Information Theory Coding And Cryptography Ranjan Bose

Information Theory, Coding and CryptographyTata McGraw-Hill EducationCryptography, Information Theory, and Error-CorrectionA Handbook for the 21st CenturyJohn Wiley & Sons
This book provides a practical introduction to the theory and practice of coding and information theory for application in the field of electronic communications. It is written at an introductory level and assumes no prior background in coding or information theory. While the mathematical level is detailed, it is still introductory. Through a discussion that balances theory and practical applications and abandons the traditional "theorem-proof" format, this valuable book presents an overview of digital communication systems and the concept of information. It is written in a easy-to-follow conversational style that integrates practical engineering issues through formal and conceptual discussions of mathematical issues. It also makes extensive use of explicit examples that illustrate methods and theory throughout the book. For the professional, it provides an essential hands-on head start for real-world projects and situations. An essential reference for professional engineers in the field of electronic communications.
The National Security Agency funded a conference on Coding theory, Cryp tography, and Number Theory (nick-named Cryptoday) at the United States Naval Academy, on October 25-27, 1998. We were very fortunate to have been able to attract talented mathematicians and cryptographers to the meeting. Unfortunately, some people couldn't make it for either scheduling or funding reasons. Some of these have been invited to contribute a paper anyway. In addition, Prof. William Tutte and Frode Weierud have been kind enough to allow the inclusion of some very interesting unpublished papers of theirs. The papers basically fall into three catagories. Historical papers on cryp tography done during World War II (Hatch, Hilton, Tutte, Ulfving, and Weierud), mathematical papers on more recent methods in cryptography (Cosgrave, Lomonoco, Wardlaw), and mathematical papers in coding theory (Gao, Joyner, Michael, Shokranian, Shokrollahi). A brief biography of the authors follows. - Peter Hilton is a Distinguished Professor of Mathematics Emeritus at the State University of New York at Binghamton. He worked from 1941 to 1945 in the British cryptanalytic headquarters at Bletchley Park. Profes sor Hilton has done extensive research in algebraic topology and group theory. - William Tutte is a Distinguished Professor Emeritus and an Adjunct Pro fessor in the Combinatorics and Optimization Department at the Univer sity of Waterloo. He worked from 1941 to 1945 in the British cryptana lytic headquarters at Bletchley Park. Professor Tutte has done extensive research in the field of combinatorics.
This book aims at presenting the field of Quantum Information Theory in an intuitive, didactic and self-contained way, taking into account several multidisciplinary aspects. Therefore, this books is particularly suited to students and researchers willing to grasp fundamental concepts in Quantum Computation and Quantum Information areas. The field of Quantum Information Theory has increased significantly over the last three decades. Many results from classical information theory were translated and extended to a scenario where quantum effects become important. Most of the results in this area allows for an asymptotically small probability of error to represent and transmit information efficiently. Claude E.Shannon was the first scientist to realize that error-free classical information transmission can be accomplished under certain conditions. More recently, the concept of error-free classical communication was translated to the quantum context. The so-called Quantum Zero-Error Information Theory completes and extends the Shannon Zero-Error Information Theory.
Discover the first unified treatment of today's most essentialinformation technologies— Compressing, Encrypting, andEncoding With identity theft, cybercrime, and digital file sharingproliferating in today's wired world, providing safe and accurateinformation transfers has become a paramount concern. The issuesand problems raised in this endeavor are encompassed within threedisciplines: cryptography, information theory, anderror-correction. As technology continues to develop, these fieldshave converged at a practical level, increasing the need for aunified treatment of these three cornerstones of the informationage. Stressing the interconnections of the disciplines, Cryptography,Information Theory, and Error-Correction offers a complete, yetaccessible account of the technologies shaping the 21st century.This book contains the most up-to-date, detailed, and balancedtreatment available on these subjects. The authors draw on theirexperience both in the classroom and in industry, giving the book'smaterial and presentation a unique real-world orientation. With its reader-friendly style and interdisciplinary emphasis,Cryptography, Information Theory, and Error-Correction serves asboth an admirable teaching text and a tool for self-learning. Thechapter structure allows for anyone with a high school mathematicseducation to gain a strong conceptual understanding, and provideshigher-level students with more mathematically advanced topics. Theauthors clearly map out paths through the book for readers of alllevels to maximize their learning. This book: Is suitable for courses in cryptography, information theory, orerror-correction as well as courses discussing all three areas Provides over 300 example problems with solutions Presents new and exciting algorithms adopted by industry Discusses potential applications in cell biology Details a new characterization of perfect secrecy Features in-depth coverage of linear feedback shift registers(LFSR), a staple of modern computing Follows a layered approach to facilitate discussion, withsummaries followed by more detailed explanations Provides a new perspective on the RSA algorithm Cryptography, Information Theory, and Error-Correction is anexcellent in-depth text for both graduate and undergraduatestudents of mathematics, computer science, and engineering. It isalso an authoritative overview for IT professionals, statisticians,mathematicians, computer scientists, electrical engineers,entrepreneurs, and the generally curious.
The inaugural research program of the Institute for Mathematical Sciences at the National University of Singapore took place from July to December 2001 and was devoted to coding theory and cryptology. As part of the program, tutorials for graduate students and junior researchers were given by world-renowned scholars. These tutorials covered fundamental aspects of coding theory and cryptology and were designed to prepare for original research in these areas. The present volume collects the expanded lecture notes of these tutorials. The topics range from mathematical areas such as computational number theory, exponential sums and algebraic function fields through coding-theory subjects such as extremal problems, quantum error-correcting codes and algebraic-geometry codes to cryptologic subjects such as stream ciphers, public-key infrastructures, key management, authentication schemes and distributed system security.
Various measures of information are discussed in first chapter. Information rate, entropy and mark off models are presented. Second and third chapter deals with source coding. Shannon's encoding algorithm, discrete communication channels, mutual information, Shannon's first theorem are also presented. Huffman coding and Shannon-Fano coding is also discussed. Continuous channels are discussed in fourth chapter. Channel coding theorem and channel capacity theorems are also presented. Block codes are discussed in chapter fifth, sixth and

seventh. Linear block codes, Hamming codes, syndrome decoding is presented in detail. Structure and properties of cyclic codes, encoding and syndrome decoding for cyclic codes is also discussed. Additional cyclic codes such as RS codes, Golay codes, burst error correction is also discussed. Last chapter presents convolutional codes. Time domain, transform domain approach, code tree, code trellis, state diagram, Viterbi decoding is discussed in detail.

Information Theory, Coding & Cryptography has been designed as a comprehensive book for the students of engineering discussing Source Encoding, Error Control Codes & Cryptography. The book contains the recent developments of coded modulation, trellises for codes, turbo coding for reliable data and interleaving. The text balances the mathematical rigor with exhaustive amount of solved, unsolved questions along with a database of MCQs.

This book is intended to introduce coding theory and information theory to undergraduate students of mathematics and computer science. It begins with a review of probablity theory as applied to finite sample spaces and a general introduction to the nature and types of codes. The two subsequent chapters discuss information theory: efficiency of codes, the entropy of information sources, and Shannon's Noiseless Coding Theorem. The remaining three chapters deal with coding theory: communication channels, decoding in the presence of errors, the general theory of linear codes, and such specific codes as Hamming codes, the simplex codes, and many others.

This book presents the benefits of the synergetic effect of the combination of coding and cryptography. It introduces new directions for the interoperability between the components of a communication system. Coding and cryptography are standard components in today’s distributed systems. The integration of cryptography into coding aspects is very interesting, as the usage of cryptography will be common use, even in industrial applications. The book is based on new developments of coding and cryptography, which use real numbers to express reliability values of bits instead of binary values 0 and 1. The presented methods are novel and designed for noisy communication, which doesn ?t allow the successful use of cryptography. The rate of successful verifications is improved essentially not only for standard or “hard” verification, but even more after the introduction of “soft” verification. A security analysis shows the impact on the security. Information security and cryptography follow the late developments of communication theory by changing from “hard” to “soft”, which results in much better results.

Covering topics in algebraic geometry, coding theory, and cryptography, this volume presents interdisciplinary group research completed for the February 2016 conference at the Institute for Pure and Applied Mathematics (IPAM) in cooperation with the Association for Women in Mathematics (AWM). The conference gathered research communities across disciplines to share ideas and problems in their fields and formed small research groups made up of graduate students, postdoctoral researchers, junior faculty, and group leaders who designed and led the projects. Peer reviewed and revised, each of this volume's five papers achieves the conference’s goal of using algebraic geometry to address a problem in either coding theory or cryptography. Proposed variants of the McEliece cryptosystem based on different constructions of codes, constructions of locally recoverable codes from algebraic curves and surfaces, and algebraic approaches to the multicast network coding problem are only some of the topics covered in this volume. Researchers and graduate-level students interested in the interactions between algebraic geometry and both coding theory and cryptography will find this volume valuable.

Basic Concepts in Information Theory and Coding is an outgrowth of a one semester introductory course that has been taught at the University of Southern California since the mid-1960s. Lecture notes from that course have evolved in response to student reaction, new technological and theoretical develop ments, and the insights of faculty members who have taught the course (in cluding the three of us). In presenting this material, we have made it accessible to a broad audience by limiting prerequisites to basic calculus and the ele mentary concepts of discrete probability theory. To keep the material suitable for a one-semester course, we have limited its scope to discrete information theory and a general discussion of coding theory without detailed treatment of algorithms for encoding and decoding for various specific code classes. Readers will find that this book offers an unusually thorough treatment of noiseless self-synchronizing codes, as well as the advantage of problem sections that have been honed by reactions and interactions of several gen erations of bright students, while Agent 00111 provides a context for the discussion of abstract concepts.

Books on information theory and coding have proliferated over the last few years, but few succeed in covering the fundamentals without losing students in mathematical abstraction. Even fewer build the essential theoretical framework when presenting algorithms and implementation details of modern coding systems. Without abandoning the theoret

Developing many of the major, exciting, pre- and post-millennium developments from the ground up, this book is an ideal entry point for graduate students into quantum information theory. Significant attention is given to quantum mechanics for quantum information theory, and careful studies of the important protocols of teleportation, superdense coding, and entanglement distribution are presented. In this new edition, readers can expect to find over 100 pages of new material, including detailed discussions of Bell's theorem, the CHSH game, Tsirelson's theorem, the axiomatic approach to quantum channels, the definition of the diamond norm and its interpretation, and a proof of the Choi–Kraus theorem. Discussion of the importance of the quantum dynamic capacity formula has been completely revised, and many new exercises and references have been added. This new edition will be welcomed by the upcoming generation of quantum information theorists and the already established community of classical information theorists.

Many people do not realise that mathematics provides the foundation for the devices we use to handle information in the modern world. Most of those who do know probably think that the parts of mathematics involvedare quite ‘cl- sical’, such as Fourier analysis and di?erential equations. In fact, a great deal of the mathematical background is part of what used to be called ‘pure’ ma- ematics, indicating that it was created in order to deal with problems that originated within mathematics itself. It has taken many years for mathema- cians to come to terms with this situation, and some of them are still not entirely happy about it. Thisbookisanintegratedintroductionto Coding.Bythis Imeanreplacing symbolic information, such as a sequence of bits or a message written in a naturallanguage,byanother messageusing (possibly) di?erentsymbols.There are three main reasons for doing this: Economy (data compression), Reliability (correction of errors), and Security (cryptography). I have tried to cover each of these three areas in su?cient depth so that the reader can grasp the basic problems and go on to more advanced study. The mathematical theory is introduced in a way that enables the basic problems to bestatedcarefully,butwithoutunnecessaryabstraction.Theprerequisites(sets andfunctions,matrices,?niteprobability)shouldbefamiliartoanyonewhohas taken a standard course in mathematical methods or discrete mathematics. A course in elementary abstract algebra and/or number theory would be helpful, but the book contains the essential facts, and readers without this background should be able to understand what is going on. vi Thereareafewplaceswherereferenceismadetocomputeralgebrasystems.

Although devoted to constructions of good codes for error control, secrecy or data compression, the emphasis is on the first direction. Introduces a number of important classes of error-detecting and error-correcting codes as well as their decoding methods. Background material on modern algebra is presented where required. The role of error-correcting codes in modern cryptography is treated as are data compression and other topics related to information theory. The definition-theorem proof style used in mathematics texts is employed through the book but

formalism is avoided wherever possible.
Conveying ideas in a user-friendly style, this book has been designed for a course in Applied Algebra. The book covers graph algorithms, basic algebraic structures, coding theory and cryptography. It will be most suited for senior undergraduates and beginning graduate students in mathematics and computer science as also to individuals who want to have a knowledge of the below-mentioned topics. Provides a complete discussion on several graph algorithms such as Prims algorithm and Kruskals algorithm for sending a minimum cost spanning tree in a weighted graph, Dijkstras single source shortest path algorithm, Floyds algorithm, Warshalls algorithm, Kuhn-Munkres Algorithm. In addition to DFS and BFS search, several applications of DFS and BFS are also discussed. Presents a good introduction to the basic algebraic structures, namely, matrices, groups, rings, fields including finite fields as also a discussion on vector spaces and linear equations and their solutions. Provides an introduction to linear codes including cyclic codes. Presents a description of private key cryptosystems as also a discussion on public key cryptosystems such as RSA, ElGamal and Miller-Rabin. Finally, the Agrawal-KayalSaxena algorithm (AKS Algorithm) for testing if a given positive integer is prime or not in polynomial time is presented- the first time in a textbook. Two distinguished features of the book are: Illustrative examples have been presented throughout the book to make the readers appreciate the concepts described. Answers to all even-numbered exercises in all the chapters are given.
Thisvolumecontainsrefereedpapersdevotedtocodingandcryptography.These papers arethe full versionsof a selectionof the best extended abstractsaccepted for presentation at the International Workshop on Coding and Cryptography (WCC 2005) held in Bergen, Norway, March 14–18, 2005. Each of the 118 - tended abstracts originallysubmitted to the workshop were reviewed by at least two members of the Program Committee. As a result of this screening process, 58 papers were selected for presentation, of which 52 were eventually presented at the workshop together with four invited talks. The authors of the presented papers were in turn invited to submit full v- sions of their papers to the full proceedings. Each of the full-version submissions were once again thoroughly examined and commented upon by at least two reviewers. This volume is the end result of this long process. I am grateful to the reviewers who contributed to guaranteeing the high standards of this volume, and who are named on the next pages. It was a pl- sure for me to work with my program co-chair Pascale Charpin, whose expe- enced advice I havefurther bene?ted greatly from during the preparationof this ? volume. Discussions with Tor Helleseth and Angela Barbero were also useful in putting the volume together. Finally, I would like to thank all the authors and all the other participants of the WCC 2005 for making it in every sense a highly enjoyable event.
A concise, easy-to-read guide, introducing beginners to the engineering background of modern communication systems, from mobile phones to data storage. Assuming only basic knowledge of high-school mathematics and including many practical examples and exercises to aid understanding, this is ideal for anyone who needs a quick introduction to the subject.
Table of contents
The work introduces the fundamentals concerning the measure of discrete information, the modeling of discrete sources without and with a memory, as well as of channels and coding. The understanding of the theoretical matter is supported by many examples. One particular emphasis is put on the explanation of Genomic Coding. Many examples throughout the book are chosen from this particular area and several parts of the book are devoted to this exciting implication of coding.
This textbook forms an introduction to codes, cryptography and information theory as it has developed since Shannon's original papers.
This book is an evolution from my book A First Course in Information Theory published in 2002 when network coding was still at its infancy. The last few years have witnessed the rapid development of network coding into a research ?eld of its own in information science. With its root in infor- tion theory, network coding has not only brought about a paradigm shift in network communications at large, but also had signi?cant in?uence on such speci?c research ?elds as coding theory, networking, switching, wireless c- munications,distributeddatastorage,cryptography,andoptimizationtheory. While new applications of network coding keep emerging, the fundamental - sults that lay the foundation of the subject are more or less mature. One of the main goals of this book therefore is to present these results in a unifying and coherent manner. While the previous book focused only on information theory for discrete random variables, the current book contains two new chapters on information theory for continuous random variables, namely the chapter on di?erential entropy and the chapter on continuous-valued channels. With these topics included, the book becomes more comprehensive and is more suitable to be used as a textbook for a course in an electrical engineering department.
These are the proceedings of the Conference on Coding Theory, Cryptography, and Number Theory held at the U. S. Naval Academy during October 25-26, 1998. This book concerns elementary and advanced aspects of coding theory and cryptography. The coding theory contributions deal mostly with algebraic coding theory. Some of these papers are expository, whereas others are the result of original research. The emphasis is on geometric Goppa codes (Shokrollahi, Shokranian-Joyner), but there is also a paper on codes arising from combinatorial constructions (Michael). There are both, historical and mathematical papers on cryptography. Several of the contributions on cryptography describe the work done by the British and their allies during World War II to crack the German and Japanese ciphers (Hamer, Hilton, Tutte, Weierud, Urling). Some mathematical aspects of the Enigma rotor machine (Sherman) and more recent research on quantum cryptography (Lomonoco) are described. There are two papers concerned with the RSA cryptosystem and related number-theoretic issues (Wardlaw, Cosgrave).
Algebraic & geometry methods have constituted a basic background and tool for people working on classic block coding theory and cryptography. Nowadays, new paradigms on coding theory and cryptography have arisen such as: Network coding, S-Boxes, APN Functions, Steganography and decoding by linear programming. Again understanding the underlying procedure and symmetry of these topics needs a whole bunch of non trivial knowledge of algebra and geometry that will be used to both, evaluate those methods and search for new codes and cryptographic applications. This book shows those methods in a self-contained form.
Boolean functions are essential to systems for secure and reliable communication. This comprehensive survey of Boolean functions for cryptography and coding covers the whole domain and all important results, building on the author's influential articles with additional topics and recent results. A useful resource for researchers and graduate students, the book balances detailed discussions of properties and parameters with examples of various types of cryptographic attacks that motivate the consideration of these parameters. It provides all the necessary background on mathematics, cryptography, and coding, and an overview on recent applications, such as side channel attacks on smart cards, cloud computing through fully homomorphic encryption, and local pseudo-random generators. The result is a complete and accessible text on the state of the art in single and multiple output Boolean functions that illustrates the interaction between mathematics, computer science, and telecommunications.
Modern introduction to theory of coding and decoding with many exercises and examples.

The fields of Information Theory, Coding and Cryptography are ever expanding, and the last six years have seen a spurt of new ideas germinate, mature and get absorbed in industrial standards and applications. Many of these new concepts* have been included.

Algorithmic Information Theory treats the mathematics of many important areas in digital information processing. It has been written as a read-and-learn book on concrete mathematics, for teachers, students and practitioners in electronic engineering, computer science and mathematics. The presentation is dense, and the examples and exercises are numerous. It is based on lectures on information technology (Data Compaction, Cryptography, Polynomial Coding) for engineers.

This textbook equips graduate students and advanced undergraduates with the necessary theoretical tools for applying algebraic geometry to information theory, and it covers primary applications in coding theory and cryptography. Harald Niederreiter and Chaoping Xing provide the first detailed discussion of the interplay between nonsingular projective curves and algebraic function fields over finite fields. This interplay is fundamental to research in the field today, yet until now no other textbook has featured complete proofs of it. Niederreiter and Xing cover classical applications like algebraic-geometry codes and elliptic-curve cryptosystems as well as material not treated by other books, including function-field codes, digital nets, code-based public-key cryptosystems, and frameproof codes. Combining a systematic development of theory with a broad selection of real-world applications, this is the most comprehensive yet accessible introduction to the field available. Introduces graduate students and advanced undergraduates to the foundations of algebraic geometry for applications to information theory Provides the first detailed discussion of the interplay between projective curves and algebraic function fields over finite fields Includes applications to coding theory and cryptography Covers the latest advances in algebraic-geometry codes Features applications to cryptography not treated in other books

The latest edition of this classic is updated with new problem sets and material The Second Edition of this fundamental textbook maintains the book's tradition of clear, thought-provoking instruction. Readers are provided once again with an instructive mix of mathematics, physics, statistics, and information theory. All the essential topics in information theory are covered in detail, including entropy, data compression, channel capacity, rate distortion, network information theory, and hypothesis testing. The authors provide readers with a solid understanding of the underlying theory and applications. Problem sets and a telegraphic summary at the end of each chapter further assist readers. The historical notes that follow each chapter recap the main points. The Second Edition features: * Chapters reorganized to improve teaching * 200 new problems * New material on source coding, portfolio theory, and feedback capacity * Updated references Now current and enhanced, the Second Edition of Elements of Information Theory remains the ideal textbook for upper-level undergraduate and graduate courses in electrical engineering, statistics, and telecommunications.

Containing data on number theory, encryption schemes, and cyclic codes, this highly successful textbook, proven by the authors in a popular two-quarter course, presents coding theory, construction, encoding, and decoding of specific code families in an "easy-to-use" manner appropriate for students with only a basic background in mathematics offerin

Student edition of the classic text in information and coding theory

This fundamental monograph introduces both the probabilistic and algebraic aspects of information theory and coding. It has evolved from the authors' years of experience teaching at the undergraduate level, including several Cambridge Maths Tripos courses. The book provides relevant background material, a wide range of worked examples and clear solutions to problems from real exam papers. It is a valuable teaching aid for undergraduate and graduate students, or for researchers and engineers who want to grasp the basic principles.

Most coding theory experts date the origin of the subject with the 1948 publication of A Mathematical Theory of Communication by Claude Shannon. Since then, coding theory has grown into a discipline with many practical applications (antennas, networks, memories), requiring various mathematical techniques, from commutative algebra, to semi-definite programming, to algebraic geometry. Most topics covered in the Concise Encyclopedia of Coding Theory are presented in short sections at an introductory level and progress from basic to advanced level, with definitions, examples, and many references. The book is divided into three parts: Part I fundamentals: cyclic codes, skew cyclic codes, quasi-cyclic codes, self-dual codes, codes and designs, codes over rings, convolutional codes, performance bounds Part II families: AG codes, group algebra codes, few-weight codes, Boolean function codes, codes over graphs Part III applications: alternative metrics, algorithmic techniques, interpolation decoding, pseudo-random sequences, lattices, quantum coding, space-time codes, network coding, distributed storage, secret-sharing, and code-based-cryptography. Features Suitable for students and researchers in a wide range of mathematical disciplines Contains many examples and references Most topics take the reader to the frontiers of research