计算机工程 2006 32 (24): 141-143 ISSN: 1000-3428 CN: 31-1289/TP

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(N3/2)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