差分隐私保护研究综述*

李 杨[a,b], 温 雯[b], 谢光强[a,b]
(广东工业大学 a. 自动化学院; b. 计算机学院, 广州 510006)

摘 要: 差分隐私保护通过添加噪声使数据失真,从而起到保护隐私的目的,对于一个严格定义下的攻击模型,其具有添加噪声少、隐私泄露风险低的优点。介绍了差分隐私保护的理论基础和最新研究进展,详细阐述了分类、聚类等差分隐私学习方法的最新研究情况,介绍了一个差分隐私保护的应用框架 PINQ(privacy integrated queries),并对未来的研究发展方向进行了展望。

关键词: 差分隐私; 隐私保护; 数据失真; 数据挖掘; 数据发布
中图分类号: TP309 **文献标志码**: A **文章编号**: 1001-3695(2012)09-3201-05
doi:10.3969/j.issn.1001-3695.2012.09.001

Survey of research on differential privacy

LI Yang[a,b], WEN Wen[b], XIE Guang-qiang[a,b]
(*a. School of Automation, b. School of Computers, Guangdong University of Technology, Guangzhou* 510006, *China*)

Abstract: Differential privacy approach makes data distortion to preserve privacy by means of adding noise. To a rigorous defined attacking model, differential privacy ensures that adding little amount of noise have a low risk of privacy disclosure. This paper surveyed the definition of differential privacy, showed the newest results in research, introduced algorithms of classify, clustering on differentially private learning, and presented a differential privacy application framework PINQ(privacy integrated queries). Finally, this paper discussed directions for future research.

Key words: differential privacy; privacy preserving; data distortion; data mining; data releasing

0 引言

随着互联网技术的迅猛发展,数据的共享变得越来越便捷,由此引发了人们对自身隐私泄露的担忧。近年来,由数据泄露引发的社会恐慌在国内外时有发生,如美国著名互联网公司美国在线(AOL)泄露了大量用户的网络搜索记录,有人根据这些搜索记录找出了对应用户的真实身份,使得大量注册用户的上网习惯被意外曝光。由该类事件可知,保护个人隐私远远不止隐藏数据记录中的敏感属性(如姓名、住址、年薪等)那么简单,还要阻止敏感属性值与特定的实体或个人关联起来,以防止由非敏感属性信息推测出个人的真实身份。近十几年来数据挖掘技术的高速发展,也为隐私信息的保护带来了新的挑战。因为数据挖掘的对象往往是海量数据,同时对这么多数据进行访问,使得身份认证、权限控制等传统的数据库安全措施毫无用武之地,因为这些手段只能防止敏感属性被用户直接获取,间接推理获得敏感信息的行为很难得到预防。由此可见,隐私保护是一项应用广泛、多领域交叉的复杂的系统工程,还有诸多方面需要深入研究并加以完善。

隐私保护技术大体分为三类:数据失真、数据加密和限制发布[1]。许多隐私保护方法融合了多种技术,很难简单将其归到上述某一类。k-匿名和 l-diversity 是基于限制发布的泛化技术的比较有代表性的两种隐私保护方法。k-匿名由 Samarati 和 Sweeney 提出,可以保证任意一条记录与另外的 $k-1$ 条记录不可区分[2,3]。k-匿名易受到一致性攻击(homogeneity attack)和背景知识攻击(background knowledge attack)[4]。基于 k-匿名在一致性攻击和背景知识攻击下所产生的隐私泄露,Machanavajjhala 等人提出了 l-diversity 原则[5]。若一个数据表满足 k-匿名,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。l-diversity 避免了一个等价类中敏感属性取值单一的情况,使得隐私泄露风险不超过 $1/l$。l-diversity 容易受到相似性攻击(similarity attack)[4]。k-匿名和 l-diversity 的不足之处在于没有严格定义攻击模型,对攻击者所具有的知识未能作出定量化定义。2006 年 Dwork 等人首次提出的 differential privacy(以下称差分隐私保护)从根本上解决了这一问题。

差分隐私保护与传统隐私保护方法的不同之处在于,它定义了一个极为严格的攻击模型,并对隐私泄露风险给出了严谨、定量化的表示和证明。差分隐私保护在大大降低隐私泄露风险的同时,极大地保证了数据的可用性。差分隐私保护方法的最大优点是,虽然基于数据失真技术,但所加入的噪声量与数据集大小无关,因此对于大型数据集,仅通过添加极少量的噪声就能达到高级别的隐私保护。正是由于差分隐私保护方法的诸多优势,使得该方法一经出现,就在国外掀起了一股研究热潮,但在国内还未见相关文献,希望本文可以对国内隐私保护领域的研究人员有所启迪,以吸引更多的学者参与到差分隐私保护的研究中。

收稿日期: 2012-03-16; **修回日期**: 2012-04-28 **基金项目**: 国家自然科学基金资助项目(61074185); 广东省中国科学院全面战略合作项目(2010B090301042)

作者简介: 李杨(1980-),女,黑龙江勃利人,讲师,博士研究生,主要研究方向为隐私保护、机器学习;温雯(1981-),女,江西人,副教授,博士,主要研究方向为机器学习、数据挖掘;谢光强(1979-),男,广东曲江人,讲师,博士研究生,主要研究方向为多智能体协调控制、人工智能。

下面先就差分隐私保护几大方向的国外最新研究情况进行简单介绍。针对特定数据类型,Cormode 等人[6]通过简化步骤、降低敏感度的方式解决了稀疏数据在差分隐私保护过程中噪音添加量过大的问题,使得差分隐私保护在稀疏数据上的应用取得了较好的效果。Sarathy 等人[7]指出了将差分隐私保护应用于数值型数据的一些局限性。Dwork 等人[8,9]针对流数据和连续观测的差分隐私保护问题,提出了隐私保护级别更强的泛隐私(pan-privacy)的概念。泛隐私基于流算法的思想,每个数据一经处理就马上丢弃,它可以抵御连续不间断的入侵方式,即使数据的内部状态已经暴露给入侵者。Li 等人[10]首次将差分隐私与 k-匿名算法结合,并应用于微数据隐私保护下的数据发布问题。Zhou 等人[11]提出了一种应用于超大型数据库的差分隐私压缩算法,研究借助高斯随机变量矩阵以随机线性或映射变换的方式压缩数据库,在实现差分隐私保护的同时保持原有数据对常见的统计学习应用的特性,如高维稀疏回归、主成分分析(PCA)和其他基于初始数据协方差的统计度量方法。在应用领域,Vu 等人[12]将差分隐私保护与传统的统计假设检验建模相结合,并应用于临床实验数据挖掘,在如何调节样本数量以获取统计效率和隐私保护级别之间的平衡问题上总结了一些规律。Gehrke 等人[13]改进了差分隐私保护算法并应用于社交网络的隐私保护建模。Zhang 等人[14]提出了应用于分布式数据挖掘下抵御联合攻击的基于安全多方计算和随机选择的差分隐私保护算法。

1 差分隐私保护理论基础

差分隐私保护[15~21]是基于数据失真的隐私保护技术,采用添加噪声的技术使敏感数据失真但同时保持某些数据或数据属性不变,要求保证处理后的数据仍然可以保持某些统计方面的性质,以便进行数据挖掘等操作。

差分隐私保护可以保证,在数据集中添加或删除一条数据不会影响到查询输出结果,因此即使在最坏情况下,攻击者已知除一条记录之外的所有敏感数据,仍可以保证这一条记录的敏感信息不会被泄露。

定理 1 对于所有差别至多为一个记录的两个数据集 D_1 和 D_2,Range(K)表示一个随机函数 K 的取值范围,Pr[E_s]表示事件 E_s 的披露风险,若随机函数 K 提供 ε-差分隐私保护,则对于所有 $S\subseteq \text{Range}(K)$,有

$$\Pr[K(D_1)\in S]\leqslant \exp(\varepsilon)\times \Pr[K(D_2)\in S] \tag{1}$$

计算出的披露风险取决于随机化函数 K 的值。

图 1 描绘了差别至多为一个记录的两个数据集 D_1 和 D_2 满足 ε-差分隐私的披露风险曲线。

随机函数 K 的选择与攻击者所具有的知识无关,只要 K 满足定理 1 就可以保护数据集中任意数据的隐私,即使攻击者已经掌握其他的所有数据。

设查询函数为 f,数据集为 X,真实的查询结果为 $f(X)$。函数 K 通过在 $f(X)$ 上加入合适选择的随机噪声的方式来保护隐私。在查询函数 f 下,ε-差分隐私保护函数 K 的响应值为

$$f(X)+(\text{lap}(\Delta f/\varepsilon))^k$$

其中,Δf 为查询函数 f 的敏感度,其计算方法参见定义 1。

定义 1 对于 $f: D\rightarrow \mathrm{R}^k$,$f$ 的敏感度定义为

$$\Delta f=\max_{D_1,D_2}\|f(D_1)-f(D_2)\|_1 \tag{2}$$

数据集 D_1 和 D_2 之间至多相差一个元素。

对于多数查询函数 f 来说,Δf 的值都比较小。如简单的计数查询(有多少行具有属性 P?)敏感度 $\Delta f=1$。值得一提的是,敏感度只是函数 f 的性质之一,与数据集 X 无关。

设噪声函数 $\text{lap}(b)=\exp(-|x|/b)$ 为标准差为 $\sqrt{2}b$ 的对称指数分布,其中 $b=\Delta f/\varepsilon$,则概率密度函数为 $p(x)=\exp(-|x|/b)/2b$,累积分布函数为 $D(x)=(1/2)(1+\text{sgn}(x)(1-\exp(|x|/b)))$。

加入的噪声与 Δf 的值成正比、与 ε 成反比,即 Δf 较小时,算法表现较好,因为加入的噪声较少。当 ε 减小时,$\text{lap}(\Delta f/\varepsilon)$ 的曲线变得扁平,意味着噪声幅度的预期变大;当 ε 固定,高敏感度的函数 f 对应的曲线更扁平,同样会使噪声幅度的预期变大。如图 2 所示。

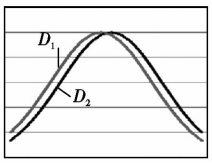

图1 数据集D_1、D_2的 ε-差分隐私披露风险曲线

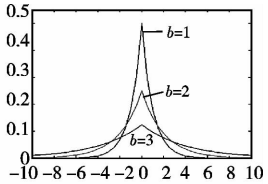

图2 拉普拉斯噪声的概率密度函数

在满足 ε-差分隐私保护时,ε 越小,加入的噪声越多,隐私保护的级别越高。因此可以通过设置不同的 ε 值来实现隐私保护等级的划分。

每一种隐私保护方法都会基于一种攻击模型(attacking model),如 k-匿名和 l-diversity 所基于的攻击模型假设攻击者对敏感属性的信息一无所知,否则隐私便无法得到保护。差分隐私所定义的攻击模型是:最坏情况下,攻击者已知除一条记录之外的所有数据的敏感属性,在这种情况下,这条记录的敏感属性信息仍然可以得到保护。因为由定理 1 可知,当数据集 D_1 和 D_2 之间只相差一个记录时,无论对 D_1 和 D_2 进行什么查询,都会得到近似"相同"的查询结果,因此攻击者在一定的概率下无法推断出该记录的任何敏感属性信息。

2 差分隐私保护算法优化

在满足差分隐私保护的基础上,为了提高查询响应的精确度,涌现了一批相关的研究成果。

2008 年,Blum 等人[22]提出了一种能够精确响应任意"查询类"的新方法,响应精确度依赖于"查询类"的 VC 维;该方法的缺陷在于效率低,其运行时间是指数级的。文献[22]还提出了一种响应域查询的有效方法,但在精确度上逊色于文献[23,24]中提出的方法。

对于复合查询的差分隐私优化问题,Hardt 等人[25]提出了基于线性查询集合的 k-模方法。该方法将线性查询映射到 L_1 球面,再根据映射的几何形状决定所添加的噪音;但由于 k-模方法要求从高维凸体中均匀采样,因此在实际应用中效率很低,另外,该方法限制了查询的次数。与此相比,文献[26]提出的方法效率较高,原因是其算法花销主要是寻找查询策略,这个过程只进行一次,一旦最优策略确定后,其效率等同于传统的拉普拉斯方法。

Roth 等人[27]假设在交互环境下,查询按时间先后依次到达,在对将要到达的查询一无所知的情况下,必须马上对到达的查询作出响应,其对传统的拉普拉斯噪音机制进行了改进,

查询响应使用中值方法对之前的查询结果进行计算得出。由于需要对具有超多项式大小的集合采样,直接应用中值方法效率很低,若要提高效率,则需牺牲隐私保护强度和隐私保护后数据的可用性。

2.1　基于分层思想优化查询响应的矩阵机制

差分隐私保护方法自出现以来,针对一组相关联的域计数查询的最优响应策略问题鲜有报道,直到 2010 年,相关的研究工作才得以开展。

Xiao 等人[23]将 Haar 小波变换应用于差分隐私保护中,在添加噪音前先对数据实施小波变换,提高了计数查询的准确度,同时将应用范围拓展至名词属性和高维直方图查询。该方法无论在理论上还是结果误差上均等价于 H 查询,相当于存在一棵查询树,树从上至下的每一层都是更细粒度的汇总数据。

Hay 等人[24]提出一种基于分层求和与最小二乘的差分隐私保护方法,将查询序列划分成满足一致性约束的分组,噪声以每个分组为单位进行添加,从而达到既满足查询精度又降低噪音添加量的目的。

Li 等人[26]提出了矩阵机制的概念,并将文献[23,24]的成果纳入矩阵机制的范畴。通过分析相互之间具有某种关联关系的查询,将每个查询看做一个基本计数操作的线性组合,将具有关联关系的查询表示成矩阵,从而在原有拉普拉斯噪音分布方法的基础上降低了噪声的添加量。

上述三种方法在本质上都基于矩阵机制,并且都针对特定查询问题进行了改进,因此在针对特定问题的算法效率上优于传统算法。

2.2　差分隐私保护下线性查询的精度范围

自差分隐私保护方法出现以来,对于满足差分隐私的查询响应的精度范围一直是学者们研究的重点,其中线性查询响应的精度范围又是学者关注的重中之重。

在非交互方式下,Blum 等人[22]提出了一种发布合成数据的差分隐私保护算法,其算法服从 $O(n^{2/3})$ 的误差范围,n 是数据集的大小,其缺点是误差随着数据集的增大而增大;Dwork 等人[28,29]对文献[22]所提出的算法进行了后续的改进。Gupta 等人[30]提出了一种基于乘性权重算法和不可知论学习的非交互的查询响应算法;Hardt 等人在文献[31]中实现了上述算法,并对其进行了实验评估,该算法不适用于交互方式,并且当查询次数数倍于数据集大小时,算法效率很低。

在交互方式下,Roth 等人[27]假设查询在线进行,必须在后续查询到来之前作出响应,可以达到 $\frac{n^{2/3}(\log k)(\log|X|)^{1/3}}{\varepsilon^{1/3}}$ 的误差范围。Hardt 等人[32]基于权重加乘的方法,将在线查询的响应误差边界缩小到 $\frac{n^{1/2}(\log k)(\log|X|)^{1/4}}{\varepsilon}$。其中的参数意义为:在 ε-差分隐私保护下,n 为数据集大小,k 是查询次数,X 是数据域。

2012 年,Gupta 等人[33]综合了交互方式下的中值算法[27]和权重加乘算法[32],归纳了非交互方式下的乘性权重算法[30,31],抽象定义了一个迭代的数据库构建(IDC)算法,算法可以在交互和非交互方式下以差分隐私保护为前提响应查询。IDC 算法以迭代的方式改进一个假设的数据结构,使得该数据结构最终可以对所有的查询作出响应;同时,算法改善了中值算法和乘性权重算法的精度范围。

3　差分隐私保护的几类重要方法

目前,差分隐私保护在多个领域都取得了突破性的进展,展现出高准确率和低风险的特性。利用挖掘技术本身所基于的统计和计算理论来解决数据挖掘中的隐私保护问题一直是隐私保护研究的热点。差分隐私保护方法出现以来,统计和数据挖掘过程中的差分隐私保护引起了研究者的关注,也出现了一些有代表性的研究成果。下面详细介绍几类重要方法的最新研究进展。

3.1　差分隐私直方图方法

作为列联表(contingency table)、边界图(marginals)分析等许多数据分析的基础,直方图查询在众多差分隐私保护方法中占有非常重要的地位。

2005 年,Chawla 等人[34]在明确提出差分隐私保护这一方法之前就开始研究直方图查询下的隐私保护方法。2006 年,Dwork 等人[35]对直方图查询的一些本质特性进行了深入的分析,指出了差分隐私直方图方法与现存方法相比,最大的优势在于敏感度的计算与维度无关,对于某些具有高维输出的列联表、协方差矩阵分析的差分隐私,可以在少量噪声加入的前提下保护隐私。2011 年,Dwork[20]对获取差分隐私保护的直方图查询方法进行了完整的归纳总结,指出虽然一个具有 k 个单元的直方图可以看做 k 个单独的计数查询,但是一行数据的增加或删除只会对这行数据所对应的那个单元的计数造成影响,这种影响最大为 1 个计数,因此一个直方图查询的敏感度为 1。这一结论为差分隐私直方图方法在各类问题中的应用奠定了基础。

3.2　差分隐私 K-means 聚类方法

2005 年,Blum 等人[36]提出了在 K-means 聚类过程中通过添加适当噪声获取差分隐私保护的方法,总结了查询函数的敏感度计算方法以及获取 ε-差分隐私保护的 K-means 算法的主要步骤。在 K-means 中,计算离每个样本点最近的中心点会泄露隐私。然而,对于一个未知集合,计算均值只需要用和除以数目。因此,只要发布集合 S_j 的近似值即可,不需要集合本身的信息。其不足之处在于没有对迭代过程中 ε 参数的变化进行分析。

2011 年,Dwork[20]针对上述不足对算法进行了补充和完善,详细分析了差分隐私 K-means 算法中每个查询函数的敏感度计算方法,并给出了整个查询序列的总敏感度。设数据空间为 $[0,1]^d$,整个查询序列的敏感度为 $d+1$,根据上述分析,Dwork 更进一步给出了迭代过程中设置 ε 参数的两种方法。假设迭代次数固定为 N,可以通过添加分布为 $\mathrm{lap}((d+1)N/\varepsilon)$ 来获取 ε-差分隐私保护;如果迭代次数未知,可以在计算过程中逐步调高参数,如第一次迭代参数为 $(d+1)(\varepsilon/2)$,下次迭代参数为 $(d+1)(\varepsilon/4)$,每次消耗剩余“预算”的一半。

目前,对差分隐私聚类方法的研究都停留在理论研究阶段,以仿真实验或实际应用进行验证并对算法加以改进的文献未见报道。

3.3　差分隐私分类方法

3.3.1　差分隐私 ERM 分类

2008 年,Chaudhuri 等人[37]将 Dwork 提出的差分隐私保护

的思想应用于正则逻辑回归,提出了一种不依赖于敏感度的改进的差分隐私分类方法,并在正则化和隐私保护之间建立了联系。

2011 年,Chaudhuri 等人[38]将文献[37]的思想拓展到正则 ERM 中损失函数和正则因子满足特定的凸函数特性和可微特性的隐私保护问题上,提出一种为正则 ERM 机器学习算法设计的隐私保护的新方法——目标函数加扰。这种方法与 Dwork 的输出加扰思想的不同之处在于需要在最优化分类器前对目标函数加扰。

目标函数加扰算法描述如下:

输入:数据集 $D=\{z_i\}$,参数 ε_p,Λ,c。

输出:f_{priv}的近似极小值。

a)最小化 $J_{\text{priv}}(f,D)=J(f,D)+\frac{1}{n}b^{\mathrm{T}}f$。其中:$J(f,D)$是规范化经验损失函数;$b$ 是密度分布为 $v(b)=\frac{1}{\alpha}\mathrm{e}^{-\beta\|b\|}$ 的随机噪声,α 是标准化常量,$\beta=\varepsilon_p$。

b)令 $\varepsilon'_p=\varepsilon_p-\log\left(1+\frac{2c}{n\Lambda}+\frac{c^2}{n^2\Lambda^2}\right)$。若 $\varepsilon'_p>0$,则令 $\Delta=0$;否则令 $\Delta=\frac{c}{n(\mathrm{e}^{\varepsilon_p/4}-1)}-\Lambda$。同时 $\varepsilon'_p=\varepsilon_p/2$,由 $\beta=\varepsilon'_p/2$,通过 $v(b)=\frac{1}{\alpha}\mathrm{e}^{-\beta\|b\|}$ 得到向量。其中 $\log\left(1+\frac{2c}{n\Lambda}+\frac{c^2}{n^2\Lambda^2}\right)$是一个松弛量。

c)计算 $f_{\text{priv}}=\operatorname{argmin} J_{\text{priv}}(f,D)+\frac{1}{2}\Delta\|f\|^2$。

Chaudhuri 提出了在通用的机器学习算法中调节参数以保护隐私的方法,从而提供了衔接各个训练过程的隐私保障。应用这些成果模拟生成隐私保护的正则化逻辑回归和支持向量机,在权衡了隐私保护和学习效果方面的综合表现都优于现存的输出加扰方法;其不足之处在于约束条件过强,适用范围有限,只适用于正则因子满足强凸函数特性的情况。

3.3.2 其他差分隐私分类器

Jagannathan 等人[39]提出了一种构造和更新差分隐私随机决策树分类器的方法。首先构造了一个 ID3 差分隐私决策树,经过实际数据集上的运行实验表明,想要获得合理的隐私保护级别,需要付出损失极大预测精度的代价;随后提出了一种基于随机决策树方法的差分隐私决策树构造改进算法。实验表明,该算法在小型数据集上也能获得较好的预测精度。文献还提出了数据增量下的差分隐私随机决策树更新算法,并通过实验证明更新数据的同时能够维持同样的隐私保护级别。

Pathak 等人[40]提出了满足差分隐私的多类高斯分类器的构造方法,算法包括向目标函数加入扰动项,证明了一个风险上界,该风险上界与数据维数成反比。

4 PINQ 框架

PINQ(privacy integrated queries)[41]是 Dwork 领导下开发的一套为隐私敏感数据提供差分隐私保护的框架。PINQ 框架类似于 LINQ,它提供一系列的 API,便于开发者以简单而富有表达力的语言进行相关的差分隐私保护系统开发,框架中还提供了丰富的差分隐私数据分析的应用实例。

图 3 展示了一个应用 PINQ 框架对外发布数据的应用示例。在框架中,需要保护的数据库的所有者设定一个隐私消费预算,用户对数据库进行的每项查询都会消费一些预算,一旦预算用尽就不能再进行查询。设数据库中某条记录为“张三,男,糖尿病患者,25 岁,居住地为番禺区华南碧桂园”。对于数据使用者来说,在参数 ε 范围内,无论张三是否在数据库中,均不会对任何查询结果造成影响。用户之间可以随意共享查询结果,也可以结合外部信息(如楼盘业主信息、移动用户信息、居民消费数据等来自其他数据库的数据),这些操作不会引起隐私泄露。

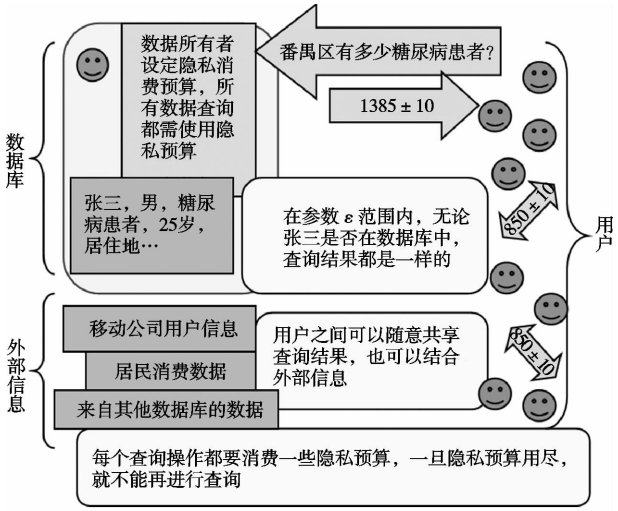

图3 一个应用PINQ框架发布数据的应用示例

5 结束语

差分隐私保护是一种通用、灵活、具有坚实的数学理论支撑的隐私保护方法,可以用来解决很多传统密码学不适合甚至不可行的问题,因此引起越来越多研究者的兴趣,焕发出了强大的生命力。差分隐私保护在近两年取得了飞速的发展,相关的研究工作扩展到了越来越广阔的领域。下面列举几个差分隐私保护领域中可深入研究的大方向供研究人员参考。

1)差分隐私与几何学

在一系列线性查询中获取差分隐私保护,若使所需添加噪声的上下界更加精确,需要掌握这一系列查询的几何意义[25]。在特定情况下,查询之间的依赖关系可被管理者用来显著地提高查询的效率。将这一研究拓展到非线性和交互式查询将是未来的一大研究热点。

2)算法复杂度

差分隐私算法的时间复杂度在很长一段时间被研究人员所忽视,当前一些算法的实现效率并不理想,目前大量的研究仍停留在实验阶段,这在相当程度上限制了差分隐私算法的实际应用。文献[42]以合成数据的生成问题为例,基于密码学假设,提出了指数级机制的实现问题。下一步需要研究以何种方式降低算法的时间复杂度,以推动差分隐私在现实环境中的广泛应用。

参考文献:

[1] 周水庚,李丰,陶宇飞,等. 面向数据库应用的隐私保护研究综述[J]. 计算机学报,2009,32(5):847-861.

[2] SWEENEY L. k-anonymity: a model for protecting privacy[J]. International Journal on Uncertainty, Fuzziness and Knowledge-based Systems,2002,10(5):557-570.

[3] SWEENEY L. Achieving k-anonymity privacy protection using generalization and suppression[J]. International Journal on Uncertainty,

Fuzziness and Knowledge-based Systems, 2002, 10(5): 571-588.

[4] Li Ning-hui, LI Tian-cheng, VENKATASUBRAMANIAN S. *t*-closeness: privacy beyond *k*-anonymity and *l*-diversity[C]//Proc of the 23rd International Conference on Data Engineering. Washington DC: IEEE Computer Society, 2007: 106-115.

[5] MACHANAVAJJHALA A, KIFER D, GEHRKE J, *et al*. *l*-diversity: privacy beyond *k*-anonymity[C]//Proc of the 22nd International Conference on Data Engineering. Washington DC: IEEE Computer Society, 2006: 24-35.

[6] CORMODE G, PROCOPIUC M, SRIVASTAVA D. *et al*. Differentially private publication of sparse data[J]. Arxiv Preprint arXiv: 1103.0825, 2011.

[7] SARATHY R, MURALIDHAR K. Some additional insights on applying differential privacy for numeric data[C]//Proc of International Conference on Privacy in Statistical Databases. Berlin: Springer-Verlag, 2010: 210-219.

[8] DWORK C, NAOR M, PITASSI T, *et al*. Pan-private streaming algorithms[C]//Proc of the 1st Symposium on Innovations in Computer Science. Beijing: Tsinghua University Press, 2010.

[9] DWORK C, NAOR M, PITASSI T, *et al*. Differential privacy under continual observation[C]//Proc of the 42nd ACM Symposium on Theory of Computing. New York: ACM Press, 2010: 715-724.

[10] LI Ning-hui, QARDAJI W, SU Dong. Provably private data anonymization: or, *k*-anonymity meets differential privacy, CERIAS TR 2010-24[R]. West Lafayette: Center for Education and Research Information Assurance and Security, Purdue University, 2010.

[11] ZHOU Shu-heng, LIGETT K, WASSERMAN L. Differential privacy with compression[C]//Proc of IEEE International Symposium on Information Theory. Washington DC: IEEE Computer Society, 2009: 2718-2722.

[12] VU D, SLAVKOVIC A. Differential privacy for clinical trial data: preliminary evaluations[C]//Proc of the 9th IEEE International Conference on Data Mining. Washington DC: IEEE Computer Society, 2009: 138-143.

[13] GEHRKE J, LUI E, PASS R. Towards privacy for social networks: a zero-knowledge based definition of privacy[C]//Proc of the 8th Conference on Theony of Cryptography. Berlin: Springer-Verlag, 2011: 432-449.

[14] ZHANG Ning, LI Ming, LOU Wen-jing. Distributed data mining with differential privacy[C]//Proc of IEEE International Conference on Communications. 2011: 1-5.

[15] DWORK C. Differential privacy[C]//Proc of the 33rd International Colloquium on Automata, Languages and Programming. Berlin: Springer-Verlag, 2006.

[16] DWORK C. Differential privacy: a survey of results[C]//Proc of the 5th International Conference on Theory and Applications of Models of Computation. Berlin: Springer-Verlag, 2008: 1-9.

[17] DWORK C. The differential privacy frontier[C]//Proc of the 6th International Conference on Theory of Cryptography Conference. Berlin: Springer-Verlag, 2009: 496-502.

[18] DWORK C. Differential privacy in new settings[C]// Proc of the 21st Annual ACM-SIAM Symposium on Discrete Algorithms. Philadelphia: Society for Industrial and Applied Mathematics, 2010: 174-183.

[19] McSHERRY F. Privacy integrated queries: an extensible platform for privacy-preserving data analysis [J]. Communications of the ACM, 2010, 53(9): 89-97.

[20] DWORK C. A firm foundation for private data analysis[J]. Communications of the ACM, 2011, 54(1): 86-95.

[21] DWORK C. The promise of differential privacy: a tutorial on algorithmic techniques[C]//Proc of the 52nd Annual IEEE Symposium on Foundations of Computer Science. Washington DC: IEEE Computer Society, 2011: 1-2.

[22] BLUM A, LIGETT K, ROTH A. A learning theory approach to non-interactive database privacy[C]//Proc of the 40th ACM SIGACT Symposium on Thoery of Computing. New York: ACM Press, 2008: 609-618.

[23] XIAO Xiao-kui, WANG Guo-zhang, GEHRKE J. Differential privacy via wavelet transforms[J]. IEEE Trans on Knowledge and Data Engineering, 2011, 23(8): 1200-1214.

[24] HAY M, RASTOGI V, MIKLAU G, *et al*. Boosting the accuracy of differentially private histograms through consistency[J]. Proceedings of the VLDB, 2010, 3(1-2): 1021-1032.

[25] HARDT M, TALWAR K. On the geometry of differential privacy [C]//Proc of the 42nd ACM Symposium on Theory of Computing. New York: ACM Press, 2010: 705-714.

[26] LI Chao, HAY M, RASTOGI V, *et al*. Optimizing linear counting queries under differential privacy[C]//Proc of the 29th ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems. New York: ACM Press, 2010: 123-134.

[27] ROTH A, ROUGHGARDEN T. Interactive privacy via the median mechanism[C]//Proc of the 42nd ACM Symposium on Theory of Computing. New York: ACM Press, 2010: 765-774.

[28] DWORK C, NAOR M, REINGOLD O, *et al*. On the complexity of differentially private data release: efficient algorithms and hardness results[C]//Proc of the 41st Annual ACM Symposium on Theory of Computing. New York: ACM Press, 2009: 381-390.

[29] DWORK C, ROTHBLUM G N, VADHAN S. Boosting and differential privacy[C]// Proc of the 51st Annual IEEE Symposium on Foundations of Computer Science. Washington DC: IEEE Computer Society, 2010: 51-60.

[30] GUPTA A, HARDT M, ROTH A, *et al*. Privately releasing conjunctions and the statistical query barrier[C]//Proc of the 43rd Annual ACM Symposium on Theory of Computing. New York: ACM Press, 2011: 803-812.

[31] HARDT M, LIGETT K, McSHERRY F. A simple and practical algorithm for differentially private data release[EB/OL]. (2012-03-15). http://www.cs.princeton.edu/~mhardt/pub/mwem.pdf.

[32] HARDT M, ROTHBLUM G N. A multiplicative weights mechanism for privacy preserving data analysis[C]//Proc of the 51st Annual IEEE Symposium on Foundations of Computer Science. Washington DC: IEEE Computer Society, 2010: 61-70.

[33] GUPTA A, ROTH A, ULLMAN J. Iterative constructions and private data release[C]//Proc of the 9th International Conference on Theory of Cryptography. Berlin: Springer-Verlag, 2012: 339-356.

[34] CHAWLA S, DWORK C, McSHERRY F, *et al*. On the utility of privacy-preserving histograms[C]//Proc of the 21st Conference on Uncertainty in Artificial Intelligence. 2005.

[35] DWORK C, McSHERRY F, NISSIM K, *et al*. Calibrating noise to sensitivity in private data analysis[C]//Proc of the 3rd International Conference on Theory of Cryptography. Berlin: Springer-Verlag, 2006: 265-284.

(下转第 3211 页)

(上接第 3205 页)

[36] BLUM A, DWORK C, McSHERRY F, *et al*. Practical privacy: the SuLQ framework[C]//Proc of the 24th ACM SIGMOD International Conference on Management of Data/Principles of Database Systems. New York: ACM Press, 2005: 128-138.

[37] CHAUDHURI K, MONTELEONI C. Privacy-preserving logistic regression[C]//Proc of the 22nd Annual Conference on Neural Information Processing Systems. 2008: 289-296.

[38] CHAUDHURI K, MONTELEONI C, SARWATE D. Differentially private empirical risk minimization[J]. Journal of Machine Learning Research, 2011, 12(2): 1069-1109.

[39] JAGANNATHAN G, PILLAIPAKKAMNATT K, WRIGHT R N. A practical differentially private random decision tree classifier[C]// Proc of IEEE International Conference on Data Mining. Washington DC: IEEE Computer Society, 2009: 114-121.

[40] PATHAK M A, RAJ B. Large margin multiclass Gaussian classification privacy[C]//Proc of International ECMI/PKDD Workshop on Privacy and Security Issues in Data Mining and Machine Learning. Berlin: Springer-Verlag, 2010: 99-112.

[41] McSHERRY F. Privacy integrated queries (PINQ)[EB/OL]. http://research.microsoft.com/en-us/projects/PINQ/.

[42] DWORK C, NAOR M, REINGOLD O, *et al*. When and how can privacy-preserving data release be done effitiently? [C]//Proc of the 41st International ACM Symposium on Theory of Computing. New York: ACM Press, 2009: 381-390.