**苹果的 Differential Privacy 差分隐私技术是什么原理？**

Craig Federighi 在 WWDC 上提到苹果做了几件事情：

* 局部抽样：与其上传用户的整体资料，苹果很可能是以某一频率，局部采集一部分用户的数据；
* 哈希加密：例如用户的键盘输入记录，可以先用布隆过滤器哈希一遍， 这样就可以在保护用户隐私的前提下，得知用户是否使用某些固定的表达；
* 注入噪音：在采集用户的数据前，向其中随机地注入一些噪音，只要被注入的噪音抽样是正态分布的，那么回到整体来看，这些噪音最终将相互抵消；

这些工作，都是为了避免在全局中暴露个人的信息

1. 什么是隐私？

\*从隐私保护的角度来说，隐私的主体是单个用户，只有牵涉到某个特定用户的才叫隐私泄露，发布群体用户的信息（一般叫聚集信息）不算泄露隐私。

2. 差分隐私

\*防止差分攻击；

\*找出一种方法让攻击者用某种方式查询100个信息和查询那99个信息得到的结果是一致的，那攻击者就没办法找出那第100个人的信息；

**\*敌人根本不知道我在不在这个数据集里**

\*差分隐私的核心思想：对于差别只有一条记录的两个数据集，查询它们获得相同值的概率非常非常的接近，*尽可能的把概率做的接近，而不是一致，以期在隐私和可用性之间找一个平衡。*

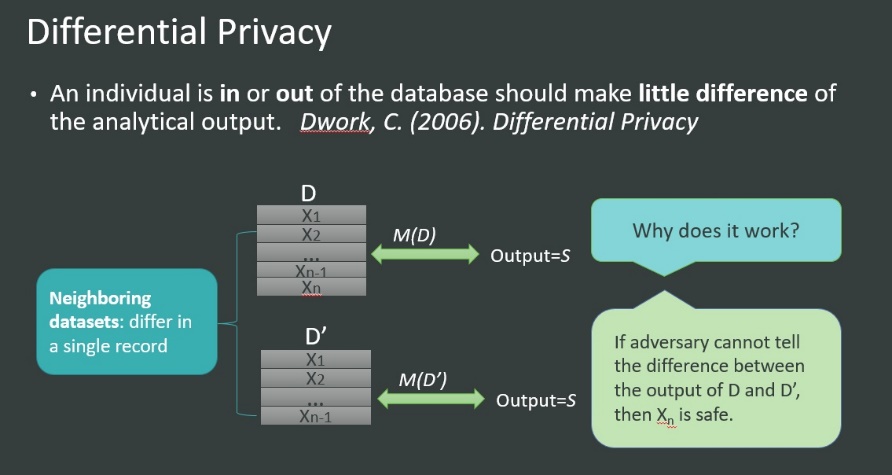
\*DP是为了允许研究者（苹果）在不泄露个体信息（用户隐私）的前提下对一个数据集的整体（用户行为）进行分析而研究出的加密手段。

\*\*\*\*\*\*对于加密，以均匀分布把明文映射到密文空间，明文加密后，以完全相同的概率有可能是密文空间中的任何一个密文，是均匀分布，这也是香农对perfect security的定义。

\*加密是要彻底破坏密文的可用性，它的可用性必须通过解密出明文来实现

\*\*\*\*\*\*对于DP，随机化后的结果不可能是均匀分布，发布均匀分布的结果就完全没意义了，所以它是Laplace分布或者高斯分布，也就是说虽然随机化了，但趋近真实值的概率高，而远离真实值的概率小。

\*DP没有逆过程，它必须在一定程度上保证随机化后结果的可用性。



3. 如何做到差分隐私

\*就是在查询结果里加入随机性，通过引入噪声，对源数据进行干扰后， 数据能够满足一定的标准，防止数据被推测；

**\*获取到的部分数据内容对于推测出更多的数据内容几乎没有用处；**

\*常用的有两种方法，一个是Laplace mechanism，在查询结果里加入Laplace分布的噪音，适用于数值型输出；另外一个是exponential mechanism，在查询结果里用指数分布来调整概率，适用于非数值型输出；还有Gaussian mechanism。

\*差分隐私是一种比较**强**的隐私保护技术，满足差分隐私的数据集能够**抵抗任何对隐私数据**的**分析**，因为它具有**信息论意义上的安全性。**

5. 差分隐私的弱点

\*由于对于背景知识的假设过于强，需要在查询结果中加入大量的随机化，导致数据的可用性急剧下降。

4. 差分隐私应用

差分隐私最美丽的一点在于只要你的算法每一个步骤都满足差分隐私的要求，那么它可以保证这个算法的最终输出结果满足差分隐私，换句话说，即使攻击者具有足够多的背景知识，也无法在最终的输出中找出单个人的某项属性。

\*算法每一个步骤都满足差分隐私的要求，那么它可以保证这个算法的最终输出结果满足差分隐私；

\*差分隐私可以被应用在推荐系统，社交网络，基于位置的服务，也包括了苹果的输入系统。

\*具体应用：差分隐私一般和获取权限控制（Access Control）以及信息流向分析（Information Flow Analysis）用来做统计分析型数据库的隐私保障。

\*应用场景包括:

1. 数据公司开放平台和数据库供第三方使用者编写用户自定义计算函数（User Defined Function），UDF可以是大数据的Map Reduce，也可以是Machine Learning，也可以是SQL

2. 大企业保护用户隐私，从采集就加密，然后所有人都只有使用数据进行分析的权力，无法获得数据本身.

3.数据分享

**DP与机器学习**

Dwork 团队 2015 年提出应用差分隐私的想法可以解决机器学习的 over-fitting 问题，一步从隐私界跨到了 AI 界。她们的论文发表在了 2015 年的 Science 上

[The reusable holdout: Preserving validity in adaptive data analysis](http://science.sciencemag.org/content/349/6248/636)