<<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

<<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

博斯，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”。

<<信息论、编码与密码学>>

书籍目录

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”（ConjugateCoding），直到1983年，这个思想才正式发表。
当时，由于熟悉Weisher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、掌纹和险）；（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。

<<信息论、编码与密码学>>

版权说明