Read Book Hyderaba India In Cryptology On Conference International Third 2002 Indocrypt Cryptology In Progress

Thank you very much for downloading **Hyderaba India In Cryptology On Conference International Third 2002 Indocrypt Cryptology In Progress**. Maybe you have knowledge that, people have search numerous times for their chosen books like this Hyderaba India In Cryptology On Conference International Third 2002 Indocrypt Cryptology In Progress, but end up in infectious downloads.
Rather than reading a good book with a cup of tea in the afternoon, instead they are facing with some infectious bugs inside their desktop computer.

Hyderaba India In Cryptology On Conference International Third 2002 Indocrypt Cryptology In Progress is available in our digital library an online access to it is set as public so you can download it instantly.
Our book servers saves in multiple countries, allowing you to get the most less latency time to download any of our books like this one.
Kindly say, the Hyderaba India In Cryptology On Conference International Third 2002 Indocrypt Cryptology In Progress is universally compatible with any devices to read

KEY=IN - ERICKSON FOLEY

PROGRESS IN CRYPTOLOGY – INDOCRYPT 2019

20TH INTERNATIONAL CONFERENCE ON CRYPTOLOGY IN INDIA, HYDERABAD, INDIA, DECEMBER 15–18, 2019, PROCEEDINGS

Springer This book constitutes the refereed proceedings of the 20th International Conference on Cryptology in India, INDOCRYPT 2019, held in Hyderabad, India, in December 2019. The 28 revised full papers presented in this book were carefully reviewed and selected from 110 submissions (of which 20 were either rejected without being reviewed or withdrawn before the deadline). The focus of the conference includes works on signatures and filter permutators; symmetric key ciphers and hash functions; blockchain, secure computation and blind coupon mechanism; oblivious transfer, obfuscation and privacy amplification; Boolean functions, elliptic curves and lattices; algorithms, attacks and distribution; and efficiency, side-channel resistance and PUFs.

PROGRESS IN CRYPTOLOGY -- INDOCRYPT 2019

20TH INTERNATIONAL CONFERENCE ON CRYPTOLOGY IN INDIA, HYDERABAD, INDIA, DECEMBER 15-18, 2019, PROCEEDINGS

This book constitutes the refereed proceedings of the 20th International Conference on Cryptology in India, INDOCRYPT 2019, held in Hyderabad, India, in December 2019. The 28 revised full papers presented in this book were carefully reviewed and selected from 110 submissions (of which 20 were either rejected without being reviewed or withdrawn before the deadline). The focus of the conference includes works on signatures and filter permutators; symmetric key ciphers and hash functions; blockchain, secure computation and blind coupon mechanism; oblivious transfer, obfuscation and privacy amplification; Boolean functions, elliptic curves and lattices; algorithms, attacks and distribution; and efficiency, side-channel resistance and PUFs.

PROGRESS IN CRYPTOLOGY - INDOCRYPT 2002

THIRD INTERNATIONAL CONFERENCE ON CRYPTOLOGY IN INDIA HYDERABAD, INDIA, DECEMBER 16-18, 2002

Springer The third successful completion of the INDOCRYPT conference series marks the acceptance of the series by the international research community as a forum for presenting high-quality research.It also marks the coming of age of cryptology research in India. The authors for the submitted papers were spread across 21 countries and 4 continents, which goes a long way to demonstrate the international interest and visibility of INDOCRYPT.In the previous two conferences, the submissions from India originated from only two institutes; this increased to six for the 2002 conference.Thus INDOCRYPT is well set on the path to achieving two main ob jectives – to provide an international platform for presenting high-quality research and to stimulate cryptology research in India. The opportunity to serve as a program co-chair for the third INDOCRYPT carries a special satisfaction for the second editor.Way back in 1998, the sci- ti?c analysis group of DRDO organized a National Seminar on Cryptology and abbreviated it as NSCR.On attending the seminar, the second editor suggested that the conference name be changed to INDOCRYPT.It is nice to see that this suggestion was taken up, giving us the annual INDOCRYPT conference - ries.Of course, the form, character, and execution of the conference series was the combined e?ort of the entire Indian cryptographic community under the dynamic leadership of Bimal Roy.

PROGRESS IN CRYPTOLOGY

INDOCRYPT 2002 : THIRD INTERNATIONAL CONFERENCE ON CRYPTOLOGY IN INDIA, HYDERABAD, INDIA, DECEMBER 16-18, 2002 : PROCEEDINGS

PROGRESS IN CRYPTOLOGY - INDOCRYPT 2010

11TH INTERNATIONAL CONFERENCE ON CRYPTOLOGY IN INDIA, HYDERABAD, INDIA, DECEMBER 12-15, 2010, PROCEEDINGS

Springer This book constitutes the refereed proceedings of the 11th International Conference on Cryptology in India, INDOCRYPT 2010, held in Hyderabad, India, in December 2010. The 22 revised full papers were carefully reviewed and selected from 72 submissions. The papers are organized in topical sections on security of RSA and multivariate schemes; security analysis, pseudorandom permutations and applications; hash functions; attacks on block ciphers and stream ciphers; fast cryptographic computation; cryptanalysis of AES; and efficient implementation.

PROGRESS IN CRYPTOLOGY - INDOCRYPT 2010

11TH INTERNATIONAL CONFERENCE ON CRYPTOLOGY IN INDIA, HYDERABAD, INDIA, DECEMBER 12-15, 2010, PROCEEDINGS

Springer This book constitutes the refereed proceedings of the 11th International Conference on Cryptology in India, INDOCRYPT 2010, held in Hyderabad, India, in December 2010. The 22 revised full papers were carefully reviewed and selected from 72 submissions. The papers are organized in topical sections on security of RSA and multivariate schemes; security analysis, pseudorandom permutations and applications; hash functions; attacks on block ciphers and stream ciphers; fast cryptographic computation; cryptanalysis of AES; and efficient implementation.

PROGRESS IN CRYPTOLOGY - INDOCRYPT 2002

THIRD INTERNATIONAL CONFERENCE ON CRYPTOLOGY IN INDIA HYDERABAD, INDIA, DECEMBER 16-18, 2002

Springer The third successful completion of the INDOCRYPT conference series marks the acceptance of the series by the international research community as a forum for presenting high-quality research.It also marks the coming of age of cryptology research in India. The authors for the submitted papers were spread across 21 countries and 4 continents, which goes a long way to demonstrate the international interest and visibility of INDOCRYPT.In the previous two conferences, the submissions from India originated from only two institutes; this increased to six for the 2002 conference.Thus INDOCRYPT is well set on the path to achieving two main ob jectives – to provide an international platform for presenting high-quality research and to stimulate cryptology research in India. The opportunity to serve as a program co-chair for the third INDOCRYPT carries a special satisfaction for the second editor.Way back in 1998, the sci- ti?c analysis group of DRDO organized a National Seminar on Cryptology and abbreviated it as NSCR.On attending the seminar, the second editor suggested that the conference name be changed to INDOCRYPT.It is nice to see that this suggestion was taken up, giving us the annual INDOCRYPT conference - ries.Of course, the form, character, and execution of the conference series was the combined e?ort of the entire Indian cryptographic community under the dynamic leadership of Bimal Roy.

SECURITY, PRIVACY, AND APPLIED CRYPTOGRAPHY ENGINEERING

6TH INTERNATIONAL CONFERENCE, SPACE 2016, HYDERABAD, INDIA, DECEMBER 14-18, 2016, PROCEEDINGS

Springer This book constitutes the refereed proceedings of the 6th International Conference on Security, Privacy, and Applied Cryptography Engineering, SPACE 2016, held in Hyderabad, India, in December 2016. This annual event is devoted to various aspects of security, privacy, applied cryptography, and cryptographic engineering. This is indeed a very challenging field, requiring the expertise from diverse domains, ranging from mathematics to solid-state circuit design.

INFORMATION SYSTEMS SECURITY

15TH INTERNATIONAL CONFERENCE, ICISS 2019, HYDERABAD, INDIA, DECEMBER 16–20, 2019, PROCEEDINGS

Springer Nature This book constitutes the proceedings of the 15th International Conference on Information Systems Security, ICISS 2019, held in Hyderabad, India, in December 2019. The 13 revised full papers and 4 short papers presented in this book together with 4 abstracts of invited talks were carefully reviewed and selected from 63 submissions. The papers cover topics such as: smart contracts; formal techniques; access control; machine learning; distributed systems; cryptography; online social networks; images and cryptography.

PROGRESS IN CRYPTOLOGY – INDOCRYPT 2019

20TH INTERNATIONAL CONFERENCE ON CRYPTOLOGY IN INDIA, HYDERABAD, INDIA, DECEMBER 15–18, 2019, PROCEEDINGS

Springer Nature This book constitutes the refereed proceedings of the 20th International Conference on Cryptology in India, INDOCRYPT 2019, held in Hyderabad, India, in December 2019. The 28 revised

full papers presented in this book were carefully reviewed and selected from 110 submissions (of which 20 were either rejected without being reviewed or withdrawn before the deadline). The focus of the conference includes works on signatures and filter permutators; symmetric key ciphers and hash functions; blockchain, secure computation and blind coupon mechanism; oblivious transfer, obfuscation and privacy amplification; Boolean functions, elliptic curves and lattices; algorithms, attacks and distribution; and efficiency, side-channel resistance and PUFs.

INFORMATION SYSTEMS SECURITY

4TH INTERNATIONAL CONFERENCE, ICISS 2008, HYDERABAD, INDIA, DECEMBER 16-20, 2008, PROCEEDINGS

Springer Science & Business Media The 4th International Conference on Information System Security (ICISS 2007) was held December 16–20, 2008 at the Jawaharlal Nehru Technological Univ- sity (JNTU) in Hyderabad, India. Although this conference is held in India, it is a decidedly international conference, attracting papers from all around the world. This year, there were 81 submissions from 18 di?erent countries. The- nal program contained papers from Australia, Austria, France, Germany, India, Poland, UK, and USA. From the 81 submissions, the Program Committee accepted 15 full papers, 4 short papers, and 2 ongoing research reports. The accepted papers span a wide rangeoftopics,includingaccesscontrol,cryptography,forensics,formalmethods and language-based security, intrusion detection, malware defense, network and Web security, operating system security, and privacy. Theconferencefeaturedfourkeynotetalks,withwrittenpapersaccompanying most of them. We would like to thank the speakers Somesh Jha, Basant Rajan, Amit Sahai,and Dawn Song for accepting our invitation to deliver keynotetalks atthis year'sconference.Theconferencewasprecededbytwo daysoftutorials. We would like to thank JNTU for hosting the conference, and EasyChair (http://www.easychair.org/) for providing conference management services to handle the paper review and selection process. Lastly, we wish to express our deepest thanks to the members of the Program Committee who give their p- sonal free time to perform the often thankless job of reviewing many papers under extremely short deadlines, and to the external reviewers, volunteers and local assistants who made this program a success.

INFORMATION SYSTEMS SECURITY

10TH INTERNATIONAL CONFERENCE, ICISS 2014, HYDERABAD, INDIA, DECEMBER 16-20, 2014. PROCEEDINGS

Springer This book constitutes the refereed proceedings of the 10th International Conference on Information Systems Security, ICISS 2014, held in Hyderabad, India, in December 2014. The 20 revised full papers and 5 short papers presented together with 3 invited papers were carefully reviewed and selected from 129 submissions. The papers address the following topics: security inferences; security policies; security user interfaces; security attacks; malware detection; forensics; and location based security services.

HARDWARE SECURITY AND TRUST

DESIGN AND DEPLOYMENT OF INTEGRATED CIRCUITS IN A THREATENED ENVIRONMENT

Springer This book provides a comprehensive introduction to hardware security, from specification to implementation. Applications discussed include embedded systems ranging from small RFID tags to satellites orbiting the earth. The authors describe a design and synthesis flow, which will transform a given circuit into a secure design incorporating counter-measures against fault attacks. In order to address the conflict between testability and security, the authors describe innovative design-for-testability (DFT) computer-aided design (CAD) tools that support security challenges, engineered for compliance with existing, commercial tools. Secure protocols are discussed, which protect access to necessary test infrastructures and enable the design of secure access controllers.

TOPICS IN CRYPTOLOGY -- CT-RSA 2005

THE CRYPTOGRAPHERS' TRACK AT THE RSA CONFERENCE 2005, SAN FRANCISCO, CA, USA, FEBRUARY 14-18, 2005, PROCEEDINGS

Springer This book constitutes the refereed proceedings of the Cryptographers Track at the RSA Conference 2005, CT-RSA 2005, held in San Francisco, CA, USA in February 2005. The 23 revised full papers presented together with 2 invited papers were carefully reviewed and selected from 74 submissions. The papers are organized in topical sections on cryptanalysis, public key encryption, signature schemes, design principles, password-based protocols, pairings, and efficient and secure implementations.

DATA-DRIVEN MINING, LEARNING AND ANALYTICS FOR SECURED SMART CITIES

TRENDS AND ADVANCES

Springer Nature This book provides information on data-driven infrastructure design, analytical approaches, and technological solutions with case studies for smart cities. This book aims to attract works on multidisciplinary research spanning across the computer science and engineering, environmental studies, services, urban planning and development, social sciences and industrial engineering on technologies, case studies, novel approaches, and visionary ideas related to data-driven innovative solutions and big data-powered applications to cope with the real world challenges for building smart cities.

CLASSICAL AND PHYSICAL SECURITY OF SYMMETRIC KEY CRYPTOGRAPHIC ALGORITHMS

Springer Nature This book consolidates several key aspects from the state-of-the-art research in symmetric key cryptography, which is among the cornerstones of digital security. It presents the content in an informative yet beginner-friendly, accompanied with toy examples and comprehensible graphics. In particular, it highlights the recent developments in tool-assisted analysis of ciphers. Furthermore, promising device-dependent attacks, such as fault attack and side channel attacks on symmetric key ciphers, are discussed in detail. One salient feature of this book is to present a detailed analysis of various fault countermeasures. The coverage of our book is quite diverse—it ranges from prerequisite information, latest research contribution as well as future research directions. It caters to students and researchers working in the field of cryptography.

VLSI AND HARDWARE IMPLEMENTATIONS USING MODERN MACHINE LEARNING METHODS

CRC Press Machine learning is a potential solution to resolve bottleneck issues in VLSI via optimizing tasks in the design process. This book aims to provide the latest machine-learning–based methods, algorithms, architectures, and frameworks designed for VLSI design. The focus is on digital, analog, and mixed-signal design techniques, device modeling, physical design, hardware implementation, testability, reconfigurable design, synthesis and verification, and related areas. Chapters include case studies as well as novel research ideas in the given field. Overall, the book provides practical implementations of VLSI design, IC design, and hardware realization using machine learning techniques. Features: Provides the details of state-of-the-art machine learning methods used in VLSI design Discusses hardware implementation and device modeling pertaining to machine learning algorithms Explores machine learning for various VLSI architectures and reconfigurable computing Illustrates the latest techniques for device size and feature optimization Highlights the latest case studies and reviews of the methods used for hardware implementation This book is aimed at researchers, professionals, and graduate students in VLSI, machine learning, electrical and electronic engineering, computer engineering, and hardware systems.

PROGRESS IN CRYPTOLOGY - INDOCRYPT 2000

FIRST INTERNATIONAL CONFERENCE IN CRYPTOLOGY IN INDIA, CALCUTTA, INDIA, DECEMBER 10-13, 2000. PROCEEDINGS

Springer The field of Cryptology witnessed a revolution in the late seventies. Since then it has been expanded into an important and exciting area of research. Over the last two decades, India neither participated actively nor did it contribute sig nificantly towards the development in this field. However, recently a number of active research groups engaged in important research and developmental work have crystalized in different parts of India. As a result, their interaction with the international crypto community has become necessary. With this backdrop, it was proposed that a conference on cryptology - INDOCRYPT, be organized for the first time in India. The Indian Statistical Institute was instrumental in hosting this conference. INDOCRYPT has generated a large amount of enthu siasm amongst the Indians as well as the International crypto communities. An INDOCRYPT steering committee has been formed and the committee has plans to make INDOCRYPT an annual event. For INDOCRYPT 2000, the program committee considered a total of 54 pa pers and out of these 25 were selected for presentation. The conference program also included two invited lectures by Prof. Adi Shamir and Prof. Eli Biham. These proceedings include the revised versions of the 25 papers accepted by the program committee. These papers were selected from all the submissions based on originality, quality and relevance to the field of Cryptology. Revisions were not checked and the authors bear the full responsibility for the contents of the papers in these proceedings.

FAULT TOLERANT ARCHITECTURES FOR CRYPTOGRAPHY AND HARDWARE SECURITY

Springer This book uses motivating examples and real-life attack scenarios to introduce readers to the general concept of fault attacks in cryptography. It offers insights into how the fault tolerance theories developed in the book can actually be implemented, with a particular focus on a wide spectrum of fault models and practical fault injection techniques, ranging from simple, low-cost techniques to high-end equipment-based methods. It then individually examines fault attack vulnerabilities in symmetric, asymmetric and authenticated encryption systems. This is followed by extensive coverage of countermeasure techniques and fault tolerant architectures that attempt to thwart such vulnerabilities. Lastly, it presents a case study of a comprehensive FPGA-based fault tolerant architecture for AES-128, which brings together of a number of the fault tolerance techniques presented. It concludes with a discussion on how fault tolerance can be combined with side channel security to achieve protection against implementation-based attacks. The text is supported by illustrative diagrams, algorithms, tables and diagrams presenting real-world experimental results.

STATISTICAL TREND ANALYSIS OF PHYSICALLY UNCLONABLE FUNCTIONS

AN APPROACH VIA TEXT MINING

CRC Press Physically Unclonable Functions (PUFs) translate unavoidable variations in certain parameters of materials, waves, or devices into random and unique signals. They have found many applications in the Internet of Things (IoT), authentication systems, FPGA industry, several other areas in communications and related technologies, and many commercial products. Statistical Trend Analysis of Physically Unclonable Functions first presents a review on cryptographic hardware and hardware-assisted cryptography. The review highlights PUF as a mega trend in research on cryptographic hardware design. Afterwards, the authors present a combined survey and research work on PUFs using a systematic approach. As part of the survey aspect, a state-of-the-art analysis is presented as well as a taxonomy on PUFs, a life cycle, and an established ecosystem for the technology. In another part of the survey, the evolutionary history of PUFs is examined, and strategies for further research in this area are suggested. In the research side, this book presents a novel approach for trend analysis that can be applied to any technology or research area. In this method, a text mining tool is used which

extracts 1020 keywords from the titles of the sample papers. Then, a classifying tool classifies the keywords into 295 meaningful research topics. The popularity of each topic is then numerically measured and analyzed over the course of time through a statistical analysis on the number of research papers related to the topic as well as the number of their citations. The authors identify the most popular topics in four different domains; over the history of PUFs, during the recent years, in top conferences, and in top journals. The results are used to present an evolution study as well as a trend analysis and develop a roadmap for future research in this area. This method gives an automatic popularity-based statistical trend analysis which eliminates the need for passing personal judgments about the direction of trends, and provides concrete evidence to the future direction of research on PUFs. Another advantage of this method is the possibility of studying a whole lot of existing research works (more than 700 in this book). This book will appeal to researchers in text mining, cryptography, hardware security, and IoT.

GUIDE TO ELLIPTIC CURVE CRYPTOGRAPHY

*Springer Science & Business Media After two decades of research and development, elliptic curve cryptography now has widespread exposure and acceptance. Industry, banking, and government standards are in place to facilitate extensive deployment of this efficient public-key mechanism. Anchored by a comprehensive treatment of the practical aspects of elliptic curve cryptography (ECC), this guide explains the basic mathematics, describes state-of-the-art implementation methods, and presents standardized protocols for public-key encryption, digital signatures, and key establishment. In addition, the book addresses some issues that arise in software and hardware implementation, as well as side-channel attacks and countermeasures. Readers receive the theoretical fundamentals as an underpinning for a wealth of practical and accessible knowledge about efficient application. Features & Benefits: * Breadth of coverage and unified, integrated approach to elliptic curve cryptosystems * Describes important industry and government protocols, such as the FIPS 186-2 standard from the U.S. National Institute for Standards and Technology * Provides full exposition on techniques for efficiently implementing finite-field and elliptic curve arithmetic * Distills complex mathematics and algorithms for easy understanding * Includes useful literature references, a list of algorithms, and appendices on sample parameters, ECC standards, and software tools This comprehensive, highly focused reference is a useful and indispensable resource for practitioners, professionals, or researchers in computer science, computer engineering, network design, and network data security.*

TOPICS IN GEOMETRY, CODING THEORY AND CRYPTOGRAPHY

Springer Science & Business Media The theory of algebraic function fields over finite fields has its origins in number theory. However, after Goppa`s discovery of algebraic geometry codes around 1980, many applications of function fields were found in different areas of mathematics and information theory. This book presents survey articles on some of these new developments. The topics focus on material which has not yet been presented in other books or survey articles.

PROGRESS IN CRYPTOLOGY – INDOCRYPT 2016

17TH INTERNATIONAL CONFERENCE ON CRYPTOLOGY IN INDIA, KOLKATA, INDIA, DECEMBER 11-14, 2016, PROCEEDINGS

Springer This book constitutes the refereed proceedings of the 17th International Conference on Cryptology in India, INDOCRYPT 2016, held in Kolkata, India, in December 2016. The 23 revised full papers presented in this book were carefully reviewed and selected from 84 submissions. The focus of the conference includes works on Public-Key Cryptography, Cryptographic Protocols, Side-Channel Attacks, Implementation of Cryptographic Schemes, Functional Encryption, Symmetric-Key Cryptanalysis, Foundations, and New Cryptographic Constructions.

INTEGRATION OF WSNS INTO INTERNET OF THINGS

A SECURITY PERSPECTIVE

CRC Press The Internet has gone from an Internet of people to an Internet of Things (IoT). This has brought forth strong levels of complexity in handling interoperability that involves the integrating of wireless sensor networks (WSNs) into IoT. This book offers insights into the evolution, usage, challenges, and proposed countermeasures associated with the integration. Focusing on the integration of WSNs into IoT and shedding further light on the subtleties of such integration, this book aims to highlight the encountered problems and provide suitable solutions. It throws light on the various types of threats that can attack both WSNs and IoT along with the recent approaches to counter them. This book is designed to be the first choice of reference at research and development centers, academic institutions, university libraries, and any institution interested in the integration of WSNs into IoT. Undergraduate and postgraduate students, Ph.D. scholars, industry technologists, young entrepreneurs, and researchers working in the field of security and privacy in IoT are the primary audience of this book.

THIRD INTERNATIONAL CONFERENCE ON IMAGE PROCESSING AND CAPSULE NETWORKS

ICIPCN 2022

Springer Nature This book provides a collection of the state-of-the-art research attempts to tackle the challenges in image and signal processing from various novel and potential research perspectives. The book investigates feature extraction techniques, image enhancement methods, reconstruction models, object detection methods, recommendation models, deep and temporal feature analysis, intelligent decision support systems, and autonomous image detection models. In addition to this, the book also looks into the potential opportunities to monitor and control the global pandemic situations. Image processing technology has progressed significantly in recent years, and it has been commercialized worldwide to provide superior performance with enhanced computer/machine vision, video processing, and pattern recognition capabilities. Meanwhile, machine learning systems like CNN and CapsNet get popular to provide better model hierarchical relationships and attempts to more closely mimic biological neural organization. As machine learning systems prosper, image processing and machine learning techniques will be tightly intertwined and continuously promote each other in real-world settings. Adopting this trend, however, the image processing researchers are faced with few image reconstruction, analysis, and segmentation challenges. On the application side, the orientation of the image features and noise removal has become a huge burden.

IOT SECURITY

ADVANCES IN AUTHENTICATION

John Wiley & Sons An up-to-date guide to an overview of authentication in the Internet of Things (IoT) The Internet of things (IoT) is the network of the countless physical devices that have the possibility to connect and exchange data. Among the various security requirements, authentication to the IoT is the first step to prevent the impact of attackers. IoT Security offers an important guide into the development of the many authentication mechanisms that provide IoT authentication at various levels such as user level, device level and network level. The book covers a wide range of topics including an overview of IoT and addresses in detail the security challenges at every layer by considering both the technologies and the architecture used. The authors—noted experts on the topic—provide solutions for remediation of compromised security, as well as methods for risk mitigation, and offer suggestions for prevention and improvement. In addition, IoT Security offers a variety of illustrative use cases. This important book: Offers an authoritative reference designed for use by all IoT stakeholders Includes information for securing devices at the user, device, and network levels Contains a classification of existing vulnerabilities Written by an international group of experts on the topic Provides a guide to the most current information available on IoT security Written for network operators, cloud operators, IoT device manufacturers, IoT device users, wireless users, IoT standardization organizations, and security solution developers, IoT Security is an essential guide that contains information on security features, including underlying networks, architectures, and security requirements.

IOT SECURITY

ADVANCES IN AUTHENTICATION

John Wiley & Sons An up-to-date guide to an overview of authentication in the Internet of Things (IoT) The Internet of things (IoT) is the network of the countless physical devices that have the possibility to connect and exchange data. Among the various security requirements, authentication to the IoT is the first step to prevent the impact of attackers. IoT Security offers an important guide into the development of the many authentication mechanisms that provide IoT authentication at various levels such as user level, device level and network level. The book covers a wide range of topics including an overview of IoT and addresses in detail the security challenges at every layer by considering both the technologies and the architecture used. The authors—noted experts on the topic—provide solutions for remediation of compromised security, as well as methods for risk mitigation, and offer suggestions for prevention and improvement. In addition, IoT Security offers a variety of illustrative use cases. This important book: Offers an authoritative reference designed for use by all IoT stakeholders Includes information for securing devices at the user, device, and network levels Contains a classification of existing vulnerabilities Written by an international group of experts on the topic Provides a guide to the most current information available on IoT security Written for network operators, cloud operators, IoT device manufacturers, IoT device users, wireless users, IoT standardization organizations, and security solution developers, IoT Security is an essential guide that contains information on security features, including underlying networks, architectures, and security requirements.

SELECTED TOPICS IN INFORMATION AND CODING THEORY

INTELLIGENT TECHNOLOGIES AND TECHNIQUES FOR PERVASIVE COMPUTING

IGI Global Pervasive computing enables users to interact with information resources in their everyday lives. The development of computational technologies that can exist in ever smaller devices while simultaneously increasing processing power allows such devices to blend seamlessly into tangible environments. Intelligent Technologies and Techniques for Pervasive Computing provides an extensive discussion of such technologies, theories and practices in an attempt to shed light on current trends and issues in the adaption of pervasive systems. Within its pages, students and practitioners of computer science will find both recent developments and practical applications an overview of the field and how intelligent techniques can help to improve user experience in the distribution and consumption of pertinent, timely information. This book is part of the Advances in Computational Intelligence and Robotics series collection.

PROGRESS IN CRYPTOLOGY – INDOCRYPT 2017

18TH INTERNATIONAL CONFERENCE ON CRYPTOLOGY IN INDIA, CHENNAI, INDIA, DECEMBER 10-13, 2017, PROCEEDINGS

Springer This book constitutes the refereed proceedings of the 18th International Conference on Cryptology in India, INDOCRYPT 2017, held in Chennai, India, in December 2017. The 19 revised full papers presented in this book were carefully reviewed and selected from 75 submissions. The focus of the conference includes works on Public-Key Cryptography, Cryptographic Protocols, Side-Channel Attacks,

Implementation of Cryptographic Schemes, Functional Encryption, Symmetric-Key Cryptanalysis, Foundations, and New Cryptographic Constructions.

PROCEEDINGS OF 3RD INTERNATIONAL CONFERENCE ON ADVANCED COMPUTING, NETWORKING AND INFORMATICS

ICACNI 2015, VOLUME 2

Springer Advanced Computing, Networking and Informatics are three distinct and mutually exclusive disciplines of knowledge with no apparent sharing/overlap among them. However, their convergence is observed in many real world applications, including cyber-security, internet banking, healthcare, sensor networks, cognitive radio, pervasive computing amidst many others. This two volume proceedings explore the combined use of Advanced Computing and Informatics in the next generation wireless networks and security, signal and image processing, ontology and human-computer interfaces (HCI). The two volumes together include 132 scholarly articles, which have been accepted for presentation from over 550 submissions in the Third International Conference on Advanced Computing, Networking and Informatics, 2015, held in Bhubaneswar, India during June 23–25, 2015.

PROGRESS IN CRYPTOLOGY - INDOCRYPT 2005

6TH INTERNATIONAL CONFERENCE ON CRYPTOLOGY IN INDIA, BANGALORE, INDIA, DECEMBER 10-12, 2005, PROCEEDINGS

Springer Science & Business Media This book constitutes the refereed proceedings of the 6th International Conference on Cryptology in India, INDOCRYPT 2005, held in Bangalore, India in December 2005. The 31 revised full papers presented together with 1 invited paper were carefully reviewed and selected from 148 submissions. The papers are organized in topical sections on sequences, boolean function and S-box, hash functions, design principles, cryptanalysis, time memory trade-off, new constructions, pairings, signatures, applications, e-cash, and implementations.

PROGRESS IN CRYPTOLOGY – INDOCRYPT 2021

22ND INTERNATIONAL CONFERENCE ON CRYPTOLOGY IN INDIA, JAIPUR, INDIA, DECEMBER 12–15, 2021, PROCEEDINGS

Springer Nature This book constitutes the refereed proceedings of the 22nd International Conference on Cryptology in India, INDOCRYPT 2021, which was held in Jaipur, India, during December 12-15, 2021. The 27 full papers included in these proceedings were carefully reviewed and selected from 65 submissions. They were organized in topical sections as follows: authenticated encryption; symmetric cryptography; lightweight cryptography; side-channel attacks; fault attacks; post-quantum cryptography; public key encryption and protocols; cryptographic constructions; blockchains.

CONFIDENTIAL COMPUTING

HARDWARE BASED MEMORY PROTECTION

Springer Nature This book highlights the three pillars of data security, viz protecting data at rest, in transit, and in use. Protecting data at rest means using methods such as encryption or tokenization so that even if data is copied from a server or database, a thief cannot access the information. Protecting data in transit means making sure unauthorized parties cannot see information as it moves between servers and applications. There are well-established ways to provide both kinds of protection. Protecting data while in use, though, is especially tough because applications need to have data in the clear—not encrypted or otherwise protected—in order to compute. But that means malware can dump the contents of memory to steal information. It does not really matter if the data was encrypted on a server's hard drive if it is stolen while exposed in memory. As computing moves to span multiple environments—from on-premise to public cloud to edge—organizations need protection controls that help safeguard sensitive IP and workload data wherever the data resides. Many organizations have declined to migrate some of their most sensitive applications to the cloud because of concerns about potential data exposure. Confidential computing makes it possible for different organizations to combine data sets for analysis without accessing each other's data.

FIRST INTERNATIONAL CONFERENCE ON ARTIFICIAL INTELLIGENCE AND COGNITIVE COMPUTING

AICC 2018

Springer This book presents original research works by researchers, engineers and practitioners in the field of artificial intelligence and cognitive computing. The book is divided into two parts, the first of which focuses on artificial intelligence (AI), knowledge representation, planning, learning, scheduling, perception-reactive AI systems, evolutionary computing and other topics related to intelligent systems and computational intelligence. In turn, the second part focuses on cognitive computing, cognitive science and cognitive informatics. It also discusses applications of cognitive computing in medical informatics, structural health monitoring, computational intelligence, intelligent control systems, bio-informatics, smart manufacturing, smart grids, image/video processing, video analytics, medical image and signal processing, and knowledge engineering, as well as related applications.

SIDE CHANNEL ATTACKS

MDPI This Special Issue provides an opportunity for researchers in the area of side-channel attacks (SCAs) to highlight the most recent exciting technologies. The research papers published in this Special Issue represent recent progress in the field, including research on power analysis attacks, cache-based timing attacks, system-level countermeasures, and so on.

MULTI-DISCIPLINARY TRENDS IN ARTIFICIAL INTELLIGENCE

5TH INTERNATIONAL WORKSHOP, MIWAI 2011, HYDERABAD, INDIA, DECEMBER 7-9, 2011. PROCEEDINGS

Springer This volume constitutes the refereed proceedings of the 5th Multi-disciplinary International Workshop On Artificial Intelligence, MIWAI 2011, held in Hyderabad, India, in December 2011. The 38 revised full papers presented were carefully reviewed and selected from 71 submissions. The papers cover the multifarious nature of the Artificial Intelligence research domain, ranging from theoretical to real world applications and address topics such as agent-based simulation, agent-oriented software engineering, agents and Web services, agent-based electronic commerce, auctions and markets, AI in video games, computer vision, constraint satisfaction, data mining, decision theory, distributed AI, e-commerce and AI, game theory, internet/www intelligence, industrial applications of AI, intelligent tutoring, knowledge representation and reasoning, machine learning, multi-agent planning and learning, multi-agent systems and their applications, multi-agent systems and evolving intelligence, natural language processing, neural networks, planning and scheduling, robotics, uncertainty in AI, and Web services.

PROGRESS IN CRYPTOLOGY – AFRICACRYPT 2016

8TH INTERNATIONAL CONFERENCE ON CRYPTOLOGY IN AFRICA, FES, MOROCCO, APRIL 13-15, 2016, PROCEEDINGS

Springer This book constitutes the thoroughly refereed proceedings of the 8th International Conference on the Theory and Application of Cryptographic Techniques in Africa, AFRICACRYPT 2016, held in Fes, Morooco, in April 2016. The 18 papers presented in this book were carefully reviewed and selected from 65 submissions. The aim of Africacrypt 2016 is to provide an international forum for practitioners and researchers from industry, academia and government from all over the world for a wide ranging discussion of all forms of cryptography. Topics of interest are such as lattices; elliptic curves; secret-key cryptanalysis; efficient implementations; secure protocols; and public-key cryptography.

PROCEEDINGS OF THE THIRD INTERNATIONAL CONFERENCE ON COMPUTATIONAL INTELLIGENCE AND INFORMATICS

ICCII 2018

Springer Nature This book features high-quality papers presented at the International Conference on Computational Intelligence and Informatics (ICCII 2018), which was held on 28–29 December 2018 at the Department of Computer Science and Engineering, JNTUH College of Engineering, Hyderabad, India. The papers focus on topics such as data mining, wireless sensor networks, parallel computing, image processing, network security, MANETS, natural language processing and Internet of things.

AMERICAN BOOK PUBLISHING RECORD