第56卷第5期
2024年10月

南京航空航天大学学报
Journal of Nanjing University of Aeronautics & Astronautics

Vol. 56 No. 5
Oct. 2024

DOI:10.16356/j.1005-2615.2024.05.002

个性化本地差分隐私机制的研究现状与展望

朱友文[1],唐　聪[1],吴启晖[2],张　焱[3]

(1.南京航空航天大学计算机科学与技术学院,南京 211106;2.南京航空航天大学电子信息工程学院,南京 211106;3.南京航空航天大学信息化处,南京 210016)

摘要: 本地差分隐私作为一个优秀的隐私保护模型,被广泛应用于数据收集和统计分析中的隐私保护问题。但是本地差分隐私没有考虑不同用户的隐私需求差异以及不同数据的属性差异,因此作为本地差分隐私的一种变体,个性化本地差分隐私被提出。本文根据上述两类差异将个性化本地差分隐私机制分为两类,并在此基础上对该领域的研究现状进行了分析和总结。首先本文介绍了个性化本地差分隐私的基本概念和理论模型。其次对近年来的个性化本地差分隐私机制的若干文献进行了分析和归类,并详细介绍了几种代表性方案的原理和特点,包括数据扰动方法和数据聚合方法等。最后本文对该领域的未来发展方向进行了讨论与分析。

关键词: 数据安全;个性化本地差分隐私;统计分析;隐私保护

中图分类号: TP393　　**文献标志码:** A　　**文章编号:** 1005-2615(2024)05-0784-17

Review and Prospects of Personalized Local Differential Privacy Mechanisms

ZHU Youwen[1], *TANG Cong*[1], *WU Qihui*[2], *ZHANG Yan*[3]

(1. College of Computer Science and Technology, Nanjing University of Aeronautics & Astronautics, Nanjing 211106, China; 2. College of Electronic and Information Engineering, Nanjing University of Aeronautics & Astronautics, Nanjing 211106, China; 3. Information Technology Center, Nanjing University of Aeronautics & Astronautics, Nanjing 210016, China)

Abstract: Local differential privacy (LDP) is a well-regarded privacy protection model widely used in data collection and statistical analysis to address privacy concerns. However, LDP does not account for the varying privacy needs of different users and the differences in data attributes. As a variant of LDP, the personalized local differential privacy (PLDP) has been proposed. This paper categorizes PLDP mechanisms into two types based on the aforementioned differences and analyzes the current research status in this field. Firstly, the paper introduces the basic concepts and theoretical models of PLDP. Then, it analyzes and classifies several recent studies on PLDP mechanisms, providing detailed explanations of representative schemes, including data perturbation methods and data aggregation methods. Finally, the paper discusses and analyzes the future development directions in this field.

Key words: data security; personalized local differential privacy; statistical analysis; privacy protection

近年来,随着互联网和智能设备的快速发展,连接到因特网的设备数量不断增长,并且生成了大量数据用于大数据分析和空间众包等[1]。这些大数据提高了各类网络服务的质量,给人们的生活带来了巨大的便利,比如用于交通流量控制、推荐系统、在线匹配等[2-4]。但是这些数据如果被滥用则会引起严重的隐私安全问题,特别是,利用先进的数据融合和分析技术,用户的隐私信息更容易受到

基金项目: 江苏省重点研发计划(BE2022068,BE2022068-1);中国高校产学研创新基金(2023IT049)。

收稿日期: 2024-08-10;**修订日期:** 2024-09-20

通信作者: 朱友文,男,教授,E-mail: zhuyw@nuaa.edu.cn。

引用格式: 朱友文,唐聪,吴启晖,等. 个性化本地差分隐私机制的研究现状与展望[J]. 南京航空航天大学学报,2024,56(5):784-800. ZHU Youwen, TANG Cong, WU Qihui, et al. Review and prospects of personalized local differential privacy mechanisms[J]. Journal of Nanjing University of Aeronautics & Astronautics, 2024, 56(5):784-800.

攻击和泄露[5-10]，例如，用户的家庭住址、日常行为习惯、身份信息、社会关系和宗教信仰等[11-14]。针对个人数据隐私保护问题，国内外已陆续出台了相应的法律法规：欧盟于2016年通过了《一般数据保护法案》[15]；自2017年6月和2021年9月，我国分别开始施行《中华人民共和国网络安全法》[16]和《中华人民共和国数据安全法》[17]。如何在数据分析时保护用户隐私安全也成为近年来学术界的研究热点。本地差分隐私(Local differential privacy，LDP)[18-22]作为一种优秀的隐私保护模型，针对的是不可信的第三方，其允许用户在本地对数据扰动后再提交给数据收集者，确保了不可信第三方无法拥有用户的原始数据，但仍然可以从扰动后的数据中获得有用的统计数据，兼顾了用户的隐私安全和数据的可用性。然而现有的本地差分隐私方案忽略了不同用户以及不同数据的多层次隐私需要，这对用户的隐私安全以及数据的效用都会造成影响。因此出现了个性化本地差分隐私的概念以及各类个性化本地差分隐私机制。

为了满足不同用户和数据的多层次的隐私需求，研究者们从不同的角度出发，提出了一系列的个性化本地差分隐私机制，大致可以分为两类：第一类是用户层面的个性化(Personalized LDP，PLDP)[23-46]，由于不同用户隐私需求的不同，允许用户自行选择隐私预算或隐私级别，或是在高维数据中自由分配总的隐私预算到不同维度；第二类是数据层面的个性化，根据数据本身敏感程度的不同给不同的数据分配不同的隐私预算(Input-discriminative LDP，ID-LDP)[47-55]，或是将扰动概率与数据间的度量(具体的度量类型根据具体场景而定，可以是欧氏距离、离散型数据间的距离等)联系起来[56-77]，即Metric LDP。在用户层面的个性化设置中，主要问题集中于在收集到来自不同隐私预算的扰动数据以后，如何对这些数据进行处理与分析，根据用户是否将自己的隐私预算或隐私等级提交给服务器有如下几种方法：根据扰动数据反推隐私预算的方法[23]、加权组合法[24]、数据回收法[24]以及极大似然估计法[30]等。在数据层面的个性化设置中可以分为两类：一类是根据不同数据敏感程度的不同给数据分配不同的隐私预算，给敏感程度较高的数据分配较低的隐私预算，而给敏感程度较低的数据分配较高的隐私预算，保证了用户隐私安全的同时相较于传统的本地差分隐私机制还提升了数据的效用；另一类是将扰动概率与数据间的度量联系起来，两个数据间的扰动概率与它们之间的度量值成反比，意味着一个数据更容易被扰动到在度量上和它更为接近的数据，这种方法也提升了数据的效用。

对现有的个性化本地差分隐私机制进行综述总结，为该领域工作提供参考，具有重要意义。本文调研了来自主流会议、期刊的个性化本地差分隐私领域的论文，聚焦最新的研究进展，基于上述提到的两类个性化本地差分隐私机制进行了总结归纳，包括现有方案的任务目标、个性化设置、后处理方法以及数据的扰动方法等，在Metric LDP中还讨论了各个方案所针对的数据类型，并对该领域的未来发展方向进行了讨论与分析。图1展示了本文的主要研究内容和调查结构。

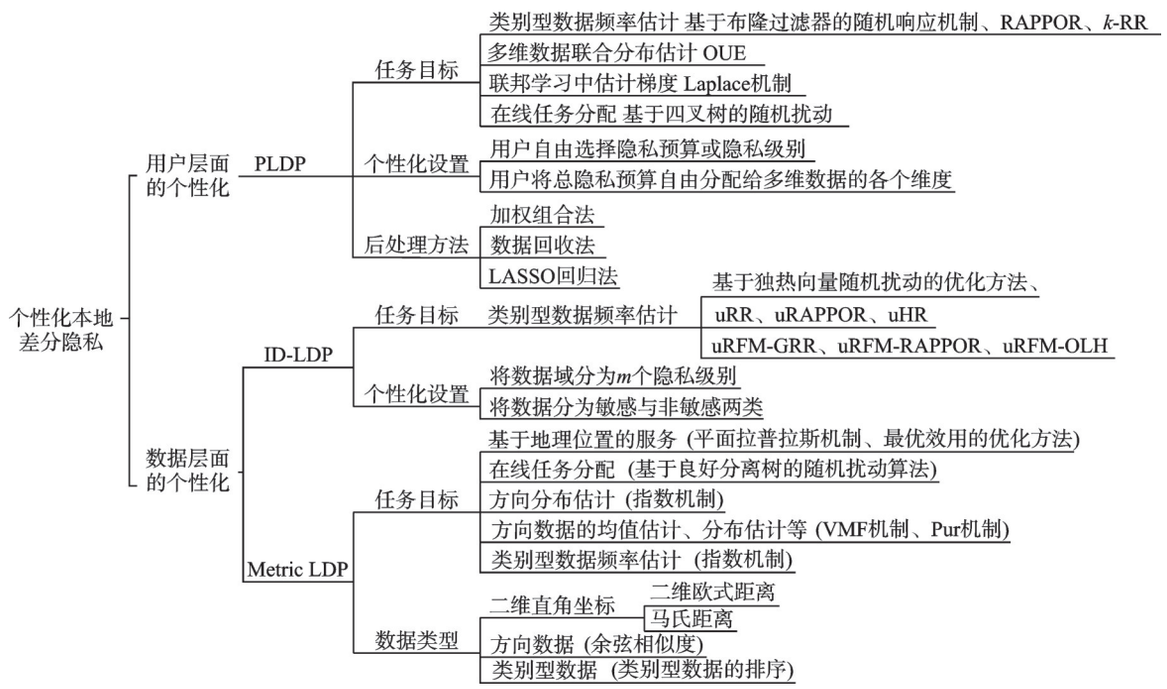


图1　个性化本地差分隐私主要研究内容分类概况

Fig.1　Overview of the main research content with personalized local differential privacy

1 个性化本地差分隐私基础

本节将介绍个性化本地差分隐私基础，包括符号介绍、个性化本地差分隐私的相关定义和性质。

1.1 符号

假设一共有n个用户，用户集可以形式化表示为$U=\{u_1,u_2,\cdots,u_n\}$。每个用户向服务器发送k维数据。对于类别型数据而言，一个属性A对应d个可能的取值，属性域$A=\{a_1,a_2,\cdots,a_d\}$。对于数值型数据而言，数据值的取值范围是全体实数。每个用户$i(1\leqslant i\leqslant n)$将编码、扰动处理后的数据发送给服务器端，服务器端的数据收集者对收集到的数据聚合以后用于数据分析、在线匹配和联邦学习等场景。常见的符号及其描述如表1所示。

表1 符号描述

Table 1 Description of notations

符号	描述
n	用户总数
k	数据维度
u	单个用户
d	属性域空间大小
v	原始数据
v^*	扰动数据
M	随机化算法
ε	隐私预算
$f_{v_i}/\hat{f}_{v_i}$	数据v_i的真实频率/估计频率

1.2 定义和性质

从隐私保护的角度来说，差分隐私(Differential privacy，DP)[78]是一个优秀的隐私保护模型，差分隐私依赖于可信的第三方服务器，但是在许多在线服务或者众包系统中服务器往往是不可信的。因此LDP[18]被人们提出，作为差分隐私的一种变体。本地差分隐私针对的是不可信的第三方，允许用户在本地将数据扰动后再上传给服务器，在不依赖于敌手先验知识的同时保证了用户的原始数据不被泄露。本地差分隐私的形式化定义如下。

定义1 ε-LDP[18] 一个随机化算法M满足ε-LDP，当且仅当对于任意的输入v、v'，以及任意可能的输出v^*满足

$$\frac{\Pr\left[M(v)=v^*\right]}{\Pr\left[M(v')=v^*\right]}\leqslant e^{\varepsilon} \tag{1}$$

式中ε被称为隐私预算，ε越大则隐私保护程度越低。

常规的本地差分隐私机制没有考虑数据提供者的不同隐私偏好和数据本身对隐私要求的不同，因此各类个性化本地差分隐私机制被提出。

用户层面的个性化本地差分隐私也可以称为PLDP[23-46]，其中每个用户可以根据自身的隐私需求选择不同的隐私预算/隐私级别或是自由的对隐私预算进行划分，PLDP形式化的定义。

定义2 ε-PLDP[24] 一个随机化算法M满足ε-PLDP，当且仅当对于任意输入v、v'和用户u，以及任意可能的输出v^*满足

$$\frac{\Pr\left[M(v)=v^*\right]}{\Pr\left[M(v')=v^*\right]}\leqslant e^{\varepsilon_u} \tag{2}$$

数据层面的个性化差分隐私也可以再分为两类：第一类为ID-LDP[47-55]；第二类为Metric LDP[56-77]。

在ID-LDP[47]中考虑到了不同数据的敏感程度可能不同，因此给不同的数据设置不同的隐私预算，ID-LDP形式化的定义如下。

定义3 ID-LDP[47] 对于属性域A给定隐私预算集合$\{\varepsilon_a\}_{a\in A}$，一个随机化算法$M$满足ID-LDP，当且仅当对于任意输入$v$、$v'\in A$，以及任意可能的输出$v^*$满足

$$\frac{\Pr\left[M(v)=v^*\right]}{\Pr\left[M(v')=v^*\right]}\leqslant e^{r\left(\varepsilon_v,\varepsilon_{v'}\right)} \tag{3}$$

式中$r(\cdot,\cdot)$为关于两个隐私预算的函数，可以是取2个隐私预算中较小的值。

效用优化的本地差与隐私(Utility-optimized LDP，ULDP)[48]可以看作是ID-LDP的一种特殊情况，在ULDP中将所有数据分为敏感数据和非敏感数据两类，其中敏感数据只会扰动为敏感数据，非敏感数据则是扰动为自身或者扰动为敏感数据。在属性域A中$A_S\subseteq A$为敏感数据组成的集合，$A_N=A\backslash A_S$为非敏感数据组成的集合，假设输出域为Y，设$Y_P\subseteq Y$为受保护数据组成的集合，$Y_I=Y\backslash Y_P$为可逆数据组成的集合。ULDP形式化的定义如下。

定义4 (A_S,Y_P,ε)-ULDP[48] 给定$A_S\subseteq A$，$Y_P\subseteq Y$，一个随机化算法M满足(A_S,Y_P,ε)-ULDP，当且仅当满足式(4)和式(5)。

(1) 对任意的$v^*\in Y_I$，存在$v\in A_N$满足$\Pr\left[M(v)=v^*\right]>0$，且对任意的$v'\neq v$满足

$$\Pr\left[M\left(v'\right)=v^*\right]=0 \tag{4}$$

(2) 对任意的v、$v'\in A$以及任意的$v^*\in Y_P$满足

$$\frac{\Pr\left[M(v)=v^*\right]}{\Pr\left[M(v')=v^*\right]}\leqslant e^{\varepsilon} \tag{5}$$

在ULDP中没有为非敏感数据提供隐私保护，可以看作是将非敏感数据的隐私预算设置为无穷大，对于敏感数据而言提供了与ε-LDP中相同的

隐私保护程度。

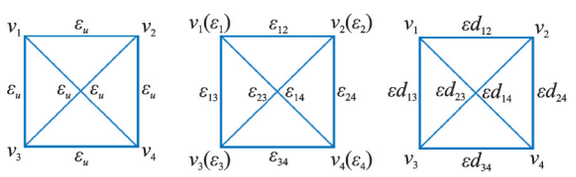
地理不可区分模型[56]可以用于保护地理位置数据隐私，它基于地理位置数据的距离，实现了εd_2-LDP，其中d_2为二维欧式距离，满足距离越近的两个数据间的扰动概率越大，相比标准的LDP具有更好的效用。可以将度量d_2推广为更一般的情况，因此有了Metric LDP。Metric LDP形式化的定义如下。

定义5　Metric LDP[56]　一个随机化算法M满足Metric LDP，当且仅当对于任意的输入v、v'，以及任意可能的输出v^*满足

$$\frac{\Pr\left[M(v)=v^*\right]}{\Pr\left[M(v')=v^*\right]}\leqslant \mathrm{e}^{\varepsilon d(v,v')} \tag{6}$$

式中$d(\cdot,\cdot)$为1个度量函数。

图2描述了在PLDP、ID-LDP和Metric LDP中不同数据相互扰动时的隐私预算，在PLDP中取决于用户所选择的隐私预算大小，在ID-LDP中取决于不同数据的敏感程度，在Metric LDP中则取决于两个数据间的距离。



ε_u:用户u所持有的隐私预算(不同用户的隐私预算可能不同)　(a) PLDP

ε_i:数据v_i的隐私预算 ε_{ij}:数据v_i和v_j相互扰动时的隐私预算　(b) ID-LDP

d_{ij}:数据v_i和v_j的距离 εd_{ij}:数据v_i和v_j相互扰动时的隐私预算　(c) Metric LDP

图2　PLDP、ID-LDP和Metric LDP中不同数据间相互扰动的隐私预算

Fig.2　Privacy budget of different data in PLDP, ID-LDP and Metric LDP

1.3　评价指标

1.3.1　隐私保护强度

数据的隐私保护强度是个性化本地差分隐私中的一个重要评价指标，反映了经过扰动处理后的数据的安全性。在PLDP方案中，隐私保护强度取决于用户在隐私预算选择和分配方面的自由度，以及用户是否需要将自己选择的隐私预算或具体的隐私预算分配方式发送给服务器。在ID-LDP中有两种个性化方案：第一种方案允许给不同的数据分配不同的隐私预算，在这种设置下可以根据实际情况为所有数据提供合适的保护力度，隐私保护强度较高；第二种方案将数据域分为敏感数据和非敏感数据两类，对于敏感数据提供与本地差分隐私中相同的保护强度，对于非敏感数据则不提供任何保护，隐私保护强度一般。在Metric LDP中输入更容易被扰动为在度量上较为接近的数据，这种方法通过牺牲数据的安全性来换取更高的数据可用性。

1.3.2　数据可用性

在个性化本地差分隐私模型中，用户在本地对数据做隐私化处理，不可避免地会对统计分析结果造成影响。因此学者们在设计个性化本地差分隐私机制时需要在隐私性和数据可用性之间做权衡。数据可用性的度量方法主要分为两类：一类是误差度量法[79]；另一类是信息损失度量法[80]。

误差度量法包括平均绝对误差(Mean absolute error, MAE)和均方误差(Mean squared error, MSE)等。将数据分析者通过接收到的扰动数据所得到的基于本地差分隐私机制的统计分析结果与真实数据的数值相比较。以属性A中各项的频率举例，属性域$A=\{a_1,a_2,\cdots,a_d\}$，基于扰动后各项数据的频率以及所使用的隐私机制得到真实频率的估计值$\hat{f}_{v_i}(v_i\in A)$，然后与真实的频率$f_{v_i}(v_i\in A)$相比较。

在信息损失度量法中可以用KL散度衡量两个概率分布之间的差异。假设$P(x)$和$Q(x)$是随机变量x上的两个概率分布，在个性化本地差分隐私模型中可以对应真实数据的频率分布和相应的估计值。误差或者信息损失值越小，则说明估计结果越接近于真实值，学者们在设计个性化本地差分隐私机制时需要在保护用户隐私安全的同时兼顾数据的可用性。

1.3.3　通信开销

在个性化本地差分隐私中，用户在本地对数据进行扰动处理后将加噪的数据发送给服务器，这里通信开销指的是用户设备与服务器之间交换数据所需要的带宽。例如在随机可聚合的隐私保护序数响应(Randomized aggregatable privacy preserving ordinal response，RAPPOR)[81]机制中数据域的大小为d，每个用户需要发送长度为d的比特串给服务器，因此通信开销为$O(d)$。

1.3.4　计算开销

个性化本地差分隐私中的计算开销分为用户端的计算开销和服务器端的计算开销两部分。在用户端需要对原始数据进行编码和扰动处理，一般计算开销取决于具体的编码和扰动方案，例如在RAPPOR中需要用户端对长度为d的比特串的每一位随机翻转，因此用户端的计算开销为$O(d)$；在服务器端收集到所有用户提交的扰动数据后一般需要做聚合处理，计算开销取决于具体的聚合方法，例如在RAPPOR中服务器需要对n个用户的所有数据计数然后聚合，因此服务器端的计算开销

为$O(nd)$。

2 用户层面的个性化

用户层面的个性化本地差分隐私机制主要是通过允许用户自由选择隐私预算/隐私级别或是自由地划分隐私预算来实现隐私的个性化。现有的关于用户层面个性化本地差分隐私的工作主要聚焦于频率估计[23-27]、在线最小二分匹配[29]、移动群智感知[30]以及联邦学习等任务[32]。本节根据任务目标的不同将用户层面的个性化本地差分隐私机制进行分类,并对它们所采用的扰动方法和聚合方法进行分析和总结。表2总结了本文所调研的文献中,作者在用户层面的个性化本地差分隐私机制领域常考虑的任务目标和常用的技术。

表2 用户层面的个性化本地差分隐私机制总结

Table 2 Summary of PLDP mechanisms

任务目标	随机化算法	个性化方案	数据聚合方法
类别型数据频率估计	基于布隆过滤器的随机响应机制[23]	用户自由选择隐私预算	加权组合法
类别型数据频率估计	RAPPOR[24]	用户自由选择隐私级别	加权组合法和数据回收法
类别型数据频率估计	最优扰动参数的RAPPOR[25]	用户自由选择隐私预算	加权组合法
多维数据联合分布估计	OUE[27]	用户自由分配隐私预算	LASSO回归
类别型数据频率估计	自适应选择RAPPOR或k-RR[27]	用户自由选择隐私预算	加权组合法
联邦学习中保护梯度	拉普拉斯机制[28]	用户自由选择隐私预算	加权组合法
在线任务分配	基于四叉树的随机扰动[29]	用户自由选择隐私预算和敏感区域	匹配距离最近的两个位置

2.1 频率估计

本地差分隐私中的频率估计是指原始的类别型数据经过编码、扰动后发送给数据收集方,由数据收集方进行聚合、校准后得到频率估计的结果。在用户层面的个性化本地差分隐私中也是类似的过程,不过由于不同用户的隐私预算或是隐私预算分配方式不同,给数据收集方所执行的聚合、校准过程带来了挑战。

2.1.1 基于布隆过滤器的随机响应方案

Wang等[23]提出了一种基于布隆过滤器上随机响应机制的个性化本地差分隐私方案,在这个方案中用户不需要将其使用的隐私预算提交给服务器,在聚合过程中服务器根据每个用户提交的布隆过滤器中1的数量来推测用户的隐私预算,然后根据隐私预算大小决定每个扰动数据的权重,最后使用加权组合的方法得到布隆过滤器上每个比特1的数量。具体方案细节如下。

布隆过滤器由1个二进制串和一系列哈希函数组成。首先定义1个长度为l的二进制串$\boldsymbol{B}$并将所有位初始化为0,对于每一个哈希函数$H_i\in H$和任意一个类别型数据$a\in A$,计算a被H_i所映射到的$\boldsymbol{B}$中的位置,并将这个位置的值置为1。因此,可以将每个类别型数据用一个二进制串$\boldsymbol{B}$来表示。对于$\boldsymbol{B}$中的每一比特,该扰动过程为

$$B_i=1,B_i'=\begin{cases}1 & \text{依概率}(1-g)/2\\ 0 & \text{依概率}(1-g)/2\\ B_i & \text{依概率}g\end{cases}\tag{7}$$

$$B_i=0,B_i'=\begin{cases}1 & \text{依概率}(1-h)/2\\ 0 & \text{依概率}(1-h)/2\\ B_i & \text{依概率}h\end{cases}\tag{8}$$

式中g、$h\in(0,1)$,称上述的随机化策略对1是g-诚实,对0是h-诚实的,将整个策略简单地用$\langle g,h\rangle$来定义,当$g=h$时称策略是对称的。假设哈希函数的数量为m,则$\langle g,h\rangle$策略满足ε-LDP,其中$\varepsilon=m\cdot\ln\left(\frac{1+g}{1-g}\cdot\frac{1+h}{1-h}\right)$。

在个性化布隆过滤器随机响应方案中,每个用户根据自身的隐私需求选择合适的隐私预算,然后用此隐私预算在本地将数据进行扰动,最后每个用户发送给数据收集方的只有扰动后的数据,而不包括他们的隐私预算,因此频率估计的主要挑战就是如何在不知道每个用户隐私预算的条件下消除随机响应机制带来的误差。

Wang等[23]提出了一种估计每个用户隐私预算的方法和一种流形式的等式,可以用于估计布隆过滤器每一位上1的个数。根据每个用户提交的布隆过滤器中1的数量可以估计出用户的$\langle g,h\rangle$的值。将每个用户的私有布隆过滤器上为1的位置改为$\frac{h+1}{g+h}$,为0的位置改为$\frac{h-1}{g+h}$,再将所有用户的的私有布隆过滤器直接求和,求和以后每一位的值就是这一位上1的数量的估计值,进而可以得到每一个类别的频率的估计值。

2.1.2 基于RAPPOR的方案

Nie等[24]提出了一种基于RAPPOR[81]的个性

化本地差分隐私机制，将隐私预算分成不同的级别，每个用户可以根据自身的隐私需求选择不同的隐私级别，在本地用RAPPOR机制将数据扰动后，把扰动数据和其选择的隐私级别一同提交给服务器。Nie等[24]在服务器端提出了加权组合和数据回收两种聚合方法，详细说明了这两类聚合方法的过程以及优缺点，然后提出了一种将加权组合和数据回收组合起来的方法，进一步提高了频率估计的准确度。具体的方案细节如下。

假设数据域的大小为d，每个类别型数据可以用一个长度为d的比特串来表示，其对应的位置为1，剩下的都为0。RAPPOR机制通过随机翻转比特串的每一位来实现对数据隐私的保护。假设用户u所选择隐私级别为τ，对应的隐私预算为ε^τ，用户u所持有的比特串为v_u，对于比特串的任意一位，翻转概率和RAPPOR机制中一致。

(1) 加权组合法

数据收集方按照隐私级别将收集到的数据分组，假设一共有m个隐私级别，在每一个级别内按照本地差分隐私中RAPPOR的聚合方法可以得到一个概率分布，可以表示为$P=\left\{\hat{P}_1,\hat{P}_2,\cdots,\hat{P}_m\right\}$。假设隐私级别$\tau$所对应的权重为$w_\tau$，$p_i$表示$\hat{P}_\tau$中第$i$位的值，$n_\tau$表示隐私级别$\tau$下的用户个数，则最终的频率分布的估计值为$\sum_{\tau=1}^{m}w_\tau\hat{P}_\tau$，其中$w_\tau$为和$p_i$、$n_\tau$、$\varepsilon^\tau$有关的定值。

(2) 数据回收法

该方法使用用户提交的扰动数据生成其他隐私级别下的数据，增加了低隐私预算下的数据量的同时不会损害高隐私预算下的结果，可以稳定地提高估计精度。

假设服务器端所收集到的所有隐私数据为Z，现在要生成隐私预算为ε^τ的数据Z^τ。假设$\varepsilon^s=\sup\{\varepsilon^s|Z^s\in Z\&\varepsilon^s\geqslant\varepsilon^\tau\}$，$\varepsilon^i=\inf\{\varepsilon^i|Z^i\in Z\&\varepsilon^i\leqslant\varepsilon^\tau\}$，$Z_{\sup}=Z^s$，$Z_{\inf}=Z^i$。当$s=i$时，说明$Z$中存在隐私级别为$\tau$的数据，直接返回$Z^\tau$；当不存在$i$时，说明$Z$中所有数据的隐私预算都大于$\tau$，这时仅使用$Z_{\sup}$中的数据来生成$Z^\tau$，具体方法为

$$Z^\tau[i]=\begin{cases}Z_{\sup}[i] & \text{依概率}(q^s+q^\tau)/2q^s\\ \bar{Z}_{\sup}[i] & \text{依概率}(q^s-q^\tau)/2q^s\end{cases}\tag{9}$$

式中：$q^s=\dfrac{e^{\frac{\varepsilon^s}{2}}-1}{e^{\frac{\varepsilon^s}{2}}+1}$；$q^\tau=\dfrac{e^{\frac{\varepsilon^\tau}{2}}-1}{e^{\frac{\varepsilon^\tau}{2}}+1}$；$i=1,2,\cdots,d$；当$s$和$i$均存在且不相等时，$Z^\tau$由$Z_{\sup}$和$Z_{\inf}$联合生成，当$Z_{\sup}[i]=Z_{\inf}[i]$时，扰动概率为

$$Z^\tau[i]=\begin{cases}Z_{\sup}[i] & \text{依概率}(1+f_1+g_1)/2\\ \bar{Z}_{\sup}[i] & \text{依概率}(1-f_1-g_1)/2\end{cases}\tag{10}$$

当$Z_{\sup}[i]\neq Z_{\inf}[i]$时，扰动概率为

$$Z^\tau[i]=\begin{cases}Z_{\sup}[i] & \text{依概率}(1+f_2-g_2)/2\\ Z_{\inf}[i] & \text{依概率}(1-f_2+g_2)/2\end{cases}\tag{11}$$

式中：$f_1=\dfrac{q^\tau}{q^s}$；$g_1=\dfrac{q^s-q^\tau}{q^s}\left(1-\dfrac{1-\dfrac{q^i}{q^\tau}}{\dfrac{q^i}{q^s}+1}\right)$，$f_2=\dfrac{q^\tau-q^i}{q^s-q^i}$；$g_2=\dfrac{q^i(q^s-q^\tau)}{q^\tau(q^s-q^i)}$；$g^i=\left(e^{\frac{\varepsilon^i}{2}}-1\right)\Big/\left(e^{\frac{\varepsilon^i}{2}}+1\right)$。

数据回收法通过回收现有的隐私数据，在不影响安全性的前提下提升了总体的数据量，因此提高了统计效率。

(3) 回收再组合法

加权组合法对于高隐私预算的数据是有效的，而对低隐私预算的数据而言几乎没有作用，数据回收法则刚好相反。因此可以将两种方法组合起来使用以提高全局的数据可用性，先用数据回收法增加总体的数据量，得到每个隐私级别的频率分布估计值后，再用加权组合法得到最终的频率估计结果。

2.1.3　最优参数的PLDP方案

Li等[25]在基本RAPPOR机制的基础上提出了一种基于最优扰动参数的LDP算法，每个用户先将自己选择的隐私预算发送给服务器，服务器根据隐私预算的取值将最优的扰动参数再发送给各个用户，用户在本地按照最优扰动参数将数据扰动后再发送给服务器。方案细节如下。

首先将RAPPOR的扰动概率改写为

$$\Pr\left[v_u[i]=1\right]=\begin{cases}p & v'_u[i]=1\\ q & v'_u[i]=0\end{cases}\tag{12}$$

式中p、$q\in(0,1)$。

根据式(12)可以推出该方案的MSE为$E[\mathrm{MSE}]=\dfrac{\left(p-pe^\varepsilon+e^\varepsilon\right)^2+(d-1)e^\varepsilon}{ndp\left(1-p\right)\left(e^\varepsilon-1\right)^2}$，进而可以推导出当隐私预算为$\varepsilon$时，使得MSE最优的扰动参数值为$p=\dfrac{e^\varepsilon(d-1+e^\varepsilon)-\sqrt{e^\varepsilon(d-1+e^\varepsilon)(e^\varepsilon d-e^\varepsilon+1)}}{e^{2\varepsilon}-1}$，$q=\dfrac{p}{p-pe^\varepsilon+e^\varepsilon}$。

服务器在接收到所有用户发来的扰动数据后，将相同扰动参数的数据分为一组，直接估计每一组内原始数据的频数然后将所有组的频数累和得到

最终的结果。

2.1.4 多维数据联合分布估计

Shen等[26]提出了一种在PLDP模型下用于多维数据联合分布估计的方案,允许每个用户u提交具有m_u个属性的数据,然后每个用户根据自己的隐私需求将隐私预算$m_u\varepsilon$分配给m_u个属性,具体的分配方式不需要提交给服务器,然后用OUE[67]机制分别扰动m_u个属性再将扰动数据上传给服务器;服务器端用平均隐私预算ε估计每个属性中各个维度的计数,再用最小绝对收缩和选择算子(Least absolute shrinkage and selection operator,LASSO)回归估计出各个数据间的联合分布。具体的方案如下。

用户u持有一个m_u维的数据,其中每个维度表示一个属性,用户u的总隐私预算为$m_u\varepsilon$,其中ε被称为平均隐私预算,每个用户的平均隐私预算是相等的,用户u根据自身的隐私需求将总隐私预算为$m_u\varepsilon$分配给每一个属性,例如某一个属性表示性别,用户u并不在意自己的性别被泄露出去,就可以给性别这个属性分配较多的隐私预算。隐私预算分配完成以后,用户在本地使用优化的一元编码(Optimized unary encoding,OUE)机制扰动每一个属性,然后将扰动后的数据发送给服务器,服务器不需要知道隐私预算的具体分配方式。

服务器端接收到所有用户发来的数据以后,针对每一个属性,服务器端按照OUE机制的聚合方法用平均隐私预算ε恢复出每个属性中各个维度值的频率。然后使用LASSO回归的方法得到各个维度数据间的联合分布。

2.1.5 自适应个性化数据收集方案

Song等[27]基于k-随机响应(k-randomized response,k-RR)[82]机制提出了一种自适应个性化数据收集方案用于频率估计,根据RAPPOR和k-RR机制在不同隐私预算下统计有效性的不同,用户在扰动数据时自适应地选择最优的扰动机制。具体的方案如下。

RAPPOR机制的MSE可以表示为$\mathrm{MSE}_{\mathrm{RAPPOR}}=\frac{d\mathrm{e}^{\frac{\varepsilon}{2}}}{n\left(\mathrm{e}^{\frac{\varepsilon}{2}}-1\right)^2}+\frac{1}{n}$,$k$-RR机制的MSE可以表示为$\mathrm{MSE}_{k\text{-RR}}=\frac{d(\mathrm{e}^{\varepsilon}+d-2)}{n(\mathrm{e}^{\varepsilon}-1)^2}+\frac{\mathrm{e}^{\varepsilon}+d-3}{n(\mathrm{e}^{\varepsilon}-1)}$。不难发现当$\varepsilon<\varepsilon_*=2\ln\left(\sqrt[3]{u+v}+\frac{4-3d^2}{9d^2\sqrt[3]{u+v}}-\frac{2}{3d}\right)$时,$\mathrm{MSE}_{\mathrm{RAPPOR}}<\mathrm{MSE}_{k\text{-RR}}$,当$\varepsilon>\varepsilon_*$时,$\mathrm{MSE}_{\mathrm{RAPPOR}}>\mathrm{MSE}_{k\text{-RR}}$,其中$u=\frac{d^2(18+27b)-16}{54d^3}$,$v=\frac{\sqrt{3\left[d^2(4a+27b^2)+32(3k-2)\right]}}{18d^2}$,$a=10d^2+27d+9$,$b=d^2-3d+2$。

用户首先在本地根据自身的隐私需求选择合适的隐私预算,然后将隐私预算发送给服务器,服务器按照最小MSE准则给每个用户发送不同的扰动方案,用户按照自己的扰动方案将数据扰动后再提交给服务器。服务器接收到所有扰动数据后,根据隐私预算的不同将所有扰动数据分组,分析出每一组内的概率分布然后将所有隐私预算的概率分布组合起来得到最终的频率估计结果。

2.2 其他应用

2.2.1 联邦学习

近年来,联邦学习作为一种先进而且实用的解决方案,被应用于解决分布式多方联邦建模中的隐私保护问题。然而,现有的联邦学习方法大多集中在相同的隐私保护预算上,而忽略了参与者的各种隐私要求。Yang等[28]提出了一种基于PLDP模型的算法,允许用户在自己选择的隐私级别上对梯度进行扰动后再上传给服务器。方案细节如下。

假设一共有n个用户和1个服务器,每个客户端有一些样本数据和隐私预算,单个客户端的数据不足以用于训练,因此需要客户端之间相互合作。首先服务器端随机选择$M=Cn$个客户端,其中$C\in[0,1]$,然后服务器端向被选中的客户端广播全局参数w_t;将客户端的样本切成大小为B的批次,每个客户端在本地采用E个本地历元,然后以学习率为η的迭代方式在每个历元的各个批次上计算梯度;假设用户u最终计算出的梯度设为g_u,则$\hat{g}_u=g_u+\mathrm{Lap}\left(\frac{S}{\varepsilon^\tau}\right)$,其中$\mathrm{Lap}\left(\frac{S}{\varepsilon^\tau}\right)$表示拉普拉斯随机数,$\varepsilon^\tau$为用户所选择的隐私预算,$S=\mathrm{median}\{g_u\}$,每个客户端将计算出的梯度发送给服务器。服务器在接收到所有M个客户端发来的梯度后,用加权组合的方法得到最终梯度为$\tilde{g}=\sum_{i=1}^{M}\lambda_i\hat{g}_i$,其中$\lambda_i=\frac{\phi_i}{\sum_{i=1}^{M}\phi_i}$,$\phi_i=\frac{1}{\sum_{j=1}^{n}\left[\mathrm{Var}\left[\hat{g}_i[r][j]\right]+\sigma_k^2\right]}$。

2.2.2 在线最小二分匹配

在很多移动应用中,用户需要向服务器提供位置以完成服务,然而不可信的服务器却不能保证用户的位置数据安全。因此Lv等[29]研究了个性化本地差分隐私中在线最小二分匹配的问题,用户根据

自身的隐私需求选择隐私预算,并且不将隐私预算提交给服务器,而是将1个平面用四叉树表示,给四叉树上每一个结点编号,用户选择1个隐私范围后将自己所在位置的编号扰动提交给服务器,服务器根据动土距离(Earth mover's distance,EMD)最近的准则匹配用户和任务。具体方案如下。

首先将平面区域用四叉树表示,假设平面区域是1个正方形,将其编号为0,表示四叉树的根节点,可以将0号区域再分割成4个大小相等的正方形,分别编号为1、2、3、4表示四叉树第1层的4个节点,然后递归地分割下去,四叉树第i层的结点数量为4^i,而且层数越高意味着分割得越细。每个用户先根据自身的隐私需求选择合适的隐私预算以及一个隐私区域,假设用户u的隐私预算为ε_u并将隐私区域设置为四叉树的第一层,如果用户u的真实位置在结点1所表示的区域内,则就用1表示用户u的真实数据。扰动概率为

$$\Pr[i'_u|i_u]=\begin{cases}\dfrac{\mathrm{e}^{-\varepsilon_u|i_u-i'_u|}}{\mathrm{e}^{-\varepsilon_u}+1} & i'_u\in B_{h_u}\\ \dfrac{(1-\mathrm{e}^{-\varepsilon_u})\mathrm{e}^{-\varepsilon_u|i_u-i'_u|}}{\mathrm{e}^{-\varepsilon_u}+1} & i'_u=i_u\end{cases}\tag{13}$$

式中$|i_u-i'_u|$表示两个节点编号值的差的绝对值,$B_{h_u}=\left\{\dfrac{4^{h_u}-1}{3},\dfrac{4^{h_u+1}-1}{3}-1\right\}$,$h_u$为$i_u$所在的层数。

服务器接收到所有用户的扰动数据后,将EMD距离最近的工人和任务匹配在一起,工人和任务之间再通过别的信道获取对方的真实位置。

3　数据层面的个性化

数据层面的个性化设置可以分为两类:第一类为ID-LDP[47-55];第二类为Metric LDP[56-77]。在ID-LDP中通过给不同敏感程度的数据分配不同的隐私预算实现个性化,给敏感程度较高的数据分配较低的隐私预算而给敏感程度较低的数据分配较高的隐私预算,保证了用户隐私安全的同时相较于传统的本地差分隐私机制还提升了数据的效用;在Metric LDP中的做法是将扰动概率与数据间的度量联系起来,两个数据间的扰动概率与它们之间的度量值成反比,意味着一个数据更容易被扰动到在度量上和它更为接近的数据,这种方法也提升了数据的效用。

3.1　ID-LDP

在传统的LDP机制中,所有数据的隐私预算是统一的,用相同的方式扰动所有的输入数据,但是在许多现实场景中,不同的数据具有不同的敏感度(例如在网页点击或者医疗记录中,癌症或者传染病比其他症状更敏感),用户很可能不希望敏感度较高的数据被透露出去,对于敏感度较低的数据则不需要过多的保护。在传统的LDP机制中一方面对于敏感数据的保护不足,另一方面对非敏感数据提供了过多的保护,这会影响统计结果的有效性。出于这样的考虑,Gu等[47]提出了ID-LDP,给不同敏感度的数据分配不同的隐私预算,不仅使得隐私机制更符合现实需要,而且提高了数据可用性。此外还有ULDP[48]、高-低-LDP(High-low-LDP, HL-LDP)[49]、(ε,δ)-ULDP[50]等,可以看作是ID-LDP的变体。表3概述了这些工作的性能和评估方法。

表3　ID-LDP机制归纳总结

Table 3　Summary of ID-LDP mechanisms

任务目标	随机化算法	个性化方案
类别型数据频率估计	基于独热向量随机扰动的优化方法[47]	将数据域分为m个隐私级别
	uRR、uRAPPOR[48]	将数据域分为敏感与非敏感两类
	uHR[49]	将数据域分为敏感与非敏感两类
	uRFM-GRR、uRFM-RAPPOR、uRFM-OLH[50]	将数据域分为敏感与非敏感两类

3.1.1　MinID-LDP

为了实现对每个输入提供不同程度的隐私保护,Gu等[47]首先提出了ID-LDP的概念,并提出了ID-LDP的一个实例MinID-LDP,然后基于MinID-LDP和OUE机制提出了一个扰动算法,而且设计了3种优化算法来找到MSE最优的机制。方案细节如下。

假设一共有n个用户,数据域为$A=\{a_1,a_2,\cdots,a_d\}$,将隐私预算分为m个级别,服务器端根据输入数据敏感程度的不同分配不同的隐私级别。每个输入数据可以用一个长度为d的独热向量表示,对于a_i它的第i个位置为1,其他位置都是0。在扰动时对向量的每一位独立地扰动,假设输入向量为$\boldsymbol{x}$输出为$\boldsymbol{y}$,具体扰动概率为

$$\begin{cases}\Pr[\boldsymbol{y}[k]=1|\boldsymbol{x}[k]=1]=a_k\\ \Pr[\boldsymbol{y}[k]=0|\boldsymbol{x}[k]=1]=1-a_k\\ \Pr[\boldsymbol{y}[k]=1|\boldsymbol{x}[k]=0]=b_k\\ \Pr[\boldsymbol{y}[k]=0|\boldsymbol{x}[k]=0]=1-b_k\end{cases}\tag{14}$$

式中$a_k>b_k$,为了满足ID-LDP的定义,对于任意两个数据a_i、a_j需要满足$\dfrac{a_i(1-b_j)}{b_i(1-a_j)}\leqslant\mathrm{e}^{r(\varepsilon_i,\varepsilon_j)}$,该方案实现了不同数据间有不同的扰动概率,可以用于类别型数据的频率分布估计,并且可以将该方案的

MSE推导出来，但是关于每个输入数据的具体扰动概率还并不清楚，为了保证数据的可用性，在MiniID-LDP模型下3种优化方法分别是：基于最差情况下MSE的优化方法、基于RAPPOR的优化方法和基于OUE的优化方法。从理论和实验中都可以看出基于ID-LDP的方案比传统的LDP方案具有更好的统计有效性。

当用户的输入是一个集合，即包含多个类别型数据时，可以用修剪或者填充的方法将集合的大小固定为l，再从大小为l的集合中均匀随机地抽样一个元素，然后按照输入为单个元素时的扰动方法将抽样得到的数据扰动后再提交给服务器。

3.1.2 ULDP

ULDP可以看作是ID-LDP的一个特例，在ULDP中将数据分为敏感和非敏感两类，所有敏感数据使用同样的隐私预算，而非敏感数据的隐私预算可以看作是无穷大。在ULDP中所有数据都可以被扰动为敏感数据，扰动方式和LDP中保持一致，而非敏感数据只可能来自它本身。基于这样的扰动方式，对于敏感数据而言提供了与LDP下相同的隐私保护效果，而对于非敏感数据则不做任何保护，对于统计有效性来说是有益的。Murakami等[48]基于随机响应和RAPPOR提出了ULDP环境下的两个扰动机制效用优化的随机响应(Utility optimized randomized response，uRR)和效用优化的RAPPOR(Utility optimized RAPPOR，uRAPPOR)，并且从理论和实验上证明了在ULDP环境下的统计有效性表现更好。

uRR机制可以用于类别型数据的隐私保护和频率估计，假设用户u的原始数据为v，则在(A_S,ε)-uRR机制满足非敏感数据可以扰动为自身或者随机的敏感数据，敏感数据内部则满足广义随机响应(Generalized random response，GRR)[82]机制。

在(A_S,ε)-uRAPPOR机制中将所有的数据用长度为d的独热向量表示，第i个数据的向量中除第i位为1以外其余位置都为0，扰动方法仍然满足非敏感数据可以扰动为自身或者随机的敏感数据，敏感数据内部则满足RAPPOR机制。

从上述介绍中可以看出对于敏感数据而言，uRR和uRAPPOR机制提供了与LDP环境下的GRR和RAPPOR机制相同的隐私保护，对于非敏感数据uRR和uRAPPOR机制不提供保护，在保证了敏感数据安全的前提下提升了统计有效性。

3.1.3 HL-LDP

Acharya等[49]提出了一种与ULDP类似的HL-LDP的概念，基于HL-LDP和哈达玛随机响应(Hardmard response，HR)机制[83-84]设计了一种效用优化的哈达玛随机响应方案(Utility optimized hardmard response，uHR)，该方案和uRAPPOR具有相同的样本复杂度，但通信开销要小得多。具体方案如下。

假设在属性域$A=[1:d]$中$A_S\subseteq A$为敏感数据组成的集合，$A_N=A\backslash A_S$为非敏感数据组成的集合，假设输出域为Y，设$Y_P\subseteq Y$为受保护数据组成的集合，$Y_I=Y\backslash Y_P$为可逆数据组成的集合。$S=2^{\lceil\log_2(|A_S|+1)\rceil}$，$\boldsymbol{H}_S$为$S$阶哈达玛矩阵[84]，有关哈达玛矩阵的性质在本文中不再过多描述。uHR机制的扰动过程与uRR和uRAPPOR中类似，仍然满足非敏感数据可以扰动为自身或者随机的敏感数据，敏感数据内部则满足HR机制[84]。

在uHR用户提交给服务器一个用来表示类别型数据的序号，即可通信开销为$\Theta(1)$，而在uRAPPOR用户需要提交给服务器长度为d的比特串通信开销为$\Theta(d)$。同时uHR的样本复杂度和统计有效性和uRAPPOR持平。

3.1.4 (ε,δ)-ULDP

基于ULDP和(ε,δ)-LDP，Zhang等[50]提出了(ε,δ)-ULDP的定义。基于GRR、RAPPOR和优化的本地哈希(Optimized local hashing，OLH)[85]机制分别提出了3个满足(ε,δ)-ULDP的扰动机制，对于敏感数据的扰动仍然满足相应的(ε,δ)-LDP，对于非敏感数据以一定概率扰动为自身或者扰动为敏感数据中的任何一个。由于在(ε,δ)-LDP和ULDP模型下的扰动机制相较于LDP下的扰动机制，在数据可用性方面本就具有优势，文献[50]将这两个模型结合起来，所提出的扰动机制使统计效用进一步提升。

3.2 Metric LDP

地理位置数据的隐私保护一直是本地差分隐私研究中的一项重要内容，Andrés等[56]提出了地理不可区分模型的概念，可以用于保护地理位置数据隐私，它基于地理位置数据的距离，实现了εd_2-LDP，其中d_2为二维欧式距离，满足距离越近的两个数据间的扰动概率越大，相比标准的LDP具有更好的效用。将度量d_2推广为更一般的情况便有了Metric LDP。Bordenabe等[56-57]在地理不可区分模型下分别设计了基于二维拉普拉斯分布和优化方法的两个扰动机制，可以在基于位置的服务(Location based service，LBS)中保护地理位置数据的安全；Tao等[58]在地理不可区分模型下基于良好分离树(Hierarchically well-separated trees，HST)提出了一种扰动机制，可以用于最小二分匹配中地理

位置数据的隐私保护，同时保证了在任务分配等场景下的实用性；Zhao 等[59]提出了一种基于马氏距离的位置数据扰动方案，用户在本地给二维位置数据加上椭圆噪声扰动为新的二维坐标后再发送给服务器，在方向分析相关的应用中相较于传统的圆形噪声方案[56]有更高的准确度；Weggenmann 等[60]基于 Von Mises-Fisher 分布[86-87]和 Purkayastha 分布[88]提出了两个扰动机制用于方向数据的隐私保护；Du 等[61]将 Weggenmann 等的方案应用到了句子嵌入中；Gursoy 等[62]提出了 CLDP 的概念，可以看作是 Metric LDP 在离散型数据下的版本。表 4 总结了 Metric LDP 中具有代表性的工作，包括这些工作的任务目标、所针对的数据类型和相应的度量以及扰动算法。表 5 分别从隐私保护强度、数据可用性、计算开销和通信开销 4 个方面对这些工作的性能做了总结。

表 4　Metric LDP 机制归纳总结

Table 4　Summary of Metric LDP mechanisms

任务目标	数据类型	度量	扰动算法
基于地理位置的服务	二维地理位置数据	二维欧氏距离	平面拉普拉斯机制[56]
基于地理位置的服务	二维地理位置数据	二维欧氏距离	优化方法[57]
在线任务分配	二维地理位置数据	二维欧氏距离	基于 HST 的随机扰动算法[58]
方向分布估计	二维地理位置数据	马氏距离	基于马氏距离的指数机制[59]
方向数据均值估计、分布估计等	方向数据	余弦相似度	VMF 机制、Pur 机制[60-61]
离散型数据频率估计、Top-k 估计等	离散型数据	离散型数据的排序	指数机制[62]

表 5　PLDP、ID-LDP 和 Metric LDP 机制性能对比和评价方法

Table 5　Comparison and evaluation methods for PLDP, ID-LDP and Metric LDP mechanisms

隐私保护模型	技术方案	隐私保护强度	数据可用性	通信开销	计算开销	
					用户端	服务器端
PLDP	基于布隆过滤器的随机响应方案[23]	较高	中等	$O(d)$	$O(d)$	$O(nd)$
	基于 RAPPOR 的方案[24]	较高	较高	$O(d)$	$O(d)$	$O(nd^2)$
	最优扰动参数的 PLDP 方案[25]	较高	中等	$O(d)$	$O(d)$	$O(nd)$
	多维数据联合分布估计方案[26]	中等	较高	$O(kd)$	$O(kd)$	$O(nkd)$
	自适应个性化数据收集方案[27]	较高	中等	$O(\log d)$或$O(d)$	$O(1)$或$O(d)$	$O(nd)$
	基于拉普拉斯机制的方案[28]	较高	中等	$O(1)$	$O(1)$	$O(n)$
	基于四叉树的随机扰动方案[29]	较高	中等	$O(1)$	$O(1)$	$O(n)$
ID-LDP	基于独热向量随机扰动的方案[47]	较高	中等	$O(d)$	$O(d)$	$O(nd)$
	基于 GRR 和 RAPPOR 的方案[48]	中等	较高	$O(\log d)$或$O(d)$	$O(1)$或$O(d)$	$O(n+d)$或$O(nd)$
	基于 HR 的方案[49]	中等	较高	$O(\log d)$	$O(1)$	$O(n)$
	基于(ε,δ)-LDP 的方案[50]	中等	较高	$O(\log d)$或$O(d)$	$O(1)$或$O(d)$	$O(n+d)$或$O(nd)$
Metric LDP	基于平面拉普拉斯机制的方案[56]	中等	中等	$O(1)$	$O(1)$	$O(n)$
	基于优化方法的方案[57]	中等	较高	$O(1)$	$O(1)$	$O(n)$
	基于 HST 的随机扰动方案[58]	中等	较高	$O(1)$	$O(D)$	$O(D)$
	基于马氏距离的方案[59]	中等	较高	$O(1)$	$O(1)$	$O(n)$
	基于余弦相似度的方案[60-61]	较高	较低	$O(1)$	$O(1)$	$O(n)$
	基于离散型数据排序的方案[62]	较高	中等	$O(\log d)$	$O(1)$	$O(n+d)$

3.2.1　地理不可区分

随着基于地理位置的服务越来越普及，有许多不可信的服务器开始大量收集用户的地理位置数据，引起了严重的隐私安全问题。在传统的本地差分隐私机制中一般将地理位置数据离散化，然后使用现有的针对离散型数据的本地差分隐私机制扰动地理位置数据，这种方法往往会使得数据的可用性降低。因此 Andrés 等[56]提出了地理不可区分的概念，可以看作是基于平面欧式距离的度量本地差分隐私模型。目前已经有许多关于地理不可区分模型的工作，其中最具代表性的是 Andrés 和 Bordenabe 等[56-57]及 Tao 等[58]的工作。

文献[56-57]分别基于二维拉普拉斯分布和优化方法设计了两个扰动机制，可以在基于位置的服

务或者是位置数据的分布估计中保护地理位置数据的隐私安全。在平面拉普拉斯机制中，用二维直角坐标表示每个用户的位置数据，假设输入为v，输出为v'，则扰动概率密度函数为$f(v'|v)=\frac{\varepsilon^2}{2\pi}e^{-\varepsilon d_2(v,v')}$，可以看作是给原始数据$v$加上了满足参数为$\varepsilon$和1的二维拉普拉斯分布的随机数。在实践中可以先均匀随机地抽样一个任意方向的单位向量x，再从伽马分布$\Gamma\left(2,\frac{1}{\varepsilon}\right)$中抽样随机数$l$作为噪声向量长度，再令$v'=v+lx$，服务器最终收集所有用户提交的扰动数据。在基于优化方法的机制中，主要目标是在满足地理不可区分性的前提下使数据可用性损失最小，Bordenabe等[57]提出了名为OptGI的扰动机制。在OptGI中首先将平面区域划分为若干个大小和形状都相同的小区域，然后用每个小区域几何中心的坐标代替整个区域范围内的点。假设位置v被扰动为位置v'的概率为$k_{vv'}$，π为所有位置的先验概率分布，$d_2(v,v')$表示位置v、v'间的欧氏距离，则效用损失可以表示为$\sum_{v,v'}\pi_v k_{vv'}d_2(v,v')$，可以通过式(15)所示的优化方法求出最优的扰动概率。

$$\begin{cases}\min\sum_{x,z}\pi_v k_{vv'}d_2(v,v')\\ \text{s.t. } k_{vv'}\leqslant e^{\varepsilon d_2(v,\hat{v})}k_{\hat{v}v'}\\ \quad\sum_{v'}k_{vv'}=1\\ \quad k_{vv'}>0\end{cases}\tag{15}$$

基于式(15)设计的扰动机制实现了效用损失的最优化，但是需要将地理位置离散化可能会对服务精度造成影响，而且这种优化方法的计算开销很大，还会受到区域范围大小的影响，相较而言，平面拉普拉斯机制所针对的是连续数据而且计算和通信开销都很友好。

针对地理不可区分模型下的任务分配问题，Tao等[58]提出了一种基于良好分离树的扰动方案。在任务分配的场景中有3个组成部分，分别是工人、任务和服务器，工人和任务分别持有一个位置数据，服务器将距离最近的工人和任务匹配在一起，这会导致工人和任务的位置数据安全受到威胁。可以用预先定义好的位置数据构建出高度为D，度为c的良好分离树，每个叶子结点可以表示大小相等的一块位置区域并且每两个叶子结点表示的区域互不相交，工人和任务在将自己的位置提交给服务器前，先将自己的位置用良好分离树上的一个叶子结点表示，再通过随机游走的方法将真实的叶子结点扰动为任意一个叶子结点后将扰动结点的编号提交给服务器。服务器收到工人和任务提交的结点编号后将距离最近的工人和任务匹配，工人和任务之间可以通过别的信道获取对方当前的真实位置。

3.2.2 方向分布估计

方向分布分析(即标准偏差椭圆)可以用来识别一组数据的方向以及分布的趋势。在方向分布分析中有时需要收集用户的地理位置和健康状况，当这些信息被不可信的第三方使用和共享时，存在用户隐私泄露的风险。目前已经有许多有效的方法来保护用户的位置隐私，但是这些方法都会导致方向分布的分析不准确，例如在平面拉普拉斯机制中可以看做是在以真实位置为圆心的圆上均匀随机的扰动，而Zhao等[59]提出了一种基于马氏距离的位置数据扰动方案，给真实位置添加椭圆噪声，可以使真实数据以更高概率沿着真实分布的方向扰动。

在平面拉普拉斯机制中扰动概率的密度函数正比于$e^{-\varepsilon d_2(v,v')}$，在椭圆噪声中则正比于$e^{-\varepsilon d_M(v,v')}$，其中$d_M(v,v')$表示点$v$、$v'$间的马氏距离，马氏距离中的参数通过预先知道一些数据计算得到。相当于在以真实位置为圆心，方向和形状确定的椭圆上均匀随机地扰动，相较于平面拉普拉斯机制给真实数据添加圆形噪声，这种扰动方式在保护了用户数据安全的同时提高了方向分布的准确性。

3.2.3 方向数据

方向数据是一类重要的数据，其中数据点的大小可以忽略，比如周期型数据(时间或者1周中的某一天)可以看作是1个二维单位向量，向量的方向就足以表示时间的值，地理位置数据也可以看作是三维单位球上的一点，可以用三维单位向量的方向来表示。在移动感知等场景下经常需要收集用户的方向数据，其中不乏一些敏感信息，Weggenmann等[60]基于Von Mises-Fisher分布和Purkayastha分布(简称VMF分布和Pur分布)提出了两个扰动机制用于方向数据的隐私保护，满足以余弦相似度为度量的Metric LDP。

VMF分布和Pur分布中都各有2个参数，分别为浓度参数和基准向量，可以表示在n维单位球上向量的分布情况，其中浓度参数越大则分布越集中于基准向量。因此可以将VMF分布和Pur分布用于隐私保护中，其中隐私预算代表浓度参数，用户的输入为基准向量，从这两个分布中随机抽样一个向量作为扰动值输出，可以满足以余弦相似度为度量的Metric LDP。VMF分布和Pur分布的概率密度函数分别为$\mathrm{VMF}(\mu,\kappa)[x]=C_{\mathrm{VMF}}(n,\kappa)e^{\kappa\mu^{\mathrm{T}}x}$，$\mathrm{Pur}(\mu,\kappa)[x]=C_{\mathrm{Pur}}(n,\kappa)e^{-\kappa\arccos(\mu^{\mathrm{T}}x)}$，其中$\kappa$为浓

度参数,μ为基准向量,n为向量的维度。

这两种扰动机制可以应用于周期型数据,例如一天 24 h的均值估计;若将地理位置看作是三维单位球上的一点,也可用于地理位置数据的分布估计。在NLP中句子的嵌入一般也是一个n维的单位向量,因此Du等[61]将这两种扰动机制应用到了NLP的句子嵌入中,在保护了用户数据隐私的同时保证了NLP的可用性。

3.2.4　离散型数据

因为涉及度量,所以通常Metric LDP方案都应用于连续型数据,Gursoy等[62]提出了浓缩LDP(Condensed LDP, CLDP)的概念,可以看作是Metric LDP在离散型数据下的版本,因此可用于离散型数据的分布估计、Top-k估计等工作。

Gursoy等[62]通过将一组离散型数据排序来定义各个数据之间的度量值的大小,每两个数据在排序中的差值就是它们之间的度量值,问题在于排序该如何确定。对于本身不存在顺序关系的数据,服务器首先任意假定1组排序,然后1组用户根据假设的排序利用指数机制将数据扰动后提交给服务器,服务器接收到第1组扰动数据以后,根据第1组扰动数据的情况再次给数据排序,并将新的排序结果发送给用户,第2组用户用新的排序结果利用指数机制将数据扰动后提交给服务器,服务器用第2次接收到的扰动数据进行分布估计或Top-k估计等工作。

4　总结与展望

本文深入分析了现有的个性化本地差分隐私机制,分别为用户层面的个性化机制和数据层面的个性化机制,同时又将数据层面的个性化机制分为了ID-LDP和Metric LDP两种。总结了近几年有关个性化本地差分隐私机制的代表性工作,并详细介绍了这些工作的任务目标、扰动算法和后处理方法等。

近年来有关个性化本地差分隐私的方法和思想不断涌现,相比较传统的隐私机制它可以为每个用户和数据提供更为精准的隐私保护,同时也提高了统计分析的准确性和各类服务的质量。然而,随着技术的不断发展以及对数据安全和有效性要求的不断提高,PLDP、ID-LDP和Metric LDP技术在不同方面仍有提升空间。

4.1　PLDP技术展望

在PLDP机制中将隐私预算分为不同级别,一般可供用户选择的级别有限,无法严格地满足所有用户的隐私需求;扰动数据的后处理方法有加权组合法和数据回收法两种,但是加权组合法对于隐私预算较小数据的有效性并不友好,而且依赖于各个隐私级别下的用户人数,数据回收法只适用于RAPPOR机制。为了解决上述问题需要一种允许用户更加自由地选择隐私预算的方案,以及配套的扰动方法和后处理方法,可以兼顾用户隐私需求的多样性、数据的安全性和可用性。

现有的PLDP机制集中于类别型数据频率估计的工作,但是在实际中还存在很多其他任务目标,例如用户输入为集合型数据时的频率估计、连续型数据均值估计、基于地理位置的服务、动态变化的数据隐私保护以及很多非结构化数据的隐私保护等。针对不同的任务目标需要考虑不同的个性化方案、扰动方法和后处理方法等,将PLDP推广到更多的应用场景仍需更加深入的研究。

4.2　ID-LDP技术展望

在MiniID-LDP方案中虽然实现了给不同数据分配不同隐私预算,但随之而来的是高额的计算开销和数据效用的损失,并且当大多数的数据隐私预算较小时对效用的影响非常大,而在其他方案中仅将数据分为敏感和非敏感两类无法满足不同数据的多级隐私需求。可以尝试设计不依赖于优化方法的ID-LDP机制,只需要确定各个数据的隐私预算即可直接获得各个数据间的扰动概率以减少计算开销。MiniID-LDP中所使用的度量函数导致隐私预算较低的数据会对效用造成更大的影响,是否存在更优秀的度量函数来设计ID-LDP机制,兼顾数据的安全性和可用性,是一个值得研究的问题。

此外,与PLDP机制类似,目前ID-LDP机制的使用场景也非常有限,主要集中于有关类别型数据频率估计的工作,能否能将ID-LDP推广到更加广泛的场景中也非常有研究价值。

4.3　Metric LDP技术展望

现有的Metric LDP机制中服务器接收到用户发来的扰动数据后都不会做任何后处理,一方面是因为在Metric LDP模型下后处理的难度较大,另一方面是因为在很多场景下(例如基于地理位置的服务、在线任务分配、方向分布估计等)并不需要对扰动数据做任何处理。但是在进行分布估计、离散型数据频率估计和均值估计等工作时,直接使用扰动数据会对效用造成很大的影响甚至效果不如传统的本地差分隐私机制。而且目前Metric LDP机制的扰动方法非常有限,对于连续型数据一般使用拉普拉斯机制,离散型数据则是指数机制,这两种扰动方法的效果并不出色。综合以上两个问题,针对不同的场景设计更加优秀的Metric LDP扰动机

制以及相应的后处理方法非常有必要,可以在很大程度上提高服务质量和数据可用性。

针对离散型数据的Metric LDP机制工作很少,主要是因为离散型数据的度量难以定义。在CLDP中一般用各个项目间的排序作为度量,但是在很多时候各个项目之间并不一定存在顺序关系,在CLDP中采用用户端和服务器端多次交互的方式假定出一个排序关系,但是这对数据的安全性和效用都会造成影响。目前也没有关于输入为集合型数据的频率估计、频繁项集挖掘等场景下的Metric LDP机制的工作。如何改善现有的有关离散型数据的Metric LDP机制以及将Metric LDP应用到更多离散型数据隐私保护的场景中也是值得深入研究的问题。

参考文献:

[1] CHENG X, FANG L, YANG L, et al. Mobile big data: The fuel for data-driven wireless[J]. IEEE Internet of Things Journal, 2017, 4(5): 1489-1516.

[2] GUO B, WANG Z, YU Z, et al. Mobile crowd sensing and computing: The review of an emerging human-powered sensing paradigm[J]. ACM Computing Surveys, 2015, 48(1): 1-31.

[3] SHU J, JIA X, YANG K, et al. Privacy-preserving task recommendation services for crowdsourcing[J]. IEEE Transactions on Services Computing, 2018, 14(1): 235-247.

[4] LU R, JIN X, ZHANG S, et al. A study on big knowledge and its engineering issues[J]. IEEE Transactions on Knowledge and Data Engineering, 2018, 31(9): 1630-1644.

[5] FUNG B C M, WANG K, CHEN R, et al. Privacy-preserving data publishing: A survey of recent developments[J]. ACM Computing Surveys, 2010, 42(4): 1-53.

[6] ZHU T, LI G, ZHOU W, et al. Differentially private data publishing and analysis: A survey[J]. IEEE Transactions on Knowledge and Data Engineering, 2017, 29(8): 1619-1638.

[7] YANG Y, WU L, YIN G, et al. A survey on security and privacy issues in internet-of-things[J]. IEEE Internet of things Journal, 2017, 4(5): 1250-1258.

[8] SORIA-COMAS J, DOMINGO-FERRER J. Big data privacy: Challenges to privacy principles and models[J]. Data Science and Engineering, 2016, 1(1): 21-28.

[9] YU S. Big privacy: Challenges and opportunities of privacy study in the age of big data[J]. IEEE Access, 2016, 4: 2751-2763.

[10] SUN Z, STRANG K D, PAMBEL F. Privacy and security in the big data paradigm[J]. Journal of Computer Information Systems, 2020, 60(2): 146-155.

[11] HINO H, SHEN H, MURATA N, et al. A versatile clustering method for electricity consumption pattern analysis in households[J]. IEEE Transactions on Smart Grid, 2013, 4(2): 1048-1057.

[12] ZHAO J, JUNG T, WANG Y, et al. Achieving differential privacy of data disclosure in the smart grid[C]//Proceedings of IEEE Conference on Computer Communications (INFOCOM). [S.l.]: IEEE, 2014: 504-512.

[13] BARBOSA P, BRITO A, ALMEIDA H. A technique to provide differential privacy for appliance usage in smart metering[J]. Information Sciences, 2016, 370: 355-367.

[14] WANG T, ZHAO J, YU H, et al. Privacy-preserving crowd-guided AI decision-making in ethical dilemmas[C]//Proceedings of the 28th ACM International Conference on Information and Knowledge Management. [S.l.]: ACM, 2019: 1311-1320.

[15] Europen Parliament, Council of the European Union. General data protection regulation[EB/OL]. (2016-01-20)[2024-07-05]. https://gdpr-info.eu/.

[16] 新华网.中华人民共和国网络安全法[EB/OL]. (2016-05-26)[2024-07-24]. http://www.xinhuanet.com/politics/2016-11/07/c_1119867015.htm.

[17] 新华网.(受权发布)中华人民共和国数据安全法[EB/OL].(2021-06-05)[2024-07-24]. http://www.xinhuanet.com/2021-06/11/c_1127552204.htm.

[18] DUCHI J C, JORDAN M I, WAINWRIGHT M J. Local privacy and statistical minimax rates[C]//Proceedings of IEEE 54th Annual Symposium on Foundations of Computer Science. [S.l.]: IEEE, 2013: 429-438.

[19] 王源源,朱友文,吴启晖,等.本地差分隐私频率估计伪数据攻击及防御方法[J/OL].软件学报,2024. https://jos.org.cn/jos/home?id=20210909102755001&name.
WANG Yuanyuan, ZHU Youwen, WU Qihui, et al. Local differential privacy frequency estimation of pseudo-data attacks and defense methods[J/OL]. Journal of Software, 2024. https://jos.org.cn/jos/home?id=20210909102755001&name.

[20] 傅培旺,丁红发,刘海,等.基于本地差分隐私的分布式图统计采集算法[J].计算机研究与发展,2024,61(7): 1643-1669.
FU Peiwang, DING Hongfa, LIU Hai, et al. Distributed graph statistical acquisition algorithm based on local differential privacy[J]. Journal of Computer Research and Development, 2024,61(7): 1643-1669.

[21] 蔡梦男,沈国华,黄志球,等.本地差分隐私下的高维数据发布方法[J].计算机科学,2024,51(2): 322-332.
CAI Mengnan, SHEN Guohua, HUANG Zhiqiu, et

al. High dimensional data publishing method under local differential privacy[J].Computer Science, 2024,51(2): 322-332.

[22] 张啸剑,付楠,孟小峰.基于本地差分隐私的空间范围查询方法[J].计算机研究与发展,2020,57(4):847-858.
ZHANG Xiaojian, FU Nan, MENG Xiaofeng. Spatial range query method based on local differential privacy[J]. Journal of Computer Research and Development, 2020,57(4): 847-858.

[23] WANG S, HUANG L, TIAN M, et al. Personalized privacy-preserving data aggregation for histogram estimation[C]//Proceedings of IEEE Global Communications Conference. [S.l.]: IEEE, 2015.

[24] NIE Y W, YANG W, HUANG L, et al. A utility-optimized framework for personalized private histogram estimation[J]. IEEE Transactions on Knowledge and Data Engineering, 2018, 31(4): 655-669.

[25] LI Fen, SONG Haina, LI Jianfeng. Personalized data collection based on local differential privacy in the mobile crowdsensing[C]//Proceedings of IEEE 6th International Conference on Computer and Communications. [S.l.]: IEEE, 2020: 2048-2052.

[26] SHEN Z, XIA Z, YU P. PLDP: Personalized local differential privacy for multidimensional data aggregation[J]. Security and Communication Networks, 2021(1): 6684179.

[27] SONG H, SHEN H, ZHAO N, et al. Adaptive personalized privacy-preserving data collection scheme with local differential privacy[J]. Journal of King Saud University-Computer and Information Sciences, 2024, 36(4): 102042.

[28] YANG G, WANG S, WANG H. Federated learning with personalized local differential privacy[C]//Proceedings of 2021 IEEE 6th International Conference on Computer and Communication Systems. [S.l.]: IEEE, 2021: 484-489.

[29] LV C, ZHANG L, LI X Y. Personalized differentially private online minimum bipartite matching in spatial crowdsourcing[C]//Proceedings of the 8th International Conference on Big Data Computing and Communications. [S.l.]: IEEE, 2022: 134-143.

[30] CHEN R, LI H, QIN A K, et al. Private spatial data aggregation in the local setting[C]//Proceedings of IEEE 32nd International Conference on Data Engineering. [S.l.]: IEEE, 2016.

[31] NIU B, CHEN Y, WANG B, et al. AdaPDP: Adaptive personalized differential privacy[C]//Proceedings of IEEE Conference on Computer Communications, [S.l.]: IEEE, 2021: 1-10.

[32] SHEN X, JIANG H, CHEN Y, et al. PLDP-FL: Federated learning with personalized local differential privacy[J]. Entropy, 2023, 25(3): 485.

[33] NIU B, CHEN Y, WANG B, et al. Utility-aware exponential mechanism for personalized differential privacy[C]//Proceedings of 2020 IEEE Wireless Communications and Networking Conference. [S.l.]: IEEE, 2020: 1-6.

[34] ZHANG D, ZHANG L, ZHANG Z, et al. Adaptive personalized randomized response method based on local differential privacy[J]. International Journal of Information Security and Privacy, 2024, 18(1): 1-19.

[35] FENG X, ZHANG C. MPLDP: Multi-level personalized local differential privacy method[J]. IEEE Access, 2024,12: 99739-99754.

[36] ZHU Y, YAN Y, HAN Q. PFED-AGG: A personalized private federated learning aggregation algorithm[C]//Proceedings of 2023 International Joint Conference on Neural Networks. [S.l.]: IEEE, 2023: 1-8.

[37] LI X, ZHU H, ZHANG Z, et al. Item-oriented personalized LDP for discrete distribution estimation[C]//Proceedings of European Symposium on Research in Computer Security. Cham: Springer Nature Switzerland, 2023: 446-466.

[38] 徐川,丁颖祎,罗丽,等.车联网中基于位置服务的个性化位置隐私保护[J].软件学报,2022,33(2):699-716.
XU Chuan, DING Yingyi, LUO Li, et al. Personalized location privacy protection based on location services in the Internet of vehicles[J]. Journal of Software, 2022,33(2): 699-716.

[39] 田丰,吴振强,鲁来凤,等.面向轨迹数据发布的个性化差分隐私保护机制[J].计算机学报,2021, 44(4):709-723.
TIAN Feng, WU Zhenqiang, LU Laifeng, et al. Personalized differential privacy protection mechanism for trajectory data publishing[J]. Chinese Journal of Computers, 2021, 44(4): 709-723.

[40] 叶阿勇,孟玲玉,赵子文,等.基于预测和滑动窗口的轨迹差分隐私保护机制[J].通信学报, 2020, 41(4): 123-133.
YE Ayong, MENG Lingyu, ZHAO Ziwen, et al. Trajectory differential privacy protection mechanism based on prediction and sliding window[J]. Journal on Communication, 2020, 41(4): 123-133.

[41] 张文静,刘樵,朱辉.基于信息论方法的多等级位置隐私度量与保护[J].通信学报, 2019, 40(12): 51-59.
ZHANG Wenjing, LIU Qiao, ZHU Hui. Multi-level location privacy measurement and protection based on information theory method[J]. Journal on Communication, 2019, 40(12): 51-59.

[42] 张文静,李晖.差分隐私保护下的数据分级发布机制[J].网络与信息安全学报, 2015, 1(1): 58-65.

ZHANG Wenjing, LI Hui. Hierarchical data publishing mechanism under differential privacy protection [J]. Chinese Journal of Network and Information Security, 2015, 1(1): 58-65.

[43] 毕晓迪,梁英,史红周,等.一种基于隐私偏好的二次匿名位置隐私保护方法[J].山东大学学报(理学版),2017,52(5):75-84.
BI Xiaodi, LIANG Ying, SHI Hongzhou, et al. A secondary anonymous location privacy protection method based on privacy preference[J]. Journal of Shandong University(Natural Science), 2017, 52(5): 75-84.

[44] 谭智文,徐茹枝,关志涛.基于差分隐私的个性化联邦电力负荷预测方案[J].电子信息与通信技术,2024,22(7):18-26.
TAN Zhiwen, XU Ruzhi, GUAN Zhitao. Personalized federal power load forecasting scheme based on differential privacy[J].Electric Power Information and Communication Technology, 2024,22(7): 18-26.

[45] 徐超,张淑芬,彭璐璐,等.基于个性化差分隐私的联邦学习方法[J].华北理工大学学报(自然科学版),2024,46(2):133-144.
XU Chao, ZHANG Shufen, PENG Lulu, et al. Federated learning method based on personalized differential privacy[J]. Journal of North China University of Science and Technology (Natural Science Edition), 2024,46(2): 133-144.

[46] 李敏,肖迪,陈律君.兼顾通信效率与效用的自适应高斯差分隐私个性化联邦学习[J].计算机学报,2024,47(4):924-946.
LI Min, XIAO Di, CHEN Lvjun. Adaptive Gaussian differential privacy personalized federated learning considering communication efficiency and utility[J]. Chinese Journal of Computers, 2024,47(4): 924-946.

[47] GU X, LI M, XIONG L, et al. Providing input-discriminative protection for local differential privacy[C]//Proceedings of IEEE 36th International Conference on Data Engineering. [S.l.]: IEEE, 2020: 505-516.

[48] MURAKAMI T, KAWAMOTO Y. Utility-optimized local differential privacy mechanisms for distribution estimation[C]//Proceedings of the 28th USENIX Security Symposium. Santa Clara, CA: USENIX Association, 2019: 1877-1894.

[49] ACHARYA J, BONAWITZ K, KAIROUZ P, et al. Context aware local differential privacy[C]//Proceedings of International Conference on Machine Learning. [S.l]: PMLR, 2020: 52-62.

[50] ZHANG Y, ZHU Y, ZHOU Y, et al. Frequency estimation mechanisms under $\epsilon\delta$-utility-optimized local differential privacy[J]. IEEE Transactions on Emerging Topics in Computing, 2023, 12(1): 316-327.

[51] SUN C, FU Y, ZHOU J, et al. Personalized privacy-preserving frequent itemset mining using randomized response[J]. The Scientific World Journal, 2014(1): 686151.

[52] MURAKAMI T, SEI Y. Automatic tuning of privacy budgets in input-discriminative local differential privacy [J]. IEEE Internet of Things Journal, 2023, 10(18): 15990-16005.

[53] 贺星宇,朱友文,张跃.基于OLH的效用优化本地差分隐私机制[J].密码学报,2022,9(5):820-833.
HE Xingyu, ZHU Youwen, ZHANG Yue. Utility optimized local differential privacy mechanism based on OLH[J]. Journal of Cryptologic Research, 2022, 9(5): 820-833.

[54] 曹依然,朱友文,贺星宇,等.效用优化的本地差分隐私集合数据频率估计机制[J].计算机研究与发展,2022,59(10):2261-2274.
CAO Yiran, ZHU Youwen, HE Xingyu, et al. Utility optimized local differential privacy mechanism for set data frequency estimation[J]. Journal of Computer Research and Development, 2022,59(10): 2261-2274.

[55] 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. Local differential privacy joint distribution estimation mechanism for utility optimization[J]. Computer Science, 2023,50(10): 315-326.

[56] ANDRÉS M E, BORDENABE N E, CHATZIKOKOLAKIS K, et al. Geo-indistinguishability: Differential privacy for location-based systems[C]//Proceedings of the 2013 ACM SIGSAC Conference on Computer and Communications Security. [S.l.]: IEEE, 2013: 901-914.

[57] BORDENABE N E, CHATZIKOKOLAKIS K, PALAMIDESSI C. Optimal geo-indistinguishable mechanisms for location privacy[C]//Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. [S. l.] : ACM, 2014: 251-262.

[58] TAO Q, TONG Y, ZHOU Z, et al. Differentially private online task assignment in spatial crowdsourcing: A tree-based approach[C]//Proceedings of IEEE 36th International Conference on Data Engineering. [S.l.]: IEEE, 2020: 517-528.

[59] ZHAO Y, YUAN D, DU J T, et al. Geo-ellipse-indistinguishability: Community-aware location privacy protection for directional distribution[J]. IEEE Transactions on Knowledge and Data Engineering, 2022, 35(7): 6957-6967.

[60] WEGGENMANN B, KERSCHBAUM F. Differential privacy for directional data[C]//Proceedings of the 2021 ACM SIGSAC Conference on Computer and

Communications Security. [S.l.]: ACM, 2021: 1205-1222.

[61] DU M, YUE X, CHOW S S M, et al. Sanitizing sentence embeddings (and labels) for local differential privacy[C]//Proceedings of the ACM Web Conference. [S.l.]: ACM, 2023: 2349-2359.

[62] GURSOY M E, TAMERSOY A, TRUEX S, et al. Secure and utility-aware data collection with condensed local differential privacy[J]. IEEE Transactions on Dependable and Secure Computing, 2019, 18(5): 2365-2378.

[63] ZHAO Y, CHEN J. Vector-indistinguishability: Location dependency based privacy protection for successive location data[J]. IEEE Transactions on Computers, 2023, 73(4): 970-979.

[64] ZHAO Y, YUAN D, DU J T, et al. Geo-ellipse-indistinguishability: Community-aware location privacy protection for directional distribution[J]. IEEE Transactions on Knowledge and Data Engineering, 2022, 35(7): 6957-6967.

[65] WANG L, YANG D, HAN X, et al. Location privacy-preserving task allocation for mobile crowdsensing with differential geo-obfuscation[C]//Proceedings of the 26th International Conference on World Wide Web. Republic and Canton of Geneva, CHE: ACM, 2017: 627-636.

[66] MA X, MA J, LI H, et al. Agent: An adaptive geo-indistinguishable mechanism for continuous location-based service[J]. Peer-to-Peer Networking and Applications, 2018, 11: 473-485.

[67] QIU C, SQUICCIARINI A, PANG C, et al. Location privacy protection in vehicle-based spatial crowdsourcing via geo-indistinguishability[J]. IEEE Transactions on Mobile Computing, 2020, 21(7): 2436-2450.

[68] YANG M, TJUAWINATA I, LAM K Y. K-means clustering with local d_x-privacy for privacy-preserving data analysis[J]. IEEE Transactions on Information Forensics and Security, 2022, 17: 2524-2537.

[69] HAN Y, LI S, CAO Y, et al. Voice-indistinguishability: Protecting voiceprint in privacy-preserving speech data release[C]//Proceedings of IEEE International Conference on Multimedia and Expo. [S.l.]: IEEE, 2020: 1-6.

[70] HUA J, TONG W, XU F, et al. A geo-indistinguishable location perturbation mechanism for location-based services supporting frequent queries[J]. IEEE Transactions on Information Forensics and Security, 2017, 13(5): 1155-1168.

[71] ZHANG S, ZHANG T, LI S Z, et al. Geo-indistinguishable mechanisms for spatial crowdsourcing via multi-objective evolutionary optimization[EB/OL]. (2022-09-10) [2024-07-24]. https://arxiv.org/abs/2201.11300.

[72] ZHANG P, CHENG X, SU S, et al. Task allocation under geo-indistinguishability via group-based noise addition[J]. IEEE Transactions on Big Data, 2022, 9(3): 860-877.

[73] OYA S, TRONCOSO C, PÉREZ-GONZÁLEZ F. Is geo-indistinguishability what you are looking for?[C]//Proceedings of the 2017 on Workshop on Privacy in the Electronic Society. New York, NY, USA: ACM, 2017: 137-140.

[74] MA B, WANG X, NI W, et al. Personalized location privacy with road network-indistinguishability[J]. IEEE Transactions on Intelligent Transportation Systems, 2022, 23(11): 20860-20872.

[75] ZHANG Z, FENG T, WONG W C, et al. A geo-indistinguishable context-based mix strategy for trajectory protection in VANETs[J]. IEEE Transactions on Vehicular Technology, 2023, 72(12): 16538-16552.

[76] 闵明慧,杨爽,胥俊怀,等.三维空间位置服务中智能语义位置隐私保护方法[J].电子与信息学报, 2024, 46: 2627-2637.
MIN Minghui, YANG Shuang, XU Junhuai, et al. Intelligent semantic location privacy protection in 3D spatial location services[J]. Journal of Electronics & Information Technology, 2024, 46: 2627-2637.

[77] 侯占伟,李鑫,王辉,等.面向路网的空间众包隐私保护任务分配算法[J].计算机工程与科学, 2023, 45(8): 1624-1632.
HOU Zhanwei, LI Xin, WANG Hui, et al. Spatial crowdsourcing privacy protection task allocation algorithm for road network[J]. Computer Engineering & Science, 2023, 45(8): 1624-1632.

[78] 薛佳楣,李美珊,玄子玉.基于粒子群聚类偏移的地理位置不可区分[J].计算机应用研究, 2020, 37(8): 2446-2454.
XUE Jiamei, LI Meishan, XUAN Ziyu. The geo-indistinguishable based on particle cluster migration[J]. Application Research of Computers, 2020, 37(8): 2446-2454.

[79] CHEN B C, KIFER D, LEFEVRE K, et al. Privacy-preserving data publishing[J]. Foundations and Trends® in Databases, 2009, 2(1/2): 1-167.

[80] WAGNER I, ECKHOFF D. Technical privacy metrics: A systematic survey[J]. ACM Computing Surveys, 2018, 51(3): 1-38.

[81] KAIROUZ P, OH S, VISWANATH P. Extremal mechanisms for local differential privacy[J]. Journal of Machine Learning Research, 2016, 17(17): 1-51.

[82] 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. [S.l.]: ACM, 2014: 1054-1067.

[83] BLAIR G, IMAI K, ZHOU Y Y. Design and analysis of the randomized response technique[J]. Journal of the American Statistical Association, 2015, 110(511): 1304-1319.

[84] ACHARYA J, SUN Z, ZHANG H. Hadamard response: Estimating distributions privately, efficiently, and with little communication[C]//Proceedings of the 22nd International Conference on Artificial Intelligence and Statistics. [S.l.]: PMLR, 2019: 1120-1129.

[85] WANG T, BLOCKI J, LI N, et al. Locally differentially private protocols for frequency estimation[C]// Proceedings of the 26th USENIX Security Symposium. Vancouver, BC: USENIX Association, 2017.

[86] FISHER R A. Dispersion on a sphere[J]. Proceedings of the Royal Society of London. Series A. Mathematical and Physical Sciences, 1953, 217(1130): 295-305.

[87] VON MISES R. Über die "Ganzzahligkeit" der Atomgewichte und verwandete Fragen[J]. Physikalische Zeitschrift, 1918, 19: 490.

[88] PURKAYASTHA S. A rotationally symmetric directional distribution: Obtained through maximum likelihood characterization[J]. Sankhyā: The Indian Journal of Statistics, Series A, 1991,53(1): 70-83.

(编辑:刘彦东)