doi:10.11959/j.issn.1000-436x.2015321

差分隐私保护参数 ε 的选取研究

何贤芒[1,2]，王晓阳[2]，陈华辉[1]，董一鸿[1]
（1.宁波大学 信息科学与工程学院，浙江 宁波 315211；2. 复旦大学 计算机科学技术学院 上海数据科学重点实验室，上海 201203）

摘 要：2006 年，差分隐私保护作为一种新的隐私保护范式出现，因其不需要攻击者先验知识的假设，而被认为是一种非常可靠的保护机制。然而，作为隐私保护技术的主要参数 ε 的意义对于一般用户而言不十分明确。鉴于此，提出一个新的攻击模型，可以用来选取参数 ε 的值。详细分析了该攻击模型的特点，通过理论证明和模型的实证分析，最后给出了一个参数 ε 的选取计算式。
关键词：差分隐私；攻击模型；数据隐私
中图分类号：TP311.131 **文献标识码**：A

Study on choosing the parameter ε in differential privacy

HE Xian-mang[1,2], WANG X Sean[2], CHEN Hua-hui[1], DONG Yi-hong[1]
(1. School of Information Science and Technology, Ningbo University, Ningbo 315211, China;
2. Shanghai Key Laboratory of Data Science, School of Computer Science, Fudan University, Shanghai 201203, China)

Abstract: In 2006, differential privacy has emerged as a new paradigm for privacy protection with very conservative assumptions about the adversary's prior knowledge. It is believed that differential privacy mechanism can provide one of the strongest privacy guarantees. However, the meaning of the privacy budget parameter ε is still unclear for the general application users. In view of this, a new attack model, which can be used to choose the value for the parameter ε was proposed. A careful analytical study of the attack model and theoretical properties of the proposed approach was present.
Key words: differential privacy; attack model; data privacy

1 引言

自从 Samarati 和 Sweeney[1]在 1998 年通过连接马萨诸塞州健康信息表与选民登记表，成功得出了当时州长的健康信息后，数据发布的隐私保护技术再次得到了研究者的广泛关注。差分隐私[2]是近年出现的一种新的隐私保护技术，与传统的数据发布隐私保护技术不同，传统隐私保护技术通常做法是对原始数据进行匿名化数据隐蔽处理，而差分隐私使用随机算法对查询输出进行干扰处理。实现 ε-差分隐私算法比较简单，对于任何数据库 D 上的查询 q，随机算法 A 在正确查询结果 $q(D)$的基础之上，加上满足拉普拉斯(Laplace)分布的噪音 x，返回 $q(D)+x$ 给用户。可以证明，上述算法 A 满足 ε-差分隐私。

传统的隐私保护技术通常需要假设隐私保护信任模型的应用场景，需要攻击者的能力方面的假设和背景攻击知识方面的假设。而差分隐私保护技术允许攻击者拥有无穷的计算能力和其他任何有用的背景知识，也不需要关心攻击者具体的攻击策略。即使在最坏情况下，假设攻击者知道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通过此查询被泄露，因为攻击者无法从查询输出结果判断这条记录是否在数据集内。

收稿日期：2015-08-24；**修回日期**：2015-12-01
基金项目：国家自然科学基金资助项目(61202007, 61370080)；信息与通信工程浙江省重中之重学科开放基金资助项目；博士后基金资助项目(2013M540323)
Foundation Items: The National Natural Science Foundation of China (61202007, 61370080); Top Priority of the Discipline (Information and Communication Engineering) Open Foundation of Zhejiang Province; The Postdoctoral Science Foundation (2013M540323)

例 1　下面以表 1 和表 2 为例来说明。假设攻击者已经知道了所有人的信息，除了 Alex 的敏感属性值 Disease，攻击者知道的背景知识如表 2 所示。攻击者试图获取 Alex 的 Disease 属性值，于是向表 1 发出了如下的查询语句 q_0。

q_0: select count(*) from table1 where Disease= Bronchitis。

表 1　　**数据集 *D***

Name	Age	Zipcode	Disease
Alex	20	15k	Bronchitis
Bob	21	14k	Bronchitis
Jane	33	71k	Pneumonia
Cathy	38	25k	Gastritis
Eva	44	56k	Bronchitis
Frank	47	18k	Dyspepsia

考虑到攻击者已经知道了所有人(除了 Alex)的信息，所以他知道上面查询语句返回值是 2 或 3。差分隐私算法 *A* 在返回值为 3 的基础上，加上一个噪音 *x*，比如 *x*=−0.6，则返回 2.4 给攻击者。结果 2.4 对于攻击者来说，难以确定 Alex 的 Disease 是否对查询结果有贡献。这是由于按照差分隐私算法的定义，Alex 在不在这个结果集，对返回的结果 2.4 影响不大。换句话说，攻击者不能确定结果是 2 或者 3，从而保证了 Alex 的隐私。

1) 研究动机

2006 年机器学习会议(ICALP2006)和密码学理论会议(TCC2006)上，Dwork 等[2,3]首次正式提出了 ε-差分隐私保护技术，并提出了一种通用实现框架。在传统隐私保护研究中，比如 *k*-匿名模型中的 *k*[1]，*l*-多样性中的 *l*[4]，(ε, *m*)-匿名中的 *m*[5]，这些数字明确地告诉大家，在其模型定义下的隐私保护场景中和攻击者攻击能力假设下，攻击者能够攻击成功的概率分别是 $\frac{1}{k}$，$\frac{1}{l}$，$\frac{1}{m}$。目前，研究者认为差分隐私保护技术能够提供很强的隐私保护力度，参数 ε 衡量了随机算法 *A* 在抵抗攻击的能力，而且参数 ε 越小，其提供的隐私保护力度越大，这是由于 ε 越小，ε 反比于拉普拉斯噪音的幅度(scale)，即 $b=\Delta\frac{q}{\varepsilon}$，那么随机算法 *A* 返回结果中加入的噪音也就越大。同样地，从另一个角度来看，ε 越小，差分隐私要求随机算法 *A* 对数据集 D_1 和 D_2 输出的结果相差越小，对于攻击者来说，攻击的困难程度也就随之增加。

表 2　　**攻击者背景知识**

Name	Age	Zipcode	Disease
Alex	20	15k	?
Bob	21	14k	Bronchitis
Jane	33	71k	Pneumonia
Cathy	38	25k	Gastritis
Eva	44	56k	Bronchitis
Frank	47	18k	Dyspepsia

一般在实验中，研究者给出了不同的 ε，然后对比这些不同算法的查询平均差错率来评估算法优劣性。如果能够得出参数 ε 与攻击者成功的概率二者之间的关系，那么无疑给出了差分隐私保护力度的直观认识。

2) 目前的解决方案

为了恰当的选取参数 ε，Lee 和 Cliton 提出了一种攻击模型[6]，可以给出参数 ε 选取的一个上界。下面用例 2 来说明。

例 2　数据集 CENSUS 有 60 万条元组，每条元组通过 8 个属性描述一个美国人的信息：Age、Gender、Education、Marital、Race、Country、Work-class 和 Occupation。现在假设要控制攻击者攻击成功的概率不超过 $\frac{1}{3}$，对于 count 查询语句（比如 select count(*) from CENSUS）的参数 ε 的最大上界可达到

$$\varepsilon \leqslant \frac{\Delta q}{\Delta v}\ln\left(\frac{(n-1)\rho}{1-\rho}\right)=\ln\frac{(600\,000-1)\times\frac{1}{3}}{1-\frac{1}{3}}\approx 12.6 \quad (1)$$

具体的细节在第 3 节讨论。Lee 和 Cliton 提出的上界计算式，即式(1)，参数 ε 的选取依赖于 4 个参数：ρ、Δq、Δv 和 n。

有个问题自然而然地产生：参数 ε 的选取是不是可以依赖于其他参数？鉴于此，本文提出了一个新的攻击模型来度量差分隐私保护技术的安全性，基于这个模型，提出了一个差分隐私保护技术的攻击算法和参数 ε 的选取计算式。

3) 本文的贡献

本文的贡献主要包括以下 3 个方面。

①本文提出了一个差分隐私保护攻击模型，并详细地分析了该模型的特点，最后验证这个模型的

成功概率。

②提出了一个差分隐私保护的攻击算法，可以根据查询语句的返回值来回答攻击对象是否在查询数据集合中。

③给出了选取参数 ε 上界的一个计算式。只要给定查询函数的敏感度 Δq，查询的容错区间长度 L 和攻击者成功概率 ρ，就可以直接计算出参数 ε 上界。

2 基本概念

2.1 差分隐私保护框架

差分隐私保护是一种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。

定义 1 （差分隐私）。一个随机算法 A 满足 ε-差分隐私保护，当且仅当对于任何相差仅一个元组的 2 个集合 D_1、D_2 和任何输出 S，满足如下条件

$$\left|\frac{Prob(A(D_1))=S}{Prob(A(D_2))=S}\right|\leqslant \mathrm{e}^{\varepsilon} \tag{2}$$

其中，ε 是使用者指定的常数，D_1 和 D_2 至多相差一个元组，e 是自然对数常数。从数学上看，只要这个参数 ε 足够小，攻击者很难区分出来对同样的输出 S，查询函数到底是作用在 D_1 还是在 D_2 上。当参数 ε 等于 0 的时候，那么输出的仅仅是噪音才能满足上述要求，所以参数 ε 只有大于 0 才有实际的意义。同样条件下，参数 ε 越小私密性越好。

一般来说，差分隐私保护的实现技术是基于拉普拉斯分布来完成的，对于任何查询函数 q 作用于数据集 D 上，返回值是 $q(D)+x$，其中的 $q(D)$是查询的真实值，x 是满足拉普拉斯分布 $f(\mu,b)$ 的采样值：$x\propto f(\mu,b)$，这里 $b=\dfrac{\Delta q}{\varepsilon}$。容易证明，这个方法实现了差分隐私保护技术的要求。可以注意到，ε 越大，b 就可以越小。

定义 2 (敏感度)。Δq 是查询函数 q 的敏感度,其定义如下。

$$\Delta q=\max_{D_1,D_2}|q(D_1)-q(D_2)|$$

数据集 D_1 和 D_2 之间至多相差一个元素。

2.2 拉普拉斯分布

在概率与统计理论里，如果随机变量 x 的概率密度函数分布为

$$f(x\,|\,\mu,b)=\frac{1}{2b}\mathrm{e}^{-\frac{x-\mu}{b}} \tag{3}$$

那么它就是拉普拉斯分布。其中，μ 是位置参数，b>0 是尺度参数。为了讨论的方便，在不影响讨论和阅读的情况下，μ 默认是 0。

根据绝对值函数,如果将一个拉普拉斯分布分成 2 个对称的情形，那么很容易对拉普拉斯分布进行积分，其累积分布函数为

$$\begin{aligned}F(x)&=\int_{-\infty}^{x}f(\mu)\mathrm{d}\mu=\begin{cases}\dfrac{1}{2}\mathrm{e}^{\frac{(x-\mu)}{b}}, x<\mu\\ 1-\dfrac{1}{2}\mathrm{e}^{-\frac{(x-\mu)}{b}}, x\geqslant\mu\end{cases}\\&=\frac{1}{2}+\frac{1}{2}\mathrm{sign}(x-\mu)\left(1-\mathrm{e}^{-\frac{|x-\mu|}{b}}\right)\end{aligned} \tag{4}$$

3 现有的方案

在这一节，简单讨论 Lee 和 Clifton[6]的主要工作，并对其主要结论进行简要分析。

首先假设数据库有 n 条元组，除了攻击对象的敏感属性值外，攻击者知道所有的背景知识。攻击者对任意的 n−1 个元素集合 D'($|D'|=|D|-1$)，维持着一个元组 $<\omega,\alpha,\beta>$，容易得出这样的 D'共有 n 个可能，记为 Ψ，称潜在输入集。α、β 分别表示攻击者在获取回答 γ 前后 $w=D'$的前验与后验概率。

一般情况下，可以假设 α 满足平均分布,即 $\forall w\in\Psi$，都有 $\alpha(w)=\dfrac{1}{n}$，而后验概率从条件概率推导出来

$$\begin{aligned}\beta(W)&=P(w=D'\,|\,\gamma)\\&=\frac{\alpha(w)Prob(A(w)=\gamma)}{\sum_{\varphi\in\psi}\alpha(w)Prob(A(\varphi)=\gamma)}\\&=\frac{Prob(A(w)=\gamma)}{\sum_{\varphi\in\psi}Prob(A(\varphi)=\gamma)}\end{aligned} \tag{5}$$

从式(5)出发，经过推导和简单的数学不等式处理（具体证明过程参考文献[6]中 5.1 节），可以得出参数 ε 上界

$$\varepsilon\leqslant\frac{\Delta q}{\Delta v}\ln\left(\frac{(n-1)\rho}{1-\rho}\right) \tag{6}$$

其中，$\Delta v=\max_{1\leqslant i,j\leqslant n}|q(w_1)-q(w_2)|, i\neq j,\ w_1,w_2\in\psi$，$\rho$ 表示攻击者得出攻击对象在或者不在结果集的概率。注意到这个上界与 ln(n−1)成正比，而 n 是潜

在输入集的大小(即 D'的可能取法的数量，$n=|\Psi|$)，因此，当潜在输入集比较大时，参数 ε 取值比较大，这由例 2 可以看出。

式(6)隐藏了一个假设：攻击者不能区分 D'存在的 n 种可能取法，因此，ρ 必须大于$\frac{1}{n}$，否则没有意义。用例 3 来说明(用表 1 中的名字作为对应的元组)。

例 3　接例 1，根据文献[6]的定义，D={Bob, Alex, Eva}，D'共有 3 种可能取法: {Bob, Alex}、{Bob, Eva}、{Eva, Alex}。

对于查询 q_0，攻击者可能知道 D'只有一种可能：{Eva, Bob}。由于 Lee 和 Clifton 没有把 D 也看做是一种潜在输入，事实上，Ψ 应该有 n+1 种可能的取法，因此其式可以考虑改为

$$\varepsilon \leqslant \frac{\Delta q}{\Delta v}\ln\left(\frac{n\rho}{1-\rho}\right) \tag{7}$$

此外，文献[6]没有提供一种攻击算法,就是说攻击者在拿到回答 $q(D)+x$ 后,依然不能回答攻击对象是否在结果集里。这就要求攻击算法的设计必须从另外角度去思考。

在实际应用场景下，对于差分隐私保护技术的使用者来说，参数 ε 的选取是不可避免的问题，探究参数表达含义具有重要的理论价值和现实需求。要达到一定的隐私保护的要求，选取恰当的参数是使用者必须面对的问题。从上面的讨论可以得出，这个问题依然是开放的。

4　攻击模型

在本节，假设在最坏情况下，即潜在输入集只有 2 个（$|\Psi|$=2），探讨如何根据给定的查询返回值 $q(D)+x$ 猜测其真实值 $q(D)$，从而得出攻击对象在不在其集合中的结论。攻击者针对攻击对象，提出了一个查询问题 q，数据库拥有者根据问题查询得出结果 $q(D)$，加上噪音 x 后返回给攻击者，攻击者根据得到的 $q(D)+x$，他需要做出一个判断：某个攻击对象在不在集合中。

首先，注意到每个噪音 x 都是满足拉普拉斯分布的，因此，对于攻击者来说,不可能准确地猜出这个 x。考虑到一些查询函数的特点，攻击者只要猜出 x 落在某个范围之内就可以了。比如数据查询中最为常见的 count 查询,只要噪音 x 落在[−0.5, 0.5]之间，那么攻击者很容易得出真实值 $q(D)$，从而得出攻击对象在不在其查询结果中的结论。把[−0.5, 0.5]称为 count 查询的容错区间，区间的半长度记为 L。

从图 1 所示的拉普拉斯分布 $f(\mu,b)$ 看，位置参数 μ 对于攻击者是没有影响的。而参数 $b=\frac{\Delta q}{\varepsilon}$ 直接影响了攻击的容易程度，显而易见，当参数 b 比较小，经过拉普拉斯采样的数据 x 比较靠近位置参数 μ；相反，当参数 b 足够大，采样的数据 x 相当于平均分布在 $(-\infty,+\infty)$ 上，对于攻击者来说是很困难的。因此，参数 ε 的选取要能够反映上面的现象。

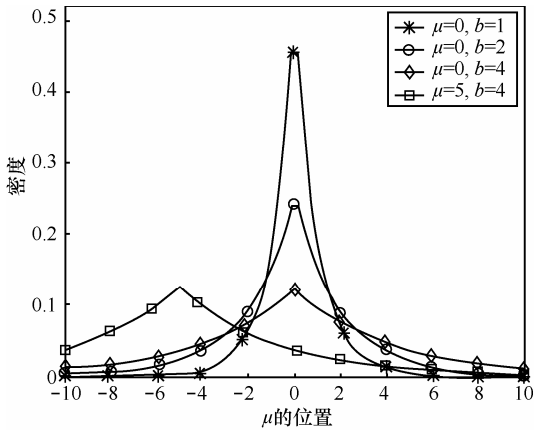

图 1　拉普拉斯分布

4.1　主要定理

为了刻画上述的现象，发现采样数据 x 落在 $[\mu-L, \mu+L]$的概率随着 b 的增大而变小，而这个概率正好可以反映攻击者的难度。基于上述观察，本文提出如下主要定理。

定理 1　若用采样上述拉普拉斯分布来给 $q(D)$ 加噪音 x，则 $q(D)+x$ 落在$(-\infty, q(D)+\mu+L)$概率为 $1-\frac{1}{2}\mathrm{e}^{-\frac{L\varepsilon}{\Delta q}}$。

证明　从定义出发，$q(D)+x$ 落在区间（$-\infty$, $q(D)+\mu+L$）的概率等于 x 落在区间$(-\infty, \mu+L)$的概率，因此，从拉普拉斯的累积函数出发，x 落在区间$(-\infty, \mu+L)$的概率等于 $F(\mu+L)=\frac{1}{2}+\frac{1}{2}(1-\mathrm{e}^{-\frac{L}{b}})=1-\frac{1}{2}\mathrm{e}^{-\frac{L}{b}}$，最后将 $b=\frac{\Delta q}{\varepsilon}$ 代入，就得到了上述的结果。

4.2　攻击算法

在 4.1 节基础上，比较容易可以给出攻击算法。为了问题的叙述方便和表述清楚，以 count 统计查询为例，其他统计函数也完全可以类似得

到。设位置参数 μ=0，L=0.5，框架如算法 1 所示，攻击者根据返回值的大小来确定攻击对象是否结果集中。

定理 2 算法 1 攻击者对于 count 查询的成功的概率是$1-\frac{e^{-\frac{\varepsilon}{2}}}{2}$。

证明 假设 $q(D)=m$ 或 $m+1$，给定 $q(D)+x$，考虑 2 个区间$(-\infty,m+0.5]$和$[m+0.5, +\infty)$。从定理 1 可知，若 $q(D)=m$，则 $q(D)+x$ 落在第一个区域的概率是$1-\frac{e^{-\frac{\varepsilon}{2}}}{2}$。若 $q(D)=m+1$，则 $q(D)+x$ 落在第 2 个区域的可能性相同。因此，根据 $q(D)+x$ 所落入的区域，有$1-\frac{e^{-\frac{\varepsilon}{2}}}{2}$的成功概率，即若落入第一个区域，则假设 $q(D)=m$，否则就假设 $q(D)=m+1$。注意，$q(D)=m$ 表示被攻击者不在原始数据内，而 $q(D)=m+1$ 则表示被攻击者在原始数据内。

算法 1 Attack Algorithm For Count Query

Input: $A(q(D)) = x + q(D)$

Output: Present or Absence

Method:

/* Laplace $f(\mu,b)$ distribution, and $q(D)\in\{m, m+1\}$*/

1) $y = x + q(D)$

2) if $y\in[m+0.5,+\infty)$

3) return Present

4) else

5) return Absence

图 2 给出了 count 查询的成功概率示例。

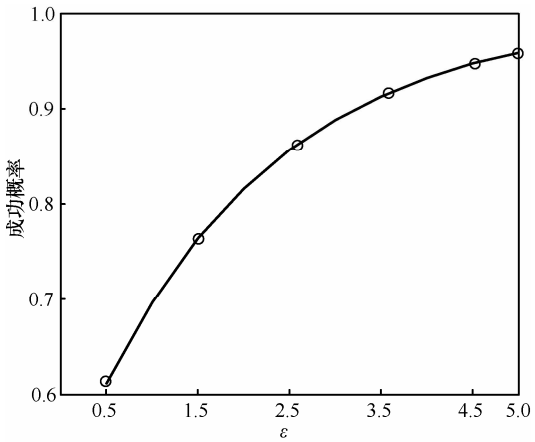

图 2 count 查询的成功概率示例

对于一般的查询函数，类似地容易推导得出攻击者能够成功的概率$1-\frac{1}{2}e^{-\frac{L\varepsilon}{\Delta q}}$。

4.3 参数 ε 的选取

有了 4.1 节主要定理和 4.2 节的攻击算法,参数 ε 的选取问题就变得容易，只要攻击者的成功概率 $\rho\leqslant(1-\frac{1}{2}e^{-\frac{L\varepsilon}{\Delta q}})$，解这个不等式,容易得出参数 ε 选取上界满足如下的条件

$$\varepsilon\leqslant\frac{\ln 2(1-\rho)\Delta q}{L} \tag{8}$$

式(8)给出的参数 ε 上界与数据集大小无关,仅仅与查询函数$(\Delta q, L)$和攻击者的成功概率 ρ 有关。

5 相关工作

当前，差分隐私保护技术的研究融合了数据库理论、统计学知识和现代密码学的观点，它定义了一个极为严格的数学模型，并对隐私泄露风险给出了严谨、定量化的表示和证明。本文将差分隐私保护的研究工作分成 3 个部分。

1) 差分隐私保护基础理论的研究，Gehrke, Kifer 等[7]提出了差分隐私的扩展版本：(ε,δ)-差分隐私,它比通常意义下的 ε-差分隐私在相同的条件和参数下要弱。Frank[7]则提出了另一种定义差分隐私的办法：$\Pr(A(D_1)=S)\leqslant\Pr(A(D_2)=S)\,e^{\varepsilon(D_1\oplus D_2)}$，并且提出了一个实现差分隐私的原型 LINQ，证明多个随机算法 A_1, A_2,…,A_r 分别满足 ε_1,ε_2 ,…,ε_r-差分隐私，那么随机算法 A_1,A_2,…,A_r 序列提供($\sum\varepsilon_i$)-差分隐私保护。Dinur, Nissim[9]指出了噪音的加入不能是完全对称的，否则一直要随机算法 A 回答相同的问题导致加入的噪音被抵销，容易遭到攻击。文献[10]进一步推广差分隐私保护技术，同时结合零知识理论,提出一种新的隐私保护模型 Crowd-Blending Privacy。Chris 与 Tamir[11]比较了差分隐私保护技术与隐私保护数据发布技术，认为二者不可互相取代,各有应用场景。差分隐私保护技术适合于隐私保护数据挖掘(PPDM)，而隐私保护数据发布技术在隐私保护数据发布中有更好的应用。

2) 探讨了差分隐私的各种性质及其如何在实现差分隐私的前提下，降低加入到数据集中的噪音。Nissim 等[12]提出了 2 种技术来提高满足差分隐私数据的可用性:其一是降低 $\max|A(D_1)-A(D_2)|$的值，其二是用 Subsample-and- aggregate 方法。文献

[13]则提出了 Propose-Test- Release 方法来提高数据的可用性。Mironov 等[14]提出了一个密码学协议，如果攻击者的能力不是无限的，那么满足差分隐私的数据可用性就可以提高,在现代密码学的理论观点来看,这个假设是合理的。Xiao 等[15]提出了用小波变换的思想来降低差分隐私带来的信息损失,而后他又提出 iReduct 算法[16]来降低数据查询的平均相对差错率。文献[15]小波变换只能处理低维数据，文献[17]试图控制维数来降低隐私保护数据发布的信息损失，而文献[18]利用贝叶斯网络处理高维数据差分隐私发布问题。文献[19]提出了基于采样的数据隐私发布技巧。Li 等[20]提出的方法可以一定意义上可以实现加入最优的噪音方差，但是需要很大的计算代价，其后续改进工作参考文献[21]。

3) 差分隐私保护的应用，尤其在机器学习与数据挖掘领域的应用。Bhaskar 等[22]将其应用到交易数据上的频繁项数据发布上。Korolova[23]和 Götz[24]研究了搜索历史记录差分隐私发布，Mcsherry 等[25]用于网络痕迹分析。Rastogi 和 Nathan[26]则提出了时间序列的数据发布，其技术也是通过在时间序列数据加入噪音。Xu 等[27]在 ICDE 会议上研究了差分隐私应用于柱行图发布。文献[28]提出了差分隐私频繁项集挖掘，而 Friedman 等[29]则应用差分隐私到构建决策树。Rubinstein 等[30]则将差分隐私技术应用到了支持向量机的学习训练，此外 Xiao 等[31]将差分隐私应用在图的统计发布工作。

6 结束语

尽管差分隐私保护技术得到了大家的广泛关注,但是如何在实际中选取其参数 ε 依然是个开放问题，参数 ε 选取的重要性是不言而喻的。有鉴于此，提出了一个基于攻击模型的参数 ε 选取算法，只要给定攻击者成功的概率 ρ 和 L，通过式(8)总是可以找出一个合适的 ε 参数值。

参考文献：

[1] SAMARATI P, SWEENEY L. Generalizing data to provide anonymity when disclosing information (abstract)[A]. Proceedings of the seventeenth ACMSIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems[C]. NewYork, 1998.188-188.

[2] DWORK C. Differential privacy[A]. Proceeding of the 33rd International Colloquium on Automata, Languages and Programming (ICALP)[C]. 2006.1-12

[3] DWORK C, MCSHERRY F, NISSIM K, et al. Calibrating Noise to Sensitivity in Private Data Analysis[M]. Theory of cryptography. Berlin: Springer, 2006.265-284.

[4] MACHANAVAJJHALA A, KIFER D, GEHRKE J, et al. *L*-diversity: privacy beyond k-anonymity[A]. Proceeding of the 22nd International Conference on Data Engineering (ICDE)[C]. 2006.1-24.

[5] LI J X, TAO Y F, XIAO X K. Preservation of proximity privacy in publishing numerical sensitive data[A]. Proceeding of the 37th ACM SIGMOD International Conference on Management of Data (SIGMOD)[C]. 2008.473-486.

[6] LEE J, CLIFTON C. How much is enough? Choosing ε for differential privacy[A]. Proceeding of the 14th International Conference on Information Security (ISC)[C]. Berlin, 2011.325-340.

[7] GEHRKE J, KIFER D, MACHANAVAJJHALA A, et al. Privacy: theory meets practice on the map[A]. Proceeding of the 24th International Conference on Data Engineering (ICDE)[C]. 2008. 277-286.

[8] FRANK M. Privacy integrated queries-an extension platform for privacy preserving data analysis[A]. Proceedings of the 2009 ACM SIGMOD International Conference on Management of Data[C]. 2009.19-30.

[9] NISSIM K, RASKHODNIKOVA S, SMITH A. Smooth sensitivity and sampling in private data analysis[A]. Proceeding of the 39th ACM Symposium on Theory of Computing (TCC)[C]. 2007.75-84.

[10] JOHANNES G, MICHAEL H, EDWARD L, et al. Crowd-blending pivacy[A]. Proceeding of the 32nd International Conference on Cryptology (CRYPTO)[C]. Berlin, 2012. 479-496.

[11] CHRIS C, TAMIR T. On syntactic anonymity and differential privacy[J]. Transcations on Data Privacy, 2013,6(2): 161-183.

[12] NISSIM K, RASKHODNIKOVA S, SMITH A. Smooth sensitivity and sampling in private data analysis[A]. Proceedings of the 39th ACM Symposium on Theory of Computing[C]. 2007. 75-84.

[13] DWORK C, LEI J. Differential privacy and robust statistics[A]. Proceedings of the 41st Annual ACM Symposium on Theory of Computing[C]. 2009.371-380.

[14] MIRONOV I, PANDEY O, REINGOLD O, et al. Computationaldifferential privacy[A]. Advances in Cryptology, 29th Annual InternationalCryptology Conference[C]. Santa Barbara, 2009.126-142.

[15] XIAO X K, WANG G Z, JOHANNES G. Differential privacy via wavelet transforms[A]. Proceeding of the 26th Int Conference on Data Engineering (ICDE)[C]. Washington, 2010.225-236.

[16] XIAO X, BENDER G, HAY M, et al. Ireduct: differential privacy with reduced relative errors[A]. Proceedings of the 2010 ACM SIGMOD International Conference on Management of Data[C]. 2011.229-240.

[17] CORMODE G, PROCOPIUC C, SRIVASTAVA D, et al. Differentially private spatial decompositions[A]. Proceeding of the 28th International Conference on Data Engineering (ICDE)[C]. 2012.20-31.

[18] ZHANG J, CORMODE G, PROCOPIUC C M, et al. Privbayes: private data release via bayesian networks[A]. Proceedings of the 2014 ACM SIGMOD International Conference on Management of Data[C]. 2014.1423-1434.

[19] CORMODE G, PROCOPIUC C, SRIVASTAVA D, et al. Differentially private spatial decompositions[A]. Proceeding of the 28th International Conference on Data Engineering (ICDE)[C]. 2012. 20-31.

[20] LI C, HAY M, RASTOGI V, et al. Optimizing linear counting queries under differential privacy[A]. Proceedings of the 31st ACM SIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems[C]. 2010. 123-134.

[21] LI C, MIKLAU G. Optimal error of query sets under the differentially-private matrix mechanism[A]. Proceedings of the Joint 2013 EDBT/ICDT Conferences[C]. Italy, 2013.272-283.

[22] BHASKAR R, LAXMAN S, SMITH A, et al. Discovering frequent patterns in sensitive data[A]. Proceedings of the 16th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining[C]. Washington, DC, USA, 2010.503-512.

[23] KOROLOVA A, KENTHAPADI K, MISHRA N, et al. Releasing search queries and clicks privately[A]. Proceedings of the 18th International Conference on World Wide Web[C]. Madrid, Spain, 2009.171-180.

[24] GÖTZ M, MACHANAVAJJHALA A, WANG G, et al. Gehrke: publishing search logs—a comparative study of privacy guarantees[J]. Publication, 2011,24(3): 520-532.

[25] MCSHERRY F, MAHAJAN R. Differentially-private network trace analysis[A]. Proceedings of the ACMSIGCOMM 2010 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications[C]. New Delhi, India, 2010.123-134.

[26] RASTOGI V, NATH S. Differentially private aggregation of distributed time-series with transformation and encryption[A]. Proceedings of the 2010 ACM SIGMOD International Conference on Management of Data[C]. 2010.735-746.

[27] XU J, ZHANG Z, XIAO X, et al. Differentially private histogram publication[J]. Journal on Very Large Data Bases,2013,22(6): 797-822.

[28] LI N H, QARDAJI W, SU D, et al. Privbasis: frequent itemset mining with differential privacy[J]. PVLDB, 2012, 5(11): 1340-1351.

[29] FRIEDMAN A, SCHUSTER A. Data mining with differential privacy[A]. Proceedings of the 16th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining[C]. 2010.493-502.

[30] RUBINSTEIN B I P, BARTLETT P L, HUANG L, et al. Learning in a large function space: privacy-preserving mechanisms for SVMLearning[J]. Journal of Privacy and Confidentiality, 2012, 4(1):65-100.

[31] ZHANG J, CORMODE G, PROCOPIUC C M, et al. Private release of graph statistics using ladder functions[A]. Proceedings of the 2015ACMSIGMOD International Conference on Management of Data[C]. 2015.731-745.

作者简介：

何贤芒[通信作者]（1981-），男，浙江三门县人，宁波大学讲师，主要研究方向为差分隐私保护与密码编码学。E-mail: hexianmang@nbu.edu.cn。

王晓阳（1960-），男，上海人，复旦大学教授，主要研究方向为时空移动数据分析、数据系统安全及私密、大数据并行式分析。

陈华辉（1964-），男，浙江鄞州人，宁波大学教授，主要研究方向为数据挖掘、数据流处理。

董一鸿（1969-），男，浙江宁波人，宁波大学教授，主要研究方向为大数据、数据挖掘、人工智能。