Cryptography Using Chebyshev Polynomials

This book constitutes the refereed proceedings of the 31st Annual International Cryptology Conference, CRYPTO 2011, held in Santa Barbara, CA, USA in August 2011. The 42 revised full papers presented were carefully reviewed and selected from 230 submissions. The volume also contains the abstract of one invited talk. The papers are organized in topical sections on randomness and its use; computer-assisted cryptographic proofs; outsourcing and delegatin computation; symmetric cryptanalysis and constructions; secure computation: leakage and side channels; quantum cryptography; lattices and knapsacks; public-key encryption; symmetric schemes; signatures; obilvious transfer and secret sharing; and multivariate and coding-based schemes.

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 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.

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.

This book constitutes the refereed proceedings of the 30th IFIP TC 11 International Information Security and Privacy Conference, SEC 2015, held in Hamburg, Germany, in May 2015. The 42 revised full papers presented were carefully reviewed and selected from 212 submissions. The papers are organized in topical sections on privacy, web security, access control, trust and identity management, network security, security management and human aspects of security, software security, applied cryptography, mobile and cloud services security, and cyber-physical systems and critical infrastructures security.

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.

An international community of researchers is now flourishing in the area of cryptology-there was none half-a-dozen years ago. The intrinsic fascination of the field certainly is part of the explanation. Another factor may be that many sense the importance and potential consequences of this work, as we move into the information age. I believe that the various meetings devoted to cryptology over the past few years have contributed quite significantly to the formation of this community, by allowing those in the field to get to know each other and by providing for rapid exchange of ideas. CRYPTO 83 was once again truly the cryptologic event of the year. Many of the most active participants continue to attend each year, and attendance continues to grow at a healthy rate. The informal and collegial atmosphere and the beach side setting which contribute to the popularity of the event were again supported by flawless weather. The absence of parallel sessions seemed to provide a welcome opportunity to keep abreast of developments in the various areas of activity. Each session of the meeting organized by the program committee is repre sented by a section in the present volume. The papers were accepted by the program committee based on abstracts, and appear here without having been otherwise refereed. The last section contains papers presented at the informal rump session. A keyword index and an author index to the papers is provided at the end of the volume.

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.

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.

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.

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.

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.

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.

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.

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 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.

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.

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 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 reports on the latest research and developments in the field of cybersecurity, placing special emphasis on personal security and new methods for reducing human error and increasing cyber awareness, as well as innovative solutions for increasing the security of advanced Information Technology (IT) infrastructures. It covers a broad range of topics, including methods for human training; novel Cyber-Physical and Process-Control Systems; social, economic, and behavioral aspects of cyberspace; issues concerning the cybersecurity index; security metrics for enterprises; risk evaluation, and many others. Based on the AHFE 2017 International Conference on Human Factors in Cybersecurity, held on July 17–21, 2017, in Los Angeles, California, USA, the book not only presents innovative cybersecurity technologies, but also discusses emerging threats, current gaps in the available systems, and future challenges that may be successfully overcome with the help of human factors research.

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.

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.

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 volume contains the proceedings of the 12th conference on Arithmetic, Geometry, cryptography and coding Theory, held in Marseille, France from March 30 to April 3, 2009, as well as the first Geocrypt conference, held in pointe-a-pitre, guadeloupe, from April 27 to may 1, 2009, and the European science Foundation exploratory workshop on curves, coding Theory, and Cryptography, held in Marseille, France from March 25 to 29, 2009. The articles Contained in this volume come from three related symposia organized by the group

Arithmetique et Theorie de I' Information in Marseille. The topics cover arithmetic properties of curves and higher dimensional varieties with applications to codes and cryptography.

This book constitutes the thoroughly refereed post-conference proceedings of the 22nd International Conference on Financial Cryptography and Data Security, FC 2018, held in Nieuwport, Curaçao, in February/ March 2018. The 27 revised full papers and 2 short papers were carefully selected and reviewed from 110 submissions. The papers are grouped in the following topical sections: Financial Cryptography and Data Security, Applied Cryptography, Mobile Systems Security and Privacy, Risk Assessment and Management, Social Networks Security and Privacy and much more.

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, Decemben 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.. ...

This book presents recent developments in nonlinear dynamics with an emphasis on complex systems. The volume illustrates new methods to characterize the solutions of nonlinear dynamics associated with complex systems. This book contains the following topics: new solutions of the functional equations, optimization algorithm for traveling salesman problem, fractals, control, fractional calculus models, fractional discretization, local fractional partial differential equations and their applications, and solutions of fractional kinetic equations.

Advances in Cryptology - CRYPTO 200727th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2007, ProceedingsSpringer

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.

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.

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.

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.

At its core, information security deals with the secure and accurate transfer of information. While information security has long been important, it was, perhaps, brought more clearly into mainstream focus with the so-called “Y2K” issue. Te Y2K scare was the fear that c- puter networks and the systems that are controlled or operated by sofware would fail with the turn of the millennium, since their clocks could lose synchronization by not recognizing a number (instruction) with three zeros. A positive outcome of this scare was the creation of several

Computer Emergency Response Teams (CERTs) around the world that now work - operatively to exchange expertise and information, and to coordinate in case major problems should arise in the modern IT environment. Te terrorist attacks of 11 September 2001 raised security concerns to a new level. Te - ternational community responded on at least two fronts; one front being the transfer of reliable information via secure networks and the other being the collection of information about - tential terrorists. As a sign of this new emphasis on security, since 2001, all major academic publishers have started technical journals focused on security, and every major communi- tions conference (for example, Globecom and ICC) has organized workshops and sessions on security issues. In addition, the IEEE has created a technical committee on Communication and Information Security. Te ?rst editor was intimately involved with security for the Athens Olympic Games of 2004.

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.

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.

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 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.