

图书基本信息

书名：《密码学进展 CHINACRYPT'2000》

13位ISBN编号：9787030082626

10位ISBN编号：7030082621

出版时间：2001-01-01

出版社：科学出版社

作者：王萼芳

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：www.tushu000.com

内容概要

本书是2000年5月在武汉召开的第六届中国密码学学术会议论文集。书中收集了密码学各分支的研究论文40篇，主要内容包括序列密码和线性阵列、分组密码和公钥密码、自动机密码、认证理论和秘密共享、数字签名、Bent函数和布尔函数、与密码有关的代数、逻辑、混沌理论和零知识证明以及密码的应用等。

本书可供从事密码学、数学和计算机通讯专业的科技人员以及高等院校相关专业的师生参考。

书籍目录

序列密码和线性阵列

环 $Z/(2e)$ 上本原序列导出序列的0、1分布 ...朱风翔 戚文峰

交换环上线性递归阵列的代数表示...陆佩忠

QF环上零维理想是线性递归阵列的零化理想的判别...佩忠 刘木兰

GR(4, r)上本原序列的元素分布...张亚娟 祝跃飞

分组密码和公钥密码

基于中国剩余定理的MC公钥密码体制...曹珍富 张 彪

The Lower Bound for the Numbers

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:www.tushu000.com