<<数论中的伪随机二进制数列>>

图书基本信息

书名：<<数论中的伪随机二进制数列>>

13位ISBN编号：9787030217486

10位ISBN编号：7030217489

出版时间：2008-5

出版时间：科学出版社

作者：刘华宁

页数：170

<<数论中的伪随机二进制数列>>

内容概要

随着通信与计算机网络的发展，伪随机二进制数列得到了广泛的应用，并已成为密码学的一个基本工具，在构造密码系统中起着重要的作用。
本书介绍了如何基于数论中的Legendre符号、Liouville函数、最大素因子、丢番图逼近、指标、最小非负剩余、Lehmer问题与Gallagher问题等来生成伪随机二进制数列，使用的方法涉及多项式特征和的估计、多项式指数和的估计、Dirichlet L函数均值、有限域上多项式理论等。
该书是对这一新兴领域十余年来研究工作的一个阶段性总结，其中包含了作者近几年来的研究成果。
本书可供高等院校数学系、计算机系研究生或高年级本科生学习，也可供数论、信息安全与密码学相关专业人员参考。

<<数论中的伪随机二进制数列>>

书籍目录

<<数论中的伪随机二进制数列>>

章节摘录

第1章　伪随机二进制数列的测度　　当前人类已经进入了一个崭新的时代，传统的商务活动、事务处理以及政府服务等越来越多地通过开放的计算机和通信网络来实施和提供。
只有在开放网络能提供安全通信的情况下，上述活动才能顺利实现，而各种形式的密码则是解决这一问题的基本理论和方法。
一个密码系统的安全性可以通过破译该系统的最好算法的计算复杂性来度量，因而计算复杂性理论已成为现代密码学的基础。
与此同时，伪随机二进制数列得到了广泛的应用，并已成为密码学的一个基本工具，在构造密码系统中起着重要的作用。
具体来说，基于计算复杂性理论构造的伪随机二进制数列与真随机数列是多项式时间不可区分的，也是多项式时间不可预测的。
这种类型的伪随机二进制数列具有重要的意义，用它构造的密码体制具有与用相同长度的真随机数列构造的密码体制同样的安全性。
目前已有的基于计算复杂性理论构造的伪随机二进制数列都是基于大数分解或离散对数等数学难题的，由于生成速度慢等缺点，不能完全满足实际的需要。
在实际应用中，当需要伪随机二进制数列时，人们通常利用硬件设备或数学方法来获得所需数列。
然而对于得到的数列，人们往往事先不知道其伪随机性如何，因此必须进行某些统计测试，使得伪随机数列满足真随机数列所应具有的某些统计性质或能通过某些统计测试。
……

<<数论中的伪随机二进制数列>>