计算机工程　2008 34 (8): 162-163　ISSN: 1000-3428　CN: 31-1289/TP

安全技术

基于LUC密码体制的广义秘密共享方案

张建中，李文敏

(陕西师范大学数学与信息科学学院，西安 710062)

收稿日期　修回日期　网络版发布日期 2008-4-11　接受日期

摘要　给出一个安全性基于LUC密码体制的广义秘密共享方案，其中，每个参与者的私钥即为其子秘密，在秘密分发者和参与者之间不需要维护一条安全信道，降低了系统的代价。秘密恢复过程中，每位参与者都能够验证其他参与者是否进行了欺骗，并且只需维护一个子秘密，就可以实现对多个秘密的共享。

关键词　广义秘密共享；LUC密码体制；接入结构；授权子集

分类号　TP309

DOI:

对应的英文版文章：080850

通讯作者:

作者个人主页: 张建中;李文敏