<<密码学中的有关概率模型>>

图书基本信息

书名：<<密码学中的有关概率模型>>

13位ISBN编号：9787121018084

10位ISBN编号：712101808X

出版时间：2005-11

出版时间：电子工业出版社

作者：李世取

页数：449

字数：742400

<<密码学中的有关概率模型>>

内容概要

信息安全在当今社会的重要性是众所周知的，而概率论的思想和方法在密码设计和分析中一直占有重要的地位，这里建立合适的概率模型是解决问题的关键。

本书可作为信息安全、密码学与应用数学、计算机网络安全方面的理论工作者的参考书，也可作为相应专业研究开展课题研究的指导书和参考用书。

对从事密码设计、算法研究和密码分极及通信编码方面的工程技术人员也有使用价值和参考意义。

<<密码学中的有关概率模型>>

书籍目录

第1章 概率论基础 1.1 概率空间及概率测度 1.2 随机变量及其分布函数 1.3 随机变量的特征函数及其与分布函数的关系 参考文献第2章 概率极限理论 2.1 大数定律 2.2 分布函数列的弱收敛 2.3 特征函数列的正极限定理和逆极限定理 2.4 中心极限定理和重对数律 2.5 随机变量序列的r阶矩收敛 2.6 平稳随机变量序列及其遍历性 2.7 离散参数的马尔科夫链及其遍历性 2.8 取值为-1和+1的独立同分布随机变量序列的性质 2.9 混合相依随机变量序列的极限定理 参考文献第3章 密码学中非线性组合生成器的概率模型及其输出序列的极限性质 3.1 非线性组合生成器概率模型输出序列的极限性质 3.2 非线性组合生成器概率模型输出序列的有关精确分布 3.3 非线性组合生成器概率模型输出序列与多条仿射序列的综合分析 参考文献第4章 钟控生成器的概率模型 4.1“ 停走生成器 ”的一种概率模型 4.2“ 停走生成器 ”输出序列与输入序列间的符合率问题 4.3“ 停走生成器 ”输出序列的a一混合性验证· 4.4“ 停走生成器 ”中的另一类符合率问题 4.5“ 停走生成器 ”输出序列的大数性质 4.6“ 加法型 ”组合器的一种概率模型 4.7“ 乘法型 ”组合器的一种概率模型 4.8 多个“ 停走生成器 ”构成的组合器的概率模型 4.9“ 另类钟控生成器 ”的一种概率模型 4.10“ 衮特(Gunther)生成器 ”和“ 变形的衮特生成器 ”的概率模型 4.11“ 停走生成器 ”概率模型输出序列的子序列和原序列的符合率问题 4.12 多值钟控生成器的概率模型 参考文献第5章 带“ 记忆的,,ffi合器的概率模型 5.1 带lbit记忆的组合器的概率模型 5.2 带多bit记忆的组合器的概率模型 5.3 带1bit记忆组合器的概率模型输出序列的性质分析 5.4 带多bit记忆组合器的概率模型输出序列的相关性分析 结束语 参考文献第6章 m值随机变量的极限理论 6.1 马氏链与剩余类环或有限域上的独立随机变量和的极限分布定理 6.2 特征函数与剩余类环或有限域上独立同分布随机变量和的极限分布定理 6.3 特征函数与剩余类环上独立同分布随机变量和的极限分布定理 ’ 6.4 收敛速度 6.5 在逻辑函数的密码学性质分析中的应用 参考文献第7章 其他模型 7.1 序列的线性复杂度和定长二元随机序列的线性复杂度的数学期望 7.2 关于密码学中的周期随机序列 7.3 周期随机序列的线性复杂度的数学期望 7.4“ 秘密共享方案 ”中的一个概率模型 7.5 RSA的非完全映射特征分析中的概率模型 7.6 关于“ 缩减生成器 ”的概率模型 7.7 关于广义“ 缩减生成器 ”的概率模型 7.8 一般有限时态“ 钟控生成器 ”的概率模型 参考文献

<<密码学中的有关概率模型>>

版权说明