

安全技术

基于MH树的外包数据库查询验证方法

袁多宝, 王晓明

(暨南大学计算机系, 广州 510632)

收稿日期 修回日期 网络版发布日期 接受日期

摘要 分析Merkle Hash(MH)树的结构特征, 针对MH树的验证对象大、验证过程存在冗余、安全性低等不足, 提出一种新的外包数据库查询验证方法, 使用部分物化中间节点的签名方法进行优化。分析结果表明, 该方法具有网络附加负载小、验证快、安全性较高、能迅速实现篡改定位等优点。

关键词 [外包数据库](#); [查询验证](#); [数据库安全](#); [Merkle Hash树](#)

分类号 [TP309](#)

DOI:

通讯作者:

作者个人主页: [袁多宝](#); [王晓明](#)

扩展功能

本文信息

- ▶ [Supporting info](#)
- ▶ [PDF\(103KB\)](#)
- ▶ [\[HTML全文\]\(0KB\)](#)
- ▶ [参考文献\[PDF\]](#)
- ▶ [参考文献](#)

服务与反馈

- ▶ [把本文推荐给朋友](#)
- ▶ [加入我的书架](#)
- ▶ [加入引用管理器](#)
- ▶ [引用本文](#)
- ▶ [Email Alert](#)
- ▶ [文章反馈](#)
- ▶ [浏览反馈信息](#)

相关信息

- ▶ [本刊中 包含“外包数据库; 查询验证; 数据库安全; Merkle Hash树”的相关文章](#)
- ▶ [本文作者相关文章](#)