Cryptography Using Chebyshev Polynomials

This book presents the proceedings of International Conference on Emerging Research in Computing, Information, Communication and Applications, ERCICA 2016. ERCICA provides an interdisciplinary forum for researchers, professional engineers and scientists, educators, and technologists to discuss, debate and promote research and technology in the upcoming areas of computing, information, communication and their applications. The book discusses these emerging research areas, providing a valuable resource for researchers and practicing engineers alike.
Survey articles on modern topics related to the work of Harald Niederreiter, written by close colleagues and leading experts.
With the prevalence of digital information, IT professionals have encountered new challenges regarding data security. In an effort to address these challenges and offer solutions for securing digital information, new research on cryptology methods is essential. Multidisciplinary Perspectives in Cryptology and Information Security considers an array of multidisciplinary applications and research developments in the field of cryptology and communication security. This publication offers a comprehensive, in-depth analysis of encryption solutions and will be of particular interest to IT professionals, cryptologists, and researchers in the field.
This book constitutes the refereed post-conference proceedings of the First International Conference on Number-Theoretic Methods in Cryptology, NuTMiC 2017, held in Warsaw, Poland, in September 2017.The 15 revised full papers presented in this book together with 3 invited talks were carefully reviewed and selected from 32 initial submissions. The papers are organized in topical sections on elliptic curves in cryptography; public-key cryptography; lattices in cryptography; number theory; pseudorandomness; and algebraic structures and analysis.
Challenges, Advances, and Analytics
Algorithms—Advances in Research and Application: 2012 Edition
Concepts, Methodologies, Tools, and Applications
5th International Symposium, CSCML 2021, Be'er Sheva, Israel, July 8–9, 2021, Proceedings
Applications and Techniques in Cyber Security and Intelligence
Topics in Polynomials of One and Several Variables and Their Applications
Cyber Security, Cryptology, and Machine Learning
The book discusses the latest developments and outlines future trends in the fields of microelectronics, electromagnetics and telecommunication. It contains original research works presented at the International Conference on Microelectronics, Electromagnetics and Telecommunication (ICMEET 2018), organised by GVP College of Engineering (A), Andhra Pradesh, India. The respective papers were written by scientists, research scholars and practitioners from leading universities, engineering colleges and R&D institutes from all over the world, and share the latest breakthroughs in and promising solutions to the most important issues facing today's society.
The three volume-set LNCS 11476, 11477, and 11478 constitute the thoroughly refereed proceedings of the 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2019,held in Darmstadt, Germany, in May 2019. The 76 full papers presented were carefully reviewed and selected from 327 submissions. The papers are organized into the following topical sections: ABE and CCA security; succinct arguments and secure messaging; obfuscation; block ciphers; differential privacy; bounds for symmetric cryptography; non-malleability; blockchain and consensus; homomorphic primitives; standards; searchable encryption and ORAM; proofs of work and space; secure computation; quantum, secure computation and NIZK, lattice-based cryptography; foundations; efficient secure computation; signatures; information-theoretic cryptography; and cryptanalysis.
This book constitutes the refereed proceedings of 5 workshops held at the 21st International Conference on Financial Cryptography and Data Security, FC 2017, in Sliema, Malta, in April 2017.The 39 full papers presented were carefully reviewed and selected from 96 submissions. They feature the outcome of the 5th Workshop on Encrypted Computing and Applied Homomorphic Cryptography, WAHC 2017, the 4th Workshop on Bitcoin and Blockchain Research, BITCOIN 2017, the Second Workshop on Secure Voting Systems, VOTING 2017, the First Workshop on Trusted Smart Contracts, WTSC 2017, and the First Workshop on Targeted Attacks, TA 2017.The papers are grouped in topical sections named: encrypted computing and applied homomorphic cryptography; bitcoin and blockchain research; advances in secure electronic voting schemes; trusted smart contracts; targeted attacks.
This volume of Smart Innovation, Systems and Technologies contains accepted papers presented in IIH-MSP-2016, the 12th International Conference on Intelligent Information Hiding and Multimedia Signal Processing. The conference this year was technically co-sponsored by Tainan Chapter of IEEE Signal Processing Society, Fujian University of Technology, Chaoyang University of Technology, Taiwan Association for Web Intelligence Consortium, Fujian Provincial Key Laboratory of Big Data Mining and Applications (Fujian University of Technology), and Harbin Institute of Technology Shenzhen Graduate School. IIH-MSP 2016 is held in 21-23, November, 2016 in Kaohsiung, Taiwan. The conference is an international forum for the researchers and professionals in all areas of information hiding and multimedia signal processing.
Network and Parallel Computing
Proceedings of the 11th Joint International Computer Conference
International Conference on Applications and Techniques in Cyber Security and Intelligence ATCI 2018
Applied Algebra and Number Theory
Fog Computing for Healthcare 4.0 Environments
Proceeding of the Twelfth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Nov., 21-23, 2016, Kaohsiung, Taiwan, Volume 1
Text, Speech, and Dialogue

This book constitutes the refereed proceedings of the 5th International Symposium on Cyber Security Cryptography and Machine Learning, CSCML 2021, held in Be'er Sheva, Israel, in July 2021. The 22 full and 13 short papers presented together with a keynote paper in this volume were carefully reviewed and selected from 48 submissions. They deal with the theory, design, analysis, implementation, or application of cyber security, cryptography and machine learning systems and networks, and conceptually innovative topics in these research areas.
This book constitutes the refereed proceedings of the IFIP International Conference on Network and Parallel Computing, NPC 2007. It covers network applications: cluster and grid computing, peer-to-peer computing; network technologies: network algorithms, network reliability and dependability; network and parallel architectures: multicore design issues, performance modeling and evaluation; and parallel and distributed software: data mining, parallel programming tools and compilers.
This book summarizes recent inventions, provides guidelines and recommendations, and demonstrates many practical applications of homomorphic encryption. This collection of papers represents the combined wisdom of the community of leading experts on homomorphic encryption. In the past 3 years, a global community consisting of researchers in academia, industry, and government, has been working closely to standardize homomorphic encryption. This is the first publication of whitepapers created by these experts that comprehensively describes the scientific inventions, presents a concrete security analysis, and broadly discusses applicable use scenarios and markets. This book also features a collection of privacy-preserving machine learning applications powered by homomorphic encryption designed by groups of top graduate students worldwide at the Private AI Bootcamp hosted by Microsoft Research. The volume aims to connect non-expert readers with this important new cryptographic technology in an accessible and actionable way. Readers who have heard good things about homomorphic encryption but are not familiar with the details will find this book full of inspiration. Readers who have preconceived biases based on out-of-date knowledge will see the recent progress made by industrial and academic pioneers on optimizing and standardizing this technology. A clear picture of how homomorphic encryption works, how to use it to solve real-world problems, and how to efficiently strengthen privacy protection, will naturally become clear.
Cyber security is the protection of information systems, hardware, software, and information as well from theft, damages, interruption or misdirection to any of these resources. In other words, cyber security focuses on protecting computers, networks, programs and data (in use, in rest, in motion) from unauthorized or unintended access, change or destruction. Therefore, strengthening the security and resilience of cyberspace has become a vital homeland security mission. Cyber security attacks are growing exponentially. Security specialists must occupy in the lab, concocting new schemes to preserve the resources and to control any new attacks. Therefore, there are various emerging algorithms and techniques viz. DES, AES, IDEA, WAKE, CAST5, Serpent Algorithm, Chaos-Based Cryptography McEliece, Niederreiter, NTRU, Goldreich-Goldwasser-Halevi, Identity Based Encryption, and Attribute Based Encryption. There are numerous applications of security algorithms like cyber security, web security, e-commerce, database security, smart card technology, mobile security, cloud security, digital signature, etc. The book offers comprehensive coverage of the most essential topics, including: Modular Arithmetic, Finite Fields Prime Number, DLP, Integer Factorization Problem Symmetric Cryptography Asymmetric Cryptography Post-Quantum Cryptography Identity Based Encryption Attribute Based Encryption Key Management Entity Authentication, Message Authentication Digital Signatures Hands-On "SageMath" This book serves as a textbook/reference book for UG, PG, PhD students, Teachers, Researchers and Engineers in the disciplines of Information Technology, Computer Science and Engineering, and Electronics and Communication Engineering.
Agent and Multi-Agent Systems: Technologies and Applications
FC 2017 International Workshops, WAHC, BITCOIN, VOTING, WTSC, and TA, Sliema, Malta, April 7, 2017, Revised Selected Papers
Emerging Research in Computing, Information, Communication and Applications
Volume Dedicated to the Memory of P.L. Chebyshev (1821-1894)
Number-Theoretic Methods in Cryptology
21st International Conference, TSD 2018, Brno, Czech Republic, September 11-14, 2018, Proceedings
Technical, Societal, and Future Implications

This book contains the proceedings of EUROCRYPT 85, held in Paris in 1984, April 9-11, at the University of Paris, Sorbonne. EIJROCRYPT is now an annual international European meeting in cryptology, intended primarily for the international of researchers in this area. EUROCRYPT 84 was community following previous meetings held at Burg Feuerstein in 1982 and at IJdine in 1983. In fact EUROCRYPT 84 was thc first such meeting being organized under IXCR (International Association of Cryptology Research). Other sponsors were the well-known French association on cybernetics research AFCET, the LITP (Laborstoire d' Informntique thcorique called et de Programmation), which is a laboratory of computer science associated with CNRS, and the department of mathematics and computer science at the Ilniversity RenE Descartcs, Sorbonne. EUROCRYPT 83 was very successfull, with about 180 participants from a great variety of foreign countries and 50 papers addressing all aspects of cryptology, close to applied as well as theoretical. It also had a special feature, i.e. a special session on smart cards particularly welcome at the time, since France was then carrying on an ambitious program on smart cards. EUROCRYPT 84 was a great experience. We like to thank all the sponsors and all the authors for their submission of papers. Pakin, December 74ti4. CONTENTS SECTION I: GENERAL THEORY, CLASSICAL METHODS 3 Cryptology and Complexity Theories ... G. RLiGGTU 1 0 On Cryptosystems based on Folynomials md I'inite Fields.. ... R. irvi 16 Algehraical Structures of Cryptographic lransformations.. ...
The book highlights innovative ideas, cutting-edge findings, and novel techniques, methods and applications touching on all aspects of technology and intelligence in smart city management and services. Above all, it explores developments and applications that are of practical use and value for Cyber Intelligence-related methods, which are frequently used in the context of city management and services.
This book provides an analysis of the role of fog computing, cloud computing, and Internet of Things in providing uninterrupted context-aware services as they relate to Healthcare 4.0. The book considers a three-layer patient-driven healthcare architecture for real-time data collection, processing, and transmission. It gives insight to the readers for the applicability of fog devices and gateways in Healthcare 4.0 environments for current and future applications. It also considers aspects required to manage the complexity of fog computing for Healthcare 4.0 and also develops a comprehensive taxonomy.
Chaos-based cryptography, attracting many researchers in the past decade, is a research field across two fields, i.e., chaos (nonlinear dynamic system) and cryptography (computer and data security). It Chaos' properties, such as randomness and ergodicity, have been proved to be suitable for designing the means for data protection. The book gives a thorough description of chaos-based cryptography, which consists of chaos basic theory, chaos properties suitable for cryptography, chaos-based cryptographic techniques, and various secure applications based on chaos. Additionally, it covers both the latest research results and some open issues or hot topics. The book creates a collection of high-quality chapters contributed by leading experts in the related fields. It embraces a wide variety of aspects of the related subject areas and provide a scientifically and scholarly sound treatment of state-of-the-art techniques to students, researchers, academics, personnel of law enforcement and IT practitioners who are interested or involved in the study, research, use, design and development of techniques related to chaos-based cryptography.
Proceedings of the 2014 International Conference on Control Engineering and Information Systems (ICCEIS 2014, Yueyang, Hunan, China, 20-22 June 2014).
Entropy in Image Analysis
Chaos-based Cryptography
8th International Conference, GPC 2013, and Colocated Workshops, Seoul, Korea, May 9-11, 2013, Proceedings
Mathematics Applied to Engineering, Modelling, and Social Issues
Algorithmic Strategies for Solving Complex Problems in Cryptography
Control Engineering and Information Systems

Algorithms—Advances in Research and Application: 2012 Edition is a ScholarlyEditions™ eBook that delivers timely, authoritative, and comprehensive information about Algorithms. The editors have built Algorithms—Advances in Research and Application: 2012 Edition on the vast information databases of ScholarlyNews.™ You can expect the information about Algorithms in this eBook to be deeper than what you can access anywhere else, as well as consistently reliable, authoritative, informed, and relevant. The content of Algorithms—Advances in Research and Application: 2012 Edition has been produced by the world's leading scientists, engineers, analysts, research institutions, and companies. All of the content is from peer-reviewed sources, and all of it is written, assembled, and edited by the editors at ScholarlyEditions™ and available exclusively from us. You now have a source you can cite with authority, confidence, and credibility. More information is available at http://www.ScholarlyEditions.com/.
This volume presents an account of some of the most important work that has been done on various research problems in the theory of polynomials of one and several variables and their applications. It is dedicated to P L Chebyshev, a leading Russian mathematician.
Following from the very successful First KES Symposium on Agent and Multi-Agent Systems – Technologies and Applications (KES-AMSTA 2007), held in Wroclaw, Poland, 31 May–1 June 2007, the second event in the KES-AMSTA symposium series (KES-AMSTA 2008) was held in Incheon, Korea, March 26–28, 2008. The symposium was organized by the School of Computer and Information Engineering, Inha University, KES International and the KES Focus Group on Agent and Mul- agent Systems. The KES-AMSTA Symposium Series is a sub-series of the KES Conference Series. The aim of the symposium was to provide an international forum for scientific research into the technologies and applications of agent and multi-agent systems. Agent and multi-agent systems are related to the modern software which has long been recognized as a promising technology for constructing autonomous, complex and intelligent systems. A key development in the field of agent and multi-agent systems has been the specification of agent communication languages and formalization of ontologies. Agent communication languages are intended to provide standard declarative mechanisms for agents to communicate knowledge and make requests of each other, whereas ontologies are intended for conceptualization of the knowledge domain. The symposium attracted a very large number of scientists and practitioners who submitted their papers for nine main tracks concerning the methodology and applications of agent and multi-agent systems, a doctoral track and two special sessions.
This book constitutes the refereed proceedings of the Cryptographer's Track at the RSA Conference 2020, CT-RSA 2020, held in San Francisco, CA, USA, in February 2020. The 28 papers presented in this volume were carefully reviewed and selected from 95 submissions. CT-RSA is the track devoted to scientific papers on cryptography, public-key to symmetric-key cryptography and from crypto-graphic protocols to primitives and their implementation security.
18th International Conference, EANN 2017, Athens, Greece, August 25–27, 2017, Proceedings
Multidisciplinary Perspectives in Cryptology and Information Security
40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17–21, 2021, Proceedings, Part I
IFIP International Conference, NPC 2007, Dalian, China, September 18-21, 2007, Proceedings
Advances in Cryptology
Advances in Cryptology – EUROCRYPT 2021
Microelectronics, Electromagnetics and Telecommunications

The proceedings of the 4th International Conference on Frontiers in Intelligent Computing: Theory and Applications 2015 (FICTA 2015) serves as the knowledge centre not only for scientists and researchers in the field of intelligent computing but also for students of post-graduate level in various engineering disciplines. The book covers a comprehensive overview of the theory, methods, applications and tools of Intelligent Computing. Researchers are now working in interdisciplinary areas and the proceedings of FICTA 2015 plays a major role to accumulate those significant works in one arena. The chapters included in the proceedings inculcates both theoretical as well as practical aspects of different areas like Nature Inspired Algorithms, Fuzzy Systems, Data Mining, Signal Processing, Image processing, Text Processing, Wireless Sensor Networks, Network Security and Cellular Automata.
Cryptography is a field that is constantly advancing, due to exponential growth in new technologies within the past few decades. Applying strategic algorithms to cryptic issues can help save time and energy in solving the expanding problems within this field. Algorithmic Strategies for Solving Complex Problems in Cryptography is an essential reference source that discusses the evolution and current trends in cryptology, and it offers new insight into how to use strategic algorithms to aid in solving intricate difficulties within this domain. Featuring relevant topics such as hash functions, homomorphic encryption schemes, two party computation, and integer factoring, this publication is ideal for academicians, graduate students, engineers, professionals, and researchers interested in expanding their knowledge of current trends and techniques within the cryptology field.
Combinatorics and finite fields are of great importance in modern applications such as in the analysis of algorithms, in information and communication theory, and in signal processing and coding theory. This book contains survey articles on topics such as difference sets, polynomials, and pseudorandomness.
At the code level, discrete-time chaotic systems can be used to generate spreading codes for DS-SS systems. At the signal level, continuous-time chaotic systems can be used to generate wideband carriers for digital modulation schemes. The potential of chaos engineering is now recognized worldwide, with research groups actively pursuing the exploitation of chaotic phenomena in cryptography, spread spectrum communications, electromagnetic interference reduction, and many other applications. Although some noteworthy results have already been achieved, until now, the field has lacked both a systematic treatment of these developments and a careful, quantitative comparison of chaos-based and conventional techniques. Chaotic Electronics in Telecommunications fills both of those needs. It addresses the use of chaos in digital communications applications, from the coding level to circuit design. Each chapter offers a formal exposition of the theoretical and engineering tools needed to apply chaos, followed by discussion of the algorithms and circuits needed to apply the theory to real-world communications systems.
Third International Symposium, UNet 2017, Casablanca, Morocco, May 9-12, 2017, Revised Selected Papers
Grid and Pervasive Computing
ERCICA 2016
2011 International Conference in Electrics, Communication and Automatic Control Proceedings

Difference Sets, Polynomials, Pseudorandomness and Applications
JICC 2005
This volume constitutes the refereed proceedings of the 27th Annual International Cryptology Conference held in Santa Barbara, California, in August 2007. Thirty-three full papers are presented along with one important invited lecture. The papers address current foundational, theoretical, and research aspects of cryptology, cryptography, and cryptanalysis. In addition, readers will discover many advanced and emerging applications.
This book constitutes the refereed proceedings of the 13th International Conference on Security, Privacy, and Anonymity in Computation, Communication, and Storage, SpaCCS 2020, held in Nanjing, China, in December 2020. The 30 full papers were carefully reviewed and selected from 88 submissions. The papers cover many dimensions including security algorithms and architectures, privacy-aware policies, regulations and techniques, anonymous computation and communication, encompassing fundamental theoretical approaches, practical experimental projects, and commercial application systems for computation, communication and storage. SpaCCS 2020 is held jointly with the 11th International Workshop on Trust, Security and Privacy for Big Data (TrustData 2020), the 10th International Symposium on Trust, Security and Privacy for Emerging Applications (TSP 2020), the 9th International Symposium on Security and Privacy on Internet of Things (SPIoT 2020), the 6th International Symposium on Sensor-Cloud Systems (SCS 2020), the 2nd International Workshop on Communication, Computing, Informatics and Security (CCIS 2020), the First International Workshop on Intelligence and Security in Next Generation Networks (ISNGN 2020), the First International Symposium on Emerging Information Security and Applications (EISA 2020).
Organizations, governments, and corporations are all concerned with distributing their goods and services to those who need them most, consequently benefiting in the process. Only by carefully considering the interrelated nature of social systems can organizations achieve the success they strive for. Economics: Concepts, Methodolgies, Tools, and Applications explores the interactions between market agents and their impact on global prosperity. Incorporating both theoretical background and advanced concepts in the discipline, this multi-volume reference is intended for policymakers, economists, business leaders, governmental and non-governmental organizations, and students of economic theory.
This book constitutes the refereed proceedings of the Third International Symposium on Ubiquitous Networking, UNet 2017, held in Casablanca, Morocco, in May 2017. The 56 full papers presented in this volume were carefully reviewed and selected from 127 submissions. They were organized in topical sections named: context-awareness and autonomy paradigms; mobile edge networking and virtualization; ubiquitous internet of things: emerging technologies and breakthroughs; and enablers, challenges and applications.
38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19–23, 2019, Proceedings, Part II
Cryptography and Lattices
Combinatorics and Finite Fields
Advances in Cryptology - CRYPTO 2007
Proceedings of EUROCRYPT 84. A Workshop on the Theory and Application of Cryptographic Techniques - Paris, France, April 9-11, 1984
Engineering Applications of Neural Networks
Proceedings of the 4th International Conference on Frontiers in Intelligent Computing: Theory and Applications (FICTA) 2015

This book constitutes the refereed proceedings of the 8th International Conference on Grid and Pervasive Computing, GPC 2013, held in Seoul, Korea, in May 2013 and the following colocated workshops: International Workshop on Ubiquitous and Multimedia Application Systems, UMAS 2013; International Workshop DATICS-GPC 2013: Design, Analysis and Tools for Integrated Circuits and Systems; and International Workshop on Future Science Technologies and Applications, FSTA 2013. The 111 revised papers were carefully reviewed and selected from numerous submissions. They have been organized in the following topical sections: cloud, cluster and grid; middleware resource management; mobile peer-to-peer and pervasive computing; multi-core and high-performance computing; parallel and distributed systems; security and privacy; ubiquitous communications, sensor networking, and RFID; ubiquitous and multimedia application systems; design, analysis and tools for integrated circuits and systems; future science technologies and applications; and green and human information technology.
This book constitutes the refereed proceedings of the 6th International Symposium on Cyber Security Cryptography and Machine Learning, CSCML 2022, held in Be'er Sheva, Israel, in June - July 2022. The 24 full and 11 short papers presented together with a keynote paper in this volume were carefully reviewed and selected from 53 submissions. They deal with the theory, design, analysis, implementation, or application of cyber security, cryptography and machine learning systems and networks, and conceptually innovative topics in these research areas.
2011 International Conference in Electrics, Communication and Automatic Control Proceedings examines state-of-art and advances in Electrics, Communication and Automatic Control. This book presents developments in Power Conversion, Signal and image processing, Image & video Signal Processing. The conference brings together researchers, engineers, academic as well as industrial professionals from all over the world to promote the developments of Electrics, Communication and Automatic Control.
Control Engineering and Information Systems contains the papers presented at the 2014 International Conference on Control Engineering and Information Systems (ICCEIS 2014, Yueyang, Hunan, China, 20-22 June 2014). All major aspects of the theory and applications of control engineering and information systems are addressed, including: – Intelligent systems – Teaching cases – Pattern recognition – Industry application – Machine learning – Systems science and systems engineering – Data mining – Optimization – Business process management – Evolution of public sector ICT – IS economics – IS security and privacy – Personal data markets – Wireless ad hoc and sensor networks – Database and system security – Application of spatial information system – Other related areas Control Engineering and Information Systems provides a valuable source of information for scholars, researchers and academics in control engineering and information systems.
Security, Privacy, and Anonymity in Computation, Communication, and Storage
Financial Cryptography and Data Security
Chaotic Electronics in Telecommunications
Theory, Algorithms and Applications
13th International Conference, SpaCCS 2020, Nanjing, China, December 18-20, 2020, Proceedings
Economics: Concepts, Methodologies, Tools, and Applications

Most of the devices in the Internet of Things will be battery powered sensor devices. All the operations done on battery powered devices require minimum computation. Secure algorithms like RSA become useless in the Internet of Things environment. Elliptic curve based cryptography emerges as a best solution for this problem because it provides higher security in smaller key size compare to RSA. This book focuses on the use of Elliptic Curve Cryptography with different authentication architectures and authentication schemes using various security algorithms. It also includes a review of the math required for security and understanding Elliptic Curve Cryptography.
This book constitutes the refereed proceedings of the 18th International Conference on Engineering Applications of Neural Networks, EANN 2017, held in Athens, Greece, in August 2017. The 40 revised full papers and 5 revised short papers presented were carefully reviewed and selected from 83 submissions. The papers cover the topics of deep learning, convolutional neural networks, image processing, pattern recognition, recommendation systems, machine learning, and applications of Artificial Neural Networks (ANN) applications in engineering, 5G telecommunication networks, and audio signal processing. The volume also includes papers presented at the 6th Mining Humanistic Data Workshop (MHDW 2017) and the 2nd Workshop on 5G-Putting Intelligence to the Network Edge (5G-PINE).
This book constitutes the thoroughly refereed post-proceedings of the International Conference on Cryptography and Lattices, CaLC 2001, held in Providence, RI, USA in March 2001. The 14 revised full papers presented together with an overview paper were carefully reviewed and selected for inclusion in the book. All current aspects of lattices and lattice reduction in cryptography, both for cryptographic construction and cryptographic analysis, are addressed.
This book presents several aspects of research on mathematics that have significant applications in engineering, modelling and social matters, discussing a number of current and future social issues and problems in which mathematical tools can be beneficial. Each chapter enhances our understanding of the research problems in a particular an area of study and highlights the latest advances made in that area. The self-contained contributions make the results and problems discussed accessible to readers, and provides references to enable those interested to follow subsequent studies in still developing fields. Presenting real-world applications, the book is a valuable resource for graduate students, researchers and educators. It appeals to general readers curious about the practical applications of mathematics in diverse scientific areas and social problems.
Topics in Cryptology – CT-RSA 2020
Emerging Security Algorithms and Techniques
Advances in Intelligent Information Hiding and Multimedia Signal Processing
6th International Symposium, CSCML 2022, Be'er Sheva, Israel, June 30 – July 1, 2022, Proceedings
International Conference, CaLC 2001, Providence, RI, USA, March 29-30, 2001. Revised Papers
Ubiquitous Networking
Advances in Cryptology – EUROCRYPT 2019

Image analysis is a fundamental task for extracting information from images acquired across a range of different devices. Since reliable quantitative results are requested, image analysis requires highly sophisticated numerical and analytical methods—particularly for applications in medicine, security, and remote sensing, where the results of the processing may consist of vitally important data. The contributions to this book provide a good overview of the most important demands and solutions concerning this research area. In particular, the reader will find image analysis applied for feature extraction, encryption and decryption of data, color segmentation, and in the support new technologies. In all the contributions, entropy plays a pivotal role.
This book constitutes the refereed proceedings of the 21st International Conference on Text, Speech, and Dialogue, TSD 2018, held in Brno, Czech Republic, in September 2018. The 56 regular papers were carefully reviewed and selected from numerous submissions. They focus on topics such as corpora and language resources, speech recognition, tagging, classification and parsing of text and speech, speech and spoken language generation, semantic processing of text and search, integrating applications of text and speech processing, machine translation, automatic dialogue systems, multimodal techniques and modeling.
The 3-volume-set LNCS 12696 – 12698 constitutes the refereed proceedings of the 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Eurocrypt 2021, which was held in Zagreb, Croatia, during October 17–21, 2021. The 78 full papers included in these proceedings were accepted from a total of 400 submissions. They were organized in topical sections as follows: Part I: Best papers; public-key cryptography; isogenies; post-quantum cryptography; lattices; homomorphic encryption; symmetric cryptanalysis; Part II: Symmetric designs; real-world cryptanalysis; implementation issues; masking and secret-sharing; leakage, faults and tampering; quantum constructions and proofs; multiparty computation; Part III: Garbled circuits; indistinguishability obfuscation; non-malleable commitments; zero-knowledge proofs; property-preserving hash functions and ORAM; blockchain; privacy and law enforcement.
Advances in Cryptology – CRYPTO 200727th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19–23, 2007, ProceedingsSpringer
First International Conference, NuTMiC 2017, Warsaw, Poland, September 11–13, 2017, Revised Selected Papers
Second KES International Symposium, KES-AMSTA 2008, Incheon, Korea, March 26–28, 2008, Proceedings
Internet of Things Security
The Cryptographers' Track at the RSA Conference 2020, San Francisco, CA, USA, February 24–28, 2020, Proceedings
Protecting Privacy Through Homomorphic Encryption
Cyber Security Cryptography and Machine Learning
Proceedings of the Fourth ICMEET 2018