计算机科学
COMPUTER SCIENCE

效用优化的本地差分隐私联合分布估计机制

尹诗玉, 朱友文, 张跃

引用本文

尹诗玉, 朱友文, 张跃. 效用优化的本地差分隐私联合分布估计机制[J]. 计算机科学, 2023, 50(10): 315-326.

YIN Shiyu, ZHU Youwen, ZHANG Yue. Utility-optimized Local Differential Privacy Joint Distribution Estimation Mechanisms [J]. Computer Science, 2023, 50(10): 315-326.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.221000053

效用优化的本地差分隐私联合分布估计机制

尹诗玉　朱友文　张　跃
南京航空航天大学计算机科学与技术学院　南京 211106
(shiyu.y@nuaa.edu.cn)

摘　要　相对于传统的中心化差分隐私,本地差分隐私(Local Differential Privacy,LDP)具有不依赖可信第三方等优势,但也存在数据效用较低的问题。效用优化本地差分隐私模型ULDP(Utility-Optimized Local Differential Privacy)利用不同输入的敏感度差异,可以提升估计结果的准确度。二维数据联合分布计算可广泛应用于众多数据分析场景,然而,如何在ULDP模型下实现二维数据联合分布估计,仍然是尚未解决的重要问题。针对这一问题,首先给出了二维ULDP模型的定义,兼顾了两个属性分别敏感与否的4种情况;其次,在该模型下,针对联合分布估计问题,提出了JuRR(Joint Utility-Optimized Randomized Response)与CPRR(Cartesian Product Randomized Response)2种机制,并理论证明了估计结果的无偏性;最后,在真实数据集上进行对比实验,讨论了不同参数对估计误差的影响。实验结果表明,所提2种机制具有更高的数据效用。

关键词:本地差分隐私;效用优化;联合分布;频率估计;敏感度差异
中图法分类号　TP309

Utility-optimized Local Differential Privacy Joint Distribution Estimation Mechanisms

YIN Shiyu,ZHU Youwen and ZHANG Yue
College of Computer Science and Technology,Nanjing University of Aeronautics and Astronautics,Nanjing 211106,China

Abstract　Compared with traditional centralized differential privacy,local differential privacy(LDP) has the advantage of not relying on trusted third parties,but it also has the problem of low data utility. The utility-optimized local differential privacy(ULDP) can improve the accuracy of estimation results by taking advantage of the sensitivity differences of different inputs. Two-dimensional data joint distribution calculation can be widely used in many data analysis scenarios. However,how to realize two-dimensional data joint distribution estimation under the ULDP model is still an important problem that has not yet been solved. Aiming at this problem,the definition of the two-dimensional ULDP model is given first,taking into account the four cases of whether the two attributes are sensitive or not. Secondly,under this model,for the joint distribution estimation problem,two mechanisms joint utility-optimized randomized response(JuRR) and cartesian product randomized response(CPRR) are proposed,and the unbiasedness of the estimation results is proved theoretically. Finally,comparative experiments are carried out on real datasets to discuss the influence of different parameters on the estimation error. Experimental results show that the proposed two mechanisms have better data utility.

Keywords　Local differential privacy,Utility-optimized,Joint distribution,Frequency estimation,Difference in sensitivity

1　引言

随着大数据的不断发展,数据的整合和挖掘越来越便利,与此同时用户信息安全问题成为关注的焦点。用户在APP上的浏览记录和位置信息等,都会被互联网存储、计算并集合成大数据。政府、企业以及相关研究人员都在利用这些数据,获取其中的有效知识信息。目前有3种常见的隐私保护技术:匿名化[1-3],安全多方计算[4],以及差分隐私[5-6]。为了更好地保护用户的个人信息,差分隐私已经成为隐私数据发布上的一个标准。它的保护效果以及易实施性得到了学术界以及工业界的广泛关注。中心化差分隐私要求用户将真实信息发送给数据收集者(可信第三方),然而现实生活中很少见可信的第三方,不可信的第三方可能会导致用户隐私信息的泄露,因此中心化差分隐私具有一定的局限性。在此基础上

到稿日期:2022-10-09　返修日期:2023-02-15
基金项目:国家重点研发计划(2020YFB1005900);国家自然科学基金(62172216);江苏省自然科学基金(BK20211180);广西密码学与信息安全重点实验室研究课题(GCIS202107)
This work was supported by the National Key Research and Development Program of China(2020YFB1005900),National Natural Science Foundation of China(62172216),Natural Science Foundation of Jiangsu Province,China(BK20211180) and Guangxi Key Laboratory of Cryptography and Information Security(GCIS202107).
通信作者:朱友文(zhuyw@nuaa.edu.cn)

发展出了本地差分隐私(LDP)[7]。LDP 不需要可信的第三方,用户在本地对数据进行扰动,将扰动后的数据再发给数据收集方,数据收集方利用接收到的这些扰动数据提取出所需的统计结果。常见的 2 种 LDP 频率估计协议是 GRR(Generalize Randomized Response)和 SUE(Symmetric Unary Encoding)[8],均值估计协议是 SR(Stochastic Rounding)[9]与 PM(Piecewise Mechanism)[10]。其他也有更多的学者对频率以及均值估计协议做了优化。目前,Google[11]、Apple[12]、华为[13]等公司都已经将 LDP 应用到信息保护领域。

目前很多学者的研究更聚焦于单值数据的处理,多维数据的分析要比单值数据更加具有挑战性。在实际应用中,用户大多会报告不止 1 条数据。例如,在朴素贝叶斯分类[14]等机器学习应用中会涉及条件概率以及二维联合分布的估计,这时如果简单地将一维数据的机制运用至二维或多维场景下,就需要对隐私预算进行划分,我们将这种机制称作 TDRR(Two Dimention Randomized Response)。TDRR 中每个属性获得的隐私预算较少,造成保护强度过高以及数据效用性过低。因此,研究二维数据的联合分布估计问题显得尤为重要。

目前,LDP 已经被应用于估计隐私数据的分布等问题。关于联合分布估计的相关工作,已有的研究包括 Yilmaz 等[14]将二维属性通过运算转变为一维数据,采用已有的 LDP 频率估计方案进行估计。实验结果表明,使用 GRR 进行估计时效果最佳。

LDP 不需要可信的第三方,然而,它认为所有的个人数据都同样敏感,这会导致部分数据被过度保护,从而导致数据效用过低。例如,在询问用户是否患有某些疾病时,“艾滋”“癌症”这些回答显然比“感冒”更为敏感。这时如果再采用 LDP 的扰动机制对数据进行扰动,则容易造成对敏感数据的保护力度不够,或者是对非敏感数据保护过度。为了解决这一问题,Murakami 等提出了效用优化本地差分隐私(Utility-optimized Local Differential Privacy, ULDP)[15]的概念,它只对敏感数据提供了 ε-LDP 的隐私保障。ULDP 对敏感数据仍然利用满足 LDP 的扰动机制,从而保证对敏感数据的保护力度不变;而对于非敏感数据,则是以较高的概率保持自身不变,否则扰动到保护输出域中的任一值,从而在一定程度上降低对非敏感数据的保护力度,提高整体的数据效用。ULDP 实际上是 LDP 的一个优化,其对敏感数据和非敏感数据使用不同的扰动方式,更适用于非敏感数据较多的情况,在保证敏感数据安全的同时,解决了 LDP 数据效用低的问题。

然而目前在 ULDP 模型下,还未涉及对二维联合分布的估计问题,已有的研究仅针对单值数据,也就是每个用户只报告 1 个属性,已有的方案有 uRR(Utility-Optimized Randomized Response)和 uRAPPOR(Utility-Optimized Randomized Aggregatable Privacy-preserving Ordinal Response)[15]。然而在实际应用中,用户大多会报告不止 1 条数据,这时研究 ULDP 模型下的二维联合分布估计具有重要意义。

为了解决上述多维数据统计问题,本文立足于二维数据,提出了二维数据的 ULDP 模型,并且基于模型定义以及联合分布估计这一待解决问题提出了 JuRR(Joint Utility-Optimized Randomized Response)和 CPRR(Cartesian Product Randomized Response)两种机制。本文的研究在未来还可以扩展到更高维的问题中。

本文的主要贡献包括 3 个方面:

1)针对一维 ULDP 模型的局限性,提出了二维数据下的效用优化本地差分隐私模型,并给出了模型的具体定义。

2)设计了 2 种效用优化的本地差分隐私联合分布估计机制 JuRR 及 CPRR,并且证明了估计结果的无偏性,计算了理论方差,同时给出了其应用领域。

3)通过在不同数据集上分别选取不同的特征与类标签组成二维数据进行对比实验,使用欧氏距离作为误差的衡量指标。对比了不同参数取值下误差的数值,由实验结果不难发现,所提 2 种机制中效果最好的是 CPRR,其与已有的 JD_GRR 以及利用一维 ULDP 模型的 TDRR 机制相比,在相同隐私保护强度下,误差最多可降低 1/2 左右。因此,文中所提机制可以有效提高估计的准确度以及数据效用,同时没有过多增加运行时间。

本文第 2 章为相关工作;第 3 章介绍了差分隐私等预备知识;第 4 章给出了二维 ULDP 模型的具体定义以及该模型下所研究的联合分布估计问题;第 5 章主要阐述了所提出的 2 种效用优化的本地差分隐私联合分布估计机制;第 6 章对机制的期望与方差进行了理论分析;第 7 章在真实数据集上进行对比实验,验证了上述机制的有效性。

2 相关工作

Dwork 在 2006 年提出的差分隐私(Differential Privacy, DP)[5]概念,又被称作中心化差分隐私,主要用于保护攻击者具有强大背景知识时的个人隐私数据。DP 用数学语言进行严格的定义,最大的一个特点就是可以对保护程度进行量化,其中隐私预算 ε 是较为重要的一个参数。通常情况下,隐私预算的取值越小,表示保护强度越高,对应的数据效用也就越差。目前,差分隐私已经逐渐作为数据隐私保护的实施标准,然而实际的应用却很少,因为 DP 需要一个可信的数据收集方,而现实生活中可信的数据收集方并不常见。在此基础上,LDP[7]被提出,其将用户视为可信界的边缘。通用操作步骤是,每个用户自己在本地对隐私数据进行扰动,然后将噪声值提交给数据收集方,数据收集方再通过统计聚合等操作对频率和均值等进行估计。这样可以保证数据收集方获得的是扰动后的噪声数据,不会造成对用户隐私数据的泄露。LDP 目前的研究问题主要分为以下几种:频率估计[8,16]、频繁项挖掘[17]、均值估计[9-10,18]、边缘发布[19]、键值对数据中 key 的频率与 key 所对应的 value 的均值估计[20-22]等。如今,差分隐私更多地被应用在轨迹发布[23]等问题中。由于 DP 与 LDP 的隐私保护程度与数据效用之间难以平衡,混洗差分隐私模型(Shuffled Differential Privacy, SDP)[24]被提出。该模型在用户与数据收集方之间加入 Shuffler,使得用户与数据之间的关联关系被打乱。陆续也有学者在 SDP 模型下研究多维数据的频率估计[25]等问题。

LDP 模型中,将用户所有的数据取值都视为敏感的,也就是用相同的隐私保护力度对用户的数据进行扰动,这忽略了隐私保护等级的差别。然而实际数据中取值的敏感性往往

不同，有的是敏感的，有的是非敏感的。为了满足不同的隐私保护需求，提高数据效用，ULDP[15]被提出。该模型按照隐私保护程度不同等级的需求，将数据划分为敏感和非敏感2个部分，并针对不同的部分设计不同的扰动算法，从而在不降低对敏感区域保护力度的同时，又不会对非敏感部分产生过保护的现象，进一步提高了数据估计的准确度。通过对数据隐私保护等级进行进一步划分，Gu等提出了输入可区分的本地差分隐私模型ID-LDP(Input-Discriminative Protection for Local Differential Privacy)[26]，用户可以自定义隐私数据的保护等级，实现了更细粒度的保护。

针对联合分布，目前相关工作可总结为表1所列，文献[14]是基于LDP模型的工作，其将二维数据通过运算转换为一维数据后使用LDP频率估计方案进行估计。目前针对ULDP模型下的研究，文献[15]更多地集中在一维数据，Murakami等基于GRR和SUE提出了uRR和uRAP[15]机制。但目前对ULDP下的二维联合分布估计的研究仍然还是空白。对于二维数据的联合分布，我们可以考虑采用ULDP现有的一维频率估计的方案，即将2个属性分开考虑，利用uRR或者uRAP机制估计频率后，将各维频率相乘即可得到联合分布的取值。但是这种处理方法需要对隐私预算进行划分，目前使用最多的处理方法是将隐私预算均分，从而保证二维数据整体的隐私预算为ε，那么每一维属性获得的隐私预算就会变少，可能会导致准确度以及数据效用的降低。目前的机制均无法很好地解决二维数据联合分布这一问题。因此，本文提出的可用于估计联合分布的二维ULDP模型是非常有必要的；并且文中设计了两种具体的机制JuRR与CPRR，同时通过理论以及实验验证了其效用。

表1 相关工作总结

Table 1 Summary of related works

文献	总结
文献[14]	LDP模型下的工作，LDP将属性的所有取值都视为敏感的，在属性存在非敏感取值时并不适用，会导致过保护，降低数据效用
文献[15]	首先，如果将该文献的频率估计方案用于联合分布，需要对隐私预算进行划分，从而降低每个属性可获得的隐私预算，数据效用也随之降低；其次，如果将2个属性分开进行扰动，会忽略2个属性之间的相关性

3 预备知识

3.1 本地差分隐私

在本地差分隐私模型中，首先，用户会在本地独立地扰动自己的数据。每个用户都是可信边界的边缘。然后，用户将扰动后的噪声数据报告给不可信的数据收集方。最后，数据收集方对数据进行统计分析，并发布分析结果。

定义1(ε-LDP)[6] 有一个输入域为X、输出域为W的数据扰动算法$\mathcal{A}$满足ε-LDP，当且仅当对于任意输入x_1，$x_2\in X$得到任意输出$w\in W$的概率满足式(1)：

$$Pr[\mathcal{A}(x_1)=w]\leqslant e^{\varepsilon}Pr[\mathcal{A}(x_2)=w] \tag{1}$$

直观来看，本地差分隐私的定义保证了数据收集方很难根据扰动之后的结果推断出原始的输入值，从而起到了保护隐私数据的作用。定义中的ε被称作隐私预算。隐私预算的取值越大，表明保护效果越差，但与此同时也会伴随着数据效用的提升。因此，如何在保护力度和数据效用之间寻得一个平衡点，是在实际应用中需要考虑的问题。

3.2 效用优化本地差分隐私

在ULDP模型中，数据也是用户自己在本地进行扰动的，其与LDP的不同之处在于，ULDP将数据初始划分为了敏感数据域X_S和非敏感数据域X_N两部分，扰动结果被划分为保护数据域W_P和可逆数据域W_I两部分。ULDP的形式化定义如定义2所示。

定义2((X_S,W_P,ε)-ULDP)[15] 给定$X_S\subseteq X$，$W_P\subseteq W$，$\varepsilon>0$，对于输入域为X，输出域为W的数据扰动算法$\mathcal{A}:X\to W$，该数据扰动算法$\mathcal{A}$满足(X_S,W_P,ε)-ULDP模型的定义，当且仅当满足下列两条性质：

1)对于任意$w\in W_I$，有且仅有一个$x\in X_N$满足不等式(2)：

$$Pr[\mathcal{A}(x)=w]>0 \tag{2}$$

且对于任意$x'\neq x$，均满足式(3)：

$$Pr[\mathcal{A}(x')=w]=0 \tag{3}$$

2)对于任意$x_1,x_2\in X$，任意$w\in W_P$，其均满足不等式(4)：

$$Pr[\mathcal{A}(x_1)=w]\leqslant e^{\varepsilon}Pr[\mathcal{A}(x_2)=w] \tag{4}$$

直观来看，ULDP就是对于敏感数据仍然利用满足LDP的扰动机制，从而保证对敏感数据的保护力度相同，仍然满足ε-LDP；而对于非敏感数据，则是以较高的概率扰动到可逆输出域，否则扰动到保护输出域中的任一值，从而在一定程度上降低对非敏感数据的保护力度，提高整体的数据效用。

4 模型定义及问题描述

由于一维效用优化本地差分隐私模型的局限性，本章首先提出了可用于二维数据的效用优化本地差分隐私模型，其次介绍了在该模型下所要研究与解决的问题。

4.1 二维数据的ULDP模型

目前Murakami等提出的效用优化本地差分隐私(ULDP)[15]模型，仅适用于用户只报告一个隐私数据的情况。首先，在用户拥有二维数据并且数据的隐私保护等级包含敏感和非敏感两种情况时，就有可能会出现用户其中一个属性是敏感的取值而另一个属性在非敏感的取值域的情形，这时一维ULDP模型无法直接应用；其次，对于二维数据，如果尝试将其拆分开，用一维数据的模型分别进行估计，就需要将隐私预算进行划分，这时每一个属性获得的隐私预算的取值为$\varepsilon/2$，而隐私预算降低可能会导致过保护的现象，使得数据可用性也随之降低。因此，对于二维数据，需要提出一个新的模型用于联合分布的估计。文中提出的可用于二维数据的ULDP模型，兼顾了两个属性分别敏感与否的4种情况。

在该模型中，用户报告二维类别型数据(x,y)，其中x的输入域分为敏感部分X_S和非敏感部分X_N，相对应的输出域为保护输出域W_P和可逆输出域W_I；y的输入域也分为敏感部分Y_S和非敏感部分Y_N，相对应输出与也分为V_P和V_I。二维ULDP模型的定义如图1所示。

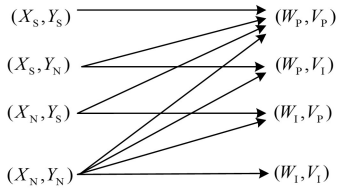


图 1 二维 ULDP 模型图

Fig. 1 Two-dimensional ULDP model

定义 3((X,Y,W,V,ε)-ULDP) 给定 $X_S,X_N\subseteq X;Y_S,Y_N\subseteq Y;W_P,W_I\subseteq W;V_P,V_I\subseteq V$。对于输入域为 X,Y,输出域为 W,V 的数据扰动算法 $\mathcal{A}:(X,Y)\to(W,V)$,其满足$(X,Y,W,V,\varepsilon)$-ULDP 模型的定义,当且仅当满足以下 6 条性质:

1) $\forall(\tilde{x},\tilde{y})\in(W_P,V_P)$ 且 $(x_0,y_0),(x_0',y_0')\in(X_S\cup X_N,Y_S\cup Y_N)$,对于任意的 $(x_0,y_0)\neq(x_0',y_0')$,满足不等式(5):

$$\frac{Pr[(\tilde{x},\tilde{y})|(x_0,y_0)]}{Pr[(\tilde{x},\tilde{y})|(x_0',y_0')]}\leqslant e^{\varepsilon} \tag{5}$$

其中,ε 为隐私预算。

2) $\forall(*,\tilde{y})\in(W_P,V_I)$,有且仅有一个 y_0,$(*,y_0),(*,y_0')\in(X_S\cup X_N,Y_N)$,对于任意的 $y_0\neq y_0'$,满足式(6):

$$Pr[(*,\tilde{y})|(*,y_0)]>0,Pr[(*,\tilde{y})|(*,y_0')]=0 \tag{6}$$

3) $\forall(\tilde{x},\tilde{y})\in(W_P,V_I)$,对于一个给定的 y_0,$(x,y_0),(x',y_0)\in(X_S\cup X_N,Y_N)$,对于任意的 $x\neq x'$,有不等式(7):

$$\frac{Pr[(\tilde{x},\tilde{y})|(x,y_0)]}{Pr[(\tilde{x},\tilde{y})|(x',y_0)]}\leqslant e^{\varepsilon} \tag{7}$$

4) $\forall(\tilde{x},*)\in(W_I,V_P)$,有且仅有一个 x_0,$(x_0,*),(x_0',*)\in(X_N,Y_S\cup Y_N)$,对于任意的 $x_0\neq x_0'$,满足式(8):

$$Pr[(\tilde{x},*)|(x_0,*)]>0,Pr[(\tilde{x},*)|(x_0',*)]=0 \tag{8}$$

5) $\forall(\tilde{x},\tilde{y})\in(W_I,V_P)$,对于一个给定的 x_0,$(x_0,y),(x_0,y')\in(X_N,Y_S\cup Y_N)$,对于任意的 $y\neq y'$,有不等式(9):

$$\frac{Pr[(\tilde{x},\tilde{y})|(x_0,y)]}{Pr[(\tilde{x},\tilde{y})|(x_0,y')]}\leqslant e^{\varepsilon} \tag{9}$$

6) $\forall(\tilde{x},\tilde{y})\in(W_I,V_I)$,有且仅有一个$(x_0,y_0)$,对于$(x_0,y_0),(x_0',y_0')\in(X_N,Y_N)$,任意的$(x_0,y_0)\neq(x_0',y_0')$,满足式(10):

$$Pr[(\tilde{x},\tilde{y})|(x_0,y_0)]>0,Pr[(\tilde{x},\tilde{y})|(x_0',y_0')]=0 \tag{10}$$

该定义中的条件 1)保证了(x,y)整体满足 ε-LDP 的定义;条件 2)与 3)则保证了对非敏感 Y_N 部分的扰动结果是可逆的,同时对敏感 X_S 部分的保护效果不降低,仍然满足 ε-LDP;条件 4)与 5)保证了对非敏感 X_N 部分的扰动结果是可逆的,同时对敏感 Y_S 部分的保护效果不降低,仍然满足 ε-LDP;条件 6)则保证了对 x,y 的非敏感部分的扰动结果都是可逆的。对于一个二维数据,需要同时满足以上 6 个条件才可认为其满足(X,Y,W,V,ε)-ULDP 模型的定义。

4.2 问题描述及符号表示

在实际应用中,用户往往不只是报告单值数据,而目前对 ULDP 模型的研究均立足于单值数据的频率估计。基于此,本文考虑用户报告二维类别型数据,在二维数据的效用优化本地差分隐私(X,Y,W,V,ε)-ULDP 模型下所要解决的问题是二维数据的联合分布估计。

本文所研究的模型如图 2 所示,模型中包含两方,分别是用户和数据收集方。图 2 中只有中间部分是用户进行的操作。模型中有 N 个用户,每个人拥有真实二维类别型隐私数据(x,y),二维数据的取值集合记为 X,Y,取值域大小相应为 $|X|,|Y|$;数据收集方将原始数据划分为敏感部分 X_S,Y_S 与非敏感部分 X_N,Y_N,并且设置了隐私保护的等级,二维数据需要满足的隐私预算记为 ε;每个用户根据不同的隐私保护要求在本地对自己的真实数据进行编码扰动,扰动后的输出域记作保护域 W_P,V_P 与可逆域 W_I,V_I;用户将扰动后的二维数据噪声值$(\tilde{x},\tilde{y})$发送至数据收集方,数据收集方经过聚合与统计分析后,估计出联合分布的取值 $\hat{f}_{ij}$,下标 i,j 分别表示的是 x,y 二维数据的取值所对应的索引。

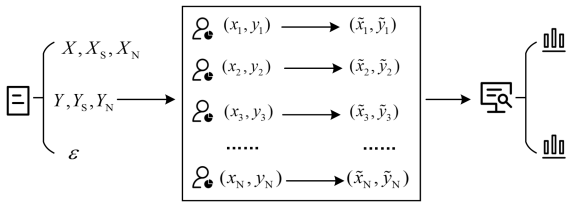


图 2 系统模型图

Fig. 2 System model

每个用户从多个特征中随机采样 1 个特征与类标签组成二维数据,即可对联合分布进行估计。获得联合分布的估计值后,针对其中任一维数据的边缘分布,可以通过对联合分布进行求和得到。对数据集进行划分,80%的数据用于训练分类器,20%的用于估计。后续可将该机制应用于朴素贝叶斯分类等机器学习问题中。

本文中涉及的重要符号描述如表 2 所列。

表 2 符号描述

Table 2 Symbol description

符号	说明
ε	隐私预算
(x,y)	用户真实的二维类别型隐私数据
$(\tilde{x},\tilde{y})$	用户扰动后的二维类别型隐私数据
X_S	数据 x 的敏感输入域
X_N	数据 x 的非敏感输入域
Y_S	数据 y 的敏感输入域
Y_N	数据 y 的非敏感输入域
N	总用户数量
$\hat{f}_{ij}$	$x=i,y=j$ 的联合分布估计值
f_{ij}^{*}	$x=i,y=j$ 的联合分布真实值
W_P	数据 x 的保护输出域
W_I	数据 x 的可逆输出域
V_P	数据 y 的保护输出域
V_I	数据 y 的可逆输出域

5 效用优化的本地差分隐私联合分布估计机制

第 4 章中提出了二维 ULDP 模型的定义,为了实现二维联合分布的估计,本章设计了两种具体的实现机制。这两种实现机制均包含数据扰动以及数据估计两个部分。

5.1 JuRR 机制

JuRR 机制包含数据扰动以及数据估计两个过程,其中数据扰动过程是用户自己在本地进行的,而数据估计部分则是由数据收集方根据用户提交的噪声数据进行统计分析。

5.1.1 数据扰动

在两个属性的情况下，假设 x 的敏感输入域为 $X_S=\{x_1,x_2\}$，非敏感输入域为 $X_N=\{x_3,x_4,x_5\}$，同理 y 的敏感输入域与非敏感输入域分别为 $Y_S=\{y_1,y_2\}$，$Y_N=\{y_3,y_4,y_5\}$；在 ULDP 模型中，通常将输出域视为与输入域相同，x 的保护输出域为 $W_P=X_S$，可逆输出域为 $W_I=X_N$，y 的保护与可逆输出域同理，$V_P=Y_S$，$V_I=Y_N$。根据定义 3，我们设计了 JuRR 的扰动算法 1。

算法 1 JuRR 扰动算法

输入：$X_S,X_N,Y_S,Y_N,(x,y),\varepsilon,W_P,W_I,V_P,V_I$

输出：$(\tilde{x},\tilde{y})$

1. if $x\in X_S$ and $y\in Y_S$，扰动过程如式(11)所示：

$$\Pr[(\tilde{x},\tilde{y})|(x,y)]=\begin{cases}a, & \text{if}(\tilde{x},\tilde{y})=(x,y)\\ b, & \text{if}(\tilde{x},\tilde{y})=(W_P,V_P)\backslash(x,y)\end{cases}\tag{11}$$

2. else if $x\in X_S$ and $y\in Y_N$，扰动概率为：

$$\Pr[(\tilde{x},\tilde{y})|(x,y)]=\begin{cases}b, & \text{if } (\tilde{x},\tilde{y})\in(W_P,V_P)\\ p, & \text{if } (\tilde{x},\tilde{y})=(x,y)\\ q, & \text{if } (\tilde{x},\tilde{y})\in(W_P,V_I)\backslash(x,y)\\ & \text{and } \tilde{y}=y\end{cases}\tag{12}$$

3. else if $x\in X_N$ and $y\in Y_S$，可按照式(13)的概率进行扰动：

$$\Pr[(\tilde{x},\tilde{y})|(x,y)]=\begin{cases}b, & \text{if } (\tilde{x},\tilde{y})\in(W_P,V_P)\\ m, & \text{if } (\tilde{x},\tilde{y})=(x,y)\\ n, & if\ (\tilde{x},\tilde{y})\in(W_I,V_P)\backslash(x,y)\\ & \text{and } \tilde{x}=x\end{cases}\tag{13}$$

4. else

$$\Pr[(\tilde{x},\tilde{y})|(x,y)]=\begin{cases}b, & \text{if } (\tilde{x},\tilde{y})\in(W_P,V_P)\\ q, & \text{if } (\tilde{x},\tilde{y})=(W_P,V_I) \text{ and } \tilde{y}=y\\ n, & \text{if } (\tilde{x},\tilde{y})\in(W_I,V_P) \text{ and } \tilde{x}=x\\ t, & \text{if } (\tilde{x},\tilde{y})=(x,y)\end{cases}\tag{14}$$

5. end if

6. 输出扰动后的二维数据$(\tilde{x},\tilde{y})$。

JuRR 的扰动算法中，首先需要判断二维数据(x,y)在哪一个取值域中。若在(X_S,Y_S)中，就以 a 的概率保持自身不变，否则扰动至(W_P,V_P)中除自身外的任一值；若取值在(X_S,Y_N)中，则以 p 的概率保持自身不变，以 b 的概率扰动至保护输出域(W_P,V_P)中的任一值，否则以 q 的概率扰动至(W_P,V_I)中除自身外的任一值，且要保证 y 的值不变；若输入值在(X_N,Y_S)中，以 m 的概率保持不变，以 b 的概率扰动至保护输出域(W_P,V_P)中的任一值，否则以 n 的概率扰动至(W_I,V_P)中除自身外的任一值，且要保证 x 的取值不变；对于输入域在(X_N,Y_N)的数据，以 t 的概率保持不变，以 b 的概率扰动至(W_P,V_P)，以 q 的概率扰动至(W_P,V_I)且保证 y 的值不变，以 n 的概率扰动至(W_I,V_P)时需要保证 x 的值可逆。其中各个参数的取值为：

$$a=\frac{e^{\varepsilon}}{e^{\varepsilon}+|Y_S||X_S|-1},b=\frac{1}{e^{\varepsilon}+|Y_S||X_S|-1}\tag{15}$$

$$p=\frac{e^{2\varepsilon}-e^{\varepsilon}}{(e^{\varepsilon}+|Y_S||X_S|-1)(e^{\varepsilon}+|X_S|-1)}\tag{16}$$

$$q=\frac{e^{\varepsilon}-1}{(e^{\varepsilon}+|Y_S||X_S|-1)(e^{\varepsilon}+|X_S|-1)}\tag{17}$$

$$m=\frac{e^{2\varepsilon}-e^{\varepsilon}}{(e^{\varepsilon}+|Y_S||X_S|-1)(e^{\varepsilon}+|Y_S|-1)}\tag{18}$$

$$n=\frac{e^{\varepsilon}-1}{(e^{\varepsilon}+|Y_S||X_S|-1)(e^{\varepsilon}+|Y_S|-1)}\tag{19}$$

$$t=1-|Y_S||X_S|b-|X_S|q-|Y_S|n\tag{20}$$

为了保证该方案中概率 t 的取值大于 0，经过计算，JuRR 的使用需要满足不等式(21)的限制。

$$|X_S||Y_S|<(e^{\varepsilon}-1)^2\tag{21}$$

5.1.2 数据估计

用户通过数据扰动步骤，在本地将自己的隐私数据加以扰动后提交给数据收集方，数据收集方收集到所有用户的噪声数据后开始统计分析，从而完成数据估计的步骤。我们可以对 4 个联合取值域分别进行联合分布的估计。

1)输出在(W_P,V_P)部分，根据扰动过程可以得到式(22)，其中 c_{ij}^* 表示的是二维数据的真实频数，$\tilde{c}_{ij}$ 为经验频数。

$$ac_{ij}^*+(N-c_{ij}^*)b=\tilde{c}_{ij}\tag{22}$$

因此联合分布可以用式(23)进行估计：

$$\hat{f}_{ij}=\frac{\frac{\tilde{c}_{ij}}{N}-b}{a-b}\tag{23}$$

2)输出在(W_I,V_I)部分，由于在该输出域中的 x,y 都要满足可逆的条件，所以有：

$$tc_{ij}^*=\tilde{c}_{ij}\tag{24}$$

联合分布的估计如式(25)所示：

$$\hat{f}_{ij}=\frac{\tilde{c}_{ij}}{Nt}\tag{25}$$

3)输出在(W_P,V_I)部分，可以根据扰动过程建立线性方程组(26)：

$$\begin{cases}c_{1j}^*p+c_{2j}^*q+c_{3j}^*q+\cdots+c_{|X_S|j}^*q=\tilde{c}_{1j}-\frac{q}{t}S_{Nx}\\ c_{1j}^*q+c_{2j}^*p+c_{3j}^*q+\cdots+c_{|X_S|j}^*q=\tilde{c}_{2j}-\frac{q}{t}S_{Nx}\\ c_{1j}^*q+c_{2j}^*q+c_{3j}^*p+\cdots+c_{|X_S|j}^*q=\tilde{c}_{3j}-\frac{q}{t}S_{Nx}\\ \quad\vdots\\ c_{1j}^*q+c_{2j}^*q+c_{3j}^*q+\cdots+c_{|X_S|j}^*p=\tilde{c}_{|X_S|j}-\frac{q}{t}S_{Nx}\end{cases}\tag{26}$$

为了求解这个线性方程组，需要对它的增广矩阵进行初等行变换。该方程组有且仅有一个解，最终可以得到联合分布的估计式(27)。

$$\hat{f}_{ij}=\frac{\frac{\tilde{c}_{ij}}{N}-\frac{q}{tN}S_{Nx}-\left(\frac{S_{Sx}}{N}-\frac{q}{tN}S_{Nx}|X_S|\right)\frac{q}{p+(|X_S|-1)q}}{p-q}\tag{27}$$

其中：

$$S_{Sx}=\tilde{c}_{1j}+\tilde{c}_{2j}+\cdots+\tilde{c}_{|X_S|j}\tag{28}$$

$$S_{Nx}=\tilde{c}_{|X_S|+1,j}+\tilde{c}_{|X_S|+2,j}+\cdots+\tilde{c}_{|X_N|j}\tag{29}$$

4)输出在(W_I,V_P)部分，可以类比 3)中(W_P,V_I)部分进行分析，最终同样可以得到联合分布的估计公式(30)。

$$\hat{f}_{ij}=\frac{\frac{\tilde{c}_{ij}}{N}-\frac{q}{tN}S_{Ny}-\left(\frac{S_{Sy}}{N}-\frac{n}{tN}S_{Ny}|Y_S\right)\frac{n}{m+(|Y_S|-1)n}}{m-n}\tag{30}$$

其中：

$$S_{Sy}=\tilde{c}_{i1}+\tilde{c}_{i2}+\cdots+\tilde{c}_{i|Y_S|} \tag{31}$$

$$S_{Ny}=\tilde{c}_{i,|Y_S|+1}+\tilde{c}_{i,|Y_S|+2}+\cdots+\tilde{c}_{i|Y_N|} \tag{32}$$

根据上面的推导，JuRR 的估计过程可总结为算法 2。

算法 2 JuRR 估计算法

输入：总用户个数 N，所有用户的扰动值集合 $S_{(\tilde{x},\tilde{y})}$，扰动后的输出域 W_P, W_I, V_P, V_I

输出：联合分布估计值 $\hat{f}_{ij}$

1. for i=1 to $|X_S|$
2. for j=1 to $|Y_S|$
3. 根据 $S_{(\tilde{x},\tilde{y})}$ 统计出经验频数 $\tilde{c}_{ij}$
4. if $\tilde{x}\in W_P$ and $\tilde{y}\in V_P$
5. 联合分布估计公式为 $\hat{f}_{ij}=\frac{\tilde{c}_{ij}}{Nt}$
6. else if $\tilde{x}\in W_I$ and $\tilde{y}\in V_I$
7. 联合分布的估计公式为 $\hat{f}_{ij}=\frac{\tilde{c}_{ij}}{Nt}$
8. else if $\tilde{x}\in W_P$ and $\tilde{y}\in V_I$
9. 联合分布的估计公式为

$$\hat{f}_{ij}=\frac{\frac{\tilde{c}_{ij}}{N}-\frac{q}{tN}S_{Nx}-\left(\frac{S_{Sx}}{N}-\frac{q}{tN}S_{Nx}|X_S|\right)\frac{q}{p+(|X_S|-1)q}}{p-q}$$

10. else
11. 联合分布的估计公式为

$$\hat{f}_{ij}=\frac{\frac{\tilde{c}_{ij}}{N}-\frac{q}{tN}S_{Ny}-\left(\frac{S_{Sy}}{N}-\frac{n}{tN}S_{Ny}|Y_S|\right)\frac{n}{m+(|Y_S|-1)n}}{m-n}$$

12. 输出联合分布估计值 $\hat{f}_{ij}$

5.2 CPRR 机制

JuRR 机制中，我们考虑了二维属性中每一维都敏感与否共 4 种情况，之后对敏感与非敏感部分采用不同的方式进行扰动。JuRR 机制是基于 ULDP 提出的，由于 ULDP 将属性的取值分为敏感与非敏感两部分，核心是优化非敏感部分的扰动，非敏感部分以较高的概率保持不变，这一概率就是 JuRR 机制中的概率参数 t，否则扰动到保护输出域中的任一值。然而在 JuRR 机制中，这一概率可能会很小，因此会导致效果降低。分析其原因，可能是因为在 JuRR 中将扰动区域划分得较细，每部分的扰动都需消耗一部分概率。

综上考虑，我们进一步提出了 CPRR 机制。在 CPRR 机制中，将只要有一个属性是敏感取值就都视为敏感部分，虽然我们对取值域进行了粗化，但由于仅考虑了二维数据，维度较少，因此对准确度的影响不大。采用这种方式，可以提高非敏感部分扰动至本身的概率，从而比 JuRR 的效用更优。CPRR 机制同样包含数据扰动以及数据估计两个过程，其中数据扰动过程由用户端在本地完成，数据估计过程则由数据收集方完成。

5.2.1 数据扰动

CPRR 机制将 (X_S,Y_S)，(X_S,Y_N)，(X_N,Y_S) 这 3 部分均视作敏感域，记作 S，放在一起进行扰动，扰动后的输出域记作 S'，那么 $S'=(W_P,V_P)\cup(W_P,V_I)\cup(W_I,V_P)$。这里仅将 (X_N,Y_N) 部分视作非敏感的，对应的输出域为 (W_I,V_I)。两个属性的敏感输入域大小记作 $|X_S|$，$|Y_S|$。CPRR 扰动过程如算法 3 所示。

算法 3 CPRR 扰动算法

输入：S，S′，$|X_S|$，$|Y_S|$，(x,y)，ε

输出：$(\tilde{x},\tilde{y})$

1. if $(x,y)\in S$
2. 扰动概率如式(33)所示：

$$\Pr[(\tilde{x},\tilde{y})|(x,y)]=\begin{cases}a', & if\ (\tilde{x},\tilde{y})=(x,y)\\ b', & \text{if } (\tilde{x},\tilde{y})=S'\backslash(x,y)\end{cases} \tag{33}$$

3. else
4. 按照式(34)进行扰动：

$$\Pr[(\tilde{x},\tilde{y})|(x,y)]=\begin{cases}t', & \text{if}(\tilde{x},\tilde{y})=(x,y)\\ b', & \text{if } (\tilde{x},\tilde{y})\in S'\end{cases} \tag{34}$$

5. end if
6. 输出扰动后的二维数据 $(\tilde{x},\tilde{y})$。

在 CPRR 的扰动过程中，由于将输入域进行了简化，因此只用考虑两种情况。如果用户输入的数据 (x,y) 在集合 S 中，那么就以 a' 的概率保持自身不变，否则扰动至保护输出域 S' 中除自身外的其他任意一个值；如果用户输入的数据 (x,y) 不在集合 S 中，那么就以 t' 的概率扰动为自身，否则以 b' 的概率扰动至保护输出域 S' 中的任意一个值。

令 $d=|Y_S||X_S|+|Y_N||X_S|+|Y_S||X_N|$，参数取值如式(35)所示：

$$a'=\frac{e^{\varepsilon}}{e^{\varepsilon}+d-1},b'=\frac{1}{e^{\varepsilon}+d-1},t'=\frac{e^{\varepsilon}-1}{e^{\varepsilon}+d-1} \tag{35}$$

5.2.2 数据估计

同理，对于 CPRR 机制，可以利用式(37)和式(39)对联合分布进行估计。算法 4 是详细的估计过程。

1)输出在 S' 的部分，根据扰动过程可以得到式(36)：

$$a'c_{ij}^{*}+(N-c_{ij}^{*})b'=\tilde{c}_{ij} \tag{36}$$

因此联合分布可以用式(37)进行估计：

$$\hat{f}_{ij}=\frac{\tilde{c}_{ij}/N-b'}{a'-b'} \tag{37}$$

2)输出在 (W_I,V_I) 的部分，由于该输出域中的 x,y 都要满足可逆的条件，因此有：

$$t'c_{ij}^{*}=\tilde{c}_{ij} \tag{38}$$

联合分布的估计公式为：

$$\hat{f}_{ij}=\frac{\tilde{c}_{ij}/N}{t'} \tag{39}$$

算法 4 CPRR 估计算法

输入：总用户个数 N，所有用户的扰动值集合 $S_{(\tilde{x},\tilde{y})}$，扰动后的保护输出域 S′，可逆输出域 (W_I,V_I)

输出：联合分布估计值 $\hat{f}_{ij}$

1. for i=1 to $|X_S|$
2. for j=1 to $|Y_S|$
3. 根据 $S_{(\tilde{x},\tilde{y})}$ 统计出经验频数 $\tilde{c}_{ij}$
4. if $(\tilde{x},\tilde{y})\in S'$
5. 联合分布估计公式为 $\hat{f}_{ij}=\frac{\tilde{c}_{ij}/N-b'}{a'-b'}$
6. else
7. 联合分布估计公式为 $\hat{f}_{ij}=\frac{\tilde{c}_{ij}}{Nt}$
8. 输出联合分布的估计值 $\hat{f}_{ij}$

6 理论分析

6.1 隐私保护效果证明

推论 1 JuRR 机制满足(X,Y,W,V,ε)-ULDP 模型的定义。

证明：根据定义 3 中(X,Y,W,V,ε)-ULDP 的要求，可以将推论 1 转化为证明以下条件：1）输入域为$(X_S\cup X_N,Y_S\cup Y_N)$扰动至输出域$(W_P,V_P)$时，$(x,y)$整体需满足 ε-LDP；2）输入域$(X_S\cup X_N,Y_N)$扰动至$(W_P,V_I)$的部分，$y$ 的扰动过程是可逆的，而 x 仍然满足 ε-LDP；3）输入域在$(X_N,Y_S\cup Y_N)$且输出域在(W_I,V_P)的部分，x 的扰动过程是可逆的，而 y 仍然满足 ε-LDP；4）从(X_N,Y_N)扰动至(W_I,V_I)时，x,y 的扰动均是可逆的。我们将按照顺序分别对上述 4 条进行证明：

1）对于任意不同的输入$(x_0,y_0),(x_0',y_0')\in(X_S\cup X_N,Y_S\cup Y_N)$，将其扰动至任意同一输出$(\tilde{x},\tilde{y})\in(W_P,V_P)$的概率比值可以表示为：

$$\frac{Pr[(\tilde{x},\tilde{y})|(x_0,y_0)]}{Pr[(\tilde{x},\tilde{y})|(x_0',y_0')]}=\frac{a}{b}=\frac{\dfrac{e^{\varepsilon}}{e^{\varepsilon}+|Y_S||X|-1}}{\dfrac{1}{e^{\varepsilon}+|Y_S||X|-1}}=e^{\varepsilon}\quad(40)$$

2）根据 5.1 节中的式(12)及式(14)可知，y 的扰动显然是可逆的；对于给定的 $y_0\in Y_N$，x 的任意两个不同输入$(x,y_0),(x',y_0)\in(X_S\cup X_N,Y_N)$，扰动至同一输出$(\tilde{x},\tilde{y})\in(W_P,V_I)$的概率比为：

$$\frac{Pr[(\tilde{x},\tilde{y})|(x,y_0)]}{Pr[(\tilde{x},\tilde{y})|(x',y_0)]}=\frac{p}{q}=\frac{\dfrac{e^{2\varepsilon}-e^{\varepsilon}}{(e^{\varepsilon}+|Y_S||X_S|-1)(e^{\varepsilon}+|X_S|-1)}}{\dfrac{e^{\varepsilon}-1}{(e^{\varepsilon}+|Y_S||X_S|-1)(e^{\varepsilon}+|X_S|-1)}}=e^{\varepsilon}\quad(41)$$

3）根据 5.1 节中的式(13)及式(14)可知，x 的扰动显然是可逆的；对于给定的 $x_0\in X_N$，y 的任意两个不同输入$(x_0,y),(x_0,y')\in(X_N,Y_S\cup Y_N)$，扰动至同一输出$(\tilde{x},\tilde{y})\in(W_I,V_P)$的概率比为：

$$\frac{Pr[(\tilde{x},\tilde{y})|(x_0,y)]}{Pr[(\tilde{x},\tilde{y})|(x_0,y')]}=\frac{m}{n}=\frac{\dfrac{e^{2\varepsilon}-e^{\varepsilon}}{(e^{\varepsilon}+|Y_S||X_S|-1)(e^{\varepsilon}+|Y_S|-1)}}{\dfrac{e^{\varepsilon}-1}{(e^{\varepsilon}+|Y_S||X_S|-1)(e^{\varepsilon}+|Y_S|-1)}}=e^{\varepsilon}\quad(42)$$

4）根据 5.1 节中的式(14)可知，x,y 的扰动过程显然都是可逆的。式(40)—式(42)均满足 3.1 节中的定义 1。故推论 1 得证。

推论 2 CPRR 机制满足(X,Y,W,V,ε)-ULDP 模型的定义。

证明：令 $S=(X_S,Y_S)\cup(X_N,Y_S)\cup(X_S,Y_N)$是敏感输入域，$S'=(W_P,V_P)\cup(W_P,V_I)\cup(W_I,V_P)$为保护输出域，根据定义 3 可以将其转化为证明：1）$S\to S'$部分的扰动需要二维数据整体满足 ε-LDP 模型的定义；2）(X_N,Y_N)扰动到(W_I,V_I)的部分满足 x,y 均是可逆的。下面依次对上述两条进行证明。

1）将只要有一个属性包含敏感取值的区域就视作敏感输入域，因此对于 $S\to S'$的扰动过程，任意不同的输入$(x_0,y_0),(x_0',y_0')\in S$ 扰动至同一输出$(\tilde{x},\tilde{y})\in S'$的概率比值为：

$$\frac{Pr[(\tilde{x},\tilde{y})|(x_0,y_0)]}{Pr[(\tilde{x},\tilde{y})|(x_0',y_0')]}=\frac{a'}{b'}=\frac{\dfrac{e^{\varepsilon}}{e^{\varepsilon}+d-1}}{\dfrac{1}{e^{\varepsilon}+d-1}}=e^{\varepsilon}\quad(43)$$

2）(X_N,Y_N)扰动到(W_I,V_I)的部分，根据 5.2 节中的式(34)可知，以概率 t' 保持真实值不变，显然是可逆的。式(43)显然满足定义 1。故推论 2 得证。

6.2 期望与方差分析

针对第 5 章中所提出的两个方案，下面对 JuRR 以及 CPRR 机制的估计结果进行理论分析，用期望验证估计结果的无偏性，用方差衡量估计机制的准确度。

6.2.1 期望分析

推论 3 JuRR 机制得到的联合分布结果为无偏估计。

证明：由于 JuRR 将输入划分为了 4 个部分，下面分别对其无偏性进行证明。

1）输出在(W_P,V_P)的部分，根据式(23)可知，其中 f_{ij}^* 表示的是联合分布的真实值，$\hat{f}_{ij}$是联合分布的估计值。

$$\mathbb{E}(\hat{f}_{ij})=\frac{\mathbb{E}(\tilde{c}_{ij})/N-b}{a-b}=\frac{[af_{ij}^*+(1-f_{ij}^*)b]-b}{a-b}=f_{ij}^*\quad(44)$$

2）输出在(W_I,V_I)的部分，根据式(25)有：

$$\mathbb{E}(\hat{f}_{ij})=\frac{\mathbb{E}(\tilde{c}_{ij})}{Nt}=\frac{tf_{ij}^*}{t}=f_{ij}^*\quad(45)$$

根据式(44)与式(45)可知前两部分的估计结果显然是无偏的。

3）输出域在(W_P,V_I)的部分，由于表达式较为繁琐，为了简化公式表达，令 $h=\dfrac{\mathbb{E}(S_{Sx})}{N}-\dfrac{q|X_S|}{t}\mathbb{E}(S_{Nx})$，那么该部分的期望可以表示为式(46)。

$$\mathbb{E}(\tilde{f}_{ij})=\frac{\mathbb{E}(\tilde{c}_{ij})/N-\dfrac{q}{tN}\mathbb{E}(cS_{Nx})-\dfrac{q}{p+(|X_S|-1)q}}{p-q}\quad(46)$$

其中：

$$\mathbb{E}(\tilde{c}_{ij})f_{ij}^*p+(f_{1j}^*+f_{2j}^*+\cdots+f_{|X_S|j}^*-f_{ij}^*)q+\frac{q}{t}\mathbb{E}(S_{Nx})\quad(47)$$

$$\begin{aligned}\mathbb{E}(S_{Sx})&=\mathbb{E}(\tilde{c}_{1j})+\mathbb{E}(\tilde{c}_{2j})+\cdots+\mathbb{E}(\tilde{c}_{|X_S|j})\\&=N(f_{1j}^*+f_{2j}^*+\cdots+f_{|X_S|j}^*)[p+(|X_S|-1)q]+N\frac{q|X_S|}{t}\mathbb{E}(S_{Nx})\end{aligned}\quad(48)$$

将式(47)和式(48)代入式(46)可以得到：

$$\mathbb{E}(\hat{f}ij)=f_{ij}^*\quad(49)$$

因此该部分的估计也是无偏的。

4）输出域在(W_I,V_P)的部分，证明过程与上述 3）中输出域在(W_P,V_I)的部分基本相同，区别仅在于 x,y 的敏感取值域与非敏感取值域以及概率参数做了更改。由于篇幅限制，这里我们就不再详细列出推导过程。该部分的估计同样是无偏的。

故推论 3 得证。

推论 4 CPRR 机制得到的联合分布结果为无偏估计。

证明：

1)输出在 S' 的部分，根据式(37)可知：

$$\mathbb{E}(\hat{f}_{ij})=\frac{\mathbb{E}(\tilde{c}_{ij})/N-b'}{a'-b'}=\frac{[a'f_{ij}^*+(1-f_{ij}^*)b']-b'}{a'-b'}=f_{ij}^* \tag{50}$$

2)输出在 (W_1,V_1) 的部分，根据式(39)有：

$$\mathbb{E}(\hat{f}_{ij})=\frac{\mathbb{E}(\tilde{c}_{ij})/N}{t'}=\frac{t'f_{ij}^*}{t'}=f_{ij}^* \tag{51}$$

根据 1)和 2)，CPRR 机制的估计是无偏的。

故推论 4 得证。

6.2.2 方差分析

在方差的计算过程中涉及的变量过多，符号表示较繁杂，无法得到较为简便的表达式。因此，对于无法进一步化简的部分，下文仅列出方差的计算表达式。

JuRR 机制的方差：

1)输出在 (W_P,V_P) 的部分，方差可以表示为：

$$\begin{aligned}Var(\hat{f}_{ij})_{PP}&=\frac{1}{N(a-b)}Var(\tilde{c}_{ij})\\&=\frac{1}{N(a-b)}[f_{ij}^*a(1-a)+(1-f_{ij}^*)b(1-b)]\\&=\frac{b(1-b)}{N(a-b)^2}+\frac{f_{ij}^*(1-a-b)}{N(a-b)}\end{aligned} \tag{52}$$

2)输出在 (W_1,V_1) 的部分，方差如式(53)所示：

$$\begin{aligned}Var(\hat{f}_{ij})_{II}&=\frac{1}{Nt^2}Var(\tilde{c}_{ij}\\&=\frac{1}{Nt^2}[f_{ij}^*a(1-a)+(1-f_{ij}^*)b(1-b)]\end{aligned} \tag{53}$$

3)输出在 (W_P,V_I) 的部分，由于变量较多，无法得到简化后的结果，因此令 $g=q/[p+(|X_S|-1)q]$，则有：

$$Var(\hat{f}_{ij})_{PI}=Var\left(\frac{\frac{\tilde{c}_{ij}}{N}-\frac{q}{tN}S_{Nx}-\left(\frac{S_{Sx}}{N}-\frac{q}{tN}S_{Nx}|X_S|\right)g}{p-q}\right) \tag{54}$$

4)输出在 (W_I,V_P) 的部分，与 3)的推导过程一致，区别仅在于将 x,y 的敏感与非敏感区域进行调换，以及概率参数由 p,q 更改为 m,n。

JuRR 的总方差为上述 4 个部分方差之和：

$$\begin{aligned}Var(\hat{f}_{ij})_{JuRR}=&Var(\hat{f}_{ij})_{PP}+Var(\hat{f}_{ij})_{II}+Var(\hat{f}_{ij})_{PI}+\\&Var(\hat{f}_{ij})_{IP}\end{aligned} \tag{55}$$

CPRR 机制的方差：

1)输出域在 S' 的部分，方差可以用式(56)计算：

$$\begin{aligned}Var(\hat{f}_{ij})_S'&=\frac{1}{N(a'-b')^2}Var(\tilde{c}_{ij})\\&=\frac{1}{N(a'-b')^2}[f_{ij}^*a'(1-a')+(1-f_{ij}^*)b'\\&\quad(1-b')]\\&=\frac{b'(1-b')}{N(a'-b')^2}+\frac{f_{ij}^*(1-a'-b')}{N(a'-b')}\end{aligned} \tag{56}$$

2)输出域在 (W_1,V_1) 的部分，方差可以表示为式(57)：

$$\begin{aligned}Var(\hat{f}_{ij})_{II}&=\frac{1}{Nt^2}Var(\tilde{c}_{ij})\\&=\frac{1}{Nt^2}[f_{ij}^*a'(1-a')+(1-f_{ij}^*)b'(1-b')]\end{aligned} \tag{57}$$

CPRR 的总方差为上述两个部分方差的和：

$$\begin{aligned}Var(\hat{f}_{ij})_{CPRR}&=Var(\hat{f}_{ij})_S'+Var(\hat{f}_{ij})_{II}\\&=\frac{1}{N}\left[\frac{1}{(a'-b')^2}+\frac{1}{t^2}\right][f_{ij}^*a'(1-a')+\\&\quad(1-f_{ij}^*)b'(1-b')]\end{aligned} \tag{58}$$

7 实验及结果

本章设计对比实验对两个机制 JuRR 与 CPRR 的准确度以及有效性进行验证。分别对隐私预算 N 的取值、敏感取值域 $|X_S|$ 和 $|Y_S|$ 的大小，以及总用户数量 N 进行设置，以探讨不同参数取值时两种机制的误差变化。为了验证机制的效用，将 JuRR 和 CPRR 与 Yilmaz 等[14]在 LDP 模型下提出的联合分布估计机制进行实验对比。文献[16]的主要思想是将二维数据转化为一维数据，之后采用 LDP 已有的频率估计方案进行估计，实验中选取 GRR 方案，并将这种机制称作 JD_GRR。

7.1 实验环境

实验设置如下：Windows 10 操作系统，16 GB 内存，处理器为 Intel Corei5-1135G7，实验语言为 Python 3.8.3。为了避免实验的随机性对实验结果产生影响，将每个实验重复进行 10 次，取 10 次实验的平均值作为最终的结果。

本节设置了 4 个对比机制：在二维 ULDP 模型下提出的两种联合分布估计机制 JuRR 和 CPRR；将隐私预算均分后使用一维 ULDP 模型对联合分布进行估计，下文将这一机制称作 TDRR；以及 LDP 模型下的联合分布估计机制 JD_GRR。使用以上 4 种机制分别进行实验，对联合分布的估计准确度以及运行时间进行对比。

7.2 衡量标准

实验中采用欧氏距离(Euclid Distance，ED)作为误差的衡量标准。为了评估联合分布的估计误差，可将二维数据间的联合分布取值视作一个矩阵，矩阵的行数和列数分别为 $|X|$ 和 $|Y|$。对该矩阵求欧氏距离，并将其作为误差的衡量标准。式(59)中的 f^*，$\hat{f}$ 分别代表二维联合分布的真实值与估计值，i,j 是二维数据取值在矩阵中的索引。

$$ED(f^*,\hat{f})=\sqrt{\sum_{i=1,j=1}^{i=|X|,j=|Y|}(f_{ij}^*-\hat{f}_{ij})^2} \tag{59}$$

将欧氏距离(ED)与差分隐私中常用的均方误差(Mean Square Error，MSE)(MSE 的计算方式如式(60)所示)进行对比，可以看出这两种计算方式的区别仅在于常数 N 及平方根等运算，其对误差的分析无影响。本文用欧氏距离以及均方误差均进行了实验，为了保证实验结果的美观以及曲线的平滑度，最终选取欧氏距离作为衡量标准，即实验图中的纵坐标。

$$MSE=\frac{1}{N}\sum_{i=1,j=1}^{i=|X|,j=|Y|}(f_{ij}^*-\hat{f}_{ij})^2 \tag{60}$$

7.3 实验数据集

本次实验选取两个真实的数据集：一个是 nursery[27]数据集，该数据集是根据父母的职业、家庭形式、子女个数、住房条件和家庭财务状况等数据对托儿所进行推荐，共 12 960 条记录，其中包含 8 个特征与 1 个类标签，其特征及类标签均

为类别型数据，类标签按照推荐程度分为了 5 个等级，将取值较小的视为敏感的；另一个是学生成绩数据集 score[28]，该数据集共包含记录 1000 条，特征分别为性别、种族、父母受教育程度及考试前是否做准备等。

在进行实验之前，首先对数据集进行预处理。数据集中各参数取值如表 3 所列。

表 3 数据集的参数描述

Table 3 Parameter description of datasets

	nursery	score
隐私预算 ε	0.5～6	0.5～6
记录数 N	12960	1000
选取的特征	第 1，第 3	第 2，第 3
$\lvert X\rvert$	3，4	5，6
$\lvert Y\rvert$	5	3
$\lvert X_S\rvert$	2	2，4
$\lvert Y_S\rvert$	2，4	2

对于 nursery 数据集，总记录个数 $N=12960$，将类标签视为其中的一维属性，类标签即为对托儿所的评价等级，从低到高分为 5 个等级，即 $|Y|=5$。根据实际情况，将较低的评价视为敏感的，后续的实验考虑了敏感取值域分别为 $|Y_S|=2$ 和 $|Y_S|=4$ 两种情况下的误差。对于另一维属性，在实验中选取的是第 1 个和第 3 个特征，第 1 个特征代表父母的成就，分为 3 个等级，即 $|X|=3$，将较低的等级作为敏感的；第 3 个特征为家庭形式，有 4 种取值，即 $|X|=4$，显然不完整和寄养家庭会被视作敏感的；由于取值个数比较少，因此对于这一维属性，均选取敏感取值域的大小为 2，即 $|X_S|=2$。

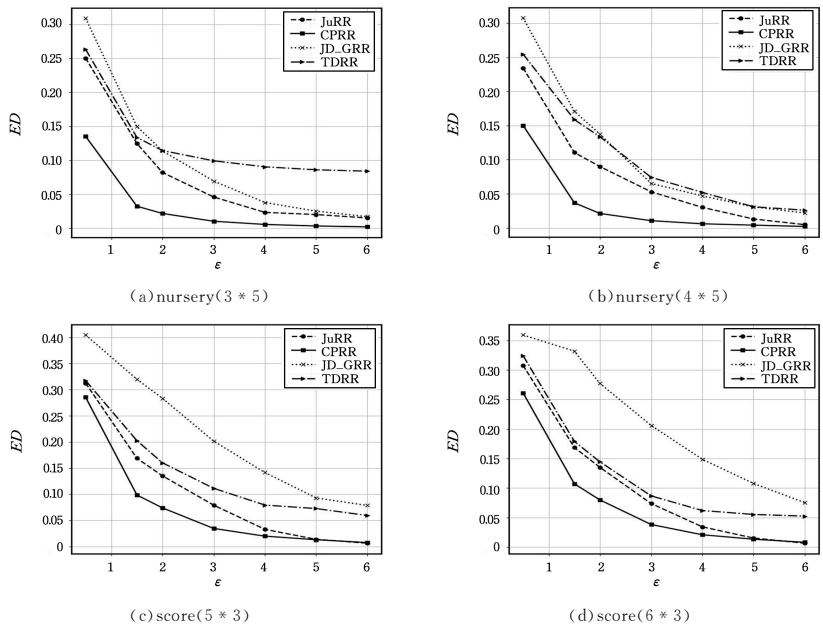
在 score 数据集中，总用户个数 $N=1000$，其中一维属性为类标签，将数学成绩、阅读成绩和写作成绩进行加和后作为类标签，并且按照从低到高的顺序划分为 3 类，将较低的成绩视作敏感的，这时 $|Y|=3$，将前两类视为敏感取值域；另一维属性，在实验时选取的是第 2 和第 3 个特征，数据规模分别为 $|X|=5$ 和 $|X|=6$，在后续的实验中我们讨论了不同的敏感取值域大小 $|X_S|=2$ 以及 $|X_S|=4$ 两种情况下的误差变化。

在本地差分隐私的研究中，隐私预算 ε 的取值设置得过大会导致保护力度过低，对于隐私数据无法起到很好的保护效果；设置得过小又会导致数据效用较低。因此，通常在 0.5～6 的范围内进行实验分析。

7.4 实验结果

7.4.1 ε 取值的影响

在两个数据集上分别进行实验，并且在 0.5～6 之间选取了 7 个不同的隐私预算取值，横坐标是隐私预算 ε 的取值，纵坐标是误差欧氏距离(ED)的值。在 nursery 数据集中，选取第 1，3 个特征，对第 1，3 个特征与类标签之间的联合分布进行估计，数据规模分别为 3 * 5，4 * 5。在 score 数据集中，选取第 2，3 个特征，数据规模分别为 5 * 3，6 * 3。均选取前两个取值作为敏感输入域，即 ε。实验结果如图 3 所示。



(a)nursery(3 * 5)　(b)nursery(4 * 5)

(c)score(5 * 3)　(d)score(6 * 3)

图 3 ε 的变化对误差 ED 的影响

Fig. 3 Effect of ε on ED

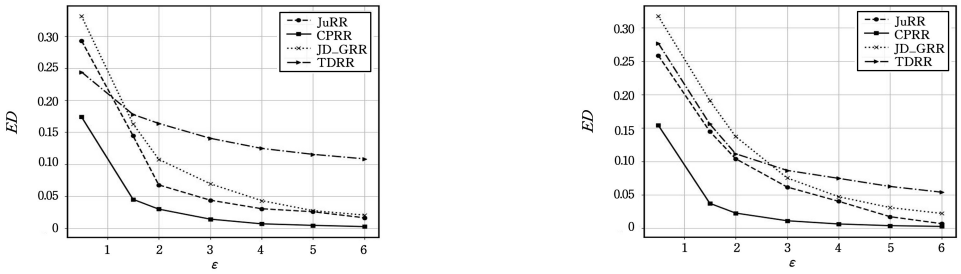
从实验结果可以得知，随着隐私预算的不断增大，隐私保护程度降低，误差也在不断减小，并且 4 个机制的误差都越来越接近，逐渐趋近于 0；其次，CPRR 比 JuRR 误差小，是由于 JuRR 在使用时非敏感属性扰动到自身的概率较小，导致对非敏感取值的保护力度的减弱程度不高，所以效果不如 CPRR。实验结果与 5.2.1 节中的分析是一致的。

接下来对比所提出的机制与本地差分隐私模型下的联合分布估计机制 JD_GRR 以及把隐私预算均分后将一维 ULDP 机制用于联合分布估计的 TDRR 机制。从图 3 中的 4 张图均可以明显看出 JuRR 与 CPRR 的误差比 JD_GRR 的误差更小，由此证明在 ULDP 模型下提出的两种估计机制的数据效用更好。分析其原因，JD_GRR 是在 LDP 模型下提出的方法，它将所有数据均视为敏感的，而我们所提出的机制是在 ULDP 模型下考虑了二维数据取值分别敏感与否的 4 种情况，提高了数据效用，也减小了

估计的误差。TDRR 总体上比 JD_GRR 效果好的原因是 TDRR 考虑了取值的敏感与否，而 JD_GRR 将其全部视为敏感的。然而，在图 3(a)中，TDRR 的效果不稳定，在隐私预算较小时，误差比 JD_GRR 小，而随着隐私预算的增大效果又比其他几种机制差，这可能是在使用 TDRR 时，我们对隐私预算进行了均分，在隐私预算较小时，均分后差距也较小，对准确度的影响较低导致的。但是总体来看 JuRR 比 TDRR 误差小且稳定，且 CPRR 机制的误差一直是最小的。

7.4.2 敏感取值域大小 $|X_S|$，$|Y_S|$ 的影响

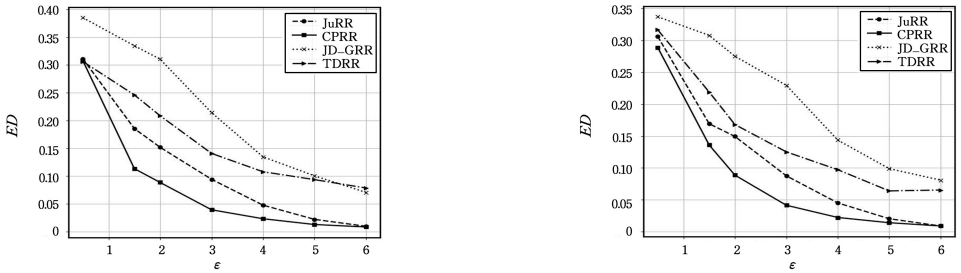
在 7.4.1 节的实验中将属性的前两个取值视为敏感的，为了确定敏感取值域对结果的影响，对敏感取值域进行变化后再次进行实验。根据数据集的原始规模，nursery 数据集中数据的初始规模为 3 * 5，4 * 5，我们对敏感区域的划分更改为 $|X_S|=2$，$|Y_S|=4$，Y 的敏感区域占比从 7.4.1 节中的 40%变化为 80%；而对于 score 数据集，数据规模为 5 * 3，6 * 3，因此保持 $|Y_S|$ 不变，提高 X 中敏感区域的占比，选取 $|X_S|=4$，$|Y_S|=2$ 进行实验。实验结果如图 4 和图 5 所示。



(a)nursery(3 * 5) (b)nursery(4 * 5)

图 4 nursery 数据集中 $|Y_S|=4$ 时 ED 的变化

Fig. 4 Variations of ED on nursery dataset when $|Y_S|=4$



(a)score(5 * 3) (b)score(6 * 3)

图 5 score 数据集中 $|X_S|=4$ 时 ED 的变化

Fig. 5 Variations of ED on score dataset when $|X_S|=4$

将实验结果与图 3 中各图的纵坐标对比可知，随着敏感区域的扩大，JuRR 与 CPRR 这两种机制在误差上均有不同程度的增大，即估计准确度降低。这与 ULDP 的原理是一致的。ULDP 更适用于非敏感取值较多的情况，它的原理是通过将非敏感取值以较大概率保持不变，从而适当降低对非敏感取值的保护力度，达到数据效用提升的目的。本文所提出的两个机制是基于 ULDP 的，同样也满足这一原理，因此其在敏感取值域较小时表现亦较好。

举例来说，观察图 3(a)中 CPRR 的纵坐标可以看出，在隐私预算 $\varepsilon=0.5$，$|Y_S|=2$ 取值较小时，误差在 0.1～0.15 之间；而图 4(a)中，隐私预算 $\varepsilon=0.5$，$|Y_S|=4$ 时，随着 $|Y_S|$ 增大，纵坐标的取值大于 0.15，误差有所增大。JuRR 机制同理。总体来看，CPRR 机制在敏感取值域 $|X_S|$ 或 $|Y_S|$ 增大时，即便效果有所降低，但仍然优于 JuRR。

在与 JD_GRR 以及 TDRR 机制进行对比时，本文所提出的机制显然优于 JD_GRR 机制。观察图 4(a)可以发现，在隐私预算较小时，TDRR 有时比 JuRR 的效果好，可能是因为隐私预算均分后差值较小，对误差的影响不大，这与图 3 中的分析是一致的。但是随着隐私预算的增加，TDRR 的误差明显比 JuRR 以及其他机制大许多。虽然 JuRR 在个别情况下可能比 TDRR 误差大，但是差值均不超过 0.05，而 CPRR 与 TDRR，JD_GRR 相比效果更优。因此，文中所提出的两个机制在隐私保护效果上较为稳定，并且在一定程度上也提高了数据效用。

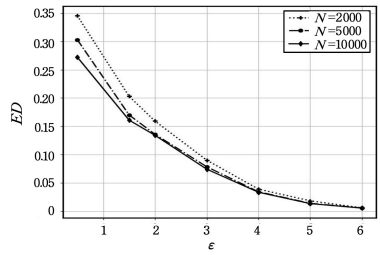
7.4.3 数据集大小 N 的影响

讨论数据集中记录个数对误差的影响时，我们统一使用 nursery 数据集，该数据集共包含 12960 条记录。对数据集进行截取，分别截取 2000，5000，10000 条记录，形成 3 个数据集。用 nursery 的第 2 个特征与类标签进行实验，数据规模为 5 * 5，实验结果如图 6 所示。

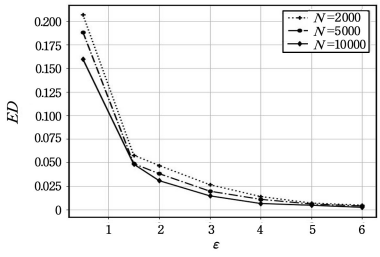
根据实验结果，在数据量较大时，误差更小，估计的准确度更高。本文所提出的两个机制均在数据量较大时效果更显著。数据量为 2000 和 5000 时，由于数值较为接近，因此二者的差距不大。

结合以上所有实验结果可知，我们所提出的两种效用优化的本地差分隐私联合分布估计机制更适用于数据量较大并且敏感取值域较小的数据集。该机制与 LDP 模型下的联合分布机制相比，缩小了估计的误差，提高了数据效用，其中

CPRR 比 JuRR 的效果更为显著。



(a)JuRR



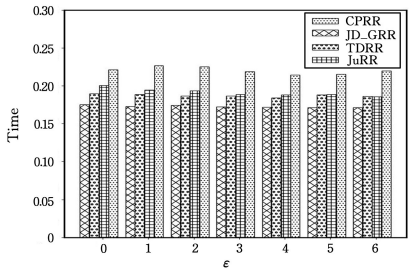
(b)CPRR

图 6 不同数据集大小 N 对误差 ED 的影响

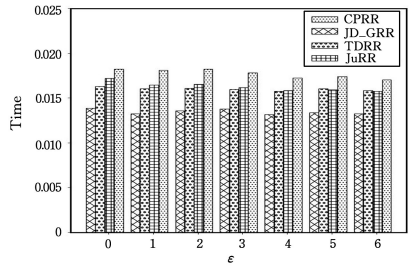
Fig. 6 Effect of N on ED

7.4.4 运行时间

仍然在不同隐私预算的取值下做 10 次实验，取平均值作为最终运行时间。横坐标为隐私预算的取值，纵坐标为运行时间，单位为 s。分别在 nursery 和 score 数据集上进行实验，选取 nursery 数据集的第 1 个特征和 score 数据集的第 3 个特征，数据规模分别为 3 * 5 和 5 * 3，选取前两个取值作为敏感输入域，即 $|X_S|=2$，$|Y_S|=2$。实验结果如图 7 所示。



(a)nursery



(b)score

图 7 各机制的运行时间

Fig. 7 Running time of each mechanism

根据图 7，首先可以分析得到各个方案的运行时间，从低到高依次是 LDP 模型下的 JD_GRR 机制、一维 ULDP 机制 TDRR、JuRR 以及 CPRR。进一步进行分析，图 7(b)中时间消耗最少的数值在 0.013 s，而运行时间的最高数值为 0.019 s 左右，只相差了 0.006 s，几乎可忽略不计；图 7(a)也同理，最高与最低的时间差不超过 0.05 s。在实际运行中，该误差几乎可忽略不计。其次，两图的时间差有所差异的原因是数据集大小不同，nursery 数据集的记录数是 score 数据集的 10 倍，因此耗时也相对长一点。

虽然本文提出的两种方案的耗时相比其他两种机制较长，但时间差不超过 0.1 s，而两种方案在估计的准确度上有了很大的提升，JuRR 与 CPRR 的总体效果更好。

结束语 如何在 ULDP 模型下对联合分布进行估计是目前亟待解决的问题。本文提出了效用优化的本地差分隐私联合分布估计机制。首先，给出了二维 ULDP 模型的定义。其次，设计了两种 ULDP 模型下对二维数据进行扰动的机制，并且给出了相应的联合分布估计方法，同时理论证明了其无偏性；最后，利用真实数据集，将这两种机制与 LDP 模型下的 JD_GRR 机制进行对比实验，讨论了不同参数下的误差变化，同时也对联合分布的估计误差以及数据可用性进行了评估。实验验证了 JuRR 以及 CPRR 机制可以有效提高估计的准确度以及数据效用，其中 CPRR 的估计误差较优。

在得到联合分布估计值之后，还可进一步计算其中某一维数据的边缘分布，从而推导条件概率的取值。根据这一结果，后续可将该机制应用于机器学习等算法，在保证用户隐私数据的基础上，完成分类或预测等数据挖掘工作。

结合目前的发展趋势，未来的主要工作有以下两点：首先，可以将该机制扩展到更高维数据的联合分布中，以更好地解决复杂的问题；其次，本文将用户的隐私数据分为敏感和非敏感两个等级，在未来还可以将敏感度进一步细分。

参 考 文 献

[1] SWEENEY L. k-anonymity: A Model for Protecting Privacy [J]. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 2002, 10(5): 557-570.

[2] MACHANAVAJJHALA A, KIFER D, GEHRKE J, et al. l-diversity: Privacy beyond k-anonymity [C] // 22nd International Conference on Data Engineering. 2006.

[3] LI N, LI T, VENKATASUBRAMANIAN S. t-closeness: Privacy beyond k-anonymity and l-diversity [C] // IEEE 23rd International Conference on Data Engineering. Istanbul: IEEE Press, 2007: 106-115.

[4] YAO A C. Protocols for Secure Computations [C] // 23rd Annual Symposium on Foundations of Computer Science. Chicago: IEEE Press, 1982: 160-164.

[5] DWORK C. Differential privacy: A survey of results [C] // International Conference on Theory and Applications of Models of Computation. Berlin, Heidelberg: Springer Press, 2008: 1-19.

[6] KASIVISWANATHAN S P, LEE H K, NISSIM K, et al. What Can We Learn Privately? [J]. SIAM Journal on Computing, 2011, 40(3): 793-826.

[7] DUCHI J C, JORDAN M I, WAINWRIGHT M J. Local Privacy and Statistical Minimax Rates [C] // IEEE 54th Annual Symposium on Foundations of Computer Science. Berkeley: IEEE Press, 2013: 429-438.

[8] WANG T, BLOCKI J, LI N, et al. Locally Differentially Private Protocols for Frequency Estimation [C] // 26th USENIX Securi-

ty Symposium. Vancouver: USENIX Press, 2017: 729-745.
[9] DUCHI J C, JORDAN M I, WAINWRIGHT M J. Minimax Optimal Procedures for Locally Private Estimation[J]. Journal of the American Statistical Association, 2018, 113(521): 182-201.
[10] WANG N, XIAO X, YANG Y, et al. Collecting and Analyzing Multidimensional Data with Local Differential Privacy[C]// IEEE 35th Inter-national Conference on Data Engineering. Macao: IEEE Press, 2019: 638-649.
[11] ERLINGSSON Ú, PIHUR V, KOROLOVA A. Rappor: Randomized Aggregatable Privacy-Preserving Ordinal Response [C]// Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. Scottsdale: ACM Press, 2014: 1054-1067.
[12] TEAM A D P. Learning with Privacy at Scale[J]. Apple Mach. Learn. J, 2017, 1(8): 1-25.
[13] SAMARATI P, SWEENEY L. Generalizing Data to Provide Anonymity when Disclosing Information[C]// PODS. Seattle: ACM Press, 1998, 98(188): 1045-1145.
[14] YILMAZ E, AL-RUBAIE M, CHANG J M. Naive Bayes Classification under Local Differential Privacy[C]// IEEE 7th International Conference on Data Science and Advanced Analytics. Adelaide: IEEE Press, 2020: 709-718.
[15] MURAKAMI T, KAWAMOTO Y. Utility-Optimized Local Differential Privacy Mecha-nisms for Distribution Estimation[C]// 28th USENIX Security Symposium. Santa Clara: USENIX Press, 2019: 1877-1894.
[16] CORMODE G, MADDOCK S, MAPLE C. Frequency Estimation under Local Differential Privacy[J]. Proceedings of the VLDB Endowment, 2021, 14(11): 2046-2058.
[17] WANG T, LI N, JHA S. Locally Differentially Private Frequent Itemset Mining[C]// 2018 IEEE Symposium on Security and Privacy. San Francisco: IEEE Press, 2018: 127-143.
[18] ZHU S X, WANG L, SUN G L. A Perturbation Mechanism for Classified Transformation Satisfying Local Differential Privacy [J]. Journal of Computer Research and Development, 2022, 59(2): 430-439.
[19] ZHANG Z, WANG T, LI N, et al. Calm: Consistent Adaptive Local Marginal for Marginal Release under Local Differential Privacy[C]// Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2018: 212-229.
[20] YE Q, HU H, MENG X, et al. PrivKV: Key-Value Data Collection with Local Differential Privacy[C]// 2019 IEEE Symposium on Security and Privacy. San Francisco: IEEE Press, 2019: 317-331.
[21] GU X, LI M, CHENG Y, et al. PCKV: Locally Differentially Private Correlated Key-Value Data Collection with Optimized Utility[C]// 29th USENIX Security Symposium. Boston: USENIX Press, 2020: 967-984.
[22] YE Q, HU H, MENG X, et al. PrivKVM*: Revisiting Key-Value Statistics Estimation with Local Differential Privacy[J]. IEEE Transactions on Dependable and Secure Computing, 2021, 14(8): 1-18.
[23] TIAN F, WU Z Q, LU L F, et al. A Sample Based Personalized Differential Privacy Mechanism for Trajectory Data Publication [J]. Chinese Journal of Computers, 2021, 44(4): 709-723.
[24] BALLE B, BELL J, GASCÓN A, et al. The Privacy Blanket of The Shuffle Model[C]// Annual International Cryptology Conference. Cham: Springer Press, 2019: 638-667.
[25] LIU Y F, WANG N, WANG Z G. Collecting and Analyzing Multidimensional Categorical Data Under Shuffled Differential Privacy[J]. Journal of Software, 2022, 33(3): 1093-1110.
[26] GU X, LI M, XIONG L, et al. Providing Input-Discriminative Protection for Local Differential Privacy[C]// IEEE 36th International Conference on Data Engineering. Dallas: IEEE Press, 2020: 505-516.
[27] UCI MACHINE LEARNING REPOSITORY. Nursery Data Set [DB/OL]. [2022-05-16]. https://archive.ics.uci.edu/ml/datasets/Nursery.
[28] KAGGLE. Performance in Exams [DB/OL]. [2022-06-25]. https://www.kaggle.com/datasets/spscientist/students-performance-in-exams.

YIN Shiyu, born in 1998, postgraduate, is a student member of China Computer Federation. Her main research interests include data security and differential privacy.

ZHU Youwen, born in 1986, Ph.D, professor, is a member of China Computer Federation. His main research interests include data security, privacy computing, and applied cryptography.

(责任编辑:柯颖)