

Multiple Privacy Regimes Mechanism For Local Differential Privacy (本地差分隐私应用中的一种多隐私预算机制)

叶宇桐, 张敏, 冯登国, 李昊, 迟佳琳
可信计算与信息保障实验室
yeyutong@is.iscas.ac.cn

24TH International Conference on Database Systems for
Advanced Applications(DASFAA) 2019

• 问题背景

本地差分隐私 (LDP) 由于其去中心化的特性广泛应用于隐私数据分享领域, 它使用户的隐私数据只保存于用户的客户端。本地差分隐私需要预置一个隐私预算因子 ϵ , ϵ 的大小决定LDP的安全性, 然而其值目前都由LDP的服务端控制。

• 多隐私预算因子LDP框架

本论文提出一种由客户端 (用户) 自主确认隐私预算因子 ϵ 的LDP框架 (图 1), 可以使客户端自定义自身的隐私级别, 同时有效的防止一些非可信的数据收集者恶意使用高预算因子 ϵ 套取用户真实隐私数据。

服务端先将客户端依据隐私预算因子分组, 然后依次计算每组用户的产生的统计信息, 并最终使用最大似然函数计算得到最终结果, 我们将其命名为MLE方法, 当用户的预算因子呈现连续分布时, 我们改进MLE得到S-MLE方法。

我们将框架分为几个模块, 详细模块的功能请参考我们的论文。

• 实验结果

该框架能够应用于多种基于Frequency Oracle (FO) 的经典本地差分隐私协议 (如 Base Rappor, OUE, GRR等), 使其能够处理多隐私预算因子的场景。进一步的, 该框架可以使不同的客户端使用不同的本地差分隐私协议, 并通过实验证明, 这种混搭的方法能最终提高统计结果的准确率。在图 2中我们通过调整LDP协议的参数, 表明我们的框架能够在多隐私预算因子情形中实现最优的结果, 参数包括待统计的候选项频率, 客户端的隐私因子的分布, 不同协议的适用性等等。

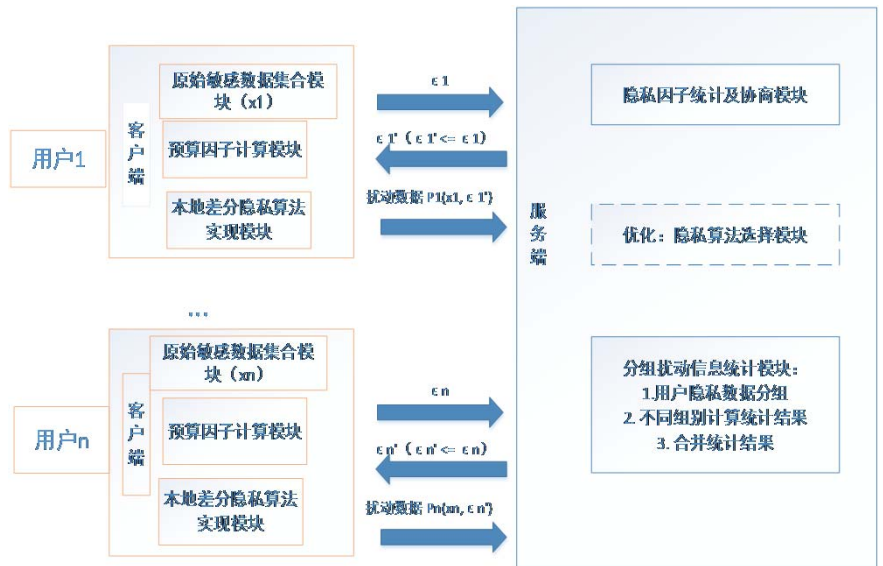


图1 多隐私因子LDP框架

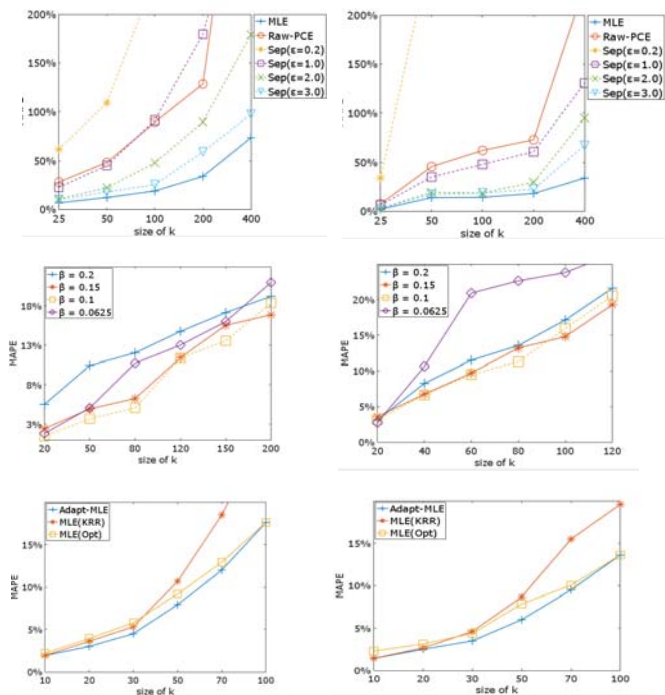


图2 LDP协议的参数对实验结果的影响

• 结论

我们的工作直接在服务端和客户端两处, 分别添加支持自选择预算因子的模块, 实现了多隐私因子的框架, 满足了用户不同级别的隐私需求。