第一图书网, tushu007.com

<<移位寄存器序列应用教程>>

图书基本信息

书名：<<移位寄存器序列应用教程>>

13位ISBN编号：9787810910200

10位ISBN编号：7810910205

出版时间：2009-6

出版时间：河南大学出版社

作者：李正朝 等 著

页数：131

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：http://www.tushu007.com

第一图书网, tushu007.com

前言

当前，人类社会已经进入高度的信息化阶段，发达国家把信息化作为强国、富民、振兴经济、抢占新世纪制高点的国策，网络化、数字化的特点使信息空间跨越国界，有别于传统的运作模式，信息安全成为数字化安全生存的基础和信息革命成败的关键，“信息就是财富，安全才有价值”，我们知道，密码技术是信息安全技术中的核心技术，而序列密码一直是作为军事和外交场合使用的主要密码技术，它的主要原理是：通过有限状态机产生性能优良的伪随机序列，使用该序列加密信息流得到密文序列，所以，序列密码算法的安全强度完全决定于它所产生的伪随机序列的好坏，产生好的序列密码的主要途径之一是利用移位寄存器产生伪随机序列，典型方法有：1）采用n阶非线性反馈函数产生大周期的非线性序列（如M序列），2）利用线性反馈移位寄存器加非线性前馈函数，产生前馈序列，3）利用一个寄存器序列作为时钟控制另一个寄存器序列（或自己控制自己）来产生钟控序列，4）通过组合运用以上方法，产生更复杂的网络，来实现复杂的序列，5）利用混沌理论、细胞自动机等方法产生伪随机序列，当然，伪随机序列在其他方面有着广泛的应用，如通信、雷达、导航、自动控制、计算机、声学和光学测量、数字式跟踪、距离测量系统、数字网络系统的故障检测等等，反馈移位寄存器优美奇妙的数学理论以及许多尚未解决的数学问题也引起了许多理论工作者的极大兴趣，为了适应伪随机序列理论的不断发展和研究以及现实教学的需要，作者结合多年的教学实践，参考相关教材和大量资料，编写了这本教材，本书是适用于信息安全、网络安全、应用数学、密码学及其他相关专业本科生的伪随机序列课程的教材，共分11章，第1～4章由李正朝编写，第5～8章由王伟编写，第9～11章由李新国编写，本书约有200道练习题，主要集中在线性移位寄存器部分，由于非线性部分的理论还不十分成熟，因此练习题就相对少一些，为了充分理解教材内容，应该尽量解答大量的习题，否则就不可能有很大的进步，许多习题都是例行的练习，当然部分习题也有一定的难度，但也不是深不可测的。

第一图书网, tushu007.com

<<移位寄存器序列应用教程>>

内容概要

当前，人类社会已经进入高度的信息化阶段，发达国家把信息化作为强国、富民、振兴经济、抢占新世纪制高点的国策，网络化、数字化的特点使信息空间跨越国界，有别于传统的运作模式，信息安全成为数字化安全生存的基础和信息革命成败的关键，“信息就是财富，安全才有价值”，我们知道，密码技术是信息安全技术中的核心技术，而序列密码一直是作为军事和外交场合使用的主要密码技术，它的主要原理是：通过有限状态机产生性能优良的伪随机序列，使用该序列加密信息流得到密文序列，所以，序列密码算法的安全强度完全决定于它所产生的伪随机序列的好坏。

第一图书网, tushu007.com

<<移位寄存器序列应用教程>>

书籍目录

第一图书网, tushu007.com

<<移位寄存器序列应用教程>>

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:http://www.tushu007.com