HZ BOOKS
华章教育

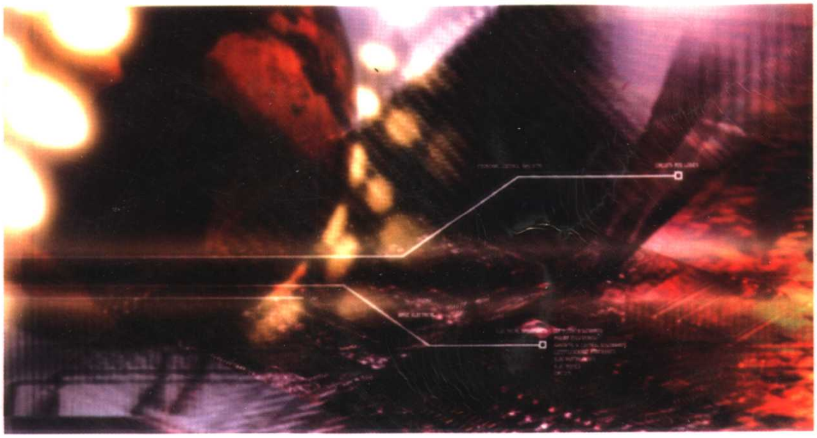
经典原版书库

信息论、编码与密码学

（英文版）

INTERNATIONAL EDITION

INFORMATION THEORY CODING AND CRYPTOGRAPHY



COMMUNICATION ENGINEERING

RANJAN BOSE

（美）Ranjan Bose 著

机械工业出版社
China Machine Press

Mc Graw Hill Education

信息论、编码与密码学

[illegible]

[illegible]

经典原版书库

信息论、编码与密码学

（英文版）

Information Theory, Coding and Cryptography

（美）Ranjan Bose 著

机械工业出版社
China Machine Press

Ranjan Bose:Information Theory, Coding and Cryptography (ISBN:0-07-048297-7).

本书版权登记号：图字：01-2003-5136

图书在版编目（CIP）数据

信息论、编码与密码学（英文版）/（美）鲍斯（Bose, R.）著. –北京：机械工业出版社，2003.9

（经典原版书库）

书名原文：Information Theory, Coding and Cryptography

ISBN 7-111-12770-6

I. 信… II. 鲍… III. ①信息论–英文 ②信息–编码–英文 ③密码–理论–英文 IV. ①TN911.2 ②TN918.1

中国版本图书馆CIP数据核字（2003）第068442号

机械工业出版社（北京市西城区百万庄大街22号　邮政编码　100037）
责任编辑：迟振春
北京昌平奔腾印刷厂印刷・新华书店北京发行所发行
2003年9月第 1 版第 1 次印刷
787mm × 1092mm 1/16・18.75印张
印数：0 001-3000 册
定价：30.00元

凡购本书，如有倒页、脱页、缺页，由本社发行部调换
本社购书热线电话：（010）68326294

出版者的话

文艺复兴以降，源远流长的科学精神和逐步形成的学术规范，使西方国家在自然科学的各个领域取得了垄断性的优势；也正是这样的传统，使美国在信息技术发展的六十多年间名家辈出、独领风骚。在商业化的进程中，美国的产业界与教育界越来越紧密地结合，计算机学科中的许多泰山北斗同时身处科研和教学的最前线，由此而产生的经典科学著作，不仅擘划了研究的范畴，还揭橥了学术的源变，既遵循学术规范，又自有学者个性，其价值并不会因年月的流逝而减退。

近年，在全球信息化大潮的推动下，我国的计算机产业发展迅猛，对专业人才的需求日益迫切。这对计算机教育界和出版界都既是机遇，也是挑战；而专业教材的建设在教育战略上显得举足轻重。在我国信息技术发展时间较短、从业人员较少的现状下，美国等发达国家在其计算机科学发展的几十年间积淀的经典教材仍有许多值得借鉴之处。因此，引进一批国外优秀计算机教材将对我国计算机教育事业的发展起积极的推动作用，也是与世界接轨、建设真正的世界一流大学的必由之路。

机械工业出版社华章图文信息有限公司较早意识到“出版要为教育服务”。自1998年开始，华章公司就将工作重点放在了遴选、移译国外优秀教材上。经过几年的不懈努力，我们与Prentice Hall，Addison-Wesley，McGraw-Hill，Morgan Kaufmann等世界著名出版公司建立了良好的合作关系，从它们现有的数百种教材中甄选出Tanenbaum，Stroustrup，Kernighan，Jim Gray等大师名家的一批经典作品，以“计算机科学丛书”为总称出版，供读者学习、研究及珍藏。大理石纹理的封面，也正体现了这套丛书的品位和格调。

“计算机科学丛书”的出版工作得到了国内外学者的鼎力襄助，国内的专家不仅提供了中肯的选题指导，还不辞劳苦地担任了翻译和审校的工作；而原书的作者也相当关注其作品在中国的传播，有的还专诚为其书的中译本作序。迄今，“计算机科学丛书”已经出版了近百个品种，这些书籍在读者中树立了良好的口碑，并被许多高校采用为正式教材和参考书籍，为进一步推广与发展打下了坚实的基础。

随着学科建设的初步完善和教材改革的逐渐深化，教育界对国外计算机教材的需求和应用都步入一个新的阶段。为此，华章公司将加大引进教材的力度，在“华章教育”的总规划之下出版三个系列的计算机教材：除“计算机科学丛书”之外，对影印版的教材，则单独开辟出“经典原版书库”；同时，引进全美通行的教学辅导书“Schaum's Outlines”系列组成“全美经典学习指导系列”。为了保证这三套丛书的权威性，同时也为了更好地为学校和老师们服务，华章公司聘请了中国科学院、北京大学、清华大学、国防科技大学、复旦大学、上海交通大学、南京大学、浙江大学、中国科技大学、哈尔滨工业大学、西安交通大学、中国人民大学、北京航空航天大学、北京邮电大学、中山大学、解放军理工大学、郑州大学、湖北工学院、中国国

家信息安全测评认证中心等国内重点大学和科研机构在计算机的各个领域的著名学者组成“专家指导委员会”，为我们提供选题意见和出版监督。

这三套丛书是响应教育部提出的使用外版教材的号召，为国内高校的计算机及相关专业的教学度身订造的。其中许多教材均已为M. I. T.，Stanford，U.C. Berkeley，C. M. U. 等世界名牌大学所采用。不仅涵盖了程序设计、数据结构、操作系统、计算机体系结构、数据库、编译原理、软件工程、图形学、通信与网络、离散数学等国内大学计算机专业普遍开设的核心课程，而且各具特色——有的出自语言设计者之手、有的历经三十年而不衰、有的已被全世界的几百所高校采用。在这些圆熟通博的名师大作的指引之下，读者必将在计算机科学的宫殿中由登堂而入室。

权威的作者、经典的教材、一流的译者、严格的审校、精细的编辑，这些因素使我们的图书有了质量的保证，但我们的目标是尽善尽美，而反馈的意见正是我们达到这一终极目标的重要帮助。教材的出版只是我们的后续服务的起点。华章公司欢迎老师和读者对我们的工作提出建议或给予指正，我们的联系方法如下：

电子邮件：hzedu@hzbook.com
联系电话：(010) 68995264
联系地址：北京市西城区百万庄南街1号
邮政编码：100037

About the Author

Ranjan Bose is an Associate Professor in the department of Electrical Engineering at the Indian Institute of Technology (IIT), Delhi. He did his B. Tech. in Electrical Engineering from IIT, Kanpur and his M.S. and Ph. D. in Electrical Engineering from the University of Pennsylvania, Philadelphia. He then worked at Alliance Semiconductors Inc. as a Senior Design Engineer. Since November 1997, he has been with the Indian Institute of Technology (IIT), Delhi, as a faculty member. Dr. Bose frequently lectures on coding and cryptography. Dr. Bose was awarded the URSI Young Scientist award in 1999 and the Humboldt Fellowship in July 2000.

Preface

Information theory, error control coding and cryptography are the three load-bearing pillars of modern digital communication systems. All the three topics are vast, and there are many good books that deal with these topics individually. In this book, an attempt has been made to incorporate all the important concepts of *information theory, error control coding and cryptography* in-between the two covers, without making the covers too far apart. This is intended as a simple and lively book on the subject.

This book results from my teaching of different topics on information theory and coding at Indian Institute of Technology, Delhi. While writing this book, I had to take a decision regarding how mathematical the book should be. Quoting Richard W. Hamming: "*Mathematics is an interesting intellectual sport but it should not be allowed to stand in the way of obtaining sensible information about physical processes*". Too mathematical a book has the potential danger of scaring away students who lack a strong background in mathematics. On the other hand, the use of mathematics cannot be reduced beyond a limit, if the concepts in information theory and error control coding have to be studied with a certain amount of rigor. But then, life is all about striking a balance. I have tried to traverse the path of golden mean in this book. Mathematics has been used wherever necessary, and only to the extent that it is essential. Intuitive explanations have been provided wherever possible. I also believe that teaching by example is a very effective method of instruction. Therefore, as soon as a new concept is introduced, I have tried to provide at least one numerical example.

HOW TO READ THIS BOOK

This book has been written to be both a lively introduction as well as a fairly detailed reference to the fascinating world of information theory, coding and cryptography. The entire book has been divided into three logical parts:

Part I—Information Theory and Source Coding,
Part II—Error Control Coding (Channel Coding), and
Part III—Coding for Secure Communications.

Part I contains two chapters—Chapter 1 deals with the concept of information and its efficient representation. Efficient representation of information leads to data compression. The chapter also introduces the concept of run length coding, the rate distortion function and the design of an optimal quantizer. The chapter concludes by giving a brief introduction to image compression.

Chapter 2 deals with the concepts of a communication channel and the channel capacity. This chapter tries to answer the question: How many bits per second can be sent over a channel of a given bandwidth and for a given signal to noise ratio? It also brings out the need for error control coding.

Part II contains five chapters, all on error control coding—Chapter 3 introduces the reader to the class of linear block codes. Linear block codes are useful, instructive and simple. Encoding and decoding strategies are discussed for this class of codes. The notions of perfect codes, optimal linear codes and maximum distance separable (MDS) codes are also introduced.

Chapter 4 deals with cyclic codes, a sub-class of linear block codes. Cyclic codes are particularly useful for burst error correction. Fire codes, Golay codes and Cyclic Redundancy Check (CRC) codes are discussed as specific examples of cyclic codes. The chapter concludes with a section on the circuit implementation of cyclic codes.

Chapter 5 takes the reader to the world of Bose–Chaudhuri Hocquenghem (BCH) codes, a very powerful class of multiple error correcting codes. The Reed-Solomon codes, a sub-class of BCH codes, is also discussed in this chapter.

Chapter 6 takes a look at convolutional codes, which are essentially codes with memory. The concept of Trellis codes is introduced to the reader and the Viterbi decoding technique is discussed in detail. Some known good convolutional codes are also studied. Finally, the reader is given a flavor of the hot-so-old Turbo codes.

Chapter 7 on Trellis Coded Modulation (TCM) talks about the combined coding and modulation schemes. TCM encoding and decoding are discussed. The reader also learns how to design TCM schemes for additive white Gaussian noise channels as well as fading channels.

Part III contains a chapter on Cryptography—Chapter 8 looks at yet another application of coding, i.e. secure communications. The chapter discusses both the secret key and public key encryption techniques using specific examples. Other techniques such as one-way hashing and encryption using chaos functions are also discussed. The chapter concludes with a note on the politics of cryptography.

I have tried to include numerical examples as and when required. Each chapter ends with a concluding remark, which contains brief historical notes describing the origins of the important results and contributions. Also, there is a telegraphic summary at the end of each chapter, which can be used as a ready reference, or a quick search mechanism for a particular formula or definition, or simply a confidence builder prior to an exam. The end of the chapter problems should help the enthusiastic reader crystallize the concepts discussed in the text. I have also added computer-based exercises at the end of each chapter. It is recommended that these computer problems should be made a part of learning this subject.

I have tried my best to free the book from all errors. Unfortunately there does not exist a foolproof error control technique for that! I have tried to include all the important, practical and interesting concepts related to this area. Comments from the readers regarding errors, omissions and other constructive suggestions are welcome at rbose@ee.iitd.ac.in

Finally, I would like to quote Blaise Pascal, who said, "*The last thing one knows when writing a book is what to put first*".

Ranjan Bose
New Delhi

Acknowledgements

I would like to thank the Department of Electrical Engineering at the Indian Institute of Technology (IIT), Delhi for providing a stimulating academic environment that inspired this book. In particular, I would like to thank Prof. S.C. Dutta Roy, Prof. Surendra Prasad, Prof. H.M. Gupta, Prof. V.K. Jain, Prof. Vinod Chandra, Prof. Santanu Chaudhury, Prof. S.D. Joshi, Prof. Sheel Aditya, Prof. Devi Chadha, Prof. D. Nagchoudri, Prof. G.S. Visweswaran, Prof. R. K. Patney, Prof. V. C. Prasad, Prof. S. S. Jamuar and Prof. R. K. P. Bhatt. I am also thankful to Dr. Subrat Kar, Dr. Ranjan K. Mallik and Dr. Shankar Prakriya for friendly discussions. I have been fortunate to have several batches of excellent students whose feedback have helped me improve the contents of this book. Many of the problems given at the end of the chapters have been tested either as assignment problems or examination problems.

My heartfelt gratitude is due to Prof. Bernard D. Steinberg, University of Pennsylvania, who has been my guide, mentor, friend and also my Ph. D thesis advisor. I am also grateful to Prof. Avraham Freedman, Tel Aviv University, for his support and suggestions as and when sought by me. I would like to thank Prof. B. Sundar Rajan of the Electrical Communication Engineering group at the Indian Institute of Science, Bangalore, with whom I had a preliminary discussion about writing this book.

I wish to acknowledge valuable feedback on this initial manuscript from Prof. Ravi Motwani, IIT Kanpur, Prof. A.K. Chaturvedi, IIT Kanpur, Prof. N. Kumaravel, Anna University, Prof. V. Maleswara Rao, College of Engineering, GITAM, Visakhapatnam, Prof. M. Chandrasekaran, Government College of Engineering, Salem and Prof. Vikram Gadre, IIT Mumbai.

I am indebted to my parents, for their love and moral support throughout my life. I am also grateful to my grandparents for their blessings, and to my younger brother, Shantanu, for the infinite discussions on finite topics.

Finally, I would like to thank my wife and best friend, Aloka, who encouraged me at every stage of writing this book. Her constructive suggestions and balanced criticism have been instrumental in making the book more readable and palatable. It was her infinite patience, unending support, understanding and the sense of humour that were critical in transforming my dream into this book.

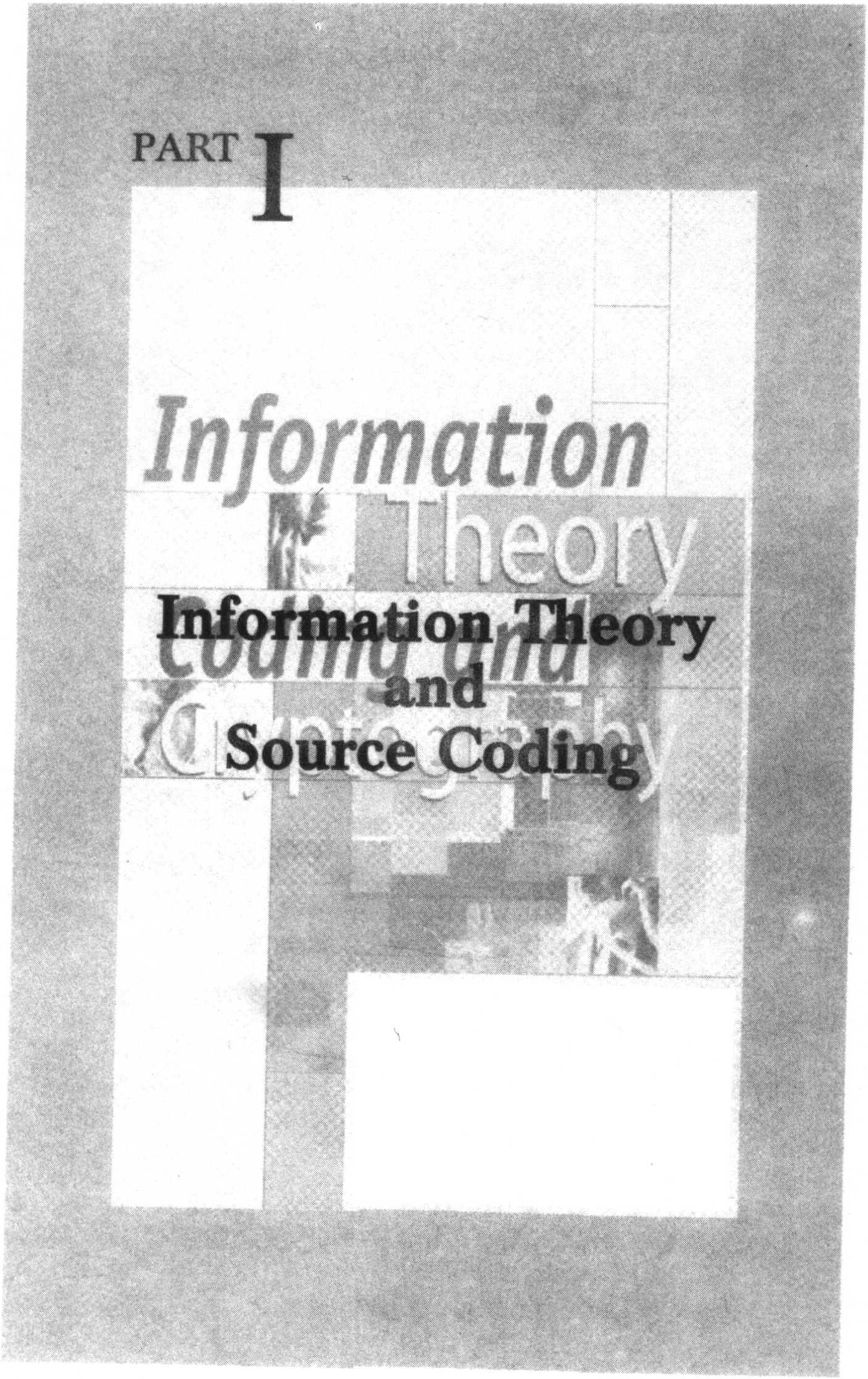
RANJAN BOSE
New Delhi

Contents

Part I
Information Theory and Source Coding

Part II
Error Control Coding
(Channel Coding)

Part III
Coding for Secure Communications



PART I

Information Theory and Source Coding