搜索完整性验证的可搜索加密

针对已有可搜索加密方案搜索语句单一且验证机制不完善等不足,提出一种支持布尔搜索完整性验证的可搜索加密方案。提出面向布尔搜索的动态自适应选择关键字安全性定义。设计支持动态更新的链表结构倒排索引,并利用可证安全的对称加密和同态加密机制对索引进行加密。针对布尔搜索结果完整性验证的需求,给出布尔搜索可验证性定义,提出基于双线性映射累加器和扩展欧几里德算法的布尔搜索结果完整性验证方法,基于双线性阶强Diffie-Hellman假设对布尔搜索结果的可验证性进行严格证明。最后对方案进行实现,并对该方案与已有方案进行了性能对比分析。

相关成果: "Integrity-verifiable conjunctive keyword searchable encryption in cloud storage," International Journal of Information Security (SCI 收录); "Integrity Preserving Multi-keyword Searchable Encryption for Cloud Computing," International Conference on Provable Security (EI 收录)。

#### > 协同架构下支持排序的可搜索加密

针对当前可搜索加密方法动态更新效率低且搜索结果不准确的问题,提出一种协同架构下支持排序的可搜索加密方案。在双敌手半可信场景下给出方案的安全性定义。融合正交向量基和同态加密思想设计向量级安全倒排索引结构,实现索引轻量灵活的动态更新。构建双服务器协同处理机制,在不向协同云服务器泄露搜索模式与访问模式的前提下,实现对于搜索结果的安全排序。对方案的正确性进行分析,并对安全性进行了详细证明,证明其在随机预言模型下抵抗自适应性选择关键字攻击。对方案的算法进行了效率分析,并与其它方案进行了对比。

相关成果: "An Efficient Two-Server Ranked Dynamic Searchable Encryption Scheme", IEEE Access(SCI 收录); "双服务器模型下支持相关度排序的多关键字密文搜索方案", 计算机研究与发展(EI 收录)。

可搜索加密 云存储安全 同态加密 应用密码学

至今  
-2015年9月

### 面向动态外包数据的可搜索加密方法研究,东北大学-佐治亚理工学院,博士课题

#### > 隐藏访问模式的多层次可搜索加密

围绕多用户可搜索加密的用户隐私泄漏以及访问控制力度粗放问题,提出一种隐藏访问模式的多层次可搜索加密方案。面向多层次用户给出方案的安全性定义。基于伪随机思想设计动态数据安全外包存储算法,保证了数据的机密性。设计两轮访问协议实现不经意文件更新及存取,在隐藏了访问模式的同时大大降低了动态更新时访问交互次数。针对多用户场景,提出多层次访问策略,并基于此设计多层次安全索引,从而实现外包数据的细粒度访问控制。提出基于广播加密的多层次用户动态管理机制,实现高效用户权限授予与撤销。在随机预言模型下对方案的密文安全性、多层次访问安全性以及撤销安全性进行严格的安全性证明,并将所提方案进行了性能分析。

相关成果:“隐藏访问模式的高效安全云存储方案”,东北大学学报:自然科学版(EI收录)。

可搜索加密 广播加密 访问模式 细粒度访问控制

至今  
-2018年6月

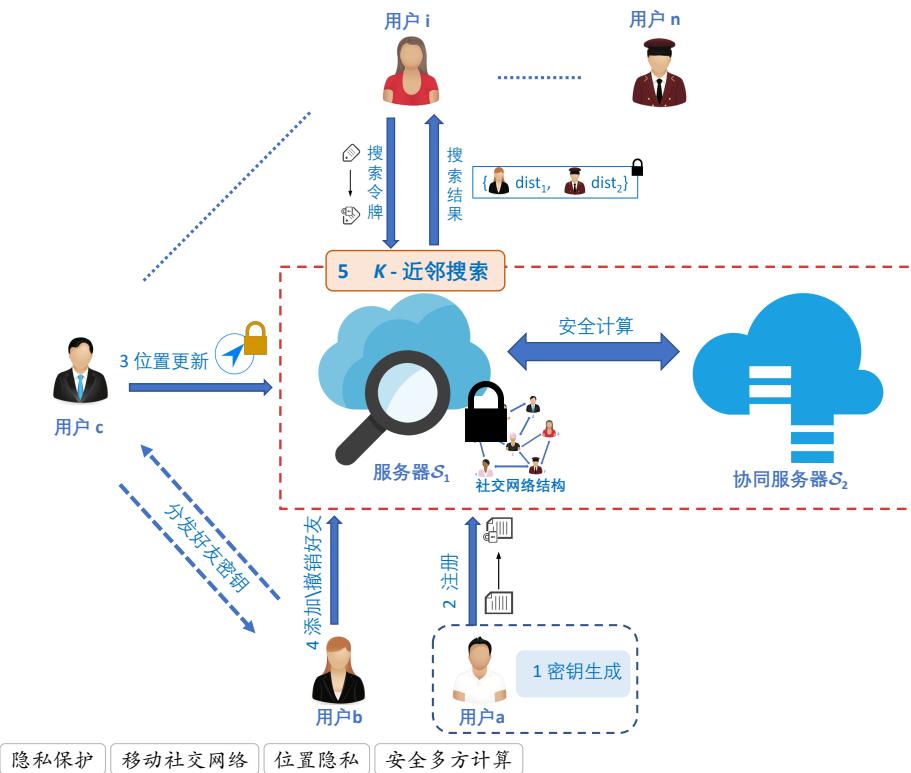
### 面向社交网络的隐私保护方法研究,东北大学,博士课题

尽管移动社交网络的服务能为用户带来诸多益处,但是由于用户的隐私信息脱离了其本地物理控制,因此用户无法对其信息的安全性和隐私性进行有效监控,也不能保证其是否被合法获取以及利用。而且,随着网络上信息的不断膨胀以及数据挖掘技术的快速发展,社交网络服务提供商和恶意敌手获取社交网络中人们的隐私信息越来越便利,因此,本课题主要研究面向社交网络的隐私保护方法。

#### > 移动社交网络隐私保护查询方法

针对移动社交网络的特征和用户位置隐私保护的多元需求,提出支持 $k$ -近邻搜索的社交网络隐私保护方案。针对用户位置隐私泄露问题,方案利用伪随机函数设计轻量级位置加密算法,构建安全可信的双服务器协同搜索架构,融合安全多方计算思想和同态加密机制设计面向位置密文的 $k$ -近邻搜索协议,在保护用户位置隐私的同时满足其近邻搜索需求。

相关成果:“Privacy-Preserving Friends Retrieval over Online Social Networks”, International Conference on Science of Cyber Security”,(EI收录);“支持 $k$ -近邻搜索的移动社交网络隐私保护方案”,计算机学报(在审)。



2015年9月  
-2014年7月

### 面向社交网络的隐私保护方法研究,东北大学,博士课题

#### > P2P社交网络隐私保护方法

针对用户的细粒度访问控制需求,设计面向P2P社交网络的隐私保护方法。为了实现高效的基于加密的访问控制机制,使其能够进行高性能的加解密而不受系统内个体数量影响,课题引入具有接收者匿名性的广播加密方案来实现P2P社交网络系统中的消息的加、解密与分发。在Android客户端设计与实现了关键算法及系统的功能模块,并对各模块进行了功能验证。验证结果表明该匿名广播加密算法在保证对用户数据进行分发同时,解决了已有P2P社交网络中依赖高代价匿名技术来对用户数据进行隐私保护或者用户权限的过度开放等问题,有效地保护了接收者的隐私性。

相关成果:“基于匿名广播加密的P2P社交网络隐私保护系统”,山东大学学报:理学版。

细粒度访问控制 P2P社交网络 隐私保护 匿名广播加密

2014年7月  
-2012年9月

### 电子现金系统设计,东北大学,硕士课题

在对现有电子现金系统进行理论研究与分析的基础上,围绕电子现金系统不足展开研究。为了实现成员的动态加入和群签名的可追踪性,中设计了一种新型的可追踪动态群签名方案,该方案基于BSZ安全模型,并采用Waters签名思想,实现群签名的匿名性和不可伪造性。在此群签名方案基础上,构建了一种在标准模型下具有CCA匿名性的公平离线电子现金系统,并对文中提出的电子现金系统的体系结构以及各个协议进行了详细描述,给出了标准模型下严格的安全性证明,证明其具有CCA匿名性、不可伪造性、可追踪性以及不可重复花费性等性质。最后,设计与实现了具有CCA匿名性的公平离线电子现金原型系统,与传统的电子现金系统相比,该系统在设计上实现了多银行结构,使得中央银行不必参与到每次发行现金中,因而可有效解决传统电子现金系统中的性能瓶颈问题。

相关成果:“The electronic cash system based on non-interactive zero-knowledge proofs”, International Journal of Computer Mathematics (SCI收录); “A Fair Off-line Electronic Cash Scheme with Multiple-Bank in Standard Model”, Journal of the Chinese Institute of Engineers(SCI收录)。

电子现金 动态群签名 非交互式零知识证明 Groth-Sahai证明技术

## 学术论文及专利

### 学术论文

- [1] **Li Yuxi**, Zhou Fucai, Zifeng Xu, Ge Yue. An Efficient Two-Server Ranked Dynamic Searchable Encryption Scheme[J], IEEE ACCESS, ISSN : 2169-3536; DOI : 10.1109/ACCESS.2020.2992773, (SCI收录, JCR一区, IF:4.96)
- [2] **Li Yuxi**, Zhou Fucai, Alex X Liu, Lin Muqing, Xu Zifeng, Integrity-Verifiable Conjunctive Keyword Searchable Encryption in Cloud Storage[J], International Journal of Information Security, 2018,17(5) :549-568. (密码学会推荐B类期刊, SCI收录, JCR二区, IF:1.683)
- [3] Zhou Fucai, **Li Yuxi**. The electronic cash system based on non-interactive zero-knowledge proofs[J], International Journal of Computer Mathematics,2016, 93(2) :239-257. (SCI收录, JCR二区, IF:1.054)
- [4] **Li Yuxi**, Zhou Fucai and Zifeng Xu. A Fair Off-line Electronic Cash Scheme with Multiple-Bank in Standard Model[J], Journal of the Chinese Institute of Engineers, 2019, 42(1) : 87-96. (SCI收录, JCR四区, IF:0.51)
- [5] **Li Yuxi**, Zhou Fucai, Zifeng Xu, PPFQ : Privacy-Preserving Friends Query over Online Social Networks, (Information Systems Frontiers 在审, JCR二区, IF:4.42)
- [6] Zhou Fucai, Lin Muqing, Zhou Yang and **Li Yuxi**. Efficient Anonymous Broadcast Encryption with Adaptive Security[J], KSII Transactions on Internet and Information Systems, 2015, 9(11), 4680-4700. (SCI收录, JCR三区, IF:0.71)
- [7] **Li Yuxi**, Zhou Fucai and Zifeng Xu. Privacy-Preserving Friends Retrieval over Online Social Networks, International Conference on Science of Cyber Security. Springer, Cham, 2019.(EI)

- [8] Zhou Fucai, **Li Yuxi**, Liu A X, et al. Integrity Preserving Multi-keyword Searchable Encryption for Cloud Computing[C], International Conference on Provable Security. Springer International Publishing, 2016: 153-172. (中国密码学会推荐 C 类会议, EI)
- [9] Zhou Fucai, Lin Muqing, Zhou Yang and **Li Yuxi**, Efficient Anonymous Broadcast Encryption with Adaptive Security[J], KSII Transactions on Internet and Information Systems, 2015, 9(11), 4680-4700. (SCI 收录, JCR 三区 , IF:0.71)
- [10] 李宇溪,周福才,徐剑,徐紫枫.双服务器模型下支持相关度排序的多关键字密文搜索方案[J].计算机研究与发展,2018,55(10):2149-2163. (EI)
- [11] 李宇溪,周福才,徐紫枫.隐藏访问模式的高效安全云存储方案[J].东北大学学报(自然科学版),2018,39(08):1086-1091. (EI)
- [12] 李宇溪,周福才,徐紫枫.支持 k- 近邻搜索的移动社交网络隐私保护方案,(计算机学报小修在审, EI)
- [13] Xu Zifeng, Zhou Fucai, **Li Yuxi**, Xu Jian, Qiang Wang. Private Subgraph Matching Protocol[C], Provable Security. 11th International Conference, ProvSec 2017, 2017.10.23-2017.10.25. (EI)
- [14] Zhou Fucai, Xu Zifeng, **Li Yuxi**, Xu Jian, Peng Su, Private Graph Intersection Protocol[C], 22nd Australasian Conference on Information Security and Privacy, ACISP 2017, 2017.7.3-2017.7.5. (CCF C 类 )
- [15] 吴淇毓,周福才,王强,李宇溪.可有效更新的低存储开销公共可验证数据库方案[J].计算机研究与发展,2018,55(08):1800-1808. (EI)
- [16] 徐紫枫,周福才,李宇溪,秦诗悦.支持邻接关系查询的图结构密文搜索方案[J].东北大学学报(自然科学版),2018,39(08):1092-1097. (EI)
- [17] 王恺璇,李宇溪,周福才,王权琦.面向多关键字的模糊密文搜索方法[J].计算机研究与发展,2017,54(02):348-360. (EI)
- [18] 柳璐,李宇溪,周福才.基于非交互零知识证明的匿名电子调查系统[J].网络与信息安全学报,2016,2(12):39-46.
- [19] 李宇溪,王恺璇,林慕清,周福才.基于匿名广播加密的 P2P 社交网络隐私保护系统[J].山东大学学报(理学版),2016,51(09):84-91.
- [20] 黄雪刚,高天寒,李宇溪.面向流式数据认证的变色龙认证树算法研究[J].四川大学学报(工程科学版),2016,48(02):139-144. (EI)
- [21] 王思飞,岳笑含,李宇溪,周福才.标准模型下可证安全的动态短群签名方案[J].东北大学学报(自然科学版),2013,34(08):1073-1077. (EI)

## 专利

- [1] 电子现金系统 CN201711346525.0 公开日：2017.12.15 周福才, 李宇溪, 徐紫枫, 柳璐, 秦诗悦
- [2] 一种云环境下抗访问模式泄露的盲存储方法 CN201711298089.4 公开日：2017.12.08 周福才, 李宇溪, 徐紫枫, 张鑫月, 张宗烨

## 参与科研项目

2019 年 1 月 至今	新型高效的可验证流模型及其关键技术研究(在研) 国家自然科学基金面上项目, 61872069
2019 年 1 月 -2018 年 1 月	基于结构化加密的密文搜索方法及安全性证明(已结题) 国家自然科学基金面上项目, 61772127
2018 年 1 月 -2013 年 3 月	公有云环境中具有机密性与鲁棒性的安全云存储系统研究(已结题) 沈阳市自然科学基金项目, F14-231-1-08

## ≡ 相关经历

在国际会议做过数次学术报告，曾受邀为 TIFS, IEEE access, Provsec 等国际有影响力期刊及会议评审论文，参与多个国家及省级科研项目，并多次参与国内外学术合作交流：

1. 2013 年 7 月 25-26 日，赴中国科学院信息工程研究所，参加安全协议研讨会并作报告“Electronic Casn Protocol Based on Non-interactive Zero Knowledge Proofs”。
2. 2015 年 10 月 17-19 日，赴西安参加第九届中国可信计算与信息安全学术会议，并作报告“Research on Chameleon Certification Tree Algorithm for Streaming Data Authentication”。
3. 2016 年 11 月 10-12 日，赴南京参加第十届可证明安全国际会议 (The 10th International Conference on Provable Security, ProvSec 2016)，并作学术报告“Integrity Preserving Multi-keyword Searchable Encryption for Cloud Computing”。
4. 2017 年 5 月 22 日 -6 月 2 日，赴广州参加第二届网络空间安全和隐私过国际暑期学校 (The 2nd International Summer School on Cyber Security and Privacy)，进行为期 10 天的学习交流。
5. 2018 年 7 月 8-11 日，赴意大利贝尔蒂诺罗参加 Second Workshop on Encryption for Secure Search and other Algorithms(ECCA2) 研讨会，与可搜索加密领域世界级专家学者进行深入讨论与交流。
6. 2019 年 8 月 9-11 日，赴南京参加第二届网络安全科学国际会议 (The 2nd International Conference on Science of Cyber Security, SciSec 2019)，并作学术报告“PAFR : Privacy-Aware Friends Retrieval over Online Social Networks”。

## ⊕ 兴趣爱好

跑步，书法，羽毛球，户外徒步