MULKASE：一种针对多个所有者数据的新型密钥聚合可搜索加密方法

Mukti PADHYA[1], Devesh C. JINWALA[2]
[1]Sardar Vallabhbhai国家技术学院计算机工程系，印度苏拉特，394000
[2]印度理工大学计算机科学与技术系，印度查谟，180001

摘要：最新密钥聚合可搜索加密（KASE）尝试将搜索加密数据与支持数据所有者相结合，共享一个聚合的可搜索密钥；该密钥授权用户搜索数据。相应地，用户需提交一个单一聚合陷门至云端，在共享数据集上执行关键词搜索。然而，现有KASE方法不支持使用单一聚合陷门在由多个所有者共享的数据上搜索。因此，本文提出MULKASE方法，该方法允许用户使用单一陷门在由多用户拥有的不同数据记录上搜索。在MULKASE方法中，聚合密钥尺寸不依赖于数据所有者拥有的文档数量，即使外包密文数量超出预定限值，聚合密钥尺寸维持不变。安全性分析证实MULKASE方法对所选消息攻击和关键词攻击安全，亦证实该方法对交叉配对攻击安全，且提供查询隐私。理论和实验分析表明MULKASE方法性能优于现有KASE方法。文中还演示了MULKASE方法如何执行联合搜索。

关键词：可搜索加密；云存储；密钥聚合加密；数据共享
https://doi.org/10.1631/FITEE.1800192