

安全技术

基于可信计算的PIR

高利源, 倪佑生

(上海交通大学电子信息与电气工程学院, 上海 200030)

收稿日期 修回日期 网络版发布日期 2006-12-18 接受日期

摘要 介绍了私有信息获取和可信计算的概念, 由此引出了基于可信计算PIR的概念并列举了几种现有模型及其性能, 并为进一步提高PIR的性能提出了一种新的模型, 该模型可以把安全处理器(SC)读写数据库的时间复杂度从 $O(N^3/2)$ 降低到 $O(cN)$, 其中 c 是大于1的常数。

关键词 [私有信息获取](#) [可信计算](#) [安全处理器](#)

分类号

DOI:

通讯作者:

作者个人主页: [高利源; 倪佑生](#)

扩展功能

本文信息

▶ [Supporting info](#)

▶ [PDF \(203KB\)](#)

▶ [\[HTML全文\] \(0KB\)](#)

▶ [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“私有信息获取”的相关文章](#)

▶ [本文作者相关文章](#)

· [高利源, 倪佑生](#)