

<<信息论、编码与密码学>>

图书基本信息

书名：<<信息论、编码与密码学>>

13位ISBN编号：9787111308881

10位ISBN编号：7111308883

出版时间：2010-9

出版时间：机械工业

作者：博斯

页数：231

译者：武传坤,李徽

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>

## <<信息论、编码与密码学>>

### 内容概要

信息论、错误控制编码和密码学是现代数字通信系统中的三大支柱，本书用有限的篇幅将三者中所有重要的概念有机地结合起来，涉及信息论、信源编码、信道编码和密码学等方面的知识，不仅内容丰富，而且技术深度适当。

本书适合作为高等院校信息安全、电子工程及相关专业信息论和编码课程的教材，从事相关工作的专业技术人员也能从中受益。

#### 作者简介

波斯，在美国宾夕法尼亚大学获电气工程博士学位。  
曾在位于美国加利福尼亚州圣何塞的Alliance半导体公司任高级设计工程师。  
现任印度理工学院教授。  
2003年荣获印度国家工程师学会（INAE）颁发的“杰出青年工程师奖”。

## &lt;&lt;信息论、编码与密码学&gt;&gt;

## 书籍目录

出版者的话译者序第2版前言第1版前言第一部分 信息论和信源编码 第1章 信源编码 1.1 信息论简介 1.2 不确定性和信息 1.3 平均互信息和熵 1.4 连续随机变量的信息度量 1.5 信源编码定理 1.6 霍夫曼编码 1.7 Shannon—Fano—Elias编码 1.8 算术编码 1.9 Lempel—Ziv算法 1.10 游程编码和PCX格式 1.11 率失真函数 1.12 优化量化器的设计 1.13 随机过程的熵率 1.14 图像压缩简介 1.15 无损压缩的JPEG标准 1.16 有损压缩的JPEG标准 1.17 评注 1.18 小结 习题 上机习题 第2章 信道容量和编码 2.1 引言 2.2 信道模型 2.3 信道容量 2.4 信道编码 2.5 信息容量定理 2.6 Shannon限 2.7 MIMO系统的信道容量 2.8 码的随机选取 2.9 评注 2.10 小结 习题 上机习题第二部分 错误控制编码(信道编码) 第3章 纠错线性分组码 3.1 纠错码简介 3.2 基本定义 3.3 线性分组码的矩阵描述 3.4 等价码 3.5 奇偶校验矩阵 3.6 线性分组码的译码 3.7 伴随式译码 3.8 译码后的错误概率(纠错概率) 3.9 完备码 3.10 汉明码 3.11 低密度奇偶校验(LDPC)码 3.12 最优线性码 3.13 最大距离可分(MDS)码 3.14 最小距离的界 3.15 空时分组码 3.16 评注 3.17 小结 习题 上机习题 第4章 循环码 4.1 循环码简介 4.2 多项式 4.3 多项式的除法算法 4.4 一种循环码的生成方法 4.5 循环码的矩阵描述 4.6 准循环码和截短循环码 4.7 突发错误纠错 4.8 Fire码 4.9 Golay码 4.9.1 二元Golay码 4.9.2 三元Golay码 4.10 循环冗余校验(CRC)码 4.11 循环码的电路实现 4.12 评注 4.13 小结 习题 上机习题 第5章 BCH码 5.1 BCH码简介 5.2 基本引理 5.3 极小多项式 5.4 极小多项式作为生成多项式 5.5 一些BCH码实例 5.6 BCH码的译码 5.7 Reed—Solomon码 5.8 Reed—Solomon; 编码器和译码器的实现 5.8.1 硬件实现 5.8.2 软件实现 5.9 实信道上 $R_s$ 码性能 5.10 嵌套码 5.11 评注 5.12 小结 习题 上机习题 第6章 卷积码 6.1 卷积码简介 6.2 树码和网格码 6.3 卷积码的多项式描述(解析表示) 6.4 卷积码的距离概念 6.5 生成函数 6.6 卷积码的矩阵描述 6.7 卷积码的维特比译码 6.8 卷积码的距离界 6.9 性能界 6.10 著名的好卷积码 6.11 Turbo码 6.12 Turbo译码 6.12.1 改进的Bahl、Cocke、Jelinek Raviv(BCJR)算法 6.12.2 迭代MAP译码 6.13 Turbo码的交织器设计 6.14 评注 6.15 小结 习题 上机习题 第7章 网格编码调制 7.1 网格编码调制(TCM)简介 7.2 编码调制的概念 7.3 通过集合分割的映射 7.4 Ungerboeck的TCM设计准则 7.5 TCM译码器 7.6 AWGN信道性能评估 7.7 靠的计算 7.8 衰退信道的TCM 7.9 空时网格码 7.9.1 缓慢雷利衰退 7.9.2 快速雷利衰退 7.10 评注 7.11 小结 习题 上机习题第三部分 安全通信编码 第8章 密码学 8.1 密码学简介 8.2 加密技术概述 8.3 加密算法所用到的运算 8.4 对称(保密密钥)密码学 8.5 数据加密标准(DES) 8.6 国际数据加密算法(IDEA) 8.7 RC密码 8.8 非对称(公钥)算法 8.9 RSA算法 8.10 全球电子邮件加密标准 8.11 单向散列变换 8.12 其他技术 8.13 椭圆曲线密码学 8.14 Diffie—Hellman密钥协商协议 8.15 利用混沌理论实现安全通信 8.16 量子密码学 8.17 生物加密 8.18 密码分析 8.19 密码学中的政治因素 8.20 评注 8.21 小结 习题 上机习题

章节摘录

量子密码学源于Stephen Weisner在20世纪70年代初期提出的“共轭编码”(Conjugate Coding),直到1983年,这个思想才正式发表。

当时,由于熟悉Weisner的理论,Bennett和Brassard已经准备提出他们自己的想法。

他们在1984年提出了“BB84”——第一个量子密码协议。

直到1991年,基于这个思想的第一个实验原型系统才得以实现(距离是32厘米)。

最近一段时期,跨越千米距离的光纤电缆的若干系统被测试成功。

混沌理论,非线性动力系统理论的一个分支,作为密码学领域的一个新方向,其相关研究越来越多。

低维度动力系统有非常复杂并且不可预测的性质,而这些性质对于信息的扩散和混淆非常有利。

此方向最近的动态是由Baptista、Kocarev和Bose提出的。

从20世纪70年代早期开始,基于大量广泛的生物信息模板的身份识别系统引起了学术界、工业界以及科幻电影的广泛兴趣。

当前的研究使用各种不同的生物统计信息:(1)传统的生物统计信息(例如指纹、掌形、虹膜、视网膜),(2)最近的生物信息模板(例如声音、签名、掌纹和脸);(3)新方法(例如耳形、DNA、击键节奏、脸的不对称性和体味)。

由于生物信息不是一成不变的,所以生物模板不能作为密钥。

基于生物统计信息加密的研究源于1990年,并且成为当今一个热点研究方向。

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>