ICS 33.050
CCS M 30

团　体　标　准

T/TAF 137—2022

基于差分隐私的用户个人信息保护技术要求

Technical requirements for Differential Privacy-based user personal information protection

2022-11-25 发布　　2022-11-25 实施

电信终端产业协会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由电信终端产业协会提出并归口。

本文件起草单位：阿里巴巴(中国)有限公司、中国信息通信研究院、蚂蚁科技集团股份有限公司、OPPO广东移动通信有限公司、小米通讯技术有限公司、北京快手科技有限公司、北京三快在线科技有限公司。

本文件主要起草人：黄天宁、彭立、傅山、王嘉义、刘陶、李世奇、刘巍然、冯翰文、昌文婷、白晓媛、彭晋、王俊、孟丹、付艳艳、顾泽宇、落红卫、王昕、黄坤。

引　言

随着移动通信技术和人工智能技术的快速发展，移动互联网应用和 AI 产品正逐渐渗透到人们的生活当中，互联网数据引发的隐私泄漏、安全威胁等一系列个人信息安全问题成为各方关注的重点。同时，《个人信息保护法》已于 2021 年 11 月正式实施，对数据处理者的对个人数据的保护能力提出了新的要求。近年来，为了让数据能够在最大化发挥价值的同时，防止个人信息的泄漏，信息安全从业者从多种角度进行了多种探索。从目前发展现状和趋势来看，以差分隐私为代表的隐私计算技术成为了实现这一突破的关键。世界经济论坛 2019 年 9 月发布的白皮书认为，以差分隐私技术为代表的隐私计算技术将成为释放行业新价值的突破口。

如何解决数据统计查询、数据采集等场景中的用户隐私泄露问题，同时保证数据的可用性，成为了广大终端厂商、数据服务提供商以及互联网企业的重要工作。为解决这些问题，差分隐私技术应运而生。该技术提供了一种严格、可证明的隐私保护手段，且其保护强度不依赖于攻击者所掌握的背景知识。由于这些特点，差分隐私一经提出便得到了学术界和工业界的广泛认可和应用。

差分隐私是一种可以在保护个人数据本身不对外泄漏的前提下实现数据处理的个人信息保护技术。差分隐私通过在数据中加入噪声，使得数据分析者很难判定某个个体数据是否存在于数据集中，从而保护个人数据隐私。近几年，伴随着技术的不断成熟，国内外差分隐私产业化应用的步伐明显加快，诸多数据安全企业、金融风控企业、电信企业等也纷纷拥抱差分隐私技术。作为缓解个人隐私泄露问题、实现数据价值流通的关键技术，差分隐私技术未来的发展前景非常广阔。为了进一步地推动差分隐私技术和产业发展，开展基于差分隐私的用户个人信息保护标准制定十分必要且急迫。

目前行业中尚未有从用户个人信息保护出发针对差分隐私技术的要求与测试评估方法，缺乏统一的标准。基于上述考虑，提出本标准，旨在对使用了差分隐私技术进行用户个人信息保护提出技术要求，进一步促进产业的健康稳定发展。

基于差分隐私的用户个人信息保护技术要求

1 范围

本文件规范了基于差分隐私的用户个人信息保护技术要求，包括差分隐私系统技术架构、差分隐私能力要求、差分隐私保护分级、差分隐私保护效果评定。

本文件适用于应用在移动智能终端的差分隐私技术，也适用于评估机构基于本文件开展差分隐私产品保护个人信息的评估工作。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069-2022 信息安全技术 术语

GB/T 35273-2020 信息安全技术 个人信息安全规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

差分隐私 differential privacy

一种个人信息的数据保护技术，通过随机响应或对原始数据加入噪声的方式，使得对数据集的计算处理结果对于具体某个记录的变化是不敏感的，单个记录在或不在数据集中，对计算结果的影响微乎其微，并能保护个人信息不被泄露。

注：差分隐私保护重在提供可度量的数据隐私保护方法。

3.2

隐私预算 privacy budget

衡量差分隐私保护效果的参数，在一定程度上给出了隐私保护效果的度量。

注：隐私预算越小，对数据的隐私保护程度越强，但是数据的可用性越差；隐私预算越大，数据的可用性越好，但是隐私保护能力越差。

3.3

本地差分隐私 local differential privacy

不依赖于可信第三方，直接在终端进行数据的隐私化处理，处理后的数据满足差分隐私保护要求。

3.4

中心化差分隐私 centralized differential privacy

将原始终端数据集中到一个可信第三方,由第三方对数据进行处理，处理后的数据满足差分隐私保护要求。

3.5

编码器 encoder

智能终端上对原始个人信息进行编码、加噪等处理的组件。

3.6

数据管理器 data curator

对从智能终端接收到的数据进行解密、存储、聚合等操作，并根据查询请求进行数据处理和添加噪声，对查询进行隐私预算管理，最终发布满足差分隐私要求结果的组件。

3.7

数据信道 data channel

实现数据在终端（编码器）、数据管理器和查询处理器之间流转的组件。

3.8

查询处理器 query processor

发起数据查询请求并接受结果的实体。

3.9

数据采集者 data collector

在过程中负责采集数据的实体，可以为数据管理器或查询处理器。

4 缩略语

下列缩略语适用于本文件。

LDP：本地差分隐私（Local Differential Privacy）

TLCP：传输层密码协议（Transport Layer Cryptographic Protocol）

TLS：传输层安全协议（Transport Layer Security）

5 概述

5.1 差分隐私用于个人信息保护

数据处理是数字经济社会生产中的重要步骤，数据集通常包含大量的个人隐私数据，企业在业务中对数据处理不当可能会造成个人隐私的泄露。《个人信息保护法》等对企业数据处理行为中的个人信息保护提出了要求，企业须采取措施确保数据处理过程中个人信息不被泄露。

差分隐私是针对数据隐私泄露问题提出的一种隐私保护方法。在此定义下，对数据集的计算处理结果对于某条具体记录的变化是不敏感的，单条记录存在或不存在数据集中，对计算结果的影响微乎其微。所以，一条记录因其加入到数据集中所产生的隐私泄露风险被控制在极小的、可接受的范围内，攻击者无法通过观察计算结果而获取准确的个体信息，从而在数据发布、查询等过程中保护个体信息隐私。通常，差分隐私通过在真实数据中加入随机化噪声扰动的方式来实现保护。

5.2 差分隐私的概述

差分隐私技术可以分为中心化差分隐私和本地化差分隐私。中心化差分隐私定义为假设有随机算法M，S为M所有可能输出结果构成的集合，$Pr[]$表示概率，对于任意两个差别只有1条记录的相邻数据集D, D'，如果满足：

$$Pr[M(D) \in S] \leq e^{\epsilon} Pr[M(D') \in S] + \delta$$

则称算法M提供(ε, δ)-中心化差分隐私保护，其中ε为差分隐私预算，用来保证数据集中增加或者减少一条记录，随机算法M的输出结果一致的概率；δ指算法M有δ的概率不满足ε-DP.

本地化差分隐私与中心化差分隐私不同，用户之间并不能知道相互之间的记录，也没有一个中心化的数据管理器，因此在本地化差分隐私中，我们将两个相邻数据集替换成两条来自不同用户的不同记录。本地差分隐私定义为，假设有随机算法M，t为M的任意一个输出结果，$Pr[]$表示概率，对于任意两条记录m, m'，如果满足：

$$Pr[M(m) = t] \leq e^{\epsilon} Pr[M(m') = t] + \delta$$

则称算法M提供(ε, δ)-本地化差分隐私保护，其中ε为差分隐私预算，用来保证任意两个用户的记录，随机算法M的输出结果一致的概率；δ指算法M有δ的概率不满足ε-DP。

在相同数据集和使用相同的差分隐私算法的前提下，差分隐私预算ε越小，隐私保护效果越好。

特别地，δ 表示大小为常数的概率扰动，是允许随机算法在一定程度上不满足差分隐私严格定义的一个松弛项。具体地，当δ =0时，我们称(ε, δ)-差分隐私为ε-差分隐私。当δ >0时，(ε, δ)-差分隐私相对ε-差分隐私而言很大可能会存在概率大于0的额外信息泄露。故我们称ε-差分隐私是严格的差分隐私定义，而(ε, δ)-差分隐私则是松弛的差分隐私定义。

5.3 差分隐私系统的技术架构

5.3.1 差分隐私数据处理框架

根据隐私计算框架中的数据管理器是否可信，可将移动智能终端个人信息保护的差分隐私数据处理模式可分为两种框架类型：

a) 本地化差分隐私：包含终端与数据管理器两种角色，数据管理器不可信。终端个人信息在添加噪声后向数据管理器发送，且数据管理器无法查看原始个人信息。

b) 中心化差分隐私

包含终端与数据管理器两种角色，数据管理器可信。终端个人信息直接发送并存储于数据管理器中，再由数据管理器对查询结果添加噪声。可信的数据管理器不会直接查看、共享个人信息，也不会与攻击者共谋。图1中的信任边界表示数据管理器是否被用户终端信任。

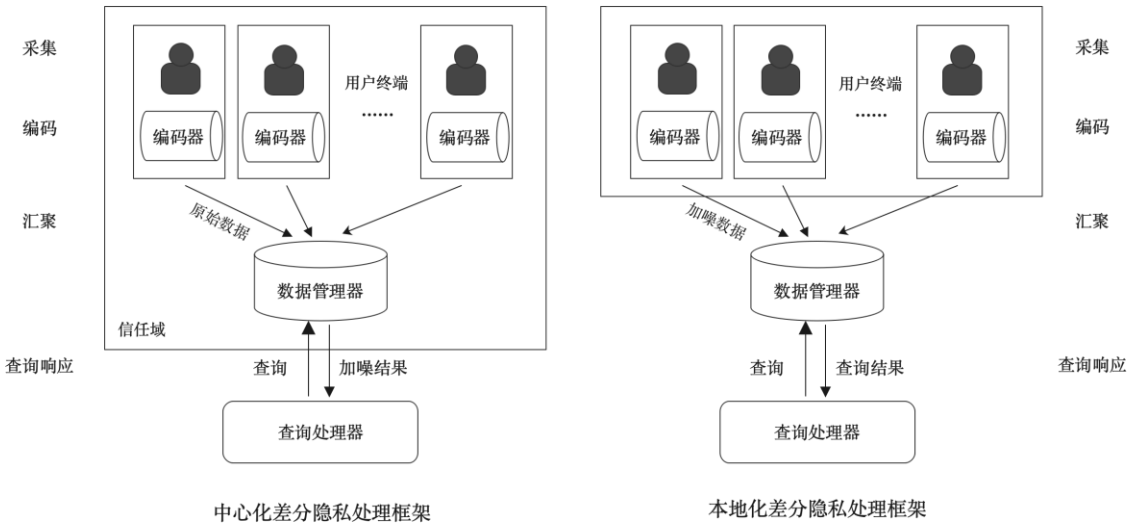

图 1　两类差分隐私数据处理模式

5.3.2 差分隐私系统组成与角色关系

基于差分隐私的个人信息保护系统常见组成结构如图1所示。系统的工作流程主要分为：

a) 采集：终端对个人信息进行采集操作；

b) 编码：在本地化模式中，终端通过编码器对个人信息进行编码、加噪等处理；在中心化模式中，终端通过编码器对个人信息进行编码等处理。

c) 汇聚：终端将原始个人信息（中心化模式）或经过编码器加噪的数据（本地化模式）发送给数据管理器；

d) 查询响应：数据管理器针对查询请求，对从终端接受到的数据进行聚合、解码、加噪等处理后，输出满足差分隐私要求的查询结果。在多次查询场景中，数据管理器需进行隐私预算的控制。

5.3.3 差分隐私系统的分类

用于个人信息保护的差分隐私系统可以按以下维度进行分类：

a) 差分隐私的算法分类

根据差分隐私算法支持的精度、预算分配合理性等，将算法分类为基础差分隐私算法和优化差分隐私算法，见表 1。

表 1　差分隐私算法

分类	中心化差分隐私	本地化差分隐私
基础差分隐私算法	拉普拉斯机制、指数机制	Direct Encoding
优化差分隐私算法	阶梯机制、几何机制、高斯机制、高精度拉普拉斯机制、高精度高斯机制、离散拉普拉斯机制、离散高斯机制、Base2-指数机制、其他证明完备的中心化差分隐私机制	Histogram Encoding, Unary Encoding, Binary Local Hashing, Optimal Local Hashing及其他证明完备的本地化差分隐私机制

b) 查询类型的分类

个人信息保护场景常见的差分隐私查询类型包括：

1） 频数统计：分为多值频数统计以及单值频数统计，包括计数、众数、直方图、列联表等查询；
2） 均值统计：包括平均值等查询；
3） 极值查询：包括极大值、极小值、Top-K等查询；
4） 数据挖掘与机器学习：包括分类树、支持向量机、对率回归、K-均值等；
5） 基础统计估计：计数，求和，平均数，分位数，最小值，最大值，方差等；
6） 直方图发布：普通直方图发布、约束条件直方图发布、本地差分隐私直方图发布；
7） 隐私保护统计问询：隐私乘法权重、稀疏向量技术、合成数据集技术；
8） 支持灵活统计问询（如SQL查询等）。

6 差分隐私能力要求

6.1 总体要求

差分隐私能力总体要求见图2，包括基础能力要求、系统安全要求、算法安全要求、优化算法要求、场景化安全要求五部分，具体要求如下。

a) 基础能力要求包括协议模式、数据输入、查询模型、算法支持、数据可用性等差分隐私基本能力要求；
b) 系统数据安全要求包括数据采集安全、数据传输安全、输出存储安全等系统层面数据保护要求；
c） 算法安全要求包括参数安全、查询安全、计算结果安全等算法层面安全要求；
d） 优化算法要求对差分隐私能力提出了进一步的能力要求和安全性要求；
e） 场景化安全要求提出了在不同数据敏感场景下的安全保护差异化要求。

图 2 差分隐私对个人信息保护的总体要求

6.2 差分隐私基础能力要求

6.2.1 差分隐私模式

应支持5.3.1 中的至少一种差分隐私数据处理模式。

6.2.2 数据输入

数据输入要求包括：

a） 应支持整数、小数、字符串等至少一种基本数据类型；

b） 对于数值型数据、枚举型数据应添加适配于该类型的噪声。

6.2.3 查询类型

对于支持数据查询的差分隐私系统，应支持计数、均值、直方图、频率估计等至少一种常见查询类型。

6.2.4 算法支持

应支持 5.3.3 a）表 1 中基础差分隐私算法中的至少一种算法。

6.2.5 数据可用性要求

数据可用性要求包括数据一致性和数据准确性：

a） 数据一致性：差分隐私处理后的数据，不应出现语义矛盾的情况，如应满足：计数问询的统计结果为正整数（包括 0）、频率估计中各个频率的和为 100%、且未出现不可能出现的枚举值、差分隐私机器学习输出模型应可直接执行预测算法；

b） 数据准确性：宜支持对数据准确性的评估，能根据理论给出差分隐私输出数据的方差等统计型指标，能使用统计性检测等手段验证满足理论准确性结果。

6.3 差分隐私系统数据安全要求

6.3.1 数据采集安全

数据采集安全要求包括：

a） 采集的数据及采集过程应严格按照 GB/T 35273-2020 执行；

b） 数据采集者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的方式和范围；

c） 数据采集者应制定标准的采集模板、数据采集方法、策略和规范，采集策略参数配置应包括采集周期、有效性、检测时间、入口地址和采集深度等；

d） 对于初次采集的数据，宜用人工与技术相结合的方式根据其来源、类型或重要程度进行分类；

e） 数据采集者宜明确数据来源、采集方式、采集范围等内容，并记录存档；

f） 在数据采集前后应采用校验技术对数据完整性进行校验。

g） 针对端侧采集经过本地差分隐私算法处理后的个人信息的场景，应在用户协议等文本中对算法的使用做出说明，满足透明性要求。

6.3.2 数据传输安全

数据传输安全要求包括：

a） 数据传输时应建立安全的通信信道，使用 TLCP 或 TLS v1.2 及以上版本进行通信；

b) 应采用密码技术保证通信中数据的机密性和完整性保护，采用的密码技术应符合国家行业主管部门和相应国家标准和行业标准的要求。

6.3.3 数据存储安全

数据存储安全要求包括：

a) 应采用密码技术保证敏感个人信息的机密性保护，采用的密码技术应符合国家行业主管部门和相应国家标准和行业标准的要求；

b) 应设置合理的存储期限，应为实现个人信息主体授权使用的目的所必需的最短时间，对超期数据进行删除或匿名化处理。

6.4 差分隐私算法安全要求

6.4.1 概述

差分隐私参数 ε 是差分隐私算法安全的重要参数，但在实际过程中还包括系统设计、应用场景等多种因素，如扰动函数、相邻数据集定义、保护粒度、实际使用过程中的查询损耗、差分隐私计算结果的分布情况等。差分隐私参数 ε 的配置应考虑多个因素，针对实际业务场景设置合理的大小。差分隐私算法安全验证建议按附录 C 提供验证信息清单，或自主提供完备的验证方案和过程。本节给出其中重要的参数和查询、结果安全的基本要求。

注：差分隐私参数的配置可在参考文献[3][6]中查看。

6.4.2 参数安全

在采用 ε-DP 定义的差分隐私应用中，差分隐私参数 ε 宜不大于以下基础推荐值，以达到基本的保护效果：

表 2　差分隐私参数基础推荐值

基础推荐值	中心化差分隐私	本地化差分隐私
ε	2	8

6.4.3 查询安全

在支持多次查询（或 LDP 中的数据上传）的场景中，应采取措施保证累计查询的预算消耗不超过所声明的差分隐私预算总量，如在一定时间内合理限制查询（上传）次数。

6.4.4 计算结果安全

计算结果安全要求包括：

a) 应确保算法计算过程中，除了计算结果和其可推导的信息外，不会泄露其他敏感数据；

b) 采用差分隐私保护后的计算结果的分布测量值，应与所采用的差分隐私算法、参数两者共同计算的理论值保持一致。验证过程建议按附录 B 执行，或自主提供完备的验证方案和过程。

6.4.5 差分隐私优化算法要求

6.4.5.1 优化算法能力要求

宜支持 5.3.3 a)表 1 中优化差分隐私算法中的至少一种算法。

6.4.5.2 优化算法安全性要求

对于声明支持的优化差分隐私机制及参数，应满足 6.4.1，6.4.2，6.4.3，6.4.4 差分隐私算法安全性要求。

6.5 差分隐私场景化安全要求

6.5.1 算法能力要求

对于不同的业务场景，应具备能力来配置、优化、组合使用已有成熟算法或设计新的算法，来解决场景化业务问题，并提供报告说明可行性和安全性，报告内容宜根据不同场景给出单独的算法配置说明，报告内容参考附录 C。

6.5.2 参数安全

对于不同的业务场景，应根据不同的安全性要求对参数进行对应的配置。如对于数据保护要求更高的数据场景，应设置更严格的差分隐私参数。对于采用(,δ)-DP 定义的差分隐私应用，差分隐私参数宜不大于以下场景化推荐值来达到差异化的保护强度：

表 3　差分隐私参数场景化推荐值

业务场景	ε 场景化推荐值		δ场景化推荐值
	中心化差分隐私	本地化差分隐私	
金融	0.25	2	10^{-6}
政务	0.5	4	10^{-5}
医疗	0.5	4	10^{-5}
其他	1	6	10^{-4}

7　差分隐私保护分级

7.1　概述

根据差分隐私系统满足第五章能力要求的程度，对于差分隐私的保护效果可将差分隐私保护系统分为由低到高共3级。

表 4　差分隐私保护分级对应表

	6.2 差分隐私基础能力要求	6.3 差分隐私系统数据安全要求	6.4 差分隐私算法安全要求	6.5 差分隐私场景化安全要求
1级	√	√	—	—
2级	√	√	√	—
3级	√	√	√	√

7.2　1 级

满足差分隐私基础能力要求和系统数据安全要求，能够在数据采集、传输、存储等过程满足安全要求的前提下，对查询数据加入差分隐私噪声进行扰动。

7.3 2级

在满足1级要求的基础上，满足差分隐私算法安全要求，对差分隐私算法参数进行了正确配置，通过了实验验证。验证过程建议按附录B执行，或自主提供完备的验证方案和过程。

7.4 3级

在满足2级要求的基础上，满足差分隐私场景化安全要求，对于不同数据敏感程度的场景，提供差异化的差分隐私保护等级。

8 差分隐私保护效果评定

差分隐私保护效果评定流程如图3所示：

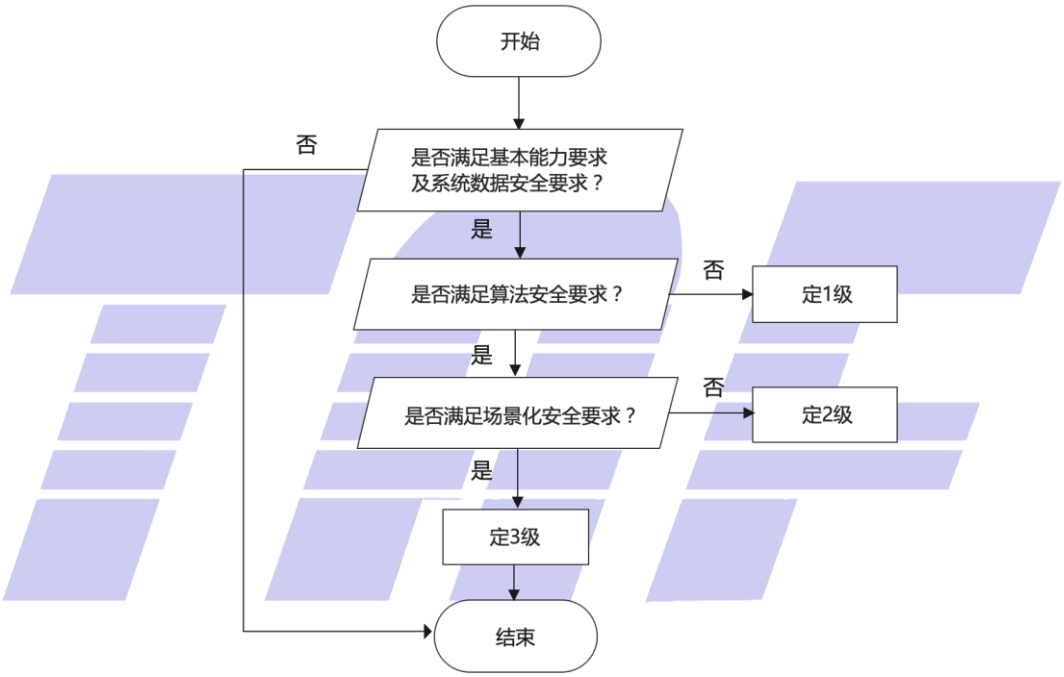

图 3 差分隐私保护效果评定流程

附 录 A
（资料性）
应用场景

在数据发布领域，支持差分隐私的数据发布算法的应用包括但不限于社交网络、地理位置服务（LBS）、推荐系统。

在数据挖掘领域，差分隐私一般通过结合具体的挖掘算法，根据挖掘结果的性能指标进行调整，以实现数据安全性和模型可用性之间的平衡。目前，支持差分隐私的数据挖掘算法的应用包括：线性回归、逻辑回归、决策树、深度学习、聚类，隐私保护模型预测，决策树构造、频繁模式挖掘、和联邦学习。

在本地差分隐私保护中，隐私保护数据从终端获得后可以直接用于后续计算。具体支持以下场景：

a） 发布终端的行为数据：将用户使用偏好等数据加入噪声并发布，用于服务端统计数据分布；

b） 发布终端数据统计信息：将终端原始数据进行求最大值，均值等统计后发布统计结果；

c） 发布基于终端数据的预训练模型：终端上用原始数据进行训练得到模型，并将预训练模型进行分享和发布。由于存在通过预训练模型推断终端原始数据的风险，因此需要在预训练过程中或对结果模型进行随机扰动以达到对原始数据的隐私保护。

在中心化差分隐私保护中，终端数据可能具备一定的差分隐私保护(或者没有任何隐私保护)，终端数据通过在可信第三方聚合后进行计算并发布计算结果，具体支持以下场景：

a） 分享基于众多终端数据的统计信息：将终端原始数据安全聚合后进行求最大值，均值等统计后发布统计结果；

b） 联邦学习：目标是在保证终端用户数据隐私安全及合法合规的基础上，实现利用大量用户数据共同建模，提升人工智能模型的效果。

附 录 B
（资料性）
测试方法

验证差分隐私算法的执行结果是否符合算法设置及参数配置，可参考以下测试过程。对于满足5.3.3 a)表1的基础差分隐私算法，宜按以下过程进行测试；对于优化差分隐私算法，需给出合理的测试评估标准和方法。测试内容中的符号含义见表B.1。

表 B.1 符号含义

符号	含义
ε	差分隐私参数
v	输入数据
S	输入数据集
n	测试轮数
v'	输出加噪结果
d	输入离散值的枚举数量

a) 拉普拉斯机制

输入数据：$v = 1.0$；

测试轮数：$n = 100000$；

结果验证：对输出的加噪结果进行统计，须满足

1） 加噪结果v_i'与输入数据v的绝对差的均值，与差分隐私参数的倒数$\frac{1}{\varepsilon}$接近一致，即

$$\frac{\sum_{i=1}^{n}|v_i'-v|}{n}-\frac{1}{\varepsilon}<0.1$$ 。

2）加噪结果v_i'的均值与输入数据v接近一致，即

$$\frac{\sum_{i=1}^{n}v_i'}{n}-v<0.1$$

b) 指数机制

初始化：设定输入数据有$d = 10$种可能，$v \in \{1,2,3,\ldots,10\}$，原始数据集为$S$。设定查询函数$f$的功能为查询众数，$f$的输出为$o = f(S) \in \{1,2,3,\ldots,10\}$。为每种输出可能分别设定打分函数，$q(o,S) = m_o$，其中$m_o$为输入数据集中$v = o$的元素数量。

输入数据集：设定输入数据集S=

{1,
2, 2,
3, 3, 3,
4, 4, 4, 4,
5, 5, 5, 5, 5,
6, 6, 6, 6, 6, 6,
7, 7, 7, 7, 7, 7, 7,
8, 8, 8, 8, 8, 8, 8, 8,

9, 9, 9, 9, 9, 9, 9, 9, 9,
10, 10, 10, 10, 10, 10, 10, 10, 10, 10}

测试轮数：$n = 100000$

结果验证：对输出的加噪结果v_j进行统计，应满足

$$|1 - \left(\frac{n_{v_j}}{n} / \frac{e^{\varepsilon m_{v_j}}}{\sum_k^d e^{\varepsilon m_{v_k}}}\right)| < 0.1$$

对于所有j都成立。

c） Direct Encoding 机制

初始化：设定输入数据有$d = 10$种可能，$v \in$ {data0,data1,...,data9}。

输入数据：$v =$ "data0"

测试轮数：$n = 100000$

结果验证：对输出的加噪结果进行统计，须满足

1） 输出结果为$v_0' =$ "data0"的比例与理论值应接近一致，即

$$|1 - \frac{n_{v_0'}}{n} / \frac{e^{\varepsilon}}{e^{\varepsilon} + d - 1}| < 0.1$$

2） 输出任意其他结果v_j'的比例与理论值应接近一致，即

$$|1 - \frac{n_{v_j'}}{n} / \frac{1}{e^{\varepsilon} + d - 1}| < 0.1$$

对于所有$j \neq 0$都成立。

附 录 C
（资料性）
差分隐私算法安全验证信息清单

验证差分隐私算法安全的方案，可提供以下清单。

a) 选择使用的差分隐私模型 M,见表 C.1。
b) 确定需要保护的数据类型 T,见表 C.2。
c) 选择需要进行扰动的查询函数 F,见表 C.3。
d) 选择相邻数据集定义 A,见表 C.4（可选）。
e) 选择敏感度定义 S,见表 C.5，及计算公式或上界（可选）。
f) 选择差分隐私定义 D,见表 C.6。
g) 确定噪声添加机制 N,见表 C.7。
h) 选择保护粒度 G,见表 C.8（可选）。
i) 确定隐私预算 B：总体的隐私预算、每个步骤消耗的隐私预算、使用的组合定理（串行、并行）、哪些步骤使用了采样使得隐私预算降低、哪些步骤因为后处理机制所以不消耗隐私预算。
j) 确定隐私预算消耗率 R（可选）：在多次使用同一数据集的情况下，其隐私保护能力会降低。常用的方式有：限制用户在多长的单位时间内最多贡献多少次数据、每个接口最多询问请求数据库多少次。
k) 确定数据情况（可选）：样本数量级、样本属性维度、样本分布、数据之间的相关性，IID 或 non-IID。
l) 确定评估方法 E：参考附录 B 或自主提供实验评估方法。

表 C.1 差分隐私模型（M）示例

差分隐私模型（M）	中心化	本地化

表 C.2 保护的数据类型（T）示例

数据类型（T）	连续型	离散型

表 C.3 扰动的查询函数（F）示例

扰动函数（F）	平均数	中位数	求和	协方差	直方图	SGD

表 C.4 相邻数据集定义（A）示例

相邻数据集定义（A）	有界	无界

注：有界（Bounded）：数据量不变，等同于替换一条数据；无界（Unbounded）：数据量相差 1，等同于删除或添加一条数据。

表 C.5　敏感度定义（S）示例

敏感度定义（S）	全局敏感度	局部敏感度

表 C.6　差分隐私定义（D）示例

差分隐私定义（D）	ε-DP	$(,\delta)$-DP	Concentrated DP	zero Concentrated DP	Rényi DP

表 C.7　噪声机制（N）示例

噪声机制（N）	拉普拉斯机制	指数机制	高斯机制	随机响应

表 C.8　保护粒度（G）示例

保护粒度（G）	样本级	用户级

注：　数据集中可能包含了同一用户在不同时间、不同空间的多条数据，或数据间具有较强的相关性，这也称为群体隐私（Group Privacy）。

参 考 文 献

[1] 中华人民共和国全国人民代表大会常务委员会，中华人民共和国个人信息保护法，2021年11月.

[2] Mironov I., Pandey O., Reingold O., Vadhan S. (2009) Computational Differential Privacy. In: Halevi S. (eds) Advances in Cryptology - CRYPTO 2009. CRYPTO 2009. Lecture Notes in Computer Science, vol 5677. Springer, Berlin, Heidelberg.

[3] https://www.apple.com/privacy/docs/Differential_Privacy_Overview.pdf

[4] Wang, Tianhao, et al. "Locally differentially private protocols for frequency estimation." 26th {USENIX} Security Symposium ({USENIX} Security 17). 2017.

[5] Li, Ninghui, et al. "Differential privacy: From theory to practice." Synthesis Lectures on Information Security, Privacy, & Trust 8.4 (2016): 1-138.

[6] Lee, Jaewoo, and Chris Clifton. "How much is enough? choosing ε for differential privacy." International Conference on Information Security. Springer, Berlin, Heidelberg, 2011.

电信终端产业协会团体标准

基于差分隐私的用户个人信息保护技术要求

T/TAF 137—2022

*

电信终端产业协会印发
地址：北京市西城区新街口外大街 28 号
电话：010-82052809
电子版发行网址：www.taf.org.cn