中南大学学报 自然科学版 英 文 版
教育部 主管
中南大学 主办

论文摘要

中南大学学报(自然科学版)
ZHONGNAN DAXUE XUEBAO(ZIRAN KEXUE BAN)
Vol.40 No.6 Dec.2009

[PDF全文下载] [全文在线阅读]

文章编号：1672-7207(2009)06-1660-06

基于B^+树的索引字段加密

王正飞[1, 2]，汪 卫[3]，施伯乐[3]

(1. 湖南商学院 计算机系，湖南 长沙，410205；
2. 国防科技大学 计算机学院 并行与分布式处理国家重点实验室， 湖南 长沙，410073；
3. 复旦大学 计算机学院，上海，200433)

摘 要：针对索引字段加密难的问题，提出一种基于B^+树的索引字段加密处理技术。该技术采用DBMS内部加密机制，选取在页/段映射到块时使用加密组件对索引字段进行加密，它能够使加密后的索引仍然保持有序，不会失去索引的快速查询功能。为了进一步保证索引字段本身的安全性，对索引按结点实施加密。实验中，模拟Postgresql中B^+树的构造方法，研究基于B^+树的加密索引字段的查询性能，并在页结点数和B^+树深度参数变化时，对分结点加密的查询性能进行测试。研究结果表明：基于B^+树的索引字段加密的查询速度虽然比明文查询速度下降20%左右，但采用分结点加密方式能够有效地减少解密代价，避免索引字段加密对查询性能产生较大影响。

关键字：数据库安全；加密；B^+树；索引；查询
中图分类号：TP311 文献标志码：A

Encryption over index fields based B^+ tree

HE Ji-shan, TONG Tie-gang, LIU Jian-xin

（1. Department of Computer, Hunan Business College, Changsha 410205, China;
2. National Key Laboratory for Parallel and Distributed Processing, School of Computer, National University of Defense Technology, Changsha 410073, China;
3. School of Computer Science, Fudan University, Shanghai 200433, China）

Abstract: In order to solve the problem of encrypting the index fields, a new way, i.e., encryption over the index fields based B^+ tree, was proposed. The encrypted mechanism inside DBMS was adopted, the index fields were encrypted by the encryption component during the process of mapping page or segment to block. The new method could preserve its order after the index fields was encrypted, and the function of fast querying was not lost. Furthermore, in order to ensure the security, the index itself was encrypted according to each node. In the experiments, the B^+ tree was constructed by simulating the Postgresql. Querying performance over the encrypted index fields was studied, and the querying performance over each encrypted node was tested by varying the numbers of the pages and B+ tree depths. The results show that the query velocity over the encrypted index fields can be accepted although it decreases by about 20% compared with the plaintext, and encryption over each node can efficiently reduce the

decryption cost so as to avoid the influence of querying on the encrypted index fields.

Key words:database security; encryption; B^+ tree; index; query