

Information Security And Cryptology 10th International Conference Inscrypt 2014 Beijing China December 13 15 2014 Revised Selected Papers Lecture Notes In Computer Science

Yeah, reviewing a ebook **Information Security And Cryptology 10th International Conference Inscrypt 2014 Beijing China December 13 15 2014 Revised Selected Papers Lecture Notes In Computer Science** could mount up your near links listings. This is just one of the solutions for you to be successful. As understood, execution does not recommend that you have astounding points.

Comprehending as skillfully as pact even more than further will meet the expense of each success. bordering to, the statement as competently as acuteness of this Information Security And Cryptology 10th International Conference Inscrypt 2014 Beijing China December 13 15 2014 Revised Selected Papers Lecture Notes In Computer Science can be taken as competently as picked to act.

Computer and Cyber Security - Brij B. Gupta 2018-11-19

This is a monumental reference for the theory and practice of computer security. Comprehensive in scope, this text covers applied and practical elements, theory, and the reasons for the design of applications and security techniques. It covers both the management and the engineering issues of computer security. It provides excellent examples of ideas and mechanisms that demonstrate how disparate techniques and principles are combined in widely-used systems. This book is acclaimed for its scope, clear and lucid writing, and its combination of formal and theoretical aspects with real systems, technologies, techniques, and policies.

Advances in Cryptology - ASIACRYPT 2004 - Pil Joong Lee 2004-11-16

The 10th Annual ASIACRYPT 2004 was held in Jeju Island, Korea, during December 5-9, 2004. This conference was organized by the International Association for Cryptologic Research (IACR) in cooperation with KIISC (Korea Institute of Information Security and Cryptology) and IRIS (International Research center for Information Security) at ICU (Information and Communications University), and was financially supported by MIC (Ministry of Information and Communication) in Korea. The conference received, from 30 countries, 208 submissions that represent the current state of work in the cryptographic community worldwide, covering all areas of cryptologic research. Each paper, without the authors' information, was reviewed by at least three members of the program committee, and the papers (co-)authored by members of the program committee were reviewed by at least six members. We also blinded the reviewers' names among the reviewers until the final decision, by using pseudonyms. The reviews were then followed by deep discussions on the papers, which greatly contributed to the quality of the final selection. In most cases, extensive comments were sent to the authors. Among 208 submissions, the program committee selected 36 papers. Two submissions were merged into a single paper, yielding the total of 35 papers accepted for presentation in the technical program of the conference. Many high-quality works could not be accepted because of the competitive nature of the conference and the challenging task of selecting a program. These proceedings contain revised versions of the accepted papers. These revisions have not been checked for correctness, and the authors bear full responsibility for the contents of their papers.

Information Security and Cryptology - ICISC 2007 - Kil-Hyun Nam 2007-11-13

This book constitutes the refereed proceedings of the 10th International Conference on Information Security and Cryptology, ICISC 2007, held in Seoul, Korea, November 29-30, 2007. The papers are organized in topical sections on cryptanalysis, access control, system security, biometrics, cryptographic protocols, hash functions, block and stream ciphers, copyright protection, smart/java cards, elliptic curve cryptosystems as well as authentication and authorization.

International Joint Conference: 12th International Conference on Computational Intelligence in Security for Information Systems (CISIS 2019) and 10th International Conference on European Transnational Education (ICEUTE 2019) - Francisco Martínez Álvarez 2019-04-27

This volume presents papers presented at CISIS 2019 and ICEUTE 2019, held in the beautiful and historic city of Seville (Spain) in May 2019. The 12th CISIS 2019 conference offered a meeting opportunity for

academic and industry-related researchers from the various communities of computational intelligence, information security and data mining, and the need for intelligent, flexible behaviour by large, complex systems, especially in mission-critical domains, was the catalyst and the aggregation stimulus for the event. The book covers current topics such as cryptographic and data analytics solutions to fulfil least minimum privilege and endorse least minimum effort in information systems. The book also includes 15 papers from the 10th ICEUTE 2019, covering topics like new approaches to assess competencies and innovation in computer science education.

Progress in Cryptology - Mycrypt 2005 - Ed Dawson 2005-09-14

This book constitutes the refereed proceedings of the First International Conference on Cryptology hosted in Malaysia, held in Kuala Lumpur, Malaysia in September 2005, in conjunction with the e-Secure Malaysia 2005 convention. The 19 revised full papers presented together with 3 invited papers were carefully reviewed and selected from a total of 90 submissions. The papers are organized in topical sections on stream ciphers analysis, cryptography based on combinatorics, cryptographic protocols, implementation issues, unconventional cryptography, block cipher cryptanalysis, and homomorphic encryption.

Information Security and Cryptology - Fuchun Guo 2019-03-21

This book constitutes the post-conference proceedings of the 14th International Conference on Information Security and Cryptology, Inscrypt 2018, held in Fuzhou, China, in December 2018. The 31 full papers presented together with 5 short papers and 1 invited paper were carefully reviewed and selected from 93 submissions. The papers cover topics in the field of blockchain and crypto currency; lattice-based cryptology; symmetric cryptology; applied cryptography; information security; asymmetric encryption; and foundations.

Cloud Computing Security - John R. Vacca 2016-09-19

This handbook offers a comprehensive overview of cloud computing security technology and implementation, while exploring practical solutions to a wide range of cloud computing security issues. With more organizations using cloud computing and cloud providers for data operations, proper security in these and other potentially vulnerable areas have become a priority for organizations of all sizes across the globe. Research efforts from both academia and industry in all security aspects related to cloud computing are gathered within one reference guide.

Power Analysis Attacks - Stefan Mangard 2008-01-03

Power analysis attacks allow the extraction of secret information from smart cards. Smart cards are used in many applications including banking, mobile communications, pay TV, and electronic signatures. In all these applications, the security of the smart cards is of crucial importance. *Power Analysis Attacks: Revealing the Secrets of Smart Cards* is the first comprehensive treatment of power analysis attacks and countermeasures. Based on the principle that the only way to defend against power analysis attacks is to understand them, this book explains how power analysis attacks work. Using many examples, it discusses simple and differential power analysis as well as advanced techniques like template attacks. Furthermore, the authors provide an extensive discussion of countermeasures like shuffling, masking, and DPA-resistant logic styles. By analyzing the pros and cons of the different countermeasures, this volume allows

practitioners to decide how to protect smart cards.

The Routledge Companion to Technology Management - Tugrul Daim 2022-08-31

Bringing together an international range of expertise, this comprehensive Companion to Technology Management is designed to facilitate the development of management frameworks adaptable for a wide range of organizations, as well as an overview of the development and integration of technology in advanced and emerging economies. Research-based and drawing on a range of practical tools and international cases, it covers the diverse spectrum of the challenges of technology management and how to approach them: I Fundamentals of Technology Management provides an overview of the fundamental aspects of technology management. II Technology Planning focusses on technology-driven organizations, government labs and universities. III Technology Evaluation includes evaluation and assessment, adoption and forecasting through management tools. IV Technology Development and Transfer includes integration, marketing and intellectual property management. V Managing Technological Innovations addresses policy, open innovation and technology entrepreneurship. VI Society and Technology Management focusses on social issues which impact technology and its management. VII New Technologies and Emerging Regions includes blockchain, biotechnologies and smart cities. This Companion is an essential comprehensive source of new and emerging approaches for researchers and advanced students in engineering and technology management, as well as professionals seeking an authoritative global reference source.

Information Security - Juan Garay 2007-09-19

This book constitutes the refereed proceedings of the 10th International Conference on Information Security Conference, ISC 2007. Coverage in the 28 revised full papers presented includes intrusion detection, digital rights management, symmetric-key cryptography, cryptographic protocols and schemes, identity-based schemes, cryptanalysis, DoS protection, software obfuscation, public-key cryptosystems, elliptic curves and applications and security issues in databases.

Security of Ubiquitous Computing Systems - Gildas Avoine 2021-01-14

The chapters in this open access book arise out of the EU Cost Action project Cryptacus, the objective of which was to improve and adapt existent cryptanalysis methodologies and tools to the ubiquitous computing framework. The cryptanalysis implemented lies along four axes: cryptographic models, cryptanalysis of building blocks, hardware and software security engineering, and security assessment of real-world systems. The authors are top-class researchers in security and cryptography, and the contributions are of value to researchers and practitioners in these domains. This book is open access under a CC BY license.

Applied Cryptography and Network Security - Feng Bao 2012-06-14

This book constitutes the refereed proceedings of the 10th International Conference on Applied Cryptography and Network Security, ACNS 2012, held in Singapore, in June 2012. The 33 revised full papers included in this volume were carefully reviewed and selected from 192 submissions. They are organized in topical sessions on authentication, key management, block ciphers, identity-based cryptography, cryptographic primitives, cryptanalysis, side channel attacks, network security, Web security, security and privacy in social networks, security and privacy in RFID systems, security and privacy in cloud systems, and security and privacy in smart grids.

Security, Privacy, and Applied Cryptography Engineering - Shivam Bhasin 2019-11-20

This book constitutes the refereed proceedings of the 9th International Conference on Security, Privacy, and Applied Cryptography Engineering, SPACE 2019, held in Gandhinagar, India, in December 2019. The 12 full papers presented were carefully reviewed and selected from 24 submissions. This annual event is devoted to various aspects of security, privacy, applied cryptography, and cryptographic engineering. This is a very challenging field, requiring the expertise from diverse domains, ranging from mathematics to solid-state circuit design.

Soft Computing in Data Analytics - Janmenjoy Nayak 2018-08-21

The volume contains original research findings, exchange of ideas and dissemination of innovative, practical development experiences in different fields of soft and advance computing. It provides insights into the International Conference on Soft Computing in Data Analytics (SCDA). It also concentrates on both theory and practices from around the world in all the areas of related disciplines of soft computing. The

book provides rapid dissemination of important results in soft computing technologies, a fusion of research in fuzzy logic, evolutionary computations, neural science and neural network systems and chaos theory and chaotic systems, swarm based algorithms, etc. The book aims to cater the postgraduate students and researchers working in the discipline of computer science and engineering along with other engineering branches.

Advances in Network Analysis and its Applications - Evangelos Kranakis 2012-10-23

As well as highlighting potentially useful applications for network analysis, this volume identifies new targets for mathematical research that promise to provide insights into network systems theory as well as facilitating the cross-fertilization of ideas between sectors. Focusing on financial, security and social aspects of networking, the volume adds to the growing body of evidence showing that network analysis has applications to transportation, communication, health, finance, and social policy more broadly. It provides powerful models for understanding the behavior of complex systems that, in turn, will impact numerous cutting-edge sectors in science and engineering, such as wireless communication, network security, distributed computing and social networking, financial analysis, and cyber warfare. The volume offers an insider's view of cutting-edge research in network systems, including methodologies with immense potential for interdisciplinary application. The contributors have all presented material at a series of workshops organized on behalf of Canada's MITACS initiative, which funds projects and study grants in 'mathematics for information technology and complex systems'. These proceedings include papers from workshops on financial networks, network security and cryptography, and social networks. MITACS has shown that the partly ghettoized nature of network systems research has led to duplicated work in discrete fields, and thus this initiative has the potential to save time and accelerate the pace of research in a number of areas of network systems research.

Cryptology and Network Security - Dongdai Lin 2011-11-23

This book constitutes the refereed proceedings of the 10th International Conference on Cryptology and Network Security, CANS 2011, held in Sanya, China, in December 2011. The 18 revised full papers, presented were carefully reviewed and selected from 65 submissions. The book also includes two invited talks. The papers are organized in topical sections on symmetric cryptanalysis, symmetric ciphers, public key cryptography, protocol attacks, and privacy techniques.

Multivariate Public Key Cryptosystems - Jintai Ding 2006-11-24

Multivariate public key cryptosystems (MPKC) is a fast-developing area in cryptography. This book systematically presents the subject matter for a broad audience and is the first book to focus on this exciting new topic. Information security experts in industry can use the book as a guide for understanding what is needed to implement these cryptosystems for practical applications, and researchers in both computer science and mathematics will find it a good starting point for exploring this new field. It is also suitable as a textbook for advanced-level students.

Information Theoretic Security - Junji Shikata 2017-11-25

This book constitutes the refereed proceedings of the 10th International Conference on Information Theoretic Security, ICITS 2017, held in Hong Kong, China, in November/December 2017. The 12 full papers were carefully reviewed and selected from 42 submissions. They are organized around the following topics: quantum cryptography; quantum information theory; post-quantum cryptography (e.g. lattices and cryptography); physical layer security; wiretap channels; adversarial channel models; cryptography from noisy channels; bounded storage models; network coding security; biometric security; randomness extraction; key and message rates; secret sharing; authentication codes; multiparty computations; information theoretic reductions; and implementation challenges.

Protecting Mobile Networks and Devices - Weizhi Meng 2016-11-25

This book gathers and analyzes the latest attacks, solutions, and trends in mobile networks. Its broad scope covers attacks and solutions related to mobile networks, mobile phone security, and wireless security. It examines the previous and emerging attacks and solutions in the mobile networking worlds, as well as other pertinent security issues. The many attack samples present the severity of this problem, while the delivered methodologies and countermeasures show how to build a truly secure mobile computing environment.

Information Security and Cryptology - Dongdai Lin 2015-04-08

This book constitutes the thoroughly refereed post-conference proceedings of the 10th International Conference on Information Security and Cryptology, Inscrypt 2014, held in Beijing, China, in December 2014. The 29 revised full papers presented were carefully reviewed and selected from 93 submissions. The papers are organized in topical sections on privacy and anonymity, multiparty and outsource computation, signature and security protocols, lattice and public key cryptography, block cipher and hash function, authentication and encryption, elliptic curve, and cryptographic primitive and application.

Fog/Edge Computing For Security, Privacy, and Applications - Wei Chang 2021-01-04

This book provides the state-of-the-art development on security and privacy for fog/edge computing, together with their system architectural support and applications. This book is organized into five parts with a total of 15 chapters. Each area corresponds to an important snapshot. The first part of this book presents an overview of fog/edge computing, focusing on its relationship with cloud technology and the future with the use of 5G communication. Several applications of edge computing are discussed. The second part of this book considers several security issues in fog/edge computing, including the secure storage and search services, collaborative intrusion detection method on IoT-fog computing, and the feasibility of deploying Byzantine agreement protocols in untrusted environments. The third part of this book studies the privacy issues in fog/edge computing. It first investigates the unique privacy challenges in fog/edge computing, and then discusses a privacy-preserving framework for the edge-based video analysis, a popular machine learning application on fog/edge. This book also covers the security architectural design of fog/edge computing, including a comprehensive overview of vulnerabilities in fog/edge computing within multiple architectural levels, the security and intelligent management, the implementation of network-function-virtualization-enabled multicasting in part four. It explains how to use the blockchain to realize security services. The last part of this book surveys applications of fog/edge computing, including the fog/edge computing in Industrial IoT, edge-based augmented reality, data streaming in fog/edge computing, and the blockchain-based application for edge-IoT. This book is designed for academics, researchers and government officials, working in the field of fog/edge computing and cloud computing. Practitioners, and business organizations (e.g., executives, system designers, and marketing professionals), who conduct teaching, research, decision making, and designing fog/edge technology will also benefit from this book. The content of this book will be particularly useful for advanced-level students studying computer science, computer technology, and information systems, but also applies to students in business, education, and economics, who would benefit from the information, models, and case studies therein.

Cyber Crime: Concepts, Methodologies, Tools and Applications - Management Association, Information Resources 2011-11-30

Threatening the safety of individuals, computers, and entire networks, cyber crime attacks vary in severity and type. Studying this continually evolving discipline involves not only understanding different types of attacks, which range from identity theft to cyberwarfare, but also identifying methods for their prevention. *Cyber Crime: Concepts, Methodologies, Tools and Applications* is a three-volume reference that explores all aspects of computer-based crime and threats, offering solutions and best practices from experts in software development, information security, and law. As cyber crime continues to change and new types of threats emerge, research focuses on developing a critical understanding of different types of attacks and how they can best be managed and eliminated.

Selected Areas in Cryptography - SAC 2019 - Kenneth G. Paterson 2020-01-09

This book contains revised selected papers from the 26th International Conference on Selected Areas in Cryptography, SAC 2019, held in Waterloo, ON, Canada, in August 2019. The 26 full papers presented in this volume were carefully reviewed and selected from 74 submissions. They cover the following research areas: Design and analysis of symmetric key primitives and cryptosystems, including block and stream ciphers, hash functions, MAC algorithms, and authenticated encryption schemes, efficient implementations of symmetric and public key algorithms, mathematical and algorithmic aspects of applied cryptology, cryptography for the Internet of Things.

Cyber Security - M. U. Bokhari 2018-04-27

This book comprises select proceedings of the annual convention of the Computer Society of India. Divided

into 10 topical volumes, the proceedings present papers on state-of-the-art research, surveys, and succinct reviews. The volume covers diverse topics ranging from information security to cryptography and from encryption to intrusion detection. This book focuses on Cyber Security. It aims at informing the readers about the technology in general and the internet in particular. The book uncovers the various nuances of information security, cyber security and its various dimensions. This book also covers latest security trends, ways to combat cyber threats including the detection and mitigation of security threats and risks. The contents of this book will prove useful to professionals and researchers alike.

Information Security and Cryptology - Dongdai Lin 2015-03-27

This book constitutes the thoroughly refereed post-conference proceedings of the 10th International Conference on Information Security and Cryptology, Inscrypt 2014, held in Beijing, China, in December 2014. The 29 revised full papers presented were carefully reviewed and selected from 93 submissions. The papers are organized in topical sections on privacy and anonymity, multiparty and outsource computation, signature and security protocols, lattice and public key cryptography, block cipher and hash function, authentication and encryption, elliptic curve, and cryptographic primitive and application.

Cryptography with Shrinking Generators - Sara Díaz Cardell 2019-05-02

This book offers a broad survey of all information made public - from 1993 until today - on keystream sequence generators based on irregular decimation, which are referred to as shrinking generators. Starting with an overview of cryptography, it describes each type of generator - shrinking, self-shrinking, modified self-shrinking, generalized self-shrinking and the DECIM algorithm - with examples and references. Further, the book discusses several attacks on these generators and applications. It concludes by demonstrating how the output sequences can be modeled by means of different families of one-dimensional cellular automata, rendering the generators vulnerable to attacks. Intended for researchers and graduate students, the book will hopefully inspire them to search for more details on this family of generators and to address the open problems in this field.

Advances in Cyber Security: Principles, Techniques, and Applications - Kuan-Ching Li 2018-12-06

This book provides state-of-the-art coverage of the principles, techniques, and management of issues in cyber security, including threat attacks, privacy, signature and encryption schemes. One of the most important topics addressed concerns lightweight solutions for public key encryption in resource-constrained environments; the book highlights the latest developments in this area. Authentication is another central issue in cyber security. In this book, we address this aspect and sub-aspects ranging from cryptographic approaches to practical design issues, such as CAPTCHA. Privacy is another main topic that is discussed in detail, from techniques for enhancing privacy to pseudonymous schemes. Addressing key issues in the emerging field of cyber security, this book effectively bridges the gap between computer security and threat attacks, and showcases promising applications involving cryptography and security.

Information Security and Cryptology - ICISC 2004 - Choonsik Park 2005-06

This book constitutes the thoroughly refereed postproceedings of the 7th International Conference on Information Security and Cryptology, ICISC 2004, held in Seoul, Korea in December 2004. The 34 revised full papers presented have gone through two rounds of reviewing and improvement and were selected from 194 submissions. The papers are organized in topical sections on block ciphers and stream ciphers, public key cryptosystems, PKI and related implementations, digital signatures, elliptic curve cryptosystems, provable security and primitives, network security, steganography, and biometrics.

Information and Communications Security - Peng Ning 2006-11-17

This book constitutes the refereed proceedings of the 8th International Conference on Information and Communications Security, ICICS 2006, held in Raleigh, NC, USA, December 2006. The 22 revised full papers and 17 revised short papers cover security protocols, applied cryptography, access control, privacy and malicious code, network security, systems security, cryptanalysis, applied cryptography and network security, and security implementations.

Information Security Practice and Experience - Xinyi Huang 2014-04-28

This book constitutes the proceedings of the 10th International Conference on Information Security Practice and Experience, ISPEC 2014, held in Fuzhou, China, in May 2014. The 36 papers presented in this volume were carefully reviewed and selected from 158 submissions. In addition the book contains 5 invited

papers. The regular papers are organized in topical sections named: network security; system security; security practice; security protocols; cloud security; digital signature; encryption and key agreement and theory.

Cryptography and Coding - Nigel Smart 2005-12-09

This book constitutes the refereed proceedings of the 10th IMA International Conference on Cryptography and Coding, held in Cirencester, UK, in December 2005. The 26 revised full papers presented together with 4 invited contributions were carefully reviewed and selected from 94 submissions. The papers are organized in topical sections on coding theory, signatures and signcryption, symmetric cryptography, side channels, algebraic cryptanalysis, information theoretic applications, number theoretic foundations, and public key and ID-based encryption schemes.

Information Security Applications - Jae-Kwang Lee 2007-05-30

This book constitutes the refereed proceedings of the 7th International Workshop on Information Security Applications, WISA 2006, held in Jeju Island, Korea in August 2006. Coverage in the 30 revised full papers includes public key crypto applications and virus protection, cyber indication and intrusion detection, biometrics and security trust management, secure software and systems, smart cards and secure hardware, and mobile security.

Multidisciplinary Perspectives in Cryptology and Information Security - Sadkhan Al Maliky, Sattar B. 2014-03-31

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.

Classical and Physical Security of Symmetric Key Cryptographic Algorithms - Anubhab Baksi 2022-01-01

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.

Hardware Security and Trust - Nicolas Sklavos 2017-01-11

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.

The 10th International Conference on Computer Engineering and Networks - Qi Liu 2020-10-05

This book contains a collection of the papers accepted by the CENet2020 - the 10th International Conference on Computer Engineering and Networks held on October 16-18, 2020 in Xi'an, China. The topics focus but are not limited to Internet of Things and Smart Systems, Artificial Intelligence and Applications, Communication System Detection, Analysis and Application, and Medical Engineering and Information Systems. Each part can be used as an excellent reference by industry practitioners, university faculties, research fellows and undergraduates as well as graduate students who need to build a knowledge base of the most current advances and state-of-practice in the topics covered by this conference proceedings. This will enable them to produce, maintain, and manage systems with high levels of trustworthiness and complexity.

Applications and Techniques in Information Security - V. S. Shankar Sriram 2019-11-15

This book constitutes the refereed proceedings of the 10th International Conference on Applications and Techniques in Information Security, ATIS 2019, held in Tamil Nadul, India, in November 2019. The 22 full papers and 2 short papers presented in the volume were carefully reviewed and selected from 50 submissions. The papers are organized in the following topical sections: information security; network security; intrusion detection system; authentication and key management system; security centric applications.

Innovative Security Solutions for Information Technology and Communications - Diana Maimut 2021-02-03

This book constitutes the thoroughly refereed post-conference proceedings of the 13th International Conference on Security for Information Technology and Communications, SecITC 2020, held in Bucharest, Romania, in November 2020. The 17 revised full papers presented together with 2 invited talks were carefully reviewed and selected from 41 submissions. The conference covers topics from cryptographic algorithms, to digital forensics and cyber security and much more.

Security, Privacy, and Applied Cryptography Engineering - Lejla Batina 2021-02-27

This book constitutes the refereed proceedings of the 10th International Conference on Security, Privacy, and Applied Cryptography Engineering, SPACE 2020, held in Kolkata, India, in December 2020. Due to COVID-19 pandemic, the conference was held virtual. The 13 full papers presented were carefully reviewed and selected from 48 submissions. This annual event is devoted to various aspects of security, privacy, applied cryptography, and cryptographic engineering. This is a very challenging field, requiring the expertise from diverse domains, ranging from mathematics to solid-state circuit design.

Information Security in Diverse Computing Environments - Kayem, Anne 2014-06-30

"This book provides the latest empirical research and theoretical frameworks in the area of information security, presenting research on developing sufficient security measures for new environments by discussing challenges faced by researchers as well as unconventional solutions to these problems"-- Provided by publisher.