分类号: TP39 单位代码: 10335

密 级: 学 号: 11432005

浙江大学

博士学位论文

中文论文题目: 面向本地差分隐私的数据可用性优化方法研究

英文论文题目: Data Utility Optimization for Local Differential Privacy

申请人姓名: 张治坤

指导教师: 陈积明 教授

贺诗波 研究员

专业名称: 控制科学与工程

研究方向: 数据隐私

所在学院: 控制科学与工程学院

论文提交日期: 二〇一九年六月

致谢

行文至此，意味着五年博士生涯行将结束。一路走来，经历了论文不断被拒的痛苦与挫败，也经历了论文被顶级期刊和会议接收的喜悦与成就。回想读博五年，并非一帆风顺，不过正是这段经历让我学会了坦然面对科研和生活中的喜与悲，让我更加相信坚持一定会有收获。在博士生涯进入尾声之际，我要向一直以来支持和帮助我成长的师长、同窗和亲友们表示最诚挚的谢意，你们的关心与支持我将铭记于心，这篇博士论文是对你们最好的答谢。

在此，谨向敬爱的孙优贤院士表示深深的敬意和衷心的感谢，感谢您和课题组为我提供了一流的科研平台和舒适的科研环境。您踏实严谨、亲临一线的科研作风深深得鼓舞和激励着我，我将受用终身。

感谢我的导师陈积明教授无微不至的关怀和事无巨细的指导。陈老师为我开启了信息安全研究的大门，培养了我求是创新的科研态度、缜密严谨的逻辑思维和踏实肯干的处事风格，您教会的这些将成为我一生的财富。陈老师为课题组争取的资源和平台让我们每个人都有机会走出去，到国外知名大学访问学习，参加各类顶级学术会议，极大地扩展了我的视野。感谢您一直以来的信任和支持，我将更加努力，争取早日成为一名优秀的科研工作者。

感谢合作导师贺诗波老师对我科研工作的悉心指导和大力支持。博士五年，贺老师一直扮演着亦师亦兄的角色。在科研上，您严谨的治学态度和精益求精的工作作风深深地影响了我的科研态度和科研品味；在生活上，您在我最迷茫的时候提供了最大的支持与鼓励，让我倍感温暖并充满力量。再一次衷心感谢您！

感谢林庆老师在工作、学习和生活上的帮助与支持。正因为您在背后的默默奉献与支持，才让课题组的每一个成员能心无旁骛地科研。

感谢在普渡大学访问期间的指导老师李宁辉教授。您对于科研的热情和洞察力深深得感染着我，让我终身受益。时至今日，依然清晰记得为了赶 CCS 论文，您陪我连续奋战的两个通宵；依然清晰记得参加差分隐私挑战赛时，您陪我改进算法到凌晨一两点的日子。跟着您做科研的一年半让我充满了成就感，我将终身铭记！

感谢普渡大学王天豪博士，很庆幸博士期间能和北美安全界的 rising star 一起并肩作战，一起熬夜改论文，一起熬夜做比赛！希望我们友谊长存，日后继续合作，做出更多更好的成果。感谢一起在普渡访学的张啸剑老师在生活和科研上无私的支持与帮助。感谢在普渡访学期间的室友何高辉和赵祖松颖，你们为我枯燥的科研生活增添了很多乐趣，美西自驾游是我永远珍贵的回忆！感谢德国 CISPA 信息安全研究中心的张阳博士在我面临毕业选择时提供的建议和帮助。

感谢课题组程鹏教授、吴均峰研究员和邓瑞龙研究员的关心与支持。感谢张恒和齐义飞师兄在我科研初期的悉心指导，你们为我打开了科研的大门。感谢何建平、张永敏、何立栋、史秀纺、唐晓宇、刘浩、李超、刘恩东、赵成成、尤鹏程、杨梓东、崔现斌等师兄师姐在生活和科研上的支持和帮助；感谢郭进、柯晓杰、范博、张梦源、张勇涛等的大力支持；感谢杨光、王鑫、孙羽羿等师弟师妹在论文校对上的帮助。同时也要感谢网络传感与控制研究组 (NeSC-IIPC) 每一位在读和毕业的成员。五年来我见证了整个课题组的快速成长，希望 NeSC 课题组以后变得越来越好！

最后要衷心感谢我的父母和家人。在整个成长过程中，不管我做出何种选择，你们都在背后默默地支持和鼓励着我，使得我没有任何后顾之忧，我今天的成绩有你们一半的功劳！特别感谢陈敏一直以来的理解与支持，你的存在是我继续前行的最大动力！

谨以此文献给所有帮助和支持我的亲人和朋友们。

张治坤

二零一九年九月于求是园

摘要

随着大数据和人工智能技术的发展，数据的重要性变得越来越凸显，并被经济学人杂志称为数字时代的石油。然而，随着各国政府日趋严格的隐私保护法案的出台，以及互联网用户隐私保护意识的觉醒，如何在保护隐私的前提下收集数据成为各大互联网公司的当务之急。在学术界和工业界的共同推动下，本地差分隐私技术逐渐成为用户隐私数据收集的黄金标准。目前谷歌、苹果和微软等互联网巨头已把本地差分隐私集成到产品中用于用户隐私数据的收集与分析。

本地差分隐私的核心思想是用户在本地对数据进行随机扰动处理，并提供严格的隐私保护量化标准。然而，随机扰动的引入不可避免地影响了数据可用性。如何优化数据可用性成为各大互联网公司大规模部署本地差分隐私需要解决的首要问题。对本地差分隐私数据可用性的优化可以从两个维度展开：融合算法优化和隐私预算优化。其中，融合算法优化通过改进数据编解码方式以降低随机扰动对数据可用性的影响，隐私预算优化在融合算法给定时通过进一步优化隐私保护程度来降低扰动水平。根据数据拥有者与数据使用者之间的关系，隐私预算优化可以分为激励设计和协同优化两种方法。当数据拥有者不是使用者时，可以通过激励设计补偿数据拥有者隐私损失的方式使其选择更高的隐私预算；当数据拥有者同时也是使用者时，可以通过协同优化隐私预算与数据质量的方式来获得最优的数据可用性。近年来，研究人员对数据可用性优化方法研究取得了一定进展，然而现有工作仍然存在以下不足：a) 现有高维数据融合算法数据可用性比较低，无法满足高维数据分析的需求；b) 现有激励设计方法无法解决用户与融合中心之间信息不对称的问题，也无法满足实时数据融合的需求；c) 协同优化是数据拥有者与使用者相同场景下数据可用性优化的关键技术，然而相关研究非常缺乏。本文结合国内外研究现状，针对本地差分隐私数据可用性优化研究中存在的不足进行了探索和改进，具体包括：

1. 研究了高精度的高维数据融合算法。边缘列联表是进行高维属性关联分析的基础，也是高维数据分析与融合的关键技术。因此，本文以边缘列联表发布为切入点，研究高维数据融合算法的优化问题。本文提出的 CALM 方法，通过一组称为视图的边缘列联表获取高维属性之间的关联关系，并使用一致化视图和最大熵优化理论来重构剩余

边缘列联表。CALM 方法的创新性在于，通过对多个误差源的定量分析，提出了一套选取最优视图的算法，极大降低了随机扰动对数据可用性的影响。CALM 能高效处理高维的非二元属性，并把现有最好算法的融合精度提高了一到两个数量级。

2. 研究了基于静态激励的隐私预算优化问题。基于激励设计的隐私预算优化方法的核心思想是，通过补偿用户隐私损失的方式激励其使用更高的隐私预算，从而提升数据可用性。用户隐私损失决定于隐私预算和用户隐私偏好，而不同用户的隐私偏好往往不同。比如女性往往比男性更看重自己的年龄，病人往往比健康人更看重自己的位置。在激励设计过程中，融合中心很难得知不同用户的具体隐私偏好，造成了融合中心和用户之间的信息不对称问题。本文借助经济学中的契约理论设计了 REAP 机制来解决信息不对称问题。具体来说，假设融合中心拥有所有用户隐私偏好分布的先验知识，并为不同隐私偏好种类的用户设计不同契约，每个契约对应一个隐私预算及相应补偿。所有契约都广播给所有用户，每个用户可以选择使得自身效用最大的契约。最优契约设计的难点在于，如何保证用户真实地选择自身隐私偏好对应的契约，REAP 通过求解满足激励兼容约束的优化问题解决了用户真实性选择的问题。

3. 研究了基于动态激励的隐私预算优化问题。实时数据融合在现实生活中广泛存在，比如公共健康监测机构可以通过实时收集用户体征信息对传染疾病进行监测与控制。实时数据融合需要周期性收集用户信息，因此需要保证用户的长期参与。现有静态激励机制无法满足实时数据融合的需求，因为很容易导致部分用户长期未被选中并退出系统。为了保证实时数据融合中用户的长期参与，本文设计了 LEPA 机制，使用在线算法来联合优化各个时隙之间的系统效用并保证所有用户都有一定概率被选中，以此防止用户中途退出。

4. 研究了基于协同优化的隐私预算优化问题。基于协同优化的方法适用于数据拥有者与使用者相同的场景，本文研究了该场景下的典型应用——数据库驱动认知无线电中的位置隐私保护与频谱分配问题。数据库驱动认知无线电技术是解决一级用户和二级用户之间相互干扰的有效手段。然而该技术的实现要求一级用户和二级用户直接或间接提供自身位置信息进行动态频谱分配。本文设计了一个保护隐私的效用最大化数据库访问协议 UMax ，通过位置隐私保护与频谱利用率之间的协同优化，允许双方用户选择最优隐私预算来最大化数据可用性，并提升频谱利用率。

关键词： 本地差分隐私，融合算法优化，激励设计，协同优化，群智感知

Abstract

The recent proliferation of big data and artificial intelligence have given prominence to the importance of data, which is referred as oil of the digital era by Economist magazine. However, in recent years, governments have proposed stricter privacy protection acts, and Internet users care more about their data privacy. These have enforced Internet companies to develop new technologies to privately collect sensitive data from their users. With the promotion of academia and industry, Local Differential Privacy (LDP) has been the golden standard for private data collection, and been deployed by many Internet giants such as Google, Apple and Microsoft.

The main idea of LDP is to perturb the raw data locally to enforce privacy, and provide strict mathematical definition. However, data perturbation will inevitably impact the data utility, and how to improve data utility has been the core for its widely deployment. There are two dimensions to improve data utility for LDP: aggregation algorithm optimization and privacy budget optimization. Aggregation algorithm optimization improves data utility by designing more efficient encoding algorithm to compress data; privacy budget optimization further optimizes the privacy-preserving level to alleviate the impact of perturbation when the aggregation algorithm is fixed. Based on the relationship between data owner and data consumer, the privacy budget optimization can be classified into two methods: incentive mechanism design and collaborative optimization. When data owner is not data consumer, one can induce data owner to adopt higher privacy budget by compensating their privacy loss; when data owner is also data consumer, one can collaboratively optimize data owner's privacy loss and data quality to decide the optimal privacy budget. Recent studies have seen many progress in data utility optimization for LDP, but still exist some drawbacks: a) Data utility of existing aggregation algorithms for high-dimensional data is very low, thus cannot meet the demand for high-dimensional data analysis; b) Existing incentive mechanisms cannot resolve the information asymmetry problem between fusion center and data owners, and

cannot deal with the real-time aggregation applications; c) Collaborative optimization is the key for privacy budget optimization when data owner is also data consumer, while related works is absent. Based on the state-of-the-art, this thesis proposes some mechanisms to improve the drawbacks, including:

1. Study high-dimensional data aggregation algorithm with high data utility. Marginal table is the work horse of high-dimensional data analysis. Thus, we take marginal release as an study object and explore the aggregation algorithm optimization strategy for high-dimensional data analysis. This thesis propose CALM to utilize a set of carefully chosen marginals, which we call views, to capture the correlation of all high-dimensional attributes. Then, all the other marginals can be reconstructed by using consistent views and maximum entropy optimization. The novelty of CALM is that, we propose a practical algorithm to choose an optimal set of views by analyzing multiple error sources. This has significantly alleviate the impact of perturbation. Further, CALM can deal with non-binary attributes with too many attributes, and improve the performance of the state-of-the-art by 1 to 2 orders of magnitude.

2. Study static incentive based privacy budget optimization. The main idea is to induce users to adopt higher privacy budget by compensating their privacy loss, thus improving the data utility. The privacy loss is determined by both privacy budget and privacy preference which varies among users. For example, women care more about their age than men, patients care more about their location than healthy people. In incentive mechanism design, fusion center always do not know users exact privacy preferences, leading to information asymmetry problem. This thesis design REAP to solve the information asymmetry problem by resorting to Contract Theory. Specifically, assume that fusion center knows the distribution of users' privacy preferences and intend to design a contract for each type of users, each contract consists of a tuple of privacy budget and the corresponding compensation. The fusion center broadcasts all the contracts to all users, and each user can choose one contract that optimize his utility. The challenge lies in how to ensure all users to truthfully reveal their privacy preferences. REAP deal with this problem through solving an optimization problem with incentive compatibility constraints.

3. Study dynamic incentive based privacy budget optimization. Real-time data aggrega-

tion holds a wide spectrum of crowdsensing applications. For example, public health monitoring organizations can periodically collect physical index data from users to monitor and control the spread of disease, thus requires users' long-term participation. Previous studies on static incentive cannot fullfill this requirement, since they may cause some users unselected for a long time and then quit. To guarantee long-term participation in real-time data aggregation, this thesis design LEPA that uses on-line algorithm to jointly optimize the system utility in each time slot, and guarantees all users to be selected with certain probability.

4. Study the collaborative optimization for privacy budget and data utility. Collaborative optimization method is designed for the scenario where data owner is also the data consumer, this thesis investigates one typical application, i.e., location privacy protection and spectrum allocation in database driven cognitive radio. Database driven cognitive radio is an effective method for solving the interference between primary users and secondary users. However, this technology requires primary users and secondary users to provide their location information directly or indirectly for dynamic spectrum allocation. This thesis designs a privacy-preserving utility maximization database query protocol UMax. By collaboratively optimizing location privacy and spectrum utilization, UMax allows two parties to choose their optimal privacy budget to optimize the data utility, thus improving the spectrum utilization.

Keywords: Local differential privacy, aggregation algorithm optimization, incentive mechanism design, collaborative optimization, crowd sensing system

目录

插图

表格

第一章 绪论

本章摘要： 本章首先介绍了本地差分隐私的研究背景，并指出隐私保护与数据可用性之间的矛盾；然后介绍了提升数据可用性方法的研究现状，并指出现有研究工作中存在的不足；最后，介绍本文研究动机和研究内容。

关键词： 本地差分隐私，数据可用性优化，融合算法优化，隐私预算优化，激励设计，协同优化，研究现状，研究不足，研究动机，研究内容

1.1 研究背景

1.1.1 数据隐私及其保护技术

随着互联网与通信技术的高速发展，全球数据总量正以惊人的速度增长，预计到 2020 年全球数据使用量将达到 35ZB[1]。数据的不断累积形成了丰富的大数据资源，并蕴含了大量潜在的有价值信息，对这些信息的挖掘与使用能带来巨大的经济与社会效益。例如，医疗机构可以通过对大量医疗数据的挖掘，得到对疾病更深入的认识，并促进诊断及治疗技术的进展；互联网服务商可以通过分析用户的上网行为，为用户提供更加便捷和个性化的服务。麦肯锡公司指出，目前大数据贯穿了包括教育、交通、商业、电气、石油天然气，卫生保健和金融在内的七大行业，如果这些行业都公开各自数据集，将带来 3 万亿美元的经济收益[2]。正因如此，经济学人杂志把数据称为数字时代的石油[3]。然而数据并不是凭空产生的，一般都以人作为载体，因此包含着大量的个人私密信息，比如医疗记录和上网足迹等。如果不加约束得使用这些数据将不可避免得泄露个体用户的隐私并可能造成恶劣影响[4–6]。

近年来，由于隐私保护措施不力导致的严重隐私泄露事件时有发生[7]。例如，在 2006 年，美国在线公布了 650,000 名用户三个月内的搜索日志，并简单得采用把用户 ID 替换成随机编码的方式来保护隐私。在数据集公布后的几天，两名纽约时报记者通过对照电话本中的公开信息推断出了数据集中某些用户的真实身份。这个丑闻直接导致了针对美国在线的大量诉讼，及其首席技术官的辞职[8]。网飞公司于 2009 年公布了 500,000 用户的电影打

分数据，旨在举办一场数据挖掘比赛来获得用户偏好估计算法，并简单采用匿名化方法来保护隐私。研究者发现，尽管该数据集不包含用户身份信息，通过对照 IMDB 数据集还是可以识别出部分网飞数据集中用户的身份[9]。2014 年，纽约城市交通和汽车委员会公布了 17.3 亿条出租车出行记录，并去除了乘客身份等敏感信息。然而通过对比网络上收集的名人乘车照片和出租车车牌号，攻击者成功识别出了某些名人的上下车时间、上下车地点和乘车费用等敏感信息[10]。

为此，各国政府陆续出台了相应的法律法规用于保护消费者的数据隐私。2012 年 2 月，美国总统奥巴马签署了《消费者隐私权利法案》，用于限制互联网公司对用户隐私数据的滥用，为消费者提供更强的网络隐私保护[11]。欧盟于 2018 年 5 月开始实行号称史上最严隐私保护法案《一般数据保护法案》(General Data Protection Regulation，简称 GDPR)，要求互联网公司必须遵循严格的用户隐私保护条例，否则将被处以非常严厉的罚款[12]。我国也在”十三五”规划中提出了加强数据资源安全保护的方针。《2006-2020 年中长期规划(纲要)》中提出了发展信息产业的七大优先主题，其中“面向核心应用的信息安全技术”是其中之一，《纲要》中明确要求重点突破国家基础信息网络和重要信息系统中的安全保障技术[13]。

在学术界，研究者们从技术层面提出了大量数据隐私保护技术。目前主流的数据隐私保护技术主要分为以下三大类：

- **加密技术**。基于加密的数据分析与挖掘主要基于非对称加密技术[14–16]，主要用于保密的交互式计算协议，以支持分布式环境下的数据挖掘。其中，不经意传输机制 (Oblivious Transfer，简称 OT) [17–19] 和安全多方计算 (Multi-party Computation，简称 MPC) [20–22] 是实现加密数据挖掘的代表性技术。加密技术的优点是能实现高可用性的数据挖掘。然而，由加密解密和验证环节带来的计算代价随着训练数据的增长而急剧增长，当数据量巨大时，基于加密的数据挖掘方法计算代价巨大。

- **匿名方法**。匿名方法[23–25] 的主要思想是通过保证多条记录间的不可区分性来保护单个用户的隐私。k-anonymity[23] 和 ℓ-diversity[24] 是比较有代表性的基于匿名方法的隐私保护技术。k-anonymity 保证任意一条记录与至少 $k-1$ 条其他记录的不可区分性，其主要缺点是容易受到一致性攻击(homogeneity attack)和背景知识攻击(background knowledge attack)。为了弥补 k-anonymity 的弱点，研究者们提出了 ℓ-diversity 原则，如果一个数据表满足 k-anonymity，且每个等价类中的敏感属性至少有 ℓ 个值，则称其满足 ℓ-diversity 原则。然而，ℓ-diversity 技术容易受到相似性攻击 (similarity attack)。匿名方法主要的不足在于它们对于攻击模型没有严格定义，因此容易受到很

多新型攻击。

- **数据扰动**。数据扰动技术[26–29] 的核心思想是在处理数据或发布数据时加入适量的扰动，保证在损失少量统计信息精度的情况下，攻击者无法准确推断出个体用户的隐私信息。基于数据扰动的隐私保护技术具有实现简单，计算代价小等优点，因此被广泛应用于隐私保护的数据分析领域。针对数据扰动技术，研究人员提出了很多隐私定义，包括差分隐私（differential privacy）[30]，差分能识性（differential identifiability）[31]，最小熵（minimum entropy）[32] 和互信息（mutual information）[26] 等。其中，差分隐私技术因其严格的数学定义，以及能提供不依赖于攻击者背景知识的隐私保障，得到了学术界和工业界的广泛认可，并已经成为隐私研究的黄金标准。

1.1.2 差分隐私技术

差分隐私的核心思想是通过对原始数据进行随机扰动处理，使得有任意背景知识的攻击者在得到扰动数据后无法准确推断出原始数据，并提供了对隐私保护程度的精确数学定义。差分隐私技术包括集中式差分隐私和本地差分隐私。其中，集中式差分隐私用于有可信数据中心的场景，数据中心拥有所有用户的原始数据，仅在处理或发布统计信息的过程中加入扰动。本地差分隐私用于没有可信数据中心的场景，用户自身控制隐私数据，并在上传给数据中心之前，对隐私数据进行扰动处理。在差分隐私文献中，集中式差分隐私往往直接称为差分隐私，以区分于本地差分隐私。本文为了表述清晰，如无特殊说明，差分隐私代表集中式差分隐私和本地差分隐私的统称。

集中式差分隐私的概念最早由 Dwork 等[30] 于 2006 年提出。通过在数据分析过程或者结果中添加扰动，集中式差分隐私保证了数据集中任意一条数据对统计结果的影响都是有限的。这保证了即使攻击者获得了除了某个特定用户的数据外，也无法从统计结果中推断出该特定用户的隐私信息。这是一个非常强的隐私保护手段，只要证明某种算法满足差分隐私，攻击者不可能获得关于目标用户更多的知识[33–35]。实现集中式差分隐私的主要方法有拉普拉斯机制[36]，高斯机制[37] 和指数机制[38]。目前，集中式差分隐私技术已被 Uber 公司部署用于数据库 SQL 查询[39]。

本地差分隐私的概念最早由 Kasiviswanathan 等[40] 于 2011 年提出，该概念刚被提出来时并未受到学术界和工业界的重视。2014 年，谷歌研究人员在信息安全顶级会议 ACM CCS 上提出了著名的 RAPPOR[41] 算法，并积极部署到 Chrome 浏览器中，用于统计不同网页被设置为主页的频率。此后，苹果将本地差分隐私技术嵌入到 iOS 和 macOS 系统中，用于改进 QuickType 和表情符号建议，以及备忘录中的查找提示[42]。微软也使用本地差分

隐私技术用于收集用户在各个 APP 上的使用时长[43]。在众多互联网巨头的推动下，本地差分隐私技术越来越受到工业界和学术界的重视，并迅速成为数据隐私研究领域的热点。

虽然差分隐私技术为数据隐私研究带来了一个黄金标准，但其需要对数据进行扰动的本质不可避免得影响了数据可用性，导致很多互联网公司在把差分隐私应用在自身核心产品上还有很多顾虑。为此，如何在保护隐私的同时，有效提升差分隐私的数据可用性成为其能否实际部署的关键。随着 5G 技术、车联网技术和边缘计算技术的蓬勃发展，本地差分隐私技术的应用范围越来越广。然而，由于本地差分隐私要求每个用户对数据都进行扰动，导致在隐私预算相同的情况下，添加噪音的量级比集中式差分隐私大很多，大大影响了数据可用性。目前，学术界和工业界对本地差分隐私的研究刚刚兴起，对数据可用性优化的研究也相对较少。因此，本文主要针对本地差分隐私的数据可用性优化方法进行深入研究。由于数据可用性在不同应用场景下有不同的定义，比如融合误差、融合精度、频谱利用率等，因此在接下来的章节中，如无特殊说明，这些名词都指代数据可用性。

1.2 研究现状

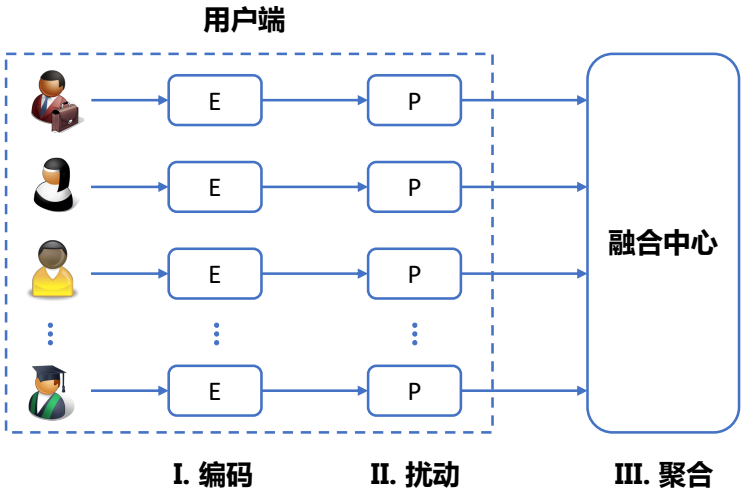


图 1.1 本地差分隐私算法流程

本地差分隐私的数据分析流程可以分成三步[44,45]：编码 (encode)，扰动 (perturb) 和聚合 (aggregate)，如图 1.1所示。其中编码的目的是对原始数据进行压缩以减小随机扰动对数据可用性的影响，同时降低通信代价；扰动的目的是对编码后的数据进行随机化处理以满足本地差分隐私；聚合的目的是针对不同的编码方式，对从用户端收集的随机扰动数据进行聚合解码，从而得到有用的统计信息。分析本地差分隐私算法的三个步骤可以看出，提

升数据可用性可以从两个维度展开——改进编解码算法以及降低扰动水平。具体来说，可以总结成以下两种策略：

1. **融合算法优化**。融合算法优化通过改进编解码算法来降低随机扰动对数据可用性的影响，通常使用不同的数据结构对原始数据进行编码，比如构建前缀树[46]，二叉树[47]和哈希映射[48]等。融合算法优化是目前最主流的本地差分隐私数据可用性优化策略，其设计核心在于如何根据用户拥有的数据类型和融合中心期望的数据分析任务选取合适的数据结构，并通过误差分析确定数据结构的关键结构参数和融合算法的核心参数。

2. **隐私预算优化**。在本地差分隐私中，扰动水平一般通过隐私预算（privacy budget）[1]进行控制。该策略的核心是当融合算法给定时，如何选择最优的隐私预算来最大化数据可用性。目前，隐私预算优化主要有两种方法：激励设计[49,50]和协同优化[51,52]。其中，i）激励设计适用于数据可用性对数据拥有者没有直接影响的场景，融合中心可以通过补偿数据拥有者隐私损失的方式引导其选择更高的隐私预算来提升数据可用性。对于融合中心来说，需要权衡激励成本和数据可用性提升带来的收益。ii）协同优化适用于数据可用性对数据拥有者有直接影响的场景，在这种情况下扰动过大将影响数据拥有者自身的服务质量，因此可以直接站在数据拥有者的角度协同优化隐私预算与数据可用性。

接下来，分别总结融合算法优化和隐私预算优化的国内外研究现状。

1.2.1 融合算法优化

融合算法优化针对不同的数据分析任务进行算法优化设计，因此，接下来将总结一些典型数据分析任务的融合算法优化的研究现状。数据分析认为可以根据用户拥有的数据类型属性分成两类：一类为离散属性数据（包括人的性别，种族，工作类型等，以及商品的种类，品牌，功能等。）分析任务（包括频率估计，高频项估计，频繁项集挖掘等），另一类为连续属性数据（包括人的身高，体重等，以及商品的重量，价格等）分析任务（包括均值估计和基于位置的服务等）。其中，离散属性数据分析的基础为频率估计，连续属性数据分析的基础为均值估计。

[1]在本地差分隐私中，隐私预算代表隐私保护程度参数 ϵ，其中 ϵ 越大，隐私预算越高，隐私保护程度越低。在后文叙述过程中将根据方便程度交叉使用 ϵ，隐私预算和隐私保护程度。

1.2.1.1 离散属性

频率估计。频率估计（frequency estimation）[53–56] 用于估计离散属性的频率分布。目前所有的频率估计方法都基于随机响应技术（random response）[57]。随机响应技术最早于 1965 年提出，用于敏感问题的问卷调查，比如是否身患癌症等。在回答敏感问题之前，被调研用户随机掷一枚硬币，如果正面朝上，回答自己真实情况；如果反面朝上，再掷一枚硬币，并根据硬币朝向进行回答。Dwork 等[58] 证明随机响应方法满足本地差分隐私的定义。基本的随机响应方法只能处理二元属性，后续所有高级频率估计方法都是对随机响应方法的扩展或改进。Wang 等[59] 将随机响应方法扩展到具有 d 个取值的属性，其核心思想是每个用户以概率 p 回答自己的正确取值，并以概率 $(1-p)/(d-1)$ 回答其他取值。文献[41] 提出了另一种处理具有 d 个取值属性的方法。首先对取值进行一元编码（unary encoding），也就是构建一个长度为 d 的二元向量，用户取值所对应的位置为 1，其他位置全部为 0。然后使用基本随机响应方法处理二元向量的每一个位。当属性取值空间很大时，以上方法的通信代价很大。为此，Bassily 等[60] 提出使用哈希映射的方式来减小通信代价。具体来说，每个用户首先在一个哈希函数族里随机选取一个哈希函数，然后把取值映射到一个二元值上并使用基本随机响应扰动该二元值，最后把随机选取的哈希函数和扰动的二元值上传到融合中心。Wang 等[44] 对所有频率估计方法进行了系统化总结，并提出了一个统一的框架。然后通过方差分析，提出了对一元编码方法和哈希映射方法的改进方法。Jia 等[45] 提出，在经典的编码，扰动和聚合三步骤外，可以进一步利用先验知识来提升系统效用。作者指出，实际生活中的大多数据集都服从幂律分布，并且根据分析扰动噪音服从正态分布。结合原始数据集和噪音的先验分布，可以通过求解优化问题来获得误差更小的频率分布估计。

Heavy Hitter **估计**。Heavy hitter 估计[61,62] 研究如何寻找出现频率排名前 k 的取值，比如统计用户浏览器中被设置为主页最多 k 个网页。研究该问题最直观的方法是利用频率估计方法获得属性的频率分布，然后得到排名前 k 的取值。然而，当属性取值空间巨大时，往往无法直接估计频率分布。比如互联网上有上亿个网页，直接估计频率分布的时间复杂度非常高，并且噪音的大小将超过有用信息。已有工作的核心思想是把隐私预算分成两部分，一部分用于寻找取值空间相对较小的候选取值，另一部分在候选取值里使用频率估计方法得到排名前 k 的取值。Heavy Hitter 估计研究的属性往往以字符串的形式出现，比如网站域名和单词等，因此可以使用字符串的性质来选取候选取值。Fanti 等[63] 首先把字符串切分成取值空间相对较小的片段，然后分别使用频率估计方法寻找每个片段中的高频字符串，最后把所有片段中的高频字符串的笛卡尔积作为候选字符串。Bassily 等[60] 设计了一种哈希函数，可以把整个字符串映射到一个整数上，并保证两个高频字符串映射到同一

个整数的概率极低。然后可以针对每一个哈希值，计算出一个高频字符串作为候选字符串。文献[64–66] 分别独立提出了利用前缀树的方法来选取候选字符串。其核心思想是使用频率估计方法来构建前缀树，当得到前缀树每一层节点的频率后，可以通过删除频率较低的节点来减小取值空间。这样做的合理性在于，前缀频率低的字符串是高频字符串的概率极低。最后，通过剪枝形成的前缀树便可以找出候选字符串。

频繁项集挖掘。频繁项集挖掘 (frequent itemset mining) [67–70] 研究当每个用户拥有一个或多个取值时，如何找出频率排名前 k 的取值组合。比如把超市购物记录中的所有商品作为一个集合，每个用户的购物记录包含一个或多个商品。进行频繁集项挖掘的作用在于，如果发现某两件商品同时出现的频率很高，超市可以通过把两件物品摆放在临近位置的方式来增加销量。Qin 等[71] 最早开始研究本地差分隐私设定下的频繁集项挖掘挖掘问题，其核心思想是把隐私预算分成两部分，一部分用于在原始数据的取值空间内上传数据，融合中心选出一部分候选集合；另一部分在候选集合的取值空间内上传数据，融合中心最终确定出现频率最高的取值组合。为了减小通信代价，每个用户随机采样一个取值，然后用任意一种频率估计方法进行扰动。为进一步提高系统效用，Wang 等[72] 对 Qin 的算法进行了改进。作者发现，每个用户的采样行为对隐私保护具有增强作用，因此在调用频率估计方法时可以使用更高的隐私预算，这极大提升了融合精度。此外，Wang 等提出的方法可以处理频繁集合大小任意的情况。

边缘列联表发布。 边缘列联表发布 (marginal release) [73–75] 研究当用户有多个属性并且每个属性有多个取值时，如何计算一部分属性的联合概率分布，也即边缘列联表。目前所有边缘列联表发布的研究均假设需要回答的边缘列联表是未知的，只知道需要回答的边缘列联表包含的属性数量。因此，所有开发的算法需要能回答给定属性数量的所有边缘列联表。解决该问题最直观的方法是首先把所有属性编码成一个属性，然后利用频率估计方法得到全列联表 (full contingency table)，最后通过累加全关联表中的不相关属性，就能得到任意边缘列联表。该方法主要缺点是当用户的属性数量很大时，全列联表的取值空间巨大，无法使用频率估计方法得到。为此，Fanti 等[63] 提出把用户隐私预算分成 d 份，分别用于扰动所有 d 个属性。收到经过扰动处理的属性值后，融合中心可以通过期望最大化算法 (Expectation Maximization，简称 EM) 来估计所需要的边缘列联表。该方法只能处理两个属性的情况，随后 Ren 等[76] 把该方法扩展到能够处理多个属性的情况。该方法的主要缺点是，隐私预算必须被切分成 d 份，当 d 很大时，将对数据造成太大的扰动，从而影响融合精度。Kulkarni 等[77] 提出使用傅里叶变换把原始数据映射到傅里叶空间，然后使用少量傅里叶系数构建任意边缘列联表。该方法的合理性在于，构建任意 k-路边缘列联表，只需要用到少数傅里叶系数。

范围查询。范围查询（range query）[78–81] 计算处于某些属性给定范围内的用户数量。比如在人口普查数据集中，计算满足身高在 160 厘米到 180 厘米，年龄在 20 到 40 岁，年收入在 8 万到 12 万的用户数量。该问题在传统差分隐私里面有大量研究，但在本地差分隐私设定下，目前只有一个研究工作[82]。Wang 等提出了一种基于层级结构（hierarchy-based）的方法把属性构建成二叉树。二叉树的顶层包含所有可能取值，第二层把取值空间平均分成两份，以此类推，直到某一层的属性分成只有一个取值为止。然后把隐私预算平均分配给各层，每个用户对每一个层级利用一种频率估计方法上传数据。融合中心在收到所有用户数据后可以得到二叉树所有节点的频率值，有了这些频率值便可以回答任意范围查询。具体来说，给定一个范围查询，首先从根节点遍历二叉树，如果给定范围不包含于某个分支，直接丢弃该分支数据；如果给定范围完全包含于某个分支，直接使用该层的数据进行频率估计，不再向下遍历；如果给定范围部分包含在某个分支，那么继续向下遍历二叉树直到给定范围完全包含在某个二叉树分支。

合成数据集。目前，大多数已有研究工作均针对特定数据分析任务进行融合算法优化，这种方法很有效然而却费时费力。一种更加通用的解决方案是利用本地差分隐私收集上来的数据生成一个合成数据集（synthetic dataset），数据分析人员接下来可以在该合成数据集上执行任何数据分析任务[83–85]。但该领域的研究尚处于初步阶段，现有方法很难达到专门为特定数据分析任务设计的优化算法，因此是一个很有潜力的研究方向。Ren 等[76] 提出了一种发布高维离散数据的方法。每个用户拥有多个属性，每个属性拥有多个可能取值。其核心思想是利用边缘概率表发布方法获得一系列边缘概率表来捕捉属性之间的联合概率分布，接下来利用边缘概率表对属性进行顺序抽样，最终生成拟合原始数据集分布的合成数据集。

1.2.1.2 连续属性

相较于离散属性，连续属性的研究目前还处于初级研究阶段，并且主要集中在简单的均值估计和基于位置的服务。

均值估计。均值估计（mean estimation）的研究目标是估计所有用户某个连续属性的均值。研究该问题最简单的方式是经典的拉普拉斯机制[36]，每个用户直接在隐私数据上加入拉普拉斯噪音，并上传给融合中心。由于拉普拉斯机制的融合误差与隐私预算成反比，导致其隐私预算很小时误差巨大。并且由于拉普拉斯分布具有长尾效应，用户上传的数值是没有边界的，这进一步增大了误差。为解决拉普拉斯机制上传数值无界的问题，Duchi 等[86] 提出了一种上传数值有界的方法。在 Duchi 的方法中，每个用户只可能上传两种可能取值 d

和 $-d$，上传两个取值的概率与其真实取值有关。直观上来说，真实取值越大，上传 d 的概率越高，反之上传 $-d$ 的概率越高。Duchi 方法在隐私预算较小时融合误差较小，而当隐私预算较大时，其性能甚至低于拉普拉斯机制。为此，Wang 等[87] 提出了一种同时具有拉普拉斯机制和 Duchi 机制优点的新方法——分段机制（Piecewise Mechanism）。在分段机制中，用户上传的数值也是有界的，但与 Duchi 机制不同的是，分段机制允许用户上传某个区间 $[-C, C]$ 里面的值，上传不同取值的概率与用户的真实取值有关。

基于位置的服务。基于位置的服务（location-based service）[88–92] 的研究目标是，如何在不暴露自身精确位置的情况下，获得某种基于位置的服务，比如寻找附近餐馆，使用签到应用程序等。该问题可以看成用户拥有一个二维的连续属性。Andres 等[93] 从差分隐私的定义出发，提出了 geo-indistinguishability 的概念，用于位置隐私保护。Geo-indistinguishability 允许用户以真实位置为中心，通过二维拉普拉斯分布采样一个虚假位置上传给服务器。当用户处于运动状态并且需要连续上传位置信息时，由于位置之间具有关联性，如果每次都单独使用 Geo-indistinguishability 机制上传位置，将无法保证用户期望的差分隐私保护。为解决连续位置上传的问题，Xiao 等[94] 首先提出了 δ-位置集的概念来建模位置序列之间的关联性，然后使用基于闵可夫斯基范数[95] 的采样机制来产生虚假位置。

1.2.2 隐私预算优化

相对于融合算法优化，目前对隐私预算优化的研究工作相对较少。接下来分别针对隐私预算优化的两种策略（采用激励设计和协同优化隐私与效用），进行研究现状总结。

1.2.2.1 采用激励设计

激励设计的思想最早应用于集中式差分隐私，目前只有少量工作把该思想应用于本地差分隐私。为了梳理清楚该思想的发展脉络，我们首先介绍激励设计思想在集中式差分隐私上的应用，然后介绍已有的应用于本地差分隐私中研究。

集中式差分隐私。Gosh 等[49] 于 2011 年首次提出利用激励设计的思想来提升集中式差分隐私的系统效用，并研究了两种不同设定：一种假设隐私偏好不是敏感信息，另一种假设隐私偏好是敏感信息。对于第一种设定，作者设计了两个基于拍卖理论的收购方案，一个在经济预算固定的情况下，尽可能收购质量高的数据来最大化系统效用，另一个在系统效用给定的情况下，最小化收购预算。对于第二种设定，作者证明我们无法设计一种满足个体理性的机制来获得足够精确的融合数据。为了避开第二种设定下不可能的结果，研究者们陆续提出了一些改进策略[96–99]。文献[96,97] 等考虑了贝叶斯设定，假设融合中心对用户

的某些属性有一定的先验知识。其中，Fleischer 等[96] 假设用户的隐私偏好满足一个已知分布，并证明在这种设定下可以得到一个满足 Bayes-Nash 真实性，个体理性的激励机制。Roth 等[97] 假设用户的效用函数服从一个已知分布，并提出了一种满足个体理性和后验真实性的激励机制。Nissim 等[99] 放松了贝叶斯先验假设，只假设用户数据和隐私偏好之间的关联性满足某种单调特性，同时提出了一种满足个体理性和真实性的激励机制。以上研究都假设用户的隐私数据之间不存在关联性。最近，Niu 等[100] 借用文献[101–103] 中对关联差分隐私（dependent differential privacy）的定义，解决了在用户隐私数据之间存在关联性的情况下设计有效的激励机制的问题。

本地差分隐私。Wang 等[50] 最早将激励设计的思想引入到本地差分隐私中，并研究了一个非常简单的融合任务。假设每个用户拥有一个 $\{0,1\}$ 二元取值，代表用户是否具有某种属性（比如是否身患癌症），融合中心的目标是统计拥有取值 1 的用户数量。作者提出使用博弈论的思想来协调用户与融合中心之间的效用，并达到用户之间的纳什均衡。在这种框架下，融合中心无法使用最优的经济预算来获得期望的融合精度。文献[104] 使用拍卖理论来出售用户隐私，该论文研究的融合任务是连续属性的均值估计。作者假设所有用户都在原始数据上加入满足 β 分布的噪音，使得所有用户的噪音叠加起来满足拉普拉斯分布，这显然不满足本地差分隐私的定义。此外，现有两个研究工作都只能处理融合中心拥有一个任务的情形。

1.2.2.2 协同优化隐私与效用

隐私保护与系统效用协同优化的核心思想是，协同考虑隐私保护带来的收益和服务质量带来的收益，通过求解优化问题的方式来决定最优的隐私预算。不同应用场景对于服务质量的定义不一样，因此需要根据不同的应用场景建立不同的优化问题。使用该思想进行隐私预算优化的研究工作目前非常少，接下来总结两个已有研究工作。Shokri 等[51] 研究了基于位置的服务的隐私保护问题。给定服务质量损失，通过构建一个线性规划问题，来决策最优的隐私预算。Bordenabe 等[52] 在提出 geo-indistinguishability 的定义后，在后续工作中使用协同优化隐私保护与系统效用的方法对隐私预算进行了优化。具体来说，建立了一个线性优化问题，以服务质量损失为优化目标，以隐私预算为约束，求解出最优的隐私预算。通过分析优化问题的结构，给出了一个低计算复杂度的求解方案。

1.2.3 现有工作存在的不足

近年来，研究者们对本地差分隐私数据可用性优化的研究取得了很多进展，然而现有工作仍然存在以下四方面的不足:

- **高维数据融合算法数据可用性太低：** 目前大多数融合算法研究都针对低维数据，对高维数据融合算法的研究尚处于初步阶段。现有针对高维数据的融合算法不仅数据可用性低，而且计算时间复杂度非常高。在现实生活中，更常见的场景是用户拥有高维属性，融合中心期望获得高维属性之间的关联关系，因此有效提升高维数据的数据可用性至关重要。

- **无法解决融合中心与用户存在的信息不对称问题：** 基于激励设计的隐私预算优化方法的核心思想是，通过补偿用户隐私损失的方式激励其使用更高的隐私预算。用户隐私损失决定于隐私预算和用户隐私偏好，而不同用户的隐私偏好往往是不同的。在激励设计过程中，融合中心很难得知不同用户的具体隐私偏好，造成了融合中心和用户之间的信息不对称问题，现有激励设计方法无法解决这种信息不对称问题。

- **无法满足实时数据融合应用的需求：**实时数据融合应用广泛存在于现实生活，并要求用户连续不断得贡献数据。然而，目前大多数基于静态激励的方法无法保证用户的长期参与。因为在实时数据融合场景中，如果某些用户长期未被选中将选择退出系统，最终导致后期融合中心用户数量不足严重影响数据可用性。

- **缺乏对基于协同优化的隐私预算优化方法研究：** 数据拥有者与使用者相同的场景在生活中广泛存在，并且基于协同优化的隐私预算优化方法是该场景下数据可用性提升的关键技术，然而这方面相关研究工作仍然比较缺乏。

1.3 本文研究内容

1.3.1 研究思路

针对现有本地差分隐私系统数据可用性优化方法中存在的问题，本文探索了一些解决方案。全文组织结构如图3.2所示。第 1 章绪论介绍本地差分隐私技术的研究背景及数据可用性优化的国内外研究现状，第 2 章介绍本地差分隐私的定义及基础理论，第 3-6 章为论文主体部分，第 7 章对全文进行总结与展望。本文首先研究了高维数据的融合算法优化问题，针对高维数据分析的关键技术——边缘列联表发布——提出了高精度的融合算法，对

应内容为第 3 章。接下来针对现有隐私预算优化方法中存在的不足，提出了相应的解决方案。其中第 4 章提出了基于静态激励的隐私预算优化方法解决了融合中心与用户之间的信息不对称问题；第 5 章提出了基于动态激励的隐私预算优化方法解决了实时数据融合中用户的长期参与问题；第 6 章使用基于协同优化的隐私预算优化方法，解决了数据库驱动认知无线电中位置隐私保护与频谱分配的问题。

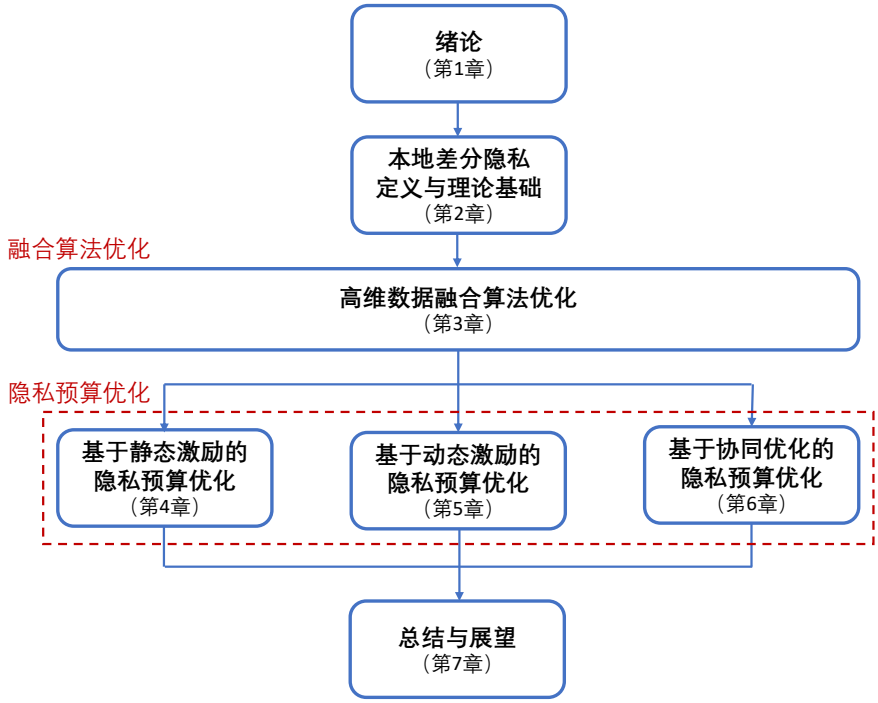


图 1.2　全文组织结构

1.3.2　研究内容

本文具体研究内容和贡献总结如下：

- 第 3 章考虑高维数据的融合算法优化问题。本章以高维数据分析的关键技术边缘列联表发布为切入点，研究高维数据的融合算法优化。为解决现有边缘列联表发布算法数据可用性低和计算时间复杂度高等问题，本章提出了一个高效的边缘列联表发布算法 CALM 。该算法首先通过系统的误差分析选出一组称为视图的边缘概率表；然后使用频率估计方法生成一组满足本地差分隐私的视图，为了提高视图可用性，需要对带扰动的视图进行一致性和非负性处理；最后使用一致性视图和最大熵优化理论重构出所有边缘概率表。在真实数据集上的大规模实验证明 CALM 能显著提升边缘列联表数据可用性以及降低算法复杂性。

- 第 4 章考虑基于静态激励的隐私预算优化问题。基于激励设计的隐私预算优化方法通过补偿用户隐私损失的方式激励其使用更高的隐私预算，从而间接提升数据可用性。用户隐私损失与隐私预算和隐私偏好密切相关。为解决融合中心与用户之间的信息不对称问题，也就是融合中心无法得知用户具体隐私偏好，本章提出了一种基于契约理论的静态激励方法 REAP 。融合中心为不同隐私偏好用户设计不同的契约，每个契约包含一种隐私预算，以及用户采用该隐私预算可以获得的补偿。设计最优契约的核心是，如何保证用户在选择自身隐私偏好对应的契约时才能获得最大的效用。大量仿真结果证明了 REAP 能有效提升融合中心的数据可用性。

- 第 5 章考虑基于动态激励的隐私预算优化问题。上一章提出的静态激励方法不适用于实时数据融合的场景，因为实时数据融合应用需要周期性得收集用户信息，而静态激励方法容易导致某些用户长期未被选中从而退出系统，无法保证用户的长期参与。本章设计了 LEPA 方法来保证实时数据融合场景下用户的长期参与。具体来说，首先推导出不同任务的融合精度要求与用户隐私预算之间的定量关系；然后设计一个在线算法来联合优化各个时隙之间的系统效用，以此防止用户中途退出。考虑到用户的自私行为以及感知任务的组合特性，本章提出了一种高效的在线拍卖机制，该机制具有近似最优解，真实性以及个体理性等性质。

- 第 6 章考虑基于协同优化的隐私预算优化问题。基于协同优化的方法适用于数据拥有者与使用者相同的场景，本章研究一个典型场景——数据库驱动认知无线电动态频谱分配问题。数据库驱动认知无线电技术是解决一级用户和二级用户之间相互干扰的有效技术手段。然而该技术的实现要求一级用户和二级用户直接或间接得提供自身位置信息进行动态频谱分配，产生了隐私泄露的风险。本章研究了如何在同时保护一级用户和二级用户位置隐私的前提下，最大化频谱利用率的方法。具体来说，设计了一种隐私保护的效用最大化数据库访问协议 UMax ，通过位置隐私保护与频谱利用率之间的协同优化，允许一级用户和二级用户选择最优隐私预算来最大化频谱利用率。

最后，第 7 章对全文进行了总结，并提出了未来可能的研究方向。

第二章　本地差分隐私定义与理论基础

本章摘要： 本章分别介绍集中式差分隐私和本地差分隐私的定义、区别及联系；介绍离散属性数据分析任务基础——频率估计，及三种经典频率估计方法和适用范围；介绍连续属性数据分析任务基础——均值估计，及三种经典均值估计方法和适用范围。

关键词： 集中式差分隐私，本地差分隐私，频率估计，均值估计

2.1　差分隐私定义

为了更好得理解本地差分隐私，首先简单介绍一下集中式差分隐私。

2.1.1　集中式差分隐私

集中式差分隐私应用于有可信融合中心的场景，融合中心拥有所有用户的原始数据，仅在处理或发布统计结果时进行扰动处理。直观上来看，集中式差分隐私保证了数据集中任意一条记录对输出结果的影响是有限的。集中式差分隐私的正式定义如下：

定义 2.1.1 (ϵ-集中式差分隐私). 一个算法 A 满足 ϵ-集中式差分隐私，其中 $\epsilon \geq 0$，当且仅当对于任意两个相差一条记录的数据库 DS 和 DS'，有

$$\forall T \subseteq \text{Range(A)}: \ \Pr\left[\text{A}(DS) \in T\right] \leq e^{\epsilon} \Pr\left[\text{A}(DS') \in T\right],$$

其中，Range(A) 表示扰动算法 A 所有可能的输出。

2.1.2　本地差分隐私

在差分隐私的本地设定下，每个用户拥有一个在取值空间 D 内的取值 v。融合中心的目标是，在保证个体用户数据隐私的前提下，获得所有取值的频率分布。更复杂的数据分析任务均可以通过数据结构的编解码转化成这种模型。具体来说，每个用户使用扰动算法

Ψ 来处理隐私数据 v，并把 $\Psi(v)$ 发送给融合中心进行处理。正式的，算法 $\Psi(\cdot)$ 需要满足以下属性：

定义 2.1.2 (ϵ-本地差分隐私). 算法 $\Psi(\cdot)$ 满足 ϵ-本地差分隐私，其中 $\epsilon \geq 0$，当且仅当 $v_1, v_2 \in D$，有

$$\forall T \subseteq \text{Range}(\Psi): \Pr[\Psi(v_1) \in T] \leq e^{\epsilon} \Pr[\Psi(v_2) \in T],$$

其中 Range(Ψ) 表示 Ψ 所有可能的输出.

由于用户不把 v 上传给融合中心，而只是上传 $\Psi(v)$，因此即使融合中心是恶意的，用户的隐私同样能得到很好的保护。

2.1.3 集中式差分隐私与本地差分隐私区别

根据集中式差分隐私和本地差分隐私的定义，可以总结出两者有以下三个核心区别：

- **可信边界不同**。集中式差分隐私的融合中心拥有所有用户的原始数据，仅在发布统计信息时添加扰动，因此可信边界为融合中心。本地差分隐私允许个体用户在自身隐私数据上加入扰动，因此其可信边界为用户自身。

- **实现机制不同**。集中式差分隐私的主要实现机制为拉普拉斯机制，高斯机制和指数机制。而本地差分隐私的实现机制主要为随机响应及其扩展和改进。

- **噪音量级不同**。由于集中式差分隐私只在整体发布结果上进行扰动，而本地差分隐私需要在每个用户的数据上添加扰动，因此本地差分隐私的噪音水平往往比集中式差分隐私高出几个数量级。理论上对于大多数数据分析任务来说，本地差分隐私的噪音方差水平为 $\Theta\left(\frac{1}{\sqrt{n}}\right)$，集中式差分隐私方差水平为 $\Theta\left(\frac{1}{n}\right)$，其中 n 为用户数量，即本地差分隐私的噪音水平为集中式差分隐私的 $\sqrt{n}$ 倍。

2.2 频率估计

频率估计 (Frequency Oracle，简称 FO) 的研究目标是在满足本地差分隐私的基础上，计算任意取值 $x \in D$ 的频率分布。FO 由一对算法 $\{\Psi, \Phi\}$ 组成：用户使用 Ψ 来扰动自身隐私数据，融合中心使用 Φ 来获得频率分布。

2.2.1　广义随机响应法

广义随机响应法（Generalized Randomized Response，简称 GRR）是基本随机响应技术[57] 的直接扩展。具体来说，拥有隐私数据 $v \in D$ 的用户以概率 p 上传真实取值 v，并以概率 $1-p$ 随机上传一个 $v' \in D$ 使得 $v' \neq v$。扰动函数正式定义如下：

$$\forall_{y \in D} \Pr\left[\Psi_{\mathrm{GRR}(\epsilon)}(v) = y\right] = \begin{cases} p = \frac{e^{\epsilon}}{e^{\epsilon}+d-1}, & \text{if } y = v \\ q = \frac{1}{e^{\epsilon}+d-1}, & \text{if } y \neq v \end{cases} \tag{2.1}$$

由于 $\frac{p}{q} = e^{\epsilon}$，因此以上扰动算法满足 ϵ-本地差分隐私。为了估计任意 $v \in D$ 的频率（也就是拥有取值 v 的用户比例），融合中心可以计算 v 被上传的次数 $C(v)$，并通过以下融合算法对 $C(v)$ 进行校正以获得真实频率：

$$\Phi_{\mathrm{GRR}(\epsilon)}(v) = \frac{C(v)/n - q}{p - q}$$

其中 n 为总的用户数量。

举例来说，如果真实有 20% 用户拥有取值 v，扰动后上传取值 v 的用户数量的期望为 $0.2*n*p+0.8*n*q$。如果融合中心刚好收到取值 v 的数量为 $0.2*n*p+0.8*n*q$，那么真实 v 的数量估计值为

$$\frac{(0.2np+0.8nq)/n - q}{p-q} = \frac{0.2p+0.8q-q}{p-q} = \frac{0.2p-0.2q}{p-q} = 0.2$$

文献[44] 证明了 $\Phi_{\mathrm{GRR}(\epsilon)}(v)$ 为无偏估计，估计方差为

$$\mathrm{Var}[\Phi_{\mathrm{GRR}(\epsilon)}(x)] = \frac{|D| - 2 + e^{\epsilon}}{(e^{\epsilon}-1)^2 \cdot n} \tag{2.2}$$

当取值空间 $|D|$ 逐渐增大时，GRR 方法的精度急剧下降。从公式 (2.2)可以看出，GRR 的方差与 $|D|$ 成正比。

2.2.2　最优一元编码法

最优一元编码法（Optimized Unary Encoding，简称 OUE）通过对原始数据进行一元编码的方法，解决了估计方差依赖于 $|D|$ 的问题。具体来说，把取值 $v \in [0..d-1]$ 编码成一个长度为 d 的二元向量，该向量第 v 位为 1 其他所有位都为 0。因此，两个不同取值经过一元编码后最多只有两个位是不一样的。接下来 OUE 对每一个位进行 GRR 操作。为了获得最低的估计方差，对二元向量中的 1 和 0 进行扰动的概率可以不同。所有的 1 都以 0.5 的概率变成 0，这可以看成使用 $\epsilon = 0$ 的 GRR，这样做的好处是融合中心可以最大的

隐私预算 ϵ 来处理剩下的 $|D|-1$ 个 0，使得从 0 变成 1 的数量尽可能少。这种方法可以使得在 $|D|$ 很大时，估计方差最小[44]。

从用户 $j \in [n]$ 中分别收到数据 y^j 后，融合中心可以统计出二元向量中每一位被置为 1 的数量，也就是 $C(x) = |\{j \mid y_x^j = 1\}|$。接下来，可以使用以下变换得到每一位真实计数的无偏估计

$$\Phi_{\mathrm{OUE}(\epsilon)}(x) = \frac{C(x)/n - q}{\frac{1}{2} - q}$$

文献[44] 证明了扰动算法 $\Psi_{\mathrm{OUE}}(\cdot)$ 满足本地差分隐私，融合算法 $\Phi_{\mathrm{OUE}(\epsilon)}(x)$ 是无偏的并且方差为

$$\mathrm{Var}[\Phi_{\mathrm{OUE}(\epsilon)}(x)] = \frac{4e^\epsilon}{(e^\epsilon - 1)^2 \cdot n} \tag{2.3}$$

2.2.3 最优本地哈希法

最优本地哈希法（Optimized Local Hashing, 简称 OLH ）适用于取值空间 $|D|$ 巨大的情形。其核心思想是使用哈希映射的方法把巨大的原始取值空间映射到相对较小的取值空间来降低通信代价。首先利用哈希函数把输入值映射到一个取值区间为 g 的空间（一般 $g \ll |D|$），然后利用 GRR 扰动哈希值并上传。OLH 方法中的哈希操作和扰动操作都会导致信息损失，因此在选择 g 时需要权衡两种操作之间的信息损失。文献[44] 指出，g 的最优取值为 $\lceil e^\epsilon + 1 \rceil$。

在 OLH 中，扰动机制为

$$\Psi_{\mathrm{OLH}(\epsilon)}(v) = \{H, \Psi_{\mathrm{GRR}(\epsilon)}(H(v))\},$$

其中 H 是从可以把取值空间 D 映射到 $\{1 \ldots g\}$ 中的哈希函数族中随机选择的。$\Psi_{\mathrm{GRR}(\epsilon)}$ 的定义为公式 (2.1)，该操作的取值空间为 $\{1 \ldots g\}$。

令 $\{H^j, y^j\}$ 代表第 j 个用户的上传值。对任意 $x \in D$，统计出频率 $C(x) = |\{j \mid H^j(x) = y^j\}|$，其中 $C(x)$ 代表融合中心接收到 x 的数量。接下来，使用下面公式把 $C(x)$ 变换成无偏的估计值：

$$\Phi_{\mathrm{OLH}(\epsilon)}(x) \frac{C(x) - n/g}{p - 1/g}. \tag{2.4}$$

$\Phi_{\mathrm{OLH}(\epsilon)}(x)$ 的估计方差为

$$\mathrm{Var}[\Phi_{\mathrm{OLH}(\epsilon)}(x)] = \frac{4e^\epsilon}{(e^\epsilon - 1)^2 \cdot n}. \tag{2.5}$$

2.2.4　方法比较与选择

从公式 (2.3)和 (2.5)中可以发现，OUE 和 OLH 的估计方差相同。从通信代价的角度来看，OUE 的通信代价为 $\Theta(|D|)$，OLH 的通信代价为 $\Theta(\log n)$。比较 (2.2)和 (2.3)，可以发现，GRR 的估计方差依赖于 $|D|$，而 OUE 和 OLH 仅仅依赖于 ϵ 和 n。通过以上观察，可以总结出以下频率估计方法的选取准则[44]：

- 当 $|D|$ 很小时（$|D|-2<3e^{\epsilon}$），GRR 方法是最好的选择。
- 当 $|D|-2<3e^{\epsilon}$，并且通信代价 $\Theta(|D|)$ 可以接受时，应该选择 OUE 。因为相比较于 OLH ，OUE 实现比较简单，而且由于不需要进行哈希运算，计算速度也更快。
- 当 $|D|$ 非常大以至于通信代价过高时，应该选择 OLH 。因为 OLH 在保证与 OUE 具有相同估计误差的情况下，通信代价小很多

2.3　均值估计

均值估计为连续属性数据分析任务的基础，并每个用户拥有一个取值范围为 $[-1,1]$ 的连续值 v_i。如果 v_i 的取值范围为 $[a,b]$，可以通过公式 $(2v_i-a-b)/(b-a)$ 将 v_i 映射到 $[-1,1]$ 内。均值估计也可以用一对算法 $\{\Psi,\Phi\}$ 来分别表示用户的扰动机制和融合中心的融合机制。

2.3.1　拉普拉斯机制

拉普拉斯机制（Laplace Mechanism，简称 LM ）是实现集中式差分隐私最基本的方法，也可以用来实现连续属性的本地差分隐私。当属性 a 的取值范围为 $[-1,1]$ 时，可以认为其敏感度为 2。因此扰动机制可以定义为

$$\Psi_{\mathrm{LM}(\epsilon)}(v_i)=v_i+Lap(\frac{2}{\epsilon})$$

其中 $Lap(\lambda)$ 表示服从拉普拉斯分布的随机变量，其概率密度函数为 $Lap(x)=\frac{1}{\lambda}exp(\frac{-|x|}{\lambda})$。

由于加入的拉普拉斯噪音均值为 0，因此 $\Psi_{\mathrm{LM}(\epsilon)}(v_i)$ 是无偏的。融合中心可以直接计算 $\Psi_{\mathrm{LM}(\epsilon)}(v_i)$ 的均值，也就是

$$\Phi_{\mathrm{LM}(\epsilon)}(v_i)\frac{1}{n}\sum_{i=1}^{n}\Psi_{\mathrm{LM}(\epsilon)}(v_i) \tag{2.6}$$

其中，n 为所有用户的数量。

由于 $\Phi_{\mathrm{LM}(\epsilon)}(v_i)$ 和 $\Psi_{\mathrm{LM}(\epsilon)}(v_i)$ 的估计方差只相差一个 $\sqrt{n}$ 的因子，所以可以通过讨论 $\Psi_{\mathrm{LM}(\epsilon)}(v_i)$ 的估计方差来分析均值估计的方差，也就是

$$\mathrm{Var}[\Psi_{\mathrm{LM}(\epsilon)}(v_i)] = \frac{8}{\epsilon^2} \tag{2.7}$$

从公式 (2.7)可以看出，估计方差与 ϵ^2 成反比，当 ϵ 很小时，估计方差非常大。另外，由于拉普拉斯分布具有长尾效应，用户上传的扰动数据是无界的，这进一步增大融合误差。

2.3.2 杜奇机制

为解决 LM 方法扰动数据无界的问题，Duchi 等[86] 提出了一种保证扰动数据有界的方法（Duchi's Mechanism，简称 DM）。DM 方法中所有用户只会给融合中心上传两个取值，$\frac{e^\epsilon+1}{e^\epsilon-1}$ 或者 $-\frac{e^\epsilon+1}{e^\epsilon-1}$，它们的概率取决于隐私预算 ϵ 和用户的真实值 v_i。具体来说

$$\Pr\left[\Psi_{\mathrm{DM}(\epsilon)}(v_i) = y\right] = \begin{cases} \frac{e^\epsilon-1}{2e^\epsilon+2} \cdot v_i + 0.5, & \text{if } y = \frac{e^\epsilon+1}{e^\epsilon-1} \\ -\frac{e^\epsilon-1}{2e^\epsilon+2} \cdot v_i + 0.5, & \text{if } y = -\frac{e^\epsilon+1}{e^\epsilon-1} \end{cases}$$

Duchi 等[86] 证明了 $\Psi_{\mathrm{DM}(\epsilon)}(v_i)$ 是无偏估计，因此其融合算法 $\Phi_{\mathrm{DM}(\epsilon)}(v_i)$ 与 (2.6) 相同。类似得，可以通过 $\Psi_{\mathrm{DM}(\epsilon)}(v_i)$ 的估计方差来分析均值估计的方差

$$\mathrm{Var}[\Psi_{\mathrm{DM}(\epsilon)}(v_i)] = \left(\frac{e^\epsilon+1}{e^\epsilon-1}\right)^2 - v_i^2. \tag{2.8}$$

从公式 (2.8)中可以发现，$\mathrm{Var}[\Psi_{\mathrm{DM}(\epsilon)}(v_i)]$ 的最差情况为 $\left(\frac{e^\epsilon+1}{e^\epsilon-1}\right)^2 - v_i^2$，此时 $v_i = 0$。回想 DM 不管在 ϵ 取任何值时，都只上传两个可能值，并且当 $v_i = 0$ 时，$\mathrm{Var}[\Psi_{\mathrm{DM}(\epsilon)}(v_i)]$ 永远大于 1。上面现象导致了当 ϵ 很大时，DM 的估计方差比 LM 还大。

2.3.3 分段机制

分段机制（Piecewise Mechanism，简称 PM）的目标是借鉴 DM 输出有界扰动值的思路，并解决当 ϵ 很大时方差较大的缺点。其核心思想是，根据指定概率在一个有界区间 $[-C, C]$ 内输出任意值。具体来说

$$\Pr\left[\Psi_{\mathrm{PM}(\epsilon)}(v_i) = y\right] = \begin{cases} p, & \text{if } y \in [\ell(v_i), r(v_i)] \\ \frac{p}{e^\epsilon}, & \text{if } y \in [-C, \ell(v_i)] \cup [r(v_i), C] \end{cases}$$

其中

$$
\begin{aligned}
C &= \frac{e^{\epsilon/2}+1}{e^{\epsilon/2}-1} \\
p &= \frac{e^{\epsilon}-e^{\epsilon/2}}{2e^{\epsilon/2}+2} \\
\ell(v_i) &= \frac{C+1}{2}\cdot v_i - \frac{C-1}{2} \\
r(v_i) &= \ell(v_i) + C - 1.
\end{aligned}
$$

文献[87]证明了 $\Psi_{\mathrm{PM}(\epsilon)}(v_i)$ 是无偏估计，因此其融合算法 $\Phi_{\mathrm{PM}(\epsilon)}(v_i)$ 与 (2.6) 相同。因此也可以通过分析 $\Psi_{\mathrm{PM}(\epsilon)}(v_i)$ 的估计方差来分析均值估计的方差

$$
\mathrm{Var}[\Psi_{\mathrm{PM}(\epsilon)}(v_i)] = \frac{v_i^2}{e^{\epsilon/2}-1} + \frac{e^{\epsilon/2}+3}{3(e^{\epsilon/2}-1)^2} \tag{2.9}
$$

2.3.4　方法比较与选择

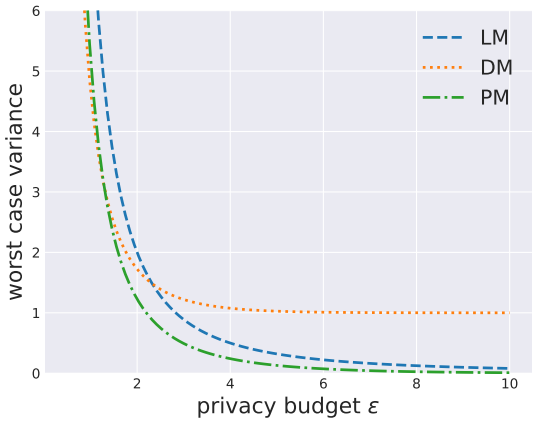


图 2.1　不同均值估计方法在不同 ϵ 下的最差方差

观察公式 (2.8)和 (2.9)可以发现，DM 和 PM 方法单个用户扰动数据的方差与其真实值 v_i 有关，因此最终均值估计的方差与 v_i 的分布有关。为了简化分析，可以通过考虑公式 (2.8)和 (2.9)的最差情况来比较集中方法的均值估计方差。对于 DM 方法，当 $v_i = 0$ 时，公式 (2.8)取得最大值 $(\frac{e^{\epsilon}+1}{e^{\epsilon}-1})^2$；对于 PM 方法，当 $v_i = 1$ 是，公式 (2.9)取得最大值 $\frac{4e^{\epsilon/2}}{3(e^{\epsilon/2}-1)^2}$。

图 2.1展示了三种方法扰动数据的最差方差。从图中可以看出，当 ϵ 很小时，DM 的方差最小；当 ϵ 逐渐增大时，DM 的方差渐进趋向于 1，而 LM 和 PM 的方差渐进趋向于 0。通过以上观察，可以总结出均值估计方法的以下选取准则[87]：

- 当 $\epsilon < 1.29$ 时，DM 在三种方法中的方差最小，因此是最优选择。
- 当 $\epsilon >= 1.29$ 时，PM 在三种方法中的方差最小，因此是最优选择。
- 当 $\epsilon >= 10$ 时，从图中可以看出 LM 渐进趋向于 PM 。考虑到 PM 方法实现的复杂性，可以考虑使用简单的 LM 来替代 PM 。

第三章　高维数据融合算法优化

本章摘要： 边缘列联表是进行高维属性关联分析的基础，也是高维数据分析的关键技术。本章以边缘列联表发布为切入点，研究高维数据的融合算法优化。现有边缘列联表发布算法不仅数据可用性低，而且计算复杂度高。为此，本章提出了一种低复杂度、高可用性的边缘列联表发布算法 CALM 。该算法的核心思想是通过一组称为视图的边缘列联表来获取高维属性之间的关联关系，并使用视图一致性算法和最大熵优化方法重构所有边缘列联表。在 CALM 中只有生成视图时需要接触原始数据，因此极大降低了扰动对数据可用性的影响。基于大量真实数据集的实验结果表明 CALM 比现有最好算法的融合误差降低了一到两个数量级。我们同时评估了 CALM 算法和现有算法在训练分类模型上的表现，在大多数情况下，CALM 算法都能获得接近无噪音情况下的性能，而某些现有算法的性能甚至低于只输出多数标签的基准算法。

关键词： 高维数据分析，边缘列联表发布，误差分析，最大熵优化

3.1　引言

目前大多数融合算法优化的研究都集中于低维属性的频率分析[41,44,60,64,65,71,72]。然而，在现实生活中，更常见的场景是用户拥有高维属性，融合中心期望获得高维属性之间的关联关系。边缘列联表可以通过计算部分属性之间的联合概率分布获取高维属性之间的关联关系，是进行高维属性关联分析的基础。因此，本章以边缘列联表发布为切入点，研究高维属性的融合算法优化问题。

目前只有两个在本地差分隐私设定下的边缘列联表发布算法[76,77]。Kulkarni 等[77] 提出使用傅里叶变换法（Fourier Transformation，简称 FT）对原始数据进行压缩编码，以减小扰动对边缘列联表发布的影响。该方法最早应用于集中式差分隐私的边缘列联表发布问题[74]。Ren 等[76] 提出使用期望最大化方法（Expectation Maximization，简称 EM）来发布边缘列联表，该方法最早由 Fanti 等[63] 提出用于发布仅有两个属性的边缘列联表。然而，现有边缘列联表发布算法在数据维度很高时不仅数据可用性非常低，而且计算时间复杂度非常高。

为此，本章提出了计算效率和数据可用性都更高的 CALM（Consistent Adaptive Local Marginal）方法。CALM 主要受集中式差分隐私中 PriView 方法[73] 的启发，通过选取 m 个大小为 ℓ 的视图来重构出任意边缘列联表。但 PriView 方法只能处理二元属性数据。与 PriView 方法类似，CALM 方法也通过选取一组视图来重构任意边缘列联表。然而，从集中式差分隐私转化到本地差分隐私设定面临许多挑战，因为需要利用复杂的频率估计方法（而非集中式差分隐私中简单的拉普拉斯机制）来构建视图。同时，本章还期望 CALM 方法能够处理非二元属性数据。

进一步，误差分析是本地差分隐私融合算法优化中核心参数选取的基础，而本地设定下的误差分析与集中式设定差异巨大。在大多数本地差分隐私融合算法优化的研究中，主要挑战都是如何设置算法的核心参数，因为核心参数对系统性能的影响是巨大的。之前大多数研究工作都是通过多次试验的方法从经验的角度来选取核心参数，而无法给出理论保障。CALM 方法从误差分析的角度给出了理论上选取核心参数的最优方法。在 PriView 和 CALM 方法中，都需要设定两个核心参数——视图数量和视图大小。相比于集中式差分隐私，在本地差分隐私中多了一种误差来源需要考虑，因此更具挑战性。本章首先分析了不同误差来源对核心参数的影响，并推导出了核心参数与误差之间的定量关系。在误差分析的基础上，本章提出了一套有效的选取最优核心参数的算法。该算法首先设定一个目标误差阈值，然后利用参数误差公式来确定核心参数值。

本章实现了 CALM 方法并通过在真实数据集上的大量实验来评估 CALM 方法的性能。实验结果显示，相比于现有最好算法[77]，CALM 方法的平方和误差（Sum of Squared Errors，简称 SSE）降低了一到两个数量级。另外，只有 CALM 方法能处理属性数量很大的情况，因为其他方法的运算时间复杂度随着属性数量的增加变得非常高。为了展示边缘列联表在实际应用中的重要性，本章同样通过实验评估了 CALM 方法和其他方法在训练预测模型上的表现。在大多数情况下，CALM 方法都能获得接近不加噪情况下的性能，而某些现有算法的性能甚至低于只输出多数标签的基准方法。

本章的贡献总结如下：

- 提出了一种低复杂度、高数据可用性的边缘列联表发布方法 CALM，并能处理非二元属性。
- 通过分析 CALM 方法的三种误差来源，提出了一种有效选取算法核心参数的算法。
- 利用多个真实数据集验证了 CALM 方法相对于现有最好算法的优越性。

本章剩余部分安排如下：第3.2节介绍了边缘列联表发布问题的定义和现有方法；紧接

符号	含义	符号	含义
n	用户数量	F	全列联表
v^j	用户 j 拥有的数值	A	某个属性集合
d	属性数量	M_A	属性集合 A 代表的边缘列联表
$\mathbb{A}$	所有属性的集合	m	本文提出方法输出视图的数量
a_i	属性 i	ℓ	本文提出方法视图的大小
c_i	属性 a_i 所有可能取值的数量	L	所有视图单元数量的平均值
k	目标边缘列联表大小		

表 3.1　第三章符号及含义列表

着第3.3节介绍了本章提出的算法；然后第3.4节给出实验结果；最后第3.5节对本章进行了总结。

表3.1总结了本章用到的所有符号。

3.2　边缘列联表发布问题定义与现有方法总结

本章考虑每个用户拥有高维属性的场景，融合中心需要计算一部分高维属性的联合概率分布。这种高维属性的场景在本地差分隐私的研究中经常出现，比如研究人员在文献[76,77]中研究了满足本地差分隐私的边缘列联表发布问题。

3.2.1　问题定义：集中式差分隐私情形

假设每个用户有 d 个属性 $\mathbb{A} = \{a_1, a_2, \ldots, a_d\}$，其中属性 a_i 有 c_i 种取值，分别表示为 $[c_i] = \{0, 1, \cdots, c_i - 1\}$。每个用户的每个属性有一个取值，因此，用户 j 拥有一个 d 维向量的数据，可以表示成 $v^j = \langle v_1^j, v_2^j, \ldots, v_d^j \rangle$，其中 $v_i^j \in [c_i]$。用户数据的取值空间为 $D = [c_1] \times [c_2] \times \cdots \times [c_d]$，其中 $\times$ 表示笛卡尔积，取值空间大小为 $|D| = \prod_{i=1}^{d} c_i$。

首先考虑融合中心拥有所有用户原始数据的集中式差分隐私设定。当数据集中有 n 个用户时，全列联表 (full contingency table) 代表所有取值 $v \in D$ 的用户比例。用 F 表示全列联表，并称每一个 $v \in D$ 的用户比例为全列联表的一个单元 (cell)。

全列联表计算的是所有属性的联合概率分布。然而，当取值空间非常大时，计算全列联表的代价非常高。在实际生活中，人们往往只对数据集中一部分属性的联合概率分布感

兴趣。对于属性 $A \subseteq \mathbb{A}$，可以用 $V_A = \{\langle v_1, v_2, \ldots, v_d\rangle : v_i \in [c_i] \text{ if } a_i \in A, \text{ or } v_i = *\}$ 来表示 A 的所有可能取值。

对于拥有 k 个属性的集合 A，关于 A 的边缘列联表称为 k-路边缘列联表（k-way marginal），表示为 M_A。k-路边缘列联表给出了 V_A 中所有取值的用户比例。边缘列联表中的每一个取值也叫做一个单元。显然，M_A 比全列联表 F 包含的单元少很多。M_A 中的每个单元都可以通过累加 F 中不在 A 中的属性得到。

	性别	年龄
v^1	男	青年
v^2	女	青年
v^3	女	成年
v^4	女	成年
$\cdots$	$\cdots$	$\cdots$
v^n	男	老年

(a) 数据集

v	$\mathrm{F}(v)$
〈 男，青年 〉	0.20
〈 男，成年 〉	0.15
〈 男，老年 〉	0.20
〈 女，青年 〉	0.15
〈 女，成年 〉	0.20
〈 女，老年 〉	0.10

(b) 全列联表

v	$\mathrm{M}_{\{\text{性别}\}}(v)$
〈 男，$*$〉	0.55
〈 女，$*$〉	0.45

(c) 性别边缘列联表

v	$\mathrm{M}_{\{\text{年龄}\}}(v)$
〈$*$，青年 〉	0.35
〈$*$，成年 〉	0.35
〈$*$，老年 〉	0.30

(d) 年龄边缘列联表

图 3.1　数据集，全列联表和边缘列联表示例

图 3.1给出了一个拥有两个属性的数据集。在集中式差分隐私设定下，融合中心拥有所有用户的原始数据，也就是图 3.1(a)，并可以直接计算出全列联表（图 3.1(b)）。然后，通过全列联表可以分别计算出关于性别和年龄的两个边缘列联表（图 3.1(c,d)）。

3.2.2　问题定义：本地差分隐私情形

在本地差分隐私设定下，融合中心不能直接得到图 3.1(a) 中所示用户的原始数据。相反，每个用户只拥有该数据集中某一行数据，并只上传给融合中心经过扰动处理的数据。本章的目标是使得融合中心在得到扰动处理的数据后，仍然能以较高精度计算出所有 k-路边缘列联表。很多已有方法要求事先指定 k[77]，而本文方法可以支持任意取值的 k。

本文采用平方和误差（Sum of Squared Error，简称 SSE）来衡量算法性能，也就是真实边缘列联表 M_A 与重构边缘列联表 T_A 之间 ℓ_2 距离的平方。当需要计算多个 k-路边缘列联表时，可以利用所有边缘列联表的 SSE 均值来衡量算法性能。

由于重构的边缘列联表 T_A 是通过扰动数据得到的，因此可以看成一个随机变量。当重构算法能保证无偏估计时，T_A 的期望可以作为真实的边缘列联表 M_A，SSE 的期望可以看做随机变量 T_A 的方差。

在本地差分隐私情形下，同样以图 3.1为例。每个用户只拥有图 3.1a中的一行数据，为了得到图 3.1c和 3.1d中的边缘列联表，最简单的方法是首先让每个用户把所有属性编码成一个属性，并使用第二章中的 FO 来获得全列联表，然后通过全列联表计算出边缘列联表。该方法将在后文详细阐述。

3.2.3　全列联表法

全列联表法（Full Contingency Table Method，简称 FC ）是估计 M 最直接的方法，其核心思想是首先构建一个全列联表 F，然后通过全列联表计算所有的 M。在这种方法中，每个用户通过 FO 的扰动算法上传数据 $v \in D$，然后融合中心使用 FO 的融合算法估计出所有取值的频率分布，也就是全列联表。有了全列联表，融合中心可以很容易得计算出任意的 k-路边缘列联表。

FC 的主要缺点是时间复杂度和空间复杂度都随着属性数量 d 的增加而指数型增加。当 d 很大时，FC 在实际使用中的计算成本是不可接受的。

进一步，即使融合中心有足够算力来构建全列联表，构建出来的边缘列联表的误差也会很大。举例来说，假设有 32 个二元属性，取值空间大小为 2^{32}。如果要计算 4-路边缘列联表，每个边缘列联表的每个单元需要累加全列联表中的 2^{28} 个单元。用 Var_0 表示全关量表中每个单元的方差，每个边缘列联表单元的方差就是 $2^{28} \times \mathrm{Var}_0$，因此最终的 SSE 为 $2^4 \times 2^{28} \times \mathrm{Var}_0 = 2^{32} \times \mathrm{Var}_0$。综上，计算 k-路边缘列联表的方差为

$$\mathrm{Var}_{\mathrm{FC}} = 2^d \cdot \mathrm{Var}_0 \tag{3.1}$$

3.2.4　全边缘列联表法

为避免边缘列联表方差对于 d 的指数型依赖，融合中心可以直接构建所有的 k-路边缘概率，称为全边缘列联表法（All Marginal Method，简称 AM ）。该方法有两种实现途径，一种是把隐私预算 ϵ 划分成 $\binom{d}{k}$ 份，每个用户上传 $\binom{d}{k}$ 次数据，每次上传一个边缘列联表。

第二种途径是把用户群体划分成不重叠的 $\binom{d}{k}$ 组，每组用户只上传一个边缘列联表。在本地差分隐私设定下，划分用户比划分隐私预算能获得更好的精度，因为过低的隐私预算会带来过大的扰动。

对本地差分隐私来说，对小群体进行频率估计比对大群体精度更差，因为当群体数量很小时噪音的影响会增大，也就是会有更小的信噪比。一般来说，边缘列联表的方差与群体数量是成反比的。把用户群体划分成 $\binom{d}{k}$ 份会对方差造成 $\binom{d}{k}$ 倍的影响，因此，该方法的方差为

$$\mathrm{Var}_{\mathrm{LM}} = 2^k \cdot \binom{d}{k} \cdot \mathrm{Var}_0 \tag{3.2}$$

从以上两种方法的方差中可以看出，当 k 很小时（也就是 $\binom{d}{k}$ 很小），AM 精度比 FC 高；当 k 很大时，AM 精度比 FC 低。该方法的另外一个局限性是 k 的取值必须事先指定，当算法执行完以后，融合中心无法计算 $t > k$ 的 t-路边缘列联表。

3.2.5 傅里叶变换法

傅里叶变换法（Fourier Transformation Method，简称 FT）最早用于集中式差分隐私的 k-路边缘列联表发布[74]。此后，Kulkarni 等人[77] 把该技术用于本地设定。

FT 的核心思想是，计算所有 k-路边缘列联表只需要用到少量的傅里叶参数。因此，用户只需要上传计算 k-路边缘列联表所需要的那些傅里叶参数即可。

FT 方法的具体步骤如下：定义一个可以把 d 维数据 v 转化成一个整数的函数 $b(\cdot)$，其中 $b(v) = \sum_{i=1}^{d} 2^{d-i} \cdot v_{a_i}$。傅里叶变换的目标是把 $b(v)$ 的标准基 $\mathrm{e}_{b(v)}$ 映射到傅里叶基。具体来说，把所有傅里叶基表示成一个形状为 $2^d \times 2^d$ 的矩阵 $\Omega = \{\omega_{ij}\}$，其中 $\omega_{ij} = 2^{-d/2}(-1)^{\langle i|j\rangle}$，$\langle i|j\rangle$ 表示 i 和 j 在二进制表示下的内积。用户 j 利用基本随机响应上传本地傅里叶参数 $(\Omega \mathrm{e}_{b(v^j)})$ 的第 i 位，i 的二进制表示中 1 的个数小于等于 k。接下来融合中心可以通过下面公式重构出期望的边缘列联表

$$\mathrm{T}_A(v) = \sum_{\alpha \in V_{[d]}, \alpha_{[d]\setminus A}=0} \theta_{b(\alpha)} \cdot \left(\sum_{\eta \in V_{[d]}, \eta_A = v_A} \omega_{b(\alpha),b(\eta)} \right) \tag{3.3}$$

上式中，当 α 固定时，对于所有的 η，$\omega_{b(\alpha),b(\eta)}$ 是相等的。这是因为 α 使得所有不包含在 A 中的位为 0，同时 η 枚举了所有位。因此，只需要枚举所有的 α 即可计算公式 (3.3)。

该方法的优点是计算所有 k-路边缘列联表只需要用到 $\sum_{j=0}^{k} \binom{d}{j}$ 个傅里叶参数。该方法的方差为

$$\mathrm{Var}_{\mathrm{FT}} = \sum_{s=0}^{k} \binom{d}{s} \cdot \mathrm{Var}_0 \tag{3.4}$$

与 AM 方法类似，当 k 和 d 很大时，构建 k-路边缘列联表所需要的傅里叶参数也很大。进一步，该方法只能处理二元属性，如果要处理非二元属性，需要先将其编码成二元属性，这样一来将使得 d 变得更大。举例来说，一个具有 c 个取值的属性需要编码成至少 $\lceil \log_2 c \rceil$ 个二元属性。

3.2.6　期望最大化法

期望最大化法（Expectation Maximization Method，简称 EM）要求每个用户把隐私预算分成 d 份，每份用来上传一个属性。然后融合中心使用期望最大化方法来重构所有的边缘列联表。Fanti[63] 等人首先利用该方法来计算两个属性的联合概率分布，随后 Ren[76] 等人把该方法推广到了多属性的情形。

具体来说，把用户 j 上传的数据表示成 $y^j = \langle y_1^j, y_2^j, \ldots, y_d^j \rangle$，该方法的目标是找到一个概率分布 A，使得对于所有 A，用户 j 上传 y^j 的概率最大。EM 算法主要由两部分组成，E 步和 M 步。在 E 步中，通过以下公式计算似然概率

$$\Pr\left[v|y^j\right]_t = \frac{\Pr[v]_t \cdot \Pr[y^j|v]}{\sum_v \Pr[v]_t \cdot \Pr[y^j|v]},$$

其中 $\Pr[v]_t$ 表示 v 在第 t 轮的概率，$\Pr[v]_0$ 被初始化为 $\frac{1}{|V_A|}$。接下来，通过 M 步更新 $\Pr[v]_t$

$$\Pr[v]_{t+1} = \frac{1}{n}\sum_{j=1}^{n} \Pr\left[v|y^j\right]_t$$

直到对于给定阈值 $\delta > 0$，$\max_v |\Pr[v]_{t+1} - \Pr[v]_t| \leq \delta$。该算法通过 E 步和 M 步迭代最终可以收敛到最大似然函数。

原始的 EM 算法运行效率非常低，因此，本文使用[64] 附录中提出的改进方法来计算 A。大多数情况下，如果使用该方法作为 EM 算法的初始值，EM 算法将会快速收敛。具体来说，改算法首先计算单个属性的分布，然后用这些分布去估计所有属性对的分布，依此类推。Wang 等[64] 证明了该算法是无偏的。

总体来说，EM 方法可以计算任意 k-路边缘列联表，但由于对隐私预算 ϵ 进行了划分，该方法的方差非常大。

3.3　本文方法

由于本章的思想主要受集中式差分隐私中 PriView 方法的启发，因此本部分首先简单介绍一下 PriView 方法。

3.3.1 PriView 方法概述

PriView 方法是为集中式设定下二元属性的边缘列联表发布问题提出的。PriView 的核心思想是首先发布一个满足集中式差分隐私的概要 (synopsis)，然后利用该概要重构出任意 k-路边缘列联表。这里的概要是一个包含 m 个 ℓ-路边缘列联表的集合，我们称这部分边缘列联表为视图 (views)。接下来通过一个例子来说明 PriView 方法的基本思想。假设有 8 个属性 $\{a_1, a_2, \cdots, a_8\}$，目标是计算所有 3-路边缘列联表。PriView 有以下四个步骤 (具体步骤参考[73])：

选取一组最优视图。 第一步是选取一组最少的 m 个视图，使得这些视图能覆盖所有的 2 元或 3 元属性组。比如说，如果目标是覆盖所有的 2 元属性组，可以选取以下 $m = 6$ 组视图：

$$\{a_1, a_2, a_3, a_4\} \quad \{a_1, a_5, a_6, a_7\} \quad \{a_2, a_3, a_5, a_8\}$$
$$\{a_4, a_6, a_7, a_8\} \quad \{a_2, a_3, a_6, a_7\} \quad \{a_1, a_4, a_5, a_8\}$$

我们注意到任意 2 元属性组都被至少一个视图覆盖了。

生成带噪音的视图。 在这一步中，PriView 对每一个视图加入拉普拉斯噪音 $\left(\frac{m}{\epsilon}\right)$ 来保证集中式差分隐私。这一步是唯一需要直接访问数据集的步骤，之后所有都属于后续处理因此不需要再访问数据集。

保证视图一致性和非负性。 得到一组带噪音的视图后，可以直接计算出一部分 3-路边缘列联表。比如说，为了得到包含属性 $\{a_1, a_2, a_3\}$ 的 3-路边缘列联表，可以通过累加视图 $\{a_1, a_2, a_3, a_4\}$ 的属性 a_4 来得到。然而，大多数 3-路边缘列联表都没有被任意一个视图覆盖。比如说，包含属性 $\{a_1, a_2, a_3\}$ 的 3-路边缘列联表没有包含在任意一个视图里，因此需要融合多个视图的信息来重构。融合中心可以首先计算包含属性 $\{a_1, a_3\}$，$\{a_1, a_5\}$ 和 $\{a_3, a_5\}$ 的边缘列联表，然后通过融合这三个边缘列联表来估计 $\{a_1, a_3, a_5\}$。

观察到 $\{a_1, a_5\}$ 既可以从视图 $\{a_1, a_5, a_6, a_7\}$ 中得到，也可以从视图 $\{a_1, a_4, a_5, a_8\}$ 中得到。然而由于这两个视图中都含有相互独立的噪音，因此通过它们得到的 $\{a_1, a_5\}$ 一般来说会不相等。另一方面，带噪音的视图也可能包含负数。PriView 使用约束推断 (constrained inference) 技术来保证所有视图之间的一致性和非负性。具体方法可以参考[73]。

重构所有 k-路边缘列联表。 利用经过一致性处理后的 m 个视图，融合中心可以重构出任意的 k-路边缘列联表。给定 k 个属性，如果这 k 个属性完全包含于某个视图，便可以直接计算出该 k-路边缘列联表。如果没有任意一个视图包含这 k 个属性，PriView 可以通过最大熵估计 (Maximum Entropy Estimation) 方法来计算该 k-路边缘列联表。举例来说，对于给定的三个边缘列联表 $\{a_1, a_3\}$，$\{a_1, a_5\}$ 和 $\{a_3, a_5\}$，最大熵估计可以找到一个对于

$\{a_1, a_3, a_5\}$ 具有最大熵的概率分布，使得它与已知的三个边缘列联表保持一致性。注意到在估计包含属性 $\{a_1, a_3, a_5\}$ 的边缘列联表时，有 7 个未知量（因为该边缘列联表的 8 个单元相加等于 1，减少了一个未知量）。$\{a_1, a_3\}$，$\{a_1, a_5\}$ 和 $\{a_3, a_5\}$ 中每个边缘列联表能给出 3 个等式约束，但他们之间并非相互独立，事实上只有 6 个等式约束是相互独立的。我们知道，一个具有 7 个未知量和 6 个等式约束的方程是没有唯一解的，因此需要通过最大熵估计来找到最优解。

讨论。 利用 PriView 方法，可以得到任意 k-路边缘列联表并且 k 可以任意取值。利用 PriView 生成的 k-路边缘列联表有两个误差来源。噪音误差来源于为满足集中式差分隐私而加入的拉普拉斯噪音，重构误差来源于通过融合多个视图的部分信息来估计 k-路边缘列联表。

有两个关键的算法参数会影响这两类误差，那就是视图数量 m 以及视图大小 ℓ（视图拥有的属性数量）。当 ℓ 变大时，视图将覆盖更多的属性组合，从而减小重构误差，然而边缘列联表需要累加更多的噪音单元，从而增大噪音误差。同理，当 m 变大时，能覆盖更多的属性组合因而能减小重构误差，而更大的 m 也意味着分给每个视图的隐私预算减小，从而增大噪音误差。继续拿前面的 8 个属性举例，使用 14 个（而不是前面的 6 个）大小为 4 的视图可以覆盖所有的 3 元属性组，回答所有的 3-路边缘列联表基本上没有重构误差。然而，这样做的代价是需要对视图中每个单元加入服从 $\left(\frac{14}{\epsilon}\right)$ 的噪音，而非 $\left(\frac{6}{\epsilon}\right)$。需要注意的是，虽然在这种情况下，所有的 3-路边缘列联表都被覆盖了，当回答 $k > 3$-路边缘列联表时同样会有重构误差。

文献[73] 证明，视图大小 ℓ 与数据集大小 n，隐私预算 ϵ 和属性个数 d 无关。在实际应用中，ℓ 取 8 性能最好。视图数量 m 与 n, ϵ, d 以及数据集的分布都有关。在文献[73] 中，可以通过覆盖设计[105,106] 来选取覆盖所有 2 元或 3 元属性组合，从而确定 m。

3.3.2　本章提出的 CALM 方法

CALM 方法的核心思想主要受 PriView 方法启发，但在本地差分隐私设定下，带噪音的视图无法直接通过对真实视图加入拉普拉斯噪音得到，而是需要使用复杂得多的 FO 来实现。在 PriView 中，所有 m 个视图都需要用到所有用户的数据，并且把隐私预算平均划分成 m 份。但在本地设定下，很多现有工作指出使用划分用户的方法更加有效。这样一来，所有用户都能使用全部的隐私预算，从而获得更小的噪音误差[44,64,107]。CALM 也采用该方法并把用户分成多个组，每组用户只为一个视图贡献数据。

图 3.2展示了 CALM 方法的工作原理。融合中心首先选取一组 m 个视图，并使用 FO

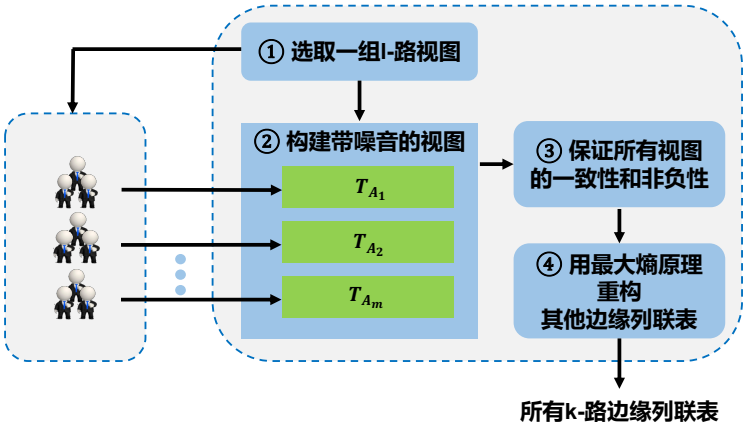


图 3.2　CALM 方法概述图。左侧用户被分成多个组，右侧融合中心给每个用户分配一个需要上传的视图并生成相应的视图。接下来融合中心对视图进行处理并发布所有边缘列联表

来收集数据，其中 FO 根据视图的单元数量进行自适应选取，也就是当单元数量小于 $3e^{\epsilon}+2$ 时，使用 GRR ，否则使用 OUE 。为方便起见，后面使用 FO 表示自适应选取的方法。这样的 FO 具有以下方差

$$\mathrm{Var}[\Phi_{\mathrm{FO}(\epsilon)}(x)] = \min\left(\frac{4e^{\epsilon}}{(e^{\epsilon}-1)^2}, \frac{|D|-2+e^{\epsilon}}{(e^{\epsilon}-1)^2}\right)\cdot\frac{1}{n} \tag{3.5}$$

接下来，融合中心为每个用户分配一个视图，并通知每个用户上传该视图对应的属性。本文不考虑具体的分配过程。一种方法是融合中心把用户群体随机划分成 m 组，并给同一组的用户分配同一个视图。另一种方法是融合中心利用用户的公开信息（比如说 IP 地址）进行划分，以确保每一组用户对整体分布都具有代表性。还有一种方法是让融合中心把 m 个视图发给用户，然后用户自行随机选择一个视图进行上传。

每个用户把他的隐私数据 v 投影到分配的视图上，并利用 FO 的扰动算法来上传投影后的数据。收到用户数据后，融合中心使用 FO 的融合算法来得到带噪音的视图。接下来融合中心执行一致性和非负性操作，并使用重构算法得到所有 k-路边缘列联表。

该问题的主要挑战在于如何选取一组最优的视图，也就是如何确定视图数量 m 和视图大小 ℓ。PriView[73] 中的分析不再适用于本地设定。本文将在 3.3.3节详细讨论该问题。另外，本文想要处理非二元属性，并在 3.3.4节详细讨论。

3.3.3　视图选取方法

本章最重要的算法参数为视图数量 m 和视图大小 ℓ。简单起见，假设所有的视图大小相同，贡献数据的用户数量也相同。

与 PriView 类似，在本地差分隐私设定下有噪音误差（使用 FO 上传数据引入）和重构误差（由于某些 k-路边缘列联表未被任意视图完全覆盖，并需要用最大熵估计算法进行估计）。除此之外，CALM 还有一类在 PriView 中不存在的误差。CALM 需要对用户进行分组，每个视图只能使用一组用户的数据。而一组用户的数据对整体用户的分布可能没有代表性从而产生误差，这种误差叫做抽样误差。接下来将详细分析这三类误差。

噪音误差。为了理解噪音误差，首先分析生成 1-路边缘列联表的整体方差，并分析该方差如何受 m 和 ℓ 的影响。对于大小为 ℓ 的视图，共有 $\frac{n}{m}$ 个用户贡献数据。根据公式 (3.5)，视图中每个单元的方差与用户数量成反比，也就是

$$\mathrm{Var}_c = \min\left(\frac{4e^\epsilon}{(e^\epsilon-1)^2}, \frac{L-2+e^\epsilon}{(e^\epsilon-1)^2}\right)\cdot\frac{m}{n}$$

其中 L 表示视图中单元的数量，对于二元属性和大小为 ℓ 的视图，$L=2^\ell$。当每个属性有不同的取值数量时，L 为所有视图单元数量的平均值。

为计算一个 1-路边缘列联表，需要累加大小为 ℓ 的视图的某些单元。根据方差的线性叠加属性，任意 1-路边缘列联表的方差为 $\mathrm{Var}_1 = \mathrm{Var}_c \cdot L$。以上分析显示增加 m 将对方差产生线性增加的影响。另一方面，增加 m 也会让 1-路边缘列联表被更多视图覆盖。当一个 1-路边缘列联表被 t 个视图覆盖时，可以分别从所有大小为 ℓ 的视图中得到 t 个估计值。对这 t 个估计值取平均将以 t 的比例降低方差。具体来说，每个大小为 ℓ 的视图包含 ℓ 个属性，因此从平均意义上来说，每个属性将获得 $\frac{m\cdot\ell}{d}$ 个视图的信息。这些估计的平均误差为

$$\begin{aligned}
&\mathrm{NE}(n,d,\epsilon,\ell) = \frac{\mathrm{Var}_1}{\frac{m\cdot\ell}{d}} \\
=&\min\left(\frac{4e^\epsilon}{(e^\epsilon-1)^2}, \frac{L-2+e^\epsilon}{(e^\epsilon-1)^2}\right)\cdot\frac{m}{n}\cdot L\cdot\frac{d}{m\cdot\ell} \\
=&\min\left(\frac{4e^\epsilon}{(e^\epsilon-1)^2}, \frac{L-2+e^\epsilon}{(e^\epsilon-1)^2}\right)\cdot\frac{L}{\ell}\cdot\frac{d}{n}
\end{aligned} \tag{3.6}$$

从这个式子可以看出，与 PriView 不同的是，CALM 的噪音误差不依赖于 m，而是依赖于 ℓ 和 ϵ。其中，ϵ 影响第一项，也就是 FO 的方差。参数 ℓ 同时影响 $\frac{L}{\ell}$ 和 FO 的方差。同时注意到 k-路边缘列联表的误差受 k 个属性影响，其误差也受 k 个属性影响，因此可以用 $k\cdot\mathrm{NE}(n,d,\epsilon,\ell)$ 来估计 k-路边缘列联表的噪音误差。

重构误差。重构误差产生的原因是某些 k-路边缘列联表没有被任何一个视图完全覆盖，其大小与数据集本身的分布有关。极端情况下，当所有属性相互独立，重构误差就不存在了。当属性之间存在关联时，整体趋势是越大的 m 和 ℓ 将覆盖越多的属性组合，从而带来越低的重构误差。但是随着 m 的增大，其对重构误差减小的效应也会减小。比如说，如果所有的 k-路边缘列联表都被完全覆盖了，重构误差就变成了 0，继续增加 m 和 ℓ 不能继续减小

重构误差。就算所有 k-路边缘列联表不能被完全覆盖，不断增加 m 也无法继续有效减小重构误差。由于重构误差跟数据集本身的分布有关，所有无法使用显示表达式进行估计。

抽样误差。抽样误差产生的原因是使用一组用户估计的视图可能偏离整体用户分布。参数 ℓ 对抽样误差没有影响，而增加 m 将使得对每个视图贡献数据的用户数量 $\frac{n}{m}$ 变小，从而增加抽样误差。当使用一组数量为 $s = n/m$ 的用户来构建某个视图时，每个视图单元可以看成 s 个伯努利随机变量叠加后除以 s。换句话说，每个单元都是一个伯努利随机变量除以 s。因此，每个单元的方差为 $\frac{\mathrm{M}_A(v)(1-\mathrm{M}_A(v))}{s}$，其中 $\mathrm{M}_A(v)$ 是取值为 v 的用户在整体用户中的比例。大小为 ℓ 的视图的抽样误差可以通过以下公式计算:

$$\sum_{v \in V_A} \frac{\mathrm{M}_A(v)(1-\mathrm{M}_A(v))}{s} = \frac{m \times \sum_{c \in V_A} \mathrm{M}_A(v)(1-\mathrm{M}_A(v))}{n}$$

因为 $\sum_{v \in V_A} \mathrm{M}_A(v) = 1$，所以 $\sum_{v \in V_A} \mathrm{M}_A(v)(1-\mathrm{M}_A(v)) < \sum_{v \in V_A} \mathrm{M}_A(v) \cdot 1 = 1$。

因此，抽样误差有一个上界

$$\mathrm{SE}(n, m) = \frac{m}{n} \tag{3.7}$$

选取 m 和 ℓ 的方法。从以上分析可以看出核心参数 m 和 ℓ 都会影响重构误差，而 m 会同时影响抽样误差，ℓ 会同时影响噪音误差。我们确定核心参数的原则是选取合适的 m 和 ℓ 来最小化三类误差中最大的那一个，因为最大的那类误差对最终误差的影响是最大的。这里的难点在于重构误差没有显示表达式，因此无法使用优化技术进行核心参数选取。

因此，本章提出了一种新的核心参数选取策略。首先确定一个目标误差阈值 θ 来近似估计重构误差，并使用如下方法来选取 m 和 ℓ:

- 计算使得 $k \cdot \mathrm{NE} < \theta$ 时，最大的视图大小 ℓ_u。
- 当 $\ell_u < k$ 时，计算 ℓ_u 和最大的 m 使得 $\mathrm{SE} < \theta$。
- 否则，选择 m 和 $\ell_t \in [k, \ell_u]$，使得 NE 和 SE 两者的最大值最小化。

虽然 θ 是重构误差的一个近似估计，但并不依赖于具体数据集。实际中，可以使用相似属性的公开数据集来尝试不同参数，并选择能获得最小 SSE 的那个参数用于近似估计重构误差。如果没有公开数据集，可以根据某些相关性假设生成一个合成数据集来做实验。在本章的所有实验中，我们选取 $\theta = 0.001$。

算法 3.1给出了计算 m 和 ℓ 的伪代码。该算法使用公式 (3.6)来计算噪音误差 (Noise Error，简称 NE)，使用公式 (3.7)来计算抽样误差 (Sampling Error，简称 SE)。CoverDesign

算法 3.1: 计算 m 和 ℓ 的伪代码

Input: 数据集参数 n, d, ϵ, k，误差阈值 θ

Output: m 和 ℓ

Initialization: $m_u \leftarrow \theta \cdot n$, $\ell_u \leftarrow 2$;
while $k \cdot \mathrm{NE}(n, d, \epsilon, \ell_u + 1) \leq \theta$ do
    更新 $\ell_u \leftarrow \ell_u + 1$;
end while
if $\ell_u < k$ then
    return $\min(m_u, \binom{d}{\ell_u}), \ell_u$;
end if
赋值 $\ell_b \leftarrow \ell_u$
while $\ell_b > k$ and $\mathrm{CoverDesign}(d, k, \ell_b - 1) \leq m_u$ do
    更新 $\ell_b \leftarrow \ell_b - 1$
end while
if $\ell_b == \ell_u$ then
    return $\min(m_u, \binom{d}{\ell_u}), \ell_u$;
end if
赋值 $\mathrm{E} \leftarrow 1, m \leftarrow m_u, \ell \leftarrow \ell_u$
for ℓ_t in $[\ell_b, \ell_u]$ do
    赋值 $m_t \leftarrow \mathrm{CoverDesign}(d, k, \ell_t)$ if $\max(\mathrm{SE}(n, m_t), k \cdot \mathrm{NE}(n, d, \epsilon, \ell_t)) < \mathrm{E}$ then
        更新 $\mathrm{E} \leftarrow \max(\mathrm{SE}(n, m_t), k \cdot \mathrm{NE}(n, d, \epsilon, \ell_t))$;
        更新 $m \leftarrow m_t, \ell \leftarrow \ell_t$;
    end if
end for
return m, ℓ.

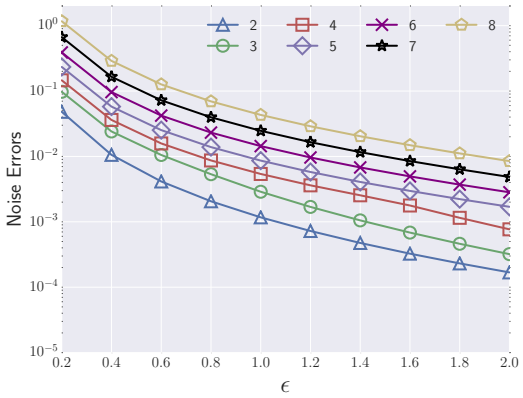


图 3.3　当 $n = 2^{16}, d = 8, k = 3$ 时，噪音误差乘以 k

是一个外部算法，用来计算完全覆盖所有 k-路边缘列联表的大小为 ℓ 的视图的数量。注意到 NE 是对单个属性的方差估计，在算法中需要用 k 倍的 NE 来估计 k-路边缘列联表的噪音误差。

举个例子，图 3.3给出当 ϵ 从 0.2 变化到 2.0 时噪音误差乘以 k 的值，图中 $n = 2^{16}, d = 8, k = 3$。当 $\theta = 10^{-3}$，从图中可以看到当 $\epsilon \leq 1.4$，只有 $\ell = 2$ 是满足阈值条件的。因为更大的 ℓ 将导致更大的 NE，因此可以选择容忍一定的 RE 存在。当 ϵ 继续增大时（比如 $\epsilon = 2.0$），NE 已经很小了，因此可以容忍更大的 NE 来减小 RE。在这种情况下，$\ell = 3$ 和 $\ell = 4$ 都能保证 $k \cdot \mathrm{NE} < \theta$，所以需要选择一个 ℓ 使得 $k \cdot \mathrm{NE}$ 和 SE 中的最大值最小化。具体来说，当 $\ell = 3$ 时，使用 CoverDesign 可以算出 $m = \binom{8}{3} = 56$ 能完全覆盖所有的 3-路边缘列联表，这种情况下 $\max\{\mathrm{NE} = 0.00032, \mathrm{SE} = 0.00085\} = 0.00085$。当 $\ell = 4$ 时，使用 CoverDesign 可以算出 $m = 14$（也就是 14 个大小为 4 的视图可以完全覆盖所有 3-路边缘列联表），这种情况下 $\max\{\mathrm{NE} = 0.00076, \mathrm{SE} = 0.00021\} = 0.00076$。因此，$\ell = 4$ 和 $m = 14$ 是更好的选择。

3.3.4　带噪音视图一致性处理方法

当不同的视图包含了一些相同属性时，这些属性实际上被估计了多次，融合这些估计往往能获得更好的精度。假设一个属性集合 A 被 s 个视图共同包含，表示为 $A_1, A_2, \ldots, A_s$，也就是 $A = A_1 \cap \ldots \cap A_s$。接下来每个 A 单元可以通过累加所有视图得到 s 个估计，也就是 $A_i(v) = \sum_{v' \in V_{A_i}, v'_A = v_A} \mathrm{T}_{A_i}(v')$。

为得到对 A 更好的估计，可以对所有 A_i 进行加权平均处理，也就是

$$A(v) = \sum_i w_i \cdot A_i(v).$$

由于 A_i 是无偏的，因此他们的平均值 $A(v)$ 也是无偏的。为视图分配不同权重的核心思想是给拥有更精确估计的视图分配更多权重。具体来说，我们需要最小化 $A(v)$ 的方差，也就是 $\mathrm{Var}\left[A(v)\right] = \sum_i w_i^2 \cdot \mathrm{Var}\left[A_i(v)\right] = \sum_i w_i^2 \cdot C_i \cdot \mathrm{Var}_0$，其中 C_i 是通过视图 A_i 计算 A 时所累加的单元数量，$C_i = |\{v' : v' \in V_{A_i}, v'_A = v_A\}|$，$\mathrm{Var}_0$ 为估计单个单元的方差。因此，可以构建以下优化问题：

$$\begin{aligned} \text{minimize} \quad & \textstyle\sum_i w_i^2 \cdot C_i \\ \text{subject to} \quad & \textstyle\sum_i w_i = 1 \end{aligned}$$

接下来通过 KKT 条件[108,109] 进行推导：令 $L = \sum_i w_i^2 \cdot C_i + \mu \cdot (\sum_i w_i - 1)$，对每个 w_i 求 L 的偏导，得到 $w_i = -\frac{\mu}{2C_i}$。μ 可以通过解方程 $\sum_i w_i = 1$ 得到，也就是 $\mu = -\frac{2}{\sum_i \frac{1}{C_i}}$，$w_i = \frac{\frac{1}{C_i}}{\sum_i \frac{1}{C_i}}$。因此，最优加权平均为

$$A(v) = \frac{\sum_i \frac{1}{C_i} \cdot A_i(v)}{\sum_i \frac{1}{C_i}}$$

得到最优 A 后，便可以更新视图 A_i。对任意视图 A_i，使用 v 来更新所有 $v' \in V_{A_i}$，其中 $v \in VA$ 和 $v'_A = v_A$。具体来说

$$A_i(v') \leftarrow A_i(v') + \frac{1}{C_i}\Big(A(v) - A_i(v)\Big)$$

以上仅讨论了非二元属性的本地一致性方法，如何达到全局一致性可以参考文献[73] 中的方法。

3.3.5　复杂度分析

	时间复杂性	空间复杂性	通信代价
CALM	$\Theta\left(n \cdot 2^{\ell}\right)$ or $\Theta\left(n + m \cdot 2^{\ell}\right)$	$\Theta\left(m \cdot 2^{\ell}\right)$	$\Theta\left(2^{\ell}\right)$
FC	$\Theta\left(n \cdot 2^{d}\right)$ or $\Theta\left(n + 2^{d}\right)$	$\Theta\left(2^{d}\right)$	$\Theta\left(2^{d}\right)$
LM	$\Theta\left(n \cdot 2^{k}\right)$ or $\Theta\left(n + \binom{d}{k} \cdot 2^{k}\right)$	$\Theta\left(2^{k}\right)$	$\Theta\left(2^{k}\right)$
FT	$\Theta\left(n + \binom{d}{k} \cdot 2^{2k}\right)$	$\Theta\left(\sum_{s=0}^{k} \binom{d}{s}\right)$	$\Theta\left(d\right)$
EM	$\Theta\left(n \cdot \sum_{s=0}^{k} \binom{d}{s} 2^{s}\right)$	$\Theta\left(\sum_{s=0}^{k} \binom{d}{s} 2^{s}\right)$	$\Theta\left(d\right)$

表 3.2　复杂度分析，分别列出了融合中心端的计算代价，存储代价和通信代价。所有复杂度均在二元属性假设下给出。

表 3.2给出了不同方法的时间复杂度，空间复杂度以及通信代价。为了方便分析，表中的结果都是在二元属性的假设下给出的，这些结果可以很容易得推广到非二元属性的情形。

时间复杂度： CALM 方法的计算时间主要花在用户上传数据的处理，对每个用户花费 $\Theta\left(2^{\ell}\right)$，总共花费 $\Theta\left(n\cdot 2^{\ell}\right)$。FC 和 AM 的情况差不多，每个用户分别上传大小为 $\Theta\left(2^{d}\right)$ 和 $\Theta\left(2^{k}\right)$ 的向量。当 ϵ 很小并且使用 GRR 时，每个用户只需上传一个值而非一个向量，因此融合中心只需要融合一个值，使得 CALM，FC 和 AM 三种方法的时间复杂度分别为 $\Theta\left(n+m\cdot 2^{\ell}\right), \Theta\left(n+2^{d}\right)$, 和 $\Theta\left(n+\binom{d}{k}\cdot 2^{k}\right)$。对于算法 FT，由于一直使用 GRR 方法，运行时间只与 n 相关，但是计算公式 (3.3)需要花费 $\Theta\left(2^{k}\right)$ 时间来枚举所有 α。因此，为构建 $\binom{n}{k}$ 个边缘列联表需要花费 $\Theta\left(n+2^{2k}\cdot\binom{d}{k}\right)$。对于算法 EM，运行时间主要花费在计数上面。具体来说，该方法首先计算上传任意单一属性的用户数量，然后计算任意两个属性的数量，以此类推。总共有 $\sum_{s=0}^{k}\binom{d}{s}2^{s}$ 可能的值需要计数，融合中心需要对每个用户进行计数，因此最终时间复杂度为 $\Theta\left(\sum_{s=0}^{k}\binom{d}{s}2^{s}\right)$。

空间复杂度： 这里不计算所有的输入和输出占用的内存，因为所有方法都是一样的。对于内存占用，CALM 方法需要存储 m 个大小为 ℓ 的视图。对于 FC 来说，需要存储一个完整的全列联表，大小为 $\Theta\left(2^{d}\right)$。FT 方法需要存储 $2^{k}\cdot\binom{d}{k}$ 个傅里叶参数。最后 EM 方法需要存储所有的中间计数结果。

通信代价： 用户与融合中心之间的通信与用户上传数据的大小有关。注意到 FT 和 EM 都使用 GRR 进行数据上传。因此 FT 只需要上传 1 比特数据和表示成 d 比特的傅里叶参数索引。EM 需要上传 d 比特数据。对于 CALM 来说，可以采用 OLH 来替代 OUE 。文献[44]证明 OLH 与 OUE 是等效的，并且把通信代价降低到一个常数。但 OLH 带来的代价是融合中心需要通过额外的计算（比如说评估哈希函数）来估计频率分布。

3.3.6 讨论

本章提出的 CALM 满足 ϵ-本地差分隐私，因为所有传入融合中心的数据都使用了 FO，并且之后没有任何其他信息泄露。

虽然 CALM 的核心思想受 PriView 启发，但两种方法存在着大量区别。在这些区别中，大多数是因为两种方法的隐私需求不一样。PriView 适用于集中式差分隐私，而 CALM 适用于本地差分隐私。两种方法主要区别总结如下：

- 在 PriView 中，融合中心可以访问所有用户的原始数据，只在输出结果上进行扰动处理；而在 CALM 中，融合中心只能得到一个扰动处理后的数据，并需要通过融合扰动数据来计算视图。

- CALM 可以处理包含非二元属性的数据集；而 PriView 只能处理二元属性。
- 在 PriView 中，每个视图都使用了所有用户的数据，并划分了隐私预算；而 CALM 使用了精度更高的划分用户的策略，每个视图只使用一组用户的信息。
- 由于 CALM 选择了划分用户，相比较于 PriView 来说新引入了抽样误差，增加了核心参数 m 和 ℓ 的选取难度。
- 在 PriView 中，误差与视图数量 m 和数据集分布关系很大；而 CALM 对于视图数量的依赖小很多。
- 在 PriView 中，最优视图大小 ℓ 与 ϵ 无关；而对于 CALM 来说，视图大小取决于使用何种 FO 并受 ϵ 影响。

3.4 性能评估

本部分使用大量真实数据集来验证 CALM 方法的有效性。

3.4.1 实验设置

本章实验借鉴了文献[77] 的相关设置，并比较了第3.2节中讨论的现有算法。

实验环境。 所有算法均使用 Python 3.5 实现，服务器配置为 Intel Core i7-4790 3.60GHz 和 16GB 内存。

数据集。 本实验使用了以下四个数据集：

- POS[110]：该数据集包含大约 50 万条超市购物记录。
- Kosarak[111]：该数据集包含大约 100 万条匈牙利某网站的点击数据。
- Adult[112]：该数据集来源于 UCI 机器学习库。在移除缺失数据后，包含大约 5 万条数据，所有的连续属性都被切分成了离散属性。
- US[113]：该数据集来源于 IPUMS 数据库（Integrated Public Use Microdata Series），包含大约 4 万条美国 2010 年的人口普查数据。

前两个数据集都属于事务型数据集，原始数据集的每条记录包含一个或多个项。本实验把是否包含排名前 d 的频繁项看成一个二元属性，并把数据集预处理成包含 d 个属性的

二元数据集，包含相关项设置属性值为 1，否则为 0。后面两个数据集为非二元数据集，也就是说每个属性包含不止两种取值。

评价方法。本实验使用 SSE 来评估不同算法的性能。对于每个数据集和每种算法，随机选取 50 个 k-路边缘列联表进行测试并计算它们的 SSE。该步骤重复 20 遍，并分别记录均值和标准差。

比较方法。FC，AM 和 EM 算法直接使用原始文献设置，为公平起见，这些方法也使用了动态调整的 FO，也就是根据边缘列联表的单元数量选取不同的 FO 方法。

原始的 FT 方法无法直接处理非二元属性，本实验通过把非二元属性编码成二元属性的方式实现了可以处理非二元属性的 FT。

此外，本实验引入了一个基准算法——均匀分布法（用 Uni 表示），该算法把所有测试边缘列联表都设置成均匀分布，也就是没有任何先验知识的瞎猜。显然，如果某种算法的性能比 Uni 还要差，那么该算法是没有任何意义的。

实验参数设置。不同算法能处理的属性数量 d 和边缘列联表大小 k 都不一样，而且性能都与数据集大小 n 有关。因此，本实验使用了三个 d 的取值 8，16 和 32。$k=3$ 使用了全部三个取值，$k=6$ 使用了 $d\in\{16,32\}$，$k=8$ 仅使用了 $d=32$。这样设置的原因是，更大的 k 对于大 d 来说更有意义。与文献[77] 类似，本实验使用了 $n=2^{16}$ 和 $n=2^{18}$ 两种取值。由于 n 对所有的方法的影响都是相同的，因此本章实验结果对其他 n 的取值同样有效。

本实验中可能用到的 m 和 ℓ 的取值如表 3.3所示，这些取值都是根据算法 3.1计算得到的。

3.4.2 二元数据集性能比较

图 3.4展示了 CALM 与已有算法在二元数据集 Kosarak 和 POS 上的性能比较。

在所有参数设置下，CALM 的性能都比现有算法有明显提升，当 d 和 k 很大 ϵ 很小时，CALM 的优势更加明显。在大多数参数设定下，CALM 比现有最好算法 FT 的 SSE 降低了一到两个数量级。当 ϵ 非常小时（比如 $\epsilon=0.2$），现有算法的性能都趋近于基准方法 Uni，意味着当隐私预算很小时现有算法能提供非常少的有效信息。然而在 ϵ 很小时，CALM 的精度仍然非常。另外，很多现有算法由于时间复杂度过高而无法处理 $d=32$ 的设定。

EM 算法在所有参数设置下表现都很差，甚至于比基准算法 Uni 还要差。这是因为 EM 要求用户必须上传所有 d 个属性，意味着需要把隐私预算划分成 d 份，从而引入过大的扰动。与 EM 不同，其他算法可以通过划分用户群体来获得更好的性能。同时，当 k 大于等

d,k,n \ ϵ	0.2	0.4	0.6	0.8	1	1.2	1.4	1.6	1.8	2
$8,3,2^{16}$	$2,28$	$2,28$	$2,28$	$2,28$	$2,28$	$2,28$	$2,28$	$3,56$	$3,56$	$4,14$
$8,4,2^{16}$	$2,28$	$2,28$	$2,28$	$2,28$	$2,28$	$2,28$	$2,28$	$3,56$	$3,56$	$3,56$
$8,5,2^{16}$	$2,28$	$2,28$	$2,28$	$2,28$	$2,28$	$2,28$	$2,28$	$2,28$	$3,56$	$3,56$
$8,6,2^{16}$	$2,28$	$2,28$	$2,28$	$2,28$	$2,28$	$2,28$	$2,28$	$2,28$	$3,56$	$3,56$
$8,7,2^{16}$	$2,28$	$2,28$	$2,28$	$2,28$	$2,28$	$2,28$	$2,28$	$2,28$	$2,28$	$3,56$
$16,3,2^{16}$	$2,65$	$2,65$	$2,65$	$2,65$	$2,65$	$2,65$	$2,65$	$2,65$	$3,65$	$3,65$
$16,4,2^{16}$	$2,65$	$2,65$	$2,65$	$2,65$	$2,65$	$2,65$	$2,65$	$2,65$	$2,65$	$3,65$
$16,5,2^{16}$	$2,65$	$2,65$	$2,65$	$2,65$	$2,65$	$2,65$	$2,65$	$2,65$	$2,65$	$2,65$
$16,6,2^{16}$	$2,65$	$2,65$	$2,65$	$2,65$	$2,65$	$2,65$	$2,65$	$2,65$	$2,65$	$2,65$
$16,7,2^{16}$	$2,65$	$2,65$	$2,65$	$2,65$	$2,65$	$2,65$	$2,65$	$2,65$	$2,65$	$2,65$
$32,3,2^{16}$	$2,65$	$2,65$	$2,65$	$2,65$	$2,65$	$2,65$	$2,65$	$2,65$	$2,65$	$2,65$
$32,4,2^{16}$	$2,65$	$2,65$	$2,65$	$2,65$	$2,65$	$2,65$	$2,65$	$2,65$	$2,65$	$2,65$
$32,6,2^{16}$	$2,65$	$2,65$	$2,65$	$2,65$	$2,65$	$2,65$	$2,65$	$2,65$	$2,65$	$2,65$
$32,8,2^{16}$	$2,65$	$2,65$	$2,65$	$2,65$	$2,65$	$2,65$	$2,65$	$2,65$	$2,65$	$2,65$
$8,3,2^{18}$	$2,28$	$2,28$	$2,28$	$2,28$	$3,56$	$3,56$	$3,56$	$3,56$	$3,56$	$4,14$
$8,4,2^{18}$	$2,28$	$2,28$	$2,28$	$2,28$	$3,56$	$3,56$	$4,70$	$4,70$	$4,70$	$4,70$
$8,5,2^{18}$	$2,28$	$2,28$	$2,28$	$2,28$	$2,28$	$3,56$	$3,56$	$4,70$	$5,56$	$5,56$
$8,6,2^{18}$	$2,28$	$2,28$	$2,28$	$2,28$	$2,28$	$3,56$	$3,56$	$4,70$	$4,70$	$5,56$
$8,7,2^{18}$	$2,28$	$2,28$	$2,28$	$2,28$	$2,28$	$3,56$	$3,56$	$3,56$	$4,70$	$5,56$
$16,3,2^{18}$	$2,120$	$2,120$	$2,120$	$2,120$	$2,120$	$3,262$	$3,262$	$4,140$	$4,140$	$4,140$
$16,4,2^{18}$	$2,120$	$2,120$	$2,120$	$2,120$	$2,120$	$2,120$	$3,262$	$3,262$	$4,262$	$4,262$
$16,5,2^{18}$	$2,120$	$2,120$	$2,120$	$2,120$	$2,120$	$2,120$	$3,262$	$3,262$	$4,262$	$4,262$
$16,6,2^{18}$	$2,120$	$2,120$	$2,120$	$2,120$	$2,120$	$2,120$	$2,120$	$3,262$	$3,262$	$4,262$
$16,7,2^{18}$	$2,120$	$2,120$	$2,120$	$2,120$	$2,120$	$2,120$	$2,120$	$3,262$	$3,262$	$4,262$
$32,3,2^{18}$	$2,262$	$2,262$	$2,262$	$2,262$	$2,262$	$2,262$	$2,262$	$3,262$	$3,262$	$4,262$
$32,4,2^{18}$	$2,262$	$2,262$	$2,262$	$2,262$	$2,262$	$2,262$	$2,262$	$3,262$	$3,262$	$3,262$
$32,6,2^{18}$	$2,262$	$2,262$	$2,262$	$2,262$	$2,262$	$2,262$	$2,262$	$2,262$	$3,262$	$3,262$
$32,8,2^{18}$	$2,262$	$2,262$	$2,262$	$2,262$	$2,262$	$2,262$	$2,262$	$2,262$	$2,262$	$3,262$

表 3.3　通过算法 3.1得到的参数 ℓ 和 m 取值。每个单元格都是 (ℓ,m) 元组的形式

于 5 时，EM 的运行时间太长（计算每个边缘列联表需要大约 20 分钟），因此在图中没有画出当 $k=6,8$ 时 EM 的性能曲线。

在所有现有方法中，FT 表现最好。当 $d=8,k=3$ 时，可以利用公式 (3.1)，(3.2)和(3.4)来计算 FC ，AM 和 FT 算法的方差，其中 FC 的方差是 $256\cdot \mathrm{Var}_0$，AM 的方差是 $448\cdot \mathrm{Var}_0$，FT 的方差是 $93\cdot \mathrm{Var}_0$。从图 3.4a 和 3.4g中可以看出，实验结果和理论分析的结果吻合。

当 $d=16$ 时，CALM 的性能与 $k=8$ 时很接近，而其他算法在两种参数设置下的性能差距很大。比如，在图 3.4b中，当 $\epsilon=0.2$ 时，CALM 的 SSE 为 0.0055，比 FT 的 SSE (0.2266) 降低了 41 倍。FC 算法的性能不依赖于 k，因为它的方差只取决于全列联表的大小。

所有现有算法都无法处理 $d=32$ 的设置，特别当 $k=8$ 时。对于 AM 算法来说，所有可能的边缘列联表组合数量为 $\binom{32}{8}=10518300$。因此，当 $n=2^{16}$ 和 2^{18} 时，贡献数据给每个边缘列联表的平均用户数量小于 1。同样的，重构所有 8-路边缘列联表所需要的傅里叶系数数量为 $\sum_{s=1}^{8}\binom{32}{s}=15033173$，导致 FT 方法也无法处理该参数设置。

3.4.3 非二元数据集性能比较

非二元数据集 Adult 和 US 的实验结果见图 3.5。实验结果显示 CALM 的性能比现有算法有 1 到 2 个数量级的提升。

比较二元数据集和非二元数据集在 $d=8,k=3$ 设置下的性能，也就是图 3.4和图 3.5，可以观察到 FT 在二元数据集下比 FC 和 AM 性能好，而在非二元数据集下表现更差。原因是，对于非二元数据集来说，FT 算法需要首先把非二元属性编码成二元属性，导致重构边缘列联表的傅里叶参数数量急剧增加。比如，考虑有 8 个属性的数据集，每个属性有 3 种取值，经过二元编码的 d 和 k 分别变成 16 和 6。通过方差分析，方差变成了 $14893\cdot \mathrm{Var}_0$，而在二元数据集下方差仅仅为 $93\cdot \mathrm{Var}_0$。

为了展示本章提出的处理非二元数据集算法的优越性，本实验通过二元编码方式实现了变种的 CALM 算法，使得可以直接使用 PriView 的一致化算法，我们称这种基于二元编码的算法为 BE 。实验显示 CALM 方法性能明显超过 BE 。原因与 FT 类似，经过二元编码后的 d 和 k 都变得非常大，导致方差巨大。当 $d=16,k=6$ 时，BE 在进行最大熵估计时耗时太长，因此没有在图中画出。

3.4.4　分类性能比较

为测试 CALM 方法在实际应用中的性能，本实验使用 Adult 和 US 数据集来训练 SVM 分类器，分类器的目标是预测用户的年收入是否大于 $50k$。为了训练模型，首先选取五个属性（特征）并让每种算法都输出一个 6-路边缘列联表（五个特征加上一个年收入标签）。Adult 数据集的五个特征为 age, workclass, education, education-num 和 occupation。US 数据集的五个特征为 WRKRECAL, GRADEATT, SCHLTYPE, SCHOOL 和 DIFFPHYS。这些特征是通过它们的语意关系手动选取的。得到一个带扰动的边缘列联表后，首先根据该边缘列联表的分布生成一个合成数据集，然后利用合成数据集来训练 SVM 分类器。本实验使用了两个基准算法：

- NoNoise 表示没有对原始数据进行扰动处理，显然该算法的精度为所有算法精度的上限。
- Majority 表示利用训练数据集中多数标签对未知用户进行分类，是机器学习中普遍采用的基准算法。

所有算法都使用 80% 的数据作为训练集，20% 的数据作为测试集，并使用在测试集上的误分类率来衡量性能，也就是测试集中被错误分类的比例。

图 3.6展示了通过不同算法训练的 SVM 分类器的误分类率。实验显示，在多数情况下 CALM 的平均误分类率非常接近 NoNoise 。当 ϵ 很小的时候，通过 FC 和 AM 方法训练的分类器比 Majority 还要差，甚至偶尔比随机猜测的误分类率还要高（50%）。

在图 3.6中的最右侧两列，把数据集分别扩充了 4 倍和 16 倍，实验显示更多的数据能有效提升精度。比如，对于二元划分的 Adult 数据集来说，当数据集被扩充了 4 倍时，CALM 在 $\epsilon = 1.4$ 时就接近于最优精度，当数据集被扩充了 16 倍时，CALM 在 $\epsilon = 0.8$ 时就接近于最优精度。从图中同样可以观察到当数据集为非二元划分时（图 3.6的偶数行），其精度比二元划分时要稍微差一些，这是由于在非二元划分中，每个属性拥有更多的取值并带来更多的噪音，从而使得精度变低。

3.4.5　验证算法参数合理性

图 3.7使用热力图分别显示了视图大小 ℓ，视图数量 m 和隐私预算 ϵ 对 SSE 的影响。**图** 3.7a**和图** 3.7d 分别显示了在 POS 和 Kosarak 两个数据集中 ℓ 和 m 两个参数的相互影响，参数设置为 $d = 8, k = 3, \epsilon = 0.6$。两个热力图都显示，当 ℓ 不等于 1 和 8 时，增加 m

会逐渐降低 SSE，这与3.3.3小节中的分析相符，因为增加 m 将覆盖更多的边缘列联表，从而降低了重构误差。虽然增大 m 也会增加抽样误差，但可以看到当 $m=32$ 时，抽样误差仅为 $2^{-11}=0.0005$。需要注意的是，当 $\ell=1$ 时，所有视图仅仅包含一个属性，这个时候增加 m 不会降低重构误差。同样地，当 $\ell=1$ 时，所有的属性都被所有的视图覆盖了，因此增加 m 不会改变误差。

图 3.7b，3.7c，3.7e **和** 3.7f 显示了当 m 固定时 ℓ 与 ϵ 的相互关系。从图中可以观察到当 ϵ 很小时，倾向于选择更小的 ℓ。原因在于此时噪音误差最大，因此需要选择更小的 ℓ 来减小噪音误差的影响。当 ϵ 变大时，倾向于选择更大的 ℓ，因为此时重构误差最大。图中蓝色数字显示了通过算法 3.1计算得到的最优参数，实验显示理论分析与实验结果相吻合。

3.4.6 k 及本地设定对性能的影响

图 3.8中的实验有两个目的：一个是研究当 CALM 期望的边缘列联表大小为 k 时，针对 k' $(k'\neq k)$ 优化的参数 m 和 ℓ 对性能的影响；另一个通过比较 CALM 和集中式方法 PriView 来理解，当隐私保护模型变换到本地模型时性能损失了多少。

图 3.8的第一行显示了当参数为 $k'\in\{3,6,8\}$ 优化时，计算 k-路边缘列联表的精度，同时显示了集中式算法 PriView 的精度。当 $k=3$ 时，不同的 k' 取值性能类似。当 $k=6$ 时，为 $k'=3$ 优化的参数在 $\epsilon=1.2$ 和 1.4 时性能显然更差。这是因为对于 $k'=3$ 的优化参数，ϵ 从 1 变化到 1.2 导致 ℓ 从 2 变化到 3，然而对于 $k'=6$ 的优化参数来说，ℓ 从 2 变化到 3 发生在 $\epsilon=1.6$ 时。对比表 3.3中在不同设置下的参数选择，同样的现象也发生在 $k=8$ 时，$k'=3$ 的优化参数在 $\epsilon=1.6$ 和 1.8 时表现非常差。整体来看，当 $k=k'$ 时，性能是最好的。另外，如果融合中心事先不知道计算的边缘列联表大小 k，可以使用相对大的 k' 的最优参数。

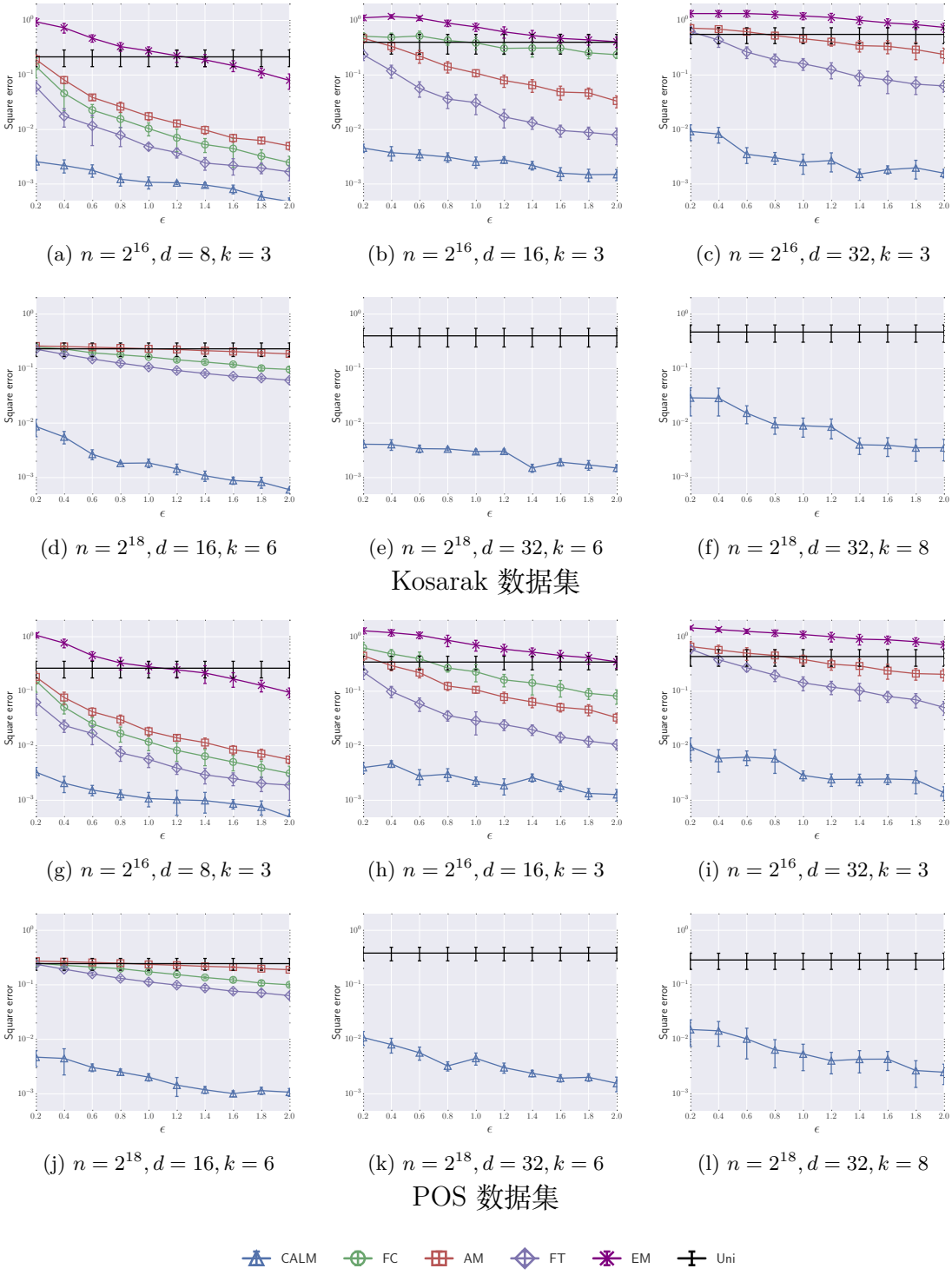
从图 3.8的第一行同样也能看到 PriView 的性能比 CALM 好 1 到 2 个数量级。因为在集中式设定下，加入的扰动远远小于本地设定。理论上来说，本地设定下加入扰动的大小为 $\Theta\left(\frac{1}{\sqrt{n}}\right)$，而集中式设定下加入扰动的大小为 $\Theta\left(\frac{1}{n}\right)$。

图 3.8的第二行显示了当 k' 从 2 变化到 16 时回答 k-路边缘列联表的精度。ϵ 的取值为 $\epsilon\in\{0.5,1.0,1.5,2.0\}$。当某些设定下 m,ℓ 的取值相同时，图中重用了实验结果而非重新跑一次实验。因此，图中引起不同的地方体现在 m,ℓ 发生改变时。观察到当 ϵ 很小时（比如 $\epsilon\in\{0.5,1.0\}$），所有 k' 都拥有相同的最优参数，也就是 $m=65,\ell=2$。当 $\epsilon=1.5$ 和 $k=6$ 时，为 $k'\geq 8$ 优化的参数是次优的。从最右侧子图中可以看出，当要计算 $k=8$-路边缘列联表时，为 $k'\leq 3$ 优化的参数会导致很差的精度，特别是当 $\epsilon=1.5$ 时。

图 3.9显示的是当固定 $n = 2^{18}$ 和 $d = 16$ 时，不同 k-路边缘列联表的 SSE。当 $\epsilon \in \{0.5, 1, 1.5, 2\}$ 时，图中展示了两种设定：m 和 ℓ 是为 $k' = 3$ 优化的；m 和 ℓ 是为 $k' = k$ 优化的。实验结果表明，在大多数情况下两种设定的结果相似，因为两种设定下选取的 m 和 ℓ 是一样的。当 $\epsilon = 1.5$ 和 $k > 7$ 时，两者的差距变得很显著。这主要是因为两种设定下选取的 ℓ 是不一样的：当 $k' = 3$ 时 $\ell = 3$，当 $k' = k \in \{8, 9, 10\}$ 时 $\ell = 2$。

3.5　本章小结

本章研究了高维数据分析的关键技术——边缘列联表发布——的融合算法优化问题。我们提出了一套高精度的边缘列联表发布新算法 CALM ，该算法首先通过系统的误差分析，选出一组包含少量边缘列联表的集合，称为视图；然后使用频率估计方法生成带扰动的视图；接下来对扰动视图进行一致性和非负性处理；最后使用一致的视图和最大熵优化理论推断出所有边缘列联表。通过在真实数据集上大量的实验，证明 CALM 比现有最好方法的融合误差降低了一到两个数量级。



(a) $n = 2^{16}, d = 8, k = 3$ (b) $n = 2^{16}, d = 16, k = 3$ (c) $n = 2^{16}, d = 32, k = 3$

(d) $n = 2^{18}, d = 16, k = 6$ (e) $n = 2^{18}, d = 32, k = 6$ (f) $n = 2^{18}, d = 32, k = 8$

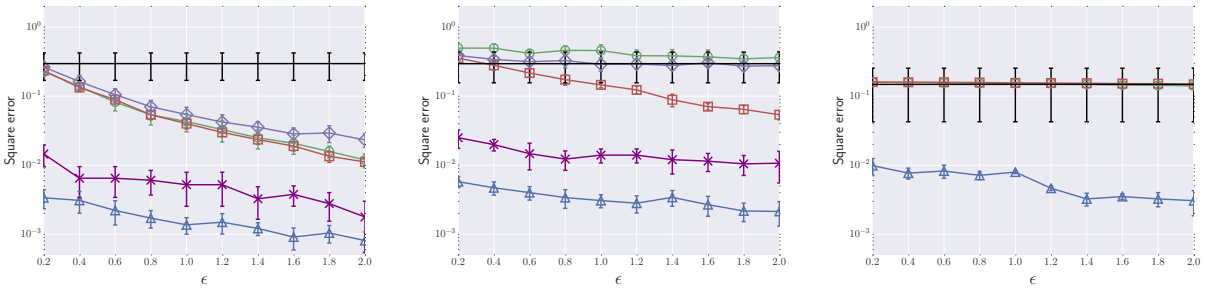
Kosarak 数据集

(g) $n = 2^{16}, d = 8, k = 3$ (h) $n = 2^{16}, d = 16, k = 3$ (i) $n = 2^{16}, d = 32, k = 3$

(j) $n = 2^{18}, d = 16, k = 6$ (k) $n = 2^{18}, d = 32, k = 6$ (l) $n = 2^{18}, d = 32, k = 8$

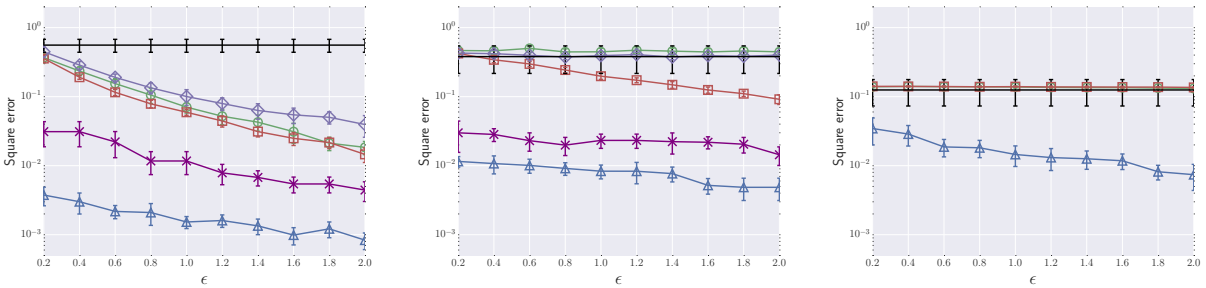
POS 数据集

图 3.4　二元数据集上不同算法的性能比较。图中只画出了相应设置下有处理能力的算法，其中 Uni 是基准算法。图中纵坐标使用 log 坐标



(a) $d = 8, k = 3$　(b) $d = 15, k = 3$　(c) $d = 15, k = 6$

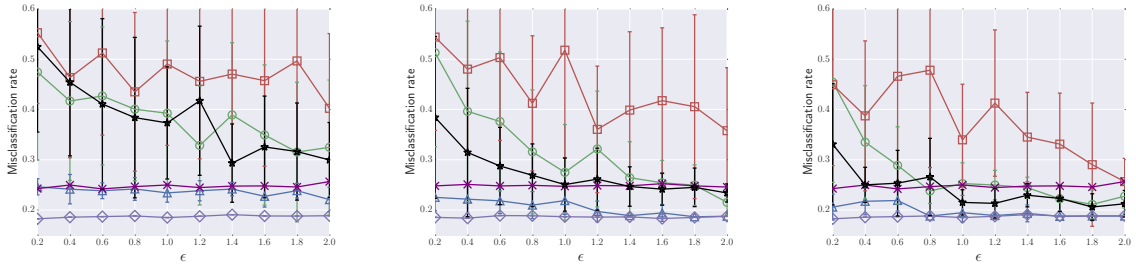
Adult 数据集, $n = 2^{16}$



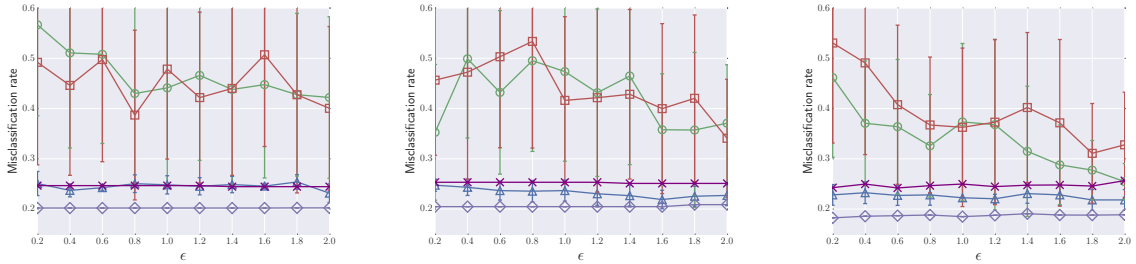
(d) $d = 8, k = 3$　(e) $d = 16, k = 3$　(f) $d = 16, k = 6$

US 数据集, $n = 2^{16}$

图 3.5　非二元数据集上不同算法的性能比较。图中只画出了相应设置下有处理能力的算法，其中 Uni 是基准算法，BE 是通过二元编码方式实现的 CALM 方法。图中纵坐标使用 log 坐标

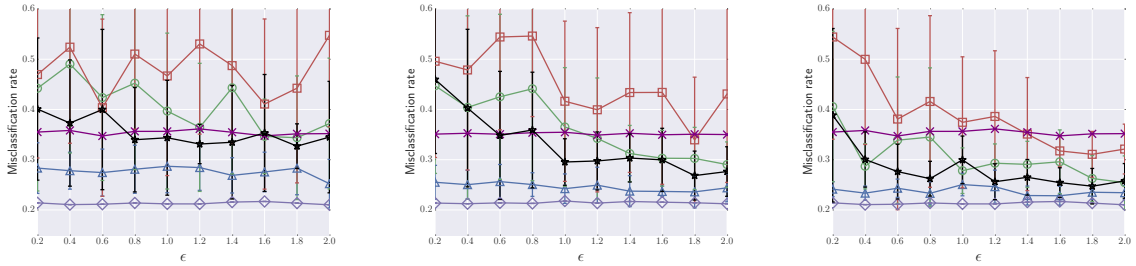


(a) 二元划分, $n = 2^{16}$　(b) 二元划分, $n = 2^{18}$　(c) 二元划分, $n = 2^{20}$

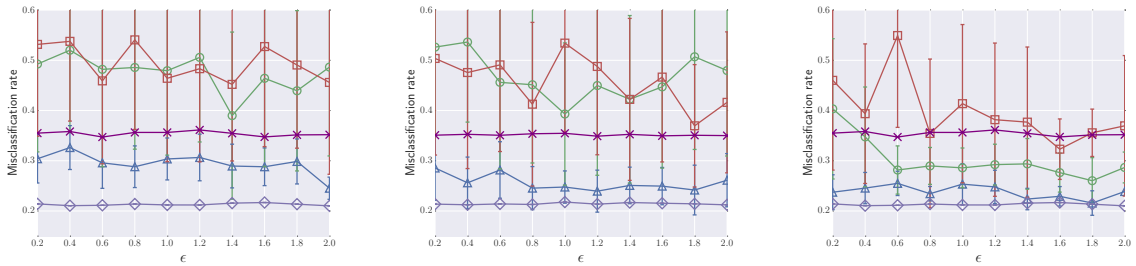


(d) 非二元划分, $n = 2^{16}$　(e) 非二元划分, $n = 2^{18}$　(f) 非二元划分, $n = 2^{20}$

Adult 数据集, $d = 15, k = 6$



(g) 二元划分, $n = 2^{16}$　(h) 二元划分, $n = 2^{18}$　(i) 二元划分, $n = 2^{20}$



(j) 非二元划分, $n = 2^{16}$　(k) 非二元划分, $n = 2^{18}$　(l) 非二元划分, $n = 2^{20}$

US 数据集, $d = 16, k = 6$

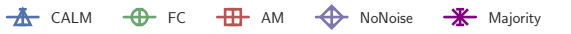
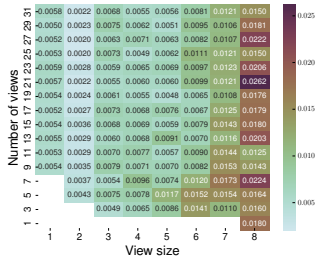
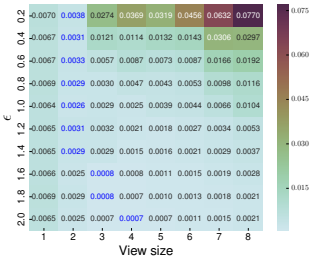


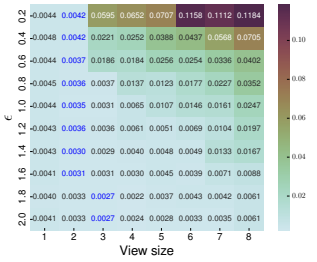
图 3.6　分类性能比较。图中只画出了相应设置下有处理能力的算法，NoNoise 方法为不添加噪音时的基准方法，Majority 方法是一直回答多数标签时的基准方法



(a) ℓ vs m, $d = 8, k = 3, \epsilon = 0.6$

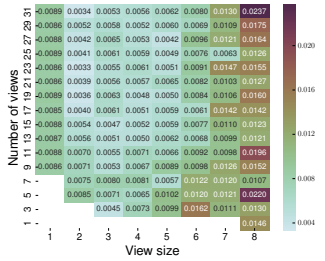


(b) ℓ vs ϵ, $n = 2^{16}, d = 8, k = 3, m = 16$

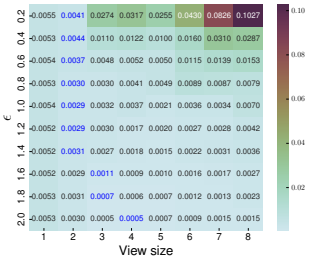


(c) ℓ vs ϵ, $n = 2^{16}, d = 16, k = 3, m = 16$

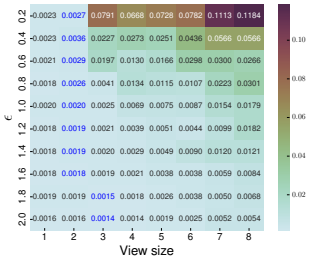
POS 数据集, $n = 2^{16}$



(d) ℓ vs m, $d = 8, k = 3, \epsilon = 0.6$



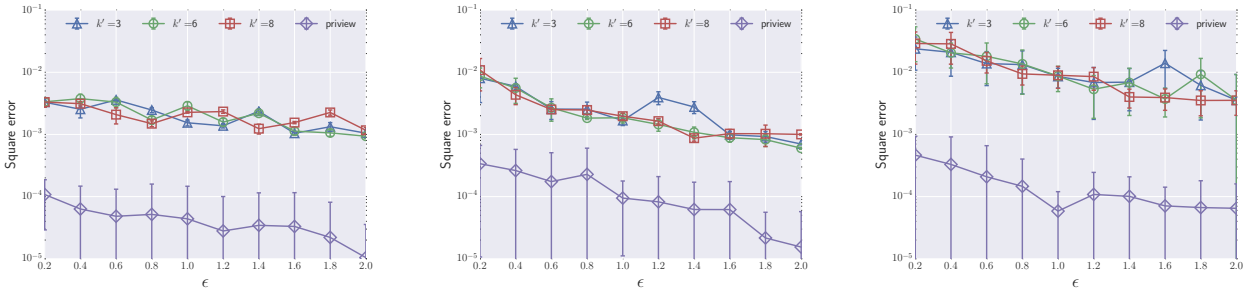
(e) ℓ vs ϵ, $d = 8, k = 3, m = 16$



(f) ℓ vs ϵ, $d = 16, k = 3, m = 16$

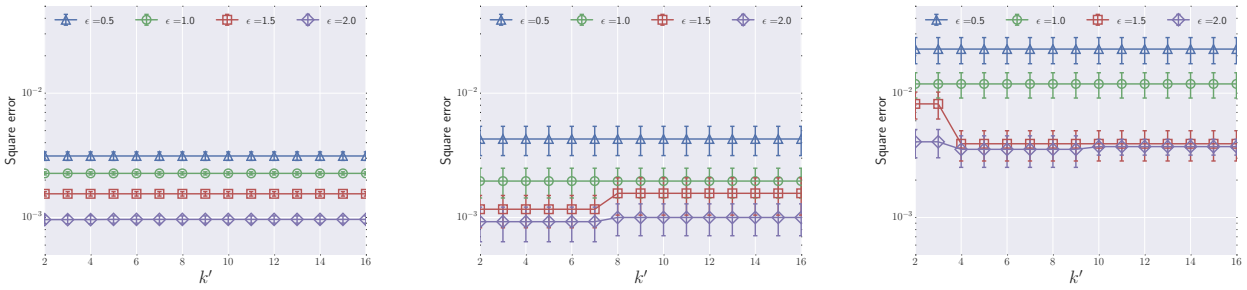
Kosarak 数据集, $n = 2^{16}$

图 3.7　视图大小 ℓ，视图数量 m 和隐私预算 ϵ 之间的相互关系



(a) $n = 2^{16}, d = 16, k = 3$　(b) $n = 2^{18}, d = 16, k = 6$　(c) $n = 2^{18}, d = 32, k = 8$

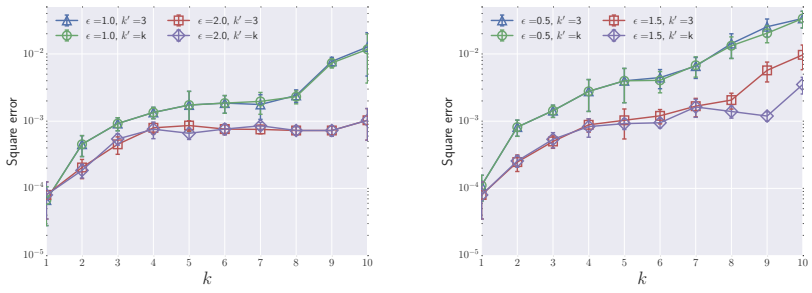
ϵ 变化



(d) $n = 2^{16}, d = 16, k = 3$　(e) $n = 2^{18}, d = 16, k = 6$　(f) $n = 2^{18}, d = 32, k = 8$

k' 变化

图 3.8　Kosarak 数据集，针对不同 k' 优化的 m 和 ℓ 值对性能的影响



(a) $\epsilon \in \{1.0, 2.0\}$　(b) $\epsilon \in \{0.5, 1.5\}$

图 3.9　Kosarak 数据集，$n = 2^{18}, d = 16$

第四章　基于静态激励的隐私预算优化

本章摘要： 基于激励设计的隐私预算优化方法通过补偿用户隐私损失的方式激励其使用更高的隐私预算，从而提升数据可用性。用户隐私损失与隐私预算和隐私偏好密切相关。为解决融合中心与用户之间的信息不对称问题，也就是融合中心无法得知用户具体隐私偏好，本章提出了一套基于契约理论的静态激励方法 REAP 。具体来说，本章首先推导出隐私预算与融合精度之间的定量关系；然后在经济预算一定的情况下，使用契约理论设计了一套有效的契约来最大化数据可用性。REAP 假设融合中心拥有用户隐私偏好分布的先验知识，并为拥有不同隐私偏好的用户提供不同的契约，以此解决融合中心和用户之间的信息不对称问题。本章推导出了在完全信息和不完全信息下最优契约的解析表达式，并且把契约设计推广到用户隐私偏好连续取值的情形。仿真结果验证了 REAP 的可行性和有效性。

关键词： 群智感知，信息不对称，契约理论，隐私偏好

4.1　引言

基于激励设计的隐私预算优化方法适用于数据拥有者不是数据消费者的场景，近年来兴起的群智感知系统是这种场景下的一个典型应用。众多移动设备（比如智能手机，智能手表和平板电脑等）集成的大量传感器（比如 GPS，摄像头和加速度计等）为移动群智感知技术[114,115] 的兴起提供了条件。群智感知系统因其低成本和可大规模部署等优点，已被大量应用于现实生活中，比如智能交通，环境监测和健康医疗等[116–119]。

在典型的群智感知系统中，融合中心需要从用户端收集感知数据，并对这些数据进行分析与融合以挖掘有用信息。以公共健康监测为例，融合中心可以从用户端获取日常锻炼数据，并通过对这些数据的分析可以对这些数据执行诸如均值估计和直方图统计等分析。显然，向融合中心贡献数据对于用户来说成本是很高的，比如这将消耗用户移动设备的电量和数据流量，同时也存在着潜在的隐私泄露风险。因此，如果没有获得有效的补偿，用户将不愿意贡献数据。

大多数现有工作都只考虑移动设备资源的消耗[120–122]，仅有少数考虑用户的隐私损失。

在文献[50]中，作者提出了一种基于博弈论的方法，该方法的目的是获得用户之间的纳什均衡，而那时均衡点往往不是系统最优点，也就说说融合中心无法在经济预算一定的情况下获得最优融合精度[1]。文献[104]提出了一种基于拍卖理论的方法，但只能处理一个任务的情况，而且该论文提出的隐私保护方法实际上并不满足本地差分隐私。本章研究的是连续数据的激励设计，并能在经济预算一定的情况下获得最优数据可用性。

解决以上问题的第一个研究挑战是：用户想要在感知数据中添加更多的噪音来获得更高的隐私保护程度，而融合中心想要获得更高质量的数据来获得更好的融合精度。另一个研究挑战是如何克服融合中心和用户之间的信息不对称问题，也就是融合中心无法得知用户的隐私偏好。而不同用户的隐私偏好往往是不相同的，比如女性用户往往比男性用户更看重自己的年龄，病人往往比健康人更关注自己的位置信息。用户之间隐私偏好的不同将造成其隐私损失的不同。因此，一个有效的激励机制需要能够区分不同用户的隐私损失并给不同用户提供不同的补偿方案。

为解决以上研究挑战，本章提出了基于契约理论的 REAP 方法[2]。激励机制为不同用户设计不同的契约，每个契约包含一种隐私预算，以及用户采用该隐私预算时可以获得的补偿。设计一套有效契约的核心是，保证用户在选择自身隐私偏好对应的契约时能获得最大的效用。

具体来说，本章首先推导出了用户隐私预算与融合中心融合精度之间的定量关系。一旦该定量关系确定，便可以在经济预算一定的情况下，设计一套最优契约来最大化数据可用性。首先考虑完全信息情形下的契约设计，融合中心拥有所有用户的精确隐私偏好，该情形可以作为可获取的最优数据可用性基准。然后考虑了非对称信息情形下的最优契约设计，此时融合中心只拥有用户隐私偏好的分布信息，而不知道每个用户具体的隐私偏好。本章得到了两种情形下最优契约的闭式解，并进一步扩展到了用户隐私偏好连续取值的情形。在这种情况下，可用性优化问题变成了泛函求极值的问题，可以使用最优控制理论进行求解。

本章贡献总结如下：

- 提出基于契约理论的 REAP 方法来解决融合中心与用户之间的信息不对称问题。
- 推导出用于隐私预算与融合中心数据可用性之间的定量关系。

[1]在群智感知系统中，数据可用性一般用融合精度表示，因此在下文表述中将根据方便程度交叉使用融合精度和数据可用性

[2]REAP 的名字来源为 REconciling Aggregation accuracy and individual Privacy.

- 推导出完全信息和非完全信息下最优契约的闭式解，并把结果推广到了用户隐私偏好连续取值的情形。

本章剩余部分组织如下。第 4.2节概述了本章研究的群智感知系统，并推导了用户隐私预算与融合中心融合精度之间的定量关系。在第 4.3节中，使用契约理论解决了用户与融合中心之间信息不对称问题，并把结果在第 4.4节中进行了推广。第 4.5节的实验结果验证了契约设计的有效性，最后第 4.6节总结全章。

表 4.1总结了本章用到的所有符号。

符号	含义	符号	含义
$\mathcal{U}$	用户集合	λ_k	类型 k 用户属两个
$\mathcal{D}$	感知数据集合	u_i	用户 i 效用
d_i	用户 i 的原始感知数据	p_i	用户 i 获得报酬
γ	感知数据取值范围	ϵ_i	用户 i 隐私预算
η_i	加到用户 i 感知数据的拉普拉斯噪音	θ_i	用户 i 隐私偏好
b_i	拉普拉斯噪音 η_i 参数	α	融合中心融合误差
n	用户数量	δ	融合中心融合误差执行度
k	用户类型数量	B	融合中心经济预算

表 4.1　第四章符号及含义列表

4.2　系统模型

本部分首先介绍了群智感知系统模型及激励机制运行流程，然后推导出了用户隐私预算和融合中心融合精度之间的定量关系，最后介绍用户效用定义。

4.2.1　群智感知系统概述

本章考虑的群智感知系统包含一个融合中心，一个任务发布机构以及 n 个用户 $\mathcal{U} = \{u_1, u_2, \cdots, u_n\}$，如图 4.1所示。融合中心的目标是从 n 个用户中收集一组感知数据 $\mathcal{D} = \{d_1, d_2, \cdots, d_n\}$，其中 $d_i \in \mathbb{R}$ 是一个连续数值。接下来，融合中心对收集数据进行分析与融合以获取有用信息。简单起见，本章只讨论均值融合，也就是 $s = \frac{1}{n}\sum_{i=1}^{n} d_i$。均值融合算法在实际生活中经常用到，比如地图应用通过收集用户 GPS 信息，并执行均值融合算法

来估计车流速度。在医疗健康应用中，融合中心通过收集用户运动数据，并执行均值融合算法来监测公共健康状况。本章以及下一章的均值估计方法均采用了拉普拉斯机制，原因有两个：i) 拉普拉斯机制实现起来最简单，能够有效减轻系统计算与通信代价；ii) 本章的主要目的是验证激励设计方法的有效性，并希望探索采用最简单的拉普拉斯机制后，激励设计方法带来的数据可用性提升能否超越单纯采用最优均值估计方法，第4.5节通过实验验证了该想法。需要指出的是，本章框架同样适用于第二章中讨论的其他两种均值估计方法 DM 和 PM 。

4.2.2 静态激励机制工作流程

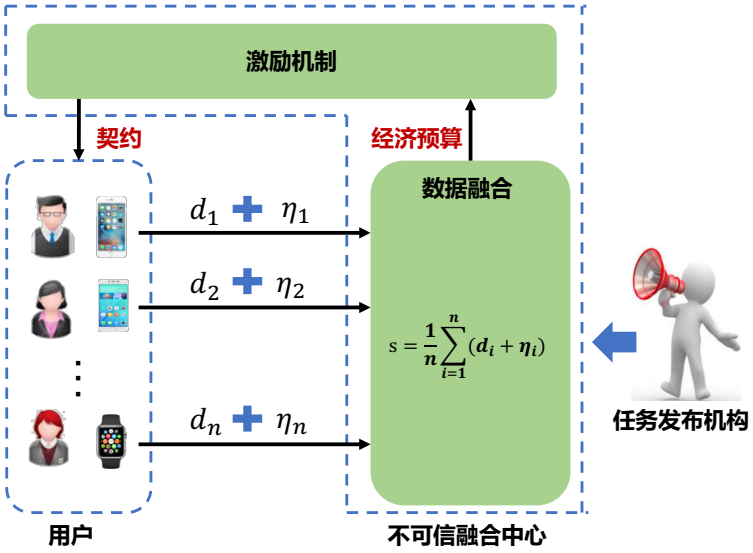


图 4.1 REAP 方法系统框架

本章研究的激励机制工作流程如下：

- 首先，任务发布机构向融合中心发出感知任务请求。
- **激励机制**。接下来融合中心在经济预算一定的情况下设计一套有效的契约来最大化融合精度，并把他们广播给所有用户，其中每个契约都是一个隐私预算与相应报酬的元组。每个用户都可以任意选择一个最大化自身效用的契约。一旦契约签订完成，所有用户都必须按照契约中指定的隐私预算来对感知数据进行加噪处理；作为回报，他们将获得相应契约中指定的报酬。
- **数据融合**。在收到所有用户的扰动数据后，融合中心执行均值融合来获得所需均值。

- 最后，融合中心把融合数据返回给任务发布机构。

4.2.3　隐私预算与融合精度定量关系

精度定义。本章使用以下融合精度定义：

定义 4.2.1 ((α,δ)-精度). *扰动数据均值 $\hat{s}$ 满足 (α,δ)-精度，如果*

$$Pr[|\hat{s}-s|\geq\alpha]\leq 1-\delta,$$

其中 s 是真实数据的均值。

直观上来看，该定义表示融合误差超过 α 的概率不大于 $1-\delta$。从估计理论的角度来看，α 表示置信区间，δ 表示置信度。显然，如果给定置信度，置信区间越小意味着融合精度越高。因此，可以使用在给定置信度下的置信区间 α 来衡量融合精度，其中 α 越小表示融合精度越高。

定量关系。隐私预算与融合精度之间的定量关系由以下引理给出：

引理 4.2.2. *对于给定的置信度 $\delta\leq 1$，融合精度 α 可以表示为*

$$\alpha=\frac{\sqrt{2}\gamma}{n\sqrt{1-\delta}}\sqrt{\sum_{i=1}^{n}\frac{1}{\epsilon_i^2}}. \tag{4.1}$$

其中 ϵ_i 表示用户 i 的隐私预算，n 表示用户数量，γ 表示用户感知数据的取值范围。需要注意的是，对于特定的群智感知任务来说，所有用户感知数据的取值范围都是相同的，比如正常成年人的心跳速率一般都在 $60\sim 100$ bpm 之间。因此，所有用户的 γ_i 取值相同，也就是 $\gamma_i=\gamma,\forall\gamma_i$。

证明. 扰动数据的融合精度可以表示为

$$\hat{s}-s=\frac{1}{n}\sum_{i=1}^{N}(d_i+\eta_i)-\frac{1}{n}\sum_{i=1}^{N}d_i=\frac{1}{n}\sum_{i=1}^{N}\eta_i.$$

拉普拉斯变量 $\eta_i\sim Lap(0,b_i)$ 的方差为 $2b_i^2$，也就是 $Var(\eta_i)=2b_i^2$，因此

$$Var(\frac{1}{n}\sum_{i=1}^{N}\eta_i)=\frac{2}{n^2}\sum_{i=1}^{n}b_i^2.$$

根据切比雪夫不等式

$$P[|s-\hat{s}| \geq \alpha] \leq \frac{2}{\alpha^2 n^2} \sum_{i=1}^{n} b_i^2,$$

该公式表示扰动数据满足 $(\alpha, \frac{2}{\alpha^2 n^2} \sum_{i=1}^{n} b_i^2)$-精度.

因此，对于给定的置信度 $\delta \leq 1$

$$\alpha = \frac{\sqrt{2}\gamma}{n\sqrt{1-\delta}} \sqrt{\sum_{i=1}^{n} b_i^2}$$

把 $b_i = \frac{\gamma_i}{\epsilon_i}$ 带入上式，并令 $\gamma_i = \gamma$，得到

$$\alpha = \frac{\sqrt{2}\gamma}{n\sqrt{1-\delta}} \sqrt{\sum_{i=1}^{n} \frac{1}{\epsilon_i^2}}.$$

□

由于更小的 ϵ_i 表示更高的隐私保护程度，观察公式 (5.1)可以发现，融合中心的融合误差 α 随着用户隐私保护程度的减小而减小，符合直观理解。

4.2.4 用户效用定义

根据差分隐私的效用理论，两个相邻数据的期望效用可以表示为 e^{ϵ_i}。由于在实际使用中 ϵ_i 往往取值比较小，因此可以使用它的线性近似 $e^{\epsilon_i} \approx 1 + \epsilon_i$。进一步，隐私损失可以定义为真实数据和扰动数据效用之间的差值，并且是 ϵ_i 的线性函数。基于此，可以定义用户的效用函数：

定义 4.2.3 (用户效用). 用户 u_i 的效用函数可以定义为

$$U_i = p_i - \theta_i \epsilon_i, \tag{4.2}$$

其中 p_i 是用户 i 贡献数据时的收益。θ_i 表示用户 i 的隐私偏好 (privacy preference)，也就是用户对其自身隐私的看重程度。显然，不同用户拥有不同的隐私偏好。比如，病人一般比健康人更加看中自己的位置信息。在实际生活中，用户的隐私偏好是他们的隐私信息，融合中心事先无法得知。换句话说，用户与融合中心之间存在着信息不对称。

为保证叙述清晰，本章只考虑了用户的隐私损失。用户由于感知数据造成的其他损失可以很容易得囊括到本章框架中。比如，把用户 u_i 其他类型的损失定义为 s_i，他的效用变成 $U_i = p_i - s_i - c_i$，其中 p_i 和 c_i 分别表示用户 u_i 的报酬和隐私损失。定义 $p_i' = p_i - s_i$，用户 u_i 的效用变成 $U_i = p_i' - c_i$，这就转化成了本章的效用函数。

4.3　基于契约理论的激励机制设计

4.3.1　契约建模

契约理论研究的是在存在信息不对称的情况下，如何在经济决策者之间构建契约并达成共识。本章中，融合中心不知道用户具体的隐私偏好 θ_i，并且想要设计一套契约来激励用户参与到群智感知系统中。为方便后续讨论，可以根据隐私偏好将所有用户分成不同组，使得类型 i 用户的隐私偏好为 θ_i。

本节首先考虑用户类型是有限的，共 k 组 $\Theta = \{\theta_i, \theta_2, \cdots \theta_k\}$（$\theta$ 连续取值的情形将在下一节讨论）。为简化分析，首先把用户类型进行升序排序，也就是 $\theta_1 \leq \theta_2 \leq \cdots \leq \theta_k$。使用契约理论，融合中心将给每一类用户设计一个包含隐私保护程度 ϵ 和相应的报酬 p_i 的契约。具体来说，融合中心想要设计一套隐私-报酬对 $\mathcal{C} = \{(\epsilon_1, p_1), \cdots, (\epsilon_k, p_k)\}$，这些隐私-报酬对被称为契约项目。每个用户都可以自行选择签署一个契约项目 (ϵ_i, p_i)，并且通过上传满足 ϵ_i-本地差分隐私的数据来获得报酬 p_i。

每类用户都可以选择一个契约项目来最大化他们的效用（定义见公式 (4.2)）。融合中心的目标是设计一套最优契约来最小化融合误差 α。由于 $\frac{\sqrt{2}\gamma}{n\sqrt{1-\delta}}$ 是一个非负常量，最小化 $\alpha = \frac{\sqrt{2}\gamma}{n\sqrt{1-\delta}}\sqrt{\sum_{i=1}^{n}\frac{1}{\epsilon_i^2}}$ 等价于最小化 $\alpha = \sum_{i=1}^{n}\frac{1}{\epsilon_i^2}$。

接下来，将分别介绍以下两种信息假设下的最优契约设计：

- **完全信息：**研究完全信息情形的目的提供一个基准，此时融合中心准确知道所有用户的准确类型，因此可以给每类用户提供精确的契约。显然，在这种情形下融合中心可以获得最低的融合误差，因为不需要付出任何额外的报酬。这种情形也可以作为融合中心的融合误差下界。

- **不完全信息：**在不完全信息情形中，融合中心不知道每个用户的精确类型，但是知道用户类型的分布，也就是类型 i 的用户有 λ_i 个。在这种情形下，融合中心可以设计并广播一套契约给所有用户，每个用户可以自行选取其中一个契约来最大化效用。

4.3.2　完全信息下最优契约设计

在完全信息情形下，融合中心知道每个用户的精确类型，因此可以为每个用户设计精确的契约。融合中心只需要保证每个用户的效用为非负以保证用户参与性。在契约理论中，这个要求被称作个体理性（Individual Rationality，简称 IR）约束，正式定义如下：

定义 4.3.1 (个体理性). 一套契约满足个体理性如果它们能使所有用户的效用非负，也就是

$$p_i - \theta_i \epsilon_i \geq 0, \forall i. \tag{4.3}$$

因此，在完全信息情形下，可以通过求解以下优化问题来设计最优契约：

问题 4.3.2.

$$\begin{aligned} \min \ & \sum_{i=1}^{k} \frac{\lambda_i}{\epsilon_i^2}, \\ s.t. \ & \sum_{i=1}^{k} \lambda_i p_i \leq B, & (4.4) \\ & p_i - \theta_i \epsilon_i \geq 0, \quad \forall i. & (4.5) \end{aligned}$$

其中 B 表示融合中心的经济预算。

接下来讨论该问题的解法。首先引入以下引理

引理 4.3.3. 不等式 (4.4)和(4.5)可以同时取等号，也就是 $\sum_{i=1}^{k} \lambda_i p_i = B$ and $p_i - \theta_i \epsilon_i = 0$。

通过反证法可以很容易得到公式 (4.4)和 (4.5)可以取等号。给定 p_i，如果存在一个契约使得 $p_i - \theta_i \epsilon_i > 0$，那么一定可以找到一个更大的 ϵ_i 来获得更低的融合误差，直到等号成立。同理，如果存在一个契约使得 $\sum_{i=1}^{k} \lambda_i p_i < B$ 成立，一定可以找到一个更大的 p_i（对应更大的 ϵ_i）来获得更低的融合误差，直到等号成立。证明完成。

引理4.3.3显示个体理性和经济预算约束在优化问题（4.3.2）中都是紧的，这也意味着融合中心可以把所有类型的用户效用降低到 0（这里需要注意的是，效用为 0 并不代表报酬为 0，在经济学中，只要保证理性用户的效用非负，他们就有足够的动机参与到经济活动中），也就是 $p_i^* = \theta_i \epsilon_i^*$。因此，问题4.3.2可以转化成以下问题：

问题 4.3.4.

$$\begin{aligned} \min \ & \sum_{i=1}^{k} \frac{\lambda_i}{\epsilon_i^2}, \\ s.t. \ & \sum_{i=1}^{k} \lambda_i p_i = B, & (4.6) \\ & p_i - \theta_i \epsilon_i = 0, \quad \forall i. & (4.7) \end{aligned}$$

通过求解问题4.3.4可以得到以下定理：

定理 4.3.5. 在完全信息情形下，最优契约 $\{\epsilon_i^*, p_i^*\}$ 可以通过下列公式得到

$$\epsilon_i^* = \frac{B}{\sum_{j=1}^k \lambda_j \theta_j^{\frac{2}{3}}} \theta_i^{-\frac{1}{3}}, \tag{4.8}$$

$$p_i^* = \frac{B}{\sum_{j=1}^k \lambda_j \theta_j^{\frac{2}{3}}} \theta_i^{\frac{2}{3}}. \tag{4.9}$$

证明. 把公式 (4.7)带入到 (4.6)中可以得到

$$\sum_{i=1}^k \lambda_i \theta_i \epsilon_i = B \tag{4.10}$$

问题 4.3.4的拉格朗日乘子为

$$L(\epsilon_i, \alpha) = \sum_{i=1}^k [\frac{\lambda_i}{\epsilon_i^2} + \alpha \lambda_i \theta_i \epsilon_i] - \alpha B,$$

其中 α 为拉格朗日乘数。

根据 KKT 条件可以得到

$$\frac{\partial L}{\partial \epsilon_i} = \frac{-2\lambda_i}{\epsilon_i^3} + \alpha \lambda_i \theta_i = 0, \quad \forall i.$$

求解上述方程可以得到 $\epsilon_i = \sqrt[3]{\frac{2}{\alpha}} \theta_i^{-\frac{1}{3}}$。把这个公式带入 (4.10)可以得到

$$\sqrt[3]{\frac{2}{\alpha}} = \frac{B}{\sum_{i=1}^k \lambda_i \theta_i^{\frac{2}{3}}}.$$

因此，ϵ_i^* 为

$$\epsilon_i^* = \frac{B}{\sum_{j=1}^k \lambda_j \theta_j^{\frac{2}{3}}} \theta_i^{-\frac{1}{3}}, \tag{4.11}$$

把公式 (4.11)带入 $p_i^* - \theta_i \epsilon_i^* = 0$，$p_i^*$ 可以计算得到

$$p_i^* = \frac{B}{\sum_{j=1}^k \lambda_j \theta_j^{\frac{2}{3}}} \theta_i^{\frac{2}{3}}. \tag{4.12}$$

□

通过对定理 4.3.5的参数进行分析，可以得到以下观察。

观察 1. 由于 ϵ_i 越小表示隐私保护程度越高，定理 4.3.5显示类型 i 用户的隐私保护程度会随着经济预算 B 的增加而减小，并随着 θ_i 的增大而增大，这是符合直观理解的。换句话说，越多的隐私预算可以使得用户选择更低的隐私保护程度来获得更低的融合误差，融合中心倾向于从隐私偏好高的用户那里购买更少的隐私来降低成本。

4.3.3 不完全信息下最优契约设计

在不完全信息情形下，融合中心不知道每个用户的具体类型，只知道所有用户类型的分布，也就是类型 i 用户的数量为 λ_i。在实际中，用户类型的分布可以通过问卷调查得到，或者通过分析用户的历史行为来得到[123,124]。显然，融合中心需要为每一类用户设计一个契约来最小化融合误差，但是由于其不知道每个用户的具体类型，只能选择把所有契约广播给所有用户。然而，如果对于某个用户来说，选择其他契约能带来更高的效用，他将假装其他组成员来获得更高效用。为鼓励所有用户真实选择对应契约，需要保证为每类用户设计的契约能为他们带来最高的效用。该要求在契约理论中被称作激励兼容（Incentive Compatibility，简称 IC）

定义 4.3.6 (激励兼容). 一套契约满足激励兼容，如果类型 i 对应的契约能为他们带来最高的效用，也就是

$$p_i - \theta_i \epsilon_i \geq p_j - \theta_i \epsilon_j, \quad \forall j \neq i. \tag{4.13}$$

除了激励兼容约束，不完全信息情形同样需要满足个体理性约束。因此，可以通过求解以下优化问题来设计不完全信息下的最优契约：

问题 4.3.7.

$$\min \sum_{i=1}^{k} \frac{\lambda_i}{\epsilon_i^2},$$

$$s.t. \sum_{i=1}^{k} \lambda_i p_i \leq B, \tag{4.14}$$

$$p_i - \theta_i \epsilon_i \geq 0, \quad \forall i, \tag{4.15}$$

$$p_i - \theta_i \epsilon_i \geq p_j - \theta_i \epsilon_j, \quad \forall j \neq i. \tag{4.16}$$

注意到问题 4.3.7中有 k 个 IR 约束和 $k(k-1)$ 个 IC 约束，当 k 很大时，求解将变得

很困难。幸运的是，这些约束可以通过以下两个引理进行简化。

引理 4.3.8. k 个 IR 约束可以简化成下面一个约束：

$$p_k - \theta_k \epsilon_k = 0. \tag{4.17}$$

证明. 由于所有用户类型都被升序排序了，也就是 $\theta_1 \leq \theta_2 \leq \cdots \leq \theta_k$，根据 IC 可以得到

$$p_i - \theta_i \epsilon_i \geq p_k - \theta_i \epsilon_k \geq p_k - \theta_k \epsilon_k, \forall i \neq k.$$

因此，如果类型 k 的 IR 约束被满足了，也就是 $p_k - \theta_k \epsilon_k \geq 0$，其他所有类型的约束也能自动满足。因此，可以只保留最后一个 IR 约束。进一步，如果存在一个最优契约满足 $p_k - \theta_k \epsilon_k > 0$，一定可以找到一个更大的 ϵ_k 来获得更低的融合误差，直到 $p_k - \theta_k \epsilon_k = 0$。证明完成。 □

引理 4.3.8显示，契约设计只能做到让最高类型的用户效用为 0，随着类型的降低，用户可以逐渐获得更高的效用。原因是融合中心不知道每个用户的真实类型，只能提供给低类型用户大于其隐私损失的报酬以使他们选择对应类型的契约；否则他们将选择更高类型的契约来最大化自身效用。这个现象被称为相对于完全信息情形的信息损失。

引理 4.3.9 (单调性质). 如果 $\theta_1 \leq \theta_2 \leq \cdots \leq \theta_k$，那么 $\epsilon_1 \geq \epsilon_2 \geq \cdots \geq \epsilon_k$ 成立

证明. 通过 IC 约束，我们可以得到

$$p_i - \theta_i \epsilon_i \geq p_j - \theta_i \epsilon_j,$$
$$p_j - \theta_j \epsilon_j \geq p_i - \theta_j \epsilon_i.$$

将这两个公式累加，可以得到 $\epsilon_i(\theta_j - \theta_i) \geq \epsilon_j(\theta_j - \theta_i)$。因此，如果 $\theta_i \leq \theta_j$，那么 $\epsilon_i \geq \epsilon_j$。证明结束。 □

直观上来看，引理 4.3.9显示，越高类型的用户将被分配到更低的隐私保护程度，因为收购它们的单位成本更高并导致融合中心需要付出更大的成本来达到相同的融合精度。此外，该引理可以用来证明引理 4.3.10。

引理 4.3.10. $k(k-1)$ 个 IC 约束可以简化成以下 $k-1$ 个约束：

$$p_i - \theta_i \epsilon_i = p_{i+1} - \theta_i \epsilon_{i+1}, \forall i \leq k-1. \tag{4.18}$$

证明. 该引理的证明可以分成三步。

首先，可以证明，如果 $p_i - \theta_i\epsilon_i \geq p_{i-1} - \theta_i\epsilon_{i-1}$ 成立，那么 $p_i - \theta_i\epsilon_i \geq p_j - \theta_i\epsilon_j$ 对于所有的 $j \in \{i-1, i-2, \cdots, 1\}$ 都成立。

根据 IC 约束，可以得到

$$p_i - \theta_i\epsilon_i \geq p_{i-1} - \theta_i\epsilon_{i-1}, \tag{4.19}$$

$$p_{i-1} - \theta_{i-1}\epsilon_{i-1} \geq p_{i-2} - \theta_{i-1}\epsilon_{i-2}. \tag{4.20}$$

公式 (4.20)可以进一步转化成以下形式

$$\theta_{i-1}(\epsilon_{i-2} - \epsilon_{i-1}) \geq p_{i-2} - p_{i-1}.$$

回想引理 4.3.9中的单调性质，可以得到 $\theta_{i-1} \leq \theta_i$ 和 $\epsilon_{i-2} \geq \epsilon_{i-1}$。因此，$\theta_i(\epsilon_{i-2} - \epsilon_{i-1}) \geq p_{i-2} - p_{i-1}$ 或者 $p_{i-1} - \theta_i\epsilon_{i-1} \geq p_{i-2} - \theta_i\epsilon_{i-2}$。使用同样的方法，可以得到

$$p_i - \theta_i\epsilon_i \geq p_{i-1} - \theta_i\epsilon_{i-1} \geq \cdots \geq p_1 - \theta_i\epsilon_1.$$

这组不等式证明了第一步的正确性。

其次，需要证明，如果 $p_i - \theta_i\epsilon_i \geq p_{i+1} - \theta_i\epsilon_{i+1}$ 满足，那么 $p_i - \theta_i\epsilon_i \geq p_j - \theta_i\epsilon_j$ 对于所有的 $j \in \{i+1, i+2, \cdots, k\}$ 都满足。

与第一步证明类似，可以得到

$$p_i - \theta_i\epsilon_i \geq p_{i+1} - \theta_i\epsilon_{i+1} \geq \cdots \geq p_1 - \theta_i\epsilon_1,$$

这也就证明了第二步的正确性。另外注意到，对于一个最优契约来说，一定满足 $p_i - \theta_i\epsilon_i = p_{i+1} - \theta_i\epsilon_{i+1}$，否则，永远可以找到一个更大的 ϵ_i 来获得更低的融合误差，直到等号满足。

最后，需要证明 $p_i - \theta_i\epsilon_i = p_{i+1} - \theta_i\epsilon_{i+1}$ 可以推导出 $p_i - \theta_i\epsilon_i \geq p_{i-1} - \theta_i\epsilon_{i-1}$。

显然，$\theta_i(\epsilon_{i-1} - \epsilon_i) \geq \theta_{i-1}(\epsilon_{i-1} - \epsilon_i)$，重新整理该公式可以得到

$$p_i - \theta_i\epsilon_i \geq p_i + \theta_{i-1}\epsilon_{i-1} - \theta_{i-1}\epsilon_i - \theta_i\epsilon_{i-1}.$$

因为 $p_i - \theta_i\epsilon_i = p_{i+1} - \theta_i\epsilon_{i+1}$，所以 $p_{i-1} - \theta_{i-1}\epsilon_{i-1} = p_i - \theta_{i-1}\epsilon_i$ 满足，也就是 $p_i + \theta_{i-1}\epsilon_{i-1} - \theta_{i-1}\epsilon_i = p_{i-1}$。因此，可以得到 $p_i - \theta_i\epsilon_i \geq p_{i-1} - \theta_i\epsilon_{i-1}$。

综上所述，$p_i - \theta_i\epsilon_i = p_{i+1} - \theta_i\epsilon_{i+1}$ 可以导出 $p_i - \theta_i\epsilon_i \geq p_j - \theta_i\epsilon_j, \forall j \neq i$。证明结束。 □

引理 4.3.10保证了，当第 i 类用户的契约 (ϵ_i, p_i) 给他们带来的收益与第 $i+1$ 类用户的契约 $(\epsilon_{i+1}, p_{i+1})$ 相同时，所有的 IC 约束都自动满足。

利用引理 4.3.8和引理 4.3.10，问题 4.3.7可以简化成：

问题 4.3.11.

$$\begin{aligned}
&\min \sum_{i=1}^{k} \frac{\lambda_i}{\epsilon_i^2}, \\
&s.t. \quad \sum_{i=1}^{k} \lambda_i p_i = B, && (4.21)\\
&\qquad p_k - \theta_k \epsilon_k = 0, && (4.22)\\
&\qquad p_i - \theta_i \epsilon_i = p_{i+1} - \theta_i \epsilon_{i+1}, \forall i \leq k-1. && (4.23)
\end{aligned}$$

求解问题 4.3.11，可以得到非对称信息情形下的最优契约设计为：

定理 4.3.12. 在不完全信息的情形下，最优契约 $\{\epsilon_i^*, p_i^*\}$ 为

$$\begin{aligned}
\epsilon_i^* &= G H_i^{-\frac{1}{3}} \lambda_i^{\frac{1}{3}}, \\
p_i^* &= \begin{cases} G(\theta_i H_i^{-\frac{1}{3}} \lambda_i^{\frac{1}{3}} + \sum_{j=i+1}^{k} \Delta\theta_j H_j^{-\frac{1}{3}} \lambda_j^{\frac{1}{3}}), & i \neq k, \\ G\theta_k H_k^{-\frac{1}{3}} \lambda_k^{\frac{1}{3}}, & i = k, \end{cases}
\end{aligned}$$

其中

$$\Delta\theta_i = \theta_i - \theta_{i-1}, \tag{4.24}$$

$$H_i = \begin{cases} \lambda_1 \theta_1, & i = 1, \\ \lambda_i \theta_i + \Delta\theta_i \sum_{j=1}^{i-1} \lambda_j, & i > 1, \end{cases} \tag{4.25}$$

$$G = \frac{B}{\sum_{j=1}^{k} H_j^{\frac{2}{3}} \lambda_j^{\frac{1}{3}}}. \tag{4.26}$$

证明. 根据公式 (4.22)和 (4.23)，可以得到

$$\begin{aligned}
p_{k-1} - \theta_{k-1}\epsilon_{k-1} &= p_k - \theta_{k-1}\epsilon_k \\
&= \theta_k \epsilon_k - \theta_{k-1}\epsilon_k \\
&= (\theta_k - \theta_{k-1})\epsilon_k
\end{aligned} \tag{4.27}$$

令 $\Delta\theta_k = \theta_k - \theta_{k-1}$，公式 (4.27)可以写成 $p_{k-1} = \theta_{k-1}\epsilon_{k-1} + \Delta\theta_k \epsilon_k$。

使用同样的方法，可以得到

$$p_i = \begin{cases} \theta_i \epsilon_i + \sum_{j=i+1}^{k} \Delta\theta_j \epsilon_j, & i \neq k, \\ \theta_k \epsilon_k, & i = k, \end{cases} \tag{4.28}$$

其中 $\Delta\theta_i$ 的定义在公式 (4.24)中。

然后，可以得到

$$\begin{aligned}\sum_{i=1}^{k}\lambda_i p_i =&\sum_{i=1}^{k-1}[\lambda_i\theta_i\epsilon_i+\lambda_i\sum_{j=i+1}^{k}\Delta\theta_j\epsilon_j]+\lambda_k\theta_k\epsilon_k\\ =&\lambda_k\theta_k\epsilon_k+\lambda_{k-1}\theta_{k-1}\epsilon_{k-1}+\lambda_{k-1}\Delta\theta_k\epsilon_k\\ &+\lambda_{k-2}\theta_{k-2}\epsilon_{k-2}+\lambda_{k-2}[\Delta\theta_{k-1}\epsilon_{k-1}+\Delta\theta_k\epsilon_k]\\ &\vdots\\ &+\lambda_1\theta_1\epsilon_1+\lambda_1[\Delta\theta_2\epsilon_2+\cdots+\Delta\theta_k\epsilon_k]\\ =&\epsilon_k[\lambda_k\theta_k+\Delta\theta_k(\lambda_{k-1}+\cdots+\lambda_1)]\\ &+\epsilon_{k-1}[\lambda_{k-1}\theta_{k-1}+\Delta\theta_{k-1}(\lambda_{k-2}+\cdots+\lambda_1)]\\ &\vdots\\ &+\epsilon_1\lambda_1\theta_1.\end{aligned}$$

通过 ϵ_i 对以上公式进行重新整理，可以得到

$$\sum_{i=1}^{k}\lambda_i p_i=\sum_{i=1}^{k}H_i\epsilon_i=B, \tag{4.29}$$

其中 H_i 的定义在公式 (4.25)中。

因此，问题 4.3.11的拉格朗日公式为

$$L(\epsilon,\alpha)=\sum_{i=1}^{k}[\frac{\lambda_i}{\epsilon_i^2}+\alpha H_i\epsilon_i]-\alpha B,$$

其中 α 为拉格朗日乘子。

根据 KKT 条件，可以得到

$$\frac{\partial L}{\partial\epsilon_i}=\frac{-2\lambda_i}{\epsilon_i^3}+\alpha H_i=0.$$

接下来，可以计算 ϵ_i

$$\epsilon_i=\sqrt[3]{\frac{2}{\alpha}}(\frac{\lambda_i}{H_i})^{\frac{1}{3}} \tag{4.30}$$

把公式 4.30带入 4.29中可以得到

$$\sqrt[3]{\frac{2}{\alpha}}=\frac{B}{\sum_{j=1}^{k}H_j^{\frac{2}{3}}\lambda_j^{\frac{1}{3}}}$$

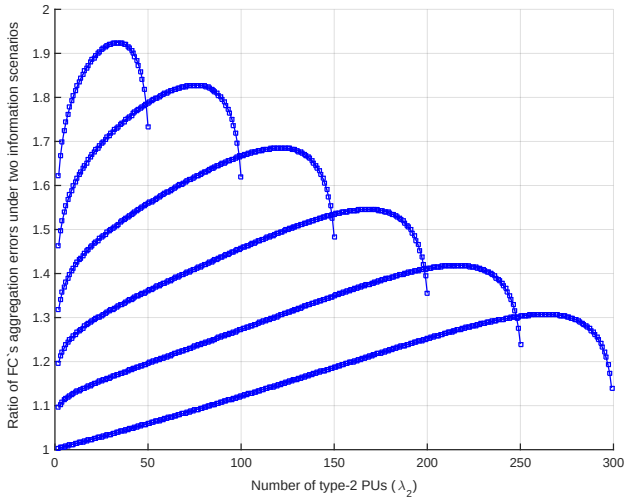


图 4.2　当用户类型为 3 时，融合中心在非完全信息和完全信息下融合误差的比值，也就是 $\frac{\alpha_I}{\alpha_C}$

因此最优契约 ϵ_i^* 为

$$\epsilon_i^* = \frac{B}{\sum_{i=1}^{k} H_i^{\frac{2}{3}} \lambda_i^{\frac{1}{3}}} H_i^{-\frac{1}{3}} \lambda_i^{\frac{1}{3}} \tag{4.31}$$

最后可以计算第 k 个契约为

$$p_k^* = \theta_k \epsilon_k^* = \frac{B}{\sum_{j=1}^{k} H_j^{\frac{2}{3}} \lambda_j^{\frac{1}{3}}} \theta_k H_k^{-\frac{1}{3}} \lambda_k^{\frac{1}{3}}.$$

将公式 (4.31)带入 (4.28)并重新整理可以得到当 $i \neq k$ 时的最优契约。 □

接下来，可以通过图 4.2来比较在完全信息和不完全信息下的融合误差。图 4.2展示了当用户类型数量为 3 时，完全信息和不完全信息的融合误差的比值。$\lambda_1 = 0, 50, 100, 150, 200, 250$ 分别对应图中从下到上的曲线。图中仅展示了 λ_1 和 λ_2，因为 $\lambda_3 = N - \lambda_1 - \lambda_2$。其他参数设置为 $N = 300, B = 1000, \gamma = 10, \delta = 0.9, \theta_1 = 1, \theta_2 = 2, \theta_3 = 3$。图中的比值是用户三种类型 $\{\lambda_i\}_{i=1}^3$ 的函数，并且一定大于或等于 1，因为用户在完全信息下的融合误差永远是最低的。通过分析图 4.2，可以得到以下观察。

观察 2. 融合中心的融合精度在不完全信息下的误差永远比在完全信息下更大。当所有用户都属于最高类型时，两种场景下误差的差距最小。对于相同的 λ_1，误差差距将随着最高类型用户数量的减少而增加，直到一个很小的值。

以上观察发生的原因如下：当所有用户属于最高类型时，所有用户的效用可以跟完全信息一样达到 0。因此，融合误差比值达到 1。当最高类型用户数量减少时，信息损失越来

越大，导致误差差距越来越大。然而，当最高类型用户的数量达到一个很小的值时，信息损失的影响下降，导致融合误差比值上升。

4.3.4 讨论

通过求解优化问题，融合中心可以得到一套最优契约。然而，如果融合中心无法有效监控用户行为，某些用户可能违背契约精神，比如添加比契约中指定的隐私保护程度更大的噪音。为保证所有用户严格按照契约来产生噪音，用户需要在移动设备上安装一个可信的群智感知应用程序。一旦契约签署，可信应用程序将严格按照契约来添加噪音。

传统群智感知任务的目标是选择所有愿意参与用户的一部分来执行某项特定任务，比如汇报交通是否拥堵等。而本章研究的是群智感知任务的数据融合，它的目标是尽可能收集更多的感知数据来进行统计分析，比如本章研究的均值估计。从统计学观点来看，本章目标是计算特定人群的均值特征，因此需要收集所有用户的感知数据来得到真实的总体均值。在实际应用中，如果人群数量太大，可以通过随机抽样的方式来估计人群均值。文献[?]指出，样本均值是总体均值的无偏估计。然而需要指出的是，无偏估计并不严格等于真实估计，如果人群数量本来就很小，收集所有用户的感知数据将是最好的选择。

4.4 连续情况扩展

本部分讨论当用户的隐私偏好连续取值时的最优契约设计。

假设用户类型 θ 的取值范围为 $[\underline{\theta}, \overline{\theta}]$，$\theta$ 的概率密度函数为 $h(\theta)$。与离散情况类似，融合中心可以通过求解以下优化问题来得到最优契约：

问题 4.4.1.

$$\min \int_{\underline{\theta}}^{\overline{\theta}} \frac{h(\theta)}{\epsilon^2(\theta)} d\theta,$$

$$s.t. \int_{\underline{\theta}}^{\overline{\theta}} p(\theta)h(\theta)d\theta \leq B, \tag{4.32}$$

$$p(\theta) - \theta\epsilon(\theta) \geq 0, \tag{4.33}$$

$$p(\theta) - \theta\epsilon(\theta) \geq p(\hat{\theta}) - \theta\epsilon(\hat{\theta}), \forall \hat{\theta} \neq \theta. \tag{4.34}$$

其中 (4.32)为经济预算约束，(4.33)为 IR 约束，(4.34)为 IC 约束。

由于 θ 是连续的，因此 (4.33)和 (4.34)中的 IR 和 IC 约束的数量是无限的。与离散情形类似，这些 IR 和 IC 约束可以通过以下两个引理进行简化。

引理 4.4.2. 无限个 IR 约束可以简化成以下一个约束

$$p(\overline{\theta}) - \overline{\theta}\epsilon(\overline{\theta}) = 0. \tag{4.35}$$

证明. 利用 IC 约束，可以得到以下不等式

$$\begin{aligned} p(\theta) - \theta\epsilon(\theta) &\geq p(\overline{\theta}) - \theta\epsilon(\overline{\theta}) \\ &\geq p(\overline{\theta}) - \overline{\theta}\epsilon(\overline{\theta}), \forall \theta \neq \overline{\theta}. \end{aligned}$$

以上两个不等式显示，类型 $\overline{\theta}$ 的 IR 约束满足意味着 IR 约束对于所有的 $\theta \in [\underline{\theta}, \overline{\theta}]$ 都满足。因此，IR 约束可以简化成 $p(\overline{\theta}) - \overline{\theta}\epsilon(\overline{\theta}) \geq 0$。进一步，可以证明不等式 $p(\overline{\theta}) - \overline{\theta}\epsilon(\overline{\theta}) \geq 0$ 可以取等号。如果存在契约 $(\epsilon(\overline{\theta}), p(\overline{\theta}))$ 使得 $p(\overline{\theta}) - \overline{\theta}\epsilon(\overline{\theta}) > 0$，一定可以找到一个更大的 $\epsilon(\overline{\theta})$ 来获得更小的融合误差，直到 $p(\overline{\theta}) - \overline{\theta}\epsilon(\overline{\theta}) = 0$。证明结束。 □

引理 4.4.3. 无限多个 IC 约束可以简化成以下两个约束：

$$\frac{d\epsilon(\theta)}{d\theta} \leq 0, \tag{4.36}$$

$$\frac{dp(\theta)}{d\theta} - \theta\frac{d\epsilon(\theta)}{d\theta} = 0. \tag{4.37}$$

证明. 根据公式 (4.34)，可以推导出类型 θ 用户的以下两个本地条件

$$\frac{dp(\hat{\theta})}{d\hat{\theta}}\Big|_{\hat{\theta}=\theta} - \theta\frac{d\epsilon(\hat{\theta})}{d\hat{\theta}}\Big|_{\hat{\theta}=\theta} = 0, \tag{4.38}$$

$$\frac{d^2p(\hat{\theta})}{d\hat{\theta}^2}\Big|_{\hat{\theta}=\theta} - \theta\frac{d^2\epsilon(\hat{\theta})}{d\hat{\theta}^2}\Big|_{\hat{\theta}=\theta} \leq 0. \tag{4.39}$$

由于 (4.38)和 (4.39)对所有的 $\theta \in [\underline{\theta}, \overline{\theta}]$ 都成立，因此

$$\frac{dp(\theta)}{d\theta} - \theta\frac{d\epsilon(\theta)}{d\theta} = 0, \tag{4.40}$$

$$\frac{d^2p(\theta)}{d\theta^2} - \theta\frac{d^2\epsilon(\theta)}{d\theta^2} \leq 0. \tag{4.41}$$

对公式 (4.40)进行求导，公式 (4.41)可以简化成

$$\frac{d\epsilon(\theta)}{d\theta} \leq 0. \tag{4.42}$$

接下来证明 (4.40)和 (4.42)对全局成立。对 (4.40)从 $\hat{\theta}$ 到 θ 求定积分得到

$$p(\theta) - p(\hat{\theta}) = \theta\epsilon(\theta) - \theta\epsilon(\hat{\theta}) - \int_{\hat{\theta}}^{\theta} \epsilon(u)du. \tag{4.43}$$

整理 (4.43)可得

$$p(\theta) - \theta\epsilon(\theta) = p(\hat{\theta}) - \hat{\theta}\epsilon(\hat{\theta}) + (\hat{\theta} - \theta)\epsilon(\hat{\theta}) - \int_{\hat{\theta}}^{\theta} \epsilon(u)du.$$

由于 $\epsilon(\theta)$ 是非增的，$(\hat{\theta} - \theta)\epsilon(\hat{\theta}) - \int_{\hat{\theta}}^{\theta} \epsilon(u)du \geq 0$，因此 $p(\theta) - \theta\epsilon(\theta) \geq p(\hat{\theta}) - \hat{\theta}\epsilon(\hat{\theta})$ 对所有的 $\hat{\theta} \neq \theta$ 都成立。证明结束。 □

与离散情形类似，经济预算约束 (4.32)可以取等号，也就是

$$\int_{\underline{\theta}}^{\overline{\theta}} p(\theta)h(\theta)d\theta = B. \tag{4.44}$$

综上，问题 4.4.1可以转化为

问题 4.4.4.

$$\begin{aligned} &\min \int_{\underline{\theta}}^{\overline{\theta}} \frac{h(\theta)}{\epsilon^2(\theta)}d\theta, \\ &s.t.\ \ (4.44)(4.35)(4.36)(4.37). \end{aligned}$$

问题 4.4.4是一个泛函求极值问题,因此可以通过最优控制理论进行求解。令 $u(\theta) = \epsilon(\theta)$ 为控制变量，令 $x_1(\theta) = p(\theta) - \theta\epsilon(\theta)$ 为状态变量，可以得到

$$\begin{aligned} \dot{x}_1(\theta) &= \dot{p}(\theta) - \epsilon(\theta) - \theta\dot{\epsilon}(\theta) \\ &= -\epsilon(\theta) = -u(\theta), \end{aligned}$$

其中第二个等式成立是因为公式 (4.37)。

为处理经济预算约束 (4.32)，可以定义一个新的状态变量

$$\dot{x}_2(\theta) = p(\theta)h(\theta) = [x_1(\theta) + \theta u(\theta)]h(\theta) \tag{4.45}$$

根据 (4.32)，可以推导出以下横截条件

$$x_2(\overline{\theta}) - x_2(\underline{\theta}) = B. \tag{4.46}$$

因此，最优控制问题的汉密尔顿函数为

$$\begin{aligned}&H[x(\theta),u(\theta),\lambda(\theta),\theta]\\=&\frac{h(\theta)}{u^2(\theta)}-\lambda_1(\theta)u(\theta)+\lambda_2(\theta)[x_1(\theta)+\theta u(\theta)]h(\theta),\end{aligned}$$

其中 $\lambda_1(\theta)$ 和 $\lambda_2(\theta)$ 为协状态变量。

根据最优控制问题的欧拉-拉格朗日方程，可以得到以下条件

$$\begin{aligned}\frac{\partial H}{\partial u}&=\frac{-2h(\theta)}{u^3(\theta)}-\lambda_1+\lambda_2\theta h(\theta)=0,\\\dot{\lambda}_1(\theta)&=-\frac{\partial H}{\partial x_1}=-\lambda_2 h(\theta),\\\dot{\lambda}_2(\theta)&=-\frac{\partial H}{\partial x_2}=0.\end{aligned}$$

因此，协状态变量为

$$\begin{aligned}\lambda_2(\theta)&=c_1,\\\lambda_1(\theta)&=-c_1H(\theta)+c_2,\end{aligned}$$

其中 c_1 和 c_2 可以通过横截条件 (4.46)和 (4.35)得到。

综上所述，最优契约 $[\epsilon^*(\theta),p^*(\theta)]$ 为

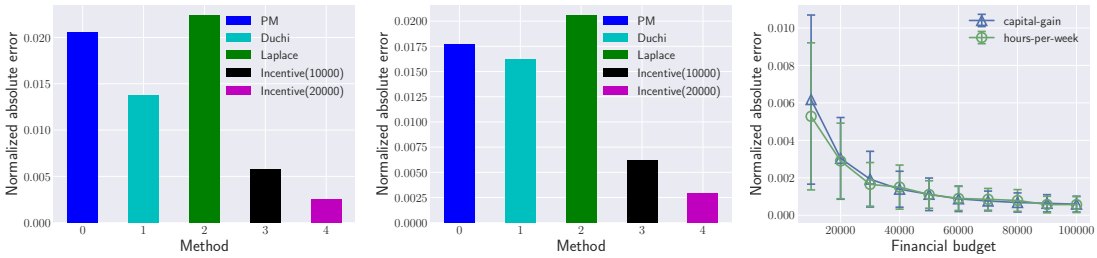
$$\begin{aligned}\epsilon^*(\theta)&=u^*(\theta)\\&=\sqrt[3]{\frac{2h(\theta)}{c_1\theta h(\theta)-c_1H(\theta)-c_2}},\\p^*(\theta)&=x_1(\theta)+\theta\epsilon(\theta)\\&=\theta\epsilon^*(\theta)-\int_{\underline{\theta}}^{\theta}\epsilon^*(\tau)d\tau.\end{aligned}$$

4.5 仿真评估

本小节首先验证激励设计方法相对于单纯采用最优均值估计方法的优越性，然后分别验证本章提出契约的可行性以及不同系统参数对融合误差的影响。

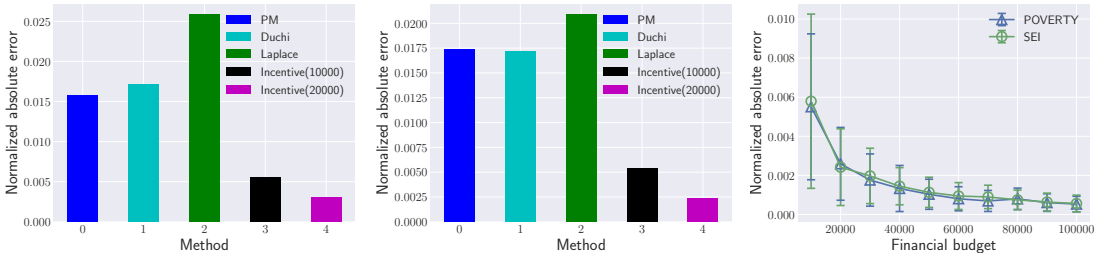
4.5.1 激励设计优越性评估

数据集。本实验使用以下两个真实数据集：



(a) capital-gain. (b) hours-per-week. (c) 经济预算 Vs. 绝对误差

UCI Adult 数据集



(d) POVERTY. (e) SEI. (f) 经济预算 Vs. 绝对误差

IPUMS US 数据集

图 4.3 验证激励方法的有效性，其中激励方法括号后面的数字表示经济预算

- UCI Adult[112]：该数据集来自 UCI 机器学习库并包含 14 个属性。这些属性包含离散属性（比如种族，年龄和教育程度等）和连续属性（比如年龄，资本收益和周工作时间等）。为评估均值估计的性能，本实验使用两个连续属性——资本收益和周工作时间。
- IPUMS US[113]：该数据集来自美国人口普查数据库（IPUMS），包含美国 2016 年的人口普查数据。本实验使用两个连续属性“POVERTY”（考虑了通货膨胀的一个贫困指数）和“SEI”（某项工作的 Duncan Socioeconomic 指数）。

对比算法。 本实验比较了第二章中讨论的 DM 和 PM 两种目前最好的均值估计方法。为了探索激励机制对数据可用性的提升效果，本实验同时比较了不采用激励机制时的拉普拉斯机制 LM 。

评估指标。 本实验使用归一化绝对误差（Normalized Absolute Error，NAE ）来衡量算法性能，也就是

$$\mathrm{NAE} = \frac{|s - \hat{s}|}{\zeta}$$

其中 s 和 $\hat{s}$ 分别表示真实数据和扰动数据的均值，ζ 表示数据取值范围。

对于每个数据集和每种方法，重复 100 次试验并记录 NAE 均值和标准差。

实验设置。从 Adult 和 US 数据集中分别随机抽样 10000 条数据进行试验。对于 PM，DM 和 LM 方法，ϵ 设置为 0.5。对于激励设计方法，用户的隐私偏好 c^p 从 $[0,1]$ 中随机取值，ϵ 设置为刚好能使得所有用户的效用非负，也就是 $\sum_{i:u_i\in\mathcal{U}}\epsilon c_i^p = B$，其中 B 为经济预算。

实验结果。图 4.3a和图 4.3b分别显示了在 Adult 数据集上不同方法的 NAE （US 数据集的结果在图 4.3d和图 4.3e中展示)。与现有最好均值估计算法（PM 和 DM ）相比较，激励设计方法能够获得更小的 NAE 。原因很简单，激励机制能够刺激用户选择更大的 ϵ 来减小扰动，从而减小 NAE 。比如说，当经济预算 $B = 10000$ 时，融合中心可以选择 $\epsilon \geq 1.0$，比 PM 和 DM 采用的 0.5 引入的扰动小很多。

图 4.3c和图 4.3f分别显示了经济预算 B 对 NAE 的影响。实验结果显示，经济预算越多，NAE 越小。进一步，当经济预算超过某个阈值时（比如说 30000)，NAE 已经足够小以至于继续增大投资对性能提升越来越不明显。因此，在实际中，融合中心可以用有限的投入获得想要的融合精度。在极端情况下，如果经济预算足够，NAE 可以无限接近于 0，这对于诸如医疗应用的场景来说是非常有利的。

4.5.2　激励设计有效性评估

表 4.2　实验参数设置

参数	Value	
用户数量 (n)	200	
隐私偏好 (θ)	$[5,15]$	
用户类型 (k)	可行性评估	20
	性能评估	$[5,20]$
经济预算 (B)	可行性评估	1000
	性能评估	$[500,1000]$

实验设置。仿真设定如表 5.2所示。假设有 200 个用户，隐私偏好的取值范围从 5 到 15。为简单起见，假设用户的隐私偏好服从均匀分布。为验证提出契约的可行性，需要证明最优契约满足单调性和激励兼容性，用户类型数量 k 和经济预算 B 分别设置为 20 和 1000。为评估系统参数 k 和 B 对融合误差的影响，分别设置它们的取值范围为 $[5,20]$ 和 $[500,1000]$。

契约可行性验证。图 4.4显示，当用户类型数量增大时，ϵ 减小。由于 ϵ 越小意味着越高的隐私保护程度，图 4.4显示越高类型的用户倾向于选择越高的隐私保护程度，这也就验证了

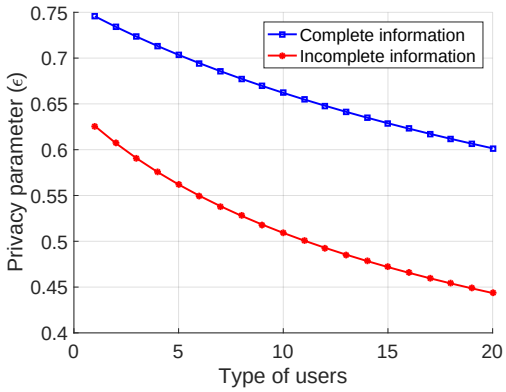


图 4.4　契约单调性验证

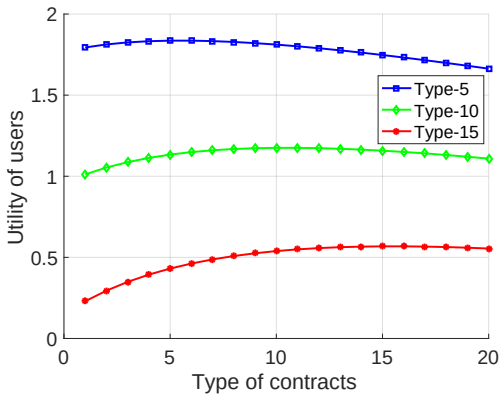


图 4.5　契约激励兼容性验证

单调性。另外，实验结果符合这样一个直观认识，融合中心应该从更高类型的用户那里购买更少的隐私来节省预算。另一方面，当经济预算相同时，用户在完全信息情形下的隐私保护程度低于非完全信息情形。

图 4.5显示了类型为 5，10 和 15 的用户选择不同契约时的效用函数。注意到所有的效用函数都是凹的，并且所有类型用户都在选择对应类型契约时获得最大效用，比如说类型 5 用户选择类型 5 契约时能获得最大效用，这也直接验证了激励兼容性质。另外，当选择同一个契约时，类型越低的用户能获得越高的效用。原因是类型越低的用户拥有越低的隐私偏好 θ_i，根据效用函数定义 $u_j = p_j - \theta_i \epsilon_j, \forall j$，$\theta_i$ 越小效用越高。

系统参数影响。 图 4.6显示了当其他参数固定时，经济预算对融合误差的影响。实验显示经济预算 B 越多融合精度 α 越小。原因显而易见，当融合中心拥有越多隐私预算时，可以使得用户选择更低的隐私保护程度来获得更低的融合误差。

图 4.7评估了在其他参数固定的情况下，用户类型数量对融合误差的影响。实验显示，

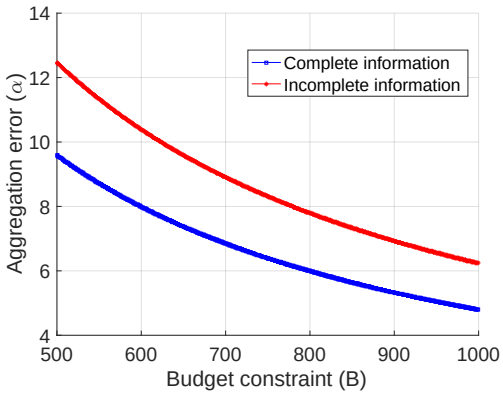


图 4.6　融合精度 Vs. 经济预算

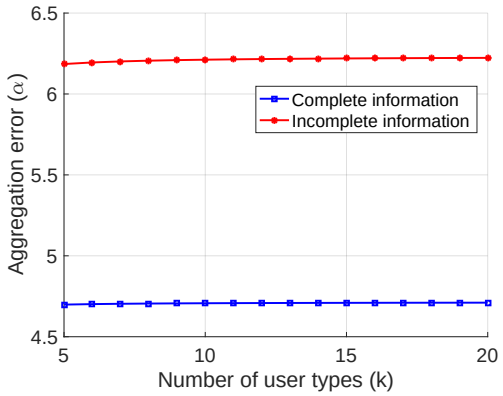


图 4.7　融合精度 Vs. 用户类型数量

融合误差随着用户类型数量的减小而减小。根据 IR 约束 $p_k - \theta_k \epsilon_k = 0$ 和 IC 约束 $p_i - \theta_i \epsilon_i = p_{i+1} - \theta_i \epsilon_{i+1}$，融合中心可以把更高类型用户的效用设置得更接近 0，也就意味着付出更少的额外代价。也就是说，增加用户类型数量将引入更大的额外代价，当经济预算给定时将增大融合误差。

4.6　本章小结

本章首先推导出隐私保护程度与融合精度之间的定量关系；然后在经济预算一定的情况下，使用契约理论设计了一套有效的契约来最大化融合中心融合精度。本章提出的激励机制为拥有不同隐私偏好的用户提供不同的契约，因此解决融合中心和用户之间信息不对称的问题（融合中心不知道每个用户具体的隐私偏好）。我们推导出了在完全信息和不完全信息下最优契约的解析表达式，并且把契约设计推广到用户隐私偏好连续取值的情形。仿

真结果验证了 REAP 的可行性和有效性。

第五章　基于动态激励的隐私预算优化

本章摘要： 实时数据融合在群智感知中占有很大比重，上一章中提出的静态激励机制不适用于实时数据融合的场景，因为其无法保证用户的长期参与。本章设计了 LEPA 机制来保证实时数据融合应用中的用户长期参与。具体来说，首先推导了所有任务的融合精度要求与用户隐私预算之间的定量关系；然后，设计了一套在线框架来联合优化各个时隙之间的数据可用性，以此来防止用户中途退出群智感知系统。考虑到用户的自私行为以及感知任务的组合特性，本章提出了一种计算高效的在线反向组合拍卖机制，该机制具有近似最优解，真实性以及个体理性等性质。理论分析和仿真实验证明了 LEPA 方法的有效性。

关键词： 群智感知，实时数据融合，长期激励，组合拍卖理论，李雅普诺夫优化

5.1　引言

实时数据融合在群智感知系统中占有很大比重。举例来说，为了持续监控公众健康状况，公共健康机构（也就是融合中心）可以持续从用户可穿戴设备（比如智能手表，智能手环等）中收集用户身体指标数据（比如体温，心跳等）。通过分析收集到的身体指标，融合中心可以监测并绘制疾病传染趋势图。比如，如果发现城市中某个区域的平均体温异常偏高，那么那个区域很大的可能性爆发了某种疾病。

第四章中提出的静态激励方法不适用于实时数据融合的场景，原因如下：用户在参与群智感知任务时，在直接贡献数据之外经常会产生一些非直接的成本，比如群智感知程序在后台运行时消耗的电量和数据流量等。如果用户长期未被选中，非直接成本便得不到充分补偿，因此很可能中途退出系统并最终导致后期参与群智感知任务的用户数量不足。针对实时数据融合应用，需要联合优化不同时隙的数据可用性来保证用户的长期参与。因此，本章提出了一种能够保证用户长期参与的激励机制 LEPA[1]。该机制能处理多用户和多任务的情形，并能够通过联合优化不同时隙来保证用户的长期参与。

设计 LEPA 有两个主要挑战。首先，为了保证用户的长期参与，需要保证每个用户的

[1]LEPA 的命名来源于 Long-tErm Privacy-preserving data Aggregation

选中率不低于某个阈值。而计算选中率不仅仅需要过去和现在的用户选择策略，还需要用到将来的用户选择策略，这使得每一时刻的用户选择都是耦合的，导致长期激励设计变得更具挑战性。其次，在拍卖机制中，用户往往是自私的并有可能误报竞标来获得更大的收益，这种现象将大大增加融合中心的成本。因此，在自私用户存在的情况下，如何让所有用户诚实汇报自己的竞标也是一个挑战。

本章的主要贡献总结如下:

- 第一次系统研究了保证用户长期参与的动态激励机制。
- 通过把长期参与约束转化成队列稳定问题，解决了不同时隙用户选择策略相互耦合的问题。具体来说，为每个用户构建一个具有固定输入率的虚拟队列，输出率与用户被选中率成正比。根据李雅普诺夫优化理论，满足长期参与约束等效于保证所有虚拟队列的稳定性。因此，问题转化成在每个时隙联合优化融合中心成本和队列稳定性的问题。
- 使用反向组合拍卖理论来解决存在自私用户的问题。为解决组合拍卖的 NP-难问题，提出了一个可以计算有效近似解的最优算法，并同时满足了用户的诚实性和个体理性约束。
- 分别从理论分析和仿真的角度验证了所提出激励机制的有效性。

本章剩余部分组织如下。第5.3节介绍了问题建模；问题求解和理论分析分别在第5.4节和第5.5节给出；在第5.6节，使用实验验证了 LEPA 的有效性；最后，第5.7节总结全章。

本章用到的所有符号在表5.1中列出。为方便起见，当某些变量对应于某个时隙 t 时，省略了后缀 (t)。

5.2 系统模型

本部分首先介绍群智感知系统模型和激励机制工作流程，然后介绍反向组合拍卖的定义和设计目标。

5.2.1 群智感知系统模型

本章研究的群智感知系统包含一个融合中心 (Fusion Center，简称 FC) 和 n 个用户 $\mathcal{U} = \{u_1, u_2, \ldots, u_n\}$，如图 5.1所示。其中，融合中心拥有一个包含 k 个感知任务 $\mathcal{T} =$

符号	含义	符号	含义
$\mathcal{U}$	用户集合	q_i	用户 i 的虚拟队列
$\mathcal{T}$	感知任务集合	P_i	融合中心的总成本
n	用户数量	$\mathcal{S}$	中标用户集合
k	感知任务数量	$\mathcal{P}$	中标用户报酬集合
u_i	用户 i	ζ	感知数据取值范围
τ_j	任务 j	b_i	噪音 η_i 分布参数
y_{ij}	指示用户 i 是否能完成任务 j	α_j	融合误差置信区间
y_i	用户 i 的能力向量，长度为 k	δ_j	融合误差置信度
Γ_i	y_i 的集合表示	ϵ_i	用户 i 隐私保护水平
x_i	指示用户 i 是否被选中	r_j	任务 j 融合精度要求
b_i	用户 i 的竞标	D	最小选中概率要求
U_i	用户 i 的效用	γ	李雅普诺夫优化调节参数

表 5.1　第五章符号及含义列表

$\{\tau_1, \tau_2, \ldots, \tau_k\}$ 的任务池。任务池里的任务每隔一段时间发起一次感知申请，申请频率从几分钟到几个小时不等。在时隙 t，每个用户都能完成一组任务 $\mathcal{T}$。用户完成任务的种类取决于其当前位置和移动设备上传感器的种类。令 $y_{ij}(t) \in \{0,1\}$ 表示用户 u_i 是否能完成任务 τ_j，$y_i(t)$ 表示 u_i 在时隙 t 的能力向量 $[y_{i0}, y_{i1}, \cdots, y_{ik}]$。

对于每个任务 τ_j，融合中心需要从用户侧收集足够的感知数据来执行数据融合，本章只考虑应用广泛的平均值融合。比如，在交通监测系统中，可以利用用户的 GPS 信息来估计特定路段的平均车速。融合中心可以从 $\mathcal{U}$ 中选择一部分用户来完成所有感知任务。用 $x_i(t) \in \{0,1\}$ 表示 u_i 在时隙 t 是否被选中，并用向量 $x(t)$ 表示时隙 t 的用户选择策略。

5.2.2　激励机制工作流程

本章的研究目标是设计一种能够处理多任务，多用户，并保证所有用户长期参与的激励机制。因此，可以采用反向组合拍卖理论 (reverse combinatorial auction)。具体来说，工作流程如下：

- 首先，在时隙 t，每个任务发起一个感知请求，并指定融合精度需求 (步骤①)。
- **激励机制：**收到感知任务请求后，融合中心通过执行反向组合拍卖来收购用户隐私。

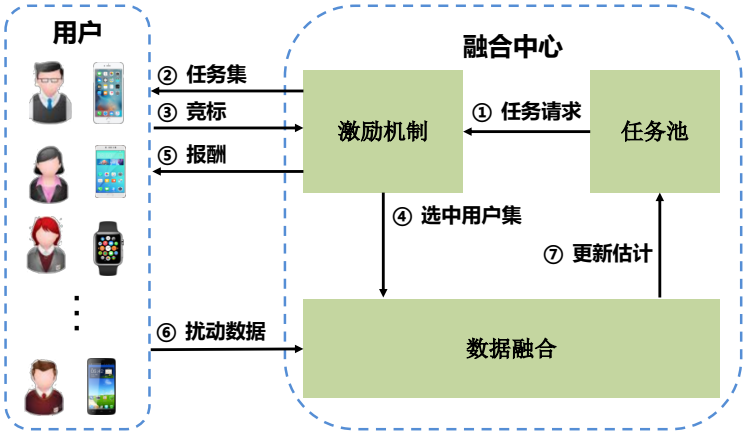


图 5.1　LEPA 方法系统框架，带圈数字表示系统运行步骤

具体来说，融合中心首先给所有用户广播所有的感知请求，并指定一个隐私保护程度（步骤②）。然后每个用户分别向融合中心提交一个竞标 $b_i(t) = \{\Gamma_i(t), b_i^s(t), b_i^p(t)\}$，其中 $\Gamma_i(t)$ 为 $y_i(t)$ 的几何表示[2]，$b_i^s(t)$ 和 $b_i^p(t)$ 分别表示 u_i 在时隙 t 的感知成本和单位隐私成本（步骤③）。最后，融合中心选取一组最优用户 $\mathcal{S} = \{u_1, u_2, \ldots, u_l\}$（步骤④）并提供给他们相应的报酬 $\mathcal{P} = \{p_1, p_2, \ldots, p_l\}$（步骤⑤）。

- **数据融合：**所有被选中的用户对自己的感知数据进行加噪处理，也就是 $\tilde{d}_i = d_i + \eta_i$，并把 $\tilde{d}_i$ 上传到融合中心（步骤⑥）。接下来，融合中心对每个任务得到的数据进行融合处理。

- 最后，使用融合结果对所有感知任务进行更新（步骤⑦）。

5.2.3　反向组合拍卖定义

本章研究的感知任务需要收集实时的感知数据，并且所有用户都是自私的。因此，可以建模成一个长期隐私保护的反向组合（the Long-term Privacy-preserving Reverse Combinatorial, LPRC）拍卖模型。

定义 5.2.1 (LPRC 拍卖模型). 在 LPRC 拍卖模型中，每个用户在时隙 t 都能完成一组任务 $\Gamma_i(t)$，并提交一个包含感知成本 $b_i^s(t)$ 和单位隐私成本 $b_i^p(t)$ 的竞标。$b_i^s(t)$ 和 $b_i^p(t)$ 都是 u_i 的个人信息，融合中心无法得知。

[2]在接下来的叙述中，如果没有歧义，将交叉使用这两种表示方法。

接下来定义用户的效用函数和融合中心的支出成本。

定义 5.2.2 (用户效用函数). 用户效用函数定义为

$$U_i(t) = \begin{cases} p_i(t) - c_i^s(t) - c_i^p(t)\epsilon, & i \in \mathcal{S}, \\ 0, & otherwise, \end{cases}$$

定义 5.2.3 (融合中心支出成本). 在时隙 t，融合中心的支出成本 $P(t)$ 为

$$P(t) = \sum_{i:u_i \in \mathcal{S}} p_i(t)$$

5.2.4　激励机制设计目标

由于所有理性用户都是自私的，而融合中心无法得知他们的感知成本。因此，某些用户可能虚报竞标来获得更高的收益。比如说，某个自私的用户可能报告更高的感知成本来获得更高的收益。因此，LPRC 拍卖必须满足以下的真实性（truthfulness）约束：

定义 5.2.4 (真实性). 一个 LPRC 拍卖满足真实性当且仅当提交真实竞拍 $b_i = (\Gamma_i, c_i^s, c_i^p)$ 能给用户带来最大收益，也就是 $U_i(b_i, b_{-i}) \geq U_i(b_i', b_{-i}), \forall b_i' \neq b_i$.

真实性保证了提交真实的竞拍能给用户带来最大的收益，这就使得用户没有虚报竞标的动机。除了诚实性，LPRC 拍卖还需要满足个体理性（individual rationality）约束，也就是所有用户的效用都是非负的。

定义 5.2.5 (个体理性). 一个 LPRC 拍卖满足个体理性当且仅当 $U_i \geq 0$ 对所有 $u_i \in \mathcal{U}$ 成立。

对于实时数据融合任务，用户需要承担一些非直接成本。因此，如果某个用户在很长一段时间内未被选中，她将很有可能离开整个群智感知系统。为保证用户活跃度，需要保证每个用户被选中的概率不低于某个指定阈值 D。长期参与约束可以正式定义为：

定义 5.2.6 (长期参与). 一个 LPRC 拍卖满足长期参与约束当且仅当 u_i 被选中的概率满足

$$\frac{1}{T}\sum_{t \in T} x_i(t) \geq D, \quad \forall u_i \in \mathcal{U}.$$

在实际应用中，可以通过大量的前期用户问卷调查来确定 D。也可以在群智感知系统的试运行阶段，不断调整 D 来寻找使得离线用户最少的值。后一种方法的好处是系统可以周期性更新 D，因为用户的参与意愿可能是时变的。

5.3 动态激励设计问题建模

本章首先推导出用户隐私预算与融合中心融合精度之间的定量关系，然后介绍了具体的问题建模。

5.3.1 隐私预算与融合精度之间定量关系

本章继续使用第4.2节中的 (α_j, δ_j)-精度定义，并在存在多任务的情况下，推导出以下定量关系：

引理 5.3.1. 在时隙 t，任务 τ_j 具有 (α_j, δ_j)-精度如果

$$\frac{\sum\limits_{i:u_i\in\mathcal{U}} x_i(t)y_{ij}(t)\frac{\zeta}{\epsilon_i^2(t)}}{\left(\sum\limits_{i:u_i\in\mathcal{U}} x_i(t)y_{ij}(t)\right)^2} \leq \frac{\alpha_j^2(t)\delta_j(t)}{2}, \tag{5.1}$$

其中，ζ 表示用户感知数据的取值范围。

证明. 扰动融合数据和原始融合数据之间的误差可以定义为

$$\hat{s}_j - s_j = \frac{1}{|\mathcal{S}|}\sum_{i:u_i\in\mathcal{S}}(d_i+\eta_i) - \frac{1}{|\mathcal{S}|}\sum_{i:u_i\in\mathcal{S}} d_i = \frac{1}{|\mathcal{S}|}\sum_{i:u_i\in\mathcal{S}}\eta_i.$$

其中，$|\mathcal{S}|$ 表示被选中用户集合 $\mathcal{S}$ 的数量，d_i 和 η_i 分别表示原始感知数据以及需要添加的噪音。

由于拉普拉斯随机变量 $\eta_i \sim Lap(0, a_i)$ 的方差是 $2a_i^2$，也就是 $Var(\eta_i) = 2a_i^2$，因此，对于相互独立的拉普拉斯随机变量有

$$Var(\frac{1}{|\mathcal{S}|}\sum_{i:u_i\in\mathcal{S}}\eta_i) = \frac{2}{|\mathcal{S}|^2}\sum_{i:u_i\in\mathcal{S}} a_i^2.$$

根据切比雪夫不等式，可以得到

$$\mathbb{P}[|\hat{s}_j - s_j| \geq \alpha_j] \leq \frac{2}{\alpha_j^2|\mathcal{S}|^2}\sum_{i:u_i\in\mathcal{S}} a_i^2.$$

为达到 (α_j, δ_j)-精度，需要保证

$$\frac{2}{\alpha_j^2|\mathcal{S}|^2}\sum_{i:u_i\in\mathcal{S}} a_i^2 \le \delta_j.$$

因此，在时隙 t，把 $a_i = \frac{\zeta}{\epsilon_i}$ 带入以上公式可以推导出引理 5.3.1。证明完成。 □

在本章中，融合中心向所有用户广播一个相同的 ϵ。为简化分析，可以把公式 (5.1) 转化成

$$\sum_{i:u_i\in\mathcal{U}} x_i(t)y_{ij}(t) \ge \frac{2\zeta}{\epsilon^2\alpha_j^2(t)\delta_j(t)}.$$

令 $r_j(t) = \frac{2\zeta}{\epsilon^2\alpha_j^2(t)\delta_j(t)}$ 表示任务 τ_j 的融合精度需求，并使用向量 $\mathrm{r(t)} = [r_1(t), \cdots, r_k(t)]$ 表示融合精度需求向量。

5.3.2　数学模型

本章的整体目标是设计一个 LPRC 拍卖机制来最小化融合中心的总支出，并满足所有感知任务的融合精度要求。因此，在每个时隙，融合中心需要通过求解 LPRC-LTPM (Long-term Total Payment Minimization，LTPM) 优化问题来选择一组用户并决定付给他们相应的报酬。

LPRC-LTPM **问题**.

$$\min \quad \sum_{t\in T}\sum_{i:u_i\in\mathcal{U}} p_i(t)x_i(t) \tag{5.2}$$

$$s.t. \quad \frac{1}{T}\sum_{t\in T} x_i(t) \ge D, \forall u_i \in \mathcal{U}, \tag{5.3}$$

$$\sum_{i:u_i\in\mathcal{U}} x_i(t)y_{ij}(t) \ge r_j(t), \forall \tau_j \in \mathcal{T}, \tag{5.4}$$

$$x_i(t) \in \{0,1\}, p_i(t) \in [0, +\infty], \tag{5.5}$$

常量：在时隙 t，LPRC-LTPM 优化问题接收用户集合 $\mathcal{U}$ 及其竞标 $\{y_i(t), b_i^s(t), b_i^p(t)\}, \forall u_i \in \mathcal{U}$，任务集合 $\mathcal{T}$ 及其融合精度要求 r(t)，以及最小选中概率 D。

优化变量：LPRC-LTPM 优化问题有一组二元变量 $\mathrm{x(t)} = [x_1(t), x_2(t), \cdots, x_n(t)]$，其中 $x_i(t) = 1$ 表示 u_i 在时隙 t 是否被选中，也就是 $u_i \in \mathcal{S}$。另外有一组非负连续变量 $\mathrm{p(t)} = [p_1(t), p_2(t), \cdots, p_n(t)]$ 分别表示融合中心付给用户的报酬。如果 $u_i \notin \mathcal{S}$，$p_i(t) = 0$。

优化目标：优化目标为最小化融合中心的总支出。

约束： 公式 (5.3)为长期参与约束，约束 (5.4)保证所有任务的融合精度需求都能被满足。此外，LPRC-LTPM 问题需要满足两个隐藏约束——真实性和个体理性。

约束 (5.3)是一个时间平均约束，也就是当前选择策略与未来选择策略是耦合的。然而，未来用户的选择策略对于当前决策来说是未知的，使得解决该问题变得很困难。

5.4 动态激励设计问题求解

为解决第5.3节中遇到的困难，可以把 LPRC-LTPM 转化成一个在线优化问题。本节首先设计了一种在线激励机制，然后讨论了在实际部署中存在的问题。

5.4.1 在线拍卖转换

在线拍卖设计的核心思想是把长期参与约束转换成队列稳定约束，并利用李雅普诺夫优化定理[125–127] 来联合优化队列稳定性和融合中心的总支出。基于这种思想，可以为每个用户构建一个虚拟队列，队列到达率为 D，队列积压代表用户的累积感知请求。如果 u_i 在时隙 t 被选中，也就是 $x_i(t)=1$，那么一个虚拟积压弹出队列。

根据虚拟队列定义，可以得到以下动态方程：

$$q_i(t+1)=[q_i(t)-x_i(t)]^+ + D,$$

其中 $q_i(t)$ 表示用户 u_i 的虚拟队列积压，$[x]^+=\max\{x,0\}$。

接下来使用李雅普诺夫漂移来分析队列稳定性，定义为两个相邻时隙的李雅普诺夫函数之差。其中李雅普诺夫函数定义为所有队列的平方和

$$L(t) \triangleq \frac{1}{2}\sum_{i:u_i\in\mathcal{U}}(q_i(t))^2.$$

因此，李雅普诺夫漂移为

$$\Delta(t) \triangleq L(t+1)-L(t).$$

李雅普诺夫定理指出，如果一个算法在每个时隙都能够最小化 $\Delta(t)$ 便能保证所有队列的稳定性，也因此能够满足长期参与约束。

由于 LPRC-LTPM 问题的优化目标是在满足长期参与约束的前提下最小化融合中心总支出，根据李雅普诺夫优化定理，可以通过最小化以下漂移惩罚来同时满足队列稳定和最优化目标函数。

$$\Delta(t)+\gamma\sum_{i:u_i\in\mathcal{U}}p_i(t)x_i(t),$$

其中 γ 是一个调节系数，用于平衡队列稳定性和目标函数最优性。

观察到 $\Delta(t)$ 是一个在优化问题中很难处理的二次函数，因此我们可以通过最小化一个线性上界来简化问题。

$$\begin{aligned}\Delta(t) =& L(t+1) - L(t) && (5.6)\\ =& \frac{1}{2}\left(\sum_{i:u_i\in\mathcal{U}}([q_i(t) - x_i(t)]^+ + D)^2 - \sum_{i:u_i\in\mathcal{U}} q_i(t)^2\right) && (5.7)\\ \leq& \frac{1}{2}\Bigg(\sum_{i:u_i\in\mathcal{U}}\left(q_i(t)^2 + D^2 + x_i(t)^2 + 2q_i(t)(D - x_i(t))\right) && (5.8)\\ & - \sum_{i:u_i\in\mathcal{U}} q_i(t)^2\Bigg) && (5.9)\\ \leq& \sum_{i:u_i\in\mathcal{U}}\frac{D^2+1}{2} + \sum_{i:u_i\in\mathcal{U}} q_i(t)D - \sum_{i:u_i\in\mathcal{U}} q_i(t)x_i(t), && (5.10)\end{aligned}$$

其中第一个不等式成立是因为 $(\max[q-x,0]+D)^2 \leq q^2 + D^2 + x^2 + 2q(D-x)$，第二个不等式成立是因为 $x_i(t) \in \{0,1\}$。

注意到公式 (5.10)的前两部分是常数，最小化 (5.10)等价于最小化 $\sum_{i:u_i\in\mathcal{U}} -q_i(t)x_i(t))$。因此，LPRC-LTPM 问题可以转化成以下 LPRC-OTPM（On-line Total Payment Minimization）问题：

LPRC-OTPM **问题**.

$$\begin{aligned}\min \quad & \sum_{i:u_i\in\mathcal{U}}[\gamma p_i(t) - q_i(t)]x_i(t)\\ s.t. \quad & \sum_{i:u_i\in\mathcal{U}} x_i(t)y_{ij}(t) \geq r_j(t), \forall\tau_j \in \mathcal{T}\\ & x_i(t) \in \{0,1\}, p_i(t) \in [0,+\infty],\end{aligned}$$

由于 LPRC-OTPM 问题可以在多项式时间内规约成最小权重集合覆盖问题，因此 LPRC-OTPM 问题是一个 NP-难问题。当用户数量和任务数量很大时，无法在有限时间内求解。为解决该问题，下一节将介绍一种有效的近似算法。

5.4.2　在线 LPRC 拍卖设计

本章提出的在线 LPRC 拍卖机制如算法 5.1所示。由于在线 LPRC 拍卖机制只关注某个具体时隙 t 的用户选择策略和报酬决定策略，为简化描述，下文去掉了所有后缀 (t)，比

算法 5.1: 在 LPRC 拍卖设计

Input: ϵ, b, r, γ, $\mathcal{U}$, $\mathcal{T}$;

Output: $\mathcal{S}$, p;

1 Initialization: q $= \{0, \cdots, 0\}$;

2 foreach 时隙 $t = 0, 1, \cdots, T$ do

3 用户选择策略:

4 运行 **算法** 5.2 并输出中标用户集合 $\mathcal{S}$;

5 报酬规则:

6 运行 **算法** 5.3 并输出报酬 p;

7 更新规则:

8 $q_i(t+1) = [q_i(t) - x_i(t)]^+ + D$;

9 end foreach

如 p(t) 简化成 p。LPRC 算法首先调用算法 5.2和算法 5.3来确定选中用户集合 $\mathcal{S}$ 和报酬集合 p。接下来，更新所有用户的虚拟请求队列。用户选择策略和报酬决定策略将在后面小节中详细介绍。

用户选择策略如算法 5.2所示，该算法需要输入隐私保护程度 ϵ，竞标 b（包含每个用户 u_i 的成本 c_i^s, c_i^p 和能力向量 y_i），融合精度要求向量 r，李雅普诺夫优化调节系数 γ，队列向量 q，用户集合 $\mathcal{U}$ 以及任务集合 $\mathcal{T}$。首先，初始化选中用户集合 $\mathcal{S}$（第 1 行）；然后在每个循环，选择具有最小竞标精度比的用户，直到满足所有任务的精度要求，也就是 $\sum_{j:\tau_j \in \mathcal{T}} r_j = 0$，竞标精度比的定义在第 3 行给出，代表用户对优化问题的贡献度；最后，在每次循环结束前，更新所有任务的精度要求向量（第 7 行）。

接下来，可以通过算法 5.3来确定付给选中用户的报酬。因为报酬决定算法需要调用用户选择算法，因此需要用到算法 5.2所有的输入参数，除此之外需要输入算法 5.2输出的选中用户集合 $\mathcal{S}$。首先，初始化报酬向量 p；然后，对于每个选中用户 u_i，在不包含 u_i 的用户集合上运行算法 5.2，将输出的选中用户集合表示为 $\mathcal{S}'$（第 3-4 行）；最后，每个选中用户 $u_i \in \mathcal{S}$ 的报酬确定为使得她能取代 $u_k \in \mathcal{S}'$ 中任意用户的最大竞标 b_{ik}^v（第 5-7 行）。为了保证这一点，需要满足

$$\frac{b_{ik}^v - \frac{q_i}{\gamma}}{\sum_{j:\tau_j \in \Gamma_i} \min\{r'_j, 1\}} = \frac{b_k^s + b_k^p \epsilon - \frac{q_k}{\gamma}}{\sum_{j:\tau_j \in \Gamma_k} \min\{r'_k, 1\}}$$

算法 5.2: 用户选择算法

Input: ϵ, b, r, γ, q, $\mathcal{U}$, $\mathcal{T}$;

Output: $\mathcal{S}$;

Initialization: $\mathcal{S} \leftarrow \varnothing$; $\mathrm{r}' \leftarrow \mathrm{r}$;

while $\sum_{j:\tau_j \in \mathcal{T}} r'_j \neq 0$ do

    // 选择具有最小竞标精度比的用户

    $l = _{i \in \mathcal{U}} \frac{b_i^s + b_i^p \epsilon - \frac{q_i}{\gamma}}{\sum_{j:\tau_j \in \Gamma_i} \min\{r'_j, 1\}}$;

    $\mathcal{S} \leftarrow \mathcal{S} \cup \{u_l\}$;

    $\mathcal{U} \leftarrow \mathcal{U} \setminus \{u_l\}$;

    // 更新 r'_j

    foreach $j : \tau_j \in \Gamma_l$ do

        $r'_j \leftarrow r'_j - \min\{r'_j, 1\}$;

    end foreach

end while

return $\mathcal{S}$;

因此

$$b_{ik}^v = \max_{k:u_k \in \mathcal{S}'} \left\{ \frac{\sum_{j:\tau_j \in \Gamma_i} \min\{r'_j, 1\}}{\sum_{j:\tau_j \in \Gamma_k} \min\{r'_j, 1\}} (b_k^s + b_k^p \epsilon - \frac{q_k}{\gamma}) + \frac{q_i}{\gamma} \right\}$$

5.4.3　讨论

需要指出的是，本章的根本目标不是保证所有群智感知系统注册用户一直在线，因为在某些情况下，某些注册用户根本无法完成任何感知任务。比如说在交通监测应用中，某些注册用户已经到达家里或者工作单位，无法报告任何一条道路的交通信息。本文实际上需要保证的是，一旦注册用户决定参与群智感知系统，并成为在线用户，融合中心需要保证他们不会由于隐私被泄露或很少被选中而主动离线。

在实际部署中，本章提出的框架可以很容易得处理注册用户随机上线和离线的情况。具体来说，一旦某个注册用户进入群智感知系统，融合中心可以为她创建一个虚拟请求队列，而当她离开系统时清空队列。在这种情况下，队列更新方法与算法 5.1相同，用户选择策略和报酬决定策略与算法 5.2和算法 5.3相同。进一步，本章框架可以解决任务池中任务更新频率不一样的情况。每个任务可以根据自身需求向融合中心请求数据更新，比如有些

算法 5.3: 报酬决定算法

Input: ϵ, b, r, γ, q, $\mathcal{U}$, $\mathcal{T}$, $\mathcal{S}$;

Output: p

Initialization: p $\leftarrow (0, \cdots, 0)$;

foreach $i : u_i \in \mathcal{S}$ do

  在 $\mathcal{U} \setminus \{u_i\}$ 上运行算法5.2;

  $\mathcal{S}' \leftarrow$ 第三步选取的用户;

  // 计算报酬

  foreach $k : u_k \in \mathcal{S}'$ do

    $r' \leftarrow r'$，当 u_k 被选取时;

    $p_i \leftarrow \max\{p_i, \frac{\sum_{j:\tau_j \in \Gamma_i} \min\{r'_j, 1\}}{\sum_{j:\tau_j \in \Gamma_k} \min\{r'_j, 1\}}(b^s_k + b^p_k \epsilon - \frac{q_k}{\gamma}) + \frac{q_i}{\gamma}\}$;

  end foreach

end foreach

return p

任务要求一分钟更新一次而另一些任务要求半小时更新一次。在这种情况下，每个时隙里只需要在优化问题里面满足提出数据更新请求的任务的精度要求即可，在线机制设计与算法 5.1相同。

5.5 在线拍卖机制理论分析

本部分提供在线 LPRC 拍卖的理论分析，包括真实性，个体理性，算法复杂度以及渐进界。

证明真实性需要用到以下引理:

引理 5.5.1. 一个拍卖机制满足真实性当且仅当以下两个性质满足[128]:

- **单调性:** 如果用户 u_i 通过竞拍 b_i 和 y_i 赢得了拍卖，那么当其他用户的竞拍不变时，u_i 通过竞拍 $b'_i \leq b_i$ 和 $\Gamma'_i \supset \Gamma_i$ 同样能赢得拍卖。
- **临界报酬:** 被选中用户得到的报酬应该确定为保证该用户赢得拍卖的最高竞拍价 b'_i，也就是说通过竞拍 (Γ_i, b'_i) 该用户刚好能赢得拍卖，竞拍价格继续增加将使得该用户落选。这里的最大拍卖价格被称为临界报酬。

定理 5.5.2 (真实性). 本章提出的在线 LPRC 拍卖机制满足真实性。

证明. 证明在线 LPRC 拍卖机制满足真实性只需要证明它同时满足单调性和临界报酬。

- **单调性：**由于算法每次选择竞拍精度比最大的用户，因此在给定 ϵ 的情况下，用户 u_i 通过竞拍 $\tilde{\Gamma}_i \supset \Gamma_i$ 和 $\tilde{b_i^s} + \tilde{b_i^p}\epsilon \leq b_i^s + b_i^p\epsilon$ 依然能够赢得拍卖。

- **临界报酬：** 根据算法 5.3，被选中用户得到的报酬是最大竞拍价格 b_{ik}^v。

□

需要注意的是，用户 u_i 有可能使用竞拍 $b_i^s \neq c_i^s$ 和 $b_i^p \neq c_i^p$，同时满足 $b_i^s + b_i^p\epsilon = c_i^s + c_i^p\epsilon$。由于这种方法并不会增加用户报酬，因此用户还是会真实提交自己的竞标。

定理 5.5.3 (个体理性). 本章提出的在线 LPRC 拍卖机制满足个体理性。

证明. 根据定义 5.2.2，未被选中的用户效用为 0。对于被选中用户来说，她们提交了真实竞标 (c_i^s, c_i^p) 并得到能让他们刚好中标的最大竞标价格，这就保证了 $p_i \geq c_i^s + c_i^p\epsilon$。因此，$u_i \geq 0, \forall u_i \in \mathcal{U}$。证明结束。 □

定理 5.5.4 (计算时间复杂度). 本章提出的在线 LPRC 拍卖机制的计算时间复杂度为 $\mathcal{O}(n^3 + n^2k)$.

证明. 在最差情况下，算法 5.2需要运行 n 轮。在每一轮，用户选择步骤和精度需求向量更新步骤的复杂度分别为 $\mathcal{O}(n)$ 和 $\mathcal{O}(k)$。因此，算法 5.2的时间复杂度为 $\mathcal{O}(n^2 + nk)$。算法 5.3有 n 轮循环，在每轮循环里面需要运行一次算法 5.2。因此，整个算法的时间复杂度为 $\mathcal{O}(n^3 + n^2k)$。 □

接下来分析在线 LPRC 拍卖机制的近似界。观察到 LPRC-OTPM 问题的目标函数有两类变量：二元变量 x(t) 和连续变量 p(t)，使得问题变得比较复杂。进一步，LPRC-OTPM 问题的最优解并不是非负的，所以无法得到一个乘性近似界。为解决该问题，可以首先构建以下 LPRC-OTCM（On-line Total Cost Minimization）问题：

LPRC-OTCM **问题**.

$$\begin{aligned} \min \quad & \sum_{i:u_i \in \mathcal{U}} [c_i^s + c_i^p \epsilon - \frac{q_i}{\gamma} + m] x_i \\ s.t. \quad & \sum_{i:u_i \in \mathcal{U}} y_{ij} x_i \geq r_j, \forall \tau_j \in \mathcal{T} \\ & x_i \in \{0, 1\}, \end{aligned}$$

其中，$m = \max_{i:u_i \in \mathcal{U}} \frac{q_i}{\gamma}$。

观察到优化问题 LPRC-OTCM 的目标函数仅仅包含二元变量 x(t) 并且是非负的，因此可以推导出乘性近似界。令优化问题 LPRC-OTCM 的最优解为 $M^*, \theta = max_{i,j:u_i \in \mathcal{U}, \tau_j \in \mathcal{T}} y_{ij} |\Gamma_i|$ 和 $d = \frac{1}{\Delta r} \sum_{j \in \mathcal{T}} r_j$，其中 Δr 是 r_j 中元素的单位度量。根据文献[128]，可以得到

$$\sum_{i \in \mathcal{S}} (c_i^s + c_i^p \epsilon - \frac{q_i}{\gamma} + m) \leq 2\theta H_d M^*$$

其中 $H_d = 1 + \frac{1}{2} + \cdots + \frac{1}{d}$。

接下来，可以推导出优化问题 LPRC-OTCM 和 LPRC-OTPM 的最优解 M^* 和 P^* 之间的关系。

引理 5.5.5. *M^* 和 P^* 之间的关系为*

$$M^* \leq P^* + mn.$$

其中 n 是用户总数。

证明. 假设 (x^*, p^*) 是 LPRC-OTPM 问题的最优解，显然有 $P^* = \sum_{i \in \mathcal{U}} (p_i^* - \frac{q_i}{\gamma})$。进一步，因为 LPRC 拍卖机制是满足真实性和个体理性，有 $p^* \geq c_i^s + c_i^p \epsilon$。

由于 LPRC-OTPM 问题和 LPRC-OTCM 问题的约束是相同的，(x^*, p^*) 也是问题 LPRC-OTCM 的可行解。因此

$$\begin{aligned} M^* &\leq \sum_{i \in \mathcal{U}} (c_i^s + c_i^p \epsilon - \frac{q_i}{\gamma} + m) x_i^* \\ &\leq \sum_{i \in \mathcal{U}} (p_i^* - \frac{q_i}{\gamma} + m) x_i^* \\ &= P^* + \sum_{i \in \mathcal{U}} m x_i^* \\ &\leq P^* + mn \end{aligned}$$

证明结束。 □

定义 $\delta = (\max_{i\in\mathcal{U}}(b^s_{k_i} + b^p_{k_i}\epsilon - \frac{q_{k_i}}{\gamma})/(\min_{i\in\mathcal{U}}(b^s_{k_i} + b^p_{k_i}\epsilon - \frac{q_{k_i}}{\gamma} + m))$。LPRC 拍卖机制有以下近似界：

定理 5.5.6 (近似界). 本章提出的 LPRC 拍卖机制的近似界为

$$P \le 2\delta\theta d H_d(P^* + mn)$$

证明. 观察到

$$\sum_{i\in\mathcal{S}}(c^s_i + c^p_i\epsilon - \frac{q_i}{\gamma} + m) \ge |\mathcal{S}| \min_{i\in\mathcal{U}}\{c^s_i + c^p_i\epsilon - \frac{q_i}{\gamma} + m\}$$

从算法 5.3中可以得到，对于每一个用户 u_i，存在一个用户 u_{k_i} 使得

$$p_i = (b^s_{k_i} + b^p_{k_i}\epsilon - \frac{q_{k_i}}{\gamma})\frac{\sum_{j:\tau_j\in\Gamma_i}\min\{r'_j, 1\}}{\sum_{j:\tau_j\in\Gamma_{k_i}}\min\{r'_j, 1\}} + \frac{q_i}{\gamma}$$

因此

$$\begin{aligned}
\sum_{i\in\mathcal{S}} p_i - \frac{q_i}{\gamma} =& (b^s_{k_i} + b^p_{k_i}\epsilon - \frac{q_{k_i}}{\gamma})\frac{\sum_{j:\tau_j\in\Gamma_i}\min\{r'_j, 1\}}{\sum_{j:\tau_j\in\Gamma_{k_i}}\min\{r'_j, 1\}} \\
\le& d|\mathcal{S}| \max_{i\in\mathcal{U}}(b^s_{k_i} + b^p_{k_i}\epsilon - \frac{q_{k_i}}{\gamma}) \\
\le& d\frac{\max_{i\in\mathcal{U}}(b^s_{k_i} + b^p_{k_i}\epsilon - \frac{q_{k_i}}{\gamma})}{\min_{i\in\mathcal{U}}(b^s_{k_i} + b^p_{k_i}\epsilon - \frac{q_{k_i}}{\gamma} + m)}\sum_{i\in\mathcal{S}}(c^s_i + c^p_i\epsilon - \frac{q_i}{\gamma} + m) \\
=& d\delta\sum_{i\in\mathcal{S}}(c^s_i + c^p_i\epsilon - \frac{q_i}{\gamma} + m) \\
\le& 2\theta\delta d H_d M^* \\
\le& 2\theta\delta d H_d(P^* + mn)
\end{aligned}$$

证明结束。 □

5.6 性能评估

5.6.1 实验设置

基准方法。本实验使用两种基准方法。第一种方法为没有长期参与约束的静态拍卖机制，融合中心在每一个时刻仅仅最小化成本而不考虑用户的选中率。在这种静态拍卖机制中，融

合中心同样选择有最高竞拍精度比的用户并支付他们临界报酬。另一种方法是强制 LPRC 拍卖。该方法通过竞拍精度比来选择用户并且保证每个用户在 $\frac{1}{D}$ 个时隙内至少被选中一次（本实验设置 $D = 0.2$），被选中用户收到临界报酬。

表 5.2　实验参数设置

Setting	α_j	δ_j	c_i^s, c_i^p	$\lvert\Gamma_i\rvert$	ϵ	n	k
I	$[1,2]$	$[0.1,0.2]$	$[1,2]$	$[5,10]$	1	100	10
II	$[1,2]$	$[0.1,0.2]$	$[1,2]$	$[5,10]$	1	$[100,200]$	10
III	$[1,2]$	$[0.1,0.2]$	$[1,2]$	$[5,10]$	$[0.5,2]$	100	10

参数设置。 参数设置如表 5.2所示。在设置 I，II，III 中，τ_j 的精度要求 α_j, δ_j 和 u_i 的成本 c_i^s, c_i^p 都在表中给出的范围内均匀取值。$|\Gamma_i|$ 表示用户 u_i 可以完成的任务数量，并且从 $[5,10]$ 中均匀取值。用户 u_i 能完成的任务从任务集合 $\mathcal{T}$ 中随机抽取 $|\Gamma_i|$ 个。在设置 I 中，固定 ϵ，用户数量 n 和任务数量 k，验证在线 LPRC 拍卖机制的优越性。在设置 II 中，固定 ϵ 和 k，验证用户数量对平均报酬的影响。在设置 III 中，固定 n 和 k，展示 ϵ 对平均报酬的影响。

5.6.2　性能比较。

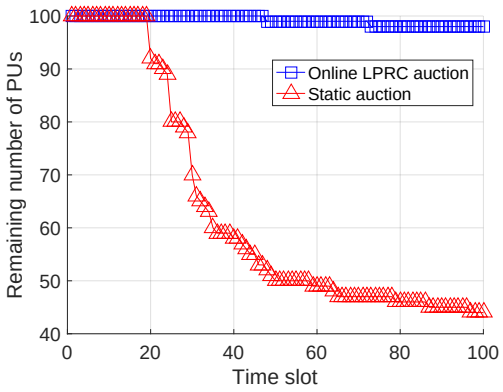


图 5.2　剩余用户数量 Vs. 时隙

图 5.2显示了在设置 I 下每个时隙剩余用户的数量。本实验假设，如果用户连续 20 次未被选中，将会选择离开群智感知系统。由于在这种情况下，强制 LPRC 拍卖机制能保证用户不离开系统，本实验只比较在线 LPRC 拍卖机制与静态拍卖机制。实验显示，随着时间的推移，采用在线 LPRC 拍卖机制后的用户数量基本保持不变。而采用静态拍卖机制时，

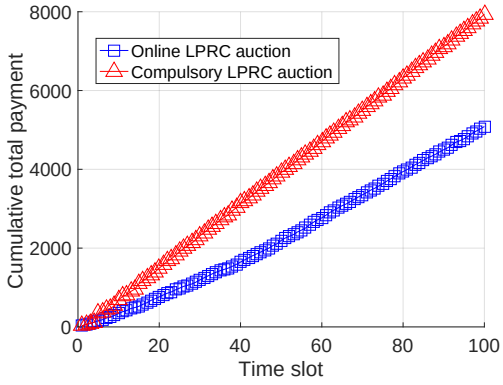


图 5.3　融合中心总成本 Vs. 时隙

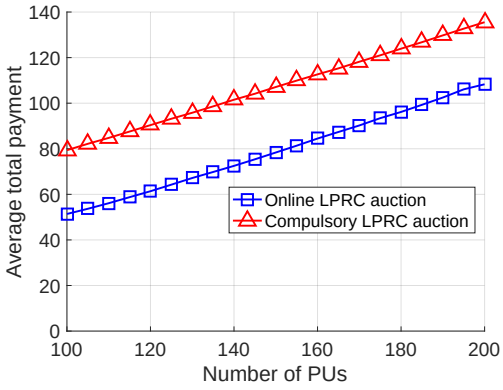


图 5.4　用户数量 Vs. 融合中心平均成本

20 个时隙后用户数量急剧下降。经过 100 个时隙后，损失了大于一半的用户。实验结果表明，本章提出的在线 LPRC 拍卖机制能有效保证用户的长期参与。

图 5.3比较了在设置 I 下在线 LPRC 拍卖机制和强制 LPRC 机制的累积成本。实验显示在线 LPRC 拍卖机制能有效减少融合中心的累积成本。原因是在线 LPRC 拍卖机制联合优化了融合中心的成本和用户的长期参与约束，而强制 LPRC 拍卖机制严格保证了用户的长期参与约束并忽略了融合中心成本的最优性。

图 5.4显示了在设置 II 下用户数量对融合中心平均成本的影响。实验显示当用户数量增加时，平均成本增加。这是因为用户数量越多，越多虚拟请求队列需要稳定，增加了融合中心的平均成本。

图 5.5显示了在设置 III 下 ϵ 对融合中心平均成本的影响。实验显示，当 ϵ 很小时，平均成本随着 ϵ 的增大而减小。原因是 ϵ 越大意味着越高的数据质量，这样一来，融合中心可以招募越少的用户来完成任务，导致平均成本下降。然而，当 ϵ 继续增大，用户的隐私损失急剧增大，需要付给当个用户的成本也随之增加，导致平均成本增加。实验结果显示，

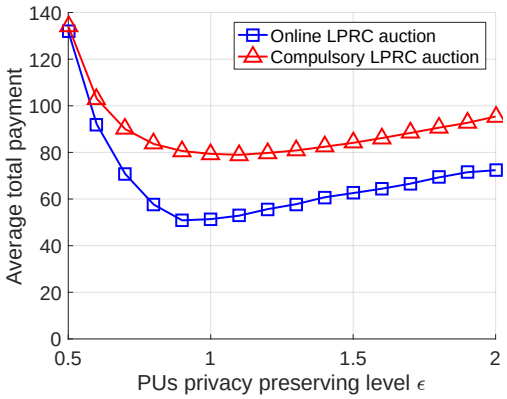


图 5.5　隐私预算 ϵ Vs. 融合中心平均成本

存在一个最优的 ϵ 来最小化融合中心的平均成本。在实际应用中，融合中心可以通过数字实验来确定最优的 ϵ。

5.7　本章小结

本章针对实时数据融合的应用场景，设计了 LEPA 方法来最大化系统效用。首先推导了每个任务的融合精度要求与用户隐私保护程度之间的定量关系；然后设计一个在线算法来联合优化各个时隙之间的系统效用，以此来防止用户中途离开群智感知系统。考虑到用户的自私行为以及感知任务的组合特性，我们提出了一种计算高效的在线拍卖机制，该机制被证明接近最优解，具有真实性以及个体理性等性质。我们通过理论分析和仿真验证证明了 LEPA 方法的有效性。

第六章　基于协同优化的隐私预算优化

本章摘要： 基于协同优化的方法适用于数据拥有者同时也是数据消费者的场景，本章考虑该场景下的一个典型应用——基于数据库的认知无线电中的频谱分配问题。基于数据库的认知无线电技术是解决一级用户和二级用户之间相互干扰的有效技术手段。然而该技术的实现要求一级用户和二级用户直接或间接得提供自身位置信息进行动态频谱分配，这就产生了隐私泄露的风险。本章研究了如何在同时保护一级用户和二级用户位置隐私的前提下，最大化频谱利用率。具体来说，设计了一种隐私保护的效用最大化数据库访问协议 UMax，通过位置隐私保护与频谱利用率之间的协同优化，允许一级用户和二级用户选择最优的隐私预算来最大化系统效用。实验显示 UMax 能有效提升位置数据可用性并提升频谱利用率。

关键词： 认知无线电，频谱分配，数据库访问协议，位置隐私保护

6.1　引言

基于协同优化的隐私预算优化方法适用于数据拥有者同时也是数据消费者的场景，基于数据库的认知无线电中的频谱分配问题是该场景下的一个典型应用。认知无线电是一项能有效提升频谱资源利用率的技术[129–134]。在认知无线电中有两类用户：一级用户（Primary Users，简称 PUs）和二级用户（Secondary Users，简称 SUs）。一级用户在频谱管理机构注册了一个频段，因此拥有对该频段的优先使用权；二级用户只有在频段中某个信道空闲时才允许机会性接入。

认知无线电的应用场景广泛，比如智能电网，公共安全网络和医疗体域网等[135]。以医疗体域网为例，该网络是一项很有前景的技术，可以很高的性价比实现用户重要的体征采集和传输，方便医疗机构进行快速诊断和治疗。医疗体域网对服务质量要求非常高，因此要求传输频谱干扰少。然而，免费的 2.4GHz 频段已被众多无线通信技术共享，变得非常拥堵，因此不适用于性命攸关的医疗领域。而如果能通过认知无线电技术来使用某些注册频段的空闲信道，医疗体域网的服务质量将能得到极大提升[135–138]。

为了动态访问空闲信道，二级用户需要获取当前位置的信道占用情况。目前有两种技术可以实现该目标：频谱感知和数据库查询。其中，频谱感知技术要求二级用户配备专门的频谱检测传感器，来检测当前位置频谱的占用情况[139–142]。然而，由于障碍物遮挡和信道衰减现象的存在，很容易产生干扰和误检。在数据库查询方法中，二级用户只需要查询数据库，便可以轻松得到当前位置的频谱使用情况[143–145]。由于数据库中精确存储了频谱中各个信道在各个空间位置的使用情况，因此能有效防止干扰的产生。

虽然基于数据库查询的认知无线电拥有众多优点，然而二级用户必须暴露自身位置来获取精确的频谱使用情况。如果二级用户是使用医疗体域网的病人，该病人的敏感位置信息将被不可避免得暴露。另一方面，数据库返回的频谱使用信息间接包含了一级用户和二级用户之间的距离信息。因此，恶意二级用户可以通过多次查询来确定一级用户的位置。一级用户和二级用户的位置隐私泄露风险极大阻碍了基于数据库查询的认知无线电的推广。

目前已有相关研究工作单独考虑了一级用户[146] 或二级用户[147] 的位置隐私保护问题，但缺乏对同时保护一级用户和二级用户位置隐私的研究。进一步，已有方法使用了直观的隐私保护措施，没有精确量化隐私保护程度，无法协同优化隐私保护和频谱利用率。因此，直接分别使用已有隐私保护机制来同时保护一级用户和二级用户的位置隐私可能使双方的系统效用都承受巨大损失。作为理性用户，双方用户都想要选取最大的隐私保护程度来保护隐私。然而，隐私保护和系统效用往往是相互矛盾的，提高隐私保护程度将不可避免得影响系统效用。因此，双方用户的位置隐私保护问题需要被协同解决，并通过优化隐私预算来最大化双方系统效用。

为解决以上问题，我们首先设计了一个允许双方用户灵活调整隐私预算的隐私保护框架；然后提出了一种新型的数据库访问协议 UMax 来允许双方用户通过优化隐私预算来最大化系统效用。在 UMax 中，双方用户需要通过交换信息来决定最优的隐私预算。首先，二级用户根据效用函数计算最优隐私预算，并把感兴趣的信道、期望的传输半径以及根据最优隐私预算生成的虚假位置上传给数据库。接下来，数据库根据二级用户提供的信息来决定一级用户的最优隐私预算和二级用户的可用传输功率。

本章主要贡献总结如下：

- 本章首次提出了一个可量化框架来同时保护一级用户和二级用户的位置隐私，并解决了通过同时优化一级用户和二级用户隐私预算来最大化双方系统效用的问题。

- 提出了新型数据库访问协议 UMax ，允许双方用户调整隐私预算来最大化系统效用，并证明了双方用户所选择隐私预算的最优性。

- 把 UMax 协议扩展到具有复杂相对位置组合和分配策略的多一级用户多二级用户场景。

本章剩余部分组织如下。第 6.2节介绍了基本的数据库访问协议以及攻击模型；在第 6.3节中提出了同时保护双方用户隐私的可量化框架；第 6.4节研究了单一级用户单二级用户情形下的数据库访问协议，该协议在第 6.5节扩展到多一级用户多二级用户的场景；第 6.6节通过实验证明了 UMax 的有效性；最后，第 6.7节总结了全章。

表 6.1总结了本章用到的符号。

符号	含义
$r_{p,i}^0$	一级用户 PU_i 的保护域半径
$r_{p,i}^\epsilon$	加入一级用户 PU_i 保护域半径的随机长度
$L_{p,i}$	一级用户 PU_i 的隐私保护程度，也就是 $E(r_{p,i}^\epsilon)$
$T_{p,i}$	一级用户 PU_i 收益
$C_{p,i}^{pri}$	一级用户 PU_i 的隐私代价
loc_j	二级用户 SU_j 的精确位置
loc_j'	二级用户 SU_j 的虚假位置
$r_{s,j}^0$	二级用户 SU_j 的期望传输半径
R_j	二级用户 SU_j 的最大传输半径
P_j	二级用户 SU_j 的最大传输能量
$r_{s,j}^\epsilon$	二级用户 SU_j 隐私保护圈半径
$L_{s,j}$	二级用户 SU_j 的隐私保护程度，也就是 $r_{s,j}^\epsilon$
$T_{s,j}$	二级用户 SU_j 的收益
$C_{s,j}^{pri}$	二级用户 SU_i 的隐私代价
$C_{s,j}^{buy}$	二级用户 SU_i 购买频谱的成本

表 6.1　第六章符号及含义列表

6.2　背景与攻击模型介绍

本节首先介绍在不考虑隐私保护情形下的数据库访问协议，然后介绍攻击模型与假设。

6.2.1 基本数据库访问协议

数据库驱动认知无线电网络包含三个实体：一级用户（Primary Users，简称 PUs），二级用户（Secondary Users，简称 SUs）和频谱管理数据库。数据库存储着一级用户的位置信息以及频谱的使用情况。当一级用户的频谱使用情况发生变化时，它们会及时通知数据库更新数据。

假设认知无线电网络中有 m 个一级用户和 n 个二级用户，分别表示为 PU_i 和 SU_j。每个 PU_i 都拥有一个信道 ch_i[1]，每个信道有两种状态——空闲和占用。当 ch_i 空闲时，二级用户可以在任何地方任意使用该信道；当 ch_i 被占用时，PU_i 将划定一个保护区域并禁止任何二级用户在该区域内使用信道，只有当二级用户在保护区域以外时信道才能被使用，并且二级用户距离一级用户越远能使用的传输功率越大。

图 6.1展示了一个基本的不考虑隐私保护的数据库访问协议。假设数据库访问发生在每个时隙的开始时刻，并且在每个时隙内信道使用状态不变。在每个时隙开始时刻，二级用户发起查询 $Q=(loc_j, ch_i)$，其中 $loc_j=(x_j, y_j)$ 是 SU_j 的准确位置，ch_i 是对 SU_j 来说质量最好的信道。接下来，数据库返回 $R=P_j$ 和 SU_j，其中 P_j 是 SU_j 在使用 ch_i 时可以使用的最大传输功率（Maximum Transmission Power，简称 MTP）。MTP 可以使用以下函数进行计算[146]：

$$P_j=\begin{cases}0, & d_{ij}\le r_{p,i}^0,\\ h(d_{ij}-r_{p,i}^0), & d_{ij}>r_{p,i}^0,\end{cases} \tag{6.1}$$

其中 $r_{p,i}^0$ 是 ch_i 保护区域的半径，d_{ij} 是 SU_j 和 PU_i 之间的距离，$h(\cdot)$ 是一个连续单调递增函数。

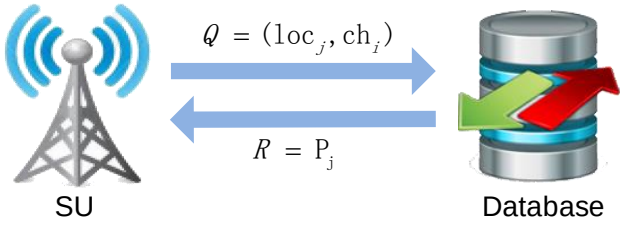


图 6.1 基本数据库访问协议

[1]在不引起歧义的情况下，下文将交叉使用 PU_i 和 ch_i。

6.2.2　攻击模型与假设

在基本数据库访问协议中，数据库和二级用户都是可信的。而在实际部署中，该假设往往得不到保证。原因是某些好奇的数据库管理人员可能通过收集二级用户的位置信息进行商业运作，比如进行精确的广告投送等。另一方面，某些恶意的二级用户也可以通过对数据库的多次查询来确定一级用户的位置。

假设数据库是一级用户的附属设施，比如说中国移动可以维护一个频谱管理数据库来共享频谱。因此可以假设一级用户和数据库之间是相互信任的，数据库不会有意泄露一级用户的任何敏感信息。与文献[146]相同，本章还假设恶意的二级用户可以获得数据库使用的 MTP 函数。

6.3　可量化隐私保护机制

本部分首先介绍一级用户和二级用户的定量隐私保护机制，然后介绍一个防干扰框架来简化后续分析。

6.3.1　二级用户隐私保护机制

为保护二级用户的位置隐私，本章借用了文献[93]中的 ϵ-geo-indistinguishability（ϵ-geoin)）隐私定义，ϵ-geoin 可以认为是本地差分隐私在二维位置数据上的应用。为适应数据库驱动认知无线电中动态频谱分配的需求，本章使用了 ϵ-geoin 隐私定义的另一种表现形式，我们称之为 l-geo-indistinguishability（简称 l-geoin）机制。直观上来看，l-geoin 允许二级用户以真实位置为圆心，以二维拉普拉斯分布采样一个随机位置。l-geoin 保证当攻击者得到二级用户的随机扰动位置后，无法准确推断出二级用户的准确位置。l-geoin 的正式定义如下：

定义 6.3.1. 一个隐私保护的机制满足 l-geoin 当且仅当对于扰动位置，有

$$\frac{P(x|x_0)}{P(x|x_0')} \leq e^l, \forall r_s^\epsilon > 0, d(x_0, x_0') \leq r_s^\epsilon,$$

$$l = \epsilon r_s^\epsilon,$$

其中 r_s^ϵ 表示二级用户随机扰动位置的最大偏移半径。x_0 和 x_0' 分别表示二级用户可能的真实位置，$d(x_0, x_0')$ 表示 x_0 和 x_0' 之间的距离。

定义 6.3.1显示，无论二级用户的真实位置是 x_0 还是 x_0'，随机扰动位置都能以一定概率落在 x 上。并且如果 x_0 和 x_0' 的距离小于 r_s^ϵ，由它们所产生的随机扰动位置落在 x 上的概率的比值上界为 e^l。注意到 l 越大，攻击者越难推断二级用户的位置，因此代表着更大的隐私保护程度。文献[93] 指出，对于给定的 r_s^ϵ，ϵ 越大意味着越大的隐私保护程度。切换到 l-geoin 的视角，当 l 给定时，可以通过调整 ϵ 来获得更大的 r_s^ϵ，每一个 r_s^ϵ 都对应着一个 ϵ。因此，可以使用 r_s^ϵ 来表示二级用户的隐私保护程度 L_s[2]，其中更大的 r_s^ϵ 表示二级用户可以在更大程度上对其位置进行随机扰动处理。在 l-geoin 机制的定义下，二级用户可以灵活选择保护域，而非像 ϵ-geoin 机制一样在固定的保护域调整隐私保护程度。

Andres 等[93] 证明，二维拉普拉斯噪音满足 ϵ-geoin，因此也满足 l-geoin。二维拉普拉斯噪音的概率密度函数为

$$f(x|x_0) = \frac{\epsilon^2}{2\pi} e^{-\epsilon d(x_0,x)}, \tag{6.2}$$

其中 $x_0 \in \mathbb{R}^2$ 和 $x \in \mathbb{R}^2$ 分别表示二级用户的精确位置和扰动位置，$d(x_0,x)$ 表示 x_0 和 x 之间的距离。图 6.2展示了该机制的工作原理，位于 x_0 的二级用户可以在半径为 r_s^ϵ 的圆内通过二维拉普拉斯分布随机产生一个位置 x。

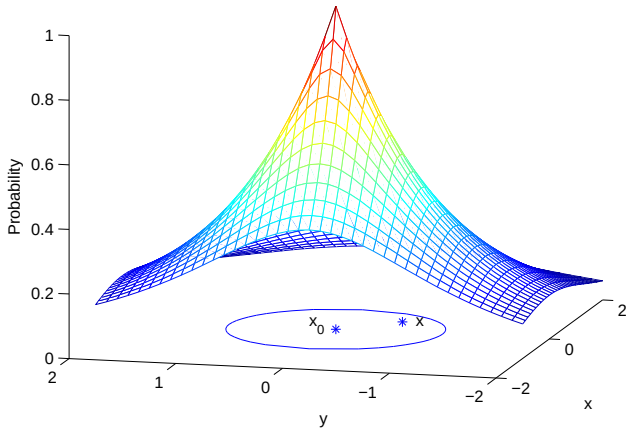


图 6.2　真实位置在 x_0 的二级用户以纵坐标所示概率产生虚假位置 x

6.3.2　一级用户隐私保护机制

一级用户的隐私威胁没有二级用户那么直观，因此需要首先简单介绍该威胁的来源。简单来说，恶意二级用户可以通过多次查询的方式来对某个一级用户进行定位，如图 6.3a所

[2]如果没有歧义，下文将交叉使用 r_s^ϵ 和 L_s 来表示二级用户的隐私保护程度。

示。具体来说，由于某些高级的二级用户可以得到数据库采用的 MTP，因此可以通过数据库返回的最大传输功率计算出自身与一级用户的距离，也就是图中的 d_1，d_2，d_3 和 d_4 分别加上一级用户的保护区域半径 r_p^0。因此，通过多次查询，二级用户可以通过求解以下方程组来确定一级用户的位置：

$$\begin{aligned}(x_1-x_p)^2+(y_1-y_p)^2&=(d_1+r_p^0)^2\\(x_2-x_p)^2+(y_2-y_p)^2&=(d_2+r_p^0)^2\\(x_3-x_p)^2+(y_3-y_p)^2&=(d_3+r_p^0)^2\\(x_4-x_p)^2+(y_4-y_p)^2&=(d_4+r_p^0)^2\end{aligned}\tag{6.3}$$

其中 (x_i,y_i) 为查询 Q_i 的位置，(x_p,y_p) 表示待推断一级用户的位置。通过求解以上方程组，二级用户便能成功解出一级用户的精确位置 (x_p,y_p) 及其保护区域半径 r_p^0。

为保护一级用户位置隐私，本章提出图 6.3b所示的隐私保护方法。在计算二级用户最大传输功率之前，可以在一级用户真实保护区域半径上加入噪音，即 $r_p=r_p^0+r_p^\epsilon$。噪音的引入是的攻击者无法准确求解出方程组中的 r_p^0，使得推断 (x_p,y_p) 变得更加困难。注意到 r_p^ϵ 必须是正数以保证扰动的保护区域大于实际保护区域，否则计算出的二级用户最大传输功率会造成对一级用户的干扰。因此，本章不能使用拉普拉斯分布进行扰动，造成不能使用严格的差分隐私来保护一级用户位置隐私。为了有效保护一级用户位置隐私，本章采用指数分布对 r_p^ϵ 进行加噪，并采用一种更加直观的方法来衡量隐私保护程度。观察到噪音越大方程组求解越难，因此可以采用 r_p^ϵ 的期望，也就是 $E[r_p^\epsilon]$ 来衡量一级用户的隐私保护程度 L_p[3]。

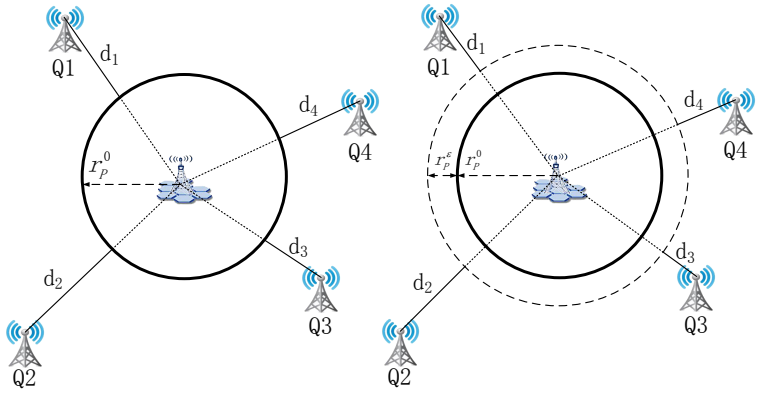
6.3.3　防干扰框架

本小节介绍一个动态频谱分配时的防干扰框架来简化分析，如图 6.4所示。

假设每个二级用户根据自身服务需求，拥有一个期望的传输半径 r_s^0。数据库可以根据二级用户的扰动位置 x 和期望传输半径 r_s^0 来决定其最大传输功率。在查询开始时刻，二级用户给数据库上传一个扰动位置 x，根据 l-geoin 机制的定义，二级用户的真实位置可能在以 x 为圆心 r_s^ϵ 为半径的圆内任意位置，如图 6.4中内圈实线所示。从数据库的角度来看，为二级用户分配频谱时最保险的做法是假设二级用户的真实位置就处于实现内圈的边缘上，也就是图中的 x_0^1 和 x_0^2，否则有一定概率造成干扰。

简单起见，下文分别使用**隐私保护圈**和**防干扰圈**来表示图 6.4中的实线内圈和实线外圈。需要注意的是，当两个二级用户的隐私保护圈相交时，它们的真实位置可能任意接近。

[3]如果没有歧义，下文将交叉使用 $E[r_p^\epsilon]$ 和 L_p 来表示一级用户的隐私保护程度。



(a) 针对一级用户的推断攻击　　(b) 针对一级用户的隐私保护方法

图 6.3　一级用户的位置隐私威胁和保护方法。Q_1，Q_2，Q_3 和 Q_4 分别表示四个不同的查询位置，d_1，d_2，d_3 和 d_4 分别表示在四个位置的最大传输半径

也就是说无论分配给他们的传输距离是多少都无法完全避免干扰，在这种情况下只允许其中一个二级用户访问信道。

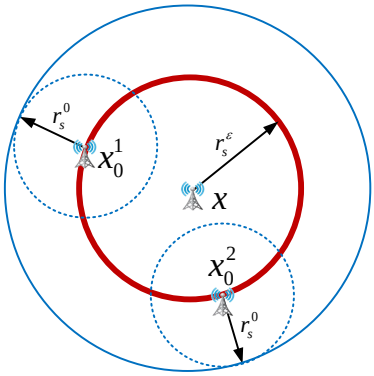


图 6.4　防干扰框架。x 表示二级用户上传的虚假位置，x_0^1 和 x_0^2 分别表示两个可能的真实位置

6.4　隐私保护的数据库访问协议

本节提出一种新型数据库访问协议 UMax，使得一级用户和二级用户都可以选择最优的隐私保护程度来最大化自身效用，从而最优化数据可用性和频谱利用率。本节首先考虑单一级用户单二级用户的情况，并在下节推广到多一级用户多二级用户的情形。

6.4.1　协议概述

UMax 协议工作流程主要分成两步。

第一步：二级用户求解最优隐私保护程度并查询数据库：二级用户向数据库发起查询 $Q = (ch_i, r_s^0, loc', r_s^\epsilon)$，其中 ch_i 表示该二级用户感兴趣的信道，r_s^0 为二级用户期望的传输半径，$loc' = (x', y')$ 是通过隐私保护程度 r_s^ϵ 生成的虚拟位置。最优隐私保护程度可以通过求解以下优化问题得到：

问题 6.4.1.

$$\begin{aligned} &\underset{L_s}{\operatorname{argmax}}\ U_s(L_s) = T_s - C_s^{buy} - C_s^{pri}, \\ &s.t.\ L_s > 0. \end{aligned}$$

在问题 6.4.1中，$U_s(L_s)$ 表示二级用户的效用函数，包含三部分：T_s 是二级用户使用频谱带来的收益，C_s^{buy} 是二级用户使用频谱时支付给一级用户的费用，C_s^{pri} 是二级用户的隐私损失。该优化问题的具体细节将在 6.4.2中介绍。

第二步：数据库根据信道状态决定二级用户的最大传输功率：当二级用户感兴趣的信道空闲时，数据库根据 r_s^0 计算最大传输功率；当信道被占用时，数据库首先计算一级用户的最优隐私保护程度，然后计算最大传输功率。一级用户的最优隐私保护程度可以通过求解以下优化问题得到：

问题 6.4.2.

$$\begin{aligned} &\underset{L_p}{\operatorname{argmax}}\ E[U_p(L_p)] = T_p - C_p^{pri}, \\ &s.t.\ L_p > 0. \end{aligned}$$

问题 6.4.2中的 $E[U_p(L_p)]$ 表示一级用户在期望意义下的效用函数，包含两部分：T_p 表示一级用户出售频谱得到的收益，该收益等于二级用户的支出成本 C_s^{buy}，C_p^{pri} 表示一级用户的隐私损失。一级用户的最优决策过程细节将在 6.4.3中讨论。

接下来，数据库可以根据最优隐私保护程度 $E[r_p^\epsilon]$ 采样生成一个随机距离 r_p^ϵ。二级用户的最大传输半径[4]为 $R = d_{sp} - r_p^0 - r_p^\epsilon - r_s^\epsilon$，如图 6.5所示，其中 d_sp 表示一级用户和二级

[4]二级用户的最大传输功率是由其最大传输半径决定的，因此如果没有歧义，下文将交叉使用最大传输功率和最大传输半径。

用户之间的距离。

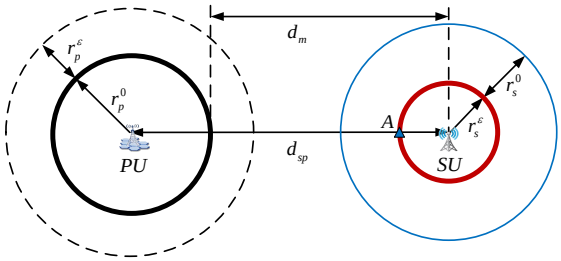


图 6.5　一级用户和二级用户相对位置

6.4.2　二级用户最优决策

定义二级用户使用频谱的收益为

$$T_s = k_2\pi(r_s^0)^2, \tag{6.4}$$

其中 k_2 表示二级用户使用单位面积频谱的收益，r_s^0 表示二级用户的期望传输半径。

如图 6.4所示，二级用户的期望传输半径为 r_s^0。直观上来看，一级用户应该根据二级用户的实际传输半径 r_s^0 来收费。实际上，为了保证二级用户的位置隐私，一级用户分配了半径为 $r_s^0 + r_s^{\epsilon}$ 的区域来避免干扰，这多出来的一部分区域也应该由二级用户来买单。因此，二级用户的支出成本为：

$$C_s^{buy} = k_1\pi(r_s^{\epsilon} + r_s^0)^2,$$

其中 k_1 表示使用单位面积频谱的成本，$\pi(r_s^{\epsilon} + r_s^0)^2$ 表示分配给二级用户的频谱面积。由于二级用户的隐私保护程度 L_s 等于 r_s^{ϵ}，上面的公式可以简写成

$$C_s^{buy} = k_1\pi(L_s + r_s^0)^2. \tag{6.5}$$

隐私损失的定义参考了文献[49]：

$$C_s^{pri} = \frac{k_s}{L_s}, \tag{6.6}$$

其中 k_s 表示隐私损失系数。

结合公式 (6.4)，(6.5)和 (6.6)，问题 6.4.1可以写成

问题 6.4.3.

$$\begin{aligned}\underset{L_s}{\operatorname{argmax}}\ & E[U_s] = k_2\pi(r_s^0)^2 - k_1\pi(L_s + r_s^0)^2 - \frac{k_s}{L_s},\\ & s.t.\ L_s > 0.\end{aligned}$$

接下来证明问题 6.4.3存在最优解并提供一种有效的解法。

定理 6.4.4. 对于问题 6.4.3，二级用户存在最优的隐私保护程度，即 L_s^*。

证明. $E[U_s]$ 的二阶导数为

$$\frac{d^2E[U_s]}{dL_s^2} = -2k_1\pi - 2\frac{k_s}{L_s^3},$$

注意到 $\frac{d^2E[U_s]}{dL_s^2}$ 恒小于 0，意味着 $E[U_s]$ 是一个凹函数。另外问题 6.4.3的约束都是凸的，因此问题 6.4.3是一个凸优化问题并存在最优解。证明结束。 □

由于问题 6.4.3是凸优化问题，因此可以通过现成的凸优化求解器进行求解，比如梯度下降法[148] 等。

6.4.3　一级用户最优决策

为避免干扰，二级用户的期望传输半径 r_s^0 极有可能无法被完全满足。为激励二级用户持续使用空闲信道，一级用户可以通过降低单位频谱价格来补偿二级用户。因此，一级用户的收益为

$$\begin{aligned}T_p &= \frac{R}{r_s^0}k_1\pi(r_s^\epsilon + R)^2\\ &= \frac{k_1\pi}{r_s^0}(d_m - L_p - r_s^\epsilon)(d_m - L_p)^2,\end{aligned} \tag{6.7}$$

其中 R 表示二级用户的最大传输半径，$\frac{R}{r_s^0}$ 表示二级用户的满足率。

一级用户的隐私损失定义为

$$C_p^{pri} = \frac{k_p}{L_p} \tag{6.8}$$

结合公式 (6.7)和 (6.8)，一级用户的期望收益可以写成

$$E[U_p] = \frac{k_1\pi}{r_s^0}(d_m - L_p - r_s^\epsilon)(d_m - L_p)^2 - \frac{k_p}{L_p}$$

如图 6.5所示，L_p 的最优值落在区间 $[d_m-r_s^\epsilon-r_s^0, d_m-r_s^\epsilon]$。原因是如果 $L_p \le d_m-r_s^\epsilon-r_s^0$，二级用户的期望传输半径将被完全满足，在这种情况下，收益 $T_p = k_1\pi(r_s^\epsilon+r_s^0)^2$ 是一个常数，L_p 可以继续增大来提升效用。另一方面，如果 $L_p \ge d_m - r_s^\epsilon$，任意传输半径都会引起干扰，如图 6.5中 A 点所示。因此，问题 6.4.2变成了

问题 6.4.5.

$$\begin{aligned}\underset{L_p}{\text{argmax}}\ & E[U_p] = \frac{k_1\pi}{r_s^0}(d_m - L_p - r_s^\epsilon)(d_m - L_p)^2 - \frac{k_p}{L_p},\\ s.t.\ & L_p > 0,\\ & d_m - r_s^\epsilon - r_s^0 \le L_p \le d_m - r_s^\epsilon.\end{aligned}$$

接下来证明问题 6.4.5存在最优解并提供有效解法。

定理 6.4.6. 对于问题 6.4.5，一级用户存在最优隐私保护程度，即 L_p^*。

证明. $E[U_p]$ 的一阶导数为

$$\frac{dE[U_p]}{dL_p} = \frac{k_1\pi}{r_s^0}\Big[-3L_p^2 + (6d_m - 2r_s^\epsilon)L_p - 3d_m^2 + 2r_s^\epsilon d_m\Big] + \frac{k_p}{L_p^2}.$$

注意到方程 $\frac{dE[U_p]}{dL_p} = 0$ 的解为目标函数 $E[U_p]$ 的驻点，而 $\frac{dE[U_p]}{dL_p} = 0$ 是四次函数因此有 4 个驻点。进一步，由于 $E[U_p]$ 是连续函数，问题 6.4.5的可行域为 $L_p \in [d_m-r_s^\epsilon-r_s^0, d_m-r_s^\epsilon]$，因此问题 6.4.5在区间 $[d_m - r_s^\epsilon - r_s^0, d_m - r_s^\epsilon]$ 内存在最优解。证明结束。 □

为计算一级用户最优隐私保护程度，首先利用四次方程求解器[149] 计算 $\frac{dE[U_p]}{dL_p} = 0$ 的实根，并分别计算 $E[U_p]$ 在所有实根和边界上的取值。这些取值中最大的值对应的 L_p 就是最优隐私保护程度。如果存在两个不同值所对应的 $E[U_p]$ 值相等，取最大的 L_p。

6.5 多用户数据库访问协议

本节把基本的 UMax 协议扩展到多一级用户多二级用户的情形。由于不同一级用户拥有不同信道，分配策略完全解耦，因此问题便简化成了单一级用户多二级用户的情形。需要注意的是，当申请同一个信道的二级用户的数量无限多时，他们之间相对位置的组合是无穷的，导致问题很难处理。因此，本节只讨论最多有两个二级用户申请同一个信道的情况。

具体来说，UMax 在多一级用户多二级用户情形下的数据库访问协议如下：

第一步：所有二级用户通过求解问题 6.4.3得到各自的最优隐私保护程度，并向数据库发送查询 $Q=(ch_i, loc'_j, r^0_{s,j}, r^\epsilon_{s,j})$，其中 ch_i 表示二级用户 SU_j 感兴趣的信道，loc'_j 为二级用户使用最优隐私保护程度 $r^\epsilon_{s,j}$ 生成的虚假位置，$r^0_{s,j}$ 为二级用户 SU_j 的期望传输半径。

第二步：数据库根据信道 ch_i 的状态确定频谱分配策略。当 ch_i 空闲时，数据库只需要在保证二级用户之间不相互干扰的前提下决定它们的传输半径。当 ch_i 被占用时，数据库需要首先计算一级用户 PU_i 的最优隐私保护程度，并保证一级用户和所有二级用户之间都不发生干扰。

接下来分情况讨论不同信道状态下的频谱分配策略。

6.5.1　信道空闲情形

定义一级用户 PU_i 的收益为 $T_{p,i}=T^1_{p,i}+T^2_{p,i}$，并且

$$T^1_{p,i}=\frac{R_1}{r^0_{s,1}}k_1\pi(r^\epsilon_{s,1}+R_1)^2,$$
$$T^2_{p,i}=\frac{R_2}{r^0_{s,2}}k_1\pi(r^\epsilon_{s,2}+R_2)^2,$$

其中 $T^1_{p,i}$ 和 $T^2_{p,i}$ 分别表示来自二级用户 SU_1 和 SU_2 的收入。$R_j(j=1,2)$ 表示 SU_j 的最大传输半径，$r^\epsilon_{s,j}$ 表示 SU_j 的最优隐私保护程度，$r^0_{s,j}$ 表示 SU_j 的期望传输半径。

当有两个二级用户同时申请信道 ch_i 时，有以下三种情形：

情形 1：防干扰圈不相交，如图 6.6所示。在这种情形下，SU_1 和 SU_2 都能以期望传输半径使用信道。

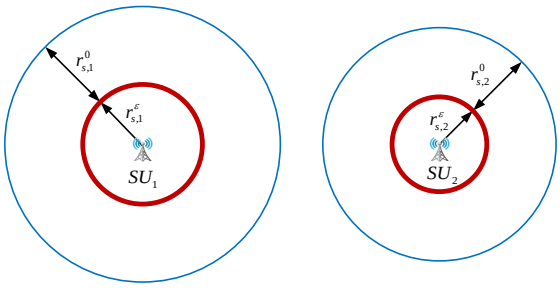


图 6.6　防干扰圈不相交

情形 2：防干扰圈相交，如图 6.7所示。在这种情形下，需要最大化一级用户 PU_i 的收益

$$T_{p,i}=\frac{R_1}{r^0_{s,1}}k_1\pi(r^\epsilon_{s,1}+R_1)^2+\frac{R_2}{r^0_{s,2}}k_1\pi(r^\epsilon_{s,2}+R_2)^2. \tag{6.9}$$

直观上来看，只有当 SU_1 和 SU_2 的防干扰圈相切时 PU_i 的收益才能最大化。原因是如果有某种分配策略使得两个防干扰圈不相交，一定可以通过增大其中一个二级用户的防干扰圈来找到一个更好的分配策略。因此有

$$R_2 = d_{12} - r_{s,1}^{\epsilon} - r_{s,2}^{\epsilon} - R_1,$$

定义 $M = d_{12} - r_{s,1}^{\epsilon} - r_{s,2}^{\epsilon}$，其中 M 是常量。因此，最优分配策略可以通过求解以下优化问题得到：

问题 6.5.1.

$$\begin{aligned} \underset{R_1}{\text{argmax}}\ T_{p,i} =& \frac{R_1}{r_{s,1}^0} k_1 \pi (r_{s,1}^{\epsilon} + R_1)^2 + \frac{M - R_1}{r_{s,2}^0} k_1 \pi (r_{s,2}^{\epsilon} + M - R_1)^2, \\ s.t. \qquad & 0 \le R_1 \le r_{s,1}^0, \\ & M - r_{s,2}^0 \le R_1 \le M, \end{aligned}$$

接下来证明问题 6.5.1存在最优解，并提供有效的求解方法。

定理 6.5.2. 对于问题 6.5.1，二级用户的隐私保护程度存在最优解，即 L_s^*。

证明. R_p 的二阶导数为

$$\frac{d^2 T_{p,i}}{dT_{p,i}^2} = \frac{4k_1\pi}{r_{s,1}^0}(r_{s,1}^{\epsilon} + R_1) + \frac{2k_1\pi}{r_{s,2}^0}(M - R_1).$$

由于 $\frac{d^2 T_{p,i}}{dT_{p,i}^2}$ 恒大于 0，因此 $T_{p,i}$ 是一个凸函数。另外，问题 6.5.1的所有约束都是凸的，因此问题 6.5.1是凸优化问题，存在最优解。证明结束。 □

因为问题 6.5.1是凸优化问题，因此可以使用现成的凸优化求解器进行求解。

情形 3： 隐私保护圈相交，如图 6.8所示。在这种情形下，根据第 6.3.3小节中的讨论，至多有一个二级用户可以访问信道 ch_i。最优分配策略为选择带来最大收益的二级用户。排除掉其中一个二级用户后，剩下的二级用户可以使用期望传输半径访问信道。此时，一级用户 PU_i 的最大收益是 $T_{p,i}^* = max\{T_{p,i}^1, T_{p,2}^2\}$。

6.5.2 信道占用情形

当信道被占用时，数据库需要确定 PU_i 的最优隐私保护程度和每个二级用户的最大传输半径。与 6.5.1相同，这里只考虑两个二级用户的情形。

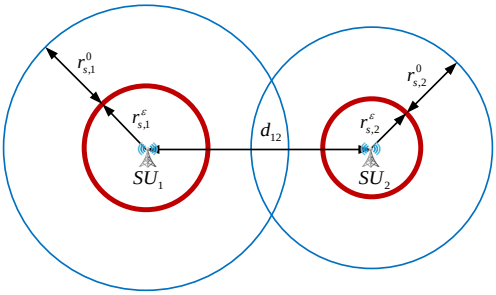


图 6.7　防干扰圈相交

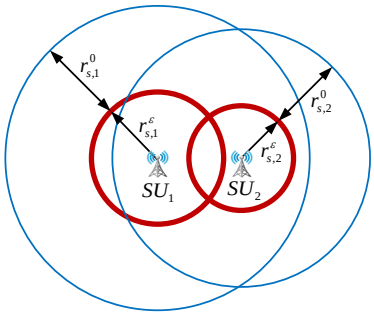


图 6.8　隐私保护圈相交

情形 1：防干扰圈不相交，如图 6.9所示。

为简化分析，考虑一个特殊情形：一级用户 PU_i 和两个二级用户都处于同一条直线上，如图 6.9所示。其他相对位置都可以转化成该情形，因为数据库的分配策略仅取决于一级用户和两个二级用户的相对距离，而非相对位置。

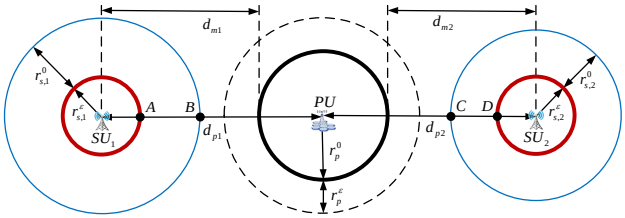


图 6.9　防干扰圈不相交

当 PU_i 的防干扰圈与 SU_j 的防干扰圈相切时，

$$\begin{aligned} T_{p,i}^1 &= \frac{R_1}{r_{s,1}^0} k_1 \pi (r_{s,1}^\epsilon + R_1)^2 \\ &= \frac{k_1 \pi}{r_{s,1}^0} (d_{m1} - r_{s,1}^\epsilon - L_p)(d_{m1} - L_p)^2, \\ T_{p,i}^2 &= \frac{R_2}{r_{s,2}^0} k_1 \pi (r_{s,2}^\epsilon + R_2)^2, \\ &= \frac{k_1 \pi}{r_{s,2}^0} (d_{m2} - r_{s,2}^\epsilon - L_p)(d_{m2} - L_p)^2. \end{aligned}$$

在这种情况下，PU_i 的效用函数是分段的。原因是当 L_p 从 0 开始变大时，PU_i 的防干扰圈将分别与 A，B，C 和 D 相交。当 PU_i 与 A，B，C 和 D 相交的顺序不同时，效用函数也不相同。接下来讨论所有可能的顺序。

(a) $B \to C \to A \to D$。

$$E[U_p] = \begin{cases} T_{p,i}^1 + k_1 \pi (r_{s,2}^\epsilon + r_{s,2}^0)^2 - \frac{k_p}{L_p} \\ \quad \text{if } d_{m1} - r_{s,1}^\epsilon - r_{s,1}^0 \le L_p \le d_{m2} - r_{s,2}^\epsilon - r_{s,2}^0 \\ T_{p,i}^1 + T_{p,i}^2 - \frac{k_p}{L_p} \\ \quad \text{if } d_{m2} - r_{s,2}^\epsilon - r_{s,2}^0 < L_p \le d_{m1} - r_{s,1}^\epsilon \\ T_{p,i}^2 - \frac{k_p}{L_p} \\ \quad \text{if } d_{m1} - r_{s,1}^\epsilon < L_p \le d_{m2} - r_{s,2}^\epsilon \end{cases}$$

(b) $B \to C \to D \to A$。

$$E[U_p] = \begin{cases} T_{p,i}^1 + k_1 \pi (r_{s,2}^\epsilon + r_{s,2}^0)^2 - \frac{k_p}{L_p} \\ \quad \text{if } d_{m1} - r_{s,1}^\epsilon - r_{s,1}^0 \le L_p \le d_{m2} - r_{s,2}^\epsilon - r_{s,2}^0 \\ T_{p,i}^1 + T_{p,i}^2 - \frac{k_p}{L_p} \\ \quad \text{if } d_{m2} - r_{s,2}^\epsilon - r_{s,2}^0 < L_p \le d_{m2} - r_{s,2}^\epsilon \\ T_{p,i}^1 - \frac{k_p}{L_p} \\ \quad \text{if } d_{m2} - r_{s,2}^\epsilon < L_p \le d_{m1} - r_{s,1}^\epsilon \end{cases}$$

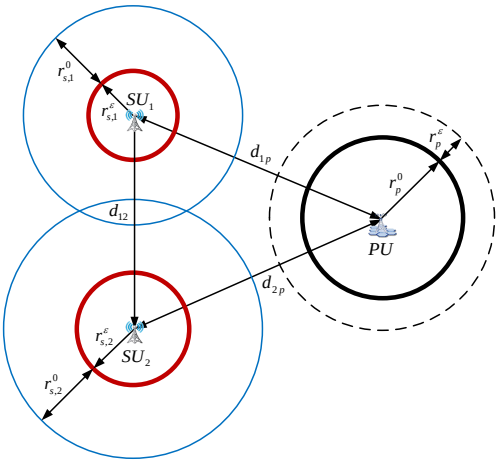


图 6.10　防干扰圈相交

(c) $B \to A \to C \to D$

$$E[U_p] = \begin{cases} T^1_{p,i} + k_1\pi(r^\epsilon_{s,2} + r^0_{s,2})^2 - \frac{k_p}{L_p} \\ \quad \text{if } d_{m1} - r^\epsilon_{s,1} - r^0_{s,1} \le L_p \le d_{m1} - r^\epsilon_{s,1} \\ k_1\pi(r^\epsilon_{s,2} + r^0_{s,2})^2 - \frac{k_p}{L_p} \\ \quad \text{if } d_{m1} - r^\epsilon_{s,1} < L_p \le d_{m2} - r^\epsilon_{s,2} - r^0_{s,2} \\ T^2_{p,i} - \frac{k_p}{L_p} \\ \quad \text{if } d_{m2} - r^\epsilon_{s,2} - r^0_{s,2} < L_p \le d_{m2} - r^\epsilon_{s,2} \end{cases}$$

其他顺序都与上述三种顺序对称，因此不在此列出。

这里的目标是计算最优 L^*_p 来最大化 $E[U_p]$。解决该优化问题的方法是分别找到分段函数每一段的最优值，然后取使得 $E[U_p]$ 最大的 L^*_p。观察所有分段函数可以发现，它们都与问题 6.4.5类似，因此可以使用问题 6.4.5的解法分别进行求解。

情形 2： 防干扰圈相交，如图 6.10所示。

在这种情况下,除了计算一级用户的最优隐私保护程度和二级用户的最大传输半径,还需要保证它们之间的防干扰圈不相交。PU_i 的最优隐私保护程度可能存在于两种不同的情形，一种是只有一个二级用户能使用信道，另一种是两个二级用户都能使用信道。

当只有一个二级用户能使用信道时，可以参考第 6.4节对于单一级用户单二级用户场景下的分析方法，分别计算每个二级用户分别的最优隐私保护程度 $L^{1*}_{p,1}$ 和 $L^{1*}_{p,2}$。

当两个二级用户都能使用信道时，可以求解以下优化问题:

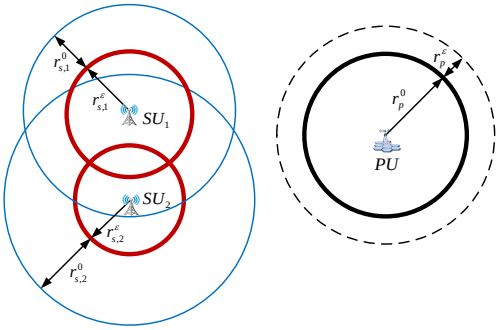


图 6.11　隐私保护圈相交

问题 6.5.3.

$$\begin{aligned}\underset{R_1,R_2,L_p}{\operatorname{argmax}} E[U_p] =& k_1\pi[\frac{R_1}{r^0_{s,1}}(r^\epsilon_{s,1}+R_1)^2+\frac{R_2}{r^0_{s,2}}(r^\epsilon_{s,2}+R_2)^2] \\ & -\frac{k_p}{L_p} \\ s.t.\quad & R_1+r^\epsilon_{s,1}+r_p+L_p\le d_{1p} \\ & R_2+r^\epsilon_{s,2}+r_p+L_p\le d_{2p} \\ & R_1+r^\epsilon_{s,1}+R_2+r^\epsilon_{s,2}\le d_{12} \\ & 0\le R_1\le r^0_{s,1} \\ & 0\le R_2\le r^0_{s,2} \\ & L_p>0\end{aligned}$$

由于目标函数是非凸的，只能通过梯度下降法[148]来找到近似最优解 L_p^{2*}。然后比较三种情况来决定全局最优的隐私保护程度

$$L_p^* = max\{L_{p,1}^{1*}, L_{p,2}^{1*}, L_p^{2*}\}.$$

情形 3： 隐私保护圈相交，如图 6.11所示。

在这种情形下，类似于信道空闲时的情形 3，只能满足其中一个二级用户的需求。为得到最大收益，分别计算只有一个二级用户存在时的最优隐私保护程度 $L_{p,1}^*$ 和 $L_{p,2}^*$，PU_i 的全局最优隐私保护程度为

$$L_p^* = max\{L_{p,1}^*, L_{p,2}^*\}.$$

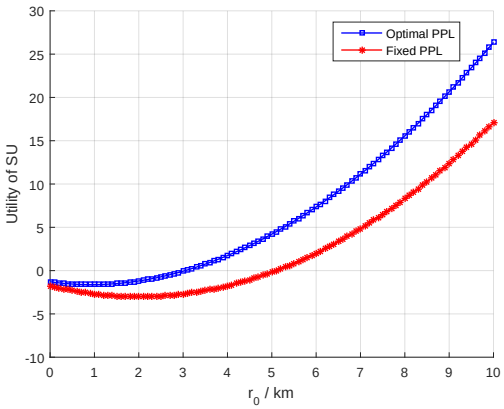


图 6.12　隐私保护经过最优决策和未经最优决策时二级用户效用

6.6　性能评估

本部分首先介绍实验设置，然后揭示与基准算法相比较 UMax 协议的优势。

6.6.1　实验设置

首先介绍基准算法：与 UMax 在线优化隐私保护程度不同，基准算法每次都使用一个固定的隐私保护程度。

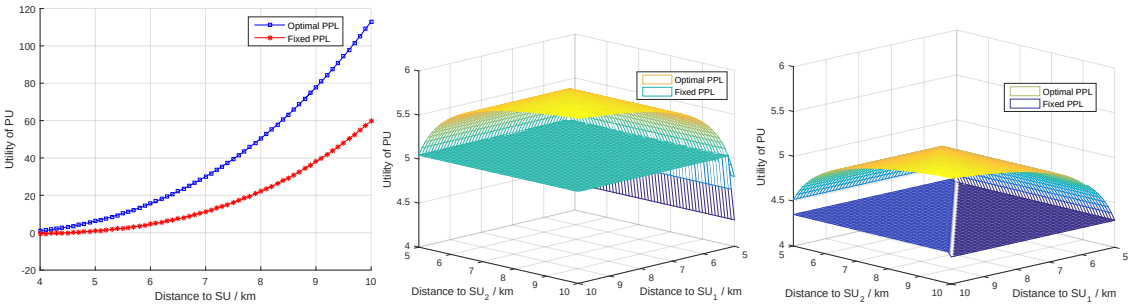
为方便起见，实验中使用的距离单位为千米，并只使用数字来表示距离。在基准算法中，一级用户和二级用户的隐私保护程度分别为 1 和 2。隐私损失系数 k_s 和 k_p 分别为 1 和 2，k_1 和 k_2 分别设置为 0.1 和 0.2。

接下来介绍实验设置：1) 比较二级用户选择不同的期望传输半径时的系统效用；2) 在不同的一级用户二级用户相对距离设定下，一级用户的系统效用；3) 构建一个 $20 * 20$ 的区域，并随机部署 10 个一级用户和 20 个二级用户，然后比较不同一级用户的系统效用。

6.6.2　性能比较

图 6.12比较了在不同协议下二级用户的系统效用。实验结果显示 UMax 在不同期望传输半径 r_0 下能有效提升系统效用。注意到当 r_0 小于某个阈值时，二级用户的系统效用为负。这是因为当 r_0 很小时，从问题 6.4.3中可以得知，二级用户的收益 R_s 将会非常小。另一方面，二级用户需要保证一定程度的隐私，导致二级用户的成本 C_{buy} 大于收益 R_s，从而导致效用为负。

图 6.13比较了不同协议在不同位置设定下一级用户的效用。实验考虑了三种场景：(i)

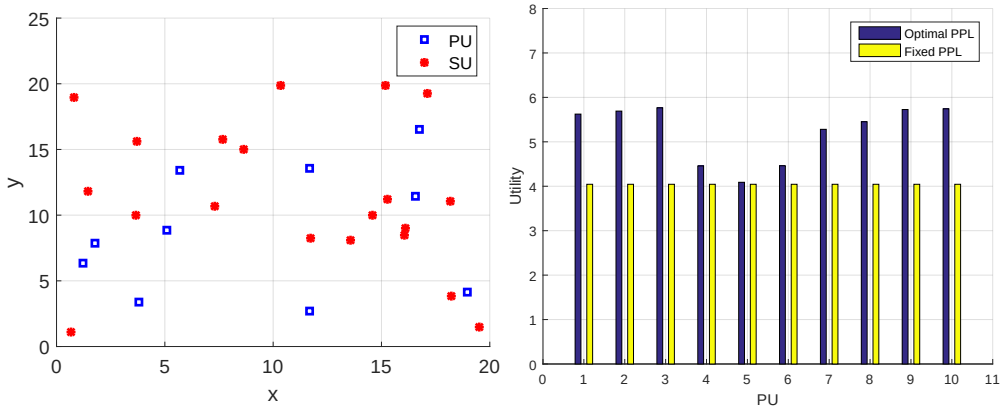


(a) 单一级用户和单二级用户场景

(b) 单一级用户和双二级用户场景，并且二级用户之间不相交

(c) 单一级用户和双二级用户场景，并且二级用户之间相交

图 6.13　隐私保护程度经过最优决策和未经最优决策时一级用户效用对比



(a) 一级用户和二级用户位置分布图

(b) 不同一级用户效用

图 6.14　随机部署场景下一级用户效用

单一级用户单二级用户；(ii) 单一级用户双二级用户，其中二级用户防干扰圈不相交；(iii) 单一级用户双二级用户，其中二级用户防干扰圈相交。图 6.13a显示，在单一级用户单二级用户场景下，UMax 的效用比基准协议高，并且一级用户和二级用户之间距离越大，提升效果越明显。原因是随着距离增加，一级用户能够出售更大的频谱使用面积，从而得到更多的收益。图 6.13b和图 6.13c显示了在单一级用户双二级用户场景下，UMax 的优越性，其中 x 坐标表示一级用户与二级用户 SU_1 之间的距离，y 坐标表示一级用户与二级用户 SU_2 之间的距离。两个图都显示 UMax 协议比基准协议取得了更高的效用。

图 6.14比较了一级用户和二级用户随机部署在某个区域时的效用。图 6.14a表示实验部署图，面积为 $20*20$，包含 10 个一级用户和 20 各二级用户。实验结果显示，UMax 对于所有的一级用户都能取得更高的效用。

6.7　本章小结

本章研究了基于数据库的认知无线电中位置隐私与频谱利用率之间的协同优化。我们设计了一种隐私保护的效用最大化数据库访问协议 UMax，通过位置隐私保护与频谱利用率之间的协同优化，允许一级用户和二级用户动态调整隐私预算来最大化系统效用。实验结果显示，UMax 能有效提升系统效用。

第七章 总结与展望

本章摘要： 本章总结全文主要工作及得到的主要结果，同时对未来工作进行展望。

7.1 全文总结

在学术界和工业界的共同推动下，本地差分隐私技术逐渐成为隐私数据收集的黄金标准。然而，本地差分隐私需要对数据进行随机扰动处理的本质不可避免得影响了数据可用性，阻碍了本地差分隐私的大规模部署。因此，数据可用性优化成为本地差分隐私研究的重点。本地差分隐私数据可用性优化可以从两个维度展开：融合算法优化和隐私预算优化，其中隐私预算优化包括激励设计和协同优化两种方法。但是，现有研究工作中的高维数据融合算法数据可用性比较低、计算复杂度高，激励设计方法无法解决信息不对称问题、无法满足实时数据融合应用的需求，协同优化方法的研究匮乏。本文针对现有研究工作中存在的不足进行了探索和改进，主要结论如下：

- 研究了高维数据分析的关键技术——边缘列联表发布——的融合算法优化问题。本文提出的高精度边缘列联表发布算法 CALM，首先通过对三种误差来源（噪音误差，重构误差和抽样误差）的定量分析，选出了一组称为视图的边缘列联表；然后使用频率估计方法生成一组满足本地差分隐私的视图；接下来对带有扰动的视图进行一致性和非负性处理；最后使用一致性视图和最大熵优化理论重构出所有边缘列联表。基于真实数据集的大规模实验证明 CALM 比现有方法的融合误差降低了一到两个数量级。

- 研究了基于激励设计的隐私预算优化方法中，如何解决融合中心与用户之间的信息不对称问题。借助于经济学中的契约理论，本文提出了一种解决信息不对称的激励机制 REAP 。在经济预算一定的情况下，使用契约理论设计了一套有效的契约来最大化融合中心数据可用性。REAP 为拥有不同隐私偏好的用户提供不同的契约，并保证用户选择自身隐私偏好对应的契约时能获得最大收益。本文推导出了在完全信息和不完全信息下最优契约的解析表达式，并且把契约设计推广到用户隐私偏好连续取值的情形。仿真结果验证了 REAP 的可行性和有效性。

- 研究了针对实时数据融合应用的动态激励设计方法。本文设计的 LEPA 机制通过把长期参与约束转化成队列稳定问题，解决了不同时隙用户选择策略相互耦合的问题，并通过一个在线算法来联合优化各个时隙之间的系统效用，以此来防止用户中途离开群智感知系统。考虑到用户的自私行为以及感知任务的组合特性，本文提出了一种计算高效的在线拍卖机制，该机制被证明接近最优解，具有真实性以及个体理性等性质。本文分别通过理论分析和仿真实验证明了 LEPA 方法的有效性。

- 研究了数据库驱动认知无线电中位置隐私保护与频谱利用率之间的协同优化问题。本文设计了一种隐私保护的效用最大化数据库访问协议 UMax ，通过位置隐私保护与频谱利用率之间的协同优化，允许一级用户和二级用户选择最优的隐私预算来最大化系统效用。实验结果显示，通过分别优化一级用户和二级用户的隐私预算，UMax 能有效提升提升了位置数据的可用性，从而提升了频谱利用率。

在各国政府陆续出台日趋严格的隐私保护方案的风口，本地差分隐私技术为各大互联网公司合法收集用户隐私数据提供了强有力的技术手段。为了减轻随机扰动对数据质量的影响，针对本地差分隐私数据可用性优化的研究至关重要。本文从两个维度研究了本地差分隐私数据可用性优化方法，并针对现有方法的不足提供了有效的解决方案，为本地差分隐私的大规模部署提供了可靠的理论与技术支撑。

7.2 研究展望

本文针对本地差分隐私数据可用性优化的全流程进行了探索，并解决了目前研究工作中存在的不足。但由于时间限制，还有很多尚未解决的问题，值得进一步研究和探索。因此，我们将一些潜在的研究方向总结如下:

- **高精度的数据集合成算法：** 目前大多数融合算法优化都是针对具体数据任务设计的，这种方法很有效但却费时费力。一个更有前景的方案是发布一个满足本地差分隐私的合成数据集，数据分析者可以基于该合成数据集完成很多数据分析任务。现有数据集合成算法数据可用性非常低，并且只能处理低维数据。我们目前正在研究开发一个高可用性的数据集合成算法，初步试验结果表明数据可用性相比于现有工作获得了巨大提升。

- **数据之间存在关联性的激励设计：** 目前的激励设计均假设用户数据之间不存在关联性，因此可以独立地对不同用户数据进行随机化处理。而在现实生活中，很多用户数

据之间是存在关联性的。因此，需要考虑在用户数据相互关联的情况下如何设计激励机制。

- **任意数据分析任务的激励设计：** 目前的激励设计方法主要针对简单的数据分析任务，比如均值估计。然而在真实场景中，需要对数据进行更加复杂的分析。为了使得激励设计方法能有效部署于真实场景，开发针对更加复杂甚至通用的数据分析任务的激励机制显得至关重要。

参考文献

[1] John Gantz, David Reinsel. Extracting value from chaos[J]. IDC iview, 2011. 1142(2011):1–12.

[2] 吴小同. 大数据环境下隐私保护及其关键技术研究 [D]. [PHD Thesis] 南京大学, 2017.

[3] 经济学人：数据是未来的石油. https://pit.ifeng.com/a/20170506/51054293_0.shtml?_share=sina&tp=1494000000000.

[4] 陈世熹. 提供差分隐私保护的线性查询新方法 [D]. [PHD Thesis] 复旦大学, 2012.

[5] 李杨. 差分隐私保护数据聚合优化方法及其在数据可视化中的应用 [D]. [PHD Thesis] 广东工业大学, 2013.

[6] 许胜之. 满足差分隐私保护的频繁模式挖掘关键技术研究 [D]. [PHD Thesis] 北京邮电大学, 2016.

[7] Ninghui Li, Wahbeh Qardaji, Dong Su, Yi Wu, Weining Yang. Membership privacy: a unifying framework for privacy definitions[C]//Proceedings of ACM CCS'13:889–900.

[8] Michael Barbaro, Tom Zeller. A face is exposed for aol searcher no. 4417749[J]. The New York Times, 2006. 9.

[9] Arvind Narayanan, Vitaly Shmatikov. Robust de-anonymization of large sparse datasets[C]//Proceedings of IEEE SP'08:111–125.

[10] John Bohannon. Credit card study blows holes in anonymity, 2015.

[11] https://www.eff.org/deeplinks/2012/02/obama-administration-unveils-promising-consumer-privacy-plan-dev

[12] https://eugdpr.org/.

[13] 中华人名共和国国务院. 国家中长期科学和技术发展规划纲要 (2006-2020 年), 2006.

[14] Mihir Bellare, Phillip Rogaway. Optimal asymmetric encryption[C]//Workshop on the Theory and Application of of Cryptographic Techniques. Springer, 1994:92–111.

[15] Eiichiro Fujisaki, Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes[C]//Annual International Cryptology Conference. Springer, 1999:537–554.

[16] Eiichiro Fujisaki, Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes[J]. Journal of cryptology, 2013. 26(1):80–101.

[17] Yehuda Lindell, Benny Pinkas. Privacy preserving data mining[C]//Annual International Cryptology Conference. Springer, 2000:36–54.

[18] Benny Pinkas. Cryptographic techniques for privacy-preserving data mining[J]. ACM Sigkdd

Explorations Newsletter, 2002. 4(2):12–19.

[19] Bart Goethals, Sven Laur, Helger Lipmaa, Taneli Mielikäinen. On private scalar product computation for privacy-preserving data mining[C]//International Conference on Information Security and Cryptology. Springer, 2004:104–120.

[20] Bing Wang, Wei Song, Wenjing Lou, Y Thomas Hou. Inverted index based multi-keyword public-key searchable encryption with strong privacy guarantee[C]//2015 IEEE Conference on Computer Communications (INFOCOM). IEEE, 2015:2092–2100.

[21] Ronald Cramer, Ivan Damgård, Jesper B Nielsen. Multiparty computation from threshold homomorphic encryption[C]//International conference on the theory and applications of cryptographic techniques. Springer, 2001:280–300.

[22] Kai-Min Chung, Yael Kalai, Salil Vadhan. Improved delegation of computation using fully homomorphic encryption[C]//Annual Cryptology Conference. Springer, 2010:483–501.

[23] Latanya Sweeney. k-anonymity: A model for protecting privacy[J]. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 2002. 10(05):557–570.

[24] Ashwin Machanavajjhala, Daniel Kifer, Johannes Gehrke, Muthuramakrishnan Venkitasubramaniam. l-diversity: Privacy beyond k-anonymity[J]. ACM Transactions on Knowledge Discovery from Data (TKDD), 2007. 1(1):3.

[25] Ninghui Li, Tiancheng Li, Suresh Venkatasubramanian. t-closeness: Privacy beyond k-anonymity and l-diversity[C]//2007 IEEE 23rd International Conference on Data Engineering. IEEE, 2007:106–115.

[26] Paul Cuff, Lanqing Yu. Differential privacy as a mutual information constraint[J]. arXiv preprint arXiv:1608.03677, 2016.

[27] Weina Wang, Lei Ying, Junshan Zhang. On the relation between identifiability, differential privacy, and mutual-information privacy[J]. IEEE Transactions on Information Theory, 2016. 62(9):5018–5029.

[28] David Rebollo-Monedero, Jordi Forne, Josep Domingo-Ferrer. From t-closeness-like privacy to postrandomization via information theory[J]. IEEE Transactions on Knowledge and Data Engineering, 2009. 22(11):1623–1636.

[29] Darakhshan J Mir. Information-theoretic foundations of differential privacy[C]//International Symposium on Foundations and Practice of Security. Springer, 2012:374–381.

[30] Cynthia Dwork. Differential privacy: A survey of results[C]//International Conference on Theory and Applications of Models of Computation. Springer, 2008:1–19.

[31] Jaewoo Lee, Chris Clifton. Differential identifiability[C]//Proceedings of the 18th ACM SIGKDD international conference on Knowledge discovery and data mining. ACM, 2012:1041–1049.

[32] Mário S Alvim, Miguel E Andrés, Konstantinos Chatzikokolakis, Pierpaolo Degano, Catuscia Palamidessi. Differential privacy: on the trade-off between utility and information leakage[C]//International Workshop on Formal Aspects in Security and Trust. Springer, 2011:39–54.

[33] 张啸剑, 孟小峰. 面向数据发布和分析的差分隐私保护 [J]. 计算机学报, 2014. 37(4):927–949.

[34] 熊平, 朱天清, 王晓峰. 差分隐私保护及其应用 [J]. 计算机学报, 2014. 37(1):101–122.

[35] 李杨, 温雯, 谢光强. 差分隐私保护研究综述 [J]. 计算机应用研究, 2012. 29(9):3201–3205.

[36] Cynthia Dwork, Frank McSherry, Kobbi Nissim, Adam Smith. Calibrating noise to sensitivity in private data analysis[C]//Theory of cryptography conference. Springer, 2006:265–284.

[37] Aleksandar Nikolov, Kunal Talwar, Li Zhang. The geometry of differential privacy: the sparse and approximate cases[C]//Proceedings of the forty-fifth annual ACM symposium on Theory of computing. ACM, 2013:351–360.

[38] Frank McSherry, Kunal Talwar. Mechanism design via differential privacy.[C]//FOCS. volume 7. 2007:94–103.

[39] Noah Johnson, Joseph P Near, Dawn Song. Practical differential privacy for sql queries using elastic sensitivity[J]. arXiv preprint arXiv:1706.09479, 2017.

[40] Shiva Prasad Kasiviswanathan, Homin K Lee, Kobbi Nissim, Sofya Raskhodnikova, Adam Smith. What can we learn privately?[J]. SIAM Journal on Computing, 2011. 40(3):793–826.

[41] Úlfar Erlingsson, Vasyl Pihur, Aleksandra Korolova. Rappor: Randomized aggregatable privacy-preserving ordinal response[C]//Proceedings of the 2014 ACM SIGSAC conference on computer and communications security. ACM, 2014:1054–1067.

[42] Apple differential privacy team, learning with privacy at scale. Available at https://machinelearning.apple.com/docs/learning-with-privacy-at-scale/appledifferentialprivacysystem.pdf.

[43] Bolin Ding, Janardhan Kulkarni, Sergey Yekhanin. Collecting telemetry data privately[C]//Advances in Neural Information Processing Systems. 2017:3574–3583.

[44] Tianhao Wang, Jeremiah Blocki, Ninghui Li, Somesh Jha. Locally differentially private protocols for frequency estimation.[C]//Proceedings of USENIX. USENIX Association, 2017.

[45] Jinyuan Jia, Neil Zhenqiang Gong. Calibrate: Frequency estimation and heavy hitter identification with local differential privacy via incorporating prior knowledge[J]. arXiv preprint arXiv:1812.02055, 2018.

[46] Trie, wikipedia. Available at https://en.wikipedia.org/wiki/Trie.

[47] Binary tree, wikipedia. Available at https://en.wikipedia.org/wiki/Binary_tree.

[48] Hash, wikipedia. Available at https://en.wikipedia.org/wiki/Hash_function.

[49] Arpita Ghosh, Aaron Roth. Selling privacy at auction[C]//Proceedings of the 12th ACM confer-

ence on Electronic commerce. ACM, 2011:199–208.

[50] Weina Wang, Lei Ying, Junshan Zhang. The value of privacy: Strategic data subjects, incentive mechanisms and fundamental limits[J]. ACM SIGMETRICS Performance Evaluation Review, 2016. 44(1):249–260.

[51] Reza Shokri, George Theodorakopoulos, Carmela Troncoso, Jean-Pierre Hubaux, Jean-Yves Le Boudec. Protecting location privacy: optimal strategy against localization attacks[C]//Proceedings of the 2012 ACM conference on Computer and communications security. ACM, 2012:617–627.

[52] Nicolás E Bordenabe, Konstantinos Chatzikokolakis, Catuscia Palamidessi. Optimal geo-indistinguishable mechanisms for location privacy[C]//Proceedings of the 2014 ACM SIGSAC conference on computer and communications security. ACM, 2014:251–262.

[53] Michael Hay, Vibhor Rastogi, Gerome Miklau, Dan Suciu. Boosting the accuracy of differentially private histograms through consistency[J]. Proceedings of the VLDB Endowment, 2010. 3(1-2):1021–1032.

[54] Xiaojian Zhang, Rui Chen, Jianliang Xu, Xiaofeng Meng, Yingtao Xie. Towards accurate histogram publication under differential privacy[C]//Proceedings of the 2014 SIAM international conference on data mining. SIAM, 2014:587–595.

[55] Gergely Acs, Claude Castelluccia, Rui Chen. Differentially private histogram publishing through lossy compression[C]//2012 IEEE 12th International Conference on Data Mining. IEEE, 2012:1–10.

[56] Jia Xu, Zhenjie Zhang, Xiaokui Xiao, Yin Yang, Ge Yu, Marianne Winslett. Differentially private histogram publication[J]. The VLDB Journal—The International Journal on Very Large Data Bases, 2013. 22(6):797–822.

[57] Stanley L Warner. Randomized response: A survey technique for eliminating evasive answer bias[J]. Journal of the American Statistical Association, 1965. 60(309):63–69.

[58] Cynthia Dwork, Aaron Roth, et al. The algorithmic foundations of differential privacy[J]. Foundations and Trends® in Theoretical Computer Science, 2014. 9(3–4):211–407.

[59] Shaowei Wang, Liusheng Huang, Pengzhan Wang, Hou Deng, Hongli Xu, Wei Yang. Private weighted histogram aggregation in crowdsourcing[C]//International Conference on Wireless Algorithms, Systems, and Applications. Springer, 2016:250–261.

[60] Raef Bassily, Adam Smith. Local, private, efficient protocols for succinct histograms[C]//Proceedings of the forty-seventh annual ACM symposium on Theory of computing. ACM, 2015:127–135.

[61] T-H Hubert Chan, Mingfei Li, Elaine Shi, Wenchang Xu. Differentially private continual monitoring of heavy hitters from distributed streams[C]//International Symposium on Privacy Enhancing

Technologies Symposium. Springer, 2012:140–159.

[62] Wennan Zhu, Peter Kairouz, Haicheng Sun, Brendan McMahan, Wei Li. Federated heavy hitters discovery with differential privacy[J]. arXiv preprint arXiv:1902.08534, 2019.

[63] Giulia Fanti, Vasyl Pihur, Úlfar Erlingsson. Building a rappor with the unknown: Privacy-preserving learning of associations and data dictionaries[J]. Proceedings on Privacy Enhancing Technologies, 2016. 2016(3):41–61.

[64] Tianhao Wang, Ninghui Li, Somesh Jha. Locally differentially private heavy hitter identification[J]. arXiv:1708.06674, 2017.

[65] Raef Bassily, Kobbi Nissim, Uri Stemmer, Abhradeep Guha Thakurta. Practical locally private heavy hitters[C]//Advances in Neural Information Processing Systems. 2017:2288–2296.

[66] Ning Wang, Xiaokui Xiao, Yin Yang, Ta Duy Hoang, Hyejin Shin, Junbum Shin, Ge Yu. Privtrie: Effective frequent term discovery under local differential privacy[C]//2018 IEEE 34th International Conference on Data Engineering (ICDE). IEEE, 2018:821–832.

[67] Ninghui Li, Wahbeh Qardaji, Dong Su, Jianneng Cao. Privbasis: Frequent itemset mining with differential privacy[J]. Proceedings of the VLDB Endowment, 2012. 5(11):1340–1351.

[68] Rui Chen, Noman Mohammed, Benjamin CM Fung, Bipin C Desai, Li Xiong. Publishing set-valued data via differential privacy[J]. Proceedings of the VLDB Endowment, 2011. 4(11):1087–1098.

[69] Chen Zeng, Jeffrey F Naughton, Jin-Yi Cai. On differentially private frequent itemset mining[J]. Proceedings of the VLDB Endowment, 2012. 6(1):25–36.

[70] Ning Wang, Xiaokui Xiao, Yin Yang, Zhenjie Zhang, Yu Gu, Ge Yu. Privsuper: A superset-first approach to frequent itemset mining under differential privacy[C]//2017 IEEE 33rd International Conference on Data Engineering (ICDE). IEEE, 2017:809–820.

[71] Zhan Qin, Yin Yang, Ting Yu, Issa Khalil, Xiaokui Xiao, Kui Ren. Heavy hitter estimation over set-valued data with local differential privacy[C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2016:192–203.

[72] Tianhao Wang, Ninghui Li, Somesh Jha. Locally differentially private frequent itemset mining[C]//2018 IEEE Symposium on Security and Privacy (SP). IEEE, 2018:127–143.

[73] Wahbeh Qardaji, Weining Yang, Ninghui Li. Priview: practical differentially private release of marginal contingency tables[C]//Proceedings of SIGMOD. ACM, 2014:1435–1446.

[74] Boaz Barak, Kamalika Chaudhuri, Cynthia Dwork, Satyen Kale, Frank McSherry, Kunal Talwar. Privacy, accuracy, and consistency too: a holistic solution to contingency table release[C]//Proceedings of the twenty-sixth ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems. ACM, 2007:273–282.

[75] Bolin Ding, Marianne Winslett, Jiawei Han, Zhenhui Li. Differentially private data cubes: optimizing noise sources and consistency[C]//Proceedings of the 2011 ACM SIGMOD International Conference on Management of data. ACM, 2011:217–228.

[76] Xuebin Ren, Chia-Mu Yu, Weiren Yu, Shusen Yang, Xinyu Yang, Julie A McCann, S Yu Philip. Lopub: High-dimensional crowdsourced data publication with local differential privacy[J]. IEEE Transactions on Information Forensics and Security, 2018. 13(9):2151–2166.

[77] Graham Cormode, Tejas Kulkarni, Divesh Srivastava. Marginal release under local differential privacy[C]//Proceedings of ACM SIGMOD'18:131–146.

[78] Chao Li, Michael Hay, Vibhor Rastogi, Gerome Miklau, Andrew McGregor. Optimizing linear counting queries under differential privacy[C]//Proceedings of the twenty-ninth ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems. ACM, 2010:123–134.

[79] Chao Li, Michael Hay, Gerome Miklau, Yue Wang. A data-and workload-aware algorithm for range queries under differential privacy[J]. Proceedings of the VLDB Endowment, 2014. 7(5):341–352.

[80] Xiaokui Xiao, Guozhang Wang, Johannes Gehrke. Differential privacy via wavelet transforms[J]. IEEE Transactions on knowledge and data engineering, 2010. 23(8):1200–1214.

[81] Wahbeh Qardaji, Weining Yang, Ninghui Li. Understanding hierarchical methods for differentially private histograms[J]. Proceedings of the VLDB Endowment, 2013. 6(14):1954–1965.

[82] Tianhao Wang, Boling Ding, Jingren Zhou, Cheng Hong, Zhicong Huang, Ninghui Li, Somesh Jha. Answering multi-dimensional analytical queries under local differential privacy[C]//Proceedings of ACM SIGMOD'19:to appear.

[83] Jun Zhang, Graham Cormode, Cecilia M Procopiuc, Divesh Srivastava, Xiaokui Xiao. Privbayes: Private data release via bayesian networks[J]. ACM Transactions on Database Systems (TODS), 2017. 42(4):25.

[84] Rui Chen, Qian Xiao, Yu Zhang, Jianliang Xu. Differentially private high-dimensional data publication via sampling-based inference[C]//Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. ACM, 2015:129–138.

[85] Ryan McKenna, Daniel Sheldon, Gerome Miklau. Graphical-model based estimation and inference for differential privacy[J]. arXiv preprint arXiv:1901.09136, 2019.

[86] John C Duchi, Michael I Jordan, Martin J Wainwright. Minimax optimal procedures for locally private estimation[J]. Journal of the American Statistical Association, 2018. 113(521):182–201.

[87] Ning Wang, Xiaokui Xiao, Yin Yang, Jun Zhao, Siu Cheung Hui, Hyejin Shin, Junbum Shin, Ge Yu. Collecting and analyzing multidimensional data with local differential privacy[C]//Proceedings of IEEE ICDE'19:638–649.

[88] Hidetoshi Kido, Yutaka Yanagisawa, Tetsuji Satoh. Protection of location privacy using dummies for location-based services[C]//21st International Conference on Data Engineering Workshops

(ICDEW'05). IEEE, 2005:1248–1248.

[89] Pravin Shankar, Vinod Ganapathy, Liviu Iftode. Privately querying location-based services with sybilquery[C]//Proceedings of the 11th international conference on Ubiquitous computing. ACM, 2009:31–40.

[90] Bhuvan Bamba, Ling Liu, Peter Pesti, Ting Wang. Supporting anonymous location queries in mobile environments with privacy grid[C]//Proceedings of the 17th international conference on World Wide Web. ACM, 2008:237–246.

[91] Matt Duckham, Lars Kulik. A formal model of obfuscation and negotiation for location privacy[C]//International conference on pervasive computing. Springer, 2005:152–170.

[92] Mingqiang Xue, Panos Kalnis, Hung Keng Pung. Location diversity: Enhanced privacy protection in location based services[C]//International Symposium on Location-and Context-Awareness. Springer, 2009:70–87.

[93] Miguel E Andrés, Nicolás E Bordenabe, Konstantinos Chatzikokolakis, Catuscia Palamidessi. Geo-indistinguishability: differential privacy for location-based systems[C]//Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security. ACM, 2013:901–914.

[94] Yonghui Xiao, Li Xiong. Protecting locations with differential privacy under temporal correlations[C]//Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. ACM, 2015:1298–1309.

[95] Moritz Hardt, Kunal Talwar. On the geometry of differential privacy[C]//Proceedings of the forty-second ACM symposium on Theory of computing. ACM, 2010:705–714.

[96] Lisa K Fleischer, Yu-Han Lyu. Approximately optimal auctions for selling privacy when costs are correlated with data[C]//Proceedings of the 13th ACM Conference on Electronic Commerce. ACM, 2012:568–585.

[97] Aaron Roth, Grant Schoenebeck. Conducting truthful surveys, cheaply[C]//Proceedings of the 13th ACM Conference on Electronic Commerce. ACM, 2012:826–843.

[98] Katrina Ligett, Aaron Roth. Take it or leave it: Running a survey when privacy comes at a cost[C]//International Workshop on Internet and Network Economics. Springer, 2012:378–391.

[99] Kobbi Nissim, Salil Vadhan, David Xiao. Redrawing the boundaries on purchasing data from privacy-sensitive individuals[C]//Proceedings of the 5th conference on Innovations in theoretical computer science. ACM, 2014:411–422.

[100] Chaoyue Niu, Zhenzhe Zheng, Fan Wu, Shaojie Tang, Xiaofeng Gao, Guihai Chen. Unlocking the value of privacy: Trading aggregate statistics over private correlated data[C]//Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining. ACM, 2018:2031–2040.

[101] Daniel Kifer, Ashwin Machanavajjhala. A rigorous and customizable framework for pri-

vacy[C]//Proceedings of the 31st ACM SIGMOD-SIGACT-SIGAI symposium on Principles of Database Systems. ACM, 2012:77–88.

[102] Changchang Liu, Supriyo Chakraborty, Prateek Mittal. Dependence makes you vulnberable: Differential privacy under dependent tuples.[C]//NDSS. volume 16. 2016:21–24.

[103] Shuang Song, Yizhen Wang, Kamalika Chaudhuri. Pufferfish privacy mechanisms for correlated data[C]//Proceedings of the 2017 ACM International Conference on Management of Data. ACM, 2017:1291–1306.

[104] Lei Yang, Mengyuan Zhang, Shibo He, Ming Li, Junshan Zhang. Crowd-empowered privacy-preserving data aggregation for mobile crowdsensing[C]//Proceedings of the Eighteenth ACM International Symposium on Mobile Ad Hoc Networking and Computing. ACM, 2018:151–160.

[105] Daniel M Gordon, Oren Patashnik, Greg Kuperberg. New constructions for covering designs[J]. Journal of Combinatorial Designs, 1995. 3(4):269–284.

[106] Dan Gordon. La jolla covering repository. Available at https://www.ccrwest.org.

[107] Thông T Nguyên, Xiaokui Xiao, Yin Yang, Siu Cheung Hui, Hyejin Shin, Junbum Shin. Collecting and analyzing data from smart device users with local differential privacy[J]. arXiv:1606.05053, 2016.

[108] Harold W Kuhn, Albert W Tucker. Nonlinear programming. //Traces and emergence of nonlinear programming. Springer, 2014. 247–258.

[109] William Karush. Minima of functions of several variables with inequalities as side constraints[J]. M. Sc. Dissertation. Dept. of Mathematics, Univ. of Chicago, 1939.

[110] Zijian Zheng, Ron Kohavi, Llew Mason. Real world performance of association rule algorithms[C]//Proceedings of SIGKDD. ACM, 2001:401–406.

[111] Frequent itemset mining dataset repository. Available at http://fimi.ua.ac.be/data/.

[112] A. Asuncion, D.J. Newman. UCI machine learning repository, 2010.

[113] Steven Ruggles, J. Trent Alexander, Katie Genadek, Ronald Goeken, Matthew B. Schroeder, Matthew Sobek. Integrated public use microdata series: Version 5.0 [machine-readable database], 2010.

[114] Xiaoming Duan, Chengcheng Zhao, Shibo He, Peng Cheng, Junshan Zhang. Distributed algorithms to compute walrasian equilibrium in mobile crowdsensing[J]. IEEE Transactions on Industrial Electronics, 2016. 64(5):4048–4057.

[115] Shibo He, Dong-Hoon Shin, Junshan Zhang, Jiming Chen. Near-optimal allocation algorithms for location-dependent tasks in crowdsensing[J]. IEEE Transactions on Vehicular Technology, 2016. 66(4):3392–3405.

[116] Raghu K Ganti, Nam Pham, Hossein Ahmadi, Saurabh Nangia, Tarek F Abdelzaher. Greengps:

a participatory sensing fuel-efficient maps application[C]//Proceedings of ACM MobiSys'10:151–164.

[117] Jiming Chen, Kang Hu, Qi Wang, Yuyi Sun, Zhiguo Shi, Shibo He. Narrowband internet of things: Implementations and applications[J]. IEEE Internet of Things Journal, 2017. 4(6):2309–2314.

[118] Yun Cheng, Xiucheng Li, Zhijun Li, Shouxu Jiang, Yilong Li, Ji Jia, Xiaofan Jiang. Aircloud: a cloud-based air-quality monitoring system for everyone[C]//Proceedings of ACM SenSys'14:251–265.

[119] Shaohan Hu, Lu Su, Hengchang Liu, Hongyan Wang, Tarek F Abdelzaher. Smartroad: Smartphone-based crowd sensing for traffic regulator detection and identification[J]. ACM Transactions on Sensor Networks, 2015. 11(4):55.

[120] Guang Yang, Shibo He, Zhiguo Shi, Jiming Chen. Promoting cooperation by the social incentive mechanism in mobile crowdsensing[J]. IEEE Communications Magazine, 2017. 55(3):86–92.

[121] Qi Zhang, Yutian Wen, Xiaohua Tian, Xiaoying Gan, Xinbing Wang. Incentivize crowd labeling under budget constraint[C]//Proceedings of IEEE INFOCOM'15:2812–2820.

[122] Xiang Zhang, Guoliang Xue, Ruozhou Yu, Dejun Yang, Jian Tang. Truthful incentive mechanisms for crowdsourcing[C]//Proceedings of IEEE INFOCOM'15:2830–2838.

[123] Yanru Zhang, Lingyang Song, Walid Saad, Zaher Dawy, Zhu Han. Contract-based incentive mechanisms for device-to-device communications in cellular networks[J]. IEEE Journal on Selected Areas in Communications, 2015. 33(10):2144–2155.

[124] Lingjie Duan, Lin Gao, Jianwei Huang. Cooperative spectrum sharing: a contract-based approach[J]. IEEE Transactions on Mobile Computing, 2014. 13(1):174–187.

[125] Michael J Neely. Stochastic network optimization with application to communication and queueing systems[J]. Synthesis Lectures on Communication Networks, 2010. 3(1):1–211.

[126] Lei Zheng, Lin Cai. A distributed demand response control strategy using lyapunov optimization[J]. IEEE Transactions on Smart Grid, 2014. 5(4):2075–2083.

[127] Yuyi Mao, Jun Zhang, Khaled B Letaief. A lyapunov optimization approach for green cellular networks with hybrid energy supplies[J]. IEEE Journal on Selected Areas in Communications, 2015. 33(12):2463–2477.

[128] Haiming Jin, Lu Su, Danyang Chen, Klara Nahrstedt, Jinhui Xu. Quality of information aware incentive mechanisms for mobile crowd sensing systems[C]//Proceedings of ACM MobiHoc'15:167–176.

[129] Ying-Chang Liang, Kwang-Cheng Chen, Geoffrey Ye Li, Petri Mahonen. Cognitive radio networking and communications: An overview[J]. IEEE Transactions on Vehicular Technology, 2011. 60(7):3386–3407.

[130] Ruilong Deng, Jiming Chen, Xianghui Cao, Yan Zhang, Sabita Maharjan, Stein Gjessing. Sensing-performance tradeoff in cognitive radio enabled smart grid[J]. IEEE Transactions on Smart Grid, 2013. 4(1):302–310.

[131] Jiming Chen, Qing Yu, Bo Chai, Youxian Sun, Yanfei Fan, Xuemin Shen. Dynamic channel assignment for wireless sensor networks: a regret matching based approach[J]. IEEE Transactions on Parallel and Distributed Systems, 2015. 26(1):95–106.

[132] Jiming Chen, Kang Hu, Qi Wang, Yuyi Sun, Zhiguo Shi, Shibo He. Narrow-band internet of things: Implementations and applications[J]. IEEE Internet of Things Journal, to appear. DOI: 10.1109/JIOT.2017.2764475.

[133] Shibo He, Jiming Chen, Fachang Jiang, David KY Yau, Guoliang Xing, Youxian Sun. Energy provisioning in wireless rechargeable sensor networks[J]. IEEE Transactions on Mobile Computing, 2013. 12(10):1931–1942.

[134] Jiming Chen, Xianghui Cao, Peng Cheng, Yang Xiao, Youxian Sun. Distributed collaborative control for industrial automation with wireless sensor and actuator networks[J]. IEEE Transactions on Industrial Electronics, 2010. 57(12):4219–4230.

[135] Jianfeng Wang, Monisha Ghosh, Kiran Challapali. Emerging cognitive radio applications: A survey[J]. IEEE Communications Magazine, 2011. 49(3):74–81.

[136] Maulin Patel, Jianfeng Wang. Applications, challenges, and prospective in emerging body area networking technologies[J]. IEEE Wireless communications, 2010. 17(1):80–88.

[137] Ex-parte comments of ge healthcare in docket 06-135. http://fjallfoss.fcc.gov/ecfs/document/view?id=6519820996/.

[138] Xiaoming Duan, Chengcheng Zhao, Shibo He, Peng Cheng, Junshan Zhang. Distributed algorithms to compute walrasian equilibrium in mobile crowdsensing[J]. IEEE Transactions on Industrial Electronics, 2017. 64(5):4048–4057.

[139] Ankit Singh Rawat, Priyank Anand, Hao Chen, Pramod K Varshney. Collaborative spectrum sensing in the presence of byzantine attacks in cognitive radio networks[J]. IEEE Transactions on Signal Processing, 2011. 59(2):774–786.

[140] Jiming Chen, Junkun Li, Shibo He, Tian He, Yu Gu, Youxian Sun. On energy-efficient trap coverage in wireless sensor networks[J]. ACM Transactions on Sensor Networks, 2013. 10(1):2.

[141] Jiming Chen, Junkun Li, Ten H Lai. Energy-efficient intrusion detection with a barrier of probabilistic sensors: Global and local[J]. IEEE Transactions on Wireless Communications, 2013. 12(9):4742–4755.

[142] Jiming Chen, Junkun Li, Ten H Lai. Trapping mobile targets in wireless sensor networks: An energy-efficient perspective[J]. IEEE Transactions on Vehicular Technology, 2013. 62(7):3287–3300.

[143] Youping Zhao, Joseph Gaeddert, Kyung K Bae, Jeffery H Reed. Radio environment map enabled situation-aware cognitive radio learning algorithms[C]//Proceedings of SDR Forum Technical Conference'06:1–9.

[144] Shah Nawaz Khan, Mohamed A Kalil, Andreas Mitschele-Thiel. Distributed resource map: A database-driven network support architecture for cognitive radio ad hoc networks[C]//Proceedings of ICUMT'12:188–194.

[145] Rohan Murty, Ranveer Chandra, Thomas Moscibroda, Paramvir Bahl. Senseless: A database-driven white spaces network[J]. IEEE Transactions on Mobile Computing, 2012. 11(2):189–203.

[146] Behnam Bahrak, Sudeep Bhattarai, Abid Ullah, Jung-Min Jerry Park, Jeffery Reed, David Gurney. Protecting the primary users' operational privacy in spectrum sharing[C]//Proceedings of IEEE DYSPAN'14:236–247.

[147] Zhaoyu Gao, Haojin Zhu, Yao Liu, Muyuan Li, Zhenfu Cao. Location privacy in database-driven cognitive radio networks: Attacks and countermeasures[C]//Proceedings of IEEE INFOCOM'13:2751–2759.

[148] Stephen Boyd, Lieven Vandenberghe. Convex optimization[M]. Cambridge University Press, 2004.

[149] Raymond Garver. On the nature of the roots of a quartic equation[J]. Mathematics News Letter, 1933:6–8.

攻读博士学位期间主要研究成果及参与的科研项目

一、完成的学术论文：

发表/录用的期刊论文

1. Zhikun Zhang, Shibo He, Junshan Zhang, Jiming Chen. REAP: An Efficient Incentive Mechanism for Reconciling Aggregation Accuracy and Individual Privacy in Crowdsensing, IEEE Transactions on Information Forensics Security (TIFS), 8(5): 2049-2061, 2017. （CCF A 类期刊）

2. Zhikun Zhang, Heng Zhang, Shibo He, Peng Cheng. Bilateral Privacy-preserving Utility Maximization Protocol in Database-driven Cognitive Radio Networks, IEEE Transactions on Dependable and Secure Computing (TDSC), DOI:10.1109/TDSC.2017.2781248. （CCF A 类期刊）

3. Yuyi Sun, Fei Tong, Zhikun Zhang, Shibo He. Throughput Modeling and Analysis of Random Access in Narrow-band Internet of Things, IEEE Internet of Things Journal, 5(3): 1485-1493, Jun, 2018.

发表/录用的会议论文

1. Zhikun Zhang, Tianhao Wang, Ninghui Li, Shibo He, Jiming Chen. CALM: Consistent Adaptive Local Marginal for Marginal Release under Local Differential Privacy, ACM CCS, 2018, Toronto, Canada.（CCF A 类会议）

2. Zhikun Zhang, Heng Zhang, Shibo He, Peng Cheng. Achieving Bilateral Utility Maximization and Location Privacy Preservation in Database-driven Cognitive Radio Networks, IEEE MASS, 2015, Dallas, USA.

3. Jiajun Zhang, Xiaohui Liang, Shibo He, Zhikun Zhang, Zhiguo Shi. Re-DPoctor: Real-time Health Data Releasing with w-day Differential Privacy, IEEE GLOBECOM, 2017, Singapore.

在投期刊论文

1. Zhikun Zhang, Shibo He, Mengyuan Zhang, Jiming Chen. LEPA: Incentivizing Long-term Privacy-perserving Data Aggregation in Crowdsensing, submitted to IEEE Transactions on Networking (TON)

二、参与的科研项目：

1. 国家自然科学基金面上项目：面向灾后救援的群智感知空间信息网络基础理论（No. 61672458）
2. 国家自然科学基金重点项目：车联网复杂移动环境感知与建模理论（No. 61731004）