计算机科学
COMPUTER SCIENCE

差分隐私研究进展综述

赵禹齐, 杨敏

引用本文

赵禹齐，杨敏. 差分隐私研究进展综述[J]. 计算机科学, 2023, 50(4): 265-276.

ZHAO Yuqi, YANG Min. Review of Differential Privacy Research[J]. Computer Science, 2023, 50(4): 265-276.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.220500292

差分隐私研究进展综述

赵禹齐　杨　敏
空天信息安全与可信计算教育部重点实验室(武汉大学国家网络安全学院)　武汉 430072
(nkiszyq@163.com)

摘　要　在过去的十年里,普遍的数据收集已经成为常态。随着大规模数据分析和机器学习的快速发展,数据隐私正面临着根本性的挑战。探索隐私保护和数据收集与分析之间的权衡是一个关键的科学问题。差分隐私已经成为实际上的数据隐私标准并得到了广泛的研究与应用,该技术可通过一定的随机化机制为用户数据提供严格的隐私保护。文中给出了差分隐私技术的全面概述,总结并分析了差分隐私的最新进展。具体来说,首先给出了差分隐私的理论总结,包括中心化模型、本地化模型和近年提出的洗牌模型,并对它们作了详细比较,分析了不同模型的优势和缺点。接着,在3个模型的基础上,从算法的角度介绍并分析了文献中一些典型的差分隐私机制,然后介绍了当前差分隐私技术在多个领域的应用。最后介绍了一些关于差分隐私的新研究课题,它们为差分隐私技术拓展了丰富的研究方向。

关键词:差分隐私;隐私保护;统计查询;洗牌模型;随机化机制;误差界
中图法分类号　TP309.2

Review of Differential Privacy Research

ZHAO Yuqi and YANG Min
Key Laboratory of Aerospace Information Security and Trusted Computing,Ministry of Education,School of Cyber Science and Engineering,Wuhan University,Wuhan 430072,China

Abstract　In the past decade,widespread data collection has become the norm. With the rapid development of large-scale data analysis and machine learning,data privacy is facing fundamental challenges. Exploring the trade-offs between privacy protection and data collection and analysis is a key scientific question. Differential privacy has become a de facto data privacy standard and has been widely studied and applied. Differential privacy technology can provide strict privacy protection for user data through a certain randomization mechanism. This paper provides a comprehensive overview of differential privacy technology and a summary and analysis of the latest progress of differential privacy. Specifically,this paper first gives a theoretical summary of differential privacy,including the central model,the local model and the shuffle model proposed in recent years. The three models are compared,and the advantages and disadvantages of different models are analyzed. Then,on the basis of the three models,some typical differential privacy mechanisms in literatures are analyzed from the perspective of algorithms. Then the current application of differential privacy technology in various fields is introduced. Finally,some new research topics about differential privacy technology are introduced,which expand the rich research direction for differential privacy technology.

Keywords　Differential privacy,Privacy preserving,Statistical query,Shuffle model,Randomization mechanism,Error bound

1　引言

随着计算机和互联网的飞速普及,智能设备不断增加,产生了海量数据。从无处不在的联网设备中进行数据收集已经成为常态,数据也被定义为与土地、劳动力、资本、技术等传统生产要素并列的新型生产要素[1]。对用户数据的收集和分析具有极大的潜在价值,且这一价值已经深刻地改变了我们的经济社会,例如运营商可通过收集用户的偏好选项来研究应用的使用情况并改善用户体验,借助机器学习建立分类器或使用模型进行预测,乃至典型的大规模数据统计分析——人口普查。但随之而来的,这样收集并分析数据产生了明显的隐私问题,例如2018年著名社交网络Facebook就曾泄露约2.67亿用户的包括姓名、账号、电话号码在内的个人信息。因此,人们对数据隐私的关注也在持续增加,例如2018年欧盟出台《通用数据保护条例》[2],对任何收集、传输、保留和处理个人敏感数据的行为制定法律规范;2021年6月10日我国颁布的《中华人民共和国数据安全法》[3]对数据安全以及数据处理活动作出了详细的规范和监管,建立了数据安全制度

到稿日期:2022-05-31　返修日期:2022-09-23
基金项目:国家自然科学基金(62172308);国家重点基础研究发展计划(2021YFB2700200)
This work was supported by the National Natural Science Foundation of China(62172308) and National Basic Research Program of China(2021YFB2700200).
通信作者:杨敏(yangm@whu.edu.cn)

和数据安全保护义务。

差分隐私技术是一种用于解决上述隐私问题的隐私增强技术，差分隐私技术以牺牲一定的数据准确度为代价，能够为用户数据提供严格的隐私保护。自2006年差分隐私的首次提出至今已有十余年，随着近年来的使用和发展，差分隐私技术逐渐成为了实际上的数据隐私保护标准，并在推荐系统、网页域名检测、人群流量监测、社交网络分析等诸多场景中得到了应用。因此，本文意在为差分隐私技术提供一个全面的概述，关注差分隐私技术的最新进展，把握未来的发展趋势。本文首先对差分隐私的基本理论做出简要的描述和总结，具体分为中心化差分隐私、本地化差分隐私和洗牌模型差分隐私3个部分，详细比较了3个模型的特点和优劣；第3节给出了差分隐私在3种模型下的多种算法协议，其中除了包括一些经典算法外，例如指数机制、Laplace机制和随机响应机制，还包括一些新机制，例如在洗牌模型下的一些创新性成果；第4节介绍了当前差分隐私技术在多个领域中的应用，具体包括机器学习、车联网、社交网络分析、多方安全计算、推荐系统和位置隐私，列举了现有工作，并指出了相关研究面临的问题与挑战；第5节给出了一些有关差分隐私技术的拓展性工作，包括差分隐私编程框架、差分隐私的形式化验证等，这些工作的开展有助于差分隐私的进一步实践；最后总结全文。

2 差分隐私理论总结

差分隐私[4]技术自提出至今已经十多年，它是一个数学上严格的隐私保护概念，最初是用于数据收集服务器上的隐私保护技术，可抵抗利用统计查询的差分攻击，通过对统计查询的输出添加适量的噪音，使敌手几乎无法分辨两个相邻数据集之间的统计差别，从而保护个体数据的隐私性。后来的研究提出了本地化的差分隐私模型，该模型将噪音添加步骤从服务器端转移到每一个客户端，解除了对可信第三方服务器的依赖，但在数据集上叠加的噪音规模也对服务器的统计精度带来了一定的困扰。近年来，相关研究提出了差分隐私洗牌模型，它建立于本地化模型的基础上，在服务器和客户端之间添加了可信的洗牌器，洗牌器将用户群体提交的数据项进行乱序处理以达到匿名化效果，然后转发给服务器进行聚合统计，为用户数据提供了额外的隐私保护。本节将给出差分隐私技术的理论总结，包括对差分隐私三大模型的总结和比较。本文中的常用符号如表1所列。

表1 常用符号表示

Table 1 Commonly used notations

Notation	Explanation
N	Number of users
U_i	The i-th user in the user population
V_i	Original value of U_i
y_i	Perturbed value of U_i
D	Domain of user data
d	Size of D
S	Original dataset
S'	Neighboring dataset of S
ε	Privacy budget
δ	Probability of failure
M	Randomization mechanism
f_V	Frequency of V in the user population

2.1 中心化差分隐私

最早由Dwork等提出的差分隐私[4]是一个中心化差分隐私模型(Central Differential Privacy，CDP)，中心化服务器需要收集分布于N个用户端的数据项来进行聚合和统计，从而为数据库查询提供关于数据集的统计信息，如频率、均值或更多复杂的统计信息。为了抵抗差分攻击、保护用户数据，在发布统计信息时，服务器需要使用随机化机制对其添加额外的噪声。中心化差分隐私模型如图1所示，其中函数$f(\cdot)$代表对数据集的统计查询，函数$M(\cdot)$代表满足差分隐私的随机化机制。

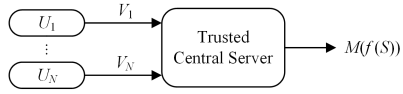


图1 中心化差分隐私模型

Fig. 1 Central differential privacy

直观来讲，差分隐私能保护隐私的关键在于为统计信息添加了一定的随机性，适量的随机性可以使得两个相邻数据集发布的统计信息有一定概率相等。因此，攻击者在对相邻数据集的统计结果使用差分攻击时就无法准确地分析出两个数据集之间的信息差，从而保护了用户的隐私。另一方面，为保证统计数据集的可用性，两个相邻数据集得到同一输出的概率并不完全相同，即从统计学的角度看，两个相邻数据集得到相同统计输出的概率要有一定的差距。差分隐私使用了严格的数学定义来限制这一概率差距，其定义如定义1所示。

定义1(ε-差分隐私) 一个随机化机制M满足ε-差分隐私($\varepsilon>0$)，当且仅当对于任何相邻的输入数据集S和S'以及任意可能的输出值集合R，有$Pr[M(S)\in R]\leqslant e^{\varepsilon}\cdot Pr[M(S')\in R]$成立。

其中相邻数据集指仅相差一条用户数据记录的两个数据集，即$S-S'=\{V\}$或$S'-S=\{V\}$。定义中的非负参数ε被称为隐私预算，该参数的大小直接限制着上述概率差距。对敌手来说，差距越大，可能分析出的信息越多，则用户的隐私性越弱；对统计来说，差距越大，统计所得的信息越多，统计精度就越高，这就是差分隐私中隐私性与数据效用的权衡问题。除了上述定义外，还有一种常用的松弛型的(或近似的)差分隐私定义，使用ε和δ两个参数来描述概率差距，其中的δ称为失败概率。

定义2((ε,δ)-差分隐私(松弛型差分隐私)) 一个随机化机制M满足(ε,δ)-差分隐私($\varepsilon>0,\delta>0$)，当且仅当对于任何相邻的输入数据集S和S'以及任意可能的输出值集合R，有$Pr[M(S)\in R]\leqslant e^{\varepsilon}\cdot Pr[M(S')\in R]+\delta$成立。

概括来说，松弛型的差分隐私定义(ε,δ)-DP可以理解为该机制以最小$1-\delta$的概率满足ε-DP[5]。

2.2 本地化差分隐私

本地化差分隐私[6](Local Differential Privacy，LDP)是对中心化模型的一种分布式改进，消除了对可信服务器的假设。在这种模型下，分布于N个用户端的数据项分别在用户本地被随机化机制处理，随后用户端将处理后的信息经过安全信道提交给服务器，服务端对数据进行聚合，使用与随机化机制相对应的修正算法得到统计量的无偏估计量。因为服务端从

每个用户得到的数据项都经过了客户端的本地随机化处理，所以在 LDP 模型中不需要假设服务器是受信任的。本地化差分隐私模型如图 2 所示。

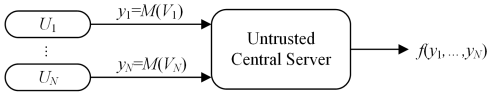


图 2 本地化差分隐私模型

Fig. 2 Local differential privacy

除了随机性添加的阶段不同之外，CDP 和 LDP 的另一个区别在于，前者的噪音添加对象是数据集的统计信息，而后者的噪音添加对象是每个用户的原始数据项。因此，基于 CDP 的思想，针对单个数据项的 LDP 定义如定义 3 所示。

定义 3(ε-LDP) 一个随机化机制 M 满足 ε-$LDP(\varepsilon>0)$，当且仅当对于任何输入值对 V 和 V' 以及任意可能的输出值 y，有 $Pr[M(V)=y]\leqslant e^{\varepsilon}\cdot Pr[M(V')=y]$ 成立。

直观上讲，该定义限制了任何两个输入值得到相同输出值的概率的差距，差距量由隐私预算 ε 描述，预算越多则可允许的差距越大。此外，与松弛型 CDP 的定义类似，LDP 也有松弛型定义，相应地被称为(ε,δ)-LDP，具体定义如定义 4 所示。

定义 4(ε,δ)-LDP 一个随机化机制 M 满足(ε,δ)-LDP ($\varepsilon>0$,$\delta>0$)，当且仅当对于任何输入值对 V 和 V' 以及任意可能的输出值 y，有 $Pr[M(V)=y]\leqslant e^{\varepsilon}\cdot Pr[M(V')=y]+\delta$ 成立。

2.3 差分隐私洗牌模型

差分隐私洗牌模型(Shuffle Model Differential Privacy)最早由 Bittau 等[7]提出，他们提出了一个隐私保护的软件监控系统架构，整体架构分为编码器(Encoder)、洗牌器(Shuffler)和分析器(Analyzer)3 个组件，因此也被称为 ESA 架构。编码器与分析器会完成 LDP 模型中的客户端与服务端的相应功能，即编码器为用户输入值添加扰动噪声得到随机化输出，分析器收集用户的输出并通过修正方法计算得到所需统计信息的无偏估计量，而洗牌器则在这两者之间将编码器提交的消息进行匿名处理并随机排序，然后将其转发给分析器，这一步骤就被称为洗牌。洗牌步骤消除了数据项和其拥有者之间的直接关联性，在面对非受信的服务器时提供了匿名化效果，从而增强了数据的隐私性。差分隐私洗牌模型如图 3 所示，其中函数 $\pi(\cdot)$ 表示经过洗牌处理后的顺序。

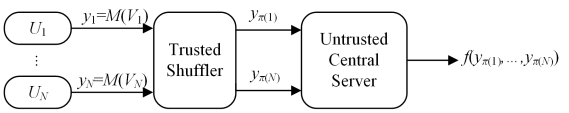


图 3 差分隐私洗牌模型

Fig. 3 Differential privacy shuffle model

在 ESA 架构的基础上，Cheu 等[8]建立了单消息洗牌协议的理论模型，并推广到了多消息洗牌协议。该工作分析了洗牌模型下差分隐私算法的性能，并证明了洗牌模型的精度水平严格介于 CDP 和 LDP 之间，还得出了洗牌模型可以通过增加消息数来提高精度的结论。

2.4 3 个模型的比较结果

差分隐私的 3 种模型各有一定的优缺点。在模型和信任依赖方面，相比由持有数据库的数据发布者进行随机化处理的 CDP 模型，LDP 模型和洗牌模型的扰动过程都是本地化的，因此它们都不依赖可信服务器来确保随机化机制的正确执行，但洗牌模型需要依赖可信的洗牌器中介将用户提交的隐私值匿名化处理并转发给第三方服务器。此外，由于扰动过程是本地化的，LDP 模型和洗牌模型的噪音扰动对象都是属于单一用户的数据记录，而 CDP 模型则是对数据集的统计输出结果添加噪音，这一区别也体现在了 LDP 和 CDP 在形式化定义上的差异。针对不同的噪音扰动对象，其一般扰动机制也不相同：CDP 模型针对连续型输出结果常用加性噪音(例如 Laplace 噪音)以及离散型输出结果常用指数机制；而 LDP 模型和洗牌模型的基本方法大多是随机响应机制。

误差界是衡量不同差分隐私模型性能的一个重要指标，文献中为比较误差界常用的方法是分析不同模型在满足 ε-差分隐私(或(ε,δ)-差分隐私)的条件下解决求和估计问题(即估计 N 个用户隐私值的和)时所产生的额外误差的渐进界，误差指标通常使用绝对误差或平方误差。例如，Chan 等[9]研究了本地化模型下的整数求和问题，得到了额外误差具有 $\Omega(\sqrt{N})$ 的下界，并证明了该下界的紧确性；Beimel 等[10]研究了本地化模型下的比特求和问题，得到了至少 $O(\sqrt{N})$ 的额外误差，并证明了不存在误差小于 $O(\sqrt{N})$ 的 LDP 比特求和协议；而 Dwork 等[11]研究了中心化模型下包括比特求和在内的一系列估计问题，并给出了中心化模型下具有 O(1)额外误差的随机化机制。因此，一般认为 CDP 模型的误差界是 O(1)，LDP 模型的误差界是 $O(\sqrt{N})$，这两种模型间的误差呈现严重分离的情况，也为实践中的方案选择带来了困难，而洗牌模型的出现则一定程度地缓解了该问题。Cheu 等[8]证明了实数求和问题中一般多消息洗牌模型协议的误差界为 $O(\log N)$，该结果严格介于 O(1)和 $O(\sqrt{N})$ 之间，此外还研究了洗牌模型的样本复杂度问题。样本复杂度也被作为比较不同模型性能的指标之一。样本复杂度指对于一个具体的优化问题，ε-差分隐私协议对任意数据集 S 能够以常数概率 $1-\beta$ 成功解决该问题至少需要的样本数量 N 的复杂度。例如在经典的变量选择问题中，Ullman 等[12]指出了一个(ε,0)-LDP 协议以 0.9 的概率解决变量选择问题的样本复杂度为 $\Omega(b\log b/(e^{\varepsilon}-1)^2)$，其中参数 b 是变量选择问题的维度。在该结果的基础上，Cheu 等[8]证明了一个(1,0)-DP 的单消息洗牌协议以 0.99 的概率解决变量选择问题的样本复杂度为 $\Omega(b^{1/17})$。相对地，在中心化差分隐私模型下，Bafna 等[13]证明了指数机制[14]解决变量选择问题所需的样本复杂度为最优的 $\Theta(\log b)$。类似地，在直方图问题中，中心化模型下可以得到最优的样本复杂度为 $O(\min\{\log\delta,\log d\})$[15]，($\varepsilon$,0)-LDP 协议以 0.9 的概率解决直方图问题的样本复杂度为 $\Omega(\log d/(e^{\varepsilon}-1)^2)$[16]，(1,0)-DP 的单消息洗牌模型协议以 0.99 的概率解决直方图问题的样本复杂度为 $\Omega(\log^{1/17}d)$[8]。误差界和样本复杂度从两个不同角度体现了 3 种差分隐私模型的特性。有关 3 个模型的比较结果如表 2 所列。

表 2 3 个差分隐私模型的比较

Table 2 Comparison of three differential privacy models

Model	Trust dependence	Disturbed object	Basic mechanism	Error bound	Sample complexity
Central model	Centralized server	Statistics of datasets	Laplace/Exponential mechanism	$O(1)$	Low
Local model	Nothing	Single data item	Randomized response	$O(\sqrt{N})$	High
Shuffle model	Shuffler	Single data item	Randomized response	$O(\log N)$	Medium

在实用性和效率考量方面，基于不同模型的随机化机制也有不同的目标。在 CDP 模型下，随机化机制由受信服务器执行，通常算力充足，能够承担复杂的计算任务，因此主要的考量目标是随机化机制的估计精度。在 LDP 模型和洗牌模型下，用户端需要本地执行编码和随机化计算，并将结果发送给服务器或洗牌器，最后由服务器进行统计和修正，因此除考虑精度外，还需要考虑用户端承载的计算复杂度和通信复杂度。此外，在洗牌模型下，可信洗牌器的高效实现是一个有待优化的问题。文献[8]使用混合网络(Mixnet)来实现安全的洗牌器，文献[7]则使用在可信硬件上设计的高效盲洗牌算法来达到洗牌的目的。以上两种方案中，前者将大大增加协议整体的通信复杂度，而后者的盲洗牌算法将带来额外的计算负担，虽然实践中也可以通过多方安全计算来实现安全洗牌，但都面临着效率问题，因此如何实现高效的洗牌器仍然是一个待解决的问题。

3 各模型下的差分隐私算法

自差分隐私被提出以来，不同模型下都出现了大量的随机化方法，本节简要介绍了其中最典型的若干机制。随机化算法是差分隐私协议的核心部分，在 CDP 模型中由服务器应用随机化算法后的统计输出，可以直接作为统计结果发布，而在 LDP 模型和洗牌模型中，由用户端对原始值应用随机化算法并将输出值直接或通过洗牌器发送给服务器，服务器在计算统计输出时要使用相应的统计修正算法来得到统计结果。

3.1 CDP 模型中的经典算法

在 CDP 模型下，最典型的两种方法分别是适用数值型输出的 Laplace 机制和适用非数值型输出的指数机制。

3.1.1 Laplace 机制

Laplace 机制[11,17]是一种著名的加性噪声机制，会向数值型的统计输出结果添加从位置参数为 0 的 Laplace 分布中采样得到的噪声。为了满足严格的差分隐私定义，所使用的 Laplace 分布必须有合适的尺度参数，因此该机制为统计输出函数引入了敏感度的概念。

定义 5(统计函数的敏感度) 对于任何一个数值型统计函数 $f: D^N \to \mathbb{R}$，敏感度 $\Delta f := \max_{S,S' \in D^N} |f(S)-f(S')|$。

直观来看，敏感度指任意两个相邻数据集所得统计输出的最大差值。为了使任意两个相邻数据集的统计输出有概率相等，且概率差距比例最大为 e^{ε}，就要使两次噪音采样的差值为 Δf 的概率之比最大为 e^{ε}。由 Laplace 分布的轴对称特性和轴两侧的凹函数特性易知，两次采样分别在 0 和 $\pm\Delta f$ 处满足概率之比最大。记 Laplace 分布的概率密度函数为 $Lap(x|0,\lambda)$，根据 $Lap(0)/Lap(\Delta f)=e^{\varepsilon}$ 求解可得 $\lambda=\Delta f/\varepsilon$。因此，一个满足 ε-DP 的 Laplace 机制对敏感度为 Δf 的统计函数结果所添加的随机噪声 γ 应取自分布 $Lap(x|0,\Delta f/\varepsilon)$，该机制的扰动后输出结果为 $f(S)+\gamma$。因为 $E(\gamma)=0$，所以 Laplace 机制的输出结果为真实结果的无偏估计量，该估计量的方差为 $D(\gamma)=2\Delta f^2/\varepsilon^2$。

3.1.2 指数机制

不同于 Laplace 机制，指数机制是适用于非数值型输出的[14]，即对数据集进行的统计查询的输出域是一个离散的域，也可视作一个有限集合。针对一个具体的统计任务，指数机制定义一个可用性函数映射，为每个数据集和其可能的输出值构成的二元组映射到一个实数值上，即 $u:=D^N\times O\to\mathbb{R}$，其中 O 表示对数据集进行统计查询的输出域。一个指数机制 M 对数据集 S 的输出为 o_i 的概率为 $Pr[M(S)=o_i]=\exp(\varepsilon\cdot u(S,o_i)/2\Delta u)/\sum_{o_j\in O}\exp(\varepsilon\cdot u(S,o_j)/2\Delta u)$，其中 Δu 为可用性函数 u 的敏感度，$\Delta u:=\max_{S,S'\in D^N}|u(S,o_i)-u(S',o_i)|$。直观来讲，对于任何一个特定的数据集，可能的统计输出从域 O 中随机选择，输出值 o_i 所对应的可用性函数值越大，其被选择的概率也越大。此外，概率差距也受到隐私预算 ε 的直接影响，从概率公式可见，ε 作为效用函数的乘法因子，ε 越大，由效用函数带来的概率区分度就越高，在减弱隐私性的同时提高了统计精度；而当 ε 趋近于 0 时，输出所有值的概率都相等，此时的隐私性最强但统计输出完全随机，失去了统计意义。

3.1.3 小结

Laplace 机制和指数机制是 CDP 模型下最典型的两种方法，有关中心化模型下差分隐私的文献中大都基于相同的思想。例如，高斯机制[17]使用加性高斯噪音来处理统计输出，可用于实现松弛型的差分隐私；指数机制是为每一种特定输出定义输出概率的方法，该思想也常见于其他适用于非数值型输出的机制中。

3.2 LDP 模型中的经典算法

适用于 LDP 模型的算法在文献中有很多研究，针对不同类型的统计任务或不同类型的统计数据衍生出了大量的工作，本节介绍了其中一些经典的 LDP 机制。通常来说，一个本地化的随机化算法首先将原始信息进行适当编码，然后在编码的基础上进行随机扰动，掩盖原始信息。适当的编码方式可以降低用户端的通信复杂度，利于实现更优化的随机扰动算法，但也会为通信双方带来一定的计算负担。

3.2.1 k 维随机响应机制(k-RR)

在 LDP 模型中，最经典的实现方法是随机响应[18-20]，这是针对分类数据的一种常用方法，指数机制及大多数 LDP 机制都具有随机响应的部分思想。该方法最初被提出，是用于消除回避性回答偏差的一种统计调查技术[18]，在抽样调查中，受试者可能因为各种各样的原因逃避诚实回答，这种误差在统计学中被称为回避性回答偏差。简单来说，随机响应指提交信息的用户以一定概率提交真实信息，否则随机提交

其他信息。例如，每个真实值为V_i的用户U_i使用如下规则提交其信息：$Pr[y_i=V_i]=a$，$Pr[y_i=V_j, j\neq i]=(1-a)/(d-1)$。为使这样一个随机响应机制满足ε-LDP，就需要使不同原始值V_i映射到同一输出值y_i的概率之比最大为e^ε，即$a(d-1)/(1-a)=e^\varepsilon$，由此计算出$a$的表达式就得到了满足ε-LDP的$d$维随机响应机制$M$：$Pr[M(V_i)=V_i]=e^\varepsilon/(e^\varepsilon+d-1)$，$Pr[M(V_i)=V_j, j\neq i]=1/(e^\varepsilon+d-1)$。

在LDP模型中，当用户在本地执行随机响应算法后，服务器收集所有扰动值并对各类数据计数，然后使用相应的修正算法计算每类数据的真实频率。在上述例子中，服务端对数据V的频率估计值为$\hat{f}_V=\{N_V(e^\varepsilon+d-1)-N\}/N(e^\varepsilon-1)$，其中$N_V$表示服务器收集得到的值$V$的数量，可以证明该估计量为值$V$的真实频率的无偏估计量，方差为$Var_V=\{e^\varepsilon+d-2+f_V(e^\varepsilon-1)(d-2)\}/N(e^\varepsilon-1)^2$，由于值$V$的频率值一般较小，在考虑误差时通常将分子中的$f_V$一项忽略。

3.2.2 最优一元编码机制(OUE)

上述的随机响应机制没有使用任何编码方法，直接对原始数据进行扰动变换，而一元编码机制[21]使用了最简单直接的编码方式。在一元编码机制中，每一个原始值$V_i\in D$都被编码成一个d比特长的特征向量$\boldsymbol{B}$，其索引对应为V_i的比特被置1，其余比特置0。在随机化步骤中，用户对向量$\boldsymbol{B}$的每一个比特进行扰动，如果原$\boldsymbol{B}[i]=1$，则扰动后$\boldsymbol{B}[i]$仍为1的概率是p；如果原$\boldsymbol{B}[i]=0$，则扰动后$\boldsymbol{B}[i]$变为1的概率是q，其中概率值$p>q$。直观来说，每一个仅含一个特征位的特征向量都会被随机化为包含若干个特征位的向量，原始特征位会以较大概率p保留，而非特征位会以较小的概率q反转为特征位。

同样地，满足ε-LDP的定义需要使不同原始值映射到同一输出向量的概率之比最大为e^ε。考虑任意两个特征位不同的特征向量$\boldsymbol{B}$和$\boldsymbol{B}'$，计算它们映射到同一向量$\boldsymbol{B}^*$的概率之比$Pr[\boldsymbol{B}^*|\boldsymbol{B}]/Pr[\boldsymbol{B}^*|\boldsymbol{B}']$，对于$\boldsymbol{B}$和$\boldsymbol{B}'$都为0的$d-2$个比特位，不论$\boldsymbol{B}^*$对应位是0或1，分子分母中的概率都是相消的，而对于$\boldsymbol{B}$和$\boldsymbol{B}'$不同的2个比特位，在4种情况中仅当$\boldsymbol{B}^*$和$\boldsymbol{B}$完全相同时分子概率项最大而分母概率项最小，从而得到条件式$Pr[\boldsymbol{B}^*|\boldsymbol{B}]/Pr[\boldsymbol{B}^*|\boldsymbol{B}']\leqslant p(1-q)/q(1-p)=e^\varepsilon$，任何满足该条件式的$p$和$q$的设置都可以得到满足ε-LDP的一元编码机制。当服务器对值V的频率进行统计计算时，首先对收集到的N个d比特向量的V索引位进行计数得到X_V，然后计算无偏估计量$\hat{f}_V=(X_V-Nq)/N(p-q)$。一元编码机制对频率估计的理论方差为$Var_V=(1-q+qe^\varepsilon)^2/Nq(1-q)(e^\varepsilon-1)^2$，为得到最优的理论方差，将$Var_V$对$q$求导，计算极小值点处的$q$取值，可得到$p=1/2$，$q=1/(e^\varepsilon+1)$，从而得到最优的一元编码机制，此时的最优方差为$Var^*=4e^\varepsilon/N(e^\varepsilon-1)^2$。

3.2.3 最优本地哈希机制(OLH)

本地哈希机制[21]是一个使用哈希函数进行编码的LDP机制，相比OUE机制使用每个用户$O(d)$的通信开销，本地哈希机制能够在数据域较大时降低用户的通信开销。在该机制中，每个用户首先从哈希函数族$\mathcal{H}$中选取一个哈希函数H_i，该哈希函数会将大小为d的数据域D映射到大小为g的域G上($g<d$)，用户端计算其真实值V_i的映射$x_i=H_i(V_i)$，然后对域G中的值x_i应用g维随机响应机制得到输出结果y_i，最终用户上传一个二元组$\langle H_i, y_i\rangle$到服务器。从本质上说，本地哈希机制可以分为两部分，第一部分通过哈希函数族将原数据域D压缩到更小的数据域G上，第二部分则在压缩后的数据域上部署随机响应。

不同于随机响应机制的是，本地哈希的参数g是一个可以优化的参数，通过用理论方差对g进行求导，可得到使理论方差最小化的取值$g=e^\varepsilon+1$，从而在给定的隐私预算条件下选择最优的参数g，实现最优的统计精度，即最优本地哈希机制，其估计方差与最优一元编码相同。

服务器进行统计时，首先将消息$\langle H_i, y_i\rangle$进行解码，即对所有满足$H_i(V)=y_i$条件的值V增加计数。假设对全部消息解码后得到值V的计数为θ，则值V所出现频率的无偏估计值为$\hat{f}_V=(g\theta-N)/N(pg-1)$，其中参数$p$是$g$维随机响应中原值扰动后保持不变的概率。

3.2.4 k-子集选择机制(k-Subset)

上述几种方法可以归纳为从一个值映射到另一个值的随机化方法，而k-子集选择机制[22]则将一个值映射到值域上的一个大小为k的随机子集(即k-子集)。对于一个数据域D，其大小为k的子集有C_d^k个，对于数据域上任意一个值V，这些大小为k的子集中有k/d的比例包含值V，剩余$1-k/d$不包含值V。在k-子集选择机制中，每个原始值V以概率p被随机编码为一个包含V在内的k-子集，以概率q被随机编码为一个不包含V的k-子集，其中概率p和q满足$p(k/d)C_d^k+q(1-k/d)C_d^k=1$且$p/q=e^\varepsilon$。

服务器的聚合过程与OUE机制类似，在收集了所有用户提交的子集之后，计算所有子集中出现值V的次数N_V，则值V频率的无偏估计量为$\hat{f}_V=(N_V-Q)/(P-Q)$，其中$P=p(k/d)C_d^k$，$Q=pC_d^k\frac{k(k-1)}{d(d-1)}+qC_d^k\frac{k(d-k)}{d(d-1)}$。

3.2.5 Hadamard响应机制

Hadamard响应机制[23](以下简称Hadamard机制)是一个基于Hadamard矩阵进行编码的LDP机制，利用了Hadamard矩阵的行间汉明距离大的特点，提高了统计性能，利用快速Walsh-Hadamard变换提高了计算效率。具体来说，该机制首先根据输入域$D=[d]$的大小来确定输出域K的大小$k=2^{\lceil\log_2(d+1)\rceil}$，然后使用$k$阶Hadamard矩阵$\boldsymbol{H}_k$行编码，每个值$x\in[d]$对应于$H_k$的第$x+1$行，记元素集合$C_x=\{i|H_k[x+1][i]=1\}$，$C_x\subseteq K$，则值$x$的扰动输出$y$根据以下概率随机响应：如果$y\in C_x$，则$Pr[y|x]=\frac{2e^\varepsilon}{k(e^\varepsilon+1)}$，如果$y\in K-C_x$，则$Pr[y|x]=\frac{2}{k(e^\varepsilon+1)}$。

服务器对值x的频率进行估计时，统计所收集的N个扰动值中属于集合C_x的值的频率$p(C_x)$，即可计算值x频率的无偏估计量$\hat{f}_x=\frac{2(e^\varepsilon+1)}{e^\varepsilon-1}(p(C_x)-1/2)$。服务器可以通过快速Walsh-Hadamard变换对Hadamard矩阵进行高效的矩阵

乘法，一次性完成所有值的频率估计计算。Hadamard 机制在保证了估计精度与子集选择机制接近的情况下，利用 Hadamard 矩阵编码，降低了协议的通信复杂度，并显著地提高了计算效率。

3.2.6 用于键值数据的 LDP 机制

除了上述几种机制中的离散型分类数据之外，键值数据也是实践中经常会遇到的一类数据，例如推荐系统中的电影评分数据。对于键值类型的数据，统计中需要同时估计键的频率和每个键对应值的均值。对键值类型数据统计的难点在于，键值数据具有两个不同的数据维度，且两个维度之间存在着内在的关联性，因此在对每个维度进行随机化的过程中就必须考虑其中的关联性，若两个维度独立地添加噪声则会对数据效用产生很大影响。此外，每个用户也可能会有多个键值数据，使得每一个键值数据可分配的隐私预算更小，迫使噪音扰动更大。

Ye 等[24]首次提出了名为 PrivKVM 的机制来估计键值数据的频率和均值，考虑到键值相关性，该协议使用了多轮交互的方式迭代地改进对键值的均值估计，当迭代次数足够多时，可证明其均值估计值为原始值的无偏估计量。Gu 等[25]改进了这一工作，提出了非交互式的单轮协议框架 PCKV，改进了 PrivKVM 的采样协议和预算分配策略，一方面降低了多轮交互导致的误差，另一方面通过近似最优的预算分配策略进一步提高了隐私效用权衡。Gu 等还在该框架下提出了 PCKV-UE 机制和 PCKV-GRR 机制，并证明了其渐进无偏性和近似最优的预算分配策略。

3.2.7 针对多维数据的采样方法

在多维数据的处理中，一个关键的问题是隐私预算的分配，基本的方法是基于组合原理[17]，将隐私预算平均分配到需要收集的每个维度上，假设数据维度为 w，则每个属性获得的隐私预算是 ε/w，当隐私预算较小或数据维度较高时，平均分配到每个属性的隐私预算就更受限，显著降低了数据效用。因此，文献[26-28]提出了采样机制，每个用户在提交数据时，从 w 个属性中随机选择一个属性并分配全部隐私预算来进行扰动，仅提交所选属性的扰动值给服务器。服务器在对某属性进行统计时，等同于从用户群体中随机选择了 N/w 个用户来进行该属性的统计计算，因此还可以借助采样放大原理[29]，使用比 ε 稍大的隐私预算 ε' 来实现 ε-LDP，从而进一步提高了数据效用，并且能够弥补由随机采样带来的采样误差[26,30]。Wang 等[26]还提出了从 w 个属性中随机选择 m 个属性进行扰动和提交的采样思想。通过以最小化噪音误差为标准来选择最优的 m 值，可以在保证隐私的情况下有效提高数据效用。

此外，Arcolezi 等[30]指出，相比平均分配的隐私预算 ε/w，随机采样某一属性并分配全部的隐私预算 ε 面临着更高的隐私风险，意味着服务器能够以更高的概率获取用户特定属性的真实信息。因此，文献[30]提出了加入假数据的随机采样机制，通过对采样外的其余属性添加随机的假数据项，使服务器无法直接确定用户所采样的特定属性。该方案在解决了上述隐私风险的情况下能够实现与现有采样方案相同甚至更好的数据效用。

3.2.8 差分隐私的后处理优化算法

如前文所述，通常差分隐私算法所得的输出量是真实统计值的无偏估计量，因此所得结果是一个以真实值为中心的波动值。在最基本的频率查询任务中，数据域较大的情况下，大部分类型值的频率都将接近于 0，当添加了一个期望值为 0 的随机噪声时，经修正后的频率估计值可能产生小于 0 的无意义结果，同时如果要统计数据域内所有值的频率，这些频率之和可能不为 1。

意识到这一点后，Wang 等[31]提出了利用非负性约束和归一性约束对 LDP 的频率查询结果进行后处理的 10 种机制，并研究分析了不同机制的性能，该工作通过实验证明针对不同的频率查询类型宜使用不同的后处理方法，并给出了详细的后处理方案选择策略，例如针对全数据域的频率估计建议使用 Base-Cut 方法，针对最频繁值的频率估计则应使用 Norm 方法。此外，Jia 等[32]提出利用有关待测数据集分布的先验知识来优化估计精度，例如假设所统计的数据集已经服从某一参数的正态分布或齐夫分布，利用已获得的先验知识可以对频率估计的结果进行进一步优化，但是这样的先验知识在实践中并不总是存在的。

3.2.9 小结

本节介绍了在 LDP 模型下的一些随机化机制，包括随机响应机制、一元编码机制、哈希编码机制、子集选择机制、Hadamard 响应机制以及用于键值数据的相关算法。其中，随机响应机制的思想对目前的 LDP 算法有着深刻影响，大多数 LDP 算法都基于随机扰动的方法，有一些还结合了经典 CDP 机制中所使用的加性噪音。然后，介绍了在处理多维数据时使用的采样方法，合适的采样方法既能够降低通信复杂度，又能够提高数据效用，同时仍然保持严格的隐私性。最后，介绍了针对 LDP 机制提出的后处理优化算法，利用了频率估计任务中基本的先验知识来对估计结果做进一步优化。

3.3 洗牌模型下的差分隐私协议

有关洗牌模型差分隐私协议的研究目前正处于起步阶段，Cheu 等[8]的研究表明，一个满足 ε-LDP 的协议可以通过添加洗牌器中介得到一个洗牌模型下的具有更好隐私参数的协议，从而可以在使用相同隐私预算的条件下获得更高的统计精度。下文列举了现有文献中的若干工作。

Bell 等[33]首次提出将安全向量聚合协议应用在安全洗牌协议的实现中。该项工作首先设计了一个能够实现对数级开销的安全聚合协议，然后提出可使用安全向量聚合协议来实现一个差分隐私洗牌模型的实例。该实例借助名为可逆布隆查找表(Invertible Bloom Lookup Table，IBLT)的数据结构，IBLT 表是近似成员查询(Approximate Membership Queries，AMQ)数据结构的一种，作为对多重集的一种有损表示，IBLT 表可以用较小的空间表示一个完整多重集，同时以一定概率可逆地恢复所有数据项。该方案利用了 IBLT 的表示特性，首先用户端将其任意差分隐私消息 V_i 编码为一个长度为 L 的 IBLT 表，用户端和服务端借助该工作提出的安全向量聚合协议，将 N 个具有向量形式的 IBLT 表进行安全求和，并使服务器得到求和后的结果表，然后服务器可通过 IBLT 表的可逆性依次恢复全部原始消息，但无法区分消息内容和

对应的发送者。该方案实现的洗牌模型差分隐私协议能够继承安全向量求和协议的鲁棒性、可扩展性和密码安全性，但受限于 IBLT 结构为确保可逆性的要求，每个用户提交表的长度 L 至少达到 $1.3N$ 才能够保证稳定地恢复全部信息，该线性复杂度能否进一步优化目前被作为一个开放性问题。

Cheu 等[8]提出了洗牌模型下的简单布尔求和协议，基于一般随机响应的方法，每个用户持有的布尔值以一定概率诚实回答，否则以均匀随机的布尔值回答，所有用户扰动后的布尔值经过随机洗牌打乱顺序后发送给聚合器，聚合器通过计算无偏估计量恢复 N 个比特的和。基于上述简单布尔求和协议，Cheu 等[8]还提出了多消息洗牌模型下的实数求和协议，该协议首先将任意范围内的实数值标准化为$[0,1]$上的实数值，然后将$[0,1]$上的实数 V 编码成 k 个布尔值消息，服务器经过洗牌器收集 $N*k$ 个布尔值进行求和，然后计算无偏估计量得到求和结果，该工作证明了通过每个用户发送 $k=O(\sqrt{N})$的消息数量足以实现一个误差为 O(1)的多消息实数求和协议。

Balle 等[34]设计了单消息洗牌模型的实数求和协议，通过设置一个精度参数 r，该协议将$[0,1]$上的实数 V 编码成精度 r 范围(即集合$\{0,1,\cdots,r-1\}$)内的一个整数值，用户在随机化步骤中以 p 概率从精度 r 范围内均匀随机选择一个整数作为响应，以 $1-p$ 的概率以编码后的整数值作为响应。一方面，以 r 精度进行舍入编码引入了一定的误差，另一方面，以概率 p 从精度 r 中选取随机值作为响应也引入了与参数 r 和 p 大小相关的误差。该工作通过优化参数 r 和 p 的选择来平衡精度舍入和随机响应带来的误差，从而达到了最优的单消息实数求和协议，其误差界为 $O(N^{1/3})$。Balle 等的后续工作[35]又提出了基于上述协议的递归结构，将实数 V 的一级精度 p 划分为更多级细化的精度$p_1,p_2,\cdots,p_m$，得到一个每用户提交 m 个消息的多消息洗牌模型的实数求和协议，可以针对每一段细化的精度级定义不同的随机响应概率，在对误差影响较敏感的精度级下设置较低的随机响应概率可以有效地降低噪音规模，其误差界在消息数 $m=O(\log(\log N))$时达到 $O((\log(\log N))^2)$。

基于 Ishai 等[36]提出的一个从安全精确求和到洗牌模型的归约，Balle 等[35]还提出了对该归约的新分析，从而得到在洗牌模型下具有常数级误差和常数级消息数的实数求和协议。文献[36]提出的是一个使用模 h 的群内的加法秘密共享体制和洗牌器来进行安全求和的协议，该协议将每个用户的持有值V_i编码为Z_h群上的 m 个加法秘密共享份额，然后通过洗牌器发送给服务端，服务端执行Z_h群上的加法求和即可得到正确结果。该协议给出的安全性声明是：只要 $m=O(\log(hN)+\sigma)$，就足以以最坏情况统计安全参数 σ 保证聚合器无法从视野中区分两个和均为V_i的 m 元组。通过对该结论的改进分析，Balle 等证明了使用一个 $m=O(1)$的多消息安全求和仍然可以达到同样的统计安全性，此外，因为一个离散的 Laplace 噪声变量 $X\sim Lap(0,\alpha)$可以分解为 N 个独立同分布的噪声变量 Y 之和，其中 $Y=Z_1-Z_2$，$Z_i\sim$Pólya$(1/N,\alpha)$，$i=1,2$。协议通过将 N 个噪声变量 Y 分布到 N 个用户端，使最终求和结果达到了与中心化 Laplace 机制相同的常数级误差。该工作得到了一个在差分隐私洗牌模型下的具有常数级别消息和常数级误差的实数求和协议，但一个潜在的问题是每个用户端添加的随机化噪音规模与 $1/N$ 呈正比，当用户数量较大时，用户端所添加的噪音规模很小。

有关差分隐私洗牌模型的理论研究和协议设计正处于起步阶段，有关洗牌模型的精度提升已有一些研究，实践中如何高效地实现安全可靠的洗牌模型仍是一个关键问题。

4 差分隐私技术在多领域的应用

4.1 机器学习

已有文献提出了使用差分隐私来部署保护隐私的机器学习[37-40]。在一个中心化的隐私数据集上进行的机器学习算法可以通过添加噪音的方法实现差分隐私，例如 Chaudhuri 等[37]通过界定正则逻辑回归的敏感度并根据敏感度校准噪声对学习来的分类器进行扰动，提出了一个满足差分隐私的正则逻辑回归算法，该方案已被用于研究隐私和学习效用之间的权衡。Zhang 等[38]通过对机器学习训练算法的目标函数添加适量的扰动，开发出了一系列基于优化的差分隐私机器学习算法，该机制被用于线性回归和逻辑回归模型，并表现出了很高的精度。Wu 等[39]则关注于分布式机器学习场景，将随机噪声扰动应用在学习者对分布式数据库的梯度查询响应中，开发了分布式隐私数据机器学习的差分隐私梯度下降算法。通过将适应度成本作为隐私预算和分布式数据集大小的函数，该工作将训练模型的质量量化，可以在执行机器学习算法之前预测所得模型的实际性能。此外，该项工作还证明了，在分布式机器学习模型的基础上添加差分隐私梯度查询机制所带来的适应度差异与训练集大小的平方和隐私预算的平方成反比。目前结合差分隐私的机器学习已逐渐得到关注，如何在提供足够隐私的情况下降低数据维度、提高模型精度以及应用更多种目标函数将是未来的研究重点。

4.2 车联网

车联网是实现智能交通管理、智能车辆控制的有效方案，然而车辆数据的隐私问题是车联网应用和发展的主要阻碍，因此差分隐私作为一个严格的隐私概念被应用到车联网这一分布式网络模型中。Ghane 等[41]提出了 LDP 模型下隐私保护的车联网数据流收集系统，该方案采用了适合车联网边缘网络结构的用户分组思想，在每个边缘控制器所通信的车辆群组中通过算法选择一个作为群主，群主收集组内成员的各种状态信息(如移动方向、速度、位置、环境条件等)并进行处理。考虑到所收集信息的强关联性，群主首先对聚合得到的数据矩阵做哈尔小波变换来进行压缩，哈尔小波变换是一种正交变换，可消除矩阵中各项数据之间的关联性，然后群主再对各数据项添加独立的拉普拉斯噪声。此外，考虑到在每一个时间戳都会实时地收集数据流，将导致过多的隐私预算消耗，因此在添加噪声之后，群主会对数据矩阵做阈值化处理，只有当前矩阵和上一时间戳所得矩阵在概率分布上的差异超过一定阈值时才会向边缘控制器提交新的数据矩阵，从而降低了频繁连续数据流的隐私开销。目前差分隐私技术在车联网场景的应用仍处于初级阶段，面临着诸多挑战，包括复杂的数据类型、多样的分析查询任务、高维度的数据以及车辆间

数据的关联性等。有关 LDP 在车联网隐私保护的更多应用详见 Zhao 等的综述[42]。

4.3 社交网络分析

随着对社交网络分析、知识图谱等领域的广泛研究，图数据的差分隐私保护也引起了人们的关注[43-48]。在传统的社交网络模型下，中心服务器可以掌握整个社交网络的信息，而在进行图相关的统计和发布时，为保护原始图中的敏感信息，可以使用相应的差分隐私机制。基于图数据的结构，对其进行的隐私保护可以分为对边的隐私保护和对节点的隐私保护，分别称为 Edge-DP 和 Node-DP，Node-DP 可以提供更强的隐私保护，但实践中对数据效用的影响较明显。目前已有的主要方案是基于查询的敏感度添加噪音[43-44]，而面临关于图的大多数分析任务，查询函数的敏感度通常较高，导致效用难以提升。文献[49]为缓解该问题提出了两类方法。第一类方法是通过一定的图转换技术将原始图转换为一个度数有界的新图，从而降低对新图进行统计查询的敏感度，缺点是图转换过程中也会引入一定的误差。第二类方法是在查询的全局敏感度的基础上提出了与原始图有关联性的局部敏感度概念，由于全局敏感度是查询函数本身的内在属性，其与数据集无关的特点常常使噪音添加规模不合理，引入与原始图有关联的局部敏感度可以根据原始图本身调节噪音的规模，而由于局部敏感度也会泄露原始图的信息，因此一般使用局部敏感度的平滑界作为噪音规模的标准，该方法的缺点是局部敏感度的紧缺平滑界通常难以计算。

在分布式社交网络模型下，没有可信方持有完整的网络图，为重构一个去中心化的社交网络图，分析者需要从每个用户端收集其本地视角，但出于隐私考量，这一过程需要在差分隐私限制下进行。相应地，图数据的本地化差分隐私保护也分为两个方面，即 Edge-LDP[50] 和 Node-LDP[51]。在 Edge-LDP 场景下，一种直接的方式是对每个用户提交的邻接关系向量逐比特使用随机响应机制，该方法被称为随机邻接列表机制(RNL)[52]。服务器收集所有邻接关系向量并合成邻接关系矩阵，从而得到合成网络图，但该方法会为网络图引入较多虚假边，导致合成网络图的精度较低。另一种直接的方式是仅对每个用户收集其节点度数，用户在本地使用任意扰动机制对度数添加适量的噪音，例如 Laplace 机制，然后服务器收集汇总所有用户的节点度数，再通过 BTER 图生成算法[53]来合成最终的社交网络图，但这种方法仅收集节点度数而不包含节点间邻接关系，导致生成图损失了相当一部分的结构信息。Qin 等[52]提出了名为 LDPGen 的 Edge-LDP 社交网络图机制，该方案基于分组和迭代的方法，在每一迭代轮次中都使用合适的隐私预算收集用户的少量邻接信息(以组内邻接和组外邻接的方式)，进而逐步将节点分组为若干个连接紧密的子图，经过若干迭代后聚合器通过每一组节点的组内和组外的邻接信息，使用 BTER 图合成方法合成社交网络图。LDPGen 机制中迭代分组的方法适当地保留了网络图中的结构信息，每轮迭代中添加的 LDP 噪声也能够提供一定的隐私保护。由于针对节点的差分隐私概念对数据效用的影响严重，目前还没有高效的 Node-LDP 算法。

在一般的社交网络分析任务中，图数据通常以无向图的形式存在，而在软件的使用数据分析任务中出现了一种控制流图的概念。控制流图是一个有向图，节点代表软件的各个组件，边代表组件之间的控制流转移。每个用户在使用软件时，其动作都会生成一个控制流图并缓存下来，最终被发送给远程服务器用于数据分析。使用差分隐私保护软件使用数据流图的挑战在于：控制流图是一个有向图，且特定的控制流和节点之间存在很强的相关性，差分隐私关于无向图相邻的传统定义对于控制流图是没有意义的。Zhang 等[54]提出了第一个使用差分隐私技术进行控制流图节点覆盖分析的解决方案。在软件的使用数据分析中，对控制流图的节点覆盖分析是一个基本的任务，该工作围绕这一任务设计了针对控制流图的相邻定义和敏感度概念，并进一步引入了差分隐私技术来提供对图节点的隐私保障。

除了上述无向图和有向图两个方面之外，图数据的分析还面临很多复杂的情形，例如带权重的图、带节点属性或者边属性的图以及子图计数、频繁子图结构挖掘等统计任务，对这些问题的解决方案将是未来的研究方向。

4.4 安全多方计算

安全多方计算(Secure Multi-Party Computation，SMPC)是一个密码学原语，常被用于分布式隐私数据学习的场景，可以在多参与方无需可信服务器的情况下，对多方拥有的数据总体准确地计算所需的统计信息。Dwork 等[4]首次指出 SMPC 可以很好地与差分隐私结合，例如差分隐私求和就可以很容易地通过安全计算和加性噪声来实现[55]。一般而言，本地化差分隐私可与 SMPC 相结合来提供最佳的精度，但也可以用于安全计算的隐私保护中，例如 Boehler 等[56]研究了安全的差分隐私中值计算，考虑到多方计算的数据集中值可以被用于有针对性的推理攻击，该工作提出了基于指数机制的差分隐私中值安全计算协议，用差分隐私中值代替实际中值可以有效抵抗推理攻击，同时该协议还可以拓展为对任意 p 分位数的差分隐私安全计算。

4.5 推荐系统

推荐系统可以通过分析、挖掘用户行为来发现用户的个性化需求，进而从大量数据中向用户推荐可能感兴趣的信息。推荐系统的经典方法是基于协同过滤算法，该算法需要对大量的用户数据进行协同过滤，因此推荐系统的隐私保护也得到了广泛关注[57-59]。McSherry 等[60]首次将差分隐私引入推荐系统，该工作指出推荐系统的历史数据可用于推理用户的隐私信息，通过向推荐系统所需的统计信息添加基于敏感度的噪音来实现差分隐私保护，该工作证明了可以在不显著影响精度的情况下实现一个具有差分隐私保证的推荐系统。考虑到现有工作只能保护用户的条目或评级，Shin 等[61]提出了一个可同时保护用户条目和评级的本地化差分隐私推荐系统，通过设计新的矩阵分解算法，让用户本地对私有数据进行随机化处理，确保用户的条目和评级对推荐系统来说都是具有隐私性的。此外，该工作还采用了降维技术，解决了矩阵分解带来的高维计算问题。Gao 等[62]提出了一个差分隐私协同过滤的通用框架，首先采用本地差分隐私机制对用户设备上的行为日志进行扰动，服务器收集模糊的记录之后运行一个估计模型得出每个条目之间的相似度，并发送给用户端，

最终用户端通过相似度矩阵以及本地存储的原始行为数据自行判断推荐结果。由于用于推荐系统的数据通常具有纬度高、稀疏率高的特点，目前针对推荐系统的差分隐私协议仍需进一步研究。

4.6 位置隐私

由于全球定位系统(Global Positioning System，GPS)在智能设备上的大规模普及，位置信息已经成为被普遍收集的个人信息之一，并产生了大量基于位置的服务，例如地图应用、基于位置的广告、位置感知的社交网络等。出于对位置隐私的担忧，部分学者也提出了应用差分隐私来保护用户位置的研究。Andrés 等[63]最早提出了基于中心化差分隐私的地理不可区分性(Geo-Indistinguishability)概念，并通过添加随机噪声的方法实现了满足地理不可区分性的机制，允许基于位置的系统得到服务所必须的近似位置信息，而无法得到用户的确切位置。Zhao 等[64]提出了称为 LDPart 的可适用于发布高维位置记录数据的 LDP 算法，采用层次分区树来自顶向下地将整片区域划分为若干子区，最终生成近似的人口位置记录数据。用户的位置数据作为一种分类属性常常具有很高的维度，这为差分隐私算法的设计带来了挑战，如何有效降低维度、降低统计方差是目前研究的关键问题。

5 有利于差分隐私实践的研究课题

5.1 差分隐私编程框架

差分隐私的一个重要特性是组合性[12,17,65]，即多个差分隐私数据分析可以通过合适的隐私参数来进行组合。这个属性允许将隐私作为预算来进行推理，数据分析员可以决定给每项分析分配多少隐私预算。该组合性激发了一些编程框架[66-69]的设计，这些编程框架具有内置的基本数据分析，可帮助数据分析人员设计个性化的差分隐私查询方案并进行隐私性的推理。Lobo-Vesga 等[70]提出的编程框架 DPella 使用污点分析技术，除了提供了对隐私性的推理，还提供了对数据分析精度的自动推理，且可以与隐私推理相结合提供隐私与精度的权衡方案。

5.2 隐私正确性的形式化验证

隐私机制的正确性是差分隐私系统的关键，但实践中手动地生成严格的正确性证明是困难且易错的，文献或系统中都曾出现过一些重大错误[71-73]，因此出现了研究如何形式化验证差分隐私机制正确性的工作。Zhang 等[67]设计了一种简单的命令式语言，其推理引擎可以推理出大部分的证明细节，从而可以用很少的人工工作验证复杂的差分隐私算法。Bichsel 等[74]提出的 DP-Finder 系统使用采样搜索差分隐私反例的方法来发现潜在的隐私泄露可能性，反例的搜索往往需要在一个几乎无限大的稀疏空间中进行，该工作设计了有效的关联抽样方法来对隐私泄露的量进行估计，并使用启发式方法来减小搜索的范围并降低搜索难度，从而可以系统地对大量的随机化算法计算差分隐私下界。相比上述几个需要手动处理或调节输入的工作，Wang 等[75]提出了一种完全自动化的可集成的差分隐私验证工具 CheckDP，该工具使用静态程序分析代替采样搜索来自动化寻找反例，而不需要动态运行差分隐私机制，可以自动地为满足差分隐私的机制生成正确性证明，而为不满足既定隐私性的错误机制生成反例。

5.3 理论与实践的精度差异

在中心化模型下，大多数差分隐私机制都是先对原始数据集做所需的统计计算，然后对统计结果添加校准的噪音，以保证外部观察者无法从统计结果上区分任意两个相邻的数据集。但一些工作指出，实践中在有限精度的输出值上添加由不精确计算产生的噪声，所留下的痕迹可能会泄露关于原始值的重要信息[76-78]。例如 Mironov[71]指出，在 Laplace 机制对随机噪声的采样过程中，由于理论精度和实际精度的差异，很难从任意精度的 Laplace 分布中采样所有可能的噪音值，敌手可以利用这一点，通过检查发布结果的最高精度位来区分原始值与加噪值。Gazeau 等[78]指出，在理想情况下，无限精度的计算才能实现正确的隐私保护，而实践中的有限精度计算会破坏理想的隐私保护。该工作提出可以使用固定精度的计算来应对上述情况，但代价是允许增加一定的舍入误差，作者为此对有限精度计算所带来的隐私损失进行了定量分析，证明了有限精度计算仅为隐私参数增加了一个加法因子，并在常用的一维 Laplace 噪音分布和二维 Laplace 噪音分布上验证了该结果。此外，Ilvento[79]指出，并非只有添加不精确噪声的差分隐私机制(如 Laplace 机制)容易受到浮点计算精度的攻击，从数据域上依概率选择结果进行响应的指数机制也极易受到这一攻击，因此该工作提出了以 2 为底数替换以 e 为底数的指数机制，从而执行以 2 为底的精确算术运算，抵抗由精度差异导致的攻击。

5.4 差分隐私的用户调查

随着 CDP 和 LDP 技术越来越多地被应用到产业界，关于持有隐私数据的用户是否理解、相信这些技术并愿意披露更多隐私数据的问题也成为了一个研究点，理解这一问题有助于更好地向用户交流差分隐私技术的内涵，从而促进用户的数据共享决策。Xiong 等[80]通过 4 项社会实验调查了这一问题，比较了差分隐私的不同文本描述方法对用户的数据共享决策产生的影响。该项研究表明，提供了隐私和效用含义的描述可以促进人们的数据共享决策和他们对 DP 和 LDP 技术的理解。Cummings 等[81]同样研究了用户对数据隐私的期望和对差分隐私技术的理解问题，并合成了一个框架来理解用户向差分隐私系统共享隐私信息的意愿。了解用户对数据隐私的期望和需求并针对性地向用户解释差分隐私技术的内涵，将有助于用户接受该技术并促进开放数据共享，有利于差分隐私技术的普及使用。

结束语 大规模的数据收集和统计分析极大地促进了信息社会的发展。作为一种严格的隐私概念，差分隐私已被接纳为实际上的数据隐私标准并在广泛的数据收集模式中得到了应用。当前实践中最常使用的是中心化的差分隐私，具有较高精度和较低的实现成本，本地化差分隐私技术的实际部署由于受到用户规模和统计精度的限制而较少出现，洗牌模型作为最新提出的差分隐私模型，由于其引人注目的隐私与精度权衡特性，在学界中已有一些研究。本文给出了差分隐私技术的详细介绍，包括差分隐私的理论模型、差分隐私随机化算法以及应用和实践中的差分隐私技术。本文对差分隐私技术的 3 个模型进行了详细的总结和比较，对于每一种模型，

从算法角度分析了一些典型的或最新的差分隐私机制，然后对差分隐私技术在多个领域的应用现状进行了介绍，最后介绍了一些有利于差分隐私实践的新研究课题。

参 考 文 献

[1] CPC CENTRAL COMMITTEE and STATE COUNCIL. Opinions on building a more perfect market-oriented allocation system and mechanism of factors [EB/OL]. (2020-04-09)[2022-05-22]. http://www.gov.cn/zhengce/2020-04/09/content_5500622.htm.

[2] EUROPEAN UNION. General Data Protection Regulation [EB/OL]. (2018-05-25)[2022-05-22]. https://gdpr-info.eu/.

[3] THE NATIONAL PEOPLE'S CONGRESS OF CHINA. Data Security Law of the People's Republic of China [EB/OL]. (2021-06-10)[2022-05-22]. http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml.

[4] DWORK C, KENTHAPADI K, MCSHERRY F, et al. Our Data, Ourselves: Privacy Via Distributed Noise Generation [C]// International Conference on Advances in Cryptology. Berlin: Springer, 2006: 486-503.

[5] TENG W, ZHANG X F, FENG J Y, et al. A Comprehensive Survey on Local Differential Privacy Toward Data Statistics and Analysis in Crowdsensing [J]. Sensors. 2020, 20(24): 7030-7077.

[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] BITTAU A, ERLINGSSON Ú, MANIATIS P, et al. Prochlo: Strong Privacy for Analytics in the Crowd [C]// Proceedings of the 26th Symposium on Operating Systems Principles. New York: ACM, 2017: 441-459.

[8] CHEU A, SMITH A, ULLMAN J, et al. Distributed Differential Privacy via Shuffling [C]// Advances in Cryptology — EUROCRYPT 2019. Berlin: Springer, 2019: 375-403.

[9] CHAN T H H, SHI E, SONG D. Optimal Lower Bound for Differentially Private Multi-party Aggregation [C]// Algorithms-ESA 2012. ESA 2012. Berlin: Springer, 2012: 277-288.

[10] BEIMEL A, NISSIM K, OMRI E. Distributed Private Data Analysis: Simultaneously Solving How and What [C]// Advances in Cryptology — CRYPTO 2008. Berlin: Springer, 2008: 451-468.

[11] DWORK C, MCSHERRY F, NISSIM K, et al. Calibrating Noise to Sensitivity in Private Data Analysis [C]// Theory of Cryptography. Berlin: Springer, 2006: 265-284.

[12] ULLMAN J. Tight lower bounds for locally differentially private selection. [EB/OL]. (2018-03-09)[2022-05-22]. https://www.thetalkingmachines.com/sites/default/files/feeds/2018/02/10/15/1802.02638.pdf.

[13] BAFNA M, ULLMAN J. The price of selection in differential privacy [C]// Proceedings of The 30th Conference on Learning Theory. New York: PMLR, 2017: 151-168.

[14] MCSHERRY F, TALWAR K. Mechanism Design via Differential Privacy [C]// Proceedings of the 48th Annual IEEE Symposium on Foundations of Computer Science. Piscataway: IEEE, 2007: 94-103.

[15] VADHAN S. The Complexity of Differential Privacy [M]. Berlin: Springer, 2017: 347-450.

[16] BASSILY R, SMITH A. Local, Private, Efficient Protocols for Succinct Histograms [C]// Proceedings of the Forty-Seventh Annual ACM on Symposium on Theory of Computing. New York: ACM, 2015: 127-135.

[17] DWORK C, ROTH A. The algorithmic foundations of differential privacy[J]. Found. Trends Theor. Comput. Sci., 2014, 9(3/4): 211-407.

[18] WARNER S L. Randomized Response: A Survey Technique for Eliminating Evasive AnswerBias [J]. Journal of the American Statistical Association, 1965, 60(309): 63-69.

[19] KAIROUZ P, BONAWITZ K, RAMAGE D. Discrete distribution estimation under local privacy [C]// International Conference on Machine Learning. New York: PMLR, 2016: 2436-2444.

[20] WANG S W, HUANG L S, WANG P Z, et al. Private Weighted Histogram Aggregation in Crowdsourcing [C]// Wireless Algorithms, Systems, and Applications. Berlin: Springer, 2016: 250-261.

[21] WANG T H, BLOCKI J, LI N H, et al. Locally differentially private protocols for frequency estimation [C]// Proceedings of the 26th USENIX Conference on Security Symposium. Berkeley: USENIX Association, 2017: 729-745.

[22] WANG S W, HUANG L S, NIE Y W, et al. Local Differential Private Data Aggregation for Discrete Distribution Estimation [J]. IEEE Transactions on Parallel and Distributed Systems, 2019, 30(9): 2046-2059.

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

[24] YE Q Q, HU H B, MENG X F, et al. PrivKV: Key-value data collection with local differential privacy [C]// 2019 IEEE Symposium on Security and Privacy(SP). Piscataway, NJ: IEEE, 2019: 317-331.

[25] GU X L, LI M, CHENG Y Q, et al. PCKV: Locally Differentially Private Correlated Key-ValueData Collection with Optimized Utility [C]// 29th USENIX Security Symposium(USENIX Security 20). Berkeley: USENIX, 2020: 967-984.

[26] WANG N, XIAO X K, YANG Y, et al. Collecting and analyzing multidimensional data with local differential privacy[C]// 2019 IEEE 35th International Conference on Data Engineering (ICDE). IEEE, 2019: 638-649.

[27] WANG T, ZHAO J, HU Z, et al. Local Differential Privacy for data collection and analysis[J]. Neurocomputing, 2021, 426(8): 114-133.

[28] 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.

[29] LI N H, QARDAJI W, SU D. On sampling, anonymization, and differential privacy or, k-anonymization meets differential privacy[C]// Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security. 2012: 32-33.

[30] ARCOLEZI H H，COUCHOT J F，AL BOUNA B，et al. Random sampling plus fake data：Multidimensional frequency estimates with local differential privacy[C]// Proceedings of the 30th ACM International Conference on Information & Knowledge Management. 2021：47-57.

[31] WANG T H，LOPUHAÄ-ZWAKENBERG M，LI Z T，et al. Locally differentially private frequency estimation with consistency [C]// 27th Annual Network and Distributed System Security Symposium. The Internet Society，2020.

[32] JIA J Y，GONG N Z. Calibrate：Frequency estimation and heavy hitter identification with local differential privacy via incorporating prior knowledge [C]// IEEE INFOCOM 2019—IEEE Conference on Computer Communications. Piscataway，NJ：IEEE，2019：2008-2016.

[33] BELL J H，BONAWITZ K A，GASCÓN A，et al. Secure single-server aggregation with(poly) logarithmic overhead [C]// Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. New York：ACM，2020：1253-1269.

[34] BALLE B，BELL J，GASCÓN A，et al. The privacy blanket of the shuffle model [C]// Annual International Cryptology Conference. Berlin：Springer，2019：638-667.

[35] BALLE B，BELL J，GASCÓN A，et al. Private Summation in the Multi-Message Shuffle Model [C]// Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. New York：ACM，2020：657-676.

[36] ISHAI Y，KUSHILEVITZ E，OSTROVSKY R，et al. Cryptography from anonymity [C]// 2006 47th Annual IEEE Symposium on Foundations of Computer Science(FOCS'06). Piscataway，NJ：IEEE，2006：239-248.

[37] CHAUDHURI K，MONTELEONI C. Privacy-preserving logistic regression[C]// Advances in Neural Information Processing Systems 21，Proceedings of the Twenty-Second Annual Conference on Neural Information Processing Systems. New York：Curran Associates Inc. 2008：289-296.

[38] ZHANG J，ZHANG Z J，XIAO X K，et al. Functional Mechanism：Regression Analysis under Differential Privacy[J]. Proceedings of the VLDB Endowment，2012，5(11)：1364-1375.

[39] WU N，FAROKHI F，SMITH D，et al. The value of collaboration in convex machine learning with differential privacy [C]// 2020 IEEE Symposium on Security and Privacy(SP). Piscataway，NJ：IEEE，2020：304-317.

[40] DENG L，CHEN X T，ZHANG Q H，et al. Differential privacy protection algorithms based on tree model [J]. Journal of Chongqing University of Posts and Telecommunications(Natural Science Edition)，2020，32(5)：848-849.

[41] GHANE S，JOLFAEI A，KULIK L，et al. Preserving privacy in the internet of connected vehicles[J]. IEEE Transactions on Intelligent Transportation Systems，2020，22(8)：5018-5027.

[42] ZHAO P，ZHANG G L，WAN S H，et al. A survey of local differential privacy for securing internet of vehicles[J]. The Journal of Supercomputing，2020，76(11)：8391-8412.

[43] JORGENSEN Z，YU T，CORMODE G. Publishing attributed social graphs with formal privacy guarantees [C]// Proceedings of the 2016 International Conference on Management of Data. New York：ACM，2016：107-122.

[44] KASIVISWANATHAN S P，NISSIM K，RASKHODNIKOVA S，et al. Analyzing graphs with node differential privacy [C]// Theory of Cryptography Conference. Berlin：Springer，2013：457-476.

[45] DAY W Y，LI N H，LYU M. Publishing graph degree distribution with node differential privacy [C]// Proceedings of the 2016 International Conference on Management of Data. New York：ACM，2016：123-138.

[46] KARWA V，RASKHODNIKOVA S，SMITH A，et al. Private analysis of graph structure[J]. Proceedings of the VLDB Endowment，2011，4(11)：1146-1157.

[47] RASKHODNIKOVA S，SMITH A. Lipschitz extensions for node-private graph statistics and the generalized exponential mechanism [C]// 2016 IEEE 57th Annual Symposium on Foundations of Computer Science(FOCS). Piscataway，NJ：IEEE，2016：495-504.

[48] SALA A，ZHAO XIAOHAN，WILSON C，et al. Sharing graphs using differentially private graph models [C]// Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference. New York：ACM，2011：81-98.

[49] XIA S Y，CHANG B Z，KNOPF K，et al. DPGraph：A Benchmark Platform for Differentially Private Graph Analysis [C]// Proceedings of the 2021 International Conference on Management of Data. New York：ACM，2021：2808-2812.

[50] BLOCKI J，BLUM A，DATTA A，et al. The johnson-lindenstrauss transform itself preserves differential privacy [C]// 2012 IEEE 53rd Annual Symposium on Foundations of Computer Science. Piscataway，NJ：IEEE，2012：410-419.

[51] BLONDEL V D，GUILLAUME J L，LAMBIOTTE R，et al. Fast unfolding of communities in large networks[J]. Journal of Statistical Mechanics：Theory and Experiment，2008，2008(10)：P10008.

[52] QIN Z，YU T，YANG Y，et al. Generating synthetic decentralized social graphs with local differential privacy [C]// Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. New York：ACM，2017：425-438.

[53] SESHADHRI C，KOLDA T G，PINAR A. Community structure and scale-free collections of Erdős-Rényi graphs[J]. Physical Review E，2012，85(5)：056109.

[54] ZHANG H L，LATIF S，BASSILY R，et al. Differentially-Private Control-Flow Node Coverage for Software Usage Analysis. [C]// 29th USENIX Security Symposium(USENIX Security 20)，Berkeley，CA：USENIX，2020.

[55] GORYCZKA S，XIONG L. A comprehensive comparison of multiparty secure additions with differentialprivacy [J]. IEEE Transactions on Dependable and Secure Computing，2015，14(5)：463-477.

[56] BOEHLER J，KERSCHBAUM F. Secure sublinear time differentially private median computation [C]// Network and Distributed System Security Symposium. The Internet Society，2020.

[57] PATEL A A，DHARWA J N. An integrated hybrid recommendation model using graph database [C]// 2016 International Conference on ICT in Business Industry & Government(ICTBIG). Piscataway，NJ：IEEE，2016：1-5.

[58] XIONG P, ZHU T Q, WANG X F. A survey on differential privacy protection and its application[J]. Chinese Journal of Computers, 2014, 37(1): 101-122.

[59] CALANDRINO J A, KILZER A, NARAYANAN A, et al. You might also like: Privacy risks of collaborative filtering [C]// 2011 IEEE Symposium on Security and Privacy. Piscataway, NJ: IEEE, 2011: 231-246.

[60] MCSHERRY F, MIRONOV I. Differentially private recommender systems: Building privacy into the netflix prize contenders [C]// Proceedings of the 15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. New York: ACM, 2009: 627-636.

[61] SHIN H, KIM S, SHIN J, et al. Privacy enhanced matrix factorization for recommendation with local differential privacy[J]. IEEE Transactions on Knowledge and Data Engineering, 2018, 30(9): 1770-1782.

[62] GAO C, HUANG C, LIN D S, et al. DPLCF: differentially private local collaborative filtering [C]// Proceedings of the 43rd International ACM SIGIR Conference on Research and Development in Information Retrieval. New York: ACM, 2020: 961-970.

[63] 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 & Communications Security. New York: ACM, 2013: 901-914.

[64] ZHAO X G, LI Y H, YUAN Y, et al. LDPart: effective location-record data publication via local differential privacy[J]. IEEE Access, 2019, 7: 31435-31445.

[65] MCSHERRY F D. Privacy integrated queries: an extensible platform for privacy-preserving data analysis [C]// Proceedings of the 2009 ACM SIGMOD International Conference on Management of Data. New York: ACM, 2009: 19-30.

[66] BARTHE G, FARINA G P, GABOARDI M, et al. Differentially private bayesian programming [C]// Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2016: 68-79.

[67] ZHANG D F, KIFER D. LightDP: Towards automating differential privacy proofs [C]// Proceedings of the 44th ACM SIGPLAN Symposium on Principles of Programming Languages. New York: ACM, 2017: 888-901.

[68] WINOGRAD-CORT D, HAEBERLEN A, ROTH A, et al. A framework for adaptive differential privacy[J]. Proceedings of the ACM on Programming Languages, 2017, 1(ICFP): 1-29.

[69] ZHANG D, MCKENNA R, KOTSOGIANNIS I, et al. EKTELO: A framework for defining differentially-private computations [C]// Proceedings of the 2018 International Conference on Management of Data. 2018: 115-130.

[70] LOBO-VESGA E, RUSSO A, GABOARDI M. A programming framework for differential privacy with accuracy concentration bounds [C]// 2020 IEEE Symposium on Security and Privacy (SP). Piscataway, NJ: IEEE, 2020: 411-428.

[71] CHEN Y, MACHANAVAJJHALA A. On the privacy properties of variants on the sparse vector technique[J]. arXiv: 1508.07306, 2015.

[72] LYU M, SU D, LI N. Understanding the Sparse Vector Technique for Differential Privacy[J]. Proceedings of the VLDB Endowment, 2017, 10(6): 637-648.

[73] MCSHERRY F. Uber's differential privacy. probably isn't [EB/OL]. (2018-02-25) [2022-05-22]. https://github.com/frankmcsherry/blog/blob/master/posts/2018-02-25.md.

[74] BICHSEL B, GEHR T, DRACHSLER-COHEN D, et al. DP-Finder: Finding differential privacy violations by sampling and optimization [C]// Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2018: 508-524.

[75] WANG Y X, DING Z Y, KIFER D, et al. CheckDP: An automated and integrated approach for proving differential privacy or finding precise counterexamples [C]// Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2020: 919-938.

[76] BALCER V, VADHAN S. Differential privacy on finite computers[J]. arXiv: 1709.05396, 2017.

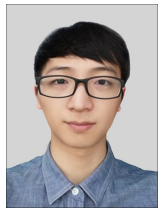
[77] MIRONOV I. On significance of the least significant bits for differential privacy [C]// Proceedings of the 2012 ACM Conference on Computer and Communications Security. New York: ACM, 2012: 650-661.

[78] GAZEAU I, MILLER D, PALAMIDESSI C. Preserving differential privacy under finite-precision semantics[J]. Theoretical Computer Science, 2016, 655(Pt. B): 92-108.

[79] ILVENTO C. Implementing the exponential mechanism with base-2 differential privacy [C]// Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2020: 717-742.

[80] XIONG A P, WANG T H, LI N H, et al. Towards effective differential privacy commu-nication for users' data sharing decision and comprehension [C]// 2020 IEEE Symposium on Security and Privacy(SP). Piscataway, NJ: IEEE, 2020: 392-410.

[81] CUMMINGS R, KAPTCHUK G, REDMILES E M. I need a better description: An Investigation Into User Expectations for Differential Privacy [C]// Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2021: 3037-3052.



ZHAO Yuqi, born in 1998, postgraduate. His main research interests include cryptography and differential privacy.

YANG Min, born in 1975, Ph. D, associate professor, master supervisor, is a member of China Computer Federation. Her main research interests include information security and applied cryptography.

(责任编辑:喻藜)