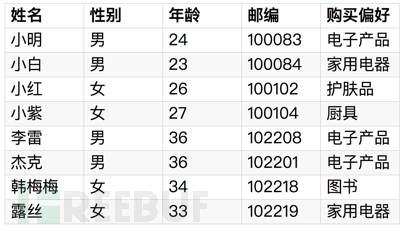
隐私保护的两种情况：

1. 公司为了学术研究和数据交流开放用户数据，学术机构或者个人可以向数据库发起查询请求，公司返回对应的数据时需要保证用户的隐私。
2. 公司作为服务提供商，为了提高服务质量，主动收集用户的数据，这些在客户端上收集的数据也需要保证隐私性。

这些方法先从直观的角度去衡量一个公开数据的隐私性，再到使用密码学、统计学等工具保证数据的隐私性。

<http://www.freebuf.com/column/147115.html>

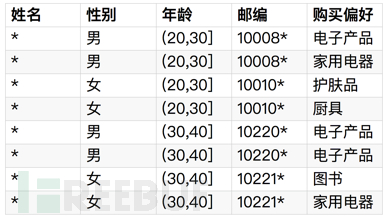
* k-anonymity（k-匿名化）



把表格中的公开属性分为以下三类：

1. Key attributes: 一般是个体的唯一标示，比如说姓名、地址、电话等等，这些内容需要在公开数据的时候删掉。
2. Quasi-identifier: 类似邮编、年龄、生日、性别等不是唯一的，但是能帮助研究人员关联相关数据的标示。
3. Sensitive attributes: 敏感数据，比如说购买偏好、薪水等等，这些数据是研究人员最关心的，所以一般都直接公开。

简单来说，k-anonymity 的目的是保证公开的数据中包含的个人信息至少 k-1 条不能通过其他个人信息确定出来。也就是公开数据中的任意 quasi-identifier信息，相同的组合都需要出现至少 k 次。



攻击方法

未排序匹配攻击 (unsorted matching attack) ：当公开的数据记录和原始记录的顺序一样的时候，攻击者可以猜出匿名化的记录是属于谁。例如如果攻击者知道在数据中小明是排在小白前面，那么他就可以确认，小明的购买偏好是电子产品，小白是家用电器。解决方法也很简单，在公开数据之前先打乱原始数据的顺序就可以避免这类的攻击。

补充数据攻击 (complementary release attack) ：假如公开的数据有多种类型，如果它们的 k-anonymity 方法不同，那么攻击者可以通过关联多种数据推测用户信息。

除此之外，如果敏感属性在同一类 quasi-identifiers 中缺乏多样性，或者攻击者有其它的背景知识，k-anonymity 也无法避免隐私泄露。

l-diversity 很难达成：例如，我们想在 10000 条数据中保证 2-diversity，那么可能最多需要10000\* 0.01 = 100 个相同的类型。这时可能通过之前介绍的 k-anonymity的方法很难达到。

偏斜性攻击 (Skewness Attack)：假如我们要保证在同一类型的数据中出现“艾滋病阳性”和出现“艾滋病阴性”的概率是相同的，我们虽然保证了 diversity，但是我们泄露隐私的可能性会变大。因为l-diversity 并没有考虑敏感属性的总体的分布。????

疑点解释：

1.很难达成

Example 2: Consider a dataset containing data for 1000 patients. The key attributes in the data set are Age, Height and Weight. There is a single confidential attribute AIDS whose values can be ”Yes” or ”No”. Assume that there are only five patients in the dataset with AIDS=”Yes”. Imagine that 2-sensitive k-anonymity is desired. Clearly, at least one patient with AIDS is needed in each group sharing a combination of key attributes, so that at most five groups can be formed. Therefore, key attributes must be heavily coarsened so that only five combinations of their values subsist.

1. Skewness attack.

If, in Example 2, a group has the same number of patients with and without AIDS; in that case, it satisfies distinct 2-diversity, entropy 2-diversity and any recursive (c,2)-diversity requirement. However, if an intruder can link a specific patient to that group, that patient can be considered to have 50% probability of having AIDS, in front of 5/1000 for the overall data set.

差分隐私

* 实现的四种方法：

1. 输出结果变换

2. 输入查询变换

3. 中间值变换

4. 抽样和聚合数据

输出结果变换的方法，主要针对查询结果是数值或者数值向量的情况，通过加入噪声使输出结果达到 ε-DP。

拉普拉斯分布

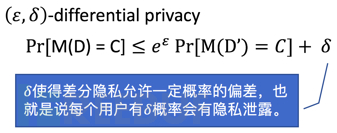
IMG_256

其中 Lap 是拉普拉斯分布，GS 表示 global sensitivity：

IMG_256

ε-DP 是一种“严格”的隐私保护保证，当在数据库中添加和删除一条数据时候，保证所有查询的输出都类似。

但是(ε, δ)-DP 在 ε-DP 的保证中允许了一定概率的错误发生，比如说，用户在 (ε, δ)-DP 的保护下会有 δ 概率的隐私泄露。



基于这些的概念，差分隐私在机器学习算法中也能够使用，常见的算法，比如说 PCA、logistic regression、SVM都有对应的差分隐私化算法。

差分隐私在数据的实用性和隐私性之间达到了平衡，使用者可以通过设定自己的“隐私预算”（privacy budget）来调整数据的实用性和隐私性。但是差分隐私也不是万能的，其中加入噪声的很多算法需要在大量的数据集上才实用。除此之外，什么才是“隐私预算”的合理设定也是一个问题。这些都是差分隐私面临的问题和挑战。并且由于差分隐私对于“背景知识”的要求过于强，所以需要在结果中加入大量随机化，导致数据的可用性（utility）急剧下降。但是差分隐私作为一个非常优雅的数学工具，是隐私保护的研究在未来的一个发展方向。差分隐私用严格的数学证明告诉人们一个匿名化的公开数据究竟能保护用户多少的隐私。

我们前面分别单独介绍了 k-匿名化和 ε-差分隐私，k-匿名化相对比较容易理解和实践，差分隐私更像是从理论上证明了隐私保护的边界。虽然方法的分析角度完全不同，但是它们之间却有着紧密的联系。普渡大学的Ninghui Li教授在 Provably PrivateData Anonymization: Or, k-Anonymity Meets Differential Privacy 文章中详细分析了 k-匿名化和 ε-差分隐私之间的关系。文章证明了在使用 k-匿名化“得当”的情况下，可以满足一定条件的 (ε, δ)-differentialprivacy。同时也提出了一种 k-anonymity 的变形：β-Sampling+ Data-independent \_Generalization + k-Suppression (k, β)-SDGS ，通过变形后的 k-anonymity 就可以使之满足差分隐私。通过使用差分隐私这种工具，我们就能精确的衡量前人提出的 k-anonymity，在理论研究上具有重要意义。

在实际应用中使用差分隐私时需要考虑的问题还有很多，我们在介绍差分隐私的时候假设所有的查询操作都由可信的数据库处理，数据库里存储着用户的原始数据。那么如果数据库被攻击了，包含用户隐私的原始数据就泄露了。

如果不收集用户的原始数据，在客户端上先做差分隐私，再上传给服务器，这个问题就解决了。最近Google率先使用RAPPOR系统在 Chrome 浏览器上通过这种方法收集用户的使用情况数据。RAPPOR 基于“随机应答”（randomized response）的方法保护用户的原始数据不被泄露，随机应答的流程如下：

1. 当用户需要上报个人数据的时候，首先“抛硬币”决定是否上报真实数据。如果是正面，则上报真实数据。如果不是，就上报一个随机的数据，再“抛一次硬币”决定随机数据的内容。

2. 服务器收到所有的数据后，因为知道“抛硬币”是正面的概率，服务器就能够判断返回的数据是正确的概率。

这种“随机应答”的方法在理论上也被证明是服从ε-差分隐私的。对于用户来说，隐私数据在上报给服务器之前就已经加了噪声，从而具有一定保证。对于公司来说，也能收集到有效的数据。

RAPPOR 使用“随机应答”的方法克服了之前只能回答简单查询语句的限制，现在可以上报包含字符串这类更加复杂的回答。RAPPOR 在上报字符串信息的时候首先使用“布隆过滤器”（bloom filter）算法把字符串哈希到一个数组中，然后再加入噪声传给服务器。布隆过滤器不需要存储元素本身，并可以用于检索一个元素是否在一个集合中。通过使用这种方法，就可以对字符串数据添加噪音，保护用户的隐私。

苹果在 2016 年的世界开发者大会（WWDC）上也宣布使用差分隐私的方法收集用户数据。虽然苹果没有透露具体的细节，我们从官方的描述中也可以推测出苹果也使用了在客户端上做匿名化再传输到服务器的方法。

Differentialprivacy is a research topic in the areas of statistics and data analytics thatuses hashing, subsampling and noiseinjection to enable…crowdsourced learning while keeping the data ofindividual users completely private. Apple has been doing some super-importantwork in this area to enable differential privacy to be deployed at scale.

我们刚才介绍的 Google 和 Apple 的模型都是先在本地做差分隐私，然后再上报给服务器，我们把这种方法叫做本地模式（local mode）。这种差分隐私的做法在上报数据可以相互关联的情况下还是存在隐私泄漏。Google的RAPPOR虽然解决了对同一个数据的多次上报的隐私泄露问题，但并没有解决多个相关数据上报后产生的隐私泄露问题。对于这一问题，Apple也没有给出详细的解释。

除了Google 和苹果在内部产品中使用差分隐私方法，哈佛大学公开了一个名为PSI (Ψ) 的项目，提供了一个便捷的差分隐私工具。使用者通过上传数据，调整差分隐私的参数，就可以获得满足差分隐私的数据集。

博士论文：

桶算法：仅仅通过将 QI 属性和敏感属性的关联切断，从而保护数据表中用户的敏感属性值信息。参考文献：两篇