北京邮电大学博士研究生创新基金

申 请 书

论文题目：量子真随机的安全性分析

学生姓名：李丹丹

指导教师：温巧燕

申请基金级别：博四

所在学院：网络技术研究院

申请日期：2016.09-2017.06

北京邮电大学研究生院

一、基本情况

<table>
<tr><td>学　　号</td><td>2013010268</td><td>姓　　名</td><td>李丹丹</td><td>二级学科</td><td>密码学</td></tr>
<tr><td>指导教师</td><td>温巧燕</td><td>所在学院</td><td>网络技术研究院</td><td>联系电话</td><td>18811727660</td></tr>
<tr><td>学生类别</td><td colspan="3">普通博士生√　　直博生□</td><td>E-mail</td><td>lidandan648755486@126.com</td></tr>
<tr><td>博士论文选题</td><td colspan="5">量子真随机数的生成及安全性分析</td></tr>
<tr><td>课 题 来 源</td><td colspan="5">A、国家自然科学基金重大、重点项目
B、国家科技攻关项目
C、973 科技创新计划
D、863 项目
E、长江学者奖励基金
F、跨世纪优秀人才计划
G、其他<u>　　国家自然科学基金　　</u></td></tr>
<tr><td>预计完成时间</td><td colspan="2">2017.06</td><td colspan="2">申请经费总额（万元）</td><td>3</td></tr>
<tr><td>研究内容及意义摘要（限300字）</td><td colspan="5">随机性反映的是自然界的本质属性，同时，随机性是一种重要的资源，在许多方面都有广泛地应用，如物理系统和生物系统的数据模拟，赌博，密码学。特别的，密码学上量子秘钥分发协议的安全性依赖于态制备和测量的随机选择，这样一来，避免敌手利用某一种攻击得到安全的秘钥信息却不被发现。显然，研究随机数的生成具有深远的意义。
在实际应用中有诸多因素会影响到是否可以产生真随机数，进一步影响到产生随机数的量，这些可归结为随机数的安全性问题。主要研究的方面有：测量的选择是否随机，探测器的效率等等。</td></tr>
</table>

二、研究课题

1、论文选题的科学依据和意义（包括选题的科学意义，本课题国内外研究概况、发展水平和趋势，选题的总体思想及理论根据，并附主要参考文献及出处）

随机性反映的是自然界的本质属性，同时，随机性是一种重要的资源，在许多方面都有广泛地应用，如物理系统和生物系统的数据模拟，赌博，密码学。特别的，密码学上量子秘钥分发协议的安全性依赖于态制备和测量的随机选择，这样一来，避免敌手利用某一种攻击得到安全的秘钥信息却不被发现。显然，研究随机数的生成具有深远的意义。

目前国内外的研究现状：Colbeck 和 Kent 研究实验参与方利用 GHZ 测试，根据得到的测量结果来认证是真正的随机数产生。S.Pironio 等人基于 CHSH 型的 Bell 不等式认证真正随机性的存在，利用条件极小熵来刻画随机性的量。CHSH 不等式违背的经典界 2，就意味着输出结果有真正随机性的存在。Colbeck 和 Rener 在测量背景任意选择的条件下，利用链式 Bell 不等式违背，在实验参与方数量趋于无穷大时，得到观测随机性等于真正的随机性。R.Gallego 等人在仅限非超光速条件和测量背景的选择具有任意小的随机性的条件下，利用 Mermin 不等式达到非超光速的最大违背时，在实验参与方数量趋于无穷大时，得到的观测随机性等于真正的随机性。C.Dhara 等人在非超光速的条件和和测量背景的选择具有任意小的随机性的条件下，利用 Mermin 不等式达到非超光速的最大违背时，在实验参与方却只用有限个，观测的随机性等于真正的随机性。Clobeck 等人分两类来对此问题进行研究，其一，实验满足量子理论，满足非超光速理论，在对选择测量背景的随机源的随机量规定一个界时，利用链式 Bell 不等式，在实验参与方的数量趋于无穷时，测量输出的结果是真正随机比特，其二，实验满足非超光速理论，在对选择测量背景的随机源的随机量规定一个界时，利用链式 Bell 不等式，在实验参与方的数量趋于无穷时，测量输出的结果是真正随机比特。随后，R.Gallego 等人在满足非超光速的理论，随机源的随机性可任意小的条件下，利用 Mermin 不等式在实验参与方趋于无穷，达到最大非超光速违背时，测量结果产生真正的随机数。

综上所述，我们的研究论题无论从理论出发，还是从实际应用角度来看，都具有坚实的理论与实践依据。

[1] J. Kofler, T. Paterek, and C. Brukner, Phys. Rev. A 73,022104 (2006).

[2]M. Hayashi, K. Iwama, H. Nishimura, R. Raymond, and S. Yamashita, New J. Phys. 8, 129 (2006).

[3]R.Koenig, R. Renner, and C. Schaffner, IEEE Trans. Inf. Theory 55, 4337 (2009).

[4]S. Pironio, A. Acin, S. Massar, A. Boyer de la Giroday, D. N.Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A.Manning, and C. Monroe, Nature (London) 464, 1021 (2010).

[5]M. Pawłowski and M. · Zukowski, Phys. Rev. A 81, 042326(2010).

[6]R. Gallego, N. Brunner, C. Hadley, and A. Acin, Phys. Rev. Lett.105, 230501 (2010).

[7] M. J.W. Hall, Phys. Rev. Lett. 105, 250404 (2010).

2、研究的目标与主要内容

真正的随机数扩展，实际上，由于需要随机数做种子来得到更多的随机数，而随机数种子其主要是用于选择测量背景和随机抽取。目前，针对于真正随机数扩展的研究主要分为两大类：设备无关随机数扩展协议和半设备无关随机数扩展协议。首先，我们介绍一下设备无关随机数扩展协议的发展。已经了解了什么是随机数扩展，那么我们需要知道什么是设备无关，设备无关就是基于实验作最少的且必要的假设条件，一般的，对设备的内部构造不做任何假设。那么，为什么会考虑设备无关下随机数扩展呢？设备无关经常被强调敌手的应用，因为协议的正确性的认证不基于设备内部的工作原理，因为这个设备有可能是是敌手制造的。如果敌手被允许制造量子设备，他可以把自己的量子态与设备纠缠起来，那么，他可以通过测量自己的系统，得到一部分实验的测量结果。因此，设备的输出产生的随机性是关于敌手的量子边信息的。其次，若敌手预先知道采样设备的输入的部分信息，某种程度上，敌手可以预先规划设备使其模拟相应的违背。

设备无关所做的假设均是一些最基本的假设，如：设备满足量子理论，分开的设备之间不进行通信，设备的使用方可以利用保密随机信源，但是我们不对应用细节做任何假设，如：具体的量子态和测量算子，所定义的希尔伯特空间的维数。而实际问题中，我们也可以认为设备提供方是诚实的，关于输出随机性的结论依赖于整个生成过程的物理性质，可能也依赖于有敌手控制的外部的随机参数，如：所需的温度或电压。S.Pironio 等人基于 CHSH 型的 Bell 不等式如何认证真正随机性的存在，实验描述如下：首先，假设满足量子理论，满足 非超光速原理，满足测量选择完全随机。Alice 和 Bob 方各有两种可供选的测量，输出结果为 +1，-1。根据随机种子，Alice 和 Bob 决定选择何种测量，实验就相应的输出测量结果，当穷尽随机种子，实验就结束。 实验方就得到的了一个概率分布表，利用条件极小熵来刻画随机性的量。惊喜的发现，只要 CHSH 不等式违背的经典界 2，就意味着输出结果有真正随机性的存在。接着，作者利用半正定规划给出极小熵的下界，这个下界本身应该是基于最大的概率，但是实验次数有限，不能很好的刻画分布，进而研究平均的 Bell 不等式违背，而它又可以与平均观测的 Bell 不等式违背建立起联系，此论文首次给出认证随机性的方法，并给出量化随机性的合理途径，具有重要的意义和研究价值。自然界中存在两类随机性：一种是表面随机性，另一类是真正的随机性。而后者是我们的研究重点。而探求真正的随机性仅仅是通过观测的概率分布，这样，学者就会想到研究观测随机性与真正的随机性之间的关系。上面提到的所有文章，均是观测的随机性等于真正的随机性。Colbeck 和 Rener 在测量背景任意选择的条件下，利用链式 Bell 不等式违背，在实验参与方数量趋于无穷大时，得到观测随机性等于真正的随机性。R.Gallego 等人在仅限非超光速条件和测量背景的选择具有任意小的随机性的条件下，利用 Mermin 不等式达到非超光速的最大违背时，在实验参与方数量趋于无穷大时，得到的观测随机性等于真正的随机性。 C.Dhara 等人在非超光速的条件和和测量背景的选择具有任意小的随机性的条件下，利用 Mermin 不等式达到非超光速的最大违背时，在实验参与方却只用有限个，观测的随机性等于真正的随机性。

3、拟采取的研究方法和技术路线（包括拟采用的计算方法、实验方法及其可行性论证，可能遇到的问题及其解决办法）

论题的研究主要采取大量阅读优质文献，设问，交流和质疑等方式来进行，注重全面培养自己自主研究和独立思考，分析问题，解决问题的能力，培养自己的逻辑思维能力和团队协作精神。针对每一篇文献，仔细研究，对论文中出现的结论和疑惑进行分析和讨论，并在最后形成书面的材料，以便后续研究的查阅和巩固。对于最后遗留的疑难问题去集中放在讨论班上，在导师的协助下努力解决。查阅文献主要借助于计算机来完成，了解所研究领域的最新研究成果，关注相关方向的优秀团队的研究动向。同时，实验室为我们提供了宝贵的对外交流的机会，积极组织学生去参加相关的会议，我们也会很珍惜这样的机会，在会后主动积极与研究方向相关或相近的专家，学者交流，尽量请专家为我们的研究提出宝贵的建议和意见，我们也会结合自身实际情况加以改正。

在我们研究文献的时候，可能会存在一些问题，如并没有从整体上把握住作者的研究思路，并未深入了解到作者的本质意图，可能仅仅是停留把文章表面东西看懂的层面。更严重的可能是，作者为什么会这样那样考虑，我们却不知道为什么这样。同时，在研究文章中会遇到一些比较基础性的内容，它是上层内容的坚实基础，是展开其他研究工作的底层，但是对这一类的内容却把握的很少，这样很不利于以后的研究。另外，在研读文章的时候，我们会发现作者会利用不同的软件画一些图，而着一些绘图软件，线性规划软件，半正定规划的软件，基于数学复杂计算的软件，我们掌握并非很熟练，针对以上存在的问题，积极加以改正。

4、本项目的特色和创新之处

该项目的研究内容关注的近些年的热点问题，课题的展开本着具有应用价值的思想进行研究，考虑产生随机性的效率和一些实际实验当中的情形，使得随机性的效率尽可能的大，研究的情况更贴合实际操作当中遇到的问题。

5、已具备的研究基础（包括已取得的研究成果、发表的学术论文或获奖情况以及已具备的研究条件，成果、论文或获奖须列出全部作者，若发表的学术论文涉及的期刊统计了影响因子，请注明刊载当年的影响因子，并注明其索引或数据库名称）

1，*Security of Semi-Device- Independent Random Number Expansion Protocols,* ***Dan-Dan Li****, Qiao-Yan Wen, Yu-Kun Wang, Yu-Qian Zhou, Fei Gao Sci. Rep.* ***5****, 15543; doi: 10.1038/srep15543 (2015).* ***SCI****, 二区, 影响因子：5.578.*

2，*Effects of measurement dependence on generalized Clauser-Horne-Shimony-Holt Bell test in the single-run and multiple-run scenarios* ***Dan-Dan Li***，*Yu-Qian Zhou, Fei Gao, Xin-Hui Li, Qiao-Yan Wen*，*PHYSICAL REVIEW A* ***94****, 012104 (2016).* ***SCI****,二区, Top 类期刊, 影响因子：2.808*

3， *Linear Complexity of Generalized Cyclotomic Quaternary Sequences with Period pq,* ***Dan-Dan Li,*** *Qiao-yan Wen, Jie Zhang, Zu-ling Chang, IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences Vol.E97-A No.5 pp.1153-1158, (2014).* ***SCI***

4*, Linear complexity of generalised cyclotomic quaternary sequences of length 2p^{m+1}q^{n+1},* ***Dan-dan Li,*** *Zu-ling Chang, Qiao-yan Wen, Jie Zhang, IET Information Security, Volume 10, Issue 2, March 2016, p. 104 – 111.* ***SCI***

5*, Linear Complexity of Generalized Cyclotomic Binary Sequences with Period 2p^{m+1}q^{n+1},* ***Dan-dan Li****, Qiaoyan Wen, Jie Zhang, Liying Jiang, IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences Vol.E98-A No.6 pp.1244-1254, (2015).* ***SCI***

荣获优秀党员， 南都企业奖学金， 校级优秀研究生。

6、预期研究成果

成果形式 （论文、专著、专利等）	学术论文形式须注明预期被 SCI 检索数及刊载期刊的影响因子 至少发表一篇高质量的论文，SCI 检索，二区。
成果内容	对影响真随机数安全性的因素进行分析，比如探测器效率，对设备的输入不是完全随机的等，研究这些因素对真随机性的安全性造成怎样的影响。

7、进度安排

2016.9-2016.10 阅读文献，给出初步研究结果
2016.11-2016.12 写文章
2017.01-2017.02 修改文章，并投文章
2017.03-结题　探究其他研究点

8、申请者承诺

我保证上述填报内容的真实性。如果获得资助，我严格遵守学校有关规定，切实保证研究工作时间，按计划认真开展研究工作，按时报送有关材料，按时完成研究项目。

申请人签字：

年　月　日

9、经费预算及其它经费来源

<table>
<tr><td rowspan="7">经费预算</td><td>支出项目</td><td>每月标准（元）</td><td>发放月数</td><td>金额（万元）</td></tr>
<tr><td>生活补贴</td><td>3000</td><td>10</td><td>3</td></tr>
<tr><td>支出项目</td><td colspan="2">计算根据及理由</td><td>金额（万元）</td></tr>
<tr><td>论文版面/知识产权事务费</td><td colspan="2"></td><td></td></tr>
<tr><td>会议费和京外差旅费</td><td colspan="2"></td><td></td></tr>
<tr><td>资料耗材费</td><td colspan="2"></td><td></td></tr>
<tr><td>交通费和通信费</td><td colspan="2"></td><td></td></tr>
<tr><td rowspan="4">其它经费来源</td><td colspan="2">项目名称</td><td>来　源</td><td>金额（万元）</td></tr>
<tr><td colspan="2"></td><td></td><td></td></tr>
<tr><td colspan="2"></td><td></td><td></td></tr>
<tr><td colspan="2"></td><td></td><td></td></tr>
</table>

10、指导教师推荐意见（请导师认真负责地介绍申请人的业务基础、研究能力、科研态度及研究条件和保证等）

申请人在博士阶段中一直致力于研究随机数问题，对相关问题做了较深入的探索，具备了一定的研究基础。该申请人已经以第一作者身份发表 SCI 论文 5 篇，二区论文 2 篇，多次参加国际，国内研讨会，在学术上取得了长足的进步。

该申请人具有良好的科研态度，刻苦勤奋，对相关领域的研究充满热情，能够保证充足的科研时间。实验室目前的条件足以支撑申请人完成本项目。如果项目申请成功，实验室将为申请人顺利完成项目提供所有必要的支持。

博士生导师（签名）：

年　　月　　日

三、审批意见

学院推荐意见
经审核，本表填写的内容真实可靠，同意推荐该生参加博士创新基金资助选拔。 主管院长（签字）： 年　　月　　日　　（公章） 年　月　　日
学校审批意见
是否同意基金资助：　　建议资助金额：_____元 研究生院负责人（签字）： （公章） 年　　月　　日
评审未通过原因：1.选题不当，不符合资助条件；2.项目论证不充分；3.申请人的素质或水平不宜承担此项目；4.预期研究成果不明确；5.不具备完成本项目的其他条件；6.其他原因（加以说明）：

北京邮电大学博士研究生创新基金

申 请 书

论文题目：内容中心无线网络中动态自适应流媒体的服务提供机制研究

学生姓名：南国顺

指导教师：乔秀全

申请基金级别：博四基金

所在学院：网络技术研究院

申请日期：2016 年 9 月 8 日

北京邮电大学研究生院

一、基本情况

<table>
<tr><td>学　　号</td><td>2013010281</td><td>姓名</td><td>南国顺</td><td>二级学科</td><td>网络理论与技术</td></tr>
<tr><td>指导教师</td><td>乔秀全</td><td>所在学院</td><td>网络技术研究院</td><td>联系电话</td><td>13810617220</td></tr>
<tr><td>学生类别</td><td colspan="3">普通博士生□　　直博生□</td><td>E-mail</td><td>nanguoshun@163.com</td></tr>
<tr><td>博士论文选题</td><td colspan="5"></td></tr>
<tr><td>课 题 来 源</td><td colspan="5">A、国家自然科学基金重大、重点项目
B、国家科技攻关项目
C、973 科技创新计划
D、863 项目
E、长江学者奖励基金
F、跨世纪优秀人才计划
G、其他_____</td></tr>
<tr><td>预计完成时间</td><td colspan="2">2017 年 5 月</td><td colspan="2">申请经费总额（万元）</td><td>3 万元</td></tr>
<tr><td>研究内容及意义摘要（限 300 字）</td><td colspan="5">根据 Cisco 预测，未来 5 年移动应用及流量将产生爆炸式的增长，其中视频将占据无线流量的 75%，因此移动互联网承载的业务模式将由传统的以文本、语音为主转向以内容分发等视频为主的发展态势，现有的 TCP/IP 体系结构在支撑这些以内容为中心应用（如视频、文件共享）上也面临许多挑战，如扩展性、动态性等问题。因此，迫切需要研究未来互联网体系结构及服务运行机理。本课题将研究内容中心无线网络 CCWN (Content-Centric Wireless Network）中动态自适应流媒体 DAS(Dynamic Adaptive Streaming)服务提供机制，内容中心无线网络将 TCP/IP 网络协议的细腰从 IP 转换到命名的数据对象，实现内容与位置的分离、网络缓存、多播等机制，可以满足网络内容的分发，移动内容的边缘缓存等需求。内容中心无线网络带来了全新的网络协议和运行机制，同时也给上层应用提供了全面的挑战和机遇，本文将研究新型内容中心无线网络中动态自适应流媒体服务的提供机制及优化策略。</td></tr>
</table>

二、研究课题

1、论文选题的科学依据和意义（包括选题的科学意义，本课题国内外研究概况、发展水平和趋势，选题的总体思想及理论根据，并附主要参考文献及出处）

1.1 研究背景和科学意义

互联网已经成为信息社会的最重要基础设施，随着智能手机、Pad等设备的普及，移动互联应用和流量产生了爆炸式的增长 [1]，移动网络承载主要业务从短信、语音转变为以内容为中心的新型应用如视频，文件分享等 [2]。移动应用和计算模式的丰富促使移动互联网接入方式和网络功能定位发生了巨大的改变，从而导致以IP地址为核心、已传输为目的、按照端到端原理设计的TCP/IP网络在扩展性、移动性、可靠性等方面的问题日益突出。迫切需要研究新型的未来互联网体系结构及服务机理 [3][4]。

近几年，国际上开始以革命式路线研究未来互联网体系结构[5][6]，2014年5月12日，NSF宣布对命名数据网络（Named Data Networking，NDN），移动优先（ MobilityFirtst），XIA（eXpressive Internet Architecture）三个项目继续资助1500万美元进行下一阶段的实验部署和测试（强调要From Architecture and Protocol Design to Advanced Services and Trial Deployments）。欧盟在FP7框架下，2007年启动了FIRE（Future Internet Research and Experimentation）计划，采用的是一种实验驱动的未来互联网研究方。进行互联网体系创新，抓住未来互联网全新设计这一战略机遇，是技术发展的必然趋势，也是国家的重大战略需要。

内容中心无线网络(Content-Centric Wireless Networking，CCWN) [2] 就是一种以命名数据对象（Named Data Object，NDO）为中心的革命性的全新无线互联网架构，内容中心无线网络是内容中心网络（Content-Centric Networking，CCN）[3] 在无线网络上的进一步扩展。内容中心无线网络提出将互联网协议栈的细腰从 IP 地址转换为命名数据对象，实现基于命名的内容查找和路由。内容中心无线网络实现了内容与位置的分离，网络内置缓存、多播等功能，从而更好满足大规模网络内容分发、移动内容存取、网络流量均衡等需求。

网络是基础、服务是关键。然而，这种全新的网络带来了全新的网络协议和全新的运行机制，给现有的服务提供带来了前所未有的挑战，更好的支撑上层的应用和服务是未来网络设计的主要目标。在无线网络中，视频业务已经成为最重要的一类基础服务，因此如何高效的支持视频应用是任何新型网络成功的关键。为了深入系统的研究全新内容为中心的网络中的服务提供机制，**申请人提出并实现了基于内容中心网络的浏览器 NDNBrowser [7]和服务器 CCNxTomcat [8] 原型系统，分别在浏览器和服务器内核层实现和优化了内容中心协议，解决了未来网络实用化推广的两个关键问题：用户接入和服务部署[9][10]，用户可以在 NDNBrowser 上通过内容中心网络观看部署 CCNxTomcat 服务器上的视频。在此基础上，申请人实现了基于内容中心无线网络的流媒体播放系统 CCNVideo，CCNVideo 系统可以在内容中心无线网络中通过移动端 VLC 视频播放器观看北邮 IPTV 的视频节目，从而解决了 TCP/IP 网络中的真实数据流量到内容中心无线网络的导入问题。同时，申请人提出了内容中心无线网络中移动终端的视频播放的节能算法[11]，利用马尔科夫决策模型，在不影响用户体验的前提下实现移动端能量节约的最大化。基于前期的研究基础，本课题将继续研究视频服务中非常重要的动态自适应流媒体 DAS(Dynamic Adaptive Streaming) [12]，** DAS 根据视频播放器的本地缓存、以及网络层的可用带宽来动态的调整视频码率，从而在动态网络可用带宽的环境中保证视频的流畅播放。在基于 TCP/IP 协议的无线网络中，针对 DAS 在 HTTP 协议之上的服务提供机制已经有系统深入的研究， 即 DASH (Dynamic Adaptive Streaming over HTTP) [12][13]。在内容中心无线网络中，目前仍然缺乏对动态自适应流媒体服务机制的深入系统化的研究，未来网络的快速发展将会产生一个全新并具有创新性的服务市场，因此，在全新的内容中心无线网络结构下，研究符合新网络服务提供机制及优化策略将具有重要的意义，本课题将基于以内容为中心的动态自适应流媒体服务为实例进行研究。

1.2 国内外研究现状和存在的问题

1.2.1 内容中心无线网络中动态自适应流媒体对网络层内容的感知问题

对于动态自适应流媒体服务，影响用户体验的[14]主要评价指标包括视频码率、码率抖动、卡顿时间、卡顿次数、启动时延，用户体验将会直接影响用户是否继续观看或者放弃，这对内容提供商来说至关重要，在基于 TCP/IP 的无线网络中，运行在 HTTP 协议上的动态自适应流媒体应用是由客户端驱动的，在服务器端，视频编码成通过不同码率的固定时长的分段[12][13]，客户端通过 HTTP 协议的 Get 请求，根据本地播放器的缓存大小、网络的可用带宽信息来动态调整可以下载的码率，从而保证视频播放的流畅度，减少缓存的饥渴而造成的视频卡顿，研究表明，视频卡顿是影响用户体验最关键的因素，对于 90 分钟的视频，每增加 1%的卡顿时间，用户的平均观看的时间将会减少至少 3 分钟 [14]，同时，应用程序在视频的启动阶段和卡顿等待阶段会选择最低的视频码率，从而使用户等待的时间最短。在基于 TCP/IP 协议栈的无线网络中，应用程序在网络层只关注其端到端的可用带宽，而在内容中心无线网络中，由于请求视频内容分段可能缓存在网络的不同位置，而不同位置上缓存中内容的分布与视频的内容流行度有极大的关系，所以动态自适应流媒体服务的用户体验与内容的流行度以及缓存的动态性有密切的联系，现有基于内容中心无线网络中动态自适应流媒体服务研究主要集中在缓存内容的置换策略、缓存大小设置及部署策略、以及路由器的自适应转发策略，通过对网络层的优化来提升用户体验，如获得更高的码率、更少的抖动及卡顿等 [15][16]，但在应用层依然使用 TCP/IP 网络中的码率适配策略，**应用层缺乏对网络层内容动态性的感知**，这会造成如下两个问题：

1）如果根据播放器的本地缓存大小进行码率适配[13] （如图 1 所示），当本地缓存较小时请求较低的视频码率，而采用这种适配策略的前提仍然是所有码率都是相同的网络吞吐量，显然在内容中心无线网络中是不成立的，所以无法适配出最优码率。

2）如果根据历史的网络吞吐量进行码率适配[13] （如图 1 所示），根据历史的网络吞吐量预测当前的吞吐量，采用这种适配策略的前提是客户端到服务器的端到端是可靠的 TCP 连接，所请求片段的不同码率部署在同一个服务器端，所以其端到端的网络吞吐量是可以预测的，但是在内容中心无线网络中，连接模式是完全是无状态的，每次请求的路由是独立的，网络中可以服务的节点是分布式的，因此不能简单采用传统的基于历史吞吐量适配策略。

因此，在新型的内容中心无线网络中，研究一种符合新网络的全新的动态自适应流媒体服务优化机制是非常有必要的。

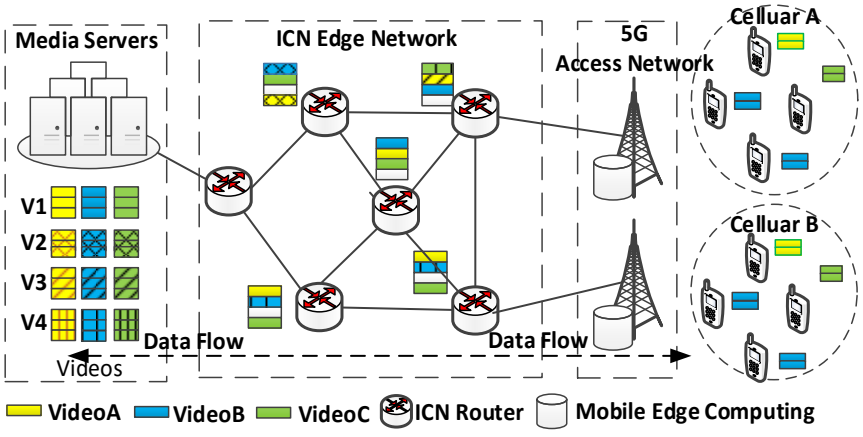

图 1：内容中心无线网络中动态自适应流媒体服务实例

1.2.2 内容中心无线网络中动态自适应流媒体服务和片段向网络边缘按需迁移问题

典型的动态自适应流媒体应用由静态内容（如视频、音频、图片等）、无状态计算服务（如视频转码、图片格式转换等）、有状态服务（如后台数据库查询）和用户数据（用户的基本信息）组成。不同的数据可以利用内容中心无线网络的分布式缓存、数据命名，以用户驱动的方式向网络边缘移动，因此内容无线中心网络为动态自适应流媒体服务的提供了一种全新的分布式运行和部署的可能性，在 TCP/IP 网络中，内容分发网络(CDN)可以实现服务及数据向用户边缘的部署，但是 CDN 只是部署在靠近用户的数据中心，在用户端和 CDN 数据中心之间仍然会有大量的重复数据。近几年，随着终端能力的增强，“ 边计算 ”(Edge Computing) 的思想开始逐渐受到关注[17]，特别是随着 4G/5G 的研究加速，移动边缘计算（Mobile Edge Computing，MEC）开始逐渐引起了产业界和标准化组织的重视[18]，然后现有的关于移动边缘计算的讨论主要还是依赖于 TCP/IP 技术，在网络层面还没深入涉及到与内容中心网络的结合。

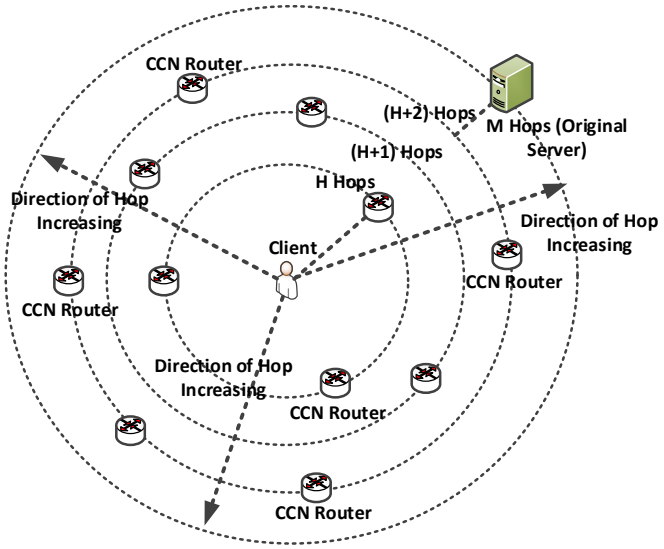

图 2： 内容中心无线网络内容及服务向网络层的按需迁移

内容中心无线网络具有网内缓存和基于名字的路由机制，基于名字的路由实现了内容和位置的分离，而分布式的网内缓存使得内容可以就近的为用户提供服务，用户可以根据内容名字从网络中请求想要的内容，而在 TCP/IP 网络中，网络层只能实现基于地址无语义的路由转发。由于内容中心无线网络的路由节点中带有缓存，内容经过路由节点时就会按一定的策略被缓存，当下次有同样的请求到达路由节点时，便可直接从缓存中取出，采用了“ 存储换带宽 ”的方式，从而避免了相同内容在网络中的重复传输，减少了网络流量，而且降低了服务器的负载和服务的响应时延。可以看出，现有的内容中心无线网络设计原理使得视频内容从应用层下沉到网络层，由于内容中心无线网络的节点中带有缓存，内容在传输过程中不断的被缓存下来，所以原来由服务器提供的内容不断向网络中迁移，用户可以在更近的地方获取到需要的内容，然而，当前内容中心无线网络中动态自适应流媒体或者流媒体的研究重点在缓存策略的研究，同时已经实现了视频内容在网络中的迁移，或者根据流行度进行提前的下载，就近的为用户提供服务，**而对应用状态驱动的视频内容和服务的按需迁移问题缺乏深入研究**（如图 2 所示），传统的方法会产生如下问题：

1）海量的视频数据会造成非常低的网络层节点缓存命中率 [19]，现有的缓存策略对内容中心无线网络视频服务的优化有限。

2）现有的机制下，当动态自适应流媒体服务在发生卡顿时，网络层无法感知应用层的状态，也无法提前采取措施，比如将合适的码率下载到边缘端从而降低视频卡顿的概率。

3）对于动态自适应流媒体，如果采取传统的基于内容流利度的提前预取或者迁移方案，同样分段的不同码率可能需要在路由器缓存中保存多份，这将会极大的浪费路由器宝贵的缓存空间，如果可以结合移动接入网络“边计算”的优势，将码率转换服务从视频服务器端按需迁移到边缘服务器，那么也将极大的提升缓存利用率，在边缘为用户提高各种码率选择，极大的提升用户体验。

因此，在新型的内容中心无线网络中，**研究应用状态驱动的视频内容和服务的按需迁移问题，结合未来移动接入的“边计算”技术，可以很大程度上提升服务质量及用户体验。**

1.3 总结

综上分析，内容中心无线网络是一种与现有 TCP/IP 网络完全不同的全新的网络体系结构，其以“内容为中心”的设计理念非常适合于流媒体业务的需求，网络是基础，服务和关键，随着智能手机、Pad 等设备的普及，以流媒体为代表基于内容的业务将占据互联网的主流，内容中心无线网络可以很好的解决 TCP/IP 网络面临的诸多问题，同时也带来了全新的挑战和机遇。在前期的研究基础之上，本课题拟对内容中心无线网络中动态自适应流媒体业务所面临的以下两个问题进行深入系统化的研究，①**研究内容中心无线网络中动态自适应流媒体对网络层内容的感知问题　②研究内容中心无线网络中动态自适应流媒体服务和片段向网络边缘按需迁移问题。**

我们在调研时发现还没有与以上两个研究点完全相同的研究成果发表。

1.4 主要参考文献

[1] Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2015-2020. [Online]. Available: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual networking-index-vni/mobile-white-paper-c11-520862.html

[2] R. Wang, X. Peng, J. Zhang, and K. B. Letaief, “Mobility-aware caching for content-centric wireless networks: modeling and methodology,” IEEE Communications Magazine, vol. 54, no. 8, pp. 77–83, August 2016.

[3] G. Xylomenos, C. Ververidis, V. Siris, et al., A survey of information centric networking research, IEEE Communications Surveys & Tutorials. vol. 16, no. 2, 2013, pp.1024–1049.

[4] V. Jacobson, D. K. Smetters, J. D. Thornton, et al. Networking Named Content. Communications of the ACM. 2012, vol. 55, no. 1, pp.117–124.

[5] A. Feldmann. Internet clean-slate design: what and why?. ACM SIGCOMM Computer Communication Review, 2007, vol.37, no. 3, pp. 59-64.

[6] J. Rexford, C. Dovrolis. Future Internet architecture: clean-slate versus evolutionary research. Communications of the ACM, 2010, vol.53, no. 9, pp. 36-40.

[7] Xiuquan Qiao, Guoshun Nan, Yue Peng, Lei Guo, Jingwen Chen, Yunlei Sun, and Junliang Chen. 2014a. NDNBrowser: An extended web browser for named data networking. Journal of Network and Computer Applications, Vol. 50, April, 2015, pp.134-147.

[8] Xiuquan Qiao, Guoshun Nan, Wei Tan, Lei Guo, Junliang Chen, Wei Quan, and Yukai Tu. 2014b. CCNxTomcat: An extended web server for Content-Centric Networking. Computer Networks , vol.75, Part A (Dec. 2014), pp.276–296.

[9] Guoshun Nan, XiuQuan Qiao, Yukai Tu, Wei Tan, Lei Guo, JunLiang Chen. Design and Implementation: the Native Web Browser and Server for Content-Centric Networking. ACM SIGCOMM Computer Communication Review, vol.45, no.5, October, 2015, pp.609-610.

[10] Guoshun Nan, XiuQuan Qiao, Yukai Tu, Wei Tan, Lei Guo, JunLiang Chen. Design and Implementation: the Native Web Browser and Server for Content-Centric Networking. ACM SIGCOMM 2015 Poster, London, United Kingdom, August 17-21, 2015, pp.609-610.

[11] Guoshun Nan, XiuQuan Qiao, Junliang Chen, A Popularity-aware Prefetching Using MDP for Wireless Video Streaming over Information-Centric Networks,accepted by International Conference on Cloud Computing and Intelligence System(CCIS 2016), August 2016

[12] Stockhammer T. Dynamic adaptive streaming over HTTP--: standards and design principles[C]//Proceedings of the second annual ACM conference on Multimedia systems. ACM, 2011: 133-144.MLA

[13] Thang T C, Le H T, Pham A T, et al. An evaluation of bitrate adaptation methods for HTTP live streaming. IEEE Journal on Selected Areas in Communications (JSAC), 2014, 32(4): 693-705.

[14] F. Dobrian, V. Sekar, A. Awan, I. Stoica, D. Joseph, A. Ganjam, J. Zhan, and H. Zhang, "Understanding the impact of video quality on user engagement," ser. SIGCOMM '11. New York, NY, USA: ACM, 2011, pp. 362–373.

[15] S. Lederer, C. Mueller, C. Timmerer, and H. Hellwagner, "Adaptivemultimedia streaming in information-centric networks," IEEE Network,vol. 28, no. 6, pp. 91–96, Nov 2014.

[16] Y. Liu, J. Geurts, J. C. Point, S. Lederer, B. Rainer, C. Mller, C. Timmerer,and H. Hellwagner, "Dynamic adaptive streaming over ccn: A caching and overhead analysis," in Communications (ICC), 2013 IEEE International Conference on, June 2013, pp. 3629–3633.

[17] P. Garcia Lopez, A. Montresor, D. Epema, et al. Edge-centric Computing: Vision and Challenges. Acm Sigcomm Computer Communication Review, 2015, vol.45, no.5, pp.37-42.

[18] Mobile-Edge Computing – Introductory Technical White Paper, http://www.etsi.org/ technologies-clusters/technologies/mobile-edge-computing, September 2014

[19] Sun Y, Fayaz S K, Guo Y, et al. Trace-driven analysis of ICN caching algorithms on video-on-demand workloads[C]//Proceedings of the 10th ACM International on Conference on emerging Networking Experiments and Technologies. ACM, 2014: 363-376.

2、研究的目标与主要内容

2.1 研究内容

针对内容中心无线网络中动态自适应流媒体业务的服务提供所面临的上述问题，本项目拟开展以下几个方面的研究：

2.1.1 内容中心无线网络中动态自适应流媒体对网络层内容的感知问题。

内容中心无线网络具有分布式的缓存、命名数据包的机制，视频的内容可以缓存在网络中，并根据数据的名称对其进行索引查询，对于动态自适应流媒体业务，由于各个分段的不同码率的内容具有不同的命名，应用层可以感知边缘网络层是否有其需要的数据，对于动态自适应流媒体，传统的 TCP/IP 网络的应用层码率适配方案基于本地缓存大小和历史网络吞吐量，无法直接使用在内容中心无线网络中，因此本课题拟在新型内容中心无线网络中环境下，研究一种符合新型网络特点的动态自适应流媒体服务优化机制，实现最大化视频质量、最小化抖动和视频卡顿等关键的用户体验评价指标，**具体包括以下几方面的研究内容：①以内容中心网络的新特征为出发点，以网络与服务融合运行为主线，分析服务的组成元素，研究内容中心无线网络中动态适应流媒体的业务特征，系统深入的研究新型网络架构下服务的提供机制的不同；②：在新型的网络体系架构下，研究动态适应流媒体对网络内容的高效感知机制，为移动用户提供更好的服务体验； ③：基于应用层的感知机制研究，进一步研究新型网络体系架构下动态适应流媒体最优的码率适配策略。**

2.2.2 内容中心无线网络中动态自适应流媒体服务和片段向网络边缘按需迁移问题

内容中心无线网络具有网内缓存的功能，内容可以按相应的策略缓存到更靠近用户的路由器节点上。因此，原来由服务器提供的内容开始向网络中迁移，用户可以在更近的地方获取到需要的内容。移动边缘计算技术可以实现服务向边缘网络的迁移。针对动态自适应流媒体服务，视频内容可以向网络边缘的路由器缓存迁移，而本身部署在视频服务器端的码率转换服务可以迁移到边缘的基站服务器上，从而实现内容中心无线网络和边缘计算的融合，实现存储资源与计算资源的优势互补，从而极大的提升动态自适应流媒体的用户体验，然而目前缺乏针对无线中心网络中如何结合边缘计算实现自适应流媒体服务和片段向网络边缘按需迁移问题的深入研究。因此，本课题拟在无线中心网络环境中，研究一种符合新网络特点的全新的分布式服务提供机制，使得内容和服务也可以按需的迁移到更靠近用户的网络边缘，从而进一步提高缓存利用率，降低网络延迟，减少网络带宽的损耗，具体包括以下几个方面的研究内容：**①:研究一种应用层与边缘节点之间状态的高效交互机制，应用层可以获取并感知边缘网络的内容，同时边缘节点也可以获知并预测到应用的状态，如果视频卡顿的发生，从而采取提前措施 ②:研究一种应用状态驱动的视频内容和服务的预取方案，将码率转换服务从视频服务器端按需迁移到边缘服务器，在边缘节点只缓存高码率的视频分片，从而提高缓存利用率。**

2.2 研究目标

针对内容中心无线网络中动态自适应流媒体业务的服务提供所面临的上述问题，本课题拟的**研究目标如下**：

1）建立内容中心无线网络中动态自适应流媒体的服务优化框架，以有效的支撑以内容为中心的未来移动互联网服务提供模式。

2）提出内容中心无线网络中动态自适应流媒体服务对动态网络内容的感知算法，解决传统方法在应用层码率适配时所造成的用户体验下降问题。

3）探索内容中心无线网络中动态自适应流媒体服务在边缘网络的缓存分布特征，以及移动边缘计算的服务提供模式，提出应用状态驱动的内容及服务的迁移方法和本地化运行机制，解决内容中心无线网络中动态自适应流媒体服务和片段向网络边缘按需迁移问题。

3、拟采取的研究方法和技术路线（包括拟采用的计算方法、实验方法及其可行性论证，可能遇到的问题及其解决办法）

3.1 研究方法

1）课题组将认真研究内容中心无线网络已有的相关标准提案，密切关注国际标准组织（如IETF）和国内外未来网络相关研究项目的最新研究动态和发展方向，积极参与同领域的国际学术会议（如 Sigcomm，ICN 等），掌握国际最新研究动态，充分利用国内外的最新研究成果，确保本课题研究活动的先进性。

2）基于在内容中心无线网络方面的已有研究基础，结合服务计算领域和动态自适应流媒体领域最新的研究成果，应用“ 实验驱动+系统验证 ”的方法来研究适合于新型内容中心无线网络特点的动态自适应流媒体服务提供机制。

3）本课题将充分借鉴“ 边计算 ”（Edge Computing）的思想，将部分计算功能迁移到网络边缘，研究从现有的“ 在应用层集中提供服务 ”的动态服务提供模式向分布式的服务运行模式的转变机制。

4）采用理论与实践相结合的方法，综合应用数学模型分析、计算机仿真、系统实验验证等手段研究得出的模型和方法，并尽可能的通过未来网络试验床的真实网络环境来进行验证，确保理论研究的正确性和方法的可行性。

3.2 技术路线、实验手段

针对研究内容，本课题拟采取以下的总体研究方案（如图 3 所示）来展开研究：分三个层面，分别是理论及方法研究、仿真和模拟验证、原型系统开发及应用验证。

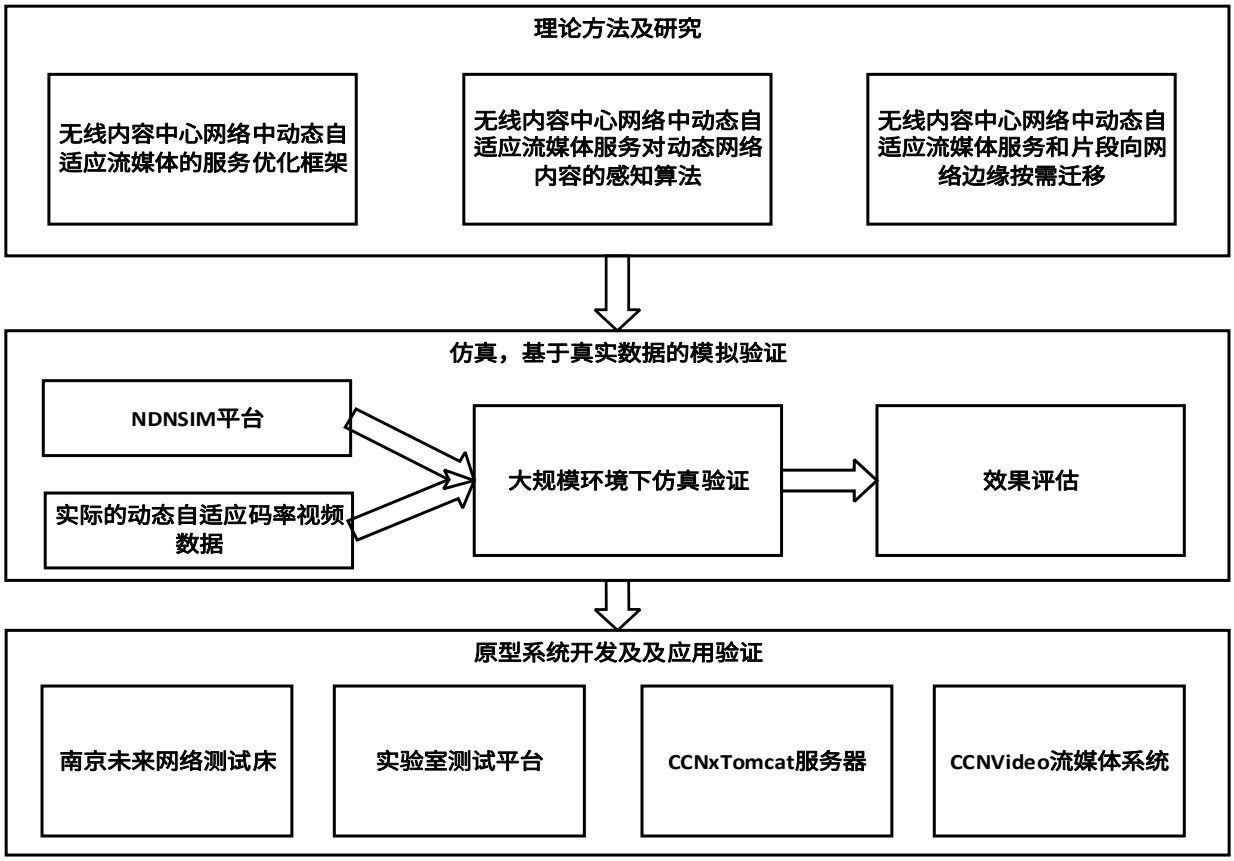

图 3：总体研究方案

具体的研究思路如下：

3.2.1 理论方法研究：

内容中心无线网络是一种完全不同于 TCP/IP 网络的体系架构，全新的网络架构带来了全新的应用上的挑战。本课题将研究内容中心无线网络中动态自适应流媒体服务提供机制和优化策略，理解新型网络体系结构中流媒体服务的流量特征，提出新型网络体系结构下服务模式；结合分布式缓存及命名数据的网络特征，研究网络层内容的高效感知算法；基于移动边缘计算，研究应用状态驱动的服务和内容按需向网络边缘的移动模型。本课题的研究场景如图 4 所示。

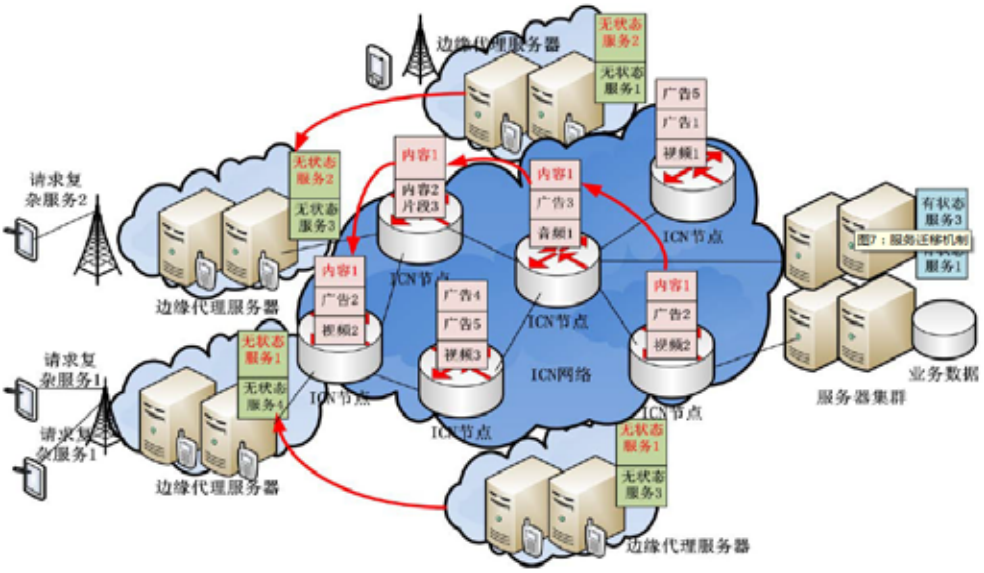

图 4：基于移动边缘计算的内容中心无线网络动态自适应流媒体服务

3.2.2 仿真平台部署实现：

基于理论研究中的模型及算法，本课题拟在内容中心无线网络的仿真平台 NDNSIM 上进行实现并且部署运行，研究大规模仿真环境下服务提供机制、内容感知算法、以及内容和服务移动模型的性能，并进行迭代优化。其中仿真拓扑示例如图 5，内容中心无线网络中动态自适应流媒体服务的仿真系统框架如图 6 所示。

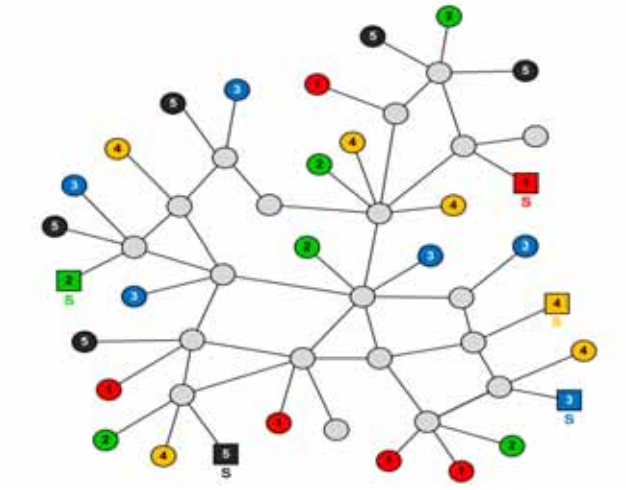

图 5：仿真实验拓扑（其中正方形节点是流媒体服务器）

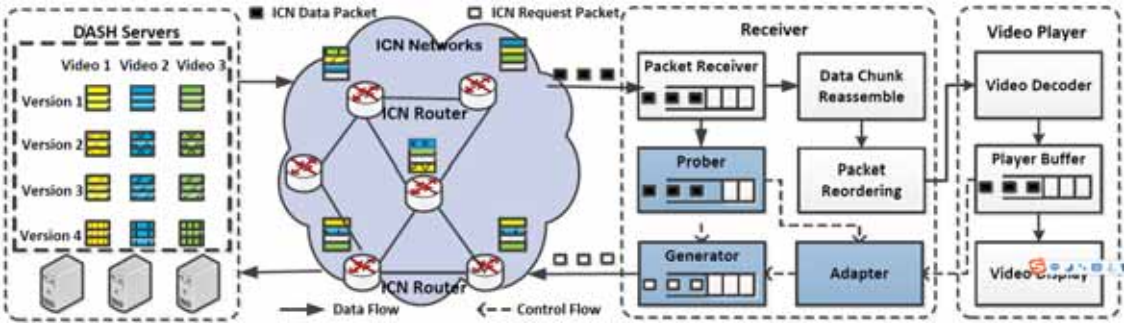

图 6：内容中心无线网络中动态自适应流媒体服务框架

3.2.2 原型系统及实际部署：

申请人已实现了内容中心无线网络流媒体服务原型系统中 CCNVideo，已经服务器 CCNxTomcat，并搭建了实验环境中。在理论模型算法研究及大规模仿真部署验证的基础上，将进一步实现本课题提出的自适应流媒体服务的算法及模型，实验拓扑如图 7，CCNVideo 的时序图如图 8。

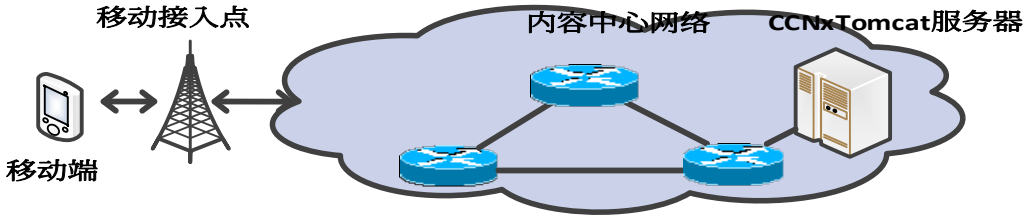

图 7：内容中心无线网络实际网络拓扑

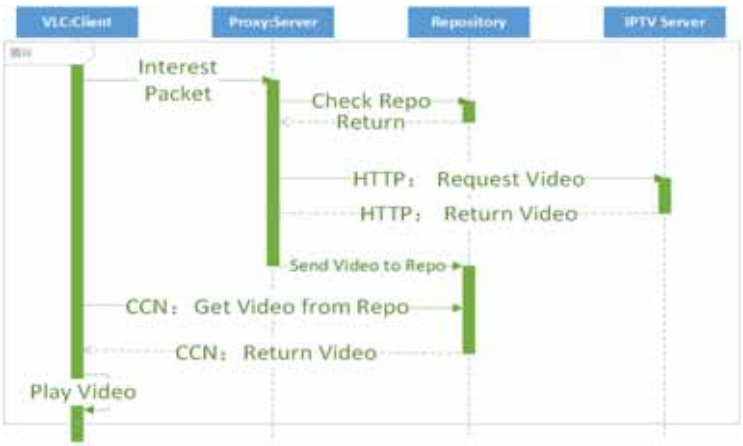

图 8：内容中心无线网络流媒体服务原型系统 CCNVideo 时序图

4、本项目的特色和创新之处

1）应用“实验驱动+系统验证”的方法来研究适合于新型内容中心无线网络特点的动态自适应流媒体服务提供机制，解决传统方法在应用层码率适配时所造成的用户体验下降问题。

2）充分借鉴“边计算”（Edge Computing）的思想，将部分计算功能迁移到网络边缘，研究从现有的“在应用层集中提供服务”的动态服务提供模式向分布式的服务运行模式的转变机制，提出应用状态驱动的内容及服务的迁移方法和本地化运行机制，解决内容中心无线网络中动态自适应流媒体服务和片段向网络边缘按需迁移问题。

5、已具备的研究基础（包括已取得的研究成果、发表的学术论文或获奖情况以及已具备的研究条件，成果、论文或获奖须列出全部作者，若发表的学术论文涉及的期刊统计了影响因子，请注明刊载当年的影响因子，并注明其索引或数据库名称）

5.1 研究成果

申请人在内容中心无线网络以及服务计算领域有扎实的研究基础，在计算机通信著名国际会议期刊中以第一作者或者导师一作、申请人二作共发表了 **4 篇 SCI，2 篇 EI**，并已**申请 3 项发明专利**，成果信息详见附件。

在导师的指导下，申请人提出并实现了基于内容中心网络的浏览器 NDNBrowser 和服务器 CCNxTomcat 原型系统，分别在浏览器和服务器内核层实现和优化了内容中心网络协议，解决了未来网络实用化推广的两个关键问题：即用户如何接入和服务的如何部署的问题，用户可以在 NDNBrowser 上通过内容中心网络观看部署 CCNxTomcat 服务器上的视频。为了将成果分享给领域内的其他研究者，我们在 GitHub 上实现了对 NDNBrowser 和 CCnxTomcat 的开源 https://github.com/buptn?tab=repositories，同时，我们在南京未来网络平台(CENI)实现了部署应用，验证了系统在较大规模的内容中心网络环境中的用户接入和服务部署问题，试验报告详见附件。

根据 Cisco 预测，视频流量将在 2020 年占据 75%以上的移动互联网流量。因此，在解决内容中心网络中客户端基本的接入问题和服务部署问题的基础上，**申请人提出并实现了基于内容中心无线网络的媒体播放系统 CCNVideo，CCNVideo 系统可以在内容中心无线网络中通过移动端 VLC 视频播放器观看北邮 IPTV 的视频节目，从而解决了 TCP/IP 网络中的真实数据流量到内容中心无线网络的导入问题，在此基础上，申请人分别提出了内容中心无线网络中移动端视频播放的节能算法，利用马尔科夫决策模型，在不影响用户体验的前提下实现移动端能量节约的最大化。同时，申请人在内容中心网络的仿平台 NDNSIM 上实现了无线流媒体播放系统 NDNVLC，研究并解决大规模网络环境下视频传输的性能问题。**

5.2 具备的实验条件

申请人所在的课题组具有小规模内容中心无线网络实验环境，包括 5 台服务器，1 个移动终端。同时，已经开发的 NDNBrowser、CCNxTomcat、CCNVideo 原型系统以及在仿真平台上开发的 NDNVLC 分别解决了用户在新型网络的接入问题、以及服务的部署问题，这些原型系统和仿真平台将是本课题的研究基础。

6、预期研究成果

成果形式 （论文、专著、专利等）	学术论文形式须注明预期被 SCI 检索数及刊载期刊的影响因子 至少一篇 CCF 列表中计算机网络方向，B 类或以上期刊论文
成果内容	1）建立内容中心无线网络中动态自适应流媒体的服务优化框架。 2）提出内容中心无线网络中动态自适应流媒体服务对动态网络内容的感知算法，解决传统方法在应用层码率适配时所造成的用户体验下降问题。 3）探索内容中心无线网络中动态自适应流媒体服务在边缘网络的缓存分布特征，以及移动边缘计算的服务提供模式，提出应用状态驱动的内容及服务的迁移方法和本地化运行机制，解决内容中心无线网络中动态自适应流媒体服务和片段向网络边缘按需迁移问题。

7、进度安排

2016 年 9 月份研究理论模型
2016 年 10-12 月份部署实验
2017 年 1 月份撰写论文
2017 年 3 月份投稿

8、申请者承诺

我保证上述填报内容的真实性。如果获得资助，我严格遵守学校有关规定，切实保证研究工作时间，按计划认真开展研究工作，按时报送有关材料，按时完成研究项目。

申请人签字：

年　月　日

9、经费预算及其它经费来源

经费预算	**支出项目**	**每月标准（元）**	**发放月数**	**金额（万元）**
	生活补贴	3000	10	3
	支出项目	**计算根据及理由**		**金额（万元）**
	论文版面/知识产权事务费			
	会议费和京外差旅费			
	设备费用			
	材料费、交通费			

其它经费来源	项目名称	来　源	金额（万元）

10、指导教师推荐意见（请导师认真负责地介绍申请人的业务基础、研究能力、科研态度及研究条件和保证等）

南国顺同学在内容中心无线网络以及流媒体服务优化领域有扎实的理论基础，发表了多篇高水平论文，并提交了多项发明专利。该同学有很强的系统开发和动手能力，能很好兼顾实验的科研任务和工程工作。

课题组有内容中心无线网络的实验平台，目前共有 3 名博士，2 名硕士参与未来网络的研究工作，我们也与国内外同行保持了紧密的交流，及时跟踪最新的研究动态。

在该同学和课题组的协助下，该同学有能力高质量完成上述研究任务。

博士生导师（签名）：

年　　月　　日

三、审批意见

学院推荐意见
经审核，本表填写的内容真实可靠，同意推荐该生参加博士创新基金资助选拔。 主管院长（签字）： 年　　月　　日　　（公章） 年　　月　　日

学校审批意见
是否同意基金资助：　　建议资助金额：_____元 研究生院负责人（签字）： （公章） 年　　月　　日
评审未通过原因：1.选题不当，不符合资助条件；2.项目论证不充分；3.申请人的素质或水平不宜承担此项目；4.预期研究成果不明确；5.不具备完成本项目的其他条件；6.其他原因（加以说明）：

北京邮电大学博士研究生创新基金

申 请 书

论文题目：满足差分隐私的多方数据发布技术研究

学生姓名：唐朋

指导教师：苏森

申请基金级别：博三基金

所在学院：网络技术研究院

申请日期：2016 年 9 月 9 日

北京邮电大学研究生院

一、基本情况

<table>
<tr><td>学　　号</td><td>2014010283</td><td>姓　　名</td><td>唐朋</td><td>二级学科</td><td>计算机应用技术</td></tr>
<tr><td>指导教师</td><td>苏森</td><td>所在学院</td><td>网络技术研究院</td><td>联系电话</td><td>18210735707</td></tr>
<tr><td>学生类别</td><td colspan="3">普通博士生☑　　直博生□</td><td>E-mail</td><td>tangpeng@bupt.edu.cn</td></tr>
<tr><td>博士论文选题</td><td colspan="5">满足差分隐私的多方数据发布技术研究</td></tr>
<tr><td>课 题 来 源</td><td colspan="5">A、国家自然科学基金重大、重点项目
B、国家科技攻关项目
C、973 科技创新计划
D、863 项目
E、长江学者奖励基金
F、跨世纪优秀人才计划
G、其他_____</td></tr>
<tr><td>预计完成时间</td><td colspan="2">2017 年 9 月</td><td colspan="2">申请经费总额（万元）</td><td>3</td></tr>
</table>

研究内容及意义摘要（限 300 字）	满足差分隐私的多方数据发布是指多个数据拥有者统一发布多组数据供数据分析者进行分析研究，并保证为每方数据提供差分隐私保护，以有效地避免各方数据中个人隐私泄露。它主要面临以下三方面的问题：如何保证为每方数据提供较强的差分隐私保护强度，如何提高整体发布数据的数据效用，如何降低数据拥有者之间的通信开销。 针对上述问题，我们将对满足差分隐私的多方数据发布进行深入研究，具体包括多方水平分割数据、多方垂直分割数据。研究成果将完善满足差分隐私保护的数据发布的理论体系，为满足差分隐私保护的数据发布提供新思路，进而推动数据发布在涉及个人敏感信息的数据领域中的应用。因此，本课题具有重要的理论价值和实际意义。

二、研究课题

1、论文选题的科学依据和意义（包括选题的科学意义，本课题国内外研究概况、发展水平和趋势，选题的总体思想及理论根据，并附主要参考文献及出处）

随着计算机和网络技术的不断发展，人们产生和收集数据的能力不断增强。大量的数据往往分布在不同的数据拥有者之间，如多家医院分别拥有一组医疗数据，医院和金融机构分别拥有一组医疗数据和金融数据。共同发布多方数据可供分析者进行数据分析，以充分挖掘数据潜在的价值，为人们提供更好的决策支持。如果共同发布多家医院的医疗数据，科研人员可拥有更多样本进行医疗数据属性间相关性分析，从而使得分析的结果更精确，进而可以帮助医疗人员做出更好的医疗决策。共同发布同一组用户的医疗数据和金融数据，可方便对用户医疗水平和经济水平的关联性分析，以帮助政府制定更好的医疗政策。然而，数据中通常蕴含大量敏感个人信息（如是否感染疾病），未经隐私处理即发布和分享数据可能导致个人隐私泄露。这不仅会对隐私泄露受害者带来伤害，同时也可能对数据发布者造成一系列的法律后果和经济损失。事实上，公众越来越关注个人隐私。由此可见，如果不能解决由于数据发布导致的个人隐私泄露的问题，数据发布的发展和应用将受到严重阻碍。

隐私保护的数据发布[1]为解决数据发布带来的个人隐私泄露问题提供一种可行的方案。近年来提出的差分隐私（Differential Privacy）[2]技术为隐私保护的数据发布提供一种较好的隐私模型。与传统的基于匿名的隐私模型（例如，k-匿名[3]和 l-多样性[4]等）不同，差分隐私提供了一种严格、可量化的隐私保护方法。差分隐私通过在数据发布过程中添加随机噪音以达到隐私保护的目的，并确保在数据集中插入或者删除某一条记录不会显著地影响数据发布结果。因此，即使攻击者获得了数据集中除一条记录之外的其他所有记录的信息，差分隐私仍可以保证攻击者并不能通过所掌握的其他记录信息推断出该条记录中蕴含的敏感信息，从而有效地避免了数据发布而导致个人隐私泄露的问题。正因为上述优点，差分隐私技术已经得到了学术界的广泛认可。满足差分隐私保护的数据发布也成为一个热点问题，受到了学者们的普遍关注。

在满足差分隐私保护的数据发布领域，国内外针对满足差分隐私保护的单方数据发布问题（即整体数据属于同一个数据拥有者）已取得一定成果[5-10]，对于满足差分隐私的多方数据发布问题尚处于起步阶段[11-13]。通过对该问题的深入分析，我们发现满足差分隐私保护的多方数据发布主要面临以下三个方面的问题：

1） 如何保证发布算法为每方数据提供较强的差分隐私保护强度。差分隐私为个人敏感信息提供了一种严格、可量化的隐私保护方法。然而，多方场景为隐私保护提出新的要求，即发布算法保证每一方数据满足差分隐私保护要求。另外，多方数据发布过程中多个数据拥有者之间存在交互，因此我们需要考虑隐私计算过程中隐私参数分配问题。

2）如何提高整体发布数据的数据效用。多方场景下为了保证发布算法对每一方数据满足差分隐私保护要求，如果每个数据拥有者简单地在自己的统计信息加入一份噪音，这将导致整体结果中含有大量噪音，发布的数据效用较差。因此我们需要考虑新的噪音加入机制，以降低整体结果中加入的噪音量规模，提高整体发布数据的数据效用。

3）如何降低分布式计算的通信复杂度。多方数据发布会涉及到分布式计算。为满足隐私保护要求，分布式计算需在安全的方式下进行，即多方安全计算。为了充分利用各方数据的统计信息，计算过程中数据交互频繁，这样会带来大量的通信开销，通信复杂度高。因此，需要考虑如何减少计算过程中交互次数，降低计算的通信复杂度。

本课题拟从上述问题出发，对满足差分隐私的多方数据发布进行深入研究，具体包括多方水平分割数据和多方垂直分割数据。研究成果将完善满足差分隐私保护的数据发布的理论体系，为满足差分隐私保护的数据发布提供新思路和新方法，进而推动数据发布在涉及个人敏感信息的数据领域中的应用。因此，本课题具有重要的理论价值和实际意义。

[1] B. Fung, K. Wang, R. Chen, and P. S. Yu. Privacy-preserving data publishing: A survey of recent developments. ACM Computing Surveys, 42(4):1–53, 2010.

[2] Cynthia Dwork, Frank McSherry, Kobbi Nissim, Adam Smith, Calibrating noise to sensitivity in private data analysis, in Proc. of TCC, pp. 265-284, 2006.

[3] Pierangela Samarati, Protecting respondents' identities in microdata release, TKDE, 13(6): 1010-1027, 2001.

[4] Ashwin Machanavajjhala, Johannes Gehrke, Daniel Kifer, Muthuramakrishnan Venkitasubramaniam, l-Diversity: Privacy beyond k-anonymity, TKDD, 1(1):3, 2007.

[5] B. Barak, K. Chaudhuri, C. Dwork, S. Kale, F. McSherry, and K. Talwar. Privacy, accuracy, and consistency too: a holistic solution to contingency table release. In PODS, pages 273–282, 2007.

[6] G. Cormode, C. M. Procopiuc, D. Srivastava, and T. T. L. Tran. Differentially private summaries for sparse data. In ICDT, pages 299– 311, 2012.

[7] G. Yaroslavtsev, G. Cormode, C. M. Procopiuc, and D. Srivastava. Accurate and efficient private release of datacubes and contingency tables. In ICDE, pages 745–756, 2013.

[8] J. Zhang, G. Cormode, C. M. Procopiuc, D. Srivastava, and X. Xiao. Privbayes: private data release via bayesian networks. In SIGMOD, pages 1423–1434, 2014.

[9] G. Kellaris, S. Papadopoulos, X. Xiao, and D. Papadias. Differentially private event sequences over infinite streams. PVLDB, 7(12):1155–1166, 2014.

[10] X. He, G. Cormode, A. Machanavajjhala, C. M. Procopiuc, and D. Srivastava. DPT: differentially private trajectory synthesis using hierarchical reference systems. PVLDB, 8(11):1154–1165, 2015.

[11] D. Alhadidi, N. Mohammed, B. C. M. Fung, and M. Debbabi. Secure distributed framework for achieving ϵ-differential privacy. In PETS, pages 120–139, 2012.

[12] Y. Hong, J. Vaidya, H. Lu, P. Karras, and S. Goel. Collaborative search log sanitization: Toward differential privacy and boosted utility. TDSC, 2015.

[13] N. Mohammed, D. Alhadidi, B. C. M. Fung, and M. Debbabi. Secure two-party differentially private data release for vertically partitioned data. IEEE Trans. Dependable Sec. Comput., 11(1):59–71, 2014.

2、研究的目标与主要内容

2.1 研究内容

国内外研究人员已经在该领域取得了一定的成果，然而，通过对相关成果的系统分析和深入研究，我们发现现有的研究成果在满足差分隐私的多方水平分割数据发布和满足差分隐私的多方垂直分割数据发布两个个方面仍然存在不足。因此，本课题拟从以下两个方面展开研究：

1、满足差分隐私保护的多方水平分割数据发布算法。多方水平分割数据是指一组关系数据库数据被分成多份，分别属于多个数据拥有者，各组局部数据之间具有相同的属性。满足差分隐私保护的多方水平分割数据发布是共同发布多组局部数据集，同时保证发布算法对每组局部数据满足 ε -差分隐私保护要求。现有的工作要么发布的数据类型单一，要么发布的数据只支持特定的数据分析任务要求。为了解决上述问题，我们需要研究：

1）适用于一般类型数据发布的模型学习方法。我们拟利用原始数据构建模型，该模型能够反映原始数据的分布特征，然后利用该模型生成新的数据。数据的属性一般包含连续型和离散型。因此，该模型应能适用于同时包含两种属性类型的数据的发布。另外，为了满足差分隐私保护要求，利用原始数据构建模型的过程中需往模型中加入噪音。当数据为高维数据，加入噪音的规模往往较大。为了降低噪音规模，提高模型的准确性，该模型应能适用于高维数据。

2）适用于水平分割数据发布的分布式模型学习方式。数据被水平分割成多组数据并分别属于多个数据拥有者。共同发布多组数据一个可行的方案是数据拥有者利用多组数据共同学习出一个模型，然后利用该模型生成新的数据。模型学习的过程中需要信息的交互。为了满足隐私保护和安全要求，交互的信息中需加入一定量的噪音，且交互的过程需按一种安全的方式进行。频繁的交互必然会带来大量的隐私参数消耗和通信开销。为了降低隐私参数消耗和通信开销，需设计新的分布式模型学习方式，减少学习过程中交互次数。

2、满足差分隐私保护的多方垂直分割数据发布算法。多方垂直分割数据是指一组关系数据库数据按属性分割成多个子列表，每个子列表拥有部分属性且属性无重叠，所有子列表中数据具有相同的 ID。每个子列表分别属于不同的数据拥有者。满足差分隐私保护的多方垂直分割数据发布是共同发布多组子列表，同时保证发布算法对每个子列表的数据满足 ε -差分隐私保护要求。现有的工作主要针对两方场景（即两个子列表），并且发布的数据只支持特定的数据分析任务（即分类）。为了解决上述问题，我们需要研究：

1）适用于更广泛的数据分析任务的模型学习方法。现有方法以目标属性为分类属性，以其他属性为预测属性，然后按照一定的规则对预测属性的取值空间进行划分，并按划分结果将数据集分组，最后将分组结果作为发布数据发布。这种模型只保留了原始数据的部分信息，发布的数据只支持分类任务。在实际场景中，发布的数据要求满足多种数据分析任务，如不同子列表间属性之间关联关系分析。为了使得发布的数据支持更广泛的数据分析任务，我们应提出新的模型学习方法，使其保留更多的原始数据信息。然而，为了满足差分隐私保护要求，构建模型中需加入一定量的噪音。为了提高模型的准确性，需要降低加入噪音的规模。因此我们需要研究使得模型中保留数据统计信息足够多，噪音规模足够小的模型学习方法。

2）不同子列表间属性之间相关性计算方法。在垂直分割数据发布场景，需要计算不同子列表间属性组合的边际分布。为了满足隐私保护需求，现有工作一般采用安全向量内积计算协议计算属性组合的边际分布，并在计算结果中加入 Laplace 噪音。然而，该方法存在两个问题：一方面，不同子列表间属性组合的数量与子列表的数量和每个子列表包含的属性的个数成正比，随着子列表的数量和每个子列表中包含的属性的个数的增加，组合的数量不断变大；另一方面，当数据规模较大时，向量长度较长。这样，边际分布计算会造成大量的通信开销和隐私参数消耗。因此，我们需要研究不同子列表间属性组合的边际分布计算方法，一方面减少不必要的属性组合的边际分布计算，另一方面缩短向量长度，以降低计算过程中通信开销和隐私参数消耗。

两个研究点相互关联，自成体系。其中，满足差分隐私保护的多方水平分割数据发布和满足差分隐私保护的多方垂直分割数据发布分别针对关系数据库的两种典型的多方场景，即水平分割场景和垂直分割场景。满足差分隐私保护的多方水平分割数据发布可以有效地解决同种类型数据分析过程中数据稀疏性问题，同时保护用户个人的敏感信息。满足差分隐私保护的多方垂直分割数据发布可以有效地解决不同类型数据间属性之间关联关系度量问题，同时满足隐私保护要求。

2.2 研究的目标和效果

1、满足差分隐私保护的多方水平分割数据发布算法研究的目标

1）数据发布算法适用于一般的数据类型，并且发布的数据支持多种数据分析任务要求。与现有算法相比，该算法中数据属性不仅可以为统计值类型，而且可以为一般的连续类型和离散类型。发布的数据支持多种分析任务要求，如分类、边际分布计算等。

2）数据发布算法满足较强的差分隐私保护强度要求，并且发布的数据具有较高的数据效用。在提供较强的隐私保护强度的同时，发布的数据中加入的噪音规模小，数据效用高，如分类结果更准确，边际分布平均误差更小。

3）数据发布算法具有较低的通信复杂度。 利用新的模型学习方式，减少数据拥有者之间交互的次数和数据规模，从而降低通信开销。

2、满足差分隐私保护的多方垂直分割数据发布算法研究的目标

1）数据发布算法适用于多方场景，并且发布的数据支持多种数据分析任务要求。

2）数据发布算法满足较强的差分隐私保护强度要求，并且发布的数据具有较高的数据效用。

3）数据发布算法具有较低的通信复杂度。减少需要计算的不同子列表间属性组合的数量，从而使得算法具有较低的通信开销。

3、拟采取的研究方法和技术路线（包括拟采用的计算方法、实验方法及其可行性论证，可能遇到的问题及其解决办法）

3.1 研究方法和技术路线

1、满足差分隐私保护的多方水平分割数据发布

为解决满足差分隐私保护的多方水平分割数据发布问题，我们拟提出序列更新贝叶斯网络方法。该方法的基本思想是利用水平分割数据之间属性间关联关系的相似性，数据拥有者采用序列方式更新贝叶斯网络，从而降低贝叶斯网络学习过程中通信开销和隐私参数消耗。具体过程如下：1）采用序列更新方法学习贝叶斯网络结构，即数据拥有者首先共同初始化贝叶斯网络结构，然后数据拥有者按照一定的次序依次利用自己的局部数据集更新贝叶斯网络结构；2）利用多方 Laplace 机制学习贝叶斯网络参数，从而使得贝叶斯网络参数中只保留一份噪音，同时保证学习的参数满足差分隐私保护；3）根据学习的贝叶斯网络生成新的数据。

2、满足差分隐私保护的多方垂直分割数据发布

为解决满足差分隐私保护的多方垂直分割数据发布问题，我们拟提出层次树融合方法。该方法的基本思想是利用多棵局部层次树匹配不同子列表间相关属性，对不相关属性进行剪枝，从而减少不同子列表间属性之间关联强度计算过程中的通信开销和隐私参数消耗。具体过程如下：1）采用自底向上的方式构建局部层次树，即首先将每层属性按照相关性分组，并为每组属性确定一个隐含属性；2）采用自顶向下的方式匹配不同子列表间相关属性；3）基于不同子列表间相关属性构建全局层次树，即把多棵局部层次树根据相关属性融合成一颗全局层次树；4）根据全局层次树生成新的数据并发布。

3.2 可行性分析

1、满足差分隐私保护的多方水平分割数据发布

水平分割数据之间属性间关联强度具有一定的相似性，前面数据拥有者的统计信息可作为先验知识指导当前数据拥有者的贝叶斯网络的学习过程。另外，贝叶斯网络学习过程是为每个属性学习一定数量的父节点。利用部分数据拥有者的统计信息可以合理地限制每个属性的候选父节点的数量，从而减小贝叶斯网络的搜索空间。因此，多个数据拥有者可利用序列更新方式学习贝叶斯网络，并降低学习过程中通信开销和隐私参数消耗。

2、满足差分隐私保护的多方垂直分割数据发布

垂直分割数据发布重点是不同子列表间相关属性之间边际分布计算。层次树构建可将相关性强的属性逐层分组并归类。利用层次树可以有效地匹配不同子列表间相关属性，从而将相关性弱的属性组合进行剪枝，只保留相关性强的属性组合。利用剪枝后的结果可简化相关属性之间边际分布计算，从而降低计算过程中通信开销和隐私参数消耗。

3.3 拟解决的关键科学问题

本课题是否能够顺利完成，依赖于以下三个关键科学问题的解决：

1、多方水平分割数据发布中贝叶斯网络边界构造问题。在多方水平分割数据发布场景中，我们拟采用序列更新方式学习贝叶斯网络，这样可使得后面的数据拥有者利用其之前的数据拥有者的统计信息作为先验知识，指导其学习过程。这些统计信息存储在边界中并在数据拥有者之间进行传递。为了降低通信开销和边界中加入噪音的规模，需限制边界的大小。然而，限制边界大小会不可避免地造成部分统计信息的损失。为了提高最终学习的贝叶斯网络的准确性，我们需保证边界包含足够多的有效信息。因此，如何构建贝叶斯网络边界，使其在一定的范围内保留足够多的有效信息是一个关键问题。

2、多方垂直分割数据发布中层次树构建问题。在多方垂直分割数据发布场景中，我们拟通过构建层次树对每个子列表中属性按照相关强度进行分类，并利用层次树匹配不同子列表间相关性较强的属性组合，从而避免不必要的属性组合关联强度的计算，进而降低计算过程中通信开销和隐私参数消耗。然而如何度量多个属性间相关强度并按照该关联强度对属性进行分类是一个难题，同时为每组关联性强的属性组合选择一个合适的父节点以构建层次树，并使得这种层次树结构符合属性匹配运算要求也是一个难题。另外，为满足差分隐私保护要求，需在层次树构建过程中加入一定量噪音。如何降低加入的噪音量，提高层次树的准确性同样是一个难题。

4、本项目的特色和创新之处

本课题可能的创新之处在于：

1、适用一般数据类型并支持多种分析任务的满足差分隐私保护的多方水平分割数据发布

在满足差分隐私保护的多方水平分割数据发布中，现有的工作要么发布的数据类型固定，数据发布算法不适用于一般的数据类型；要么发布的数据只支持分类任务，不能支持更广泛的数据分析任务要求。本课题针对上述问题，首次提出适用于一般数据类型，并且发布的数据满足多种数据分析任务要求的多方水平分割数据发布算法，同时保证该算法满足差分隐私保护要求。该算法拟采用序列更新方式学习贝叶斯网络，这样降低水平分割数据场景下学习过程中通信开销和隐私参数消耗；拟提出关联强度感知的边界构造方法合理地限制更新过程中贝叶斯网络的搜索范围，使其保留足够多的有效信息，减少信息损失；拟提出无重叠属性分割方法度量属性间关联强度，从而减少属性间关联强度计算过程中加入的噪音量。

2、支持多种数据分析任务的满足差分隐私保护的多方垂直分割数据发布

在满足差分隐私保护的多方水平分割数据发布中，现有的工作主要适用于两方，即数据发布场景中只包含两个数据拥有者，并且发布的数据只支持分类任务，不能支持更广泛的数据分析任务要求。本课题针对上述问题，提出适用于多方场景，并且发布的数据满足多种数据分析任务要求的多方垂直分割数据发布算法，同时保证该算法满足差分隐私保护要求。该算法拟采用基于层次树的相关属性匹配方法，确定不同子列表间相关性较强的属性组合，从而有效减小属性组合空间，进而降低垂直分割数据场景下属性组合相关强度计算过程中通信开销和隐私参数消耗；拟提出基于相关属性的局部层次树融合方法以构建全局层次树，从而降低全局层次树构建过程中计算复杂度；拟提出向量截断方法减小向量长度，从而降低属性间统计向量内积计算过程中通信开销和计算复杂度。

5、已具备的研究基础（包括已取得的研究成果、发表的学术论文或获奖情况以及已具备的研究条件，成果、论文或获奖须列出全部作者，若发表的学术论文涉及的期刊统计了影响因子，请注明刊载当年的影响因子，并注明其索引或数据库名称）

我们已经开展了大量的关于满足差分隐私保护的多方数据发布问题的研究工作。根据自身的具体特点，结合已有的科研经验，我们已经制定了具体的、可实施的技术路线。同时，北京邮电大学网络与交换技术国家重点实验室良好的科研氛围与优越的实验条件，为本课题的顺利开展创造了有利条件。因此，预计我们可以实现本课题的预期目标。

针对现有满足差分隐私保护的多方水平分割数据发布算法的不足，我们撰写了“ Differentially Private Multi-Party High-Dimensional Data Publishing ”论文并已被国际会议 International Conference on Data Engineering（ICDE 2016，CCF A 类会议）录用。论文作者为：Su Sen, Tang Peng, Cheng Xiang, Chen Rui, Wu Zequn.

6、预期研究成果

成果形式 （论文、专著、专利等）	学术论文形式须注明预期被 SCI 检索数及刊载期刊的影响因子 发表 CCF A 类会议（如 IEEE ICDE）或期刊（如 IEEE Transactions on Knowledge and Data Engineering）1 篇。其中，期刊 TKDE 的影响因子为 2.476。
成果内容	提出满足隐私保护的多方垂直分割数据发布算法。

7、进度安排

2016 年 9 月-2016 年 11 月，完善满足差分隐私保护的多方水平分割数据发布研究工作，完成对会议论文的期刊扩展工作。

2016 年 12 月-2017 年 7 月，开展并完成满足差分隐私保护的多方垂直分割数据发布研究工作，包括算法设计和实现、论文撰写和投稿工作。

2017 年 8 月-2017 年 9 月，对项目的研究工作进行全面地总结与归档，准备项目验收。

8、申请者承诺

我保证上述填报内容的真实性。如果获得资助，我严格遵守学校有关规定，切实保证研究工作时间，按计划认真开展研究工作，按时报送有关材料，按时完成研究项目。

申请人签字：

年　月　日

9、经费预算及其它经费来源

经费预算	**支出项目**	**每月标准（元）**	**发放月数**	**金额（万元）**
	生活补贴	3000	10	3
	支出项目	**计算根据及理由**		**金额（万元）**
	论文版面/知识产权事务费			
	会议费和京外差旅费			

其它经费来源	项目名称	来　源	金额（万元）

10、指导教师推荐意见（请导师认真负责地介绍申请人的业务基础、研究能力、科研态度及研究条件和保证等）

唐朋同学自入学以来，积极与老师配合，认真学习，专心科研。在与老师的不断交流中，掌握了科研的基本思路和技巧，学会了发现问题和解决问题的基本方法。

在数据隐私领域，阅读了大量的科技文献，对该领域拥有扎实的基础知识和全面深入的认识。不断学习最新的研究成果，及时了解该领域最新的进展。

在科研过程中，善于发现问题并深入思考。往往能够从新的角度来思考问题，并能够采用新的思路解决问题。具有较强的创新意识和一定的创新能力。

对待科研工作一丝不苟。发现问题后能认真思考和反复论证，及时与老师讨论交流，认真听取老师的意见。对于提出的方案，首先从理论上进行严格的推导和分析，保证其理论的正确性和合理性。然后，通过大量的实验对方案的有效性进行全面的验证。

北京邮电大学网络与交换技术国家重点实验室有从事数据隐私领域多年的老师和完整的实验设备，为其顺利开展本课题提供了良好的科研氛围与优越的实验条件。

博士生导师（签名）：

年　　月　　日

三、审批意见

学院推荐意见
经审核，本表填写的内容真实可靠，同意推荐该生参加博士创新基金资助选拔。 主管院长（签字）： 年　　月　　日　　（公章） 年　月　　日
学校审批意见
是否同意基金资助：　　建议资助金额：_____元 研究生院负责人（签字）： （公章） 年　　月　　日
评审未通过原因：1.选题不当，不符合资助条件；2.项目论证不充分；3.申请人的素质或水平不宜承担此项目；4.预期研究成果不明确；5.不具备完成本项目的其他条件；6.其他原因（加以说明）：

北京邮电大学博士研究生创新基金

申 请 书

论文题目：纠缠辅助区分正交量子态

学生姓名：张志超

指导教师：温巧燕

申请基金级别：博三基金

所在学院：网络技术研究院

申请日期：2016 年 9 月

北京邮电大学研究生院

一、基本情况

<table>
<tr><td>学　　号</td><td>2014010286</td><td>姓　　名</td><td>张志超</td><td>二级学科</td><td>计算机科学与技术</td></tr>
<tr><td>指导教师</td><td>温巧燕</td><td>所在学院</td><td>网络技术研究院</td><td>联系电话</td><td>18500521867</td></tr>
<tr><td>学生类别</td><td colspan="3">普通博士生 ☑　　直博生□</td><td>E-mail</td><td>zhichao1234@bupt.edu.cn</td></tr>
<tr><td>博士论文选题</td><td colspan="5">量子态与非局域性关系的研究</td></tr>
<tr><td>课 题 来 源</td><td colspan="5">A、国家自然科学基金重大、重点项目
B、国家科技攻关项目
C、973 科技创新计划
D、863 项目 E、长江学者奖励基金 F、跨世纪优秀人才计划
√G、其他 国家自然科学基金项目</td></tr>
<tr><td>预计完成时间</td><td colspan="2">2017 年 9 月</td><td>申请经费总额（万元）</td><td colspan="2">3 万元</td></tr>
</table>

研究内容及意义摘要（限 300 字）	当一组量子态不可局域区分时，就反应了这组量子态的非局域性。量子态非局域性是量子世界中最奇妙的现象，是一种非常重要的资源被广泛应用于量子信息处理，也是量子密码协议中接收者或攻击者在提取信息时所面临的关键问题，在量子密码协议设计和分析中有着重要而广泛的应用。尽管量子非局域性理论已经取得了相当数量的成果，但还有很多基本理论问题需要解决，特别是对于纠缠作为一种资源辅助区分具有非局域性的正交量子态这个问题还有待进一步的研究。本课题主要对纠缠作为一种资源辅助区分正交直积基量子态和区分不可扩展直积基量子态这两个方面进行研究。另外，也将研究纠缠作为一种资源来帮助区分非局域性的正交纠缠态这个问题。其成果一方面能丰富和完善量子非局域性理论，另一方面也将为今后可能的实际应用提供理论支持。

二、研究课题

1、论文选题的科学依据和意义（包括选题的科学意义，本课题国内外研究概况、发展水平和趋势，选题的总体思想及理论根据，并附主要参考文献及出处）**选题的科学意义：**

量子计算和量子信息处理是二十世纪八十年代后期兴起的一个新的研究方向。量子系统具有独特的物理特性，如叠加性、相干性。利用这些量子行为而设计的信息处理任务，就是量子计算和量子信息处理的目标。作为量子力学、信息科学以及数学相结合而产生的新兴交叉学科，量子计算和量子信息处理发展迅速。与经典信息论不同的是，量子信息论中可以使用量子力学独有的诸如量子叠加、量子纠缠之类的成分去完成信息处理任务，从而在某些情况下可以达到任何经典方式所无法比拟的效率。量子纠缠和量子状态的可区分性是量子信息和量子计算中的两个重要方面。前者是量子信息处理的重要资源，后者则影响量子信息学的整体面貌，对认知、表示、访问信息等问题有重要的启示。

量子纠缠和量子非局域特性是量子世界中两种独特的现象。直觉上，人们认为是因为量子纠缠的存在导致了量子的非局域性，但在实践中人们发现并非如此。目前人们还不清楚量子纠缠和量子非局域性究竟是什么关系，广大学者在开展进一步的研究。量子态区分尤其是用局域操作和经典通信来研究量子态的区分问题，是研究量子纠缠和量子非局域特性之间关系的有效手段，被广泛地用到量子信息理论的各个分支研究中，比如量子信道容量、量子密码协议分析等[1,2]。因此，探究量子纠缠与非局域性之间的关系，已经成为量子理论研究中的重要内容[3-14]。本课题将主要研究量子纠缠与非局域性的关系，计划一方面研究纠缠作为一种资源帮助区分具有非局域性的正交直积态，一方面研究纠缠辅助区分具有非局域性的纠缠态。

国内外研究概况、发展水平和趋势：

20 世纪三十年代，人们就发现了量子世界中特有的量子纠缠和量子非局域性。直觉上，人们普遍认为是纠缠导致了非局域性。1999 年，Bennett 等[3]发现了没有纠缠的非局域性这个现象，引起了广大学者的普遍关注。2000 年 Walgate 等[4]证明了任意两个正交量子态，无论纠缠与否，总是可以经局域操作和经典通信（LOCC）完美区分的。这些事实说明了纠缠既不是非局域性的充分条件，也不是非局域性的必要条件，但纠缠和非局域性又确实存在着联系，这引起了广大学者的兴趣。接下来，学者们一方面研究经 LOCC 可以完美区分的正交量子态；另一方面研究经 LOCC 不能完美区分的线性无关的量子态，包括有错区分和无错区分。

对于完美区分，一方面人们主要研究了最小不可区分子空间；另一方面是简单的 Hilbert 空间量子态的局域区分性。在最大纠缠态的完美区分问题上，2004 年 Ghosh 等[6]给出了一类最大纠缠态单向 LOCC 完美区分的充分条件。2012 年，Yu 等[8]给出了 $4\otimes4$ 中 4 个不可局域区分最大纠缠态，说明 4 是它的一个下确界。紧接着，Nathanson[10]给出了单向 LOCC 区分最大纠缠态的一个充分必要条件。

对于非完美的局域区分，2003 年，Horodecki 等[12]证明了对两体 Hilbert 空间，任意一组正交基能被 LOCC 概率区分当且仅当它是正交直积基。2005 年 Ji 等[15]给出了两个具有任意先验概率的纯态，LOCC 区分的最优概率等于全局区分的最优概率。2007 年 Duan 等[16]给出了不可扩展基区分的充要条件及任意基中可区分量子态个数的下界。2009 年 Bandyopadhyay 等[17]给出了任意三个线性无关量子态必有一个可以无错区分。

近年来，部分学者们开始研究纠缠作为一种有用资源来帮助区分具有非局域性的量子态这个问题，从而进一步研究纠缠与非局域性之间的关系。2008 年，Cohen

给出了几类不可扩展直积基在低维的最大纠缠态资源帮助下是可以区分的具体协议。最近，Groisman 和 Strelchuk 给出了区分相互正交的四个 Bell 型态所需要的最优数量的纠缠。

选题的总体思想及理论根据：

随着对纠缠与量子非局域性关系研究的逐渐深入，研究人员开始着重从两个方向进行研究：(１)继续深入研究纠缠作为一种资源帮助区分具有非局域性的正交直积态。由于具有没有纠缠的非局域性的正交直积态非常奇特，所以对于更加深入地研究纠缠与非局域性的复杂关系具有非常重要的意义；(２)研究不可局域区分的纠缠态在辅助纠缠的帮助下的区分性。由于最大纠缠态是一类非常特殊的量子态，而且在隐形传态、超密编码、量子密码协议的设计中具有非常广泛的应用，因此研究最大纠缠态在纠缠资源的帮助下的区分性这个基础性问题，能够为今后可能的实际应用提供更加充分的理论支持。正因为如此，本课题计算按照以下两个方面进行研究：

一方面，本项目计划引用辅助纠缠的方法帮助区分不可局域区分的直积态。目前对于一般系统中不可局域区分的直积态的构造已经有了很多，比较常见的就是不可扩展直积基，后来人们发现在辅助纠缠的帮助下是可以局域区分不可扩展直积基的。然而，这里仅仅给出了几类不可扩展直积基的例子，对于非不可扩展直积基的直积态还没有相似的结论。那么，对于非不可扩展直积基并且不可局域区分的直积态，本项目计划引用辅助纠缠态的方法帮助区分这些不可局域区分的直积态。

另一方面，本项目计划研究的不可局域区分的纠缠态，特别是最大纠缠态在少量的辅助纠缠的帮助下的区分性。目前，对于最大纠缠态的局域区分性问题，主要集中于低维的系统或者一些特殊的高维系统，而对于辅助纠缠帮助区分最大纠缠态

的研究就更少了，因此，本项目计划研究在辅助纠缠的帮助下来区分最大纠缠态的问题。

参考文献：

[1] D. P. DiVincenzo, D. W. Leung, and B. M. Terhal, Quantum Data Hiding, IEEE Trans. Inf. Theory 48, 580 (2002).

[2] D. Markham and B. C. Sanders, Graph states for quantum secret sharing, Phys. Rev. A 78, 042309 (2008).

[3] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, et al, Quantum nonlocality without entanglement, Physics Review A, 59, 1070 (1999).

[4] J. Walgate, A. J. Short, L. Hardy, and V. Vedral, Local distinguishability of multipartite orthogonal quantum states, Physical Review Letter, 85, 4972 (2000).

[5] H. Fan, Distinguishability and Indistinguishability by Local Operations and Classical Communication, Physical Review Letter, 92, 177905 (2004).

[6] S. Ghosh, G. Kar, A. Roy and D. Sarkar, Distinguishability of maximally entangled states. Physics Review A, 70(2), 022304 (2004).

[7] S. Bandyopadhyay, S. Ghosh, and Guruprasad Kar, LOCC distinguishability of unilaterally transformable quantum states, New Journal of Physics, 13, 123013 (2011).

[8] N. Yu, R. Duan, and M. Ying, Four Locally Indistinguishable Ququad-Ququad Orthogonal Maximally Entangled States, Physical Review Letter, 109, 020506 (2012).

[9] A. Cosentino, and V. Russo, Small sets of locally indistinguishable orthogonal maximally entangled states, Quantum Information and Computation, 14, 1098 (2014).

[10] M. Nathanson, Three maximally entangled states can require two-way local operations and classical communication for local discrimination, Physics Review A, 88, 062316 (2013).

[11] J. Niset and N. J. Cerf, Multipartite nonlocality without entanglement in many dimensions, Physics Review A, 74, 052103 (2006).

[12] M. Horodecki, A. Sen(De), U. Sen, and K. Horodecki, Local Indistinguishability: More Nonlocality with Less Entanglement, Physical Review Letter, 90, 047902 (2003).

[13] S. De Rinaldis, Distinguishability of complete and unextendible product bases, Physics Review A, 70, 022309 (2004).

[14] Y. Feng and Y. Shi, Characterizing Locally Indistinguishable Orthogonal Product States, IEEE Trans. Inf.Theory, 55, 2799 (2009).

[15] Z. F. Ji, H. E. Cao, and M. S. Ying, Optimal conclusive discrimination of two states can be achieved locally, Physics Review A, 71(3), 032323 (2005).

[16] R. Y. Duan, Y. Feng, Z. F. Ji, and M. S. Ying, Distinguishing Arbitrary Multipartite Basis Unambiguously Using Local Operations and Classical Communication, Physical Review Letter, 99(23), 019901 (2007).

[17] S. Bandyopadhyay and J. Walgate, Local distinguishability of any three quantum states, J. Phys. A: Math. Theor. 42, 072002 (2009).

[18] S. M. Cohen, Understanding entanglement as resource: Locally distinguishing unextendible product bases, Physics Review A, 77, 012304 (2008).

[19] B. Groisman and S. Strelchuk, Optimal amount of entanglement to distinguish quantum states instantaneously, Physics Review A, 92, 052337 (2015).

2、研究的目标与主要内容

量子态的区分是量子信息理论中最基本的问题之一，它是量子密码、量子通信、量子数据隐藏等各个分支的基础。所谓局域区分即从已知的正交量子态集合中任意选取一个量子态，我们仅用局域操作和经典通信(LOCC)就可以确定这个未知量子态。本课题计划按照以下两个方面进行研究：

1）设计辅助纠缠帮助区分具有非局域性的正交直积态的协议。目前对于不可局域区分的正交直积基和不可扩展直积基已经有了不少例子。例如，Bennett 等人在 1999 年构造出了 $3\otimes3$ 系统中的一个正交直积基和一个不可扩展直积基。然而，这些直积态在少量辅助纠缠的帮助下是不是可以局域区分呢？我们希望通过研究，能够设计出一个辅助纠缠帮助区分具有非局域性的正交直积态的协议，并且我们相信在一些低维的系统中，这个协议是肯定存在的。本课题预期可以设计出一般系统上某类正交直接态在少量辅助纠缠的帮助下能局域区分的协议。

2）设计辅助纠缠帮助区分具有非局域性的纠缠态，特别是最大纠缠态的协议。最近，Groisman 和 Strelchuk 给出了区分四个相互正交的 Bell 型态所需纠缠的最优量。近些年来，研究人员也构造了各种不同种类的不可局域区分的最大纠缠态组合。那么，对于这些量子态在少量纠缠资源的帮助下是不是可以局域区分呢？目前还没有得到解决。因此，我们希望通过研究设计出在少量纠缠资源的帮助下可以区分这些纠缠态的协议。本课题预期可以设计出一般双体系统上某类不可局域区分的纠缠态在少量辅助纠缠的帮助下可以局域区分的的协议。

3、拟采取的研究方法和技术路线（包括拟采用的计算方法、实验方法及其可行性论证，可能遇到的问题及其解决办法）

拟采用的计算方法、实验方法

（1）密切跟踪国际和国内一些高水平刊物上发表的量子态区分相关论文，包括Physical Review Lett./A、Physics Letters A、Quantum Information & Computation、International Journal of Quantum Information、Chinese Physics、Chinese Physics Letters、物理学报及 arXiv 网站等。

（2）小组讨论：对自己遇到的问题，以及解决方法，在小组内部进行讨论，反复论证。目前我们组织了量子态区分讨论班，每周一次，经过三年的讨论我们学到了很多新的知识，对量子态区分问题的热点，难点把握的更加准确，我们小组成员之间相互学习，互相帮助，共同解决彼此遇到的问题，目前已经取得了一定的成果，我们相信经过长期的讨论学习，我们会做出更多的成果。

（3）深入研究正交直积态的局域区分性，充分了解已有的区分正交直积态的各种方法。在此基础之上，我们计划利用辅助纠缠的帮助来区分不可局域区分的直积态，设计出用纠缠态来帮助区分不可局域区分的直积态的方案。

（4）目前对于不可局域区分的最大纠缠态的问题还没有得到完全解决。本项目计划用辅助纠缠来帮助区分具有非局域性的最大纠缠态，并设计出相对应的具体的区分协议。

可行性论证

本项目为理论研究，实验室目前的硬件条件可以支撑相关研究的顺利开展。到目前为止，我已经对量子态的区分有了充分的了解，对正交直积态的各种区分方法有了基本的认识，并且已经有了辅助纠缠帮助区分直积态的基本思路和框架。对于最大纠缠态的局域区分性问题，我们也进行了充分的研究并在此基础上已经有了部分结论，实践证明是切实可行的。

可能遇到的问题及其解决办法

我们利用辅助纠缠来帮助区分直积态，很自然地会用到什么样的辅助纠缠才是合适的，对于不同种类的直积态是不是可以找到统一的辅助纠缠，随着量子态的维数的增大，从而大大增加计算的复杂度。针对这个问题，我们将在研究中充分地运用 matlab、mathematica 等软件进行计算和仿真，以提高我们工作的准确性和效率。

4、本项目的特色和创新之处

本项目最主要的特色和创新之处是进一步完善辅助纠缠在量子态区分中的作用。考虑到纠缠与非局域性的复杂关系在各种量子密码协议中具有很广阔的应用范围，这个工作是重要而且有特色的。

5、已具备的研究基础（包括已取得的研究成果、发表的学术论文或获奖情况以及已具备的研究条件，成果、论文或获奖须列出全部作者，若发表的学术论文涉及的期刊统计了影响因子，请注明刊载当年的影响因子，并注明其索引或数据库名称）

申请人从读研开始（2012 年 9 月）一直从事量子信息理论的研究，主要致力于 研究量子态与非局域性的关系。到目前为止，已经对相关问题做了较深入的研究， 并且具备了一定的研究基础，已经作为第一完成人发表（录用）SCI 检索论文共 7 篇，其中 5 篇为二区论文。相关目录如下：

[1]. Zhi-Chao Zhang, Fei Gao, Tian-Qing Cao, Su-Juan Qin, Qiao-Yan Wen, Entanglement as a resource to distinguish orthogonal product states, Scientific Reports, 2016, 6:30493.（SCI 检索，影响因子 5.228）

[2]. Zhi-Chao Zhang, Fei Gao, Ya Cao, Su-Juan Qin, Qiao-Yan Wen, Local indistinguishability of orthogonal product states, Physical Review A, 2016, 93 (1):012314.（SCI 检索，影响因子 2.765）

[3]. Zhi-Chao Zhang, Fei Gao, Su-Juan Qin, Ying-Hui Yang, Qiao-Yan Wen, Nonlocality of orthogonal product states, Physical Review A, 2015, 92 (1):012332.（SCI 检索，影响因子 2.765）

[4]. Zhi-Chao Zhang, Ke-Qin Feng, Fei Gao, Qiao-Yan Wen, Distinguishing maximally entangled states by one-way local operations and classical communication, Physical Review A, 2015, 91(1):012329.（SCI 检索，影响因子 2.765）

[5]. Zhi-Chao Zhang, Fei Gao, Guo-Jing Tian, Tian-Qing Cao, Qiao-Yan Wen, Nonlocality of orthogonal product basis quantum states, Physical Review A, 2014, 90(2):022313.（SCI 检索，影响因子 2.765）

[6]. Zhi-Chao Zhang, Fei Gao, Su-Juan Qin, Hui-Juan Zuo, Qiao-Yan Wen, Local distinguishability of maximally entangled states in canonical form, Quantum Information Processing, 2015, 14(10):3961-3969.（SCI 检索，影响因子 1.840）

[7]. Zhi-Chao Zhang, Qiao-Yan Wen, Fei Gao, Guo-Jing Tian, Tian-Qing Cao, One-way LOCC indistinguishability of maximally entangled states, Quantum Information Processing, 2014, 13(3):795-804.（SCI 检索，影响因子 1.840）

6、预期研究成果

成果形式 （论文、专著、专利等）	学术论文形式须注明预期被 SCI 检索数及刊载期刊的影响因子 预期发表（含录用）二区期刊SCI检索论文1篇，如《Scientific Reports》、《Physical Review A》,期刊 2015 年影响因子分别为 5.228、2.765.
成果内容	设计一个不可局域区分的正交直积态在辅助纠缠资源的帮助下是可以局域区分的协议；在双体量子系统中，设计出利用纠缠帮助区分具有非局域性的纠缠态的协议。

7、进度安排

2016.09-2016.12 重点研究具有非局域性的正交直积态在纠缠资源的帮助下的局域区分性并且完成相关论文;

2017.01-2017.03 主要研究具有非局域性的纠缠态在纠缠资源的帮助下的局域区分性和书写相关论文;

2017.04-2017.08 继续研究和分析其它种类量子态的非局域性。

8、申请者承诺

我保证上述填报内容的真实性。如果获得资助，我严格遵守学校有关规定，切实保证研究工作时间，按计划认真开展研究工作，按时报送有关材料，按时完成研究项目。

申请人签字：

年　月　日

9、经费预算及其它经费来源

经费预算	**支出项目**	**每月标准（元）**	**发放月数**	**金额（万元）**
	生活补贴	3000	10	3
	支出项目	**计算根据及理由**		**金额（万元）**
	论文版面/知识产权事务费			
	会议费和京外差旅费			
其它经费来源	项目名称		来　源	金额（万元）

10、指导教师推荐意见（请导师认真负责地介绍申请人的业务基础、研究能力、科研态度及研究条件和保证等）

申请人从硕士研究生开始研究量子态的区分，至今已有将近 4 年时间。在这四年中，申请人一直致力于量子态与非局域性关系的研究，对相关问题做了较深入的探索，具备了一定的研究基础，已经以第一作者身份发表（录用）相关 SCI 检索论文 7 篇，其中有 5 篇论文为高水平二区论文。该申请人具有良好的科研态度，刻苦勤奋，对相关领域的研究充满热情，能够保证充足的科研时间。实验室目前的条件足以支撑申请人完成本项目。如果项目申请成功，实验室将为申请人顺利完成项目提供所有必要的支持。

博士生导师（签名）：

年　　月　　日

三、审批意见

学院推荐意见
经审核，本表填写的内容真实可靠，同意推荐该生参加博士创新基金资助选拔。 主管院长（签字）： 年　　月　　日　　（公章） 年　月　　日
学校审批意见
是否同意基金资助：　　建议资助金额：_____元 研究生院负责人（签字）： （公章） 年　　月　　日
评审未通过原因：1.选题不当，不符合资助条件；2.项目论证不充分；3.申请人的素质或水平不宜承担此项目；4.预期研究成果不明确；5.不具备完成本项目的其他条件；6.其他原因（加以说明）：